Contrôleurs de sécurité XS/SC26 et SC10-2

Manuel d'instructions

Traduction des instructions d'origine
174868_FR Rev. Z
2024-2-27
© Banner Engineering Corp. Tous droits réservés

ПРОМЭЛЕКТРОНИКА/ sales@prom-elec.com

Sommaire

1 À propos de ce document 6
1.1 Important… À lire attentivement avant de continuer ! 6
1.2 Utilisation des avertissements et des précautions 6
1.3 Déclaration de conformité UE/R.-U. 6
2 Description du produit 8
2.1 Termes utilisés dans ce manuel 8
2.2 Logiciel 8
2.3 Connexions USB 8
2.4 Connexions Ethernet 9
2.5 Logique interne 9
2.6 Mot de passe (Ethernet) ou code PIN (USB) 10
2.7 Carte mémoire SC-XM2/3 et outil de programmation SC-XMP2 10
3 Présentation du XS/SC26 11
3.1 Modèles XS/SC26 11
3.2 Caractéristiques et indicateurs du XS/SC26 12
3.3 Utilisation de contrôleurs de sécurité XS/SC26 avec différents FID 12
3.4 Raccordement des entrées et des sorties 13
3.4.1 Dispositifs d'entrée de sécurité et d'entrée auxiliaire du XS/SC26 13
3.4.2 Sorties de sécurité du XS/SC26 13
3.4.3 Sorties d'état et sorties d'état virtuelles du XS/SC26 14
3.5 Fonction d'optimisation automatique des bornes (ATO) du XS/SC26 15
4 Présentation du SC10-2 17
4.1 Modèles SC10-2 17
4.2 Fonctions et indicateurs du SC10-2 17
4.3 Utilisation de contrôleurs de sécurité SC10-2 avec FID différents 18
4.4 Raccordement des entrées et des sorties 19
4.4.1 Dispositifs d'entrée de sécurité et d'entrée auxiliaire du SC10-2 19
4.4.2 Sorties de relais de sécurité du SC10-2 19
4.4.3 Sorties d'état et sorties d'état virtuelles du SC10-2 19
4.5 Fonction d'optimisation automatique des bornes (ATO) du SC10-2 avec borniers externes (ETB) 19
5 Spécifications et exigences 21
5.1 Spécifications du XS/SC26 21
5.1.1 Contrôleur de base et modules d'extension 21
5.1.2 Contrôleurs de sécurité de base XS26-2, SC26-2 et XS26-ISD 21
5.1.3 Modules de sorties de sécurité électroniques XS2so et XS4so 22
5.1.4 Modules d'entrées de sécurité XS8si et XS16si 23
5.1.5 Modules de relais de sécurité XS1ro et XS2ro 23
5.1.6 Module passerelle de communication EtherCAT XSeCAT 24
5.2 Spécifications du SC10-2 25
5.3 Dimensions 28
5.4 Configuration PC requise 28
6 Installation du système 30
6.1 Installation du logiciel 30
6.2 Installation du contrôleur de sécurité 30
6.2.1 Instructions de montage 30
6.3 Installation électrique 31
7 Considérations relatives à l'installation 32
7.1 Application appropriée 32
7.2 Applications XS/SC26 32
7.3 Applications SC10-2 33
7.4 Dispositifs d'entrée de sécurité 33
7.4.1 Intégrité du circuit de sécurité et principes de circuit de sécurité ISO 13849-1 34
7.4.2 Propriétés des dispositifs d'entrée de sécurité 36
7.5 Options des dispositifs d'entrée de sécurité 38
7.5.1 Niveaux d'intégrité des circuits de sécurité 39
7.5.2 Boutons-poussoirs d'arrêt d'urgence 39
7.5.3 Interrupteur d'arrêt d'urgence à câble 40
7.5.4 Dispositif de commande 41
7.5.5 Arrêt de protection (de sécurité) 41
7.5.6 Porte ou système de protection à verrouillage 41
7.5.7 Capteur optique 42
7.5.8 Commande bimanuelle 42
7.5.9 Tapis de sécurité 45
7.5.10 Capteur d'inhibition 48
7.5.11 Interrupteur de dérivation 49
7.5.12 Fonction AVM (Adjustable Valve Monitoring - surveillance de vanne réglable) 50
7.5.13 Entrées ISD 51
7.5.14 Démarrage d'un cycle pour un bloc fonction Commande de presse 57
7.5.15 Fonction d'arrêt séquentiel de la commande de la presse (SQS) 58
7.5.16 Capteur d'inhibition de la commande de presse 59
7.5.17 Interrupteur au pied 60
7.6 Dispositifs d'entrée auxiliaire 60
7.6.1 Entrée de reset manuel 62
7.7 Dispositifs d'entrée auxiliaire virtuelle 64
7.7.1 Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels 64
7.7.2 Marche/arrêt et Inhibition activée virtuels 67
7.8 Sorties de sécurité 67
7.8.1 Sorties de sécurité électroniques 70

7.8.2 Sorties de relais de sécurité 73
7.8.3 Raccordement EDM et FSD 74
7.9 Sorties d'état 81
7.9.1 Conventions pour les signaux d'état des sorties 81
7.9.2 Fonctions des sorties d'état 82
7.9.3 Fonctions de sortie d'état de la commande de presse 83
7.10 Sorties d'état virtuelles 84
8 Mise en route 86
8.1 Création d'une configuration 86
8.2 Ajout d'entrées et de sorties d'état 86
8.2.1 Ajout d'entrées de sécurité et d'entrées auxiliaires 86
8.2.2 Ajout de sorties d'état 90
8.3 Conception de la logique de contrôle 91
8.4 Enregistrement et confirmation d'une configuration 92
8.4.1 Enregistrement d'une configuration 92
8.4.2 Confirmation d'une configuration 92
8.4.3 Écrivez une configuration confirmée sur la carte SC-XM2/3 avec l'outil de programmation. 94
8.4.4 Remarques sur la confirmation ou l'écriture d'une configuration sur un contrôleur SC10-2 ou XS/SC26 configuré FID 3 ou ultérieur 94
8.5 Exemples de configuration 95
8.5.1 Exemple de configuration du XS/SC26 95
8.5.2 XS/SC26 : Exemple de configuration d'une commande de presse simple avec arrêt d'urgence inhibable 97
8.5.3 XS/SC26 : Exemple de configuration d'une commande de presse avec fonctionnalités complètes 100
9 Connexion au contrôleur de sécurité sur le réseau 104
9.1 Connexion au contrôleur de sécurité 104
9.2 Autorisation du logiciel via le pare-feu Windows 105
9.3 Recherche de contrôleurs de sécurité sur le réseau 106
9.3.1 Recherche manuelle de contrôleurs sur le réseau 108
9.4 Connexion à un contrôleur de sécurité via Ethernet 108
9.5 Reset du système via la connexion Ethernet 109
9.5.1 Changement d'adresse IP 109
9.5.2 Modification de la configuration 110
9.6 Raccourcis 110
10 Logiciel 111
10.1 Abréviations 111
10.2 Présentation du logiciel 112
10.3 Nouveau projet 115
10.4 Paramètres du projet 115
10.5 Onglet Équipement 116
10.6 Onglet Vue fonctionnelle 117
10.6.1 Blocs logiques 118
10.6.2 Blocs fonction 121
10.7 Onglet Schéma de câblage 121
10.8 Onglet Logique Ladder 122
10.9 Onglet ISD 123
10.10 Onglet Ethernet industriel 125
10.10.1 Paramètres réseau : Onglet Base 128
10.10.2 Paramètres réseau : onglet Accès réseau 129
10.10.3 Paramètres réseau : onglet Bus de terrain 129
10.10.4 Création de tags d'API / fichier d'étiquettes 132
10.10.5 EtherNet/IP - Objets assemblés 133
10.11 Onglet Résumé de la configuration 133
10.12 Options d'impression 134
10.13 Gestionnaire des mots de passe 135
10.13.1 Gestionnaire des mots de passe du XS/SC26 135
10.13.2 Gestionnaire des mots de passe du SC10-2 136
10.13.3 Récupération du code PIN ou du mot de passe 136
10.14 Affichage et importation des données du contrôleur 137
10.14.1 Voir le journal de défauts 138
10.14.2 Afficher le journal de configuration 139
10.14.3 Afficher les informations sur le module 139
10.15 Mode temps réel 140
10.16 Mode simulation 142
10.16.1 Mode temporisation 146
10.17 Paramètres 147
10.18 Aide 147
10.19 Signaux de référence 148
11 Descriptions des blocs fonction 150
11.1 Bloc de dérivation 150
11.1.1 Consignations 150
11.2 Bloc de temporisation 151
11.3 Bloc dispositif de commande 152
11.4 Bloc de reset à verrouillage 153
11.5 Bloc d'inhibition 156
11.5.1 Attributs d'inhibition facultatifs 161
11.6 Bloc 1 impulsion 164
11.7 Commande de presse 165
11.7.1 Bloc fonction Mode 167
11.7.2 Bloc fonction Entrées de commande de presse 167
11.7.3 Exemples de bloc fonction de commande de presse 168
11.7.4 Commande en boucle fermée 171
11.8 Bloc Commande bimanuelle (pour XS/SC26 FID 3 et antérieurs et SC10-2 FID 1) 171
11.9 Bloc Commande bimanuelle (XS/SC26 FID 4 et ultérieur et SC10-2 FID 2 et ultérieur) 175
12 Interface embarquée du XS/SC26 176
12.1 Mode de configuration du XS/SC26 177
13 Présentation de l'Ethernet industriel (bus de terrain) 179

13.1 Configuration du contrôleur de sécurité 179
13.1.1 Processus Clickset IP 180
13.2 Définitions relatives à l'Ethernet industriel 181
13.3 Récupération des informations du défaut actuel 183
13.4 EtherNet/IP™ 183
13.4.1 Connexion du fichier L5X 183
13.4.2 Connexion du fichier EDS 186
13.4.3 Connexion du module Ethernet générique 195
13.4.4 Entrées du contrôleur de sécurité (sorties de l'API) 201
13.4.5 Sorties du contrôleur de sécurité (entrées vers l'API) 202
13.4.6 Objet Assembly de configuration 215
13.4.7 Exemples de défaut 215
13.4.8 Indicateurs 217
13.4.9 Indicateurs étendus 218
13.4.10 Mots (word) d'état de système ISD 218
13.4.11 Configuration RSLogix5000 (Message explicite) 219
13.4.12 Configuration EIP sur un API Omron 229
13.5 Modbus® TCP 241
13.5.1 Bits d'entrée et de coil 242
13.5.2 Registres d'entrée et de maintien 243
13.6 PLC5, SLC500 et MicroLogix (PCCC) 256
13.6.1 Configuration de l'API 256
13.6.2 Sorties du contrôleur de sécurité (entrées vers l'API) 258
13.6.3 Entrées du contrôleur de sécurité (sorties de l'API) 269
13.6.4 Indicateurs 270
13.6.5 Indicateurs étendus 270
13.7 PROFINET® 271
13.7.1 PROFINET® et contrôleurs de sécurité 271
13.7.2 Fichier GSD (General Station Description) 271
13.7.3 Modèle de données PROFINET® IO 271
13.7.4 Configuration du contrôleur de sécurité pour une connexion PROFINET IO 271
13.7.5 Création d'un fichier XML pour PROFINET 272
13.7.6 Description des modules 273
13.7.7 Instructions de configuration 286
13.8 EtherCAT® 299
13.8.1 EtherCAT® et les contrôleurs de sécurité 299
13.8.2 Fichier d'informations esclave EtherCAT® (ESI) 299
13.8.3 Modèle de données d'E/S EtherCAT® 300
13.8.4 Configuration du contrôleur de sécurité pour une connexion d'E/S EtherCAT® 300
13.8.5 Créer un fichier PLCopenXML pour EtherCAT® pour TwinCAT® 3.0 300
13.8.6 Description des objets de données de processus (PDO) 302
13.8.7 Instructions de configuration 307
13.8.8 Modification du PDO EtherCAT® 308
13.9 ISD : Informations complémentaires 309
13.9.1 ISD : Informations sur la conversion de la distance, tension et température 309
14 Vérification du système 312
14.1 Planning des vérifications requises 312
14.2 Procédure de vérification à la mise en route 312
14.2.1 Vérification du fonctionnement du système 313
14.2.2 Configuration initiale, procédures de vérification à la mise en route et périodiques 313
15 Informations d'état et de fonctionnement 320
15.1 État des LED du XS/SC26 320
15.2 Indicateurs d'état du module d'entrées 321
15.3 LED d'état du module de sorties (électroniques ou relais) 322
15.4 Indicateurs d'état du module de la passerelle de communication EtherCAT® 323
15.5 État des LED du SC10-2 323
15.6 Informations du mode temps réel : logiciel 325
15.7 Informations du mode temps réel : interface embarquée 325
15.8 Verrouillage 325
15.9 Récupération suite à un verrouillage 326
15.10 Option Détection auto ISD 326
15.11 SC10-2 - Utilisation de l'optimisation automatique des bornes 328
15.12 Exemple de configuration du SC10-2 sans optimisation automatique des bornes 330
15.13 Modèles XS/SC26 sans interface embarquée : utilisation de la carte mémoire SC-XM2/3 334
15.14 Modèles XS/SC26 avec interface embarquée : Utilisation de la carte mémoire SC-XM2/3 335
15.14.1 XS/SC26 FID 1 ou FID 2 avec interface embarquée : Utilisation de la carte mémoire SC-XM2/3 336
15.14.2 Contrôleurs XS/SC26 FID 3 à FID 6 avec interface embarquée : Utilisation des modèles SC-XM2/3 337
15.14.3 Contrôleurs XS/SC26 FID 7 et ultérieurs avec interface embarquée : Utilisation de la carte mémoire SC-XM2/3 341
15.15 SC10-2 : Utilisation de la carte mémoire SC-XM3 341
15.16 Réinitialisation des réglages d'usine pour le contrôleur 342
15.17 Réglages d'usine 342
16 Recherche de pannes 344
16.1 Logiciel : recherche de pannes 344
16.2 Logiciel : codes d'erreur 345
16.3 Vérification de l'installation des pilotes 347
16.4 Détection et correction des défauts 349
16.4.1 Tableaux des codes de défaut du XS/SC26 349
16.4.2 Tableau des codes de défaut du SC10-2 354
17 Composants et accessoires 358
17.1 Pièces de rechange et accessoires 358
17.2 Câbles Ethernet 358
17.3 Modules d'interface 358
17.3.1 Contacts reliés mécaniquement 358
18 Assistance et maintenance du produit 359
18.1 Nettoyage 359
18.2 Réparations et service sous garantie 359

18.3 Nous contacter 359
18.4 Garantie limitée de Banner Engineering Corp. 359
18.5 Avis de copyright du logiciel Banner Engineering Corp. 359
19 Normes et réglementations 360
19.1 Normes américaines en vigueur 360
19.2 Réglementations de l'OSHA applicables 360
19.3 Normes européennes et internationales applicables 360
20 Glossaire 362

1 À propos de ce document

1.1 Important… À lire attentivement avant de continuer !

Le concepteur de la machine, l'ingénieur électromécanicien, le constructeur, l'opérateur de la machine et/ou l'électricien chargé de l'entretien sont responsables de la conception et de l'entretien de ce dispositif conformément à toutes les normes et réglementations applicables. Le dispositif ne peut remplir la fonction de protection voulue que s'il est correctement installé, utilisé et entretenu dans le respect des consignes données. Ce manuel fournit des instructions complètes d'installation, de fonctionnement et d'entretien. *Il est vivement recommandé de lire le manuel dans son intégralité pour bien comprendre le fonctionnement, l'installation et l'entretien du produit.* Pour toute question concernant l'application ou l'utilisation du dispositif, contactez Banner Engineering

Pour en savoir plus sur les organismes américains et internationaux responsables des normes d'application des protections et des performances des dispositifs de protection, voir Normes et réglementations à la page 360.

AVERTISSEMENT:

- L'utilisateur est tenu de respecter ces instructions.
- **Le non-respect de ces consignes peut créer une situation potentiellement dangereuse susceptible d'entraîner des blessures graves, voire mortelles.**
- Lire avec attention, bien comprendre et respecter toutes les consignes relatives à ce dispositif.
- Effectuer une étude des risques de l'application de protection propre à la machine. Des consignes quant à la méthodologie à appliquer figurent dans la norme ISO 12100 ou ANSI B11.0.
- Identifier les méthodes et dispositifs de protection adaptés en fonction des résultats de l'étude de risques et les mettre en œuvre conformément à tous les codes et réglementations locales et nationales en vigueur. Référez-vous aux normes ISO 13849-1, ANSI B11.19 et/ou toute autre norme applicable.
- Vérifier que l'ensemble du système de protection (dispositifs d'entrée, systèmes de contrôle et dispositifs de sortie) est correctement configuré et installé, qu'il est opérationnel et fonctionne de la manière prévue selon l'application.
- Revérifier périodiquement, le cas échéant, que l'ensemble du système de protection fonctionne comme prévu.

1.2 Utilisation des avertissements et des précautions

Les précautions et les avertissements utilisés dans ce document sont indiqués par des symboles d'alerte et doivent être suivis pour garantir une utilisation sûre des Contrôleur de sécurité Banner. Le non-respect de ces précautions et avertissements pourrait entraîner des dangers liés à l'utilisation ou au fonctionnement. Les mots de signalement et les symboles d'alerte sont définis comme suit :

Mot de signalement	Définition	Symbole
AVERTISSEMENT:	Le mot **Avertissement** signale les situations potentiellement dangereuses qui, si elles ne sont pas circonscrites, peuvent entraîner des blessures graves ou mortelles.	
PRÉCAUTION:	Le mot **Précaution** signale les situations potentiellement dangereuses qui, si elles ne sont pas circonscrites, peuvent entraîner des blessures légères à modérées.	

Ces indications ont pour but d'informer le concepteur et le fabricant de la machine, l'utilisateur final et le personnel d'entretien des mesures ou précautions à prendre pour éviter toute utilisation inappropriée et tirer le meilleur parti du Contrôleur de sécurité Banner afin de satisfaire les différentes exigences des installations de protection. Il incombe à ces personnes de les lire et de les respecter.

1.3 Déclaration de conformité UE/R.-U.

Banner Engineering Corp. déclare par la présente que ces produits sont conformes aux dispositions des directives et des réglementations répertoriées et que toutes les exigences de santé et de sécurité sont satisfaites. Pour obtenir la déclaration de conformité complète, veuillez consulter le site www.bannerengineering.com.

Produit	Directive
Contrôleur de sécurité programmable SC26-2, contrôleur de sécurité programmable XS26-2, contrôleur de sécurité programmable XS26-ISD, modules de sortie de sécurité électronique XS2so et XS4so, modules d'entrée de sécurité XS8si et XS16si, modules de relais de sécurité XS1ro et XS2ro, module de passerelle de communication EtherCAT XSeCAT et contrôleur de sécurité SC10-2	UE : Directive sur la sécurité des machines 2006/42/CE et directive CEM 2004/108/CE
	Royaume-Uni : Réglementations 2008 sur les machines (sécurité) et réglementations CEM 2016

Représentant dans l'UE : Spiros Lachandidis, Directeur général, **Banner Engineering BV** Park Lane, Culliganlaan 2F bus 3, 1831 Diegem, BELGIQUE

Représentant au Royaume-Uni : Tony Coghlan, Directeur général, **Turck Banner LTD** Blenheim House, Blenheim Court, Wickford, Essex SS11 8YT, Grande-Bretagne

2 Description du produit

Le contrôle de la sécurité est un élément critique et indispensable de tout système de sécurité. En effet, le contrôleur de sécurité garantit 1) l'absence de défaillance de vos mesures de sécurité ou 2) si la défaillance est inévitable, une défaillance prévisible et sûre.

Un contrôleur de sécurité constitue souvent une solution idéale pour le contrôle de la sécurité car il offre plus de fonctionnalités qu'un relais de sécurité, à un coût moindre qu'un API de sécurité. En outre, un contrôleur de sécurité intelligent et extensible peut être étendu selon vos besoins et permet la télésurveillance des systèmes de sécurité de vos machines.

Les contrôleurs de sécurité de Banner Engineering sont des modules faciles à utiliser, configurables et extensibles (modèles XS26) conçus pour surveiller plusieurs dispositifs d'entrée de sécurité et auxiliaire, offrant des fonctions d'arrêt et de démarrage sécurisées pour les machines à mouvement dangereux. Le contrôleur de sécurité peut remplacer plusieurs modules relais de sécurité dans des applications incluant des dispositifs d'entrée de sécurité, notamment des boutons d'arrêt d'urgence, des interrupteurs de verrouillage de sécurité, des barrières immatérielles de sécurité, des commandes bimanuelles, des tapis de sécurité et d'autres dispositifs de protection. Les contrôleurs de sécurité peuvent également être utilisés à la place d'API de sécurité plus volumineux et plus complexes grâce à des modules d'extension d'entrées et/ou de sorties supplémentaires.

L'interface embarquée :

- Permet d'accéder au diagnostic des défauts.
- Permet de lire et d'écrire le fichier de configuration à partir de et sur les cartes SC-XM2 et SC-XM3.
- XS/SC26 : affiche le résumé de la configuration dont les assignations des bornes et les paramètres réseau.

2.1 Termes utilisés dans ce manuel

Les termes suivants sont utilisés dans ce manuel.

Contrôleur de sécurité — Version abrégée faisant référence à tout le système du contrôleur de sécurité XS/SC26 et du SC10-2, tous deux présentés dans ce manuel

Contrôleur de sécurité extensible — Désigne les modèles extensibles

Contrôleur de base — Fait référence au module principal du système du contrôleur de sécurité XS/SC26

Contrôleur de sécurité programmable SC26-2, contrôleur de sécurité programmable XS26-2, contrôleur de sécurité programmable XS26-lSD, modules de sortie de sécurité électronique XS2so et XS4so, modules d'entrée de sécurité XS8si et XS16si, modules relais de sécurité XS1ro et XS2ro, module de passerelle de communication EtherCAT XSeCAT— nom officiel de la ligne de produits XS/SC26

2.2 Logiciel

Le logiciel Contrôleur de sécurité Banner est une application logicielle avec un affichage en temps réel et des outils de diagnostic pouvant servir à :

- Concevoir et modifier des configurations
- Tester la configuration en mode simulation
- Écrire une configuration sur le contrôleur de sécurité
- Lire la configuration actuelle du contrôleur de sécurité
- Afficher des informations en temps réel, par exemple les états des dispositifs
- Afficher des informations sur les défauts

Le logiciel propose des icônes et des symboles de circuit pour faciliter la sélection des propriétés et des dispositifs d'entrée appropriés. Comme les propriétés des différents dispositifs et les relations de commande d'E/S sont définies dans l'onglet **Vue fonctionnelle**, le programme génère automatiquement les schémas de câblage et de logique Ladder correspondants.

Référez-vous à la section Présentation du logiciel à la page 112 pour plus d'informations.

2.3 Connexions USB

Le port micro USB du contrôleur de base et du SC10-2 sert à le connecter au PC (via le câble SC-USB2) et à la carte SC-XM2/3 pour lire et écrire les configurations créées avec le logiciel.

PRÉCAUTION:
- **Risque de retour à la terre imprévu**
- Une intensité importante peut endommager l'ordinateur et/ou le contrôleur de sécurité.
- L'interface USB est implémentée conformément aux normes du secteur et n'est pas isolée du trajet de retour 24 V.
- Il se peut que l'ordinateur et le contrôleur de sécurité fassent partie, par l'intermédiaire du câble USB, d'un trajet de retour à la terre imprévu pour d'autres équipements connectés. Une intensité importante peut endommager l'ordinateur et/ou le contrôleur de sécurité. Pour limiter ce risque, Banner Engineering recommande que seul le câble USB soit connecté à l'ordinateur et que ce dernier soit placé sur une surface non conductrice. Cette recommandation prévoit également la déconnexion de l'alimentation CA d'un ordinateur portable chaque fois que cela est possible.
- L'interface USB sert au téléchargement des configurations et à une surveillance ou à un dépannage temporaire. Elle n'est pas conçue pour une utilisation continue en tant que port de maintenance.

2.4 Connexions Ethernet

Les connexions Ethernet sont effectuées à l'aide d'un câble Ethernet connecté à partir du port Ethernet du contrôleur de sécurité de base (modèles compatibles Ethernet uniquement), des deux ports de la passerelle de communication XSeCAT ou du SC10-2 à un commutateur réseau ou au dispositif de commande ou de surveillance. Le contrôleur de sécurité fonctionne avec des câbles Ethernet standards ou croisés. Un câble blindé est parfois nécessaire dans les environnements parasités.

Remarque: Le câble Ethernet transférant les données de communication vers la passerelle de communication XSeCAT (c.-à-d. depuis l'API, autrement dit en amont) doit être connecté à ECAT IN en haut du module. Le câble Ethernet transférant les données de communication depuis la passerelle de communication XSeCAT (c.-à-d. vers l'API, autrement dit en aval) doit être connecté à ECAT OUT en bas du module.

Le port Ethernet peut également être utilisé pour se connecter à un PC avec le logiciel Contrôleur de sécurité Banner. Cette fonction n'est disponible que sur les modèles de contrôleur de sécurité XS/SC26 FID7 ou ultérieur compatibles Ethernet.

2.5 Logique interne

La logique interne du contrôleur de sécurité est conçue pour qu'une sortie de sécurité ne puisse s'activer que si tous les signaux du dispositif d'entrée de sécurité qui la contrôlent et les signaux d'auto-vérification du contrôleur de sécurité sont en état marche (Run) et indiquent qu'il n'y a pas d'erreur.

Le logiciel Contrôleur de sécurité Banner utilise les blocs fonction de sécurité et logiques pour configurer des installations simples et plus complexes.

Les blocs logiques sont basés sur la logique booléenne (vrai ou faux). Les blocs logiques suivants sont disponibles :
- NOT (NON)
- AND (ET)
- OR (OU)
- NAND (NON-ET)
- NOR (NON-OU)
- XOR (OU exclusif)
- Bascule (définir et réinitialiser la priorité)

Référez-vous à la section Blocs logiques à la page 118 pour en savoir plus.

Les blocs fonction sont des blocs préprogrammés avec une logique intégrée qui permettent de sélectionner divers attributs pour répondre aux besoins des installations normales et complexes. Les blocs fonction suivants sont disponibles :
- Bloc de dérivation
- Bloc de temporisation (XS/SC26 FID 2 ou ultérieur et SC10-2)
- Bloc dispositif de commande
- Bloc de reset à verrouillage
- Bloc d'inhibition
- Bloc de commande bimanuelle
- Bloc 1 impulsion (XS/SC26 FID 4 ou ultérieur)
- Bloc Commande de presse (XS/SC26 FID 4 ou ultérieur)

Référez-vous à la section Blocs fonction à la page 121 pour en savoir plus.

2.6 Mot de passe (Ethernet) ou code PIN (USB)

Pour confirmer et écrire la configuration sur le contrôleur de sécurité et accéder au gestionnaire de mots de passe via le logiciel, vous avez besoin d'un mot de passe si la connexion se fait via un port Ethernet (contrôleur de sécurité XS/SC26 FID7 ou ultérieur uniquement) ou d'un code PIN si la connexion se fait via un port USB.

Voir Gestionnaire des mots de passe du XS/SC26 à la page 135 et Gestionnaire des mots de passe du SC10-2 à la page 136 pour plus d'informations.

2.7 Carte mémoire SC-XM2/3 et outil de programmation SC-XMP2

Utilisez les cartes SC-XM2 et SC-XM3 pour enregistrer une configuration **confirmée**.

Outil de programmation **XS/SC26 :** La configuration peut être écrite directement par le contrôleur de sécurité, lorsque la carte est branchée au port micro-USB (voir Mode de configuration du XS/SC26 à la page 177) ou via l'outil de programmation SC-XMP2 en utilisant uniquement le logiciel sans devoir brancher le contrôleur de sécurité.

Important: Assurez-vous que la configuration importée vers le contrôleur de sécurité est bien la configuration appropriée (via le logiciel ou en vérifiant la configuration indiquée sur l'étiquette blanche de la carte SC-XM2/3).

Cliquez sur pour accéder aux options de l'outil de programmation :

- **Lire** — Lit la configuration actuelle du contrôleur de sécurité à partir de la carte SC-XM2/3 et la charge dans le logiciel
- **Écrire** — Écrit une configuration confirmée du logiciel sur la carte SC-XM2/3
- **Verrouiller** — Verrouille la carte SC-XM2/3 pour empêcher l'écriture de configurations sur celle-ci (une carte vide ne peut pas être verrouillée)

Remarque: Vous ne pourrez pas déverrouiller la carte SC-XM2/3 après l'avoir verrouillée.

Important: Pour un contrôleur de sécurité dont l'option Configuration via le réseau ou Surveillance en temps réel via le réseau est activée (FID 7 ou supérieur), l'utilisation d'une carte SC-XM2/3 créée avant la version 5.0 du logiciel Contrôleur de sécurité Banner ou pour un contrôleur avec un FID inférieur à 7 peut entraîner la désactivation de la fonctionnalité Configuration via le réseau ou Surveillance en temps réel via le réseau. Dans ce cas, réactivez l'option Configuration via le réseau ou la Surveillance en temps réel via le réseau à l'aide de la connexion USB.

3 Présentation du XS/SC26

Avec la possibilité d'ajouter jusqu'à huit modules d'extension d'E/S, le contrôleur de sécurité extensible XS26 peut s'adapter à un large éventail de machines, y compris des grandes machines exécutant plusieurs processus.

Illustration 1. Contrôleur de sécurité XS/SC26



- Programmation en quelques minutes à l'aide d'un logiciel de configuration convivial
- Possibilité d'ajout de 8 modules d'extension d'E/S en fonction de l'évolution des besoins d'automatisation
- Choix entre six modèles de module d'extension
- Les modèles de module d'extension proposent un large éventail d'entrées de sécurité, de sorties de sécurité électroniques et de sorties relais de sécurité.
- Affichage et diagnostic en temps réel innovants pour surveiller activement les E/S sur un PC et faciliter le dépannage et la mise en service
- Le contrôleur de sécurité et les modules d'entrée permettent de convertir les entrées de sécurité en sorties d'état et d'optimiser l'utilisation des bornes.
- Les modèles Ethernet peuvent être configurés pour avoir jusqu'à 256 sorties d'état virtuelles
- Carte SC-XM2/3 externe en option pour remplacement et configuration rapide sans PC
- La fonction ISD (In-Series Diagnostics) fournit des données détaillées sur l'état et les performances de chaque dispositif de sécurité connecté, auxquelles il est possible d'accéder à l'aide d'une IHM ou d'un dispositif similaire (modèles XS26-ISD uniquement).
- Configuration et visualisation en temps réel via une connexion Ethernet sur le contrôleur de base extensible

3.1 Modèles XS/SC26

Tous les modules de base, extensibles ou non, possèdent 18 entrées de sécurité, 8 E/S de sécurité convertibles et 2 paires de sorties de sécurité électroniques. Il est possible d'ajouter jusqu'à 8 modules d'extension, avec n'importe quelle combinaison de modules d'entrée et de sortie, aux modèles extensibles du contrôleur de sécurité. Il est possible d'ajouter une passerelle de communication à d'autres modèles extensibles Ethernet FID 6 et ultérieur du contrôleur de base.

Table 1. Modèles de base extensibles

Modèle	Afficheur	Compatible Ethernet	Nbre de voies ISD
XS26-2	Non	Non	0
XS26-2d	Oui	Non	0
XS26-2e	Non	Oui	0
XS26-2de	Oui	Oui	0
XS26-ISDd	Oui	Oui	8

Table 2. Modèles de base non extensibles

Modèle	Afficheur	Compatible Ethernet	Nbre de voies ISD
SC26-2	Non	Non	0
SC26-2d	Oui	Non	0
SC26-2e	Non	Oui	0
SC26-2de	Oui	Oui	0

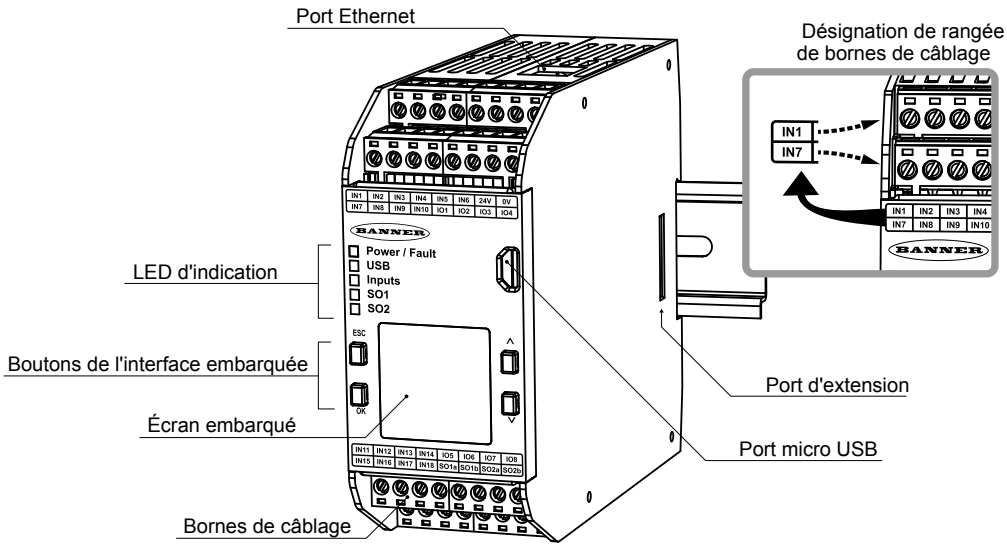
Table 3. Modules d'extension d'E/S

Modèle	Description
XS16si	Module d'entrée de sécurité - 16 entrées (4 convertibles)
XS8si	Module d'entrée de sécurité - 8 entrées (2 convertibles)
XS2so	Module à 2 sorties de sécurité électroniques double voie
XS4so	Module à 4 sorties de sécurité électroniques double voie
XS1ro	Module à 1 relais de sécurité double voie

Modèle	Description
XS2ro	Module à 2 relais de sécurité double voie
XSeCAT	Passerelle de communication EtherCAT

3.2 Caractéristiques et indicateurs du XS/SC26

Illustration 2. Caractéristiques et indicateurs du XS/SC26



3.3 Utilisation de contrôleurs de sécurité XS/SC26 avec différents FID

Avec le temps, Banner ajoute de nouvelles fonctionnalités à certains dispositifs. Le FID (Feature ID) identifie le jeu de fonctionnalités d'un modèle donné. En général, plus le FID est élevé plus le jeu de fonctionnalités est étendu. Un contrôleur dont le FID est inférieur à celui d'une fonctionnalité donnée ne peut pas prendre en charge une configuration utilisant cette fonctionnalité. Les ensembles de fonctionnalités sont compatibles avec les versions ultérieures, mais ils ne sont pas rétrocompatibles.

Il est possible d'utiliser des contrôleurs de base XS/SC26 avec différents FID au sein d'une même application, mais certaines mesures doivent être prises pour garantir la compatibilité. Consultez l'étiquette latérale sur le module (Illustration 3 à la page 12) ou accédez aux informations du contrôleur de base pour déterminer le FID d'un dispositif donné. Pour vous assurer de disposer d'un fichier de configuration qui s'applique à des dispositifs avec différents FID, créez des configurations sans utiliser les fonctionnalités répertoriées dans le tableau suivant. Confirmez toutes les configurations après leur chargement pour vous assurer qu'elles sont correctes.

Illustration 3. Exemple d'étiquette

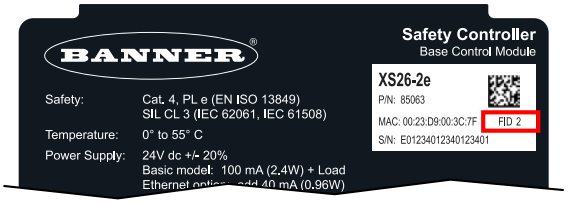


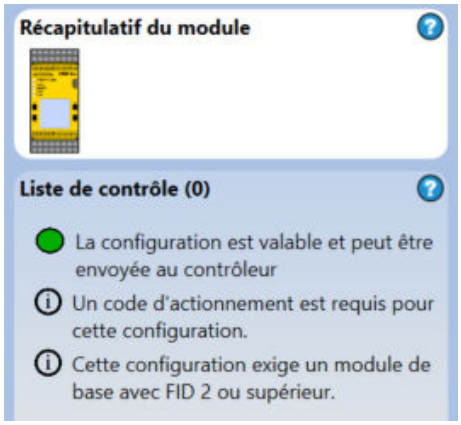
Table 4. Description des FID

Numéro FID	Ensemble de fonctionnalités ajoutées
FID 1	Ensemble de fonctionnalités initiales
FID 2	PROFINET®, entrées auxiliaires virtuelles, blocs de temporisation, sortie d'état du bloc fonction de suivi et prise en charge de 256 sorties d'état virtuelles au lieu de 64
FID 3	Fonctionnalités d'usine, transfert vers SC-XM3

Numéro FID	Ensemble de fonctionnalités ajoutées
FID 4	Bloc de commande de presse hydraulique/pneumatique, possibilité d'exécuter une logique OR sur les entrées de reset, bloc de temporisation 1 impulsion et paramétrage d'une sortie d'état physique de sorte qu'il soit possible de l'activer/désactiver
FID 5	Modèles XS26-ISD commercialisés qui ont ajouté la possibilité de convertir directement les informations de diagnostic en série de 8 chaînes ISD au format des protocoles USB (à l'aide du logiciel) et Ethernet industriel.
FID 6	Passerelle de communication XSeCAT commercialisée à utiliser avec des communications EtherCAT®.
FID 7	Possibilité de communiquer avec un contrôleur à l'aide du logiciel Contrôleur de sécurité Banner via le port Ethernet.

La liste de contrôle du logiciel Contrôleur de sécurité Banner affiche un avertissement lorsqu'une fonctionnalité ajoutée exige un contrôleur de sécurité équipé d'un micrologiciel d'une version autre que celle d'un contrôleur de sécurité FID 1.

Illustration 4. Exemple d'avertissement affiché dans la liste de contrôle



Remarque: Les modules d'extension sont FID 1. Ils peuvent exécuter la plupart des fonctionnalités car elles sont contrôlées par le contrôleur de base.

3.4 Raccordement des entrées et des sorties

3.4.1 Dispositifs d'entrée de sécurité et d'entrée auxiliaire du XS/SC26

Le contrôleur de base dispose de 26 bornes d'entrée qui peuvent être utilisées pour surveiller des dispositifs d'entrée de sécurité ou d'entrée auxiliaire. Ces dispositifs peuvent intégrer des sorties transistorisées ou à contacts. Certaines bornes d'entrée peuvent être configurées pour fournir 24 Vcc afin de surveiller les contacts ou pour communiquer l'état d'une entrée ou d'une sortie. La fonction de chaque circuit d'entrée dépend du type de dispositif qui lui est raccordé. Cette fonction est définie lors de la configuration du contrôleur.

Le contrôleur de base FID 2 et ultérieur prend également en charge les entrées auxiliaires virtuelles.

Certaines bornes d'entrée des modèles XS26-ISD peuvent être configurées pour surveiller une chaîne de dispositifs ISD ; cette fonctionnalité est établie pendant la configuration du contrôleur.

Les modules d'extension XS8si et XS16si ajoutent des entrées supplémentaires au système de contrôle de sécurité.

Contactez Banner Engineering pour en savoir plus sur le raccordement d'autres dispositifs non répertoriés dans ce manuel.

3.4.2 Sorties de sécurité du XS/SC26

Les sorties de sécurité sont conçues pour contrôler les FSD (dispositifs de commutation finaux) et les MPCE (éléments de contrôle primaire de la machine) qui représentent les derniers éléments (d'un point de vue temporel) contrôlant le mouvement dangereux. Ces éléments de contrôle incluent des relais, des contacteurs, des solénoïdes, des commandes de moteur et d'autres dispositifs intégrant généralement des contacts de surveillance à guidage forcé (reliés mécaniquement) ou des signaux électriques nécessaires à la surveillance des commutateurs externes (EDM).

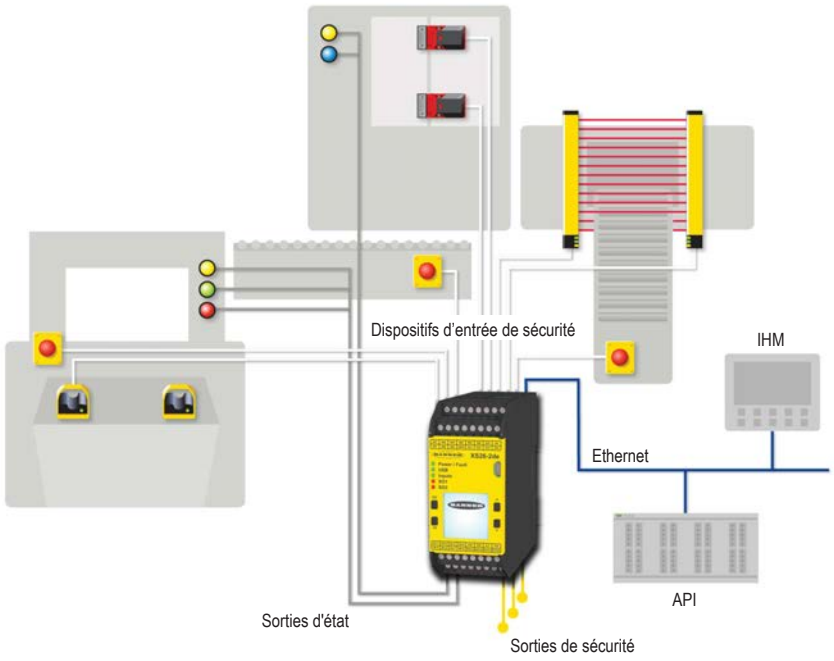
Le contrôleur de sécurité possède deux sorties de sécurité électroniques redondantes et contrôlées de façon indépendante (bornes SO1a & SO1b, et SO2a & SO2b). L'algorithme d'auto-vérification du contrôleur de sécurité s'assure que les sorties s'activent et se désactivent au moment opportun, en réponse aux signaux d'entrée assignés.

Les deux sorties de sécurité électroniques sont conçues pour fonctionner par paire ou en tant que sorties individuelles. Lorsqu'elles sont contrôlées par paire, les sorties de sécurité sont adaptées aux installations de catégorie 4. Si elles fonctionnent indépendamment l'une de l'autre, elles conviennent aux installations de catégorie 3 maximum si l'exclusion de défauts appropriée a été implémentée (voir le point *Commande à une voie* dans Circuits d'arrêt de sécurité (de protection) à la page 77 et Intégrité du circuit de sécurité et principes de circuit de sécurité ISO 13849-1 à la page 34). Voir Sorties de sécurité à la page 67 pour plus d'informations sur le raccordement, les sorties de relais de sécurité et électroniques, les circuits d'arrêt de sécurité simple et double voie et la configuration des sorties de sécurité.

Il est possible d'ajouter des sorties de relais de sécurité ou électroniques aux modèles extensibles (XS26) du contrôleur de base en intégrant des modules d'extension des sorties (XS2so, XS4so, XS1ro et XS2ro). Il est possible d'ajouter jusqu'à 8 modules d'extension, avec n'importe quelle combinaison de modules d'entrée et de sortie.

Les sorties de sécurité peuvent être contrôlées par des dispositifs d'entrée qui disposent d'un reset automatique comme d'un reset manuel.

Illustration 5. Sorties de sécurité (exemple d'application)



Arrêts fonctionnels selon les normes IEC 60204-1 et NFPA 79

Le contrôleur de sécurité est capable d'effectuer les deux types d'arrêts fonctionnels suivants :

- Catégorie 0 : arrêt non contrôlé avec coupure immédiate de l'alimentation électrique de la machine protégée
- Catégorie 1 : arrêt contrôlé avec temporisation avant coupure de l'alimentation électrique de la machine protégée

Les arrêts temporisés peuvent être utilisés dans des cas où la machine a besoin de son alimentation électrique pour arrêter le mouvement dangereux.

3.4.3 Sorties d'état et sorties d'état virtuelles du XS/SC26

Le contrôleur de base possède huit E/S convertibles (**IOx**) qui peuvent être utilisées comme sorties d'état et peuvent envoyer des signaux d'état non liés à la sécurité à des dispositifs tels que des contrôleurs logiques programmables (API) ou des voyants lumineux. En outre, n'importe quelle borne de sortie de sécurité inutilisée peut être configurée pour effectuer une fonction de sortie d'état en offrant l'avantage d'une intensité plus élevée (voir la section Spécifications du XS/SC26 à la page 21 pour plus d'informations). Pour les sorties de sécurité électroniques configurées comme sorties d'état, les impulsions de test de sécurité restent activées même si elles sont configurées comme des sorties d'état. La convention du signal de sortie d'état peut être configurée sur 24 Vcc ou 0 Vcc, ou pour l'activation/désactivation. Référez-vous à la section Conventions pour les signaux d'état des sorties à la page 81 pour en savoir plus sur les fonctions spécifiques d'une sortie d'état.

Pour les modèles Ethernet, il est possible d'utiliser le logiciel pour configurer jusqu'à 64 sorties d'état virtuelles sur les contrôleurs de sécurité XS/SC26 FID 1 et jusqu'à 256 sorties d'état virtuelles sur les contrôleurs de sécurité XS/SC26 FID 2. Ces sorties peuvent communiquer les mêmes informations que les sorties d'état sur le réseau. Référez-vous à la section Sorties d'état virtuelles à la page 84 pour en savoir plus.

AVERTISSEMENT:

- **Les sorties d'état et les sorties d'état virtuelles ne sont pas des sorties de sécurité et peuvent présenter des défaillances à l'état ON ou OFF.**
- Si une sortie d'état ou une sortie d'état virtuelle est utilisée pour commander une telle application, une défaillance pourrait se produire et constituerait un danger, susceptible de provoquer des blessures graves, voire mortelles.
- N'utilisez jamais une sortie d'état ou une sortie d'état virtuelle pour contrôler des applications de sécurité critiques.

3.5 Fonction d'optimisation automatique des bornes (ATO) du XS/SC26

L'optimisation automatique des bornes (ATO) est une caractéristique standard de tous les modèles XS/SC26. Cette fonction combine automatiquement jusqu'à deux bornes d'E/S pour deux dispositifs qui nécessitent des impulsions de test +24 V depuis le contrôleur de sécurité. Le cas échéant, le logiciel le fait automatiquement pour chaque paire de dispositifs ajoutés, jusqu'à ce qu'il n'y ait plus de bornes d'E/S disponibles. Le partage est limité à deux car les bornes à vis peuvent accepter deux fils maximum.

Le cas échéant, il est possible de réassigner manuellement les bornes dans la fenêtre **Propriétés** des dispositifs.

Les figures suivantes illustrent l'optimisation des bornes pour deux interrupteurs de porte par la fonction ATO du XS/SC26. Au total, six bornes sont utilisées au lieu de huit si la fonction ATO n'est pas utilisée. Le premier interrupteur de porte (GS1) est ajouté. Il s'agit d'un interrupteur 4 fils double voie qui nécessite deux sorties à impulsion indépendantes +24 V du contrôleur de sécurité. IO1 est assignée en tant qu'impulsion de test +24 V 1 qui passe par la voie 1 de GS1 jusqu'à IN1. IO2 est assignée en tant qu'impulsion de test +24 V 2 qui passe par la voie 2 de GS1 jusqu'à IN2. Lorsque le deuxième interrupteur de porte GS2 est ajouté, il utilise aussi IO1 et IO2 mais utilise IN3 et IN4 pour surveiller ses deux voies.

Illustration 6. Partage de IO1 et IO2 par GS1 et GS2

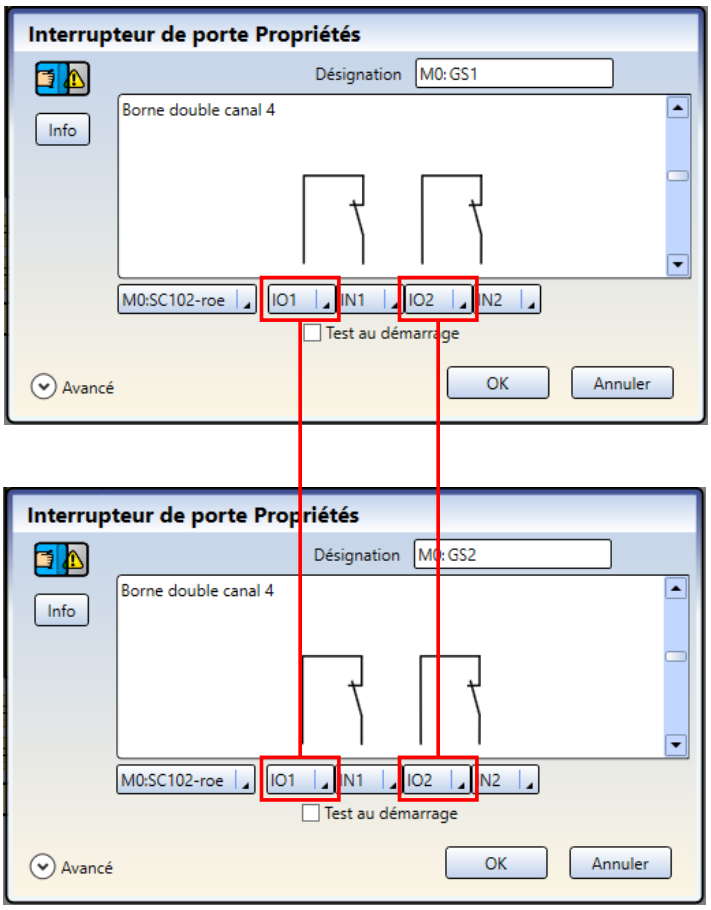
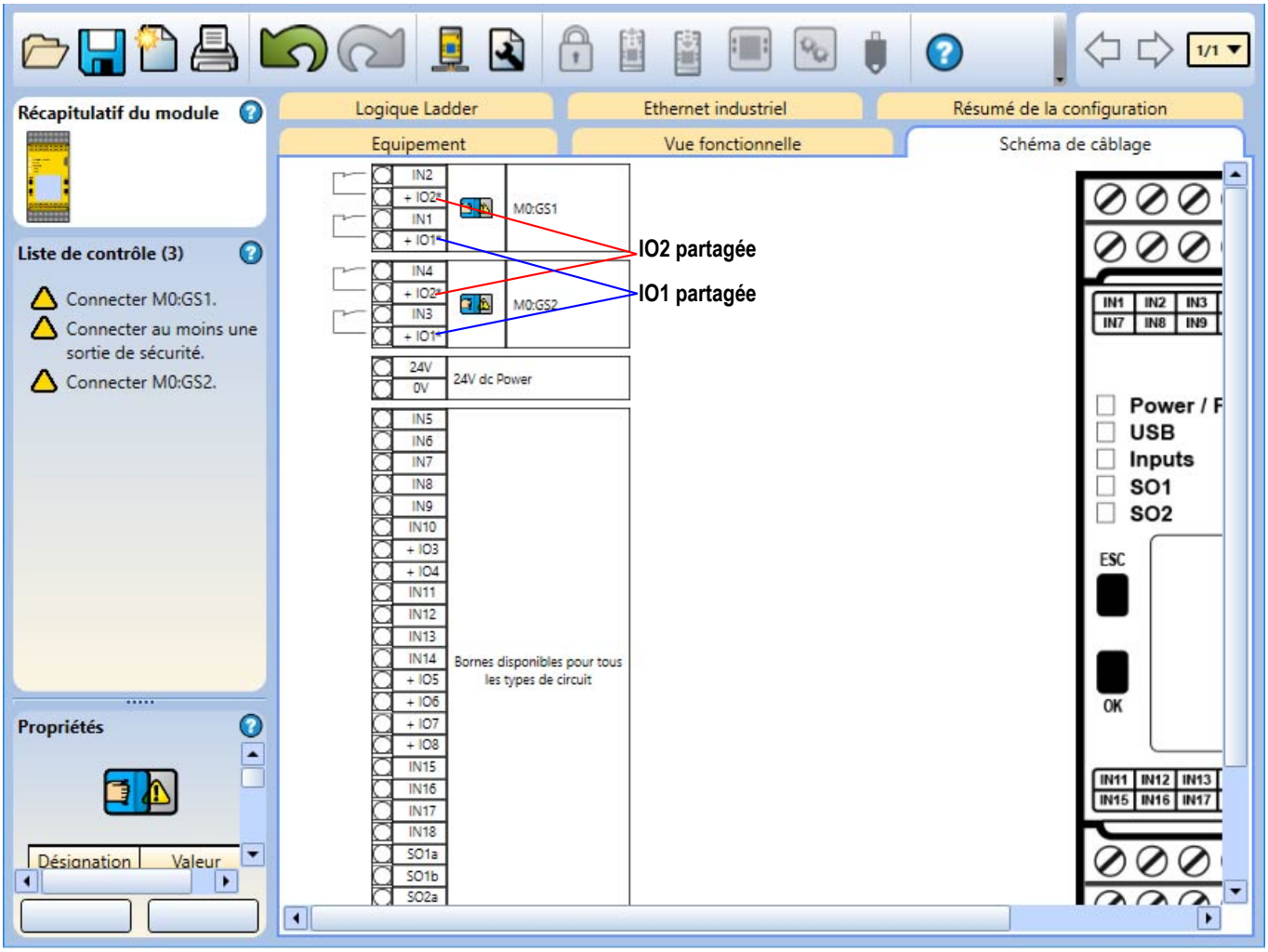


*Illustration 7. Onglet **Schéma de câblage** avec les E/S partagées*



4 Présentation du SC10-2

Illustration 8. Contrôleur de sécurité SC10-2



Le contrôleur relais de sécurité configurable SC10-2 est une solution alternative économique et conviviale aux modules relais de sécurité. Il remplace les fonctionnalités de deux modules relais de sécurité indépendants tout en offrant les possibilités de configuration, la simplicité et les fonctions de diagnostic avancées proposées par le reste de la gamme de contrôleurs de sécurité Banner Engineering.

- La fonction ISD (In-Series Diagnostics) fournit des données détaillées sur l'état et les performances de chaque dispositif de sécurité connecté, auxquelles il est possible d'accéder à l'aide d'une IHM ou d'un dispositif similaire.
- Une programmation intuitive, basée sur des icônes, et une configuration PC par glisser-déposer simplifient l'installation et la gestion du contrôleur
- Le système prend en charge une large gamme de dispositifs de sécurité, ce qui évite d'acheter et de stocker des modules relais de sécurité dédiés à des dispositifs de sécurité spécifiques.
- Deux sorties relais de sécurité de 6 A, chacune avec trois groupes de contacts normalement ouverts (N.O.).
- Dix entrées, dont quatre à utiliser comme sorties auxiliaires
- Optimisation automatique des bornes (ATO) pour bénéficier de 14 entrées au lieu de 10
- Communication Ethernet industriel bidirectionnelle
  - 256 sorties d'état auxiliaires virtuelles
  - 80 entrées auxiliaires virtuelles (reset, ON/OFF, annulation de la temporisation d'arrêt, activation de l'inhibition)
- Carte SC-XM3 externe en option pour remplacement et configuration rapide sans PC (voir SC10-2 : Utilisation de la carte mémoire SC-XM3 à la page 341)

4.1 Modèles SC10-2

Modèle	Description
SC10-2roe	Contrôleur relais de sécurité configurable - 10 entrées (4 convertibles), 2 sorties relais de sécurité 3 voies, Ethernet industriel

4.2 Fonctions et indicateurs du SC10-2

Les points de raccordement sont des bornes débrochables à ressort.

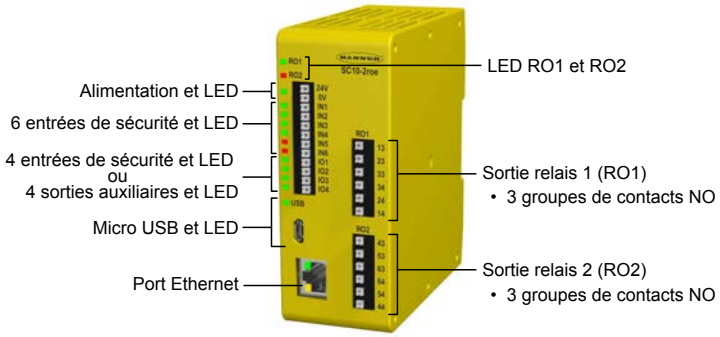
Taille du fil : 24 à 14 AWG, 0,2 mm² à 2,08 mm²

Important: Les bornes à pinces ne sont conçues que pour un seul fil. Si plusieurs fils sont raccordés à une borne, un des fils peut se desserrer ou se déconnecter de la borne, provoquant un court-circuit.

Utilisez un fil torsadé ou un fil avec ferrule. Les fils étamés ne sont pas recommandés.

Après avoir inséré le fil dans la borne, tirez sur le fil pour vérifier s'il ne bouge pas. Dans le cas contraire, envisagez une autre solution de câblage.

Illustration 9. Caractéristiques et indicateurs



4.3 Utilisation de contrôleurs de sécurité SC10-2 avec FID différents

Avec le temps, Banner ajoute de nouvelles fonctionnalités à certains dispositifs. Le FID (Feature ID) identifie le jeu de fonctionnalités d'un modèle donné. En général, plus le FID est élevé plus le jeu de fonctionnalités est étendu. Un contrôleur dont le FID est inférieur à celui d'une fonctionnalité donnée ne peut pas prendre en charge une configuration utilisant cette fonctionnalité. Les ensembles de fonctionnalités sont compatibles avec les versions ultérieures, mais ils ne sont pas rétrocompatibles.

Illustration 10. Exemple d'étiquette SC10-2

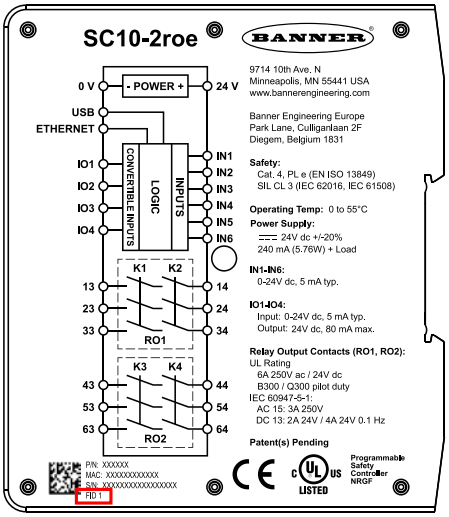
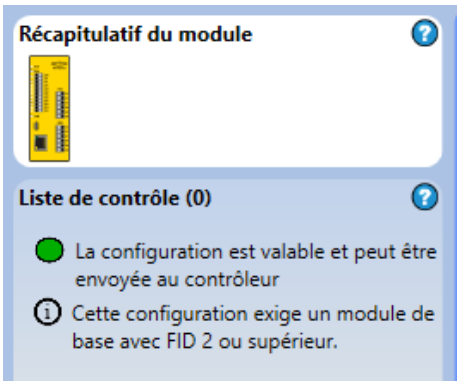


Table 5. Description des FID

Numéro FID	Ensemble de fonctionnalités ajoutées
FID 1	Ensemble de fonctionnalités initiales
FID 2	Nouvelle possibilité de convertir directement les informations de diagnostic en série au format des protocoles USB (à l'aide du logiciel) et Ethernet industriel.

La liste de contrôle du logiciel Contrôleur de sécurité Banner affiche un avertissement lorsqu'une fonctionnalité ajoutée exige un contrôleur de sécurité équipé d'un micrologiciel d'une version autre que celle d'un contrôleur de sécurité FID 1.

Illustration 11. Exemple d'avertissement affiché dans la liste de contrôle



4.4 Raccordement des entrées et des sorties

4.4.1 Dispositifs d'entrée de sécurité et d'entrée auxiliaire du SC10-2

Le contrôleur SC10-2 dispose de 10 bornes d'entrée qui peuvent être utilisées pour surveiller des dispositifs d'entrée de sécurité ou d'entrée auxiliaire. Ces dispositifs peuvent intégrer des sorties électroniques ou à contacts.

Certaines bornes d'entrée peuvent être configurées pour fournir 24 Vcc afin de surveiller les contacts ou pour communiquer l'état d'une entrée ou d'une sortie. La fonction de chaque circuit d'entrée dépend du type de dispositif qui lui est raccordé. Cette fonction est définie lors de la configuration du contrôleur.

4.4.2 Sorties de relais de sécurité du SC10-2

Le SC10-2 possède deux sorties de relais de sécurité normalement ouvertes (N.O.) à trois voies.

Les sorties de sécurité sont conçues pour contrôler les FSD (dispositifs de commutation finaux) et les MPCE (éléments de contrôle primaire de la machine) qui représentent les derniers éléments (d'un point de vue temporel) contrôlant le mouvement dangereux. Ces éléments de contrôle incluent des relais, des contacteurs, des solénoïdes, des commandes de moteur et d'autres dispositifs intégrant généralement des contacts de surveillance à guidage forcé (reliés mécaniquement) ou des signaux électriques nécessaires à la surveillance des commutateurs externes (EDM).

Arrêts fonctionnels selon les normes IEC 60204-1 et NFPA 79

Le contrôleur de sécurité est capable d'effectuer les deux types d'arrêts fonctionnels suivants :

- Catégorie 0 : arrêt non contrôlé avec coupure immédiate de l'alimentation électrique de la machine protégée
- Catégorie 1 : arrêt contrôlé avec temporisation avant coupure de l'alimentation électrique de la machine protégée

Les arrêts temporisés peuvent être utilisés dans des cas où la machine a besoin de son alimentation électrique pour arrêter le mouvement dangereux.

4.4.3 Sorties d'état et sorties d'état virtuelles du SC10-2

Le logiciel permet de configurer le SC10-2 pour avoir jusqu'à 256 sorties d'état virtuelles afin de communiquer des informations sur le réseau. Ces sorties sont capables d'envoyer des signaux d'état non liés à la sécurité aux dispositifs, par exemple des automates logiques programmables (API) ou des interfaces homme-machine (IHM). Référez-vous à la section Sorties d'état virtuelles à la page 84 pour en savoir plus.

Le SC10-2 possède 4 E/S convertibles (**IOx**) qui peuvent être utilisées comme sorties d'état pour contrôler directement des voyants lumineux ou servir d'entrées câblées aux API. Ces sorties peuvent communiquer les mêmes informations que les sorties d'état virtuelles.

AVERTISSEMENT:

- **Les sorties d'état et les sorties d'état virtuelles ne sont pas des sorties de sécurité et peuvent présenter des défaillances à l'état ON ou OFF.**
- Si une sortie d'état ou une sortie d'état virtuelle est utilisée pour commander une telle application, une défaillance pourrait se produire et constituerait un danger, susceptible de provoquer des blessures graves, voire mortelles.
- N'utilisez jamais une sortie d'état ou une sortie d'état virtuelle pour contrôler des applications de sécurité critiques.

Le SC10-2 FID 2 ou ultérieur peut servir d'interface afin de transmettre des données issues d'une chaîne de dispositifs incorporant des données ISD (In-Series Diagnostic), par exemple les interrupteurs de sécurité SI-RF de Banner, sur le réseau.

4.5 Fonction d'optimisation automatique des bornes (ATO) du SC10-2 avec borniers externes (ETB)

La fonction d'optimisation automatique des bornes (ATO) avec borniers externes (ETB) est une fonction standard de tous les modèles SC10-2 et est activée par défaut.

La fonction ATO peut étendre les 10 bornes du SC10-2 afin d'accepter des entrées supplémentaires en optimisant les bornes et en utilisant des borniers externes. Au fur et à mesure de l'ajout, de la suppression ou de la modification des dispositifs, le logiciel propose automatiquement les assignations optimales des bornes pour limiter le câblage et maximiser l'utilisation des bornes.

ATO est une fonction intelligente qui propose tous les types de dispositifs et options de configuration disponibles au moment de la création d'une configuration. Lorsque toutes les entrées et les bornes d'E/S sont occupées et qu'un autre dispositif est ajouté, ATO recherche les dispositifs qui ont besoin d'une impulsion de test +24 V du contrôleur de sécurité.

Ces dispositifs sont combinés via un bornier externe (ETB) afin de libérer une borne d'E/S. Chaque bornier externe permet à un maximum de trois dispositifs différents de partager un seul signal +24 V d'E/S.

Si vous le souhaitez, vous pouvez désactiver ATO en modifiant les propriétés du SC10-2 dans le logiciel. Les borniers externes restent actifs mais vous devez réassigner manuellement les bornes d'E/S pour optimiser l'utilisation des bornes.

5 Spécifications et exigences

5.1 Spécifications du XS/SC26

5.1.1 Contrôleur de base et modules d'extension

Résistance mécanique

Chocs : 15 *g* pendant 11 ms, demi-sinusoïde, 18 chocs au total (selon IEC 61131-2)
Vibrations : 3,5 mm occasionnelle / 1,75 mm continue de 5 Hz à 9 Hz, 1 *g* occasionnelle et 0,5 *g* continue de 9 Hz à 150 Hz : tous sous 10 cycles de balayage par axe (conformément à la norme IEC 61131-2)

Sécurité

Catégorie 4 PL e (EN ISO 13849)
SIL CL 3 (IEC 62061 et IEC 61508)

Normes de performances du produit

Référez-vous à la section Normes et réglementations à la page 360 pour voir la liste des normes américaines et internationales en vigueur dans le secteur

EMC

Répond ou dépasse toutes les exigences EMC des normes IEC 61131-2, IEC 62061 Annexe E, Tableau E.1 (niveaux d'immunité accrus), IEC 61326-1:2006 et IEC 61326-3-1:2008

Conditions d'utilisation

Température : 0° à +55 °C
Température de stockage: −30° à +65 °C
Humidité : Humidité relative max. de 90% à +50 °C (sans condensation)
Altitude de fonctionnement : 2 000 m maximum selon la norme IEC 61010-1

Indice de protection

NEMA 1 (IEC IP20), à utiliser dans une armoire de niveau NEMA 3 (IEC IP54) ou supérieur

Bornier à vis débrochable

Section des fils : 24 à 12 AWG (0,2 à 3,31 mm²)
Longueur de dénudement des fils : 7 à 8 mm
Couple de serrage : 0,565 Nm

Bornes à pinces amovibles

Important : *les bornes à pinces ne sont conçues que pour un seul fil. Si plusieurs fils sont raccordés à une borne, un des fils peut se desserrer ou se déconnecter de la borne, provoquant un court-circuit. Si plusieurs fils sont nécessaires, il faut utiliser une ferrule ou un bornier externe.*
Section des fils : 24 à 16 AWG (0,2 à 1,31 mm²)
Longueur de dénudement des fils : 8 mm

Important: L'alimentation électrique doit satisfaire les exigences en matière d'alimentation très basse tension avec séparation de protection (SELV, PELV).

5.1.2 Contrôleurs de sécurité de base XS26-2, SC26-2 et XS26-ISD

Alimentation

24 Vcc ± 20 % (ondulation comprise), 100 mA à vide
Modèles Ethernet : ajouter 40 mA
Modèles avec écran d'affichage : ajouter 20 mA
Modèles extensibles : charge maximale du bus 3,6 A

Interface réseau (modèles Ethernet uniquement)

Ethernet 10/100 Base-T/TX, connecteur modulaire RJ45
Négociation auto ou taux manuel et duplex (à sélectionner)
Auto-MDI/MDIX (auto-cross)
Protocoles : [4] EtherNet/IP™ (avec PCCC), Modbus® TCP, PROFINET® (FID 2 ou ultérieur) et EtherCAT® (passerelle XSeCAT requise)
Données : 64 sorties d'état virtuelles configurables sur les contrôleurs de sécurité XS/SC26 FID 1 ou 256 sorties d'état virtuelles sur les contrôleurs de sécurité XS/SC26 FID 2 ou ultérieur ; messages et codes de diagnostic des défauts ; accès au journal des défauts

E/S convertibles

Intensité d'alimentation : 80 mA maximum (protection contre la surintensité)
Impulsions de test : environ 1 ms toutes les 25 à 75 ms

Fonction d'optimisation automatique des bornes

Jusqu'à deux dispositifs

Impulsion de test

Largeur : 200 µs maximum
Fréquence : 200 ms normal

Protection de la sortie

Toutes les sorties transistorisées (de sécurité ou non) sont protégées contre les courts-circuits à 0 V ou 24 V, y compris en cas de surintensité.

Entrées de sécurité (et E/S convertibles si utilisées en tant qu'entrées)

Seuil d'entrée ON : > 15 Vcc (ON garanti), 30 Vcc max.
Seuil d'entrée OFF : < 5 Vcc et < 2 mA, –3 Vcc min.
Intensité d'entrée ON : 5 mA normalement sous 24 Vcc, intensité de pointe de nettoyage de contact 50 mA sous 24 Vcc
Résistance du fil d'entrée : 300 Ω max. (150 Ω par fil)
Exigences d'entrée pour un tapis de sécurité à 4 fils :
· Capacité max. entre les plaques : 0,22 µF
· Capacité max. entre la plaque et la terre : 0,22 µF
· Résistance max. entre les deux bornes d'entrée d'une plaque : 20 Ω

Sorties de sécurité électroniques

0,5 A max. sous 24 Vcc (1 Vcc max. de chute), 1 A max. d'appel
Seuil de sortie OFF : 1,7 Vcc normal (2 Vcc max.)
Courant de fuite de la sortie : 50 µA max. avec 0 V ouvert
Charge : 0,1 µF max., 1 H max., 10 ohm max. par fil

Temps de réponse et de réaction

Temps de réponse entrée - sortie (de l'arrêt de l'entrée à la désactivation de la sortie) : voir l'onglet Résumé de la configuration dans le logiciel dès lors qu'il peut varier
Délai de reprise de l'entrée (entre l'arrêt et la reprise du fonctionnement) : Retard à l'enclenchement de plus 250 ms (normal) (400 ms maximum)
Différentiel d'activation sortie xA - sortie xB (utilisées comme paire, non divisées) : 5 ms maximum
Différentiel d'activation sortie X - sortie Y (même entrée, même retard, n'importe quel module) : 3 cycles de lecture + 25 ms maximum
Temporisation d'entrée virtuelle (activation de l'inhibition et marche/arrêt) (FID 2 ou ultérieur) : RPI + 200 ms (normal)
Temporisation d'entrée virtuelle (reset manuel et annulation de temporisation) (FID 2 ou ultérieur) : voir Dispositifs d'entrée auxiliaire virtuelle à la page 64 pour plus de détails

[4] EtherNet/IP™ est une marque commerciale de ODVA, Inc.; Modbus® est une marque déposée de Schneider Electric USA, Inc.; PROFINET® est une marque commerciale de PROFIBUS Nutzerorganisation e.V.; EtherCAT® est une marque déposée et une technologie brevetée, sous licence de Beckhoff Automation GmbH, Allemagne.

Niveau de sécurité

Probabilité de défaillance par heure [1/h] : 1,05 × 10^{-9}
Intervalle de test : 20 ans

Tolérance de retard au déclenchement

La tolérance maximale est le temps de réponse donné dans le résumé de la configuration plus 0,02 %.
La tolérance minimale est le temps de retard au déclenchement moins 0,02 % (en supposant qu'il n'y ait pas de perte de puissance ni de défauts).

Tolérance de retard à l'enclenchement

La tolérance maximale est le retard à l'enclenchement configuré plus 0,02 % plus 250 ms (normal) (400 ms maximum).
La tolérance minimale est le retard à l'enclenchement configuré moins 0,02 %.

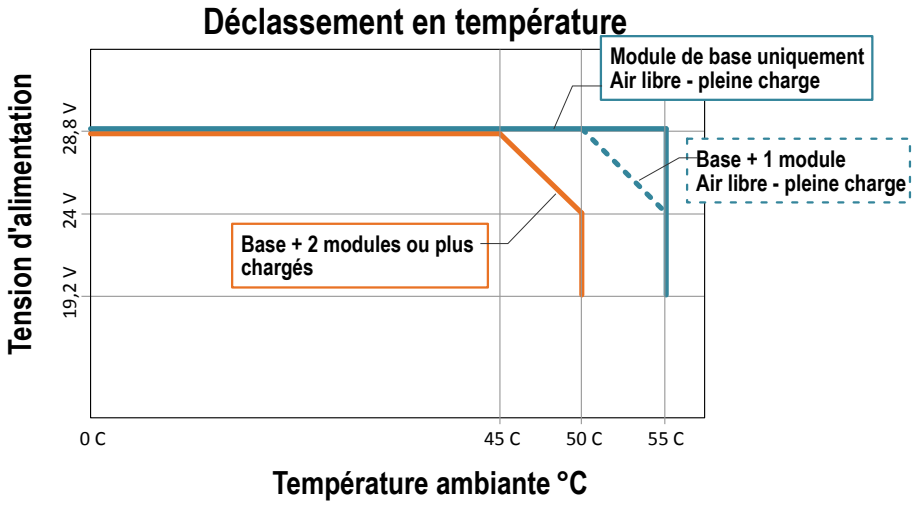
Certifications

Ne s'applique pas au XS26-ISDd.

Banner Engineering BV Park Lane, Culliganlaan 2F bus 3, 1831 Diegem, BELGIQUE

Turck Banner LTD Blenheim House, Blenheim Court, Wickford, Essex SS11 8YT, Grande-Bretagne

Illustration 12. Déclassement en température du XS26-ISD



5.1.3 Modules de sorties de sécurité électroniques XS2so et XS4so

Sorties de sécurité électroniques

XS2so : 0,75 A maximum sous 24 Vcc (1 Vcc maximum de chute)
XS4so : 0,5 A maximum sous 24 Vcc (1 Vcc maximum de chute)
Appel : 2 A maximum
Seuil de sortie OFF : 1,7 Vcc normal (2 Vcc maximum)
Courant de fuite de la sortie : 50 µA maximum avec 0 V ouvert
Charge : 0,1 µF max., 1 H max., 10 Ω maximum par fil

Niveau de sécurité

Probabilité de défaillance par heure [1/h] : 5,8 × 10^{-10}
Intervalle de test : 20 ans

Alimentation externe

XS2so : 24 Vcc ± 20 % (ondulation comprise), 0,075 A à vide, charge maximum 3,075 A
XS4so : 24 Vcc ± 20 % (ondulation comprise), 0,1 A à vide, charge maximum 4,1 A
Retard maximum à la mise sous tension : 5 secondes après le contrôleur de base
Isolation limitée : ± 30 Vcc maximum par rapport au 0 V du contrôleur de base

Alimentation du bus

0,02 A

Impulsion de test

Largeur : 200 µs maximum
Fréquence : 200 ms normal

Protection de la sortie

Toutes les sorties transistorisées (de sécurité ou non) sont protégées contre les courts-circuits à 0 V ou 24 V, y compris en cas de surintensité.

Certifications









Banner Engineering BV Park Lane, Culliganlaan 2F bus 3, 1831 Diegem, BELGIQUE



Turck Banner LTD Blenheim House, Blenheim Court, Wickford, Essex SS11 8YT, Grande-Bretagne

5.1.4 Modules d'entrées de sécurité XS8si et XS16si

E/S convertibles

Intensité d'alimentation : 80 mA max. à une température ambiante de fonctionnement de 55 °C (protection contre la surintensité)
Impulsions de test : environ 1 ms toutes les 25 à 75 ms

Alimentation du bus

XS8si : 0,07 A à vide, charge maximum 0,23 A
XS16si : 0,09 A à vide, charge maximum 0,41 A

Niveau de sécurité

Probabilité de défaillance par heure [1/h] : 4×10^{-10}
Intervalle de test : 20 ans

Entrées de sécurité (et E/S convertibles si utilisées en tant qu'entrées)

Seuil d'entrée On : > 15 Vcc (On garanti), 30 Vcc maximum
Seuil d'entrée Off : < 5 Vcc et < 2 mA, –3 Vcc minimum
Intensité d'entrée On : 5 mA normalement sous 24 Vcc, intensité de pointe de nettoyage de contact 50 mA sous 24 Vcc
Résistance du fil d'entrée : 300 Ω max. (150 Ω par fil)
Exigences d'entrée pour un tapis de sécurité à 4 fils :
· Capacité maximale entre les plaques : 0,22 µF
· Capacité maximale entre la plaque inférieure et la terre : 0,22 µF
· Résistance maximum entre les deux bornes d'entrée d'une plaque : 20 Ω

Protection de la sortie

Les entrées convertibles sont protégées contre les courts-circuits à 0 V ou 24 V, y compris en cas de surintensité.

Certifications









Banner Engineering BV Park Lane, Culliganlaan 2F bus 3, 1831 Diegem, BELGIQUE



Turck Banner LTD Blenheim House, Blenheim Court, Wickford, Essex SS11 8YT, Grande-Bretagne

5.1.5 Modules de relais de sécurité XS1ro et XS2ro

Alimentation du bus

XS1ro : 0,125 A (sorties On)
XS2ro : 0,15 A (sorties On)

Puissance maximale

2 000 VA, 240 W

Durée de vie électrique

50 000 cycles à charge résistive maximale

Catégorie de surtension

III

Niveau de pollution

2

Durée de vie mécanique

40 000 000 cycles

Remarque: La suppression de parasites est recommandée lors de la commutation des charges inductives. Installez des suppresseurs aux bornes de la charge. N'installez jamais de suppresseurs sur les contacts de sortie.

Niveau de sécurité

Probabilité de défaillance par heure [1/h] : $7,6 \times 10^{-10}$
Intervalle de test : 20 ans

Valeurs nominales des contacts

UL/NEMA :

- **Contacts N.O. :** 6 A, 250 Vca / 24 Vcc (charge résistive) ; fonctions de pilotage B300/Q300
- **Contacts N.F. :** 2,5 A, 150 Vca / 24 Vcc (charge résistive) ; fonctions de pilotage Q300

IEC 60947-5-1 :

- **Contacts N.O. :** 6 A, 250 Vca /Vcc continu ; CA 15 : 3 A, 250 V ; CC13 : 1 A, 24 V/4 A, 24 V 0,1 Hz
- **Contacts N.F. :** 2,5 A, 150 Vca /Vcc continu ; CA 15 : 1 A, 150 V ; CC13 : 1 A, 24 V/4 A, 24 V 0,1 Hz

Valeurs B10d

Tension	Intensité	B10d
230 Vca	3 A	300 000
230 Vca	1 A	750 000
24 Vcc	≤ 2 A	1 500 000

Valeurs nominales des contacts pour préserver le plaquage or 5 µm AgNi

	Minimum	Maximum
Tension	100 mVca/cc	60 Vca/cc
Intensité	1 mA	300 mA
Alimentation	1 mW (1 mVA)	7 W (7 VA)

Protection contre la surintensité requise

AVERTISSEMENT: Les raccordements électriques doivent être effectués par du personnel qualifié conformément aux réglementations et codes électriques nationaux et locaux.

Une protection de surintensité doit être fournie par l'installation du produit final, conformément au tableau fourni.
Vous pouvez utiliser un fusible externe ou la limitation de courant pour offrir une protection contre la surtension dans le cas d'une source d'alimentation de classe 2.
Les fils d'alimentation < 24 AWG ne peuvent pas être raccordés.
Pour obtenir un support produit supplémentaire, rendez-vous sur le site www.bannerengineering.com.

Câblage d'alimentation (AWG)	Protection contre la surtension requise (ampères)
20	5
22	3
24	2
26	1
28	0,8
30	0,5

Certifications

Banner Engineering BV Park Lane, Culliganlaan 2F bus 3, 1831 Diegem, BELGIQUE

Turck Banner LTD Blenheim House, Blenheim Court, Wickford, Essex SS11 8YT, Grande-Bretagne

5.1.6 Module passerelle de communication EtherCAT XSeCAT

Interface réseau

EtherCAT® [5]
Taux de transmission des données : 100 Mbits/s, 100 Base-T Autodétection
Type de connexion : Deux connecteurs RJ-45 femelles

Résistance mécanique

Chocs : 15 *g* pendant 11 ms, demi-sinusoïde, 18 chocs au total (selon IEC 61131-2)
Vibrations : 3,5 mm occasionnelle / 1,75 mm continue de 5 Hz à 9 Hz, 1 *g* occasionnelle et 0,5 *g* continue de 9 Hz à 150 Hz : tous sous 10 cycles de balayage par axe (conformément à la norme IEC 61131-2)

Certifications

EMC

Répond ou dépasse toutes les exigences EMC des normes IEC 61131-2, IEC 62061 Annexe E, Tableau E.1 (niveaux d'immunité accrus), IEC 61326-1:2006 et IEC 61326-3-1:2008

Alimentation du bus

0,06 A

Conditions d'utilisation

Température : 0° à +55 °C
Température de stockage: −30° à +65 °C
Humidité : Humidité relative max. de 90% à +50 °C (sans condensation)
Altitude de fonctionnement : 2 000 m maximum selon la norme IEC 61010-1

Indice de protection

NEMA 1 (IEC IP20), à utiliser dans une armoire de niveau NEMA 3 (IEC IP54) ou supérieur

[5] EtherCAT® est une marque déposée et une technologie brevetée, sous licence de Beckhoff Automation GmbH, Allemagne.

5.2 Spécifications du SC10-2

Alimentation

Tension : 24 Vcc ±20 % (SELV)
Intensité :

240 mA maximum, sans charge (relais activés)
530 mA maximum, pleine charge (IO1 à IO4 utilisées comme sorties auxiliaires)

Entrées de sécurité (et E/S convertibles si utilisées en tant qu'entrées)

Seuil d'entrée ON : > 15 Vcc (On garanti), 30 Vcc maximum
Seuil d'entrée OFF : < 5 Vcc et < 2 mA, –3 Vcc minimum
Intensité d'entrée ON : 5 mA normalement sous 24 Vcc, intensité de pointe de nettoyage de contact 50 mA sous 24 Vcc
Résistance du fil d'entrée : 300 Ω maximum (150 Ω par fil)
Exigences d'entrée pour un tapis de sécurité à 4 fils :
· Capacité maximale entre les plaques : 0,22 µF [6]
· Capacité maximale entre la plaque inférieure et la terre : 0,22 µF [6]
· Résistance maximum entre les deux bornes d'entrée d'une plaque : 20 Ω

Temps de réponse et de réaction

Temps de réponse entrée - sortie (de l'arrêt de l'entrée à la désactivation de la sortie) : voir l'onglet Résumé de la configuration dans le logiciel dès lors qu'il peut varier
Délai de reprise de l'entrée (entre l'arrêt et la reprise du fonctionnement) : Retard à l'enclenchement de plus 250 ms (normal) (400 ms maximum)
Temporisation d'entrée virtuelle (activation de l'inhibition et marche/arrêt) : RPI + 200 ms (normal)
Temporisation d'entrée virtuelle (reset manuel et annulation de temporisation) : voir Dispositifs d'entrée auxiliaire virtuelle à la page 64 pour plus de détails

Tolérance de retard au déclenchement

La tolérance maximale est le temps de réponse donné dans le résumé de la configuration plus 0,02 %.
La tolérance minimale est le temps de retard au déclenchement moins 0,02 % (en supposant qu'il n'y ait pas de perte de puissance ni de défauts).

Tolérance de retard à l'enclenchement

La tolérance maximale est le retard à l'enclenchement configuré plus 0,02 % plus 250 ms (normal) (400 ms maximum).
La tolérance minimale est le retard à l'enclenchement configuré moins 0,02 %.

Sorties de sécurité

3 groupes de contacts NO pour chaque voie de sortie (RO1 et RO2). Chaque sortie NO est constituée de deux relais à guidage forcé en série (reliés mécaniquement). RO1 est composée des relais K1 et K2. RO2 est composée des relais K3 et K4.

E/S convertibles

Intensité d'alimentation : 80 mA maximum (protection contre la surintensité)
Impulsions de test : ~1 ms toutes les 25 à 75 ms

Fonction d'optimisation automatique des bornes

Jusqu'à trois dispositifs raccordés avec des borniers fournis par l'utilisateur

Interface réseau

Ethernet 10/100 Base-T/TX, connecteur modulaire RJ45
Négociation auto ou taux manuel et duplex (à sélectionner)
Auto-MDI/MDIX (auto-cross)
Protocoles : [7] EtherNet/IP™ (avec PCCC), Modbus® TCP, et PROFINET®
Données : 256 sorties d'état virtuelles configurables ; codes et messages de diagnostic des défauts ; accès au journal des défauts

Conditions d'utilisation

Température : 0° à +55 °C (voir graphique de déclassement en température)
Température de stockage: −30° à +65 °C
Humidité : Humidité relative max. de 90% à +50 °C (sans condensation)
Altitude de fonctionnement : 2 000 m maximum selon la norme IEC 61010-1

Indice de protection

NEMA 1 (IEC IP20), à utiliser dans une armoire de niveau NEMA 3 (IEC IP54) ou supérieur

Résistance mécanique

Chocs : 15 g pendant 11 ms, demi-sinusoïde, 18 chocs au total (selon IEC 61131-2)
Vibrations : 3,5 mm occasionnelle / 1,75 mm continue de 5 Hz à 9 Hz, 1 g occasionnelle et 0,5 g continue de 9 Hz à 150 Hz : tous sous 10 cycles de balayage par axe (conformément à la norme IEC 61131-2)

[6] Si les tapis de sécurité partagent une E/S convertible, il s'agit de la capacitance totale de tous les tapis partagés.
[7] EtherNet/IP™ est une marque commerciale de ODVA, Inc. Modbus® est une marque déposée de Schneider Electric USA, Inc. PROFINET® est une marque commerciale de PROFIBUS Nutzerorganisation e.V.

Contacts
AgNi + or 0,2 µm

Catégorie de surtension
Tension du contact de relais de sortie de 1 à 150 Vca/cc : catégorie III
Tension du contact de relais de sortie de 151 à 250 Vca/cc : catégorie II (catégorie III avec un dispositif de limitation de la surtension approprié, tel que décrit dans ce document.)

EMC
Répond ou dépasse toutes les exigences EMC en termes d'immunité conformément à la norme IEC 61326-3-1:2012 et en termes d'émissions conformément à la norme CISPR 11:2004 pour les équipements de classe A, groupe 1.

Remarque: La suppression de parasites est recommandée lors de la commutation des charges inductives. Installez des suppresseurs aux bornes de la charge. N'installez jamais de suppresseurs sur les contacts de sortie (voir l'avertissement).

Sécurité
Catégorie 4 PL e (EN ISO 13849)
SIL CL 3 (IEC 62061 et IEC 61508)

Niveau de sécurité
Probabilité de défaillance par heure [1/h] : $5{,}01 \times 10^{-10}$
Intervalle de test : 20 ans

Normes de performances du produit
Référez-vous à la section Normes et réglementations à la page 360 pour voir la liste des normes américaines et internationales en vigueur dans le secteur

Durée de vie mécanique
20 000 000 cycles

Durée de vie électrique
50 000 cycles à charge résistive maximale

Fonctions de pilotage UL
B300 Q300

Bornes débrochables à ressort
Taille du fil : 24 à 14 AWG, 0,2 mm² à 2,08 mm²

Important: Les bornes à pinces ne sont conçues que pour un seul fil. Si plusieurs fils sont raccordés à une borne, un des fils peut se desserrer ou se déconnecter de la borne, provoquant un court-circuit.

Utilisez un fil torsadé ou un fil avec ferrule. Les fils étamés ne sont pas recommandés.

Après avoir inséré le fil dans la borne, tirez sur le fil pour vérifier s'il ne bouge pas. Dans le cas contraire, envisagez une autre solution de câblage.

Valeurs B10d

Tension	Intensité	B10d
230 Vca	2 A	350 000
230 Vca	1 A	1 000 000
24 Vcc	≤ 4 A	10 000 000

Courant des contacts individuels
Consultez le graphique Déclassement en température si plusieurs sorties de contact sont utilisées.

	Minimum	Maximum
Tension	10 Vca/cc	250 Vca / 24 Vcc
Intensité	10 mA ca/cc	6 A
Alimentation	100 mW (100 mVA)	200 W (2000 VA)

Capacité de commutation (IEC 60947-5-1)

CA 15	NO : 250 Vca, 3 A
CC 13	NO : 24 Vcc, 2 A
CC 13 à 0,1 Hz	NO : 24 Vcc, 4 A

Protection contre la surintensité requise

AVERTISSEMENT: Les raccordements électriques doivent être effectués par du personnel qualifié conformément aux réglementations et codes électriques nationaux et locaux.

Une protection de surintensité doit être fournie par l'installation du produit final, conformément au tableau fourni.
Vous pouvez utiliser un fusible externe ou la limitation de courant pour offrir une protection contre la surtension dans le cas d'une source d'alimentation de classe 2.
Les fils d'alimentation < 24 AWG ne peuvent pas être raccordés.
Pour obtenir un support produit supplémentaire, rendez-vous sur le site www.bannerengineering.com.

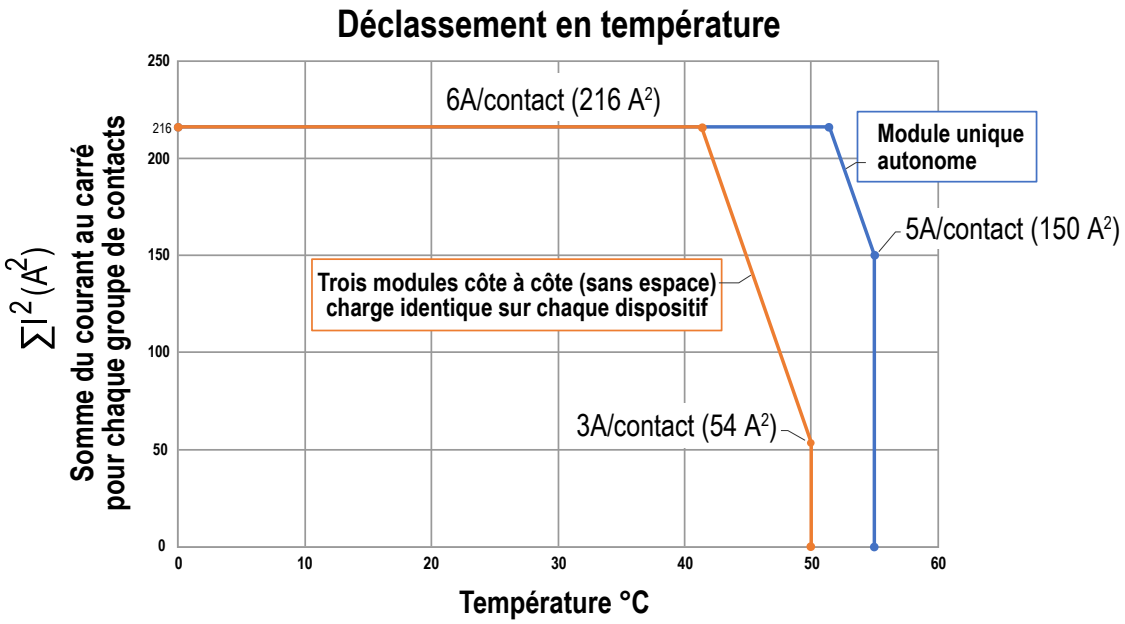
Câblage d'alimentation (AWG)	Protection contre la surtension requise (ampères)
20	5
22	3
24	2
26	1
28	0,8
30	0,5

Certifications

Banner Engineering BV Park Lane, Culliganlaan 2F bus 3, 1831 Diegem, BELGIQUE

Turck Banner LTD Blenheim House, Blenheim Court, Wickford, Essex SS11 8YT, Grande-Bretagne

Illustration 13. SC10-2 Déclassement en température



Exemples de calcul de déclassement en température	
Une seule unité, autonome	**Trois modules**
$\sum I^2 = I_1{}^2 + I_2{}^2 + I_3{}^2 + I_4{}^2 + I_5{}^2 + I_6{}^2$	$\sum I^2 = I_1{}^2 + I_2{}^2 + I_3{}^2 + I_4{}^2 + I_5{}^2 + I_6{}^2$ (les six modules)
I_1 = 4 A (sortie RO1 normalement ouverte voie 1)	I_1 = 4 A
I_2 = 4 A (sortie RO1 normalement ouverte voie 2)	I_2 = 4 A
I_3 = 4 A (sortie RO1 normalement ouverte voie 3)	I_3 = 4 A
I_4 = 4 A (sortie RO2 normalement ouverte voie 4)	I_4 = 4 A
I_5 = 4 A (sortie RO2 normalement ouverte voie 5)	I_5 = 4 A
I_6 = 4 A (sortie RO2 normalement ouverte voie 6)	I_6 = 4 A
$\sum I^2 = 4^2 + 4^2 + 4^2 + 4^2 + 4^2 + 4^2 = 96\ A^2$	$\sum I^2 = 4^2 + 4^2 + 4^2 + 4^2 + 4^2 + 4^2 = 96\ A^2$
T_{max} = 55 °C	T_{max} = 46 °C

5.3 Dimensions

Toutes les mesures sont indiquées en millimètres, sauf indication contraire.

Illustration 14. Dimensions du contrôleur de base XS/SC26

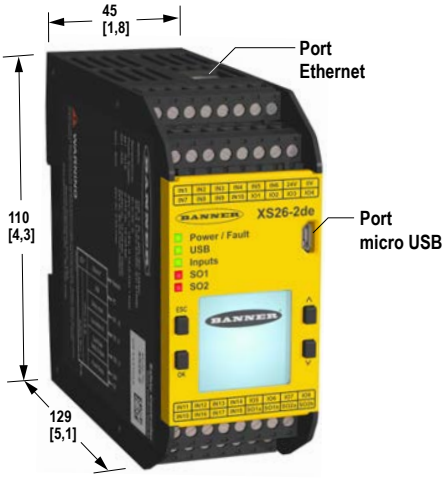


Illustration 15. Dimensions du module d'extension

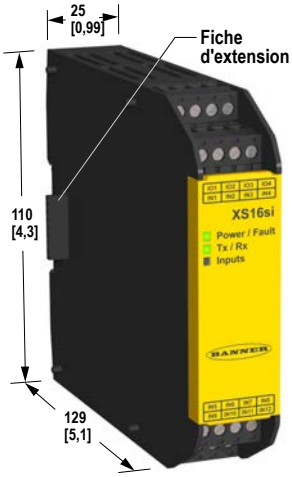


Illustration 16. Dimensions du SC10-2

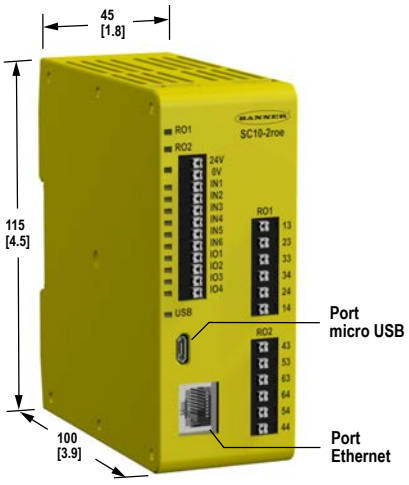
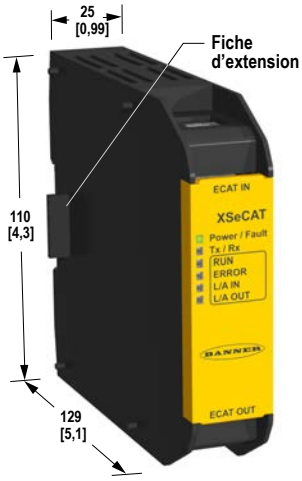


Illustration 17. Module EtherCAT



5.4 Configuration PC requise

Important: Des droits d'administrateur sont nécessaires pour installer les pilotes du contrôleur de sécurité (requis pour communiquer avec le contrôleur).

Système d'exploitation :	Microsoft Windows 7, Windows 10, ou Windows 11 [8]
Type de système :	32 bits, 64 bits
Espace sur le disque dur :	80 Mo (plus jusqu'à 280 Mo pour Microsoft. NET 4.0, s'il n'est pas encore installé)
Mémoire (RAM) :	512 Mo minimum, 1 Go et plus recommandé
Processeur :	1 GHz minimum, 2 GHz et plus recommandé
Résolution d'écran :	résolution couleur 1024 X 768 pixels minimum, résolution couleur 1650 × 1050 recommandée
Logiciels tiers :	Microsoft .NET 4.0 (inclus avec le programme d'installation), visualiseur de PDF (par ex. Adobe Acrobat)

[8] Microsoft et Windows sont des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

Port USB : USB 2.0 (non requis pour créer des configurations)

L’ordinateur doit avoir une interface Ethernet disponible.

6 Installation du système

6.1 Installation du logiciel

Important: Des droits d'administrateur sont nécessaires pour installer les pilotes du contrôleur de sécurité (requis pour communiquer avec le contrôleur).

1. Téléchargez la dernière version du logiciel à l'adresse www.bannerengineering.com/safetycontroller.
2. Accédez au fichier téléchargé et ouvrez-le.
3. Cliquez sur **Next** (Suivant) pour commencer l'installation.
4. Confirmez la destination et l'accessibilité du logiciel aux utilisateurs et cliquez sur **Next** (Suivant).
5. Cliquez sur **Installer** pour installer le logiciel.
6. Selon vos paramètres système, un message peut s'afficher et vous demander d'autoriser le Contrôleur de sécurité Banner à apporter des modifications à votre ordinateur. Cliquez sur **Oui**.
7. Cliquez sur **Finish** (Terminer) pour quitter le programme d'installation.

Ouvrez le logiciel **Contrôleur de sécurité Banner** à partir du **Bureau** ou du menu **Démarrer**.

6.2 Installation du contrôleur de sécurité

Pour garantir un fonctionnement fiable, ne dépassez pas les spécifications de fonctionnement. Le boîtier doit disposer d'une évacuation adéquate de la chaleur pour que la température de l'air autour du contrôleur de sécurité ne dépasse pas sa température maximale de fonctionnement (voir la section Spécifications et exigences à la page 21).

Important: Installez le contrôleur de sécurité dans un endroit protégé des chocs et des vibrations de grande amplitude.

Important:

- **Dispositif sensible aux décharges électrostatiques (ESD)**
- Les décharges électrostatiques peuvent endommager le dispositif. Les dégâts occasionnés par une manipulation incorrecte ne sont pas couverts par la garantie.
- Veillez à manipuler ces dispositifs avec précaution afin d'éviter qu'ils soient endommagés par des décharges électrostatiques. Il convient de laisser les dispositifs dans leur emballage antistatique jusqu'au moment de leur utilisation, de porter un bracelet antistatique et de monter les composants sur une surface reliée à la terre dissipant l'électricité statique.

6.2.1 Instructions de montage

Le contrôleur de sécurité est monté sur un rail DIN standard de 35 mm. Il doit être installé dans un boîtier aux normes NEMA3 (IEC IP54) ou supérieures. Le contrôleur doit être monté sur une surface verticale avec des orifices de ventilation au-dessus et en-dessous pour bénéficier d'une ventilation par convection naturelle.

Respectez les instructions de montage pour éviter d'endommager le contrôleur de sécurité.

Pour **monter** le contrôleur de sécurité programmable Contrôleur de sécurité programmable SC26-2, contrôleur de sécurité programmable XS26-2, contrôleur de sécurité programmable XS26-ISD, modules de sortie de sécurité électronique XS2so et XS4so, modules d'entrée de sécurité XS8si et XS16si, modules de relais de sécurité XS1ro et XS2ro, module de passerelle de communication EtherCAT XSeCAT et contrôleur de sécurité SC10-2 :

1. Inclinez légèrement la partie supérieure du module vers l'arrière et placez-le sur le rail DIN.
2. Redressez le module contre le rail.
3. Descendez le module sur le rail.

Remarque: Si vous utilisez un module EtherCAT, il doit être le premier module de la chaîne, à côté du contrôleur de base.

Pour **retirer** le contrôleur de sécurité programmable Contrôleur de sécurité programmable SC26-2, contrôleur de sécurité programmable XS26-2, contrôleur de sécurité programmable XS26-ISD, modules de sortie de sécurité électronique XS2so et XS4so, modules d'entrée de sécurité XS8si et XS16si, modules de relais de sécurité XS1ro et XS2ro, module de passerelle de communication EtherCAT XSeCAT et contrôleur de sécurité SC10-2 :

1. Poussez le bas du module vers le haut.
2. Inclinez légèrement le module vers l'avant.
3. Retirez le module dès que vous avez dégagé la fixation rigide supérieure du rail DIN.

Remarque: Pour retirer un module d'extension ou la passerelle de communication, écartez les autres modules installés de part et d'autre du module à retirer pour dégager les connecteurs de bus.

6.3 Installation électrique

Le contrôleur de sécurité doit être installé dans une armoire.

Suivez les procédures électriques adéquates lorsque vous travaillez sur le contrôleur de sécurité. Les instructions suivantes doivent être respectées, selon le type de raccordement :

- Coupez l'alimentation du contrôleur de sécurité avant de commencer à travailler sur le contrôleur (raccordement des modules ou câblage des unités).
- Utilisez uniquement une connexion sans tension du câble réseau au contrôleur de sécurité.
- Mettez sous tension uniquement après avoir réalisé tous les raccordements électriques.

7 Considérations relatives à l'installation

7.1 Application appropriée

L'utilisation appropriée du contrôleur de sécurité dépend du type de machine et des protections à connecter au contrôleur de sécurité. **S'il existe un doute quant à la compatibilité d'une machine et de ce contrôleur de sécurité, contactez Banner Engineering.**

Lisez attentivement cette section avant d'installer le système.

Le contrôleur de sécurité est un dispositif de commande conçu pour être utilisé en association avec un dispositif de protection de machine. Sa capacité à remplir cette fonction dépend de l'adéquation de l'application et de l'installation mécanique et électrique correcte du contrôleur de sécurité, ainsi que de son interfaçage avec la machine à protéger.

Si les procédures de montage, d'installation, d'interfaçage et de vérification n'ont pas été parfaitement respectées, le contrôleur de sécurité ne sera pas en mesure d'offrir la protection pour laquelle il a été conçu. L'utilisateur est responsable de la conformité à l'ensemble des lois, règles, réglementations et codes locaux, régionaux et nationaux concernant l'installation et l'utilisation de ce système de commande dans le cadre de toute application particulière. Assurez-vous que toutes les exigences de sécurité sont respectées, de même que toutes les instructions techniques d'installation et de maintenance de ce document.

AVERTISSEMENT:

- **Ce système n'est pas un dispositif de protection autonome**
- Si les zones ou équipements dangereux ne sont pas correctement sécurisés conformément à une étude de risques, aux réglementations locales ou aux normes en vigueur, cela peut entraîner des blessures graves ou mortelles.
- Ce dispositif Banner Engineering est considéré comme un dispositif complémentaire utilisé pour renforcer la protection en limitant ou éliminant l'exposition du personnel à un danger sans aucune action humaine.

AVERTISSEMENT:

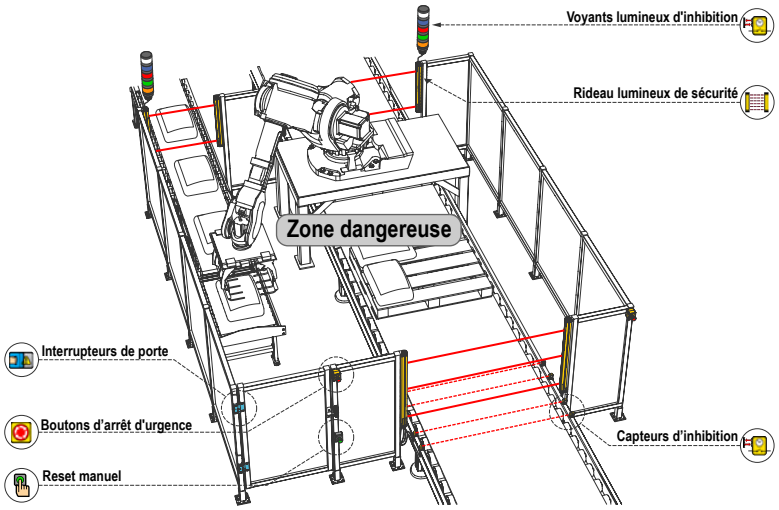
- **L'utilisateur est responsable de l'utilisation en toute sécurité de ce dispositif**
- Les exemples d'application décrits dans ce document représentent des situations de protection générales. Chaque application de protection est associée à une série d'exigences qui lui sont propres.
- Veillez à respecter toutes les exigences de sécurité ainsi que toutes les instructions d'installation. Transmettez toute question concernant la protection à Banner Engineering au numéro ou à l'adresse indiqués dans ce document.

7.2 Applications XS/SC26

Le contrôleur de sécurité peut être utilisé dans les installations intégrant des modules de sécurité. Le contrôleur de sécurité est adapté à de nombreux types d’applications, dont les suivantes :

- Commande bimanuelle avec fonction d’inhibition
- Cellules robotisées de traitement/soudage avec inhibition de double zone
- Opérations de manutention de matériaux qui nécessitent plusieurs entrées et fonctions de dérivation
- Stations de chargement manuel de carrousel
- Applications à plusieurs stations de commande bimanuelles
- Stations de fabrication
- Surveillance dynamique des solénoïdes simples ou doubles ou des soupapes de sécurité de presse

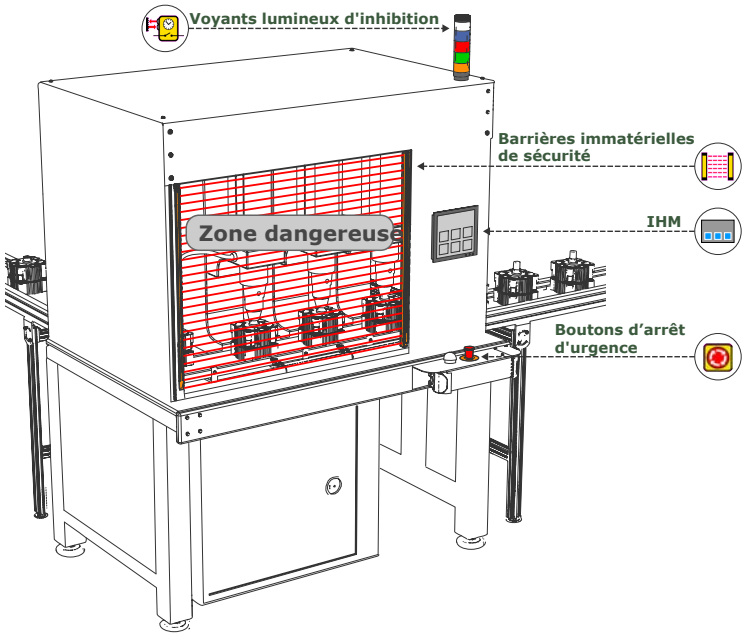
Illustration 18. Exemple d'installation - cellule robotisée



7.3 Applications SC10-2

Le contrôleur de sécurité SC10-2 est la solution idéale pour les machines de taille moyenne ou petite qui utilisent généralement deux modules relais de sécurité indépendants.

Illustration 19. Exemple d'application du SC10-2



7.4 Dispositifs d'entrée de sécurité

Le contrôleur de sécurité surveille l'état des dispositifs d'entrée de sécurité qui lui sont connectés. En général, lorsque tous les dispositifs de sécurité configurés pour contrôler une sortie de sécurité donnée sont en état marche, la sortie de sécurité s'active ou reste activée. Lorsqu'un ou plusieurs dispositifs d'entrée de sécurité passent de l'état marche à l'état d'arrêt, la sortie de sécurité se désactive. Certaines fonctions spéciales des dispositifs de sécurité peuvent, dans des circonstances prédéfinies, suspendre temporairement le signal d'arrêt de l'entrée de sécurité pour maintenir la sortie de sécurité activée, notamment les fonctions d'inhibition ou de dérivation.

Le contrôleur de sécurité peut détecter des défauts d'entrée dans certains circuits d'entrée qui, sinon, provoqueraient la perte du contrôle de la fonction de sécurité. Quand de tels défauts sont détectés, le contrôleur de sécurité désactive les sorties associées jusqu'à ce que les défauts soient corrigés. Les blocs fonction utilisés dans la configuration affectent les sorties de sécurité. Il est nécessaire d'examiner soigneusement la configuration si des défauts surviennent au niveau du dispositif d'entrée.

Pour éliminer ou limiter ce risque de défauts, plusieurs méthodes sont possibles dont les suivantes :

- Séparer physiquement les fils des commandes d'interconnexion les uns des autres et des sources d'alimentation secondaires

- Faire passer les fils d'interconnexion des commandes dans des conduits, des parcours ou des chemins de câbles différents
- Regrouper tous les éléments de contrôle (contrôleur de sécurité, modules d'interface, FSD et MPCE) dans une seule armoire, les uns à côté des autres, et raccordés directement par des fils courts
- Installer correctement des raccords à réducteur de tension sur les câbles à plusieurs conducteurs. Le serrage excessif d'un réducteur de tension peut entraîner des courts-circuits à cet endroit
- Utiliser des composants à ouverture positive ou directe, comme décrit dans la norme IEC 60947-5-1, qui sont installés et montés en mode positif
- Vérifier périodiquement l'intégrité fonctionnelle/la fonction de sécurité
- Former les opérateurs, le personnel de maintenance ainsi que les opérateurs de la machine et des dispositifs de protection à identifier et corriger immédiatement tous les défauts

Remarque: Respectez les instructions d'installation, d'utilisation et de maintenance du fabricant du dispositif et toutes les réglementations applicables. Pour toute question sur le ou les dispositifs connectés au contrôleur de sécurité, contactez Banner Engineering pour obtenir une assistance.

Illustration 20. Emplacement des bornes du XS/SC26

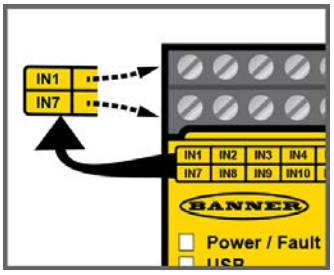
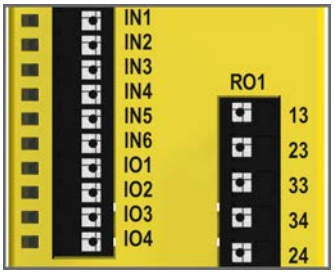


Illustration 21. Emplacement des bornes du SC10-2



AVERTISSEMENT:

- **Dispositif d'entrée et intégrité de la sécurité**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Le contrôleur de sécurité peut surveiller différents dispositifs d'entrée de sécurité. L'utilisateur doit procéder à une étude de risques de l'application de protection pour déterminer quel niveau d'intégrité de la sécurité mettre en place et savoir comment connecter correctement les dispositifs d'entrée au contrôleur de sécurité.
- L'utilisateur doit aussi éliminer ou limiter au maximum les défauts et les défaillances du signal susceptibles d'entraîner une perte des fonctions de sécurité.

7.4.1 Intégrité du circuit de sécurité et principes de circuit de sécurité ISO 13849-1

Les circuits de sécurité concernent les fonctions dédiées à la sécurité d'une machine et destinées à minimiser le risque de blessure. Ces fonctions de sécurité peuvent empêcher l'initiation ou encore arrêter ou éliminer un danger. La défaillance d'une fonction de sécurité ou du circuit de sécurité associé augmente généralement le risque de blessure.

L'intégrité d'un circuit de sécurité dépend de plusieurs facteurs, notamment la tolérance aux défaillances, la réduction des risques, la présence de composants fiables et correctement testés, des principes de sécurité éprouvés et d'autres considérations de conception.

Selon le niveau de risque associé à la machine ou à son fonctionnement, il est nécessaire d'intégrer à sa conception un circuit de sécurité dont le niveau d'intégrité (ou de performance) est adéquat. Parmi les normes régissant les niveaux de performance de sécurité figurent les normes ANSI B11.19 (Machines-outils - Protection lorsque référencée par d'autres normes B11 relatives à la sécurité des machines - Critères de performance pour la conception, la construction, l'entretien et l'utilisation) et ISO 13849-1 (Sécurité des machines - Parties des systèmes de commande relatives à la sécurité).

Niveaux d'intégrité des circuits de sécurité

Les circuits de sécurité dans les normes internationales et européennes ont été divisés en plusieurs catégories et niveaux de performance, en fonction de leur capacité à maintenir leur intégrité en cas de défaillance et la probabilité statistique d'une telle défaillance. La norme ISO 13849-1 porte sur l'intégrité des circuits de sécurité et décrit l'architecture/structure du circuit (catégories) et le niveau de performance requis des fonctions de sécurité dans des conditions prévisibles.

Aux États-Unis, le niveau normal d'intégrité d'un circuit de sécurité est désigné par l'expression « fiabilité des commandes ». La fiabilité des commandes inclut généralement la redondance des commandes et un circuit de contrôle automatique. Ce concept correspond globalement à la catégorie 3 ou 4 de la norme ISO 13849-1 et/ou au niveau de performances D ou E (voir la norme ANSI B11.19).

Procédez à une étude de risques pour vérifier que l'installation, l'interfaçage/raccordement et la réduction des risques sont appropriés (voir la norme ANSI B11.0 ou ISO 12100). Il est nécessaire de réaliser une étude de risques pour déterminer le niveau d'intégrité approprié du circuit de sécurité et réduire le risque de la façon attendue. Cette étude de ris-

ques doit prendre en compte toutes les réglementations locales et les normes applicables, notamment la fiabilité des commandes stipulée dans les normes américaines ou le niveau C des normes européennes.

Les entrées du contrôleur de sécurité peuvent prendre en charge un interfaçage/raccordement de catégorie 4 PL e maximum (ISO 13849-1) et de niveau d'intégrité de la sécurité 3 maximum (IEC 61508 et IEC 62061). Le niveau d'intégrité réel du circuit de sécurité dépend de la configuration, de l'installation correcte des circuits externes ainsi que du type des dispositifs d'entrée de sécurité et de leur installation. C'est à l'utilisateur qu'il incombe de déterminer le ou les niveaux de sécurité globaux et de garantir la conformité à toutes les normes et réglementations applicables.

Les sections suivantes ne concernent que les applications des catégories 2, 3 et 4, telles que décrites dans la norme ISO 13849-1. Les circuits des dispositifs d'entrée illustrés dans le tableau ci-dessous sont généralement utilisés dans les applications de protection, même si d'autres solutions sont possibles en fonction de l'élimination des erreurs et de l'étude de risques. Le tableau ci-dessous illustre les circuits des dispositifs d'entrée et le niveau/catégorie de sécurité possible si toutes les conditions de détection et d'élimination des erreurs sont satisfaites.

AVERTISSEMENT:
- **Détermination de la catégorie de sécurité**
- Le niveau d'intégrité du circuit de sécurité peut être fortement affecté par la conception et l'installation des dispositifs de sécurité et les méthodes de raccordement de ces dispositifs.
- Procédez à une étude de risques afin de déterminer le niveau d'intégrité du circuit de sécurité ou la catégorie de sécurité appropriée comme défini par l'ISO 13849-1, et ce afin de garantir la réduction des risques prévue et le respect de toutes les réglementations et normes applicables.

AVERTISSEMENT:
- **Pour les dispositifs d'entrée avec entrées à double contact utilisant deux ou trois bornes, la détection d'un court-circuit entre deux voies d'entrée (entrées à contact, mais pas de contacts complémentaires) n'est pas possible si les deux contacts sont fermés.**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Un court-circuit peut être détecté lorsque l'entrée est en état d'arrêt pendant au moins deux (2) secondes (voir le conseil **Bornes d'entrée INx & IOx** dans la section Options des dispositifs d'entrée de sécurité à la page 38).

AVERTISSEMENT:
- **Courts-circuits d'entrée de catégorie 2 ou 3**
- Il n'est pas possible de détecter un court-circuit entre deux voies d'entrée (entrées à contact, mais pas de contacts complémentaires), si elles sont alimentées par la même source (par exemple, la même borne du contrôleur dans une connexion à deux voies et 3 bornes ou celle d'une alimentation externe 24 V) et si les deux contacts sont fermés.
- Un tel court-circuit ne peut être détecté que si les deux contacts sont ouverts et que le court-circuit dure plus de deux (2) secondes.

Élimination d'erreurs

Les exigences de la norme ISO 13849-1 traitent d'un concept important, à savoir la probabilité de survenue d'une défaillance, laquelle peut être limitée par une technique appelée "élimination d'erreurs". Le principe de base suppose que l'éventualité de certaines défaillances bien définies peut être ramenée via la conception, l'installation ou l'improbabilité technique à un niveau où le ou les défauts résultants peuvent être, pour la plupart, écartés, c'est-à-dire exclus.

L'élimination d'erreurs est un outil qu'un concepteur peut utiliser pendant le développement de la partie sécurisée du système de surveillance et le processus d'étude de risques. L'élimination des erreurs permet d'intégrer à la conception la possibilité de plusieurs défaillances et de la justifier par le processus d'étude de risques afin de satisfaire les exigences de la norme ISO 13849-1/-2.

Les exigences varient grandement selon le niveau d'intégrité du circuit de sécurité dans les applications de sécurité (c.-à-d. la fiabilité des commandes ou la catégorie/le niveau de performances) conformément à la norme ISO 13849-1. Bien que Banner Engineering recommande toujours le niveau de sécurité le plus élevé pour n'importe quelle installation, l'utilisateur est responsable de l'installation, de l'utilisation et de l'entretien de tous les systèmes de sécurité ainsi que de leur conformité aux lois et réglementations applicables.

AVERTISSEMENT:
- **Détermination de la catégorie de sécurité**
- Le niveau d'intégrité du circuit de sécurité peut être fortement affecté par la conception et l'installation des dispositifs de sécurité et les méthodes de raccordement de ces dispositifs.
- Procédez à une étude de risques afin de déterminer le niveau d'intégrité du circuit de sécurité ou la catégorie de sécurité appropriée comme défini par l'ISO 13849-1, et ce afin de garantir la réduction des risques prévue et le respect de toutes les réglementations et normes applicables.

7.4.2 Propriétés des dispositifs d'entrée de sécurité

Le contrôleur de sécurité est configuré via le logiciel pour prendre en charge de nombreux types de dispositifs d'entrée de sécurité. Voir Ajout d'entrées et de sorties d'état à la page 86 pour en savoir plus sur la configuration des dispositifs d'entrée.

Logique de reset : reset manuel ou automatique

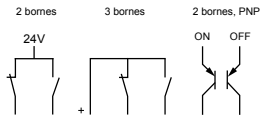
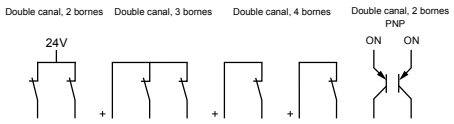
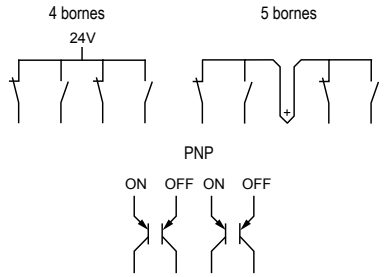
Les dispositifs d'entrée de sécurité doivent parfois faire l'objet d'un reset manuel en utilisant un bloc de reset à verrouillage ou en configurant une sortie de sécurité pour le reset à verrouillage avant que la ou les sorties de sécurité qu'ils contrôlent puissent être réactivées. Ce type de reset est parfois qualifié de mode « verrouillage » parce que la sortie de sécurité se verrouille en état Off (désactivé) jusqu'au reset du dispositif. Si un dispositif d'entrée de sécurité est configuré pour le reset automatique, la ou les sorties de sécurité qu'il contrôle sont réactivées lorsque le dispositif d'entrée passe en mode marche (Run) (pour autant que toutes les entrées de contrôle soient également en mode marche).

Raccordement des dispositifs d'entrée

Le contrôleur de sécurité doit savoir quelles lignes de signal des dispositifs sont raccordées aux différentes bornes afin de pouvoir appliquer les méthodes appropriées de surveillance du signal, les conventions de marche (Run) et d'arrêt (Stop), les règles de temporisation et de défaut. Les bornes sont attribuées automatiquement pendant le processus de configuration et peuvent être modifiées manuellement à l'aide du logiciel.

Types de changement d'état du signal

Il est possible d'utiliser deux types de changement d'état (COS, Change-of-State) lors de la surveillance des signaux d'un dispositif d'entrée de sécurité double voie : Simultané ou Concurrent.

Circuit d'entrée	Règles de minutage du changement d'état du signal d'entrée	
	État d'arrêt — Désactivation (Off) de la sortie de sécurité quand [9]:	**État de marche — Activation (On) de la sortie de sécurité quand [10]:**
Double voie A et B complémentaires 	L'entrée d'une voie (A ou B) au moins est en état d'arrêt.	**Simultané :** A et B sont toutes les deux en état d'arrêt puis passent en état marche en moins de 3 secondes avant que les sorties soient activées (On). **Concurrent :** A et B sont l'une après l'autre en état d'arrêt puis toutes deux passent en état marche sans simultanéité, pour activer les sorties (On).
Double voie A et B 		
2 A et B complémentaires 	Au moins 1 voie (A ou B) d'une paire de contacts est en état d'arrêt.	**Simultané :** A et B sont l'une après l'autre en état d'arrêt, puis les contacts d'une voie passent en état marche en moins de 400 ms (150 ms pour une commande bimanuelle), les deux voies sont en état marche en moins de 3 secondes (0,5 seconde pour une commande bimanuelle). **Concurrent :** A et B sont l'un après l'autre en état d'arrêt. Les contacts dans une voie passent en état de marche dans les 3 secondes. Il n'y a pas d'exigence de simultanéité entre la commutation de la voie A et de la voie B.

9 Les sorties de sécurité passent sur OFF quand une des entrées les contrôlant est en état d'arrêt.
10 Les sorties de sécurité sont uniquement activées (On) quand toutes les entrées qui les contrôlent sont en état de marche et seulement après avoir effectué un reset manuel (si l'une de ces entrées de sécurité avait été configurée pour le reset manuel et était en état d'arrêt).

Circuit d'entrée	Règles de minutage du changement d'état du signal d'entrée	
	État d'arrêt — Désactivation (Off) de la sortie de sécurité quand [9]:	**État de marche — Activation (On) de la sortie de sécurité quand [10]:**
Tapis de sécurité à 4 fils Double canal, 4 bornes  	L'une des conditions suivantes doit être satisfaite : • Les canaux d'entrée sont court-circuités ensemble (fonctionnement normal). • Au moins un des fils est déconnecté. • L'un des canaux avec un état normalement bas est détecté avec un état haut. • L'un des canaux avec un état normalement haut est détecté avec un état bas.	Chaque voie détecte ses propres impulsions.

Temps anti-rebond d'un signal

Temps anti-rebond fermé à ouvert (de 6 ms à 1000 ms à intervalles de 1 ms ; 6 ms à 1500 ms pour les capteurs d'inhibition). Le temps anti-rebond fermé à ouvert est le temps limite que prend le signal pour passer de l'état haut (24 Vcc) à l'état bas stabilisé (0 Vcc). Il est nécessaire d'augmenter ce temps limite en cas de vibrations de forte amplitude, de chocs d'impact ou de perturbations du dispositif, lesquels nécessitent un temps de transition du signal plus long. Si le temps anti-rebond est trop court dans ces conditions difficiles, le système peut détecter un défaut de disparité du signal et se bloquer. La valeur par défaut est de 6 ms.

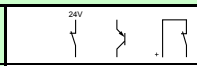
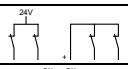
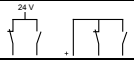
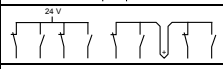
PRÉCAUTION: Réponse et anti-rebond — Toute modification du temps anti-rebond peut affecter le temps de réponse de la sortie de sécurité (désactivation). Cette valeur est calculée et affichée pour chaque sortie de sécurité quand une configuration est créée.

Temps anti-rebond fermé à ouvert (de 10 ms à 1000 ms à intervalles de 1 ms ; 10 ms à 1500 ms pour les capteurs d'inhibition). Le temps anti-rebond ouvert à fermé est le temps limite que prend le signal pour passer de l'état bas (0 Vcc) à l'état haut stabilisé (24 Vcc). Il est nécessaire d'augmenter ce temps limite en cas de vibrations de forte amplitude, de chocs d'impact ou de perturbations du dispositif, lesquels nécessitent un temps de transition du signal plus long. Si le temps anti-rebond est trop court dans ces conditions difficiles, le système peut détecter un défaut de disparité du signal et se bloquer. La valeur par défaut est de 50 ms.

9 Les sorties de sécurité passent sur OFF quand une des entrées les contrôlant est en état d'arrêt.
10 Les sorties de sécurité sont uniquement activées (On) quand toutes les entrées qui les contrôlent sont en état de marche et seulement après avoir effectué un reset manuel (si l'une de ces entrées de sécurité avait été configurée pour le reset manuel et était en état d'arrêt).

7.5 Options des dispositifs d'entrée de sécurité

Illustration 22. Circuit du dispositif d'entrée — Guide des catégories de sécurité

Symboles généraux des circuits		Circuits illustrés en état Run							Circuits illustrés en état Stop	
		ES	GS	OS	RP	PS	SM	ISD	THC	ED
Simple voie 1 et 2 bornes (voir remarque 1)		Cat. 2	Cat. 2	Cat. 2	Cat. 2	Cat. 2				
Double voie 2 et 3 bornes (voir remarque 2)		Cat. 3	Cat. 3	Cat. 3	Cat. 3	Cat. 3			Type IIIa Cat. 1 Type IIIb Cat. 3	Cat. 3
Double voie, 2 bornes PNP avec surveillance intégrale (voir remarque 3)		Cat. 4	Cat. 4	Cat. 4	Cat. 4	Cat. 4		Cat. 4	Type IIIa Cat. 1	Cat. 4
Double voie 3 et 4 bornes (voir remarques 2 et 4)		Cat. 4	Cat. 4	Cat. 4	Cat. 4	Cat. 4			Type IIIa Cat. 1 Type IIIb Cat. 3	Cat. 4
Double voie, 2 et 3 bornes Complémentaire			Cat. 4	Cat. 4	Cat. 4	Cat. 4				Cat. 4
Double voie, 2 bornes PNP complémentaire			Cat. 4	Cat. 4	Cat. 4	Cat. 4				Cat. 4
Double voie, 4 et 5 bornes Complémentaire			Cat. 4						Type IIIc Cat. 4	Cat. 4
Double voie, 4 bornes PNP complémentaire			Cat. 4						Type IIIc Cat. 4	Cat. 4
Tapis de sécurité à 4 bornes							Cat. 3			

Remarque:

1. Le circuit respecte généralement les exigences de la norme ISO 13849-1 Catégorie 2 si les dispositifs d'entrée offrent un certain niveau de protection et qu'ils mettent en œuvre l'exclusion des défauts pour prévenir a) des courts-circuits dans les dispositifs à sorties transistorisées ou à contacts et b) des courts-circuits vers d'autres sources d'alimentation.
2. Le circuit est généralement conforme à la norme ISO 13849-1 catégorie 3 si les dispositifs d'entrée sont dédiés à la sécurité (voir **Conseil : bornes d'entrée INx et IOx**, ci-dessous). Le circuit à 2 bornes détecte un court-circuit d'un système simple voie vers d'autres sources d'alimentation lorsque les contacts s'ouvrent et se referment (défaut de séquence). Le circuit à 3 bornes détecte un court-circuit vers d'autres sources d'alimentation, que les contacts soient ouverts ou fermés.
3. Le circuit respecte les exigences de la norme ISO 13849-1 Catégorie 4 si les dispositifs d'entrée offrent un certain niveau de protection ainsi qu'une surveillance interne des sorties PNP pour détecter a) des courts-circuits au niveau des voies et b) des courts-circuits vers d'autres sources d'alimentation.
4. Le circuit est conforme à la norme ISO 13849-1 catégorie 4 si les dispositifs d'entrée sont dédiés à la sécurité (voir **Conseil : bornes d'entrée INx et IOx**, ci-dessus). Ces circuits peuvent détecter les courts-circuits vers d'autres sources d'alimentation et entre les voies.

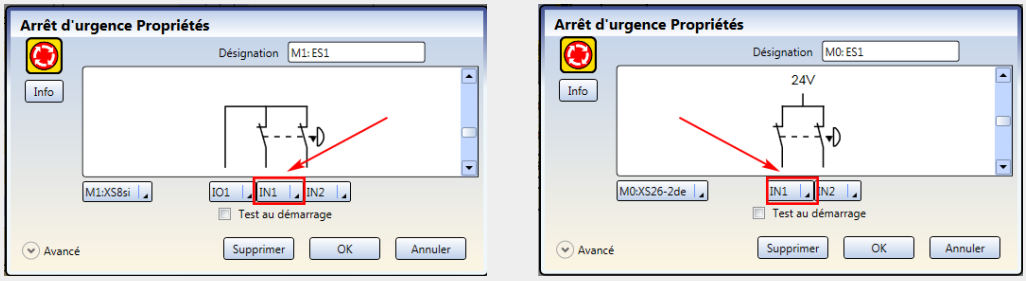
PRÉCAUTION:

- **Informations d'installation incomplètes**
- Ce document ne couvre pas toutes les consignes et procédures nécessaires à l'installation et à l'utilisation correctes de ces systèmes.
- Référez-vous aux instructions d'installation du dispositif correspondant pour garantir une application en toute sécurité du dispositif.

AVERTISSEMENT: Ce tableau répertorie les catégories de sécurité les plus élevées possibles pour les circuits des dispositifs d'entrée dédiés à la sécurité courants. Si les exigences supplémentaires stipulées dans les remarques ci-dessous ne peuvent être mises en œuvre en raison de limitations du dispositif de sécurité ou de l'installation ou si, par exemple, les bornes d'entrée IOx du contrôleur de sécurité sont toutes utilisées, il n'est pas toujours possible d'obtenir la catégorie de sécurité la plus élevée.

Astuce: Bornes d'entrée INx & IOx : ces circuits peuvent être configurés manuellement pour respecter les exigences d'un circuit de catégorie 4 en transformant la première borne d'entrée standard (INx) (la plus à gauche) en borne convertible disponible (IOx), comme illustré ci-dessous. Ces circuits détectent des courts-circuits vers d'autres sources d'alimentation et entre les canaux lorsque l'entrée est restée en état d'arrêt pendant au moins deux secondes.

Illustration 23. Circuits configurés manuellement



7.5.1 Niveaux d'intégrité des circuits de sécurité

Les exigences d'application pour les dispositifs de protection varient selon le niveau de fiabilité des commandes ou la catégorie de sécurité conformément à la norme ISO 13849-1. Bien que Banner Engineering recommande toujours le niveau de sécurité le plus élevé pour n'importe quelle installation, l'utilisateur est responsable de l'installation, de l'utilisation et de l'entretien de tous les systèmes de sécurité ainsi que de leur conformité aux lois et réglementations applicables.

La performance de sécurité (intégrité) doit réduire les risques de danger identifiés par l'évaluation des risques réalisée pour la machine. Référez-vous à la section Intégrité du circuit de sécurité et principes de circuit de sécurité ISO 13849-1 à la page 34 pour plus d'informations.

7.5.2 Boutons-poussoirs d'arrêt d'urgence

Les entrées de sécurité du contrôleur de sécurité peuvent servir à surveiller des boutons d'arrêt d'urgence.

AVERTISSEMENT:
- **Veillez à ne pas inhiber ni à dériver un dispositif d'arrêt d'urgence.**
- L'inhibition ou la dérivation des sorties de sécurité rendrait la fonction d'arrêt d'urgence inopérationnelle.
- Les normes ANSI B11.19, NFPA 79 et IEC/EN 60204-1 exigent que la fonction d'arrêt d'urgence reste active en permanence.

AVERTISSEMENT:
- **Configuration conforme aux normes applicables**
- Le fait de ne pas vérifier l'application peut entraîner des blessures graves, voire mortelles.
- Le logiciel Contrôleur de sécurité Banner vérifie principalement la configuration logique pour détecter des erreurs de connexion. Il incombe à l'utilisateur de vérifier que l'application répond aux exigences de l'évaluation des risques et qu'elle est conforme à toutes les normes applicables.

AVERTISSEMENT:
- **Séquence de reset requise**
- Le redémarrage possible de la machine sans actionner la commande ou le dispositif de démarrage normal pourrait créer une situation dangereuse pouvant entraîner des blessures graves, voire mortelles.
- Faites en sorte que la machine ne puisse pas redémarrer sans actionner la commande/dispositif de démarrage normal. Exécutez la séquence de reset après avoir éliminé la cause d'une condition d'arrêt, conformément aux normes américaines et internationales.

Outre les conditions définies dans cette section, la conception et l'installation du dispositif d'arrêt d'urgence doivent être conformes aux normes NFPA 79 ou ISO 13850. La fonction d'arrêt doit être un arrêt fonctionnel de catégorie 0 ou de catégorie 1 (voir la norme NFPA 79).

Exigences relatives au dispositif d'arrêt d'urgence

L'interrupteur d'arrêt d'urgence doit disposer d'un ou deux contacts de sécurité qui sont fermés lorsque l'interrupteur est en position armée. Lorsqu'il est activé, l'interrupteur d'arrêt d'urgence doit ouvrir tous ses contacts de sécurité et demander une action délibérée (par exemple, une rotation, une traction ou un déblocage) pour revenir en position armée avec contacts fermés. Il doit s'agir d'un interrupteur à ouverture positive (ou ouverture directe), comme stipulé dans la norme IEC 60947-5-1. Une force mécanique appliquée à ce bouton (ou interrupteur) est transmise directement aux contacts, forçant leur ouverture. De cette façon, les contacts de l'interrupteur s'ouvrent à chaque fois qu'il est activé.

Les normes NFPA 79, ANSI B11.19, IEC/EN 60204-1 et ISO 13850 spécifient des conditions supplémentaires du dispositif d'arrêt d'urgence, dont les suivantes :

- Les dispositifs d'arrêt d'urgence doivent être installés sur chaque poste de commande à partir duquel un arrêt d'urgence peut s'avérer nécessaire.
- Les boutons d'arrêt et d'arrêt d'urgence doivent être constamment opérationnels et facilement accessibles depuis tous les postes de commande où ils sont installés. **Prenez soin de ne jamais inhiber ou contourner un bouton d'arrêt d'urgence.**
- Les déclencheurs des dispositifs d'arrêt d'urgence doivent être de couleur rouge. Le fond autour du déclencheur du dispositif doit être jaune. Le déclencheur d'un dispositif à bouton poussoir doit être de type poussoir à paume ou champignon.
- L'actionneur d'un dispositif d'arrêt d'urgence doit être de type « manuel ».

Remarque: Certaines installations doivent satisfaire à des exigences supplémentaires. L'utilisateur est tenu de se conformer à toutes les réglementations applicables.

Remarque: Pour les boutons d'arrêt d'urgence éclairés d'Banner avec ISD, voir aussi Entrées ISD à la page 51. L'utilisateur doit s'assurer que l'entrée n'est pas inhibée ni dérivée. En effet, le contrôleur applique des règles pour l'interrupteur de porte car le bouton d'arrêt d'urgence est ajouté comme type de dispositif : entrée ISD, puis sélectionné comme arrêt d'urgence.

7.5.3 Interrupteur d'arrêt d'urgence à câble

Les interrupteurs d'arrêt d'urgence à câble utilisent un câble en acier pour fournir un arrêt d'urgence en continu sur une longue distance, comme le long d'un convoyeur.

Les interrupteurs d'arrêt d'urgence à câble sont assortis d'exigences comparables à celles des boutons d'arrêt d'urgence, notamment le fonctionnement à ouverture positive (directe), conformément à la norme IEC 60947-5-1. Consultez la section Boutons-poussoirs d'arrêt d'urgence à la page 39 pour des informations complémentaires.

Dans les applications d'arrêt d'urgence, les interrupteurs à câble doivent être en mesure de réagir à une traction dans n'importe quelle direction mais aussi à un relâchement ou une rupture du câble. Ils doivent également offrir une fonction de verrouillage qui exige un reset manuel après leur actionnement.

Consignes d'installation d'un interrupteur d'arrêt d'urgence à câble

Les normes NFPA 79, ANSI B11.19, IEC/EN 60204-1 et ISO 13850 spécifient les exigences d'arrêt d'urgence pour les installations incluant des interrupteurs à câble, dont les suivantes :

- Les interrupteurs à câble doivent être situés aux endroits où un arrêt d'urgence peut s'avérer nécessaire.
- Ils doivent être toujours opérationnels, clairement visibles et faciles d'accès, ils ne doivent pas être inhibés ni dérivés.
- Ils doivent assurer une tension constante du câble.
- Le système à câble doit être de couleur rouge, de même que tout autre drapeau ou marqueur.
- Le système à câble doit être capable de réagir à une force dans n'importe quelle direction.
- L'interrupteur doit :
  - Disposer d'une fonction de verrouillage automatique qui exige un reset manuel après son actionnement.
  - Fonctionner en mode d'ouverture directe.
  - Détecter un relâchement ou une rupture du câble.

Autres consignes d'installation :

- Le câble de traction doit être facile d'accès, de couleur rouge pour les fonctions d'arrêt d'urgence et visible sur toute sa longueur. Vous pouvez attacher des drapeaux ou des marqueurs sur le câble pour améliorer sa visibilité.
- Les points de montage, dont les points de support, doivent être rigides et laisser suffisamment d'espace autour du câble pour y accéder facilement.
- Le câble ne doit pas frotter au niveau des supports. Il est recommandé d'utiliser des poulies. Il peut être nécessaire de les lubrifier. La contamination du système (poussières, copeaux métalliques ou autres, etc.) doit être évitée pour ne pas perturber son fonctionnement.
- Utilisez uniquement des poulies (pas de boulons à œil) pour passer le câble autour d'un angle ou si la direction change, même légèrement.
- Ne faites pas passer le câble dans un conduit ou un tube quelconque.
- N'attachez jamais de poids au câble.

- Il est recommandé d'utiliser un ressort de tension pour respecter l'exigence d'actionnement du câble de traction indépendamment de la direction. Ce ressort doit être installé sur la structure porteuse (cadre de la machine, mur, etc.)
- La température affecte la tension du câble. Le câble de traction s'allonge lorsque la température augmente et se contracte lorsqu'elle diminue. En cas de variations fréquentes de la température, il convient de vérifier souvent le réglage de la tension.

AVERTISSEMENT: Le non-respect des procédures et des consignes d'installation peut entraîner une défaillance ou un dysfonctionnement du système d'interrupteur à câble et créer une situation dangereuse susceptible d'occasionner des blessures graves ou mortelles.

7.5.4 Dispositif de commande

Un dispositif de commande est une commande manuelle qui, lorsqu'elle est actionnée en continu, permet à la machine d'initier son cycle en conjonction avec une commande de démarrage. Parmi les normes qui couvrent la conception et l'application des dispositifs de commande, citons les normes ISO 12100-1/-2, IEC 60204-1, NFPA 79, ANSI/RIA R15.06 et ANSI B11.19.

Le dispositif de commande contrôle la suspension d'un signal d'arrêt pendant une partie du cycle de la machine susceptible de présenter un danger. Il permet à la partie dangereuse du cycle de s'exécuter mais ne doit pas la démarrer. Un dispositif de commande peut contrôler une ou plusieurs sorties de sécurité. Lorsque le signal de commande passe de l'état d'arrêt à l'état marche, le contrôleur de sécurité bascule en mode actif. Un signal de commande distinct envoyé par un autre dispositif est nécessaire pour démarrer le mouvement dangereux. **Ce dispositif de commande doit avoir le contrôle ultime de la désactivation ou de l'arrêt du mouvement dangereux.**

7.5.5 Arrêt de protection (de sécurité)

Un arrêt de protection (de sécurité) est conçu pour raccorder différents dispositifs qui peuvent inclure des dispositifs de protection et des équipements complémentaires. Cette fonction d'arrêt est une interruption du fonctionnement qui permet d'arrêter correctement le mouvement à des fins de protection. La fonction peut faire l'objet d'un reset ou être activée automatiquement ou manuellement.

Exigences en matière d'arrêt de protection (de sécurité)

Le niveau d'intégrité requis du circuit de sécurité est déterminé par une évaluation des risques et indique le niveau de commande acceptable, par exemple la catégorie 4, Fiabilité des commandes (voir Intégrité du circuit de sécurité et principes de circuit de sécurité ISO 13849-1 à la page 34). Le circuit d'arrêt de protection doit contrôler le risque surveillé en provoquant un arrêt de la situation dangereuse et en coupant l'alimentation des actionneurs de la machine dans l'intervalle du temps de réponse de la fonction de sécurité. Il s'agit normalement d'un arrêt fonctionnel de catégorie 0 ou de catégorie 1 tel que décrit dans les normes NFPA 79 et IEC60204-1.

7.5.6 Porte ou système de protection à verrouillage

Les entrées de sécurité du contrôleur de sécurité peuvent être utilisées pour surveiller les portes ou les systèmes de protection à verrouillage électrique.

Conditions d'utilisation des interrupteurs de verrouillage de sécurité

Les conditions et considérations générales suivantes s'appliquent à l'installation de portes et de systèmes de protection à verrouillage à des fins de protection. En outre, l'utilisateur doit se référer aux règlements applicables pour garantir le respect de toutes les exigences nécessaires.

Les mouvements dangereux protégés par ce système de protection à verrouillage ne doivent pas pouvoir se déclencher tant que le système de protection n'est pas fermé. Si le système de protection à verrouillage est ouvert alors qu'un danger existe, une commande d'arrêt doit être envoyée à la machine protégée. La fermeture du système ne doit pas, en soi, déclencher un mouvement dangereux ; il faut une procédure distincte pour démarrer ce mouvement. Les interrupteurs de verrouillage de sécurité ne doivent pas servir de fin de course ou d'arrêt mécanique.

Le dispositif de protection doit être situé à une distance suffisante de la zone dangereuse (pour que le danger puisse être éliminé ou arrêté avant que le dispositif de protection soit suffisamment ouvert pour permettre l'accès) et il doit s'ouvrir de façon latérale ou vers l'extérieur mais pas vers l'intérieur de la zone protégée. Par ailleurs, il ne doit théoriquement pas pouvoir se refermer de lui-même et activer le circuit de verrouillage. En outre, le personnel ne doit pas pouvoir atteindre le danger en passant par-dessus ou en-dessous du dispositif de protection ni en le contournant ou en y pénétrant. Aucune ouverture dans le dispositif de protection ne doit permettre d'accéder au danger (voir les normes OSHA 29CFR1910.217 Tableau O-10, ANSI B11.19, EN ISO 13857, ISO14120 ou toute autre norme applicable). Il doit être suffisamment robuste pour confiner le danger posé par la machine à l'intérieur de la zone protégée (danger présenté par une éjection, une chute ou une émission).

Les interrupteurs de verrouillage de sécurité, déclencheurs, capteurs et aimants doivent être conçus et installés de sorte qu'il soit difficile de les contourner. Ils doivent être solidement fixés pour éviter qu'ils ne bougent. À cette fin, utilisez des fixations solides qui ne peuvent pas être démontées sans un outil. Les fentes de montage des boîtiers ne servent que pour les réglages initiaux. Il faut utiliser des trous de fixation définitifs pour l'installation permanente.

AVERTISSEMENT: Si l'application était susceptible de provoquer un risque d'enfermement (par exemple, dans le périmètre surveillé), le dispositif de surveillance ou les MSC/MPCE de la machine surveillée entraîneraient un blocage à la suite d'une commande d'arrêt (par exemple, une interruption du champ de détection d'une barrière immatérielle ou l'ouverture d'une barrière/système de protection verrouillé). Un reset de ce blocage ne peut être effectué qu'en actionnant un interrupteur de reset séparé des mécanismes normaux de mise en marche de la machine. Cet interrupteur doit être placé comme décrit dans ce document.

AVERTISSEMENT:

- **Applications de surveillance du périmètre**
- Le non-respect de ces consignes peut entraîner des dommages corporels graves, voire mortels.
- Mettez en œuvre certaines procédures de verrouillage/étiquetage conformément à la norme ANSI Z244-1, ou d'autres dispositifs de protection comme ceux décrits dans les normes de sécurité ANSI B11.19 ou d'autres normes applicables s'il est impossible d'éliminer le risque d'enfermement ou de le limiter à un niveau de risque acceptable.

7.5.7  Capteur optique

Les entrées de sécurité du contrôleur de sécurité peuvent servir à surveiller les dispositifs optiques utilisant la lumière comme moyen de détection.

Exigences concernant les capteurs optiques

Utilisés en tant que dispositifs de protection, les capteurs optiques sont décrits par la norme IEC61496-1/-2/-3 en tant que dispositif de protection opto-électronique actif (AOPD) et dispositif de protection opto-électronique actif répondant à la réflexion diffuse (AOPDDR).

Les dispositifs de protection opto-électroniques actifs (AOPD) incluent les barrières immatérielles de sécurité et les systèmes de sécurité mono et multi faisceaux. Ces dispositifs répondent généralement aux exigences de conception de type 2 ou 4. Un dispositif de type 2 est autorisé dans une application de catégorie 2 conformément à la norme ISO 13849-1 et un dispositif de type 4 peut être utilisé dans une application de catégorie 4.

Les dispositifs de protection opto-électroniques actifs répondant à la réflexion diffuse (AOPDDR) incluent les scanners de surface ou à laser. Il s'agit essentiellement de dispositifs de type 3, à utiliser dans des installations de catégorie 3 maximum.

Les dispositifs de sécurité optiques doivent être placés à une distance de sécurité appropriée (distance minimale), selon les normes applicables. Référez-vous aux normes applicables et à la documentation du fabricant du dispositif pour les calculs. Le temps de réponse des sorties du contrôleur de sécurité à chaque entrée de sécurité figure dans la vue **Résumé de la configuration** du logiciel.

Si l'installation comporte un risque d'enfermement (une personne peut passer par les faisceaux du dispositif optique et ne pas être détectée dans la zone dangereuse), il peut être nécessaire d'ajouter d'autres protections et de sélectionner le reset manuel (voir Entrée de reset manuel à la page 62).

AVERTISSEMENT: Si l'application était susceptible de provoquer un risque d'enfermement (par exemple, dans le périmètre surveillé), le dispositif de surveillance ou les MSC/MPCE de la machine surveillée entraîneraient un blocage à la suite d'une commande d'arrêt (par exemple, une interruption du champ de détection d'une barrière immatérielle ou l'ouverture d'une barrière/système de protection verrouillé). Un reset de ce blocage ne peut être effectué qu'en actionnant un interrupteur de reset séparé des mécanismes normaux de mise en marche de la machine. Cet interrupteur doit être placé comme décrit dans ce document.

7.5.8  Commande bimanuelle

Le contrôleur de sécurité peut servir d'actionneur pour la plupart des machines dont le cycle machine est commandé par un opérateur.

Les commandes bimanuelles doivent être installées de sorte que le mouvement dangereux soit terminé ou arrêté avant que l'opérateur puisse relâcher un bouton ou les deux et atteindre la zone dangereuse (voir Distance de sécurité d'une commande bimanuelle (distance minimale) à la page 43).

Les entrées de sécurité du contrôleur de sécurité utilisées pour surveiller l'utilisation des deux mains pour la commande bimanuelle sont conformes aux exigences fonctionnelles de type III des normes IEC 60204-1 et ISO 13851 et aux exigences des normes NFPA 79 et ANSI B11.19 pour les commandes bimanuelles, résumées ci-dessous :

- Actionnement simultané par les deux mains en moins de 500 ms l'une de l'autre

- Si cette limite de temps est dépassée, les deux commandes doivent être relâchées avant de réinitialiser l'opération
- Actionnement continu pendant une situation dangereuse
- Arrêt immédiat de la situation dangereuse si l'une des deux commandes manuelles est relâchée
- Relâchement et réactivation des deux commandes manuelles pour réinitialiser le mouvement ou la situation dangereuse (anti-coincement)
- Niveau de performance approprié de la fonction de sécurité (fiabilité des commandes, catégorie/niveau de performance, réglementations et normes appropriées ou niveau d'intégrité de la sécurité), déterminé par une étude de risques

AVERTISSEMENT:
- **Utilisation d'un dispositif de protection de la zone de fonctionnement approprié**
- L'absence de dispositifs de protection appropriés autour des machines dangereuses peut entraîner un risque de blessures graves, voire mortelles.
- Installé correctement, le dispositif de sécurité de commande bimanuelle ne protège que les mains de l'opérateur de la machine. Il peut s'avérer nécessaire d'installer d'autres protections, comme des rideaux lumineux de sécurité, des commandes bimanuelles supplémentaires et/ou des carters de protection, afin de protéger le personnel des machines dangereuses.

PRÉCAUTION:
- **Évitez d'installer des commandes bimanuelles dans des environnements contaminés** — Une contamination grave ou d'autres facteurs environnementaux peuvent entraîner un ralentissement de la réponse ou un « faux » état de marche des boutons mécaniques ou ergonomiques.
- Un ralentissement de la réponse ou un « faux » état de marche présente des risques.
- L'environnement dans lequel les commandes manuelles sont installées ne doit pas affecter le mode de fonctionnement.

Le niveau de sécurité atteint (par ex. la catégorie ISO 13849-1) dépend en partie du type de circuit choisi.

Pour installer les commandes manuelles, prenez les points suivants en considération :
- Modes de défaillance, par exemple un court-circuit, un ressort cassé, un blocage mécanique, etc., qui empêcheraient de détecter le relâchement d'une commande manuelle
- Contamination sévère ou autres facteurs environnementaux susceptibles de ralentir le délai de relâchement ou d'entraîner un « faux » état de marche (ON) de la(des) commande(s) manuelle(s), par ex. le grippage d'une liaison mécanique
- Protection contre le déclenchement accidentel ou imprévu (par exemple en choisissant leur position de montage ou en utilisant des protections comme des bagues, des gardes ou des grillages)
- Limitation des possibilités de contournement (par exemple, les commandes manuelles doivent être suffisamment éloignées l'une de l'autre pour qu'elles ne puissent pas être utilisées avec un seul bras — normalement, pas moins de 550 mm en ligne droite, conformément à la norme ISO 13851)
- Fiabilité fonctionnelle et installation de dispositifs logiques externes
- Installation électrique conforme aux normes NEC et NFPA 79 ou IEC 60204

PRÉCAUTION:
- **Installez des commandes bimanuelles pour éviter toute activation accidentelle**
- Il n'est pas possible de protéger complètement le système de commande bimanuelle contre le contournement.
- L'utilisateur est tenu par les règlements OSHA de placer et de protéger les commandes manuelles afin de minimiser le risque d'actionnement accidentel ou de contournement.

PRÉCAUTION:
- **La commande de la machine doit disposer d'une commande anti-répétition.**
- Les normes des É.-U. et internationales pour les machines à simple course et à simple cycle exigent que la commande de la machine dispose d'une commande anti-répétition appropriée.
- Ce dispositif Banner Engineering peut servir à réaliser la commande anti-répétition uniquement si une étude de risques a été effectuée pour déterminer le bien-fondé de cette utilisation.

Distance de sécurité d'une commande bimanuelle (distance minimale)

Lorsque vous installez les deux commandes manuelles, celles-ci doivent être suffisamment éloignées du point de danger le plus proche pour que l'opérateur ne puisse pas atteindre la zone dangereuse avec la main ou une autre partie du corps avant l'arrêt du mouvement dangereux. Cette distance de séparation, ou de sécurité, peut être calculée comme suit :

AVERTISSEMENT:
- **Montage des commandes manuelles à une distance suffisante des pièces mobiles de la machine**
- Le non-respect de cette distance de sécurité (distance minimale) peut entraîner des blessures graves, voire mortelles.
- Montez les commandes manuelles conformément à la norme applicable. L'opérateur ou toute autre personne non qualifiée ne doit pas être en mesure de déplacer les commandes bimanuelles.

Installations américaines

Formule de la distance de sécurité, telle que spécifiée dans la norme ANSI B11.19 :

Machines à embrayages à révolution partielle (la machine et ses commandes lui permettent de s'arrêter pendant la partie dangereuse du cycle machine)

$$D_s = K \times (T_s + T_r) + D_{pf}$$

Machines à embrayage à révolution complète (la machine et ses commandes sont conçues pour effectuer un cycle complet)

$$D_s = K \times (T_m + T_r + T_h)$$

D_s
Distance de sécurité en pouces

K
Constante de vitesse de la main recommandée par les normes OSHA/ANSI (en pouces par secondes), dans la plupart des cas 63 in/sec (1600 mm/s) mais pouvant varier de 63 "/s à 100"/s (2540 mm/s) selon les circonstances de l'application.

Cette vitesse n'est pas déterminante. Il faut prendre en compte tous les facteurs, y compris les capacités physiques de l'opérateur, pour déterminer la valeur de K à utiliser.

T_h
Temps de réponse de la commande manuelle la plus lente (à partir du moment où la main quitte la commande jusqu'à ce que le contacteur s'ouvre).

T_h est généralement négligeable pour les interrupteurs purement mécaniques. Toutefois, T_h doit être pris en compte dans le calcul de la distance de séparation en cas d'utilisation de commandes manuelles électroniques ou électromécaniques.

Pour les boutons tactiles STB de Banner Engineering, le temps de réponse est égal à 0,02 seconde.

T_m
Temps maximum (en secondes) que prend la machine pour s'arrêter complètement après le déclenchement. Dans le cas de presses à embrayage à révolution complète avec un seul point d'embrayage, T_m est égal au temps nécessaire ou une révolution et demie du vilebrequin. Dans le cas de presses à embrayage à révolution complète avec plusieurs points d'embrayage, T_m est calculé comme suit :

$$T_m = (1/2 + 1/N) \times T_{cy}$$

N = nombre de points d'embrayage par révolution

T_{cy} = temps (en secondes) nécessaire à une révolution complète du vilebrequin

T_r
Temps de réponse du contrôleur de sécurité, mesuré à partir du moment où un signal d'arrêt est émis par l'une des deux commandes manuelles. Il est possible d'obtenir le temps de réponse du contrôleur de sécurité dans l'onglet **Résumé de la configuration** du logiciel.

T_s
Temps d'arrêt global de la machine (en secondes) depuis le signal d'arrêt initial jusqu'à l'arrêt définitif, incluant les temps d'arrêt de tous les éléments de commande concernés et mesuré à la vitesse la plus élevée de la machine.

T_s est généralement calculé à l'aide d'un appareil de mesure du temps d'arrêt. Si le temps d'arrêt spécifié est utilisé, ajoutez au moins 20 % comme facteur de sécurité pour pallier une éventuelle détérioration du système de freinage. Si les temps d'arrêt de deux éléments de commande redondants de la machine ne sont pas égaux, le temps le plus long doit être utilisé pour calculer la distance de séparation.

D_{pf}
Conformément à la norme ANSI B11.19, distance supplémentaire à prendre en compte pour éviter que la personne puisse atteindre la zone dangereuse avant qu'un arrêt de protection soit déclenché. Pour les applications de commande bimanuelle où l'empiètement vers le danger n'est pas limité, D_{pf} = 550 mm. Lorsque l'empiètement est obstrué (par exemple, protection des commandes d'actionnement bimanuelles, orientation du poste de travail, etc.), la distance d'accès (d_{ds}) peut être réduite à zéro. D_{pf} est aussi appelé « d_{ds} ».

Installations européennes

Formule de la distance minimale, telle que spécifiée dans la norme EN 13855 :

```
S = (K × T) + C
```

S

Distance minimale en mm

K

Constante de vitesse de la main recommandée par la norme EN 13855 (en millimètres par secondes), dans la plupart des cas 1600 mm/s mais pouvant varier de 1600 à 2500 mm/s selon les circonstances de l'application.

Cette vitesse n'est pas déterminante. Il faut prendre en compte tous les facteurs, y compris les capacités physiques de l'opérateur, pour déterminer la valeur de K à utiliser.

T

Temps de réponse global de la machine (en secondes), depuis l'activation physique du dispositif de sécurité jusqu'à la cessation définitive de tout mouvement.

C

La distance supplémentaire due au facteur de pénétration en profondeur correspond à 250 mm, selon la norme EN 13855. ISO/DIS 13855:2022 augmente le facteur C (d_{ds}) à 550 mm. Le facteur **C** de la norme EN 13855 peut être diminué si le risque d'empiètement est éliminé mais la distance de sécurité doit toujours être égale ou supérieure à 100 mm.

7.5.9 Tapis de sécurité

Le contrôleur de sécurité peut aussi servir à surveiller des tapis et des bordures de sécurité sensibles à la pression.

L'entrée Tapis de sécurité du contrôleur de sécurité a été conçue pour vérifier que les tapis de détection de présence à 4 fils fonctionnent bien. Il est possible de raccorder plusieurs tapis de sécurité en série à un contrôleur de sécurité, 150 ohms maximum par entrée (voir la section Options de raccordement du tapis de sécurité à la page 48).

Important: Le contrôleur de sécurité n'est pas conçu pour surveiller les tapis, pare-chocs ou bordures à 2 fils (avec ou sans résistance de détection).

Le contrôleur de sécurité surveille les contacts (plaques de contact) et le câblage d'un ou plusieurs tapis de sécurité pour détecter les défaillances et empêcher la machine de redémarrer en cas de défaillance. Le contrôleur de sécurité peut être configuré pour effectuer un reset après que l'opérateur se soit retiré du tapis ou, si le contrôleur est utilisé en mode de reset automatique, la fonction de reset doit être assurée par le système de commande de la machine. Cela empêche la machine surveillée de redémarrer automatiquement après que le tapis a été dégagé.

AVERTISSEMENT:

- **Application des tapis de sécurité**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Les conditions d'utilisation des tapis de sécurité varient selon la fiabilité des commandes ou la catégorie et le niveau de performance selon les normes ISO 13849-1 et ISO 13856. Bien que Banner Engineering recommande toujours le niveau de sécurité le plus élevé quelle que soit l'installation, l'utilisateur est responsable de l'installation, de l'utilisation et de l'entretien de tous les systèmes de sécurité selon les recommandations du fabricant, ainsi que de leur conformité aux lois et règlements concernés.
- N'utilisez pas les tapis de sécurité en guise de dispositif d'activation pour initier le mouvement d'une machine (comme dans le cas d'une application avec initiation par un dispositif de détection de présence), à cause du risque de démarrage ou redémarrage non prévu du cycle machine qui proviendrait d'une défaillance du tapis ou d'une erreur de câblage.
- N'utilisez pas les tapis de sécurité pour autoriser ou fournir un moyen à la commande de la machine de démarrer un mouvement dangereux en se tenant simplement sur le tapis de sécurité (par ex. au poste de commande). Ce type d'application utilise une logique inversée (négative) et certaines défaillances (par exemple, une perte d'alimentation du module) peuvent entraîner un faux signal d'activation.

Exigences en matière de tapis de sécurité

La conception, la construction et l'installation de capteur(s) de tapis de sécurité à 4 fils à interfacer avec le contrôleur de sécurité doit satisfaire les exigences minimales suivantes. Ces exigences sont extraites des normes ISO 13856-1, ANSI/RIA R15.06 et ANSI B11.19. L'utilisateur doit respecter toutes les normes et réglementations applicables.

Conception et construction d'un système de tapis de sécurité

Le capteur du tapis de sécurité, le contrôleur de sécurité et tous les dispositifs supplémentaires doivent avoir un temps de réponse suffisamment rapide pour réduire la possibilité qu'une personne puisse passer légèrement et rapidement sur la surface sensible du tapis de sécurité (moins de 100 ms à 200 ms, selon la norme appliquée).

Pour un système de tapis de sécurité, le capteur doit avoir une sensibilité minimale à un objet de 30 kg sur une pièce test en forme de disque de 80 mm de diamètre, n'importe où sur la surface sensible du tapis de sécurité, y compris aux raccords. La zone ou surface sensible effective doit être identifiable et peut comprendre un ou plusieurs capteurs. Le fabricant du tapis de sécurité doit indiquer ce poids et ce diamètre minimum en tant que sensibilité minimale aux objets du capteur.

L'utilisateur n'a pas le droit de modifier la force de déclenchement ni le temps de réponse (ISO 13856-1). Le détecteur doit être fabriqué pour éviter toute défaillance raisonnablement prévisible, par exemple l'oxydation des contacts qui pourrait entraîner une perte de sensibilité.

Le capteur doit avoir au minimum un indice de protection IP54. Si le capteur est conçu pour l'immersion dans l'eau, il doit avoir au minimum un indice d'étanchéité IP67. Le câblage d'interconnexion peut demander une attention particulière. Une pénétration capillaire peut laisser entrer du liquide dans le tapis, entraînant une perte de sensibilité du capteur. Il est parfois nécessaire de protéger le raccord de câblage dans un boîtier disposant d'un indice de protection approprié.

Le capteur ne doit pas être affecté par les conditions d'utilisation prévues du système. Les effets des liquides et d'autres substances doivent être pris en compte. Par exemple, une exposition à long terme à certains liquides peut détériorer ou faire gonfler le revêtement du capteur et provoquer une situation dangereuse.

La surface supérieure du détecteur doit être antidérapante pendant tout sa durée de vie ou il faut limiter les risques de glissement dans les conditions d'utilisation prévues.

Le raccordement à quatre fils entre les câbles et le détecteur doit supporter le déplacement et le transport du capteur par son câble sans entraîner de défaillance (par ex. un raccordement endommagé par une traction brutale ou répétée ou une flexion constante). S'il n'est pas possible d'avoir un raccordement suffisamment robuste, vous devez recourir à une autre méthode pour éviter toute défaillance, par exemple l'emploi d'un câble qui se déconnecte sans dommage ni danger.

Installation du tapis de sécurité

La qualité et la préparation de la surface d'installation du tapis de sécurité doivent répondre aux exigences indiquées par le fabricant du capteur. Des irrégularités de la surface de montage peuvent perturber le fonctionnement du tapis de sécurité et doivent être réduites au minimum acceptable. La surface d'installation doit être plane et propre. Évitez les systèmes de collecte de fluides à proximité du capteur ou sous celui-ci. Prenez les mesures requises pour éviter les défaillances dues à l'accumulation de poussières, de copeaux ou d'autres matériaux sous le ou les capteurs ou les fixations. Il faut particulièrement faire attention aux raccords entre les capteurs pour s'assurer que les corps étrangers ne s'accumulent pas sous ou dans le capteur.

Tout dommage (par ex. coupures, déchirures ou accrocs) de la gaine isolante externe du câble de raccord ou d'une partie externe du capteur doit être immédiatement réparé ou remplacé. L'entrée de particules de poussière, insectes, fluides, humidité, copeaux métalliques, etc. qui peuvent se trouver à proximité du tapis de sécurité peuvent provoquer une corrosion du capteur ou une perte de sensibilité.

Chaque tapis de sécurité doit être régulièrement inspecté et testé selon les recommandations du fabricant. Veillez à ne pas dépasser les spécifications d'utilisation (par ex. le nombre maximum de commutations).

Fixez solidement chaque tapis de sécurité pour éviter tout mouvement accidentel ou retrait non autorisé. Plusieurs méthodes sont possibles dont la fixation des bords, l'utilisation des vis à sens unique ou indévissables, le renfoncement du sol ou de la surface de montage en plus de la taille et du poids des tapis de grandes dimensions.

Chaque tapis de sécurité doit être installé pour limiter le risque de chute, surtout en direction de la machine. Il existe un risque de chute si la différence de hauteur par rapport à la surface horizontale adjacente est de 4 mm ou plus. Limitez les risques de chute aux raccords, aux jonctions et aux bords et en cas d'utilisation d'un revêtement supplémentaire. Pour éviter de tels risques, vous pouvez abaisser le tapis pour que sa surface soit au même niveau que le sol environnant ou installer une rampe qui ne doit pas dépasser 20° par rapport à l'horizontale. Utilisez des couleurs ou des marquages contrastés pour identifier les rampes et les bords.

Choisissez une taille de tapis et placez-le afin que personne ne puisse ni entrer dans la zone dangereuse sans être détecté, ni atteindre le danger avant que ce dernier ne se soit arrêté. Il est parfois nécessaire d'installer des protections ou dispositifs de protection supplémentaires pour éviter tout accès au danger en passant par-dessus, par-dessous ou autour de la surface de détection du dispositif.

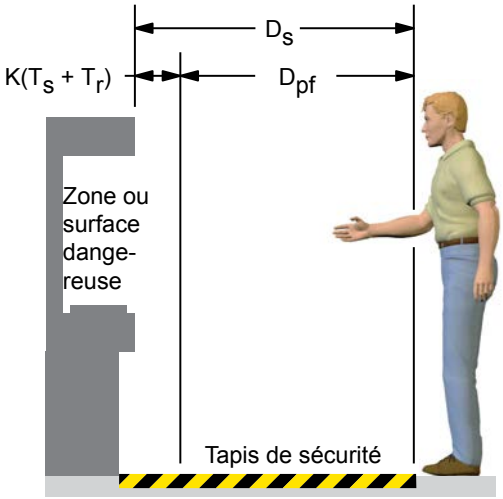
Quand vous installez un tapis de sécurité, vous devez envisager la possibilité d'enjamber la surface de détection sans être détecté. Les normes internationales et ANSI exigent que la profondeur de champ minimale de la surface du capteur (la plus petite distance entre le bord du tapis et le risque) soit comprise entre 750 mm et 1200 mm, en fonction de l'application et des normes applicables. Il faut également éviter toute possibilité de monter sur les supports de la machine ou d'autres objets pour contourner ou enjamber le capteur.

Distance de sécurité (distance minimale) pour le tapis de sécurité

En tant que protection autonome, le tapis de sécurité doit être installé à une distance de sécurité suffisante pour que le bord externe de la surface sensible soit situé à cette distance ou au-delà, sauf s'il est utilisé uniquement pour éviter un démarrage ou un redémarrage ou s'il est utilisé uniquement comme dispositif de dégagement (référez-vous aux normes ANSI B11.19, ANSI/RIA R15.06 et ISO 13855).

La distance de sécurité (minimale) prévue pour une installation dépend de plusieurs facteurs, dont la vitesse de la main (ou de l'individu), le temps d'arrêt total du système (qui comprend plusieurs critères de temps de réponse) et le facteur de pénétration en profondeur. Référez-vous à la norme appropriée pour déterminer la distance ou le moyen nécessaire pour éviter toute exposition du personnel au(x) risque(s).

Illustration 24. Détermination de la distance de sécurité pour le tapis de sécurité



Installations américaines

Formule de la distance de sécurité, telle que spécifiée dans la norme ANSI B11.19 :

$$D_s = K \times (T_s + T_r) + D_{pf}$$

D_s
Distance de sécurité en pouces

T_r
Temps de réponse du contrôleur de sécurité, mesuré à partir du moment où un signal d'arrêt est émis par l'une des deux commandes manuelles. Il est possible d'obtenir le temps de réponse du contrôleur de sécurité dans l'onglet **Résumé de la configuration** du logiciel.

K
Constante de vitesse de la main recommandée par les normes OSHA/ANSI (en pouces par secondes), dans la plupart des cas 63 in/sec (1600 mm/s) mais pouvant varier de 63 "/s à 100"/s (2540 mm/s) selon les circonstances de l'application.

Cette vitesse n'est pas déterminante. Il faut prendre en compte tous les facteurs, y compris les capacités physiques de l'opérateur, pour déterminer la valeur de K à utiliser.

T_s
Temps d'arrêt global de la machine (en secondes) depuis le signal d'arrêt initial jusqu'à l'arrêt définitif, incluant les temps d'arrêt de tous les éléments de commande concernés et mesuré à la vitesse la plus élevée de la machine.

T_s est généralement calculé à l'aide d'un appareil de mesure du temps d'arrêt. Si le temps d'arrêt spécifié est utilisé, ajoutez au moins 20 % comme facteur de sécurité pour pallier une éventuelle détérioration du système de freinage. Si les temps d'arrêt de deux éléments de commande redondants de la machine ne sont pas égaux, le temps le plus long doit être utilisé pour calculer la distance de séparation.

D_{pf}
Distance ajoutée par le facteur de pénétration en profondeur.

Équivaut à 48 pouces, conformément à la norme ANSI B11.19.

Installations européennes

Formule de la distance minimale, telle que spécifiée dans la norme EN 13855 :

$$S = (K \times T) + C$$

S
Distance minimale en mm

K

Constante de vitesse de la main recommandée par la norme EN 13855 (en millimètres par secondes), dans la plupart des cas 1600 mm/s mais pouvant varier de 1600 à 2500 mm/s selon les circonstances de l'application.

Cette vitesse n'est pas déterminante. Il faut prendre en compte tous les facteurs, y compris les capacités physiques de l'opérateur, pour déterminer la valeur de K à utiliser.

T

Temps de réponse global de la machine (en secondes), depuis l'activation physique du dispositif de sécurité jusqu'à la cessation définitive de tout mouvement.

C

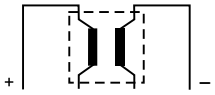
La distance supplémentaire due au facteur de pénétration en profondeur correspond à 1200 mm, selon la norme EN 13855.

Options de raccordement du tapis de sécurité

Les tapis de sécurité sensibles à la pression et les sols sensibles à la pression doivent répondre aux exigences de la catégorie pour lesquels ils sont spécifiés et marqués. Ces catégories sont définies dans la norme ISO 13849-1.

Le tapis de sécurité, son contrôleur de sécurité et tous les dispositifs de commutation des signaux de sortie doivent respecter, au minimum, les exigences de sécurité de la catégorie 1. Référez-vous aux normes ISO 13856-1 et ISO 13849-1 pour plus de détails sur les exigences à respecter.

Le contrôleur de sécurité est conçu pour surveiller des tapis de sécurité à 4 fils et n'est pas compatible avec les dispositifs à 2 fils (tapis, bordures de détection ou tout autre dispositif à deux fils et une résistance de détection).

4 fils
Ce circuit satisfait généralement les exigences de la norme ISO 13849-1 Catégorie 2 ou 3, en fonction du niveau de sécurité et de l'installation du ou des tapis. Le contrôleur de sécurité bascule en mode de verrouillage en cas de détection d'un fil à nu, d'un court-circuit au 0 V ou vers une autre source d'alimentation. 

7.5.10 Capteur d'inhibition

L'inhibition d'un dispositif de sécurité est la suspension automatique et contrôlée d'un ou de plusieurs signaux d'arrêt d'une entrée de sécurité pendant une partie du fonctionnement de la machine quand il n'existe pas de danger immédiat ou quand l'accès au danger est protégé. Les capteurs d'inhibition peuvent être assignés à un ou plusieurs dispositifs d'entrée de sécurité, notamment les suivants :

- Interrupteurs de verrouillage de sécurité
- Capteurs optiques
- Commandes bimanuelles
- Tapis de sécurité
- Arrêts de protection

Les normes américaines et internationales exigent de concevoir, d'installer et d'utiliser le système de sécurité de façon à protéger le personnel et à minimiser le risque de contournement du dispositif de protection.

Exemples de capteurs et d'interrupteurs d'inhibition

AVERTISSEMENT:

- **Prévention des installations dangereuses**
- Un mauvais réglage ou positionnement peut entraîner des blessures graves, voire mortelles.
- Deux ou quatre interrupteurs de position indépendants doivent être positionnés et réglés correctement pour se fermer uniquement lorsque le danger a été écarté et se rouvrir en fin du cycle ou si le risque se représente.
- L'utilisateur a la responsabilité de s'assurer que l'ensemble des lois, règlements, codes et normes locales, de l'état et nationales applicables à l'application sont respectés. Il est important de s'assurer que toutes les exigences des agences concernées ont été remplies et que toutes les instructions d'installation et d'entretien des manuels impliqués sont suivies.

Capteurs photoélectriques (mode barrière)

Les capteurs en mode barrière doivent être configurés pour une commutation sombre et avoir des contacts de sortie ouverts (non conducteurs) quand ils sont hors tension (OFF). L'émetteur et le récepteur de chaque paire doivent être alimentés à partir de la même source, afin de limiter le risque de défaillances de mode commun.

Capteurs photoélectriques (mode rétro-réflectif polarisé)

L'utilisateur doit s'assurer que les fausses alarmes (activation par des surfaces brillantes ou réfléchissantes) ne sont pas possibles. Les capteurs LP de Banner Engineering avec polarisation linéaire peuvent réduire ou éliminer cet effet.

Utilisez un capteur configuré pour une commutation claire (LO ou NO) afin d'initier une inhibition quand la cible ou la bande rétro-réfléchissante est détectée (position de base). Utilisez un capteur configuré pour une commutation sombre (DO ou NF) si la situation d'inhibition est déclenchée par le blocage d'un faisceau (entrée/sortie). Dans les deux cas, les contacts de sortie doivent être ouverts (non conducteurs) lorsque le système est hors tension.

Contacteurs de sécurité à ouverture positive

On utilise généralement deux (ou quatre) contacteurs indépendants, chacun avec au moins un contact de sécurité fermé pour initier le cycle d'inhibition. Une application qui utiliserait un contacteur unique avec un seul actionneur et deux contacts fermés peut entraîner une situation dangereuse.

Capteurs de proximité inductifs

En règle générale, les capteurs de proximité inductifs servent à initier un cycle d'inhibition en cas de détection d'une surface métallique. N'utilisez pas de capteurs à deux fils en raison du risque de fuite excessive de courant pouvant entraîner une fausse situation d'activation (On). Seuls des capteurs à trois ou quatre fils ayant des sorties PNP logiques ou à contacts rigides séparés de l'alimentation d'entrée peuvent être utilisés.

Conditions des dispositifs d'inhibition

Les dispositifs d'inhibition doivent répondre au minimum aux conditions suivantes :

1. Il doit y avoir un minimum de deux dispositifs d'inhibition câblés indépendamment l'un de l'autre.
2. Les dispositifs d'inhibition doivent satisfaire à l'une des conditions suivantes : contacts normalement ouverts, sorties PNP (répondant toutes deux aux exigences d'entrée indiquées dans la section Spécifications et exigences à la page 21) ou action de commutation complémentaire. Au moins un des contacts doit se fermer quand le commutateur est actionné et doit s'ouvrir (ou être non conducteur) quand l'interrupteur n'est pas actionné ou en mode hors tension.
3. L'activation des entrées vers la fonction d'inhibition doit provenir de sources distinctes. Ces sources doivent être montées séparément pour éviter de déclencher une inhibition non intentionnelle résultant d'un mauvais réglage ou alignement ou d'une défaillance de mode commun, par exemple un dommage physique de la surface de montage. Seule l'une de ces sources peut traverser, ou être affectée par, un API ou un dispositif similaire.
4. Les dispositifs d'inhibition doivent être installés de façon à ce qu'ils ne puissent pas être aisément contournés.
5. Les dispositifs d'inhibition doivent être montés de façon à ce que leur position et leur alignement ne puissent pas être facilement modifiés.
6. Il faut absolument empêcher qu'une condition environnementale (contamination extrême de l'air par exemple) puisse initier une inhibition.
7. Les dispositifs d'inhibition ne doivent pas être configurés pour utiliser une fonction de retard ou de temporisation quelconque (sauf si ces fonctions sont exécutées de telle sorte qu'aucune défaillance unique d'un composant n'empêche l'élimination du risque et l'arrêt des cycles machine suivants jusqu'à ce que la défaillance soit corrigée et qu'aucun nouveau risque ne survienne en raison de l'extension de la période d'inhibition).

7.5.11  Interrupteur de dérivation

Toujours effectuée sous le contrôle d'un superviseur, la dérivation d'un dispositif de sécurité est une suspension temporaire activée manuellement d'un ou plusieurs signaux d'arrêt des entrées de sécurité quand il n'y a pas de risque immédiat. Pour ce faire, il faut généralement sélectionner un mode de dérivation utilisant un interrupteur à clé pour faciliter la configuration de la machine, l'alignement/ajustement de faisceaux, l'apprentissage d'un robot et la résolution de problèmes liés aux processus.

Les interrupteurs de dérivation peuvent être assignés à un ou plusieurs dispositifs d'entrée de sécurité et notamment les suivants :

- Interrupteurs de verrouillage de sécurité
- Capteurs optiques
- Commandes bimanuelles
- Tapis de sécurité
- Arrêt de protection

Exigences en matière de dérivation des protections

Les exigences relatives à la dérivation d'un dispositif de sécurité sont les suivantes [11]:

- La fonction de dérivation doit être temporaire.
- Le mécanisme de sélection ou d'activation de la dérivation doit pouvoir être supervisé.
- Le fonctionnement automatique de la machine doit être interdit en limitant l'ampleur du mouvement, sa vitesse ou sa puissance (par ex. en n'utilisant que le mode d'approche, pas à pas ou à vitesse lente). Le mode de dérivation ne doit pas être utilisé pour la production.
- Des protections supplémentaires doivent être mises en place. Le personnel ne doit pas être exposé aux dangers.
- Le mécanisme de dérivation doit être bien en vue de l'emplacement de la protection qui est dérivée.

[11] Ce résumé a été compilé à partir de différentes sources dont les normes NFPA79, ANSI/RIA R15.06, ISO 13849-1, IEC60204-1 et ANSI B11.19. L'utilisateur est tenu de vérifier les protections requises par ces spécifications et toutes les autres lois et réglementations applicables.

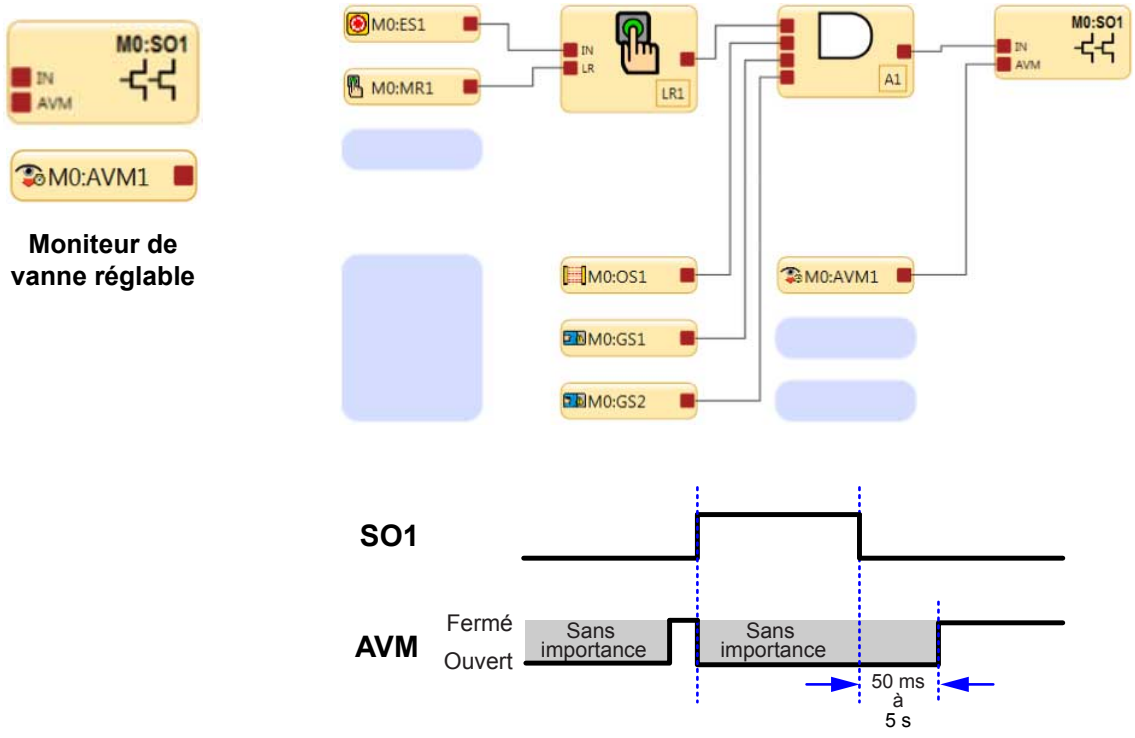
- L’initiation du mouvement ne doit être possible qu'avec une commande qui doit être maintenue pour fonctionner.
- Tous les arrêts d’urgence doivent rester actifs.
- Le mécanisme de dérivation doit être employé au même niveau de fiabilité que la protection.
- Une indication visuelle de la dérivation du dispositif de protection doit être en place et être clairement visible de l’emplacement de la protection.
- Le personnel doit être formé à l’utilisation de la protection et à l’utilisation de la dérivation.
- Il faut effectuer une étude de risques et une réduction des risques (selon la norme applicable).
- Le reset, l'actionnement, la désactivation ou l'activation du dispositif de protection ne doit pas initier de mouvement dangereux ni créer de situation dangereuse.

La dérivation d'un dispositif de protection ne doit pas être confondue avec *« l'inhibition »*, qui correspond à une suspension automatique et temporaire de la fonction de protection d’un dispositif de sécurité pendant une partie non dangereuse du cycle machine. L'inhibition permet d'introduire manuellement ou automatiquement un objet ou un produit dans une machine ou un processus sans déclencher de commande d'arrêt. Un autre terme souvent confondu avec la dérivation est le « *blanking* » (suppression de faisceau) qui désensibilise une partie du champ de détection d'un dispositif de sécurité optique (par ex. en désactivant un ou plusieurs faisceaux d'une barrière immatérielle de sécurité) afin d'ignorer une intrusion dans le champ d'un faisceau spécifique.

7.5.12 Fonction AVM (Adjustable Valve Monitoring - surveillance de vanne réglable)

D'un point de vue fonctionnel, la fonction AVM (Adjustable Valve Monitoring) est similaire à l'EDM (External Device Monitoring - surveillance des commutateurs externes) une voie (voir Surveillance des commutateurs externes (EDM) à la page 74). La fonction AVM surveille l'état du ou des dispositifs contrôlés par la sortie de sécurité à laquelle la fonction est assignée. Lorsque la sortie de sécurité se désactive, l'entrée AVM doit avoir le niveau haut/être activée (tension de +24 Vcc appliquée) avant que la temporisation de la fonction AVM expire sans quoi un verrouillage se produit. L'entrée AVM doit également avoir le niveau haut/être activée lorsque la sortie de sécurité tente de s'activer sans quoi un verrouillage se produit.

Illustration 25. Logique de temporisation — Fonction AVM



L'AVM (Adjustable Valve Monitoring, Moniteur de vanne réglable) est une méthode permettant de vérifier le fonctionnement de vannes double voie. Les contacts de surveillance N.F. à guidage forcé des vannes sont utilisés comme entrée pour détecter un défaut de type « blocage en position On » et empêchent l'activation des sorties du contrôleur de sécurité.

Remarque: Il est possible de régler le délai de 50 ms à 5 s par intervalle de 50 ms (la valeur par défaut est 50 ms).

La fonction AVM (Adjustable Valve Monitoring) est utile pour assurer une surveillance dynamique des dispositifs sous le contrôle de la sortie de sécurité dans l'éventualité où ils ralentiraient, se coinceraient ou tomberaient en panne dans une position ou un état sous tension et dont le fonctionnement doit être vérifié après l'envoi d'un signal d'arrêt. A titre d'exemple, citons les solénoïdes simples ou doubles qui contrôlent les mécanismes d'embrayage/freinage et les capteurs de position qui surveillent la position initiale d'un vérin linéaire.

Pour synchroniser ou contrôler la temporisation différentielle maximale entre deux ou plusieurs dispositifs, par exemple les doubles solénoïdes, vous pouvez assigner plusieurs fonctions AVM à une même sortie de sécurité et configurer la temporisation des AVM avec les mêmes valeurs. Il est possible d'assigner un nombre quelconque d'entrées AVM à une même sortie de sécurité. Un signal d'entrée peut être généré par une sortie PNP transistorisée ou à contact de relais/mécanique.

AVERTISSEMENT:

- **Surveillance des vannes proportionnelles (AVM)**
- Lorsque la fonction AVM est utilisée, la ou les sortie(s) de sécurité ne s'activent pas tant que l'entrée AVM n'est pas satisfaite. Cela peut se traduire par un retard à l'enclenchement correspondant au temps de surveillance configuré pour l'AVM.
- C'est à l'utilisateur qu'il incombe de configurer correctement le temps de surveillance de l'AVM selon l'application et d'avertir les utilisateurs de la machine de la possibilité d'une temporisation à l'enclenchement, ce dont l'opérateur de la machine ou d'autres membres du personnel ne sont peut-être pas conscients.

7.5.13 ISD Entrées ISD

Des entrées ISD sont disponibles sur les modèles SC10-2 et XS26-ISD.

Les entrées de sécurité SC10

- ISD Ethernet IN3/IN4 Chaîne 2
- ISD Ethernet IN5/IN6 Chaîne 1

et les entrées de sécurité XS26-ISD

- ISD Ethernet IN1/IN2 Chaîne 1
- ISD Ethernet IN3/IN4 Chaîne 2
- ISD Ethernet IN5/IN6 Chaîne 3
- ISD Ethernet IN7/IN8 Chaîne 4
- ISD Ethernet IN9/IN10 Chaîne 5
- ISD Ethernet IN11/IN12 Chaîne 6
- ISD Ethernet IN13/IN14 Chaîne 7
- ISD Ethernet IN15/IN16 Chaîne 8

peuvent être utilisées pour surveiller des chaînes de dispositifs avec des données ISD (In-Series Diagnostic) incorporées, par exemple les interrupteurs de sécurité SI-RFD Banner, les boutons d'arrêt d'urgence lumineux compatibles ISD Banner ou le système ISD Connect de Banner. Les interrupteurs de sécurité SI-RFD de Banner utilisent la technologie RFID comme méthode de détection.

Les dispositifs compatibles ISD ont une longueur de câble maximum de 30 mètres entre les dispositifs ainsi qu'entre le dernier dispositif et le contrôleur.

Remarque: La réponse du contrôleur de sécurité est basée sur l'état des dispositifs de commutation du signal de sortie (OSSD) des entrées ISD et non sur les informations ISD transportées sur les OSSD. Les informations ISD sont des informations d'état de la chaîne ou du dispositif non liées à la sécurité.

Les dispositifs ISD, comme les interrupteurs de sécurité SI-RFD, doivent être placés à une distance de sécurité appropriée (distance minimale), conformément aux normes de l'application. Référez-vous aux normes applicables et à la documentation de votre dispositif pour les calculs. Le temps de réponse des sorties du contrôleur de sécurité à chaque entrée de sécurité figure dans la vue **Résumé de la configuration** du logiciel. Celui-ci doit être ajouté au temps de réponse de la chaîne de dispositifs ISD. Consultez les manuels individuels des dispositifs ISD pour déterminer le temps de réponse de la chaîne ISD.

Les sorties électroniques des dispositifs ISD actifs sont (et doivent être) capables de détecter les courts-circuits externes à l'alimentation, à la terre et entre elles. Les dispositifs se verrouillent en cas de détection d'un tel court-circuit.

Si l'installation comporte un risque d'enfermement (une personne peut passer par une porte ouverte et ne pas être détectée dans la zone dangereuse), il peut être nécessaire d'ajouter d'autres protections et de sélectionner le reset manuel. Référez-vous à la section Entrée de reset manuel à la page 62.

AVERTISSEMENT:
- Configuration conforme aux normes applicables
- Le fait de ne pas vérifier l'application peut entraîner des blessures graves, voire mortelles.
- Le logiciel Banner Safety Controller vérifie principalement la configuration logique pour détecter les erreurs de connexion. Il incombe à l'utilisateur de vérifier que l'application répond aux exigences de l'évaluation des risques et qu'elle est conforme à toutes les normes applicables.
- L'utilisateur est responsable du raccordement de la chaîne ISD en fonction de la configuration ; les erreurs de longueur de chaîne et/ou d'ordre sont uniquement signalées via Ethernet (entrée toujours considérée comme ON).

Important: Le constructeur de la machine (l'utilisateur) est tenu de s'assurer que le câblage ne peut pas être facilement manipulé par un opérateur pour contourner la ou les fonctions de sécurité, par exemple, rendre impossible le retrait d'un dispositif du système.

Remarque: Dans une longue chaîne ou des chaînes comportant de nombreux dispositifs ISD, la tension du premier dispositif (le plus proche du connecteur d'extrémité) doit rester au-dessus de 19,5 volts pour que la chaîne fonctionne correctement.

Remarque: Le logiciel Contrôleur de sécurité Banner applique les règles de l'interrupteur de porte aux entrées ISD.

Demande d'informations d'état et de performance sur un dispositif individuel via ISD

Utilisez la procédure suivante pour obtenir des informations de performance et d'état sur un dispositif ISD individuel via ISD.

1. Modifiez le registre Chaîne ISD demandé pour qu'il corresponde au numéro de chaîne ISD du dispositif en question (1 ou 2).
2. Modifiez le registre Dispositif ISD demandé pour qu'il corresponde au numéro de l'appareil en question (1 à 32).
3. Basculez le registre Demande de lecture ISD de 0 à 1 pour effectuer une lecture ponctuelle.
4. Observez la table Données spécifiques à un dispositif ISD individuel pour lire les données du dispositif requis.

Demander la liste des dispositifs et recréer une base de référence pour une chaîne ISD via ISD

Utilisez la procédure suivante pour obtenir une liste des dispositifs ISD dans l'ordre d'une chaîne et pour réinitialiser la base de référence.

1. Entrez le numéro de chaîne souhaité dans le registre Chaîne ISD demandé (1–8).
2. Entrez `2` dans le registre Demande de lecture ISD.

   Lorsque le registre Accusé réc. demande de lecture ISD indique également `2`, le processus est terminé. Une table de 32 octets est fournie dans la liste des dispositifs ISD détectés sur un bloc de registre Chaîne, indiquant le code de chaque dispositif ISD, et une nouvelle base de référence pour le nombre de dispositifs, le type et l'ordre est établie.

Demander la liste des dispositifs et effacer l'indicateur de changement de nombre dans une chaîne ISD via ISD

Utilisez la procédure suivante pour obtenir une liste des dispositifs ISD dans l'ordre d'une chaîne et pour effacer l'indicateur de changement de nombre.

1. Entrez le numéro de chaîne souhaité dans le registre Chaîne ISD demandée (1–8).
2. Entrez `4` dans le registre Demande de lecture ISD.
   Lorsque le registre Accusé réc. demande de lecture ISD indique également `4`, le processus est terminé. Une table de 32 octets est fournie dans la liste des dispositifs ISD détectés sur un bloc de registre Chaîne, indiquant le code de chaque dispositif ISD.

Remarque: Cela n'établit pas de nouvelle base de référence.

État système de la chaîne ISD

Banner Engineering a créé quelques mots (word) auxquels l'API peut rapidement accéder pour indiquer la présence éventuelle de problèmes liés à la chaîne ISD.

Remarque: Les données ISD ne sont pas immédiatement disponibles à la mise sous tension. Les données ISD peuvent être retardées jusqu'à 10 secondes après la mise sous tension du système.

Ces informations ont le format suivant :

Informations	Type	Taille des données	Procédure de résolution
Le nombre de systèmes dans la chaîne ISD ne correspond pas à la configuration [12]	Alerte du contrôleur	1 bit	Vérifiez que le nombre d'unités physiques correspond au nombre configuré dans la chaîne.
L'ordre des systèmes dans la chaîne ISD ne correspond pas à la configuration [12]	Alerte du contrôleur	1 bit	Vérifiez que l'ordre des unités physiques correspond à l'ordre configuré. Notez l'emplacement de la fiche de terminaison et du contrôleur.
Mise à jour des données ISD en attente (pas de données ou données en mémoire tampon)	Alerte du contrôleur	1 bit	Causé par des dispositifs non ISD en chaîne ou une situation de mise en mémoire tampon. Si les données ne sont pas présentes dès la mise sous tension (jamais présentes) : • Vérifiez que tous les dispositifs de la chaîne ISD sont des dispositifs compatibles ISD. Si les données étaient présentes mais ont ensuite été perdues : • Vérifiez que la chaîne n'a pas été rompue. • Les données ont pu être interrompues et reviendront dans quelques secondes.
Dispositif non valide (non ISD) dans la chaîne ISD	Alerte du contrôleur	1 bit	Des types de données incorrects sont reçus • Vérifiez que tous les dispositifs de la chaîne ISD sont des dispositifs Banner compatibles ISD.
Dispositif ISD détecté mais non configuré (*réservés* dans le dispositif XS26-ISD)	Information	1 bit	• Vérifiez que la chaîne ISD est câblée aux bornes adéquates. • Vérifiez que le type de dispositif d'entrée (ISD) sélectionné est adapté pour cette entrée dans la configuration.
Connecteur d'extrémité manquant dans la chaîne ISD	État ISD	1 bit	• Vérifiez que la fiche de terminaison ne s'est pas détachée. • Vérifiez que la chaîne n'a pas été rompue (connexions détachées).
Pas d'apprentissage de l'actionneur par le capteur SI-RF à codage unique ou élevé	Défaut ISD	1 bit	Un commutateur SI-RF (-UP8 ou -HP8) n'a pas été appris • Configurez l'unité à son actionneur selon les instructions de la fiche technique Banner p/n 208885.
Mauvais actionneur présenté à un capteur à codage unique ou élevé	Défaut ISD	1 bit	Un commutateur SI-RF (-UP8 ou -HP8) détecte un actionneur, mais pas celui pour lequel il a été configuré. • Vérifiez qu'il n'y a pas eu d'altération (utilisation d'un mauvais actionneur). • Apprenez le nouvel actionneur au capteur à code élevé (-HP8).
Erreur interne sur un dispositif ISD de la chaîne	Défaut ISD	1 bit	• Vérifiez quel dispositif présente l'erreur, puis mettez le système sous tension. • Si l'erreur persiste, remplacez le dispositif.

[12] XS26-ISD FID 5 ou ultérieur (uniquement si vous n'utilisez pas le mode de détection automatique) et SC10 FID 2 ou ultérieur.

Informations	Type	Taille des données	Procédure de résolution
Défaut de sortie ISD détecté, compteur de désactivation de sortie enclenché	Défaut ISD	1 bit	La sortie du dispositif ISD s'éteindra dans 20 minutes. • Vérifiez quel dispositif présente l'erreur, recherchez des courts-circuits dans le câblage. • Mettez le système sous tension. Si le problème persiste, remplacez le dispositif.
Changement de chaîne ISD détecté (uniquement dans XS26-ISD FID 5 ou ultérieur)	État ISD	1 bit	Si la fonction AutoDetect ISD est configurée et que la longueur ou l'ordre d'une chaîne ISD a changé, ce drapeau est activé et doit être reconnu par l'automate. Référez-vous à la section Demander la liste des dispositifs et recréer une base de référence pour une chaîne ISD via ISD à la page 52.
Changement du nombre de dispositifs ISD par rapport à la référence détectée	État ISD	1 bit	Le nombre de dispositifs ISD a changé par rapport au nombre de référence, vérifiez que le nombre de dispositifs de la chaîne correspond à la configuration de la machine. Référez-vous à la section Demander la liste des dispositifs et effacer l'indicateur de changement de nombre dans une chaîne ISD via ISD à la page 52.
Statut du dispositif de commutation du signal de sortie (OSSD) de la chaîne ISD	État ISD	1 bit	

Données spécifiques à un dispositif ISD individuel

Remarque: Les données ISD ne sont pas immédiatement disponibles à la mise sous tension. Les données ISD peuvent être retardées jusqu'à 10 secondes après la mise sous tension du système.

Informations	Taille des données	Applicable au dispositif Banner (Oui/Non/Réservé)		
		SI-RF	Interrupteur	ISD Connect
Défaut d'entrée de sécurité	1 bit	Y	Y	Y
réservé	1 bit	*réservé*	*réservé*	*réservé*
Capteur non couplé	1 bit	Y	N	N
Erreur de données ISD	1 bit	Y	Y	Y
Mauvais actionneur/État du bouton/État de l'entrée	1 bit	Y	Y	Y
Portée marginale/État du bouton/État de l'entrée	1 bit	Y	Y	Y
Actionneur détecté	1 bit	Y	N	N
Erreur de sortie	1 bit	Y	Y	Y
Entrée 2	1 bit	Y	Y	Y
Entrée 1	1 bit	Y	Y	Y
Reset local attendu	1 bit	Y	Y	N
Avertissement de tension de fonctionnement	1 bit	Y	Y	Y
Erreur de tension de fonctionnement	1 bit	Y	Y	Y
Sortie 2	1 bit	Y	Y	Y
Sortie 1	1 bit	Y	Y	Y
Remise sous tension requise	1 bit	Y	Y	Y

Informations	Taille des données	Applicable au dispositif Banner (Oui/Non/Réservé)		
		SI-RF	Interrup-teur	ISD Con-nect
Sorties à tolérance de panne	1 bit	Y	Y	Y
Dispositif de reset local	1 bit	Y	Y	N
En cascade	1 bit	Y	Y	Y
Niveau de codage élevé	1 bit	Y	N	N
Apprentissages restants	4 bits	Y	N	N
ID dispositif	5 bits	Y	Y	Y
Nombre d'avertissements de portée	6 bits	Y	N	N
Délai de désactivation de la sortie	5 bits	Y	Y	Y
Nombre d'erreurs de tension	8 bits	Y	Y	Y
Température interne [13]	8 bits	Y	Y	Y
Distance de l'actionneur [13]	8 bits	Y	N	N
Tension d'alimentation [13]	8 bits	Y	Y	Y
Nom de société attendu	4 bits	Y	N (toujours « 6 »)	N (toujours « 6 »)
Nom de société reçu	4 bits	Y	N	N
Code attendu	16 bits	Y	N	N
Code reçu	16 bits	Y	N	N
Erreur interne A	16 bits	Y	Y	Y
Erreur interne B	16 bits	Y	Y	Y

Dispositif SI-RF

Dans le cas d'un interrupteur de porte ISD (SI-RF), les données spécifiques à un dispositif ISD individuel renvoyées par le dispositif SI-RF ont le format suivant :

Informations	Taille des données
Défaut d'entrée de sécurité	1 bit
réservé	1 bit
Capteur non couplé	1 bit
Erreur de données ISD	1 bit
Mauvais actionneur	1 bit
Portée marginale	1 bit
Actionneur détecté	1 bit
Erreur de sortie	1 bit
Entrée 2	1 bit
Entrée 1	1 bit
Reset local attendu	1 bit
Avertissement de tension de fonctionnement	1 bit
Erreur de tension de fonctionnement	1 bit
Sortie 2	1 bit
Sortie 1	1 bit
Remise sous tension requise	1 bit

[13] Pour la conversion de la température interne, de la distance de l'actionneur et de la tension, voir la section ISD : Informations sur la conversion de la distance, tension et température à la page 309.

Informations	Taille des données
Sorties à tolérance de panne	1 bit
Dispositif de reset local	1 bit
En cascade	1 bit
Niveau de codage élevé	1 bit
Apprentissages restants	4 bits
ID de dispositif	5 bits
Nombre d'avertissements de portée	6 bits
Délai de désactivation de la sortie	5 bits (la valeur de 31 signifie que le minuteur est désactivé)
Nombre d'erreurs de tension	8 bits
Température interne [14]	8 bits
Distance de l'actionneur [14]	8 bits
Tension d'alimentation [14]	8 bits
Nom de société attendu	4 bits
Nom de société reçu	4 bits
Code attendu	16 bits
Code reçu	16 bits
Erreur interne A	16 bits
Erreur interne B	16 bits

Dispositif d'arrêt d'urgence et connecteur ISD Connect

Dans le cas d'un bouton d'arrêt d'urgence ISD ou d'un connecteur ISD Connect, les données spécifiques au dispositif ISD renvoyées ont le format suivant :

Informations	Taille des données
Défaut d'entrée de sécurité	1 bit
réservé	2 bits
Erreur de données ISD	1 bit
réservé	3 bits
Erreur de sortie	1 bit
Entrée 2	1 bit
Entrée 1	1 bit
Reset local attendu	1 bit (toujours faux pour les connecteurs ISD Connect)
Avertissement de tension de fonctionnement	1 bit
Erreur de tension de fonctionnement	1 bit
Sortie 2	1 bit
Sortie 1	1 bit
Remise sous tension requise	1 bit
Sorties à tolérance de panne	1 bit (toujours vrai pour les boutons d'arrêt d'urgence et connecteurs ISD Connect)

[14] Pour la conversion de la température interne, de la distance de l'actionneur et de la tension, voir la section ISD : Informations sur la conversion de la distance, tension et température à la page 309.

Informations	Taille des données
Dispositif de reset local	1 bit (toujours faux pour les connecteurs ISD Connect)
En cascade	1 bit (toujours vrai pour les boutons d'arrêt d'urgence et connecteurs ISD Connect)
réservé	5 bits
ID de dispositif	5 bits (toujours une valeur de 7 pour les boutons d'arrêt d'urgence ISD) (toujours une valeur de 9 pour les connecteurs ISD Connect)
réservé	6 bits
Délai de désactivation de la sortie	5 bits (la valeur de 31 signifie que le minuteur est désactivé)
Nombre d'erreurs de tension	8 bits
Température interne [15]	8 bits
réservé	8 bits
Tension d'alimentation [15]	8 bits
Nom de société attendu	4 bits (toujours une valeur de 6 pour les boutons d'arrêt d'urgence et connecteurs ISD Connect)
réservé	36 bits
Erreur interne A	16 bits
Erreur interne B	16 bits

7.5.14 Démarrage d'un cycle pour un bloc fonction Commande de presse

Cette fonction est disponible sur le XS/SC26 FID 4 et ultérieur.

Un actionneur momentané unique peut être utilisé comme dispositif de démarrage pour les petites presses hydrauliques/pneumatiques lorsqu'il est utilisé avec le bloc fonction Commande de presse configuré pour une commande à actionneur unique. Il s'agit d'une entrée de démarrage pour démarrer le cycle de la presse. Lorsque la commande à actionneur unique est sélectionnée, l'opérateur peut démarrer le cycle avec cette entrée, puis la désactiver et effectuer d'autres tâches.

PRÉCAUTION: D'autres moyens doivent être prévus pour garantir la protection des opérateurs contre les risques car leurs mains n'ont pas à actionner le bouton pendant tout le mouvement de la presse.

L'accès au danger doit être protégé par des moyens autres qu'un bouton de maintien en position ouverte, par exemple des barrières lumineuses, des portails, etc. Ces dispositifs de sécurité doivent également être connectés aux entrées du bloc fonction Commande de presse.

L'entrée Démarrage de cycle peut être connectée au nœud GO du bloc fonction Commande de presse ou au nœud IN d'un bloc de dérivation qui est connecté au nœud GO du bloc fonction Commande de presse.

Le dispositif de démarrage de cycle doit être monté à un endroit qui respecte l'avertissement suivant.

[15] Pour la conversion de la température interne, de la distance de l'actionneur et de la tension, voir la section ISD : Informations sur la conversion de la distance, tension et température à la page 309.

AVERTISSEMENT:
- **Installez correctement les dispositifs de démarrage de cycle.**
- Si les dispositifs de démarrage de cycle ne sont pas correctement installés, des dommages corporels graves ou mortels ne sont pas à exclure.
- Installez les dispositifs de démarrage de cycle de manière à ce qu'ils soient uniquement accessibles de l'extérieur et bien en vue de la zone protégée. Les dispositifs de démarrage de cycle ne peuvent pas être accessibles depuis la zone protégée. Protégez les dispositifs de démarrage de cycle contre toute utilisation accidentelle ou non autorisée (à l'aide d'anneaux ou de protections). S'il existe des zones dangereuses qui ne sont pas visibles depuis les dispositifs de démarrage de cycle, prévoyez des mesures de protection supplémentaires.

7.5.15  Fonction d'arrêt séquentiel de la commande de la presse (SQS)

Cette fonction est disponible sur le XS/SC26 FID 4 et ultérieur.

L'entrée SQS (arrêt séquentiel de la commande de la presse) fournit un signal au système de contrôle de la presse indiquant que le coulisseau de la presse a atteint une position telle qu'il n'y a plus de risque d'écrasement (moins de 6 mm d'écart). À ce stade, le mouvement descendant du coulisseau s'arrête. L'opérateur peut retirer ses mains de la commande bimanuelle pour s'assurer que la pièce à usiner est bien placée (l'entrée d'arrêt d'urgence inhibable est alors inhibée). Une fois que l'opérateur s'est assuré que la pièce à usiner est dans la bonne position, il engage l'entrée de l'interrupteur au pied pour terminer la course descendante.

Remarque: Ce qui précède est une méthode de contrôle du processus de commande de la presse. Il existe trois processus autorisés :

1. L'entrée Commande manuelle (TC1) active l'entrée GO pour entraîner le coulisseau au point SQS. Relâchez TC1 et engagez le FS1 pour activer l'entrée Ft Switch (Interrupteur au pied) et entraîner le coulisseau vers le point Bas de course (BOS), relâchez FS1 et engagez TC1 pour monter le coulisseau.
2. FS1 active l'entrée GO pour entraîner le coulisseau au point SQS. relâchez FS1. Si vous réengagez FS1, le coulisseau est entraîné au point BOS (bas de course), puis à nouveau au point TOS (haut de course). (L'entrée Ft Switch disparaît lorsque FS1 est connecté au nœud GO.)
3. TC1 active l'entrée GO pour entraîner le coulisseau au point SQS. Vous pouvez alors relâcher TC1. La réactivation de TC1 entraîne le coulisseau au point BOS, puis le ramène au point TOS. (Pour configurer le système pour cette méthode, ne sélectionnez PAS le nœud Ft Switch dans le bloc fonction Entrées de commande de presse.)

Remarque: L'entrée Arrêt séquentiel est généralement utilisée lorsque Dual Pression (double pression) est sélectionné. La fonction Dual Pressure nécessite quatre sorties de sécurité (haut, bas, basse pression et haute pression). Pour cette raison, l'entrée Arrêt séquentiel n'est pas disponible sur les modèles non extensibles.

L'entrée Arrêt séquentiel peut inhiber directement l'entrée Arrêt d'urgence inhibable ou elle peut fonctionner conjointement avec l'entrée Capteur d'inhibition de commande de presse pour inhiber l'entrée Arrêt d'urgence inhibable du système de commande de presse (pour en savoir plus sur l'entrée Capteur d'inhibition de commande de presse, voir Capteur d'inhibition de la commande de presse à la page 59).

L'entrée Arrêt séquentiel peut être une entrée à simple ou double voie selon les exigences du système. Les dispositifs d'entrée doivent être positionnés de manière à ce que le coulisseau de la presse s'arrête dans une position qui ne présente pas d'espace suffisant pour y introduire un doigt (cet espace doit être inférieur à 6 mm).

Remarque: Si une configuration à simple voie est sélectionnée pour l'entrée Arrêt séquentiel, elle doit fonctionner conjointement avec l'entrée Capteur d'inhibition de commande de presse pour inhiber l'entrée d'arrêt d'urgence inhibable de la commande de presse. Si une configuration à deux voies est sélectionnée pour l'entrée Arrêt séquentiel, elle peut directement inhiber l'entrée d'arrêt d'urgence inhibable de la commande de presse.

Les normes américaines et internationales exigent de concevoir, d'installer et d'utiliser le système de sécurité de façon à protéger le personnel et à minimiser le risque de contournement du dispositif de protection.

AVERTISSEMENT:
- Prévention des installations dangereuses
- Un dispositif SQS à une voie n'est pas autorisé, sauf s'il est utilisé en conjonction avec un dispositif d'entrée de type PCMS (capteur d'inhibition de commande de presse). Lorsqu'une entrée SQS à deux voies est utilisée sans capteur d'inhibition PCMS, chaque voie SQS doit être un commutateur de position indépendant et doit être correctement réglée ou positionnée pour se fermer uniquement lorsque le danger a été écarté et se rouvrir en fin de cycle ou si le risque se représente. Si ces interrupteurs étaient mal positionnés ou réglés, des blessures graves, voire mortelles, pourraient en résulter.
- L'utilisateur est tenu de respecter l'ensemble des législations, réglementations, règlements et codes locaux et nationaux concernant l'utilisation de l'équipement de sécurité adéquat dans une application particulière. Veillez à respecter toutes les exigences légales ainsi que les instructions d'installation et de maintenance des manuels appropriés.

Les dispositifs SQS doivent répondre au minimum aux conditions suivantes. Si le dispositif SQS est utilisé comme entrée d'inhibition avec le capteur d'inhibition de commande de presse, la paire doit satisfaire les exigences suivantes :

1. Il doit y avoir un minimum de deux dispositifs câblés indépendamment l'un de l'autre.
2. Les dispositifs doivent satisfaire à l'une des conditions suivantes : contacts normalement ouverts, sorties PNP (répondant toutes deux aux exigences d'entrée indiquées dans la section Spécifications et exigences à la page 21) ou action de commutation complémentaire. Au moins un des contacts doit se fermer quand le commutateur est actionné et doit s'ouvrir (ou être non conducteur) quand l'interrupteur n'est pas actionné ou en mode hors tension.
3. L'activation des entrées de cette fonction d'inhibition doit provenir de sources distinctes. Ces sources doivent être montées séparément pour éviter tout danger résultant d'un mauvais réglage ou alignement ou d'une défaillance de mode commun, par exemple un dommage physique de la surface de montage. Seule l'une de ces sources peut être affectée à un API (automate) ou un dispositif similaire.
4. Les dispositifs doivent être installés de telle sorte qu'il soit difficile de les contourner ou de les dériver.
5. Les dispositifs doivent être montés de façon à ce que leur position et leur alignement ne puissent pas être facilement modifiés.
6. Il faut absolument empêcher qu'une condition environnementale (contamination extrême de l'air par exemple) puisse initier une inhibition.
7. Les dispositifs ne doivent pas utiliser une fonction de retard ou de temporisation quelconque (sauf si ces fonctions sont exécutées de telle sorte qu'aucune défaillance unique d'un composant n'empêche l'élimination du risque et l'arrêt des cycles machine suivants jusqu'à ce que la défaillance soit corrigée et qu'aucun nouveau risque ne survienne en raison de l'extension de la période d'inhibition).

7.5.16 Capteur d'inhibition de la commande de presse

Cette fonction est disponible sur le XS/SC26 FID 4 et ultérieur.

L'inhibition d'un dispositif de sécurité est la suspension automatique et contrôlée de l'entrée d'arrêt d'urgence inhibable du bloc fonction Commande de presse pendant une partie du cycle de la presse quand il n'existe pas de danger immédiat ou quand l'accès au danger est protégé par d'autres dispositifs. Associez les capteurs d'inhibition de commande de presse à l'entrée M Sensor (Capteur d'inhibition) du bloc fonction Entrées de commande de presse de sorte qu'avec l'entrée d'arrêt séquentiel (SQS), il soit possible d'inhiber un ou plusieurs des dispositifs d'entrée de sécurité suivants :

- Interrupteurs de verrouillage de sécurité
- Capteurs optiques
- Tapis de sécurité
- Arrêts de protection

Les normes américaines et internationales exigent de concevoir, d'installer et d'utiliser le système de sécurité de façon à protéger le personnel et à minimiser les risques de contournement du dispositif de protection.

AVERTISSEMENT:
- Prévention des installations dangereuses
- Deux (1 SQS et 1 capteur d'inhibition de commande de presse) ou quatre (2 SQS et 2 capteurs d'inhibition de commande de presse) interrupteurs de position indépendants doivent être positionnés et réglés correctement pour se fermer uniquement lorsque le danger a été écarté et se rouvrir en fin du cycle ou si le risque se représente. Si ces interrupteurs étaient mal positionnés ou réglés, des blessures graves, voire mortelles, pourraient en résulter.
- L'utilisateur est tenu de respecter l'ensemble des législations, réglementations, règlements et codes locaux et nationaux concernant l'utilisation de l'équipement de sécurité adéquat dans une application particulière. Veillez à respecter toutes les exigences légales ainsi que les instructions d'installation et de maintenance des manuels appropriés.

Le capteur d'inhibition de la commande de presse (avec le dispositif SQS) doit répondre, au minimum, aux exigences suivantes :

1. Il doit y avoir un minimum de deux dispositifs câblés indépendamment l'un de l'autre.

2. Les dispositifs doivent satisfaire à l'une des conditions suivantes : contacts normalement ouverts, sorties PNP (répondant toutes deux aux exigences d'entrée indiquées dans la section Spécifications et exigences à la page 21) ou action de commutation complémentaire. Au moins un des contacts doit se fermer quand le commutateur est actionné et doit s'ouvrir (ou être non conducteur) quand l'interrupteur n'est pas actionné ou en mode hors tension.
3. L'activation des entrées de cette fonction d'inhibition doit provenir de sources distinctes. Ces sources doivent être montées séparément pour éviter tout danger résultant d'un mauvais réglage ou alignement ou d'une défaillance de mode commun, par exemple un dommage physique de la surface de montage. Seule l'une de ces sources peut être affectée à un API (automate) ou un dispositif similaire.
4. Les dispositifs doivent être installés de telle sorte qu'il soit difficile de les contourner ou de les dériver.
5. Les dispositifs doivent être montés de façon à ce que leur position et leur alignement ne puissent pas être facilement modifiés.
6. Il faut absolument empêcher qu'une condition environnementale (contamination extrême de l'air par exemple) puisse initier une inhibition.
7. Les dispositifs ne doivent pas utiliser une fonction de retard ou de temporisation quelconque (sauf si ces fonctions sont exécutées de telle sorte qu'aucune défaillance unique d'un composant n'empêche l'élimination du risque et l'arrêt des cycles machine suivants jusqu'à ce que la défaillance soit corrigée et qu'aucun nouveau risque ne survienne en raison de l'extension de la période d'inhibition).

7.5.17  Interrupteur au pied

Cette fonction est disponible sur le XS/SC26 FID 4 et ultérieur.

L'entrée Interrupteur au pied (FS1) peut être utilisée de plusieurs façons avec les blocs fonction Commande de presse :

- Elle peut être connectée au nœud GO du bloc fonction Commande de presse comme dispositif de démarrage de cycle lorsque le bloc est configuré pour une commande à actionneur unique.
- Elle peut être connectée au nœud GO du bloc fonction Commande de presse lorsqu'il est configuré pour le paramétrage manuel Course montante et que l'entrée SQS est activée. (L'activation de l'entrée FS1 entraîne le coulisseau au point SQS. C'est à ce moment que le FS1 est relâché. Comme l'entrée d'arrêt d'urgence inhibable est maintenant inhibée, l'opérateur peut ajuster la pièce à usiner. L'activation du FS1 entraîne à nouveau le coulisseau jusqu'au point BOS puis le ramène au point TOS.)
- Elle peut être utilisée comme décrit dans le paragraphe suivant.

L'entrée Interrupteur au pied peut être ajoutée au bloc fonction Entrée de commande de presse et configurée lors de la configuration de l'entrée SQS. La presse s'arrête à l'entrée SQS, ce qui permet à l'opérateur de retirer ses mains de l'entrée Commande bimanuelle. L'opérateur peut vérifier que la pièce est correctement positionnée et doit parfois la maintenir en place. L'opérateur peut alors enclencher le dispositif d'entrée connecté à l'entrée Interrupteur au pied pour réenclencher la presse afin de terminer le processus.

L'entrée Interrupteur au pied peut également être configurée au niveau du nœud GO de la presse. Dans ce cas, l'interrupteur au pied peut être utilisé avec ou sans arrêt séquentiel (SQS) configuré. Cela permet une plus grande flexibilité dans les scénarios d'utilisation.

Une entrée ON/OFF physique ou une entrée Interrupteur au pied peut être raccordée à l'entrée Interrupteur au pied du bloc fonction Entrée de commande de presse. Le dispositif peut être un interrupteur au pied, ou tout autre dispositif de démarrage.

L'accès au danger doit être bloqué par d'autres moyens que le dispositif d'entrée d'arrêt d'urgence inhibable (par exemple, l'ouverture interne ne doit présenter aucun danger pour les doigts et faire moins de 6 mm). La protection peut également être assurée par des dispositifs de sécurité raccordés à l'entrée Arrêt d'urgence non inhibable.



PRÉCAUTION: D'autres moyens doivent être prévus pour garantir la protection des opérateurs contre les risques car leurs mains n'ont pas à actionner le bouton pendant ce dernier mouvement de la presse. Il peut s'agir d'une entrée à simple ou double voie (2 NO ou 1 NO/1 NF).

7.6 Dispositifs d'entrée auxiliaire

Les dispositifs d'entrée auxiliaires incluent les dispositifs de reset manuel, les interrupteurs de marche/arrêt, les dispositifs d'activation d'inhibition et les entrées d'annulation de la temporisation.

Dispositifs de reset manuel

Il sont utilisés pour créer un signal de reset pour une sortie ou un bloc fonction configuré pour un reset manuel. Une action de l'opérateur est nécessaire pour activer la sortie de ce bloc. Il est également possible de créer des resets à l'aide d'une entrée de reset virtuelle ; voir Dispositifs d'entrée auxiliaire virtuelle à la page 64.

AVERTISSEMENT:

- **Reset non surveillé**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Si un reset non surveillé (reset manuel ou du système) est configuré et si toutes les autres conditions d'un reset sont vérifiées, un court-circuit de la borne de reset à +24 V active immédiatement les sorties de sécurité.

Interrupteur de marche/arrêt

Envoie une commande de marche/arrêt à la machine. Lorsque toutes les entrées de sécurité sont en état marche, cette fonction permet l'activation et la désactivation de la sortie de sécurité. Il s'agit d'un signal simple voie, l'état marche est 24 Vcc et l'état d'arrêt est 0 Vcc. Il est possible d'ajouter une entrée ON/OFF sans l'assigner à une sortie de sécurité, ce qui permet à cette entrée de ne contrôler qu'une sortie d'état. Il est également possible de créer un interrupteur de marche/arrêt à l'aide d'une entrée virtuelle ; voir Dispositifs d'entrée auxiliaire virtuelle à la page 64.

XS/SC26 FID 4 ou ultérieur : les entrées ON/OFF sont utilisées pour sélectionner le mode du bloc fonction Mode de commande de la presse. Trois entrées distinctes sont nécessaires pour ce bloc. Le bloc accepte les entrées ON/OFF virtuelles.

Interrupteur d'activation de l'inhibition

Avertit le contrôleur lorsque les capteurs d'inhibition sont autorisés à effectuer une fonction d'inhibition. Lorsque la fonction d'activation de l'inhibition est configurée, les capteurs d'inhibition ne peuvent pas effectuer une fonction d'inhibition jusqu'à ce que le signal d'activation de l'inhibition soit en état marche. Il s'agit d'un signal simple voie, l'état marche est 24 Vcc et l'état d'arrêt est 0 Vcc. Il est également possible de créer un interrupteur d'activation de l'inhibition à l'aide d'une entrée virtuelle ; voir Dispositifs d'entrée auxiliaire virtuelle à la page 64.

Dispositifs d'annulation de la temporisation d'arrêt

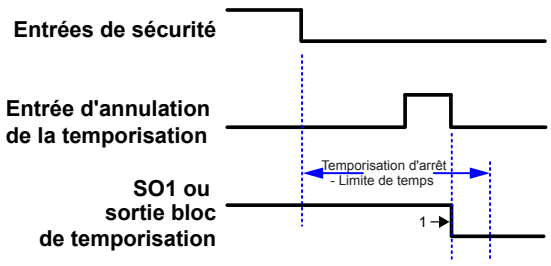
Offrent la possibilité d'annuler une temporisation d'arrêt configurée pour une sortie de sécurité ou une sortie de bloc de temporisation, ou pour annuler une durée d'impulsion configurée pour une sortie de bloc 1 impulsion. Ils fonctionnent de l'une des façons suivantes :

- Ils maintiennent activée la sortie de sécurité ou la sortie du bloc de temporisation.
- Ils désactivent la sortie de sécurité, la sortie du bloc de temporisation ou la sortie du bloc 1 impulsion immédiatement après que le contrôleur de sécurité a reçu un signal d'annulation de la temporisation d'arrêt.
- Lorsque l'option **Type d'annulation** est configurée en **Entrée de contrôle**, la sortie de sécurité ou la sortie du bloc de temporisation reste activée si l'entrée est réactivée avant la fin de la temporisation (ne s'applique pas à une sortie de bloc 1 impulsion).

Une fonction de sortie d'état (Temporisation de sortie en cours) indique quand il est possible d'activer une entrée d'annulation de temporisation afin de maintenir activée une sortie de sécurité dont l'arrêt a été retardé. Il est également possible de créer un dispositif d'annulation de temporisation d'arrêt à l'aide d'une entrée virtuelle ; voir Dispositifs d'entrée auxiliaire virtuelle à la page 64.

Temps d'annulation de la temporisation d'arrêt

Illustration 26. L'entrée de sécurité reste en mode d'arrêt.



Remarque 1 - Si la fonction de désactivation de la sortie est sélectionnée

Illustration 27. Fonction Maintien de la sortie désactivée

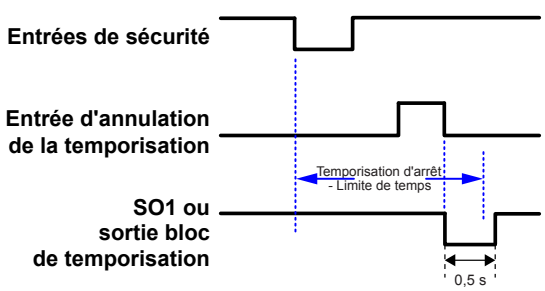


Illustration 28. Fonction Maintien de la sortie activée pour les entrées de sécurité avec reset de verrouillage

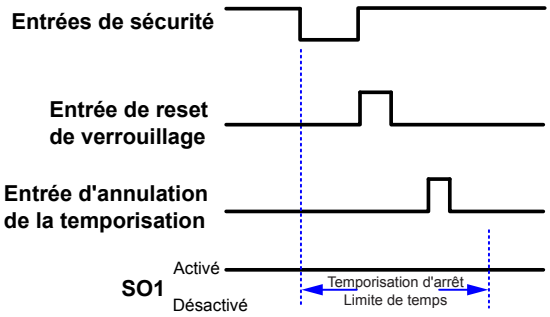
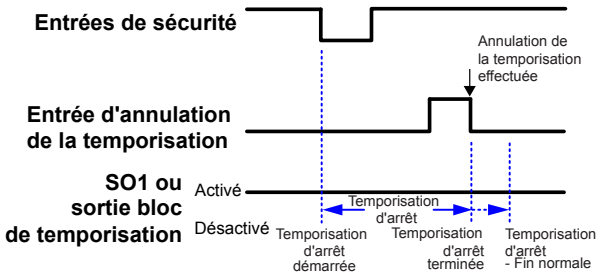


Illustration 29. Fonction Maintien de la sortie activée pour les entrées de sécurité sans reset de verrouillage



7.6.1 Entrée de reset manuel

L'entrée de reset manuel peut être configurée pour l'une des opérations suivantes ou toute combinaison de celles-ci (référez-vous à la section Ajout d'entrées et de sorties d'état à la page 86) :

Reset des entrées de sécurité

Configure la sortie du ou des blocs de reset à verrouillage pour qu'elle passe d'un état verrouillé à un état marche lorsque le nœud IN est en état marche.

Reset des sorties de sécurité

Configure la sortie pour qu'elle s'active si le bloc de sortie configuré pour le reset à verrouillage est activé (ON).

Exceptions :

Une sortie de sécurité ne peut pas être configurée pour utiliser un reset manuel lorsqu'elle est associée à une entrée de commande bimanuelle ou à un bloc fonction d'un dispositif de commande.

Reset du système

Configure le système pour qu'il passe en état marche à partir d'un état de verrouillage causé par un défaut système si la cause du défaut a été résolue. Scénarios possibles d'utilisation d'un reset système :

- Détection de signaux sur des bornes inutilisées
- Expiration du mode de configuration
- Sortie du mode de configuration
- Défauts internes
- Défauts de la commande de presse

Remarque: Un reset manuel sélectionné comme reset système peut servir à terminer la confirmation d'une nouvelle configuration afin de ne pas devoir remettre le dispositif hors/sous tension.

Remarque: Si le logiciel Contrôleur de sécurité Banner est connecté au contrôleur via une connexion Ethernet, sélectionnez **Redémarrer** dans la fenêtre Redémarrage du système.

Reset de défaut de sortie

Annule le défaut et permet de réactiver la sortie si la cause du défaut a été résolue. Scénarios possibles d'utilisation d'un reset de défaut de sortie :

- Défauts de sortie
- Défauts de l'EDM ou de l'AVM

Reset manuel à la mise sous tension

Permet de contrôler plusieurs blocs de reset à verrouillage et/ou blocs de sortie à l'aide d'une seule entrée de reset après la mise sous tension.

Sortie du mode actif

Un reset est nécessaire pour quitter le mode actif.

Reset de la fonction Tracer groupe d'entrées

Effectue un reset de la fonction de sortie d'état **Tracer groupe d'entrées** et de la fonction de sortie d'état virtuelle **Tracer groupe d'entrées**.

Le bouton de reset doit être monté à un endroit qui respecte l'avertissement ci-dessous. Un interrupteur de reset à clé offre un moyen de contrôle supplémentaire dans la mesure où il est possible de retirer la clé de l'interrupteur et de la prendre dans la zone protégée. Toutefois, cela n'évite pas un reset non autorisé ou accidentel si d'autres personnes sont en possession de clés de rechange ou si d'autres membres du personnel s'introduisent dans la zone protégée sans être détectés (risque d'enfermement).



AVERTISSEMENT:

- **Installez correctement les interrupteurs de reset**
- Si les interrupteurs de reset ne sont pas correctement installés, des dommages corporels graves ou mortels ne sont pas à exclure.
- Installez les interrupteurs de reset afin qu'ils ne soient accessible que de l'extérieur de l'espace protégé et parfaitement visibles depuis ce dernier. Il doit être impossible d'accéder aux interrupteurs de reset à partir de l'espace protégé. Protégez les interrupteurs de reset contre tout utilisation accidentelle ou non autorisée (par exemple au moyen de bagues ou de protections). Si certaines zones dangereuses ne sont pas visibles depuis l'emplacement des interrupteurs de reset, installez des dispositifs de protection supplémentaires.



Important: Le reset d'un dispositif de protection ne doit pas initier un mouvement dangereux. Les procédures de travail sécurisées doivent prévoir une procédure de démarrage établie et garantir que la personne effectuant le reset vérifie que tout le personnel a quitté la zone dangereuse, **avant chaque reset de la protection**. Si une partie de la zone n'est pas visible depuis l'emplacement de l'interrupteur de reset, il faut prévoir des protections supplémentaires, à savoir au moins un avertissement sonore et visuel du démarrage de la machine.

Remarque: Le **reset automatique** configure une entrée pour qu'elle repasse à l'état actif (ON) sans intervention de l'utilisateur dès que le ou les dispositifs d'entrée passent à l'état marche et que tous les autres blocs logiques sont en état marche. Parfois appelé « mode automatique », le reset automatique est généralement utilisé pour les installations dans lesquelles le dispositif d'entrée de sécurité détecte continuellement l'opérateur.



AVERTISSEMENT:

- **Reset automatique à la mise sous tension**
- À la mise sous tension, les sorties de sécurité et les blocs de reset à verrouillage configurés pour le reset automatique à la mise sous tension activent leurs sorties si toutes les entrées associées sont en état marche.
- Si un reset manuel est nécessaire, configurez les sorties pour un mode de reset manuel à la mise sous tension.

Entrées de reset manuel et automatique assignées à une même sortie de sécurité

Par défaut, les sorties de sécurité sont configurées pour un reset automatique (mode automatique). Elles peuvent être configurées pour un reset à verrouillage à l'aide de l'attribut Sortie électronique de la fenêtre Propriétés de la sortie de sécurité (voir Blocs fonction à la page 121).

Les dispositifs d'entrée de sécurité fonctionnent en mode de reset automatique sauf si vous ajoutez un bloc de reset à verrouillage. Si un bloc de reset à verrouillage est ajouté en ligne avec une sortie configurée en mode reset à verrouillage, le même dispositif d'entrée ou un autre dispositif d'entrée de reset manuel doit être utilisé pour procéder au reset de l'ensemble (bloc et sortie de sécurité). Si le même dispositif d'entrée de reset manuel est utilisé pour les deux et que toutes les entrées sont en état marche, une même action de reset déverrouillera le bloc fonction et le bloc de sortie. Si vous utilisez un autre dispositif d'entrée de reset manuel, le reset associé à la sortie de sécurité doit être activé en dernier. Vous pouvez utiliser cette option pour forcer une séquence de reset qui peut servir à limiter ou à éliminer les risques d'enfermement dans les applications de protection de périmètre (voir Propriétés des dispositifs d'entrée de sécurité à la page 36).

Si les entrées contrôlant un bloc de reset à verrouillage ou un bloc de sortie de sécurité ne sont pas en état marche, le reset de ce bloc sera ignoré.

Exigences relatives au signal de reset

Les dispositifs d'entrée de reset peuvent être configurés pour être surveillés ou non, comme suit :

Reset surveillé

Nécessite que le signal de reset passe de bas (0 Vcc) à haut (24 Vcc) puis de nouveau à bas. L'état haut doit avoir une durée comprise entre 0,5 et 2 secondes. Il est qualifié de front descendant.

Reset non surveillé

Nécessite que le signal de reset passe de bas (0 Vcc) à haut (24 Vcc) uniquement et qu'il reste haut pendant au moins 0,5 seconde. Après le reset, le signal de reset peut être soit haut, soit bas. Il est qualifié de front montant.

7.7 Dispositifs d'entrée auxiliaire virtuelle

Cette fonction est disponible sur le XS/SC26 FID 2 et ultérieur et le SC10-2. Les dispositifs d'entrée auxiliaire virtuelle comprennent le reset manuel, la marche/arrêt, l'activation de l'inhibition et l'annulation du retard au déclenchement.

AVERTISSEMENT: Ces dispositifs ne doivent jamais être utilisés pour commander des applications cruciales pour la sécurité. Si une sortie auxiliaire virtuelle est utilisée pour contrôler une telle application, une défaillance pourrait se produire et entraîner un danger susceptible de provoquer des blessures graves, voire mortelles.

Important: Le reset d'un dispositif de protection ne doit pas initier un mouvement dangereux. Les procédures de travail sécurisées doivent prévoir une procédure de démarrage établie et garantir que la personne effectuant le reset vérifie que tout le personnel a quitté la zone dangereuse, avant chaque reset de la protection. Si une partie de la zone n'est pas visible depuis l'emplacement de l'interrupteur de reset, il faut prévoir des protections supplémentaires, à savoir au moins un avertissement sonore et visuel du démarrage de la machine.

7.7.1 Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels

Selon la section 5.2.2 de la norme EN ISO 13849-1:2015, le reset d'une fonction de sécurité nécessite une « action délibérée » de l'opérateur. Généralement, pour répondre à cette exigence, un interrupteur mécanique et des câbles associés sont connectés aux bornes spécifiées sur le contrôleur de sécurité. Dans le cadre d'un reset surveillé, les contacts doivent être d'abord ouverts, puis fermés et ouverts à nouveau dans un délai adéquat. Si ce délai n'est ni trop court ni trop long, il est estimé qu'il s'agit d'actions délibérées et le reset est réalisé.

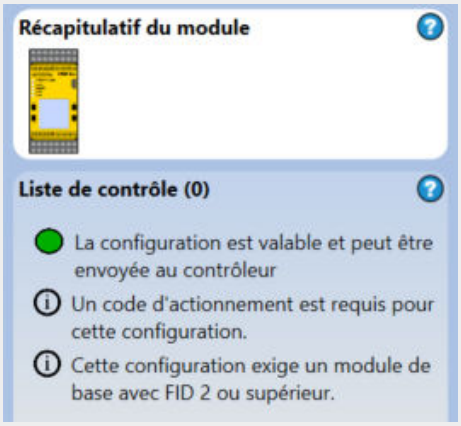
Banner Engineering a créé une solution de reset virtuel qui nécessite une intervention délibérée. Par exemple, une interface homme-machine peut remplacer l'interrupteur mécanique. Au lieu de câbles, un code d'actionnement unique est appliqué à chaque contrôleur de sécurité sur le réseau. En outre, chaque reset virtuel au sein d'un contrôleur est associé à un bit spécifique dans un registre. Ce bit, combiné au code d'actionnement, doit être écrit et effacé de façon coordonnée. Si les étapes se succèdent selon l'ordre et le délai définis, elles sont considérées comme délibérées et le reset est réalisé.

Les normes en vigueur n'exigent pas « d'action délibérée » dans le cadre de l'annulation virtuelle d'une temporisation. Toutefois, par souci de simplicité, Banner Engineering a mis en œuvre cette fonction de la même manière que celle de reset manuel virtuel.

L'utilisateur doit définir des codes d'actionnement correspondants au niveau du contrôleur de sécurité et du dispositif réseau de commande (API, IHM, etc.). Le code d'actionnement fait partie des paramètres réseau et n'est pas inclus dans le CRC (Contrôle de redondance cyclique) de configuration. Il n'existe pas de code d'actionnement par défaut. L'utilisateur doit en définir un dans l'écran **Paramètres réseau**. Ou, sur les contrôleurs dotés d'une interface embarquée, lorsque la case **Utilisez l'interface embarquée pour définir le dernier octet et code d'actionnement** est cochée, le code d'actionnement peut être défini à l'aide de l'interface embarquée. Référez-vous à la section Processus Clickset IP à la page 180. Le code d'actionnement n'est actif que pendant 2 secondes. Un code d'actionnement différent doit être utilisé pour chaque contrôleur de sécurité présent sur le réseau.

Remarque: En cas d'ajout d'un reset manuel ou d'une annulation de la temporisation virtuel dans l'onglet **Vue fonctionnelle**, la liste de contrôle ajoute une note indiquant qu'il faut définir un code d'actionnement sous **Paramètres réseau**.

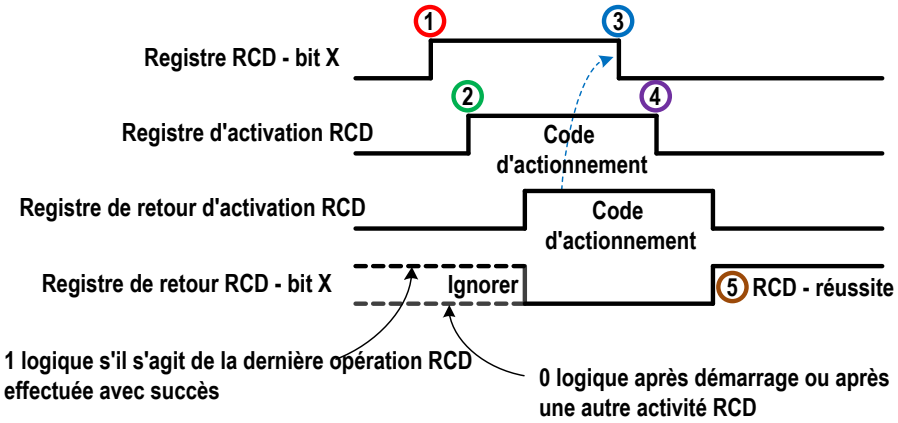
Illustration 30. Exemple d'avertissement affiché dans la liste de contrôle



Le programmeur IHM/API peut choisir entre deux méthodes selon ses préférences : une séquence avec retour ou une séquence avec délai. Ces deux méthodes sont décrites dans les figures ci-dessous. L'emplacement réel du registre dépend du protocole utilisé.

Séquence de reset ou d'annulation de la temporisation — Méthode avec retour

Illustration 31. Séquence de reset ou d'annulation de la temporisation — Méthode avec retour



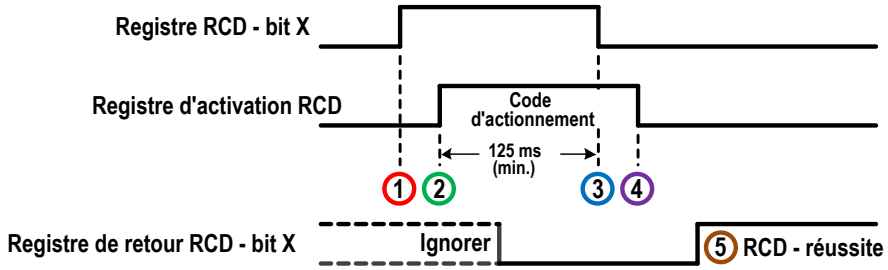
1. Écrivez un 1 logique pour le(s) bit(s) du registre RCD correspondant à l'activité virtuelle de votre choix (reset ou annulation de la temporisation).
2. Dans le même temps ou à tout moment par la suite, écrivez le code d'actionnement dans le registre d'activation RCD.
3. Vérifiez que le code d'actionnement apparaît dans le registre de retour sur l'activation RCD (généralement dans un délai de 125 ms). Ensuite, écrivez un 0 logique pour le bit du registre RCD.
4. Dans le même temps ou à tout moment par la suite, effacez le code d'actionnement (en écrivant un 0 logique dans le registre d'activation RCD). Cette étape doit être réalisée dans les deux secondes qui suivent la première écriture du code (étape 2).
5. Si vous le souhaitez, vous pouvez surveiller le registre de retour RCD pour savoir si le reset ou l'annulation de temporisation a été accepté (généralement dans un délai de 175 ms).

Remarque: Vous trouverez les différents bits de registre nécessaires dans l'onglet **Ethernet industriel** du logiciel en remplaçant la sélection Sorties d'état virtuelles par Entrées auxiliaires virtuelles. Le code d'actionnement est créé par l'utilisateur sous l'icône Paramètres réseau dans la barre d'outils.

Remarque: Un fichier AOI et un bloc fonction API sont disponibles sur le site www.bannerengineering.com, dans la page produit du contrôleur de sécurité. Le dossier AOI comprend un fichier AOI sur Activation du reset et de l'annulation de la temporisation pour les contrôleurs SC10, SC26 et XS26 de Banner qui vous aidera à mieux comprendre le processus.

Séquence de reset ou d'annulation de la temporisation — Méthode avec délai

Illustration 32. Séquence de reset ou d'annulation de la temporisation — Méthode avec délai



1. Écrivez un 1 logique pour le(s) bit(s) du registre RCD correspondant à l'activité virtuelle de votre choix (reset ou annulation de la temporisation).
2. Dans le même temps ou à tout moment par la suite, écrivez le code d'actionnement dans le registre d'activation RCD.
3. Attendez au moins 125 ms après l'étape 2, puis écrivez un 0 logique pour le bit du registre RCD.
4. Dans le même temps ou à tout moment par la suite, effacez le code d'actionnement (en écrivant un 0 logique dans le registre d'activation RCD). Cette étape doit être réalisée dans les deux secondes qui suivent la première écriture du code (étape 2).
5. Si vous le souhaitez, vous pouvez surveiller le registre de retour RCD pour savoir si le reset ou l'annulation de temporisation a été accepté (généralement dans un délai de 175 ms).

Les dispositifs à reset manuel virtuel permettent de créer un signal de reset pour une sortie ou un bloc fonction configuré pour un reset manuel. Une action de l'opérateur est nécessaire pour activer la sortie de ce bloc. Il est également possible de créer des reset à l'aide d'une entrée de reset physique ; voir Dispositifs d'entrée auxiliaire à la page 60.

AVERTISSEMENT: Reset manuel virtuel — À moins que la sécurité de toutes les zones dangereuses ne soit confirmée, il est déconseillé de configurer un reset manuel virtuel pour effectuer un démarrage manuel impliquant des équipements situés dans plusieurs emplacements.

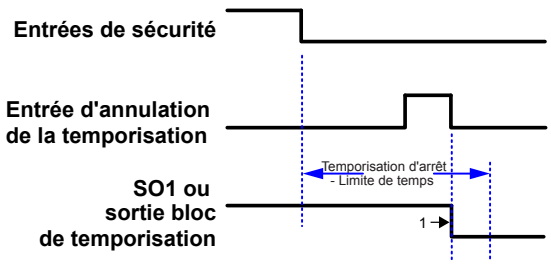
Dispositifs d'annulation de retard au déclenchement virtuelle : permettent d'annuler une période de retard au déclenchement ou d'impulsion configurée. Ils fonctionnent de l'une des façons suivantes :

- Ils maintiennent activée la sortie de sécurité ou la sortie du bloc de temporisation.
- Ils désactivent la sortie de sécurité, la sortie du bloc de temporisation ou la sortie du bloc 1 impulsion immédiatement après que le contrôleur de sécurité a reçu un signal d'annulation du retard au déclenchement.
- Lorsque l'option **Annuler le type** est configurée en « Entrée de contrôle », la sortie de sécurité ou la sortie du bloc de temporisation reste activée si l'entrée est réactivée avant la fin de la temporisation.

Une fonction de sortie d'état (Temporisation de sortie en cours) indique quand il est possible d'activer une entrée d'annulation de temporisation afin de maintenir activée une sortie de sécurité dont l'arrêt a été retardé. Il est également possible de créer un dispositif d'annulation de retard au déclenchement à l'aide d'une entrée physique ; voir Dispositifs d'entrée auxiliaire à la page 60.

Temps d'annulation du retard au déclenchement virtuelle

Illustration 33. L'entrée de sécurité reste en mode d'arrêt.



Remarque 1 - Si la fonction de désactivation de la sortie est sélectionnée

Illustration 34. Fonction Désactivation de la sortie

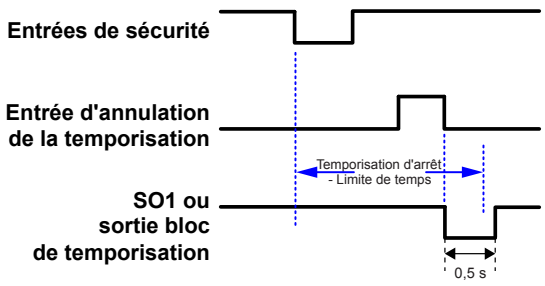


Illustration 35. Fonction Maintien de la sortie activée pour les entrées de sécurité avec reset à verrouillage

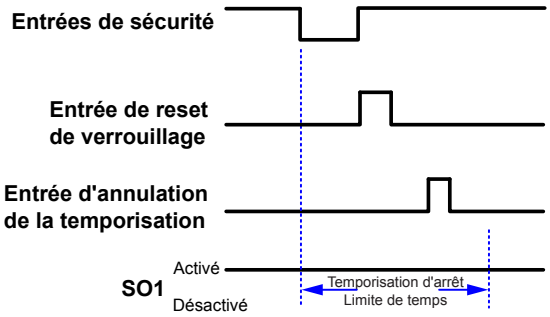
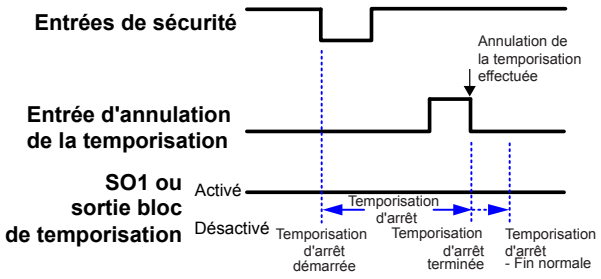


Illustration 36. Fonction Maintien de la sortie activée pour les entrées de sécurité sans reset à verrouillage



7.7.2 Marche/arrêt et Inhibition activée virtuels

Marche/arrêt virtuel

Envoie une commande de marche/arrêt à la machine. Lorsque toutes les entrées de sécurité sont en état marche, cette fonction permet l'activation et la désactivation de la sortie de sécurité. L'état Marche est un 1 logique et l'état Arrêt est un 0 logique. Il est possible d'ajouter une entrée ON/OFF sans l'assigner à une sortie de sécurité, ce qui permet à cette entrée de ne contrôler qu'une sortie d'état auxiliaire. Il est également possible de créer un interrupteur de marche/arrêt à l'aide d'une entrée physique ; voir Dispositifs d'entrée auxiliaire à la page 60.

XS/SC26 FID 4 ou ultérieur : les entrées ON/OFF virtuelles sont utilisées pour sélectionner le mode du bloc fonction Mode de commande de la presse. Trois entrées distinctes sont nécessaires pour ce bloc. Le bloc accepte les entrées ON/OFF.

Inhibition activée virtuelle

Avertit le contrôleur lorsque les capteurs d'inhibition sont autorisés à effectuer une fonction d'inhibition. Lorsque la fonction d'activation de l'inhibition est configurée, les capteurs d'inhibition ne peuvent pas effectuer une fonction d'inhibition jusqu'à ce que le signal d'activation de l'inhibition soit en état marche. L'état Marche (Run) est un 1 logique et l'état Arrêt (Stop) est un 0 logique. Il est également possible de créer un interrupteur d'inhibition à l'aide d'une entrée physique ; voir Dispositifs d'entrée auxiliaire à la page 60.

7.8 Sorties de sécurité

XS/SC26

Le contrôleur de base possède deux paires de sorties de sécurité électroniques (bornes SO1a & SO1b, et SO2a & SO2b). Ces sorties fournissent jusqu'à 500 mA chacune à 24 Vcc. Chaque sortie de sécurité électronique redondante peut être configurée pour fonctionner de manière autonome ou par paire, par exemple en utilisant SO1 comme une sortie double canal ou en la divisant pour contrôler SO1a indépendamment de SO1b.

Il est possible d'ajouter des sorties de sécurité aux modèles extensibles du contrôleur de base en intégrant des modules d'E/S. Ces sorties de sécurité supplémentaires peuvent représenter des sorties de relais isolées qui peuvent être utilisées pour contrôler/commuter un large éventail de caractéristiques d'alimentation (référez-vous à la section Spécifications du XS/SC26 à la page 21).

SC10-2

Le SC10-2 possède deux sorties relais redondantes isolées. Chaque sortie relais possède trois jeux de contacts indépendants. Voir Spécifications du SC10-2 à la page 25 pour les considérations de classement et déclassement.

XS/SC26 et SC10-2

AVERTISSEMENT:
- **Raccordez correctement les sorties de sécurité.**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Les sorties de sécurité doivent être raccordées à la commande de la machine pour que le système de commande de sécurité de la machine puisse interrompre le circuit aux éléments de contrôle primaire de la machine (MPCE) et éliminer ainsi le danger.
- Ne raccordez jamais un ou plusieurs dispositifs intermédiaires (API, système électronique programmable, PC) dont la défaillance pourrait entraîner la perte de la commande d'arrêt d'urgence ou permettrait de suspendre, de neutraliser ou de contourner la fonction de sécurité, sauf si cela apporte un niveau de sécurité équivalent ou supérieur.

La liste suivante décrit les nœuds et attributs supplémentaires qui peuvent être configurés dans la fenêtre **Propriétés** du bloc fonction de la sortie de sécurité (référez-vous à la section Ajout d'entrées et de sorties d'état à la page 86):

EDM (Surveillance des commutateurs externes)

Permet au contrôleur de sécurité de surveiller les dispositifs sous contrôle (FSD et MPCE) pour s'assurer qu'ils réagissent à la commande d'arrêt des sorties de sécurité. **Il est vivement recommandé d'inclure un EDM (ou un AVM)** dans la conception de la machine et la configuration du contrôleur de sécurité pour garantir un niveau d'intégrité approprié du circuit de sécurité (voir la section Raccordement EDM et FSD à la page 74).

AVM (Moniteur de vanne réglable)

Permet au contrôleur de sécurité de surveiller des vannes ou d'autres dispositifs susceptibles de ralentir, de se coincer ou de tomber en panne dans une position ou un état sous tension et dont le fonctionnement doit être vérifié après l'envoi d'un signal d'arrêt. Il est possible de sélectionner jusqu'à 3 entrées AVM si la fonction EDM n'est pas utilisée**. Il est vivement recommandé d'inclure un AVM (ou un EDM)** dans la conception de la machine et la configuration du contrôleur de sécurité pour garantir un niveau d'intégrité approprié du circuit de sécurité (voir la section Fonction AVM (Adjustable Valve Monitoring - surveillance de vanne réglable) à la page 50).

LR (Reset de verrouillage)

Conserve la sortie SO ou RO désactivée jusqu'à ce que l'entrée passe en état marche et qu'un reset manuel soit effectué. Référez-vous à la section Entrée de reset manuel à la page 62 pour en savoir plus.

RE (Activation de reset)

Cette option n'est disponible que si **LR (Reset de verrouillage)** est activé. Le **reset de verrouillage** peut être contrôlé par la sélection de l'option **Activation de reset** pour limiter les circonstances dans lesquelles il est possible de réinitialiser une sortie de sécurité en état marche.

FR (Reset de défaut)

Offre une fonction de reset manuel en cas de défauts d'entrée. Le nœud FR doit être connecté à un signal ou à un bouton de reset manuel. Cette fonction permet de maintenir la sortie SO ou RO en état Off jusqu'à l'élimination du défaut du dispositif d'entrée, le dispositif défaillant est en état marche et un reset manuel est effectué. Cette opération remplace un reset par un cycle de coupure et rétablissement de l'alimentation. Référez-vous à la section Entrée de reset manuel à la page 62 pour en savoir plus.

Mode à la mise sous tension

Il est possible de configurer la sortie de sécurité selon trois scénarios de mise sous tension (caractéristiques de fonctionnement à la mise sous tension) :
- Mode normal à la mise sous tension (par défaut)
- Mode manuel à la mise sous tension : nécessite une entrée de reset manuel configurée pour une mise sous tension manuelle ; cette sélection nécessite un reset à la mise sous tension pour activer les sorties, même si elle est configurée pour un reset automatique
- Mode automatique à la mise sous tension : permet aux sorties de s'activer à la mise sous tension si la logique est en état ON, même si une fonction de reset à verrouillage (bloc ou nœud de sortie) est configurée

Référez-vous à la section Entrée de reset manuel à la page 62 pour en savoir plus.

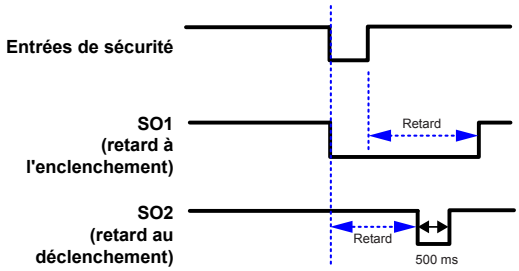
Diviser (sorties de sécurité) —XS/SC26 uniquement

Cette option n'est disponible que pour les sorties de sécurité électroniques. Chaque sortie de sécurité électronique redondante peut être configurée pour fonctionner par paire (par défaut) ou de façon individuelle. La division d'une sortie de sécurité électronique crée deux sorties simple voie indépendantes (le contrôle de SO1a est indépendant de SO1b). Pour combiner des sorties de sécurité divisées, ouvrez la fenêtre des **propriétés** Mx:SOxA et cliquez sur **Lier.**

Retards à l'enclenchement et au déclenchement

Chaque sortie de sécurité peut être configurée pour fonctionner avec un retard à l'enclenchement ou au déclenchement (voir Illustration 37 à la page 69). Dans un tel cas, la sortie s'active ou se désactive uniquement après l'expiration de la limite de temps définie. Une sortie ne peut pas être associée en même temps à un retard à l'enclenchement et un retard au déclenchement. Les limites de temps de retard à l'enclenchement et au déclenchement peuvent varier de 100 ms à 5 minutes, par incrément d'une milliseconde.

Illustration 37. Chronogramme — Retards à l'enclenchement et au déclenchement généraux d'une sortie de sécurité



AVERTISSEMENT:

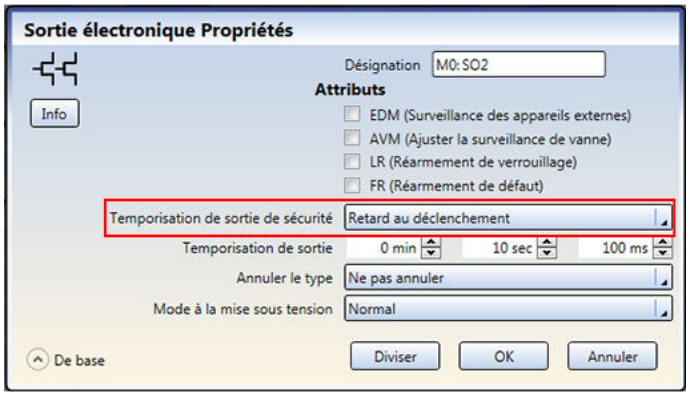
- **En cas de panne de coupure de l'alimentation ou de perte de puissance, le retard au déclenchement peut prendre fin immédiatement.**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Un temps de retard au déclenchement d'une sortie de sécurité est respecté même si l'entrée de sécurité qui a déclenché le temporisateur au déclenchement repasse dans l'état marche avant la fin du temps de retard. Si un arrêt immédiat de la machine était susceptible de créer un danger potentiel, il faudrait prendre des mesures de protection supplémentaires pour éviter toute blessure.

Liaison de sorties

Deux sorties de sécurité peuvent être reliées entre elles lorsque l'une d'elles est configurée avec un retard au déclenchement et l'autre sans retard. Une fois reliée, la sortie non temporisée ne se réactive pas immédiatement si l'entrée de commande s'active pendant le retard au déclenchement, comme illustré dans Illustration 40 à la page 70. Pour relier deux sorties de sécurité :

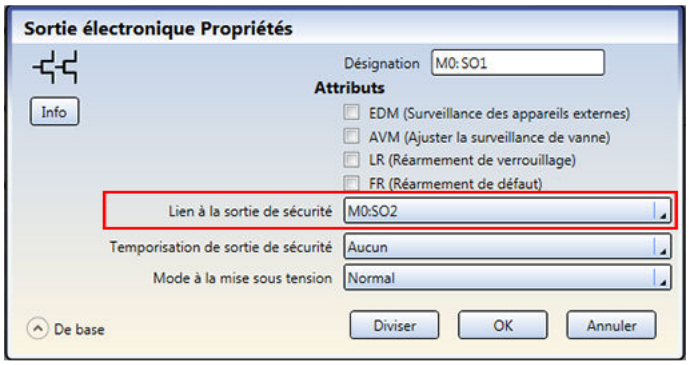
1. Ouvrez la fenêtre **Propriétés** de la sortie de sécurité qui doit avoir un retard au déclenchement.
2. Sélectionnez **Retard au déclenchement** dans la liste déroulante *Temporisation de la sortie de sécurité*.

Illustration 38. Exemple de sélection d'une temporisation de sortie de sécurité : Retard au déclenchement



3. Sélectionnez le délai de retard requis.
4. Cliquez sur **OK**.
5. Ouvrez la fenêtre **Propriétés** de la sortie de sécurité à relier à la sortie configurée avec un retard au déclenchement.
6. A partir de la liste déroulante des *affectations des sorties de sécurité*, sélectionnez la sortie de sécurité retardée au déclenchement à laquelle lier cette sortie de sécurité.

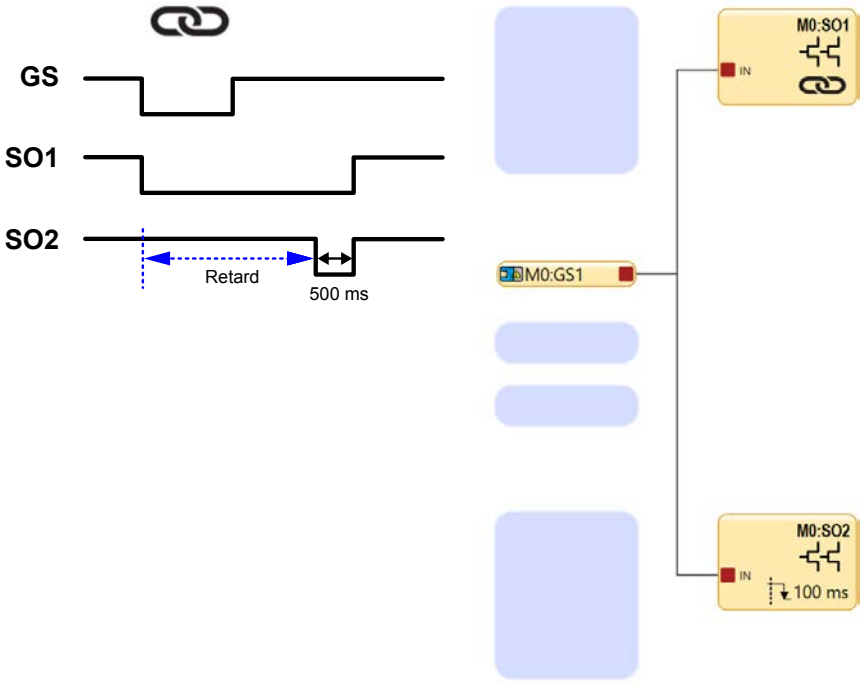
Illustration 39. Exemple de sélection d'une sortie de sécurité à lier



Remarque: La ou les mêmes entrées doivent être connectées aux deux sorties de sécurité pour que celles-ci s'affichent dans la liste des sorties disponibles.

7. Cliquez sur **OK**. La sortie de sécurité liée possédera une icône représentant un lien.

Illustration 40. Chronogramme — Sorties de sécurité liées



7.8.1 Sorties de sécurité électroniques

Cette fonction est disponible sur le XS/SC26.

Les sorties de sécurité électroniques, par exemple SO1a et b et SO2a et b, sont activement surveillées pour détecter des courts-circuits vers la tension d'alimentation, entre elles et vers d'autres sources de tension. Elles sont conçues pour les applications de sécurité de catégorie 4. Si une défaillance est détectée sur une voie d'une paire de sorties de sécurité, les deux sorties tentent de se désactiver et passent en état de verrouillage. La sortie sans défaut est en mesure d'arrêter le mouvement dangereux.

De la même manière, une sortie de sécurité utilisée individuellement (divisée) est également activement surveillée pour détecter des courts-circuits vers d'autres sources d'alimentation mais elle ne peut effectuer aucune action. Soyez très prudent lors du câblage des bornes et de la pose des fils pour éviter le risque de courts-circuits vers d'autres sources de tension, dont d'autres sorties de sécurité. Chaque sortie de sécurité divisée offre un niveau de sécurité suffisant pour les applications de catégorie 3 grâce à un raccordement en série interne de deux dispositifs de commutation mais il faut éviter le risque de court-circuit externe.

Important: Lorsque vous utilisez des modules de sortie de sécurité électroniques (XS2so ou XS4so), ces modules doivent être mis sous tension soit avant, soit dans les 5 secondes qui suivent la mise sous tension du contrôleur de base, si vous utilisez des sources d'alimentation distinctes.

Remarque: Chaque module de sortie de sécurité électronique (XS2so ou XS4so) possède deux bornes 24 V et deux bornes 0 V. Une seule paire est nécessaire pour alimenter le module individuel. La seconde peut servir à raccorder l'alimentation au module suivant.

AVERTISSEMENT:
- **Utilisation des sorties (divisées) simple voie dans des applications de sécurité critiques**
- Si les applications de sécurité critiques n'incluent pas des méthodes d'élimination d'erreurs appropriées lors de l'utilisation de sorties simple voie, vous pouvez être confronté à une perte du contrôle de la sécurité susceptible d'entraîner des blessures graves, voire mortelles.
- Si une sortie simple voie est utilisée dans une application de sécurité critique, il est indispensable d'intégrer les principes d'élimination d'erreurs pour garantir un niveau de sécurité de catégorie 3. A titre d'exemple, une bonne méthode d'élimination d'erreurs consiste à acheminer et à gérer les fils des sorties simple voie afin d'éviter tout court-circuit vers d'autres sorties ou sources de tension.

Lorsque c'est possible, il est vivement recommandé d'inclure une fonction EDM (Surveillance des commutateurs externes) et/ou une fonction AVM (Moniteur de vanne réglable) pour surveiller les dispositifs sous contrôle (FSD et MPCE) afin de détecter les défaillances dangereuses. Référez-vous à la section Surveillance des commutateurs externes (EDM) à la page 74 pour en savoir plus.

Raccordement des sorties

Les sorties de sécurité doivent être raccordées à la commande de la machine pour que le système de commande de sécurité de la machine puisse interrompre le circuit ou l'alimentation des éléments de contrôle primaire de la machine (MPCE), permettant ainsi de supprimer le danger.

Lorsque vous utilisez des dispositifs de commutation finaux (FSD), cette opération est normalement effectuée par ceux-ci lorsque les sorties de sécurité passent à l'état désactivé (Off). Consultez la section Spécifications du XS/SC26 à la page 21 avant d'effectuer les raccordements et d'interfacer le contrôleur de sécurité à la machine.

Le niveau d'intégrité du circuit de sécurité doit être déterminé par une étude de risques. Ce niveau dépend de la configuration, de l'installation correcte des circuits externes ainsi que du type des dispositifs sous contrôle (FSD et MPCE). Les sorties de sécurité électroniques sont adaptées aux applications relevant de la catégorie 4 PL e / SIL 3 lorsqu'elles sont contrôlées par paire (non divisées) et aux applications de la catégorie 3 PL d / SIL 2 maximum si elles fonctionnent de façon indépendante (divisées) pour autant que les méthodes d'élimination d'erreurs appropriées aient été implémentées. Référez-vous à la Illustration 41 à la page 72 pour des exemples de raccordement.

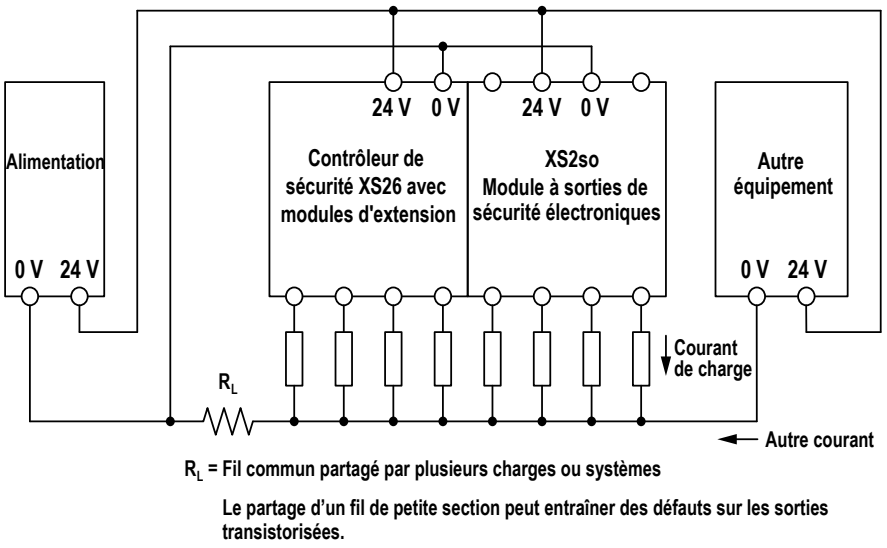
AVERTISSEMENT:
- **Résistance des fils de la sortie de sécurité**
- Une résistance supérieure à 10 ohms pourrait masquer un court-circuit entre les sorties de sécurité double voie et créer une situation dangereuse, susceptible de provoquer des blessures graves, voire mortelles.
- Ne dépassez pas une résistance de 10 ohms dans les fils des sorties de sécurité.

Installation du fil commun

Prenez en compte la résistance du fil commun 0 V et le courant passant dans ce fil pour éviter des verrouillages inopinés. Observez l'emplacement du symbole de résistance dans le schéma ci-dessous représentant la résistance du fil commun 0 V (RL).

Solutions possibles pour éviter ce problème :
- Utilisez des fils plus courts ou de section supérieure pour réduire la résistance (R_L) du fil commun 0 V.
- Séparez le fil commun 0 V des charges connectées au contrôleur de sécurité ou le fil commun 0 V d'autres équipements alimentés par la source 24 V commune.

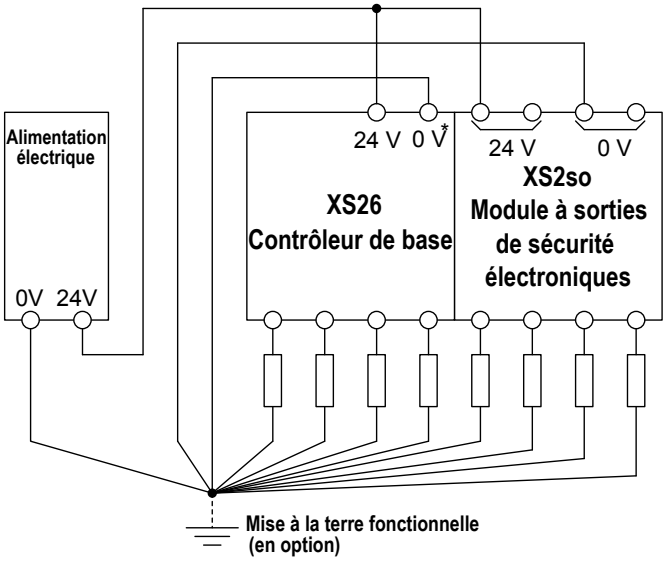
Illustration 41. Installation du fil commun



Remarque: Lorsque la sortie de sécurité se désactive, la tension à cette borne de sortie doit descendre sous 1,7 V par rapport à la borne 0 V de ce module. Si la tension est supérieure à 1,7 V, le contrôleur de sécurité considère que la sortie est toujours active, ce qui entraîne un verrouillage. Envisagez d'utiliser des fils plus courts ou de section supérieure, ou encore un schéma de mise à terre en un seul point, semblable à ceux illustrés dans les schémas suivants.

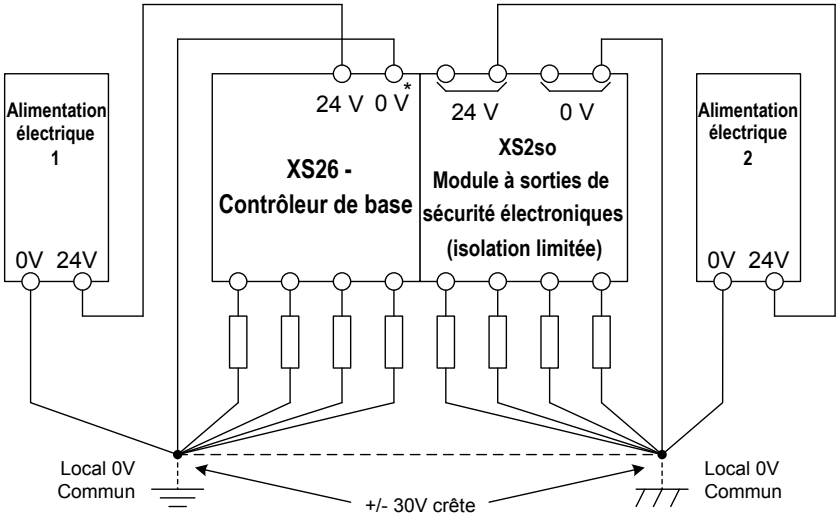
Illustration 42. Schéma de câblage — Mise à la terre recommandée

Schéma de routage 0 V à privilégier en cas d'utilisation d'une seule alimentation



* **La tension de tous les dispositifs d'entrée de sécurité (y compris tous les modules d'extension d'entrées) doit être mesurée en référence à la borne 0 V du contrôleur de base.**

Schéma de routage 0 V à privilégier en cas d'utilisation d'alimentations distinctes



Remarque: Le second jeu (les bornes 24 V et 0 V inutilisées ci-dessus) peut être utilisé pour faire passer l'alimentation d'un module au module suivant.

7.8.2 Sorties de relais de sécurité

Les modules relais de sécurité extensibles XS/SC26 et le SC10-2 possèdent des sorties relais redondantes isolées pouvant servir à contrôler/modifier un grand nombre de caractéristiques d'alimentation (référez-vous à la section Spécifications du XS/SC26 à la page 21 et à la section Spécifications du SC10-2 à la page 25). À la différence d'une sortie de sécurité électronique, dans un module de sortie, une sortie de relais de sécurité individuelle (Mx:ROx) fonctionne comme un groupe et ne peut pas être divisée.

Remarque: Chaque RO d'un module XS1ro ou XS2ro possède deux voies de commutation de sortie normalement ouvertes pour un raccordement à des circuits d'interruption d'alimentation fiables et une voie de sortie auxiliaire normalement fermée. Chaque RO du SC10-2 possède trois voies de commutation de sortie normalement ouvertes pour un raccordement à des circuits d'interruption d'alimentation fiables.

Les sorties de relais de sécurité sont contrôlées et surveillées par le contrôleur de base XS/SC26 ou le SC10-2 sans nécessiter de câblage supplémentaire.

Pour les circuits exigeant les niveaux de sécurité et de fiabilité les plus élevés, lorsqu'elles sont utilisées par paire (deux sorties NO), l'une ou l'autre sortie de sécurité doit être capable d'arrêter le mouvement de la machine surveillée en cas d'urgence. En cas d'utilisation individuelle (une seule sortie NO), l'exclusion de défauts doit prévenir toute défaillance susceptible d'entraîner la perte de la fonction de sécurité, par exemple un court-circuit vers une autre sortie de sécurité ou vers une source d'alimentation ou de tension secondaire. Pour en savoir plus, référez-vous au point *Commande à simple voie* de la section Circuits d'arrêt de sécurité (de protection) à la page 77 et à la section Élimination d'erreurs à la page 35.

Lorsque c'est possible, il est vivement recommandé d'inclure une fonction EDM (Surveillance des commutateurs externes) et/ou une fonction AVM (Moniteur de vanne réglable) pour surveiller les dispositifs sous contrôle (FSD et MPCE) afin de détecter les défaillances dangereuses. Référez-vous à la section Surveillance des commutateurs externes (EDM) à la page 74 pour en savoir plus.

Connexions de sortie — Les sorties de relais de sécurité doivent être raccordées à la commande de la machine pour que le système de commande de sécurité de la machine puisse interrompre le circuit ou l'alimentation des éléments de contrôle primaire de la machine (MPCE), permettant ainsi de supprimer le danger. Lorsque vous utilisez des dispositifs de commutation finaux (FSD), cette opération est normalement effectuée par ceux-ci lorsque les sorties de sécurité passent à l'état désactivé (Off).

Les sorties de relais de sécurité peuvent être utilisées comme dispositifs de commutation finaux (FSD) et interfacées dans un circuit d'arrêt de sécurité (protection) à simple ou double voie (voir Raccordement d'interface FSD à la page 77). Référez-vous à la section Spécifications du XS/SC26 à la page 21 et à la section Spécifications du SC10-2 à la page 25 avant d'effectuer les connexions et d'interfacer le contrôleur de sécurité à la machine.

Le niveau d'intégrité du circuit de sécurité doit être déterminé par une étude de risques. Ce niveau dépend de la configuration, de l'installation correcte des circuits externes ainsi que du type des dispositifs sous contrôle (FSD et MPCE). Les sorties de relais de sécurité sont adaptées aux applications de catégorie 4 PL e / SIL 3. Voir Illustration 41 à la page 72 pour des exemples de câblage.

Important: C'est à l'utilisateur qu'il incombe de fournir une protection contre la surtension pour toutes les sorties de relais.

Installations de catégories de surtension II et III (EN 50178 et IEC 60664-1)

Le XS/SC26 et le SC10-2 relèvent de la catégorie de surtension III lorsque des tensions de 1 à 150 Vca/cc sont appliquées aux contacts de relais de sortie. Ils relèvent de la catégorie de surtension II lorsque des tensions de 151 à 250 Vca/cc sont appliquées aux contacts de relais de sortie et qu'aucune précaution supplémentaire n'est prise pour atténuer les surtensions possibles dans la tension d'alimentation. Le XS/SC26 ou le SC10-2 peut être utilisé dans un environnement de catégorie de surtension III (avec des tensions de 151 à 250 Vca/cc) si des mesures ont été prises soit pour réduire le niveau des perturbations électriques subies par le XS/SC26 ou le SC10-2 aux niveaux de la catégorie de surtension II en installant des onduleurs (par exemple des suppresseurs d'arc), soit pour installer une isolation externe supplémentaire afin d'isoler à la fois le XS/SC26 ou le SC10-2 et l'utilisateur des niveaux de tension plus élevés d'un environnement de catégorie III.

Pour les installations de la catégorie de surtension III avec des tensions de 151 à 250 Vca/cc appliquées au(x) contact(s) de sortie : le XS/SC26 ou le SC10-2 peut être utilisé dans les conditions d'une catégorie de surtension supérieure lorsque des mesures appropriées de réduction de la surtension ont été prises. Pour ce faire, plusieurs méthodes sont envisageables :

- Dispositif de protection contre la surtension
- Transformateur avec des enroulements isolés
- Système de distribution avec plusieurs circuits de dérivation (capables de dévier l'énergie des surtensions transitoires)
- Condensateur capable d'absorber l'énergie des surtensions
- Résistance ou autre dispositif d'amortissement capable de dissiper l'énergie des surtensions

En cas de commutation de fortes charges, il est nécessaire de protéger les sorties du XS/SC26 ou du SC10-2 en installant des suppresseurs d'arc appropriés. Cependant, si vous utilisez des suppresseurs d'arc, vous devez les installer aux bornes de la charge à commuter (entre les coils des relais de sécurité externes par exemple) mais jamais aux contacts de sortie du XS/SC26 ou du SC10-2 (voir l'avertissement concernant les suppresseurs d'arc aux sections Raccordement générique du XS/SC26 : sortie de sécurité avec EDM à la page 79 et Raccordement générique du SC10-2 : sortie de sécurité avec EDM à la page 81).

7.8.3 Raccordement EDM et FSD

Surveillance des commutateurs externes (EDM)

Les sorties de sécurité du contrôleur de sécurité peuvent contrôler des relais, des contacteurs externes ou d'autres dispositifs possédant un jeu de contacts à guidage forcé (reliés mécaniquement) normalement fermés (NF) qui peuvent servir à surveiller l'état des contacts d'alimentation de la machine. Les contacts de surveillance sont normalement fermés (NF) lorsque le dispositif est hors tension. Ainsi, le contrôleur de sécurité est en mesure de détecter si les dispositifs sous tension répondent à la sortie de sécurité ou si les contacts normalement ouverts (NO) sont éventuellement soudés en position fermée ou bloqués en position ouverte.

Remarque: Les relais internes aux modèles XS1ro, XS2ro et SC10-2 sont toujours surveillés par les modules. La fonction EDM n'est nécessaire que pour les dispositifs externes aux contrôleurs.

La fonction EDM est une méthode de surveillance de ces types de défauts. Elle permet de s'assurer de l'intégrité fonctionnelle d'un système à deux voies, y compris les MPCE et les FSD.

Une même entrée EDM peut être assignée à une ou plusieurs sorties de sécurité. Pour ce faire, ouvrez la fenêtre **Propriétés** de la sortie de sécurité et vérifiez **EDM**, puis ajoutez **Surveillance des appareils externes** à partir de l'onglet **Entrée de sécurité** dans la fenêtre **Ajouter un équipement** (à laquelle vous accédez à partir de l'onglet **Équipement** ou de l'onglet **Vue fonctionnelle**) et reliez l'entrée **Surveillance des appareils externes** au nœud **EDM** de la sortie de sécurité.

Pour configurer les entrées EDM, vous avez le choix entre la surveillance à une voie ou la surveillance à deux voies. Les entrées EDM à une voie sont utilisées lorsque les sorties OSSD contrôlent directement la désactivation des MPCE ou d'autres dispositifs externes.

Surveillance à 1 voie

Un raccordement en série des contacts de surveillance fermés à guidage forcé (liés mécaniquement) de chaque dispositif contrôlé par le contrôleur de sécurité. Les contacts de surveillance doivent être fermés avant de pouvoir procéder au reset des sorties du contrôleur de sécurité (manuellement ou automatiquement). Après un reset et l'activation des sorties de sécurité, l'état des contacts de surveillance n'est plus surveillé et peut changer. Toutefois, les contacts de surveillance doivent être fermés dans les 250 millisecondes suivant la désactivation des sorties de sécurité. Référez-vous à la section Illustration 45 à la page 76.

Surveillance à deux voies

Un raccordement indépendant des contacts de surveillance fermés à guidage forcé (liés mécaniquement) de chaque dispositif contrôlé par le contrôleur de sécurité. Les deux entrées EDM doivent être fermées avant de pouvoir procéder au reset du contrôleur de sécurité et activer les OSSD. Lorsque les OSSD sont activés, les entrées peuvent changer d'état (toutes deux ouvertes ou toutes deux fermées). Si les entrées restent dans des états opposés plus de 250 millisecondes, un verrouillage se produit. Référez-vous à la section Illustration 47 à la page 77.

Pas de surveillance (par défaut)

Si vous ne souhaitez pas de surveillance, n'activez pas le nœud EDM de la sortie de sécurité. Si le contrôleur de sécurité n'utilise pas la fonction EDM dans des installations de catégorie 3 ou 4, l'utilisateur doit s'assurer que toute défaillance unique ou accumulation de défaillances des dispositifs externes n'entraîne pas de condition dangereuse et que les cycles suivants de la machine sont bloqués.

AVERTISSEMENT:

- **Surveillance des commutateurs externes (EDM)**
- L'existence d'une situation dangereuse peut entraîner des blessures graves, voire mortelles.
- Si le système est défini sur « Pas de surveillance », c'est à l'utilisateur qu'il revient de s'assurer que cela ne crée pas de situation dangereuse.

PRÉCAUTION:

- **Utilisez les contacts de surveillance des éléments de contrôle primaire de la machine (MPCE) pour maintenir la fiabilité des commandes.**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Câblez au moins un contact de surveillance à guidage forcé normalement fermé de chaque élément de contrôle primaire de la machine (MPCE) ou commutateur externe pour surveiller l'état des MPCE (comme illustré). En procédant de la sorte, il est possible de vérifier que les MPCE fonctionnent correctement.

Illustration 43. Câblage EDM à une voie

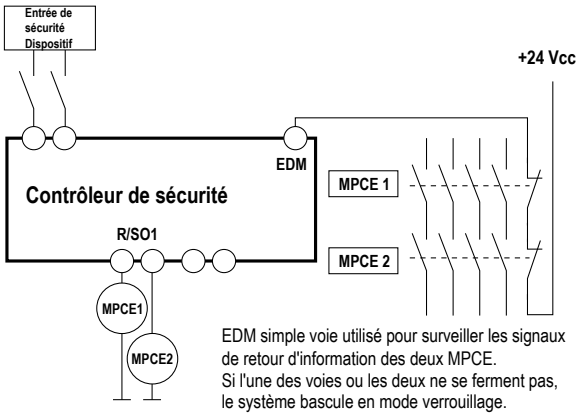


Illustration 44. Câblage EDM à deux voies

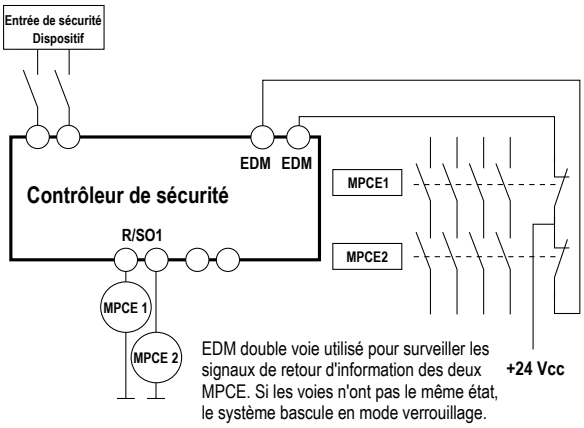
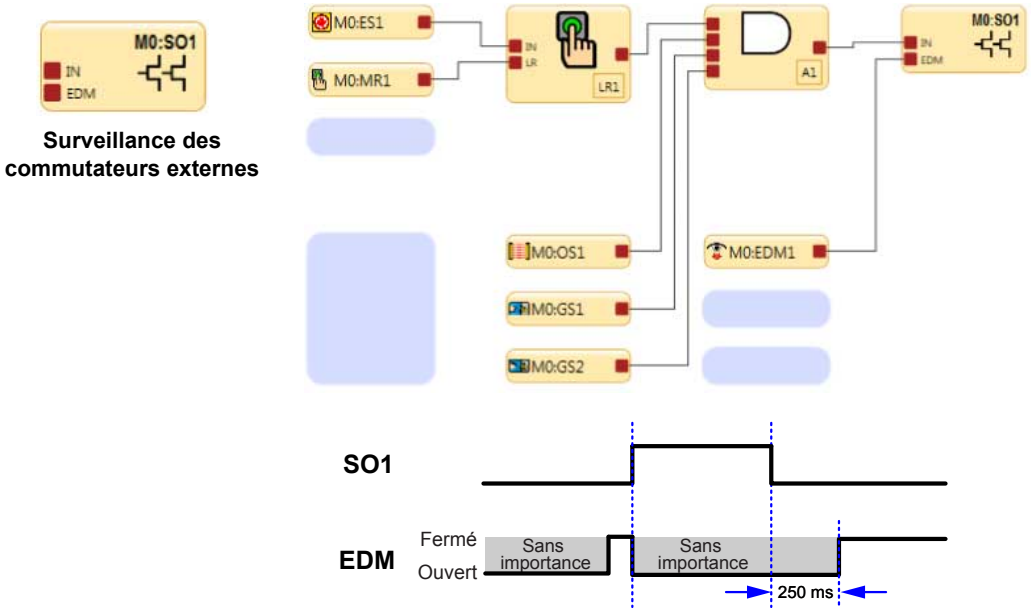


Illustration 45. Logique de temporisation : État EDM à une voie par rapport à la sortie de sécurité



L'EDM (surveillance des commutateurs externes) est une méthode permettant de vérifier le fonctionnement des dispositifs de commutation finaux (FSD) double voie ou les éléments de contrôle primaire d'une machine (MPCE). Les contacts de surveillance N.F. à guidage forcé des FSD ou MPCE sont utilisés comme entrée pour détecter un défaut de type « blocage en position On » et empêchent l'activation des sorties du contrôleur de sécurité.

Pour l'EDM à deux voies, comme illustré ci-dessous, les deux voies doivent être fermées avant que la ou les sorties de sécurité s'activent.

Illustration 46. Logique de temporisation : EDM à deux voies, temporisation entre les voies

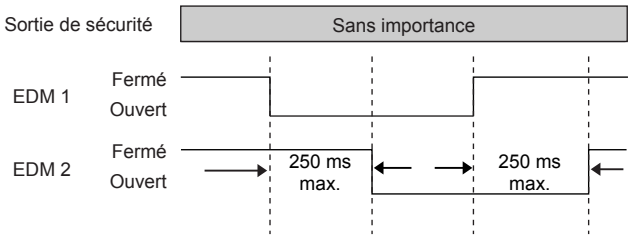
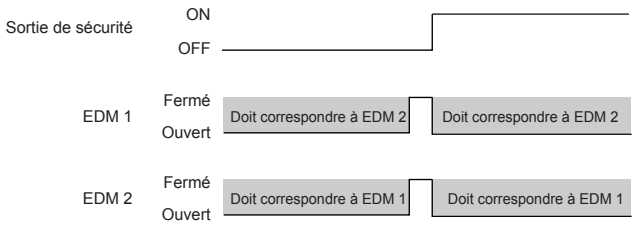


Illustration 47. Logique de temporisation : État EDM à deux voies par rapport à la sortie de sécurité



Raccordement d'interface FSD

Les FSD (Final Switching Device, dispositif de commutation final) interrompent l'alimentation du circuit vers le MPCE (Machine Primary Control Element, élément de contrôle principal de la machine) lorsque les sorties de sécurité passent à l'état désactivé (Off). Les FSD peuvent prendre de nombreuses formes, bien que les plus communes soient les relais à guidage forcé ou les modules d'interfaçage. La liaison mécanique entre les contacts permet de surveiller le dispositif via le circuit de surveillance des commutateurs externes pour certaines défaillances.

Selon l'application, l'utilisation des FSD peut faciliter le contrôle des différences de tension et de courant au niveau des sorties de sécurité du contrôleur de sécurité. Les FSD permettent également de contrôler plusieurs autres dangers en créant plusieurs circuits d'arrêt de sécurité.

Circuits d'arrêt de sécurité (de protection)

Un arrêt de sécurité permet d'arrêter le mouvement de la machine ou de mettre un terme à la situation dangereuse pour des raisons de sécurité, ce qui se traduit par un arrêt du mouvement et la coupure de l'alimentation par les MPCE (pour autant que cela ne crée pas d'autres dangers).

Un circuit d'arrêt d'urgence comprend généralement au moins deux contacts normalement ouverts (NO) provenant de relais à guidage forcé (liés mécaniquement), qui sont surveillés (via un contact normalement fermé (NF) lié mécaniquement) pour détecter certaines défaillances afin d'éviter la perte de la fonction de sécurité. Ce circuit est appelé « point de commutation de sécurité ».

En règle générale, un circuit d'arrêt de sécurité est une connexion en série d'au moins deux contacts NO provenant de deux relais à guidage positif distincts, chacun étant commandé par une sortie de sécurité séparée du contrôleur de sécurité. La fonction de sécurité utilise des contacts redondants pour contrôler un risque unique. De cette façon, si un contact ne bascule pas en position On, le second contact arrête le risque et empêche le démarrage du cycle suivant.

L'interfaçage des circuits d'arrêt d'urgence doit être effectué de sorte que la fonction de sécurité ne puisse pas être suspendue, contournée ou annulée sauf si cela entraîne un niveau de sécurité supérieur ou égal à celui du système de commande de la machine qui incorpore le contrôleur de sécurité.

Les sorties NO d'un module d'interfaçage représentent une connexion en série de contacts redondants qui forment le circuit d'arrêt de sécurité et peuvent servir dans des méthodes de commande à simple ou double voie.

Commande à double voie — Une commande à double voie (deux voies) permet d'étendre électriquement le point de commutation de sécurité au-delà des contacts FSD. Sous réserve d'une surveillance adéquate telle qu'EDM, cette méthode d'interfaçage est capable de détecter certaines défaillances du câblage de la commande entre le circuit d'arrêt d'urgence et les MPCE. A titre d'exemple de telles défaillances, citons le court-circuit d'une voie vers une source d'énergie ou de tension secondaire ou la perte de la commutation d'une des sorties FSD. Ces défaillances peuvent entraîner la perte de la redondance ou une perte complète de la fonction de sécurité si elles ne sont pas détectées et corrigées.

Le risque d'une défaillance de câblage augmente :

- Si la distance physique entre les circuits d'arrêt d'urgence FSD et les MPCE augmente
- Si la longueur ou le routage des câbles d'interconnexion augmente.
- Si les circuits d'arrêt d'urgence FSD et les MPCE sont situés dans des armoires différentes

Il est donc recommandé d'utiliser une commande à double voie conjointement à la surveillance EDM dans toute installation dont les FSD et les MPCE sont éloignés les uns des autres.

Commande à simple voie — Une commande à simple voie (ou à une voie) utilise un raccordement en série des contacts FSD pour créer un point de commutation de sécurité. Après ce point du système de commande de sécurité de la machine, des défaillances peuvent se produire et entraîner une perte de la fonction de sécurité, comme un court-circuit vers une source d'alimentation ou de tension secondaire.

C'est la raison pour laquelle cette méthode d'interfaçage ne doit être utilisée que dans les installations où les circuits d'arrêt de sécurité FSD et les MPCE se trouvent physiquement dans la même armoire, les uns à côté des autres et directement raccordés entre eux, ou lorsque toute possibilité d'une telle défaillance est exclue. Si ces conditions ne sont pas réunies, il faut utiliser une commande à deux voies.

Pour exclure la possibilité de telles défaillances, vous pouvez avoir recours aux méthodes suivantes (liste non exhaustive) :

- Séparer physiquement les fils des commandes d'interconnexion les uns des autres et des sources d'alimentation secondaires
- Faire passer les fils d'interconnexion des commandes dans des conduits, des parcours ou des chemins de câbles différents

- Utiliser une tension basse ou neutre pour les fils d'interconnexion afin d'éviter la mise sous tension du risque
- Monter tous les éléments (modules, interrupteurs, dispositifs sous contrôle, etc.) à l'intérieur de la même armoire électrique, les uns à côté des autres et raccordés directement par des fils très courts
- Installer correctement des câbles à plusieurs conducteurs ou des fils multiples qui passent dans des presse-étoupes réducteurs de tension. Le serrage excessif d'un réducteur de tension peut entraîner des courts-circuits à cet endroit
- Utiliser des composants à ouverture positive ou à entraînement direct installés et montés en mode positif

AVERTISSEMENT:
- **Installation correcte de suppresseurs d'arc ou de parasites**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Installez des suppresseurs comme illustré sur les coils des FSD ou des MPCE. N'installez jamais de suppresseurs directement sur les contacts des FSD ou des MPCE. Dans une telle configuration, les suppresseurs risqueraient de provoquer un court-circuit.

AVERTISSEMENT:
- **Interfaçage des sorties de sécurité** — Pour que le produit Banner Engineering fonctionne correctement, ses paramètres de sortie et les paramètres d'entrée de la machine doivent être pris en considération lors de l'interfaçage des sorties de sécurité transistorisées aux entrées de la machine.
- **Un raccordement inapproprié des sorties de sécurité à la machine sous surveillance pourrait entraîner des blessures graves, voire mortelles.**
- Les circuits de commande de la machine doivent être conçus de la façon suivante :

  La résistance maximale du câble entre les sorties de sécurité transistorisées du contrôleur de sécurité et les entrées de la machine ne doit pas être dépassée.

  La tension d'état OFF maximum de la sortie de sécurité transistorisée du contrôleur de sécurité n'entraîne pas de condition ON.

  Le courant de fuite maximum de sortie transistorisée du contrôleur de sécurité suite à la perte de 0 V n'entraîne pas de condition ON.

AVERTISSEMENT:
- **Risque d'électrocution**
- Prenez les précautions nécessaires pour éviter tout risque d'électrocution. Cela pourrait occasionner des blessures graves, voire mortelles.
- Coupez systématiquement l'alimentation électrique du système de sécurité (dispositif, module, interface, etc.) et de la machine surveillée avant de procéder à un raccordement ou de remplacer un composant. Il est parfois obligatoire de respecter certaines procédures de câblage/étiquetage. Reportez-vous aux normes OSHA 29CFR1910.147, ANSI Z244-1 ou aux normes applicables en matière de contrôle des énergies dangereuses.
- Limitez les raccordements au dispositif ou au système à ceux décrits dans ce manuel. L'installation et le câblage électriques doivent être effectués par du personnel qualifié [16] et répondre aux normes électriques appropriées et aux codes de câblage, notamment NEC (National Electrical Code), aux normes NFPA 79 ou IEC 60204-1, ainsi qu'à l'ensemble des normes et codes locaux applicables.

AVERTISSEMENT:
- **Câblage correct du dispositif**
- Un raccordement inapproprié du contrôleur de sécurité à une machine pourrait entraîner des risques de blessures graves, voire mortelles.
- L'utilisateur est responsable du câblage correct du contrôleur de sécurité. Les schémas de câblage généralisés sont fournis uniquement pour illustrer l'importance d'une installation correcte.

[16] Personne titulaire d'un diplôme reconnu ou d'un certificat de formation professionnelle, ou ayant démontré, par ses connaissances approfondies et son expérience, sa capacité à résoudre les problèmes relevant de son domaine de spécialité

Raccordement générique du XS/SC26 : sortie de sécurité avec EDM

Illustration 48. Raccordement générique du XS/SC26 : sortie de sécurité électronique avec EDM

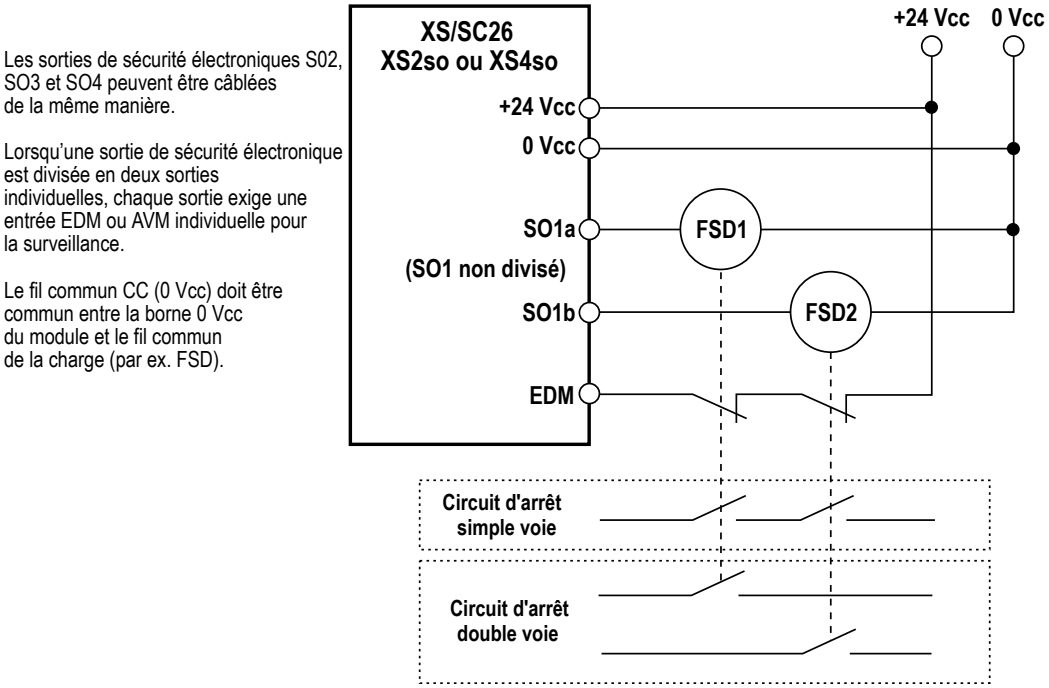
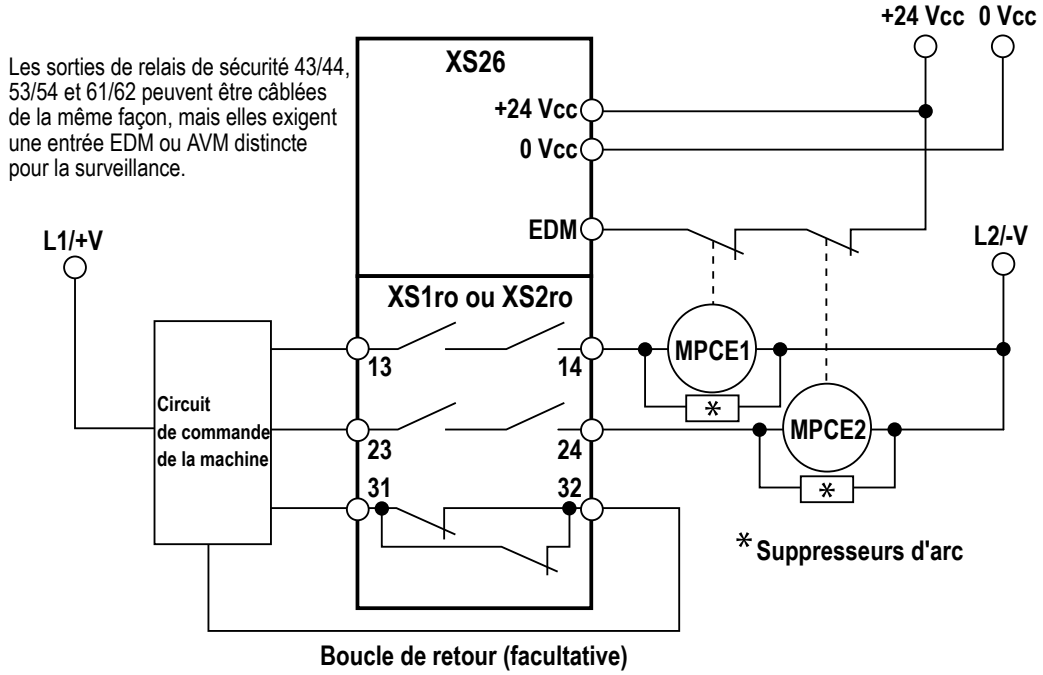


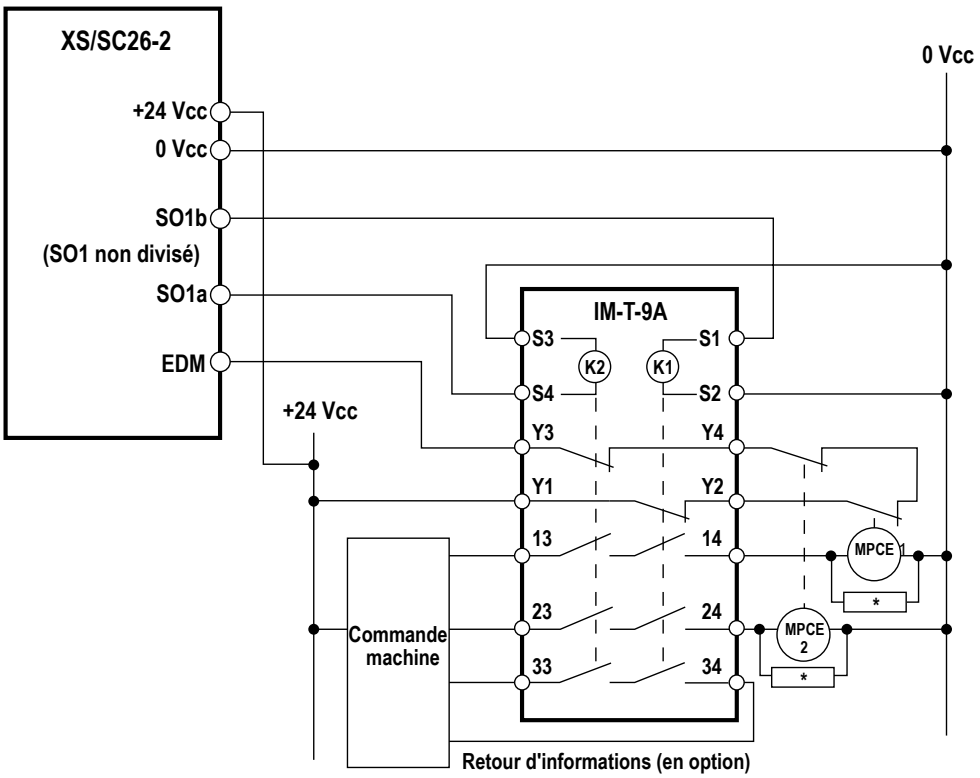
Illustration 49. Raccordement générique du XS/SC26 : sortie de relais de sécurité (double voie) avec EDM



AVERTISSEMENT:

- **Installation correcte de suppresseurs d'arc ou de parasites**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Installez les suppresseurs comme indiqué sur les bobines des éléments de contrôle primaire de la machine (MPCE). Ne les installez pas directement sur les contacts de sortie du module d'interface ou de sécurité. Dans une telle configuration, les suppresseurs pourraient provoquer un court-circuit.

Illustration 50. Raccordement générique du XS/SC26 : sortie de sécurité électronique vers le module IM-T-9A



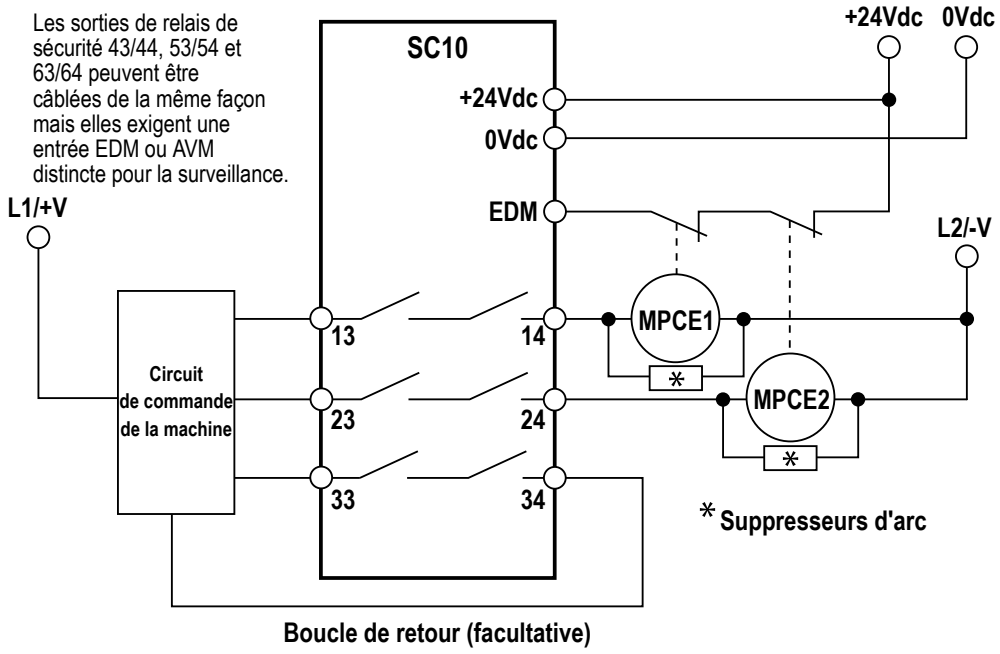
*** L'installation de suppresseurs de parasites entre les bobines de MPCE1 et de MPCE2 est recommandée (voir l'avertissement)**

AVERTISSEMENT:

- **Installation correcte de suppresseurs d'arc ou de parasites**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Installez les suppresseurs comme indiqué sur les bobines des éléments de contrôle primaire de la machine (MPCE). Ne les installez pas directement sur les contacts de sortie du module d'interface ou de sécurité. Dans une telle configuration, les suppresseurs pourraient provoquer un court-circuit.

Raccordement générique du SC10-2 : sortie de sécurité avec EDM

Illustration 51. Raccordement générique du SC10-2 : sortie de relais de sécurité (double voie) avec EDM



AVERTISSEMENT:

- **Installation correcte de suppresseurs d'arc ou de parasites**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Installez les suppresseurs comme indiqué sur les bobines des éléments de contrôle primaire de la machine (MPCE). Ne les installez pas directement sur les contacts de sortie du module d'interface ou de sécurité. Dans une telle configuration, les suppresseurs pourraient provoquer un court-circuit.

7.9 Sorties d'état

Pour savoir comment ajouter une sortie d'état, voir la section Ajout de sorties d'état à la page 90.

Une sortie d'état peut être utilisée pour envoyer un signal non lié à la sécurité à des dispositifs tels que des voyants lumineux ou des contrôleurs logiques programmables (API) pour indiquer l'état d'une entrée, d'une sortie de sécurité, d'un bloc logique ou d'un bloc fonction. Par exemple, une sortie d'état de suivi d'entrée est utilisée pour indiquer l'état (ON ou OFF) de l'entrée sélectionnée (sur le voyant lumineux ou l'API).

7.9.1 Conventions pour les signaux d'état des sorties

Remarque: Vous ne pouvez pas utiliser les sorties de sécurité comme sorties d'état dans le SC10-2.

Vous avez le choix entre deux conventions pour les signaux d'état des sorties :

- « PNP ON » (source 24 Vcc) suit l'état des éléments suivis
- « PNP OFF » (non conducteur), état opposé à l'élément suivi

La convention par défaut est Actif = PNP ON.

Pour XS/SC26 FID 4 et ultérieur, un taux de clignotement peut également être configuré pour signaler une sortie d'état active (ON). Les trois options sont les suivantes :

- Aucun (pour un état ON fixe)
- Normal (activation pendant 500 ms et désactivation pendant 500 ms)
- Rapide (activation pendant 150 ms et désactivation pendant 150 ms)

La fréquence de clignotement par défaut est « Aucun ». Il n'est pas possible de configurer une fréquence de clignotement pour une sortie d'état Inhibé (voir Inhibé dans la section Fonctions des sorties d'état à la page 82).

Table 6. Conventions pour les signaux d'état des sorties

Fonction	Conventions pour les signaux			
	Actif = PNP ON		Actif = PNP OFF	
	État de sortie d'état		État de sortie d'état	
	+24 Vcc	OFF	OFF	24 Vcc
Dérivation	Dérivé	Non dérivé	Dérivé	Non dérivé
Inhibition	Inhibé	Non inhibé	Inhibé	Non inhibé
Temporisation de sortie en cours	Retard	Pas de retard	Retard	Pas de retard
Tracer entrée	Marche	Arrêt	Marche	Arrêt
Tracer un défaut d'entrée	Défaut	OK	Défaut	OK
Tracer tout défaut d'entrée	Défaut	OK	Défaut	OK
Tracer groupe d'entrées	A initié l'arrêt	Une autre entrée a provoqué l'arrêt	A initié l'arrêt	Une autre entrée a provoqué l'arrêt
Tracer sortie	Sortie de sécurité ON	Sortie de sécurité OFF	Sortie de sécurité ON	Sortie de sécurité OFF
Tracer défaut de sortie	Défaut	OK	Défaut	OK
Tracer tous les défauts de sortie	Défaut	OK	Défaut	OK
Tracer l'état logique de sortie	Logiquement ON	Logiquement OFF	Logiquement ON	Logiquement OFF
Tracer l'état bloc fonction (XS/SC26 FID 2 ou ultérieur et SC10-2)	Marche	Arrêt	Marche	Arrêt
Tracer l'état bloc fonction (XS/SC26 FID 4 ou ultérieur)	Référez-vous à la section Fonctions de sortie d'état de la commande de presse à la page 83 pour plus d'informations.			
En attente de reset manuel	Reset nécessaire	Non satisfait	Reset nécessaire	Non satisfait
Verrouillage du système	Verrouillage	Mode RUN (marche)	Verrouillage	Mode RUN (marche)

7.9.2 Fonctions des sorties d'état

SC10-2 : il est possible d'utiliser jusqu'à 4 entrées convertibles comme sorties d'état.

XS/SC26 : il est possible d'utiliser jusqu'à 32 entrées convertibles ou sorties de sécurité comme sorties d'état. Les sorties de sécurité électroniques peuvent être divisées et utilisées en tant que sorties d'état. Les sorties de relais de sécurité ne peuvent pas être utilisées comme sorties d'états ni être divisées.

Les sorties de sécurité peuvent être configurées pour effectuer les fonctions suivantes :

Dérivation

Indique quand l'entrée reliée au bloc fonction de dérivation est dérivée.

Inhibition

Indique un état actif de l'inhibition pour l'entrée connectée au bloc fonction d'inhibition en question :

- ON quand une entrée de sécurité inhibable est inhibée
- OFF quand une entrée de sécurité inhibable n'est pas inhibée
- Clignotant en présence de conditions permettant le démarrage d'une neutralisation dépendante de l'inhibition (cycle d'inhibition inactif, sortie de sécurité inhibable en état d'arrêt et au moins un capteur d'inhibition en état d'arrêt (bloqué) ; indisponible pour une entrée d'état virtuelle
- ON pendant une fonction de neutralisation dépendante de l'inhibition active (pas une fonction de dérivation) d'une entrée de sécurité inhibable

Temporisation de sortie en cours

Indique si le retard à l'enclenchement ou au déclenchement est actif.

Tracer entrée

Indique l'état d'une entrée de sécurité donnée.

Tracer un défaut d'entrée

Indique quand une entrée de sécurité donnée présente un défaut.

Tracer tout défaut d'entrée

Indique quand n'importe quelle entrée de sécurité présente un défaut.

Tracer groupe d'entrées

Indique l'état d'un groupe d'entrées de sécurité, par exemple l'entrée de sécurité qui s'est désactivée en premier. Dès que la fonction a été exécutée, elle peut être réactivée par une entrée de reset configurée. Il est possible d'effectuer un suivi de trois groupes d'entrées maximum.

Tracer sortie

Indique l'état physique d'une sortie de sécurité donnée (ON ou OFF).

Tracer défaut de sortie

Indique quand une sortie de sécurité donnée présente un défaut.

Tracer tous les défauts de sortie

Indique un défaut de n'importe quelle sortie de sécurité.

Tracer l'état logique de sortie

Indique l'état logique d'une sortie de sécurité donnée. Par exemple, l'état logique est OFF mais la sortie de sécurité est en état Retard au déclenchement et n'est pas encore physiquement désactivée.

Tracer l'état bloc fonction (XS/SC26 FID 2 ou ultérieur et SC10-2)

Indique l'état d'un bloc fonction donné.

Tracer l'état bloc fonction (XS/SC26 FID 4 ou ultérieur)

Indique l'état d'un certain nombre d'événements du bloc fonction Commande de presse ; voir Fonctions de sortie d'état de la commande de presse à la page 83 pour plus de détails.

En attente de reset manuel

Indique quand un reset configuré spécifique est nécessaire.

Remarque: Si l'entrée de reset manuelle est connectée à un bloc OR Reset, cette sortie d'état ne peut pas être utilisée.

Verrouillage du système

Indique un verrouillage non fonctionnel, par exemple une entrée non assignée connectée à 24 V.

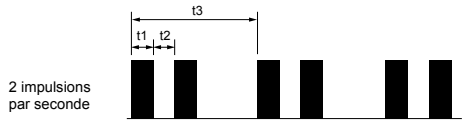
7.9.3 Fonctions de sortie d'état de la commande de presse

Cette fonction est disponible sur le XS/SC26 FID 4 et ultérieur.

Le bloc fonction Commande de presse possède plusieurs entrées et sorties. Vous bénéficiez ainsi d'une fonction de sortie d'état qui ne se résume pas à la simple mise en marche/arrêt d'un élément individuel. La sortie d'état du bloc Commande de presse comporte sept événements différents qui peuvent être signalés via la sortie d'état. La sortie d'état du bloc Commande de presse peut être configurée pour fournir un, deux ou trois signaux. Chaque signal de la sortie d'état du bloc Commande de presse se présente comme suit :

- Allumé en continu
- 2 impulsions par seconde

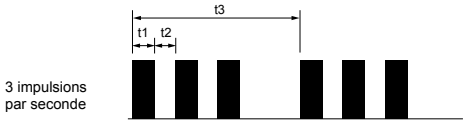
Illustration 52. 2 impulsions par seconde



t1 = 100 ms, t2 = 100 ms, et t3 = 1 seconde

- 3 impulsions par seconde

Illustration 53. 3 impulsions par seconde

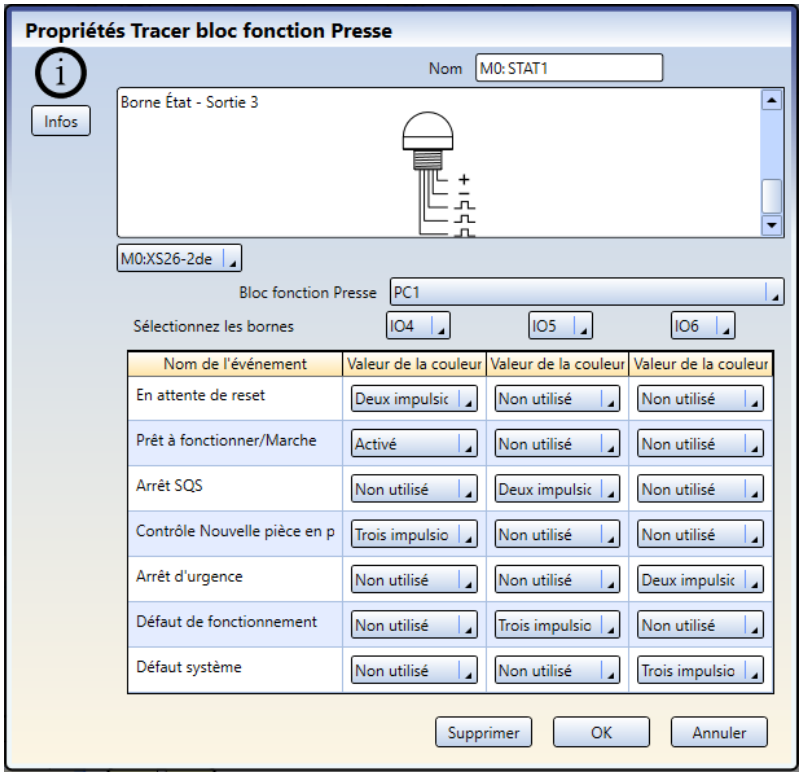


t1 = 100 ms, t2 = 100 ms, et t3 = 1 seconde

La sortie d'état du bloc Commande de presse est uniquement disponible sous la forme de sorties d'état physiques. Chaque sortie d'état physique peut être utilisée pour signaler trois événements différents.

La figure suivante illustre les paramètres par défaut de la sortie d'état du bloc fonction Commande de presse :

Illustration 54. Suivi des propriétés du bloc fonction Commande de presse



Le réglage par défaut du bloc fonction configure trois des broches d'E/S comme sorties d'état. Si vous ne devez pas afficher les sept événements pour une application donnée, utilisez la barre de défilement à droite de la figure pour sélectionner moins de broches. En montant la barre d'une position, vous réduisez le nombre de bornes à deux, en la montant de deux positions, vous réduisez le nombre de bornes à une.

La fonctionnalité de chaque événement est la suivante :

- **En attente de reset** : s'active lorsqu'une entrée de reset est nécessaire, après que les entrées d'arrêt d'urgence non inhibables et inhibables (si configurées) reviennent à l'état ON.
- **Prêt à fonctionner / Marche** : activé chaque fois que la presse est prête à fonctionner (les entrées d'arrêt d'urgence inhibables et non inhibables sont activées et ont fait l'objet d'un reset) ou la presse fonctionne en course montante ou descendante.
- **Arrêt SQS** : s'active lorsque le coulisseau de la presse atteint le point d'arrêt de la séquence.
- **Alerte de contrôle PIP** : s'active lorsque la presse est prête à fonctionner, que le système tente de démarrer un cycle de presse et que l'entrée PIP (pièce en place), si elle est configurée, est désactivée ou ne s'est pas désactivée puis réactivée (pièce non retirée et remplacée).
- **Arrêt d'urgence** : s'active lorsque l'entrée d'arrêt d'urgence inhibable ou non inhibable se désactive et que le nœud d'entrée GO passe en position basse (lorsqu'il est configuré pour le paramétrage manuel Course montante) avant que le point SQS, BOS ou TOS ne soit atteint (selon les réglages et l'étape du cycle).
- **Défaut opérationnel** : s'active lorsque des entrées opérationnelles mutuellement exclusives sont activées (par exemple, TOS et BOS, TOS et SQS, TOS et PCMS, SQS et BOS, etc. ; si plus de 3 secondes s'écoulent entre l'activation de deux signaux SQS et PCMS, si la configuration le prévoit).
- **Défaut système** : s'active en présence d'un défaut système.

7.10 Sorties d'état virtuelles

Il est possible d'ajouter jusqu'à 64 sorties d'état virtuelles à l'aide des protocoles Modbus TCP, assemblys d'entrées EtherNet/IP, messages explicites EtherNet/IP et PCCC sur des contrôleurs de sécurité XS/SC26 FID 1 et jusqu'à 256 sorties d'état virtuelles sur des contrôleurs de sécurité XS/SC26 FID 2 ou ultérieur et des contrôleurs de sécurité SC10-2. Les contrôleurs de sécurité XS/SC26 FID 2 ou ultérieur et les contrôleurs de sécurité SC10-2 peuvent également utiliser PROFINET. Les contrôleurs de sécurité XS26 FID 6 ou ultérieur, compatibles Ethernet et extensibles peuvent également utiliser EtherCAT lorsque le module de passerelle de communication XSeCAT est ajouté. Ces sorties peuvent communiquer les mêmes informations que les sorties d'état sur le réseau. Référez-vous à la section Fonctions des sorties d'état à la page 82 pour en savoir plus. La fonction **Autoconfiguration**, située dans l'onglet **Ethernet industriel** du logiciel, configure automatiquement les sorties d'état virtuelles avec un ensemble de fonctions fréquemment utilisées, sur la base de la configuration actuelle. Il est préférable d'utiliser cette fonction après avoir défini la configuration. Il est possible de modifier manuellement la configuration des sorties d'état virtuelles après avoir utilisé la fonction **Autoconfiguration**. Les informations disponibles sont cohérentes avec l'état logique des entrées et des sorties dans un délai de 100 ms ou moins pour les tableaux Sorties d'état virtuelles (que vous pouvez consulter dans le logiciel) et dans un délai d'une seconde ou moins pour les autres tableaux. L'état logique des entrées et des sorties est déterminé au terme

de tous les tests et anti-rebond internes. Référez-vous à la section Onglet Ethernet industriel à la page 125 pour plus de détails sur la configuration des sorties d'état virtuelles.

Les contrôleurs de sécurité SC10-2 FID 2 ou ultérieur et les contrôleurs de sécurité XS26-ISD FID 5 ou ultérieur peuvent fournir des informations d'état et de performance sur les dispositifs individuels et les chaînes ISD. Il est possible d'obtenir seize mots (word) (16 bits) sur l'état de chaque chaîne. Il est possible d'obtenir trois mots (word) administratifs (16 bits) et 18 octets (8 bits chacun) de données spécifiques sur un dispositif individuel d'une chaîne. Référez-vous à la section Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52 pour plus d'informations.

8 Mise en route

Mettez le contrôleur de sécurité sous tension et vérifier que la LED d'alimentation est verte fixe.

8.1 Création d'une configuration

Pour créer et confirmer (écriture sur le contrôleur) la configuration, procédez comme suit :

1. Définissez l'application de protection (étude de risques) :
   - Détermination des dispositifs nécessaires
   - Détermination du niveau de sécurité requis
2. Installez le logiciel Contrôleur de sécurité Banner. Référez-vous à la section Installation du logiciel à la page 30.
3. Familiarisez-vous avec les options du logiciel. Référez-vous à la section Présentation du logiciel à la page 112.
4. Lancez le logiciel et sélectionnez le dispositif requis.
5. Commencez un nouveau projet en cliquant sur **Nouveau projet/fichiers récents**.
6. Définissez les **paramètres du projet**. Référez-vous à la section Paramètres du projet à la page 115.
7. XS/SC26 : personnalisez le contrôleur de base et ajoutez des modules d'extension et/ou une passerelle de communication (le cas échéant). Référez-vous à la section Onglet Équipement à la page 116.
8. Ajoutez des dispositifs d'entrée de sécurité, des dispositifs d'entrée auxiliaires et des sorties d'état. Référez-vous à la section Ajout d'entrées et de sorties d'état à la page 86.
9. Créez la logique de contrôle. Référez-vous à la section Conception de la logique de contrôle à la page 91.
10. Réglez les retards à l'enclenchement ou au déclenchement des sorties de sécurité facultatives.
11. Si vous utilisez le réseau, configurez les paramètres réseau. Référez-vous à la section :
    - Paramètres réseau : Modbus TCP, Ethernet/IP, PCCC à la page 130
    - Paramètres réseau : PROFINET à la page 130
    - Paramètres réseau : EtherCAT à la page 131
12. Enregistrez et confirmez la configuration. Référez-vous à la section Enregistrement et confirmation d'une configuration à la page 92.

Les étapes suivantes sont facultatives et peuvent faciliter l'installation du système :

- Modifiez les droits d'accès à la configuration. Référez-vous à la section Gestionnaire des mots de passe du XS/SC26 à la page 135 ou Gestionnaire des mots de passe du SC10-2 à la page 136.
- Accédez à l'onglet **Résumé de la configuration** pour afficher des informations détaillées sur les dispositifs et les temps de réponse. Référez-vous à la section Onglet Résumé de la configuration à la page 133.
- Imprimez les vues de configuration, dont **Résumé de la configuration** et **Paramètres réseau**. Référez-vous à la section Options d'impression à la page 134.
- Testez la configuration avec le mode simulation. Référez-vous à la section Mode simulation à la page 142.

8.2 Ajout d'entrées et de sorties d'état

Il est possible d'ajouter des entrées de sécurité et des entrées auxiliaires dans l'onglet **Équipement** ou l'onglet **Vue fonctionnelle**. Les sorties d'état peuvent être uniquement ajoutées dans l'onglet **Équipement**. Il est uniquement possible d'ajouter des entrées auxiliaires virtuelles à partir de l'onglet **Vue fonctionnelle**. Lorsque des entrées sont ajoutées dans l'onglet **Équipement**, elles sont automatiquement placées dans l'onglet **Vue fonctionnelle**. Toutes les entrées, les **blocs logiques** et les **blocs fonction** peuvent être déplacés au sein de l'onglet **Vue fonctionnelle**. Les **entrées de sécurité** sont statiques et placées à droite.

8.2.1 Ajout d'entrées de sécurité et d'entrées auxiliaires

1. Dans l'onglet **Équipement**, cliquez sur ✚ sous le module auquel le dispositif d'entrée sera connecté (le module et les bornes peuvent être modifiés dans la fenêtre **Propriétés** du dispositif d'entrée) ou l'un des emplacements réservés dans l'onglet **Vue fonctionnelle**.

   Remarque: Les entrées auxiliaires virtuelles ne sont disponibles que dans l'onglet **Vue fonctionnelle**.

2. Cliquez sur **Entrée de sécurité** ou **Entrée auxiliaire** pour ajouter des dispositifs d'entrée :

Illustration 55. XS/SC26 : Ajout d'entrées à partir de la Vue fonctionnelle (les entrées auxiliaires virtuelles ne peuvent être ajoutées qu'à partir de cette vue)

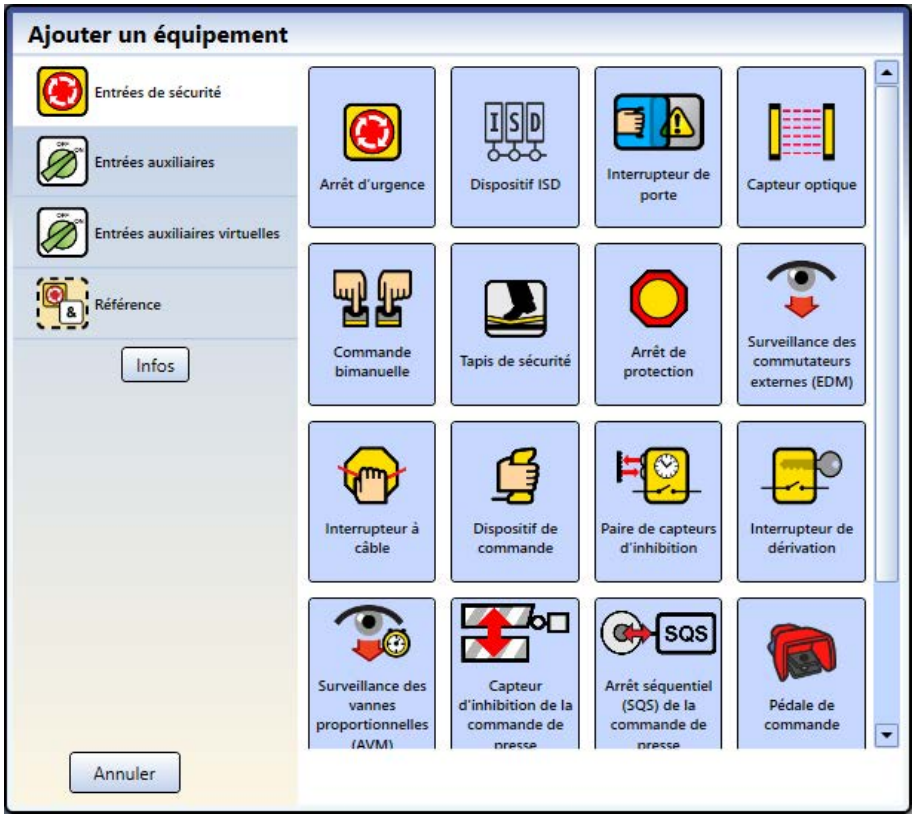
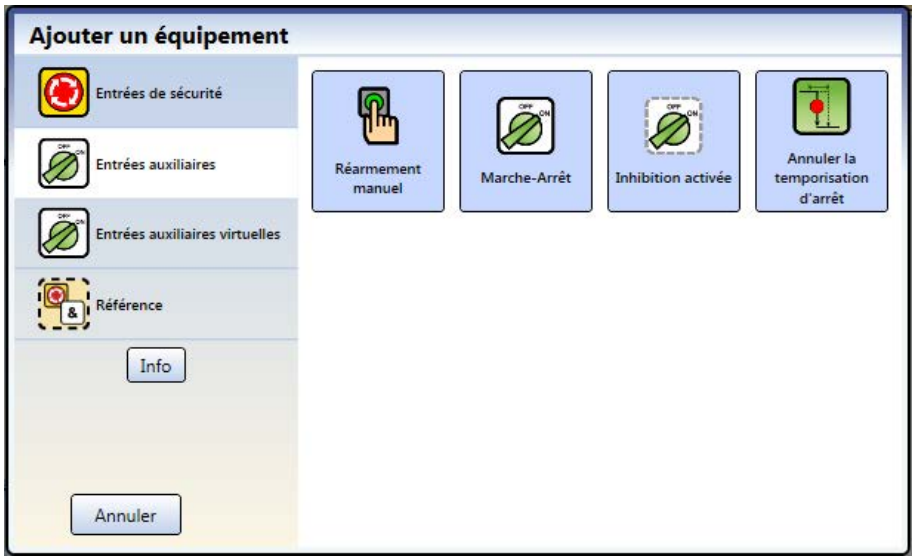


Illustration 56. SC10-2 : Ajout d'entrées à partir de la vue Équipement (la sortie d'état physique ne peut être ajoutée qu'à partir de cette vue)



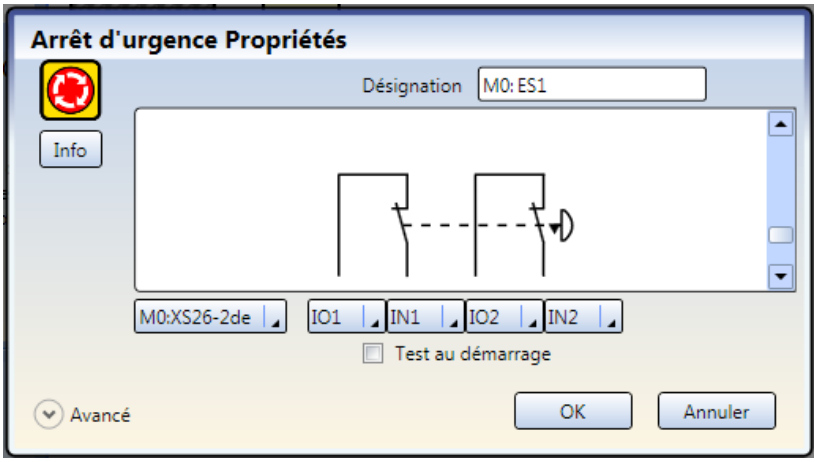
*Illustration 57. Entrées auxiliaires (entrées auxiliaires virtuelles uniquement disponibles dans l'onglet **Vue fonctionnelle**)*



3. Sélectionnez les paramètres appropriés pour le dispositif :

Paramètres de base :

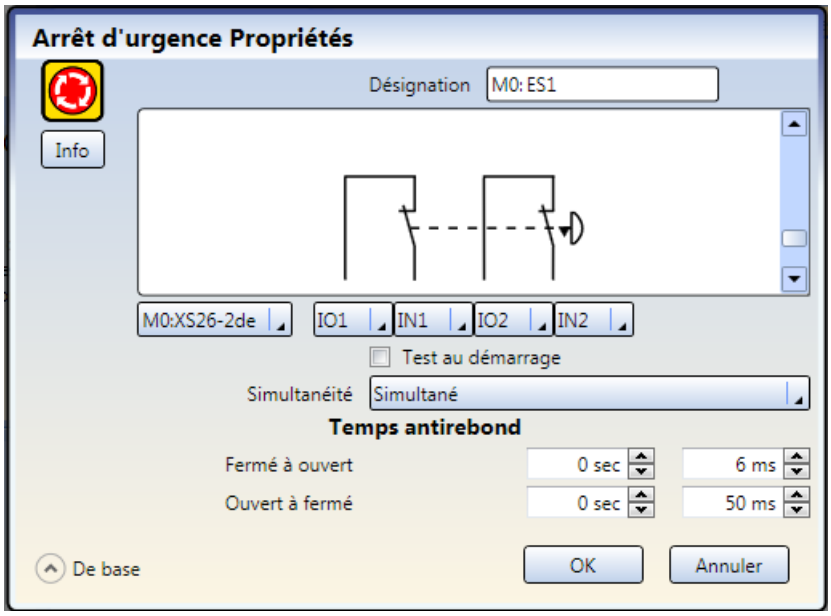
Illustration 58. Paramètres d'entrée de sécurité de base



- *Nom* — nom du dispositif d'entrée généré automatiquement, avec possibilité pour l'utilisateur de le modifier. Les noms ne peuvent pas dépasser 10 caractères. Lorsque le nom est affiché sur l'écran des modèles avec écran, 8 caractères maximum sont affichés (en raison de contraintes de taille).
- *Type de circuit* — options de circuit et de convention de signal appropriées pour le dispositif d'entrée sélectionné ; faites défiler pour consulter et sélectionner l'option souhaitée.
- *Module* — module auquel le dispositif d'entrée est connecté (par exemple, M0:XS26-2e)
- *Bornes E/S* — assignation des bornes d'entrée pour le dispositif sélectionné sur le module sélectionné
- *Test au démarrage* (dans les cas applicables) — test facultatif du dispositif d'entrée de sécurité requis après chaque mise sous tension
- *Options de reset* (dans les cas applicables) — diverses options de reset, par exemple Reset manuel à la mise sous tension, Reset du système et Reset du tracé de groupe d'entrées

Paramètres avancés (dans les cas applicables) :

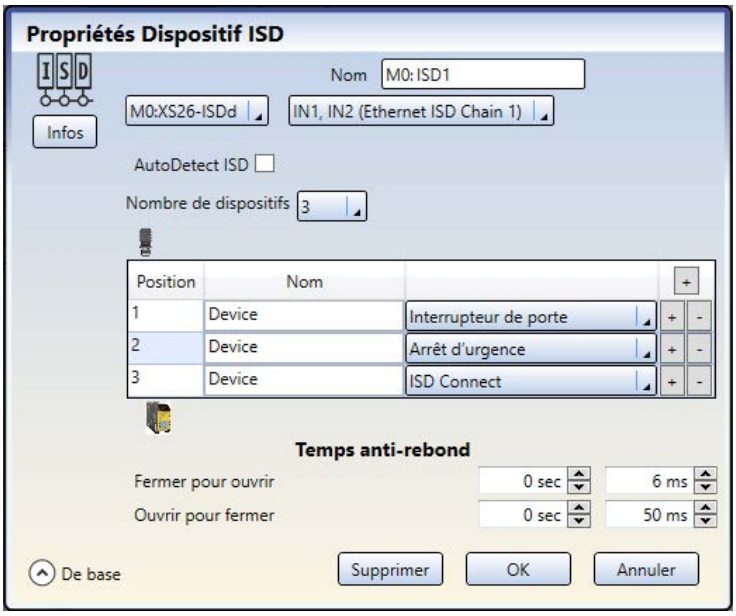
Illustration 59. Paramètres d'entrée de sécurité avancés



- *Simultanéité* (dans les cas applicables) — Simultané ou Concurrent (consultez la section Glossaire à la page 362 pour des définitions)
- *Temps anti-rebond* — durée de la transition d'état du signal
- *Surveillé / Non surveillé* (dans les cas applicables) — voir Exigences relatives au signal de reset à la page 63

Propriétés du dispositif ISD (dans les cas applicables) :

Illustration 60. Paramètres avancés du dispositif ISD



- *Nom* — nom du dispositif d'entrée généré automatiquement, avec possibilité pour l'utilisateur de le modifier Les noms ne peuvent pas dépasser 10 caractères. Lorsque le nom est affiché sur l'écran des modèles avec écran, 8 caractères maximum sont affichés (en raison de contraintes de taille)
- *Bornes E/S* — assignation des bornes d'entrée pour le dispositif sélectionné sur le module sélectionné
- *Nombre de dispositifs* (obligatoire) — nombre de capteurs ISD utilisés dans l'application
- *Détection auto ISD* (le cas échéant) — option qui, si elle est sélectionnée, permet au contrôleur de déterminer automatiquement le nombre de dispositifs et leurs types en cours de fonctionnement. Pour plus d'informations, voir Option Détection auto ISD à la page 326.
- *Base de référence manuelle à la mise sous tension* (le cas échéant) — option qui, une fois sélectionnée, permet au contrôleur de définir le bit « Nouvelle base de référence » sur le logiciel et/ou l'API connecté. Le bit « Accepter cette base de référence » doit être renvoyé au contrôleur pour accepter et définir la configuration actuelle comme base de démarrage. La case à cocher **Base de référence manuelle à la mise sous tension** est disponible lorsque la case **Détection auto ISD** est cochée.
- *Position, nom et type* — position, nom et type (interrupteur de porte, bouton d'arrêt d'urgence, système ISD Connect) des capteurs ISD utilisés dans l'application Le **nom**, ou désignation, est généré automatiquement et peut être modifié par l'utilisateur. Le **type** est un menu avec plusieurs options proposées à l'utilisateur.
- *Temps anti-rebond* — durée de la transition d'état du signal

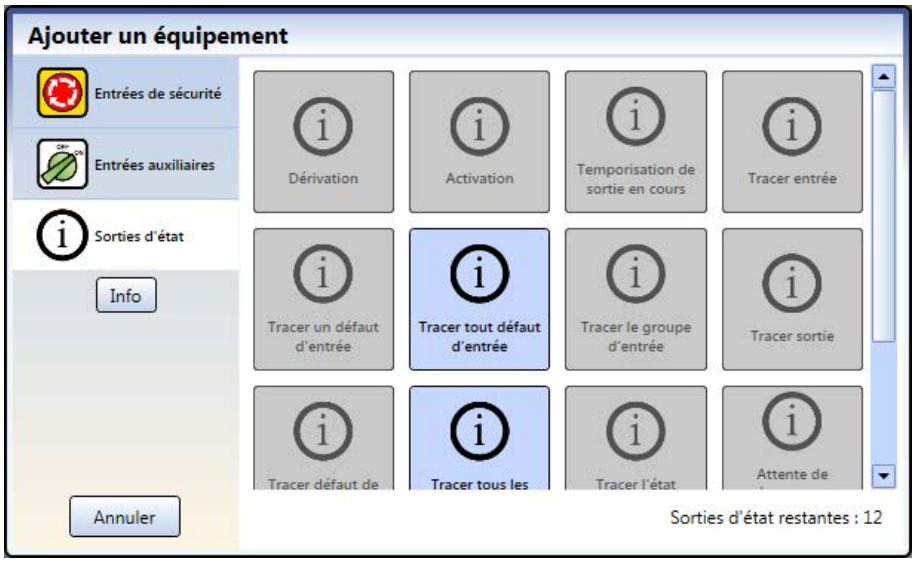
Remarque: Le logiciel Contrôleur de sécurité Banner applique les règles de l'interrupteur de porte aux entrées ISD.

8.2.2 Ajout de sorties d'état

1. Dans l'onglet **Équipement**, cliquez sur ✣ sous le module chargé de la surveillance d'états.
2. Cliquez sur **Sorties d'état** pour ajouter la surveillance d'état [17].

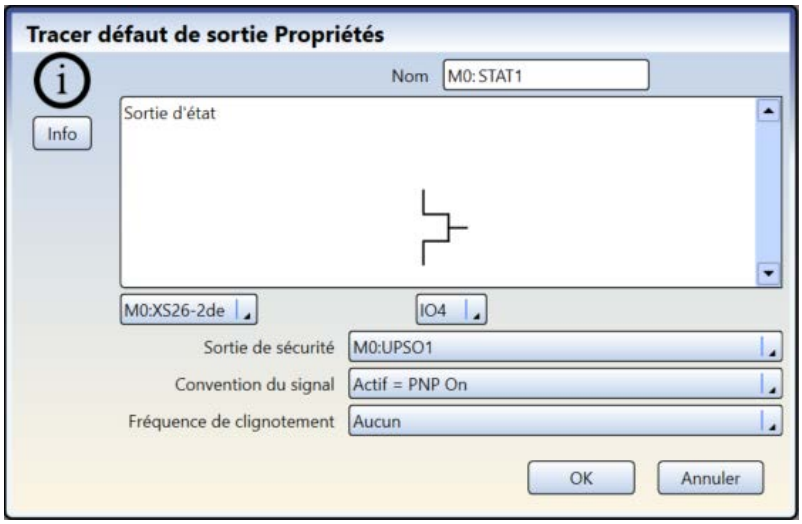
[17] Il est utile de configurer les sorties d'état lorsqu'il est nécessaire de communiquer l'état d'un dispositif d'entrée ou d'une sortie. Les bornes IOx servent à transmettre ces signaux d'état.

Illustration 61. Sorties d'état



3. Sélectionnez les paramètres de sortie d'état appropriés :

Illustration 62. Propriétés des sorties d'état



- *Nom* — Les noms peuvent comporter 10 caractères maximum. Lorsque le nom est affiché sur l'écran des modèles à écran, 8 caractères maximum sont affichés (en raison de contraintes de taille)
- *Module*
- *E/S (dans les cas applicables)*
- *Borne*
- *Entrée ou Sortie (dans les cas applicables)*
- *Convention du signal*
- *Fréquence de clignotement*

8.3 Conception de la logique de contrôle

Pour **concevoir la logique de contrôle** :

1. Ajoutez les entrées de **sécurité** et les **entrées auxiliaires** souhaitées :
   - Dans l'onglet **Équipement** : cliquez sur ✚ sous le module auquel l'entrée sera connectée (il est possible de modifier le module dans la fenêtre **Propriétés** de l'entrée).
   - Dans l'onglet **Vue fonctionnelle** : cliquez sur l'un des emplacements réservés vides dans la colonne de gauche.

   Référez-vous à la section Ajout d'entrées et de sorties d'état à la page 86 pour en savoir plus, notamment sur les propriétés des dispositifs.
2. Ajoutez des **blocs logiques** et/ou des **blocs fonction** (référez-vous aux sections Blocs logiques à la page 118 et Blocs fonction à la page 121) en cliquant sur l'un des emplacements réservés vides dans la partie centrale.

Remarque: Le temps de réponse des sorties de sécurité peut augmenter si vous ajoutez un grand nombre de blocs à la configuration. Utilisez les blocs fonction et logiques de façon efficace afin d'obtenir des temps de réponse optimaux.

3. Créez les connexions appropriées entre les entrées, les **blocs fonction** et **logiques** et les sorties de sécurité que vous avez ajoutés.

AVERTISSEMENT:
- **Configuration conforme aux normes applicables**
- Le fait de ne pas vérifier l'application peut entraîner des blessures graves, voire mortelles.
- Le logiciel Contrôleur de sécurité Banner vérifie principalement la configuration logique pour détecter des erreurs de connexion. Il incombe à l'utilisateur de vérifier que l'application répond aux exigences de l'évaluation des risques et qu'elle est conforme à toutes les normes applicables.

Remarque: La liste de contrôle à gauche affiche les connexions requises pour définir une configuration valide. Tous les éléments doivent être configurés. Le contrôleur de sécurité n'accepte pas les configurations incorrectes.

Remarque: Le nœud de sortie de n'importe quel élément peut être connecté à plusieurs nœuds d'entrée. Un nœud d'entrée ne peut avoir qu'un seul élément qui lui est connecté.

Astuce: Pour vous permettre de créer une configuration valide, le programme affiche des infobulles utiles chaque fois que vous définissez une connexion non valide.

8.4 Enregistrement et confirmation d'une configuration

La confirmation est un processus de vérification au cours duquel le contrôleur de sécurité analyse l'exhaustivité et l'intégrité logique de la configuration générée par le logiciel. L'utilisateur doit examiner et approuver les résultats avant qu'il soit possible d'enregistrer la configuration et que le contrôleur de sécurité puisse l'utiliser. Une fois confirmée, la configuration peut être envoyée à un contrôleur de sécurité ou enregistrée sur un PC ou une carte mémoire SC-XM2/3.

AVERTISSEMENT:
- **Effectuez la procédure de vérification à la mise en route.**
- Si vous ne procédez pas à une vérification à la mise en route, des dommages corporels graves ou mortels sont possibles.
- Après confirmation de la configuration, le fonctionnement du contrôleur de sécurité doit être soumis à des tests approfondis (vérification de mise en service) avant de pouvoir l'utiliser pour surveiller les risques.

8.4.1 Enregistrement d'une configuration

1. Cliquez sur **Enregistrer le projet**.
2. Sélectionnez **Enregistrer sous**.
3. Accédez au dossier dans lequel vous souhaitez enregistrer la configuration.
4. Attribuez un nom au fichier (il peut être identique ou différent du nom de la configuration).
5. Cliquez sur **Save (Enregistrer)**.

Remarque: Si la configuration n'a pas été confirmée, ce processus enregistre la configuration en tant que configuration non confirmée (fichier *.xsc).

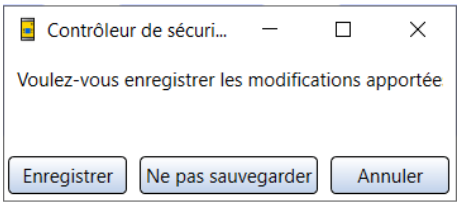
8.4.2 Confirmation d'une configuration

Le contrôleur de sécurité doit être mis sous tension et connecté au PC via le câble SC-USB2 ou via une connexion Ethernet (uniquement pour les modèles compatibles Ethernet XS/SC26 FID 7 ou ultérieur). Reportez-vous à la section Connexion à un contrôleur de sécurité via Ethernet à la page 108 pour établir des connexions entre le logiciel et un contrôleur de sécurité via une connexion réseau. Avant d'écrire la configuration sur un contrôleur d'un réseau EtherCAT actif, lisez la seconde remarque de la section EtherCAT et les contrôleurs de sécurité à la page 299.

1. Cliquez sur .
2. Cliquez sur **Écrire la configuration sur le contrôleur**.

Si la configuration n'a pas été enregistrée, le logiciel vous demandera si vous souhaitez enregistrer le projet (configuration). Cela permet d'enregistrer la configuration non confirmée. Si vous choisissez **Enregistrer**, le fichier est enregistré sous le nom actuel. Si vous choisissez **Ne pas enregistrer**, le processus d'écriture se poursuit.

Illustration 63. « Voulez-vous enregistrer ? » Message :



Si la configuration envoyée au contrôleur contient un ou plusieurs élément(s) qui ne sont pas pris en charge par le contrôleur connecté (par exemple, modules d'extension, entrées virtuelles, entrées ISD, etc.), le message suivant s'affiche :

Illustration 64. Avertissement concernant un contrôleur incompatible



Ce message est un rappel que la configuration peut être chargée dans le contrôleur connecté, mais qu'elle ne fonctionnera pas (le contrôleur se verrouillera). Le chargement de la configuration est autorisé car, pendant ce processus, la configuration peut également être confirmée. Elle ne fonctionnera pas sur ce contrôleur, mais cette configuration désormais confirmée peut être chargée sur une carte SC-XM2/3 ou envoyée par e-mail à un site distant, puis chargée sur un contrôleur compatible. Si la configuration est déjà confirmée, il est toujours possible de la charger sur le contrôleur connecté. Toutefois, une fois la configuration chargée, le contrôleur se verrouillera car la configuration contient des fonctionnalités non prises en charge.

3. Si vous y êtes invité, entrez les données suivantes :
   - Code PIN si vous utilisez une connexion USB (le code PIN par défaut est 1901)
   - Mot de passe si vous utilisez une connexion Ethernet (modèles XS/SC26 FID 7 ou ultérieur compatibles Ethernet uniquement)

   L'écran **Entrée dans le mode de configuration** s'affiche.
4. Cliquez sur **Continuer** pour basculer en mode de configuration.
   Une fois le processus **Lecture de la configuration sur le contrôleur** terminé, l'écran **Confirmer la configuration** s'affiche.
5. Vérifiez que la configuration est correcte.
6. **Faites défiler la configuration jusqu'à la fin et cliquez sur Confirmer.**
7. Une fois le processus **Écriture de la configuration sur le contrôleur** terminé, cliquez sur **Fermer**.

Remarque:
- Les paramètres réseau et les paramètres de configuration sont envoyés séparément. Cliquez sur **Envoyer** dans la fenêtre **Paramètres réseau** pour écrire les paramètres réseau sur le contrôleur de sécurité.
- SC10-2 et XS/SC26 FID 3 ou ultérieur : les paramètres réseau sont automatiquement envoyés uniquement si le contrôleur de sécurité est un contrôleur de sécurité avec une configuration d'usine. Sinon, vous devez utiliser la fenêtre **Paramètres réseau**.
- SC10-2 et XS/SC26 FID 3 ou ultérieur : les codes PIN/mots de passe sont automatiquement écrits uniquement s'il s'agit d'un contrôleur de sécurité avec une configuration d'usine ou si la configuration est confirmée. Dans tous les autres cas, utilisez la fenêtre **Gestionnaire de mots de passe** pour écrire les codes PIN/mots de passe sur le contrôleur de sécurité.

Si vous configurez un SC10-2 ou XS/SC26 FID 3 ou ultérieur, il est possible que l'écran **Souhaitez-vous modifier les mots de passe du contrôleur ?** s'affiche.

8. SC10-2 et XS/SC26 FID 3 ou ultérieur : si vous y êtes invité et que vous le souhaitez, changez les codes PIN/mots de passe.

   XS/SC26 FID 7 ou ultérieur compatibles Ethernet exigent que le mot de passe par défaut soit modifié si l'utilisateur souhaite accéder au contrôleur via une connexion Ethernet. Référez-vous à la section Gestionnaire des mots de passe du XS/SC26 à la page 135 pour plus d'informations.

9. Pour que les modifications soient appliquées dans le contrôleur de sécurité, coupez puis rétablissez l'alimentation, réinitialisez le système ou, si vous chargez la configuration via une connexion Ethernet, sélectionnez **Redémarrer** dans la fenêtre **Redémarrage du système**.
10. Enregistrez la configuration confirmée sur le PC.

Remarque: Il est recommandé d'enregistrer la configuration désormais confirmée. Les configurations confirmées ont un format de fichier différent (.xcc) d'un fichier non confirmé (.xsc). Il est indispensable que les configurations aient été confirmées pour les enregistrer sur une carte mémoire SC-XM2/3. Cliquez sur **Enregistrer** pour enregistrer la configuration.

8.4.3 Écrivez une configuration confirmée sur la carte SC-XM2/3 avec l'outil de programmation.

1. Insérez la carte SC-XM2/3 dans l'outil de programmation SC-XMP2.
2. Lorsque le logiciel Contrôleur de sécurité Banner est en cours d'exécution, insérez l'outil de programmation dans un port USB du PC.
   L'icône SC-XM2/3 devrait être activée (plus sombre que grisée).
3. Cliquez sur et sélectionnez **Écrire sur la carte mémoire XM**.

Remarque: Si l'option **Écrire sur la carte mémoire XM** est grisée, la configuration n'est pas un fichier .xcc (version confirmée).

4. Vérifiez les codes PIN souhaités.
5. Cliquez sur **Envoyer vers XM**.
   La fenêtre **Écriture de la configuration sur la carte mémoire SC-XM** s'ouvre.

Remarque: Ce processus copie toutes les données (configuration, paramètres réseau et codes PIN/mots de passe) sur la carte mémoire SC-XM2/3.

6. Après avoir terminé, cliquez sur **Enregistrer la configuration confirmée** et ensuite sur **Fermer**, ou cliquez sur **Fermer** si le fichier a déjà été enregistré sur le PC.

8.4.4 Remarques sur la confirmation ou l'écriture d'une configuration sur un contrôleur SC10-2 ou XS/SC26 configuré FID 3 ou ultérieur

Les paramètres et codes PIN/mots de passe utilisateur déterminent la réponse du système lors de la confirmation d'une configuration ou de l'écriture d'une configuration confirmée sur un contrôleur de sécurité SC10-2 ou XS/SC26 FID 3 ou ultérieur configuré.

Utilisateur1

1. Cliquez sur **Écrire la configuration sur le contrôleur** pour confirmer la configuration (ou écrire une configuration confirmée) sur un contrôleur de sécurité configuré.
2. Entrez le code PIN ou le mot de passe Utilisateur1.
   - Code PIN si vous utilisez une connexion USB
   - Mot de passe si vous utilisez une connexion Ethernet (modèles XS/SC26 FID 7 ou ultérieur compatibles Ethernet uniquement)
3. Le processus de confirmation (ou d'écriture) démarre.

Au terme de la confirmation (ou écriture), le contrôleur de sécurité aura reçu ce qui suit :
- Nouveaux mots de passe et codes PIN
- Nouvelle configuration

Les paramètres réseau restent inchangés.

Utilisateur2 ou Utilisateur3—Confirmation ou écriture de la configuration réussie

Ce scénario suppose les paramètres suivants pour Utilisateur2 ou Utilisateur3 :
- **Autorisé à modifier la configuration** = activé
- **Autorisé à modifier les paramètres réseau** = activé OU désactivé

1. Cliquez sur **Écrire la configuration sur le contrôleur** pour confirmer la configuration (ou écrire une configuration confirmée) sur un contrôleur de sécurité configuré.
2. Entrez le code PIN ou le mot de passe Utilisateur2 ou Utilisateur3.
   - Code PIN si vous utilisez une connexion USB
   - Mot de passe si vous utilisez une connexion Ethernet (modèles XS/SC26 FID 7 ou ultérieur compatibles Ethernet uniquement)

3. Le processus de confirmation (ou d'écriture) démarre.

Au terme de la confirmation (ou écriture), le contrôleur de sécurité aura reçu ce qui suit :

- Nouvelle configuration

Les codes PIN/mots de passe et les paramètres réseau ne sont pas modifiés.

Utilisateur2 ou Utilisateur3 — Échec de la confirmation ou écriture de la configuration

Ce scénario suppose les paramètres suivants pour Utilisateur2 ou Utilisateur3 :

- **Autorisé à modifier la configuration** = désactivé
- **Autorisé à modifier les paramètres réseau** = activé OU désactivé

1. Cliquez sur **Écrire la configuration sur le contrôleur** pour confirmer la configuration (ou écrire une configuration confirmée) sur un contrôleur de sécurité configuré.
2. Entrez le code PIN ou le mot de passe Utilisateur2 ou Utilisateur3.
    - Code PIN si vous utilisez une connexion USB
    - Mot de passe si vous utilisez une connexion Ethernet (modèles XS/SC26 FID 7 ou ultérieur compatibles Ethernet uniquement)
3. Le processus de confirmation (ou d'écriture) est annulé.

8.5 Exemples de configuration

Le logiciel propose plusieurs exemples de configuration illustrant les différentes fonctions ou applications du Contrôleur de sécurité. Pour accéder à ces configurations, allez à **Open Project (Ouvrir un projet)** > **Sample Projects (Exemples de projet)** et sélectionnez le projet voulu.

Le XS/SC26 propose trois catégories d'exemples de configuration :

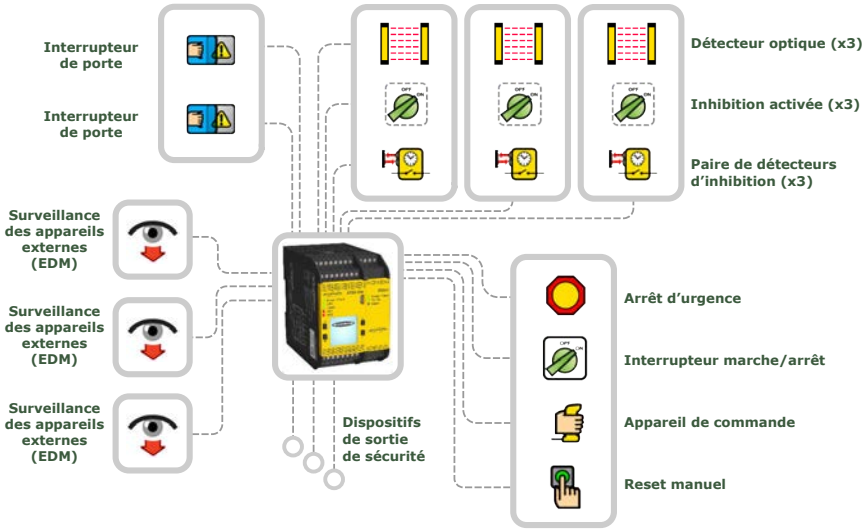
- **Applications** — Inclut des exemples possibles d'application simple du contrôleur. Deux d'entre eux sont des remplacements de modules obsolètes.
- **Documentation** — Comprend divers exemples. La plupart des exemples inclus ici sont décrits dans les sections suivantes, et l'un d'entre eux est décrit dans le guide de démarrage rapide (disponible en ligne).
- **Exemples** — Est subdivisé comme suit : **Blocs fonction**, **Blocs logiques** et **Sorties de sécurité**. Ces exemples illustrent les fonctionnalités des différents blocs. Par exemple, pour savoir comment un bloc de dérivation fonctionne, sélectionnez **Blocs fonction** > **Bloc de dérivation (Toutes fonctionnalités activées)** et exécutez-le en mode simulation.

Le SC10-2 possède plusieurs exemples de configuration. Il s'agit d'applications courantes du modèle SC10-2. Utilisez ces exemples comme point de départ et modifiez-les selon vos besoins.

8.5.1 Exemple de configuration du XS/SC26

Cette section décrit la conception de l'exemple de configuration « Manuel d'instructions d'une inhibition dans 3 zones », figurant dans la section **Documentation** des exemples de programme du XS/SC26. Cet exemple de configuration est destiné à une application de palettiseur robotisé qui utilise un contrôleur de sécurité XS26, un module d'entrée de sécurité XS8si, trois capteurs optiques (l'inhibition est ajoutée via le logiciel), deux interrupteurs de verrouillage, un reset manuel et un bouton d'arrêt d'urgence.

Illustration 65. Schéma de l'exemple de configuration



Pour concevoir la configuration de cette application :

1. Cliquez sur **Nouveau projet**.

2. Définissez les paramètres du projet. Référez-vous à la section Paramètres du projet à la page 115.
3. Sélectionnez le modèle de contrôleur de base. Référez-vous à la section Onglet Équipement à la page 116 (pour cette configuration, seule la case à cocher **Est extensible** doit être activée).
4. Ajoutez le module d'extension **XS8si** en cliquant sur ✚ à droite du module du contrôleur de base.
    a. Cliquez sur **Modules d'entrée**.
    b. Sélectionnez **XS8si**.
5. Ajoutez les entrées suivantes, en ne changeant que le type de circuit :

Entrée	Quantité	Type	Module	Bornes	Circuit
Arrêt d'urgence	1	Entrée de sécurité	XS8si	IO1, IN1, IN2	Double voie, 3 bornes
Dispositif de commande	1	Entrée de sécurité	XS8si	IO1, IN3, IN4	Double voie, 3 bornes
Surveillance des commutateurs externes (EDM)	3	Entrée de sécurité	Base	1. IO3 2. IO4 3. IO5	Simple voie, 1 borne
Interrupteur de porte	2	Entrée de sécurité	Base	1. IO1, IN15, IN16 2. IO2, IN17, IN18	Double voie, 3 bornes
Reset manuel	1	Entrée auxiliaire	XS8si	IN6	Simple voie, 1 borne
Paire de capteurs d'inhibition	3	Entrée de sécurité	Base	1. IN9, IN10 2. IN11, IN12 3. IN13, IN14	Double voie, 2 bornes
Inhibition activée	3	Entrée auxiliaire	Base	1. IN1 2. IN2 3. IO8	Simple voie, 1 borne
Marche-Arrêt	1	Entrée auxiliaire	XS8si	IN5	Simple voie, 1 borne
Capteur optique	3	Entrée de sécurité	Base	1. IN3, IN4 2. IN5, IN6 3. IN7, IN8	PNP double voie

6. Accédez à l'onglet **Vue fonctionnelle**.



Astuce: Comme vous pouvez le constater, toutes les entrées ne sont pas placées dans la page 1. Pour conserver la configuration sur une seule page, deux solutions sont possibles. Procédez de l'une des manières suivantes :

1. Ajoutez une **référence** au bloc situé dans une page différente. Cliquez sur l'un des emplacements réservés dans la section du milieu, sélectionnez **Référence** puis sélectionnez le bloc situé sur la page suivante. Seuls les blocs d'autres pages peuvent être ajoutés comme **référence.**
2. Réaffectez la page. Par défaut, toutes les entrées ajoutées dans l'onglet **Équipement** sont placées dans l'onglet **Vue fonctionnelle** au niveau du premier emplacement réservé dans la colonne de gauche. Toutefois, il est possible de déplacer les entrées vers n'importe quel emplacement de la colonne du milieu. Déplacez un des blocs vers un des emplacements réservés de la colonne du milieu. Accédez à la page contenant le bloc à déplacer. Sélectionnez le bloc et modifiez l'affectation de page sous le tableau **Propriétés**.

7. Divisez **M0:SO2** :
    a. Double-cliquez sur **M0:SO2** ou sélectionnez-la et cliquez sur **Modifier** sous le tableau **Propriétés**.
    b. Cliquez sur **Diviser.**
8. Ajoutez les **blocs fonction** suivants en cliquant sur l'un des emplacements réservés vides de la colonne du milieu dans l'onglet **Vue fonctionnelle** (voir la section Blocs fonction à la page 121 pour plus d'informations) :
    - **Bloc d'inhibition** x **3** (**mode d'inhibition** : une paire, **inhibition activée (ME)** : coché)
    - **Bloc appareil de commande** (**ES**: coché, **APPROCHE (Approche)**: coché)
9. Ajoutez les **blocs logiques** suivants en cliquant sur l'un des emplacements réservés vides de la colonne du milieu dans l'onglet **Vue fonctionnelle** (voir la section Blocs logiques à la page 118 pour plus d'informations) :
    - **AND** avec 2 nœuds d'entrée
    - **AND** avec 4 nœuds d'entrée
10. Connectez les éléments suivants à chaque **bloc d'inhibition** :
    - 1 **Capteur optique** (nœud **IN**)
    - 1 **Paire de capteurs d'inhibition** (nœud **MP1**)

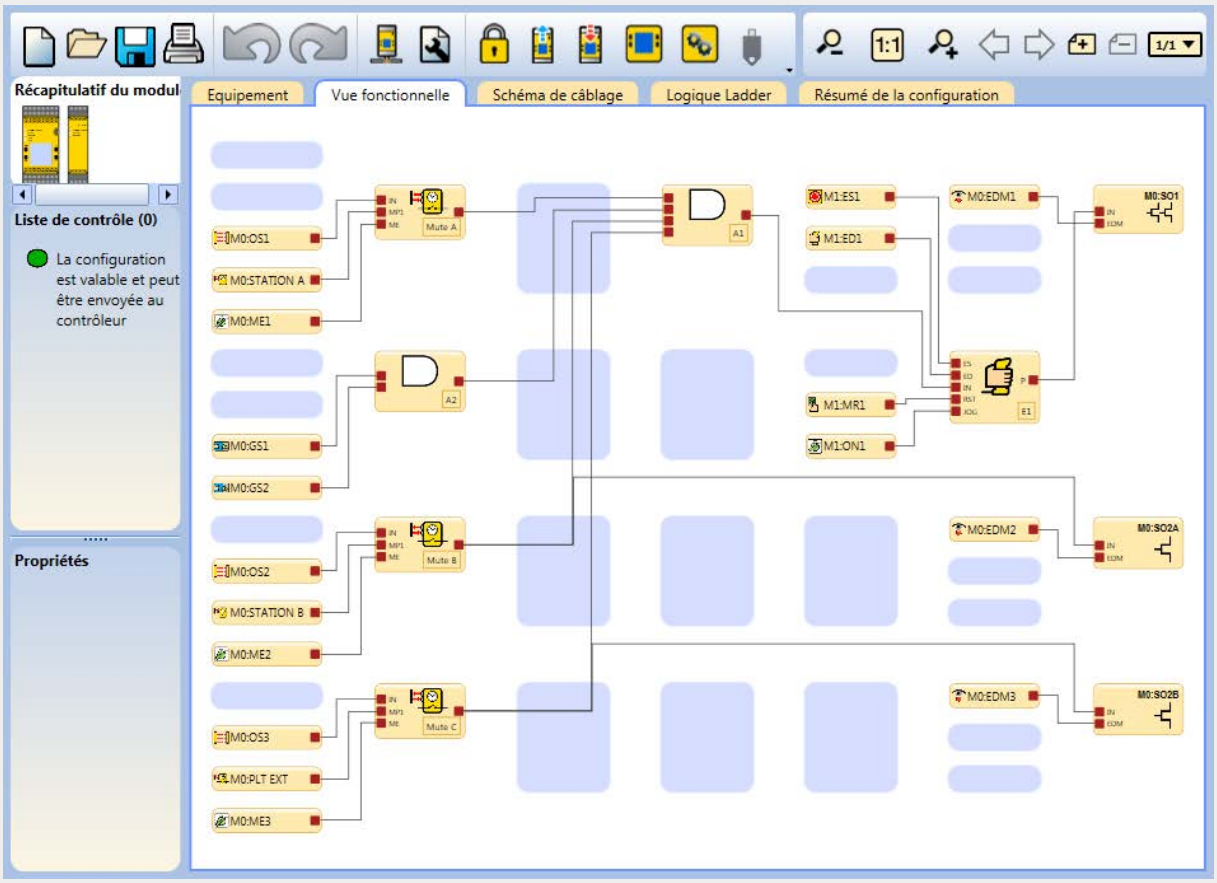
- 1 **Inhibition activée** (nœud **ME**)

11. Connectez les 2 **interrupteurs de porte** au bloc **AND (ET)** à 2 nœuds.
12. Connectez les 3 **blocs d'inhibition** et le bloc **AND (ET)** à 2 nœuds au bloc **AND** à 4 nœuds.
13. Connectez un des **blocs d'inhibition** à une des sorties de sécurité scindées (**M0:SO2A** ou **M0:SO2B**) et un à l'autre sortie de sécurité scindée.
14. Connectez les éléments suivants au **bloc appareil de commande** :
    - **Interrupteur d'arrêt d'urgence** (nœud **ES**)
    - **Appareil de commande** (nœud **ED**)
    - Bloc **AND** (ET) à 4 nœuds d'entrée (nœud **IN**)
    - **Reset manuel** (nœud **RST**)
    - **Marche-Arrêt** (nœud **APPROCHE**)
15. Connectez le **bloc appareil de commande** à la sortie de sécurité restante (**M0:SO1**).
16. Activez *EDM (surveillance des commutateurs externes)* dans chaque fenêtre **Propriétés** des sorties de sécurité.
17. Connectez 1 entrée **EDM** à chaque sortie de sécurité.

L'exemple de configuration est terminé.

Remarque: A ce stade, vous pouvez éventuellement repositionner les blocs dans l'onglet **Vue fonctionnelle** afin d'avoir une configuration plus fluide, comme illustré dans la figure suivante :

*Illustration 66. Exemple de configuration — Onglet **Vue fonctionnelle***

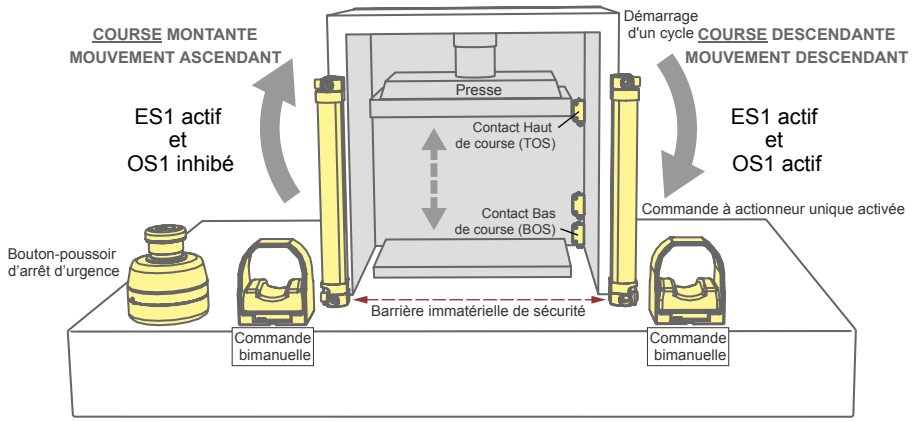


8.5.2 XS/SC26 : Exemple de configuration d'une commande de presse simple avec arrêt d'urgence inhibable

Cette section décrit la conception d'un système de commande de presse simple, figurant dans la section Documentation des exemples de programme du XS/SC26.

Cet exemple de configuration est destiné à une application de presse hydraulique/pneumatique simple qui utilise un contrôleur de sécurité XS26, des entrées d'état de la presse, un démarrage de cycle, un reset manuel, un capteur de sécurité optique et un arrêt d'urgence.

Illustration 67. Exemple de configuration simple de la commande de presse



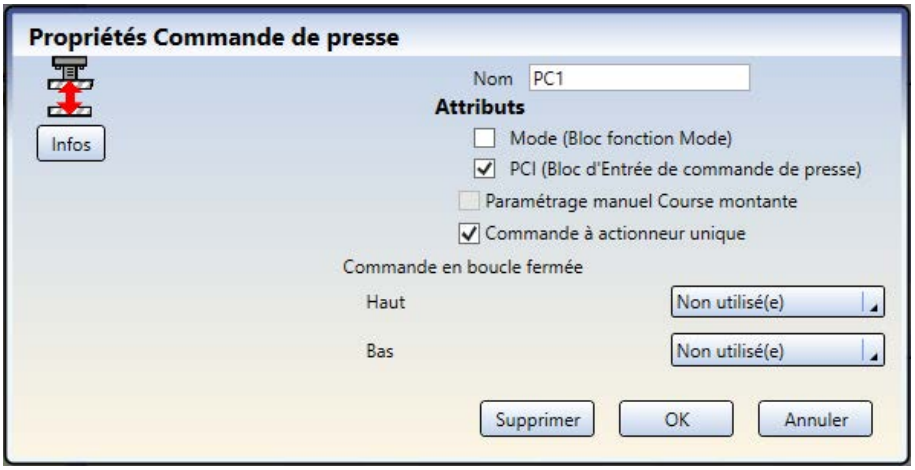
Pour concevoir la configuration de cette application :

1. Cliquez sur **Nouveau projet**.
2. Définissez les paramètres du projet.
   Référez-vous à la section Paramètres du projet à la page 115.
3. Sélectionnez le modèle de contrôleur de base voulu.
   Référez-vous à la section Onglet Équipement à la page 116.
4. Ajoutez les entrées suivantes, en changeant le nom et le type de circuit selon les besoins.

Entrée	Quantité	Type	Bornes	Circuit
Démarrage d'un cycle	1	Entrée de sécurité	IN1, IN2	Double voie, 2 bornes
TOS (on/off)	1	Auxiliaire	IN5	Simple voie, 1 borne
BOS (on/off)	1	Auxiliaire	IN6	Simple voie, 1 borne
Reset manuel	1	Auxiliaire	IN7	Simple voie, 1 borne
Arrêt d'urgence	1	Entrée de sécurité	IN10, IN11	Double voie, 2 bornes
Capteur optique	1	Entrée de sécurité	IN8, IN9	PNP double voie

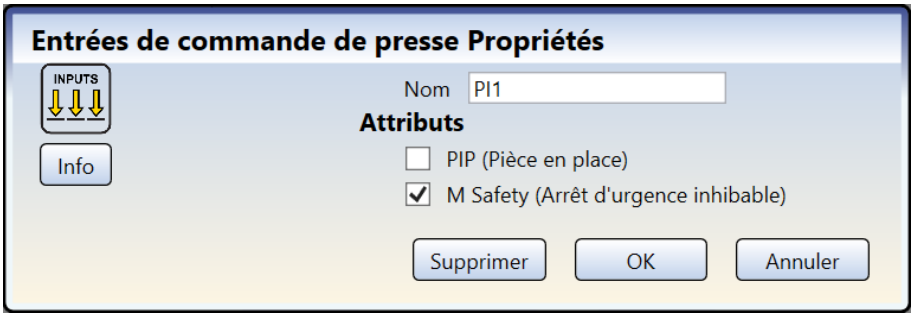
5. Accédez à l'onglet **Vue fonctionnelle**.
6. Ajoutez et configurez le bloc fonction Commande de presse.
   a) Cliquez sur l'un des emplacements réservés vides dans la partie centrale de l'onglet **Vue fonctionnelle**. Pour plus d'informations, voir Blocs fonction à la page 121.
   b) Sélectionnez **Blocs fonction** puis **Commande de presse**.
   c) Dans la fenêtre **Propriétés de commande de presse**, sélectionnez **PCI (Bloc fonction Entrées de commande de presse)** et **Commande à actionneur unique**.

*Illustration 68. **Propriétés de commande de presse***



   La coche dans la case **Paramétrage manuel Course montante** disparaît.
   d) Cliquez sur **OK**.
   La fenêtre **Propriétés des entrées de commande de presse** s'ouvre.

Illustration 69. ***Propriétés des entrées de commande de presse***



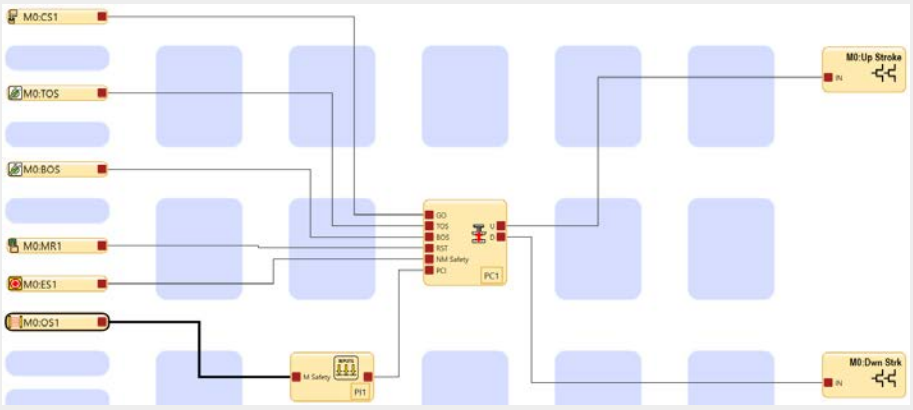
e) Sélectionnez **M Safety (Mutable Safety Stop)** (Arrêt d'urgence inhibable).
f) Cliquez sur **OK**.

7. Connectez les éléments suivants :
   - Entrée Démarrage d'un cycle au nœud GO du bloc fonction Commande de presse
   - TOS au nœud TOS du bloc fonction Commande de presse
   - BOS au nœud BOS du bloc fonction Commande de presse
   - Reset manuel au nœud RST du bloc fonction Commande de presse
   - Arrêt d'urgence au nœud NM Safety (Arrêt d'urgence non inhibable) du bloc fonction Commande de presse
   - Capteur optique au nœud M Safety (Arrêt d'urgence inhibable) du bloc fonction Entrées de commande de presse
8. Connectez le nœud de sortie U du bloc fonction Commande de presse à SO1 (remplacez le nom SO1 par Up Stroke).
9. Connectez le nœud de sortie D du bloc fonction Commande de presse à SO2 (remplacez le nom SO2 par Dwn Strk).

L'exemple de configuration est terminé.

Remarque: À ce stade, il peut être utile de repositionner les blocs dans la Vue fonctionnelle pour mieux organiser la configuration, comme illustré dans la figure suivante :

Illustration 70. ***Position des blocs fonction***



XS/SC26 : Simulation des fonctionnalités d'une configuration simple de commande de presse

La procédure suivante permet de simuler les fonctionnalités de cette configuration simple de commande de presse :

1. Cliquez sur  pour basculer en mode simulation.
2. Cliquez sur « **Play** » pour activer la minuterie de simulation (similaire à la mise en marche de la machine).
3. Cliquez sur les entrées Arrêt d'urgence, Capteur optique et TOS pour les activer (On, vert).
4. Cliquez sur l'entrée de reset MR1.
   Le bloc fonction Commande de presse doit s'activer (On, vert).
5. Cliquez sur l'entrée CS1 pour l'activer (On, vert).
   La sortie Dwn Strk (Course desc.) est activée (On, vert).
6. Cliquez sur l'entrée TOS pour la désactiver (Off, rouge).
7. Cliquez sur l'entrée BOS pour l'activer (On, vert).
   La sortie Dwn Strk est désactivée (Off, rouge) et la sortie Up Stroke (Course mont.) est activée (On, vert).
8. Cliquez sur l'entrée BOS pour la désactiver (Off, rouge).

9. Cliquez sur l'entrée TOS pour l'activer (On, vert).
   La sortie Up Stroke est désactivée (Off, rouge).
10. Cliquez sur l'entrée CS1 pour la désactiver (Off, rouge). Cette désactivation est possible dès que la sortie Dwn Strk a été activée (On, vert).
11. Cliquez sur l'entrée Capteur optique pour la désactiver (Off, rouge), puis réactivez-la (On, vert).

Le système est prêt à démarrer le cycle suivant en réactivant l'entrée CS1 (On, vert).

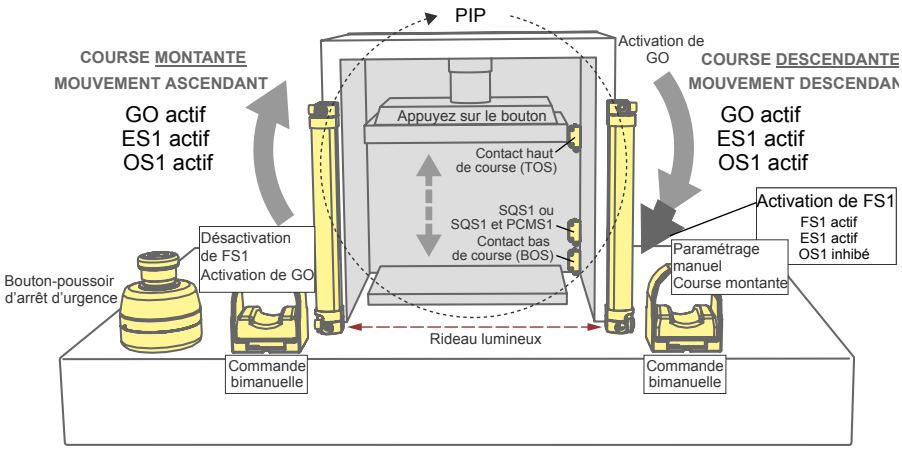
Si le capteur optique ou l'arrêt d'urgence est désactivé pendant la course montante ou descendante, l'entrée MR1 doit être désactivée puis réactivée. L'activation de CS1 activera à son tour la sortie Up Stroke.

8.5.3 XS/SC26 : Exemple de configuration d'une commande de presse avec fonctionnalités complètes

Cette section décrit la conception d'un système de commande de presse qui utilise toutes les fonctionnalités possibles (sauf l'AVM). L'exemple de configuration se trouve dans la section Documentation des exemples de programme du XS/SC26.

Cet exemple de configuration est destiné à une application de presse hydraulique/pneumatique plus complexe qui utilise un contrôleur de sécurité XS26, un module de sortie de sécurité XS2so, des entrées d'état de la presse, un démarrage de cycle, un reset manuel, un capteur de sécurité optique, un arrêt séquentiel, un capteur d'inhibition, une entrée de pédale et un bouton d'arrêt d'urgence.

Illustration 71. Configuration d'une commande de presse avec fonctionnalités complètes



Pour concevoir la configuration de cette application :

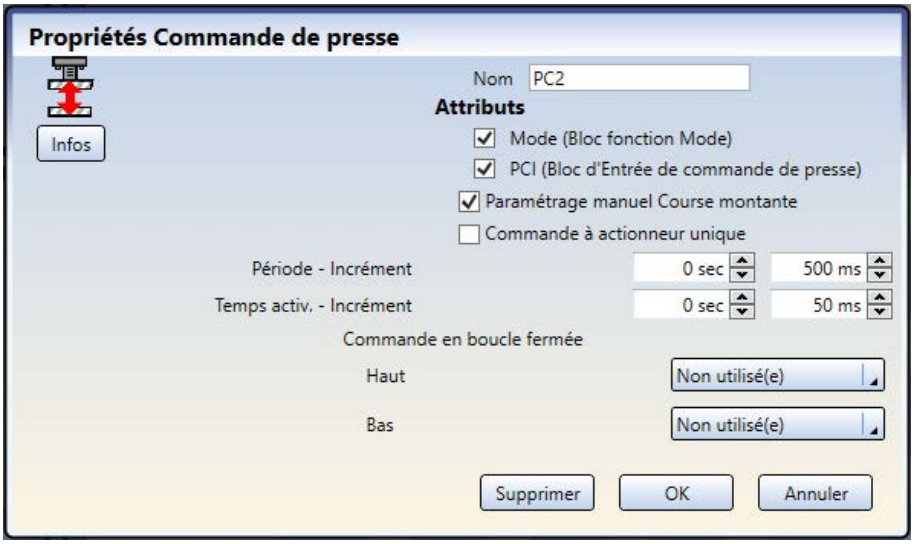
1. Cliquez sur **Nouveau projet**.
2. Définissez les paramètres du projet.
   Référez-vous à la section Paramètres du projet à la page 115.
3. Sélectionnez le modèle de contrôleur de base voulu.
   Référez-vous à la section Onglet Équipement à la page 116 (pour cette configuration, seule la case à cocher **Est extensible** doit être sélectionnée).
4. Ajoutez le module d'extension XS2so.
   a) Cliquez sur ✚ à droite du contrôleur de base.
   b) Cliquez sur **Modules de sortie**.
   c) Sélectionnez XS2so.
5. Ajoutez les entrées suivantes, en changeant le nom et le type de circuit selon les besoins.

Entrée	Quantité	Type	Bornes	Circuit
Commande bimanuelle	1	Entrée de sécurité	IN9, IN10	PNP double voie
TOS (ON/OFF)	1	Auxiliaire	IN1	Simple voie, 1 borne
BOS (ON/OFF)	1	Auxiliaire	IN2	Simple voie, 1 borne
Reset manuel	1	Auxiliaire	IN11	Simple voie, 1 borne
Arrêt d'urgence	1	Entrée de sécurité	IO1, IN3, IN4	Double voie, 3 bornes
Run (ON/OFF)	1	Auxiliaire	IN12	Simple voie, 1 borne

Entrée	Quantité	Type	Bornes	Circuit
Montée (ON/OFF)	1	Auxiliaire	IN13	Simple voie, 1 borne
Descente (ON/OFF)	1	Auxiliaire	IN14	Simple voie, 1 borne
PIP (ON/OFF)	1	Auxiliaire	IN5	Simple voie, 1 borne
Arrêt séquentiel (SQS) de la commande de presse	1	Entrée de sécurité	IN6	Simple voie, 1 borne
Interrupteur au pied	1	Entrée de sécurité	IO2	Simple voie, 1 borne
Capteur d'inhibition de la commande de presse	1	Entrée de sécurité	IO3	Simple voie, 1 borne
Capteur optique	1	Entrée de sécurité	IN7, IN8	PNP double voie

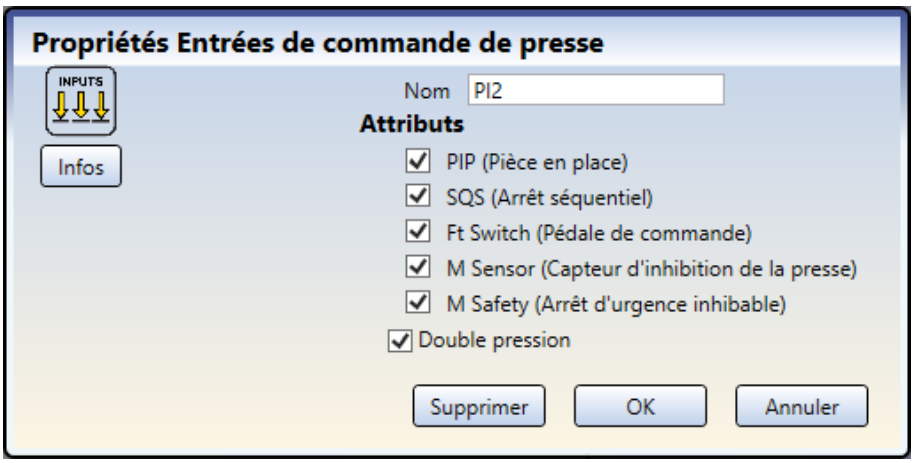
6. Accédez à l'onglet **Vue fonctionnelle**.
7. Ajoutez et configurez le bloc fonction Commande de presse.
   a) Cliquez sur l'un des emplacements réservés vides dans la partie centrale de l'onglet **Vue fonctionnelle**. Pour plus d'informations, voir Blocs fonction à la page 121.
   b) Sélectionnez **Blocs fonction** puis **Commande de presse**.
   c) Dans la fenêtre **Propriétés de commande de presse**, sélectionnez **Mode (Bloc fonction Mode)** et **PCI (Bloc fonction Entrées de commande de presse**). Laissez la case **Paramétrage manuel Course montante** cochée.

*Illustration 72. **Propriétés de commande de presse***



   d) Cliquez sur **OK**.
   La fenêtre **Propriétés des entrées de commande de presse** s'ouvre.

*Illustration 73. **Propriétés des entrées de commande de presse***



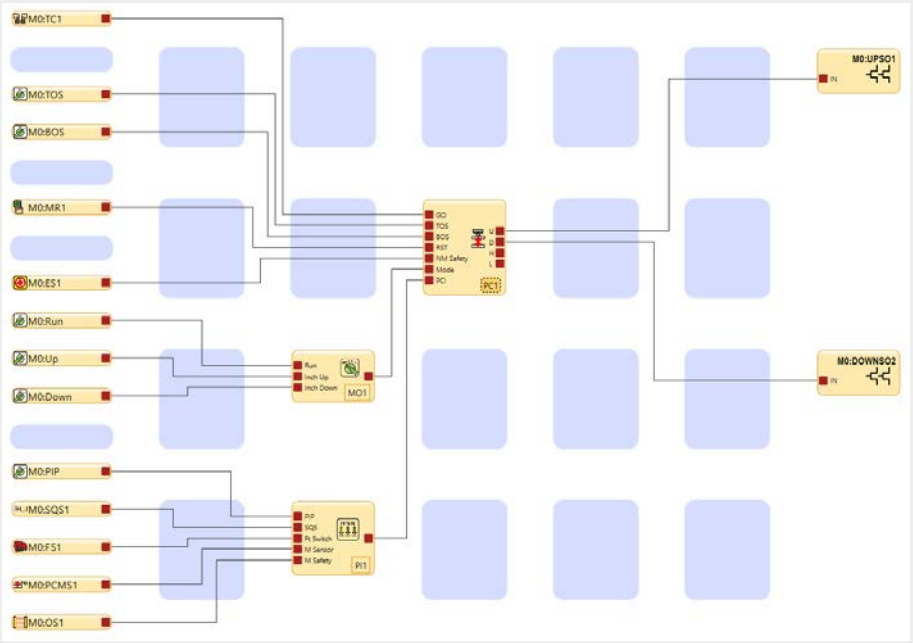
e) Cochez toutes les cases. Notez que lorsque **SQS** est sélectionné, trois autres options s'affichent ; sélectionnez-les également (les six cases doivent être cochées).
f) Cliquez sur **OK**.
La fenêtre **Propriétés du mode** s'affiche.
g) Cliquez sur **OK**.

8. Connectez les éléments suivants au bloc Sélection de mode :
   - Entrée Run au nœud d'entrée Run Input
   - Entrée Up au nœud d'entrée Inch Up
   - Entrée Down au nœud d'entrée Inch Up
9. Connectez les éléments suivants au bloc Entrées de commande de presse :
   - Entrée PIP (Part-In-Place) au nœud d'entrée PIP
   - Entrée SQS (arrêt séquentiel) au nœud d'entrée SQS
   - Entrée de l'interrupteur au pied au nœud d'entrée de l'interrupteur au pied
   - PCMS (Capteur d'inhibition de commande de presse) au nœud d'entrée M Sensor (Arrêt d'urgence inhibable)
   - Capteur optique au nœud d'entrée de sécurité M Safety (Arrêt d'urgence inhibable)
10. Connectez les éléments suivants au bloc Commande de presse :
    - Entrée Commande bimanuelle au nœud d'entrée GO
    - TOS au nœud d'entrée TOS
    - BOS au nœud d'entrée BOS
    - Reset manuel au nœud d'entrée RST
    - Arrêt d'urgence au nœud d'entrée NM Safety (Arrêt d'urgence non inhibable)
11. Connectez le nœud de sortie U du bloc fonction Commande de presse à SO1 (remplacez le nom SO1 par UPSO1).
12. Connectez le nœud de sortie D du bloc fonction Commande de presse à SO2 (remplacez le nom SO2 par DOWNSO2).
13. Allez à la page 2 de l'onglet Vue fonctionnelle (utilisez la flèche dans le coin supérieur droit).
14. Créez un nœud de référence pour PCx-H et un autre pour PCx-L.
15. Connectez PCx-H à SO1 (remplacez le nom SO1 par HIGHSO1).
16. Connectez PCx-L à SO2 (remplacez le nom SO2 par LOWSO2).

L'exemple de configuration est terminé.

Remarque: À ce stade, il peut être utile de repositionner les blocs dans la **Vue fonctionnelle** pour mieux organiser la configuration, comme illustré dans la figure suivante.

Illustration 74. ***Position des blocs fonction***



XS/SC26 : Simulation des fonctionnalités de la configuration complète de la commande de la presse

La procédure suivante permet de simuler les fonctionnalités de cette configuration de commande de presse :

1. Cliquez sur  pour basculer en mode simulation.

2. Cliquez sur « **Play** » pour activer la minuterie de simulation (similaire à la mise en marche de la machine).
3. Cliquez sur les entrées Arrêt d'urgence, Capteur optique, TOS et Run pour les activer (On, vert).
4. Cliquez sur l'entrée de reset MR1.
   Le bloc fonction Commande de presse et la sortie LOWSO2 doivent s'activer (On, vert). Vous êtes à la page 2 ; cliquez sur la flèche dans le coin supérieur droit pour changer de page.
5. Cliquez sur l'entrée PIP pour l'activer (On, vert).
6. Cliquez sur l'entrée TC1 pour l'activer (On, vert).
   La sortie DOWNSO2 est activée (On, vert).
7. Cliquez sur l'entrée TOS pour la désactiver (Off, rouge).
8. Cliquez sur les entrées SQS1 et PCMS1 pour les activer (On, vert).
   La sortie DOWNSO2 est désactivée (rouge), la sortie LOWSO2 est désactivée (rouge) et la sortie HIGHSO1 (page 2) est activée (vert).
9. Cliquez sur l'entrée TC1 pour la désactiver (Off, rouge).
10. Cliquez sur l'entrée FS1 pour l'activer (vert).
    La sortie DOWNSO2 est activée (On, vert).
11. Cliquez sur l'entrée BOS pour l'activer (On, vert).
    Les sorties DOWNSO2 et HIGHSO1 (page 2) sont désactivées (rouge) et la sortie LOWSO2 (page 2) est activée (vert).
12. Cliquez sur l'entrée FS1 pour la désactiver (rouge).
13. Cliquez sur l'entrée TC1 pour l'activer (On, vert).
    La sortie UPSO1 est activée (On, vert).
14. Cliquez sur les entrées BOS, PCMS1 et SQS1 pour les désactiver (Off, rouge).
15. Cliquez sur l'entrée TOS pour l'activer (On, vert).
    La sortie UPSO1 est désactivée (Off, rouge).
16. Cliquez sur l'entrée TC1 pour la désactiver (Off, rouge).
17. Cliquez sur l'entrée Capteur optique pour la désactiver (Off, rouge), cliquez sur l'entrée PIP pour la désactiver (Off, rouge) puis réactivez-la (On, vert), ensuite cliquez sur l'entrée Capteur optique pour la réactiver (On, vert).

Le système est prêt à démarrer le cycle suivant en réactivant l'entrée TC1 (On, vert).

Si l'entrée TC1 est désactivée (Off, rouge) pendant la course descendante, sa réactivation ne modifie pas cette course descendante ; la presse poursuit sa course descendante. Pour faire remonter la presse (au lieu de l'abaisser) après avoir désactivé l'entrée TC1, cliquez sur l'entrée MR1, puis réactivez l'entrée TC1. Si le capteur optique ou l'arrêt d'urgence sont désactivés pendant la course montante ou descendante, l'entrée TC1 doit être désactivée, l'entrée MR1 doit être désactivée puis réactivée. L'activation de TC1 activera à son tour la sortie UPSO1.

9 Connexion au contrôleur de sécurité sur le réseau

Le logiciel version 5.0 (ou ultérieure) Contrôleur de sécurité Banner utilisé avec un modèle de contrôleur de sécurité Ethernet XS/SC26 FID 7 ou ultérieur peut communiquer via le port Ethernet.

Avec la version 5.0 ou ultérieure du logiciel, un contrôleur de sécurité peut être configuré via Ethernet (configuration via le réseau) ou le mode temps réel peut être surveillé via Ethernet (surveillance en temps réel via le réseau). Une fois connecté, le logiciel fonctionne de la même façon que lorsque le contrôleur de sécurité est connecté via le port USB.

Pour plus d'informations sur l'amélioration de la cybersécurité des systèmes qui incluent les contrôleurs de sécurité XS/SC26, consultez Réf. 235668 – Guide de déploiement sécurisé des contrôleurs de sécurité XS/SC26-2, disponible à l'adresse www.bannerengineering.com.

Important: Si le mot de passe Ethernet par défaut n'est pas modifié, la possibilité de se connecter à un contrôleur avec le logiciel Contrôleur de sécurité Banner via Ethernet sera désactivée. Il s'agit d'une fonction automatique. Modifiez le mot de passe via USB ou Ethernet.

9.1 Connexion au contrôleur de sécurité

Suivez les instructions suivantes pour configurer l'adaptateur réseau et confirmer les connexions réseau.

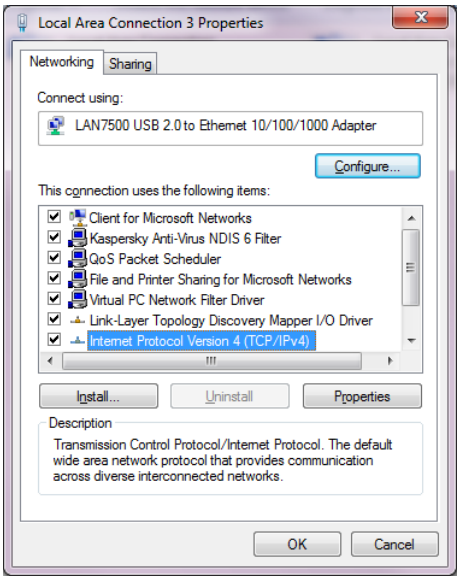
Ces instructions se rapportent au système d'exploitation Windows® version 7, 10 ou 11.

1. Ouvrez les **Paramètres Windows**.
2. Dans l'écran **Paramètres**, sélectionnez **Réseau et Internet**, puis **Centre réseau et partage**, ensuite **Modifier les paramètres de l'adaptateur**.
3. Si plusieurs adaptateurs sont présents, débranchez et rebranchez le câble Ethernet pour déterminer lequel est connecté au contrôleur de sécurité.
4. Cliquez avec le bouton droit de la souris sur la connexion à modifier et sélectionnez **Propriétés**.

Remarque: Si le système vous invite à saisir un mot de passe d'administrateur ou à le confirmer, entrez le mot de passe ou confirmez-le.

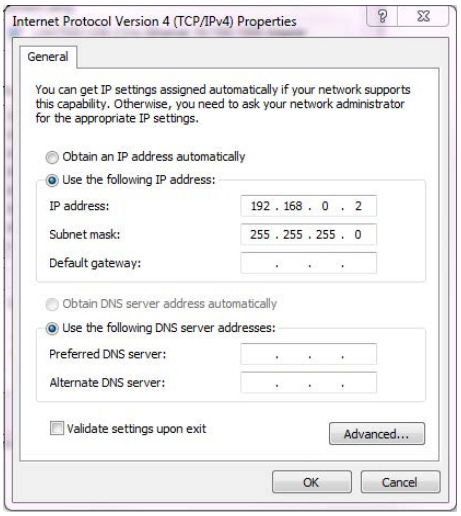
5. Dans **Propriétés**, double-cliquez sur **Protocole Internet Version 4 (TCP/IPv4)**.

Illustration 75. Onglet Connexion réseau Propriétés Ethernet



6. Sélectionnez **Utiliser l'adresse IP suivante**.
7. Saisissez l'adresse IP `192.168.0.1` et un sous-réseau de `255.255.255.0`.

Illustration 76. Propriétés du protocole Internet



Si vous utilisez plusieurs adaptateurs, attribuez les adresses disponibles suivantes aux autres adaptateurs.

8. Cliquez sur **OK** puis cliquez une seconde fois sur **OK**.

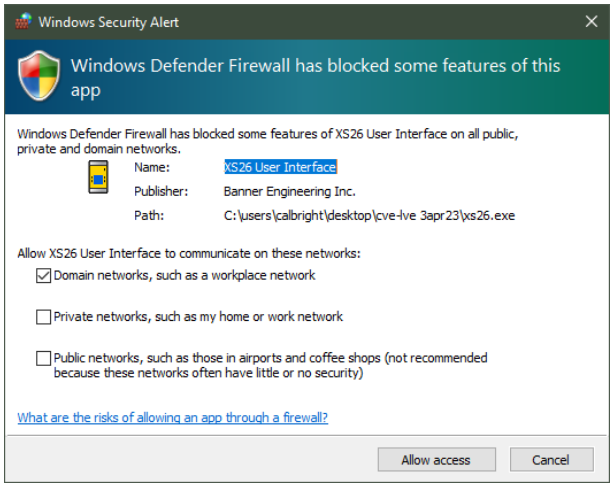
Remarque: Cette étape est nécessaire pour que l'adaptateur Ethernet du PC soit sur le même réseau qu'un contrôleur de sécurité avec les paramètres d'usine par défaut.

9.2 Autorisation du logiciel via le pare-feu Windows

La première fois que vous sélectionnez **Découvrir les contrôleurs sur le réseau**, l'invite **Pare-feu Windows** doit s'afficher.

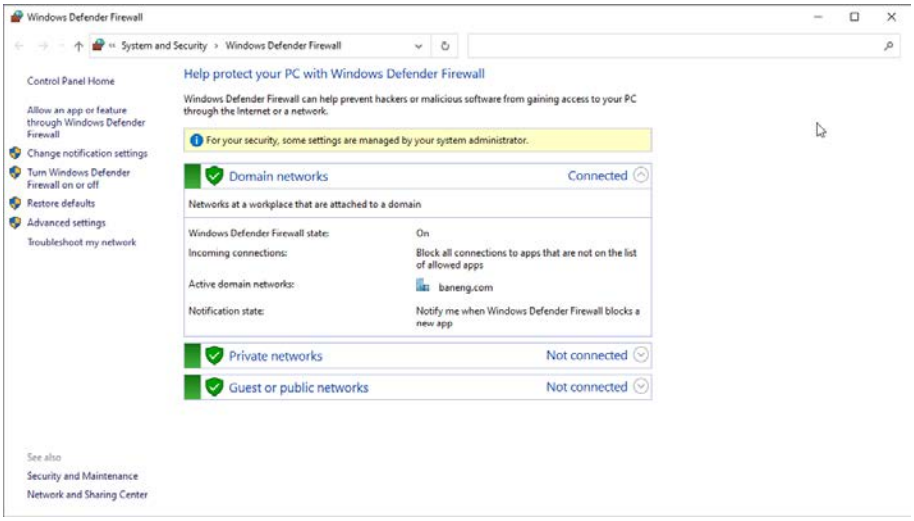
1. Dans la fenêtre **Alerte de sécurité Windows**, cochez les trois cases et cliquez sur **Autoriser l'accès**.
   - Case à cocher **Réseaux de domaine**
   - Case à cocher **Réseaux privés**
   - Case à cocher **Réseaux publics**

Illustration 77. Alerte de sécurité Windows



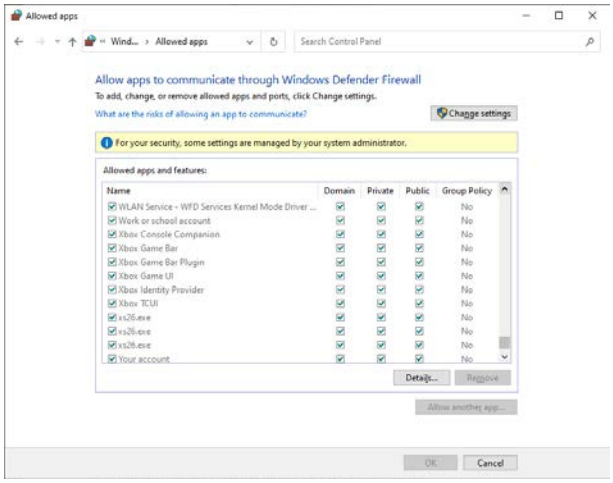
2. Si l'invite n'apparaît pas ou si elle a été annulée lors de son affichage initial, mettez à jour le pare-feu en procédant comme suit :
   a) Dans la zone de recherche à côté du symbole Windows, entrez `Pare-feu Windows`.
   b) Sélectionnez **Pare-feu Windows Defender** dans la liste.
   c) Dans la nouvelle fenêtre, sélectionnez **Autoriser une application ou une fonctionnalité via le pare-feu Windows Defender** (dans le coin supérieur gauche).

Illustration 78. Pare-feu Windows Defender



d) Recherchez **xs26.exe**, qui se trouve à la fin de la liste.
e) Assurez-vous que les quatre cases à cocher pour xs26.exe sont cochées.
Si vous ne pouvez pas cocher la case, cliquez sur **Modifier les paramètres** (en haut à droite).

Illustration 79. Autoriser une application ou une fonctionnalité via le pare-feu Windows Defender



- Case à cocher **xs26.exe** (à gauche du **nom**)
- Case à cocher **Domaine**
- Case à cocher **Privé**
- Case à cocher **Public**

3. Cliquez sur **OK** et fermez les fenêtres.

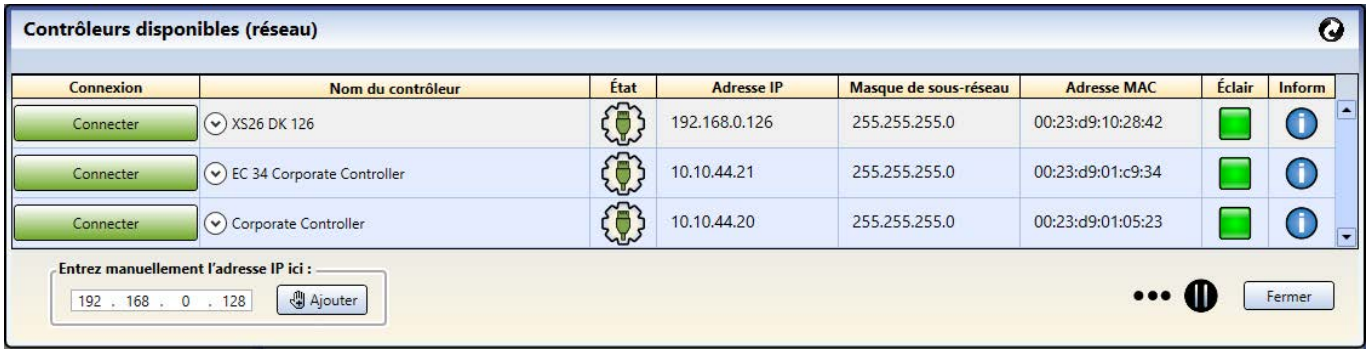
9.3 Recherche de contrôleurs de sécurité sur le réseau

Les processus suivants sont utilisés pour rechercher des contrôleurs sur le réseau de l'ordinateur, une fois que l'ordinateur est configuré pour permettre au logiciel d'explorer le réseau à la recherche de contrôleurs.

Remarque: Certains dispositifs du réseau (comme les routeurs, les pare-feux ou les VLAN utilisés pour la séparation du réseau) bloquent le message Découvrir les contrôleurs. Référez-vous à la section Recherche manuelle de contrôleurs sur le réseau à la page 108.

Sur la page de démarrage du logiciel Contrôleur de sécurité Banner ou dans la barre d'outils de navigation si vous vous trouvez déjà dans le logiciel, cliquez sur . Les contrôleurs disponibles s'affichent.

Illustration 80. Contrôleurs disponibles



La fenêtre **Contrôleurs disponibles** comprend des informations telles que :

- Nom du contrôleur de sécurité
- État
- Adresse IP
- Masque de sous-réseau
- Adresse MAC

Dans la Illustration 80 à la page 107, notez que ces deux contrôleurs de sécurité ont toujours l'adresse IP d'usine par défaut (ils ont la même adresse). Le réseau Ethernet ne peut pas distinguer les éléments ayant les mêmes adresses IP. Changez les adresses IP de ces deux contrôleurs en adresses uniques. Pour ce faire :

1. Débranchez l'un des contrôleurs en retirant physiquement le câble Ethernet du port Ethernet.
2. Paramétrez l'adresse IP du contrôleur connecté en vous y connectant (voir Connexion à un contrôleur de sécurité via Ethernet à la page 108) ou en connectant un câble USB à l'unité retirée pour accéder à l'icône **Paramètres réseau**.
3. Rebranchez ensuite le contrôleur débranché.

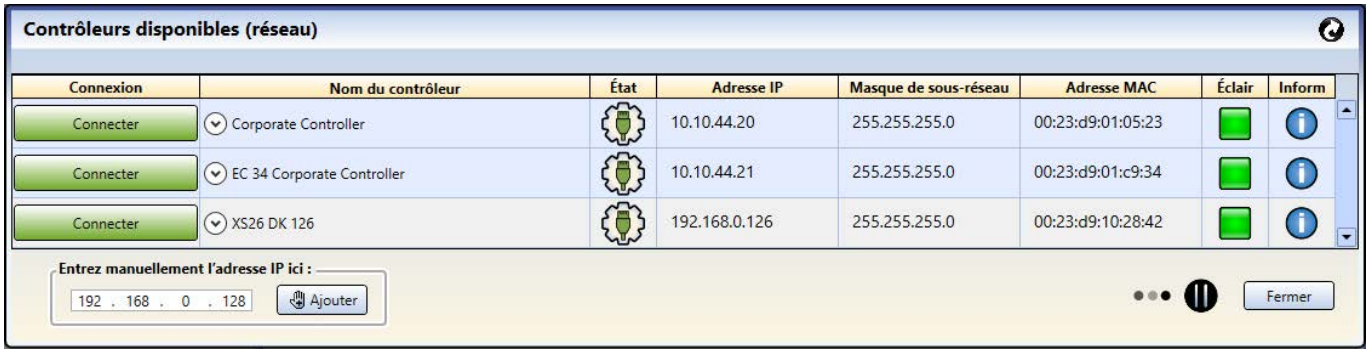
Les contrôleurs de sécurité peuvent être identifiés visuellement en cliquant sur . Cliquer sur fait clignoter les voyants du contrôleur de sécurité associé à cette ligne pendant environ 5 secondes. Cela vous permet de vérifier que l'adresse MAC du contrôleur de sécurité correspond à l'adresse MAC affichée pour l'unité.

Le tableau suivant décrit les symboles d'état :

État	Symbole	Description
Configuration via le réseau/Surveillance en temps réel via le réseau disponibles		Configuration et mode temps réel via Ethernet activés, connexion réseau autorisée
Configuration via le réseau/Surveillance en temps réel via le réseau désactivées		La configuration et le mode temps réel via Ethernet sont désactivés, aucune connexion sur le réseau n'est possible.
Dispositif non trouvé		Impossible de trouver un contrôleur de sécurité connecté au réseau, aucune connexion réseau autorisée
Connecté par USB		Le contrôleur de sécurité est déjà connecté au logiciel Contrôleur de sécurité Banner via une connexion USB, aucune connexion réseau n'est autorisée.
Réseau connecté		Le contrôleur de sécurité est déjà connecté via une connexion réseau, aucune nouvelle connexion réseau n'est autorisée.
Redémarrage du système		Le contrôleur de sécurité est en train de redémarrer, aucune connexion réseau autorisée
Connecté manuellement		Le contrôleur de sécurité a été ajouté manuellement (pas via la détection réseau), connexion réseau autorisée

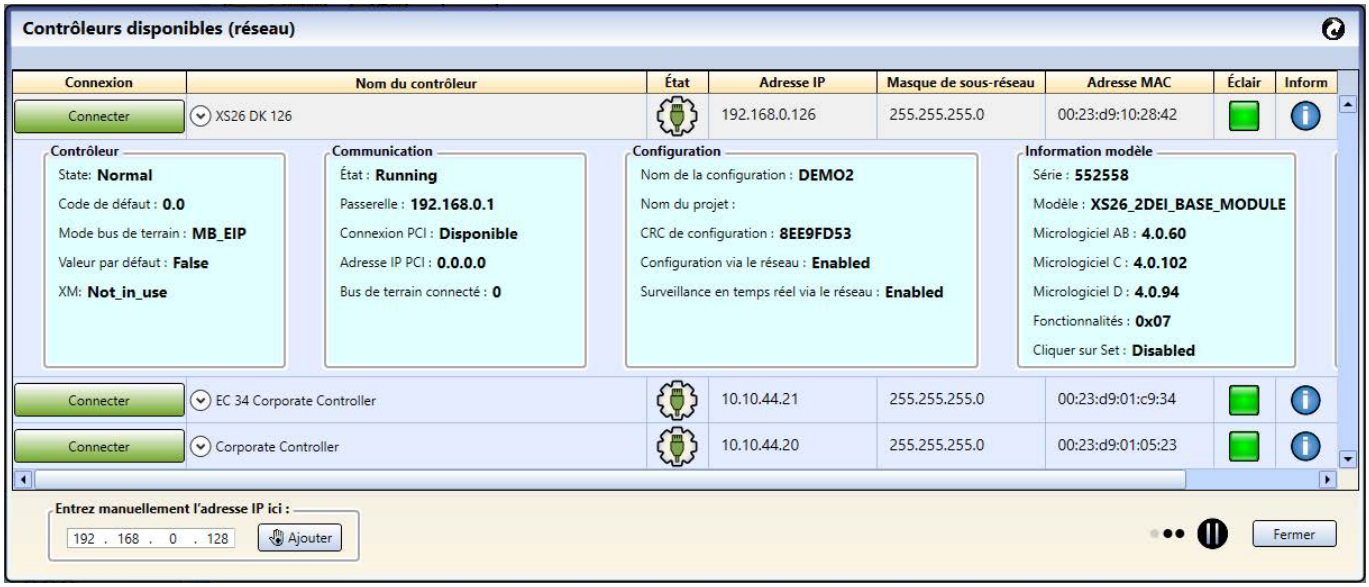
Les contrôleurs de sécurité s'affichent dans l'ordre dans lequel ils sont trouvés. Modifiez l'ordre en cliquant sur l'en-tête d'une colonne (par exemple, cliquez sur l'adresse IP pour classer les contrôleurs de l'adresse IP la plus basse à l'adresse IP la plus élevée).

Illustration 81. Ordre des contrôleurs de sécurité



Vous pouvez obtenir des informations détaillées sur un contrôleur de sécurité spécifique en cliquant sur pour ce contrôleur.

Illustration 82. Informations sur le contrôleur de sécurité



Cet écran fournit des informations sur l'état de fonctionnement du contrôleur de sécurité et sa communication. Il fournit des informations sur la configuration actuellement chargée dans le contrôleur. Il fournit des informations sur les microprocesseurs du contrôleur de sécurité ainsi que ses protocoles.

9.3.1 Recherche manuelle de contrôleurs sur le réseau

Lorsque vous cliquez sur **Découvrir les contrôleurs sur le réseau**, le logiciel Contrôleur de sécurité Banner envoie un message UDP sur le réseau. Certains dispositifs sur le réseau peuvent bloquer ces messages (par exemple, les commutateurs gérés).

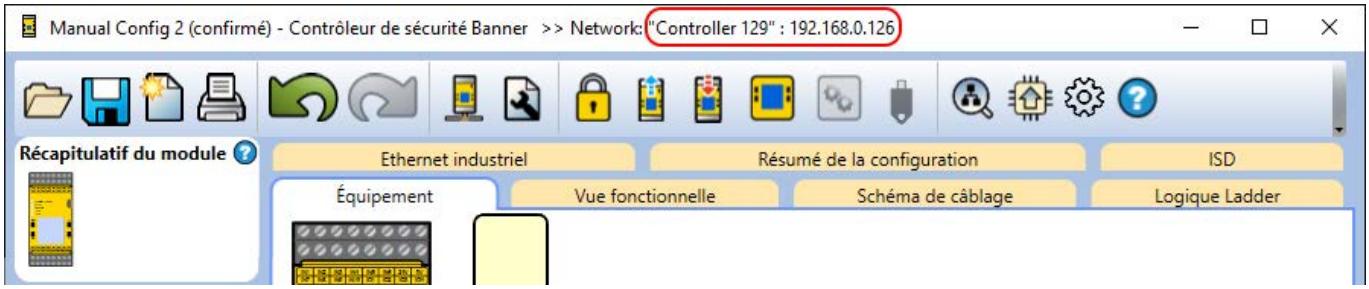
Si l'adresse IP est connue, saisissez-la dans le champ **Entrez manuellement l'adresse IP ici**. Lorsque vous cliquez sur **Ajouter**, un message direct de connexion est envoyé au contrôleur de sécurité à cette adresse. Comme il s'agit d'un message direct et non d'un message de diffusion, il devrait atteindre le contrôleur qui sera alors ajouté à la liste **Contrôleurs disponibles**.

9.4 Connexion à un contrôleur de sécurité via Ethernet

Pour vous connecter à un contrôleur de sécurité via la connexion Ethernet, cliquez sur **Connecter** à côté du contrôleur de sécurité souhaité.

Le logiciel Contrôleur de sécurité Banner se connecte au contrôleur de sécurité de la même façon que s'il était connecté via le port USB. Le voyant USB du contrôleur clignote rapidement pour indiquer qu'il est connecté au logiciel via le port Ethernet. L'adresse IP s'affiche en haut de l'écran du logiciel.

Illustration 83. Contrôleur de sécurité connecté au logiciel via Ethernet



Cliquez sur pour revenir à la fenêtre **Contrôleurs disponibles**.

Pour déconnecter le contrôleur de sécurité actuellement connecté, cliquer sur **Déconnecter**. Un seul contrôleur de sécurité peut être connecté à la fois.

9.5 Reset du système via la connexion Ethernet

Le logiciel Contrôleur de sécurité Banner permet d'effectuer un reset du système via la connexion Ethernet.

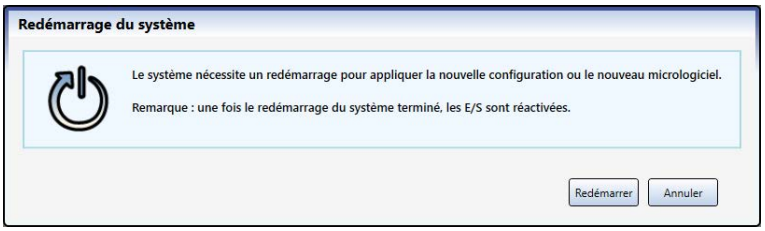
Utilisez ce reset du système, appelé Redémarrage système, pour rétablir le contrôleur en état de fonctionnement après avoir modifié l'adresse IP ou envoyé une nouvelle configuration au contrôleur.

9.5.1 Changement d'adresse IP

Lors de la modification d'une adresse IP, le redémarrage du système ne s'affiche pas tant que la fenêtre **Paramètres réseau** n'est pas fermée.

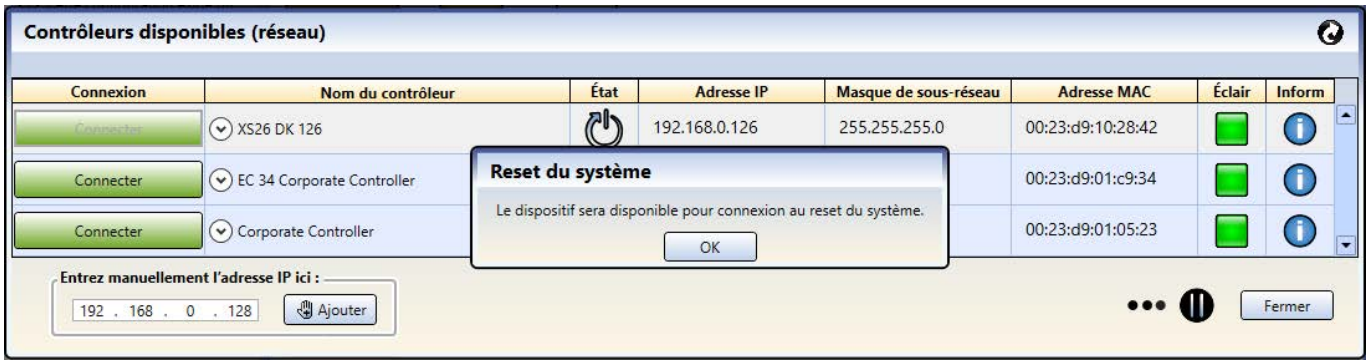
Une fois la fenêtre fermée, la fenêtre suivante s'affiche :

Illustration 84. Fenêtre de redémarrage du système



Si **Redémarrage** est sélectionné, le contrôleur de sécurité effectue le test de démarrage. Pendant ce temps, l'avertissement suivant s'affiche :

Illustration 85. Notification de redémarrage du système



Cliquez sur **OK**. Le bouton **Connecter** du contrôleur dans le logiciel Contrôleur de sécurité Banner revient à l'état actif une fois le test de démarrage du contrôleur de sécurité terminé. Cliquez sur **Connecter** pour reconnecter le logiciel au contrôleur.

Si l'option **Annuler** est sélectionnée dans la fenêtre **Redémarrage du système**, le logiciel Contrôleur de sécurité Banner permet toujours d'effectuer la fonction de redémarrage. (Redémarrage du système) s'affiche dans la barre d'outils jusqu'à ce que le contrôleur de sécurité ait terminé la fonction de redémarrage/reset. (Cela peut être effectué localement au niveau du contrôleur.)

9.5.2 Modification de la configuration

Lorsqu'une nouvelle configuration a été chargée, la fenêtre **Redémarrage du système** s'affiche après la dernière fenêtre de chargement d'une configuration (fenêtre Enregistrer ou Fermer).

Remettez le contrôleur de sécurité en état de fonctionnement en sélectionnant **Redémarrer**. Sélectionnez **Annuler** si le reset du système est effectué localement (au niveau du contrôleur).

La procédure est identique à celle de la section Changement d'adresse IP à la page 109.

9.6 Raccourcis

comprend des raccourcis pour faciliter la configuration.

Si aucun contrôleur de sécurité n'apparaît sur la page **Contrôleurs disponibles**, il est possible d'accéder rapidement aux connexions réseau, au pare-feu Windows ou à l'invite de commande (pour envoyer un ping à un contrôleur). Cliquez sur et sélectionnez le lien approprié. La fenêtre souhaitée s'ouvre.

10 Logiciel

Le logiciel Contrôleur de sécurité Banner est une application logicielle avec un affichage en temps réel et des outils de diagnostic pouvant servir à :

- Concevoir et modifier des configurations
- Tester la configuration en mode simulation
- Écrire une configuration sur le contrôleur de sécurité
- Lire la configuration actuelle du contrôleur de sécurité
- Afficher des informations en temps réel, par exemple les états des dispositifs
- Afficher des informations sur les défauts

Le logiciel propose des icônes et des symboles de circuit pour faciliter la sélection des propriétés et des dispositifs d'entrée appropriés. Comme les propriétés des différents dispositifs et les relations de commande d'E/S sont définies dans l'onglet **Vue fonctionnelle**, le programme génère automatiquement les schémas de câblage et de logique Ladder correspondants.

Référez-vous à la section Création d'une configuration à la page 86 pour en savoir plus sur la conception d'une configuration. Référez-vous à la section Exemple de configuration du XS/SC26 à la page 95 pour consulter un exemple de conception d'une configuration.

Référez-vous à la section Onglet Schéma de câblage à la page 121 pour en savoir plus sur la connexion des dispositifs et à la section Onglet Logique Ladder à la page 122 pour un rendu logique (Ladder) de la configuration.

Référez-vous à la section Mode temps réel à la page 140 pour plus d'informations sur les données d'exécution (Run time) du contrôleur de sécurité.

10.1 Abréviations

Abréviation [18]	Description
AVM	Nœud d'entrée AVM (moniteur de vanne réglable) des sorties de sécurité
AVMx	Entrée AVM (moniteur de vanne réglable)
BP	Nœud d'entrée de dérivation des blocs de dérivation et des blocs d'inhibition
BPx	Entrée Interrupteur de dérivation
BOS	Nœud d'entrée Bas de course des blocs Commande de presse (XS/SC26 uniquement)
CD	Nœud d'entrée Annulation de la temporisation des sorties de sécurité, des blocs de temporisation et des blocs 1 impulsion
CDx	Annuler l'entrée de temporisation
CSx	Entrée Démarrage de cycle
ED	Activation du nœud de dispositif d'entrée des blocs de dispositif d'activation
EDx	Activation du nœud de dispositif d'entrée
EDM	Nœud d'entrée EDM (surveillance des appareils externes) des sorties de sécurité
EDMx	Entrée Surveillance des appareils externes (EDM)
ES	Nœud d'entrée Arrêt d'urgence des blocs de dispositif d'activation
ESx	Entrée Arrêt d'urgence
ETB	Bornier externe (SC10-2 uniquement)
FID	Identification des fonctionnalités
FSx	Entrée Interrupteur au pied
FR	Nœud d'entrée Reset de défaut des sorties de sécurité
Ft Switch	Nœud d'entrée Interrupteur au pied des blocs Commande de presse (XS/SC26 uniquement)
GO	Nœud d'entrée Début de cycle des blocs Commande de presse (XS/SC26 uniquement)
GSx	Entrée Interrupteur pour porte
JOG	Nœud d'entrée JOG des blocs de dispositif d'activation
IN	Nœud d'entrée normal des blocs fonction et des blocs de sortie de sécurité
ISD	In-Series Diagnostic
LR	Nœud d'entrée Reset à verrouillage du bloc de reset à verrouillage et des sorties de sécurité

[18] Le suffixe « x » représente le numéro automatiquement assigné.

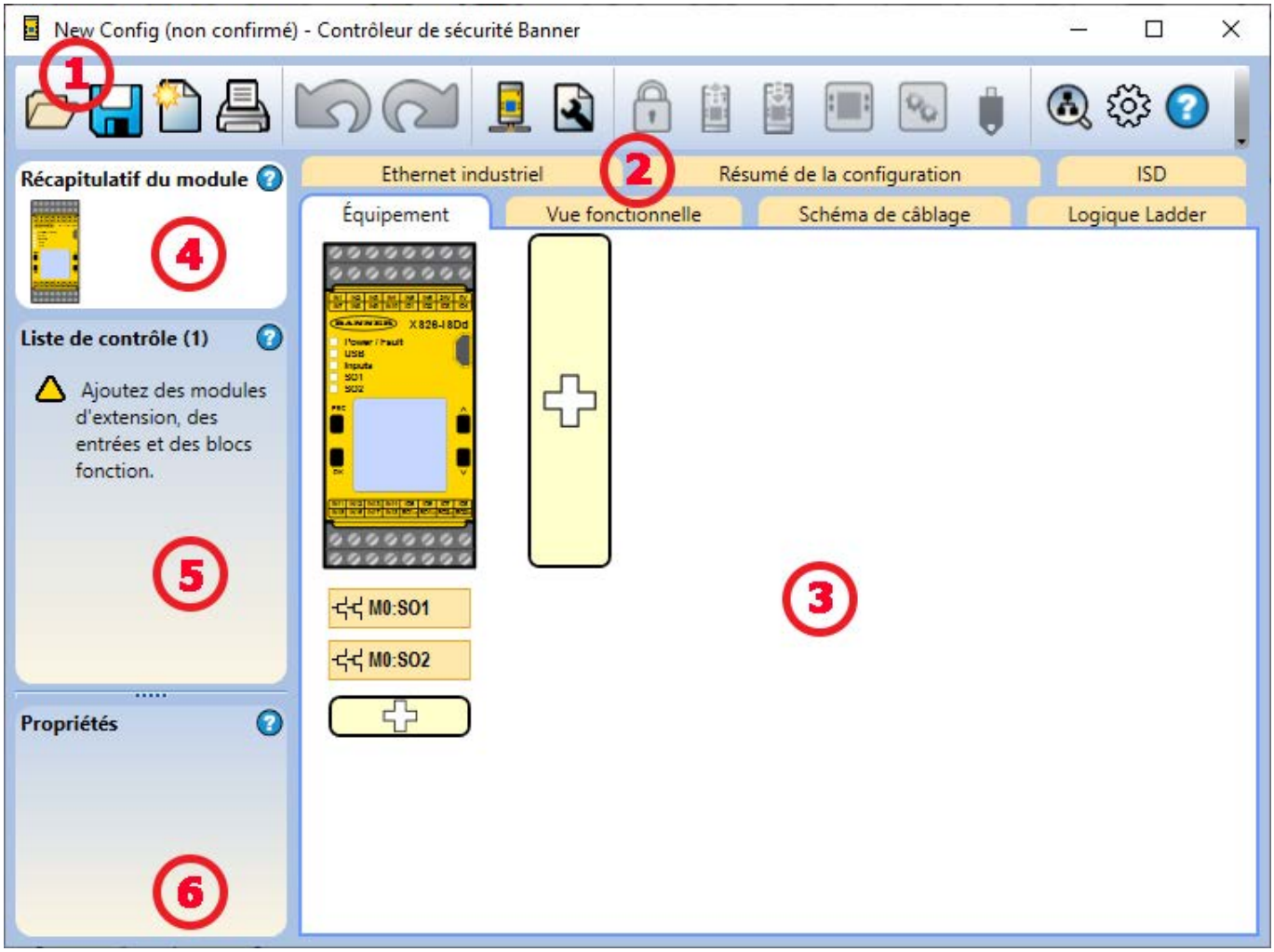
Abréviation [18]	Description
ME	Nœud d'entrée Inhibition activée des blocs d'inhibition et des blocs de commande bimanuelle
MEx	Entrée Inhibition activée
MP1	Nœud d'entrée de la première paire de capteurs d'inhibition des blocs d'inhibition et des blocs de commande bimanuelle
MP2	Nœud d'entrée de la deuxième paire de capteurs d'inhibition des blocs d'inhibition uniquement
M Safety	Nœud d'entrée de sécurité inhibable des blocs Commande de presse (XS/SC26 uniquement)
M Sensor	Nœud d'entrée du capteur d'inhibition de commande de presse des blocs Commande de presse (XS/SC26 seulement)
Mx	Contrôleur de base et modules d'extension (dans l'ordre affiché dans l'onglet **Équipement**)
MRx	Entrée de reset manuel
MSPx	Entrée Paire de capteurs d'inhibition
NM Safety	Nœud d'entrée de sécurité non inhibable des blocs Commande de presse (XS/SC26 uniquement)
ONx	Entrée Marche-Arrêt
OSx	Entrée Capteur optique
PCMSx	Entrée du capteur d'inhibition de commande de presse
PIP	Nœud d'entrée Pièce en place des blocs Commande de presse (XS/SC26 uniquement)
PSx	Entrée Arrêt de protection
RE	Nœud d'entrée Activation de reset des blocs de reset à verrouillage et des sorties de sécurité
ROx	Sortie relais
RPI	Intervalle de données demandé
RPx	Entrée Interrupteur à câble
RST	Nœud de reset des blocs Bascule SR, Bascule RS, des blocs de reset à verrouillage, des blocs Commande de presse et des blocs Dispositif d'activation
RUN	Nœud d'entrée du mode de fonctionnement standard (RUN) des blocs Mode de commande de presse (XS/SC26 uniquement)
SET	Nœud de paramètre des blocs Bascule SR et RS
SMx	Entrée Tapis de sécurité
SOx	Sortie de sécurité
SQS	Nœud d'entrée d'arrêt séquentiel des blocs Commande de presse (XS/SC26 uniquement)
SQSx	Entrée d'arrêt séquentiel (SQS) de commande de presse
STATx	Sortie d'état
TC	Nœud d'entrée Commande bimanuelle des blocs de commande bimanuelle
TCx	Entrée Commande bimanuelle
TOS	Nœud d'entrée Haut de course des blocs Commande de presse (XS/SC26 uniquement)

10.2 Présentation du logiciel

Remarque: Les sections suivantes utilisent le XS/SC26 comme exemple. L'interface du SC10-2 est similaire.

[18] Le suffixe « x » représente le numéro automatiquement assigné.

Illustration 86. Logiciel Contrôleur de sécurité Banner — XS/SC26 illustré



(1) Barre d'outils de navigation


Ouvre un projet existant, un projet **récent** ou des **exemples de projet**


Enregistre le projet dans l'emplacement défini par l'utilisateur


Démarre un **nouveau projet**


Imprime un résumé de la configuration personnalisable


Annule jusqu'à 10 actions précédentes


Réapplique jusqu'à 10 actions précédemment annulées


Affiche les paramètres réseau et les écrit sur le contrôleur de sécurité


Affiche les paramètres du projet


Ouvre le gestionnaire des mots de passe


Lit les données du contrôleur de sécurité, par exemple le journal des défauts, la configuration, les paramètres réseau et les informations sur les dispositifs


S'affiche lorsqu'une mise à jour du micrologiciel est disponible.


Écrit les données, par exemple les paramètres de configuration, sur le contrôleur de sécurité


Permet d'accéder au Mode temps réel


Permet d'accéder au Mode simulation


Indique la connexion à la carte mémoire SC-XM2 ou SC-XM3


Ouvre la fenêtre **Contrôleurs disponibles**


Ouvre les options **Paramètres**

- **Icônes** — Bascule entre les icônes américaines et européennes
- **Langue** — Sélectionne les options de langue du logiciel
- **Mises à jour logicielles** — Indique si le logiciel est à jour
- **Préférences** — Définit les paramètres par défaut du logiciel selon les besoins habituels de l'utilisateur


Ouvre les options de l'**Aide**

- **Aide** — Ouvre les rubriques d'aide
- **À propos** — Affiche le numéro de version du logiciel et un avertissement sur les responsabilités de l'utilisateur
- **Notes de publication** — Affiche les notes de publication de chaque version du logiciel
- **Informations de support** — Explique comment demander une assistance auprès du service de support technique avancé de Banner Engineering


Réinitialise le système. S'affiche lorsqu'un reset système est nécessaire jusqu'à ce que le contrôleur de sécurité ait terminé la fonction de redémarrage/reset.

(2) Onglets pour les feuilles de travail et les schémas

Équipement — Affiche une vue modifiable de tous les équipements connectés

Vue fonctionnelle — Affiche des icônes représentant la logique de contrôle

Schéma de câblage — Affiche les détails du câblage des E/S des dispositifs, utilisés par l'installateur

Logique Ladder — Affiche des symboles représentant la logique de protection du contrôleur de sécurité, utilisée par le concepteur de la machine ou l'ingénieur électromécanicien

Ethernet industriel (si activé) — Affiche des options de configuration du réseau modifiables

Résumé de la configuration — Affiche un résumé détaillé de la configuration

Mode temps réel (si activé) — Affiche les données du mode temps réel, y compris les défauts actuels

Mode simulation (si activé) — Affiche les données du mode simulation

ISD (SC10-2 FID 2 ou ultérieur et modèles XS26-ISD) — Affiche la chaîne ISD

(3) Vue sélectionnée

Affiche la vue correspondant à l'onglet sélectionné (ici la vue **Équipement**)

(4) Récapitulatif du module

Affiche le contrôleur de base ainsi que les modules connectés ou affiche le SC10-2

(5) Liste de contrôle

Propose des actions pour configurer le système et corriger d'éventuelles erreurs en vue de finaliser la configuration

(6) Propriétés

Affiche les propriétés de la connexion, du dispositif ou du bloc fonction sélectionné (les propriétés ne peuvent pas être modifiées dans cette vue, il faut cliquer sur **Modifier** sous le tableau pour apporter des modifications)

Supprimer — Supprime l'élément sélectionné

Modifier — Affiche les options de configuration du dispositif ou du bloc fonction sélectionné

Voir la section Logiciel : recherche de pannes à la page 344 pour résoudre des problèmes liés aux fonctionnalités du logiciel.

10.3 Nouveau projet

Cliquez sur **Nouveau projet** pour sélectionner le contrôleur souhaité et ouvrir l'écran **Démarrer un nouveau projet**. Cet écran comprend des informations de projet uniquement disponibles à la création initiale d'un projet mais pas dans l'écran **Paramètres du projet**.

XS/SC26

Toutes les cases à cocher sont sélectionnées par défaut. Les options suivantes sont disponibles :

Avec afficheur
Cochez cette case si votre contrôleur est équipé d'un écran. Lorsque cette case est cochée, un « d » s'affiche après le « -2 » dans la référence du modèle indiquée dans le logiciel.

Avec Ethernet industriel
Cochez cette case si votre contrôleur possède une connexion Ethernet industriel. Lorsque cette case est cochée, un « e » s'affiche après le « -2 » dans la référence du modèle indiquée dans le logiciel.

Est extensible
Cochez cette case si votre contrôleur est un XS26. Décochez cette case si votre contrôleur est un SC26-2.

Avec ISD
Cochez cette case si votre contrôleur est un XS26-ISDd. Décochez cette case si votre contrôleur est un autre modèle. Lorsque cette case est cochée, le « -2xx » est remplacé par « -ISDd » dans la référence du modèle indiquée dans le logiciel.

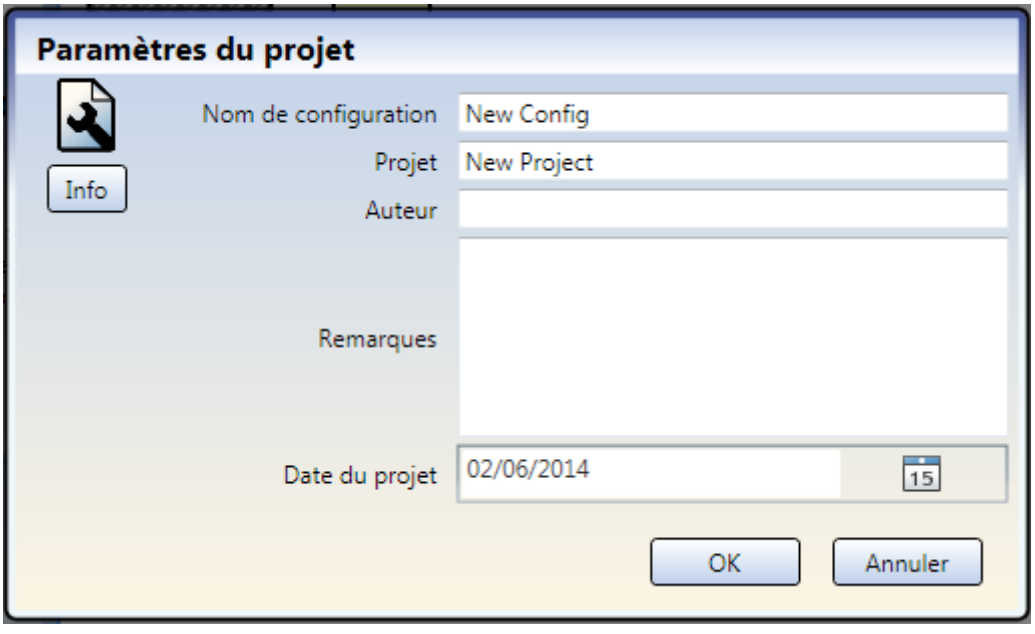
SC10-2

Désactiver la fonction d'optimisation automatique des bornes (SC10-2 uniquement)
Activez ou désactivez l'optimisation automatique des bornes, ce qui permet d'augmenter le nombre d'entrées à l'aide d'un bornier externe (ETB).

Remarque: Les informations de projet mentionnées ci-dessus ne sont pas disponibles dans **Paramètres du projet**, mais elles peuvent être modifiées à l'aide de la fonction **Modifier** de l'écran **Propriétés du module**.

10.4 Paramètres du projet

Illustration 87. Paramètres du projet



Pour chaque configuration, vous avez la possibilité d'inclure des informations de projet supplémentaires afin de distinguer plus facilement les différentes configurations. Pour entrer ces informations, cliquez sur **Paramètres du projet**.

Nom de la configuration
Nom de la configuration, affiché sur le contrôleur de sécurité (modèles avec écran d'affichage), différent du nom de fichier. Le nom de la configuration doit contenir entre 1 et 16 caractères.

Projet
Nom du projet, utile pour différencier les différents domaines d'application.

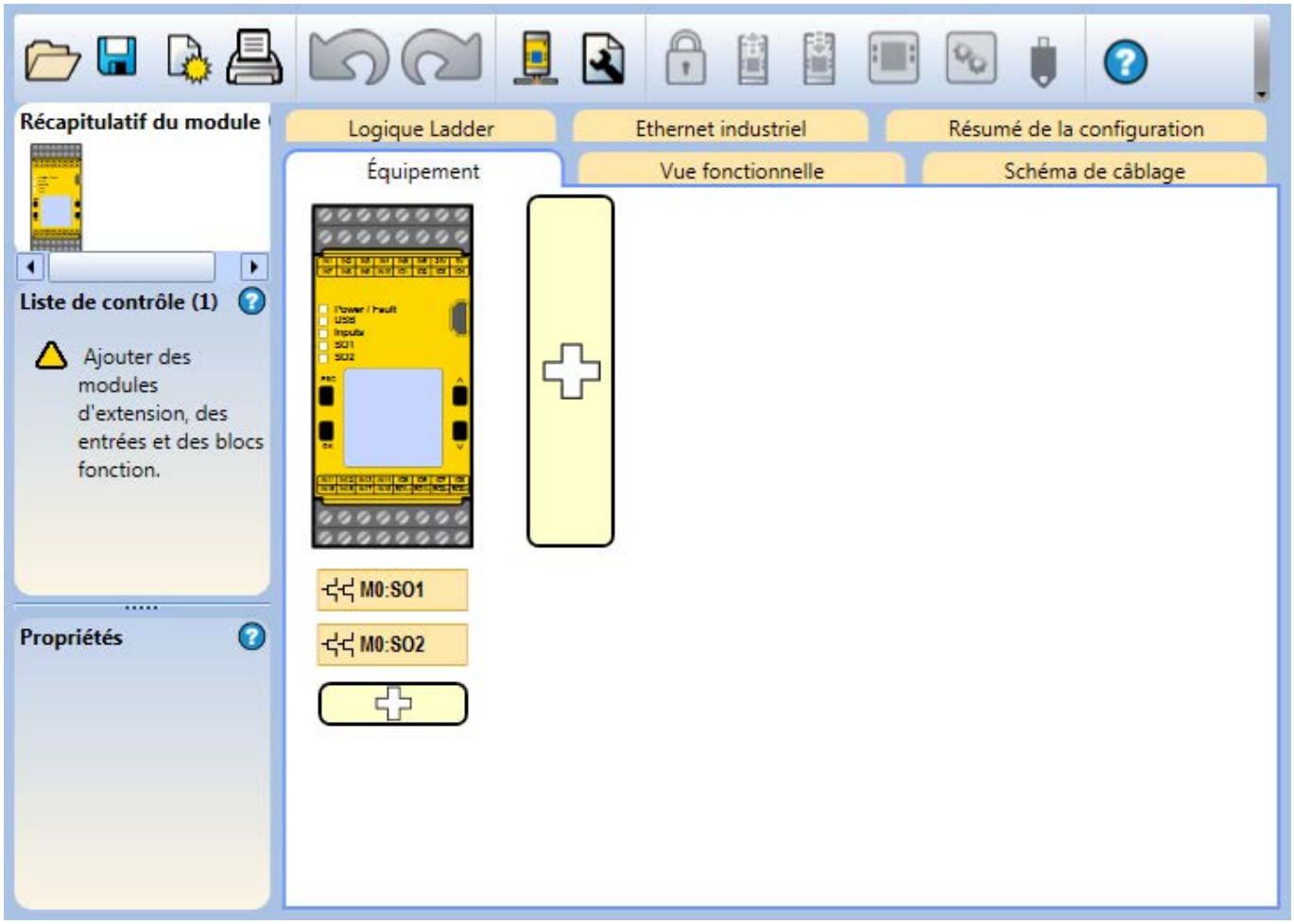
Auteur
Personne ayant conçu la configuration.

Remarques
Informations supplémentaires sur cette configuration ou projet.

Date du projet
Date associée au projet.

10.5 Onglet Équipement

Illustration 88. Exemple − Onglet XS/SC26 ***XS/SC26***



XS/SC26 : l'onglet **Équipement** permet de sélectionner le modèle de base, d'ajouter les modules d'extension (entrée, sortie et passerelle de communication) ainsi que les dispositifs d'entrée et les sorties d'état. Ajoutez les modules d'extension en cliquant sur ✚ à droite du module du contrôleur de base.

Remarque: Si vous utilisez un module EtherCAT, il doit être le premier module de la chaîne, à côté du contrôleur de base.

SC10-2 : l'onglet **Équipement** permet d'ajouter les dispositifs d'entrée et les sorties d'état.

Personnalisez le module du contrôleur de base ou le SC10-2 en double-cliquant sur le module ou en le sélectionnant et en cliquant sur **Modifier** sous le tableau **Propriétés** à gauche et en sélectionnant les fonctions appropriées du contrôleur de sécurité (affichage, Ethernet, extensibilité, ISD, optimisation automatique des bornes). Les propriétés des entrées de

sécurité et des entrées auxiliaires, des sorties d'état, des blocs logiques et des blocs fonction sont également configurées soit en double-cliquant sur le bloc, soit en le sélectionnant et en cliquant sur **Modifier** sous le tableau **Propriétés**. Un second clic sur le bloc permet de le désélectionner.

Illustration 89. Propriétés du module XS/SC26

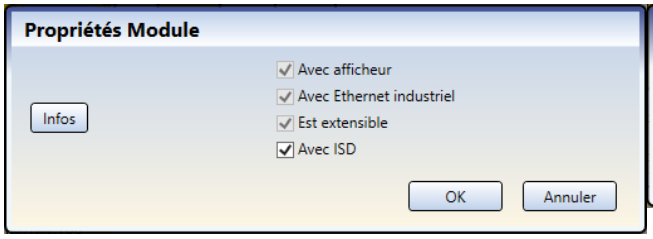
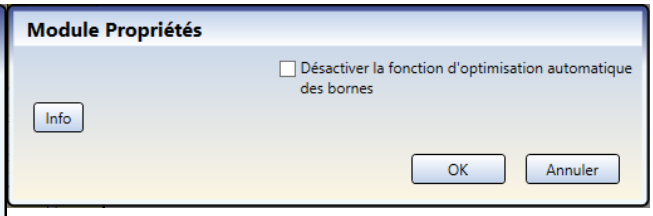
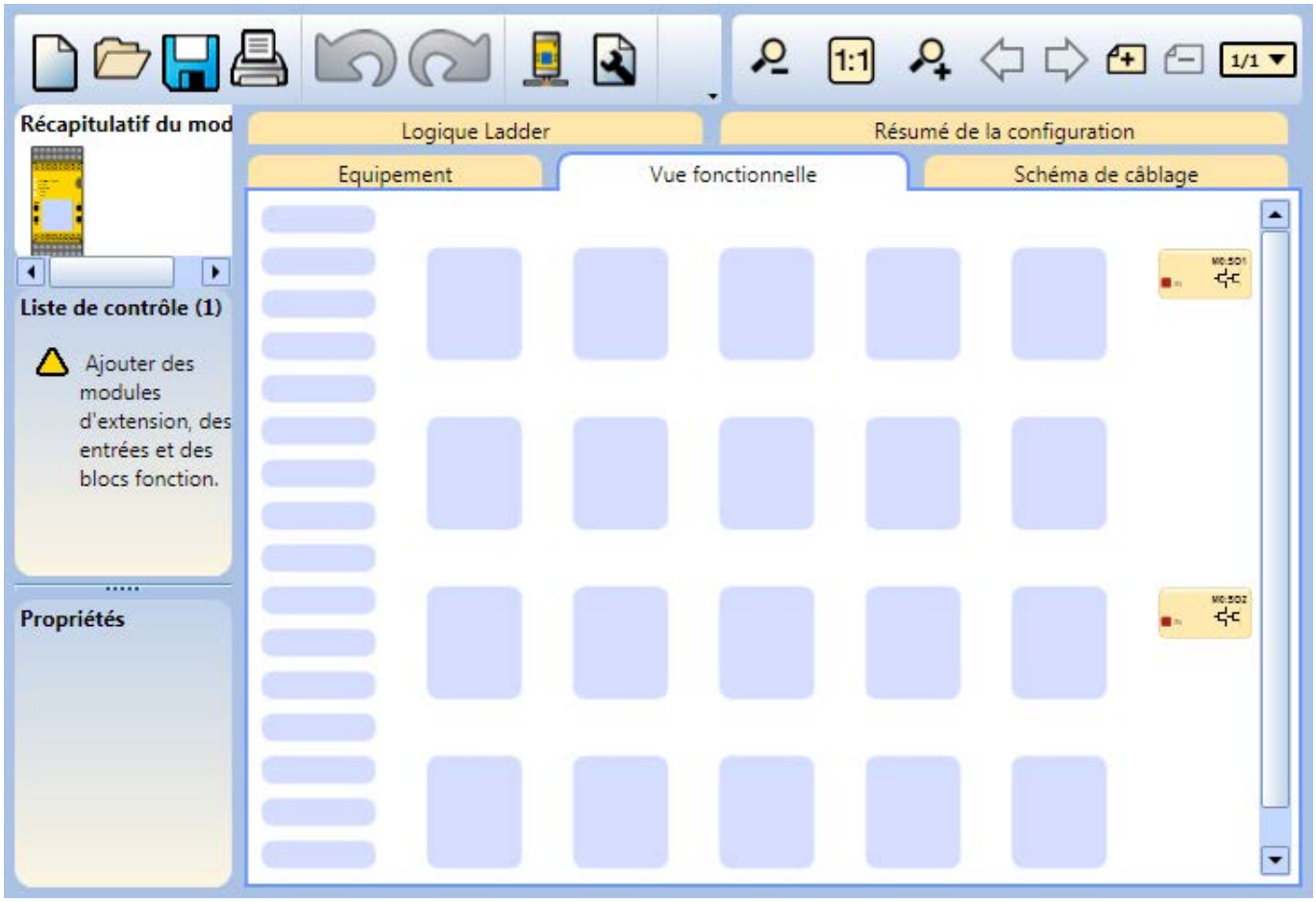


Illustration 90. Propriétés du module SC10-2



10.6 Onglet Vue fonctionnelle

*Illustration 91. Onglet **Vue fonctionnelle***



L'onglet **Vue fonctionnelle** permet de créer la logique de contrôle. La colonne de gauche de l'onglet **Vue fonctionnelle** est utilisée pour les entrées de sécurité et les entrées auxiliaires, la colonne du milieu pour les blocs logiques et fonction et celle de droite pour les sorties de sécurité. Il est possible de déplacer les entrées de sécurité et les entrées auxiliaires entre les colonnes de gauche et du milieu. Les blocs fonction et logiques peuvent être uniquement déplacés au sein de la colonne du milieu. Les sorties sont statiques (placées par le programme) et ne peuvent pas être déplacées. Les différents types de blocs de référence peuvent être placés n'importe où dans les sections de gauche et du milieu.

Important: Le logiciel Contrôleur de sécurité Banner est conçu pour vous aider à créer une configuration valide. Toutefois, c'est à l'utilisateur qu'il incombe de vérifier l'intégrité, la sécurité et le fonctionnement de la configuration en suivant la Procédure de vérification à la mise en route à la page 312.

Dans l'onglet **Vue fonctionnelle**, vous pouvez réaliser les tâches suivantes :

- Personnaliser l'apparence du schéma en repositionnant les entrées, les blocs logiques et les blocs fonction

- **Annuler** et **rétablir** jusqu'à 10 actions récentes
- Ajouter des pages supplémentaires pour les configurations importantes grâce à la barre d'outils de navigation (voir la Illustration 92 à la page 118)
- Effectuer un zoom avant et arrière de la vue du schéma ou l'adapter automatiquement en fonction de la taille de la fenêtre (voir la Illustration 92 à la page 118)

Illustration 92. Barre d'outils pour la navigation entre les pages et la définition de la taille du schéma



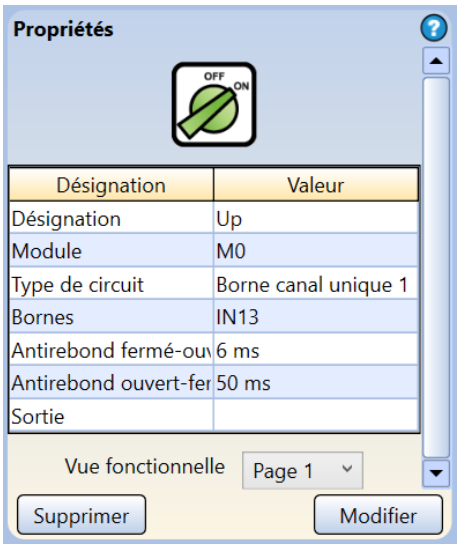
- Naviguer d'une page à l'autre en cliquant sur les flèches gauche et droite dans la zone de navigation de pages dans le coin supérieur droit du logiciel
- Modifier les propriétés des blocs en double-cliquant sur un bloc ou en sélectionnant un bloc et en cliquant sur **Modifier** dans le tableau **Propriétés**
- Supprimer n'importe quel bloc ou connexion en sélectionnant l'élément et en appuyant sur la touche **Suppression** du clavier ou en cliquant sur **Supprimer** sous le tableau **Propriétés**

Remarque: Il n'existe aucune confirmation de la suppression d'objets. Vous pouvez annuler la suppression en cliquant sur **Annuler**.

Par défaut, toutes les entrées ajoutées dans l'onglet **Équipement** sont placées dans l'onglet **Vue fonctionnelle** au niveau du premier emplacement réservé dans la colonne de gauche. Pour déplacer des signaux d'une page à une autre, deux méthodes sont possibles. Pour ce faire, procédez de l'une des manières suivantes :

1. Ajoutez une **référence** au bloc situé dans une page différente. Cliquez sur l'un des emplacements réservés dans la section du milieu, sélectionnez **Référence** puis sélectionnez le bloc situé sur la page suivante. Seuls les blocs d'autres pages peuvent être ajoutés comme **référence.**
2. Réaffectez la page. Dans la page où vous souhaitez conserver la configuration, déplacez l'un des blocs vers l'un des emplacements réservés dans la section du milieu. Accédez à la page contenant le bloc à déplacer. Sélectionnez le bloc et modifiez l'affectation de page sous le tableau **Propriétés**.

*Illustration 93. Tableau **Propriétés***



10.6.1 Blocs logiques

Les blocs logiques sont utilisés pour créer des relations fonctionnelles booléennes (vrai ou faux) entre les entrées, les sorties et d'autres blocs logiques ou blocs fonction.

Les blocs logiques acceptent les entrées de sécurité, les entrées auxiliaires ou les sorties de sécurité appropriées en tant qu'entrées. L'état de la sortie reflète le résultat logique booléen de la combinaison des états de ses entrées (**1** = On (activé), **0** = Off (désactivé), **x** = sans importance).

PRÉCAUTION: Logique inversée

Il n'est pas recommandé d'utiliser des configurations de logique inversée dans les applications de sécurité présentant des risques.

Il est possible d'inverser les états des signaux en utilisant les blocs logiques NOT, NAND et NOR ou en sélectionnant les cases à cocher « Inverser sortie » ou « Inverser source d'entrée » (si disponibles). Dans une entrée de bloc logique, la logique inversée traite un état d'arrêt (0 ou Off) comme un « 1 » (vrai ou On) et entraîne l'activation d'une sortie en supposant que toutes les conditions des entrées sont satisfaites. De la même manière, la logique inversée entraîne la fonction inverse d'une sortie lorsque le bloc devient « vrai » (la sortie passe de On à Off). En raison de certains modes de

défaillance susceptibles d'entraîner une perte de signal, par exemple un câble rompu, un court-circuit vers la terre/0 V, l'interruption de l'alimentation d'un dispositif de protection, etc., la logique inversée n'est généralement pas utilisée dans les applications de sécurité. Une situation dangereuse peut se produire suite à la perte du signal d'arrêt sur une entrée de sécurité, provoquant l'activation d'une sortie de sécurité.

AND (ET)

	Entrée 1	Entrée 2	Sortie
(États-Unis) (Union européenne)	0	x	0
La valeur de sortie est basée sur le ET logique de **2** à **5** entrées.	x	0	0
La sortie est activée (On) quand toutes les entrées sont activées.	1	1	1

OR (OU)

	Entrée 1	Entrée 2	Sortie
(États-Unis) (Union européenne)	0	0	0
La valeur de sortie est basée sur le OR logique de **2** à **5** entrées.	1	x	1
La sortie est activée (On) quand au moins une entrée est activée.	x	1	1

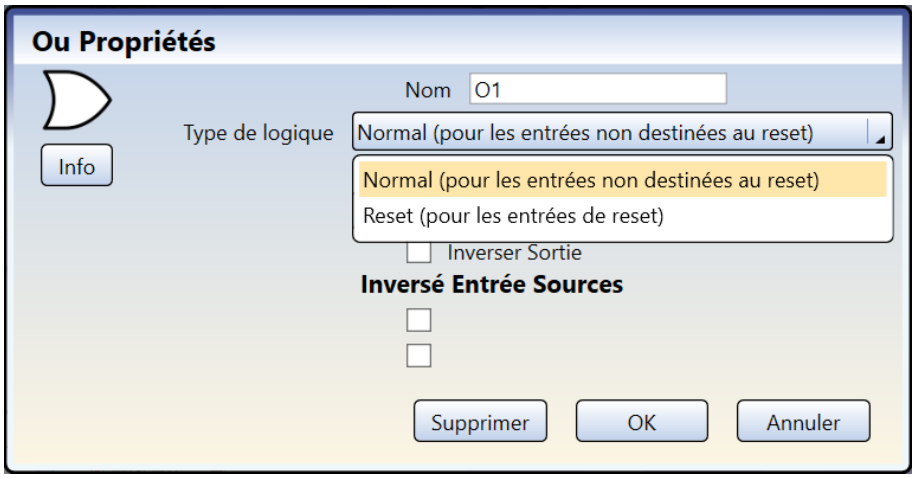
Il existe deux types de blocs logiques OR (OU) : Normal et Reset (modèles XS/SC26 FID 4 ou ultérieurs uniquement).

Bloc OR de type reset Pour que plusieurs resets puissent exécuter la même fonction de reset (comme un reset manuel câblé et un reset manuel virtuel), un bloc fonction OR de reset a été créé. Ce type spécial de bloc OR n'accepte que les entrées de reset et ne peut être connecté que comme une entrée de reset manuel dans la logique.

Bloc OR de type normal Pour exécuter une logique OR sur toute fonction pouvant être connectée à un bloc OR (outre les resets), le type de logique normal doit être sélectionné. Il s'agit du paramètre par défaut du bloc logique OR.

Pour sélectionner le type de logique souhaité (normal ou reset), utilisez le menu **Type de logique** dans la page **Propriétés OR**.

*Illustration 94. **Propriétés OR***



NAND (NON-ET)

	Entrée 1	Entrée 2	Sortie
 (États-Unis)  (Union européenne)	0	x	1
La valeur de sortie est basée sur l'inversion du ET logique de 2 à 5 entrées.	x	0	1
La sortie est désactivée (Off) quand toutes les entrées sont activées.	1	1	0

NOR (NON-OU)

	Entrée 1	Entrée 2	Sortie
 (États-Unis)  (Union européenne)	0	0	1
La valeur de sortie est basée sur l'inversion du OR logique de 2 à 5 entrées.	1	x	0
La sortie est activée (On) quand toutes les entrées sont désactivées.	x	1	0

XOR (OU exclusif)

	Entrée 1	Entrée 2	Sortie
 (États-Unis)  (Union européenne)	0	0	0
	0	1	1
La valeur de sortie est un OR exclusif de 2 à 5 entrées.	1	0	1
La sortie est activée (On) quand une seule entrée (exclusive) est activée.	1	1	0

NOT (NON)

	Entrée	Sortie
 (États-Unis)  (Union européenne)	0	1
La sortie est l'inverse de l'entrée.	1	0

Bascule RS

	Entrée 1 (Set)	Entrée 2 (Reset)	Sortie
	0	0	La valeur reste identique.
	0	1	0 (Reset)
Ce bloc est à reset « dominant » (le reset est prioritaire si les deux entrées sont actives).	1	0	1 (Set)
	1	1	0 (le reset a la priorité)

Bascule SR

	Entrée 1 (Set)	Entrée 2 (Reset)	Sortie
	0	0	La valeur reste identique.
	0	1	0 (Reset)
Ce bloc est à activation (Set) « dominante » (l'activation a la priorité si les deux entrées sont activées ON).	1	0	1 (Set)
	1	1	1 (l'activation (Set) a la priorité)

10.6.2 Blocs fonction

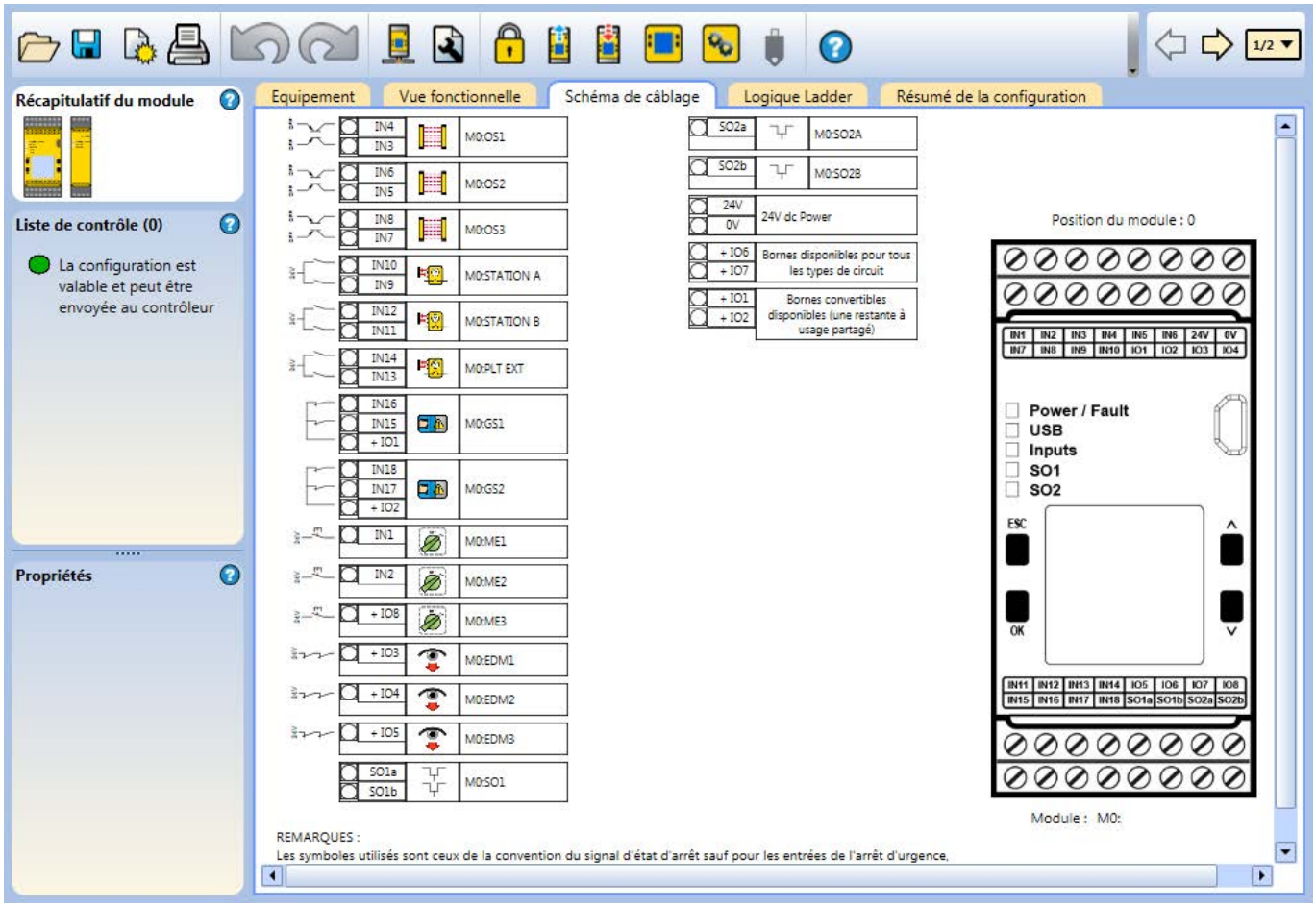
Les blocs fonction offrent des fonctionnalités intégrées pour la plupart des applications courantes dans un seul bloc. Bien qu'il soit possible de concevoir une configuration sans bloc fonction, l'utilisation des blocs fonction simplifie la configuration, facilite l'utilisation et offre des fonctionnalités plus complètes.

En règle générale, il est nécessaire de connecter à la plupart des blocs fonction le dispositif d'entrée de sécurité correspondant. La liste de contrôle à gauche génère une notification en cas de connexions manquantes. Selon l'application, certains blocs fonction peuvent être connectés à d'autres blocs fonction et/ou des blocs logiques.

Les dispositifs d'entrée de sécurité double voie possèdent des lignes de signal distinctes. Les signaux double voie de certains dispositifs sont tous deux positifs (+24 Vcc) lorsque ces dispositifs sont en état de marche. D'autres peuvent avoir un circuit complémentaire lorsqu'un canal a une tension de 24 Vcc et l'autre de 0 Vcc lorsque le dispositif est en état de marche. Dans ce manuel, par convention, on dit d'un dispositif d'entrée de sécurité qu'il est en état de marche ou arrêt au lieu de dire qu'il est activé (On, 24 Vcc) ou désactivé (Off, 0 Vcc).

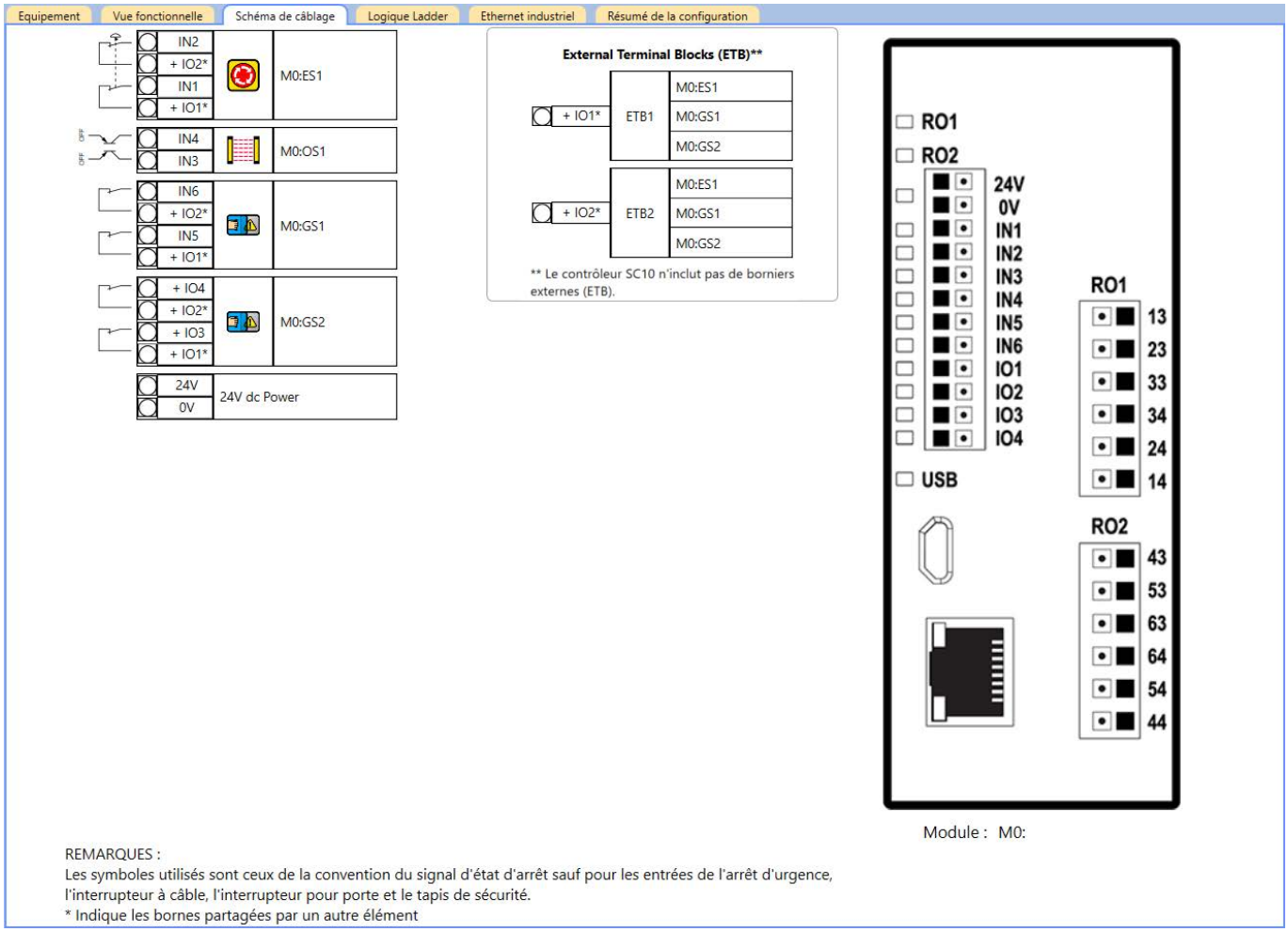
10.7 Onglet Schéma de câblage

*Illustration 95. Onglet **Schéma de câblage** — XS26*



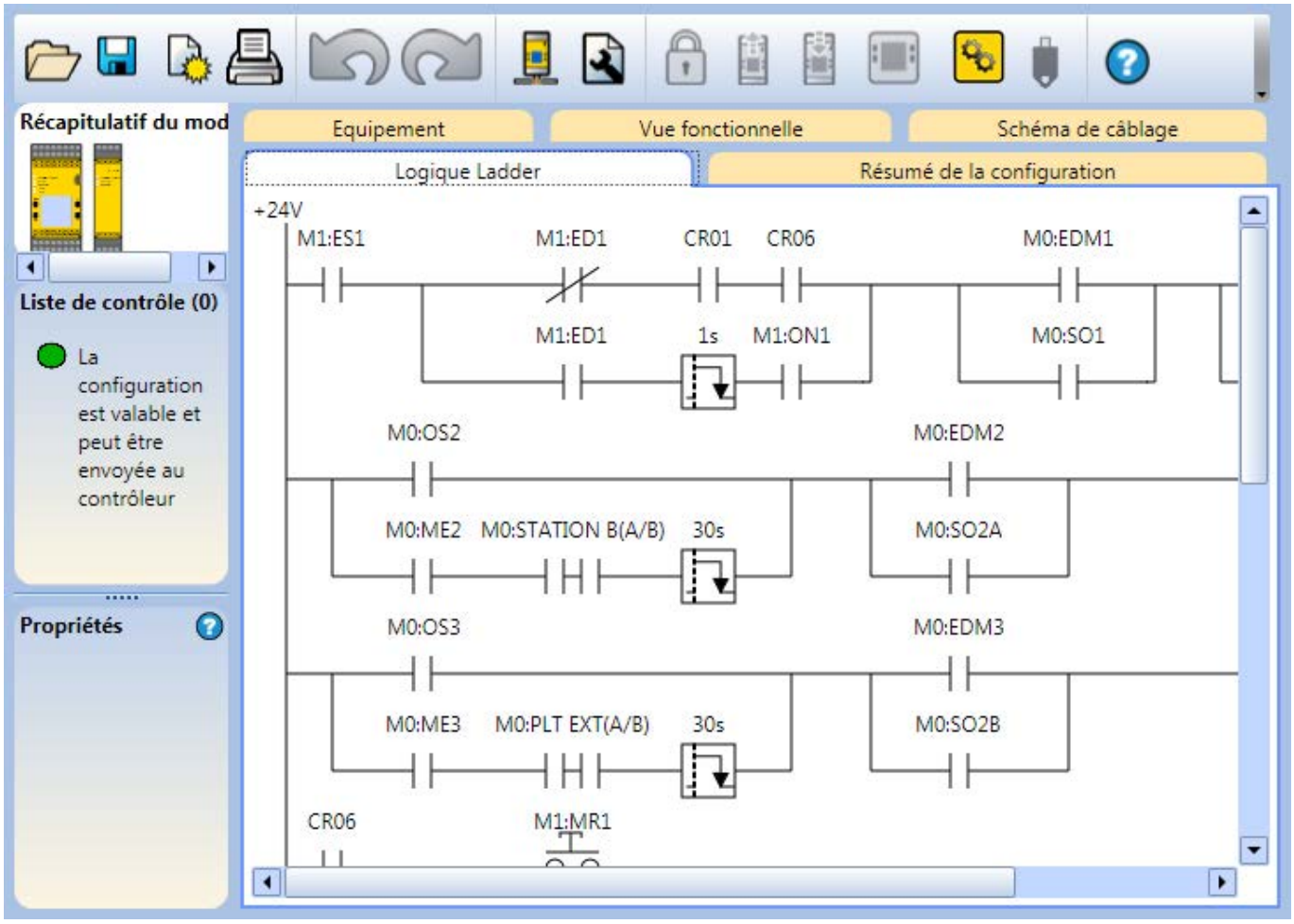
La vue **Schéma de câblage** affiche les assignations de bornes et les circuits électriques des entrées de sécurité et des entrées auxiliaires, des sorties de sécurité et des sorties d'état ainsi que toutes les bornes encore disponibles sur le module sélectionné. Utilisez le schéma de câblage comme guide pour raccorder physiquement les dispositifs. Naviguez entre les modules à l'aide de la barre d'outils de navigation de pages dans le coin supérieur droit du logiciel.

*Illustration 96. Onglet **Schéma de câblage** — SC10-2 avec borniers externes*



10.8 Onglet Logique Ladder

*Illustration 97. Onglet **Logique Ladder***



L'onglet **Logique Ladder** affiche un rendu logique de relais simplifié de la configuration.

10.9 Onglet ISD

*Illustration 98. Onglet SC10-2 du **SC10-2***

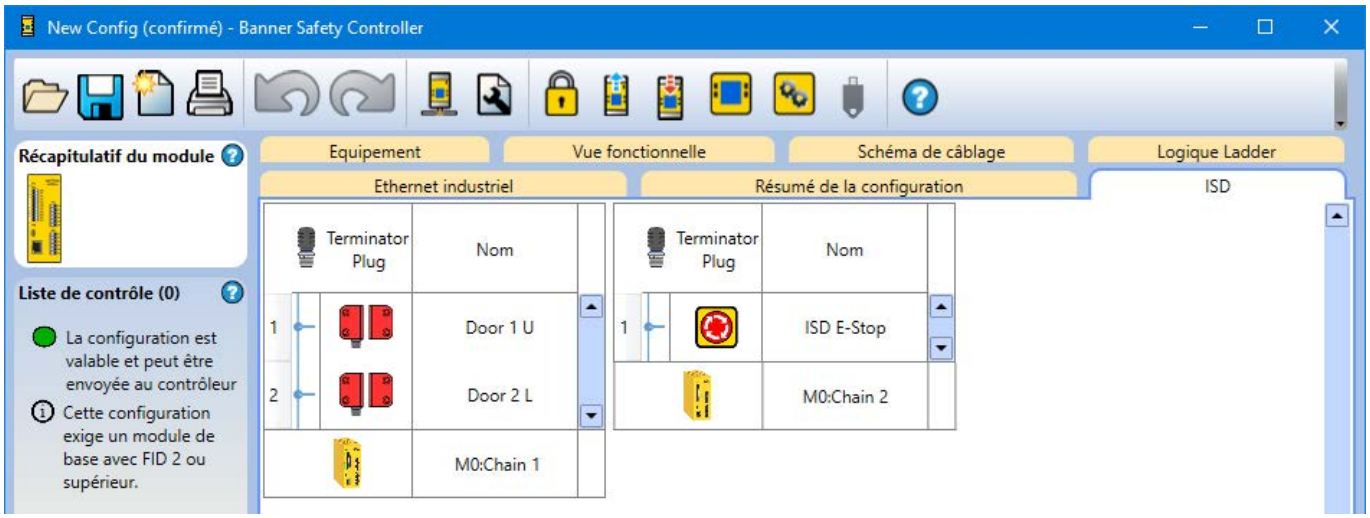
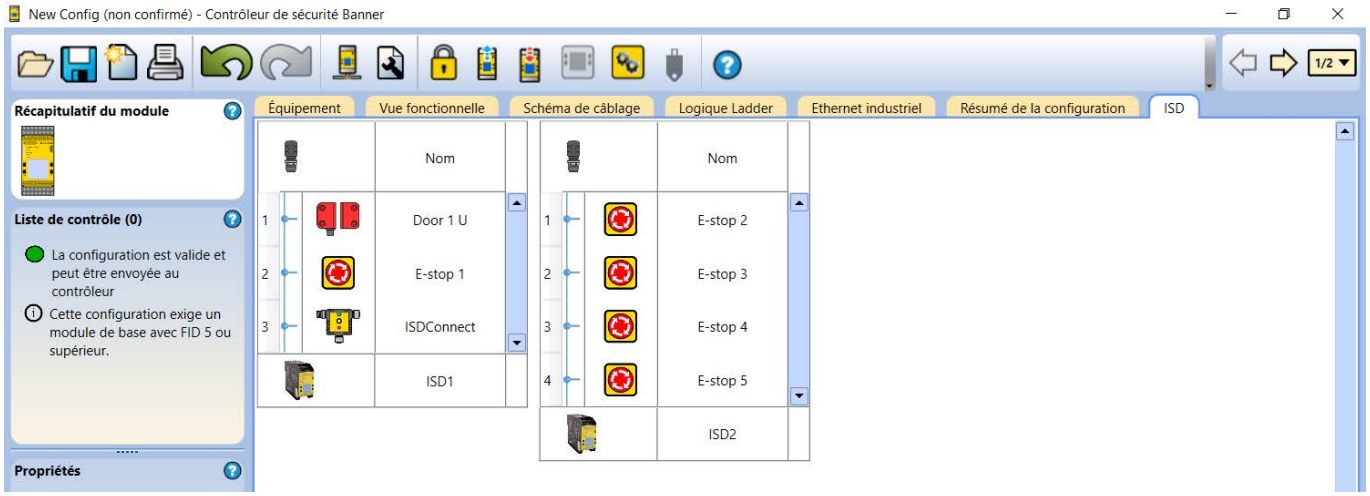


*Illustration 99. Onglet **ISD** du XS26-ISD*



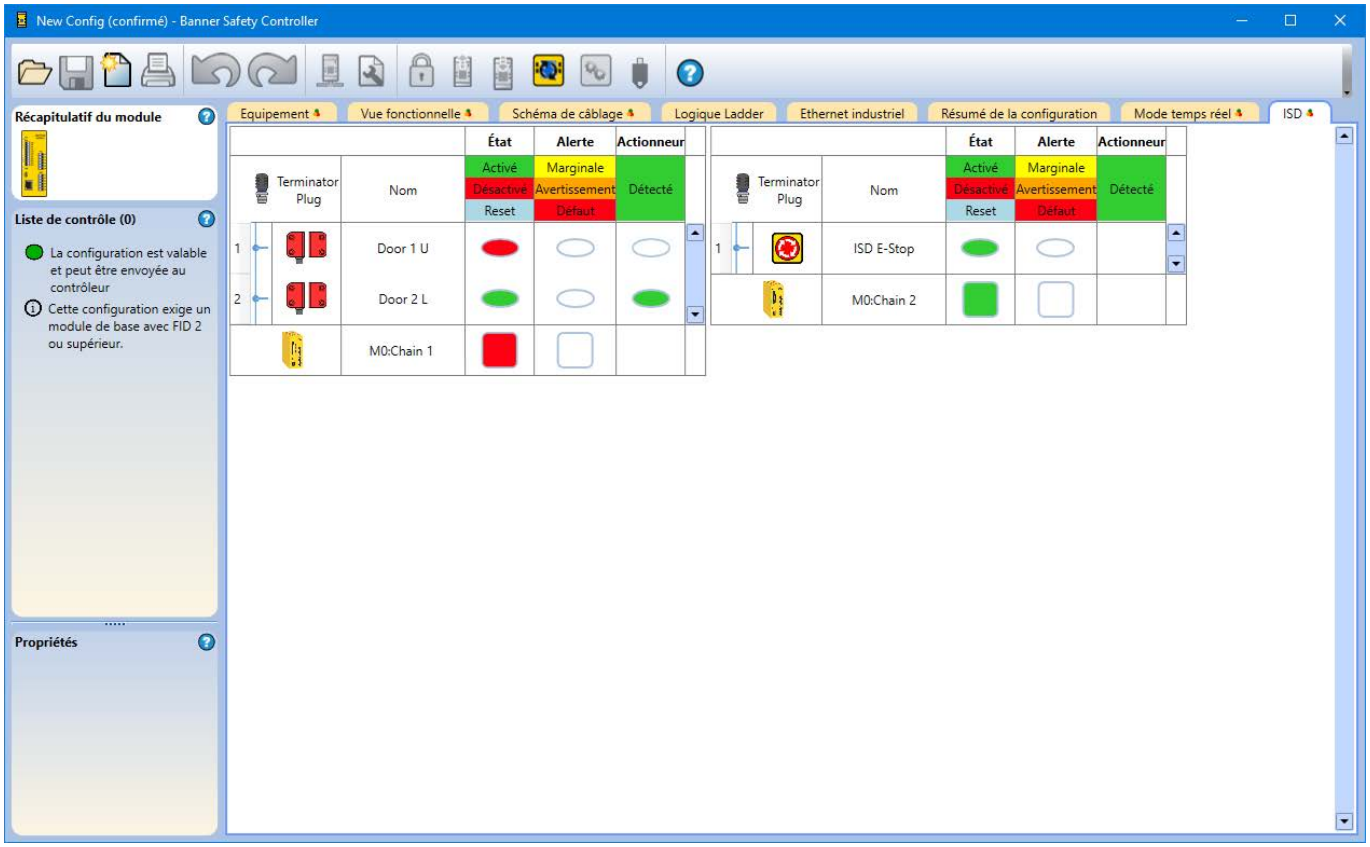
L'onglet **ISD** affiche l'ordre et les noms des dispositifs ISD connectés dans chaque chaîne ISD.

Pour les modèles XS26-ISD avec plus de deux chaînes, utilisez les flèches en haut à droite pour voir les chaînes supplémentaires.

En mode temps réel, l'onglet **ISD** affiche des informations en temps réel (actualisées environ toutes les unes à trois secondes) sur les dispositifs connectés. Dans l'exemple suivant, un interrupteur de porte est ouvert, comme indiqué par l'indicateur rouge, ou l'état Off, et l'indicateur sans couleur sous Actionneur.

Remarque: Il y a un retard de démarrage des données d'environ 10 secondes.

*Illustration 100. Onglet **ISD** en mode temps réel avec un interrupteur ouvert*

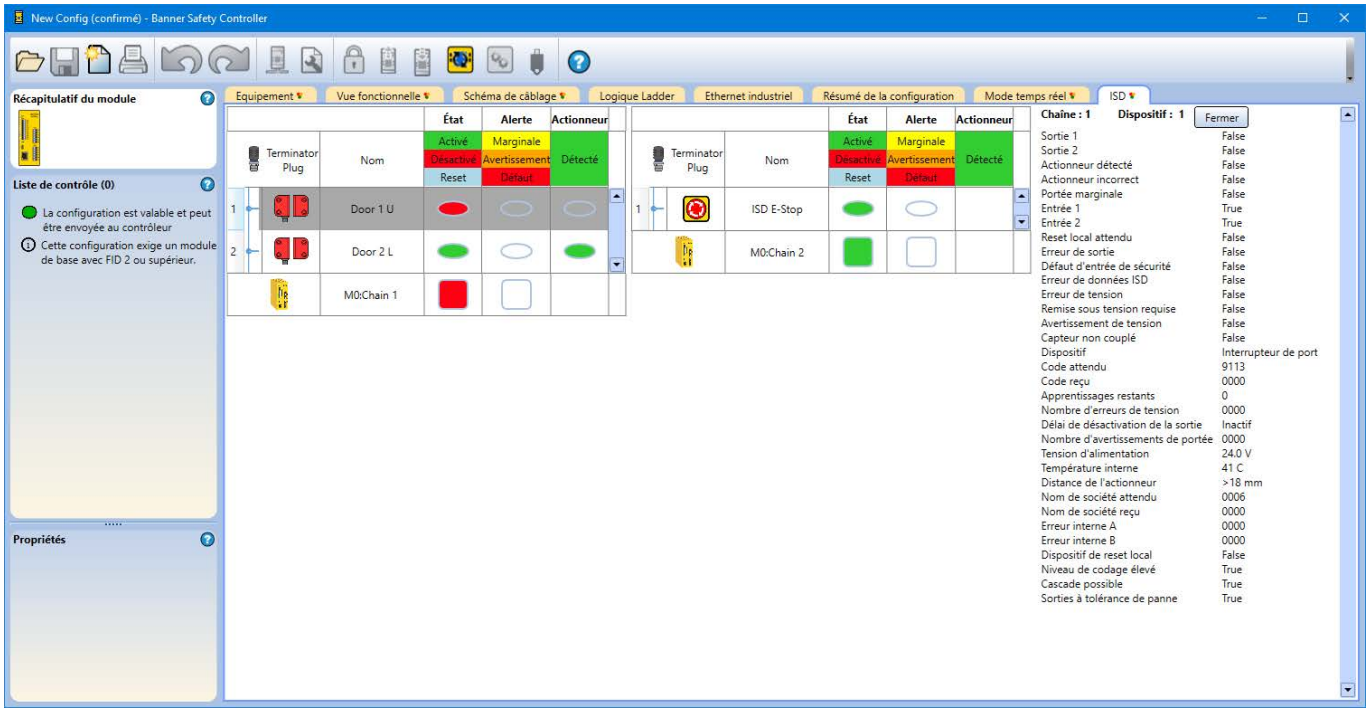


Lorsque les dispositifs ISD sont saisis manuellement, le dispositif 1 est positionné le plus près du connecteur de terminaison dans l'onglet **ISD**. Les numéros des dispositifs augmentent à mesure qu'ils se rapprochent du contrôleur.

Lorsque l'option **Détection auto ISD** est sélectionnée, le dispositif 1 est placé le plus près du contrôleur dans l'onglet **ISD**. Les chiffres augmentent à mesure qu'ils s'éloignent du contrôleur, vers le connecteur de terminaison. Cela part de l'hypothèse que la plupart des changements apportés à la longueur de la chaîne interviennent au niveau du connecteur de terminaison de la chaîne.

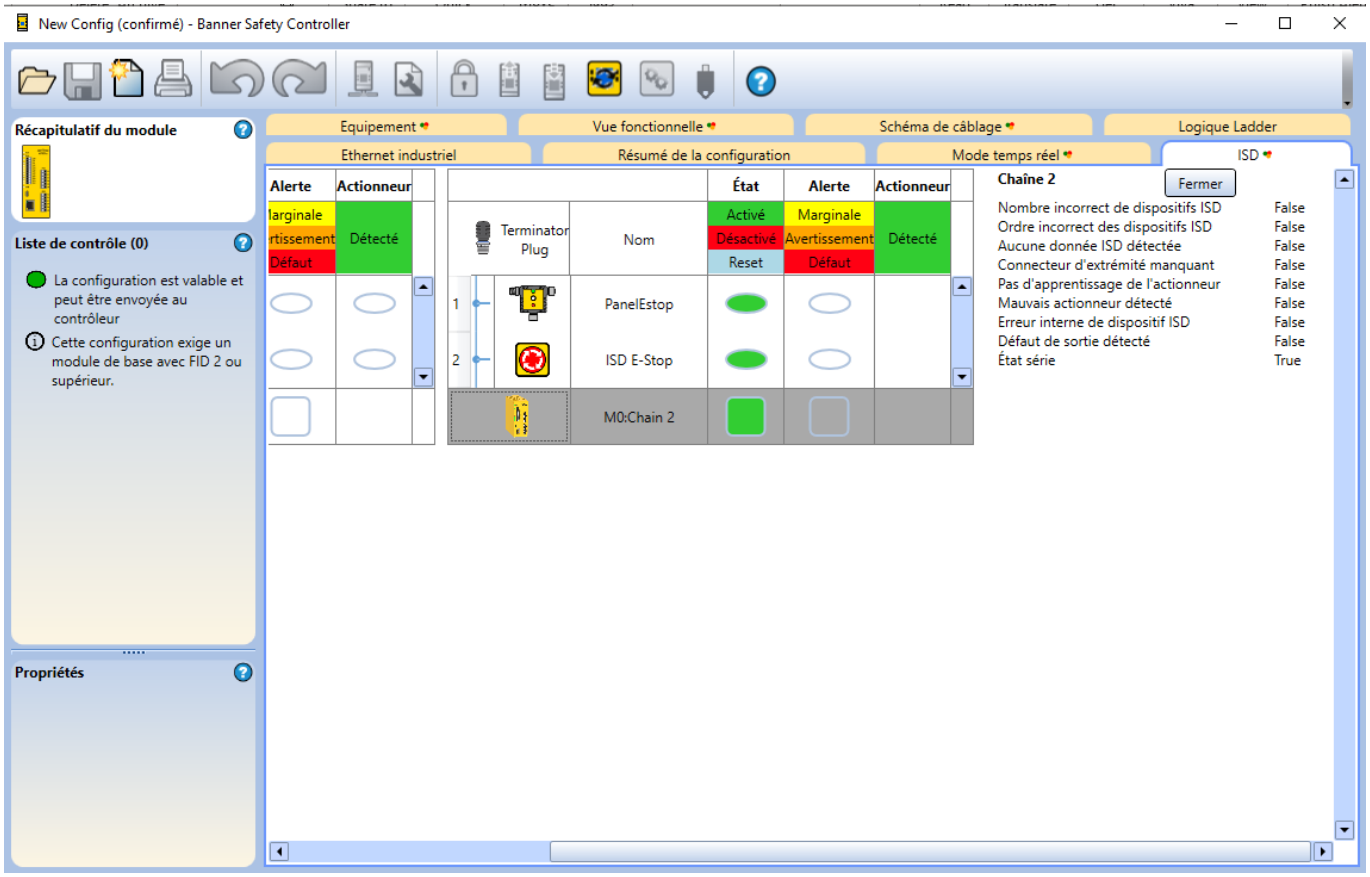
En mode temps réel, cliquez sur un dispositif pour afficher des données de diagnostic sur celui-ci. Les données incluent des informations sur l'entrée, la sortie et indiquent si l'actionneur est détecté.

*Illustration 101. Onglet **ISD** en mode temps réel avec des données de diagnostic*



En mode temps réel, cliquez sur le nom d'une chaîne pour afficher les données de diagnostic de la chaîne.

*Illustration 102. Onglet **ISD** en mode temps réel avec des données de chaîne*



10.10 Onglet Ethernet industriel

*Illustration 103. Onglet **Ethernet industriel** XS/SC26 — Sorties d'état virtuelles*

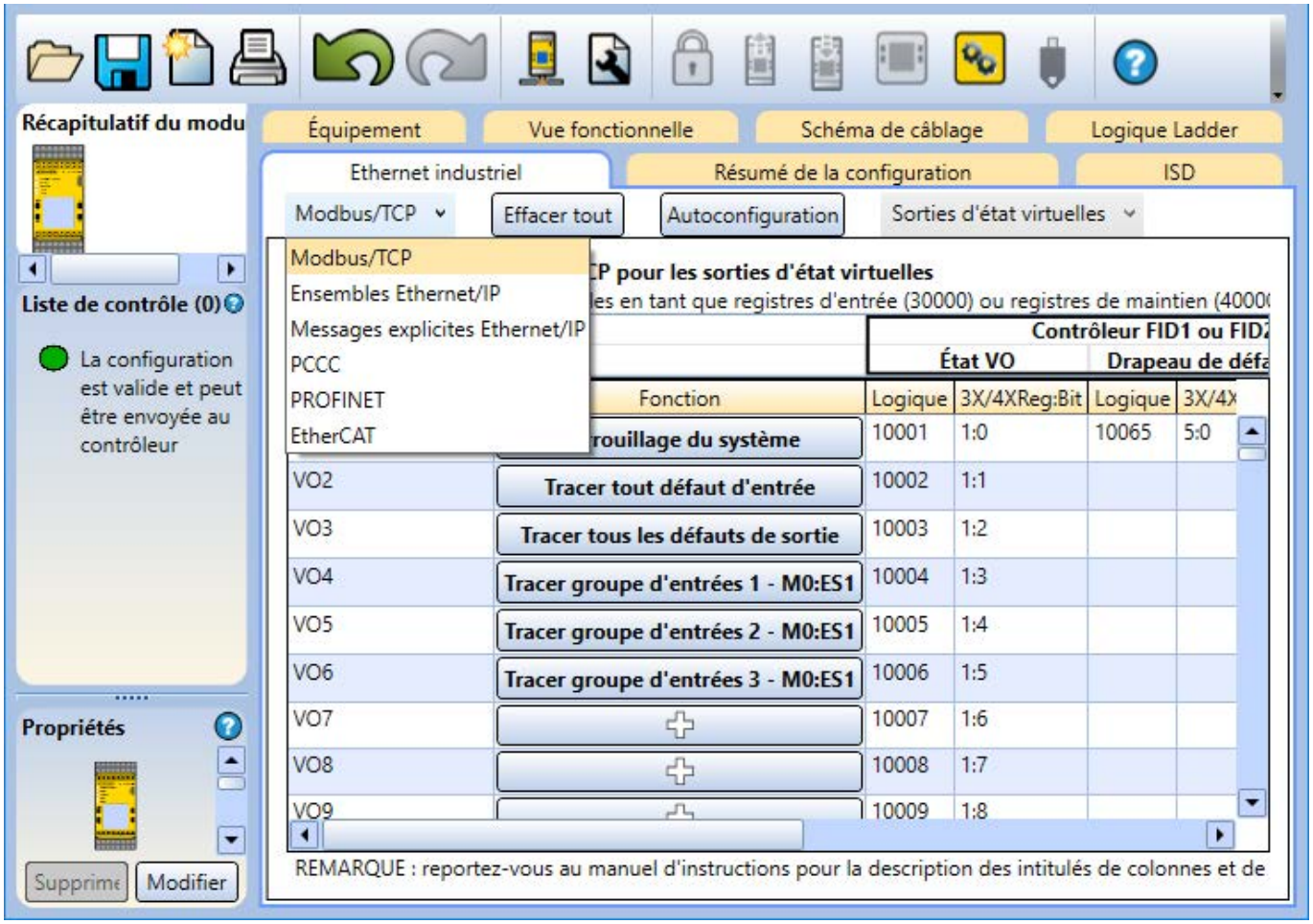
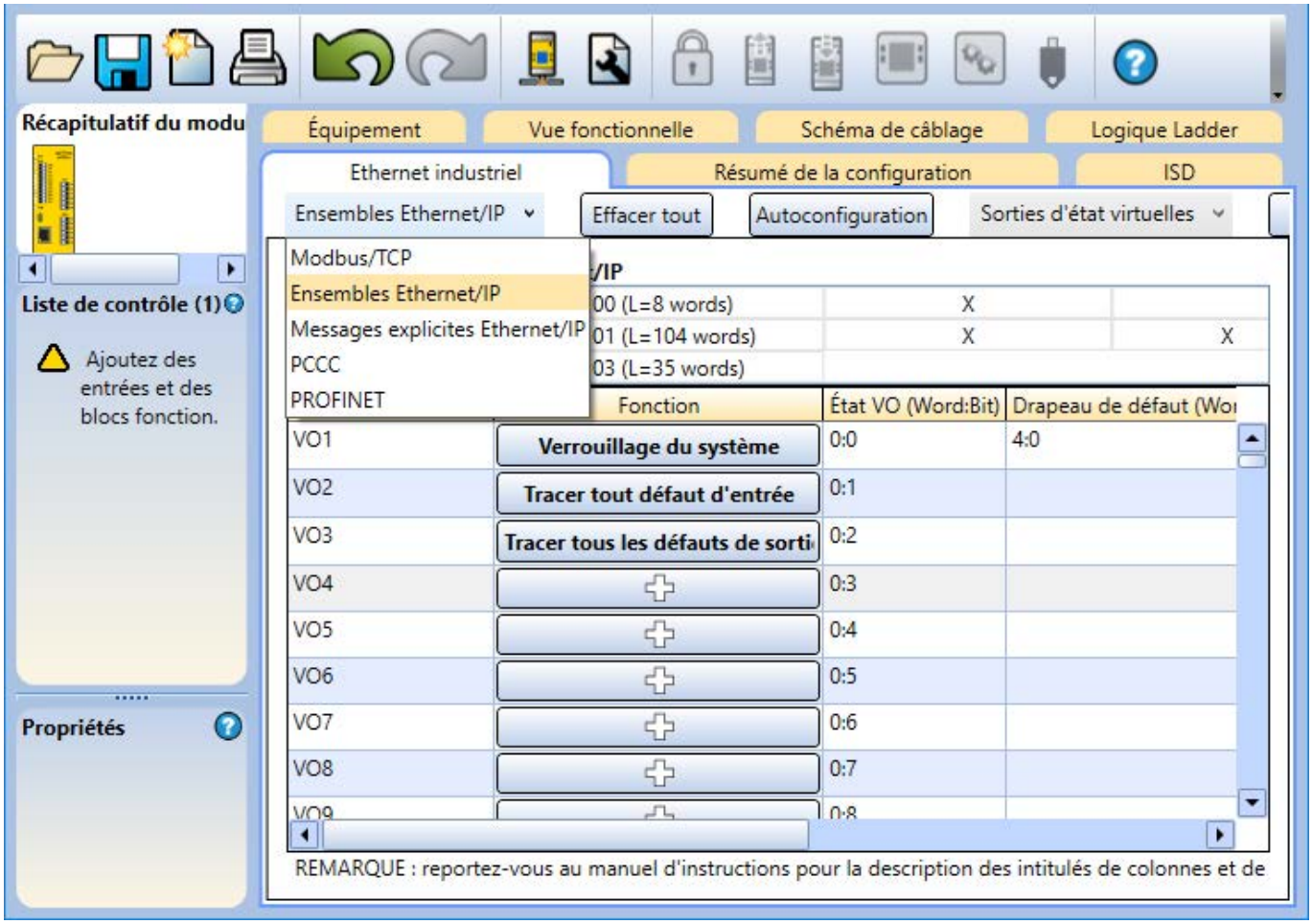


*Illustration 104. Onglet **Ethernet industriel** SC10-2 — Sorties d'état virtuelles*



L'onglet **Ethernet industriel** permet de configurer les sorties d'état virtuelles, lesquelles offrent les mêmes fonctions que les **sorties d'état** (ajoutées dans l'onglet **Équipement**) sur le réseau (voir les sections Conventions pour les signaux d'état des sorties à la page 81 et Fonctions des sorties d'état à la page 82 pour en savoir plus). Il est possible d'ajouter jusqu'à 64 sorties d'état virtuelles à l'aide des protocoles Modbus TCP, assemblys d'entrées EtherNet/IP, messages explicites EtherNet/IP et PCCC sur des contrôleurs de sécurité XS/SC26 FID 1 et jusqu'à 256 sorties d'état virtuelles sur des contrôleurs de sécurité XS/SC26 FID 2 ou ultérieur et des contrôleurs de sécurité SC10-2. Les contrôleurs de base FID 2 ou ultérieur et les contrôleurs de sécurité SC10-2 peuvent également utiliser PROFINET. Les contrôleurs de base XS26 Ethernet extensibles FID 6 ou ultérieurs peuvent également utiliser EtherCAT lorsque la passerelle de communication XSeCAT est ajoutée.

Pour accéder à l'onglet **Ethernet industriel** :

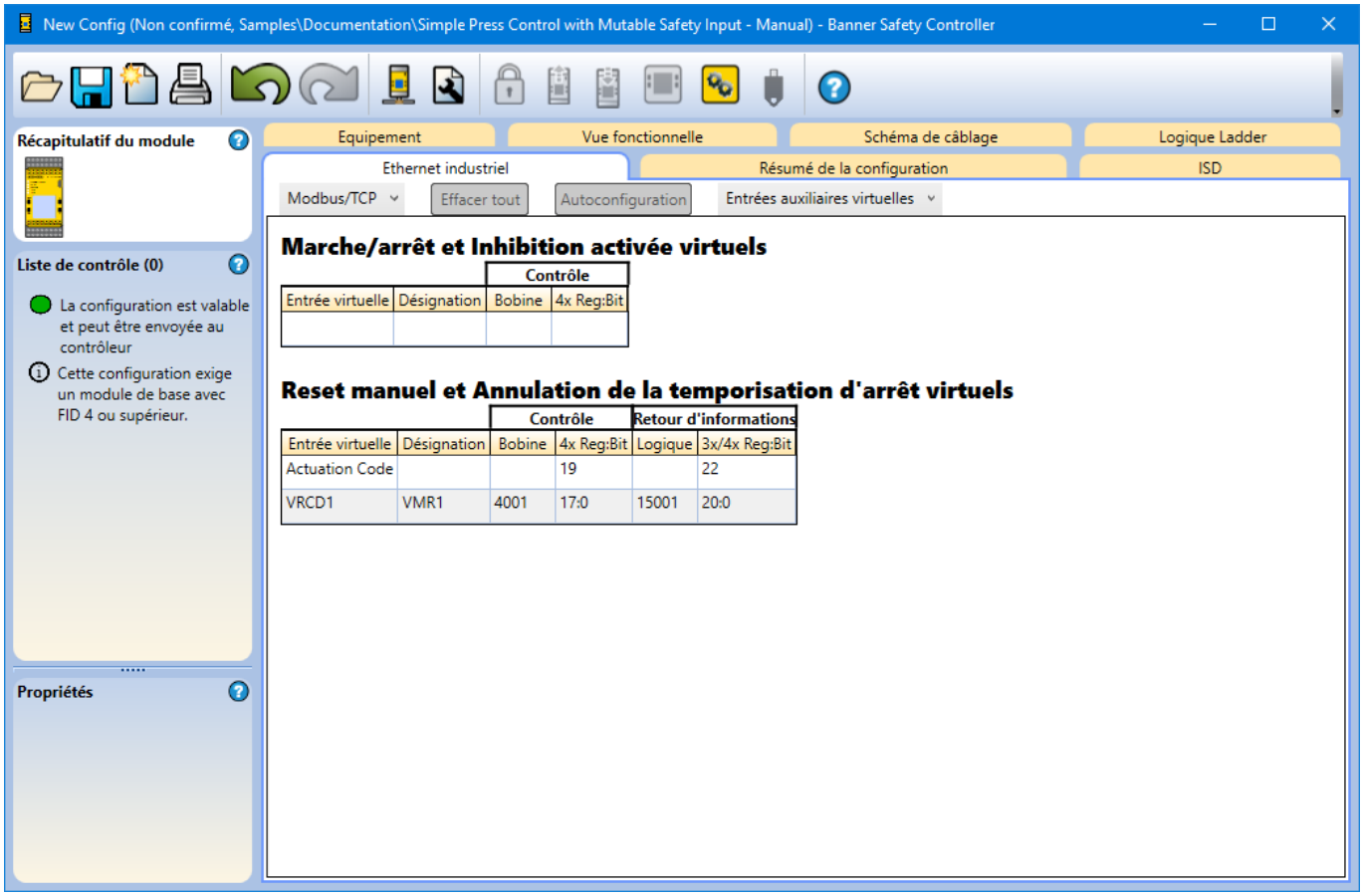
1. Cliquez sur **Paramètres réseau**.
2. Sélectionnez **Activer l'interface réseau**.
3. Dans l'onglet **Ethernet industriel**, utilisez la liste déroulante pour sélectionner le protocole souhaité.
4. Modifiez certains paramètres, le cas échéant. Voir :
   - Paramètres réseau : Modbus TCP, Ethernet/IP, PCCC à la page 130
   - Paramètres réseau : PROFINET à la page 130
   - Paramètres réseau : EtherCAT à la page 131
5. Cliquez sur **OK**.

Utilisez la fonction **Autoconfiguration**, située dans l'onglet **Ethernet industriel** pour configurer automatiquement les sorties d'état virtuelles avec un ensemble de fonctions fréquemment utilisées, sur la base de la configuration actuelle.

Cliquez sur ✚ dans la colonne **Fonction** à côté d'une des cellules **VOx** pour ajouter manuellement une sortie d'état virtuelle. Il est possible de modifier les fonctions de toutes les sorties d'état virtuelles en cliquant sur le bouton portant le nom de la fonction de la sortie d'état virtuelle ou en cliquant sur **Modifier** sous le tableau **Propriétés** une fois que vous avez sélectionné VOx.

Pour afficher des informations sur les entrées auxiliaires virtuelles, sélectionnez **Entrées auxiliaires virtuelles** dans le menu déroulant en haut à droite.

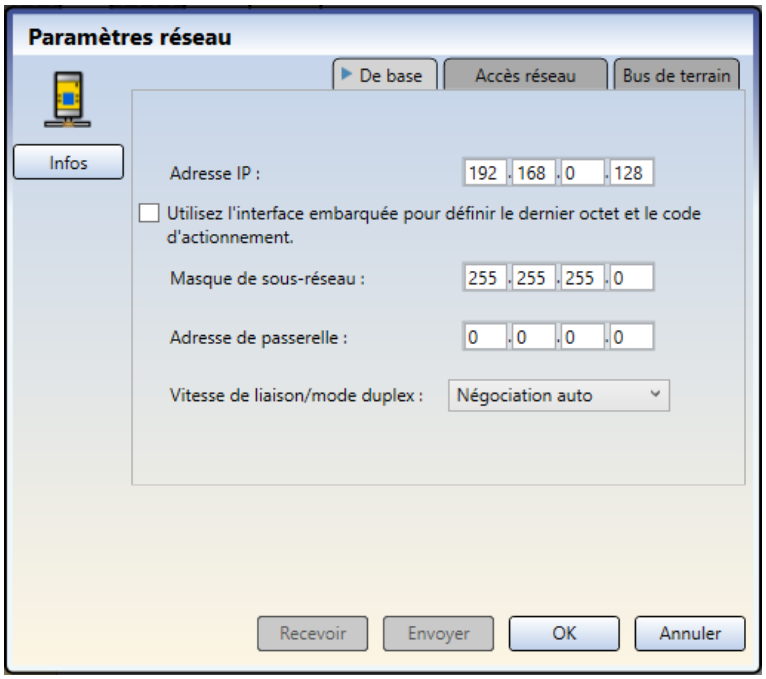
Illustration 105. Onglet Ethernet industriel — Entrées auxiliaires virtuelles



10.10.1 Paramètres réseau : Onglet Base

Cliquez sur **Paramètres réseau** pour ouvrir la fenêtre **Paramètres réseau**. L'onglet **Base** s'affiche.

*Illustration 106. Paramètres réseau : Onglet **Base***



Définissez l'adresse IP directement dans la fenêtre Paramètres réseau en saisissant les informations souhaitées comme indiqué dans la section Table 7 à la page 129. La case à cocher **Utilisez l'interface embarquée pour définir le dernier octet et le code d'actionnement** vous permet de définir les informations de base de l'adresse IP, mais de finaliser le

dernier octet (et le code d'actionnement, le cas échéant) lorsque l'unité est installée. Référez-vous à la section Processus Clickset IP à la page 180.

Remarque: Utilisez le **Gestionnaire de mots de passe** pour autoriser ou interdire à Utilisateur2 et Utilisateur3 de modifier les paramètres réseau.

Cliquez sur **Envoyer** pour écrire les paramètres réseau sur le contrôleur de sécurité. Les paramètres réseau et les paramètres de configuration sont envoyés séparément. Pour SC26-2 et XS/SC26 FID 3 ou ultérieur, les paramètres réseau sont automatiquement envoyés uniquement si le contrôleur de sécurité est un contrôleur de sécurité avec une configuration d'usine.

Table 7. Paramètres réseau par défaut

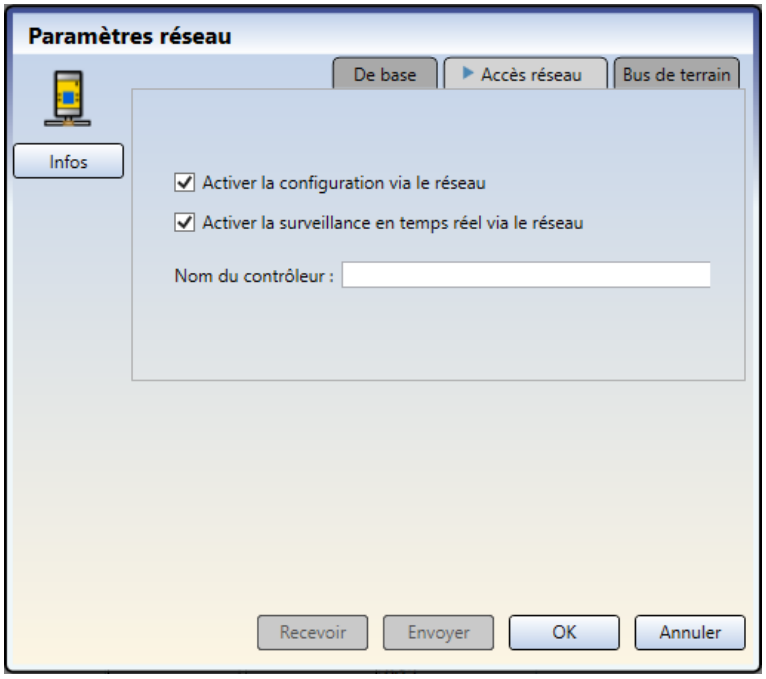
Nom du paramètre	Valeur d'usine par défaut
Adresse IP	192.168.0.128
Masque de sous-réseau	255.255.255.0
Adresse de passerelle	0.0.0.0
Vitesse de liaison et mode duplex	Négociation auto

Notez que l'onglet **Base** de l'écran Paramètres réseau est vide pour PROFINET car l'adressage est effectué via l'API.

10.10.2 Paramètres réseau : onglet Accès réseau

Utilisez l'onglet **Accès réseau** pour spécifier si les options Configuration via le réseau et Surveillance en temps réel via le réseau sont disponibles.

*Illustration 107. Paramètres réseau : onglet **Accès réseau***



Les modèles compatibles Ethernet XS26 FID 7 ou ultérieur peuvent être configurés via le port Ethernet (Configuration via le réseau) et surveillés en temps réel via le port Ethernet (Surveillance en temps réel via le réseau). Sélectionnez ou décochez les cases à cocher Configuration via le réseau et Surveillance en temps réel via le réseau dans l'onglet **Accès réseau** pour activer ou désactiver ces fonctionnalités.

Utilisez le champ **Nom du contrôleur** pour donner au contrôleur de sécurité un nom qui s'affiche dans la fenêtre **Contrôleurs disponibles**. Le nom a une limite de 31 caractères.

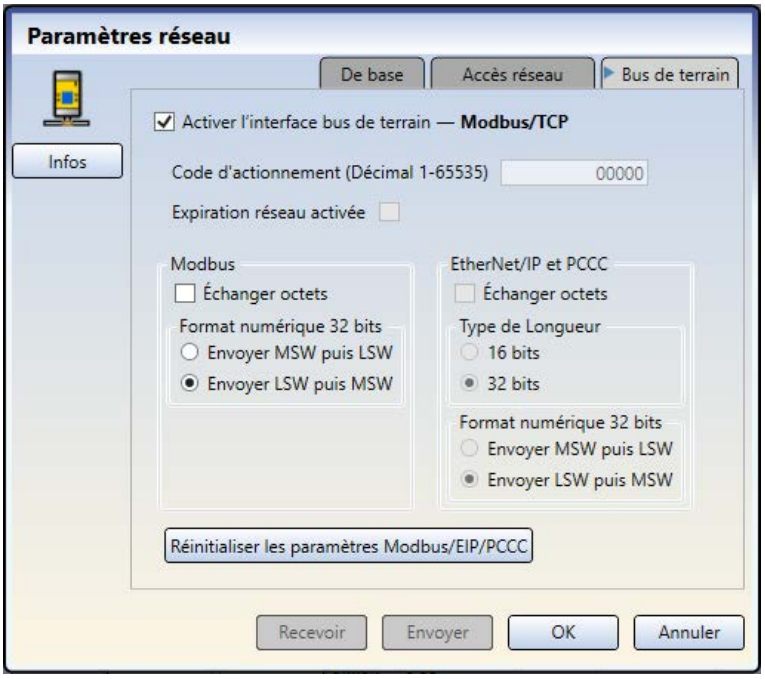
10.10.3 Paramètres réseau : onglet Bus de terrain

Utilisez l'onglet **Bus de terrain** pour créer un code d'actionnement et/ou définir d'autres informations de configuration pour Modbus TCP et Ethernet/IP.

Paramètres réseau : Modbus TCP, Ethernet/IP, PCCC

Dans le cas d'une connexion Modbus TCP, les spécifications prévoient l'utilisation du port 502 comme port TCP par défaut. Cette valeur n'est pas affichée dans la fenêtre **Paramètres réseau**.

*Illustration 108. **Paramètres réseau** — Onglet **Bus de terrain***



Cochez ou décochez la case **Activer l'interface de bus de terrain** pour activer ou désactiver l'interface de bus de terrain.

Un **code d'actionnement** est requis pour les configurations incluant une entrée virtuelle de reset ou d'annulation de la temporisation. L'entrée virtuelle de reset manuel ou d'annulation de temporisation doit être ajoutée pour activer le champ **Code d'actionnement**.

L'option **Bus de terrain** permet une configuration plus précise des paramètres Modbus TCP et EtherNet/IP, notamment grâce à des options telles que « Échanger les octets de caractère », « Envoyer LSW puis MSW », « Envoyer MSW puis LSW » et « Type de longueur de chaîne » (EtherNet/IP et PCCC).

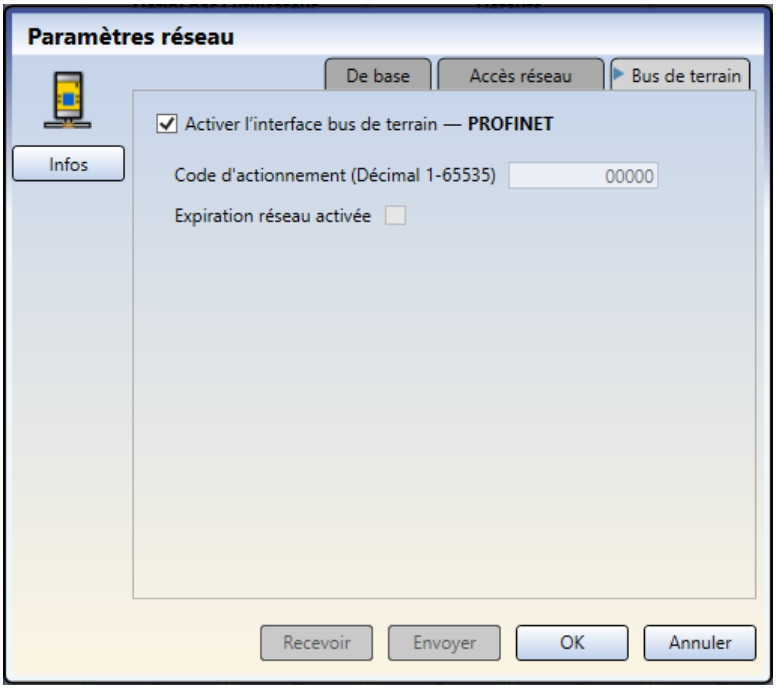
Cliquez sur **Expiration réseau activée** pour que tous les paramètres Marche/arrêt virtuel et Inhibition virtuelle activée soient désactivés en cas d'expiration réseau. Le temps d'expiration réseau est défini sur 5 secondes.

Cliquez sur **Envoyer** pour écrire les paramètres réseau sur le contrôleur de sécurité. Les paramètres réseau et les paramètres de configuration sont envoyés séparément. Pour SC26-2 et XS/SC26 FID 3 ou ultérieur, les paramètres réseau sont automatiquement envoyés uniquement si le contrôleur de sécurité est un contrôleur de sécurité avec une configuration d'usine.

Paramètres réseau : PROFINET

Après avoir sélectionné le protocole PROFINET dans l'onglet **Ethernet industriel**, cliquez sur **Paramètres réseau** pour ouvrir la fenêtre **Paramètres réseau**. PROFINET est disponible sur XS/SC26 FID 2 ou ultérieur et SC10-2.

*Illustration 109. **Paramètres réseau** — PROFINET*



Cliquez sur **Expiration réseau activée** pour que tous les paramètres Marche/arrêt virtuel et Inhibition virtuelle activée soient désactivés en cas d'expiration réseau. Le temps d'expiration réseau est défini sur 5 secondes.

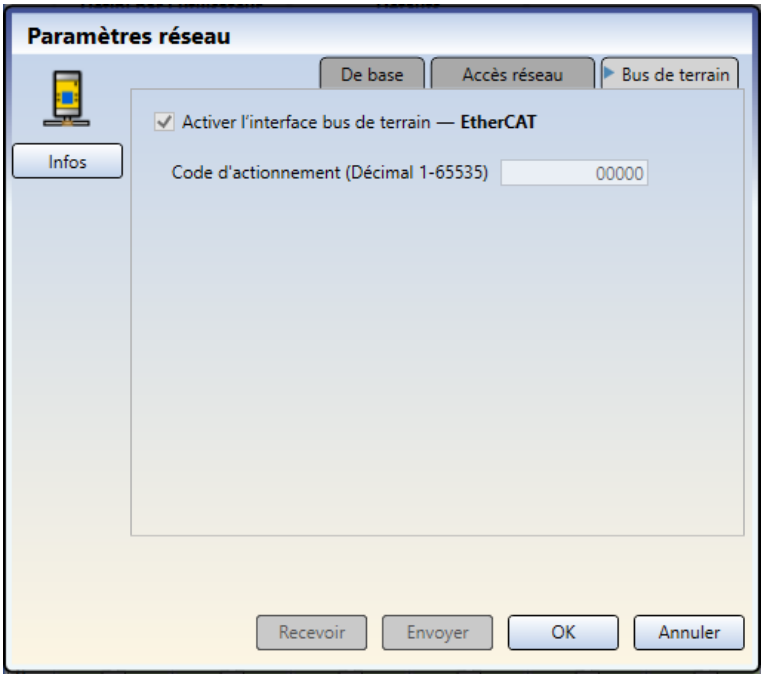
Cliquez sur **Envoyer** pour écrire les paramètres réseau sur le contrôleur de sécurité. Les paramètres réseau et les paramètres de configuration sont envoyés séparément. Pour SC10-2 et XS/SC26 FID 3 ou ultérieur : les paramètres réseau sont automatiquement envoyés uniquement si le contrôleur de sécurité est un contrôleur de sécurité avec une configuration d'usine. Notez que l'onglet **Base** de l'écran Paramètres réseau est vide pour PROFINET car l'adressage est effectué via l'API.

Remarque: Utilisez le **Gestionnaire de mots de passe** pour autoriser ou interdire à Utilisateur2 et Utilisateur3 de modifier les paramètres réseau.

Paramètres réseau : EtherCAT

Après avoir ajouté la passerelle de communication XSeCAT, le protocole EtherCAT dans l'onglet **Ethernet industriel** est le protocole figurant sous **Paramètres réseau**. Cliquez sur **Paramètres réseau** pour ouvrir la fenêtre **Paramètres réseau**. EtherCAT est disponible sur les contrôleurs de base XS26 FID 6 ou ultérieur avec une passerelle de communication XSeCAT ajoutée.

Illustration 110. Paramètres réseau — EtherCAT



Cliquez sur **Envoyer** pour écrire les paramètres réseau sur le contrôleur de sécurité. Les paramètres réseau et les paramètres de configuration sont envoyés séparément. Les paramètres réseau sont automatiquement envoyés uniquement s'il s'agit d'un contrôleur de sécurité avec une configuration d'usine. L'onglet **Base** est vide pour EtherCAT car l'adressage est effectué via l'API.

Remarque: Cliquez sur **Recevoir** pour télécharger les paramètres à partir du contrôleur de sécurité connecté.

Remarque: Utilisez le **Gestionnaire de mots de passe** pour autoriser ou interdire à Utilisateur2 et Utilisateur3 de modifier les paramètres réseau.

10.10.4 Création de tags d'API / fichier d'étiquettes

Utilisez le logiciel Contrôleur de sécurité Banner pour générer un fichier.L5X, .csv ou.xml qui contient les noms de toutes les entrées et sorties d'état virtuelles.

Pour utiliser les noms créés dans le logiciel Contrôleur de sécurité Banner comme tags/étiquettes d'API, importez le fichier .L5X, .csv ou .xml dans le logiciel de l'API pour les API utilisant les assemblys Ethernet/IP, PROFINET ou EtherCAT.

Commencez par créer toutes les entrées et sorties d'état voulues dans le logiciel Contrôleur de sécurité Banner. Attribuez un code d'actionnement sous **Paramètres réseau**, le cas échéant. Ensuite, vérifiez que le protocole requis est sélectionné (Assemblys Ethernet/IP, PROFINET ou EtherCAT).

Fichier L5X

Le fichier .L5X est un fichier XML (eXtensilble Markup Language) qui stocke les données de la connexion EtherNet/IP et les descriptions des tags. L'exportation de ce fichier à partir du logiciel du contrôleur de sécurité et son importation dans le logiciel API RS Studio 5000 permettent d'établir une connexion EtherNet/IP entre l'API et le contrôleur de sécurité avec des descriptions de tags, le tout en une seule étape.

Fichier CSV

Pour utiliser le fichier CSV exporté pour étiqueter les descriptions des tags dans le programme de l'API, utilisez d'abord le fichier EDS pour créer la connexion EtherNet/IP entre l'API et le contrôleur de sécurité. Sélectionnez la même connexion pour la connexion du fichier EDS (par exemple, 8 chaînes ISD) et dans la fenêtre **Exporter vers CSV et L5X**. Ainsi, les étiquettes du fichier CSV exporté correspondront aux tags créés par le fichier EDS.

Voir :

- Création de fichiers L5X pour les assemblys Ethernet/IP à la page 183
- Contrôleur de sécurité Banner Installation du fichier EDS dans le logiciel ControlLogix à la page 187
- Création d'un fichier XML pour PROFINET à la page 272
- Créer un fichier PLCopenXML pour EtherCAT pour TwinCAT 3.0 à la page 300

10.10.5 EtherNet/IP - Objets assemblés

Remarque: Le fichier EDS peut être téléchargé sur le site www.bannerengineering.com. Pour des informations complémentaires, voir Présentation de l'Ethernet industriel (bus de terrain) à la page 179.

Objets Assembly d'entrée (T>O)

ID d'instance	Longueur des données (mots 16 bits)	Description
100 (0×64)	8	Permet d'accéder aux informations de base sur les sorties d'état virtuelles 1–64.
101 (0×65)	104	Permet d'accéder aux informations avancées (informations de base comprises) sur les sorties d'état virtuelles.
102 (0×66)	150	Permet d'accéder aux informations du journal des défauts sans fournir aucune information sur les sorties d'état virtuelles.
103 (0×67)	35	Permet d'accéder aux informations de base sur les sorties d'état virtuelles 1 - 256 et aux informations de retour sur les entrées Reset virtuel et Annulation de temporisation virtuelle. Disponible sur les contrôleurs de base FID 2 ou ultérieurs et le SC10-2.
104 (0×68)	112	Permet d'accéder aux informations de base sur les sorties d'état virtuelles 1 - 256, aux informations de retour sur les entrées Reset virtuel et Annulation de temporisation virtuelle et de prendre en charge les communications avec les dispositifs ISD avec une ou deux chaînes.
105 (0×69)	240	Permet d'accéder aux informations de base sur les sorties d'état virtuelles 1 - 256, aux informations de retour sur les entrées Reset virtuel et Annulation de temporisation virtuelle et de prendre en charge les communications avec les dispositifs ISD avec plus de deux chaînes.

Objet Assembly de sortie (O>T)

ID d'instance	Longueur des données (mots 16 bits)	Description
112 (0×70)	2	*Réservé*
113 (0×71)	11	Permet de commander les entrées virtuelles (On/Off, activation d'inhibition, reset et annulation de la temporisation). Disponible sur les contrôleurs de base FID 2 ou ultérieurs et le SC10-2.
114 (0×72)	14	Permet de commander les entrées virtuelles (On/Off, activation d'inhibition, reset et annulation de la temporisation) et de prendre en charge les communications avec les dispositifs ISD.

Objet Assembly de configuration

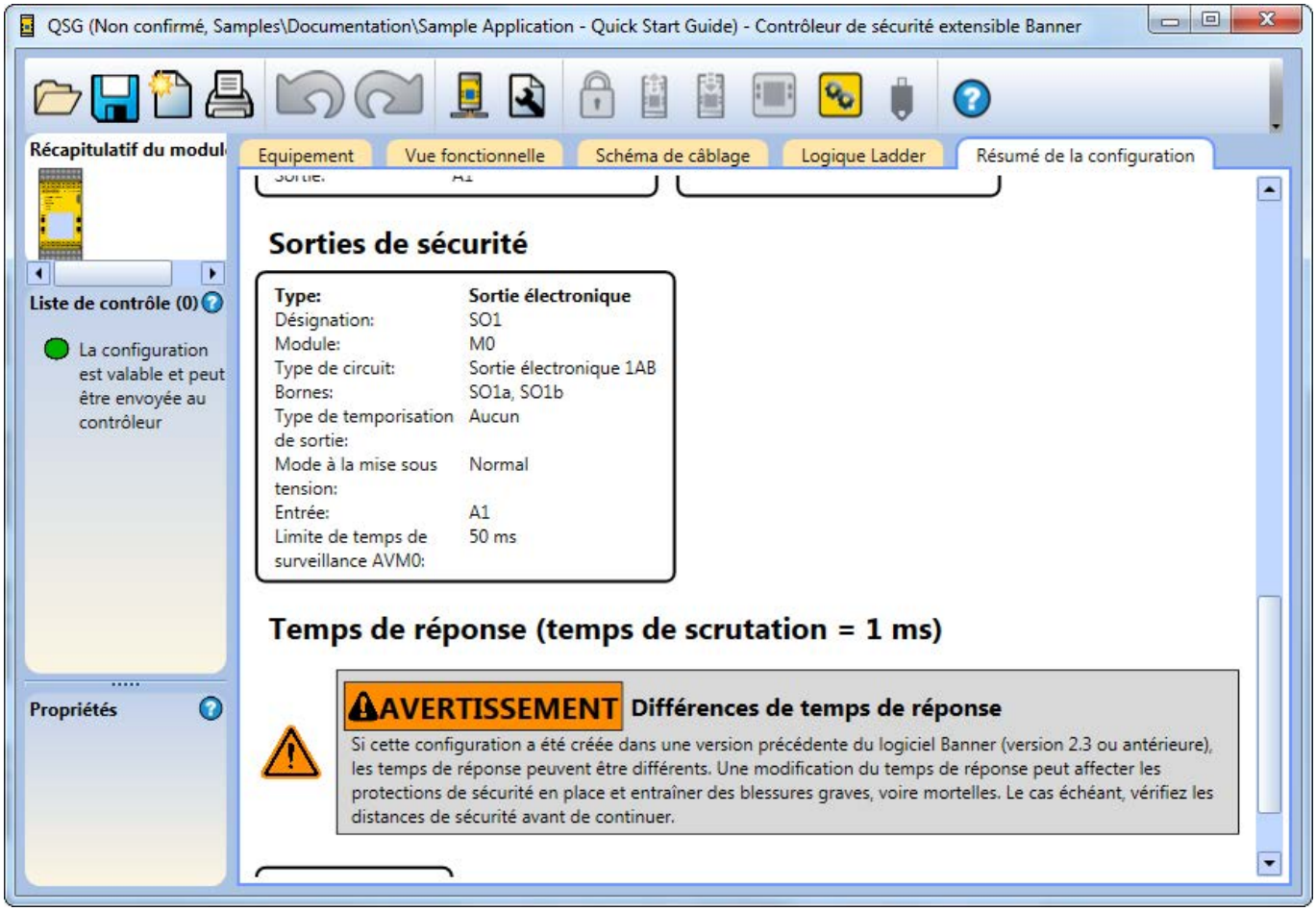
Cet objet n'est pas implémenté. Par contre, certains clients EtherNet/IP l'exigent. Si c'est le cas, utilisez l'ID d'instance 128 (0x80) avec une longueur de données de 0.

Affectez la valeur INT au type de données du format de communication.

Attribuez au RPI (intervalle demandé entre les paquets) une valeur de 150 minimum.

10.11 Onglet Résumé de la configuration

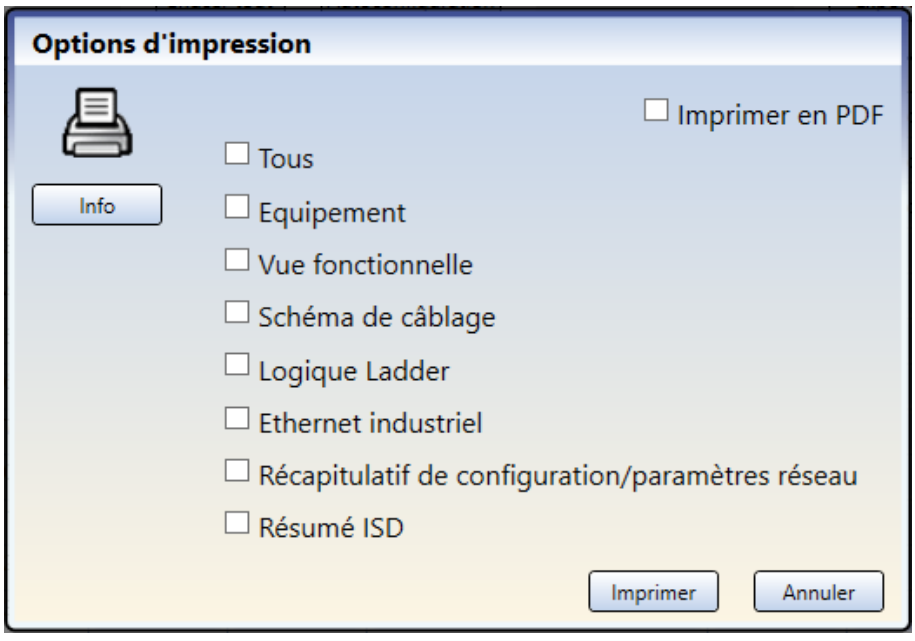
*Illustration 111. Onglet **Résumé de la configuration***



L'onglet **Résumé de la configuration** affiche au format texte des informations détaillées sur l'ensemble des entrées, blocs fonction et logiques, sorties de sécurité, sorties d'état configurés ainsi que les temps de réponse qui leur sont associés.

10.12 Options d'impression

Illustration 112. Options d'impression



Le logiciel propose plusieurs options d'impression de la configuration. Cliquez sur **Imprimer** dans la barre d'outils pour accéder à la fenêtre **Options d'impression**.

Les options d'impression suivantes sont disponibles :

- **Tous** — Imprime toutes les vues, y compris les **paramètres réseau** (dans les versions Ethernet)
- **Équipement** — Imprime l'onglet **Équipement**
- **Vue fonctionnelle** — Imprime l'onglet **Vue fonctionnelle**
- **Schéma de câblage** — Imprime l'onglet **Schéma de câblage**
- **Logique Ladder** — Imprime l'onglet **Logique Ladder**
- **Ethernet industriel** — Imprime l'onglet **Ethernet industriel**
- **Récapitulatif de configuration/paramètres réseau** — Imprime le **résumé de la configuration** et les **paramètres réseau** (si disponibles)
- **Résumé ISD** — Imprime l'onglet **ISD** (disponible sur les dispositifs SC10-2 FID 2 ou ultérieur et les dispositifs XS26-ISD FID 5 ou ultérieur)

Options d'impression :

- **Imprimer en PDF** — Imprime la sélection dans un fichier PDF stocké dans un emplacement défini par l'utilisateur
- **Imprimer** — Ouvre la boîte de dialogue d'impression par défaut de Windows et envoie la sélection vers l'imprimante définie par l'utilisateur

10.13 Gestionnaire des mots de passe

10.13.1 Gestionnaire des mots de passe du XS/SC26

Le gestionnaire des mots de passe est disponible lorsqu'un contrôleur de sécurité est connecté au PC via USB ou Ethernet (pour les modèles Ethernet XS/SC26 FID7 ou ultérieur). Les informations affichées dans le **Gestionnaire des mots de passe** proviennent du contrôleur de sécurité.

*Illustration 113. XS/SC26 **XS/SC26** — Onglet **Réseau** (logiciel v5.0 ou ultérieur avec un contrôleur FID 7 ou ultérieur)*

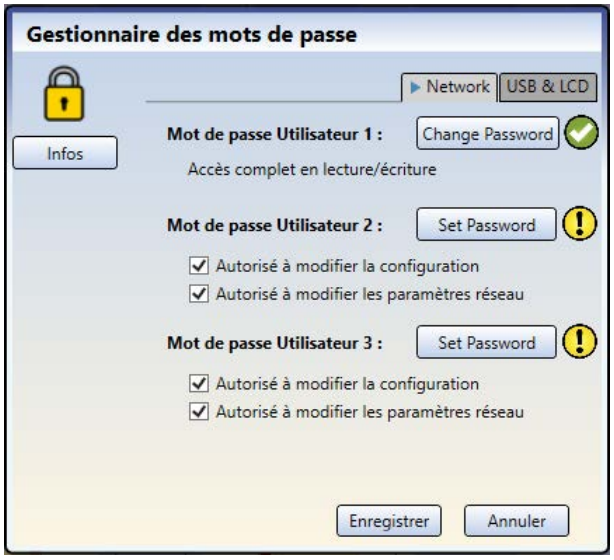


*Illustration 114. XS/SC26 **XS/SC26** — Onglet **USB/LCD***



Cliquez sur **Gestionnaire des mots de passe** dans la barre d'outils du logiciel pour modifier les droits d'accès à la configuration. Le contrôleur de sécurité peut stocker jusqu'à trois codes PIN utilisateur (pour USB) et jusqu'à trois mots de passe utilisateur (pour Ethernet) pour gérer les différents niveaux d'accès aux paramètres de configuration. Le mot de passe pour Utilisateur1 offre un accès complet en lecture-écriture et la possibilité de définir l'accès pour Utilisateur2 et Utilisateur3 (les noms d'utilisateur ne peuvent pas être modifiés). Les informations de base, notamment les paramètres réseau, les schémas de câblage et les informations de diagnostic sont accessibles sans code PIN/mot de passe. Une configuration stockée sur un PC ou une carte mémoire SC-XM2/3 n'est pas protégée par un mot de passe.

Utilisateur2 ou Utilisateur3 peut écrire la configuration sur le contrôleur de sécurité lorsque l'option **Autorisé à modifier la configuration** est activée. Ils peuvent modifier les paramètres réseau lorsque l'option **Autorisé à modifier les paramètres réseau** est activée. Pour la version 4.1 du logiciel ou une version antérieure, l'option **Autorisé à consulter la configuration** pour Utilisateur2 et Utilisateur3 est disponible et peut être activée si l'option **Demander un mot de passe pour consulter la configuration** pour Utilisateur1 est activée. Il leur faudra fournir leurs codes PIN/ mots de passe.

Cliquez sur **Enregistrer** pour écrire les informations des mots de passe sur le contrôleur de sécurité.

Seul Utilisateur1 peut rétablir les paramètres d'usine du XS/SC26.

Remarque: Les codes PIN par défaut pour Utilisateur1, Utilisateur2 et Utilisateur3 sont respectivement 1901, 1902 et 1903.

Le mot de passe Ethernet par défaut pour Utilisateur1 est 1901@Banner.

Il est vivement recommandé de remplacer les codes PIN/mots de passe par défaut par d'autres valeurs.

Si le mot de passe Ethernet par défaut n'est pas modifié, la possibilité de se connecter à un contrôleur avec le logiciel Contrôleur de sécurité Banner via Ethernet sera désactivée. Il s'agit d'une fonction automatique. Modifiez le mot de passe via USB ou Ethernet.

10.13.2 Gestionnaire des mots de passe du SC10-2

La fenêtre **Gestionnaire des mots de passe** est disponible quand un contrôleur de sécurité est connecté au PC via USB. Les informations affichées dans le **Gestionnaire des mots de passe** proviennent du contrôleur de sécurité.

*Illustration 115. **Gestionnaire des mots de passe** du SC10-2*



Cliquez sur **Gestionnaire des mots de passe** dans la barre d'outils du logiciel pour modifier les droits d'accès à la configuration. Le contrôleur de sécurité peut stocker jusqu'à trois codes PIN utilisateur pour gérer les différents niveaux d'accès aux paramètres de configuration. Le code PIN pour Utilisateur1 offre un accès complet en lecture-écriture et la possibilité de définir l'accès pour Utilisateur2 et Utilisateur3 (les noms d'utilisateur ne peuvent pas être modifiés). La configuration, les paramètres réseau, les schémas de câblage et les informations de diagnostic sont accessibles sans code PIN. Une configuration stockée sur un PC ou une carte mémoire SC-XM2/3 n'est pas protégée par un code PIN.

Utilisateur2 ou Utilisateur3 peut écrire la configuration sur le contrôleur de sécurité lorsque l'option **Autorisé à modifier la configuration** est activée. Ils peuvent modifier les paramètres réseau lorsque l'option **Autorisé à modifier les paramètres réseau** est activée. Leurs codes PIN respectifs seront nécessaires.

Cliquez sur **Enregistrer** pour appliquer les informations des codes PIN à la configuration active dans le logiciel et écrire les informations des codes PIN sur le contrôleur de sécurité.

Remarque: Les codes PIN par défaut pour Utilisateur1, Utilisateur2 et Utilisateur3 sont respectivement 1901, 1902 et 1903. Il est fortement recommandé de remplacer les codes PIN par défaut par d'autres valeurs.

Seul Utilisateur1 peut rétablir les paramètres d'usine du SC10-2.

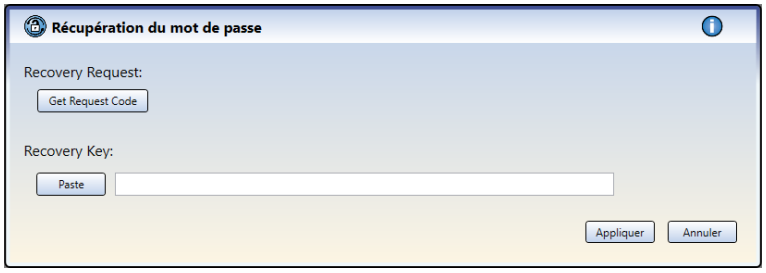
10.13.3 Récupération du code PIN ou du mot de passe

En cas d'oubli ou de perte du mot de passe du contrôleur de sécurité, suivez les instructions suivantes pour demander l'accès au contrôleur de sécurité.

Le contrôleur de sécurité doit être connecté à l'aide d'une connexion USB.

1. Connectez-vous au contrôleur via USB.
2. Cliquez sur .
   L'écran **Entrer le mot de passe du contrôleur de sécurité** s'affiche.
3. Cliquez sur .
   L'écran **Récupération du mot de passe** s'affiche.

*Illustration 116. Écran **Récupération du mot de passe***



4. Cliquez sur **Obtenir le code de demande**.
   Le texte s'affiche dans le champ.
5. Cliquez sur **Copier** pour copier le code de demande dans le presse-papiers de l'ordinateur.
   Le message « Copie dans le presse-papiers terminée » s'affiche.
6. Donnez le code de demande et les informations de vérification à Banner Engineering.
   - Pour obtenir plus rapidement une réponse, contactez le support technique de Banner Engineering au +1-888-373-6767 ou contactez votre bureau Banner national. Compte tenu de la longueur de la demande de récupération, le code de demande doit être envoyé par e-mail à la personne au téléphone.
   - Pour obtenir une assistance en dehors des heures d'ouverture, envoyez le code de demande par e-mail à ATSGroup@bannerengineering.com.

   En plus du code de demande, ajoutez les informations suivantes :
   - Nom de la société
   - Votre nom et votre fonction
   - Données de contact
   - La raison pour laquelle vous avez besoin du mot de passe

   Une fois que Banner aura validé la demande de récupération de mot de passe, une clé de récupération de mot de passe sera fournie.
7. Copiez et collez la clé de récupération du mot de passe dans le champ **Clé de récupération** de l'écran **Récupération du mot de passe**.
8. Cliquez sur **Appliquer**.
   La clé est validée et confirmée et l'écran **Gestionnaire des mots de passe** s'ouvre.
9. Modifiez le mot de passe (XS/SC26 FID 7 ou ultérieurs compatibles Ethernet uniquement) ou le code PIN et appliquez les modifications au contrôleur de sécurité.
10. Effectuez un reset du système ou une remise sous tension.
    Le nouveau mot de passe ou code PIN est implémenté.

10.14 Affichage et importation des données du contrôleur

Le logiciel du Contrôleur de sécurité Banner permet de consulter ou de copier les données actuelles du contrôleur de sécurité, par exemple, le numéro de modèle et la version du micrologiciel, la configuration et les paramètres réseau, ainsi que le schéma de câblage.

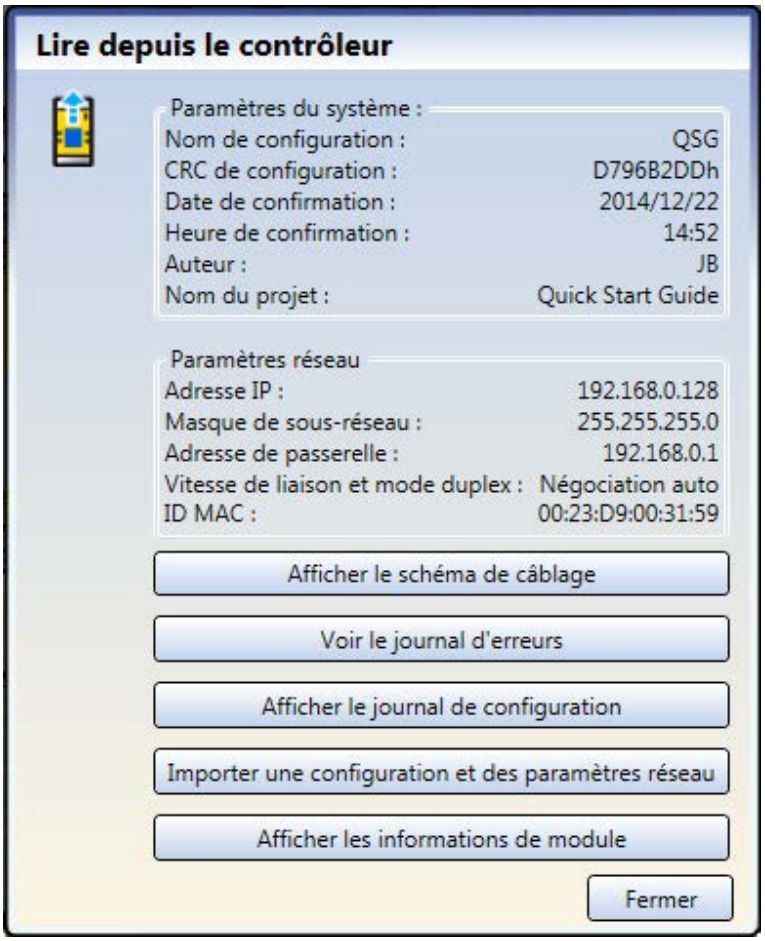
Lire les données depuis le contrôleur est disponible lorsqu'un contrôleur de sécurité est connecté au PC via USB ou Ethernet (pour les modèles Ethernet XS/SC26 FID 7 ou ultérieur).

Affichage d'un instantané des paramètres réseau et système

Cliquez sur **Lire les données depuis le contrôleur** dans la barre d'outils du logiciel. Les paramètres actuels du contrôleur de sécurité s'affichent :

- Nom de la configuration
- CRC de configuration
- Date de confirmation
- Heure de confirmation
- Auteur
- Nom du projet
- Adresse IP
- Masque de sous-réseau
- Adresse de passerelle
- Vitesse de liaison et mode duplex
- ID MAC

Illustration 117. Affichage d'un instantané des paramètres réseau et système



Voir le schéma de câblage — Supprime tous les autres onglets et feuilles de travail du logiciel et affiche uniquement les onglets **Schéma de câblage** et **Équipement**.

Voir le journal des défauts — Historique des 10 derniers défauts. Référez-vous à la section Voir le journal de défauts à la page 138.

Afficher le journal de configuration — Historique des 10 configurations les plus récentes (seule la configuration actuelle peut être affichée ou importée). Référez-vous à la section Afficher le journal de configuration à la page 139.

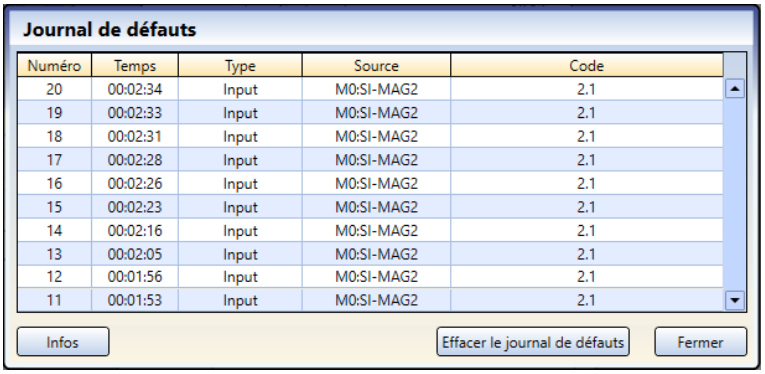
Importer une configuration et des paramètres réseau — Accès à la configuration et aux paramètres réseau actuels du contrôleur (dépend des droits d'accès de l'utilisateur, voir la section Gestionnaire des mots de passe du XS/SC26 à la page 135 ou Gestionnaire des mots de passe du SC10-2 à la page 136).

Afficher les informations sur le module — Voir Afficher les informations sur le module à la page 139.

10.14.1 Voir le journal de défauts

Le **journal de défauts** répertorie les 10 derniers défauts dans l'ordre inverse. La remise sous tension efface le journal des défauts.

Illustration 118. Journal de défauts



Temps— temps écoulé depuis la dernière mise sous tension du contrôleur de sécurité.

Type— catégorie de défaut, par exemple sortie, entrée, EDM, presse, système, etc.

Source— entrée, sortie ou fonction qui a rencontré un défaut.

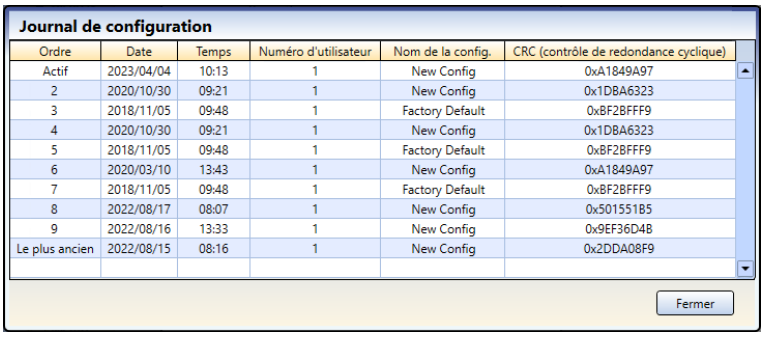
Code— code du défaut. Voir Tableaux des codes de défaut du XS/SC26 à la page 349 et Tableau des codes de défaut du SC10-2 à la page 354 pour les descriptions des codes de défaut.

Remarque: La numérotation du journal de défauts peut aller jusqu'à 4 294 967 295 sauf si vous coupez et rétablissez l'alimentation du contrôleur de sécurité, auquel cas la numérotation est réinitialisée à 1. L'effacement du journal de défauts (via le logiciel ou l'interface embarquée) supprime l'historique du journal mais conserve la numérotation.

10.14.2 Afficher le journal de configuration

Le **journal de configuration** répertorie dans l'ordre les 10 dernières configurations chargées dans le contrôleur. Le journal de configuration est maintenu même pendant les cycles de redémarrage. Les configurations sont classées de la plus récente à la plus ancienne. Seule la configuration actuelle peut être affichée ou importée.

Illustration 119. Journal de configuration



Date et **heure** — date et heure auxquelles la configuration a été confirmée. Les configurations 2 et 4 sont identiques (sur la base du CRC) ; voir Illustration 119 à la page 139. Par conséquent, la même configuration a été chargée plusieurs fois dans ce contrôleur.

Numéro d'utilisateur — code PIN ou mot de passe utilisé pour charger la configuration.

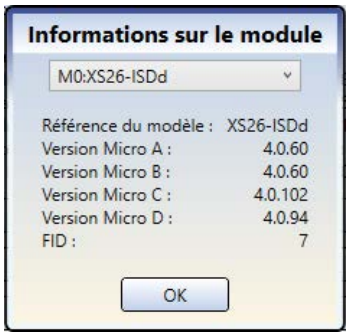
Nom de la configuration— nom de la configuration issue du fichier chargé. (Le nom par défaut est **Nouvelle configuration**.)

CRC (Contrôle de redondance cyclique) — numéro unique généré lorsqu'une configuration est confirmée. Ce numéro peut être lu par le contrôleur de sécurité pour vérifier que la configuration n'a pas été modifiée.

10.14.3 Afficher les informations sur le module

L'écran **Informations sur le module** répertorie plusieurs informations pour chaque module.

Illustration 120. Informations sur le module



Les informations incluent :

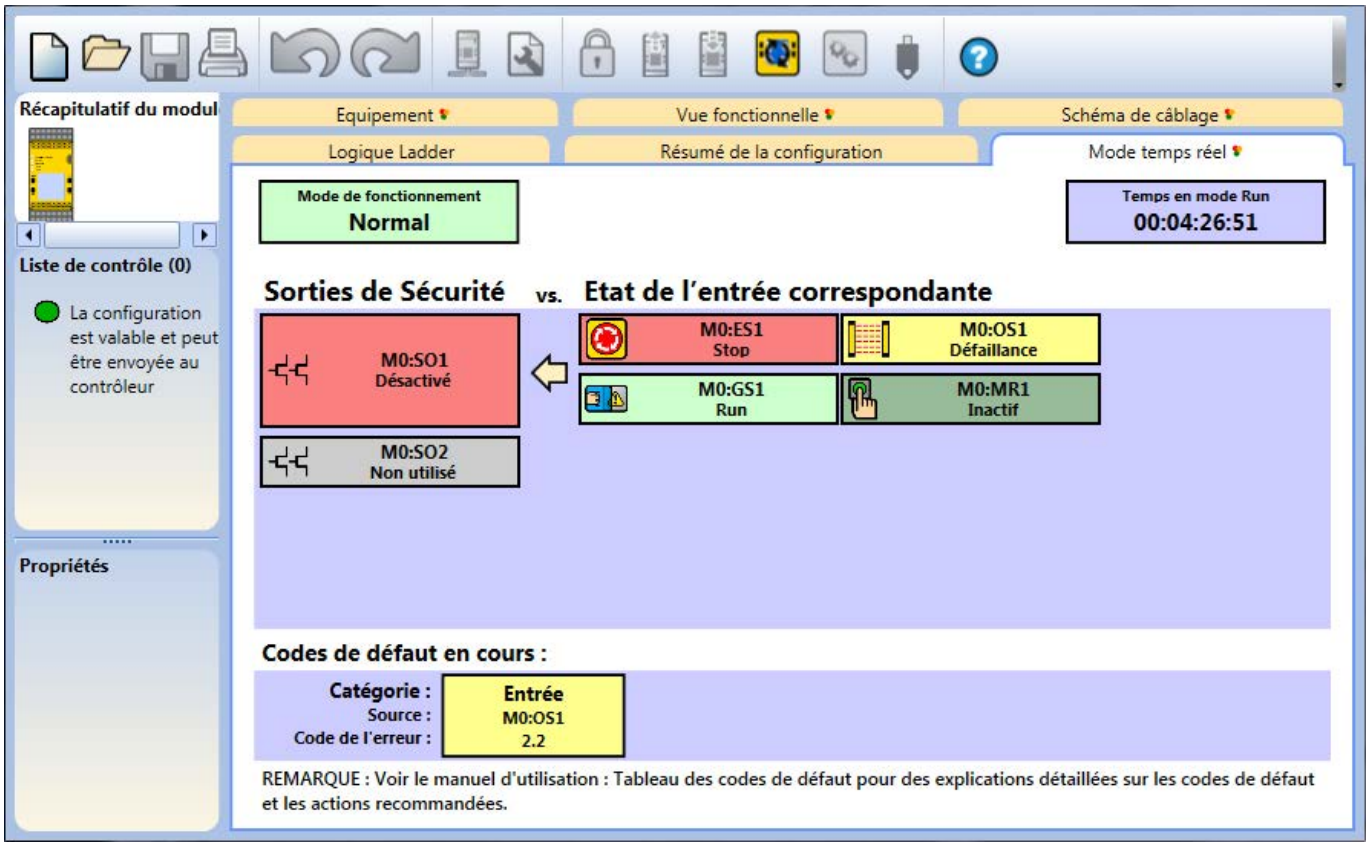
- Numéro de modèle de chaque module (pour les unités XS26, chaque module d'extension possède ses propres informations répertoriées dans le menu déroulant)
- Niveau de version de chaque microcontrôleur
- ID fonctionnel (FID) de chaque module

Ces informations peuvent être essentielles pour le support Banner en cas de problème sur le terrain.

10.15 Mode temps réel

L'onglet **Mode temps réel** est disponible quand un contrôleur de sécurité est connecté au PC via USB.

*Illustration 121. Temps d'exécution — XS/SC26 - Onglet **Mode temps réel***



L'onglet **Mode temps réel** est accessible lorsque vous cliquez sur **Mode temps réel** dans la barre d'outils. L'activation du **Mode temps réel** désactive la modification de la configuration dans toutes les autres vues. L'onglet **Mode temps réel** offre des informations supplémentaires sur les dispositifs et les défauts, dont un code de défaut (voir les sections Tableaux des codes de défaut du XS/SC26 à la page 349 et Tableau des codes de défaut du SC10-2 à la page 354 pour une description du défaut et les solutions possibles). Les données d'exécution (Run Time) sont également mises à jour dans les onglets **Vue fonctionnelle**, **Équipement** et **Schéma de câblage** offrant une représentation visuelle des états des dispositifs.

*Illustration 122. Temps d'exécution — Onglet **Équipement***

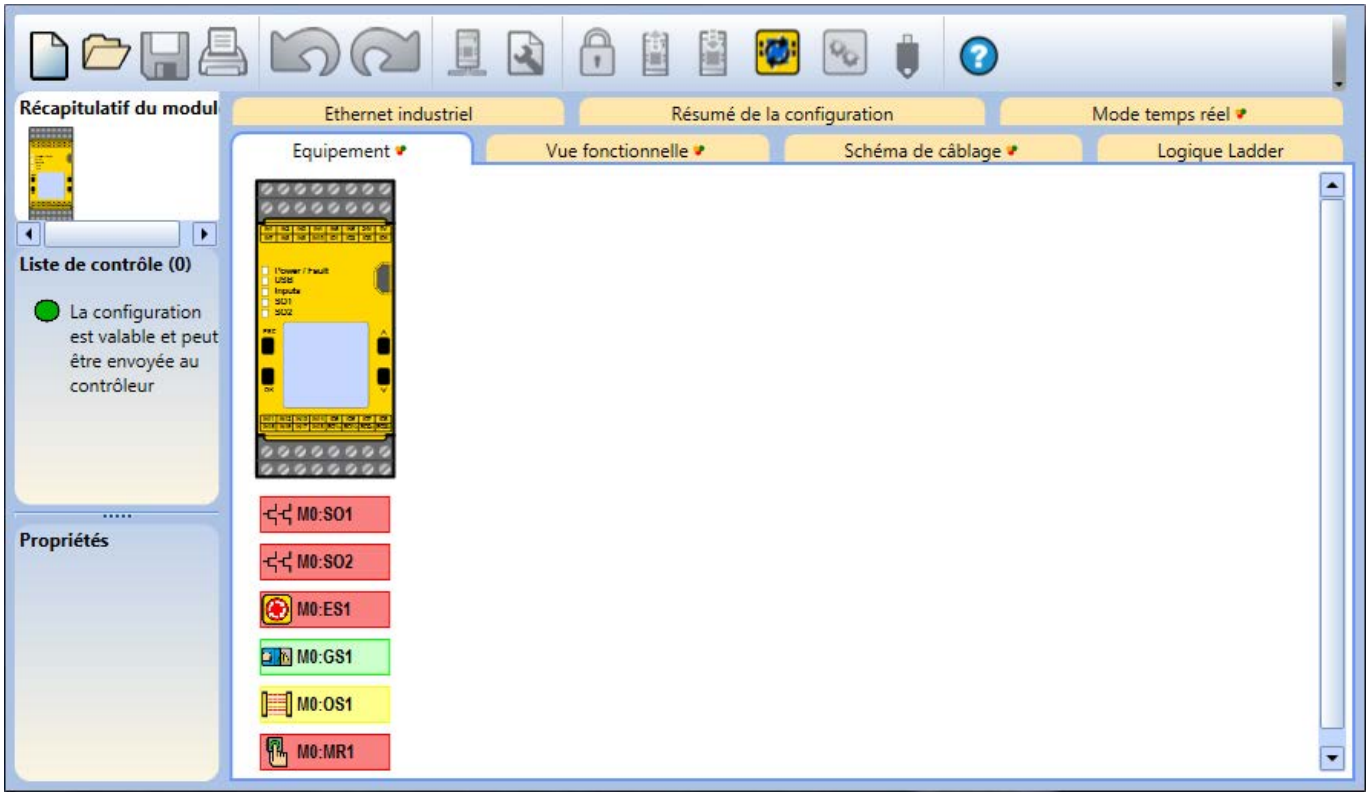


*Illustration 123. Temps d'exécution — Onglet **Vue fonctionnelle***

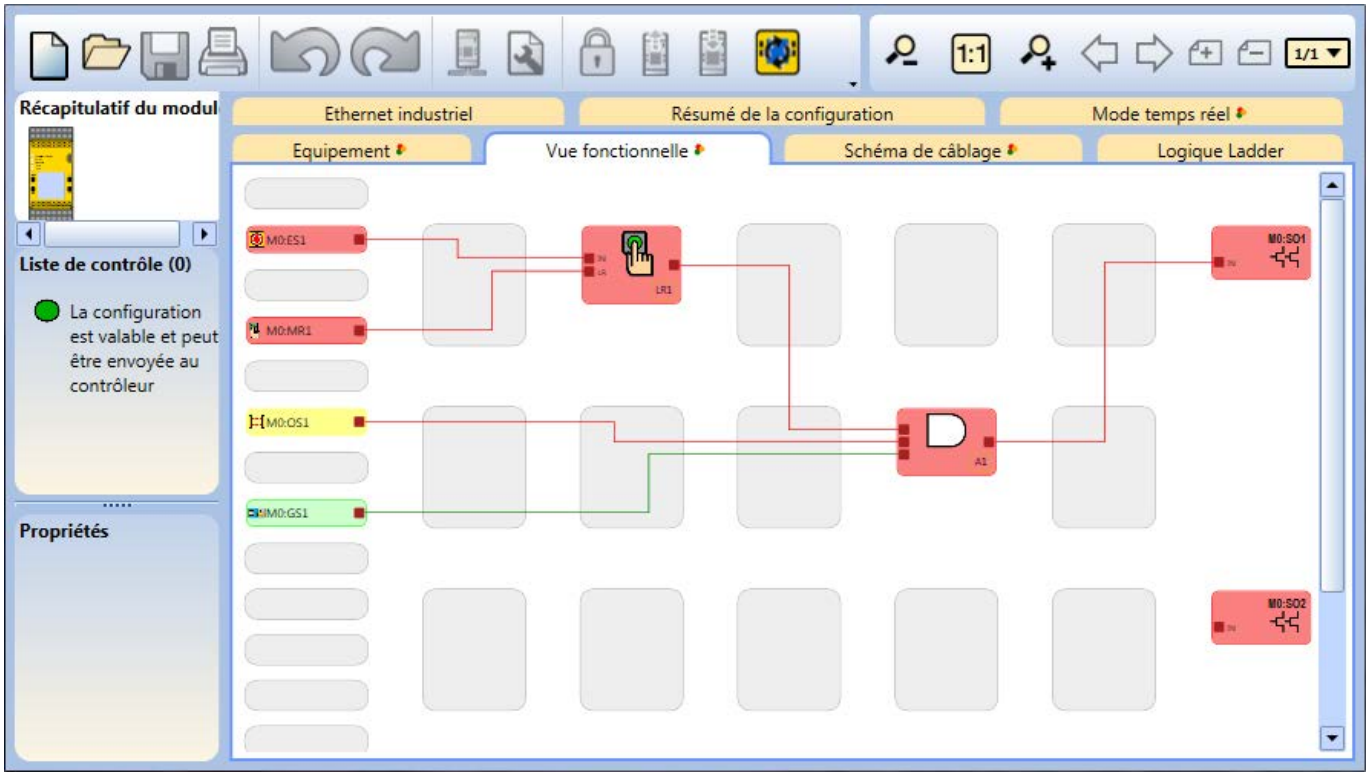


*Illustration 124. Temps d'exécution — Onglet **Schéma de câblage***

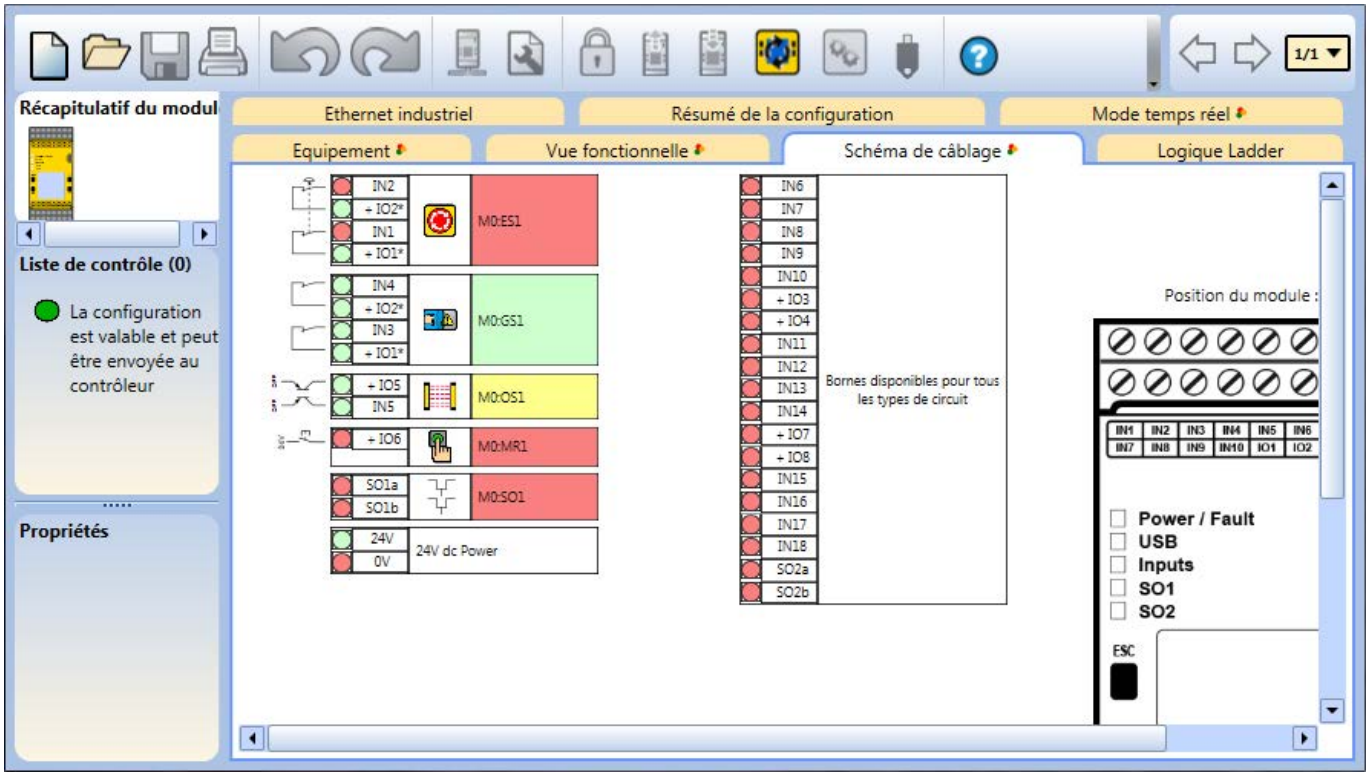
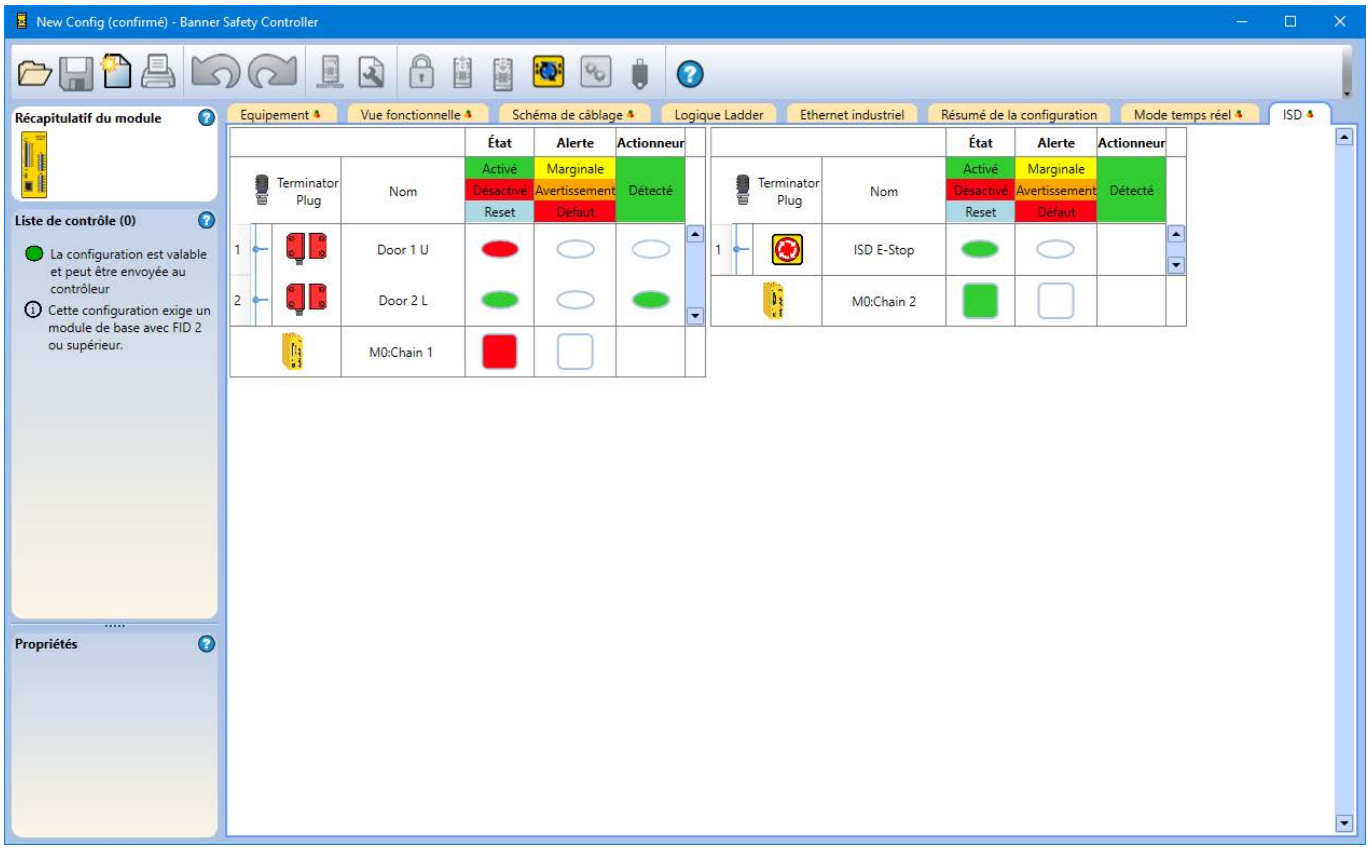


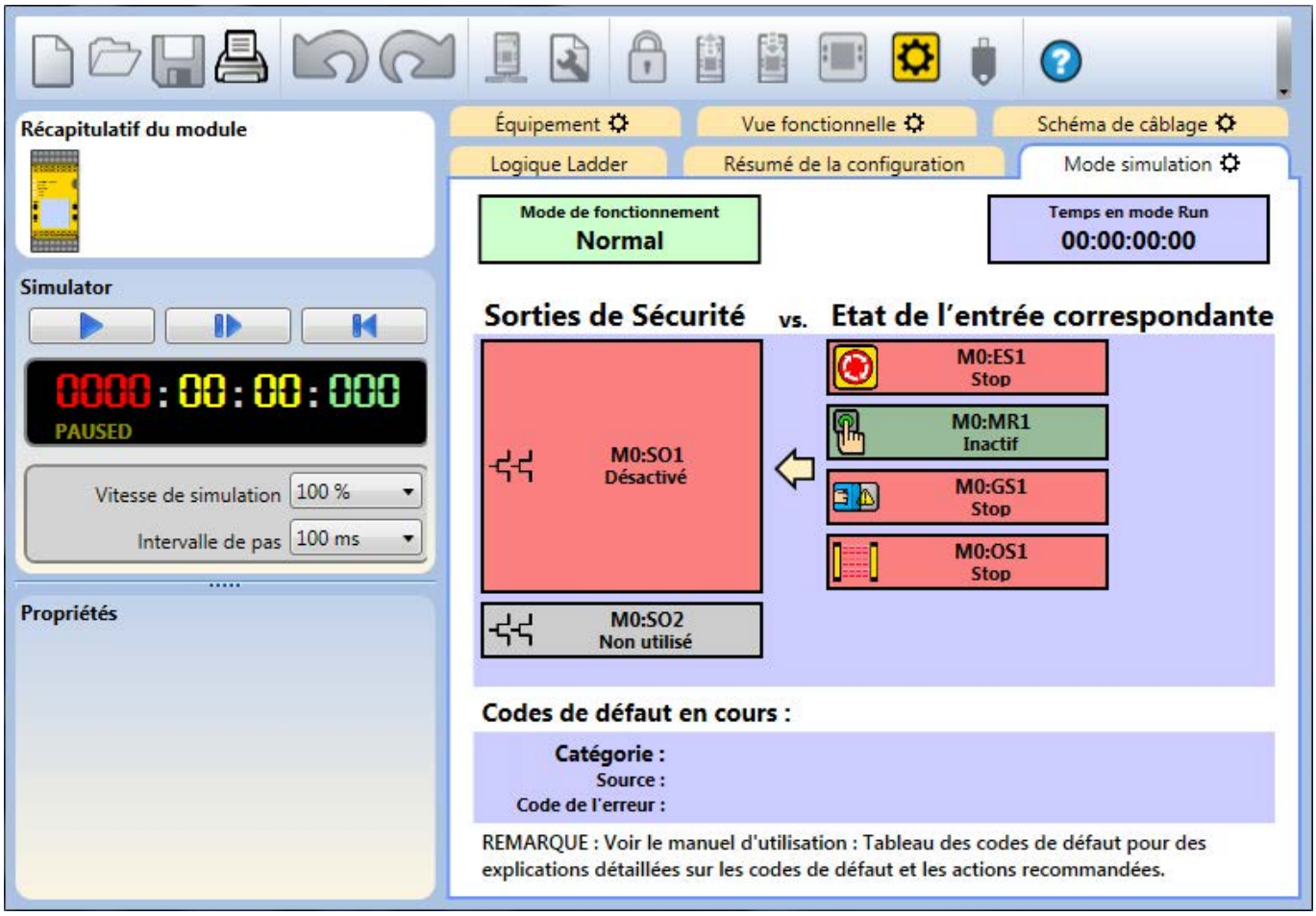
*Illustration 125. Temps d'exécution — Onglet **ISD***



10.16 Mode simulation

Important: L'utilisation du Mode simulation ne remplace pas la procédure de vérification à la mise en service du système installé. Le logiciel de simulation Contrôleur de sécurité Banner est conçu pour vous aider à créer une configuration valide. Toutefois, c'est à l'utilisateur qu'il incombe de vérifier l'intégrité, la sécurité et le fonctionnement de la configuration en suivant la Procédure de vérification à la mise en route à la page 312.

Illustration 126. Mode simulation



L'onglet **Mode simulation** devient accessible lorsque vous cliquez sur **Mode simulation** dans la barre d'outils. Les options du mode simulation sont alors accessibles dans la partie gauche de l'écran. L'onglet **Mode simulation** ne contient que des informations en lecture seule. Vous ne pouvez pas sélectionner les éléments d'entrée ou de sortie dans cette vue.

Remarque: Pour les entrées ISD, les dispositifs individuels ne sont pas simulés, seule la sortie finale connectée aux bornes d'entrée ISD est simulée (activée ou désactivée).



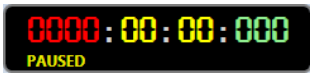
[Lecture/Pause] Lance le décompte du temps de simulation à la vitesse de simulation définie ou interrompt temporairement le temps de simulation.



[Par pas] Avance le temps de simulation d'un intervalle spécifié.



[Réinitialisation] Réinitialise le minuteur à zéro et l'équipement à l'état d'arrêt initial.



[Minuteur] Affiche le temps écoulé en heures, minutes, secondes et millièmes de seconde.

Vitesse de simulation — Définit la vitesse de la simulation.

- 1%
- 10%
- 100% (vitesse par défaut)
- 500%
- 2 000%

Intervalle de pas — Définit le temps d'avance d'un pas unique (lorsque vous cliquez sur le bouton correspondant). Le temps d'avance varie selon la taille de la configuration.

Cliquez sur **Lire** pour lancer la simulation. Le minuteur démarre et l'engrenage tourne pour indiquer que la simulation est en cours d'exécution. Les onglets **Vue fonctionnelle**, **Équipement** et **Schéma de câblage** sont mis à jour. Ils offrent une représentation visuelle des états des dispositifs simulés et permettent de tester la configuration. Cliquez sur les éléments à tester, leur couleur et leur état changent en conséquence. La couleur rouge indique un état d'arrêt ou désactivé. La couleur verte indique un état de fonctionnement ou activé. La couleur jaune indique une défaillance. La couleur orange indique que l'entrée a été activée avant le démarrage initial de la simulation. En raison d'un test de démarrage, l'entrée doit être vue comme inactive avant d'être reconnue comme active.

*Illustration 127. Mode simulation — Onglet **Équipement***

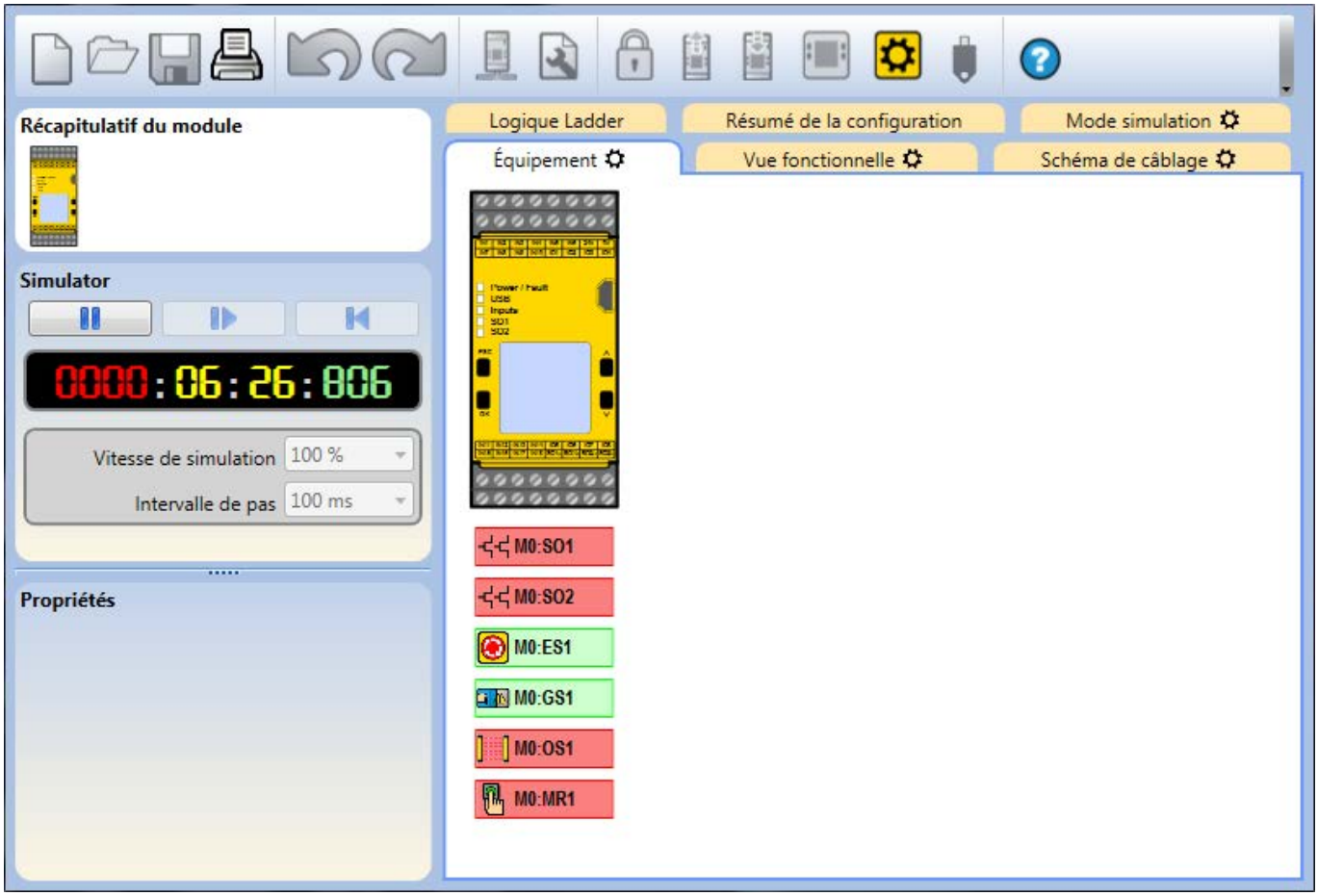


*Illustration 128. Mode simulation — Onglet **Schéma de câblage***

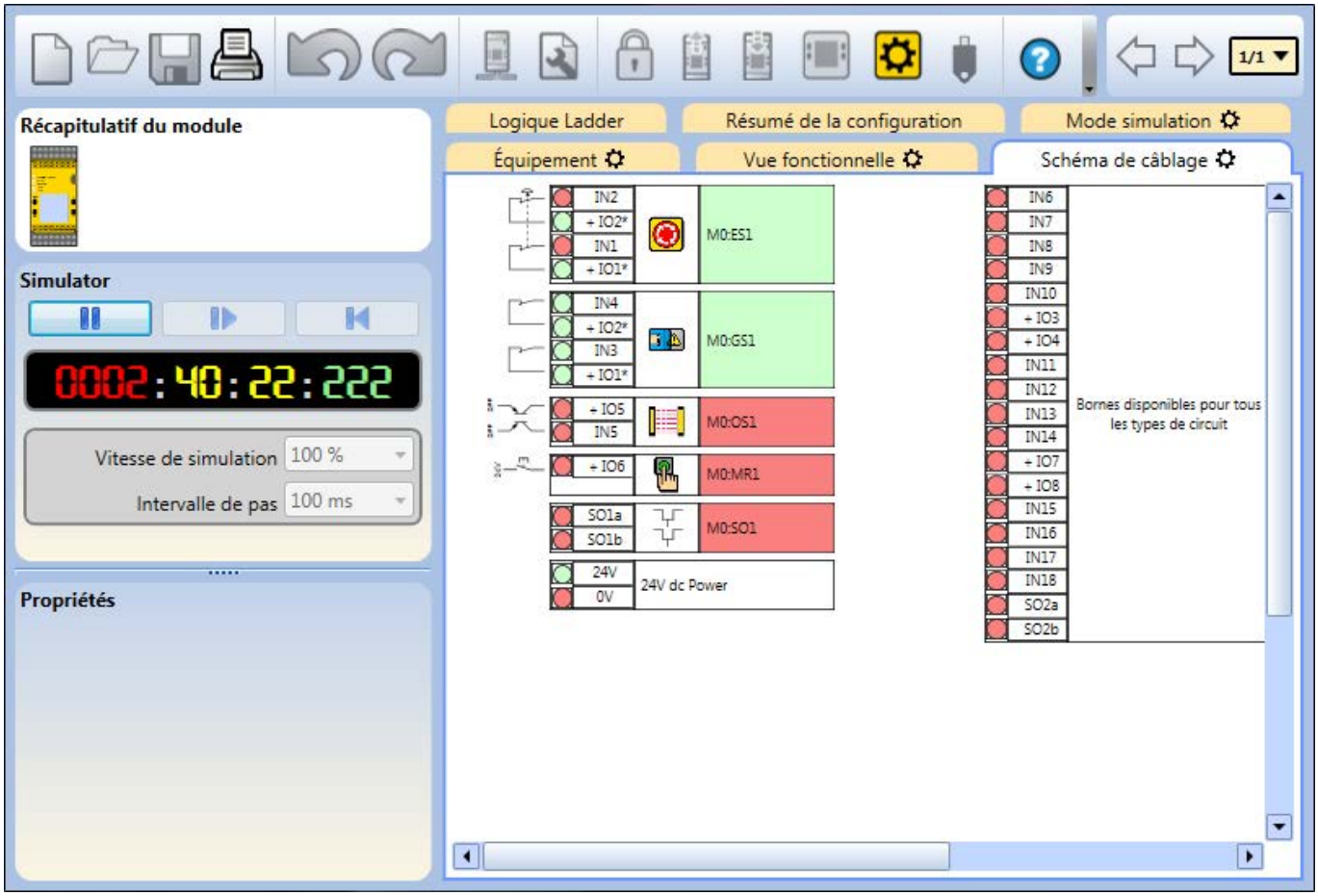
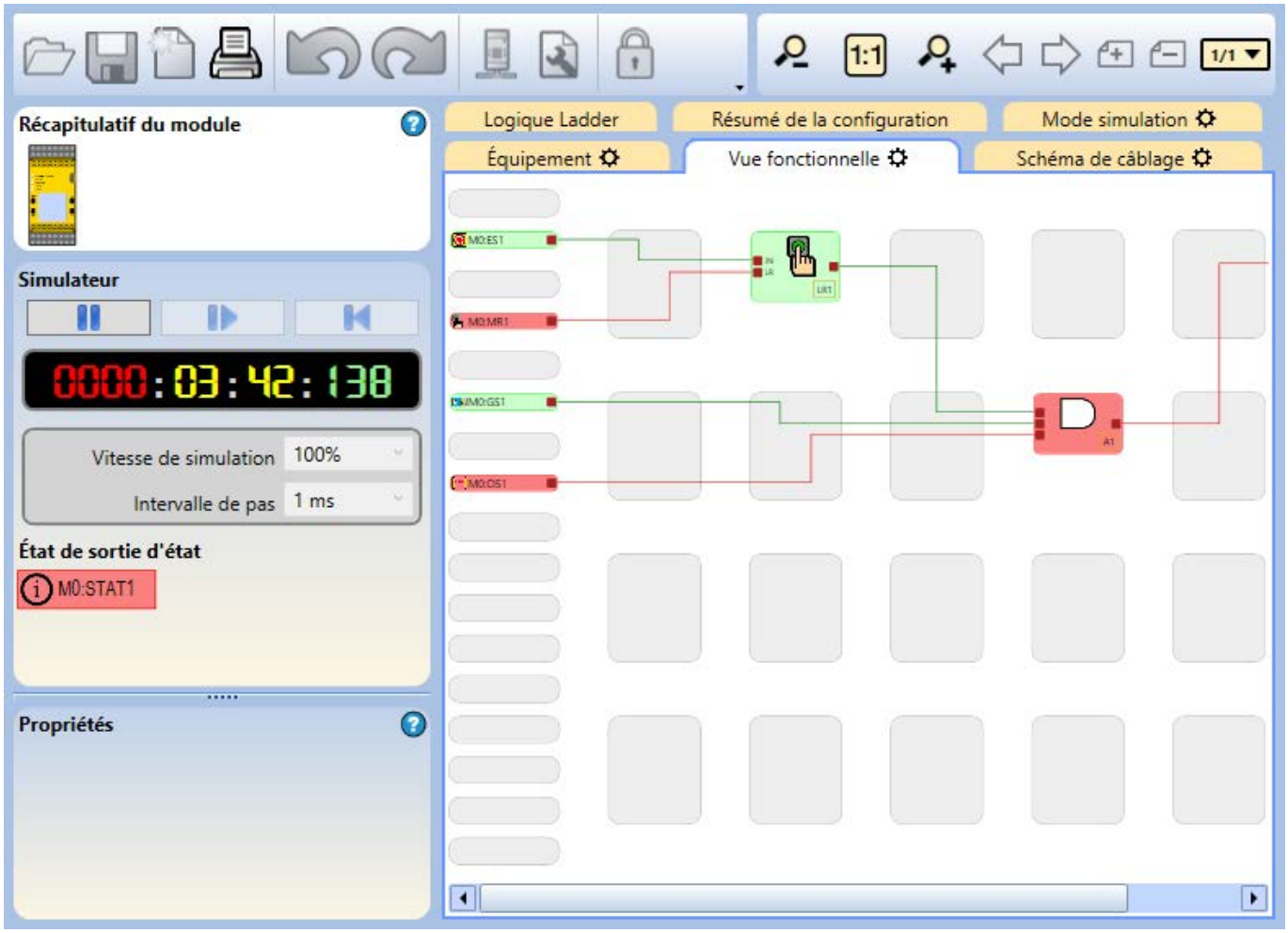


*Illustration 129. Mode simulation — Onglet **Vue fonctionnelle***



10.16.1 Mode temporisation

En mode simulation et dans l'onglet **Vue fonctionnelle**, certains éléments en mode temporisation sont affichés en mauve. La barre de progression affiche le décompte du minuteur associé à cet élément.

Les illustrations ci-dessous affichent les différents états des éléments :

Illustration 130. Sortie de sécurité en mode retard au déclenchement

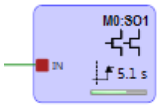


Illustration 131. Bloc d'inhibition en mode d'inhibition temporisée

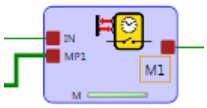
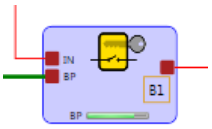


Illustration 132. Bloc de dérivation en mode de dérivation temporisée



Remarque: La lettre M située à côté de la barre de progression indique une inhibition temporisée.

Illustration 133. Bloc de temporisation— Contrôleurs de base XS/SC26 FID 2 ou ultérieur uniquement et SC10-2

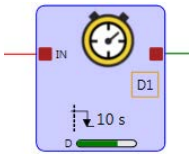
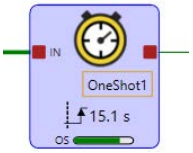


Illustration 134. Bloc de temporisation— Contrôleurs de base XS/SC26 FID 4 ou ultérieur uniquement



10.17 Paramètres

Les éléments suivants se trouvent dans le menu **Paramètres**.

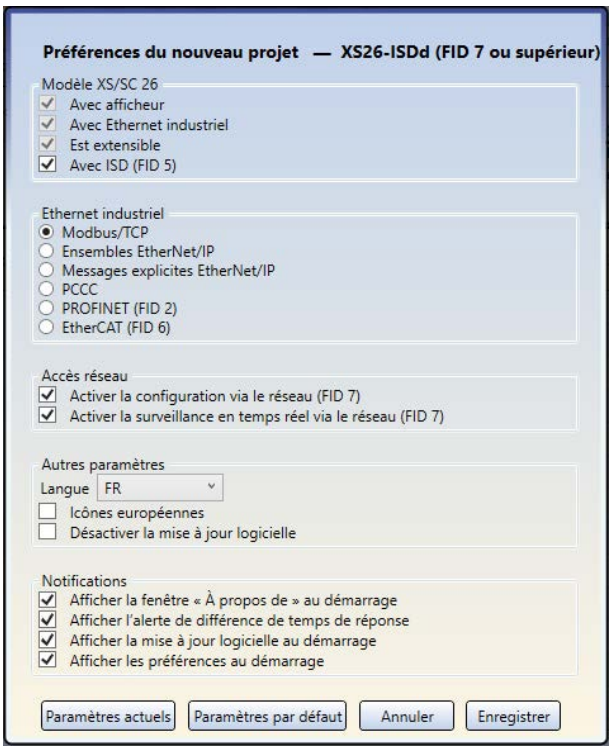
Icônes — Permet à l'utilisateur de sélectionner le style d'icônes américain (ANSI) ou européen (IEC).

Langue — Paramètre les options de langue du logiciel.

Mises à jour logicielles — Indique si le logiciel est à jour (en supposant que l'ordinateur est connecté à Internet). Permet également aux utilisateurs de désactiver la vérification automatique des mises à jour logicielles (si le logiciel met longtemps à s'ouvrir, la désactivation de la vérification automatique des mises à jour peut raccourcir le temps de démarrage).

Préférences — Permet de personnaliser le fonctionnement du logiciel pour qu'il corresponde aux paramètres de configuration habituels de l'utilisateur.

Illustration 135. Nouvelles préférences de projet — XS/SC26 illustré



- Configurez le modèle du module pour qu'il corresponde au modèle habituel utilisé dans les configurations (commencez par décocher la case ISD si vous n'utilisez pas ISD, puis désactivez les autres cases).
- Sélectionnez le protocole Ethernet industriel habituellement utilisé dans les configurations en cliquant sur la case située en face de celui-ci.
- Permet de configurer les modèles Ethernet XS/SC26 via le port Ethernet (configuration via le réseau) ou de les surveiller en mode temps réel via le port Ethernet (surveillance en temps réel via le réseau)
- La case Autres paramètres permet de sélectionner la langue à utiliser par défaut. Elle permet également de sélectionner les icônes européennes (IEC) et de désactiver la vérification automatique des mises à jour logicielles.
- La section Notifications permet d'activer ou de désactiver les fenêtres automatiques :
  - Fenêtre À propos de (révision du logiciel et avertissements au client) au démarrage
  - Alerte de différence de temps de réponse dans le résumé de la configuration
  - Notification de mise à jour logicielle au démarrage

10.18 Aide

Le menu **Aide** inclut les éléments suivants.

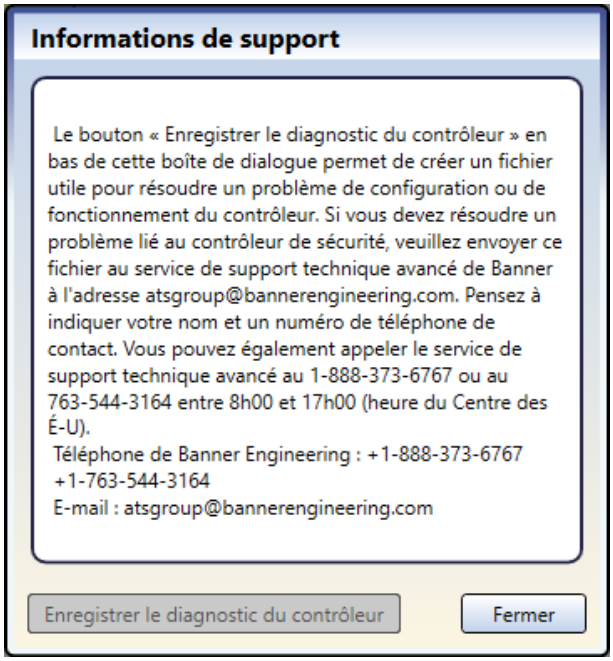
Aide — Ouvre les rubriques d'aide. Il s'agit d'un lien direct vers la version numérique du manuel d'instructions du contrôleur de sécurité.

À propos — Affiche le numéro de version du logiciel et un avertissement sur les responsabilités de l'utilisateur.

Notes de version — Affiche le tableau des notes de version indiquant les modifications (nouvelles fonctionnalités) apportées à chaque version du logiciel. La modification FID qui prend en charge la mise à jour logicielle indiquée est également incluse.

Informations de support — Aide à la création de fichiers de diagnostic qui peuvent être transférés au support technique de Banner (adresse e-mail indiquée) pour fournir des informations essentielles à Banner afin de l'aider à résoudre les problèmes.

Illustration 136. Informations de support



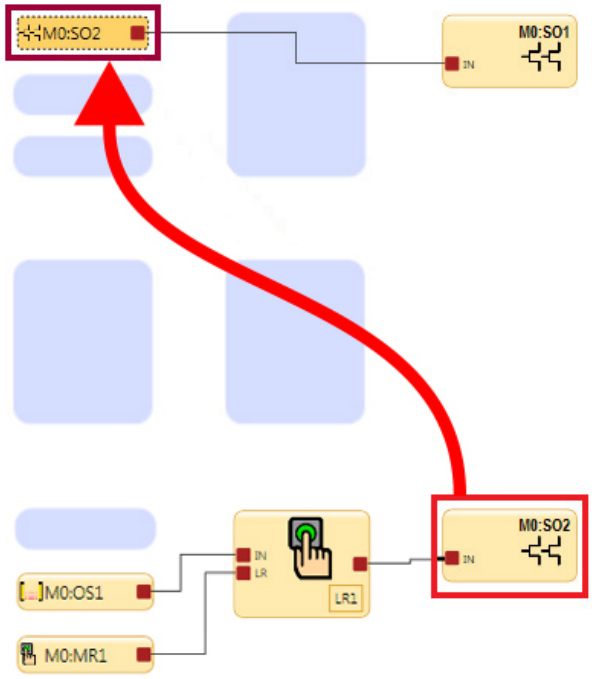
Les fichiers de diagnostic doivent être obtenus du contrôleur avant la remise sous tension car la remise sous tension efface les informations de défaut de la mémoire du contrôleur.

10.19 Signaux de référence

Important: Le logiciel de configuration intègre des signaux de référence qui représentent l'état des sorties du contrôleur de sécurité, des dispositifs d'entrée et des blocs logiques et fonction. Un signal de référence d'une sortie de sécurité peut servir à contrôler une autre sortie de sécurité. Dans ce type de configuration, l'état On (activé) physique de la sortie de sécurité configurée pour en contrôler une autre n'est pas connu. Si l'état On de la sortie de sécurité est essentiel pour la sécurité de l'installation, un mécanisme de retour d'information externe est nécessaire. Notez que ce contrôleur de sécurité est en état Safe (sûr) lorsque les sorties sont désactivées. Si la sortie de sécurité 1 s'active avant la sortie de sécurité 2, le dispositif contrôlé par la sortie de sécurité 1 doit être surveillé pour générer un signal d'entrée qui puisse être utilisé pour contrôler la sortie de sécurité 2. Il se peut que le signal de référence de la sortie de sécurité 1 ne convienne pas dans ce cas.

Illustration 137 à la page 149 montre comment une sortie de sécurité peut en contrôler une autre. Lorsque le reset manuel **M0:MR1** est enclenché, il active la sortie de sécurité **M0:SO2** qui active à son tour la sortie de sécurité **M0:SO1**.

Illustration 137. Sortie de sécurité contrôlée par une autre sortie de sécurité



11 Descriptions des blocs fonction

Les sections suivantes décrivent en détail les blocs fonction disponibles.

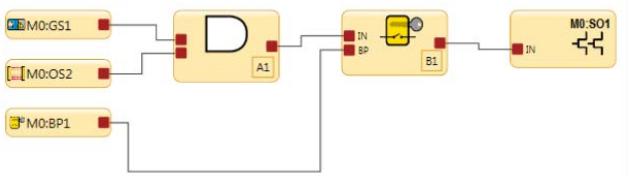
11.1 Bloc de dérivation

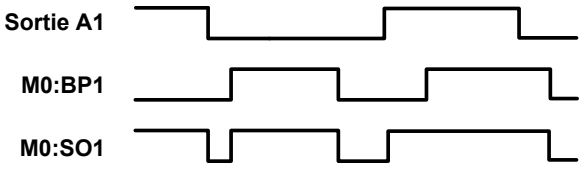
Nœuds par défaut	Nœuds supplémentaires	Remarques
BP IN	-	Lorsque le nœud BP est inactif, le signal de sécurité passe simplement par le bloc de dérivation. Lorsque le nœud BP est actif, la sortie du bloc est On indépendamment de l'état du nœud IN (si la case à cocher **La sortie est désactivée lorsque les deux entrées (IN et BP) sont activées** n'est pas cochée). La sortie du bloc de dérivation se désactive quand la limite de temps de dérivation expire.

Illustration 138. Chronogramme — Bloc de dérivation



Bloc fonction de dérivation





Limite de temps de dérivation

Une limite de temps de la fonction de dérivation doit être définie pour limiter la durée pendant laquelle la dérivation du dispositif d'entrée de sécurité reste active. La limite de temps peut varier entre 1 seconde (par défaut) et 12 heures et ne peut pas être désactivée. Vous ne pouvez définir qu'une seule limite de temps, laquelle s'appliquera à tous les dispositifs de sécurité contournés. À la fin de cette limite de temps, le contrôle de la sortie de sécurité est retransféré aux dispositifs d'entrée de sécurité qui ont été contournés.

Dérivation d'une commande bimanuelle

Le contrôleur de sécurité génère un signal d'arrêt si une entrée de commande bimanuelle est activée pendant que l'entrée est contournée. Ainsi, il est impossible que l'opérateur pense à tort que la commande bimanuelle est opérationnelle et qu'il ignore que la commande bimanuelle a été contournée et n'assure plus la fonction de protection.

11.1.1 Consignations

L'énergie dangereuse doit être sous contrôle (verrouillage/étiquetage) pendant les interventions de maintenance ou d'entretien au cours desquelles la mise sous tension, le démarrage ou la libération de l'énergie stockée peut entraîner des blessures.

Référez-vous aux normes OSHA 29CFR 1910.147, ANSI 2244.1, ISO 14118, ISO 12100 ou d'autres normes applicables pour vérifier que le contournement, ou dérivation, d'un dispositif de protection n'est pas contraire aux exigences stipulées dans les normes.

AVERTISSEMENT:

- **Utilisation limitée de la fonction de dérivation et/ou neutralisation**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Les fonctions de dérivation et/ou de neutralisation ne sont pas destinées à être utilisées en production. Elles doivent être utilisées uniquement pour des actions temporaires ou intermittentes, par exemple dégager la zone de détection d'un rideau lumineux de sécurité si des pièces se coincent. Lorsque ces fonctions sont utilisées, l'utilisateur doit les installer et les utiliser conformément aux normes applicables (telles que NFPA 79 ou IEC/EN 60204-1).

Procédures de travail sécurisées et formation

Les procédures de travail sécurisées permettent de contrôler l'exposition aux risques en se fondant sur des procédures écrites pour certaines tâches et les risques qui y sont associés. L'utilisateur doit aussi envisager la possibilité qu'une personne puisse contourner le dispositif de protection puis oublier de réarmer la protection ou de prévenir les autres membres du personnel de ce contournement du dispositif de protection. Dans les deux cas, cela peut entraîner une situation dangereuse. Pour l'éviter, une des solutions possibles consiste à rédiger une procédure de travail sécurisée et de s'assurer que le personnel est formé à la respecter.

11.2 Bloc de temporisation

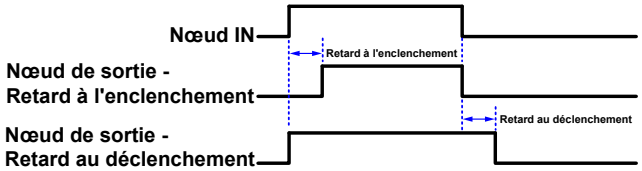
Le bloc de temporisation permet à l'utilisateur de configurer une période de temporisation au démarrage ou à l'arrêt pendant maximum 5 minutes, par incrément de 1ms. Cette fonction est disponible sur le XS/SC26 FID 2 et ultérieur et le SC10-2.

Nœuds par défaut	Nœuds supplémentaires	Remarques
IN	CD	Selon la sélection effectuée, la transition de signal/d'état sur le nœud d'entrée est retardée du délai de temporisation de sortie soit en appuyant sur la sortie d'arrêt (retard à l'enclenchement) ou la sortie de mise en marche (retard au déclenchement) après une transition de signal.

Remarque: Le délai de temporisation réel d'un bloc de fonction de temporisation ou d'une sortie de sécurité avec temporisation peut être une fois plus long que la valeur de temporisation d'une durée de balayage. La présence de plusieurs blocs de temporisation ou sorties de temporisation en série augmente le délai de temporisation final de maximum 1 durée de balayage pour chaque fonction de temporisation. Par exemple, trois blocs de fonction de temporisation de 100 ms en série et une durée de balayage de 15 ms entraînent un délai de temporisation réel pouvant atteindre 345 ms (300 ms + 45 ms).

Le nœud d'annulation de temporisation est configurable lorsque le retard au déclenchement est sélectionné.

Illustration 139. Schéma de temps d'un bloc de temporisation



PRÉCAUTION: Effet de la temporisation sur le temps de réponse

Le temps de retard au déclenchement peut augmenter considérablement le temps de réponse du contrôleur de sécurité. Cela aura un impact sur le positionnement des dispositifs de protection, dans la mesure où l'installation de ceux-ci est déterminée selon des formules de distance (minimale) de sécurité ou dépendent du temps nécessaire pour parvenir à un état non dangereux. Il faut donc tenir compte de l'augmentation du temps de réponse pour l'installation des dispositifs de protection.

Remarque: Le temps de réponse indiqué dans l'onglet **Résumé de la configuration** est le temps maximum modifiable selon l'utilisation faite des blocs de temporisation et autres blocs logiques (par ex. des fonctions OR). L'utilisateur est responsable du choix, de la vérification et de l'incorporation du temps de réponse adéquat.

Illustration 140. Propriétés du bloc de temporisation



La fenêtre **Propriétés du bloc de temporisation** permet de configurer les éléments suivants :

Nom

Crée un nom de 10 caractères maximum pour le bloc fonction.

Type de temporisation de sortie

Il s'agit du type de temporisation de sortie

- Aucune
- Retard au déclenchement
- Retard à l'enclenchement

Temporisation de sortie

Disponible lorsque l'option Temporisation de sortie de sécurité a la valeur Retard au déclenchement ou Retard à l'enclenchement

Temporisation : 1 ms à 5 minutes, par pas de 1 ms. La valeur par défaut est de 100 ms.

Type d'annulation

Disponible lorsque l'option Temporisation de sortie de sécurité a la valeur Retard au déclenchement.

- Ne pas annuler
- Entrée de contrôle (la sortie du bloc de temporisation reste activée si l'entrée est réactivée avant la fin de la temporisation.)
- Nœud d'annulation de la temporisation

Logique de fin

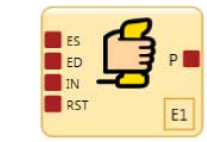
Disponible lorsque l'option Type d'annulation a la valeur Nœud d'annulation de la temporisation.

- Maintenir la sortie activée
- Désactiver la sortie

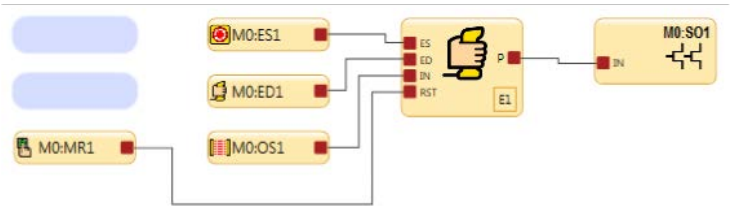
11.3 Bloc dispositif de commande

Nœuds par défaut	Nœuds supplémentaires	Remarques
ED IN RST	ES JOG	Un bloc dispositif de commande doit être directement connecté à un bloc de sortie. Grâce à cette méthode, vous êtes assuré que le contrôle ultime des sorties est entre les mains de l'opérateur qui manipule le dispositif de commande (ED). Utilisez le nœud ES pour les signaux de sécurité qui ne peuvent pas être dérivés par le nœud ED. Si aucune autre entrée du bloc fonction n'est configurée, il n'est pas nécessaire d'utiliser un bloc fonction de dispositif de commande.

Illustration 141. Chronogramme — Dispositif de commande, configuration simple



Bloc fonction appareil de commande



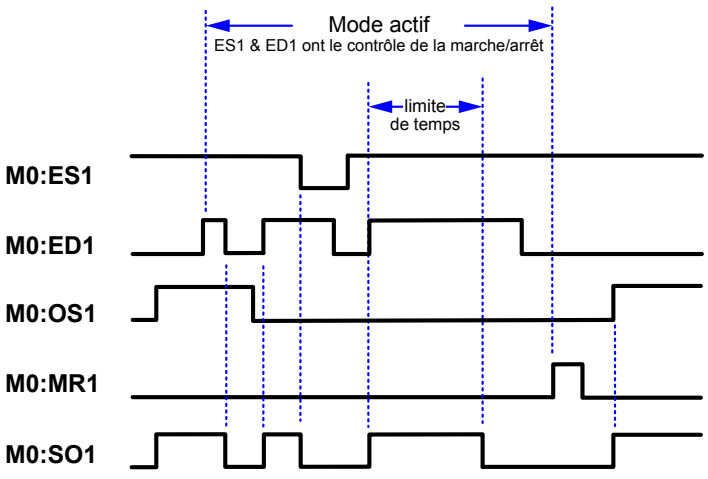
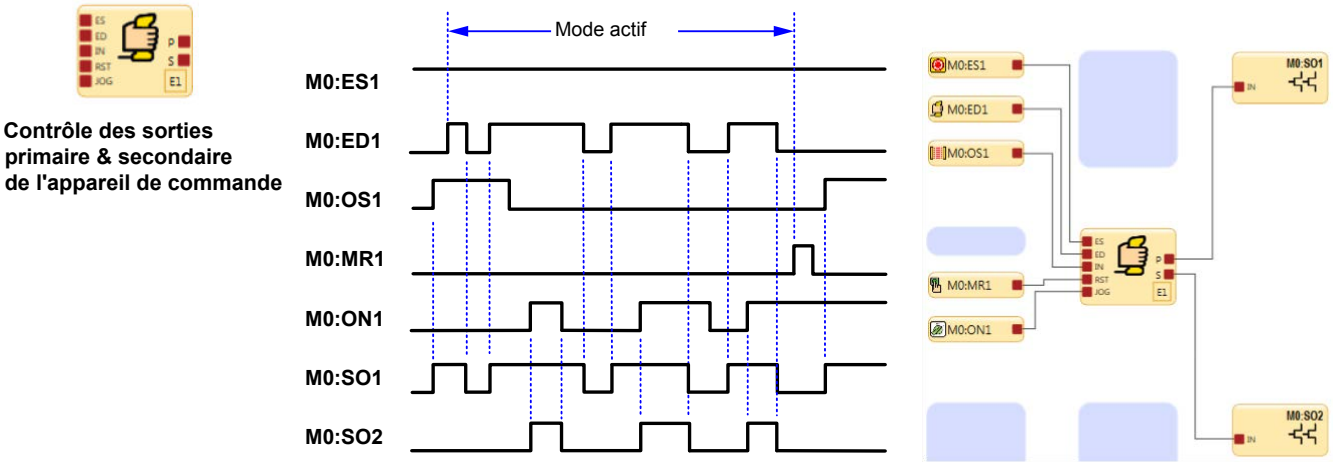


Illustration 142. Chronogramme — Dispositif de commande



Le mode actif E1 démarre lorsque l'appareil de commande ED1 passe en état marche.
Les dispositifs d'entrée ED1 et ES ont le contrôle de la marche/arrêt lorsqu'ils sont en mode actif.
Lorsque MR1 est utilisé pour effectuer un reset, le mode marche normal est rétabli et OS1
et ES1 ont le contrôle de la marche/arrêt.

Pour quitter le mode actif, le dispositif de commande doit être en état arrêt et un reset du bloc Dispositif de commande doit être effectué.

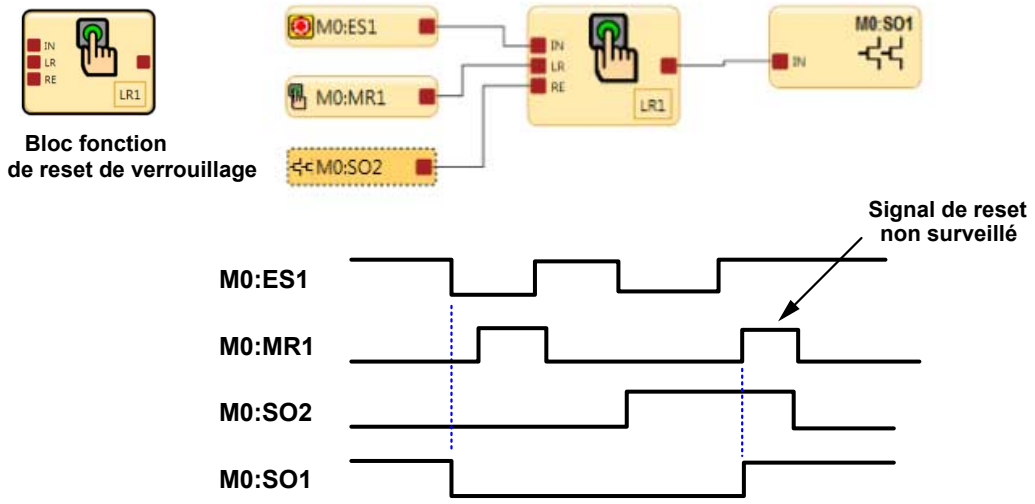
La limite de temps du dispositif de commande peut être réglée entre 1 seconde (par défaut) et 30 minutes, et ne peut pas être désactivée. Quand la limite de temps expire, les sorties de sécurité associées se désactivent. Pour démarrer un nouveau cycle du mode actif, avec la limite de temps réinitialisée à sa valeur initiale, le dispositif de commande doit passer de l'état ON à l'état OFF puis de nouveau à l'état ON.

Toutes les limites du retard au déclenchement et à l'enclenchement associées aux sorties de sécurité contrôlées par la fonction du dispositif de commande sont respectées pendant le mode actif.

11.4 Bloc de reset à verrouillage

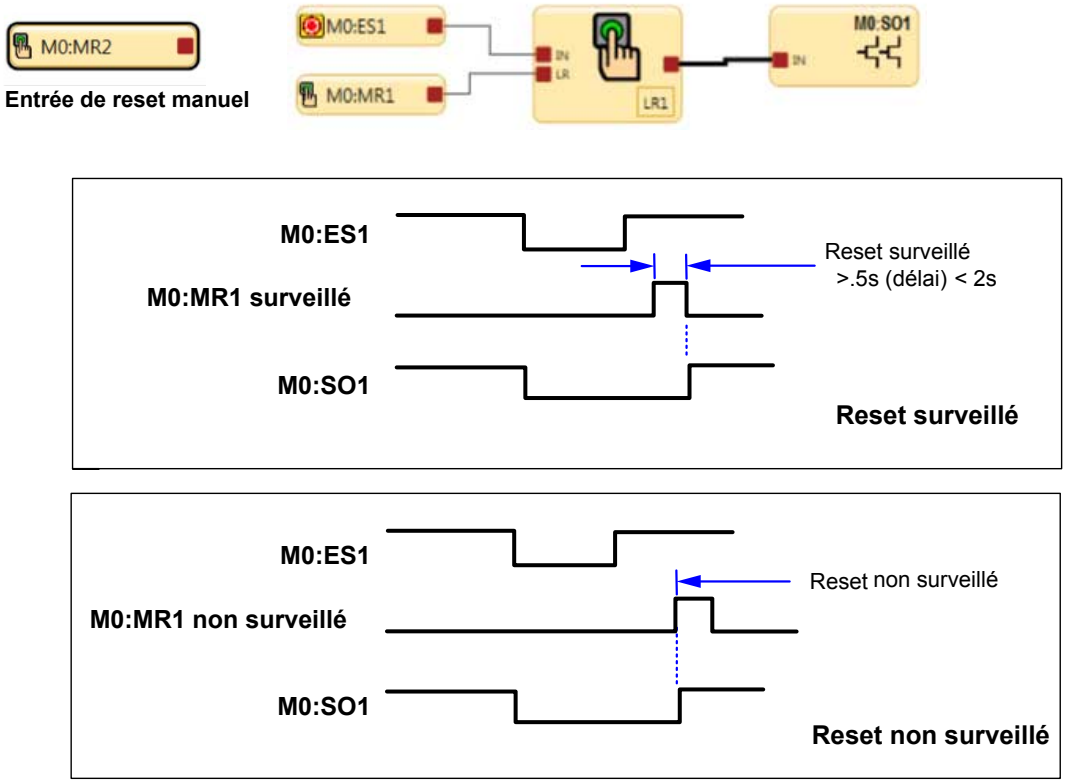
Nœuds par défaut	Nœuds supplémentaires	Remarques
IN LR	RE	Le nœud RE (Activation de reset) peut être utilisé pour activer ou désactiver la fonction de reset à verrouillage. Si les dispositifs d'entrée connectés au nœud IN sont tous en état marche et que le signal de l'entrée RE est à l'état haut, le bloc fonction LR peut faire l'objet d'un reset manuel pour que sa sortie s'active. Référez-vous à l'Illustration Illustration 143 à la page 154 illustrant le signal de référence SO2 connecté au nœud RE.

Illustration 143. Chronogramme — Bloc de reset à verrouillage



Le bloc fonction de reset de verrouillage LR1 désactive sa sortie et la sortie de sécurité SO1 quand le bouton d'arrêt d'urgence passe à l'état d'arrêt.
Il est possible d'effectuer un reset du verrouillage actuellement désactivé quand l'activation de reset RE de LR1 détecte un état de marche pour le signal de référence SO2 et MR1 est utilisé pour effectuer un reset.

Illustration 144. Chronogramme — Bloc de reset à verrouillage, reset surveillé/non surveillé



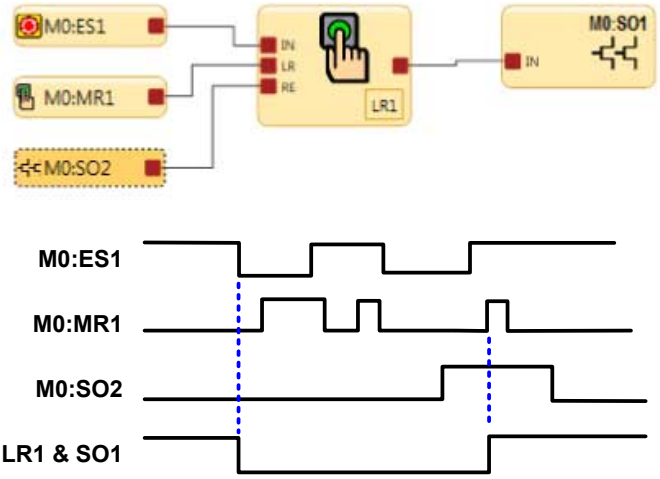
Le dispositif d'entrée de reset manuel peut être configuré pour l'un des deux types de signaux de reset suivants : Surveillé et Non surveillé.

Illustration 145. Chronogramme — Bloc de reset à verrouillage et sortie de sécurité de référence



Signaux de référence

Un signal de référence sert à :
- contrôler une sortie en fonction de l'état d'une autre sortie
- représenter l'état d'une sortie, entrée, fonction de sécurité ou bloc logique d'une autre page



Lorsque la sortie SO2 est activée, l'état du signal de référence de SO2 est activé (On) ou haut. Le bloc fonction ci-dessus montre le signal de référence SO2 connecté au nœud RE (Activation de reset) du bloc reset de verrouillage LR1.

Le reset (activation) de LR1 est uniquement possible lorsque ES1 est en état de marche (Run) et que SO2 est activé (On).

Consultez la section Signaux de référence à la page 148 pour en savoir plus sur les sorties de sécurité de référence.

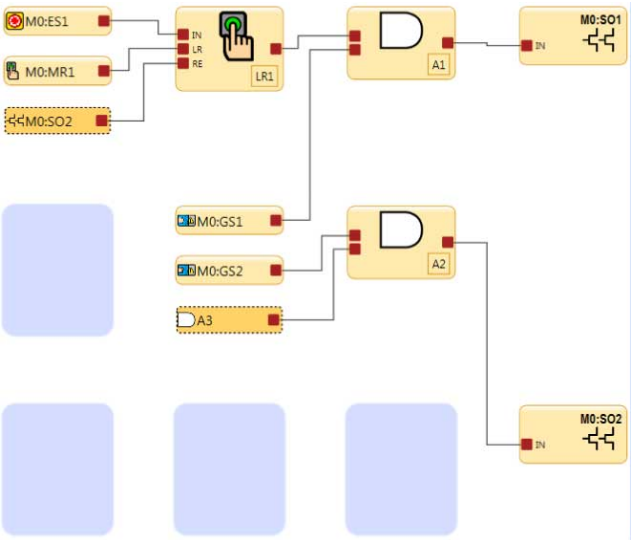
Illustration 146. Reset à verrouillage et sortie de sécurité de référence et bloc AND



Signaux de référence

Dans la figure ci-dessous, le signal de référence A3 est dans la page 1 du diagramme de blocs fonction et le bloc AND A3 est dans la page 2. Le nœud de sortie du bloc AND A3 peut être aussi utilisé dans la page 2 pour une autre logique de contrôle de sécurité.

Signal de référence A3 dans la page 1



Bloc logique AND A3 dans la page 2

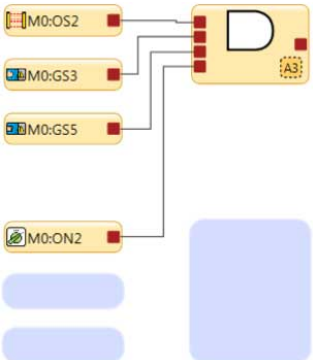
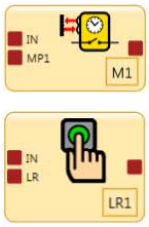
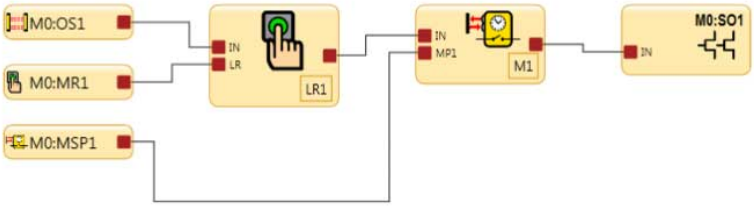
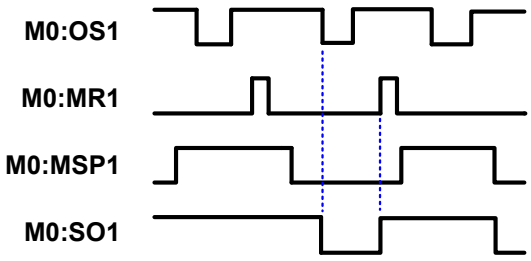


Illustration 147. Chronogramme — Bloc de reset à verrouillage et bloc d'inhibition



Fonction d'inhibition du reset de verrouillage



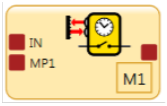


Si un dispositif de protection OS1 passe à l'état d'arrêt (Stop) au cours d'un cycle d'inhibition valide, le bloc fonction de reset de verrouillage se verrouillera et exigera un signal de reset pour que SO1 reste activé à la fin du cycle d'inhibition.
Si OS1 passe à l'état d'arrêt (Stop) au cours d'un cycle d'inhibition valide et qu'aucun signal de reset n'est généré, SO1 est désactivé à la fin du cycle d'inhibition.

11.5 Bloc d'inhibition

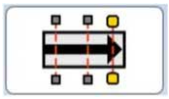
Nœuds par défaut	Nœuds supplémentaires	Remarques
IN, MP1	ME BP MP2	Les blocs d'entrée de paires de capteurs d'inhibition doivent être directement connectés au bloc fonction d'inhibition.

Illustration 148. Bloc d'inhibition — Types de fonction



Bloc fonction d'inhibition

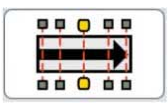
5 types de fonctions d'inhibition sont répertoriées ci-dessous.
Les schémas suivants affichent les détails des fonctions et l'ordre de changement d'état du capteur/de la protection pour chaque type de fonction d'inhibition.



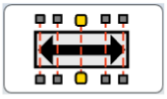
Simple voie - 1 paire de capteurs d'inhibition



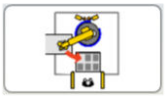
Double voie - 1 paire de capteurs d'inhibition



Simple voie - 2 paires de capteurs d'inhibition

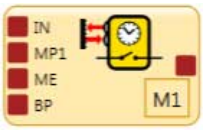


Double voie - 2 paires de capteurs d'inhibition



Double voie - 1 paire de capteurs d'inhibition

Illustration 149. Bloc d'inhibition — Options du mode de dérivation/neutralisation



Il existe deux types de dérivation de l'inhibition :
- Neutralisation dépendante de l'inhibition
- Dérivation (normale)

Dans le menu Propriétés du bloc d'inhibition des Paramètres avancés, si la case à cocher Dérivation est activée, l'option pour sélectionner une dérivation ou une neutralisation dépendante de l'inhibition est accessible.

La neutralisation dépendante de l'inhibition permet de redémarrer temporairement un cycle d'inhibition incomplet (par exemple après l'expiration du temps limite d'inhibition). Dans ce cas un ou plusieurs capteurs d'inhibition doivent être activés pendant que la protection est en état d'arrêt (Stop).

La dérivation normale est utilisée pour contourner temporairement le dispositif de sécurité afin de maintenir la sortie du bloc fonction activée ou de l'activer.

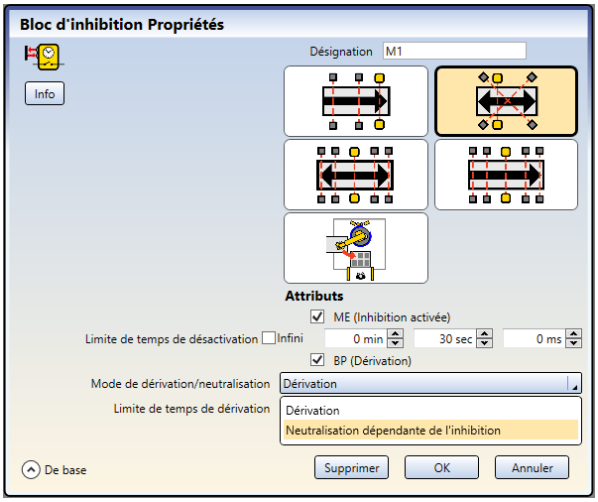


Illustration 150. Neutralisation dépendante de l'inhibition

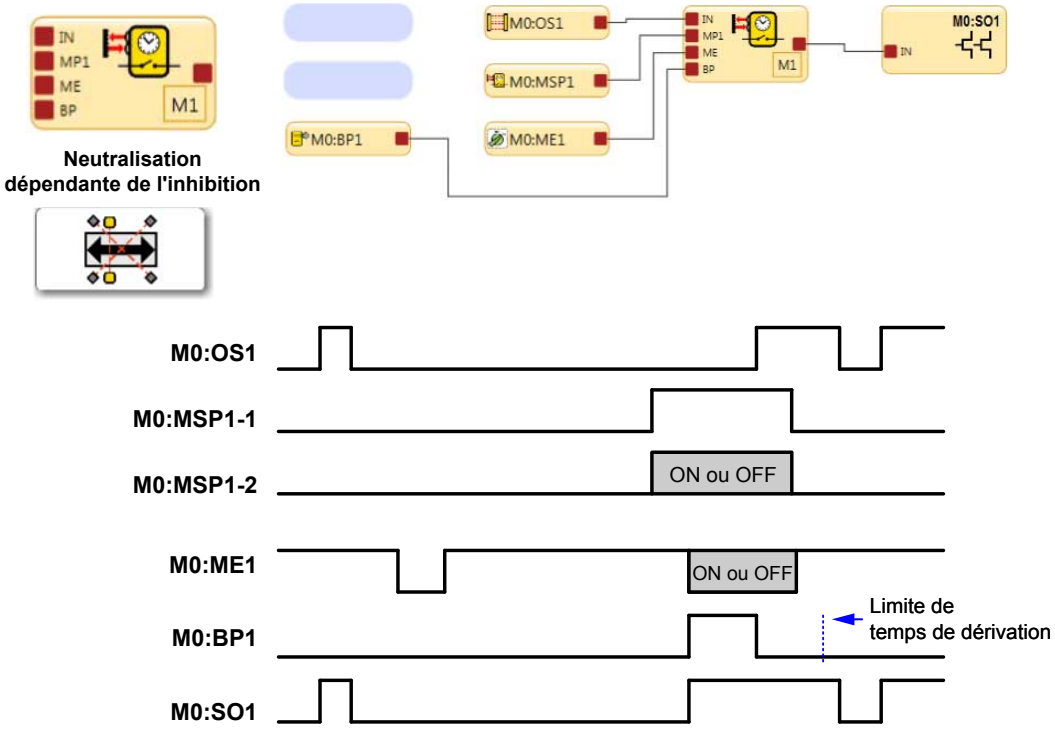


Illustration 151. Dérivation d'inhibition

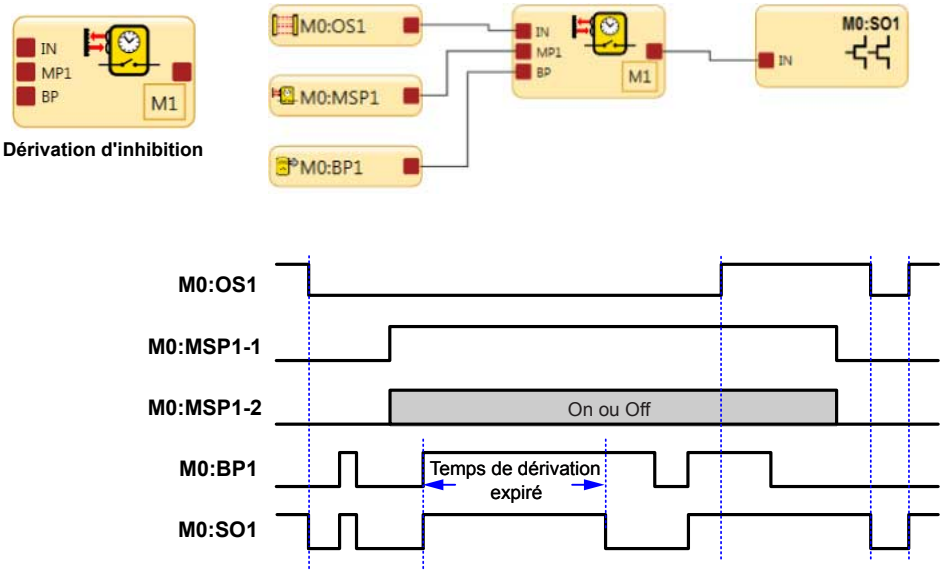
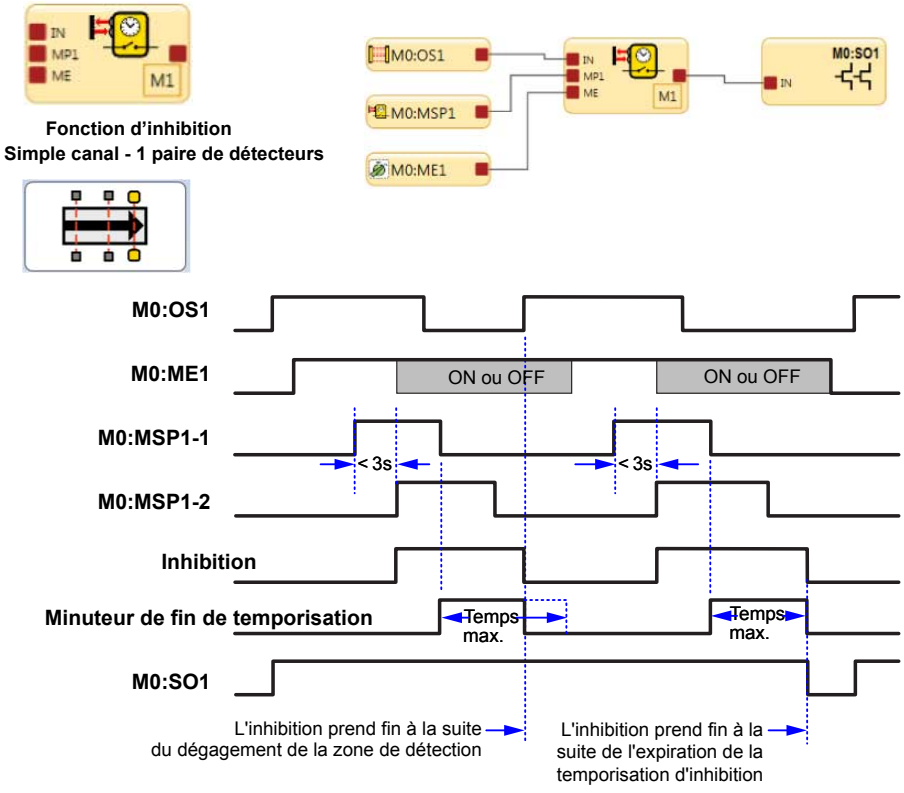


Illustration 152. Chronogramme — Bloc d'inhibition simple canal, une paire de capteurs d'inhibition



Remarque : MO:OS1 doit être bloqué avant que MSP1-1 ou MSP1-2 soit dégagé.

Illustration 153. Chronogramme — Bloc d'inhibition simple canal, deux paires de capteurs d'inhibition

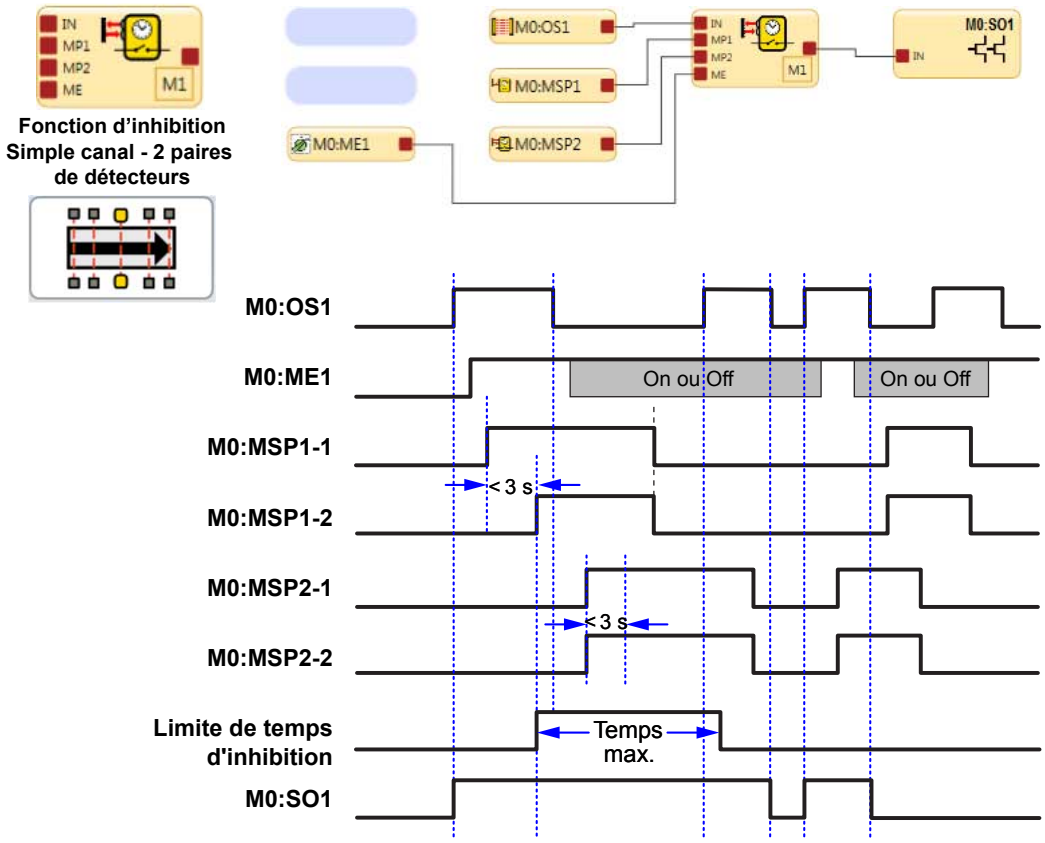


Illustration 154. Chronogramme — Bloc d'inhibition double canal, une paire de capteurs d'inhibition

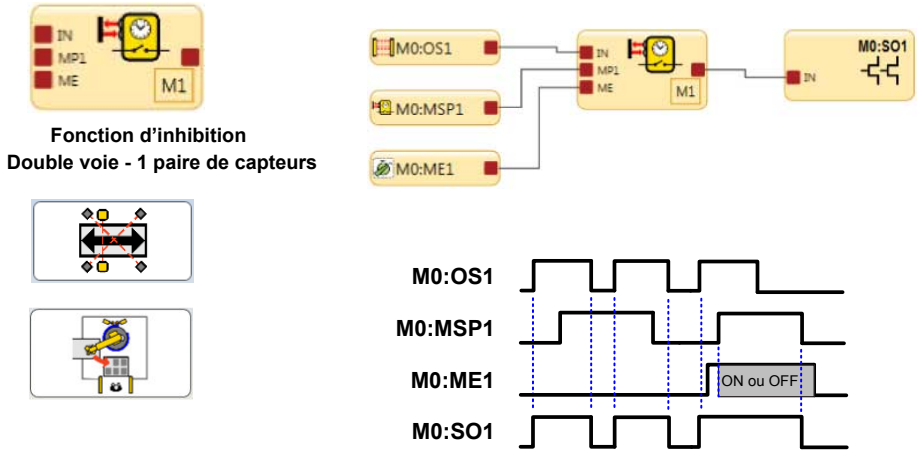
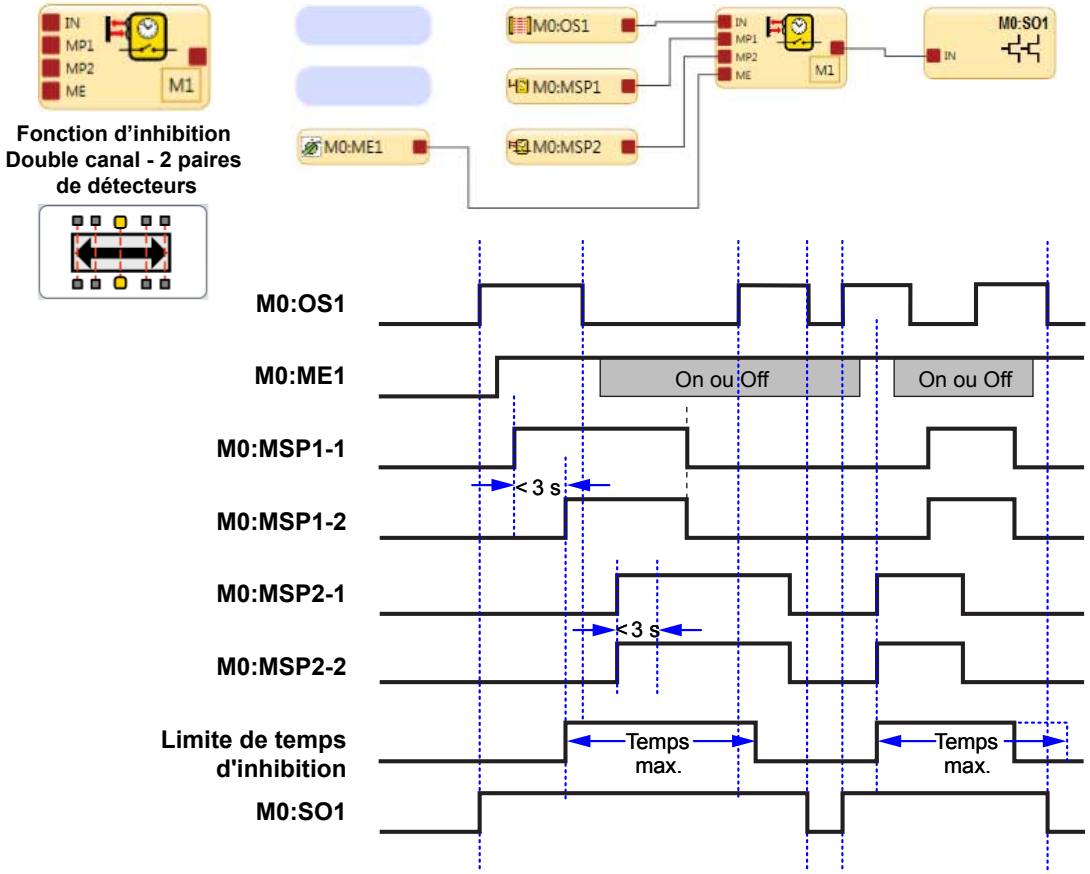


Illustration 155. Chronogramme — Bloc d'inhibition double canal, deux paires de capteurs d'inhibition

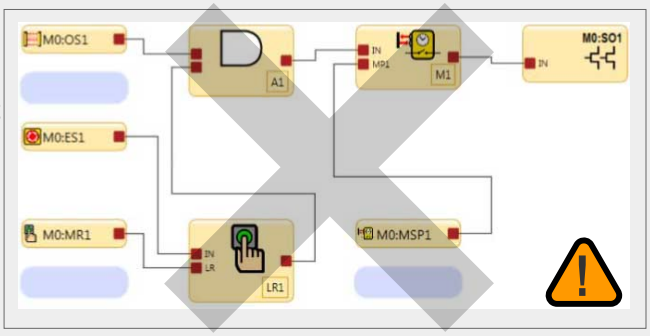


AVERTISSEMENT:

Contrôle du bouton d'arrêt d'urgence en cas d'utilisation de la fonction d'inhibition

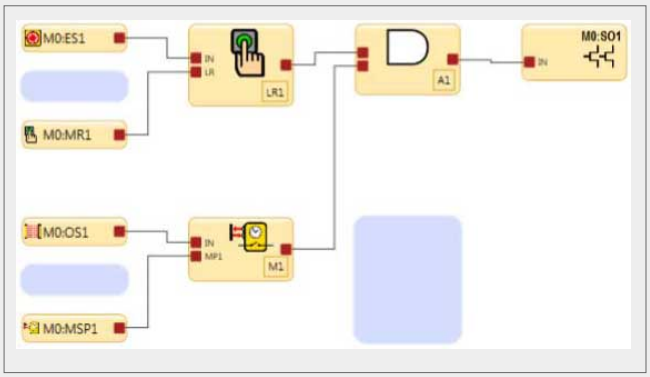
Contrôle incorrect de l'arrêt d'urgence
NON RECOMMANDÉ
La configuration en haut à droite illustre la sortie OS1 et le bouton d'arrêt d'urgence ES1 avec reset à verrouillage LR1 connectés à une fonction d'inhibition via la fonction AND. Dans ce cas, ES1 et OS1 seront tous deux inhibés.

S'il y a un cycle d'inhibition actif en cours et que l'opérateur actionne le bouton d'arrêt d'urgence (passage à l'état Stop), SO1 ne se désactivera pas. Cela entraîne une perte de la commande de sécurité et peut générer une situation dangereuse.



Contrôle correct de l'arrêt d'urgence
La configuration à droite illustre la sortie OS1 connectée directement au bloc d'inhibition M1. Tant M1 que ES1 sont des entrées de AND A1. Dans ce cas, M1 et ES1 contrôlent SO1.

S'il y a un cycle d'inhibition actif en cours et que l'opérateur actionne le bouton d'arrêt d'urgence (passage à l'état Stop), SO1 sera désactivée.



Les boutons d'arrêt d'urgence, les interrupteurs à câble, les appareils de commande, la surveillance des commutateurs externes et les interrupteurs de dérivation sont des dispositifs ou des fonctions qui ne peuvent pas être inhibés.

Pour inhiber correctement la protection principale, la conception d'un système d'inhibition doit :

1. Identifier les parties du cycle machine qui sont sans risques ;
2. Sélectionner les dispositifs d'inhibition adéquats ;
3. Intégrer le montage et l'installation corrects de ces dispositifs.

AVERTISSEMENT:
- **Les opérations d'inhibition et de dérivation doivent être effectuées de façon à minimiser le risque au personnel.**
- Le non-respect de ces consignes pourrait entraîner une situation dangereuse susceptible de provoquer des blessures graves, voire mortelles.
- Pour prévenir une suspension non voulue du signal d'arrêt, utilisez une ou plusieurs paires de capteurs d'inhibition à redondance diverse ou un interrupteur de dérivation double voie à clé.
- Réglez des limites de temps raisonnables (pas plus longues que nécessaire) pour les fonctions d'inhibition et de dérivation.

Le contrôleur de sécurité peut surveiller et répondre aux signaux redondants qui initient l'inhibition. L'inhibition suspend alors la fonction de protection en ignorant l'état du dispositif d'entrée auquel la fonction d'inhibition a été assignée. Cela permet à un objet ou à une personne de pénétrer dans la zone de détection d'une barrière immatérielle de sécurité sans déclencher de commande d'arrêt. Il ne faut pas la confondre avec le « masquage » qui désactive un ou plusieurs faisceaux d'une barrière immatérielle de sécurité, augmentant ainsi sa résolution.

La fonction d'inhibition peut être déclenchée par divers dispositifs externes. Elle propose plusieurs options afin de personnaliser le système en fonction des exigences d'une application spécifique.

Si vous utilisez une paire de dispositifs d'inhibition, ceux-ci doivent être déclenchés simultanément (à trois secondes d'intervalle maximum). Cela permet de réduire le risque de contournement ou défaillance de mode commun. L'inhibition directionnelle, qui exige que la paire de capteurs 1 soit bloquée en premier, peut également limiter le risque de contournement.

Chaque opération d'inhibition exige au moins deux capteurs d'inhibition. L'inhibition se produit généralement 100 ms après l'activation de l'entrée du deuxième capteur d'inhibition. Une ou deux paires de capteurs d'inhibition peuvent être assignées à une ou plusieurs entrées de sécurité de sorte que les sorties de sécurité qui leur sont assignées puissent rester activées (ON) pour achever l'opération.

AVERTISSEMENT:
- **L'inhibition n'est autorisée que pendant la partie non dangereuse du cycle machine**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- La fonction d'inhibition doit être conçue de façon à ce qu'aucune défaillance d'un composant unique n'empêche la commande d'arrêt de la machine et de ses cycles suivants jusqu'à ce que la défaillance soit réparée (conformément aux normes ISO 13849-1 et ANSI B11.19).

AVERTISSEMENT:
- **Les entrées d'inhibition doivent être redondantes**
- Un dispositif unique, avec plusieurs sorties, pourrait tomber en panne et entraîner une inhibition du système à un moment inopportun, susceptible de créer un risque.
- Il n'est pas recommandé d'utiliser un interrupteur, un dispositif ou un relais unique avec deux contacts normalement ouverts pour les entrées d'inhibition.

11.5.1 Attributs d'inhibition facultatifs

L'entrée paire de capteurs d'inhibition et le bloc d'inhibition possèdent plusieurs fonctions facultatives qui permettent de limiter les manipulations non autorisées et la possibilité d'un cycle d'inhibition imprévu.

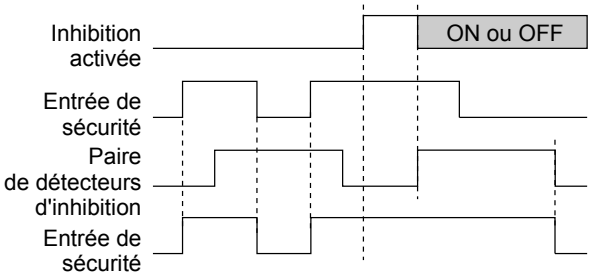
Activation de l'inhibition (ME)

L'entrée Activation de l'inhibition est une entrée non dédiée à la sécurité. Lorsque l'entrée est fermée, ou active dans le cas d'une entrée virtuelle, le contrôleur de sécurité autorise une inhibition. L'ouverture de cette entrée pendant que le système est inhibé n'a aucune incidence.

Exemples typiques d'utilisation de la fonction d'activation de l'inhibition (ME) :
- Elle permet à la logique de commande de la machine de définir une durée pour démarrer un cycle d'inhibition
- Bloquer l'inhibition
- Limiter les chances de contournement non autorisé ou non intentionnel du système de sécurité

La fonction Activation de l'inhibition en option peut être configurée de façon à ce que l'inhibition ne soit permise que pendant le temps approprié. Si un dispositif d'entrée avec activation de l'inhibition a été assigné à un bloc d'inhibition, le dispositif d'entrée de sécurité ne peut être inhibé que si l'interrupteur d'activation de l'inhibition est en état activé (24 Vcc), ou activé dans le cas d'une entrée virtuelle, au moment du démarrage du cycle d'inhibition. Un dispositif d'entrée avec activation de l'inhibition peut être dédié à un ou plusieurs blocs d'inhibition.

Illustration 156. Logique de temporisation — Paire de capteurs d'inhibition avec activation de l'inhibition



Fonction de reset de la simultanéité de la temporisation

L'entrée Inhibition activée peut également servir à remettre à zéro la simultanéité de la temporisation. Si une entrée est activée pendant plus de trois secondes avant que la seconde entrée ne s'active, la simultanéité de temporisation empêche le cycle d'inhibition de se produire. Cette situation peut survenir suite à un arrêt normal d'une chaîne de montage qui entraîne le blocage d'un dispositif d'inhibition et l'expiration du temps imparti pour l'activation simultanée des deux dispositifs.

Si l'entrée Inhibition activée (ME) effectue un cycle (fermé-ouvert-fermé ou actif-inactif-actif pour une entrée virtuelle) alors qu'une entrée d'inhibition est active, la simultanéité de temporisation est remise à zéro et, si la seconde entrée d'inhibition devient active dans les 3 secondes, un cycle normal d'inhibition démarre. La fonction peut remettre à zéro la temporisation une seule fois par cycle d'inhibition (toutes les entrées d'inhibition M1–M4 doivent s'ouvrir avant qu'un autre reset soit possible).

Dérivation

Il est possible d'activer un **mode de dérivation/neutralisation** en cochant la case **BP (dérivation)** dans la fenêtre des propriétés **Bloc d'inhibition**. Deux modes de dérivation/neutralisation sont disponibles : **Dérivation** et **Neutralisation dépendante de l'inhibition**. Le mode **Dérivation** est utilisé pour dériver temporairement le dispositif de protection et activer la sortie du bloc fonction ou la conserver activée. Le mode **Neutralisation dépendante de l'inhibition** permet de neutraliser manuellement un cycle d'inhibition incomplet (par exemple après l'expiration du temps limite d'inhibition). Dans ce cas, un ou plusieurs capteurs d'inhibition doivent être activés pendant que la protection est en état d'arrêt pour initier la neutralisation.

Sortie de voyant d'inhibition (ML)

Selon l'étude de risques et les normes applicables, certaines applications exigent l'utilisation d'un voyant (ou d'un autre moyen) pour signaler l'inhibition d'un dispositif de sécurité, par exemple un rideau lumineux. Le contrôleur de sécurité fournit un signal indiquant la suspension de la fonction de protection via la sortie d'état inhibé.

Important: Indication de l'état inhibé

Une indication visuelle de l'inhibition du dispositif de sécurité doit être en place et être clairement visible depuis l'emplacement du dispositif de sécurité inhibé. Le bon fonctionnement de ce voyant doit être vérifié régulièrement par l'opérateur.

Limite de temps d'inhibition

La limite de temps d'inhibition permet à l'utilisateur de sélectionner une durée maximale d'inhibition. Cette fonction empêche le contournement intentionnel des dispositifs d'inhibition et le déclenchement d'une inhibition inappropriée. Elle est également utile pour détecter une défaillance de mode commun susceptible d'affecter tous les dispositifs d'inhibition de l'installation. Il est possible de définir une limite de temps comprise entre 1 seconde et 30 minutes, par incrément de 100 millisecondes (la valeur par défaut est 30 s). Cette limite de temps peut également être **infinie** (désactivée).

La temporisation commence dès le déclenchement du second dispositif d'inhibition (dans les 3 secondes suivant celui du premier dispositif). Lorsque le délai de temporisation expire, l'inhibition prend fin, quels que soient les signaux émis par les dispositifs d'inhibition. Si le dispositif d'entrée inhibé est en état off, la sortie du bloc d'inhibition correspondante est désactivée.

AVERTISSEMENT: Limite de temps d'inhibition. Sélectionnez une limite de temps d'inhibition infinie uniquement si la possibilité d'un cycle d'inhibition inapproprié ou imprévu est réduite au minimum, tel que défini et autorisé par l'étude des risques de la machine. L'utilisateur est tenu de s'assurer que cela ne provoque pas de situation dangereuse.

Temps de retard au déclenchement de l'inhibition

Il est possible de définir un temps de retard pour prolonger l'état Inhibé de 1, 2, 3, 4 ou 5 secondes après que la paire de capteurs d'inhibition ne signale plus une inhibition. Le retard au déclenchement est généralement utilisé avec les applications de « sortie uniquement » de cellules de travail protégées par une barrière immatérielle de sécurité avec des cap-

teurs d'inhibition installés d'un seul côté de la zone de détection. La sortie du bloc d'inhibition reste activée pendant un maximum de 5 secondes après que le premier dispositif d'inhibition est dégagé ou jusqu'à ce que l'entrée du dispositif de sécurité inhibé (entrée de bloc d'inhibition) repasse en état de marche, quel que soit l'ordre d'arrivée.

Inhibition à la mise sous tension

Cette fonction initie un cycle d'inhibition après la mise sous tension du contrôleur de sécurité. Si la fonction Inhibition à la mise sous tension est sélectionnée, elle initie un cycle d'inhibition dans les circonstances suivantes :

- L'entrée Inhibition activée est activée (On) (si elle est configurée).
- Les entrées du dispositif de sécurité sont activées (en mode marche).
- Les capteurs d'inhibition M1-M2 (ou M3-M4, si vous les utilisez mais jamais les 4 en même temps) sont fermés.

Si le **démarrage automatique** est configuré, le contrôleur de sécurité attend 2 secondes pour permettre aux dispositifs d'entrée qui ne sont pas immédiatement actifs à la mise sous tension de s'activer.

Si un **démarrage manuel** est configuré et que toutes les autres conditions sont satisfaites, le premier reset à la mise sous tension valide après l'activation des entrées de sécurité inhibées (état marche ou fermées) initie un cycle d'inhibition. La fonction d'inhibition à la mise sous tension ne doit être utilisée que si la sécurité est assurée au moment prévu du cycle d'inhibition et que l'utilisation de cette fonction a été confirmée par l'étude de risques et exigée pour le fonctionnement de cette machine.

AVERTISSEMENT: La fonction d'inhibition à la mise sous tension ne doit être utilisée que dans les applications suivantes :

- L'inhibition du système (MP1 et MP2 fermées) est nécessaire à la mise sous tension.
- Son utilisation n'expose en aucun cas le personnel à un danger.

Temps anti-rebond d'une paire de capteurs d'inhibition

Les temps anti-rebond d'entrée, accessibles sous la section **Avancé** de la fenêtre des propriétés **Paire de capteurs d'inhibition**, permettent de prolonger un cycle d'inhibition après la suppression d'un signal de capteur d'inhibition. En configurant le temps anti-rebond fermé à ouvert, il est possible de prolonger le cycle d'inhibition de 1,5 secondes (1500 ms) maximum pour permettre au dispositif d'entrée de sécurité de s'activer. Il est également possible de retarder le début du cycle d'inhibition en configurant le temps anti-rebond ouvert à fermé.

Exigences relatives à la fonction d'inhibition

Le début et la fin d'un cycle d'inhibition sont déclenchés par les signaux d'une paire de dispositifs d'inhibition. Les options de circuit de dispositif d'inhibition peuvent être configurées et consultées dans la fenêtre **Propriétés** de la paire de capteurs d'inhibition. Un signal d'inhibition est émis lorsque les deux voies du dispositif d'inhibition passent en état Inhibition activée pendant que la protection inhibée est en état marche.

Le contrôleur de sécurité surveille les dispositifs d'inhibition pour vérifier si leurs sorties sont activées à 3 secondes d'intervalle l'une de l'autre. Si les entrées ne répondent pas à cette condition de simultanéité, l'inhibition ne peut pas avoir lieu.

Il est possible d'utiliser plusieurs types et combinaisons de dispositifs d'inhibition, et notamment les suivants : des détecteurs photoélectriques, des capteurs de proximité inductifs, des interrupteurs de position, des commutateurs de sécurité à guidage positif et des interrupteurs à tige flexible.

Miroirs à renvoi d'angle, systèmes optiques de sécurité et inhibition

Les miroirs sont généralement utilisés avec des barrières immatérielles de sécurité et des systèmes de sécurité mono- ou multi-faisceaux pour protéger plusieurs côtés d'une zone dangereuse.

Si la barrière immatérielle est inhibée, la fonction de protection est suspendue de tous les côtés. Il doit être impossible pour une personne d'entrer dans la zone protégée sans qu'elle soit détectée et qu'une commande d'arrêt ait été envoyée au dispositif de commande de la machine. Cette protection supplémentaire est habituellement assurée par un ou plusieurs dispositifs supplémentaires qui restent actifs pendant l'inhibition de la protection principale.

Par conséquent, les miroirs sont généralement interdits dans les installations incluant un système d'inhibition.

Multiples dispositifs de détection de présence

L'inhibition de plusieurs dispositifs de sécurité de détection de présence (PSSD) ou d'un PSSD avec plusieurs champs de détection n'est pas recommandée, sauf s'il est impossible à une personne d'entrer dans la zone protégée sans être détectée et sans qu'un ordre d'arrêt ne soit envoyé à la commande de la machine.

Comme dans le cas d'utilisation des miroirs d'angle (voir Miroirs à renvoi d'angle, systèmes optiques de sécurité et inhibition à la page 163), si plusieurs champs de détection sont inhibés, il est possible qu'une personne passe par une zone ou un point d'accès inhibé et accède à la zone protégée sans être détectée.

Prenons l'exemple d'une application d'entrée/sortie où l'entrée d'une palette dans le poste déclenche le cycle d'inhibition. Si les dispositifs de détection de présence à l'entrée et à la sortie PSSD sont inhibés, un individu peut entrer dans la zone protégée par la « sortie » du poste. Une solution appropriée consiste à inhiber l'entrée et la sortie avec des dispositifs de protection distincts.

AVERTISSEMENT:

- **Ne protégez pas plusieurs zones avec des miroirs ou plusieurs champs de détection si du personnel est susceptible d'entrer dans la zone dangereuse pendant l'inhibition du système de sécurité et qu'il ne peut pas être détecté.**
- Si le personnel entre dans la zone dangereuse sans être détecté peut entraîner des blessures graves, voire mortelles.
- Vérifiez que toutes les zones sont protégées et qu'une commande d'arrêt est envoyée à la machine surveillée lorsqu'une personne accède à la zone dangereuse.

11.6 Bloc 1 impulsion

Le bloc 1 impulsion permet à l'utilisateur de configurer l'état d'impulsion d'un maximum de 5 minutes, par incréments de 1 ms. Cette fonction est disponible sur le XS/SC26 FID 4 et ultérieur.

Nœuds par défaut	Nœuds supplémentaires	Remarques
IN	CD	Un passage du signal d'entrée de l'état bas à haut déclenchera le passage du nœud de sortie à l'état haut pendant le temps configuré, puis sa désactivation.

Remarque: La durée réelle d'une impulsion peut être jusqu'à une fois plus longue que la durée de balayage définie.

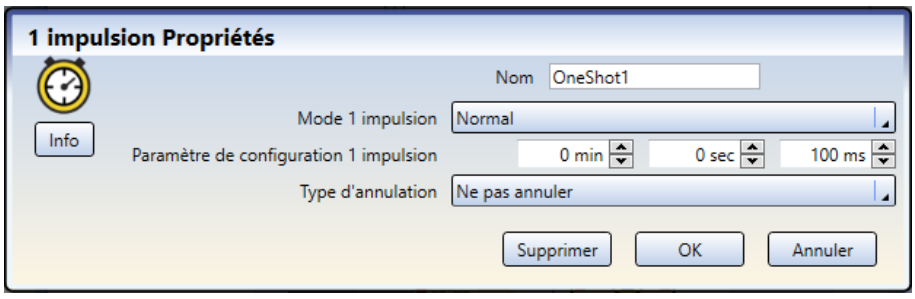
Le nœud Annulation de la temporisation est un nœud configurable pour le bloc 1 impulsion. L'entrée Annulation de la temporisation désactivera immédiatement le nœud de sortie du bloc 1 impulsion après sa détection (en raison des retards humains et système, des impulsions plus courtes se termineront très probablement avant de pouvoir annuler la temporisation).

PRÉCAUTION: Effet de la temporisation d'une impulsion sur le temps de réponse

La durée d'une impulsion peut augmenter considérablement le temps de réponse du contrôleur de sécurité. Cela a un impact sur le positionnement des dispositifs de protection, dans la mesure où l'installation de ceux-ci est déterminée selon des formules de distance (minimale) de sécurité ou dépendent du temps nécessaire pour parvenir à un état non dangereux. Il faut donc tenir compte de l'augmentation du temps de réponse pour l'installation des dispositifs de protection.

Remarque: Le temps de réponse indiqué dans l'onglet Résumé de la configuration est le temps maximum modifiable selon l'utilisation faite des blocs de temporisation, des blocs 1 impulsion et autres blocs logiques (par ex. des fonctions OR). L'utilisateur est responsable du choix, de la vérification et de l'incorporation du temps de réponse adéquat.

*Illustration 157. **Propriétés du bloc fonction 1 impulsion***



La fenêtre des propriétés du bloc fonction 1 impulsion permet de configurer les éléments suivants :

Nom

Crée un nom de 10 caractères maximum pour le bloc fonction.

Mode 1 impulsion

- Normal
- Pulsation

Paramètre de configuration 1 impulsion

Durée d'impulsion unique : de 1 ms à 5 minutes, par incréments de 1 ms.

La valeur par défaut est de 100 ms.

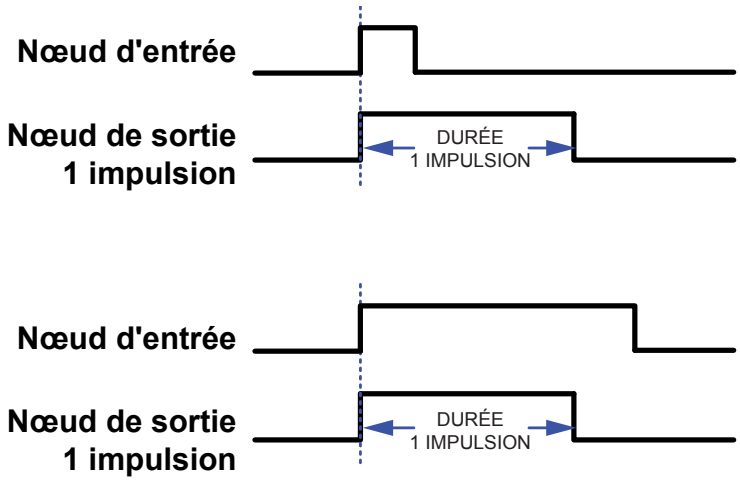
Type d'annulation

- Ne pas annuler
- Nœud d'annulation de la temporisation

Mode 1 impulsion

Lorsque le mode normal est sélectionné, le nœud de sortie s'active lorsque le nœud d'entrée s'active. La sortie reste activée pendant la durée définie pour le paramètre 1 impulsion, indépendamment de tout changement d'état de l'entrée. (Voir Illustration 158 à la page 165 pour les diagrammes de synchronisation 1 impulsion en mode normal.)

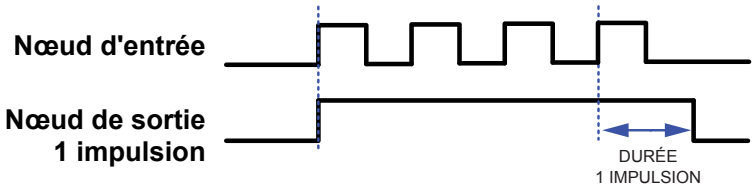
Illustration 158. Diagrammes de synchronisation 1 impulsion en mode normal



Remarque: La durée d'activation de la sortie de sécurité sera réduite du retard à l'activation de la sortie de sécurité (environ 60 ms). Plus la durée de l'impulsion unique est courte, plus la réduction est importante (pourcentage plus important de l'impulsion requise).

Lorsque le mode Pulsation est sélectionné, le nœud de sortie s'active en même temps que le nœud d'entrée. La sortie reste activée pendant la durée définie pour le paramètre 1 impulsion. Le minuteur défini pour l'impulsion unique sera remis à zéro si le nœud d'entrée se désactive puis se réactive. (Voir Illustration 159 à la page 165 pour consulter un diagramme de synchronisation 1 impulsion en mode pulsation.)

Illustration 159. Diagramme de synchronisation 1 impulsion en mode pulsation



11.7 Commande de presse

Le bloc fonction Commande de presse est conçu pour être utilisé avec des presses hydrauliques/pneumatiques simples. Cette fonction est disponible sur le XS/SC26 FID 4 et ultérieur.

Les normes suivantes s'appliquent :

B11.2-2013, Safety Requirements for Hydraulic and Pneumatic Power Presses (Exigences de sécurité pour les presses hydrauliques et pneumatiques)
EN ISO 16092-1:2018, Sécurité des machines-outils — Presses — Partie 1 : Exigences générales de sécurité
EN ISO 16092-3 Sécurité des machines-outils — Presses — Partie 3 : Exigences de sécurité pour les presses hydrauliques
EN ISO 16092-4 Sécurité des machines outils — Presses — Partie 4 : Exigences de sécurité pour les presses pneumatiques

L'utilisateur est seul responsable de la conformité de son application avec ces normes et toute autre norme appropriée (y compris les autres normes relatives aux presses).

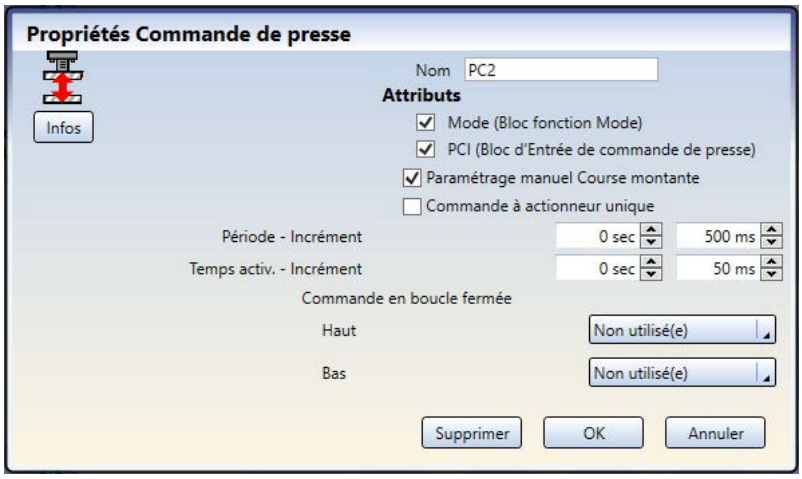
AVERTISSEMENT:
- Le bloc fonction Commande de presse comprend un dispositif de démarrage (qui déclenche un mouvement dangereux).
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- La personne qualifiée doit s'assurer que l'activation (passage à l'état ON) d'un dispositif de sécurité à l'arrêt (bouton d'arrêt d'urgence, interrupteur à câble, capteur optique, tapis de sécurité, arrêt de sécurité, etc.) par un utilisateur ne déclenche pas de mouvement dangereux lorsqu'il est raccordé à un bloc fonction Commande de presse déjà activé (état ON).

AVERTISSEMENT:
- Installez correctement ce dispositif.
- C'est à l'utilisateur qu'il incombe de vérifier que ce dispositif Banner Engineering est installé et raccordé à la machine surveillée par des personnes qualifiées conformément aux réglementations de sécurité applicables et aux instructions de ce manuel. Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Si les procédures de montage, d'installation, de raccordement et de vérification n'ont pas été respectées, le dispositif Banner Engineering ne sera pas en mesure d'offrir la protection pour laquelle il a été conçu. L'utilisateur est responsable de la conformité à l'ensemble des lois, règles, réglementations et codes locaux, régionaux et nationaux concernant l'installation et l'utilisation de ce système de commande dans le cadre de toute application particulière. Assurez-vous que toutes les exigences légales sont respectées, de même que toutes les instructions techniques d'installation et de maintenance de ce manuel.

Nœuds par défaut	Nœuds supplémentaires	Remarques
GO TOS BOS RST NM Sécurité	Mode PCI	Lors de la sélection des entrées Mode ou PCI (Press Control Input), chacune génère son propre bloc fonction d'entrées connectées au bloc fonction Commande de presse. Pour des informations complémentaires, voir Bloc fonction Mode à la page 167 et Bloc fonction Entrées de commande de presse à la page 167.

Le bloc fonction Commande de presse comprend des attributs qui peuvent être activés ou désactivés.

Illustration 160. ***Propriétés de commande de presse***



Les nœuds supplémentaires qui peuvent être ajoutés au bloc fonction Commande de presse génèrent de nouveaux blocs fonction qui leur sont propres. Le bloc de fonction Mode est ajouté si l'attribut Mode est sélectionné. Le bloc fonction Entrées de commande de presse est ajouté si la case de l'attribut PCI est activée. Les deux autres attributs, Paramétrage manuel Course montante et Commande à actionneur unique, ne peuvent pas être sélectionnés tous les deux en même temps.

Lorsque le paramétrage manuel Course montante est configuré, l'entrée GO doit être maintenue activée pendant tout le cycle (montée et descente). Le nœud d'entrée GO ne peut être connecté qu'à une entrée de commande bimanuelle ou à une entrée d'interrupteur au pied.

Lorsque la commande à actionneur unique est configurée, l'entrée GO fonctionne comme un bouton de démarrage et ne doit donc être maintenue en position ON que le temps nécessaire au démarrage du processus. Le nœud d'entrée GO ne peut être connecté qu'à une entrée de démarrage de cycle, une entrée d'interrupteur au pied ou une entrée de commande bimanuelle.

AVERTISSEMENT:
- Considérations relatives aux dangers de la course montante d'une presse.
- Si un danger existe pendant la course montante, le fait de ne pas utiliser le paramétrage manuel Course montante peut entraîner des blessures graves ou mortelles.
- Pour la commande à actionneur unique, la course montante de la presse ne doit présenter aucun danger car l'entrée d'arrêt d'urgence inhibable est inhibée pendant la course montante.

L'autre fonction du bloc fonction Commande de presse est la **commande en boucle fermée**. L'activation de la **commande en boucle fermée** oblige le contrôleur à vérifier que les dispositifs connectés aux sorties indiquées ont été désactivés au moment de la réception de la commande, avant d'activer la sortie suivante. Pour des informations complémentaires, voir Commande en boucle fermée à la page 171.

11.7.1 Bloc fonction Mode

Le bloc fonction Mode est ajouté si l'attribut Mode est sélectionné dans les **propriétés de commande de presse**.

La sélection du bloc fonction Mode permet d'ajouter un sélecteur de fonction. Les trois entrées du bloc de fonction Presse sont Run (Marche), Inch Up (Montée par à-coups) et Inch Down (Descente par à-coups).

Remarque: Selon les normes en vigueur pour les presses, le sélecteur de mode (ou menu) doit avoir au minimum ces trois positions et une position OFF (Arrêt). La position OFF ne serait pas un état OFF de sécurité, mais une presse dans un état de non-fonctionnement (non connectée au contrôleur, mais avec aussi les trois entrées Mode en état OFF). Si les 3 entrées de mode sont inactives/OFF, alors le bloc fonction Mode presse reste désactivé (rouge).

Illustration 161. Entrées du bloc fonction Commande de presse



Lorsque le bloc fonction Mode est sélectionné dans le bloc fonction Commande de presse, les attributs Inch Period (Période - Incrément) et Inch On Time (Temps activ. - Incrément) sont ajoutés au bloc fonction Commande de presse. Ces paramètres sont des valeurs définies par l'utilisateur pour leur système afin d'éviter un mouvement trop rapide de la presse lors de l'approche par à-coups (généralement utilisés en mode de réglage).

Remarque: La norme EN ISO 16092-3:2018 spécifie que la vitesse d'approche par à-coups ne peut dépasser 10 mm/seconde en mode d'approche par à-coups.

- Une approche par à-coups est un mouvement intermittent du coulisseau pour le faire monter ou descendre lentement, généralement aux fins d'entretien ou de réglage de la matrice.
- La **période - incrément** représente la durée du cycle complet, de la mise en marche à l'arrêt, d'un mouvement intermittent du coulisseau.
- Le **temps d'activation - incrément** est la partie active de cette période (activation de la période de sortie pour entraîner le mouvement du coulisseau).
- Lors du réglage de la période et du temps d'activation, tenez compte des retards au déclenchement et à l'arrêt du mouvement afin de garantir une vitesse d'approche adéquate si l'entrée GO est maintenue fermée pendant plusieurs périodes d'approche.

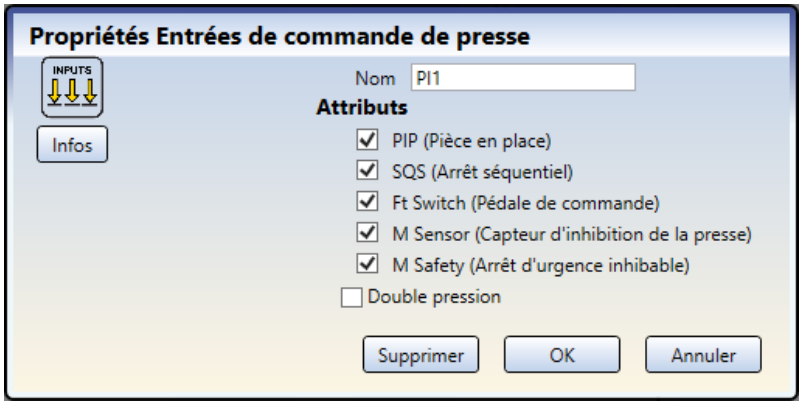
AVERTISSEMENT:
- Vitesse de la presse en mode Approche par à-coups.
- Une vitesse excessive du coulisseau en mode Approche par à-coups peut entraîner des blessures graves ou mortelles.
- Il faut faire attention au réglage des valeurs Période - Incrément et Temps d'activ. - Incrément pour garantir une vitesse d'approche du coulisseau sans danger en mode Approche par à-coups.

11.7.2 Bloc fonction Entrées de commande de presse

Le bloc fonction Entrées de commande de presse est ajouté si la case d'attribut PCI est sélectionnée dans la page des **propriétés de commande de presse**.

Lorsque le bloc fonction PCI est sélectionné, d'autres attributs de commande de presse peuvent être activés.

Illustration 162. ***Propriétés des entrées de commande de presse***



Les nœuds par défaut du bloc PCI sont l'entrée **PIP** (pièce en place), l'entrée **SQS** (arrêt séquentiel) et l'entrée **M Safety** (arrêt d'urgence inhibable). Audience=BannerSi **SQS** est sélectionné, les entrées **Ft Switch** (Interrupteur au pied) et **M Sensor** (capteur d'inhibition de la presse) sont disponibles en option et l'attribut Dual Pressure (double pression) devient disponible (ce qui permet d'ajouter des sorties haute et basse pression aux sorties standard de montée et de descente).

Utilisez l'entrée PIP dans les commandes de presse où la presse ne doit pas fonctionner en l'absence de pièces. L'entrée PIP doit être haute pour que le cycle de la presse démarre. Après que la presse quitte le point BOS, l'entrée PIP doit passer à l'état bas, puis revenir à l'état haut, avant que le cycle de presse suivant puisse être lancé ; cela peut se produire avant ou après que la presse atteigne le point TOS.

Utilisez l'entrée SQS dans les commandes de la presse où le coulisseau de la presse est abaissé jusqu'à un point jugé sans danger pour les doigts. À ce stade, l'entrée d'arrêt d'urgence inhibable peut être inhibée, l'opérateur peut relâcher l'entrée de commande bimanuelle (TC1) (configurée sur l'entrée GO du bloc fonction Commande de presse) et peut saisir la pièce, si nécessaire. L'activation de l'entrée Ft Switch (FS1) entraînera le coulisseau de la presse vers le bas de la course, où il s'arrêtera.

Remarque: Ce qui précède est une méthode de contrôle du processus de commande de presse avec un arrêt séquentiel configuré. Il existe trois processus autorisés :

1. TC1 active l'entrée GO pour entraîner le coulisseau au point SQS. Relâchez TC1 et engagez le FS1 pour activer l'entrée Ft Switch et entraîner le coulisseau vers le point BOS, relâchez FS1 et engagez TC1 pour monter le coulisseau.
2. FS1 active l'entrée GO pour entraîner le coulisseau au point SQS. Relâchez FS1. La réactivation de FS1 entraîne le coulisseau au point BOS, puis le ramène au point TOS. (L'entrée Ft Switch disparaît lorsque FS1 est connecté au nœud GO.)
3. TC1 active l'entrée GO pour entraîner le coulisseau au point SQS. Vous pouvez alors relâcher TC1. La réactivation de TC1 entraîne le coulisseau au point BOS, puis le ramène au point TOS. (Pour configurer le système pour cette méthode, ne sélectionnez PAS le nœud Ft Switch dans le bloc fonction Entrées de commande de presse.)

L'entrée M Sensor peut être utilisée conjointement avec l'entrée SQS pour inhiber l'entrée d'arrêt d'urgence inhibable lorsqu'elle atteint une position sans danger pour les doigts.

Lorsque l'entrée SQS et l'option Dual Pressure (double pression) sont configurées dans le bloc fonction Entrées de commande de presse, deux nouvelles sorties sont ajoutées au bloc fonction Commande de presse. Les nœuds de sortie **H** (Haut) et **L** (Bas) sont ajoutés en plus des sorties standard **U** (course montante, débrayage ou course retour) et **D** (course descendante, embrayage, ou course aller). H permet d'engager la haute pression pour terminer la dernière partie de la course. L permet d'engager la pression standard (basse) pour amener le coulisseau au point SQS et puis le ramener à sa position de départ.

Illustration 163. Bloc Entrées de commande de presse

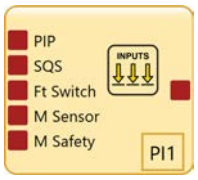
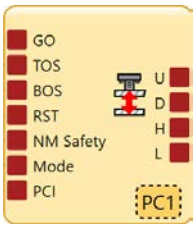


Illustration 164. Bloc fonction Commande de presse

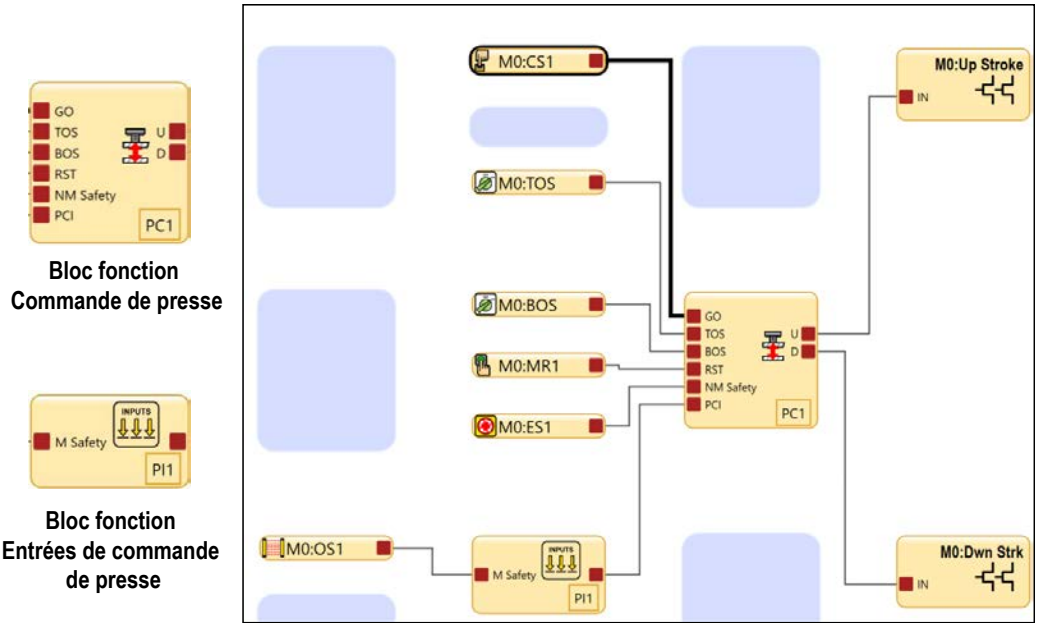


11.7.3 Exemples de bloc fonction de commande de presse

Cette section comprend deux exemples de configuration.

Voici un exemple de configuration simple pour une petite presse.

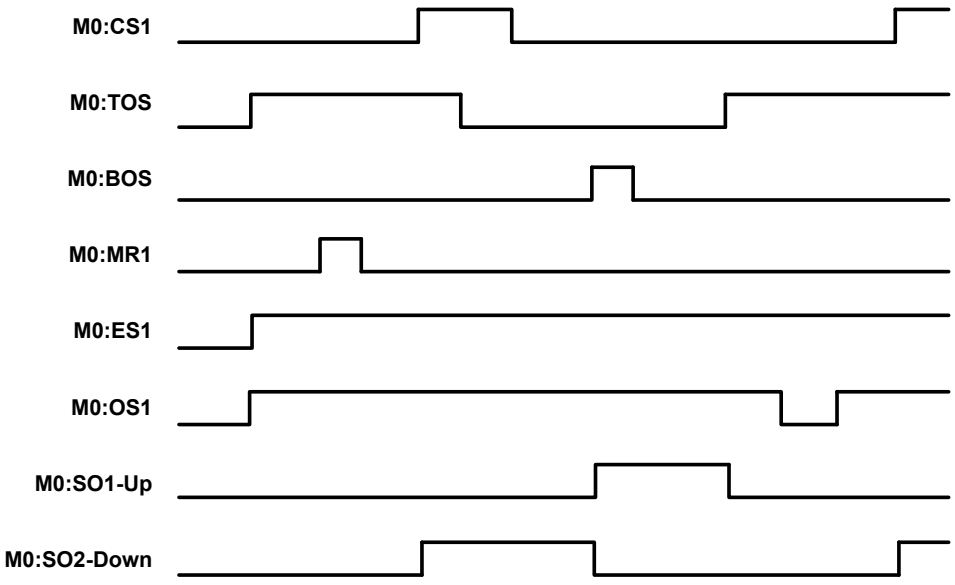
Illustration 165. Exemple de configuration pour une petite presse



Pour que le bloc fonction Commande de presse fonctionne correctement, il faut un enchaînement adéquat des signaux d'entrée. ES1, OS1 et TOS doivent être en état de marche (Run) (et avoir fait l'objet d'un reset) avant que l'entrée CS1 puisse activer la sortie appropriée. Cette configuration utilise une commande à actionneur unique. Par conséquent, une fois que l'entrée CS1 a lancé le processus, c'est l'entrée ES1, l'entrée OS1 ou la fin du cycle (réactivation de TOS) qui contrôle la désactivation. Consultez le diagramme temporel ci-dessous ou la description de la simulation à la section XS/SC26 : Exemple de configuration d'une commande de presse simple avec arrêt d'urgence inhibable à la page 97.

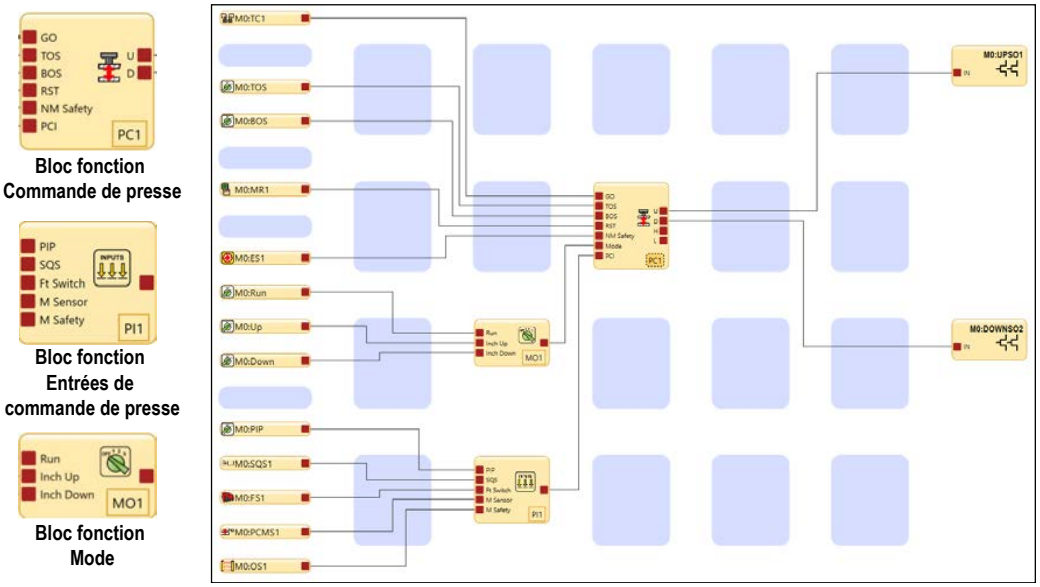
Le diagramme temporel suivant illustre la séquence (enchaînement) correcte des entrées du bloc fonction Commande de presse, laquelle permet le bon fonctionnement des sorties lorsque la commande à actionneur unique est activée.

Illustration 166. Commande de la presse — Diagramme temporel, commande à actionneur unique



Voici une configuration utilisant la plupart des fonctionnalités du bloc fonction Commande de presse.

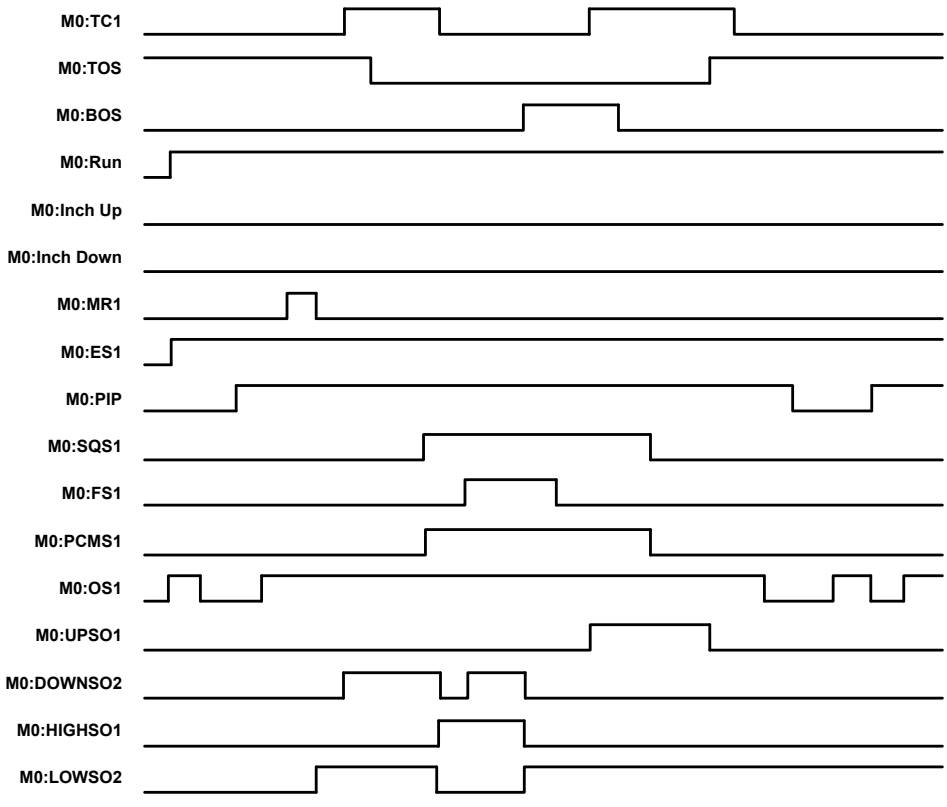
Illustration 167. Commande de presse — Exemple de configuration



Pour que le bloc fonction Commande de presse fonctionne correctement, il faut un enchaînement adéquat des signaux d'entrée. Cette configuration utilise le paramétrage manuel Course montante. ES1, OS1, PIP et TOS doivent être en état de marche (Run) (et avoir fait l'objet d'un reset) avant que l'entrée TC1 puisse activer la sortie appropriée. Pendant la course descendante, l'entrée TC1 lance le processus, après quoi c'est l'entrée ES1, l'entrée OS1, l'entrée TC1 ou l'activation de l'arrêt séquentiel (SQS est activé) qui a le contrôle la désactivation. Lorsque la presse atteint le point SQS (SQS et PCMS sont activés), elle s'arrête et OS1 est inhibé. La commande TC1 peut être relâchée. Pour terminer la course, activez l'entrée FS1. Pendant le reste de la course descendante, c'est l'entrée ES1, l'entrée FS1 ou l'accès à la position BOS (qui s'active) qui a le contrôle de la désactivation. Lorsque la séquence atteint l'entrée BOS, la FS1 est relâchée et TC1 est utilisé pour ramener la presse à la position TOS. Pendant la course montante, c'est l'entrée TC1, l'entrée ES1, l'entrée OS1, ou l'accès à la position TOS qui ont le contrôle de la désactivation. Consultez le diagramme temporel ci-dessous ou la description de la simulation à la section XS/SC26 : Exemple de configuration d'une commande de presse avec fonctionnalités complètes à la page 100.

Le diagramme temporel suivant illustre la séquence (enchaînement) correcte des entrées du bloc fonction Commande de presse, laquelle permet le bon fonctionnement des sorties lorsque le paramétrage manuel Course montante est activé.

Illustration 168. Commande presse — Diagramme temporel, paramétrage manuel Course montante



11.7.4 Commande en boucle fermée

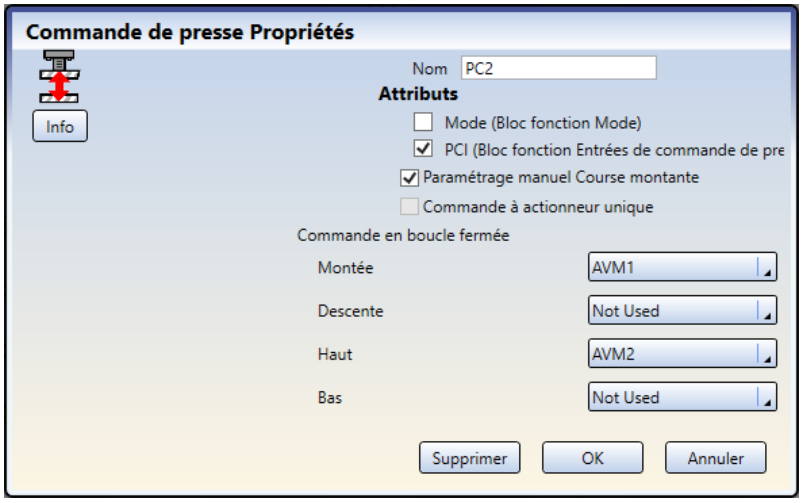
Le bloc fonction Commande de presse offre notamment la possibilité d'activer la commande en boucle fermée.

L'activation de la commande en boucle fermée oblige le contrôleur à vérifier que les dispositifs connectés aux sorties indiquées ont été désactivés au moment de la réception de la commande, avant d'activer la sortie suivante.

Pour utiliser la commande en boucle fermée :

1. Un nœud AVM doit être ajouté à la sortie de sécurité souhaitée pilotée par le bloc fonction Commande de presse.
2. L'entrée AVM fournit une indication de l'état de cette vanne de la presse.
3. Le bloc fonction Commande de presse doit être configuré pour la commande en boucle fermée sortie par sortie. Voir **Propriétés de la commande de presse** dans la figure suivante.

Illustration 169. Commande en boucle fermée



Dans cet exemple, la commande en boucle fermée est configurée pour s'assurer que la vanne de sortie en position montante a été désactivée avant d'autoriser toute autre fonction. Elle s'assure également que la vanne à l'état haut a été fermée avant d'engager la sortie en position montante.

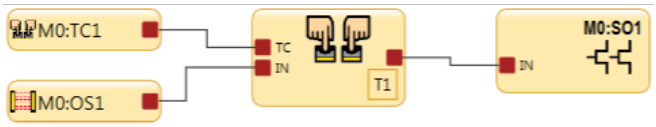
11.8 Bloc Commande bimanuelle (pour XS/SC26 FID 3 et antérieurs et SC10-2 FID 1)

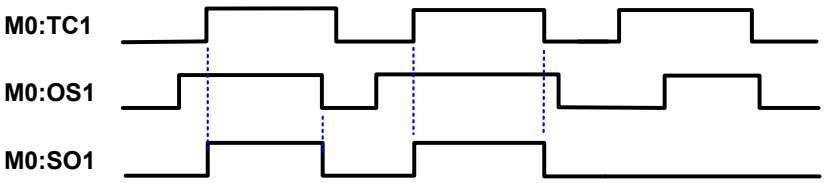
Illustration 170. Chronogramme — Bloc de commande bimanuelle

Nœuds par défaut	Nœuds supplémentaires	Remarques
TC (jusqu'à 4 nœuds TC)	IN MP1 ME	Les entrées de commandes bimanuelles doivent être connectées soit directement à un bloc de commande bimanuelle, soit indirectement via un bloc de dérivation connecté à un bloc de commande bimanuelle. Il n'est pas possible d'utiliser une entrée de commande bimanuelle sans un bloc de commande bimanuelle. Utilisez le nœud IN pour connecter les dispositifs d'entrée qui doivent être actifs (On) avant de pouvoir activer les sorties de la commande bimanuelle.



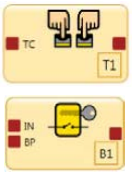
Bloc fonction de commande bimanuelle



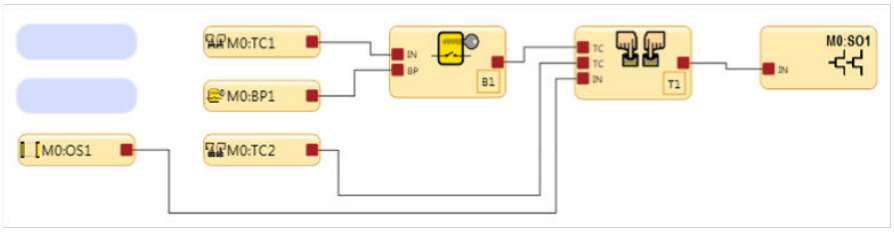


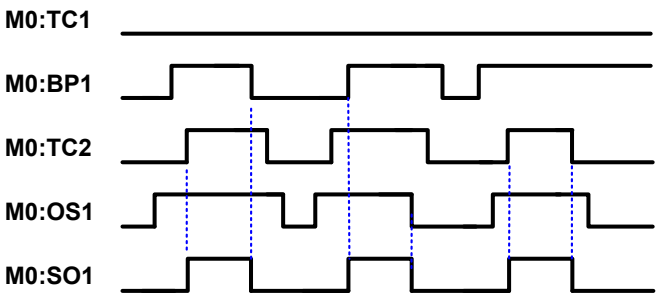
Soit l'entrée TC1, soit l'entrée OS1 a le contrôle de la désactivation.
OS1 doit être en état Run avant que TC1 puisse activer la sortie de of T1 et SO1.

Illustration 171. Chronogramme — Bloc de commande bimanuelle et blocs de dérivation



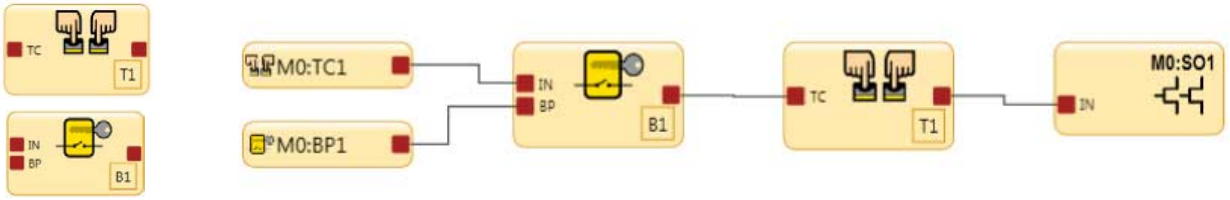
Blocs fonction Commande bimanuelle et Dérivation



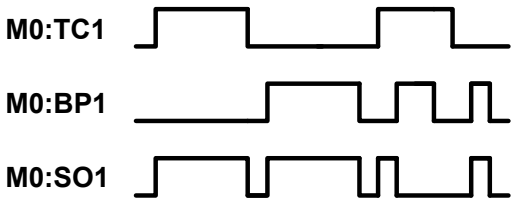


OS1 doit passer à l'état Marche (Run) avant que TC2 ne passe à l'état Marche. BP1 peut passer à l'état Marche avant ou après OS1. Si OS1 est dans l'état Marche, la séquence de transition de TC2 ou BP1 vers l'état Marche n'a pas d'importance. Le dernier à passer à l'état Marche fera passer le bloc fonction T1 à l'état Marche.

Illustration 172. Chronogramme — Bloc de commande bimanuelle et blocs de dérivation avec une (1) entrée de commande bimanuelle

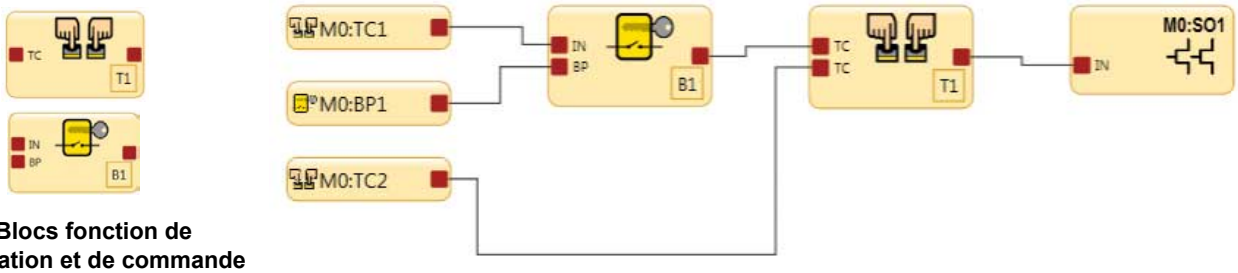


Blocs fonction de dérivation et de commande bimanuelle

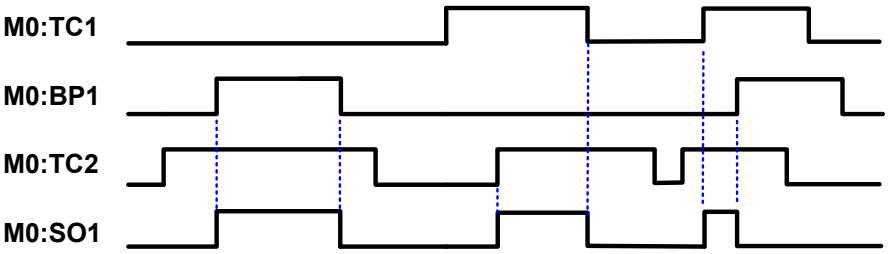


Si les deux actionneurs TC1 et l'interrupteur de dérivation BP1 sont actifs en même temps, la sortie du bloc fonction de dérivation B1 et la sortie du bloc fonction de commande bimanuelle se désactivent. Les sorties de B1 et T1 ne s'activent que lorsque les actionneurs TC1 ou l'interrupteur BP1 sont en état Run.

Illustration 173. Chronogramme — Bloc de commande bimanuelle et blocs de dérivation avec deux (2) entrées de commande bimanuelle

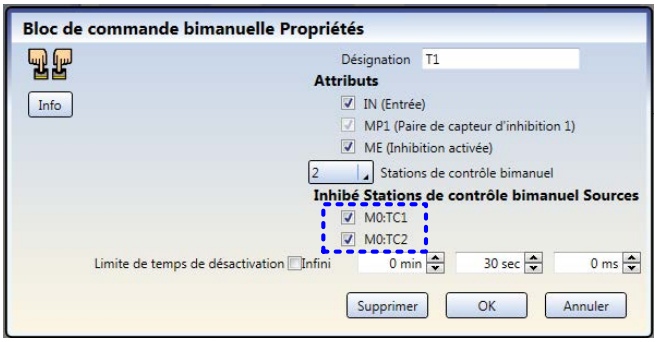


Blocs fonction de dérivation et de commande bimanuelle



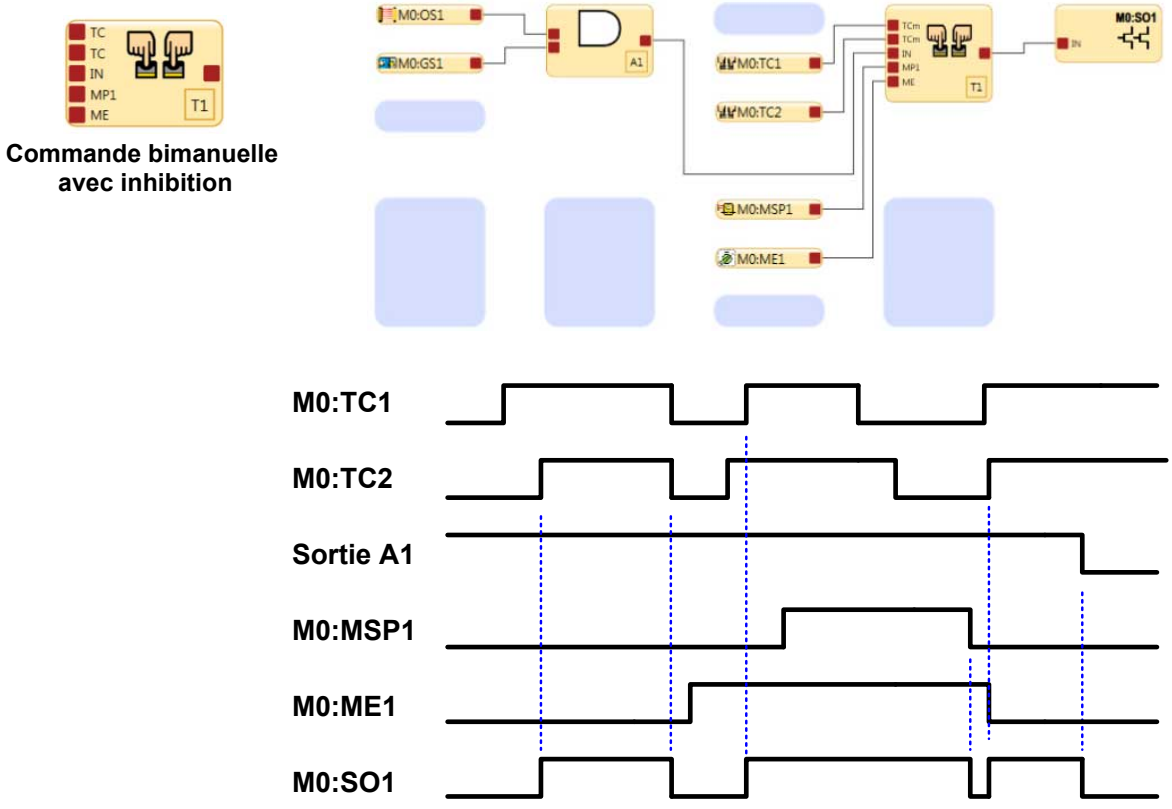
La fonction de dérivation peut être utilisée avec les actionneurs TC2 pour activer la sortie de sécurité. Lorsque les actionneurs TC1 ne sont pas dérivés, ils doivent être utilisés avec les actionneurs TC2 pour activer la sortie de sécurité. Si les actionneurs TC1 et l'interrupteur de dérivation sont tous en état Run, TI et SO1 ne peuvent pas être activés ou se désactiveront.

Illustration 174. Options d'inhibition de commande bimanuelle



Pour configurer l'option d'inhibition de commande bimanuelle, les actionneurs de la commande doivent d'abord être connectés au bloc fonction de commande bimanuelle dans la Vue fonctionnelle. Les cases à cocher (carré bleu ci-dessus) du menu Propriétés afficheront les noms de tous les dispositifs d'entrée de commande bimanuelle (TC). Seules les cases des stations THx qui sont cochées seront inhibées.

Illustration 175. Chronogramme — Bloc de commande bimanuelle avec inhibition



Les actionneurs TC1 et TC2 peuvent déclencher un cycle de commande bimanuel quel que soit l'état de l'activation de l'entrée Inhibition activée (ME1) (activée ou désactivée). ME1 doit être actif pour que les capteurs d'inhibition MSP1 maintiennent la sortie de sécurité activée une fois que les commandes TC1 et TC2 sont dans l'état Stop.

Protection contre l'activation d'une commande bimanuelle à la mise sous tension. La logique de commande bimanuelle du contrôleur de sécurité n'autorise pas l'activation de la sortie de sécurité assignée lors de la mise sous tension initiale alors que les commandes manuelles (THC) sont en état « marche ». Les commandes bimanuelles doivent passer à l'état d'arrêt puis retourner à l'état marche avant que la sortie de sécurité ne puisse s'activer. Une sortie de sécurité associée à un dispositif de commande bimanuelle n'offre aucune possibilité de reset manuel.

11.9 Bloc Commande bimanuelle (XS/SC26 FID 4 et ultérieur et SC10-2 FID 2 et ultérieur)

Dans les contrôleurs XS/SC26 FID 4 et ultérieur et SC10-2 FID 2 et ultérieur, l'entrée TC peut être directement mappée à une sortie ou à un bloc logique. Le bloc fonction Commande bimanuelle peut être directement mappé à une sortie ou à un bloc fonction.

Si plusieurs opérateurs sont affectés à une même machine et que chacun d'eux doit actionner sa commande bimanuelle, utilisez le bloc fonction Commande bimanuelle dans lequel il est possible de sélectionner plusieurs entrées TC.

Si le système est équipé d'une fonction de blocage (les entrées TC déclenchent une action qui garantit la sécurité du système de sorte que les opérateurs puissent retirer leurs mains pendant l'achèvement du processus), utilisez le bloc fonction Commande bimanuelle avec la fonction Inhibition sélectionnée.

Si la machine est équipée de dispositifs de sécurité dont certaines conditions doivent être satisfaites (et le rester) pour que l'entrée TC puisse la faire fonctionner, utilisez le bloc fonction Commande bimanuelle avec le nœud IN sélectionné.

- Si le nœud IN est désactivé, l'activation de l’entrée TC ne déclenche aucune action.
- Si le bloc fonction Commande bimanuelle est activé et que le bloc TC se désactive, la sortie est désactivée.
- Lorsque le nœud IN repasse à l'état haut, la sortie reste désactivée jusqu'à ce que l'entrée TC se désactive et se réactive.

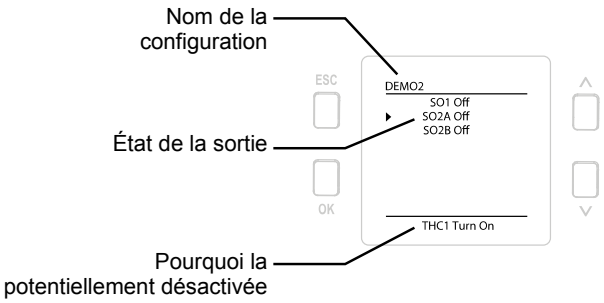
AVERTISSEMENT:

- Les commandes bimanuelles sont des dispositifs de démarrage (qui initient un mouvement dangereux).
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- La personne qualifiée doit s'assurer que l'activation (passage à l'état ON) d'un dispositif d'arrêt de sécurité (bouton d'arrêt d'urgence, interrupteur à câble, capteur optique, tapis de sécurité, arrêt de sécurité, etc.) par un utilisateur ne déclenche pas de mouvement dangereux lorsqu'il est connecté logiquement à une entrée TC ou à un bloc fonction Commande bimanuelle déjà activé (état ON).

12 Interface embarquée du XS/SC26

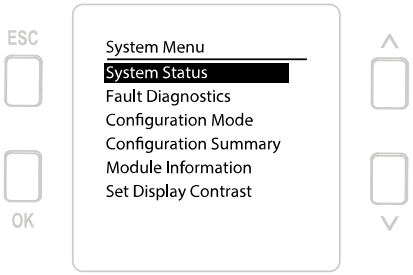
À l'exception des réglages spéciaux, l'interface embarquée du contrôleur de sécurité XS/SC26 affiche l'écran État système lors de la mise sous tension.

Illustration 176. Interface embarquée au démarrage



Pour accéder à d'autres informations via l'interface embarquée, appuyer sur le bouton Échapp. pour accéder au menu **Système**.

*Illustration 177. Interface embarquée — **Menu Système***



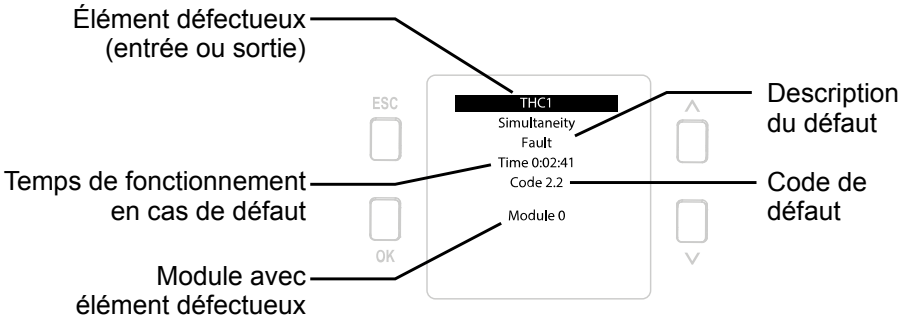
État du système

Affiche l'état actuel des sorties de sécurité et si elles sont sélectionnées, les entrées connectées à cette sortie (voir Illustration 176 à la page 176).

Diagnostic des défauts

Affiche les défauts, ou erreurs, actuels, le journal des défauts et une option pour effacer le journal des défauts (référez-vous à la section Détection et correction des défauts à la page 349).

Illustration 178. Interface embarquée — Diagnostic des défauts



Utilisez les flèches pour passer à d'autres codes de défaut.

Mode de configuration

Permet d'accéder au mode de configuration (code PIN obligatoire) et aux options de copie ou d'écriture des configurations à partir de la carte mémoire SC-XM2/3 et vers celle-ci (voir Mode de configuration du XS/SC26 à la page 177).

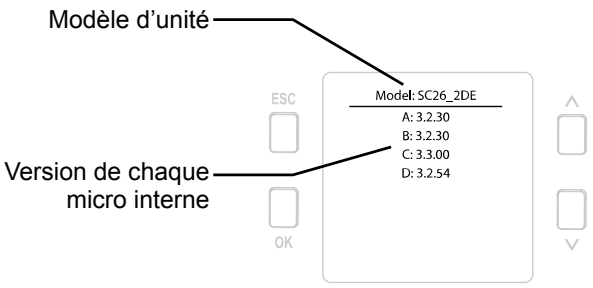
Résumé de la configuration

Permet d'accéder aux assignations de bornes, aux paramètres réseau et au CRC de la configuration.

Modèle

Affiche le numéro de modèle et les versions de chaque micrologiciel.

*Illustration 179. Interface embarquée — **Modèle***

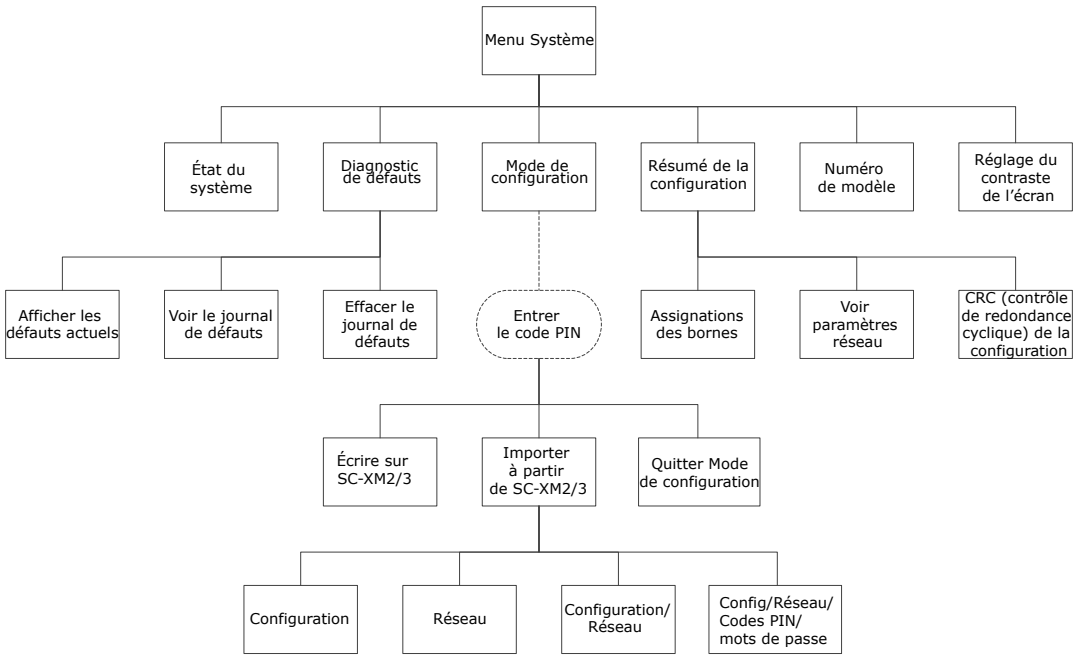


Si des modules d'extension sont raccordés au contrôleur de sécurité, utilisez les flèches pour voir les versions des modules d'extension.

Régler le contraste de l'écran

Offre des options de réglage de la luminosité de l'écran.

Illustration 180. Carte de l'interface embarquée



12.1 Mode de configuration du XS/SC26

Le mode de configuration propose des options pour envoyer la configuration active à une carte mémoire externe SC-XM2/3 et recevoir une configuration de la carte SC-XM2/3.

Important: Pour un contrôleur de sécurité dont l'option Configuration via le réseau ou Surveillance en temps réel via le réseau est activée (FID 7 ou supérieur), l'utilisation d'une carte SC-XM2/3 créée avant la version 5.0 du logiciel Contrôleur de sécurité Banner ou pour un contrôleur avec un FID inférieur à 7 peut entraîner la désactivation de la fonctionnalité Configuration via le réseau ou Surveillance en temps réel via le réseau. Dans ce cas, réactivez l'option Configuration via le réseau ou la Surveillance en temps réel via le réseau à l'aide de la connexion USB.

Remarque: Vous avez besoin d'un code PIN pour accéder au menu **Mode de configuration**.

Important: L'accès au **mode de configuration** désactive les sorties de sécurité.

Pour *écrire* des données sur la carte SC-XM2/3 via l'interface embarquée :

1. Insérez la carte mémoire SC-XM2/3 dans le contrôleur de sécurité.
2. Dans le **menu Système**, sélectionnez **Mode de configuration**.
3. Entrez le code PIN.
4. Appuyez sur **OK** jusqu'à ce que le menu **Mode de configuration** s'affiche.
5. Sélectionnez **Écrire sur la carte mémoire XM**.

Remarque: Le processus d'écriture sur la carte mémoire XM copie toutes les données (configuration, paramètres réseau et codes PIN/mots de passe) sur la carte mémoire SC-XM2/3.

6. Attendez la fin de l'écriture.
7. Réinitialisez le système.

Pour *importer* des données à partir de la carte SC-XM2/3 via l'interface embarquée :

1. Insérez la carte mémoire SC-XM2/3 dans le contrôleur de sécurité.
2. Dans le **menu Système**, sélectionnez **Mode de configuration**.
3. Entrez le code PIN.
4. Appuyez sur **OK** jusqu'à ce que le menu **Mode de configuration** s'affiche.
5. Sélectionnez **Importer depuis la carte mémoire XM** :
    - Pour la configuration uniquement, sélectionnez **Configuration**.
    - Pour les paramètres réseau uniquement, sélectionnez **Paramètres réseau**.
    - Pour importer les deux, sélectionnez **Configuration/Réseau**.
    - Pour toutes les données (configuration, paramètres réseau et codes PIN/mots de passe utilisateur) sélectionnez **Configuration/Réseau/Mots de passe**.
6. Attendez la fin de l'importation.
7. Réinitialisez le système.

13 Présentation de l'Ethernet industriel (bus de terrain)

L'Ethernet industriel facilite l'établissement de communications Ethernet entre le contrôleur de sécurité et un API ou une IHM (interface homme-machine).

Les sections suivantes comportent des instructions destinées aux contrôleurs de sécurité FID 2 avec un code de date 1717 ou ultérieur (voir étiquette) et aux contrôleurs de sécurité FID 3.

Pour les contrôleurs de sécurité FID 2 avec un code de date 1716 ou antérieur, reportez-vous au *Manuel d'utilisation Ethernet industriel XS26/SC26-2E (FID 2 1716-)*. Pour les contrôleurs de sécurité FID 1 avec un code de date 1547 ou ultérieur, reportez-vous au *Manuel d'utilisation Ethernet industriel XS/SC26-2E (FID 1)*. Pour des versions plus anciennes des contrôleurs de sécurité FID 1, reportez-vous au *Manuel d'utilisation Ethernet industriel XS/SC26-2E (ANCIEN)*. Pour savoir où trouver ces documents, consultez la section Quel fichier et documentation EDS du XS/SC26 devez-vous utiliser ? à la page 186.

For PROFINET® connections on SC10-2 controllers and FID 2 or later XS/SC26 controllers, see PROFINET à la page 271.

Pour les connexions EtherCAT® sur les contrôleurs XS26 FID 6 ou ultérieur, voir EtherCAT à la page 299.

La connexion à un contrôleur de sécurité à partir du logiciel via Ethernet ne doit pas perturber le bus de terrain sauf lorsqu'une configuration est écrite sur le contrôleur.

13.1 Configuration du contrôleur de sécurité

Vérifiez que l'option **Activer l'interface réseau** est sélectionnée et que les paramètres réseau sont correctement configurés pour le protocole sélectionné.

1. Raccordez le contrôleur de sécurité à votre PC via le câble USB SC-USB2 ou via Ethernet (pour les modèles Ethernet XS/SC26 FID7 ou ultérieurs) pour activer le port.
2. Ouvrez le logiciel Contrôleur de sécurité Banner.
3. Cliquez sur **Paramètres réseau**.
4. Sélectionnez la case à cocher **Activer l'interface réseau** dans l'onglet **Bus de terrain**.
5. Configurez l'adresse IP et le masque de sous-réseau avec les paramètres requis pour votre réseau.

   Remarque: Si vous utilisez une séquence Reset virtuel ou Annulation de la temporisation, un code d'actionnement doit être défini puis envoyé au contrôleur de sécurité.

   La sélection de la case à cocher **Utilisez l'interface embarquée pour définir le dernier octet et le code d'actionnement** permet à l'utilisateur de définir le dernier octet de l'adresse IP (et le code d'actionnement, le cas échéant) pendant le processus d'installation. Référez-vous à la section Processus Clickset IP à la page 180.
6. Cliquez sur **Envoyer**.

   La capture d'écran ci-dessous illustre les valeurs par défaut des options Ethernet industriel et du port Ethernet du contrôleur de sécurité.

*Illustration 181. Valeurs par défaut — Onglet **Base***

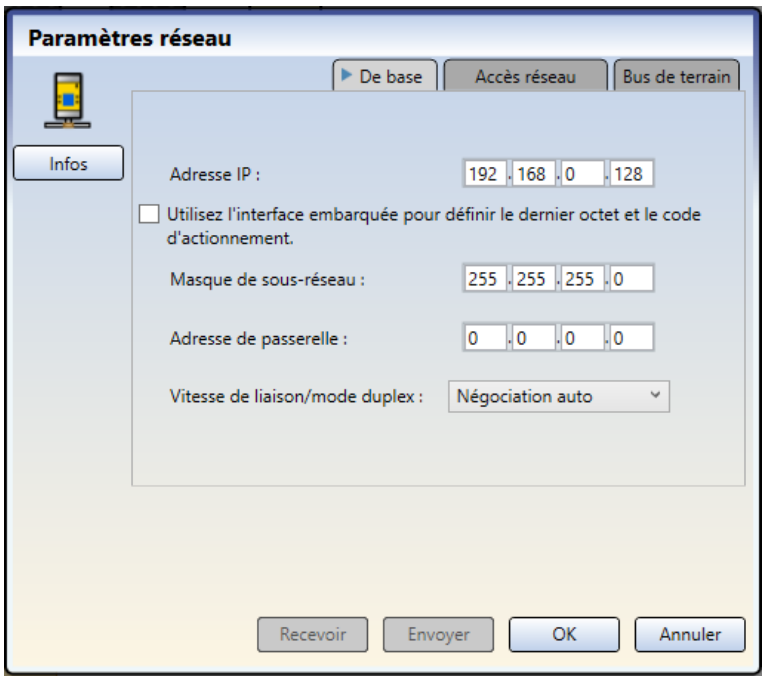
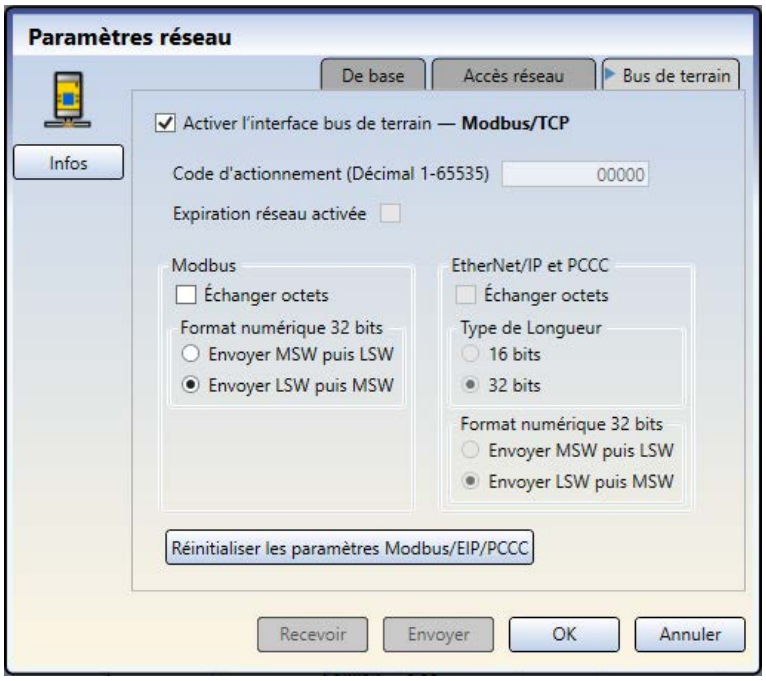


*Illustration 182. Valeurs par défaut — Onglet **Bus de terrain***



7. Saisissez le code PIN/mot de passe approprié pour modifier les paramètres de configuration et réseau du contrôleur de sécurité.
8. Vérifiez que le contrôleur de sécurité possède un fichier de configuration valide et confirmé.

Le port Ethernet est activé.

13.1.1 Processus Clickset IP

Le processus ClickSet IP est disponible sur les contrôleurs XS/SC26 FID 5 ou ultérieurs avec une interface embarquée.

Cocher la case **Utilisez l'interface embarquée pour définir le dernier octet et le code d'actionnement** dans la fenêtre **Paramètres réseau** (et l'envoyer à un contrôleur) permet à l'utilisateur de finaliser l'adresse IP et le code d'actionnement, le cas échéant, pendant le processus d'installation.

Cocher la case **Utilisez l'interface embarquée pour définir le dernier octet et le code d'actionnement** force le masque de sous-réseau à la valeur par défaut, soit 255.255.255.0.

En cas de reset ou d'annulation de la temporisation virtuels, cocher la case **Utilisez l'interface embarquée pour définir le dernier octet et le code d'actionnement** permet d'envoyer un code d'actionnement temporaire « zéro » au contrôleur. Le processus exige que le code d'actionnement soit remplacé par un nombre valide pendant le processus d'installation.

Le processus de paramétrage du dernier octet et du code d'actionnement (le cas échéant) est le suivant :

1. Cochez la case **Utilisez l'interface embarquée pour définir le dernier octet et code d'actionnement** dans la fenêtre **Paramètres réseau**.
2. Définissez les autres paramètres (c'est-à-dire les trois premiers octets). Référez-vous à la section Configuration du contrôleur de sécurité à la page 179.
3. Envoyez les paramètres réseau au contrôleur.
4. Envoyez la configuration souhaitée au contrôleur.
   Lorsque le contrôleur est sous tension, l'écran **Définir l'adresse IP** s'affiche dans l'interface embarquée.

*Illustration 183. Écran **Définir l'adresse IP***



Remarque: Pour quitter l'écran **Définir l'adresse IP**, appuyez sur le bouton Échapp. La fenêtre **État système** apparaît à l'écran. Pour revenir à l'écran **Définir l'adresse IP**, coupez puis rétablissez l'alimentation.

5. Pour modifier la valeur de l'octet, utilisez les flèches vers le haut et vers le bas pour augmenter ou diminuer le nombre d'octets.

   Si vous maintenez une flèche enfoncée, le rythme de changement des chiffres s'accélère. Lorsque vous arrivez à 1 en appuyant sur la flèche vers le bas, les chiffres reviennent à 254 et continuent. Lorsque vous arrivez à 254 en appuyant sur la flèche vers le haut, les chiffres reviennent à 1 et continuent.
6. Appuyez sur le bouton OK et maintenez-le enfoncé pour accepter (enregistrer) l'adresse IP.

   Remarque: Une fois le dernier octet accepté, vous ne pouvez plus revenir à l'écran **Définir l'adresse IP**. Utilisez le logiciel Contrôleur de sécurité Banner si vous devez modifier l'adresse IP.

   Après l'enregistrement de l'adresse IP :
   - Un message s'affiche indiquant qu'il faut couper puis rétablir l'alimentation pour terminer le processus. Passez à l'étape 8.
   - L'écran **Définir le code d'actionnement** s'affiche. Passez à l'étape suivante.
7. Si une entrée de reset manuel ou d'annulation de temporisation virtuelle est utilisée dans la configuration, l'écran **Définir le code d'actionnement** s'affiche dans l'interface embarquée après l'enregistrement de l'adresse IP. Utilisez les flèches pour paramétrer le code d'actionnement souhaité.

   *Illustration 184. Écran **Définir le code d'actionnement***

8. Appuyez sur le bouton OK et maintenez-le enfoncé pour accepter (enregistrer) le code d'actionnement.

   Remarque: Une fois le code d'actionnement accepté (enregistré), vous ne pouvez pas revenir à l'écran **Définir le code d'actionnement**. Utilisez le logiciel Contrôleur de sécurité Banner si vous devez modifier le code d'actionnement.

   Après l'enregistrement du code d'actionnement, un message s'affiche indiquant qu'il faut couper puis rétablir l'alimentation pour terminer le processus.
9. Mettez le contrôleur hors tension puis sous tension pour définir en interne la nouvelle adresse IP et le nouveau code d'actionnement (le cas échéant).

Si ce processus est interrompu par un verrouillage du système, l'écran **État du système** s'ouvre pour que le code de verrouillage du système puisse être vérifié.

Si le processus est interrompu (ou s'il n'a pas été enregistré en maintenant le bouton OK enfoncé), l'écran **Définir l'adresse IP** s'ouvre à la prochaine mise sous tension du contrôleur.

13.2 Définitions relatives à l'Ethernet industriel

Les tableaux ci-dessous proposent des descriptions des lignes et des colonnes de tableau (par ordre alphabétique) des cartes de registre de l'onglet **Ethernet industriel** du logiciel.

Table 8. Types de données

Type de données	Description
UINT	Entier non signé — 16 bits
UDINT	Double entier non signé — 32 bits
Word	Chaîne de bits — 16 bits
Dword	Chaîne de bits — 32 bits
String	Deux caractères ASCII par mot (voir les informations sur la configuration d'une chaîne ci-dessous)
Octet	Se lit en octet converti en nombre décimal séparé par un point.
Hexadécimal	Se lit en quartet converti en hexadécimal, apparié, puis séparé par un espace.
Octet	Chaîne de bits — 8 bits

Octet:Bit

Indique le décalage des octets suivi par le bit spécifique.

Drapeau de défaut

Si l'entrée ou la sortie spécifiquement surveillée provoque un verrouillage, la valeur **1** sera assignée au drapeau associé à cette sortie virtuelle. En Modbus TCP, ceci peut être lu en entrée TOR, registre d'entrée, ou registre de maintien.

Index de défaut

Si le bit du drapeau de défaut est défini pour une sortie virtuelle, l'index de défaut contiendra un nombre, qui correspond à un code de défaut. Par exemple, l'index de défaut 41 peut contenir le nombre 201, qui correspond au code de défaut 2.1; tandis que le nombre 412 correspond au code de défaut 4.12 (voir Tableaux des codes de défaut du XS/SC26 à la page 349 et Tableau des codes de défaut du SC10-2 à la page 354 pour plus d'informations).

Fonction

Fonction qui détermine l'état de cette sortie virtuelle.

Mode de fonctionnement

Valeur du mode de fonctionnement	Description
1 (0x01)	Mode de fonctionnement normal (y compris les défauts d'E/S, s'ils existent)
2 (0x02)	Mode de configuration
4 (0x04)	Verrouillage du système
65 (0x41)	Attente du reset du système/Sortie du mode de configuration
129 (0x81)	Basculement en mode de configuration

Reg:Bit

Indique le décalage de 30000 ou 40000 suivi par le bit spécifique dans le registre.

Réservé

Registres réservés pour usage interne.

Secondes depuis le démarrage

Temps écoulé (en secondes) depuis la mise sous tension du contrôleur de sécurité. Peut être utilisé conjointement avec l'horodatage dans le journal de défauts et une référence d'horloge en temps réel pour déterminer l'heure à laquelle une erreur est survenue.

Chaîne (protocoles EtherNet/IP et PCCC)

Le format de chaîne EtherNet/IP par défaut a une longueur de 32 bits précédant la chaîne (compatible avec ControlLogix). Lorsque vous configurez les **Paramètres réseau** avec le logiciel, vous pouvez remplacer cette valeur par une longueur de 16 bits qui correspond à la « chaîne » CIP standard dans le menu **Avancé**. Toutefois, lors de la lecture d'un ensemble d'entrées incluant une chaîne d'une longueur de 16 bits, la longueur de la chaîne sera précédée d'un mot de 16 bits supplémentaire (0x0000).

La chaîne elle-même est au format ASCII compressé (2 caractères par mot). Dans certains systèmes, l'ordre des caractères peut être inversé ou les caractères peuvent apparaître dans le désordre. Ainsi, le mot « Système » peut apparaître sous la forme « yStèsme ». Utilisez l'option « *Échanger les octets de caractère* » sous le menu **Avancé** de la fenêtre **Paramètres réseau** pour permuter les caractères et pouvoir lire les mots correctement.

Chaîne (protocole Modbus TCP)

La chaîne est au format ASCII compressé (deux caractères par mot). Dans certains systèmes, l'ordre des caractères peut être inversé ou les caractères peuvent apparaître dans le désordre. Ainsi, le mot « Système » peut apparaître sous la forme « yStèsme ». Utilisez l'option « *Échanger les octets de caractère* » sous le menu **Avancé** de la fenêtre **Paramètres réseau** pour permuter les caractères et pouvoir lire les mots correctement.

Même si la longueur est fournie, elle n'est généralement pas nécessaire pour les systèmes Modbus TCP. Si la longueur de chaîne est utilisée pour Modbus TCP, le format de longueur correspond aux paramètres utilisés pour EtherNet/IP.

Horodatage

Temps écoulé en secondes entre la mise sous tension et l'occurrence du défaut.

Sortie d'état virtuelle

Désignation de référence associée à une sortie d'état virtuelle donnée, par exemple VO10 est la sortie d'état virtuelle 10.

État VO

Identifie l'emplacement d'un bit indiquant l'état d'une sortie d'état virtuelle. Avec les systèmes Modbus TCP, l'état de la sortie d'état virtuelle peut être lu comme une entrée logique ou une entrée d'un registre d'entrée ou de maintien. Le registre indiqué est le décalage de 30000 ou 40000 suivi par l'emplacement du bit dans le registre.

13.3 Récupération des informations du défaut actuel

Suivez les étapes ci-dessous pour récupérer des informations sur un défaut actuellement présent via la connexion réseau :

1. Accédez à l'emplacement *Index de défaut* pour récupérer la valeur de l'index de défaut.
2. Vous trouverez la valeur d'index dans le Tableaux des codes de défaut du XS/SC26 à la page 349 ou Tableau des codes de défaut du SC10-2 à la page 354 afin de consulter une description du défaut ainsi que la procédure pour le corriger.

13.4 EtherNet/IP™

Dans ce contexte, les références à EtherNet/IP™ [23] se réfèrent spécifiquement à EtherNet/IP - classe de transport 1. Parfois appelée transfert de données d'E/S EtherNet/IP cyclique ou messagerie implicite, cette connexion est censée se rapprocher d'un transfert de données en temps réel vers et depuis l'API et le dispositif cible.

La famille d'API CompactLogix et ControlLogix ®d'Allen-Bradley® [24] Cette famille d'API utilise ce protocole de communication. Le logiciel de programmation utilisé par ces API est RSLogix5000® ou Studio 5000 Logix Designer™ [25].

Il existe trois méthodes pour établir une connexion EIP entre l'API et le contrôleur de sécurité :

- L5X — voir Connexion du fichier L5X à la page 183
- Fichier EDS (avec fichier d'étiquette/tag CSV en option) — voir Contrôleur de sécurité Banner Installation du fichier EDS dans le logiciel ControlLogix à la page 187
- Ethernet générique — voir Connexion du module Ethernet générique à la page 195

13.4.1 Connexion du fichier L5X

Création de fichiers L5X pour les assemblys Ethernet/IP

Le fichier .L5X est un fichier XML (eXtensilble Markup Language) qui stocke les données de la connexion EtherNet/IP et les descriptions des tags. L'exportation de ce fichier à partir du logiciel du contrôleur de sécurité et son importation dans le logiciel API RS Studio 5000 permettent d'établir une connexion EtherNet/IP entre l'API et le contrôleur de sécurité avec des descriptions de tags, le tout en une seule étape.

Pour créer le fichier L5X, vous devez connaître deux éléments :

- Le nom attribué au contrôleur de sécurité dans l'API. Ce nom est nécessaire pour générer le fichier à importer dans le logiciel de l'API
- Les instances d'assembly d'entrée et de sortie à demander

1. Dans l'onglet **Ethernet industriel**, vérifiez que **Assemblys Ethernet/IP** est sélectionné dans la liste à gauche.
2. Cliquez sur **Exporter**.
   La fenêtre **Exporter vers CSV et L5X** s'ouvre.

*Illustration 185. **Exportation vers CSV et L5X***



3. Dans le champ **Nom du contrôleur**, indiquez le nom attribué au contrôleur de sécurité dans le logiciel de l'API.
   Référez-vous à la section Illustration 201 à la page 191.
4. Sélectionnez la connexion souhaitée dans la liste **Sélectionner une connexion**.
   La connexion à sélectionner varie selon les instances d'assembly demandées :

*Table 9. Choix du champ **Sélectionner une connexion***

Nom de la connexion	Assembly de sortie	Taille	Assembly d'entrée	Taille
État/Défaut	112	Entier 2 bits	100	Entier 8 bits
Mots (words) de l'index de défauts	112	Entier 2 bits	101	Entier 104 bits

[23] EtherNet/IP™ est une marque commerciale de ODVA, Inc.
[24] CompactLogix® et ControlLogix® sont des marques déposées de Rockwell Automation.
[25] RSLogix5000® et Studio 5000 Logix Designer™ sont des marques déposées de Rockwell Automation.

Nom de la connexion	Assembly de sortie	Taille	Assembly d'entrée	Taille
Reset/Annulation de la temporisation	112	Entier 2 bits	103	Entier 35 bits
État/défauts VI	113	Entier 11 bits	100	Entier 5 bits
Mots (words) de l'index de défauts VI	113	Entier 11 bits	101	Entier 104 bits
Reset/Annulation de la temporisation VI	113	Entier 11 bits	103	Entier 35 bits
VRCD Plus ISD	114	Entier 14 bits	104	Entier 114 bits
Huit chaînes ISD	114	Entier 14 bits	105	Entier 240 bits

Remarque: Sélectionnez la même connexion pour la connexion au fichier EDS pour vous assurer que les étiquettes correspondent. Référez-vous à la section Illustration 202 à la page 191.

Si vous utilisez des entrées virtuelles (VI), l'assembly de sortie de l'API doit avoir la valeur 113 ou 114. Cela permet à l'API d'envoyer les mots (word) des entrées virtuelles au contrôleur de sécurité. Si vous avez besoin d'informations sur les entrées ISD pour des contrôleurs XS26-ISD FID 5 ou ultérieur ou SC10-2 FID 2 ou ultérieur, vous devez utiliser un assembly de sortie 114 pour envoyer des entrées virtuelles (si vous en utilisez) et des mots (word) supplémentaires pour demander des informations ISD (VRCD—Reset/Annulation de la temporisation virtuel).

L'assembly d'entrée 104 est utilisé pour un maximum de deux chaînes ISD (soit par le contrôleur XS26-ISD FID 5 ou ultérieur, si les chaînes sont ajoutées aux IN1/IN2 et IN3/IN4, soit par le SC10-2 FID 2 ou ultérieur). L'assembly d'entrée 105 prend en charge jusqu'à huit chaînes ISD et ne peut être utilisé que par le contrôleur XS26-ISD FID 5 ou ultérieur.

5. Cliquez sur **Exporter**.
6. Enregistrez le fichier .L5X dans l'emplacement voulu.

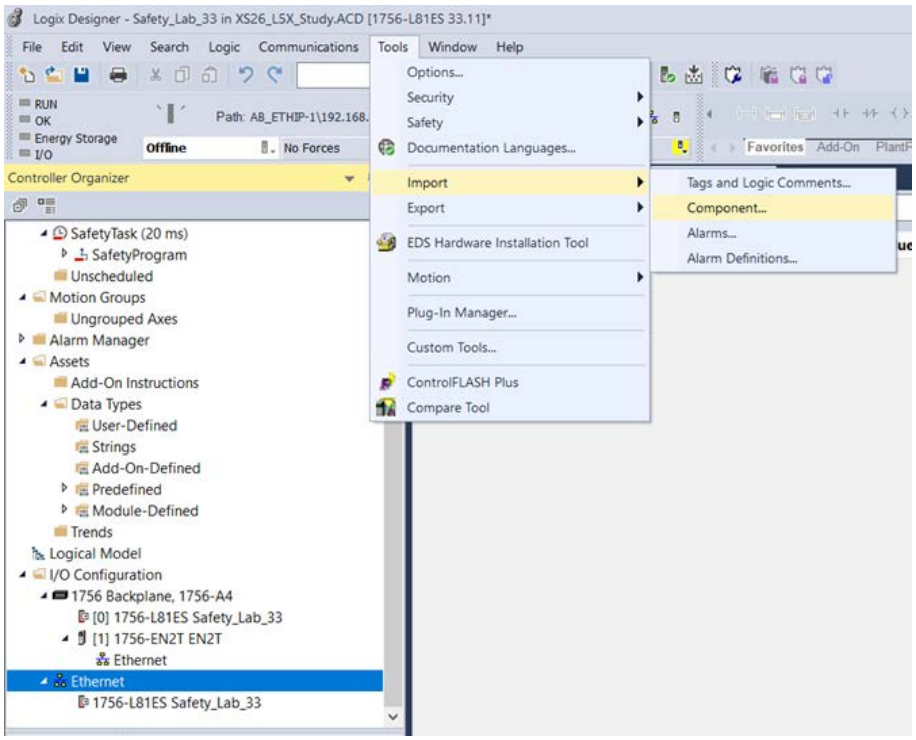
Remarque: Un fichier .L5X et un fichier.csv sont tous deux enregistrés.

Le fichier .L5X peut créer une connexion étiquetée en une seule étape. Référez-vous à la section Création de connexions étiquetées à l'aide d'un fichier L5X à la page 184.

Création de connexions étiquetées à l'aide d'un fichier L5X

1. dans Studio 5000® [27], cliquez sur le module Ethernet, puis sur **Tools (Outils)** > **Import** > **Component (Composant)**.

Illustration 186. Studio 5000

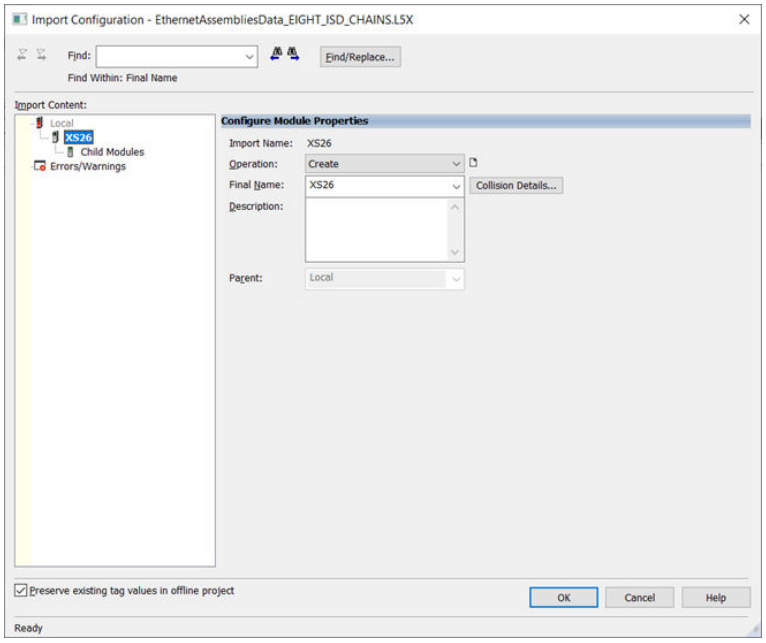


27 Studio 5000® est une marque déposée de Rockwell Automation.

La fenêtre **Import Module** (Module d'importation) s'ouvre.

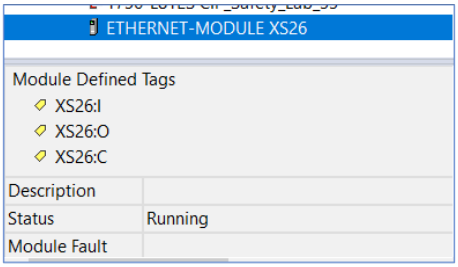
2. Accédez à l'emplacement du dossier où les fichiers .csv et .L5X sont enregistrés et sélectionnez le fichier .L5X.
3. Cliquez sur **Open** (Ouvrir).
   Studio 5000 importe le fichier .L5X.
4. Une fois le fichier .L5X importé avec succès, cliquez sur **OK** pour utiliser le fichier .L5X et établir une connexion avec les tags étiquetés.

*Illustration 187. Fenêtre **Import Configuration** (Importer la configuration)*



5. Téléchargez le projet sur l'API.
6. Passez en mode Run.

Illustration 188. Mode Run (marche)



Pour voir les données d'entrée de l'API et les données de sortie de l'API, regardez dans la fenêtre **Controller Tags** (Balises du contrôleur) sous le nom du contrôleur fourni lors de la création du fichier .L5X à partir du logiciel Contrôleur de sécurité Banner. La colonne de description affiche les étiquettes spécifiques à la configuration de votre contrôleur de sécurité.

*Illustration 189. Fenêtre **Controller tags** (Balises du contrôleur) — Données d'entrée API*

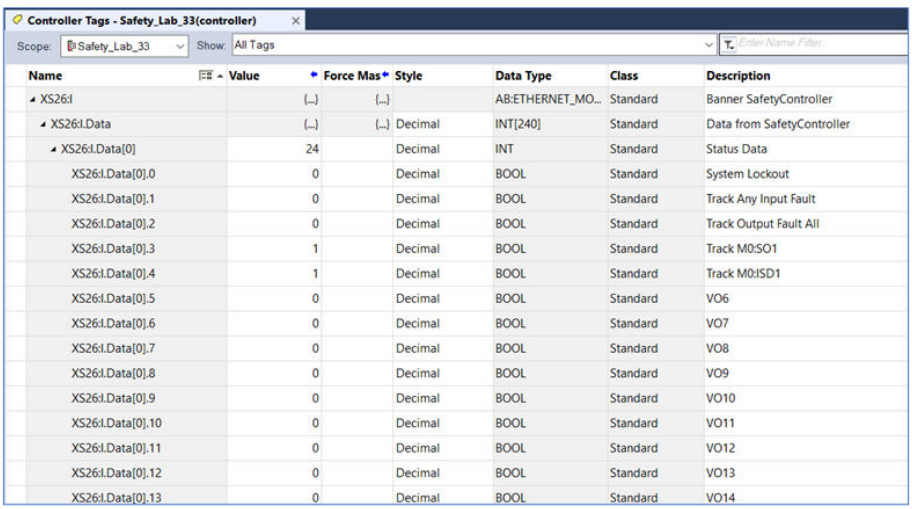
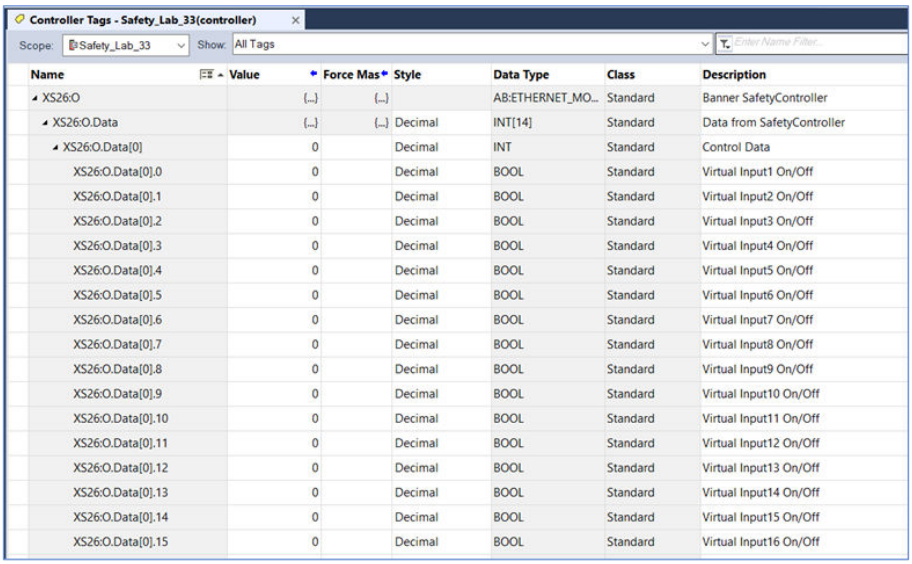


*Illustration 190. Fenêtre **Controller tags** (Balises du contrôleur) — Données de sortie API*



Controller Tags - Safety_Lab_33(controller)

Scope: Safety_Lab_33 Show: All Tags

Name	Value	Force Mas	Style	Data Type	Class	Description
XS26:O	{...}	{...}		AB:ETHERNET_MO...	Standard	Banner SafetyController
XS26:O.Data	{...}	{...}	Decimal	INT[14]	Standard	Data from SafetyController
XS26:O.Data[0]	0		Decimal	INT	Standard	Control Data
XS26:O.Data[0].0	0		Decimal	BOOL	Standard	Virtual Input1 On/Off
XS26:O.Data[0].1	0		Decimal	BOOL	Standard	Virtual Input2 On/Off
XS26:O.Data[0].2	0		Decimal	BOOL	Standard	Virtual Input3 On/Off
XS26:O.Data[0].3	0		Decimal	BOOL	Standard	Virtual Input4 On/Off
XS26:O.Data[0].4	0		Decimal	BOOL	Standard	Virtual Input5 On/Off
XS26:O.Data[0].5	0		Decimal	BOOL	Standard	Virtual Input6 On/Off
XS26:O.Data[0].6	0		Decimal	BOOL	Standard	Virtual Input7 On/Off
XS26:O.Data[0].7	0		Decimal	BOOL	Standard	Virtual Input8 On/Off
XS26:O.Data[0].8	0		Decimal	BOOL	Standard	Virtual Input9 On/Off
XS26:O.Data[0].9	0		Decimal	BOOL	Standard	Virtual Input10 On/Off
XS26:O.Data[0].10	0		Decimal	BOOL	Standard	Virtual Input11 On/Off
XS26:O.Data[0].11	0		Decimal	BOOL	Standard	Virtual Input12 On/Off
XS26:O.Data[0].12	0		Decimal	BOOL	Standard	Virtual Input13 On/Off
XS26:O.Data[0].13	0		Decimal	BOOL	Standard	Virtual Input14 On/Off
XS26:O.Data[0].14	0		Decimal	BOOL	Standard	Virtual Input15 On/Off
XS26:O.Data[0].15	0		Decimal	BOOL	Standard	Virtual Input16 On/Off

13.4.2 Connexion du fichier EDS

Quel fichier et documentation EDS du XS/SC26 devez-vous utiliser ?

Illustration 191. Numéro FID

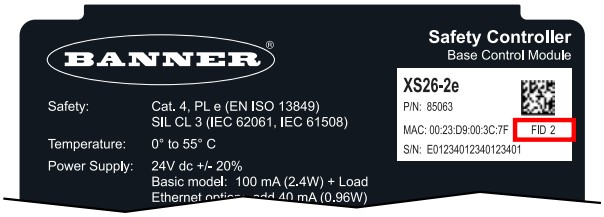
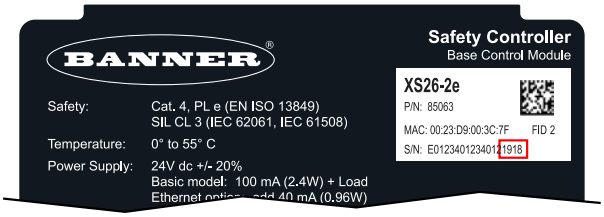


Illustration 192. Numéro de série



1. Vérifiez l'étiquette comportant la référence et prenez note du numéro FID et du code de date.

   Le code de date est constitué des 4 derniers chiffres du numéro de série du contrôleur de sécurité. Dans l'exemple illustré, « 19 » signifie 2019 et « 18 » la 18e semaine.
2. Utilisez le numéro FID et le code de date pour trouver les bons paramètres EIP, fichier EDS et manuel d'utilisation Ethernet industriel (le cas échéant) dans le tableau suivant.

Modèle et FID	Code de date	Code prod. EIP	O>T — taille	T>O — taille	Fichiers à utiliser
XS26 SC26 1	1546 ou moins	8193	112 (0×70) - 2	100 (0×64) - 8 101 (0×65) - 104 102 (0×66) - 150	**Nom du produit (Rév. Maj.Min) :** Banner XS26 (8193) [2.22] **Fichier EDS :** BannerXS_SC26_2E_8193_1_4_08102017.eds **Manuel d'utilisation Ethernet industriel :** Manuel d'utilisation Ethernet industriel XS/SC26-2E (ANCIEN)
XS26 SC26 1	1547 à 1705	300 [29]	112 (0×70) - 2	100 (0×64) - 8 101 (0×65) - 104 102 (0×66) - 150	**Nom du produit (Rév. Maj.Min) :** Banner XS26 1547 (300) [2.002] **Fichier EDS :** BannerXS_SC26_2E_300_1547_1_6_08102017.eds [29] **Manuel d'utilisation Ethernet industriel :** Manuel d'utilisation Ethernet industriel XS/SC26-2E (FID 1)

[29] Le fichier Banner_XS26_SC26_SC10_300_2_3_05192021.eds est rétrocompatible avec tous les contrôleurs avec code prod. 300 (XS26, SC26, SC10).

Modèle et FID	Code de date	Code prod. EIP	O>T — taille	T>O — taille	Fichiers à utiliser
XS26 SC26 2	1706 à 1716	301	112 (0×70) - 11	100 (0×64) - 8 101 (0×65) - 104 102 (0×66) - 150 103 (0×67) - 35	**Nom du produit (Rév. Maj.Min) :** Banner XS26 FID2 (301) [2.050] **Fichier EDS :** BannerXS_SC26_2E_301_FID2_1_2_08102017.eds **Manuel d'utilisation Ethernet industriel :** Manuel d'utilisation Ethernet industriel XS/SC26-2E (FID 2 1716-)
XS26 SC26 2 & 3	1717 ou ultérieur	300 [29]	112 (0×70) - 2 113 (0×70) - 11	100 (0×64) - 8 101 (0×65) - 104 102 (0×66) - 150 103 (0×67) - 35	**Nom du produit (Rév. Maj.Min) :** Banner XS26 FID 1/2 (300) [2.064] **Fichier EDS :** BannerXS_SC26_2E_300_1_8_11102017.eds [29] **Manuel d'utilisation Ethernet industriel :** Manuel d'utilisation Ethernet industriel XS/SC26-2E (FID 2 1717+)
XS26 SC26 2, 3 et 4 SC10 (tous)	1717 ou ultérieur	300 [29]	112 (0×70) - 2 113 (0×70) - 11 114 (0×72) - 14	100 (0×64) - 8 101 (0×65) - 104 102 (0×66) - 150 103 (0×67) - 35 104 (0×68) - 112	**Nom du produit [Maj.Min Rev] :** Banner XS26 SC26 SC10 (300) [2.090] **Fichier EDS :** Banner_XS26_SC26_SC10_300_2_1_06022020.eds [29] **Manuel d'instructions XS/SC26-2 et SC10-2 :** Rev R et ultérieur
XS26 2 et ultérieur SC10 (tous)	1717 ou ultérieur	300	112 (0×70) - 2 113 (0×71) - 11 114 (0×72) - 14	100 (0×64) - 8 101 (0×65) - 104 102 (0×66) - 150 103 (0×67) - 35 104 (0×68) - 112 105 (0×69) - 240	**Nom du produit [Maj.Min Rev] :** Contrôleur de sécurité Banner [2.001] **Fichier EDS :** Banner_XS26_SC26_SC10_300_2_3_05192021.eds **Manuel d'instructions XS/SC26 et SC10-2 :** Rev W et ultérieur

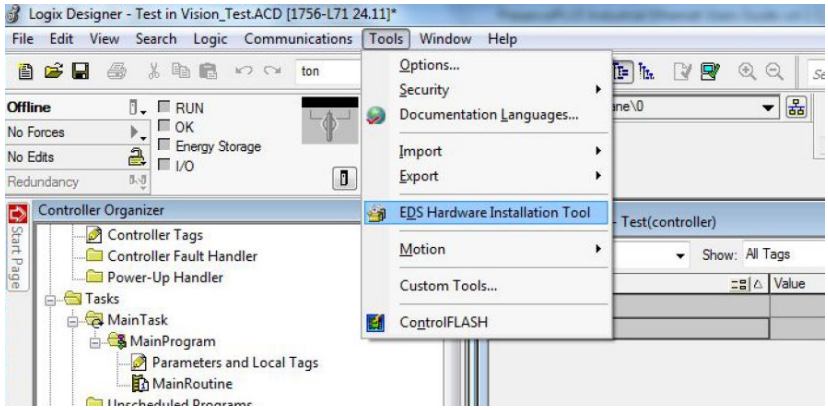
Remarque: Depuis le 1er octobre 2019, les informations actuelles sur l'Ethernet industriel sont incluses dans le *Manuel d'instructions du XS/SC26 et du SC10-2*. Le *Manuel d'utilisation Ethernet industriel* des systèmes plus anciens est inclus dans le dossier EDS disponible à la page www.bannerengineering.com/safetycontroller.

Contrôleur de sécurité Banner Installation du fichier EDS dans le logiciel ControlLogix

Utilisez l'outil **EDS Hardware Installation Tool** pour enregistrer le fichier EDS (Electronic Data Sheet).

1. Dans le menu **Tools** (Outils), cliquez sur **EDS Hardware Installation Tool**.
   La boîte de dialogue de l'Assistant **Rockwell Automation's EDS Wizard** s'affiche.

Illustration 193. Menu Tools (Outils) — EDS Hardware Installation Tool



2. Cliquez sur **Suivant**.
3. Sélectionnez l'option **Register an EDS file(s)** (Enregistrer un fichier EDS).

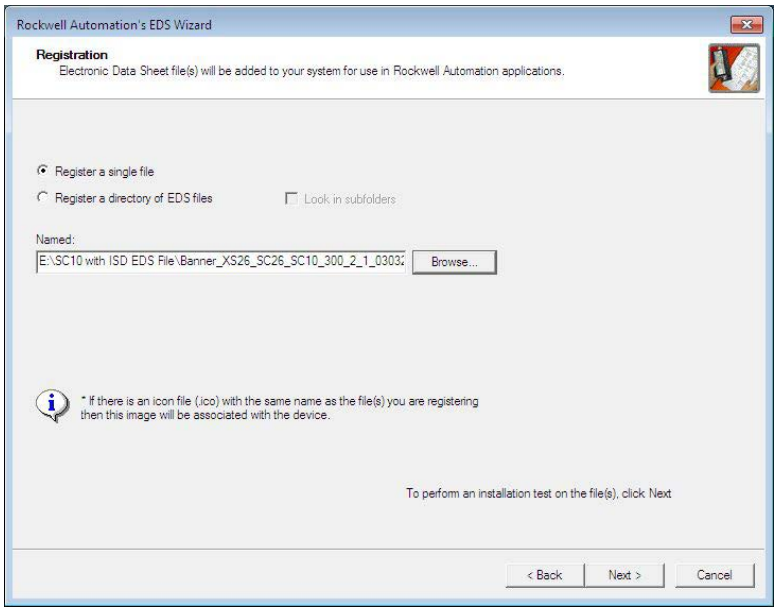
Illustration 194. Assistant Rockwell Automation's EDS Wizard — Options



4. Recherchez le fichier EDS et cliquez sur **Next**.

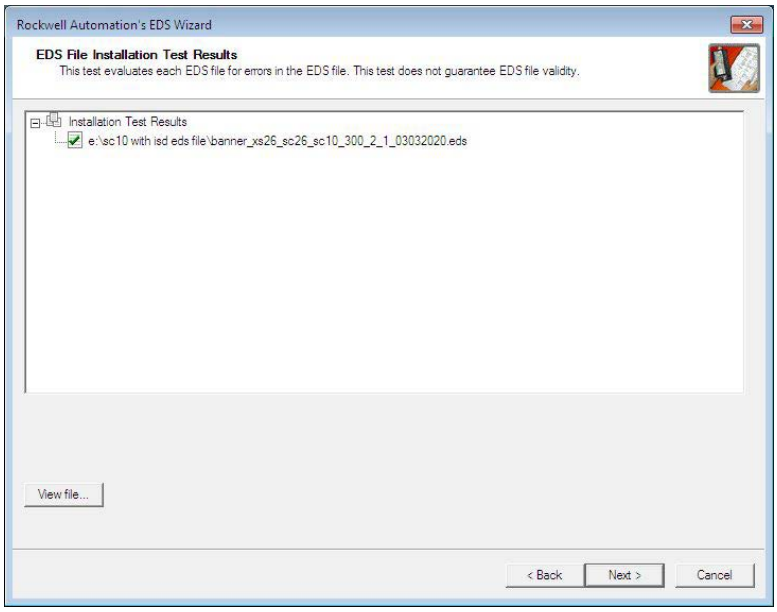
   Référez-vous à la section Quel fichier et documentation EDS du XS/SC26 devez-vous utiliser ? à la page 186 pour en savoir plus.

Illustration 195. Sélection du fichier à enregistrer



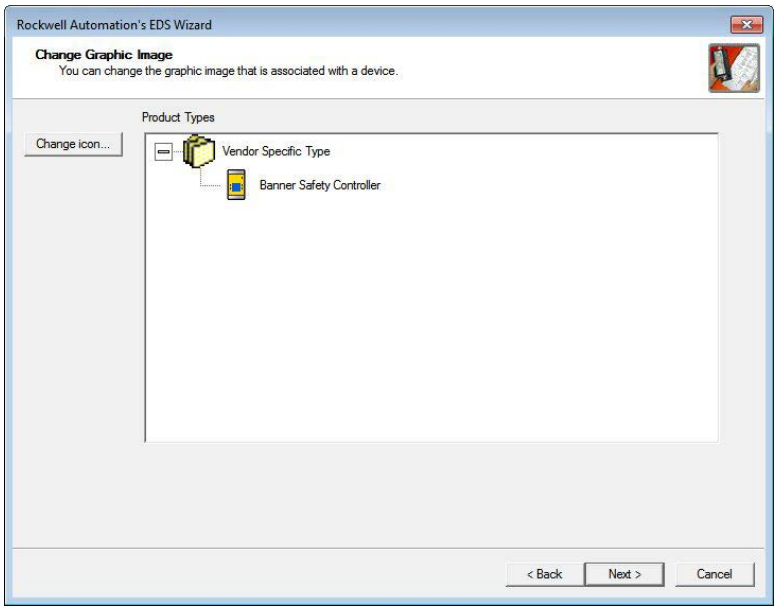
5. Cliquez sur **Next** pour enregistrer le fichier testé.

Illustration 196. Enregistrement du fichier testé



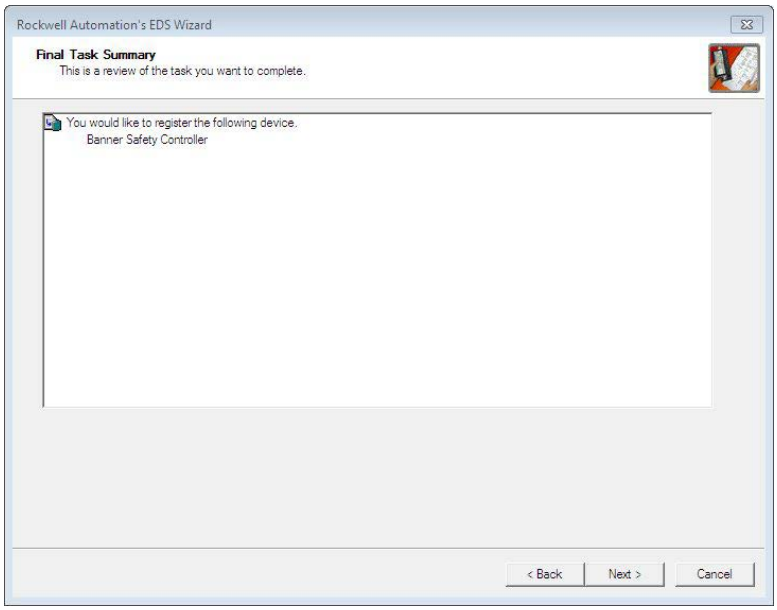
6. Cliquez sur **Next** lorsque vous voyez l'icône associée au fichier EDS.

Illustration 197. Assistant Rockwell Automation's EDS Wizard



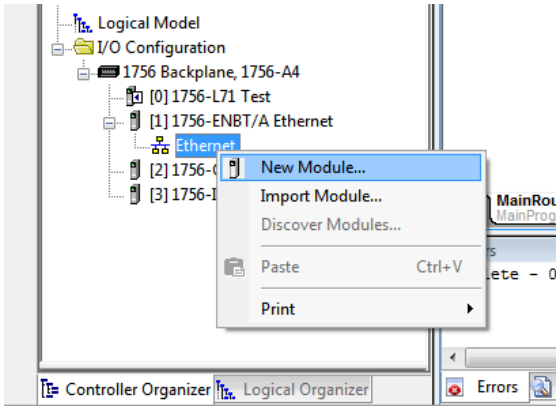
7. Cliquez sur **Next** pour enregistrer le fichier EDS.

Illustration 198. Enregistrement du fichier EDS



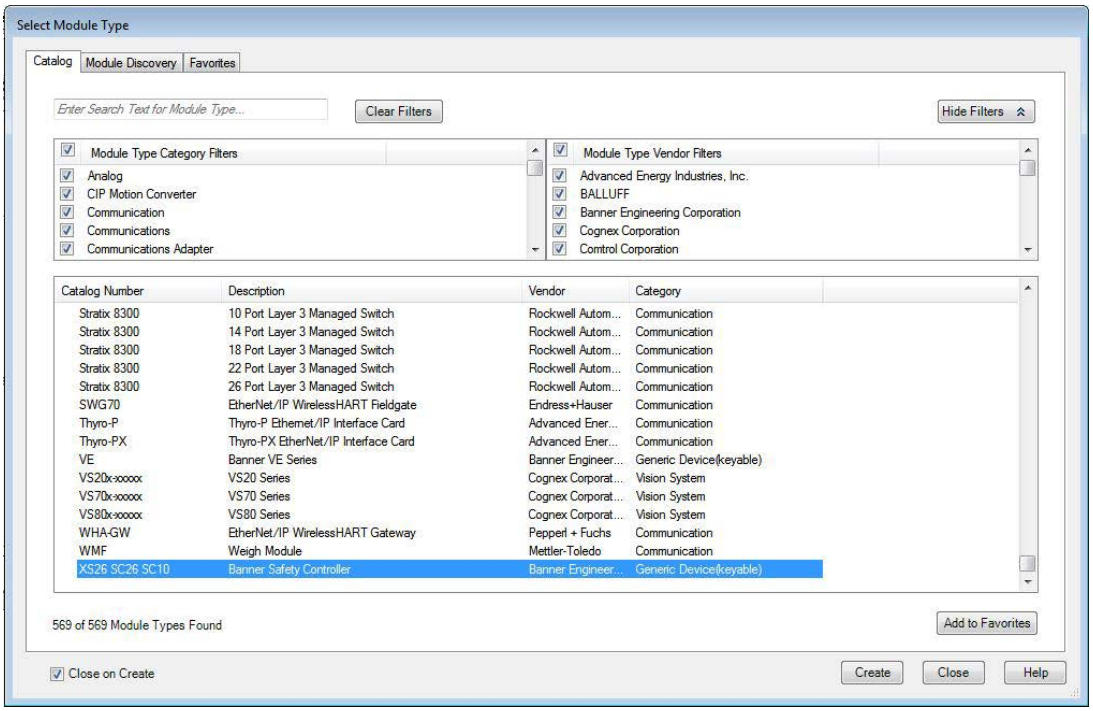
8. Cliquez sur **Finish** (Terminer) pour fermer l'Assistant **EDS Wizard**.
9. Cliquez avec le bouton droit sur la carte Ethernet de l'API et sélectionnez **New Module...** (Nouveau module).

Illustration 199. Nouveau module



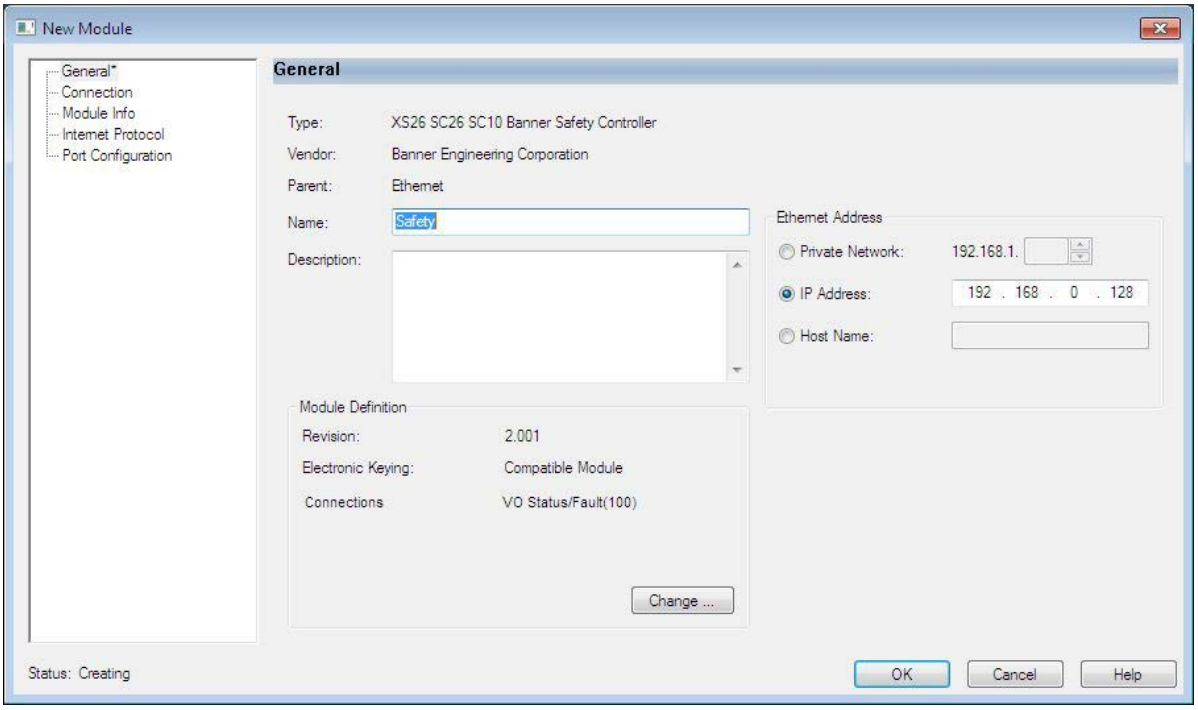
10. Recherchez le dispositif dans le catalogue et cliquez sur **Create** (Créer).

Illustration 200. Sélection du type de module



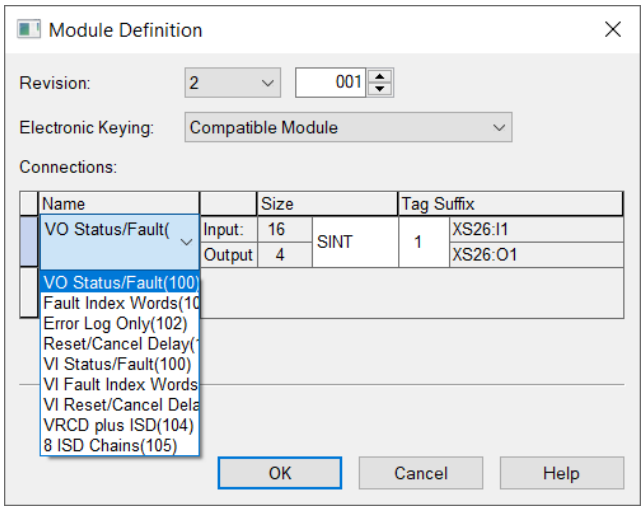
11. Indiquez un nom, une description (facultative) et une adresse IP pour le dispositif.

Illustration 201. Nouveau module



12. Cliquez sur **Change** (Modifier) dans le champ **Module Definition** (Définition du module).

Illustration 202. Définition du module



13. Sélectionnez la connexion souhaitée dans la fenêtre **Module Definition**. Chacun des éléments dans la liste **Name** (Nom) représente un groupe fixe d'instances d'assembly d'entrées et de sorties :

Remarque:

- Toutes les options de connexion ne sont pas applicables à tous les contrôleurs de sécurité.
- Sélectionnez un seul **nom** dans la liste. L'attribution de plusieurs noms provoque des problèmes de communication (activation et désactivation des bits).

État/défaut VO (100)-

- O>T - Assembly Entrée contrôleur de sécurité/Sortie API 112 (0×70), taille 2 registres 16 bits
- T>O - Assembly Entrée API/Sortie contrôleur de sécurité 100 (0×64), taille 8 registres 16 bits

Mots (word) de l'index de défauts (101)-

- O>T - Assembly Entrée contrôleur de sécurité/Sortie API 112 (0×70), taille 2 registres 16 bits
- T>O - Assembly Entrée API/Sortie contrôleur de sécurité 101 (0×65), taille 104 registres 16 bits

Journaux des erreurs uniquement (102)-

- O>T - Assembly Entrée contrôleur de sécurité/Sortie API 112 (0×70), taille 2 registres 16 bits
- T>O - Assembly Entrée API/Sortie contrôleur de sécurité 102 (0×66), taille 150 registres 16 bits

Reset/Annulation de la temporisation (103)-

- O>T - Assembly Entrée contrôleur de sécurité/Sortie API 112 (0×70), taille 2 registres 16 bits
- T>O - Assembly Entrée API/Sortie contrôleur de sécurité 103 (0×67), taille 35 registres 16 bits

État/défaut VI (100)- [30]

- O>T - Assembly Entrée contrôleur de sécurité/Sortie API 113 (0×71), taille 11 registres 16 bits
- T>O - Assembly Entrée API/Sortie contrôleur de sécurité 100 (0×64), taille 8 registres 16 bits

Mots (word) de l'index de défauts VI (101)- [30]

- O>T - Assembly Entrée contrôleur de sécurité/Sortie API 113 (0×71), taille 11 registres 16 bits
- T>O - Assembly Entrée API/Sortie contrôleur de sécurité 101 (0×65), taille 104 registres 16 bits

Reset/Annulation de la temporisation VI (103)- [30]

- O>T - Assembly Entrée contrôleur de sécurité/Sortie API 113 (0×71), taille 11 registres 16 bits
- T>O - Assembly Entrée API/Sortie contrôleur de sécurité 103 (0×67), taille 35 registres 16 bits

VRCD Plus ISD (104)- [30]

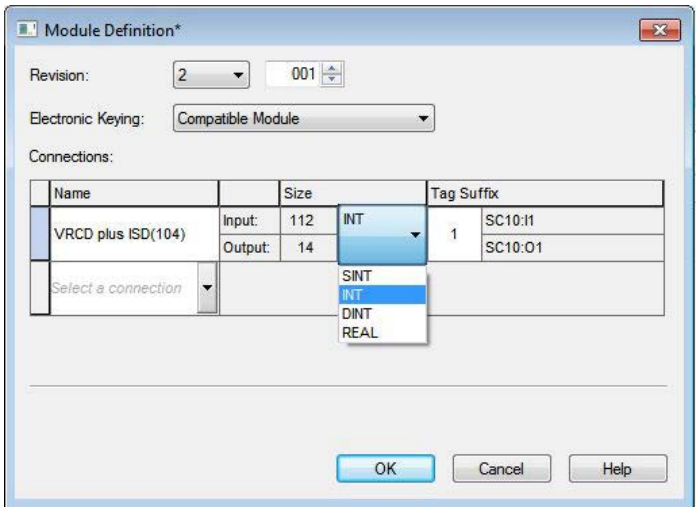
- O>T - Assembly Entrée contrôleur de sécurité/Sortie API 114 (0×72), taille 14 registres 16 bits
- T>O - Assembly Entrée API/Sortie contrôleur de sécurité 104 (0×68), taille 112 registres 16 bits

8 chaînes ISD (105)–

- O>T - Assembly Entrée contrôleur de sécurité/Sortie API 114 (0×72), taille 14 registres 16 bits
- T>O - Assembly Entrée API/Sortie contrôleur de sécurité 105 (0×69), taille 240 registres 16 bits

14. Sélectionnez **INT** comme type de données.

Illustration 203. Définition du module — Type de données



15. En option : le logiciel Contrôleur de sécurité Banner peut exporter un fichier CSV pour fournir des étiquettes de description pour les tags nouvellement créés dans l'API.

    Lorsque vous êtes hors ligne dans le logiciel API RS Studio 5000 et qu'un projet est ouvert, importez les descriptions des tags à partir d'un fichier CSV enregistré.

    Sélectionnez la même connexion pour la connexion du fichier EDS (par exemple, 8 chaînes ISD) et dans la fenêtre **Exporter vers CSV et L5X**. Ainsi, les étiquettes du fichier CSV exporté correspondront aux tags créés par le fichier EDS.

    Pour créer les fichiers CSV, deux éléments doivent être connus :

    - Le nom attribué au contrôleur de sécurité dans l'API. Ce nom est nécessaire pour générer le fichier à importer dans le logiciel de l'API
    - Les instances d'assembly d'entrée et de sortie à demander

    a) Dans le logiciel Contrôleur de sécurité Banner, sous l'onglet **Ethernet industriel**, vérifiez que **Assemblys Ethernet/IP** est sélectionné dans la liste à gauche.
    b) Cliquez sur **Exporter**.
    La fenêtre **Exporter vers CSV et L5X** s'ouvre.

[30] Sélectionnez l'une des connexions Instance d'assembly O>T 113 (0×71) ou 114 (0x72) pour utiliser Entrée virtuelle/Annulation de la temporisation.

*Illustration 204. **Exportation vers CSV et L5X***



c) Dans le champ **Nom du contrôleur**, indiquez le nom attribué au contrôleur de sécurité dans le logiciel de l'API.

d) Sélectionnez la connexion souhaitée dans la liste **Sélectionner une connexion**.

La connexion à sélectionner varie selon les instances d'assembly demandées :

*Table 10. Choix du champ **Sélectionner une connexion***

Nom de la connexion	Assembly de sortie	Assembly d'entrée
État/Défaut	112	100
Mots (words) de l'index de défauts	112	101
Reset/Annulation de la temporisation	112	103
État/défauts VI	113	100
Mots (words) de l'index de défauts VI	113	101
Reset/Annulation de la temporisation VI	113	103
VRCD Plus ISD	114	104
Huit chaînes ISD	114	105

Si vous utilisez des entrées virtuelles (VI), l'assembly de sortie de l'API doit avoir la valeur 113 ou 114. Cela permet à l'API d'envoyer les mots (word) des entrées virtuelles au contrôleur de sécurité. Si vous avez besoin d'informations sur les entrées ISD pour des contrôleurs XS26-ISD FID 5 ou ultérieur ou SC10-2 FID 2 ou ultérieur, vous devez utiliser un assembly de sortie 114 pour envoyer des entrées virtuelles (si vous en utilisez) et des mots (word) supplémentaires pour demander des informations ISD (VRCD—Reset/Annulation de la temporisation virtuels).

L'assembly d'entrée 104 est utilisé pour un maximum de deux chaînes ISD (soit par le XS26-ISD FID 5 ou ultérieur, si les chaînes sont ajoutées à IN1/IN2 et IN3/IN4, soit par les contrôleurs SC10-2 FID 2 ou ultérieur). L'assembly d'entrée 105 prend en charge jusqu'à huit chaînes ISD et ne peut être utilisé que par le contrôleur XS26-ISD FID 5 ou ultérieur.

e) Cliquez sur **Exporter**.

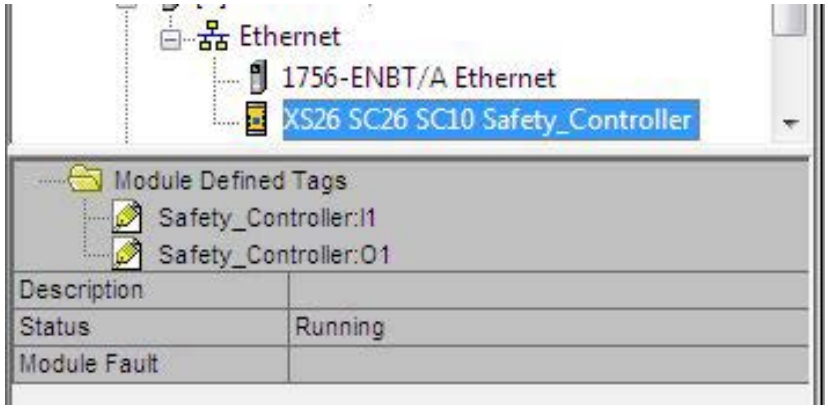
f) Enregistrez les fichiers CSV dans l'emplacement voulu.

Remarque: Le fichier.csv et le fichier.L5X sont tous deux enregistrés.

Le fichier CSV est prêt à être directement importé dans le logiciel de l'API indiqué dans Assembly Ethernet/IP ou à être ouvert avec n'importe quel logiciel capable de lire un fichier CSV (par exemple, Microsoft Excel).

16. Cliquez deux fois sur **OK** et téléchargez le programme sur l'API.

Illustration 205. Téléchargement sur l'API



La connexion ressemble à celle de la Illustration 205 à la page 193.

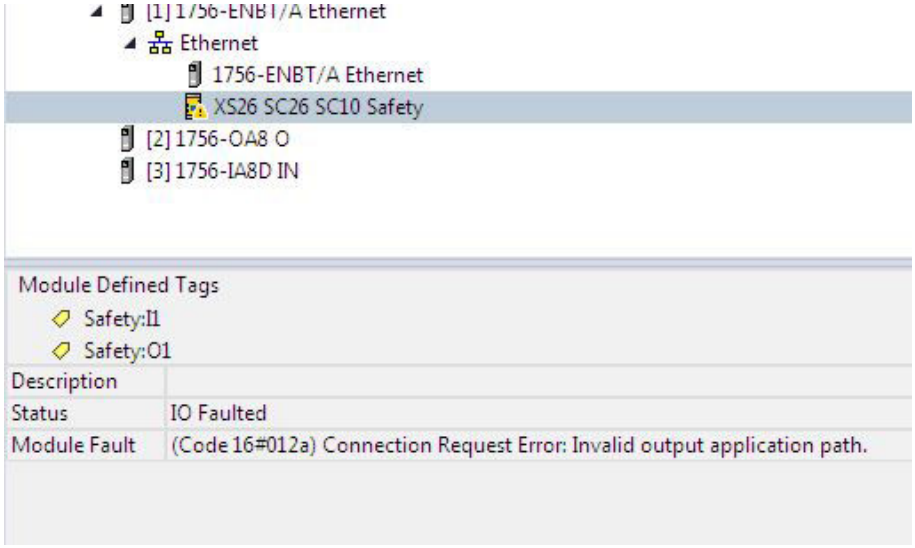
Exemples de choix de connexion incorrects

Voici trois exemples de sélection d'une connexion incorrecte dans le fichier EDS.

Exemple 1

Tentative d'utilisation de la connexion « État/Défaut VI (100) » sur un contrôleur de sécurité qui ne prend pas en charge les entrées virtuelles ; l'instance d'assembly O>T 113 n'existe pas pour ce matériel.

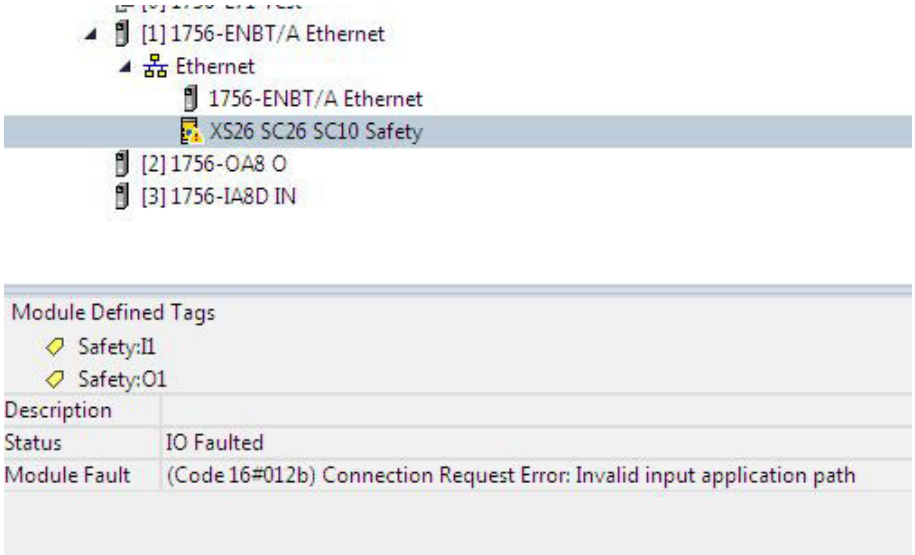
Illustration 206. Incorrect : utilisation de la connexion « État/Défaut VI » sur un contrôleur de sécurité qui ne prend pas en charge cette fonction.



Exemple 2

Tentative d'utilisation de la connexion « Reset/Annulation de la temporisation (103) » sur un contrôleur de sécurité qui ne prend pas en charge les entrées virtuelles ; l'instance d'assembly T>O 103 n'existe pas pour ce matériel.

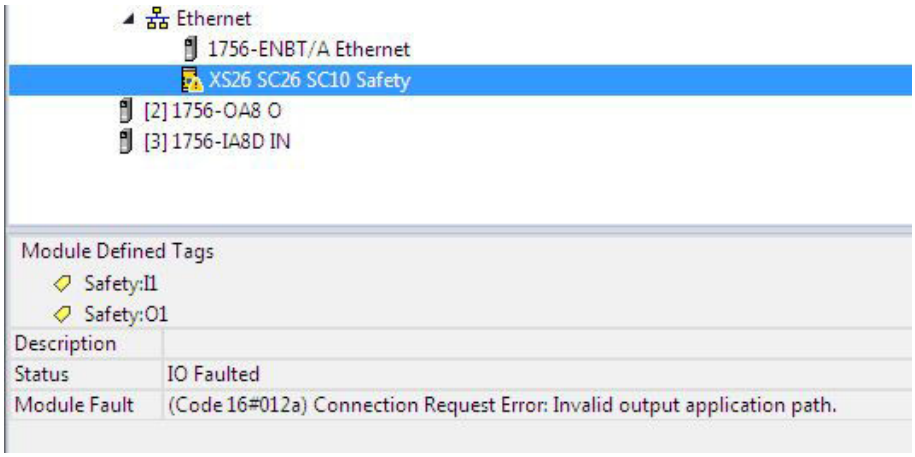
Illustration 207. Incorrect : utilisation de la connexion « Reset/Annulation de la temporisation » sur un contrôleur de sécurité qui ne prend pas en charge cette fonction.



Exemple 3

Tentative d'utilisation de la connexion « VRCD plus ISD (104) » sur un contrôleur de sécurité qui ne prend pas en charge ISD ; l'instance d'assembly T>O 104 n'existe pas pour ce matériel.

Illustration 208. Incorrect : utilisation de la connexion « VRCD plus ISD » sur un contrôleur de sécurité qui ne prend pas en charge cette fonction.



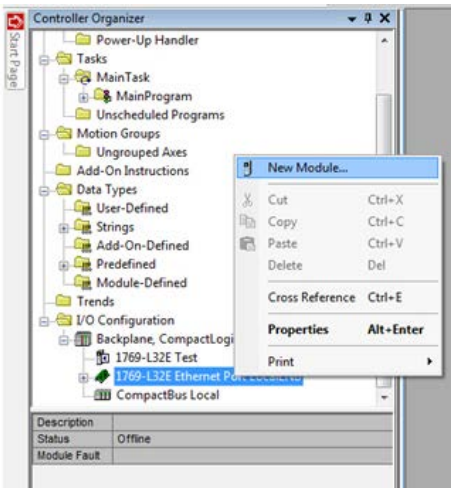
13.4.3 Connexion du module Ethernet générique

Pour créer une configuration de classe 1 implicite sur le Contrôleur de sécurité via EtherNet/IP lorsque vous utilisez un API de la gamme ControlLogix, configurez le Contrôleur de sécurité comme « Generic Ethernet Module » (Module Ethernet générique). L'exemple suivant illustre une procédure de configuration d'un dispositif Banner Engineering.

Remarque: Cette procédure est fournie à titre d'exemple.

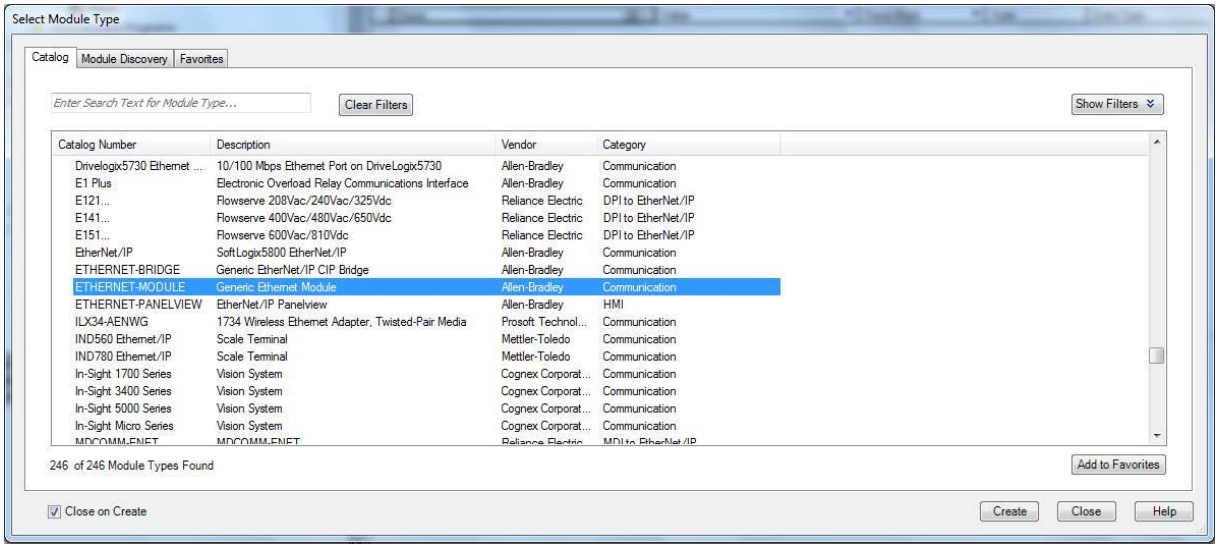
1. Ajoutez un module Ethernet générique à la carte Ethernet de l'API.
   a) Cliquez sur **New Module** (Nouveau module).

Illustration 209. Ajout d'un module Ethernet



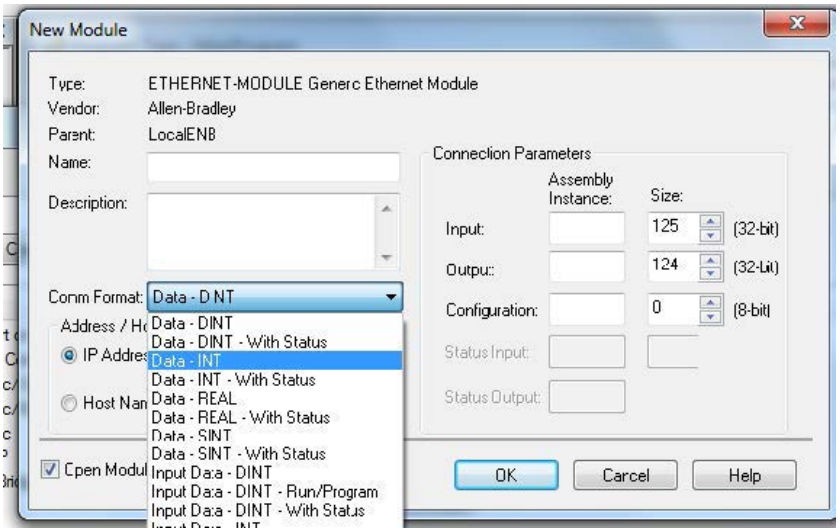
   b) Dans le catalogue, cliquez sur **Generic Ethernet Module** (Module générique Ethernet).

Illustration 210. Sélection du module



2. Configurez les propriétés du module.
   a) Sélectionnez **INT** dans la liste **Comm Format** (la valeur par défaut est DINT).

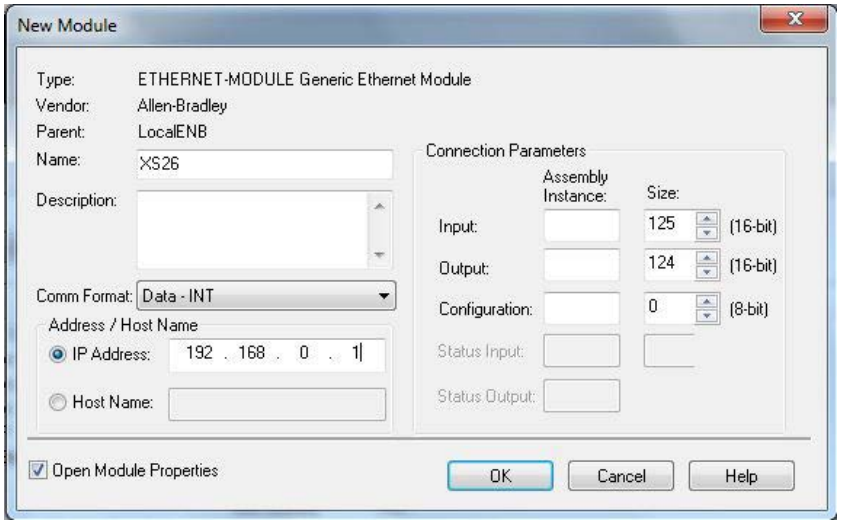
Illustration 211. Définition du format de communication



   b) Entrez le nom de module dans **Name** et l'adresse IP du contrôleur de sécurité dans **IP Address**.

      L'adresse IP par défaut du contrôleur de sécurité est 192.168.0.128 et son masque de sous-réseau est 255.255.255.0.

Illustration 212. Ajout d'un nom et d'une adresse IP



   c) Sous Connection Parameters (Paramètres de connexion), sélectionnez l'une des nombreuses configurations d'objet Assembly possibles. Référez-vous aux sections Entrées du contrôleur de sécurité (sorties de l'API) à la page 201 et Sorties du contrôleur de sécurité (entrées vers l'API) à la page 202 pour en savoir plus sur chaque possibilité.

Remarque: Sélectionnez l'une des connexions Instance d'assembly - O>T 113 (0×71) pour utiliser Entrée virtuelle/Annulation de la temporisation.

Illustration 213. Assembly d'entrée API 100 (0x64), taille 8 words (État/défaut VO)

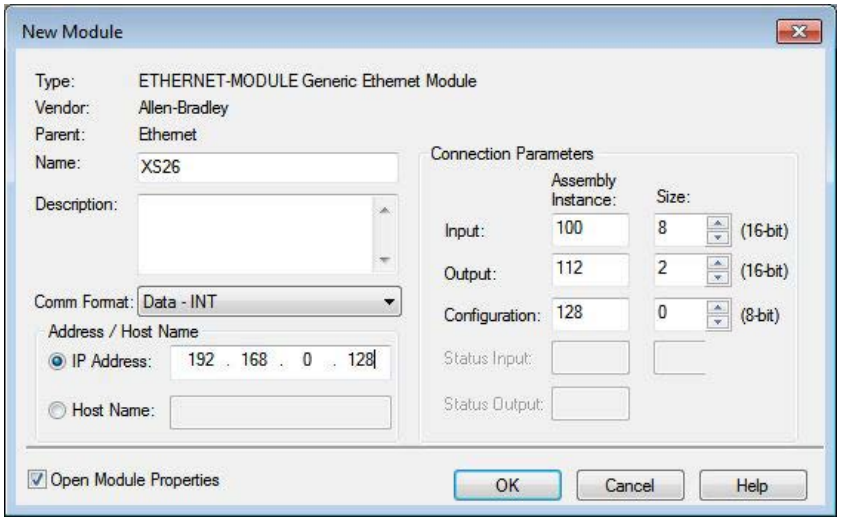


Illustration 214. Assembly d'entrée API 101 (0x65), taille 104 words (Mots de l'index de défauts)

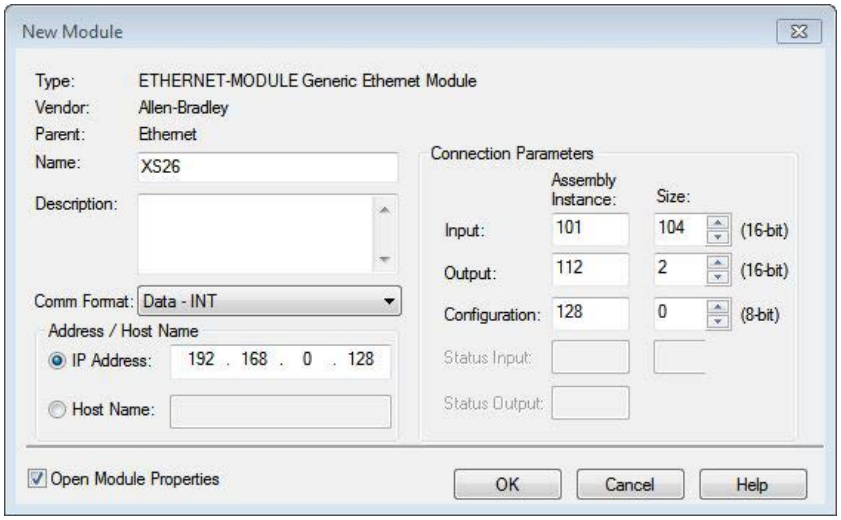


Illustration 215. Assembly d'entrée API 102 (0x66), taille 150 words (Journal des défauts du contrôleur de sécurité uniquement)

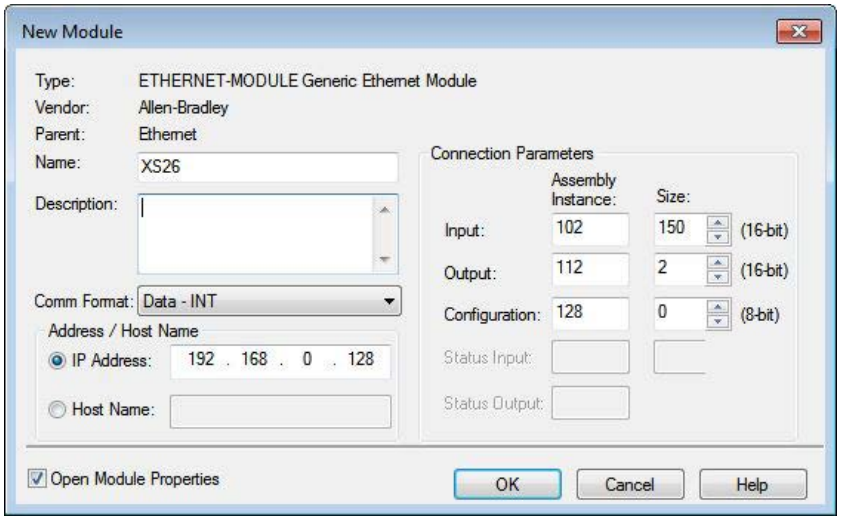


Illustration 216. Assembly d'entrée API 103 (0x67), taille 35 words (Reset/Annulation de la temporisation)

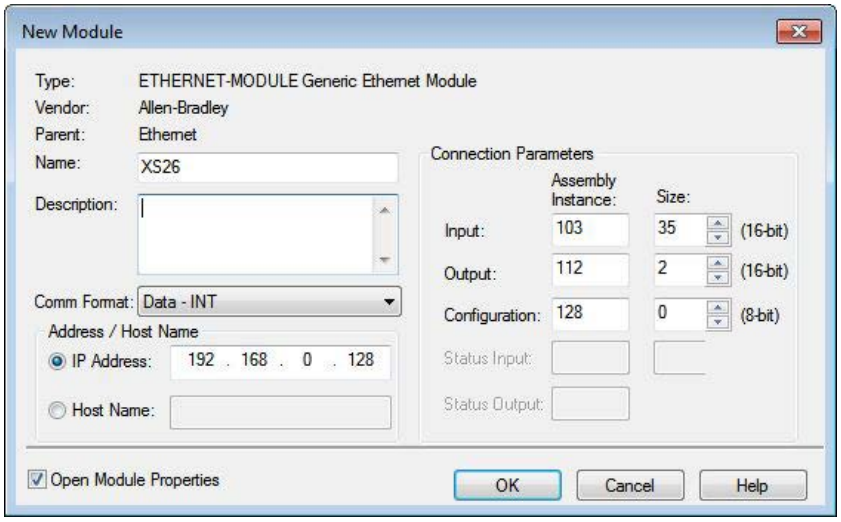


Illustration 217. Assembly d'entrée API 100 (0x64), taille 8 words (État/défaut VI)

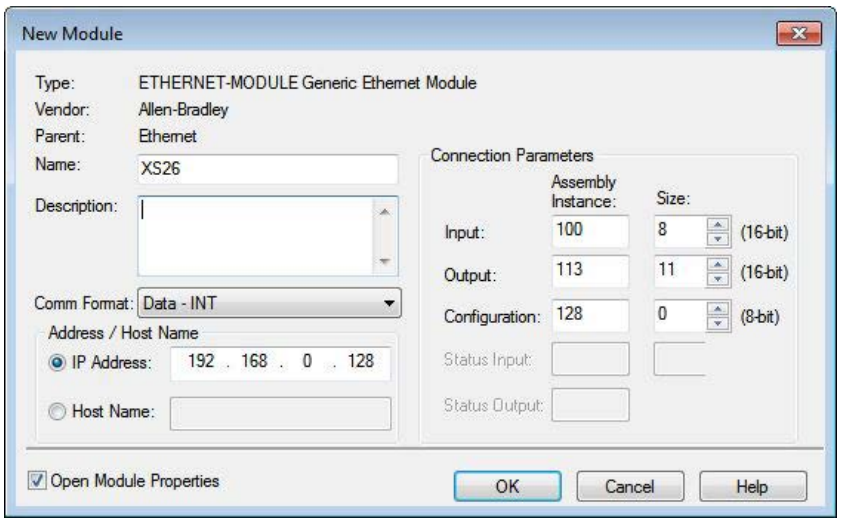


Illustration 218. Assembly d'entrée API 101 (0x65), taille 104 words (Mots de l'index de défauts VI)

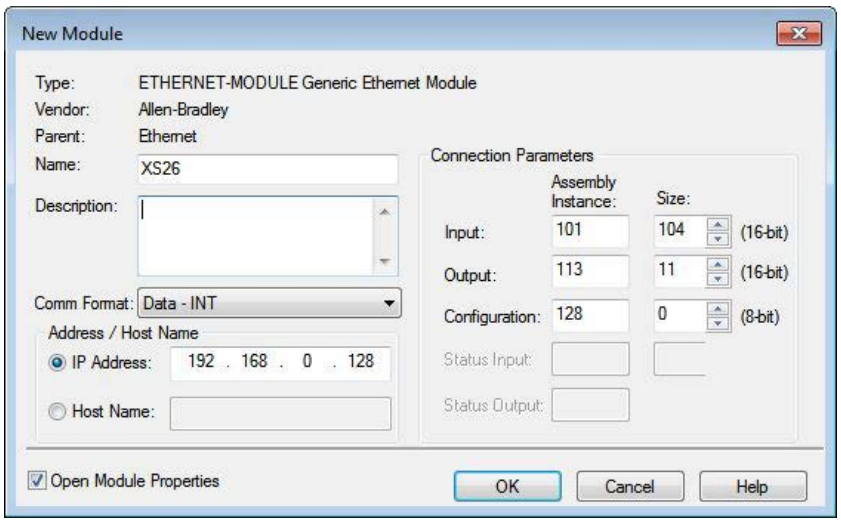


Illustration 219. Assembly d'entrée API 103 (0x67), taille 35 words (Reset/Annulation de la temporisation VI)

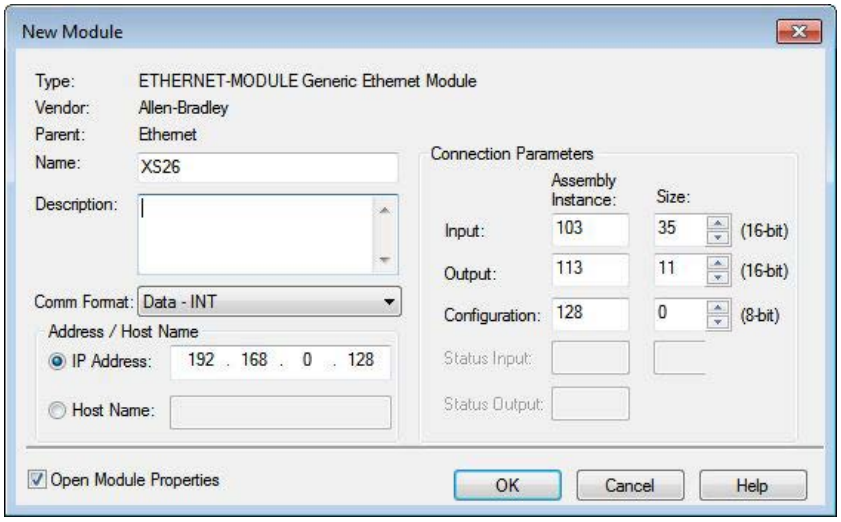


Illustration 220. Assembly d'entrée API 104 (0x68), taille 112 words (VRCD plus ISD)

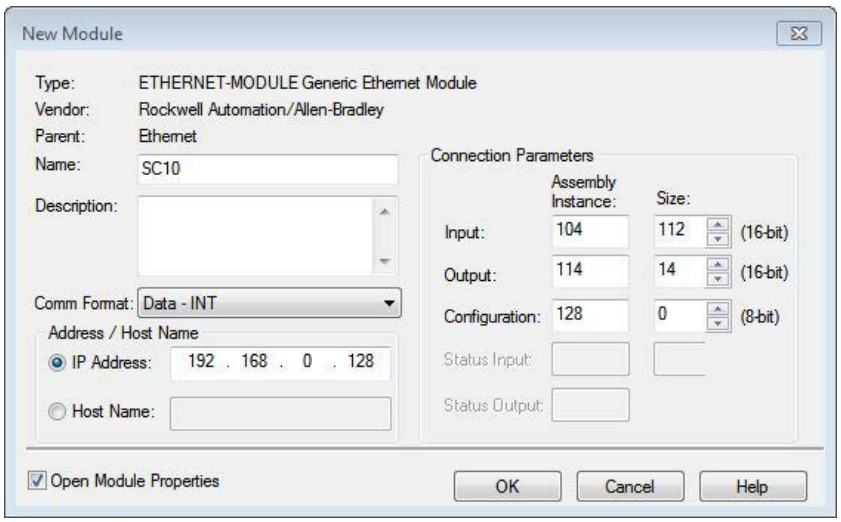
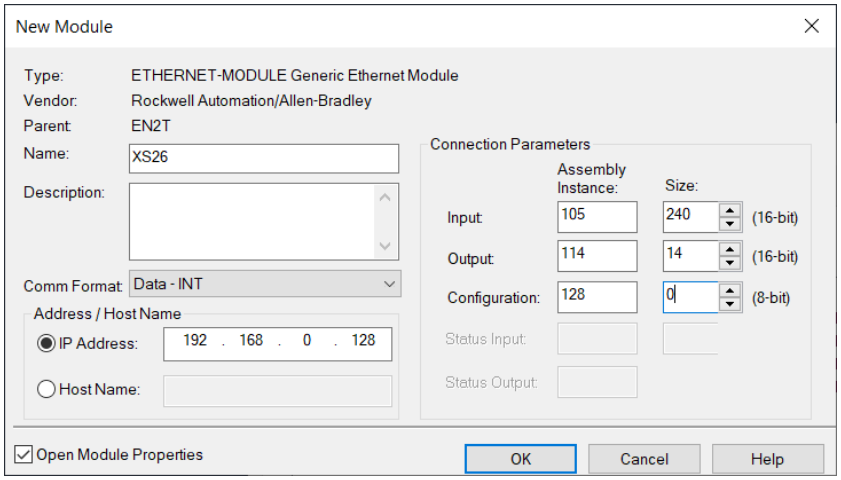


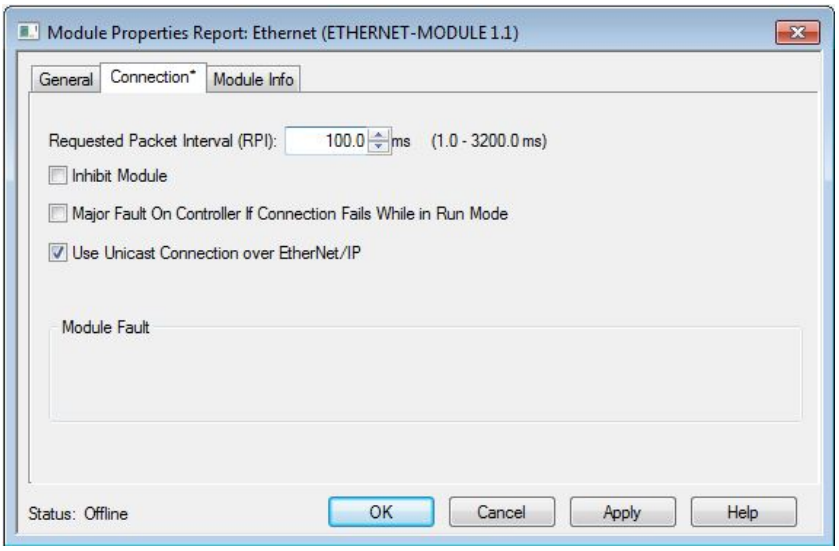
Illustration 221. Assembly d'entrée API 105 (0×69), taille 240 words (8 chaînes ISD)



d) Accédez à l'onglet **Connection** et définissez les paramètres :
   - Indiquez l'intervalle de paquets requis dans **Requested Packet Interval (RPI)**.
   - Activez ou désactivez la case à cocher de l'option **Use Unicast Connection over Ethernet/IP** (Utiliser la connexion Unicast sur Ethernet/IP).

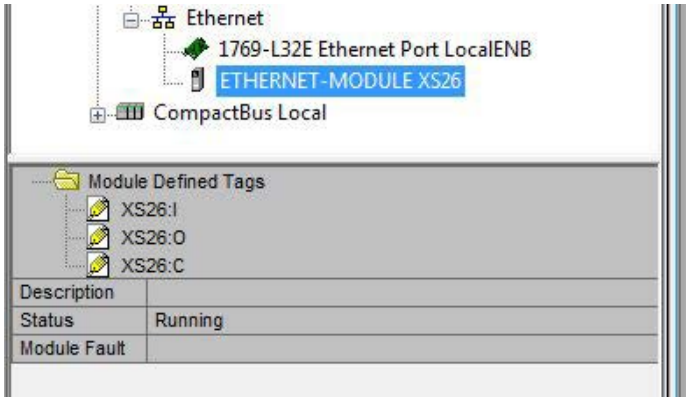
Remarque: L'intervalle de paquets minimum recommandé est 100 ms.

Illustration 222. Paramètres de connexion



Si la configuration du module est correcte, les informations suivantes s'affichent :

Illustration 223. Configuration correcte



I = Entrées vers l'API (sorties du contrôleur de sécurité)

O = Sorties de l'API (entrées vers le contrôleur de sécurité –non utilisé)

C = Configuration (non utilisé)

3. Recherchez la carte mémoire dans la liste **Controller Tags** (Tags du contrôleur). Les 8 mots (word) d'entrée de l'instance d'assembly 100 sont illustrés à titre d'exemple.

Illustration 224. Carte mémoire

XS26:I	{...}	{...}		AB:ETHERNET_MODULE_
XS26:I.Data	{...}	{...}	Decimal	INT[8]
XS26:I.Data[0]	1		Decimal	INT
XS26:I.Data[1]	128		Decimal	INT
XS26:I.Data[2]	0		Decimal	INT
XS26:I.Data[3]	8		Decimal	INT
XS26:I.Data[4]	0		Decimal	INT
XS26:I.Data[5]	0		Decimal	INT
XS26:I.Data[6]	0		Decimal	INT
XS26:I.Data[7]	0		Decimal	INT

Dans l'exemple illustré ci-dessus, nous constatons que les sorties virtuelles 1, 24 et 52 sont activées.

VO1 est le mot (word) 0, bit 0 > 2^0 = 1
VO24 est le mot (word) 1, bit 7 > 2^7 = 128
VO52 est le mot (word) 3, bit 3 > 2^3 = 8

13.4.4 Entrées du contrôleur de sécurité (sorties de l'API)

Instance d'assembly Sortie API 112 (0×70) — 2 registres (EV de base)

Le contrôleur de sécurité peut utiliser l'instance 112 (0×70) avec une taille de 2 registres (16 bits) lors de l'envoi des entrées virtuelles 1–32 au contrôleur de sécurité.

Table 11. Instance d'assembly de sortie API 112 (0x70)— Entrées du contrôleur de sécurité - O > T

WORD #	WORD NOM	TYPE DE DONNÉES
0	Entrée virtuelle On/Off (1–16)	Entier 16 bits
1	Entrée virtuelle On/Off (17–32)	Entier 16 bits

Instance d'assembly Sortie API 113 (0×71) — 11 registres (EV étendues plus VRCD)

Le contrôleur de sécurité utilise l'instance 113 (0x71) [33] avec une taille de onze registres (16 bits) comme assembly d'entrée (sortie API) lors de l'envoi d'entrées virtuelles, de resets et d'annulations de la temporisation au contrôleur de sécurité.

Table 12. Instance d'assembly de sortie API 113 (0x71)— Entrées du contrôleur de sécurité - O > T

WORD #	WORD NOM	TYPE DE DONNÉES
0	Entrée virtuelle On/Off (1–16)	Entier 16 bits
1	Entrée virtuelle On/Off (17–32)	Entier 16 bits
2	Entrée virtuelle On/Off (33–48)	Entier 16 bits
3	Entrée virtuelle On/Off (49–64)	Entier 16 bits
4	*réservé*	Entier 16 bits
5	*réservé*	Entier 16 bits
6	*réservé*	Entier 16 bits
7	*réservé*	Entier 16 bits
8	Reset/Annulation de la temporisation virtuels (1–16) [Bits de registre RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
9	*réservé*	Entier 16 bits
10	Code d'activation RCD [Registre d'activation RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits

PLC Output Assembly Instance 114 (0×72)-14 Registres (EV étendues, VRCD, plus ISD)

Le contrôleur de sécurité utilise l'instance 114 (0×72) avec une taille de 14 registres (16 bits) comme assembly d'entrée (sortie API) lors de l'envoi d'entrées virtuelles, de resets et d'annulations de la temporisation au contrôleur de sécurité et pour obtenir des informations de performance et d'état sur les dispositifs ISD.

Table 13. Instance d'assembly de sortie API 114 (0x72)— Entrées du contrôleur de sécurité - O > T

WORD #	WORD NOM	TYPE DE DONNÉES
0	Entrée virtuelle On/Off (1–16)	Entier 16 bits
1	Entrée virtuelle On/Off (17–32)	Entier 16 bits
2	Entrée virtuelle On/Off (33–48)	Entier 16 bits
3	Entrée virtuelle On/Off (49–64)	Entier 16 bits
4	*réservé*	Entier 16 bits
5	*réservé*	Entier 16 bits

[33] Cet assembly de 11 mots (word) est appelé 112 (0x70) pour les contrôleurs de sécurité FID 2 dont les codes de date sont antérieurs ou égaux à « 1716 ». Référez-vous à la section Quel fichier et documentation EDS du XS/SC26 devez-vous utiliser ? à la page 186 pour en savoir plus.

WORD #	WORD NOM	TYPE DE DONNÉES
6	*réservé*	Entier 16 bits
7	*réservé*	Entier 16 bits
8	Reset/Annulation de la temporisation virtuels (1–16) [Bits de registre RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
9	*réservé*	Entier 16 bits
10	Code d'activation RCD [Registre d'activation RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
11	Demande de lecture ISD (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
12	Chaîne ISD demandée (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
13	Dispositif ISD demandé (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits

13.4.5 Sorties du contrôleur de sécurité (entrées vers l'API)

Vous avez le choix entre cinq objets Assembly de sortie du contrôleur de sécurité.

Le premier et plus petit choix inclut des informations sur les sorties virtuelles et leurs défauts éventuels. Le deuxième ajoute des données avancées, par exemple la raison pour laquelle chacune des sorties de sécurité est désactivée, ainsi que des informations plus détaillées sur les défauts des sorties virtuelles. Le troisième est utilisé uniquement pour accéder au journal des défauts du contrôleur de sécurité. Le quatrième est utilisé pour le retour d'informations sur le reset manuel virtuel et l'annulation de la temporisation. Le cinquième permet d'accéder au retour d'informations sur le reset manuel virtuel et l'annulation de la temporisation, ainsi qu'aux informations ISD. Les cinq options sont illustrées dans les sections suivantes.

Instance d'assembly d'entrée API 100 (0×64) — 8 registres (État/défaut VO)

Cette instance d'assembly n'inclut que des informations de base sur l'état des 64 premières sorties virtuelles.

Table 14. Instance d'assembly d'entrée API 100 (0x64)— Sorties du contrôleur de sécurité - T > O

WORD #	WORD NOM	TYPE DE DONNÉES
0	VO1 – VO16 (voir Indicateurs à la page 217)	Entier 16 bits
1	VO17 – VO32 (voir Indicateurs à la page 217)	Entier 16 bits
2	VO33 – VO48 (voir Indicateurs à la page 217)	Entier 16 bits
3	VO49 – VO64 (voir Indicateurs à la page 217)	Entier 16 bits
4	Bits de défaut pour VO1 – VO16 (voir Indicateurs à la page 217)	Entier 16 bits
5	Bits de défaut pour VO17 – VO32 (voir Indicateurs à la page 217)	Entier 16 bits
6	Bits de défaut pour VO33 – VO48 (voir Indicateurs à la page 217)	Entier 16 bits
7	Bits de défaut pour VO49 – VO64 (voir Indicateurs à la page 217)	Entier 16 bits

Instance d'assembly d'entrée API 101 (0×65) — 104 registres (Mots (word) d'index de défauts)

Cette instance d'assembly inclut l'état des 64 premières sorties virtuelles ainsi que des informations avancées sur les codes d'erreur potentiels et l'état des 2 sorties de sécurité.

Table 15. Instance d'assembly d'entrée API 101 (0x65)— Sorties du contrôleur de sécurité - T > O

WORD #	WORD NOM	TYPE DE DONNÉES
0	VO1 – VO16 (voir Indicateurs à la page 217)	Entier 16 bits
1	VO17 – VO32 (voir Indicateurs à la page 217)	Entier 16 bits

WORD #	WORD NOM	TYPE DE DONNÉES
2	VO33 – VO48 (voir Indicateurs à la page 217)	Entier 16 bits
3	VO49 – VO64 (voir Indicateurs à la page 217)	Entier 16 bits
4	Bits de défaut pour VO1 – VO16 (voir Indicateurs à la page 217)	Entier 16 bits
5	Bits de défaut pour VO17 – VO32 (voir Indicateurs à la page 217)	Entier 16 bits
6	Bits de défaut pour VO33 – VO48 (voir Indicateurs à la page 217)	Entier 16 bits
7	Bits de défaut pour VO49 – VO64 (voir Indicateurs à la page 217)	Entier 16 bits
8–39	*réservé*	Entier 16 bits
40	Index de défaut VO1	Entier 16 bits
41	Index de défaut VO2	Entier 16 bits
42	Index de défaut VO3	Entier 16 bits
43	Index de défaut VO4	Entier 16 bits
44	Index de défaut VO5	Entier 16 bits
45	Index de défaut VO6	Entier 16 bits
46	Index de défaut VO7	Entier 16 bits
47	Index de défaut VO8	Entier 16 bits
48	Index de défaut VO9	Entier 16 bits
49	Index de défaut VO10	Entier 16 bits
50	Index de défaut VO11	Entier 16 bits
51	Index de défaut VO12	Entier 16 bits
52	Index de défaut VO13	Entier 16 bits
53	Index de défaut VO14	Entier 16 bits
54	Index de défaut VO15	Entier 16 bits
55	Index de défaut VO16	Entier 16 bits
56	Index de défaut VO17	Entier 16 bits
57	Index de défaut VO18	Entier 16 bits
58	Index de défaut VO19	Entier 16 bits
59	Index de défaut VO20	Entier 16 bits
60	Index de défaut VO21	Entier 16 bits
61	Index de défaut VO22	Entier 16 bits
62	Index de défaut VO23	Entier 16 bits
63	Index de défaut VO24	Entier 16 bits
64	Index de défaut VO25	Entier 16 bits
65	Index de défaut VO26	Entier 16 bits
66	Index de défaut VO27	Entier 16 bits
67	Index de défaut VO28	Entier 16 bits
68	Index de défaut VO29	Entier 16 bits
69	Index de défaut VO30	Entier 16 bits
70	Index de défaut VO31	Entier 16 bits
71	Index de défaut VO32	Entier 16 bits
72	Index de défaut VO33	Entier 16 bits

WORD #	WORD NOM	TYPE DE DONNÉES
73	Index de défaut VO34	Entier 16 bits
74	Index de défaut VO35	Entier 16 bits
75	Index de défaut VO36	Entier 16 bits
76	Index de défaut VO37	Entier 16 bits
77	Index de défaut VO38	Entier 16 bits
78	Index de défaut VO39	Entier 16 bits
79	Index de défaut VO40	Entier 16 bits
80	Index de défaut VO41	Entier 16 bits
81	Index de défaut VO42	Entier 16 bits
82	Index de défaut VO43	Entier 16 bits
83	Index de défaut VO44	Entier 16 bits
84	Index de défaut VO45	Entier 16 bits
85	Index de défaut VO46	Entier 16 bits
86	Index de défaut VO47	Entier 16 bits
87	Index de défaut VO48	Entier 16 bits
88	Index de défaut VO49	Entier 16 bits
89	Index de défaut VO50	Entier 16 bits
90	Index de défaut VO51	Entier 16 bits
91	Index de défaut VO52	Entier 16 bits
92	Index de défaut VO53	Entier 16 bits
93	Index de défaut VO54	Entier 16 bits
94	Index de défaut VO55	Entier 16 bits
95	Index de défaut VO56	Entier 16 bits
96	Index de défaut VO57	Entier 16 bits
97	Index de défaut VO58	Entier 16 bits
98	Index de défaut VO59	Entier 16 bits
99	Index de défaut VO60	Entier 16 bits
100	Index de défaut VO61	Entier 16 bits
101	Index de défaut VO62	Entier 16 bits
102	Index de défaut VO63	Entier 16 bits
103	Index de défaut VO64	Entier 16 bits

Mots (word) d'index de défaut de sortie virtuelle (VO)

Le numéro d'index de défaut de sortie virtuelle constitue un moyen de représenter le code de défaut associé à une sortie virtuelle donnée sous la forme d'un seul entier 16 bits. Cette valeur équivaut à la valeur de l'index de message d'erreur d'une sortie virtuelle donnée. Consultez les sections Tableaux des codes de défaut du XS/SC26 à la page 349 et Tableau des codes de défaut du SC10-2 à la page 354. Notez que les sorties virtuelles n'ont pas nécessairement d'index de défaut associé.

Instance d'assembly d'entrée API 102 (0×66) — 150 registres (journal des erreurs uniquement)

Cette instance d'assembly est utilisée exclusivement pour accéder aux informations du journal des défauts du contrôleur de sécurité.

Cette instance d'assembly ne contient aucune information sur l'état des sorties virtuelles.

Le contrôleur de sécurité peut stocker 10 défauts dans le journal. Le défaut 1 est le défaut le plus récent, le plus ancien étant le défaut 10.

Table 16. Instance d'assembly d'entrée API 102 (0x66)— Sorties du contrôleur de sécurité - T > O

WORD #	WORD NOM	TYPE DE DONNÉES
0–1	Horodatage Défaut 1	Entier 32 bits
2–9	Nom de l'E/S ou du système Défaut 1	Longueur de 2 mots (word) + 12 caractères ASCII
10	Code d'erreur Défaut 1	Entier 16 bits
11	Code d'erreur avancé Défaut 1	Entier 16 bits
12	Index de message d'erreur Défaut 1	Entier 16 bits
13–14	*réservé*	Entier 16 bits
15–16	Horodatage Défaut 2	Entier 32 bits
17–24	Nom de l'E/S ou du système Défaut 2	Longueur de 2 mots (word) + 12 caractères ASCII
25	Code d'erreur Défaut 2	Entier 16 bits
26	Code d'erreur avancé Défaut 2	Entier 16 bits
27	Index de message d'erreur Défaut 2	Entier 16 bits
28–29	*réservé*	Entier 16 bits
30–31	Horodatage Défaut 3	Entier 32 bits
32–39	Nom de l'E/S ou du système Défaut 3	Longueur de 2 mots (word) + 12 caractères ASCII
40	Code d'erreur Défaut 3	Entier 16 bits
41	Code d'erreur avancé Défaut 3	Entier 16 bits
42	Index de message d'erreur Défaut 3	Entier 16 bits
43–44	*réservé*	Entier 16 bits
45–46	Horodatage Défaut 4	Entier 32 bits
47–54	Nom de l'E/S ou du système Défaut 4	Longueur de 2 mots (word) + 12 caractères ASCII
55	Code d'erreur Défaut 4	Entier 16 bits
56	Code d'erreur avancé Défaut 4	Entier 16 bits
57	Index de message d'erreur Défaut 4	Entier 16 bits
58–59	*réservé*	Entier 16 bits
60–61	Horodatage Défaut 5	Entier 32 bits
62–69	Nom de l'E/S ou du système Défaut 5	Longueur de 2 mots (word) + 12 caractères ASCII
70	Code d'erreur Défaut 5	Entier 16 bits
71	Code d'erreur avancé Défaut 5	Entier 16 bits
72	Index de message d'erreur Défaut 5	Entier 16 bits
73–74	*réservé*	Entier 16 bits
75–76	Horodatage Défaut 6	Entier 32 bits
77–84	Nom de l'E/S ou du système Défaut 6	Longueur de 2 mots (word) + 12 caractères ASCII
85	Code d'erreur Défaut 6	Entier 16 bits
86	Code d'erreur avancé Défaut 6	Entier 16 bits
87	Index de message d'erreur Défaut 6	Entier 16 bits
88–89	*réservé*	Entier 16 bits
90–91	Horodatage Défaut 7	Entier 32 bits
92–99	Nom de l'E/S ou du système Défaut 7	Longueur de 2 mots (word) + 12 caractères ASCII

WORD #	WORD NOM	TYPE DE DONNÉES
100	Code d'erreur Défaut 7	Entier 16 bits
101	Code d'erreur avancé Défaut 7	Entier 16 bits
102	Index de message d'erreur Défaut 7	Entier 16 bits
103–104	*réservé*	Entier 16 bits
105–106	Horodatage Défaut 8	Entier 32 bits
107–114	Nom de l'E/S ou du système Défaut 8	Longueur de 2 mots (word) + 12 caractères ASCII
115	Code d'erreur Défaut 8	Entier 16 bits
116	Code d'erreur avancé Défaut 8	Entier 16 bits
117	Index de message d'erreur Défaut 8	Entier 16 bits
118–119	*réservé*	Entier 16 bits
120–121	Horodatage Défaut 9	Entier 32 bits
122–129	Nom de l'E/S ou du système Défaut 9	Longueur de 2 mots (word) + 12 caractères ASCII
130	Code d'erreur Défaut 9	Entier 16 bits
131	Code d'erreur avancé Défaut 9	Entier 16 bits
132	Index de message d'erreur Défaut 9	Entier 16 bits
133–134	*réservé*	Entier 16 bits
135–136	Horodatage Défaut 10	Entier 32 bits
137–144	Nom de l'E/S ou du système Défaut 10	Longueur de 2 mots (word) + 12 caractères ASCII
145	Code d'erreur Défaut 10	Entier 16 bits
146	Code d'erreur avancé Défaut 10	Entier 16 bits
147	Index de message d'erreur Défaut 10	Entier 16 bits
148–149	*réservé*	Entier 16 bits

Horodatage défaut

Temps relatif, en secondes, de l'occurrence du défaut. Il est mesuré à partir du temps 0, qui correspond à la dernière mise sous tension du contrôleur de sécurité.

Nom de l'E/S ou du système

Chaîne ASCII décrivant la source du défaut.

Code d'erreur, Code d'erreur avancé, Index de message d'erreur

Le code d'erreur plus le code d'erreur avancé constituent le code de défaut du contrôleur de sécurité. Le format du code de défaut est `Error Code 'dot' Advanced Error Code`. Par exemple le code de défaut 2.1 du contrôleur de sécurité est composé du code d'erreur `2` et du code d'erreur avancé `1`. La valeur d'index du message d'erreur est constituée du code d'erreur et du code d'erreur avancé, lequel peut être précédé d'un zéro non significatif, le cas échéant. Par exemple, le code de défaut 2.1 du contrôleur de sécurité est représenté par l'index de message d'erreur `201`. La valeur d'index du message d'erreur offre un moyen pratique d'obtenir le code de défaut complet en lisant uniquement un registre 16 bits.

Instance d'assembly d'entrée API 103 (0×67) — 35 registres (Reset/Annulation de la temporisation)

Cette instance d'assembly permet de communiquer l'état des 256 sorties virtuelles et leurs défauts et de fournir les informations de retour nécessaires pour exécuter des resets et annulations de la temporisation virtuels.

Table 17. Instance d'assembly d'entrée API 103 (0x67)— Sorties du contrôleur de sécurité - T > O

N° DE MOT (WORD)	NOM DU MOT (WORD)	TYPE DE DONNÉES
0	VO1 – VO16 (voir Indicateurs à la page 217)	Entier 16 bits
1	VO17 – VO32 (voir Indicateurs à la page 217)	Entier 16 bits

N° DE MOT (WORD)	NOM DU MOT (WORD)	TYPE DE DONNÉES
2	VO33 – VO48 (voir Indicateurs à la page 217)	Entier 16 bits
3	VO49 – VO64 (voir Indicateurs à la page 217)	Entier 16 bits
4	VO65 – VO80 (voir Indicateurs étendus à la page 218)	Entier 16 bits
5	VO81 – VO96 (voir Indicateurs étendus à la page 218)	Entier 16 bits
6	VO97 – VO112 (voir Indicateurs étendus à la page 218)	Entier 16 bits
7	VO113 – VO128 (voir Indicateurs étendus à la page 218)	Entier 16 bits
8	VO129 – VO144 (voir Indicateurs étendus à la page 218)	Entier 16 bits
9	VO145 – VO160 (voir Indicateurs étendus à la page 218)	Entier 16 bits
10	VO161 – VO176 (voir Indicateurs étendus à la page 218)	Entier 16 bits
11	VO177 – VO192 (voir Indicateurs étendus à la page 218)	Entier 16 bits
12	VO193 – VO208 (voir Indicateurs étendus à la page 218)	Entier 16 bits
13	VO209 – VO224 (voir Indicateurs étendus à la page 218)	Entier 16 bits
14	VO225 – VO240 (voir Indicateurs étendus à la page 218)	Entier 16 bits
15	VO241 – VO256 (voir Indicateurs étendus à la page 218)	Entier 16 bits
16	Bits de défaut pour VO1 – VO16 (voir Indicateurs à la page 217)	Entier 16 bits
17	Bits de défaut pour VO17 – VO32 (voir Indicateurs à la page 217)	Entier 16 bits
18	Bits de défaut pour VO33 – VO48 (voir Indicateurs à la page 217)	Entier 16 bits
19	Bits de défaut pour VO49 – VO64 (voir Indicateurs à la page 217)	Entier 16 bits
20	Bits de défaut pour VO65 – VO80 (voir Indicateurs étendus à la page 218)	Entier 16 bits
21	Bits de défaut pour VO81 – VO96 (voir Indicateurs étendus à la page 218)	Entier 16 bits
22	Bits de défaut pour VO97 – VO112 (voir Indicateurs étendus à la page 218)	Entier 16 bits
23	Bits de défaut pour VO113 – VO128 (voir Indicateurs étendus à la page 218)	Entier 16 bits
24	Bits de défaut pour VO129 – VO144 (voir Indicateurs étendus à la page 218)	Entier 16 bits
25	Bits de défaut pour VO145 – VO160 (voir Indicateurs étendus à la page 218)	Entier 16 bits
26	Bits de défaut pour VO161 – VO176 (voir Indicateurs étendus à la page 218)	Entier 16 bits
27	Bits de défaut pour VO177 – VO192 (voir Indicateurs étendus à la page 218)	Entier 16 bits
28	Bits de défaut pour VO193 – VO208 (voir Indicateurs étendus à la page 218)	Entier 16 bits
29	Bits de défaut pour VO209 – VO224 (voir Indicateurs étendus à la page 218)	Entier 16 bits
30	Bits de défaut pour VO225 – VO240 (voir Indicateurs étendus à la page 218)	Entier 16 bits
31	Bits de défaut pour VO241 – VO256 (voir Indicateurs étendus à la page 218)	Entier 16 bits
32	Retour d'infos Reset/Annulation de la temporisation virtuels (1–16) [Bits de registre de retour RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits

N° DE MOT (WORD)	NOM DU MOT (WORD)	TYPE DE DONNÉES
33	*réservés*	Entier 16 bits
34	Retour d'infos Code d'actionnement RCD [Registre de retour de l'activation RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits

Instance d'assembly d'entrée API 104 (0×68) — 112 registres (Reset/Annulation de la temporisation plus ISD)

Cette instance d'assembly peut être utilisée par les contrôleurs de sécurité SC10-2 et XS26-ISD.

Cette instance d'assembly inclut l'état de marche/arrêt des 256 sorties virtuelles et leurs défauts, le feed-back nécessaire pour exécuter des resets et des annulations de la temporisation virtuels ainsi que des informations d'état sur un maximum de deux chaînes de dispositifs ISD.

Notez que l'instance d'assembly 105 (0×69) contient des informations sur un maximum de huit chaînes de dispositifs ISD, mais ne peut être utilisée que sur le XS26-ISD.

Remarque: Les données ISD ne sont pas immédiatement disponibles à la mise sous tension. Les données ISD peuvent être retardées jusqu'à 10 secondes après la mise sous tension du système.

Table 18. Instance d'assembly d'entrée API 104 (0x68)— Sorties du contrôleur de sécurité T > O

N° DE MOT (WORD)	NOM DU MOT (WORD)	TYPE DE DONNÉES
0	VO1 – VO16 (voir Indicateurs à la page 217)	Entier 16 bits
1	VO17 – VO32 (voir Indicateurs à la page 217)	Entier 16 bits
2	VO33 – VO48 (voir Indicateurs à la page 217)	Entier 16 bits
3	VO49 – VO64 (voir Indicateurs à la page 217)	Entier 16 bits
4	VO65 – VO80 (voir Indicateurs étendus à la page 218)	Entier 16 bits
5	VO81 – VO96 (voir Indicateurs étendus à la page 218)	Entier 16 bits
6	VO97 – VO112 (voir Indicateurs étendus à la page 218)	Entier 16 bits
7	VO113 – VO128 (voir Indicateurs étendus à la page 218)	Entier 16 bits
8	VO129 – VO144 (voir Indicateurs étendus à la page 218)	Entier 16 bits
9	VO145 – VO160 (voir Indicateurs étendus à la page 218)	Entier 16 bits
10	VO161 – VO176 (voir Indicateurs étendus à la page 218)	Entier 16 bits
11	VO177 – VO192 (voir Indicateurs étendus à la page 218)	Entier 16 bits
12	VO193 – VO208 (voir Indicateurs étendus à la page 218)	Entier 16 bits
13	VO209 – VO224 (voir Indicateurs étendus à la page 218)	Entier 16 bits
14	VO225 – VO240 (voir Indicateurs étendus à la page 218)	Entier 16 bits
15	VO241 – VO256 (voir Indicateurs étendus à la page 218)	Entier 16 bits
16	Bits de défaut pour VO1 – VO16 (voir Indicateurs à la page 217)	Entier 16 bits
17	Bits de défaut pour VO17 – VO32 (voir Indicateurs à la page 217)	Entier 16 bits
18	Bits de défaut pour VO33 – VO48 (voir Indicateurs à la page 217)	Entier 16 bits
19	Bits de défaut pour VO49 – VO64 (voir Indicateurs à la page 217)	Entier 16 bits
20	Bits de défaut pour VO65 – VO80 (voir Indicateurs étendus à la page 218)	Entier 16 bits
21	Bits de défaut pour VO81 – VO96 (voir Indicateurs étendus à la page 218)	Entier 16 bits
22	Bits de défaut pour VO97 – VO112 (voir Indicateurs étendus à la page 218)	Entier 16 bits

N° DE MOT (WORD)	NOM DU MOT (WORD)	TYPE DE DONNÉES
23	Bits de défaut pour VO113 – VO128 (voir Indicateurs étendus à la page 218)	Entier 16 bits
24	Bits de défaut pour VO129 – VO144 (voir Indicateurs étendus à la page 218)	Entier 16 bits
25	Bits de défaut pour VO145 – VO160 (voir Indicateurs étendus à la page 218)	Entier 16 bits
26	Bits de défaut pour VO161 – VO176 (voir Indicateurs étendus à la page 218)	Entier 16 bits
27	Bits de défaut pour VO177 – VO192 (voir Indicateurs étendus à la page 218)	Entier 16 bits
28	Bits de défaut pour VO193 – VO208 (voir Indicateurs étendus à la page 218)	Entier 16 bits
29	Bits de défaut pour VO209 – VO224 (voir Indicateurs étendus à la page 218)	Entier 16 bits
30	Bits de défaut pour VO225 – VO240 (voir Indicateurs étendus à la page 218)	Entier 16 bits
31	Bits de défaut pour VO241 – VO256 (voir Indicateurs étendus à la page 218)	Entier 16 bits
32	Retour d'infos Reset/Annulation de la temporisation virtuels (1–16) [Bits de registre de retour RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
33	*réservé*	Entier 16 bits
34	Retour d'infos Code d'actionnement RCD [Registre de retour de l'activation RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
35-36	État système ISD – Nbre de dispositifs Chaîne 1	Entier 32 bits
37-38	État système ISD – Nbre de dispositifs Chaîne 2	Entier 32 bits
39-40	État système ISD – État On/Off des dispositifs Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
41-42	État système ISD – État On/Off des dispositifs Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
43-44	État système ISD – État de défaut Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
45–46	État système ISD – État de défaut Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
47–48	État système ISD – État marginal Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
49-50	État système ISD – État marginal Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
51-52	État système ISD – État d'alerte Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
53–54	État système ISD – État d'alerte Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
55–56	État système ISD – État de reset Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
57–58	État système ISD – État de reset Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
59-60	État système ISD – Actionneur Chaîne 1 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
61-62	État système ISD – Actionneur Chaîne 2 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits

N° DE MOT (WORD)	NOM DU MOT (WORD)	TYPE DE DONNÉES
63–64	État système ISD – État système Chaîne 1 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
65–66	État système ISD – État système Chaîne 2 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
67–82	Liste des dispositifs ISD détectés sur une chaîne	Série de 32 octets
83-99	*réservé*	Entier 16 bits
100	Accusé réc. demande de lecture ISD (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
101	Accusé réc. chaîne ISD demandée (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
102	Accusé réc. dispositif ISD demandé (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
103-111	Données spécifiques à un dispositif ISD individuel (voir Description détaillée des données spécifiques à un dispositif ISD individuel à la page 214)	Entier 16 bits

Instance d’assembly d’entrée API 105 (0×69) — 240 registres (8 chaînes ISD)

Cette instance d’assembly est utilisée uniquement par les contrôleurs de sécurité XS26-ISD.

Cette instance d'assembly inclut l'état marche/arrêt des 256 sorties virtuelles et leurs défauts, le retour d’informations nécessaire pour exécuter des resets et annulations de la temporisation virtuels ainsi que des informations d’état sur un maximum de huit chaînes de dispositifs ISD.

Remarque: Les données ISD ne sont pas immédiatement disponibles à la mise sous tension. Les données ISD peuvent être retardées jusqu'à 10 secondes après la mise sous tension du système.

Table 19. Instance d'assembly d'entrée API 105 (0–69) — Sorties du contrôleur de sécurité - T > O

N° DE MOT (WORD)	NOM DU MOT (WORD)	TYPE DE DONNÉES
0	VO1 – VO16 (voir Indicateurs à la page 217)	Entier 16 bits
1	VO17 – VO32 (voir Indicateurs à la page 217)	Entier 16 bits
2	VO33 – VO48 (voir Indicateurs à la page 217)	Entier 16 bits
3	VO49 – VO64 (voir Indicateurs à la page 217)	Entier 16 bits
4	VO65 – VO80 (voir Indicateurs étendus à la page 218)	Entier 16 bits
5	VO81 – VO96 (voir Indicateurs étendus à la page 218)	Entier 16 bits
6	VO97 – VO112 (voir Indicateurs étendus à la page 218)	Entier 16 bits
7	VO113 – VO128 (voir Indicateurs étendus à la page 218)	Entier 16 bits
8	VO129 – VO144 (voir Indicateurs étendus à la page 218)	Entier 16 bits
9	VO145 – VO160 (voir Indicateurs étendus à la page 218)	Entier 16 bits
10	VO161 – VO176 (voir Indicateurs étendus à la page 218)	Entier 16 bits
11	VO177 – VO192 (voir Indicateurs étendus à la page 218)	Entier 16 bits
12	VO193 – VO208 (voir Indicateurs étendus à la page 218)	Entier 16 bits
13	VO209 – VO224 (voir Indicateurs étendus à la page 218)	Entier 16 bits
14	VO225 – VO240 (voir Indicateurs étendus à la page 218)	Entier 16 bits
15	VO241 – VO256 (voir Indicateurs étendus à la page 218)	Entier 16 bits
16	Bits de défaut pour VO1 – VO16 (voir Indicateurs à la page 217)	Entier 16 bits

N° DE MOT (WORD)	NOM DU MOT (WORD)	TYPE DE DONNÉES
17	Bits de défaut pour VO17 – VO32 (voir Indicateurs à la page 217)	Entier 16 bits
18	Bits de défaut pour VO33 – VO48 (voir Indicateurs à la page 217)	Entier 16 bits
19	Bits de défaut pour VO49 – VO64 (voir Indicateurs à la page 217)	Entier 16 bits
20	Bits de défaut pour VO65 – VO80 (voir Indicateurs étendus à la page 218)	Entier 16 bits
21	Bits de défaut pour VO81 – VO96 (voir Indicateurs étendus à la page 218)	Entier 16 bits
22	Bits de défaut pour VO97 – VO112 (voir Indicateurs étendus à la page 218)	Entier 16 bits
23	Bits de défaut pour VO113 – VO128 (voir Indicateurs étendus à la page 218)	Entier 16 bits
24	Bits de défaut pour VO129 – VO144 (voir Indicateurs étendus à la page 218)	Entier 16 bits
25	Bits de défaut pour VO145 – VO160 (voir Indicateurs étendus à la page 218)	Entier 16 bits
26	Bits de défaut pour VO161 – VO176 (voir Indicateurs étendus à la page 218)	Entier 16 bits
27	Bits de défaut pour VO177 – VO192 (voir Indicateurs étendus à la page 218)	Entier 16 bits
28	Bits de défaut pour VO193 – VO208 (voir Indicateurs étendus à la page 218)	Entier 16 bits
29	Bits de défaut pour VO209 – VO224 (voir Indicateurs étendus à la page 218)	Entier 16 bits
30	Bits de défaut pour VO225 – VO240 (voir Indicateurs étendus à la page 218)	Entier 16 bits
31	Bits de défaut pour VO241 – VO256 (voir Indicateurs étendus à la page 218)	Entier 16 bits
32	Bits de reset/annulation de la temporisation virtuel (1 – 16) (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
33	*réservés*	Entier 16 bits
34	Retour d'infos sur l'activation RCD (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
35-36	État système ISD – Nbre de dispositifs Chaîne 1	Entier 32 bits
37-38	État système ISD – Nbre de dispositifs Chaîne 2	Entier 32 bits
39-40	État système ISD – État On/Off des dispositifs Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
41-42	État système ISD – État On/Off des dispositifs Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
43-44	État système ISD – État de défaut Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
45–46	État système ISD – État de défaut Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
47–48	État système ISD – État marginal Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
49-50	État système ISD – État marginal Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
51-52	État système ISD – État d'alerte Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits

N° DE MOT (WORD)	NOM DU MOT (WORD)	TYPE DE DONNÉES
53–54	État système ISD – État d'alerte Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
55–56	État système ISD – État de reset Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
57–58	État système ISD – État de reset Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
59–60	État système ISD – État Actionneur Chaîne 1 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
61–62	État système ISD – État Actionneur Chaîne 2 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
63–64	État système ISD – État système Chaîne 1 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
65–66	État système ISD – État système Chaîne 2 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
67–82	Liste des dispositifs ISD détectés sur une chaîne	Série de 32 octets
83–99	*réservés*	Entier 16 bits
100	Accusé réc. demande de lecture ISD	Entier 16 bits
101	Accusé réc. chaîne ISD demandée	Entier 16 bits
102	Accusé réc. dispositif ISD demandé	Entier 16 bits
103–111	Données spécifiques à un dispositif ISD individuel	Entier 16 bits
112–113	État système ISD – Nbre de dispositifs Chaîne 1	Entier 32 bits
114–115	État système ISD – État On/Off des dispositifs Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
116–117	État système ISD – État de défaut Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
118–119	État système ISD – État marginal Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
120–121	État système ISD – État d'alerte Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
122–123	État système ISD – État de reset Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
124–125	État système ISD – État Actionneur Chaîne 1 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
126–127	État système ISD – État système Chaîne 1 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
128–129	État système ISD – Nbre de dispositifs Chaîne 2	Entier 32 bits
130–131	État système ISD – État On/Off des dispositifs Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
132–133	État système ISD – État de défaut Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
134–135	État système ISD – État marginal Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
136–137	État système ISD – État d'alerte Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
138–139	État système ISD – État de reset Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
140–141	État système ISD – État Actionneur Chaîne 2 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
142–143	État système ISD – État système Chaîne 2 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
144–145	État système ISD – Nbre de dispositifs Chaîne 3	Entier 32 bits

N° DE MOT (WORD)	NOM DU MOT (WORD)	TYPE DE DONNÉES
146–147	État système ISD – État On/Off des dispositifs Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
148–149	État système ISD – État de défaut Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
150–151	État système ISD – État marginal Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
152–153	État système ISD – État d'alerte Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
154–155	État système ISD – État de reset Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
156–157	État système ISD – État Actionneur Chaîne 3 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
158–159	État système ISD – État système Chaîne 3 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
160–161	État système ISD – Nbre de dispositifs Chaîne 4	Entier 32 bits
162–163	État système ISD – État On/Off des dispositifs Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
164–165	État système ISD – État de défaut Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
166–167	État système ISD – État marginal Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
168–169	État système ISD – État d'alerte Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
170–171	État système ISD – État de reset Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
172–173	État système ISD – État Actionneur Chaîne 4 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
174–175	État système ISD – État système Chaîne 4 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
176–177	État système ISD – Nbre de dispositifs Chaîne 5	Entier 32 bits
178–179	État système ISD – État On/Off des dispositifs Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
180–181	État système ISD – État de défaut Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
182–183	État système ISD – État marginal Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
184–185	État système ISD – État d'alerte Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
186–187	État système ISD – État de reset Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
188–189	État système ISD – État Actionneur Chaîne 5 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
190–191	État système ISD – État système Chaîne 5 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
192–193	État système ISD – Nbre de dispositifs Chaîne 6	Entier 32 bits
194–195	État système ISD – État On/Off des dispositifs Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
196–197	État système ISD – État de défaut Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
198–199	État système ISD – État marginal Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits

N° DE MOT (WORD)	NOM DU MOT (WORD)	TYPE DE DONNÉES
200–201	État système ISD – État d'alerte Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
202–203	État système ISD – État de reset Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
204–205	État système ISD – État Actionneur Chaîne 6 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
206–207	État système ISD – État système Chaîne 6 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
208–209	État système ISD – Nbre de dispositifs Chaîne 7	Entier 32 bits
210–211	État système ISD – État On/Off des dispositifs Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
212–213	État système ISD – État de défaut Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
214–215	État système ISD – État marginal Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
216–217	État système ISD – État d'alerte Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
218–219	État système ISD – État de reset Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
220–221	État système ISD – État Actionneur Chaîne 7 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
222–223	État système ISD – État système Chaîne 7 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
224–225	État système ISD – Nbre de dispositifs Chaîne 8	Entier 32 bits
226–227	État système ISD – État On/Off des dispositifs Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
228–229	État système ISD – État de défaut Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
230–231	État système ISD – État marginal Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
232–233	État système ISD – État d'alerte Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
234–235	État système ISD – État de reset Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
236–237	État système ISD – État Actionneur Chaîne 8 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
238–239	État système ISD – État système Chaîne 8 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits

Description détaillée des données spécifiques à un dispositif ISD individuel

Le tableau suivant décrit l'instance d'assembly 104 (0x68) MOT (WORD) N°103-111 ou le message explicite Lire la réponse ISD MOT (WORD) N°68-76.

Table 20. Description détaillée des données spécifiques à un dispositif ISD individuel

WORD.BIT N°	Informations	Taille des données
103.0	Défaut d'entrée de sécurité	1 bit
103.1	*réservés*	1 bit
103.2	Capteur non couplé	1 bit
103.3	Erreur de données ISD	1 bit
103.4	Mauvais actionneur/État du bouton/État de l'entrée	1 bit

WORD.BIT N°	Informations	Taille des données
103.5	Portée marginale/État du bouton/État de l'entrée	1 bit
103.6	Actionneur détecté	1 bit
103.7	Erreur de sortie	1 bit
103.8	Entrée 2	1 bit
103.9	Entrée 1	1 bit
103.10	Reset local attendu	1 bit
103.11	Avertissement de tension de fonctionnement	1 bit
103.12	Erreur de tension de fonctionnement	1 bit
103.13	Sortie 2	1 bit
103.14	Sortie 1	1 bit
103.15	Remise sous tension requise	1 bit
104.0	Sorties à tolérance de panne	1 bit
104.1	Dispositif de reset local	1 bit
104.2	En cascade	1 bit
104.3	Niveau de codage élevé	1 bit
104.4 à 104.7	Apprentissages restants	4 bits
104.8 à 104.12	ID dispositif	5 bits
104.13 à 105.2	Nombre d'avertissements de portée	6 bits
105.3 à 105.7	Délai de désactivation de la sortie	5 bits
105.8 à 105.15	Nombre d'erreurs de tension	8 bits
106.0 à 106.7	Température interne [35]	8 bits
106.8 à 106.15	Distance de l'actionneur [35]	8 bits
107.0 à 107.7	Tension d'alimentation [35]	8 bits
107.8 à 107.11	Nom de société attendu	4 bits
107.12 à 107.15	Nom de société reçu	4 bits
108	Code attendu	16 bits
109	Code reçu	16 bits
110	Erreur interne A	16 bits
111	Erreur interne B	16 bits

13.4.6 Objet Assembly de configuration

Le contrôleur de sécurité n'utilise pas d'objet Assembly de configuration.

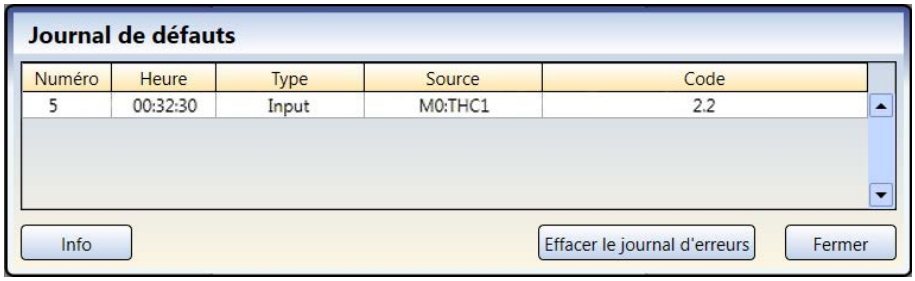
Comme certains clients Ethernet/IP en exigent un, utilisez l'instance 128 (0×80) avec une taille de zéro registre (16 bits).

13.4.7 Exemples de défaut

La figure suivante illustre un défaut dans le journal des défauts du logiciel Contrôleur de sécurité Banner.

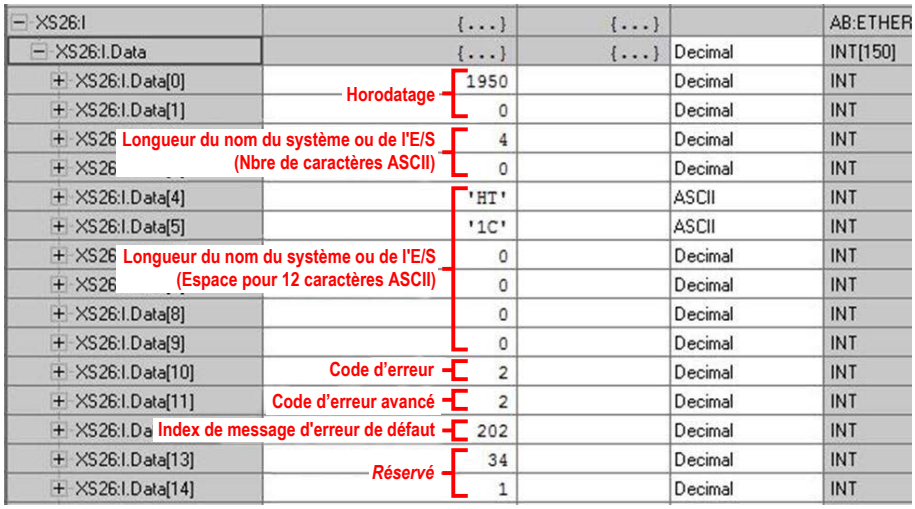
[35] Pour la conversion de la température interne, de la distance de l'actionneur et de la tension, voir la section ISD : Informations sur la conversion de la distance, tension et température à la page 309.

Illustration 225. Journal des défauts avec un seul défaut



La figure suivante illustre le même défaut, tel qu'observé dans les registres Ethernet/IP.

Illustration 226. Registres Ethernet/IP avec un seul défaut

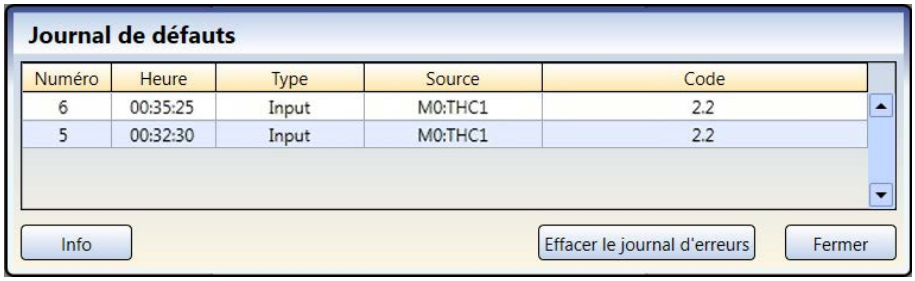


Notez le format de chaîne ControlLogix, où les caractères ASCII sont affichés, deux par registre, à l'envers. « THC1 » devient « HT » dans le registre 4, suivi de « 1C » dans le registre 5.

Index de message d'erreur de défaut 202 = Code de défaut 2.2 (Défaut de simultanéité). Pour plus d'informations sur les défauts, voir Tableaux des codes de défaut du XS/SC26 à la page 349 ou Tableau des codes de défaut du SC10-2 à la page 354.

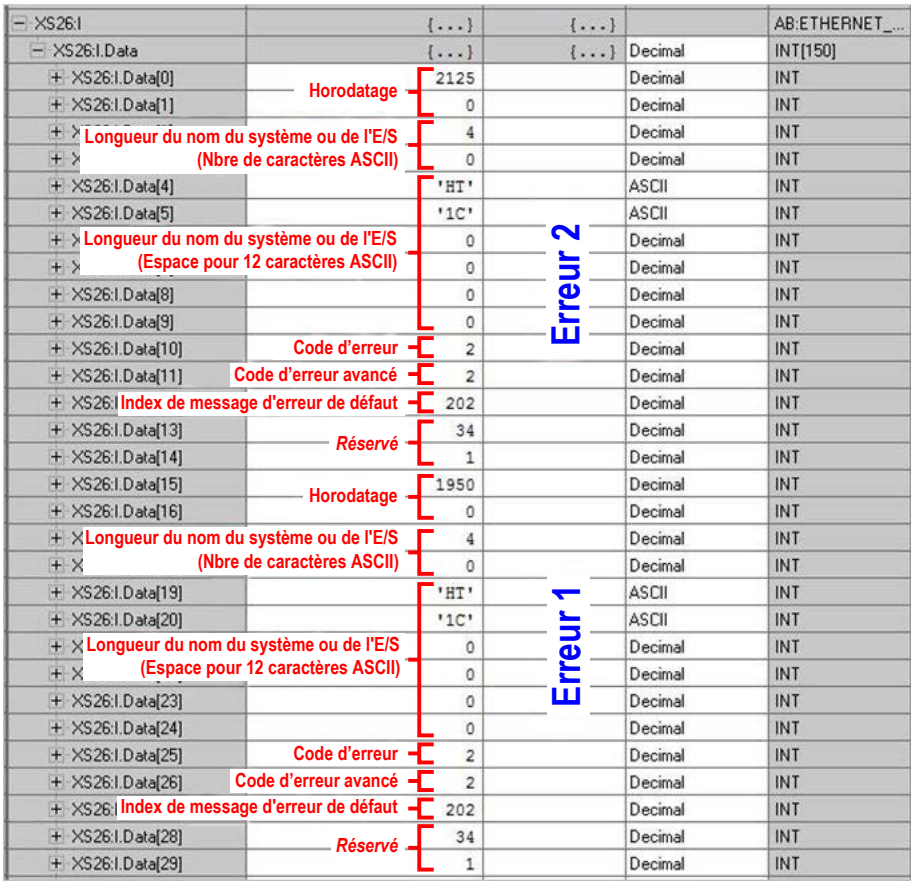
La figure suivante illustre deux défauts dans le journal des défauts du logiciel XS26-2E.

Illustration 227. Journal des défauts avec deux défauts



La figure suivante illustre les mêmes 2 défauts, tels qu'observés dans les registres de l'API. Notez aussi que l'erreur 2 plus récente fait descendre l'erreur 1 dans la liste.

Illustration 228. Registres Ethernet/IP avec deux défauts



13.4.8 Indicateurs

Les mots (word) 0 à 7, définis ci-dessous, apparaissent comme les 8 premiers mots dans les instances d'assembly 100, 101 et 103.

Table 21. Word 0, sorties virtuelles 1–16

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO16	VO15	VO14	VO13	VO12	VO11	VO10	VO9	VO8	VO7	VO6	VO5	VO4	VO3	VO2	VO1

Table 22. Word 1, Sorties virtuelles 17–32

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO32	VO31	VO30	VO29	VO28	VO27	VO26	VO25	VO24	VO23	VO22	VO21	VO20	VO19	VO18	VO17

Table 23. Word 2, sorties virtuelles 33–48

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO48	VO47	VO46	VO45	VO44	VO43	VO42	VO41	VO40	VO39	VO38	VO37	VO36	VO35	VO34	VO33

Table 24. Word 3, sorties virtuelles 49–64

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO64	VO63	VO62	VO61	VO60	VO59	VO58	VO57	VO56	VO55	VO54	VO53	VO52	VO51	VO50	VO49

Table 25. Word 4, bits d'indicateur de défaut pour les sorties virtuelles 1–16

Notez que toutes les sorties virtuelles n'ont pas d'indicateur de défaut défini.

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO16	VO15	VO14	VO13	VO12	VO11	VO10	VO9	VO8	VO7	VO6	VO5	VO4	VO3	VO2	VO1

Table 26. Word 5, bits d'indicateur de défaut pour les sorties virtuelles 17–32

Notez que toutes les sorties virtuelles n'ont pas d'indicateur de défaut défini.

Position de bit															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VO32	VO31	VO30	VO29	VO28	VO27	VO26	VO25	VO24	VO23	VO22	VO21	VO20	VO19	VO18	VO17

Table 27. Word 6, bits d'indicateur de défaut pour les sorties virtuelles 33–48

Notez que toutes les sorties virtuelles n'ont pas d'indicateur de défaut défini.

Position de bit															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VO48	VO47	VO46	VO45	VO44	VO43	VO42	VO41	VO40	VO39	VO38	VO37	VO36	VO35	VO34	VO33

Table 28. Word 7, bits d'indicateur de défaut pour les sorties virtuelles 49–64

Notez que toutes les sorties virtuelles n'ont pas d'indicateur de défaut défini.

Position de bit															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VO64	VO63	VO62	VO61	VO60	VO59	VO58	VO57	VO56	VO55	VO54	VO53	VO52	VO51	VO50	VO49

13.4.9 Indicateurs étendus

Outre les 64 premières sorties virtuelles indiquées ci-dessus, l'instance d'assembly 103 en ajoute 192 autres (pour un total de 256). Les bits de l'indicateur de défaut sont décalés vers le bas pour offrir l'espace suffisant au regroupement des 256 sorties virtuelles.

Les mots (word) 0 à 3 sont les mêmes que ceux indiqués sous Indicateurs à la page 217. Dans le cas de l'instance d'assembly 103, les modifications suivantes sont effectuées :

- Word 4 – Sorties virtuelles 65 à 80, où VO65 est à la position de bit 0 et VO80 à celle du bit 15
- Word 5 – Sorties virtuelles 81 à 96, où VO81 est à la position de bit 0 et VO96 à celle du bit 15
- Word 6 – Sorties virtuelles 97 à 112, où VO97 est à la position de bit 0 et VO112 à celle du bit 15
- Word 7 – Sorties virtuelles 113 à 128, où VO113 est à la position de bit 0 et VO128 à celle du bit 15
- Word 8 – Sorties virtuelles 129 à 144, où VO129 est à la position de bit 0 et VO144 à celle du bit 15
- Word 9 – Sorties virtuelles 145 à 160, où VO145 est à la position de bit 0 et VO160 à celle du bit 15
- Word 10 – Sorties virtuelles 161 à 176, où VO161 est à la position de bit 0 et VO176 à celle du bit 15
- Word 11 – Sorties virtuelles 177 à 192, où VO177 est à la position de bit 0 et VO192 à celle du bit 15
- Word 12 – Sorties virtuelles 193 à 208, où VO193 est à la position de bit 0 et VO208 à celle du bit 15
- Word 13 – Sorties virtuelles 209 à 224, où VO209 est à la position de bit 0 et VO224 à celle du bit 15
- Word 14 – Sorties virtuelles 225 à 240, où VO225 est à la position de bit 0 et VO240 à celle du bit 15
- Word 15 – Sorties virtuelles 241 à 256, où VO241 est à la position de bit 0 et VO256 à celle du bit 15
- Words 16 - 19 sont identiques à Words 4 > 7 figurant sous Indicateurs à la page 217. L'instance d'assembly 103 inclut également plus de bits d'indicateur de défaut, comme indiqué ci-dessous
- Word 20 – Bits de défaut pour les sorties VO65 à VO80, le défaut de la sortie VO65 étant à la position de bit 0 et celui de la sortie VO80 à la position de bit 15

Ce modèle reste d'application pour Words 21 à 31, afin de couvrir le reste des bits de défaut pour l'ensemble des 256 sorties virtuelles.

13.4.10 Mots (word) d'état de système ISD

Les mots (word) d'état du système ISD tels qu'ils figurent dans l'instance d'assembly d'entrée API 104 (0×68), mots (words) 39-62, sont définis ci-dessous.

Chacun de ces mots d'état du système n'est pas censé être considéré comme un entier 32 bits unique, mais plutôt comme une table de 32 bits d'état de dispositifs ISD individuels, où le bit 0 est attribué au dispositif ISD 1, le bit 1 au dispositif ISD 2, et ainsi de suite jusqu'au bit 31, attribué au 32e dispositif ISD de cette chaîne.

- N° mot (word) 39-40 État On/Off des dispositifs Chaîne 1 — On/Off dispositif ISD 1 Chaîne 1 est le mot 39, bit 0 ; On/Off dispositif ISD 32 Chaîne 1 est le mot 40, bit 15
- N° mot (word) 41-42 État On/Off des dispositifs Chaîne 2 — On/Off dispositif ISD 1 Chaîne 2 est le mot 41, bit 0 ; On/Off dispositif ISD 32 Chaîne 2 est le mot 42, bit 15
- N° mot (word) 43-44 État de défaut Chaîne 1 — État de défaut dispositif ISD 1 Chaîne 1 est le mot 43, bit 0 ; État de défaut dispositif ISD 32 Chaîne 1 est le mot 44, bit 15
- N° mot (word) 45-46 État de défaut Chaîne 2 — État de défaut dispositif ISD 1 Chaîne 2 est le mot 45, bit 0 ; — État de défaut dispositif ISD 32 Chaîne 2 est le mot 46, bit 15
- N° mot (word) 47-48 État marginal Chaîne 1 — État marginal dispositif ISD 1 Chaîne 1 est le mot 47, bit 0 ; État marginal dispositif ISD 32 Chaîne 1 est le mot 48, bit 15
- N° mot (word) 49-50 État marginal Chaîne 2 — État marginal dispositif ISD 1 Chaîne 2 est le mot 49, bit 0 ; État marginal dispositif ISD 32 Chaîne 2 est le mot 50, bit 15

- N° mot (word) 51-52 État d'alerte Chaîne 1 — État d'alerte dispositif ISD 1 Chaîne 1 est le mot 51, bit 0 ; État d'alerte dispositif ISD 32 Chaîne 1 est le mot 52, bit 15
- N° mot (word) 53-54 État d'alerte Chaîne 2 — État d'alerte dispositif ISD 1 Chaîne 2 est le mot 53, bit 0 ; État d'alerte dispositif ISD 32 Chaîne 2 est le mot 54, bit 15
- N° mot (word) 55-56 État de reset Chaîne 1 — État de reset dispositif ISD 1 Chaîne 1 est le mot 55, bit 0 ; État de défaut dispositif ISD 32 Chaîne 1 est le mot 56, bit 15
- N° mot (word) 57-58 État de reset Chaîne 2 — État de reset dispositif ISD 1 Chaîne 2 est le mot 57, bit 0 ; État de défaut dispositif ISD 32 Chaîne 2 est le mot 58, bit 15
- N° mot (word) 59-60 Actionneur reconnu Chaîne 1 — Actionneur reconnu dispositif ISD 1 Chaîne 1 est le mot 59, bit 0 ; Actionneur reconnu dispositif ISD 32 Chaîne 1 est le mot 60, bit 15
- N° mot (word) 61-62 Actionneur reconnu Chaîne 2 — Actionneur reconnu dispositif ISD 1 Chaîne 2 est le mot 61, bit 0 ; Actionneur reconnu dispositif ISD 32 Chaîne 2 est le mot 62, bit 15

13.4.11 Configuration RSLogix5000 (Message explicite)

Pour obtenir une valeur d'index de défaut spécifique pour l'une des 255 premières sorties virtuelles, utilisez les connexions Message explicite. En plus des instances d'assembly de la section précédente, certaines instances supplémentaires sont uniquement accessibles via des messages explicites.

Choix de connexions Message explicite

Lire les sorties du contrôleur de sécurité

Pour effectuer une lecture unique de l'une des instances d'assembly Sortie du contrôleur de sécurité/entrée API T>O des Sorties du contrôleur de sécurité (entrées vers l'API) à la page 202, utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 4, Instance 100 (0x64), 101 (0x65), 102 (0x66), 103 (0×67) ou 104 (0×68), Attribut 3. Un message explicite correct de ce type renvoie l'instance d'assembly appropriée, comme illustré dans le tableau Sorties du contrôleur de sécurité (entrées vers l'API) à la page 202.

Voir un exemple de ce type de connexion dans Exemple de lecture des sorties du contrôleur de sécurité à la page 224.

Écrire les entrées du contrôleur de sécurité

Pour écrire une seule fois les données dans les instances d'assembly Entrées du contrôleur de sécurité (Sorties de l'API) des Entrées du contrôleur de sécurité (sorties de l'API) à la page 201, utilisez le Type de service 16 (Set Attribute Single, hex 10), Classe 4, Instance 112 (0×70), 113 (0×71) ou 114 (0×72), Attribut 3. La taille de l'élément source MSG (table de tags définie par l'utilisateur) est donnée par l'objet Assembly en question. Un message explicite correct de ce type écrit les données pertinentes sur le contrôleur de sécurité ; voir Entrées du contrôleur de sécurité (sorties de l'API) à la page 201.

Voir un exemple de ce type de connexion dans Exemple d'écriture des entrées du contrôleur de sécurité à la page 225.

Remarque: Les contrôleurs de sécurité ne prennent pas tous en charge les entrées virtuelles.

État de sortie virtuelle

Pour obtenir l'état actuel des 64 premières sorties virtuelles, utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 0×64, Instance 1, Attribut 1. Un message explicite correct de ce type renvoie deux entiers 32 bits représentant l'état des sorties VO1 à VO64. Voir un exemple de ce type de connexion dans Exemple de lecture de l'état des sorties virtuelles à la page 227.

Lire l'état des sorties virtuelles étendues

Pour obtenir l'état actuel des 256 sorties virtuelles, utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 0×75, Instance 1, Attribut 1. Un message explicite réussi de ce type renvoie des entiers 32 bits contenant les bits d'état des sorties virtuelles VO1 à VO256.

Bits de défaut de sortie virtuelle

Pour obtenir l'état actuel des 64 premiers bits de défaut de sortie virtuelle, utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 0×65, Instance 1, Attribut 1. Un message explicite correct de ce type renvoie deux entiers 32 bits représentant l'état des bits de défaut des sorties VO1 à VO64.

Lire les bits de défaut de sortie virtuelle étendue

Pour obtenir l'état actuel des 256 bits de défaut des sorties virtuelles, utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 0×76, Instance 1, Attribut 1. Un message explicite réussi de ce type renvoie huit entiers 32 bits contenant les bits de défaut des sorties virtuelles, du défaut VO1 au défaut VO256.

Valeurs individuelles d'index de défauts

Pour obtenir une valeur d'index de défaut spécifique pour l'une des 64 premières sorties virtuelles, utilisez le service de type 14 (Get Attribute Single, hex 0E), la classe 0×6F, l'instance 1-64 (en choisir une), l'attribut 1. Un message explicite réussi de ce type renvoie un registre unique de 16 bits représentant la valeur de l'index d'erreur pour l'une des sorties virtuelles.

Lire les valeurs individuelles d'index de défauts étendues

Pour obtenir une valeur d'index de défaut spécifique pour l'une des 255 sorties virtuelles, utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 0×7A, Instance 1–255 (sélectionnez-en une), Attribut 1.

Un message explicite correct de ce type renvoie un registre 16 bits représentant la valeur d'index de défaut pour l'une des sorties virtuelles.

Écrire les entrées virtuelles (Activation de l'inhibition On/Off)

Pour écrire des bits d'activation de l'inhibition On/Off virtuels sur le contrôleur de sécurité, utilisez le Type de service 16 (Set Attribute Single, hex 10), Classe 0×77, Instance 1, Attribut 1. La longueur des données à écrire correspond à deux entiers 32 bits (8 octets). Un message explicite correct de ce type écrit les entrées virtuelles (activation de l'inhibition On/Off) VI1 à VI64.

N° de mot (word)	Nom du mot (word)	Type de données
0	Entrées virtuelles VI0–15	Entier 16 bits
1	Entrées virtuelles VI16–31	Entier 16 bits
2	Entrées virtuelles VI32–47	Entier 16 bits
3	Entrées virtuelles VI48–63	Entier 16 bits

Écrire les entrées virtuelles (Reset manuel et Annulation de la temporisation virtuels)

Pour écrire des bits de reset manuel/annulation de la temporisation virtuels sur le contrôleur de sécurité, utilisez le Type de service 16 (Set Attribute Single, hex 10), Classe 0×78, Instance 1, Attribut 1. La longueur des données à écrire correspond à deux entiers 32 bits (8 octets). Un message explicite correct de ce type écrit les bits de reset/annulation de la temporisation virtuels VRCD1 à VRCD32 et le code d'activation RCD.

Remarque: Les contrôleurs de sécurité ne prennent pas tous en charge les entrées virtuelles.

N° de mot (word)	Nom du mot (word)	Type de données
0	VRCD (VRCD1-16) (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
1	VRCD (VRCD17-32) (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
2	Code d'activation RCD [Activation RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
3	*réservés*	Entier 16 bits

Lire les sorties virtuelles (retour d'informations sur le reset manuel et l'annulation du retard au déclenchement)

Pour lire l'état des bits de sortie virtuelle liés au retour d'informations sur le reset manuel et l'annulation du retard au déclenchement virtuels du contrôleur de sécurité, utilisez le type de service 14 (Get Attribute Single, hex 0E), classe 0×79, instance 1, attribut 1.

Un message explicite correct de ce type renvoie deux entiers 32 bits contenant les bits de retour de reset/annulation du retard au déclenchement virtuels VRCD 1 via le retour VRCD 32 et le retour du code d'actionnement RCD.

Remarque: Les contrôleurs de sécurité ne prennent pas tous en charge les entrées virtuelles.

N° de mot (word)	Nom du mot (word)	Type de données
0	Retour d'informations VRCD (VRCD1–16) (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits

N° de mot (word)	Nom du mot (word)	Type de données
1	Retour d'informations VRCD (VRCD17–32) (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
2	Retour d'infos Code d'actionnement RCD [Retour sur l'activation RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
3	*réservés*	Entier 16 bits

Écrire une demande ISD

Pour écrire une demande d'informations sur un dispositif ISD sur le contrôleur de sécurité, utilisez le Type de service 16 (Set Attribute Single, hex 10), Classe 0×81, Instance 1, Attribut 1. La longueur des données à écrire correspond à trois entiers 16 bits (6 octets). Un message explicite correct de ce type écrit la demande ISD sur le contrôleur de sécurité.

Remarque: Les contrôleurs de sécurité ne prennent pas tous en charge ISD.

N° mot (word)	Nom du mot (word)	Type de données
0	Demande de lecture ISD (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
1	Chaîne ISD demandée (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
2	Dispositif ISD demandé (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits

Lire la réponse ISD (SC10-2 ou XS26-ISD, jusqu'à 2 chaînes ISD)

Ce message explicite peut être utilisé par les contrôleurs de sécurité SC10-2 et XS26-ISD.

Pour lire la réponse du contrôleur de sécurité à une demande ISD (voir Écrire une demande ISD à la page 221), utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 0×80, Instance 1, Attribut 1. Un message explicite correct de ce type renvoie 77 mots contenant les informations indiquées ci-dessous.

Remarque:

- Les contrôleurs de sécurité ne prennent pas tous en charge ISD.
- Les données ISD ne sont pas immédiatement disponibles à la mise sous tension. Les données ISD peuvent être retardées jusqu'à 10 secondes après la mise sous tension du système.

N° de mot (word)	Nom du mot (word)	Type de données
0–1	État système ISD – Nbre de dispositifs Chaîne 1	Entier 32 bits
2–3	État système ISD – Nbre de dispositifs Chaîne 2	Entier 32 bits
4–5	État système ISD – État On/Off des dispositifs Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
6–7	État système ISD – État On/Off des dispositifs Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
8–9	État système ISD – État de défaut Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
10–11	État système ISD – État de défaut Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
12–13	État système ISD – État marginal Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
14–15	État système ISD – État marginal Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
16–17	État système ISD – État d'alerte Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
18–19	État système ISD – État d'alerte Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits

N° de mot (word)	Nom du mot (word)	Type de données
20–21	État système ISD – État de reset Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
22–23	État système ISD – État de reset Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
24–25	État système ISD – Actionneur Chaîne 1 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
26–27	État système ISD – Actionneur Chaîne 2 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
28–29	État système ISD – État système Chaîne 1 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
30–31	État système ISD – État système Chaîne 2 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
32–47	Liste des dispositifs ISD détectés sur une chaîne	Table de 32 octets
48–64	*réservés*	Entier 16 bits
65	Accusé réc. demande de lecture ISD (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
66	Accusé réc. chaîne ISD demandée (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
67	Accusé réc. dispositif ISD demandé (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
68–76	Données spécifiques à un dispositif ISD individuel (voir Description détaillée des données spécifiques à un dispositif ISD individuel à la page 214)	Entier 16 bits

Lecture de la réponse ISD (modèles XS26-ISD uniquement, jusqu'à 8 chaînes ISD)

Ce message explicite n'est utilisé que par le contrôleur de sécurité XS26-ISD.

Pour lire la réponse du contrôleur de sécurité à une demande ISD (voir Écrire une demande ISD à la page 221), utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 0×82, Instance 1, Attribut 1. Un message explicite correct de ce type renvoie 128 mots (word) contenant les informations indiquées ci-dessous.

Remarque:
- Les contrôleurs de sécurité ne prennent pas tous en charge ISD.
- Seul le XS26-ISD prend en charge huit chaînes de dispositifs ISD.
- Les données ISD ne sont pas immédiatement disponibles à la mise sous tension. Les données ISD peuvent être retardées jusqu'à 10 secondes après la mise sous tension du système.

N° de mot (word)	Nom du mot (word)	Type de données
0-1	État système ISD – Nbre de dispositifs Chaîne 1	Entier 32 bits
2-3	État système ISD – État On/Off des dispositifs Chaîne 1	Entier 32 bits
4-5	État système ISD – État de défaut Chaîne 1	Entier 32 bits
6-7	État système ISD – État marginal Chaîne 1	Entier 32 bits
8-9	État système ISD – État d'alerte Chaîne 1	Entier 32 bits
10-11	État système ISD – État de reset Chaîne 1	Entier 32 bits
12-13	État système ISD – État Actionneur Chaîne 1 reconnu	Entier 32 bits
14-15	État système ISD – État système Chaîne 1	Entier 32 bits
16-17	État système ISD – Nbre de dispositifs Chaîne 2	Entier 32 bits
18-19	État système ISD – État On/Off des dispositifs Chaîne 2	Entier 32 bits
20-21	État système ISD – État de défaut Chaîne 2	Entier 32 bits

N° de mot (word)	Nom du mot (word)	Type de données
22-23	État système ISD – État marginal Chaîne 2	Entier 32 bits
24-25	État système ISD – État d'alerte Chaîne 2	Entier 32 bits
26-27	État système ISD – État de reset Chaîne 2	Entier 32 bits
28-29	État système ISD – État Actionneur Chaîne 2 reconnu	Entier 32 bits
30-31	État système ISD – État système Chaîne 2	Entier 32 bits
32-33	État système ISD – Nbre de dispositifs Chaîne 3	Entier 32 bits
34-35	État système ISD – État On/Off des dispositifs Chaîne 3	Entier 32 bits
36-37	État système ISD – État de défaut Chaîne 3	Entier 32 bits
38-39	État système ISD – État marginal Chaîne 3	Entier 32 bits
40-41	État système ISD – État d'alerte Chaîne 3	Entier 32 bits
42-43	État système ISD – État de reset Chaîne 3	Entier 32 bits
44-45	État système ISD – État Actionneur Chaîne 3 reconnu	Entier 32 bits
46-47	État système ISD – État système Chaîne 3	Entier 32 bits
48-49	État système ISD – Nbre de dispositifs Chaîne 4	Entier 32 bits
50-51	État système ISD – État On/Off des dispositifs Chaîne 4	Entier 32 bits
52-53	État système ISD – État de défaut Chaîne 4	Entier 32 bits
54-55	État système ISD – État marginal Chaîne 4	Entier 32 bits
56-57	État système ISD – État d'alerte Chaîne 4	Entier 32 bits
58-59	État système ISD – État de reset Chaîne 4	Entier 32 bits
60-61	État système ISD – État Actionneur Chaîne 4 reconnu	Entier 32 bits
62-63	État système ISD – État système Chaîne 4	Entier 32 bits
64-65	État système ISD – Nbre de dispositifs Chaîne 5	Entier 32 bits
66-67	État système ISD – État On/Off des dispositifs Chaîne 5	Entier 32 bits
68-69	État système ISD – État de défaut Chaîne 5	Entier 32 bits
70-71	État système ISD – État marginal Chaîne 5	Entier 32 bits
72-73	État système ISD – État d'alerte Chaîne 5	Entier 32 bits
74-75	État système ISD – État de reset Chaîne 5	Entier 32 bits
76-77	État système ISD – État Actionneur Chaîne 5 reconnu	Entier 32 bits
78-79	État système ISD – État système Chaîne 5	Entier 32 bits
80-81	État système ISD – Nbre de dispositifs Chaîne 6	Entier 32 bits
82-83	État système ISD – État On/Off des dispositifs Chaîne 6	Entier 32 bits
84-85	État système ISD – État de défaut Chaîne 6	Entier 32 bits
86-87	État système ISD – État marginal Chaîne 6	Entier 32 bits
88-89	État système ISD – État d'alerte Chaîne 6	Entier 32 bits
90-91	État système ISD – État de reset Chaîne 6	Entier 32 bits
92-93	État système ISD – État Actionneur Chaîne 6 reconnu	Entier 32 bits
94-95	État système ISD – État système Chaîne 6	Entier 32 bits
96-97	État système ISD – Nbre de dispositifs Chaîne 7	Entier 32 bits
98-99	État système ISD – État On/Off des dispositifs Chaîne 7	Entier 32 bits
100-101	État système ISD – État de défaut Chaîne 7	Entier 32 bits
102-103	État système ISD – État marginal Chaîne 7	Entier 32 bits
104-105	État système ISD – État d'alerte Chaîne 7	Entier 32 bits

N° de mot (word)	Nom du mot (word)	Type de données
106-107	État système ISD – État de reset Chaîne 7	Entier 32 bits
108-109	État système ISD – État Actionneur Chaîne 7 reconnu	Entier 32 bits
110-111	État système ISD – État système Chaîne 7	Entier 32 bits
112-113	État système ISD – Nbre de dispositifs Chaîne 8	Entier 32 bits
114-115	État système ISD – État On/Off des dispositifs Chaîne 8	Entier 32 bits
116-117	État système ISD – État de défaut Chaîne 8	Entier 32 bits
118-119	État système ISD – État marginal Chaîne 8	Entier 32 bits
120-121	État système ISD – État d'alerte Chaîne 8	Entier 32 bits
122-123	État système ISD – État de reset Chaîne 8	Entier 32 bits
124-125	État système ISD – État Actionneur Chaîne 8 reconnu	Entier 32 bits
126-127	État système ISD – État système Chaîne 8	Entier 32 bits

Entrée individuelle de journal des défauts

Pour obtenir une entrée spécifique du journal des défauts à 10 entrées, utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 0×71, Instance 1, Attribut 1–10 (sélectionnez-en un). Un message explicite correct de ce type renvoie une entrée de registre 15 unique du journal des défauts, comme défini ci-dessous. Notez que l'attribut 1 désigne l'entrée la plus récente du journal d'erreurs et l'attribut 10 la plus ancienne.

N° mot (word)	Nom du mot (word)	Type de données
0–1	Horodatage Défaut 1	Entier 32 bits
2–9	Nom de l'E/S ou du système Défaut 1	Longueur de 2 mots (word) + 12 caractères ASCII
10	Code d'erreur Défaut 1	Entier 16 bits
11	Code d'erreur avancé Défaut 1	Entier 16 bits
12	Index de message d'erreur Défaut 1	Entier 16 bits
13–14	*réservé*	Entier 16 bits

Informations système

Il est possible d'accéder à certaines informations système à l'aide du Type de service 14 (Get Attribute Single, hex 0E), Classe 0×72, Instance 1, Attribut 1–4 (sélectionnez-en un, voir le tableau suivant). Un message explicite correct de ce type renvoie les informations système ci-dessous (la taille et le type de données varient). Voir un exemple de ce type de connexion dans Exemple de lecture d'informations système à la page 227.

Attribut	Valeur système	Type de données
1	Secondes depuis le démarrage	Entier 32 bits
2	Mode de fonctionnement	Entier 16 bits
3	Nom de la configuration	Longueur de 2 mots (word) + 16 caractères ASCII
4	CRC de configuration	Entier 32 bits

Exemples de connexions Message explicite

Exemple de lecture des sorties du contrôleur de sécurité

Pour lire une seule fois l'instance d'assembly 100 (0×64), utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 4, Instance 100, Attribut 3. Un message explicite correct de ce type renvoie les 8 registres de l'instance d'assembly 100 (0×64), définie dans Objet Assembly de configuration à la page 215.

La figure suivante illustre la commande MSG pour ce message explicite.

*Illustration 229. Commande MSG — Onglet **Configuration***

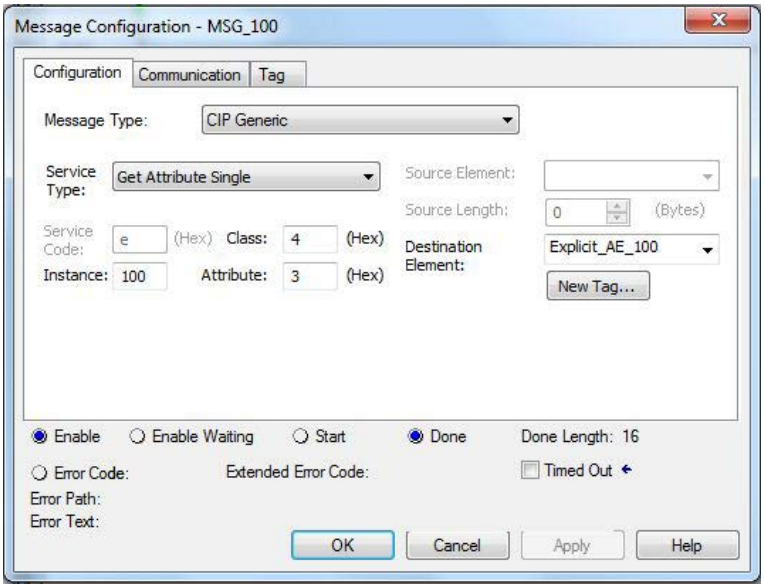
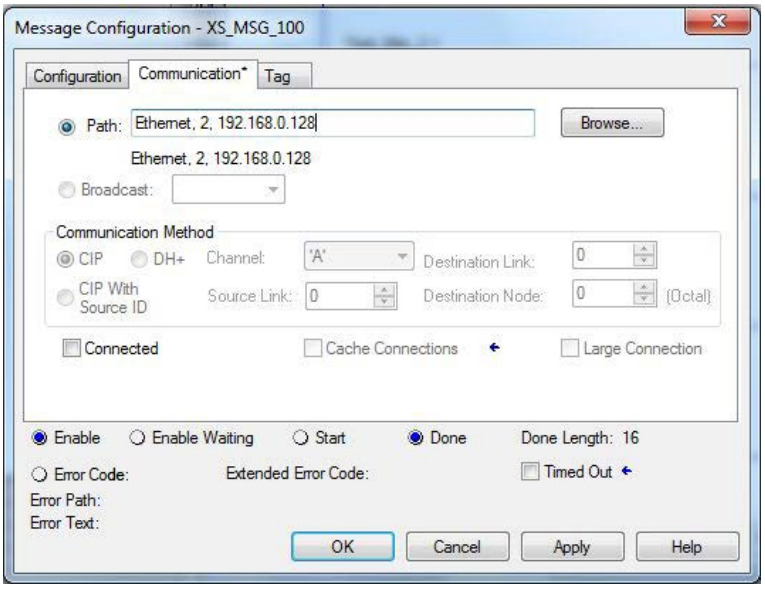


*Illustration 230. Commande MSG — Onglet **Communication***



La figure suivante illustre la table définie par l'utilisateur (appelée XS_Explicit_AE_100) affichant les 8 registres.

Illustration 231. Table définie par l'utilisateur

XS_Explicit_AE_100	{...}	{...}	Decimal	INT[8]
XS_Explicit_AE_100[0]	2		Decimal	INT
XS_Explicit_AE_100[1]	0		Decimal	INT
XS_Explicit_AE_100[2]	0		Decimal	INT
XS_Explicit_AE_100[3]	0		Decimal	INT
XS_Explicit_AE_100[4]	0		Decimal	INT
XS_Explicit_AE_100[5]	0		Decimal	INT
XS_Explicit_AE_100[6]	0		Decimal	INT
XS_Explicit_AE_100[7]	0		Decimal	INT

Dans cet exemple de données, nous pouvons voir que VO2 est actuellement activé (ON). VO2 est le mot (word) 0, bit 1> 2^1 = 2

Exemple d'écriture des entrées du contrôleur de sécurité

Pour écrire une seule fois les données dans l'instance d'assembly Entrées du contrôleur de sécurité (Sorties de l'API) 112 (0×70), utilisez le Type de service 16 (Set Attribute Single, hex 10), Classe 4, Instance 112 (0×70), Attribut 3. La taille de l'élément source MSG (table de tags définie par l'utilisateur) équivaut à 4 octets dans ce cas.

La figure suivante illustre la table définie par l'utilisateur (appelée AE112) à écrire sur le contrôleur de sécurité.

Illustration 232. Table définie par l'utilisateur à écrire sur le contrôleur de sécurité

◢ AE112	{...}	{...}	Decimal	INT[2]
▷ AE112[0]	7		Decimal	INT
▷ AE112[1]	0		Decimal	INT

La figure suivante illustre la commande MSG pour ce message explicite.

*Illustration 233. Commande MSG — Onglet **Configuration***

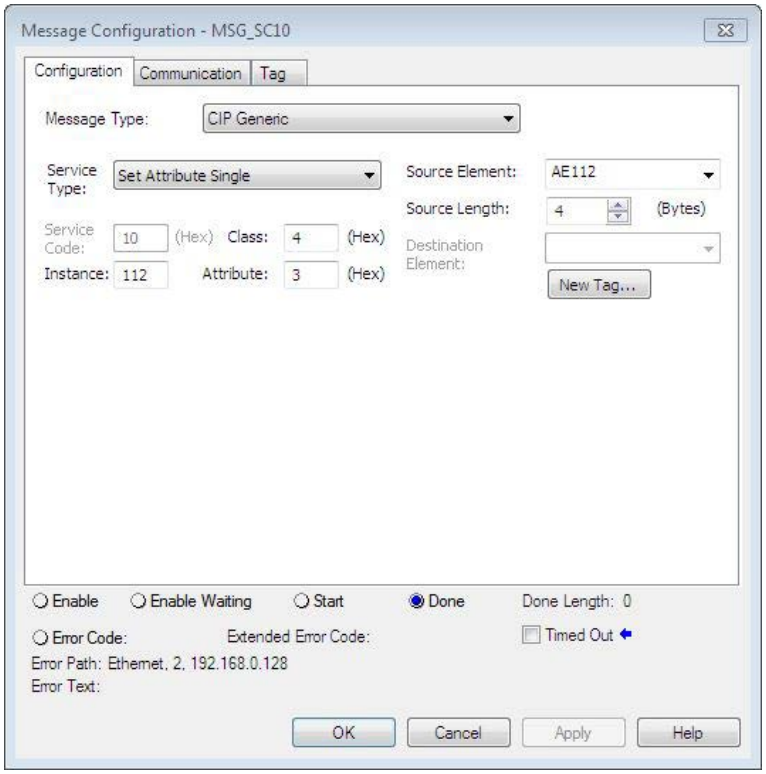
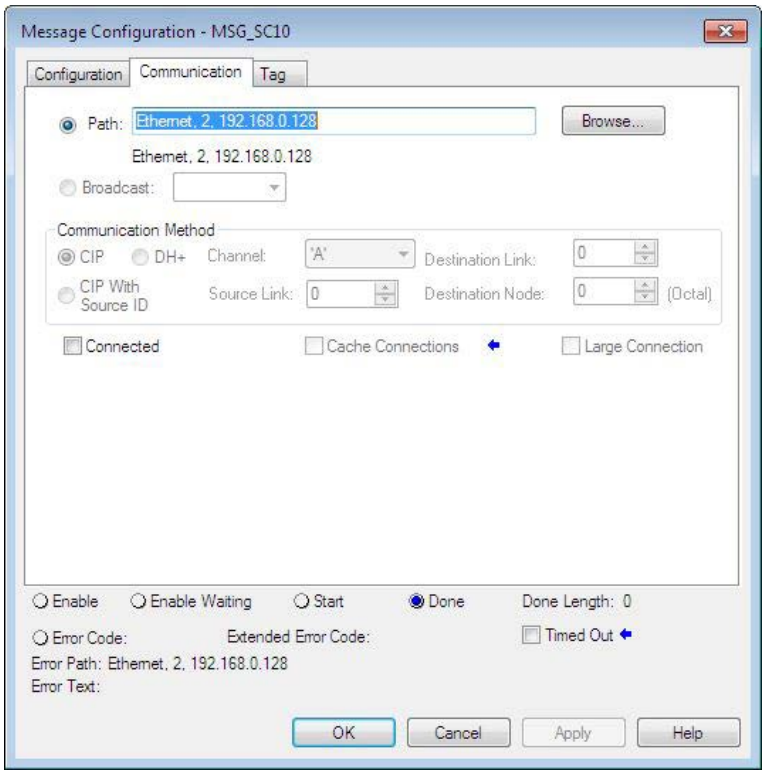


*Illustration 234. Commande MSG — Onglet **Communication***



Exemple de lecture de l'état des sorties virtuelles

Pour lire une seule fois l'état actuel des 64 premières sorties virtuelles, utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 0×64, Instance 1, Attribut 1. Un message explicite correct de ce type renvoie deux entiers 32 bits représentant l'état des sorties VO1 à VO64.

La figure suivante illustre la commande MSG pour ce message explicite.

*Illustration 235. Commande MSG — Onglet **Configuration***

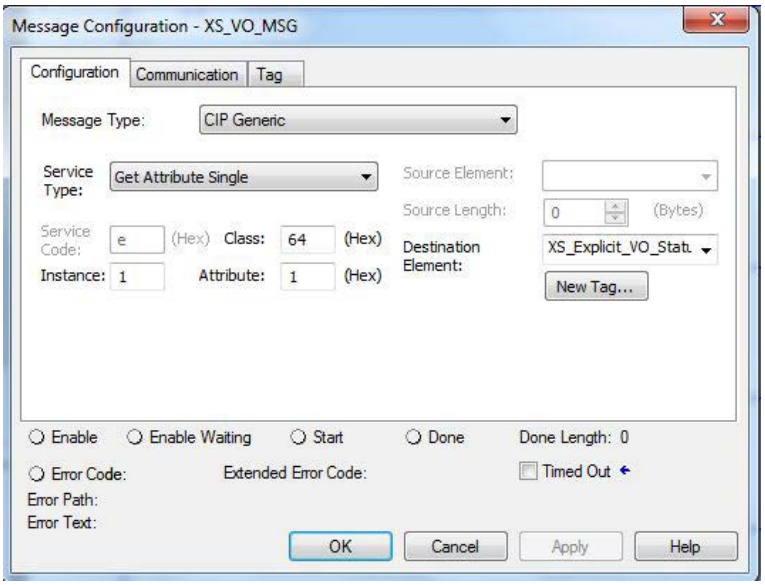
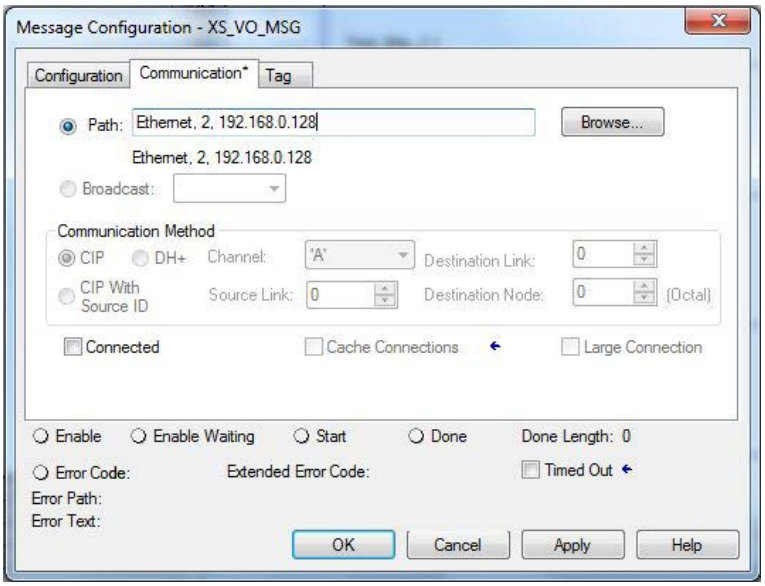


*Illustration 236. Commande MSG — Onglet **Communication***



La figure suivante illustre la table définie par l'utilisateur (appelée XS_Explicit_VO_Status) affichant deux entiers 32 bits.

Illustration 237. Table définie par l'utilisateur

XS_Explicit_VO_Status	{...}	{...}	Decimal	DINT[2]
XS_Explicit_VO_Status[0]	1		Decimal	DINT
XS_Explicit_VO_Status[1]	0		Decimal	DINT

Dans cet exemple de données, nous pouvons voir que VO1 est actuellement activé (ON). VO1 est le mot 1, bit 0 > 2^0 = 1

Exemple de lecture d'informations système

Il est possible d'accéder à certaines informations système au moyen de messages explicites Ethernet/IP, et notamment le nom de la configuration du contrôleur de sécurité. Pour obtenir ces informations, utilisez le Type de service 14 (Get Attribute Single, hex 0E), Classe 0×72, Instance 1, Attribut 3. Un message explicite correct de ce type renvoie la chaîne ASCII et 32 bits représentant le nom de la configuration du contrôleur de sécurité.

La figure suivante illustre la commande MSG pour ce message explicite.

*Illustration 238. Commande MSG — Onglet **Configuration***

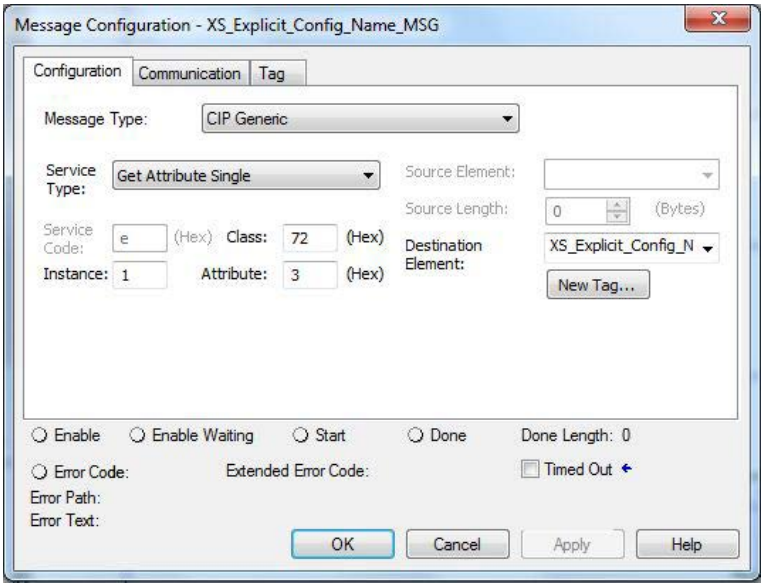
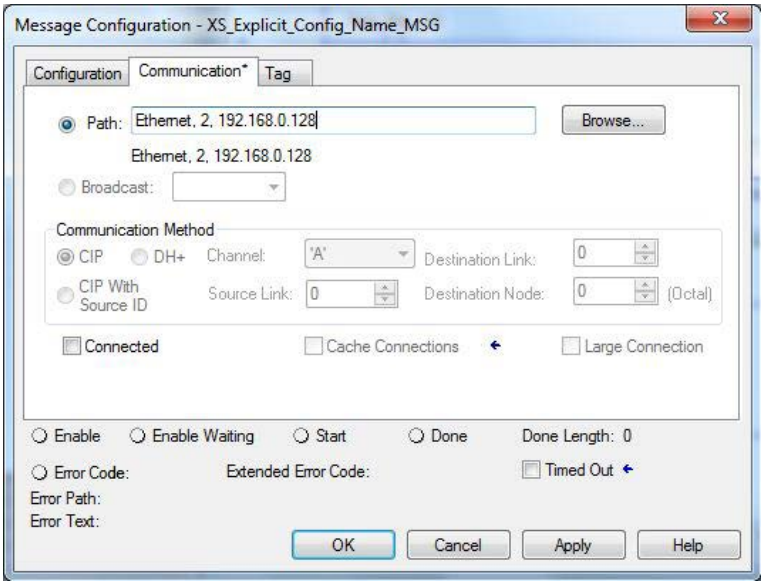


*Illustration 239. Commande MSG — Onglet **Communication***



La figure suivante illustre la table définie par l'utilisateur (appelé XS_Explicit_Config_Name) affichant les 8 registres.

Illustration 240. Table définie par l'utilisateur

XS_Explicit_Config_Name	{...}	{...}	Decimal	INT[10]
XS_Explicit_Config_Name[0]	12		Decimal	INT
XS_Explicit_Config_Name[1]	0		Decimal	INT
XS_Explicit_Config_Name[2]	'1B'		ASCII	INT
XS_Explicit_Config_Name[3]	'na'		ASCII	INT
XS_Explicit_Config_Name[4]	' k'		ASCII	INT
XS_Explicit_Config_Name[5]	'oC'		ASCII	INT
XS_Explicit_Config_Name[6]	'fn'		ASCII	INT
XS_Explicit_Config_Name[7]	'gi'		ASCII	INT
XS_Explicit_Config_Name[8]	0		Decimal	INT
XS_Explicit_Config_Name[9]	0		Decimal	INT

Notez que les deux premiers registres sont des entiers 32 bits décrivant le nombre de caractères ASCII composant le nom de la configuration. Ici, il est égal à *12*. Les caractères ASCII sont compressés, deux par registre dans le pseudo-format String de ControlLogix. Ici, le nom de la configuration est *Blank Config* (Config vide) mais le format de chaîne ControlLogix affiche ces caractères, deux par ligne, en ordre inverse.

Messages explicites - Procédure

Pour créer une toute nouvelle connexion Message explicite dans un programme d'API Allen-Bradley, procédez comme suit.

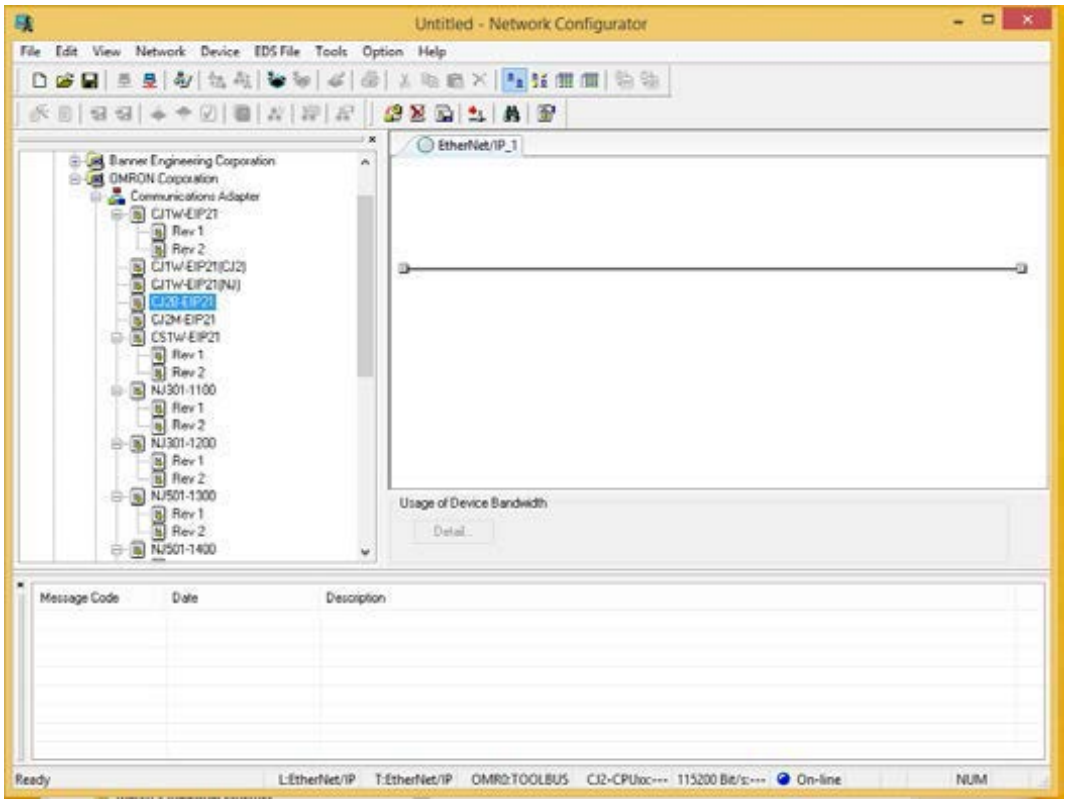
1. Créez un nouveau tag avec le type de données Message.
2. Le nouveau tag doit servir d'élément de destination (une table 16 bits suffisamment grande pour stocker les données qui seront demandées).
3. Ajoutez une commande MSG à votre logique Ladder (à l'aide du tag Message du registre 1 et de l'élément de destination du registre 2). Les valeurs de classe, d'instance et d'attribut varient selon les données voulues.
4. Dans l'onglet Communication de la commande MSG, saisissez le chemin d'accès au contrôleur de sécurité : par exemple, `Ethernet, 2, 192.168.0.128`, *2* étant utilisé pour les connexions Ethernet/IP dans l'API et l'adresse IP indiquée étant celle du contrôleur de sécurité.

13.4.12 Configuration EIP sur un API Omron

Les figures suivantes illustrent une connexion EtherNet/IP entre un contrôleur de sécurité et un API Omron CJ2H.

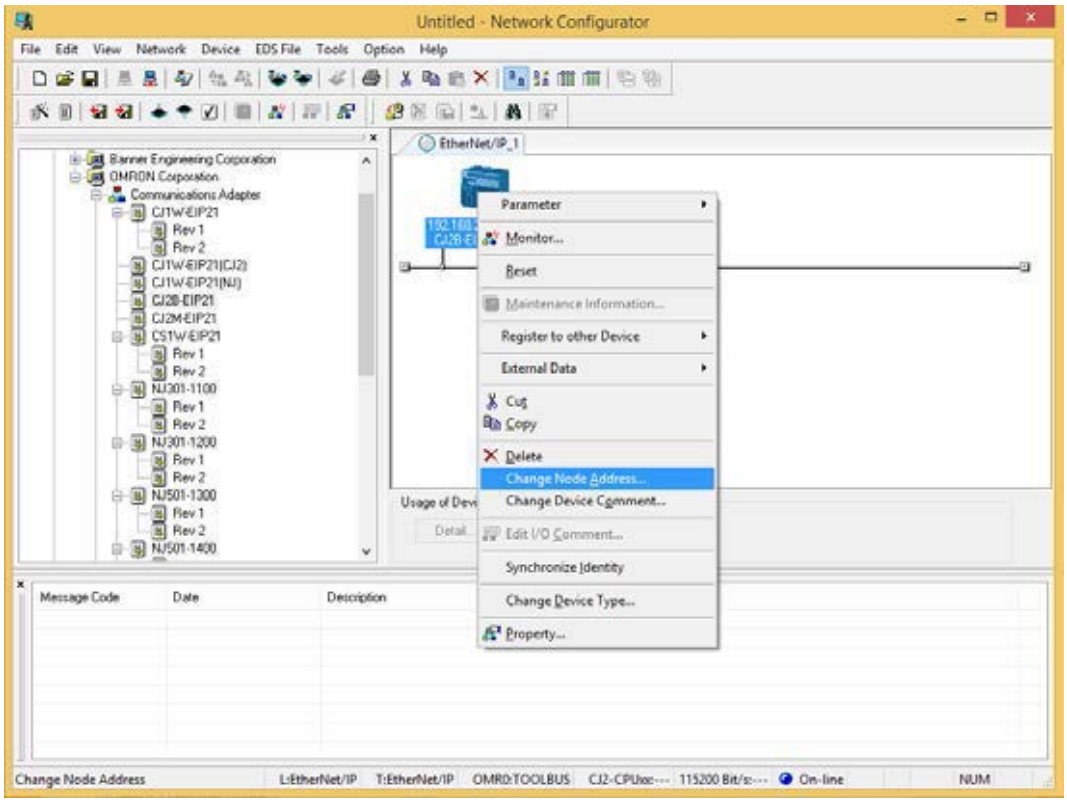
1. Ouvrez le logiciel Omron Network Configurator.

Illustration 241. Logiciel Omron Network Configurator



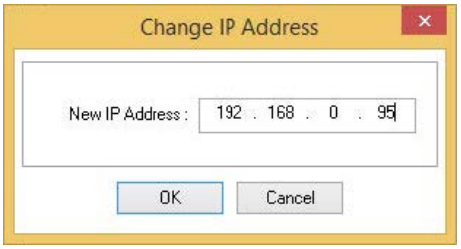
2. Ajoutez l'API correct au réseau.
3. Cliquez avec le bouton droit sur l'API et cliquez sur **Change Node Address** (Modifier l'adresse du noeud) pour changer l'adresse IP.

Illustration 242. Menu contextuel



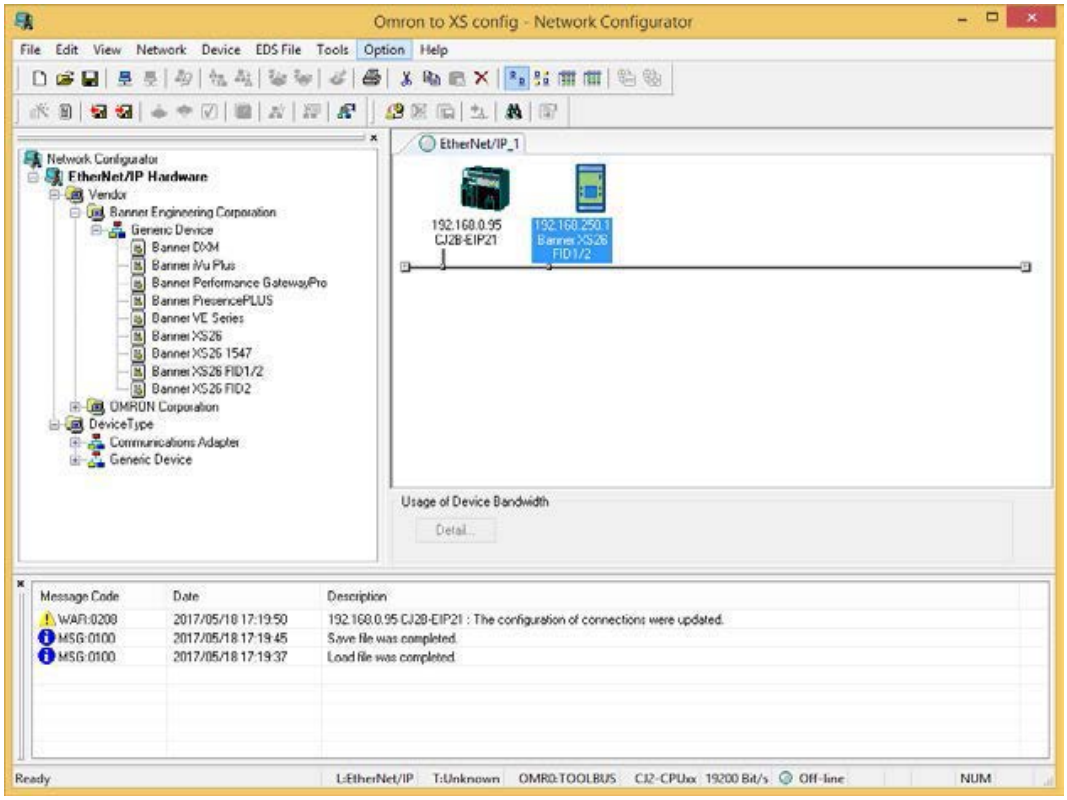
Voici l'adresse IP de l'API :

Illustration 243. Adresse IP de l'API



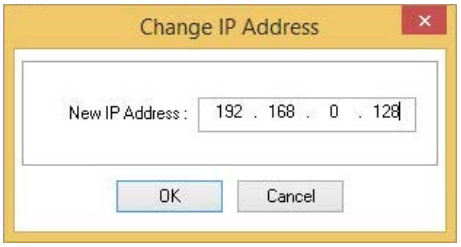
4. Installez le fichier EDS du contrôleur de sécurité.
   a) Accédez à **EDS_File** > **Install**.
   b) Recherchez le fichier EDS et sélectionnez-le.
   c) Double-cliquez sur le nouvel élément dans la liste à gauche pour l'ajouter au réseau.

Illustration 244. Ajout du contrôleur de sécurité



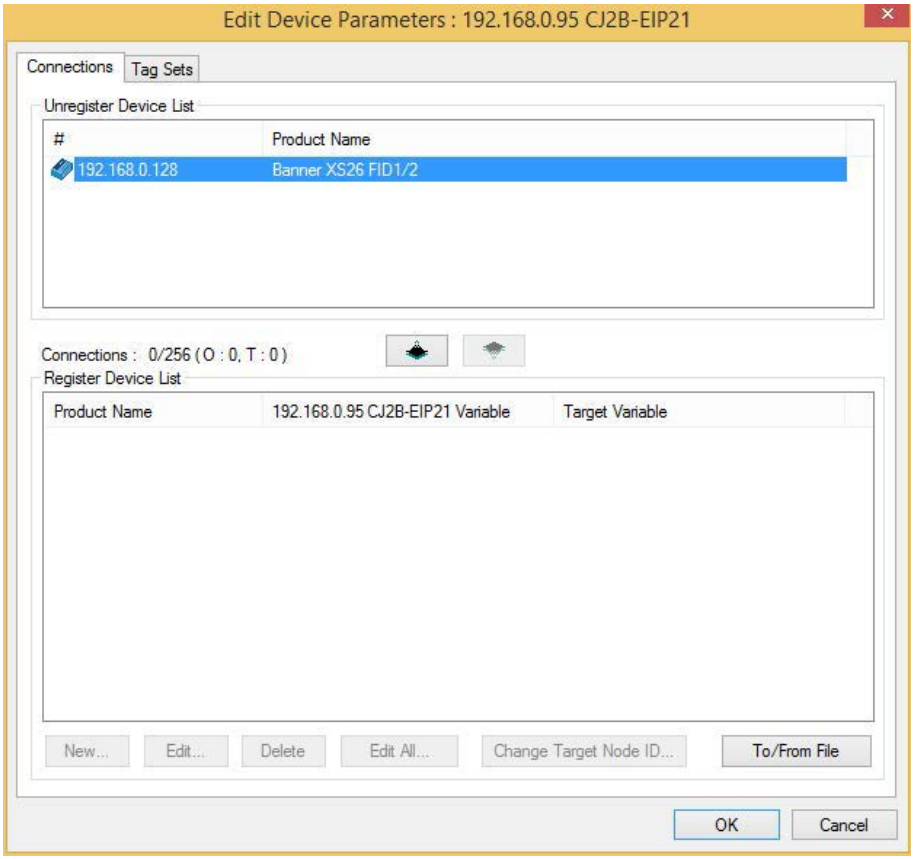
5. Cliquez avec le bouton droit sur le contrôleur de sécurité et cliquez sur **Change Node Address** (Modifier l'adresse du nœud) pour changer l'adresse IP.
6. Indiquez l'adresse IP du contrôleur de sécurité.

Illustration 245. Adresse IP du contrôleur de sécurité



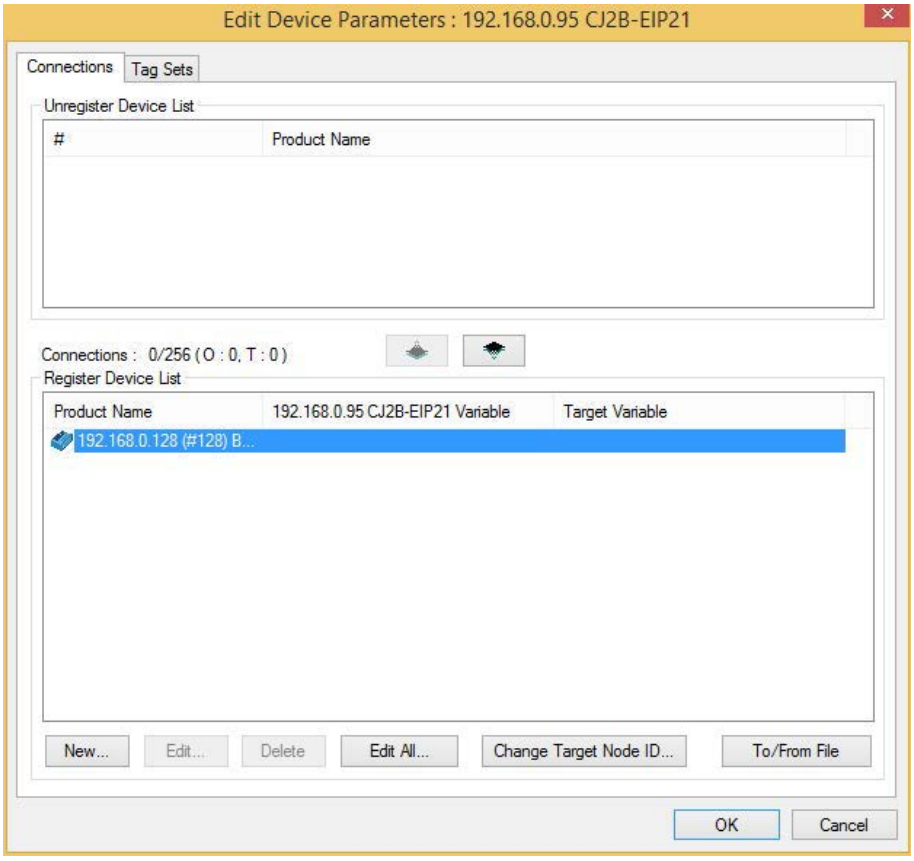
7. Double-cliquez sur l'icône de l'API pour modifier les paramètres du dispositif.
   a) Sélectionnez le contrôleur de sécurité dans la liste **Unregister Device List** (Liste des dispositifs non enregistrés).

Illustration 246. ***Liste des dispositifs non enregistrés***



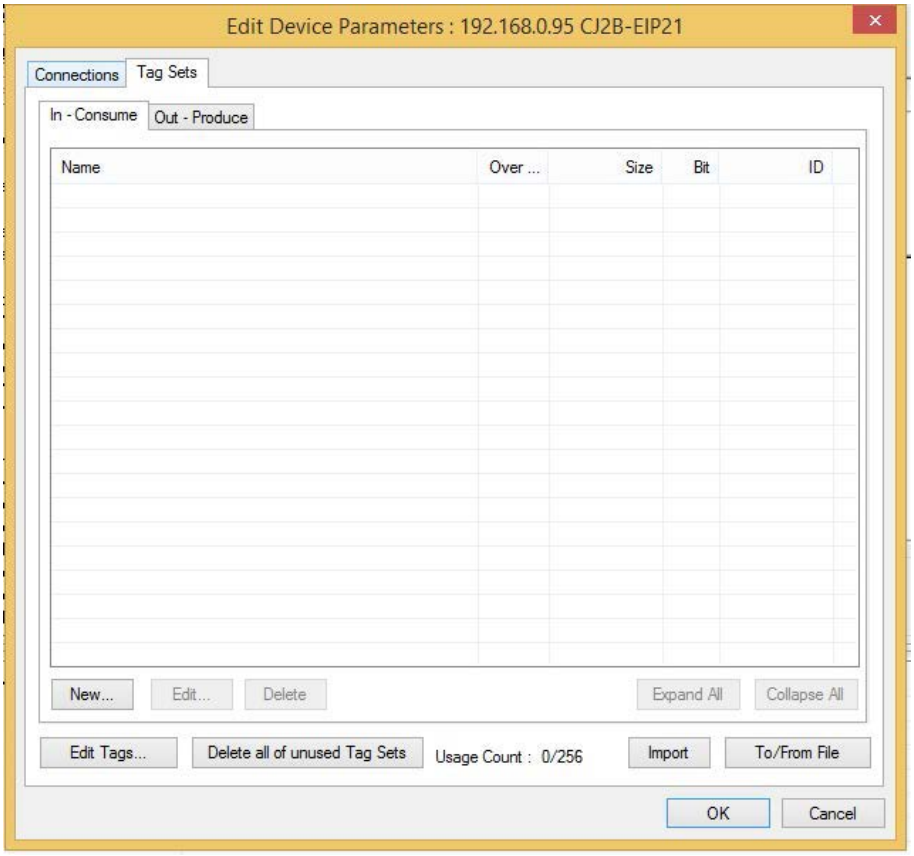
b) Cliquez sur la flèche Bas pour l'envoyer vers la liste **Register Device List** (Liste des dispositifs enregistrés).

Illustration 247. ***Register Device List (Liste des dispositifs enregistrés)***



c) Cliquez sur l'onglet **Tag Sets** (Ensembles de tags) (pour afficher la fenêtre ci-dessous).

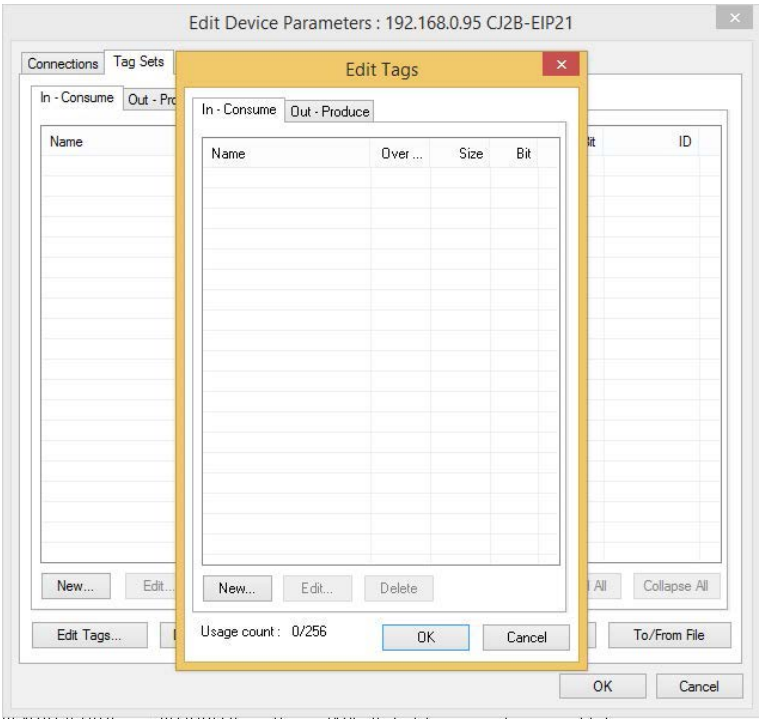
*Illustration 248. Onglet **Tag Sets***



d) Cliquez sur **Edit Tags…** (Modifier les tags).
La fenêtre **Edit Tags** s'affiche.

e) Cliquez sur l'onglet **In - Consume** (Entrée - Consommer).

*Illustration 249. Fenêtre **Edit Tag** — Onglet **In - Consume***



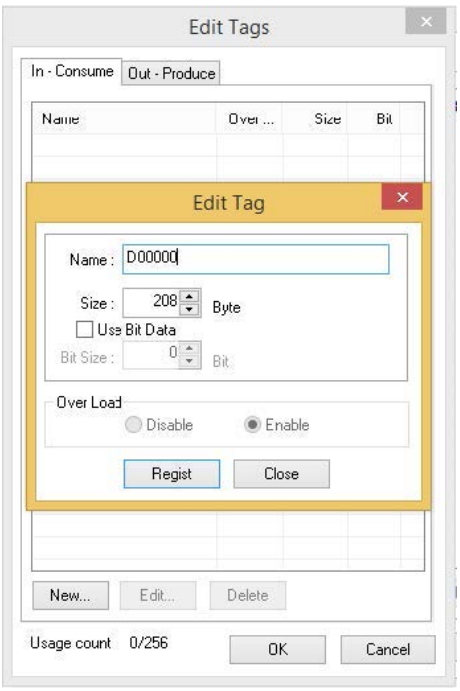
f) Cliquez sur **New** (Nouveau).
La fenêtre **Edit Tag** (Modifier le tag) s'affiche.

g) Sélectionnez une zone de données processeur de type et taille appropriés.
Dans cet exemple, le contrôleur de sécurité envoie des mots (word) de 16 bits, par conséquent vous pouvez utiliser la zone mémoire de données (DM Area). Choisissez une taille (**Size**) (nombre d'octets) égale à l'instance d'assembly EIP voulue. Ici, il s'agit d'entrées utilisées (*In - Consume*) (du point de vue de l'API), soit les assemblys de type T > O. Voir les sections Entrées du contrôleur de sécurité (sorties de l'API) à la page

201 et Sorties du contrôleur de sécurité (entrées vers l'API) à la page 202 pour en savoir plus sur les objets assembly. Les choix suivants sont possibles :

- État/défaut VO - 100 (0×64), taille 16 octets
- Mots (word) de l'index de défauts - 101 (0×65), taille 208 octets
- Journal des erreurs uniquement - 102 (0×66), taille 300 octets
- Reset/Annulation de la temporisation - 103 (0×67), taille 70 octets
- VRCD plus ISD - 104 (0×68), taille 224 octets
- 8 chaînes ISD - 105 (0×69), taille 480 octets

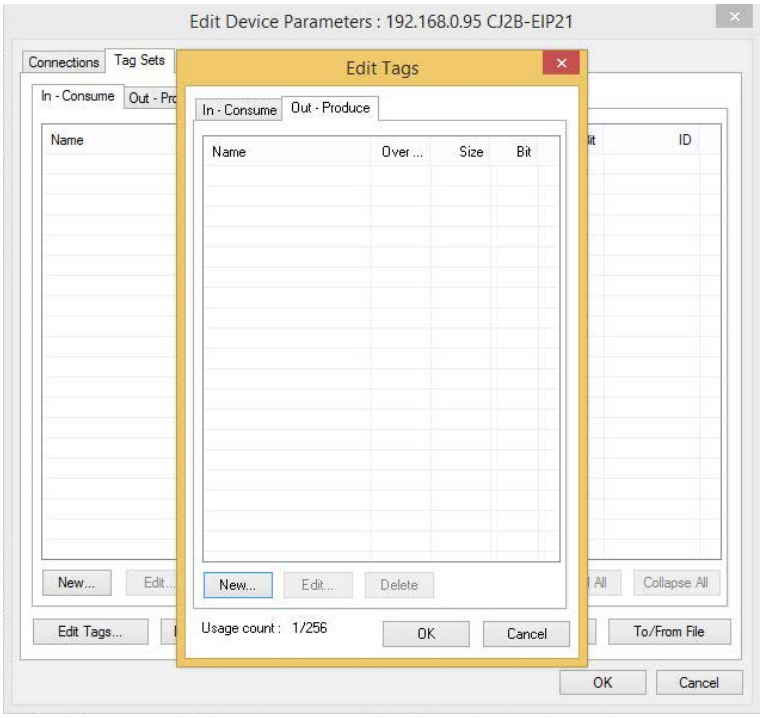
*Illustration 250. Fenêtre **Edit Tag***



h) Après avoir entré le nom dans le champ **Name** (souvenez-vous que cela fait référence à une zone de données processeur sur l'API) et la taille en octets dans le champ **Size**, cliquez sur **Regist** (Enregistrer), puis cliquez sur **Close** (Fermer).

i) Cliquez sur l'onglet **Out- Produce** (Sortie- Produire).

*Illustration 251. Onglet **Out- Produce***

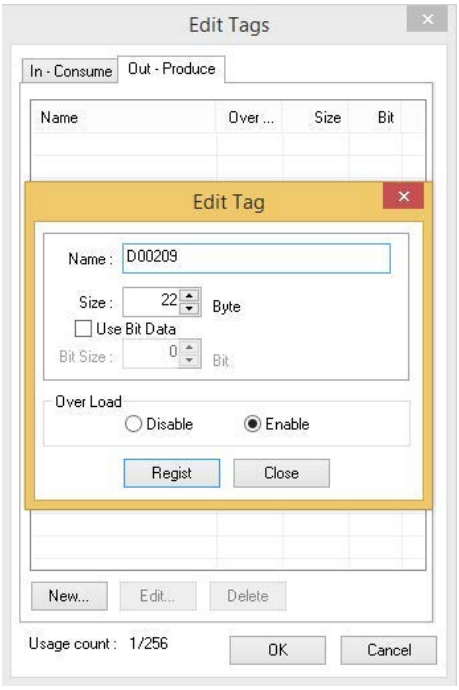


j) Cliquez sur **New** (Nouveau).

k) Sélectionnez une zone de données processeur de type et taille appropriés.
Les choix suivants sont possibles :

- 112 (0×70), taille 2 octets (pas de données dans ces registres)
- 113 (0×71), taille 22 octets (bits de reset/annulation de la temporisation virtuels)
- 114 (0×72), taille 28 octets (8 chaînes ISD)

*Illustration 252. Fenêtre **Edit Tag***



l) Après avoir entré le nom dans le champ **Name** (souvenez-vous que cela fait référence à une zone de données processeur sur l'API) et la taille en octets dans le champ **Size**, cliquez sur **Regist** (Enregistrer), puis cliquez sur **Close** (Fermer).

m) Dans la fenêtre **Edit Tags**, cliquez sur **OK**.
Le message qui s'affiche indique que les nouveaux tags seront enregistrés comme des ensembles de tags.

n) Cliquez sur **Oui**.

8. Revérifiez les tags en cliquant sur les onglets **In- Consume** et **Out- Produce**.

*Illustration 253. Onglet **In- Consume***

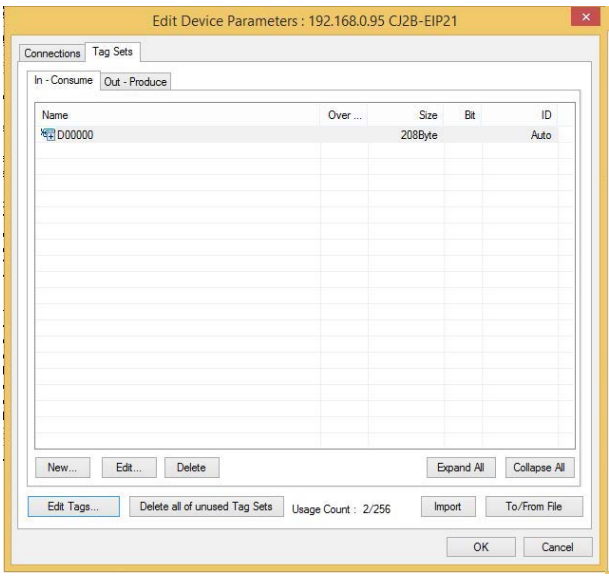
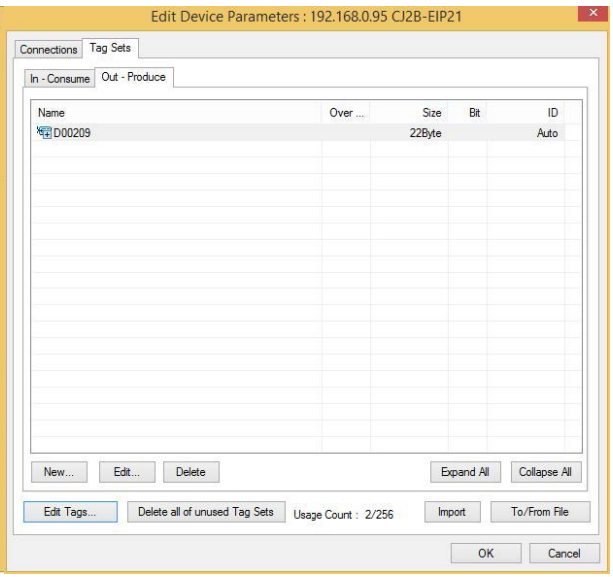
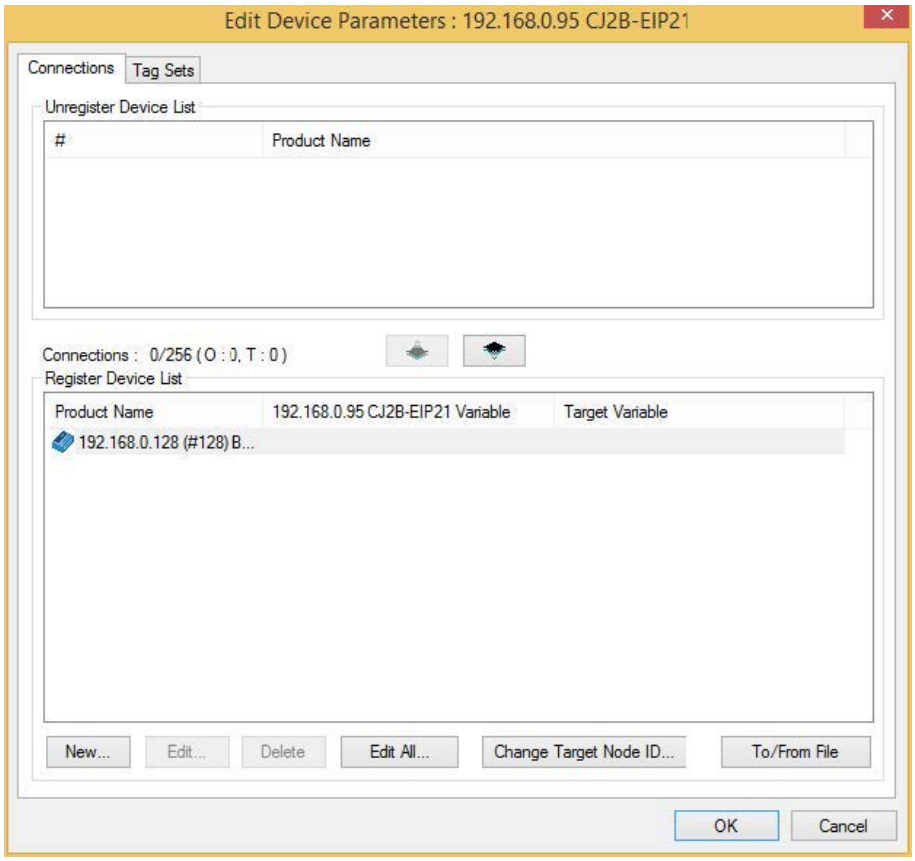


*Illustration 254. Onglet **Out- Produce***



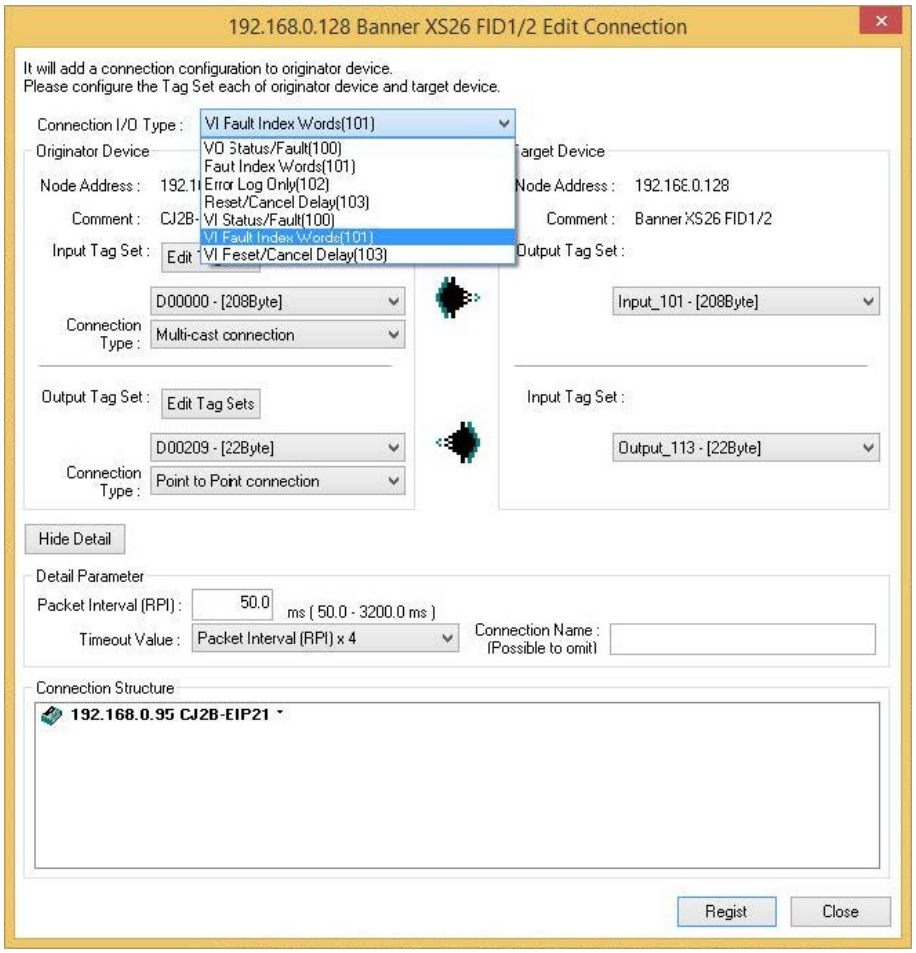
9. Revenez dans l'onglet **Connections** (pour voir la fenêtre ci-dessous).

*Illustration 255. Fenêtre **Edit Device Parameters** — Onglet **Connections***



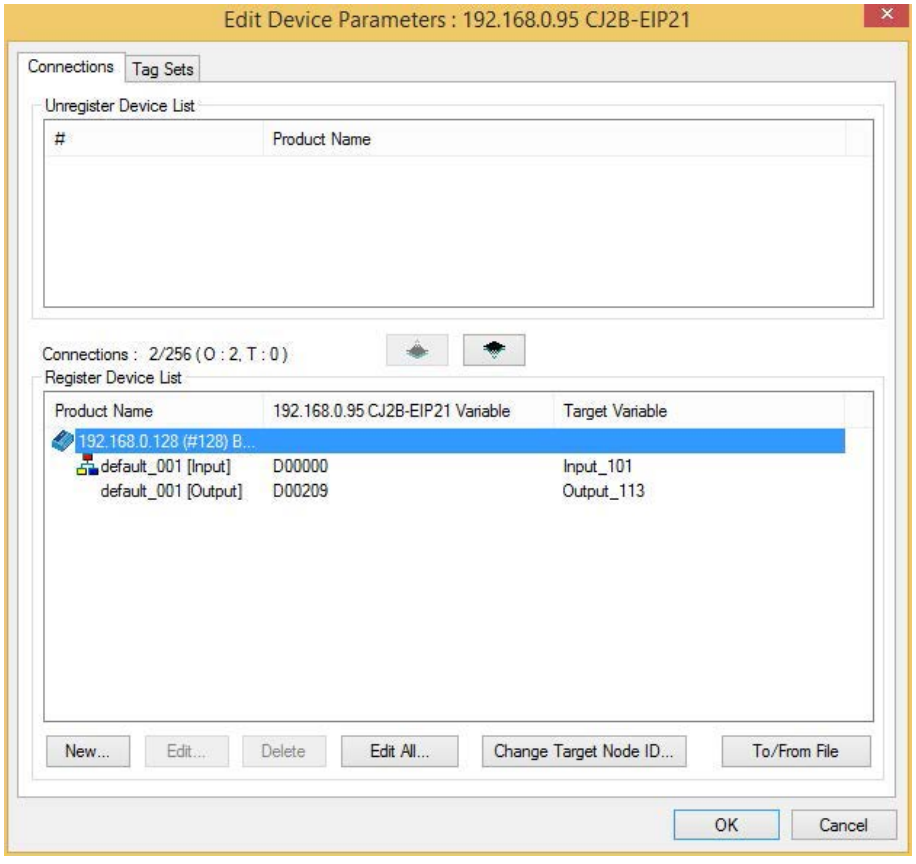
10. Double-cliquez sur le contrôleur de sécurité répertorié dans la liste **Register Device List**.
    La fenêtre **Edit Connection** (Modifier la connexion) s'affiche.
11. Sélectionnez les **connexions** et le **RPI** (intervalle de paquets) appropriés.

Illustration 256. Modification des connexions



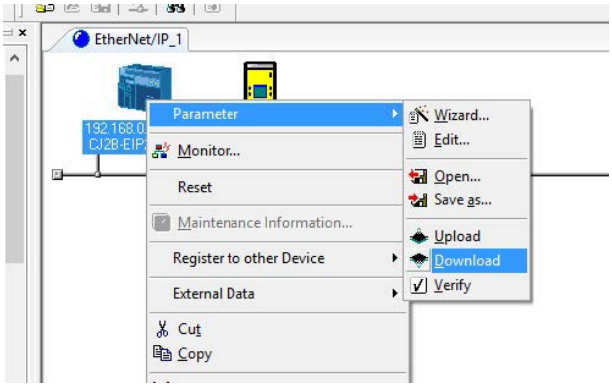
12. Cliquez sur **Regist**, puis sur **Close**.
13. Cliquez sur **OK** dans la fenêtre **Edit Parameters** (Modifier les paramètres).

*Illustration 257. Fenêtre **Edit Parameters***



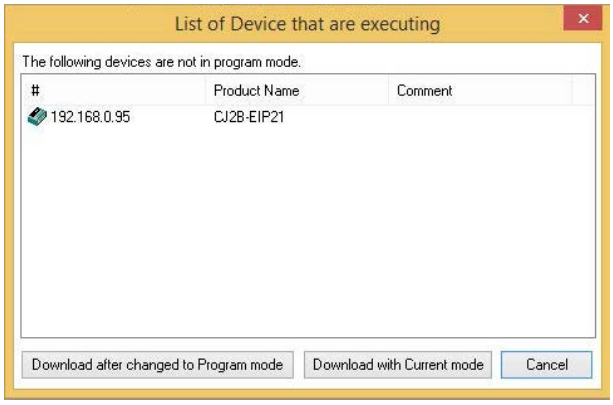
14. Basculez en mode en ligne et téléchargez la configuration vers l'API.

Illustration 258. Téléchargement de la configuration



15. Un message indiquant que le téléchargement des paramètres vers les dispositifs sélectionnés va commencer s'affiche. Cliquez sur **Yes** (Oui).
16. Sélectionnez une option de téléchargement.

Illustration 259. Options de téléchargement



17. Cliquez sur **Yes** (Oui) dans le message indiquant que le mode du contrôleur revient à l'état précédant le téléchargement, puis cliquez sur **OK** dans le message signalant la fin du téléchargement des paramètres du dispositif.
18. Cliquez avec le bouton droit sur l'icône de l'API et sélectionnez **Monitor** (Surveiller).

    Cette fenêtre indique si la connexion semble bonne. Des icônes bleues indiquent qu'une connexion fonctionne bien, sans erreur.

*Illustration 260. Fenêtre **Monitor Device** — Onglet **Status 1***

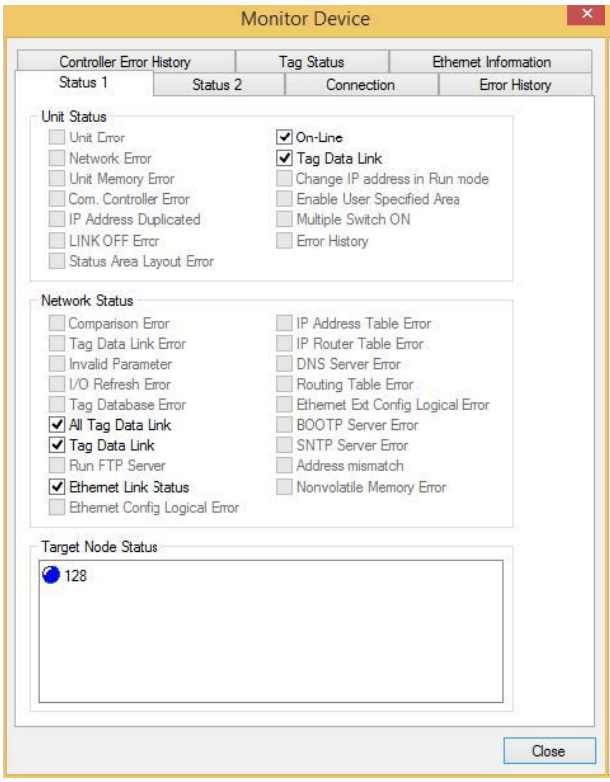
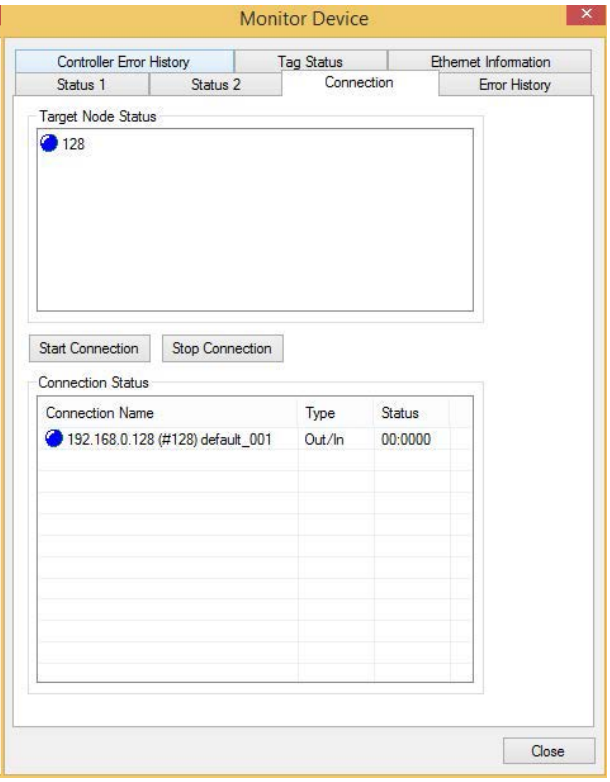
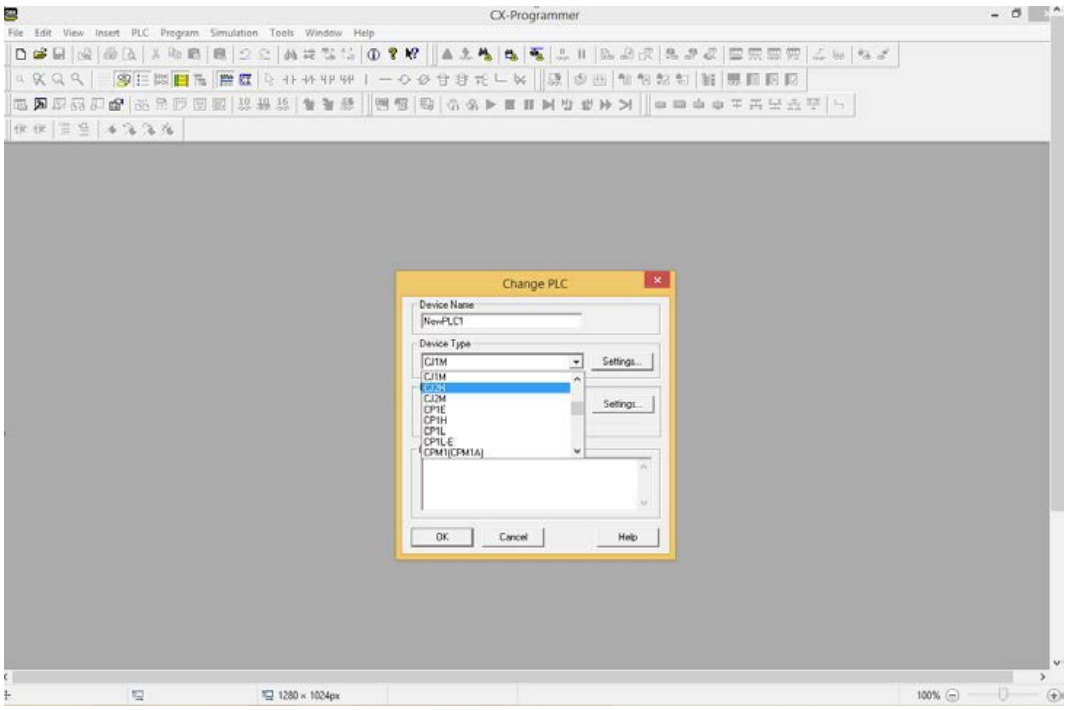


*Illustration 261. Fenêtre **Monitor Device** — Onglet **Connection***



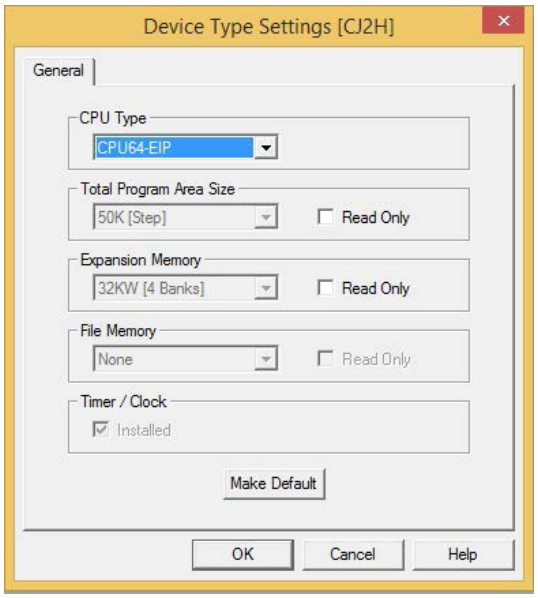
19. Ouvrez le logiciel CX Programmer.
20. Accédez à **File (Fichier)** > **New (Nouveau)**.
    La fenêtre **Change PLC** (Changer l'API) s'affiche.
21. Sélectionnez un modèle d'API, puis cliquez sur **Settings** (Paramètres).

*Illustration 262. Fenêtre **Change PLC***



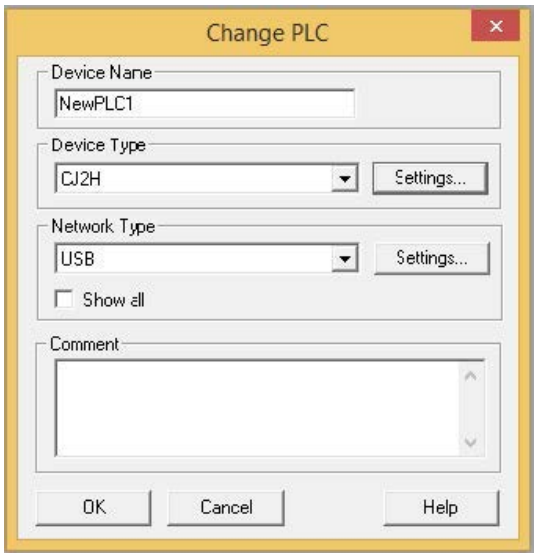
22. Sélectionnez un type de processeur dans **CPU Type** et cliquez sur **OK**.

*Illustration 263. Fenêtre **Device Type Settings***



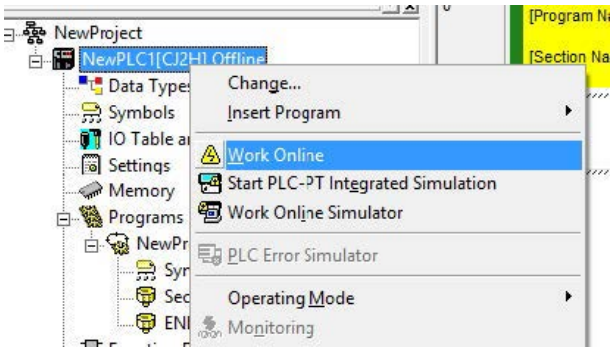
23. Sélectionnez un type de réseau dans **Network Type** et cliquez sur **OK**.

*Illustration 264. Fenêtre **Change PLC***



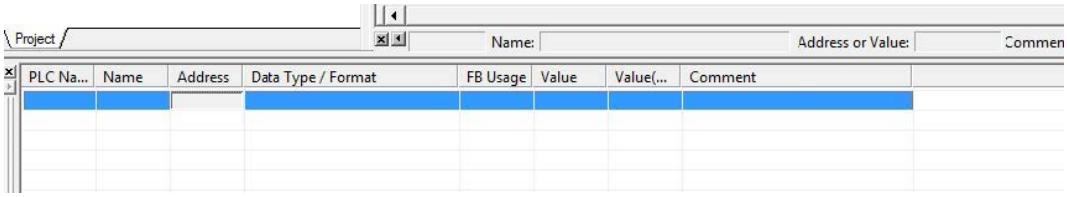
24. Basculez l'API en ligne en cliquant sur **Work Online** (Travailler en ligne).

Illustration 265. Option Work Online



25. Cliquez sur **Yes** pour vous connecter à l'API.
26. Accédez à **View (Afficher)** > **Windows (Fenêtres)** > **Watch (Surveiller)**.
27. Cliquez sur la ligne supérieure dans la fenêtre **Watch** (Surveiller).
    La fenêtre **Edit dialog** (Boîte de dialogue de modification) apparaît.

*Illustration 266. Fenêtre **Watch***

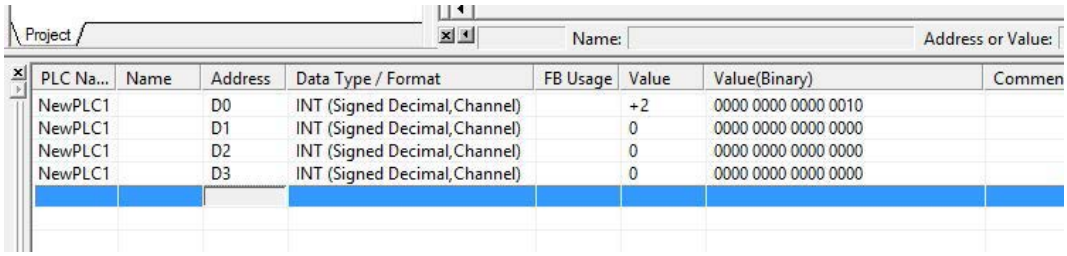


28. Ajoutez quelques registres à la fenêtre **Watch**.

*Illustration 267. **Fenêtre Edit Dialog***



*Illustration 268. Fenêtre **Watch** — 4 registres*



La fenêtre **Watch** de la figure précédente comprend 4 registres de données Sortie du contrôleur de sécurité (Entrée de l'API). Vous remarquerez que la sortie virtuelle 2 est actuellement active (registre D0, bit 1).

13.5 Modbus® TCP

Le protocole Modbus®[43] TCP fournit des informations sur les dispositifs à l'aide des banques de registres et de coils (sorties logiques) définies par le dispositif esclave.

Cette section définit les banques de registres et de coils. Par spécification, Modbus TCP utilise le port TCP 502. Le contrôleur de sécurité ne prend pas en charge un UID (Unit ID) 0 (parfois appelé ID d'esclave ou ID de dispositif).

Les registres suivants permettent d'envoyer des valeurs de sortie du contrôleur de sécurité à l'API. Ces registres peuvent être lus comme des registres d'entrée (30000) à l'aide du code de fonction 04 Modbus (Lire les registres d'entrée). Les mêmes valeurs peuvent être également lues comme des registres de maintien (40000) à l'aide du code de fonction 03 Modbus (Lire les registres de maintien). Les informations d'état de toutes les sorties virtuelles et leurs indicateurs de défaut, inclues dans les 8 premiers registres, peuvent être également lues comme des entrées (10000) à l'aide du code de fonction 02 Modbus (Lire l'état d'entrée).

Remarque: Les contrôleurs de sécurité XS/SC26 FID 2 et ultérieur diffèrent des modèles XS/SC26 FID 1 en cela que les versions FID 2 et ultérieures n'autorisent plus l'accès aux 64 premières sorties virtuelles à l'aide des coils Modbus TCP 0001–00064, ni aux 64 premiers bits de défauts de sortie virtuelle à l'aide des coils Modbus TCP 00065–00128.

[43] Modbus® est une marque déposée de Schneider Electric USA, Inc.

13.5.1 Bits d'entrée et de coil

64 premières sorties virtuelles et défauts de sortie virtuelle (entrées 10001–10128)

Table 29. 02 : Lire l'état d'entrée

N° entrée	NOM	N° entrée	NOM
10001	VO1	10065	Bit de défaut VO1
10002	VO2	10066	Bit de défaut VO2
10003	VO3	10067	Bit de défaut VO3
…	…	…	…
10063	VO63	10127	Bit de défaut VO63
10064	VO64	10128	Bit de défaut VO64

Ensemble des 256 sorties virtuelles et défauts de sortie virtuelle (entrées 11001-11256, 12001-12256)

Table 30. 02 : Lire l'état d'entrée

N° entrée	NOM	N° entrée	NOM
11001	VO1	12001	Bit de défaut VO1
11002	VO2	12002	Bit de défaut VO2
11003	VO3	12003	Bit de défaut VO3
…	…	…	…
11255	VO255	12255	Bit de défaut VO255
11256	VO256	12256	Bit de défaut VO256

Retour d'infos et commande Entrée virtuelle, Reset/Annulation de la temporisation virtuels (coils 3001–3128, 4001–4032, entrées 15001–15032)

Référez-vous à la section Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64.

Table 31. 05 : Écrire sur un seul coil ; 02 : Lire l'état d'entrée

N° entrée	NOM	N° entrée	NOM
3001	VI1 On/Off	15001	Feedback VRCD1
3002	VI2 On/Off	15002	Feedback VRCD2
…	…	…	…
3128	VI128 On/Off	15032	Feedback VRCD32
4001	VRCD1 On/Off		
4002	VRCD2 On/Off		
…			
4032	VRCD32 On/Off		

13.5.2 Registres d'entrée et de maintien

Registres de sortie du contrôleur de sécurité (Registres d'entrée ou de maintien Modbus TCP)

Table 32. Registres de sortie du contrôleur de sécurité (Registres d'entrée ou de maintien Modbus TCP)

N° REG. entrée	N° REG. maintien	NOM DU MOT (WORD)	TYPE DE DONNÉES
1	1	VO1 – VO16 (voir Indicateurs à la page 253)	Entier 16 bits
2	2	VO17 – VO32 (voir Indicateurs à la page 253)	Entier 16 bits
3	3	VO33 – VO48 (voir Indicateurs à la page 253)	Entier 16 bits
4	4	VO49 – VO64 (voir Indicateurs à la page 253)	Entier 16 bits
5	5	Bits de défaut pour VO1 – VO16 (voir Indicateurs à la page 253)	Entier 16 bits
6	6	Bits de défaut pour VO17 – VO32 (voir Indicateurs à la page 253)	Entier 16 bits
7	7	Bits de défaut pour VO33 – VO48 (voir Indicateurs à la page 253)	Entier 16 bits
8	8	Bits de défaut pour VO49 – VO64 (voir Indicateurs à la page 253)	Entier 16 bits
	9	Entrée virtuelle On/Off (1–16)	Entier 16 bits
	10	Entrée virtuelle On/Off (17–32)	Entier 16 bits
	11	Entrée virtuelle On/Off (33–48)	Entier 16 bits
	12	Entrée virtuelle On/Off (49–64)	Entier 16 bits
13–16	13–16	*réservés*	Entier 16 bits
	17	Reset/Annulation de la temporisation virtuels (1–16) [Bits de registre RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
18	18	réservés	Entier 16 bits
	19	Code d'activation RCD [Registre d'activation RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
20	20	Retour d'infos Reset/Annulation de la temporisation virtuels (1–16) [Bits de registre de retour RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
21	21	*réservés*	Entier 16 bits
22	22	Retour d'infos Code d'actionnement RCD [Registre de retour de l'activation RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
23–40	23–40	réservés	Entier 16 bits
41	41	Index de défaut VO1	Entier 16 bits
42	42	Index de défaut VO2	Entier 16 bits
43	43	Index de défaut VO3	Entier 16 bits
44	44	Index de défaut VO4	Entier 16 bits
45	45	Index de défaut VO5	Entier 16 bits
46	46	Index de défaut VO6	Entier 16 bits
47	47	Index de défaut VO7	Entier 16 bits

N° REG. entrée	N° REG. maintien	NOM DU MOT (WORD)	TYPE DE DONNÉES
48	48	Index de défaut VO8	Entier 16 bits
49	49	Index de défaut VO9	Entier 16 bits
50	50	Index de défaut VO10	Entier 16 bits
51	51	Index de défaut VO11	Entier 16 bits
52	52	Index de défaut VO12	Entier 16 bits
53	53	Index de défaut VO13	Entier 16 bits
54	54	Index de défaut VO14	Entier 16 bits
55	55	Index de défaut VO15	Entier 16 bits
56	56	Index de défaut VO16	Entier 16 bits
57	57	Index de défaut VO17	Entier 16 bits
58	58	Index de défaut VO18	Entier 16 bits
59	59	Index de défaut VO19	Entier 16 bits
60	60	Index de défaut VO20	Entier 16 bits
61	61	Index de défaut VO21	Entier 16 bits
62	62	Index de défaut VO22	Entier 16 bits
63	63	Index de défaut VO23	Entier 16 bits
64	64	Index de défaut VO24	Entier 16 bits
65	65	Index de défaut VO25	Entier 16 bits
66	66	Index de défaut VO26	Entier 16 bits
67	67	Index de défaut VO27	Entier 16 bits
68	68	Index de défaut VO28	Entier 16 bits
69	69	Index de défaut VO29	Entier 16 bits
70	70	Index de défaut VO30	Entier 16 bits
71	71	Index de défaut VO31	Entier 16 bits
72	72	Index de défaut VO32	Entier 16 bits
73	73	Index de défaut VO33	Entier 16 bits
74	74	Index de défaut VO34	Entier 16 bits
75	75	Index de défaut VO35	Entier 16 bits
76	76	Index de défaut VO36	Entier 16 bits
77	77	Index de défaut VO37	Entier 16 bits
78	78	Index de défaut VO38	Entier 16 bits
79	79	Index de défaut VO39	Entier 16 bits
80	80	Index de défaut VO40	Entier 16 bits
81	81	Index de défaut VO41	Entier 16 bits
82	82	Index de défaut VO42	Entier 16 bits
83	83	Index de défaut VO43	Entier 16 bits
84	84	Index de défaut VO44	Entier 16 bits
85	85	Index de défaut VO45	Entier 16 bits
86	86	Index de défaut VO46	Entier 16 bits
87	87	Index de défaut VO47	Entier 16 bits
88	88	Index de défaut VO48	Entier 16 bits
89	89	Index de défaut VO49	Entier 16 bits

N° REG. entrée	N° REG. maintien	NOM DU MOT (WORD)	TYPE DE DONNÉES
90	90	Index de défaut VO50	Entier 16 bits
91	91	Index de défaut VO51	Entier 16 bits
92	92	Index de défaut VO52	Entier 16 bits
93	93	Index de défaut VO53	Entier 16 bits
94	94	Index de défaut VO54	Entier 16 bits
95	95	Index de défaut VO55	Entier 16 bits
96	96	Index de défaut VO56	Entier 16 bits
97	97	Index de défaut VO57	Entier 16 bits
98	98	Index de défaut VO58	Entier 16 bits
99	99	Index de défaut VO59	Entier 16 bits
100	100	Index de défaut VO60	Entier 16 bits
101	101	Index de défaut VO61	Entier 16 bits
102	102	Index de défaut VO62	Entier 16 bits
103	103	Index de défaut VO63	Entier 16 bits
104	104	Index de défaut VO64	Entier 16 bits
105–106	105–106	Code de défaut complet VO1	Entier 32 bits
107–108	107–108	Code de défaut complet VO2	Entier 32 bits
109–110	109–110	Code de défaut complet VO3	Entier 32 bits
111–112	111–112	Code de défaut complet VO4	Entier 32 bits
113–114	113–114	Code de défaut complet VO5	Entier 32 bits
115–116	115–116	Code de défaut complet VO6	Entier 32 bits
117–118	117–118	Code de défaut complet VO7	Entier 32 bits
119–120	119–120	Code de défaut complet VO8	Entier 32 bits
121–122	121–122	Code de défaut complet VO9	Entier 32 bits
123–124	123–124	Code de défaut complet VO10	Entier 32 bits
125–126	125–126	Code de défaut complet VO11	Entier 32 bits
127–128	127–128	Code de défaut complet VO12	Entier 32 bits
129–130	129–130	Code de défaut complet VO13	Entier 32 bits
131–132	131–132	Code de défaut complet VO14	Entier 32 bits
133–134	133–134	Code de défaut complet VO15	Entier 32 bits
135–136	135–136	Code de défaut complet VO16	Entier 32 bits
137–138	137–138	Code de défaut complet VO17	Entier 32 bits
139–140	139–140	Code de défaut complet VO18	Entier 32 bits
141–142	141–142	Code de défaut complet VO19	Entier 32 bits
143–144	143–144	Code de défaut complet VO20	Entier 32 bits
145–146	145–146	Code de défaut complet VO21	Entier 32 bits
147–148	147–148	Code de défaut complet VO22	Entier 32 bits
149–150	149–150	Code de défaut complet VO23	Entier 32 bits
151–152	151–152	Code de défaut complet VO24	Entier 32 bits
153–154	153–154	Code de défaut complet VO25	Entier 32 bits
155–156	155–156	Code de défaut complet VO26	Entier 32 bits
157–158	157–158	Code de défaut complet VO27	Entier 32 bits

N° REG. entrée	N° REG. maintien	NOM DU MOT (WORD)	TYPE DE DONNÉES
159–160	159–160	Code de défaut complet VO28	Entier 32 bits
161–162	161–162	Code de défaut complet VO29	Entier 32 bits
163–164	163–164	Code de défaut complet VO30	Entier 32 bits
165–166	165–166	Code de défaut complet VO31	Entier 32 bits
167–168	167–168	Code de défaut complet VO32	Entier 32 bits
169–170	169–170	Code de défaut complet VO33	Entier 32 bits
171–172	171–172	Code de défaut complet VO34	Entier 32 bits
173–174	173–174	Code de défaut complet VO35	Entier 32 bits
175–176	175–176	Code de défaut complet VO36	Entier 32 bits
177–178	177–178	Code de défaut complet VO37	Entier 32 bits
179–180	179–180	Code de défaut complet VO38	Entier 32 bits
181–182	181–182	Code de défaut complet VO39	Entier 32 bits
183–184	183–184	Code de défaut complet VO40	Entier 32 bits
185–186	185–186	Code de défaut complet VO41	Entier 32 bits
187–188	187–188	Code de défaut complet VO42	Entier 32 bits
189–190	189–190	Code de défaut complet VO43	Entier 32 bits
191–192	191–192	Code de défaut complet VO44	Entier 32 bits
193–194	193–194	Code de défaut complet VO45	Entier 32 bits
195–196	195–196	Code de défaut complet VO46	Entier 32 bits
197–198	197–198	Code de défaut complet VO47	Entier 32 bits
199–200	199–200	Code de défaut complet VO48	Entier 32 bits
201–202	201–202	Code de défaut complet VO49	Entier 32 bits
203–204	203–204	Code de défaut complet VO50	Entier 32 bits
205–206	205–206	Code de défaut complet VO51	Entier 32 bits
207–208	207–208	Code de défaut complet VO52	Entier 32 bits
209–210	209–210	Code de défaut complet VO53	Entier 32 bits
211–212	211–212	Code de défaut complet VO54	Entier 32 bits
213–214	213–214	Code de défaut complet VO55	Entier 32 bits
215–216	215–216	Code de défaut complet VO56	Entier 32 bits
217–218	217–218	Code de défaut complet VO57	Entier 32 bits
219–220	219–220	Code de défaut complet VO58	Entier 32 bits
221–222	221–222	Code de défaut complet VO59	Entier 32 bits
223–224	223–224	Code de défaut complet VO60	Entier 32 bits
225–226	225–226	Code de défaut complet VO61	Entier 32 bits
227–228	227–228	Code de défaut complet VO62	Entier 32 bits
229–230	229–230	Code de défaut complet VO63	Entier 32 bits
231–232	231–232	Code de défaut complet VO64	Entier 32 bits
233–234	233–234	Horodatage Défaut 1	Entier 32 bits
235–242	235–242	Nom de l'E/S ou du système Défaut 1	Longueur de 2 mots (word) + 12 caractères ASCII
243	243	Code d'erreur Défaut 1	Entier 16 bits
244	244	Code d'erreur avancé Défaut 1	Entier 16 bits
245	245	Index de message d'erreur Défaut 1	Entier 16 bits

N° REG. entrée	N° REG. maintien	NOM DU MOT (WORD)	TYPE DE DONNÉES
246–247	246–247	*réservés*	Entier 16 bits
248–249	248–249	Horodatage Défaut 2	Entier 32 bits
250–257	250–257	Nom de l'E/S ou du système Défaut 2	Longueur de 2 mots (word) + 12 caractères ASCII
258	258	Code d'erreur Défaut 2	Entier 16 bits
259	259	Code d'erreur avancé Défaut 2	Entier 16 bits
260	260	Index de message d'erreur Défaut 2	Entier 16 bits
261–262	261–262	*réservés*	Entier 16 bits
263–264	263–264	Horodatage Défaut 3	Entier 32 bits
265–272	265–272	Nom de l'E/S ou du système Défaut 3	Longueur de 2 mots (word) + 12 caractères ASCII
273	273	Code d'erreur Défaut 3	Entier 16 bits
274	274	Code d'erreur avancé Défaut 3	Entier 16 bits
275	275	Index de message d'erreur Défaut 3	Entier 16 bits
276–277	276–277	*réservés*	Entier 16 bits
278–279	278–279	Horodatage Défaut 4	Entier 32 bits
280–287	280–287	Nom de l'E/S ou du système Défaut 4	Longueur de 2 mots (word) + 12 caractères ASCII
288	288	Code d'erreur Défaut 4	Entier 16 bits
289	289	Code d'erreur avancé Défaut 4	Entier 16 bits
290	290	Index de message d'erreur Défaut 4	Entier 16 bits
291–292	291–292	*réservés*	Entier 16 bits
293–294	293–294	Horodatage Défaut 5	Entier 32 bits
295–302	295–302	Nom de l'E/S ou du système Défaut 5	Longueur de 2 mots (word) + 12 caractères ASCII
303	303	Code d'erreur Défaut 5	Entier 16 bits
304	304	Code d'erreur avancé Défaut 5	Entier 16 bits
305	305	Index de message d'erreur Défaut 5	Entier 16 bits
306–307	306–307	*réservés*	Entier 16 bits
308–309	308–309	Horodatage Défaut 6	Entier 32 bits
310–317	310–317	Nom de l'E/S ou du système Défaut 6	Longueur de 2 mots (word) + 12 caractères ASCII
318	318	Code d'erreur Défaut 6	Entier 16 bits
319	319	Code d'erreur avancé Défaut 6	Entier 16 bits
320	320	Index de message d'erreur Défaut 6	Entier 16 bits
321–322	321–322	*réservés*	Entier 16 bits
323–324	323–324	Horodatage Défaut 7	Entier 32 bits
325–332	325–332	Nom de l'E/S ou du système Défaut 7	Longueur de 2 mots (word) + 12 caractères ASCII
333	333	Code d'erreur Défaut 7	Entier 16 bits
334	334	Code d'erreur avancé Défaut 7	Entier 16 bits
335	335	Index de message d'erreur Défaut 7	Entier 16 bits
336–337	336–337	*réservés*	Entier 16 bits
338–339	338–339	Horodatage Défaut 8	Entier 32 bits

N° REG. entrée	N° REG. maintien	NOM DU MOT (WORD)	TYPE DE DONNÉES
340–347	340–347	Nom de l'E/S ou du système Défaut 8	Longueur de 2 mots (word) + 12 caractères ASCII
348	348	Code d'erreur Défaut 8	Entier 16 bits
349	349	Code d'erreur avancé Défaut 8	Entier 16 bits
350	350	Index de message d'erreur Défaut 8	Entier 16 bits
351–352	351–352	*réservés*	Entier 16 bits
353–354	353–354	Horodatage Défaut 9	Entier 32 bits
355–362	355–362	Nom de l'E/S ou du système Défaut 9	Longueur de 2 mots (word) + 12 caractères ASCII
363	363	Code d'erreur Défaut 9	Entier 16 bits
364	364	Code d'erreur avancé Défaut 9	Entier 16 bits
365	365	Index de message d'erreur Défaut 9	Entier 16 bits
366–367	366–367	*réservés*	Entier 16 bits
368–369	368–369	Horodatage Défaut 10	Entier 32 bits
370–377	370–377	Nom de l'E/S ou du système Défaut 10	Longueur de 2 mots (word) + 12 caractères ASCII
378	378	Code d'erreur Défaut 10	Entier 16 bits
379	379	Code d'erreur avancé Défaut 10	Entier 16 bits
380	380	Index de message d'erreur Défaut 10	Entier 16 bits
381–382	381–382	*réservés*	Entier 16 bits
383–384	383–384	Secondes depuis le démarrage	Entier 32 bits
385	385	Mode de fonctionnement	Entier 16 bits
386–395	386–395	Nom de la configuration	Longueur de 2 mots (word) + 16 caractères ASCII
396–397	396–397	CRC de configuration	Entier 32 bits
398–900	398–900	*réservés*	Entier 16 bits
901	901	VO1 – VO16 (voir Indicateurs à la page 253)	Entier 16 bits
902	902	VO17 – VO32 (voir Indicateurs à la page 253)	Entier 16 bits
903	903	VO33 – VO48 (voir Indicateurs à la page 253)	Entier 16 bits
904	904	VO49 – VO64 (voir Indicateurs à la page 253)	Entier 16 bits
905	905	VO65 – VO80 (voir Indicateurs étendus à la page 254)	Entier 16 bits
906	906	VO81 – VO96 (voir Indicateurs étendus à la page 254)	Entier 16 bits
907	907	VO97 – VO112 (voir Indicateurs étendus à la page 254)	Entier 16 bits
908	908	VO113 – VO128 (voir Indicateurs étendus à la page 254)	Entier 16 bits
909	909	VO129 – VO144 (voir Indicateurs étendus à la page 254)	Entier 16 bits
910	910	VO145 – VO160 (voir Indicateurs étendus à la page 254)	Entier 16 bits
911	911	VO161 – VO176 (voir Indicateurs étendus à la page 254)	Entier 16 bits
912	912	VO177 – VO192 (voir Indicateurs étendus à la page 254)	Entier 16 bits

N° REG. entrée	N° REG. maintien	NOM DU MOT (WORD)	TYPE DE DONNÉES
913	913	VO193 – VO208 (voir Indicateurs étendus à la page 254)	Entier 16 bits
914	914	VO209 – VO224 (voir Indicateurs étendus à la page 254)	Entier 16 bits
915	915	VO225 – VO240 (voir Indicateurs étendus à la page 254)	Entier 16 bits
916	916	VO241 – VO256 (voir Indicateurs étendus à la page 254)	Entier 16 bits
917	917	Bits de défaut pour VO1 – VO16 (voir Indicateurs à la page 253)	Entier 16 bits
918	918	Bits de défaut pour VO17 – VO32 (voir Indicateurs à la page 253)	Entier 16 bits
919	919	Bits de défaut pour VO33 – VO48 (voir Indicateurs à la page 253)	Entier 16 bits
920	920	Bits de défaut pour VO49 – VO64 (voir Indicateurs à la page 253)	Entier 16 bits
921	921	Bits de défaut pour VO65 – VO80 (voir Indicateurs étendus à la page 254)	Entier 16 bits
922	922	Bits de défaut pour VO81 – VO96 (voir Indicateurs étendus à la page 254)	Entier 16 bits
923	923	Bits de défaut pour VO97 – VO112 (voir Indicateurs étendus à la page 254)	Entier 16 bits
924	924	Bits de défaut pour VO113 – VO128 (voir Indicateurs étendus à la page 254)	Entier 16 bits
925	925	Bits de défaut pour VO129 – VO144 (voir Indicateurs étendus à la page 254)	Entier 16 bits
926	926	Bits de défaut pour VO145 – VO160 (voir Indicateurs étendus à la page 254)	Entier 16 bits
926	926	Bits de défaut pour VO161 – VO176 (voir Indicateurs étendus à la page 254)	Entier 16 bits
928	928	Bits de défaut pour VO177 – VO192 (voir Indicateurs étendus à la page 254)	Entier 16 bits
929	929	Bits de défaut pour VO193 – VO208 (voir Indicateurs étendus à la page 254)	Entier 16 bits
930	930	Bits de défaut pour VO209 – VO224 (voir Indicateurs étendus à la page 254)	Entier 16 bits
931	931	Bits de défaut pour VO225 – VO240 (voir Indicateurs étendus à la page 254)	Entier 16 bits
932	932	Bits de défaut pour VO241 – VO256 (voir Indicateurs étendus à la page 254)	Entier 16 bits
933–934	933–934	Retour d'infos sur les bits RCD (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 32 bits
935	935	Retour d'infos sur l'activation RCD (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
936	936	Index de défaut VO1	Entier 16 bits
937	937	Index de défaut VO2	Entier 16 bits
938	938	Index de défaut VO3	Entier 16 bits
…	...	…	…
1190	1190	Index de défaut VO256	Entier 16 bits
1191–1192	1191–1192	Code de défaut complet VO1	Entier 32 bits

N° REG. entrée	N° REG. maintien	NOM DU MOT (WORD)	TYPE DE DONNÉES
1193–1194	1193–1194	Code de défaut complet VO2	Entier 32 bits
1195–1196	1195–1196	Code de défaut complet VO3	Entier 32 bits
1197–1198	1197–1198	Code de défaut complet VO4	Entier 32 bits
…	…	…	…
1702–1703	1702–1703	Code de défaut complet VO256	Entier 32 bits
1704–1705	1704–1705	État système ISD - Nbre de dispositifs Chaîne 1	Entier 32 bits
1706–1707	1706–1707	État système ISD - Nbre de dispositifs Chaîne 2	Entier 32 bits
1708–1709	1708–1709	État système ISD - État On/Off des dispositifs Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1710–1711	1710–1711	État système ISD - État On/Off des dispositifs Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1712–1713	1712–1713	État système ISD - État de défaut Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1714–1715	1714–1715	État système ISD - État de défaut Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1716–1717	1716–1717	État système ISD - État marginal Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1718–1719	1718–1719	État système ISD - État marginal Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1720–1721	1720–1721	État système ISD - État d'alerte Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1722–1723	1722–1723	État système ISD - État d'alerte Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1724–1725	1724–1725	État système ISD - État de reset Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1726–1727	1726–1727	État système ISD - État de reset Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1728–1729	1728–1729	État système ISD - Actionneur Chaîne 1 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1730–1731	1730–1731	État système ISD - Actionneur Chaîne 2 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1732–1733	1732–1733	État système ISD - État système Chaîne 1 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
1734–1735	1734–1735	État système ISD - État système Chaîne 2 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
1736–1751	1736–1751	Liste des dispositifs ISD détectés sur une chaîne	Tableau de 32 octets
1752–1768	1752–1768	*réservés*	Entier 16 bits
1769	1769	Accusé réc. demande de lecture ISD (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
1770	1770	Accusé réc. chaîne ISD demandée (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
1771	1771	Accusé réc. dispositif ISD demandé (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits

N° REG. entrée	N° REG. maintien	NOM DU MOT (WORD)	TYPE DE DONNÉES
1772–1780	1772–1780	Données spécifiques à un dispositif ISD individuel [46] (Référez-vous à la section Description détaillée des données spécifiques à un dispositif ISD individuel à la page 255)	Entier 16 bits
	1781	Demande de lecture ISD (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
	1782	Chaîne ISD demandée (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
	1783	Dispositif ISD demandé (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
1784–1785	1784–1785	État système ISD – Nbre de dispositifs Chaîne 1	Entier 32 bits
1786–1787	1786–1787	État système ISD – État On/Off des dispositifs Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1788–1789	1788–1789	État système ISD – État de défaut Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1790–1791	1790–1791	État système ISD – État marginal Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1792–1793	1792–1793	État système ISD – État d'alerte Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1794–1795	1794–1795	État système ISD – État de reset Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1796–1797	1796–1797	État système ISD – État Actionneur Chaîne 1 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1798–1799	1798–1799	État système ISD – État système Chaîne 1 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
1800–1801	1800–1801	État système ISD – Nbre de dispositifs Chaîne 2	Entier 32 bits
1802–1803	1802–1803	État système ISD – État On/Off des dispositifs Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1804–1805	1804–1805	État système ISD – État de défaut Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1806–1807	1806–1807	État système ISD – État marginal Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1808–1809	1808–1809	État système ISD – État d'alerte Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1810–1811	1810–1811	État système ISD – État de reset Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1812–1813	1812–1813	État système ISD – État Actionneur Chaîne 2 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1814–1815	1814–1815	État système ISD – État système Chaîne 2 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
1816–1817	1816–1817	État système ISD – Nbre de dispositifs Chaîne 3	Entier 32 bits
1818–1819	1818–1819	État système ISD – État On/Off des dispositifs Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits

[46] Pour la conversion de la température interne, de la distance de l'actionneur et de la tension, voir la section ISD : Informations sur la conversion de la distance, tension et température à la page 309.

N° REG. entrée	N° REG. maintien	NOM DU MOT (WORD)	TYPE DE DONNÉES
1820–1821	1820–1821	État système ISD – État de défaut Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1822–1823	1822–1823	État système ISD – État marginal Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1824–1825	1824–1825	État système ISD – État d'alerte Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1826–1827	1826–1827	État système ISD – État de reset Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1828–1829	1828–1829	État système ISD – État Actionneur Chaîne 3 re-connu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1830–1831	1830–1831	État système ISD – État système Chaîne 3 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
1832–1833	1832–1833	État système ISD – Nbre de dispositifs Chaîne 4	Entier 32 bits
1834–1835	1834–1835	État système ISD – État On/Off des dispositifs Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1836–1837	1836–1837	État système ISD – État de défaut Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1838–1839	1838–1839	État système ISD – État marginal Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1840–1841	1840–1841	État système ISD – État d'alerte Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1842–1843	1842–1843	État système ISD – État de reset Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1844–1845	1844–1845	État système ISD – État Actionneur Chaîne 4 re-connu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1846–1847	1846–1847	État système ISD – État système Chaîne 4 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
1848–1849	1848–1849	État système ISD – Nbre de dispositifs Chaîne 5	Entier 32 bits
1850–1851	1850–1851	État système ISD – État On/Off des dispositifs Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1852–1853	1852–1853	État système ISD – État de défaut Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1854–1855	1854–1855	État système ISD – État marginal Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1856–1857	1856–1857	État système ISD – État d'alerte Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1858–1859	1858–1859	État système ISD – État de reset Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1860–1861	1860–1861	État système ISD – État Actionneur Chaîne 5 re-connu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1862–1863	1862–1863	État système ISD – État système Chaîne 5 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
1864–1865	1864–1865	État système ISD – Nbre de dispositifs Chaîne 6	Entier 32 bits
1866–1867	1866–1867	État système ISD – État On/Off des dispositifs Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1868–1869	1868–1869	État système ISD – État de défaut Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits

N° REG. entrée	N° REG. maintien	NOM DU MOT (WORD)	TYPE DE DONNÉES
1870–1871	1870–1871	État système ISD – État marginal Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1872–1873	1872–1873	État système ISD – État d'alerte Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1874–1875	1874–1875	État système ISD – État de reset Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1876–1877	1876–1877	État système ISD – État Actionneur Chaîne 6 re-connu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1878–1879	1878–1879	État système ISD – État système Chaîne 6 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
1880–1881	1880–1881	État système ISD – Nbre de dispositifs Chaîne 7	Entier 32 bits
1882–1883	1882–1883	État système ISD – État On/Off des dispositifs Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1884–1885	1884–1885	État système ISD – État de défaut Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1886–1887	1886–1887	État système ISD – État marginal Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1888–1889	1888–1889	État système ISD – État d'alerte Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1890–1891	1890–1891	État système ISD – État de reset Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1892–1893	1892–1893	État système ISD – État Actionneur Chaîne 7 re-connu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1894–1895	1894–1895	État système ISD – État système Chaîne 7 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
1896–1897	1896–1897	État système ISD – Nbre de dispositifs Chaîne 8	Entier 32 bits
1898–1899	1898–1899	État système ISD – État On/Off des dispositifs Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1900–1901	1900–1901	État système ISD – État de défaut Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1902–1903	1902–1903	État système ISD – État marginal Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1904–1905	1904–1905	État système ISD – État d'alerte Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1906–1907	1906–1907	État système ISD – État de reset Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1908–1909	1908–1909	État système ISD – État Actionneur Chaîne 8 re-connu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
1910–1911	1910–1911	État système ISD – État système Chaîne 8 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits

Remarque: Les données ISD ne sont pas immédiatement disponibles à la mise sous tension. Les données ISD peuvent être retardées jusqu'à 10 secondes après la mise sous tension du système.

Indicateurs

Les registres 1 à 8, définis ci-dessous, apparaissent comme les huit premiers mots (word) dans la carte de registres.

Ils représentent les 64 premières sorties virtuelles et les indicateurs de défaut qui leur sont associés. Les informations de ces registres peuvent être lues comme des registres d'entrée (30000) à l'aide du code de fonction 04 Modbus (Lire les registres d'entrée). Les mêmes valeurs peuvent être également lues comme des registres de maintien (40000) à l'aide du code de fonction 03 Modbus (Lire les registres de maintien).

Table 33. Sorties virtuelles 1–16

Registre d'entrée 30001 ou registre de maintien 40001 de l'API, également entrées 10001-16 ou sorties logiques (coils) 00001-16

bit 15	bit 14	bit 13	bit 12	bit 11	bit 10	bit 9	bit 8	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
VO16	VO15	VO14	VO13	VO12	VO11	VO10	VO9	VO8	VO7	VO6	VO5	VO4	VO3	VO2	VO1

Table 34. Sorties virtuelles 17–32

Registre d'entrée 30002 ou registre de maintien 40002 de l'API, également entrées 10017-32 ou sorties logiques (coils) 00017-32

bit 15	bit 14	bit 13	bit 12	bit 11	bit 10	bit 9	bit 8	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
VO32	VO31	VO30	VO29	VO28	VO27	VO26	VO25	VO24	VO23	VO22	VO21	VO20	VO19	VO18	VO17

Table 35. Sorties virtuelles 33–48

Registre d'entrée 30003 ou registre de maintien 40003 de l'API, également entrées 10033-48 ou sorties logiques (coils) 00033-48

bit 15	bit 14	bit 13	bit 12	bit 11	bit 10	bit 9	bit 8	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
VO48	VO47	VO46	VO45	VO44	VO43	VO42	VO41	VO40	VO39	VO38	VO37	VO36	VO35	VO34	VO33

Table 36. Sorties virtuelles 49–64

Registre d'entrée 30004 ou registre de maintien 40004 de l'API, également entrées 10049-64 ou sorties logiques (coils) 00049-64

bit 15	bit 14	bit 13	bit 12	bit 11	bit 10	bit 9	bit 8	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
VO64	VO63	VO62	VO61	VO60	VO59	VO58	VO57	VO56	VO55	VO54	VO53	VO52	VO51	VO50	VO49

Table 37. Défaut de sorties virtuelles 1-16

Registre d'entrée 30005 ou registre de maintien 40005 de l'API, également entrées 10033-48 ou sorties logiques (coils) 00033-48

bit 15	bit 14	bit 13	bit 12	bit 11	bit 10	bit 9	bit 8	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
Défaut VO16	Défaut VO15	Défaut VO14	Défaut VO13	Défaut VO12	Défaut VO11	Défaut VO10	Défaut VO9	Défaut VO8	Défaut VO7	Défaut VO6	Défaut VO5	Défaut VO4	Défaut VO3	Défaut VO2	Défaut VO1

Table 38. Défaut de sorties virtuelles 17–32

Registre d'entrée 30006 ou registre de maintien 40006 de l'API, également entrées 10049-64 ou sorties logiques (coils) 00049-64

bit 15	bit 14	bit 13	bit 12	bit 11	bit 10	bit 9	bit 8	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
Défaut VO32	Défaut VO31	Défaut VO30	Défaut VO29	Défaut VO28	Défaut VO27	Défaut VO26	Défaut VO25	Défaut VO24	Défaut VO23	Défaut VO22	Défaut VO21	Défaut VO20	Défaut VO19	Défaut VO18	Défaut VO17

Table 39. Défaut de sorties virtuelles 33–48

Registre d'entrée 30007 ou registre de maintien 40007 de l'API, également entrées 10033-48 ou sorties logiques (coils) 00033-48

bit 15	bit 14	bit 13	bit 12	bit 11	bit 10	bit 9	bit 8	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
Défaut VO48	Défaut VO47	Défaut VO46	Défaut VO45	Défaut VO44	Défaut VO43	Défaut VO42	Défaut VO41	Défaut VO40	Défaut VO39	Défaut VO38	Défaut VO37	Défaut VO36	Défaut VO35	Défaut VO34	Défaut VO33

Table 40. Défaut de sorties virtuelles 49-64

Registre d'entrée 30008 ou registre de maintien 40008 de l'API, également entrées 10049-64 ou sorties logiques (coils) 00049-64

bit 15	bit 14	bit 13	bit 12	bit 11	bit 10	bit 9	bit 8	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
Défaut VO64	Défaut VO63	Défaut VO62	Défaut VO61	Défaut VO60	Défaut VO59	Défaut VO58	Défaut VO57	Défaut VO56	Défaut VO55	Défaut VO54	Défaut VO53	Défaut VO52	Défaut VO51	Défaut VO50	Défaut VO49

Indicateurs étendus

Il est possible d'accéder aux 256 sorties virtuelles d'une manière similaire à celle décrite dans la section Indicateurs à la page 253.

Les entrées 11001 à 11256 représentent les 256 sorties virtuelles possibles. Ces sorties virtuelles peuvent être également lues comme des registres d'entrée 901-916 ou des registres de maintien 901-916.

Les entrées 12001 à 12256 représentent les 256 défauts des sorties virtuelles. Ces défauts des sorties virtuelles peuvent être également lus comme des registres d'entrée 917-932 ou des registres de maintien 917-932.

Description détaillée des données spécifiques à un dispositif ISD individuel

Le tableau suivant décrit les registres de maintien ou d'entrée des données 1772–1780.

Table 41. Description détaillée des données spécifiques à un dispositif ISD individuel

N° REG. entrée	N° REG. maintien	Informations	Taille des données
1772.0	1772.0	Défaut d'entrée de sécurité	1 bit
1772.1	1772.1	*réservés*	1 bit
1772.2	1772.2	Capteur non couplé	1 bit
1772.3	1772.3	Erreur de données ISD	1 bit
1772.4	1772.4	Mauvais actionneur/État du bouton/État de l'entrée	1 bit
1772.5	1772.5	Portée marginale/État du bouton/État de l'entrée	1 bit
1772.6	1772.6	Actionneur détecté	1 bit
1772.7	1772.7	Erreur de sortie	1 bit
1772.8	1772.8	Entrée 2	1 bit
1772.9	1772.9	Entrée 1	1 bit
1772.10	1772.10	Reset local attendu	1 bit
1772.11	1772.11	Avertissement de tension de fonctionnement	1 bit
1772.12	1772.12	Erreur de tension de fonctionnement	1 bit
1772.13	1772.13	Sortie 2	1 bit
1772.14	1772.14	Sortie 1	1 bit
1772.15	1772.15	Remise sous tension requise	1 bit
1773.0	1773.0	Sorties à tolérance de panne	1 bit
1773.1	1773.1	Dispositif de reset local	1 bit
1773.2	1773.2	En cascade	1 bit
1773.3	1773.3	Niveau de codage élevé	1 bit
1773.4 à 1773.7	1773.4 à 1773.7	Apprentissages restants	4 bits
1773.8 à 1773.12	1773.8 à 1773.12	ID dispositif	5 bits
1773.13 à 1774.2	1773.13 à 1774.2	Nombre d'avertissements de portée	6 bits
1774.3 à 1774.7	1774.3 à 1774.7	Délai de désactivation de la sortie	5 bits
1774.8 à 1774.15	1774.8 à 1774.15	Nombre d'erreurs de tension	8 bits
1775.0 à 1775.7	1775.0 à 1775.7	Température interne [47]	8 bits
1775.8 à 1775.15	1775.8 à 1775.15	Distance de l'actionneur [47]	8 bits
1776.0 à 1776.7	1776.0 à 1776.7	Tension d'alimentation [47]	8 bits
1776.8 à 1776.11	1776.8 à 1776.11	Nom de société attendu	4 bits
1776.12 à 1776.15	1776.12 à 1776.15	Nom de société reçu	4 bits
1777	1777	Code attendu	16 bits
1778	1778	Code reçu	16 bits

[47] Pour la conversion de la température interne, de la distance de l'actionneur et de la tension, voir la section ISD : Informations sur la conversion de la distance, tension et température à la page 309.

N° REG. entrée	N° REG. maintien	Informations	Taille des données
1779	1779	Erreur interne A	16 bits
1780	1780	Erreur interne B	16 bits

13.6 PLC5, SLC500 et MicroLogix (PCCC)

Les gammes d'API PLC5, SLC 500 et MicroLogix d'Allen-Bradley utilisent le protocole de communication PCCC.

PCCC, également appelé protocole de transport EtherNet/IP de classe 3, utilise des commandes de message Read et Write explicites, ou messages EIP, placés dans le programme Ladder Logic pour communiquer avec le contrôleur de sécurité.

Ces API ne prennent pas en charge le transfert des données d'E/S EtherNet/IP cyclique (désigné par le terme EtherNet/IP). Ils utilisent le logiciel de programmation RSLogix 5 (PLC5) ou RSLogix 500 (séries SLC500 et MicroLogix).

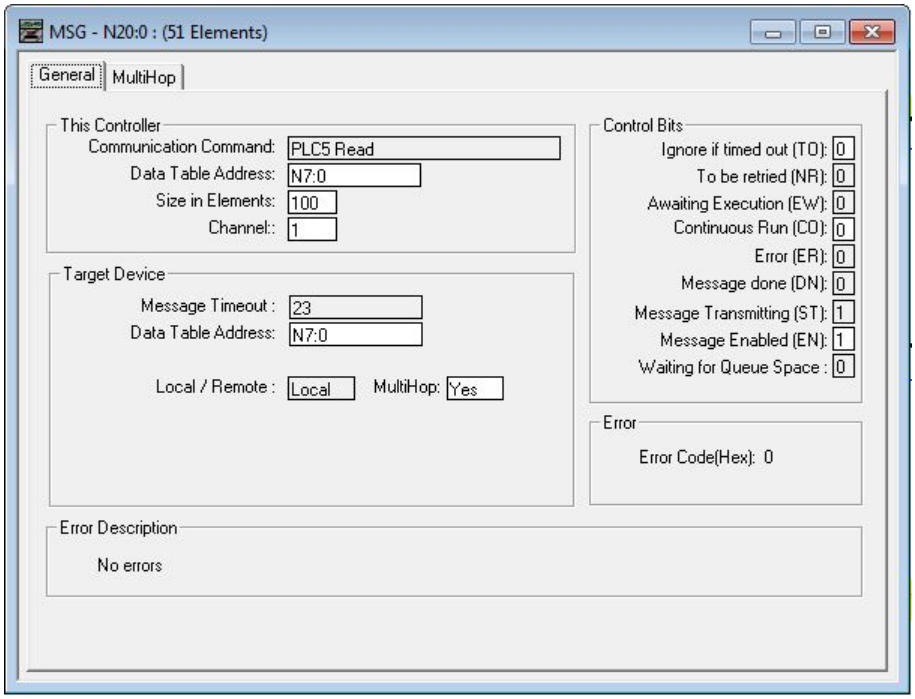
Le contrôleur de sécurité prend en charge ces API via une table de registres d'entrée. Le terme *entrée* s'entend du point de vue de l'API.

13.6.1 Configuration de l'API

Les images ci-dessous représentent une configuration normale.

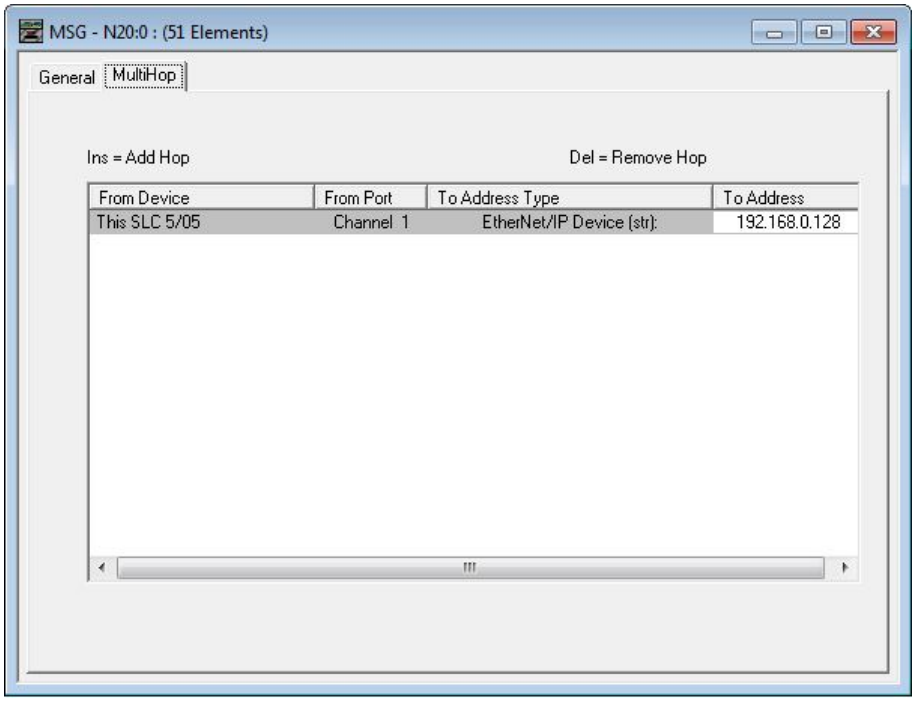
1. Read. Lecture de commande de message à partir de la table N7 sur le contrôleur de sécurité.

Illustration 269. Lecture de commande de message 100 registres à partir de la table N7 du contrôleur de sécurité.



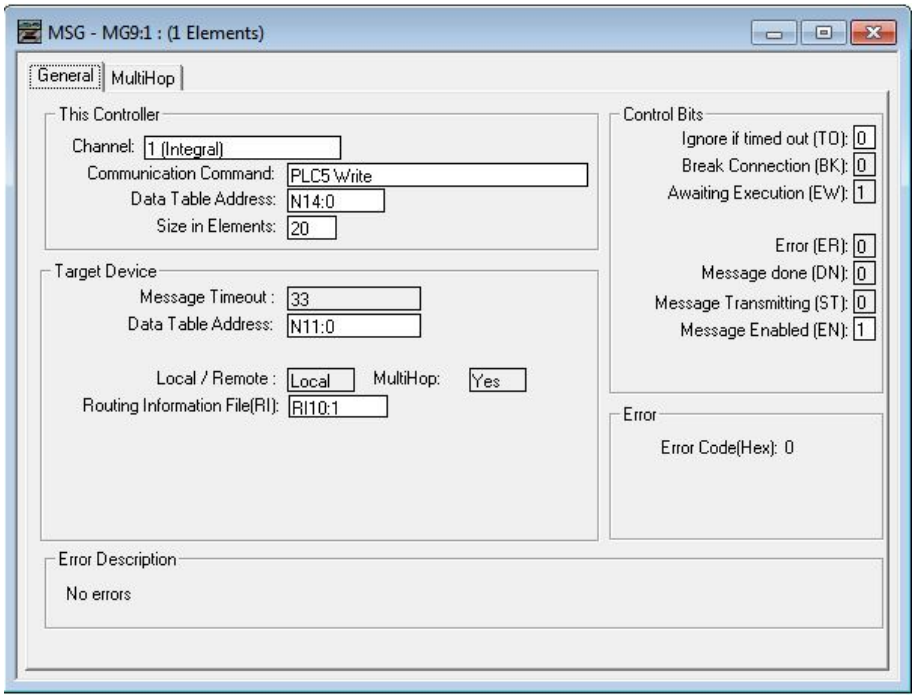
2. Read. L'adresse IP du contrôleur de sécurité est indiquée ici.

*Illustration 270. Ajout de l'adresse IP du contrôleur de sécurité dans la zone **To Address** (Adresse de destination)*



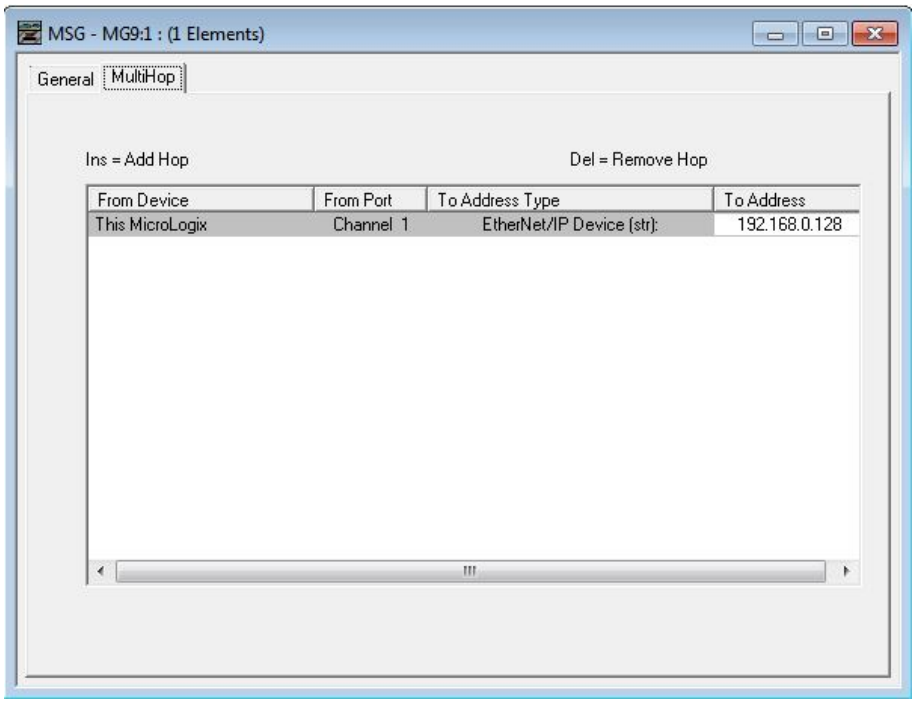
3. Write. Écriture de commande de message dans la table N11 sur le contrôleur de sécurité.

Illustration 271. Écriture de commande de message 20 registres à partir de la table N11 du contrôleur de sécurité.



4. Write. L'adresse IP du contrôleur de sécurité est indiquée ici.

*Illustration 272. Ajout de l'adresse IP du contrôleur de sécurité dans la zone **To Address** (Adresse de destination)*



13.6.2 Sorties du contrôleur de sécurité (entrées vers l'API)

Les registres de sortie permettent d'envoyer des valeurs de sortie du contrôleur de sécurité à l'API. Il existe deux tableaux de valeurs de sortie en raison de leur taille. Les commandes MSG (message) permettent de lire (N7, N20) à partir du contrôleur de sécurité.

Remarque: Les contrôleurs de sécurité ne prennent pas tous en charge ISD.

Remarque: Seul le XS26-ISD prend en charge huit chaînes de dispositifs ISD.

Table 42. Carte de registres N7

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
0	VO1 – VO16 (voir Indicateurs à la page 270)	Entier 16 bits
1	VO17 – VO32 (voir Indicateurs à la page 270)	Entier 16 bits
2	VO33 – VO48 (voir Indicateurs à la page 270)	Entier 16 bits
3	VO49 – VO64 (voir Indicateurs à la page 270)	Entier 16 bits
4	Bits de défaut pour VO1 – VO16 (voir Indicateurs à la page 270)	Entier 16 bits
5	Bits de défaut pour VO17 – VO32 (voir Indicateurs à la page 270)	Entier 16 bits
6	Bits de défaut pour VO33 – VO48 (voir Indicateurs à la page 270)	Entier 16 bits
7	Bits de défaut pour VO49 – VO64 (voir Indicateurs à la page 270)	Entier 16 bits
8-18	*réservés*	Entier 16 bits
19	Retour d'infos Reset/Annulation de la temporisation virtuels (1–16) [Bits de registre de retour RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
20	*réservés*	Entier 16 bits
21	Retour d'infos Code d'actionnement RCD [Registre de retour de l'activation RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
22-39	*réservés*	Entier 16 bits
40	Index de défaut VO1	Entier 16 bits
41	Index de défaut VO2	Entier 16 bits
42	Index de défaut VO3	Entier 16 bits
43	Index de défaut VO4	Entier 16 bits
44	Index de défaut VO5	Entier 16 bits
45	Index de défaut VO6	Entier 16 bits
46	Index de défaut VO7	Entier 16 bits
47	Index de défaut VO8	Entier 16 bits
48	Index de défaut VO9	Entier 16 bits
49	Index de défaut VO10	Entier 16 bits
50	Index de défaut VO11	Entier 16 bits
51	Index de défaut VO12	Entier 16 bits
52	Index de défaut VO13	Entier 16 bits
53	Index de défaut VO14	Entier 16 bits
54	Index de défaut VO15	Entier 16 bits
55	Index de défaut VO16	Entier 16 bits
56	Index de défaut VO17	Entier 16 bits
57	Index de défaut VO18	Entier 16 bits
58	Index de défaut VO19	Entier 16 bits
59	Index de défaut VO20	Entier 16 bits
60	Index de défaut VO21	Entier 16 bits
61	Index de défaut VO22	Entier 16 bits
62	Index de défaut VO23	Entier 16 bits
63	Index de défaut VO24	Entier 16 bits
64	Index de défaut VO25	Entier 16 bits
65	Index de défaut VO26	Entier 16 bits
66	Index de défaut VO27	Entier 16 bits
67	Index de défaut VO28	Entier 16 bits
68	Index de défaut VO29	Entier 16 bits
69	Index de défaut VO30	Entier 16 bits
70	Index de défaut VO31	Entier 16 bits
71	Index de défaut VO32	Entier 16 bits
72	Index de défaut VO33	Entier 16 bits
73	Index de défaut VO34	Entier 16 bits
74	Index de défaut VO35	Entier 16 bits
75	Index de défaut VO36	Entier 16 bits
76	Index de défaut VO37	Entier 16 bits
77	Index de défaut VO38	Entier 16 bits
78	Index de défaut VO39	Entier 16 bits
79	Index de défaut VO40	Entier 16 bits
80	Index de défaut VO41	Entier 16 bits
81	Index de défaut VO42	Entier 16 bits

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
82	Index de défaut VO43	Entier 16 bits
83	Index de défaut VO44	Entier 16 bits
84	Index de défaut VO45	Entier 16 bits
85	Index de défaut VO46	Entier 16 bits
86	Index de défaut VO47	Entier 16 bits
87	Index de défaut VO48	Entier 16 bits
88	Index de défaut VO49	Entier 16 bits
89	Index de défaut VO50	Entier 16 bits
90	Index de défaut VO51	Entier 16 bits
91	Index de défaut VO52	Entier 16 bits
92	Index de défaut VO53	Entier 16 bits
93	Index de défaut VO54	Entier 16 bits
94	Index de défaut VO55	Entier 16 bits
95	Index de défaut VO56	Entier 16 bits
96	Index de défaut VO57	Entier 16 bits
97	Index de défaut VO58	Entier 16 bits
98	Index de défaut VO59	Entier 16 bits
99	Index de défaut VO60	Entier 16 bits
100	Index de défaut VO61	Entier 16 bits
101	Index de défaut VO62	Entier 16 bits
102	Index de défaut VO63	Entier 16 bits
103	Index de défaut VO64	Entier 16 bits
104–105	Code de défaut complet VO1	Entier 32 bits
106–107	Code de défaut complet VO2	Entier 32 bits
108–109	Code de défaut complet VO3	Entier 32 bits
110–111	Code de défaut complet VO4	Entier 32 bits
112–113	Code de défaut complet VO5	Entier 32 bits
114–115	Code de défaut complet VO6	Entier 32 bits
116–117	Code de défaut complet VO7	Entier 32 bits
118–119	Code de défaut complet VO8	Entier 32 bits
120–121	Code de défaut complet VO9	Entier 32 bits
122–123	Code de défaut complet VO10	Entier 32 bits
124–125	Code de défaut complet VO11	Entier 32 bits
126–127	Code de défaut complet VO12	Entier 32 bits
128–129	Code de défaut complet VO13	Entier 32 bits
130–131	Code de défaut complet VO14	Entier 32 bits
132–133	Code de défaut complet VO15	Entier 32 bits
134–135	Code de défaut complet VO16	Entier 32 bits
136–137	Code de défaut complet VO17	Entier 32 bits
138–139	Code de défaut complet VO18	Entier 32 bits
140–141	Code de défaut complet VO19	Entier 32 bits
142–143	Code de défaut complet VO20	Entier 32 bits
144–145	Code de défaut complet VO21	Entier 32 bits

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
146–147	Code de défaut complet VO22	Entier 32 bits
148–149	Code de défaut complet VO23	Entier 32 bits
150–151	Code de défaut complet VO24	Entier 32 bits
152–153	Code de défaut complet VO25	Entier 32 bits
154–155	Code de défaut complet VO26	Entier 32 bits
156–157	Code de défaut complet VO27	Entier 32 bits
158–159	Code de défaut complet VO28	Entier 32 bits
160–161	Code de défaut complet VO29	Entier 32 bits
162–163	Code de défaut complet VO30	Entier 32 bits
164–165	Code de défaut complet VO31	Entier 32 bits
166–167	Code de défaut complet VO32	Entier 32 bits
168–169	Code de défaut complet VO33	Entier 32 bits
170–171	Code de défaut complet VO34	Entier 32 bits
172–173	Code de défaut complet VO35	Entier 32 bits
174–175	Code de défaut complet VO36	Entier 32 bits
176–177	Code de défaut complet VO37	Entier 32 bits
178–179	Code de défaut complet VO38	Entier 32 bits
180–181	Code de défaut complet VO39	Entier 32 bits
182–183	Code de défaut complet VO40	Entier 32 bits
184–185	Code de défaut complet VO41	Entier 32 bits
186–187	Code de défaut complet VO42	Entier 32 bits
188–189	Code de défaut complet VO43	Entier 32 bits
190–191	Code de défaut complet VO44	Entier 32 bits
192–193	Code de défaut complet VO45	Entier 32 bits
194–195	Code de défaut complet VO46	Entier 32 bits
196–197	Code de défaut complet VO47	Entier 32 bits
198–199	Code de défaut complet VO48	Entier 32 bits
200–201	Code de défaut complet VO49	Entier 32 bits
202–203	Code de défaut complet VO50	Entier 32 bits
204–205	Code de défaut complet VO51	Entier 32 bits
206–207	Code de défaut complet VO52	Entier 32 bits
208–209	Code de défaut complet VO53	Entier 32 bits
210–211	Code de défaut complet VO54	Entier 32 bits
212–213	Code de défaut complet VO55	Entier 32 bits
214–215	Code de défaut complet VO56	Entier 32 bits
216–217	Code de défaut complet VO57	Entier 32 bits
218–219	Code de défaut complet VO58	Entier 32 bits
220–221	Code de défaut complet VO59	Entier 32 bits
222–223	Code de défaut complet VO60	Entier 32 bits
224–225	Code de défaut complet VO61	Entier 32 bits
226–227	Code de défaut complet VO62	Entier 32 bits
228-229	Code de défaut complet VO63	Entier 32 bits
230–231	Code de défaut complet VO64	Entier 32 bits

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
232-233	Horodatage Défaut 1	Entier 32 bits
234–241	Nom de l'E/S ou du système Défaut 1	Longueur de 2 mots (word) + 12 caractères ASCII
242	Code d'erreur Défaut 1	Entier 16 bits
243	Code d'erreur avancé Défaut 1	Entier 16 bits
244	Index de message d'erreur Défaut 1	Entier 16 bits
245–246	*réservés*	Entier 16 bits
247–248	Horodatage Défaut 2	Entier 32 bits
249–256	Nom de l'E/S ou du système Défaut 2	Longueur de 2 mots (word) + 12 caractères ASCII
257	Code d'erreur Défaut 2	Entier 16 bits
258	Code d'erreur avancé Défaut 2	Entier 16 bits
259	Index de message d'erreur Défaut 2	Entier 16 bits
260–261	*réservés*	Entier 16 bits
262–263	Horodatage Défaut 3	Entier 32 bits
264–271	Nom de l'E/S ou du système Défaut 3	Longueur de 2 mots (word) + 12 caractères ASCII
272	Code d'erreur Défaut 3	Entier 16 bits
273	Code d'erreur avancé Défaut 3	Entier 16 bits
274	Index de message d'erreur Défaut 3	Entier 16 bits
275–276	*réservés*	Entier 16 bits
277–278	Horodatage Défaut 4	Entier 32 bits
279–286	Nom de l'E/S ou du système Défaut 4	Longueur de 2 mots (word) + 12 caractères ASCII
287	Code d'erreur Défaut 4	Entier 16 bits
288	Code d'erreur avancé Défaut 4	Entier 16 bits
289	Index de message d'erreur Défaut 4	Entier 16 bits
290–291	*réservés*	Entier 16 bits
292–293	Horodatage Défaut 5	Entier 32 bits
294–301	Nom de l'E/S ou du système Défaut 5	Longueur de 2 mots (word) + 12 caractères ASCII
302	Code d'erreur Défaut 5	Entier 16 bits
303	Code d'erreur avancé Défaut 5	Entier 16 bits
304	Index de message d'erreur Défaut 5	Entier 16 bits
305–306	*réservés*	Entier 16 bits
307–308	Horodatage Défaut 6	Entier 32 bits
309–316	Nom de l'E/S ou du système Défaut 6	Longueur de 2 mots (word) + 12 caractères ASCII
317	Code d'erreur Défaut 6	Entier 16 bits
318	Code d'erreur avancé Défaut 6	Entier 16 bits
319	Index de message d'erreur Défaut 6	Entier 16 bits
320–321	*réservés*	Entier 16 bits
322–323	Horodatage Défaut 7	Entier 32 bits
324–331	Nom de l'E/S ou du système Défaut 7	Longueur de 2 mots (word) + 12 caractères ASCII
332	Code d'erreur Défaut 7	Entier 16 bits

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
333	Code d'erreur avancé Défaut 7	Entier 16 bits
334	Index de message d'erreur Défaut 7	Entier 16 bits
335–336	*réservés*	Entier 16 bits
337–338	Horodatage Défaut 8	Entier 32 bits
339–346	Nom de l'E/S ou du système Défaut 8	Longueur de 2 mots (word) + 12 caractères ASCII
347	Code d'erreur Défaut 8	Entier 16 bits
348	Code d'erreur avancé Défaut 8	Entier 16 bits
349	Index de message d'erreur Défaut 8	Entier 16 bits
350–351	*réservés*	Entier 16 bits
352–353	Horodatage Défaut 9	Entier 32 bits
354–361	Nom de l'E/S ou du système Défaut 9	Longueur de 2 mots (word) + 12 caractères ASCII
362	Code d'erreur Défaut 9	Entier 16 bits
363	Code d'erreur avancé Défaut 9	Entier 16 bits
364	Index de message d'erreur Défaut 9	Entier 16 bits
365–366	réservés	Entier 16 bits
367–368	Horodatage Défaut 10	Entier 32 bits
369–376	Nom de l'E/S ou du système Défaut 10	Longueur de 2 mots (word) + 12 caractères ASCII
377	Code d'erreur Défaut 10	Entier 16 bits
378	Code d'erreur avancé Défaut 10	Entier 16 bits
379	Index de message d'erreur Défaut 10	Entier 16 bits
380–381	*réservés*	Entier 16 bits
382–383	Secondes depuis le démarrage	Entier 32 bits
384	Mode de fonctionnement	Entier 16 bits
385–394	Nom de la configuration	Longueur de 2 mots (word) + 16 caractères ASCII
395–396	CRC de configuration	Entier 32 bits
397–899	*réservés*	Entier 16 bits
900	VO1 – VO16 (voir Indicateurs à la page 270)	Entier 16 bits
901	VO17 – VO32 (voir Indicateurs à la page 270)	Entier 16 bits
902	VO33 – VO48 (voir Indicateurs à la page 270)	Entier 16 bits
903	VO49 – VO64 (voir Indicateurs à la page 270)	Entier 16 bits
904	VO65 – VO80 (voir Indicateurs étendus à la page 270)	Entier 16 bits
905	VO81 – VO96 (voir Indicateurs étendus à la page 270)	Entier 16 bits
906	VO97 – VO112 (voir Indicateurs étendus à la page 270)	Entier 16 bits
907	VO113 – VO128 (voir Indicateurs étendus à la page 270)	Entier 16 bits
908	VO129 – VO144 (voir Indicateurs étendus à la page 270)	Entier 16 bits
909	VO145 – VO160 (voir Indicateurs étendus à la page 270)	Entier 16 bits
910	VO161 – VO176 (voir Indicateurs étendus à la page 270)	Entier 16 bits
911	VO177 – VO192 (voir Indicateurs étendus à la page 270)	Entier 16 bits
912	VO193 – VO208 (voir Indicateurs étendus à la page 270)	Entier 16 bits
913	VO209 – VO224 (voir Indicateurs étendus à la page 270)	Entier 16 bits

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
914	VO225 – VO240 (voir Indicateurs étendus à la page 270)	Entier 16 bits
915	VO241 – VO256 (voir Indicateurs étendus à la page 270)	Entier 16 bits
916	Bits de défaut pour VO1 – VO16 (voir Indicateurs à la page 270)	Entier 16 bits
917	Bits de défaut pour VO17 – VO32 (voir Indicateurs à la page 270)	Entier 16 bits
918	Bits de défaut pour VO33 – VO48 (voir Indicateurs à la page 270)	Entier 16 bits
919	Bits de défaut pour VO49 – VO64 (voir Indicateurs à la page 270)	Entier 16 bits
920	Bits de défaut pour VO65 – VO80 (voir Indicateurs étendus à la page 270)	Entier 16 bits
921	Bits de défaut pour VO81 – VO96 (voir Indicateurs étendus à la page 270)	Entier 16 bits
922	Bits de défaut pour VO97 – VO112 (voir Indicateurs étendus à la page 270)	Entier 16 bits
923	Bits de défaut pour VO113 – VO128 (voir Indicateurs étendus à la page 270)	Entier 16 bits
924	Bits de défaut pour VO129 – VO144 (voir Indicateurs étendus à la page 270)	Entier 16 bits
925	Bits de défaut pour VO145 – VO160 (voir Indicateurs étendus à la page 270)	Entier 16 bits
926	Bits de défaut pour VO161 – VO176 (voir Indicateurs étendus à la page 270)	Entier 16 bits
927	Bits de défaut pour VO177 – VO192 (voir Indicateurs étendus à la page 270)	Entier 16 bits
928	Bits de défaut pour VO193 – VO208 (voir Indicateurs étendus à la page 270)	Entier 16 bits
929	Bits de défaut pour VO209 – VO224 (voir Indicateurs étendus à la page 270)	Entier 16 bits
930	Bits de défaut pour VO225 – VO240 (voir Indicateurs étendus à la page 270)	Entier 16 bits
931	Bits de défaut pour VO241 – VO256 (voir Indicateurs étendus à la page 270)	Entier 16 bits
932	Retour d'infos Reset/Annulation de la temporisation virtuels (1–16) [Bits de registre de retour RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
933	*réservés*	Entier 16 bits
934	Retour d'infos Code d'actionnement RCD [Registre de retour de l'activation RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits

Table 43. Carte de registres N20

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
1	Index de défaut VO1	Entier 16 bits
2	Index de défaut VO2	Entier 16 bits
3	Index de défaut VO3	Entier 16 bits
…	…	…
256	Index de défaut VO256	Entier 16 bits
257-258	Code de défaut complet VO1	Entier 32 bits
259-260	Code de défaut complet VO2	Entier 32 bits

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
261-262	Code de défaut complet VO3	Entier 32 bits
263-264	Code de défaut complet VO4	Entier 32 bits
…	…	…
767-768	Code de défaut complet VO256	Entier 32 bits
769-770	État système ISD – Nbre de dispositifs Chaîne 1	Entier 32 bits
771-772	État système ISD – Nbre de dispositifs Chaîne 2	Entier 32 bits
773-774	État système ISD – État On/Off des dispositifs Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
775-776	État système ISD – État On/Off des dispositifs Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
777-778	État système ISD – État de défaut Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
779-780	État système ISD – État de défaut Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
781-782	État système ISD – État marginal Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
783-784	État système ISD – État marginal Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
785-786	État système ISD – État d'alerte Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
787-788	État système ISD – État d'alerte Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
789-790	État système ISD – État de reset Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
791-792	État système ISD – État de reset Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
793-794	État système ISD – Actionneur Chaîne 1 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
795-796	État système ISD – Actionneur Chaîne 2 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
797-798	État système ISD – État système Chaîne 1 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
799-800	État système ISD – État système Chaîne 2 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
801-816	Liste des dispositifs ISD détectés sur une chaîne	Table de 32 octets
817-833	*réservés*	Entier 16 bits
834	Accusé réc. demande de lecture ISD (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
835	Accusé réc. chaîne ISD demandée (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
836	Accusé réc. dispositif ISD demandé (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
837-845	Données spécifiques à un dispositif ISD individuel [48] (Référez-vous à Description détaillée des données spécifiques à un dispositif ISD individuel à la page 268)	Entier 16 bits
846-848	*réservés*	Entier 16 bits
849-850	État système ISD – Nbre de dispositifs Chaîne 1	Entier 32 bits

[48] Pour la conversion de la température interne, de la distance de l'actionneur et de la tension, voir la section ISD : Informations sur la conversion de la distance, tension et température à la page 309.

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
851-852	État système ISD – État On/Off des dispositifs Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
853-854	État système ISD – État de défaut Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
855-856	État système ISD – État marginal Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
857-858	État système ISD – État d'alerte Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
859-860	État système ISD – État de reset Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
861-862	État système ISD – État Actionneur Chaîne 1 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
863-864	État système ISD – État système Chaîne 1 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
865-866	État système ISD – Nbre de dispositifs Chaîne 2	Entier 32 bits
867-868	État système ISD – État On/Off des dispositifs Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
869-870	État système ISD – État de défaut Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
871-872	État système ISD – État marginal Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
873-874	État système ISD – État d'alerte Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
875-876	État système ISD – État de reset Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
877-878	État système ISD – État Actionneur Chaîne 2 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
879-880	État système ISD – État système Chaîne 2 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
881-882	État système ISD – Nbre de dispositifs Chaîne 3	Entier 32 bits
883-884	État système ISD – État On/Off des dispositifs Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
885-886	État système ISD – État de défaut Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
887-888	État système ISD – État marginal Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
889-890	État système ISD – État d'alerte Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
891-892	État système ISD – État de reset Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
893-894	État système ISD – État Actionneur Chaîne 3 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
895-896	État système ISD – État système Chaîne 3 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
897-898	État système ISD – Nbre de dispositifs Chaîne 4	Entier 32 bits
899-900	État système ISD – État On/Off des dispositifs Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
901-902	État système ISD – État de défaut Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
903-904	État système ISD – État marginal Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
905-906	État système ISD – État d'alerte Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
907-908	État système ISD – État de reset Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
909-910	État système ISD – État Actionneur Chaîne 4 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
911-912	État système ISD – État système Chaîne 4 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
913-914	État système ISD – Nbre de dispositifs Chaîne 5	Entier 32 bits
915-916	État système ISD – État On/Off des dispositifs Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
917-918	État système ISD – État de défaut Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
919-920	État système ISD – État marginal Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
921-922	État système ISD – État d'alerte Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
923-924	État système ISD – État de reset Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
925-926	État système ISD – État Actionneur Chaîne 5 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
927-928	État système ISD – État système Chaîne 5 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
929-930	État système ISD – Nbre de dispositifs Chaîne 6	Entier 32 bits
931-932	État système ISD – État On/Off des dispositifs Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
933-934	État système ISD – État de défaut Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
935-936	État système ISD – État marginal Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
937-938	État système ISD – État d'alerte Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
939-940	État système ISD – État de reset Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
941-942	État système ISD – État Actionneur Chaîne 6 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
943-944	État système ISD – État système Chaîne 6 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
945-946	État système ISD – Nbre de dispositifs Chaîne 7	Entier 32 bits
947-948	État système ISD – État On/Off des dispositifs Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
949-950	État système ISD – État de défaut Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
951-952	État système ISD – État marginal Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
953-954	État système ISD – État d'alerte Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
955-956	État système ISD – État de reset Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
957-958	État système ISD – État Actionneur Chaîne 7 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
959-960	État système ISD – État système Chaîne 7 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits
961-962	État système ISD – Nbre de dispositifs Chaîne 8	Entier 32 bits

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
963-964	État système ISD – État On/Off des dispositifs Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
965-966	État système ISD – État de défaut Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
967-968	État système ISD – État marginal Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
969-970	État système ISD – État d'alerte Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
971-972	État système ISD – État de reset Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
973-974	État système ISD – État Actionneur Chaîne 8 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Entier 32 bits
975-976	État système ISD – État système Chaîne 8 (voir État système de la chaîne ISD à la page 52)	Entier 32 bits

Remarque:
- Voir Données spécifiques à un dispositif ISD individuel à la page 54 pour plus d'informations sur la structure des données ISD.
- Les données ISD ne sont pas immédiatement disponibles à la mise sous tension. Les données ISD peuvent être retardées jusqu'à 10 secondes après la mise sous tension du système.

Description détaillée des données spécifiques à un dispositif ISD individuel

Le tableau suivant décrit le REGISTRE N20 837-845.

Table 44. Description détaillée des données spécifiques à un dispositif ISD individuel

N° REG.	Informations	Taille des données
837.0	Défaut d'entrée de sécurité	1 bit
837.1	*réservé*	1 bit
837.2	Capteur non couplé	1 bit
837.3	Erreur de données ISD	1 bit
837.4	Mauvais actionneur/État du bouton/État de l'entrée	1 bit
837.5	Portée marginale/État du bouton/État de l'entrée	1 bit
837.6	Actionneur détecté	1 bit
837.7	Erreur de sortie	1 bit
837.8	Entrée 2	1 bit
837.9	Entrée 1	1 bit
837.10	Reset local attendu	1 bit
837.11	Avertissement de tension de fonctionnement	1 bit
837.12	Erreur de tension de fonctionnement	1 bit
837.13	Sortie 2	1 bit
837.14	Sortie 1	1 bit
837.15	Remise sous tension requise	1 bit
838.0	Sorties à tolérance de panne	1 bit
838.1	Dispositif de reset local	1 bit
838.2	En cascade	1 bit
838.3	Niveau de codage élevé	1 bit
838.4 à 838.7	Apprentissages restants	4 bits
838.8 à 838.12	ID dispositif	5 bits

N° REG.	Informations	Taille des données
838.13 à 839.2	Nombre d'avertissements de portée	6 bits
839.3 à 839.7	Délai de désactivation de la sortie	5 bits
839.8 à 839.15	Nombre d'erreurs de tension	8 bits
840.0 à 840.7	Température interne [49]	8 bits
840.8 à 840.15	Distance de l'actionneur [49]	8 bits
841.0 à 841.7	Tension d'alimentation [49]	8 bits
841.8 à 841.11	Nom de société attendu	4 bits
841.12 à 841.15	Nom de société reçu	4 bits
842	Code attendu	16 bits
843	Code reçu	16 bits
844	Erreur interne A	16 bits
845	Erreur interne B	16 bits

Remarque: Voir Données spécifiques à un dispositif ISD individuel à la page 54 pour plus d'informations sur la structure des données ISD.

13.6.3 Entrées du contrôleur de sécurité (sorties de l'API)

Les registres d'entrée permettent d'envoyer des informations du contrôleur de sécurité à l'API. Les commandes MSG (message) permettent d'écrire (N11, N21) sur le contrôleur de sécurité.

Table 45. Carte de registres N11

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
0-7	*réservé*	Entier 16 bits
8	Entrée virtuelle On/Off (1–16)	Entier 16 bits
9	Entrée virtuelle On/Off (17–32)	Entier 16 bits
10	Entrée virtuelle On/Off (33–48)	Entier 16 bits
11	Entrée virtuelle On/Off (49–64)	Entier 16 bits
12-15	*réservés*	Entier 16 bits
16	Reset/Annulation de la temporisation virtuels (1–16) [Bits de registre RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits
17	*réservé*	Entier 16 bits
18	Code d'activation RCD [Registre d'activation RCD] (voir Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64)	Entier 16 bits

Table 46. Carte de registres N21

N° REG.	NOM DU MOT (WORD)	TYPE DE DONNÉES
1	Demande de lecture ISD (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
2	Chaîne ISD demandée (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits
3	Dispositif ISD demandé (voir Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52)	Entier 16 bits

[49] Pour la conversion de la température interne, de la distance de l'actionneur et de la tension, voir la section ISD : Informations sur la conversion de la distance, tension et température à la page 309.

13.6.4 Indicateurs

Les registres 0 à 7, définis ci-dessous, apparaissent comme les 8 premiers mots (word) dans la carte de registres N7.

Table 47. Registre 0, Sortie virtuelle 1-16, Position de bit

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO16	VO15	VO14	VO13	VO12	VO11	VO10	VO9	VO8	VO7	VO6	VO5	VO4	VO3	VO2	VO1

Table 48. Registre 1, Sortie virtuelle 17-32, Position de bit

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO32	VO31	VO30	VO29	VO28	VO27	VO26	VO25	VO24	VO23	VO22	VO21	VO20	VO19	VO18	VO17

Table 49. Registre 2, Sortie virtuelle 33-48, Position de bit

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO48	VO47	VO46	VO45	VO44	VO43	VO42	VO41	VO40	VO39	VO38	VO37	VO36	VO35	VO34	VO33

Table 50. Registre #3, Sortie virtuelle 49-64, Position de bit

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO64	VO63	VO62	VO61	VO60	VO59	VO58	VO57	VO56	VO55	VO54	VO53	VO52	VO51	VO50	VO49

Table 51. Registre 4, Bits d'indicateur de défaut pour la sortie virtuelle 1-16, Position de bit

Notez que toutes les sorties virtuelles n'ont pas d'indicateur de défaut défini.

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO16	VO15	VO14	VO13	VO12	VO11	VO10	VO9	VO8	VO7	VO6	VO5	VO4	VO3	VO2	VO1

Table 52. Registre 5, Bits d'indicateur de défaut pour la sortie virtuelle 17-32, Position de bit

Notez que toutes les sorties virtuelles n'ont pas d'indicateur de défaut défini.

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO32	VO31	VO30	VO29	VO28	VO27	VO26	VO25	VO24	VO23	VO22	VO21	VO20	VO19	VO18	VO17

Table 53. Registre 6, Bits d'indicateur de défaut pour la sortie virtuelle 33-48, Position de bit

Notez que toutes les sorties virtuelles n'ont pas d'indicateur de défaut défini.

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO48	VO47	VO46	VO45	VO44	VO43	VO42	VO41	VO40	VO39	VO38	VO37	VO36	VO35	VO34	VO33

Table 54. Registre 7, Bits d'indicateur de défaut pour la sortie virtuelle 49-64, Position de bit

Notez que toutes les sorties virtuelles n'ont pas d'indicateur de défaut défini.

Position de bit															
15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
VO64	VO63	VO62	VO61	VO60	VO59	VO58	VO57	VO56	VO55	VO54	VO53	VO52	VO51	VO50	VO49

13.6.5 Indicateurs étendus

Il est possible d'accéder aux 256 sorties virtuelles d'une manière similaire à celle décrite dans la section Indicateurs à la page 270.

Les 256 sorties virtuelles possibles peuvent être lues en tant que registres 900-915.

Les 256 défauts de sortie virtuelle possibles peuvent être lus en tant que registres 916-931.

13.7 PROFINET®

PROFINET® [50] est un protocole de communication des données pour l'automation et les processus industriels. PROFINET IO définit comment les contrôleurs (contrôleurs d'E/S) et les périphériques (dispositifs d'E/S) échangent les données en temps réel.

Le Contrôleur de sécurité Banner prend en charge PROFINET IO. Le protocole de communication des données est TCP/IP, le support de transmission des données est le fil de cuivre et la classe de conformité est PROFINET CC-A. [51]

Remarque: Dans ce document, les sorties du dispositif Contrôleur de sécurité sont considérées comme des « entrées » vers le contrôleur (API). Les sorties du contrôleur (API) sont considérées comme des « entrées » vers le dispositif Contrôleur de sécurité.

13.7.1 PROFINET® et contrôleurs de sécurité

Cette section comporte des instructions relatives aux contrôleurs de sécurité XS/SC26 FID 2 avec un code de date 1706 ou ultérieur (voir étiquette) et aux contrôleurs de sécurité XS/SC26 FID 3 ou ultérieur.

Cette section concerne aussi le SC10-2.

Les données en temps réel PROFINET sont envoyées et reçues par les logements.

Remarque: Le fichier GSD peut être téléchargé à l’adresse www.bannerengineering.com/safetycontroller.

13.7.2 Fichier GSD (General Station Description)

Le fichier GSD (General Station Description) contient des informations de module, notamment :

- Données de configuration
- Informations de données (nombre de pièces acceptables, état du contrôle, etc.)
- Diagnostic

13.7.3 Modèle de données PROFINET® IO

Le modèle de données PROFINET IO repose sur un dispositif de terrain extensible normal équipé d'un fond de panier avec des logements. Les modules et sous-modules ont différentes fonctionnalités.

Les modules sont enfichés dans des logements et les sous-modules dans des sous-logements. Dans le modèle de données PROFINET IO, le logement 0, sous-logement 1 est réservé pour l'interface réseau ou DAP (Device Access Point).

Les modules et les sous-modules permettent de contrôler le type et le volume des données envoyées au contrôleur (API).

- En général, un sous-module peut être de trois types : entrée, sortie ou entrée/sortie combinée.
- Un sous-module d'entrée permet d'envoyer des données au contrôleur (API).
- Un sous-module de sortie permet de recevoir des données du contrôleur (API).
- Le sous-module d'entrée/sortie combinée reçoit et envoie simultanément des données dans les deux sens.

13.7.4 Configuration du contrôleur de sécurité pour une connexion PROFINET IO

1. Raccordez le contrôleur de sécurité au PC via le câble USB SC-USB2 ou via Ethernet (pour les modèles Ethernet XS/SC26 FID7 ou ultérieurs).
2. Ouvrez le logiciel Contrôleur de sécurité Banner et cliquez sur l'onglet **Ethernet industriel**.
3. Dans la liste déroulante à gauche, sélectionnez **Profinet**.
4. Cliquez sur ✚ pour ajouter des informations aux sous-modules PROFINET.

   La fonction **Configuration auto** peut vous aider dans cette tâche.
5. Saisissez le code PIN/mot de passe approprié pour modifier les paramètres de configuration et réseau du contrôleur de sécurité.
6. Vérifiez que le contrôleur de sécurité possède un fichier de configuration valide et confirmé.

[50] PROFINET® est une marque commerciale de PROFIBUS Nutzerorganisation e.V.
[51] CC-A garantit que le dispositif possède les propriétés minimales requises en termes de fonctionnalités et d'interopérabilité.

Remarque: Si vous utilisez une séquence Reset virtuel ou Annulation de la temporisation, vous devez créer un code d'actionnement dans **Paramètres réseau**. Le code doit ensuite être envoyé au contrôleur de sécurité à l'aide du bouton **Envoyer** dans la fenêtre **Paramètres réseau**.

Remarque: Le processus ClickSet IP ne s'applique pas à PROFINET, car l'adresse IP est définie par le système API et non par le logiciel du contrôleur.

13.7.5 Création d'un fichier XML pour PROFINET

Plusieurs éléments doivent être connus :

- Le nom attribué au contrôleur de sécurité dans l'API. Ce nom est nécessaire pour générer le fichier à importer dans le champ du logiciel d'API indiqué sous PROFINET.
- Emplacement d'adresse Logement 1 API
- Emplacement d'adresse Logement 13 API
- Emplacement d'adresse Logement 20 API ou Logement 22 API
- Emplacement d'adresse Logement 21 API
- Emplacement d'adresse Logement 23 API

Ces informations sont disponibles dans le logiciel de l'API. La figure suivante est un exemple provenant du logiciel Siemens TIA Portal (v15).

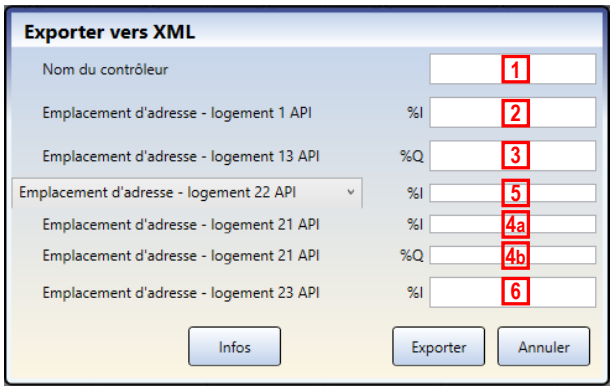
Illustration 273. ***Device overview (Aperçu des dispositifs)***

Module	Rack	Slot	I address	Q address	Type
xs26 1	0	0			XS26
I	0	0 X1			xs26
4 Status Bytes, Bits 0..31_1	0	1	2...5 2		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_2	0	2	6...9		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_3	0	3	10...13		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_4	0	4	14...17		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_5	0	5	18...21		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_6	0	6	22...25		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_7	0	7	26...29		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_8	0	8	30...33		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_9	0	9	34...37		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_10	0	10	38...41		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_11	0	11	42...45		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_12	0	12	46...49		4 Status Bytes, Bits 0..31
8 Bytes Virtual On/Off/ME Data_1	0	13		2...9 3	8 Bytes Virtual On/Off/ME Data
2 Bytes RCD Data_1	0	14		10...11	2 Bytes RCD Data
2 Byte RCD Acutation Code_1	0	15		12...13	2 Byte RCD Acutation Code
RCD Data Feedback Register_1	0	16	50...51		RCD Data Feedback Register
RCD Passcode Feedback Register_1	0	17	52...53		RCD Passcode Feedback Register
	0	18			
System Information Module_1	0	19	54...83		System Information Module
	0	20			
ISD Individual Status Information Module_1	0	21			ISD Individual Status Information Module
ISD Device Information Request	0	21 IS...	4a	14...19 4b	ISD Device Information Request
ISD Device Information Response	0	21 IS...	372...395		ISD Device Information Response
ISD Status Information Module 8 Chain_1	0	22	5 84...339		ISD Status Information Module 8 Chain
ISD Specific Chain Information Module_1	0	23	340...371 6		ISD Specific Chain Information Module

Remarque: Les logements 20, 21, 22 et 23 sont réservés aux informations ISD et ne sont disponibles qu'après avoir configuré les entrées ISD (SC10-2 FID 2 ou ultérieur, XS26-ISD FID 5 ou ultérieur). Le logement 22 n'est pas disponible avec les configurations SC10-2.

1. Dans le logiciel Contrôleur de sécurité Banner, dans l'onglet **Ethernet industriel**, assurez-vous que **PROFINET** est sélectionné dans la liste de gauche.
2. Cliquez sur **Exporter**.
   La fenêtre **Exporter vers XML** s'ouvre.

*Illustration 274. **Exporter vers XML**— XS26-ISD (capture d'écran)*



Les chiffres de cette figure correspondent aux chiffres de la Illustration 273 à la page 272.

3. Entrez les informations dans la fenêtre.
   a) Dans le champ **Nom du contrôleur**, indiquez le nom attribué au contrôleur de sécurité dans le logiciel de l'API. Voir l'élément 1 dans la Illustration 273 à la page 272. Dans cet exemple, il s'agit de `xs26`.
   b) Dans le champ **Emplacement d'adresse Logement 1 API**, indiquez l'emplacement d'adresse de début du logement 1 (sorties d'état). Voir l'élément 2 dans la Illustration 273 à la page 272. Dans cet exemple, il s'agit de `2`.
   c) Dans le champ **Emplacement d'adresse Logement 13 API**, indiquez l'emplacement d'adresse de début du logement 13 (entrées virtuelles). Voir l'élément 3 dans la Illustration 273 à la page 272. Dans cet exemple, il s'agit de `2`.
4. Entrez les informations facultatives dans la fenêtre. Ces champs doivent être vides s'ils ne sont pas utilisés.
   a) Modèles SC10-2 : dans le champ **Emplacement d'adresse Logement 20 API**, indiquez l'emplacement d'adresse de début du logement 20 (module d'informations d'état ISD 4 chaînes).
   b) Modèles XS26-ISD : dans le menu déroulant, sélectionnez l'une des options suivantes :
      - **Emplacement d'adresse Logement 20 API** pour le module d'informations d'état ISD 4 chaînes (non illustré dans la Illustration 273 à la page 272).
      - **Emplacement d'adresse Logement 22 API** pour le module d'informations d'état ISD 8 chaînes (non illustré dans la Illustration 273 à la page 272). Dans cet exemple, il s'agit de `84`.
   c) Modèles XS26-ISD : dans le champ **Emplacement d'adresse Logement 21 API**, indiquez l'emplacement d'adresse de début du logement 21 (module d'informations d'un dispositif individuel ISD). Voir les éléments 4a et 4b dans la Illustration 273 à la page 272. Dans cet exemple, il s'agit de `372` et `14`.
   d) Modèles XS26-ISD : dans le champ **Emplacement d'adresse Logement 23 API**, indiquez l'emplacement d'adresse de début du logement 23 (module d'informations d'un dispositif individuel ISD), voir l'élément 6 dans la Illustration 273 à la page 272. Dans cet exemple, il s'agit de `340`.
5. Cliquez sur **Exporter**.
6. Enregistrez le fichier .xml dans l'emplacement voulu.

Le fichier .xml est prêt à être directement importé dans le logiciel de l'API indiqué dans PROFINET ou à être ouvert avec n'importe quel logiciel capable de lire un fichier .xml.

13.7.6 Description des modules

Table 55. Attribution des logements

Dans ce tableau, la direction d'E/S est envisagée à partir de l'API.

Espace réservé	Fonction du module	E/S	Nom du module	Taille du module (octets)
1	Bits d'état définis par l'utilisateur (0–31)	In	4 octets d'état, Bits 0..31_1	4
2	Bits d'état définis par l'utilisateur (32–63)	In	4 octets d'état, Bits 0..31_2	4
3	Bits de défaut du contrôleur de sécurité (0–31)	In	4 octets d'état, Bits 0..31_3	4
4	Bits de défaut du contrôleur de sécurité (32–63)	In	4 octets d'état, Bits 0..31_4	4
5	Bits d'état d'entrée du contrôleur de sécurité (0–31)	In	4 octets d'état, Bits 0..31_5	4
6	Bits d'état d'entrée du contrôleur de sécurité (32–63)	In	4 octets d'état, Bits 0..31_6	4

Espace réservé	Fonction du module	E/S	Nom du module	Taille du module (octets)
7	Bits d'état d'entrée du contrôleur de sécurité (64–95)	In	4 octets d'état, Bits 0..31_7	4
8	Bits d'état d'entrée du contrôleur de sécurité (96–127)	In	4 octets d'état, Bits 0..31_8	4
9	Bits d'état d'entrée du contrôleur de sécurité (128–159)	In	4 octets d'état, Bits 0..31_9	4
10	Bits d'état de sortie du contrôleur de sécurité (0–31)	In	4 octets d'état, Bits 0..31_10	4
11	Bits d'état de sortie du contrôleur de sécurité (32–63)	In	4 octets d'état, Bits 0..31_11	4
12	Bits d'état de sortie du contrôleur de sécurité (64–95)	In	4 octets d'état, Bits 0..31_12	4
13	Bits d'E/S virtuelle (On/Off/Activation d'inhibition) (0–63)	Out	Données On/Off/ME virtuels 8 octets_1	8
14	Bits de reset et d'annulation de la temporisation virtuels (0–16)	Out	Données RCD 2 octets_1	2
15	Code d'actionnement du reset et de l'annulation de la temporisation	Out	Code d'actionnement RCD 2 octets_1	2
16	Retour d'informations sur les bits de reset et d'annulation de la temporisation virtuels (0–16)	In	Registre de retour de données RCD _1	2
17	Retour d'informations sur le code d'actionnement du reset et de l'annulation de la temporisation	In	Registre de retour Mot de passe RCD_1	2
18 [52]	Journal de défauts	In	Module Mémoire tampon du journal de défauts	300
19 [52]	Informations système	In	Module Informations système	30
20	État ISD (4 chaînes)	In	Module Informations d'état ISD 4 chaînes	128
21	Informations d'un dispositif ISD individuel	Entrée/ Sortie	Module Informations d'état individuel ISD	24 In/6 Out
22	État ISD (8 chaînes)	In	Module Informations d'état ISD 8 chaînes	256
23	Liste des dispositifs ISD détectés sur une chaîne	In	Module d'information de chaîne spécifique ISD	32

Remarque:

- Voir Données spécifiques à un dispositif ISD individuel à la page 54 pour plus d'informations sur la structure des données ISD.
- Les données ISD ne sont pas immédiatement disponibles à la mise sous tension. Les données ISD peuvent être retardées jusqu'à 10 secondes après la mise sous tension du système.

[52] Les modules Journal de défauts et Informations système ne sont pas utilisés par la connexion par défaut.

Bits d'état définis par l'utilisateur

Les deux premiers logements sont toujours occupés par les modules Bits d'état définis par l'utilisateur. Ces modules incluent 64 bits d'informations de sortie d'état virtuelle de tout type.

Table 56. Module Bits d'état définis par l'utilisateur (0–31) (Ident 0×100) [fixe dans le logement 1]

Nom des données d'entrée API	Type de données d'entrée
Bits d'état définis par l'utilisateur 0–7	Octet
Bits d'état définis par l'utilisateur 8–15	Octet
Bits d'état définis par l'utilisateur 16–23	Octet
Bits d'état définis par l'utilisateur 24–31	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Table 57. Module Bits d'état définis par l'utilisateur (32–63) (Ident 0×0100) [fixe dans le logement 2]

Nom des données d'entrée API	Type de données d'entrée
Bits d'état définis par l'utilisateur 32–39	Octet
Bits d'état définis par l'utilisateur 40–47	Octet
Bits d'état définis par l'utilisateur 48–55	Octet
Bits d'état définis par l'utilisateur 56–63	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Bits de défaut

Les logements 3 et 4 sont toujours occupés par 64 bits d'informations de sortie d'état virtuelle de type Défaut envoyés par le contrôleur de sécurité.

Table 58. Module Bits de défaut du contrôleur de sécurité (0–31) (Ident 0×0100) [fixe dans le logement 3]

Nom des données d'entrée API	Type de données d'entrée
Bits de défaut 0–7	Octet
Bits de défaut 8–15	Octet
Bits de défaut 16–23	Octet
Bits de défaut 24–31	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Table 59. Module Bits de défaut du contrôleur de sécurité (32–63) (Ident 0×0100) [fixe dans le logement 4]

Nom des données d'entrée API	Type de données d'entrée
Bits de défaut 32–39	Octet
Bits de défaut 40–47	Octet
Bits de défaut 48–55	Octet
Bits de défaut 56–63	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Bits d'état d’entrée

Les logements 5 à 9 sont toujours réservés pour 160 bits d'informations d'entrée du contrôleur de sécurité. Un contrôleur de sécurité extensible peut avoir jusqu'à 154 entrées, si les 8 cartes d'extension possibles sont utilisées comme 16 entrées de voie (en plus des 26 entrées intégrées du contrôleur de base).

Table 60. Module Bits d'état d'entrée du contrôleur de sécurité (0–31) (Ident 0×1000) [fixe dans le logement 5]

Nom des données d'entrée API	Type de données d’entrée
Bits d'état d’entrée 0–7	Octet
Bits d'état d’entrée 8–15	Octet
Bits d'état d’entrée 16–23	Octet
Bits d'état d’entrée 24–31	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Table 61. Module Bits d'état d'entrée du contrôleur de sécurité (32–63) (Ident 0×0100) [fixe dans le logement 6]

Nom des données d'entrée API	Type de données d’entrée
Bits d'état d’entrée 32–39	Octet
Bits d'état d’entrée 40–47	Octet
Bits d'état d’entrée 48–55	Octet
Bits d'état d’entrée 56–63	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Table 62. Module Bits d'état d'entrée du contrôleur de sécurité (64–95) (Ident 0×0100) [fixe dans le logement 7]

Nom des données d'entrée API	Type de données d’entrée
Bits d'état d’entrée 64–71	Octet
Bits d'état d’entrée 72–79	Octet
Bits d'état d’entrée 80–87	Octet
Bits d'état d’entrée 88–95	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Table 63. Module Bits d'état d'entrée du contrôleur de sécurité (96–127) (Ident 0×0100) [fixe dans le logement 8]

Nom des données d'entrée API	Type de données d’entrée
Bits d'état d’entrée 96–103	Octet
Bits d'état d’entrée 104–111	Octet
Bits d'état d’entrée 112–119	Octet
Bits d'état d’entrée 120–127	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Table 64. Module Bits d'état d'entrée du contrôleur de sécurité (128–159) (Ident 0×0100) [fixe dans le logement 9]

Nom des données d'entrée API	Type de données d’entrée
Bits d'état d’entrée 128–135	Octet
Bits d'état d’entrée 136–143	Octet
Bits d'état d’entrée 144–151	Octet
Bits d'état d’entrée 152–159	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Bits d'état de sortie

Les logements 10 à 12 sont réservés pour 96 bits de sortie d'état virtuel de type sortie du contrôleur de sécurité.

Table 65. Module Bits d'état de sortie du contrôleur de sécurité (0–31) (Ident 0×0100) [fixe dans le logement 10]

Nom des données d'entrée API	Type de données d'entrée
Bits d'état de sortie 0–7	Octet
Bits d'état de sortie 8–15	Octet
Bits d'état de sortie 16–23	Octet
Bits d'état de sortie 24–31	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Table 66. Module Bits d'état de sortie du contrôleur de sécurité (32–63) (Ident 0×0100) [fixe dans le logement 11]

Nom des données d'entrée API	Type de données d'entrée
Bits d'état de sortie 32–39	Octet
Bits d'état de sortie 40–47	Octet
Bits d'état de sortie 48–55	Octet
Bits d'état de sortie 56–63	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Table 67. Module Bits d'état de sortie du contrôleur de sécurité (64–95) (Ident 0×0100) [fixe dans le logement 12]

Nom des données d'entrée API	Type de données d'entrée
Bits d'état de sortie 64–71	Octet
Bits d'état de sortie 72–79	Octet
Bits d'état de sortie 80–87	Octet
Bits d'état de sortie 88–95	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Bits de marche/arrêt (on/off) et d'activation de l'inhibition virtuels

Le logement 13 est occupé par 64 entrées auxiliaires de sécurité, à utiliser comme entrées de marche/arrêt (on/off) virtuelles (vers le contrôleur de sécurité) ou entrées d'activation de l'inhibition (ME) virtuelles (vers le contrôleur de sécurité).

Table 68. Module Bits de marche/arrêt/activation de l'inhibition virtuels (0–63) (Ident 0×0200) [fixe dans le logement 13]

Nom des données d'entrée API	Type de données d'entrée
Sans objet	Sans objet

Nom des données de sortie API	Type de données de sortie
Bits On/Off/ME virtuels 0–7	Octet
Bits On/Off/ME virtuels 8–15	Octet
Bits On/Off/ME virtuels 16–23	Octet
Bits On/Off/ME virtuels 24–31	Octet
Bits On/Off/ME virtuels 32–39	Octet
Bits On/Off/ME virtuels 40–47	Octet
Bits On/Off/ME virtuels 48–55	Octet
Bits On/Off/ME virtuels 56–63	Octet

Bits de reset et d'annulation de la temporisation virtuels (VRCD)

Seize entrées auxiliaires virtuelles peuvent occuper le logement 14 ; à utiliser dans la séquence de reset et d'annulation de la temporisation virtuels.

Référez-vous à la section Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64.

Table 69. Module Bits de reset et d'annulation de la temporisation virtuels (0–63) (Ident 0×0300) [fixe dans le logement 14]

Nom des données d'entrée API	Type de données d'entrée
Sans objet	Sans objet

Nom des données de sortie API	Type de données de sortie
Bits VRCD 0-7	Octet
Bits VRCD 8-15	Octet

Code d'actionnement 16 bits du reset et de l'annulation de la temporisation (RCD)

Le logement 15 inclut le code d'actionnement RCD, un mot (word) de code important utilisé dans la séquence de reset et d'annulation de la temporisation virtuels.

Référez-vous à la section Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64.

Table 70. Module Code d'actionnement du reset et de l'annulation de la temporisation (Ident 0×301) [fixe dans le logement 15]

Nom des données d'entrée API	Type de données d'entrée
Sans objet	Sans objet

Nom des données de sortie API	Type de données de sortie
Code d'actionnement du reset et de l'annulation de la temporisation	Non signé 16

Bits de retour d'informations sur le reset et l'annulation de la temporisation virtuels

Le logement 16 inclut des bits de retour pour les 16 entrées auxiliaires virtuelles occupant le logement 14. Ils sont utilisés dans la séquence de reset et d'annulation de la temporisation virtuels.

Référez-vous à la section Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64.

Table 71. Module Bits de retour d'informations sur le reset et l'annulation de la temporisation virtuels (0–63) (Ident 0×0400) [fixe dans le logement 16]

Nom des données d'entrée API	Type de données d'entrée
Bits de retour VRCD 0–7	Octet
Bits de retour VRCD 8–15	Octet

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Retour d'informations sur le code d'actionnement 16 bits du reset et de l'annulation de la temporisation

Le logement 17 inclut une valeur de retour du code d'actionnement RCD, un mot (word) de code important utilisé dans la séquence de reset et d'annulation de la temporisation virtuels.

Référez-vous à la section Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64.

Table 72. Module Code d'actionnement du reset et de l'annulation de la temporisation (Ident 0×0401) [fixe dans le logement 17]

Nom des données d'entrée API	Type de données d'entrée
Retour d'informations sur le code d'actionnement du reset et de l'annulation de la temporisation	Non signé 16

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Entrées du journal des défauts

Le logement 18 peut être rempli par le module Mémoire tampon du journal des défauts optionnel.

Table 73. Module Mémoire tampon du journal des défauts du contrôleur de sécurité (Ident 0×0500) [optionnel ; fixe dans le logement 18 si utilisé]

Nom des données d'entrée API	Type de données d'entrée
Entrée de journal de défauts 1 (la plus récente)	15 mots (word)
Entrée de journal de défauts 2	15 mots (word)
Entrée de journal de défauts 3	15 mots (word)
Entrée de journal de défauts 4	15 mots (word)
Entrée de journal de défauts 5	15 mots (word)
Entrée de journal de défauts 6	15 mots (word)
Entrée de journal de défauts 7	15 mots (word)
Entrée de journal de défauts 8	15 mots (word)
Entrée de journal de défauts 9	15 mots (word)
Entrée de journal de défauts 10 (la plus ancienne)	15 mots (word)

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Entrée de journal de défauts	Type	Longueur en mots (word)
Horodatage	UDINT	2
Longueur du nom	DWORD	2
Chaîne de nom	String	6
Code d'erreur	WORD	1
Code d'erreur avancé	WORD	1
Index de message d'erreur	WORD	1
réservés	WORD	2

Horodatage défaut

Temps relatif, en secondes, de l'occurrence du défaut. Il est mesuré à partir du temps 0, qui correspond à la dernière mise sous tension du contrôleur de sécurité.

Longueur du nom

Nombre de caractères ASCII dans la « chaîne de nom ».

Chaîne de nom

Chaîne ASCII décrivant la source du défaut.

Code d'erreur, Code d'erreur avancé, Index de message d'erreur

Le code d'erreur plus le code d'erreur avancé constituent le code de défaut du contrôleur de sécurité. Le format du code de défaut est `Error Code 'dot' Advanced Error Code`. Par exemple le code de défaut 2.1 du contrôleur de sécurité est composé du code d'erreur `2` et du code d'erreur avancé `1`. La valeur d'index du message d'erreur est constituée du code d'erreur et du code d'erreur avancé, lequel peut être précédé d'un zéro non significatif, le cas échéant. Par exemple, le code de défaut 2.1 du contrôleur de sécurité est représenté par l'index de message d'erreur `201`. La valeur d'index du message d'erreur offre un moyen pratique d'obtenir le code de défaut complet en lisant uniquement un registre 16 bits.

Mémoire tampon des informations système

Le logement 19 peut être rempli avec le module tampon des informations système en option.

Table 74. Module tampon des informations système du contrôleur de sécurité (Ident 0×0600) [optionnel ; fixe dans le logement 19 si utilisé] Module tampon d'informations système du

Nom des données d'entrée API	Type de données d'entrée
Mémoire tampon des informations système	30 mots (word)

Nom des données de sortie API	Type de données de sortie
Sans objet	Sans objet

Mémoire tampon des informations système	Type	Longueur en mots (word)
Secondes depuis le démarrage	UDINT	2
Mode de fonctionnement	WORD	1
Longueur du nom de la config.	DWORD	2
Nom de la config.	String	8
CRC de configuration	WORD	2

Secondes depuis le démarrage

Représentation par un entier 32 bits du nombre de secondes écoulées depuis la mise sous tension du contrôleur de sécurité.

Mode de fonctionnement

Mode de fonctionnement actuel du contrôleur de sécurité.

Valeur du mode de fonctionnement	Description
1 (0×01)	Mode de fonctionnement normal (y compris les défauts d'E/S, s'ils existent)
2 (0×02)	Mode de configuration
4 (0×04)	Verrouillage du système
65 (0×41)	Attente du reset du système/Sortie du mode de configuration
129 (0×81)	Basculement en mode de configuration

Longueur du nom de la config.

Nombre de caractères ASCII dans le « nom de la config. ».

Nom de la config.

Chaîne ASCII décrivant la source du défaut.

CRC de configuration

Valeur CRC (contrôle de redondance cyclique) pour la configuration actuelle du contrôleur de sécurité.

Module Informations d'état ISD 4 chaînes

Le logement 20 peut être rempli par le module Informations d'état ISD 4 chaînes en option.

Remarque:

- Les contrôleurs de sécurité ne prennent pas tous en charge ISD.
- Seuls les modèles XS26-ISD prennent en charge plus de deux chaînes de dispositifs ISD.

Table 75. Module Informations d'état ISD 4 chaînes (Ident 0×0700) [en option ; fixe dans le logement 20 si utilisé]

Nom des données de sortie API	Type de données de sortie
Sans objet	Non signé 16

Nom des données d'entrée API	Type de données d'entrée
État système ISD – Nbre de dispositifs Chaîne 1	Non signé 32
État système ISD – Nbre de dispositifs Chaîne 2	Non signé 32
État système ISD – État On/Off des dispositifs Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État On/Off des dispositifs Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État d'alerte Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État d'alerte Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de reset Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de reset Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 1 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 2 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État système Chaîne 1 (voir État système de la chaîne ISD à la page 52)	Non signé 32
État système ISD – État système Chaîne 2 (voir État système de la chaîne ISD à la page 52)	Non signé 32
État système ISD – Nbre de dispositifs Chaîne 3	Non signé 32
État système ISD – Nbre de dispositifs Chaîne 4	Non signé 32
État système ISD – État On/Off des dispositifs Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État On/Off des dispositifs Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État d'alerte Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État d'alerte Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32

Nom des données d'entrée API	Type de données d'entrée
État système ISD – État de reset Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de reset Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 3 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 4 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État système Chaîne 3 (voir État système de la chaîne ISD à la page 52)	Non signé 32
État système ISD – État système Chaîne 4 (voir État système de la chaîne ISD à la page 52)	Non signé 32

Module Informations de dispositif ISD individuel

Le logement 21 peut être rempli par le module Informations de dispositif ISD individuel.

Voir aussi les sections Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52 et Description détaillée des données spécifiques à un dispositif ISD individuel à la page 282.

Table 76. Module Informations d'état individuel ISD (Ident 0×0800) [en option ; fixe dans le logement 21 si utilisé]

Nom des données d'entrée API	Type de données d'entrée
Accusé réc. demande de lecture ISD	Non signé 16
Accusé réc. chaîne ISD demandée	Non signé 16
Accusé réc. dispositif ISD demandé	Non signé 16
Données spécifiques à un dispositif ISD individuel (18 octets) [53]	Octet

Nom des données de sortie API	Type de données de sortie
Demande de lecture ISD	Non signé 16
Chaîne ISD demandée	Non signé 16
Dispositif ISD demandé	Non signé 16

Description détaillée des données spécifiques à un dispositif ISD individuel

Le tableau suivant décrit le logement 21 [54].

Table 77. Description détaillée des données spécifiques à un dispositif ISD individuel

Entrée du module	Informations	Taille des données
206.0	Défaut d'entrée de sécurité	1 bit
206.1	*réservé*	1 bit
206.2	Capteur non couplé	1 bit
206.3	Erreur de données ISD	1 bit
206.4	Mauvais actionneur/État du bouton/État de l'entrée	1 bit
206.5	Portée marginale/État du bouton/État de l'entrée	1 bit
206.6	Actionneur détecté	1 bit
206.7	Erreur de sortie	1 bit
207.0	Entrée 2	1 bit
207.1	Entrée 1	1 bit
207.2	Reset local attendu	1 bit

[53] Pour la conversion de la température interne, de la distance de l'actionneur et de la tension, voir la section ISD : Informations sur la conversion de la distance, tension et température à la page 309.

[54] L'exemple du logement 21 suppose que le logement commence à l'adresse %I200 de l'API. Les octets 0 à 5 sont utilisés par les registres Accusé réc. demande de lecture ISD, Accusé réc. chaîne ISD demandée et Accusé réc. dispositif ISD demandé. L'exemple suppose également que les données sont au format byte (octet).

Entrée du module	Informations	Taille des données
207.3	Avertissement de tension de fonctionnement	1 bit
207.4	Erreur de tension de fonctionnement	1 bit
207.5	Sortie 2	1 bit
207.6	Sortie 1	1 bit
207.7	Remise sous tension requise	1 bit
208.0	Sorties à tolérance de panne	1 bit
208.1	Dispositif de reset local	1 bit
208.2	En cascade	1 bit
208.3	Niveau de codage élevé	1 bit
208.7 à 208.4	Apprentissages restants	4 bits
209.4 à 209.0	ID dispositif	5 bits
210.2 à 209.5	Nombre d'avertissements de portée	6 bits
210.7 à 210.3	Délai de désactivation de la sortie	5 bits
211	Nombre d'erreurs de tension	8 bits
212	Température interne [55]	8 bits
213	Distance de l'actionneur [55]	8 bits
214	Tension d'alimentation [55]	8 bits
215.3 à 215.0	Nom de société attendu	4 bits
215.7 à 215.4	Nom de société reçu	4 bits
217 à 216	Code attendu	16 bits
219 à 218	Code reçu	16 bits
221 à 220	Erreur interne A	16 bits
223 à 222	Erreur interne B	16 bits

Module Informations d'état ISD 8 chaînes

Le logement 22 peut être rempli par le module Informations d'état ISD 8 chaînes en option.

Remarque:
- Les contrôleurs de sécurité ne prennent pas tous en charge ISD.
- Seul le XS26-ISD prend en charge plus de deux chaînes de dispositifs ISD.

Table 78. Module Informations d'état ISD 8 chaînes (Ident 0×0900) [en option ; fixe dans le logement 22 si utilisé]

Nom des données de sortie API	Type de données de sortie
Sans objet	Non signé 16

Nom des données d'entrée API	Type de données d'entrée
État système ISD – Nbre de dispositifs Chaîne 1	Non signé 32
État système ISD – État On/Off des dispositifs Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32

[55] Pour la conversion de la température interne, de la distance de l'actionneur et de la tension, voir la section ISD : Informations sur la conversion de la distance, tension et température à la page 309.

Nom des données d'entrée API	Type de données d'entrée
État système ISD – État d'alerte Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de reset Chaîne 1 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 1 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État système Chaîne 1 (voir État système de la chaîne ISD à la page 52)	Non signé 32
État système ISD – Nbre de dispositifs Chaîne 2	Non signé 32
État système ISD – État On/Off des dispositifs Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État d'alerte Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de reset Chaîne 2 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 2 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État système Chaîne 2 (voir État système de la chaîne ISD à la page 52)	Non signé 32
État système ISD – Nbre de dispositifs Chaîne 3	Non signé 32
État système ISD – État On/Off des dispositifs Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État d'alerte Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de reset Chaîne 3 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 3 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État système Chaîne 3 (voir État système de la chaîne ISD à la page 52)	Non signé 32
État système ISD – Nbre de dispositifs Chaîne 4	Non signé 32
État système ISD – État On/Off des dispositifs Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État d'alerte Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de reset Chaîne 4 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 4 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État système Chaîne 4 (voir État système de la chaîne ISD à la page 52)	Non signé 32
État système ISD – Nbre de dispositifs Chaîne 5	Non signé 32

Nom des données d'entrée API	Type de données d'entrée
État système ISD – État On/Off des dispositifs Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État d'alerte Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de reset Chaîne 5 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 5 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État système Chaîne 5 (voir État système de la chaîne ISD à la page 52)	Non signé 32
État système ISD – Nbre de dispositifs Chaîne 6	Non signé 32
État système ISD – État On/Off des dispositifs Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État d'alerte Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de reset Chaîne 6 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 6 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État système Chaîne 6 (voir État système de la chaîne ISD à la page 52)	Non signé 32
État système ISD – Nbre de dispositifs Chaîne 7	Non signé 32
État système ISD – État On/Off des dispositifs Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État d'alerte Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de reset Chaîne 7 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 7 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État système Chaîne 7 (voir État système de la chaîne ISD à la page 52)	Non signé 32
État système ISD – Nbre de dispositifs Chaîne 8	Non signé 32
État système ISD – État On/Off des dispositifs Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État de défaut Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État marginal Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État d'alerte Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32

Nom des données d'entrée API	Type de données d'entrée
État système ISD – État de reset Chaîne 8 (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – Actionneur Chaîne 8 reconnu (voir Mots (word) d'état de système ISD à la page 218)	Non signé 32
État système ISD – État système Chaîne 8 (voir État système de la chaîne ISD à la page 52)	Non signé 32

Module Informations de chaîne spécifique ISD

Le logement 23 peut être rempli par le module Informations de chaîne spécifique ISD.

Voir aussi Module Informations de dispositif ISD individuel à la page 282.

Voir aussi Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52.

Remarque: Les contrôleurs de sécurité ne prennent pas tous en charge ISD.

Table 79. Module Informations de chaîne spécifique ISD (Ident 0×0A00) [en option ; fixe dans le logement 23 si utilisé]

Nom des données d'entrée API	Type de données d'entrée
Liste des dispositifs ISD détectés sur une chaîne	Table de 32 octets

Nom des données de sortie API	Type de données de sortie
Sans objet	Non signé 16

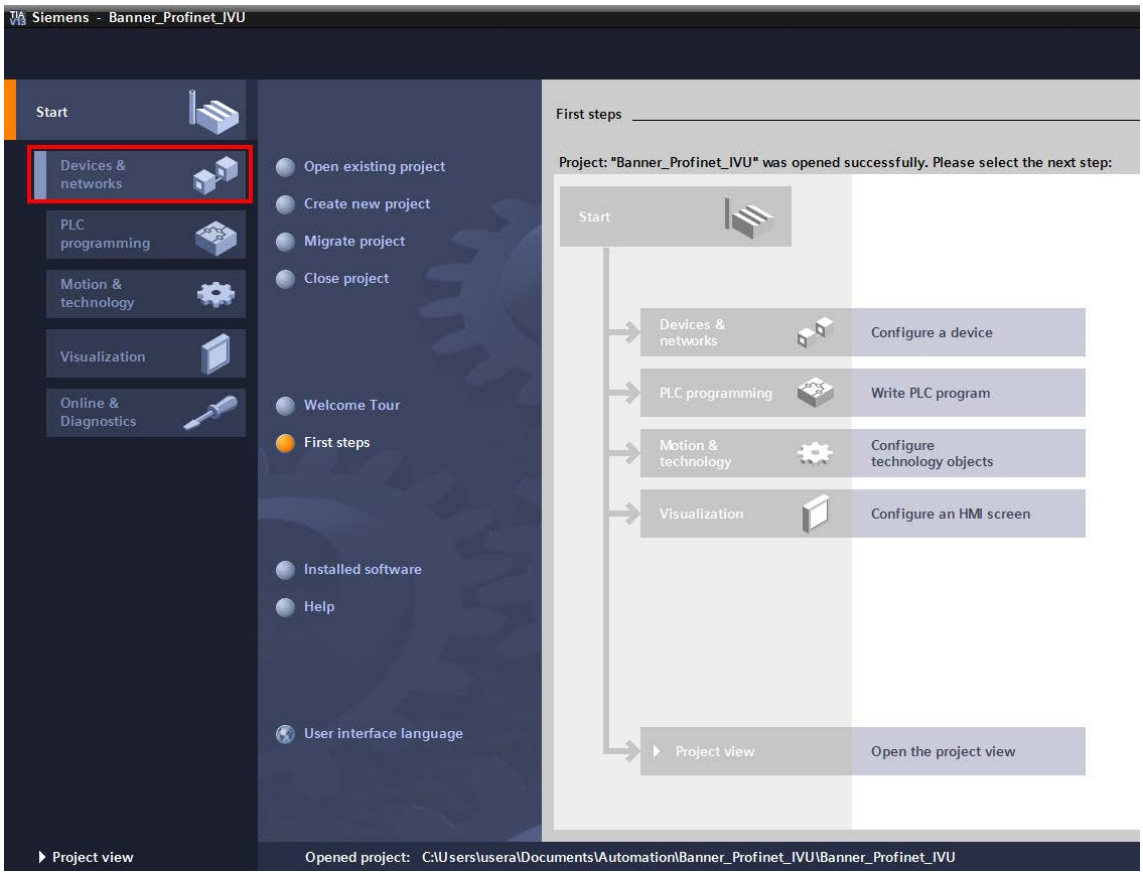
13.7.7 Instructions de configuration

Installation du fichier GSD

Utilisez ces instructions pour installer le fichier GSD dans le logiciel Siemens TIA Portal (v15 illustré). Utilisez ces instructions à titre de référence pour installer le fichier GSD sur un autre contrôleur (API).

1. Téléchargez le fichier GSD sur le site www.bannerengineering.com.
2. Lancez le logiciel Siemens TIA Portal.
3. Cliquez sur **Open existing project** (Ouvrir un projet existant).
4. Sélectionnez un projet et ouvrez-le.
5. Cliquez sur **Devices & networks** (Dispositifs et réseaux) après le chargement du projet.

Illustration 275. Option Devices and Networks



6. Cliquez sur **Configure networks** (Configurer les réseaux).

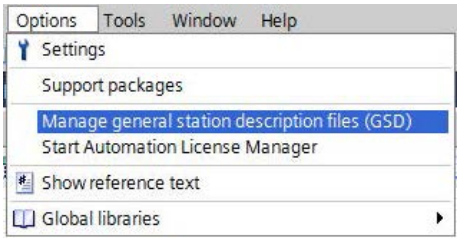
Illustration 276. Option Configure Networks



La vue **Network View** (Vue réseau) s'affiche.

7. Cliquez sur **Options** et sélectionnez **Manage general station description file (GSD)** (Gérer le fichier GSD).

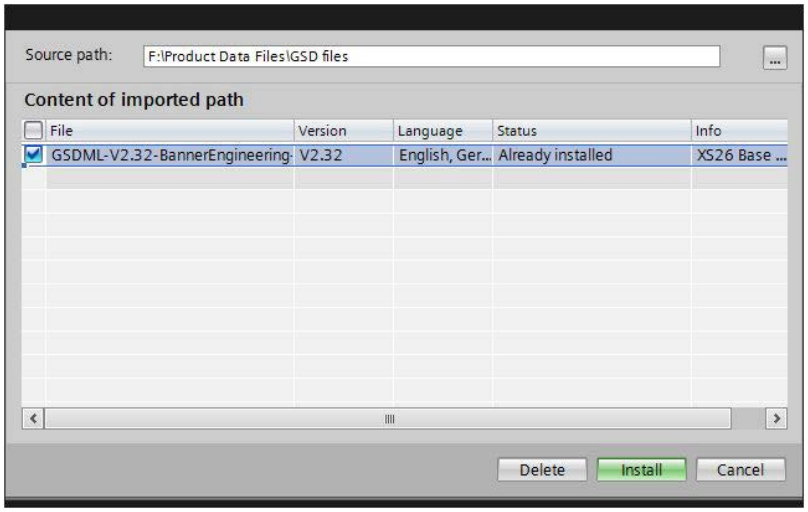
Illustration 277. Options — Installation du fichier GSD



La fenêtre **Install general station description file** (Installer le fichier GSD) s'affiche.

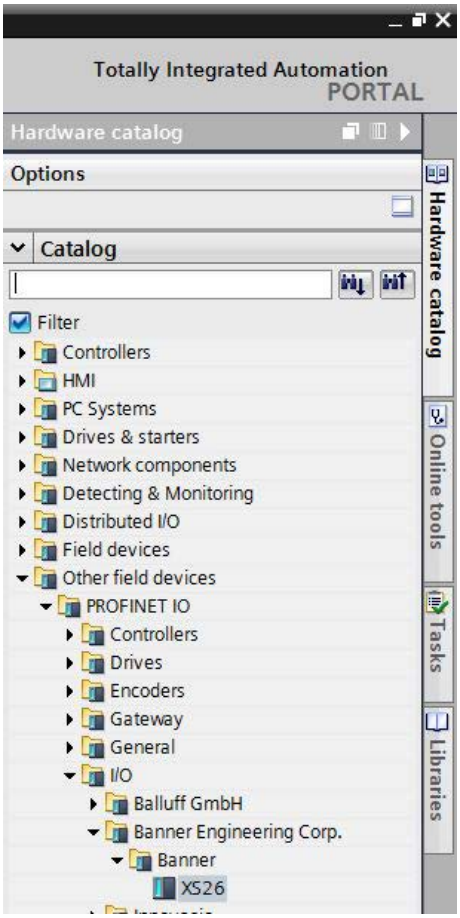
8. Cliquez sur le bouton Parcourir **(...)** à droite du champ **Source path** (Chemin de la source).

Illustration 278. Gestion des fichiers GSD



9. Accédez à l'emplacement dans lequel le fichier GSD du contrôleur de sécurité a été téléchargé.
10. Sélectionnez le fichier GSD du Contrôleur de sécurité.
11. Cliquez sur **Install** (Installer).

Illustration 279. Catalogue de matériel



12. Cliquez sur **Close** (Fermer) lorsque l'installation est terminée.
13. Cliquez sur **Devices & Networks** (Dispositifs et réseaux).
    Le système installe le fichier GSD du Contrôleur de sécurité et le place dans la section **Hardware Catalog** (Catalogue de matériel). Dans l'exemple ci-dessus, le fichier GSD du contrôleur de sécurité est situé sous **Other field devices (Autres dispositifs de terrain)** > **PROFINET IO** > **I/O** > **Banner Engineering Corp.** > **Banner**

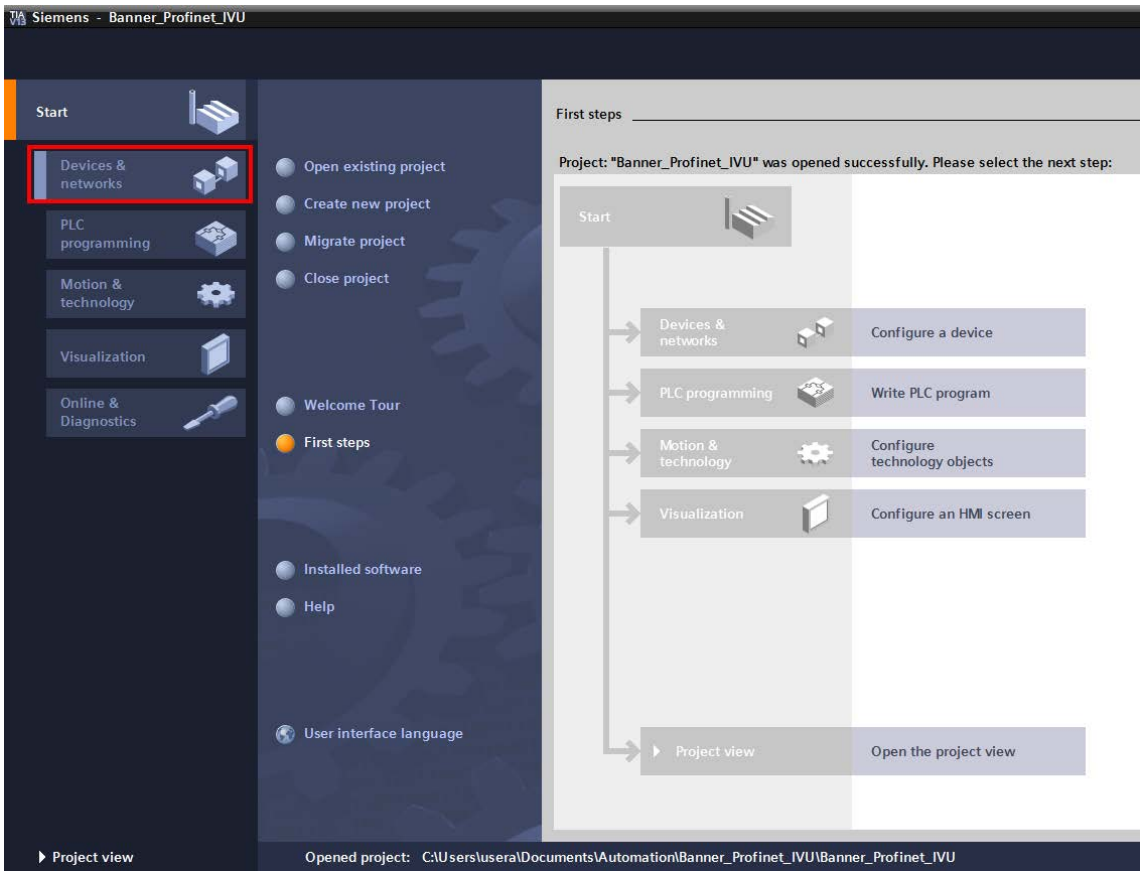
Remarque: Si le fichier GSD du Contrôleur de sécurité ne s'installe pas correctement, enregistrez le journal et contactez Banner Engineering.

Ajout d'un dispositif à un projet

Utilisez ces instructions pour ajouter un dispositif XS/SC26 à un projet Siemens TIA Portal (version 15 illustrée) et pour configurer le dispositif. Utilisez ces instructions comme base pour ajouter un dispositif XS/SC26 à un autre contrôleur (API).

1. Lancez le logiciel Siemens TIA Portal.
2. Cliquez sur **Open existing project** (Ouvrir un projet existant).
3. Sélectionnez un projet et ouvrez-le.
4. Cliquez sur **Devices & networks** (Dispositifs et réseaux) après le chargement du projet.

Illustration 280. Option Devices and Networks



5. Cliquez sur **Configure networks** (Configurer les réseaux).

Illustration 281. Option Configure Networks

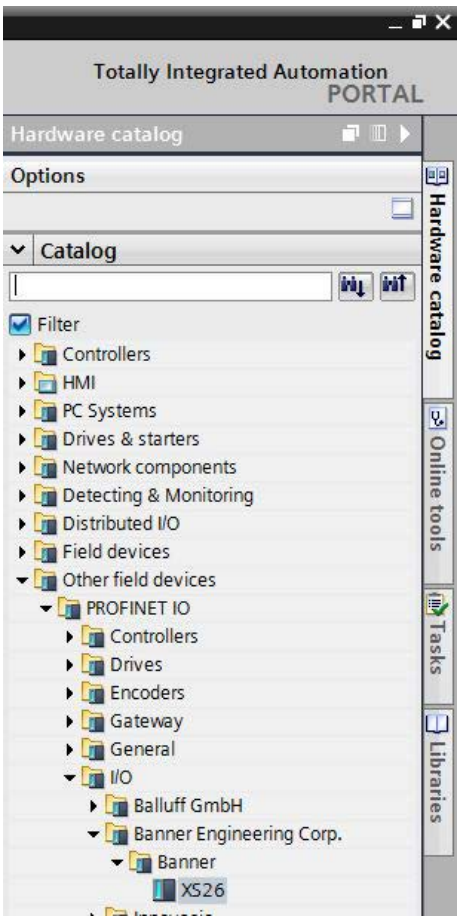


La vue **Network View** (Vue réseau) s'affiche.

Remarque: Pour les étapes 6 à 10, la vue **Network view** doit être ouverte.

6. Localisez le XS/SC26 dans le **Hardware catalog** (Catalogue de matériel).

Illustration 282. Catalogue de matériel



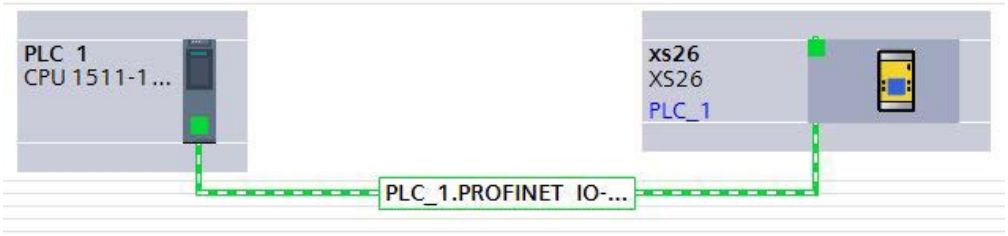
Dans l'exemple ci-dessus, le contrôleur de sécurité est situé sous **Other field devices (Autres dispositifs de terrain)** > **PROFINET IO** > **I/O** > **Banner Engineering Corp.** > **Banner**.

7. Sélectionnez le dispositif et ajoutez-le à la configuration.

Option de sélection	Description
Faire glisser	Faites glisser le Contrôleur de sécurité du **Catalogue de matériel** directement dans la configuration.
Double-clic	Double-cliquez sur le Contrôleur de sécurité et ajoutez-le à la configuration.

8. Cliquez sur le carré vert de l'icône du Contrôleur de sécurité. Faites glisser le pointeur sur le carré vert de l'icône API_1 pour connecter le dispositif au contrôleur (API).

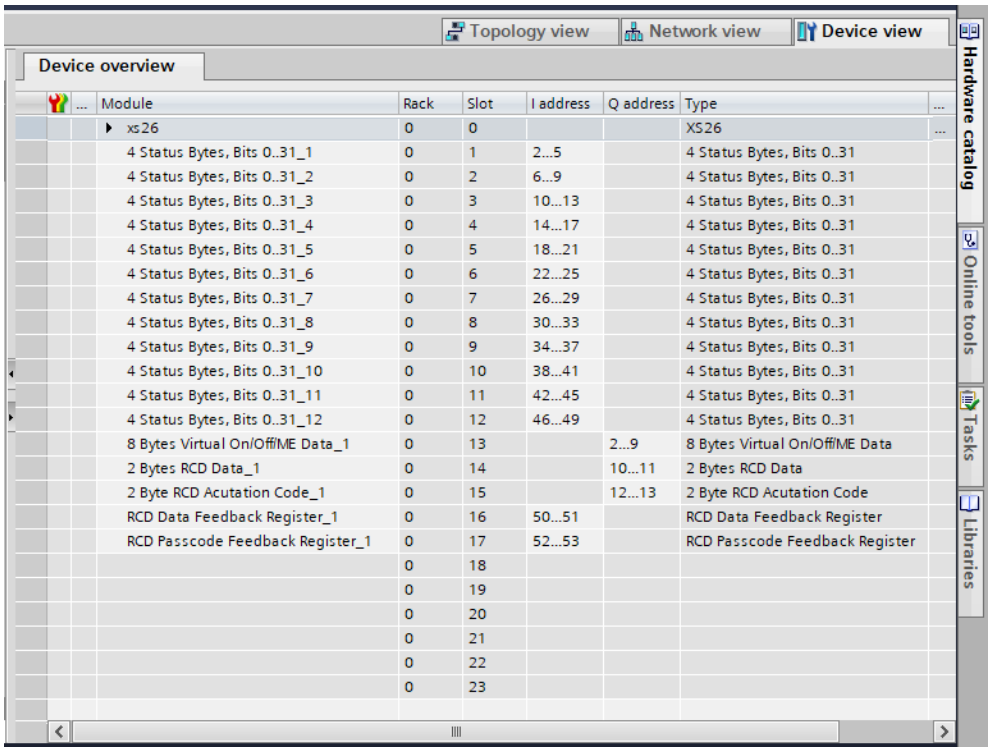
Illustration 283. Faire glisser pour se connecter



La connexion est établie.

9. Double-cliquez sur l'icône du Contrôleur de sécurité pour ouvrir la fenêtre **Device** (Dispositif).

Illustration 284. Onglet Device Overview (Aperçu des dispositifs)



Module	Rack	Slot	I address	Q address	Type
xs26	0	0			XS26
4 Status Bytes, Bits 0..31_1	0	1	2...5		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_2	0	2	6...9		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_3	0	3	10...13		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_4	0	4	14...17		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_5	0	5	18...21		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_6	0	6	22...25		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_7	0	7	26...29		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_8	0	8	30...33		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_9	0	9	34...37		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_10	0	10	38...41		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_11	0	11	42...45		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_12	0	12	46...49		4 Status Bytes, Bits 0..31
8 Bytes Virtual On/Off/ME Data_1	0	13		2...9	8 Bytes Virtual On/Off/ME Data
2 Bytes RCD Data_1	0	14		10...11	2 Bytes RCD Data
2 Byte RCD Acutation Code_1	0	15		12...13	2 Byte RCD Acutation Code
RCD Data Feedback Register_1	0	16	50...51		RCD Data Feedback Register
RCD Passcode Feedback Register_1	0	17	52...53		RCD Passcode Feedback Register
	0	18			
	0	19			
	0	20			
	0	21			
	0	22			
	0	23			

Remarque: La connexion par défaut utilise les logements 1 à 17.

10. Sélectionnez les modules ou sous-modules souhaités dans le **Catalogue de matériel** et faites-les glisser dans l'onglet **Device Overview** de l'onglet **Device view**.
    Le Contrôleur de sécurité est configuré.

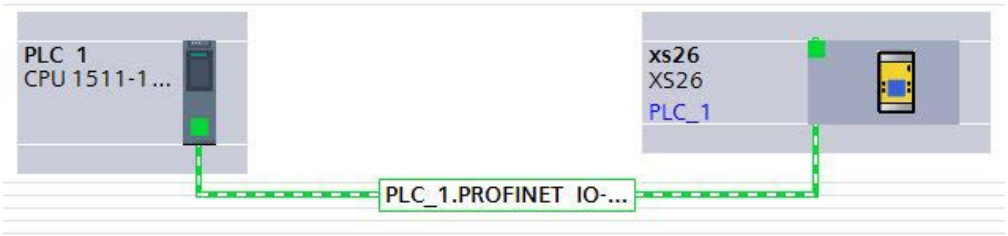
Ajout de modules en option à la configuration PROFINET

Utilisez ces instructions pour ajouter des modules XS26 en option à une configuration PROFINET existante dans le logiciel Siemens TIA Portal (v15 illustré).

Pour établir la connexion PROFINET, voir Ajout d'un dispositif à un projet à la page 289.

1. Ouvrez un projet et cliquez sur **Devices & networks** (Dispositifs et réseaux) pour accéder à la vue **Network View** (Vue réseau).

*Illustration 285. **Vue réseau***

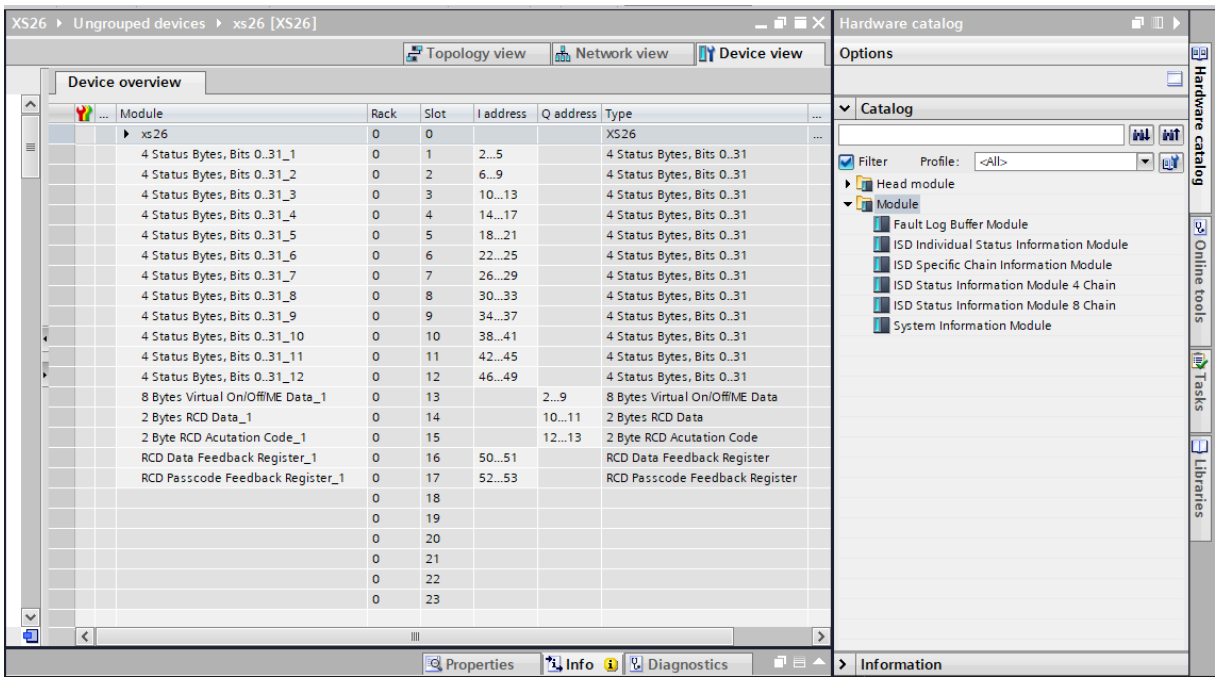


La vue **Network View** (Vue réseau) s'affiche.

2. Double-cliquez sur l'icône XS26 dans la fenêtre **Network view** pour ouvrir la fenêtre **Device overview** (Aperçu des dispositifs).
3. Cliquez sur l'onglet **Hardware catalog** (Catalogue matériel) à droite du logiciel TIA Portal, puis cliquez sur le dossier **Module**.

   Il s'agit d'une liste des modules en option disponibles pour une utilisation dans la configuration PROFINET.

*Illustration 286. **Catalogue matériel** — Dossier **Module***

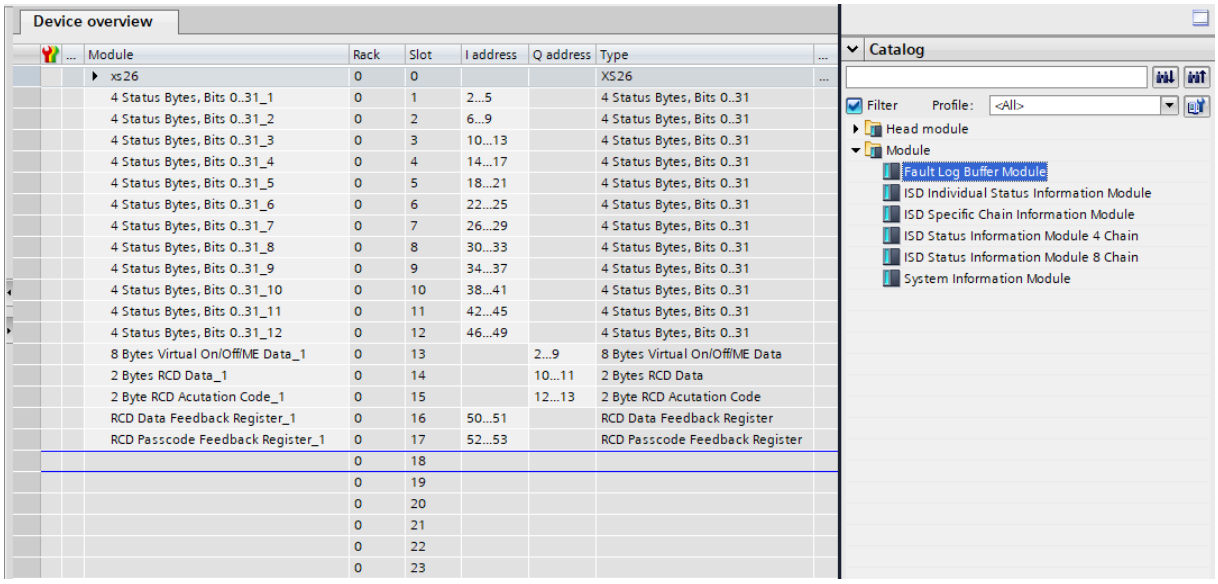


Chaque module facultatif est associé à un logement spécifique dans la configuration. Par exemple :

- Le **Module Mémoire tampon du journal des défauts** en option, par exemple, ne peut être ajouté qu'au logement 18
- Le **Module d'information de chaîne spécifique ISD** en option ne peut être ajouté qu'au logement 23
- Le **Module d'information système** en option ne peut être ajouté qu'au logement 19

4. Mettez le module en surbrillance dans le **catalogue**.
   Son logement correspondant est souligné en bleu.

*Illustration 287. **Device overview** (Aperçu des dispositifs) — Module et logement correspondant*



5. Double-cliquez sur le module dans le **catalogue** pour l'ajouter à la configuration.

Exemple de configuration

La configuration suivante utilise un large éventail de modules en option. Notez que le contrôleur d'E/S (API) a automatiquement attribué des adresses I et Q dans l'ordre dans lequel les modules ont été ajoutés à la configuration. Ces emplacements d'adresse Logement API (%I et %Q) sont nécessaires lors de la création d'un fichier XML pour PROFINET afin d'étiqueter les données.

Illustration 288. Exemple de configuration

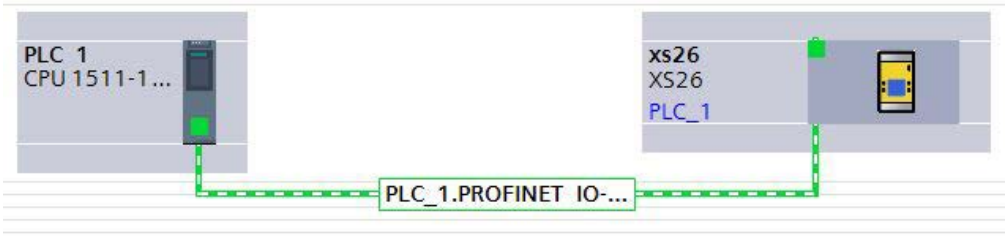
Module	Rack	Slot	I address	Q address	Type
xs26	0	0			XS26
I	0	0 X1			xs26
4 Status Bytes, Bits 0..31_1	0	1	2...5		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_2	0	2	6...9		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_3	0	3	10...13		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_4	0	4	14...17		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_5	0	5	18...21		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_6	0	6	22...25		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_7	0	7	26...29		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_8	0	8	30...33		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_9	0	9	34...37		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_10	0	10	38...41		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_11	0	11	42...45		4 Status Bytes, Bits 0..31
4 Status Bytes, Bits 0..31_12	0	12	46...49		4 Status Bytes, Bits 0..31
8 Bytes Virtual On/Off/ME Data_1	0	13		2...9	8 Bytes Virtual On/Off/ME Data
2 Bytes RCD Data_1	0	14		10...11	2 Bytes RCD Data
2 Byte RCD Acutation Code_1	0	15		12...13	2 Byte RCD Acutation Code
RCD Data Feedback Register_1	0	16	50...51		RCD Data Feedback Register
RCD Passcode Feedback Register_1	0	17	52...53		RCD Passcode Feedback Register
	0	18			
System Information Module_1	0	19	54...83		System Information Module
	0	20			
ISD Individual Status Information Module_1	0	21			ISD Individual Status Information Module
ISD Device Information Request	0	21 IS...		14...19	ISD Device Information Request
ISD Device Information Response	0	21 IS...	372...395		ISD Device Information Response
ISD Status Information Module 8 Chain_1	0	22	84...339		ISD Status Information Module 8 Chain
ISD Specific Chain Information Module_1	0	23	340...371		ISD Specific Chain Information Module

Modification du nom du dispositif

Suivez ces instructions pour modifier le nom du dispositif Contrôleur de sécurité, via le logiciel Siemens TIA Portal (v15 illustré). Utilisez ces instructions à titre de référence si vous utilisez un autre contrôleur (API).

1. Ouvrez un projet et cliquez sur **Devices & networks** (Dispositifs et réseaux) pour accéder à la vue **Network View** (Vue réseau).

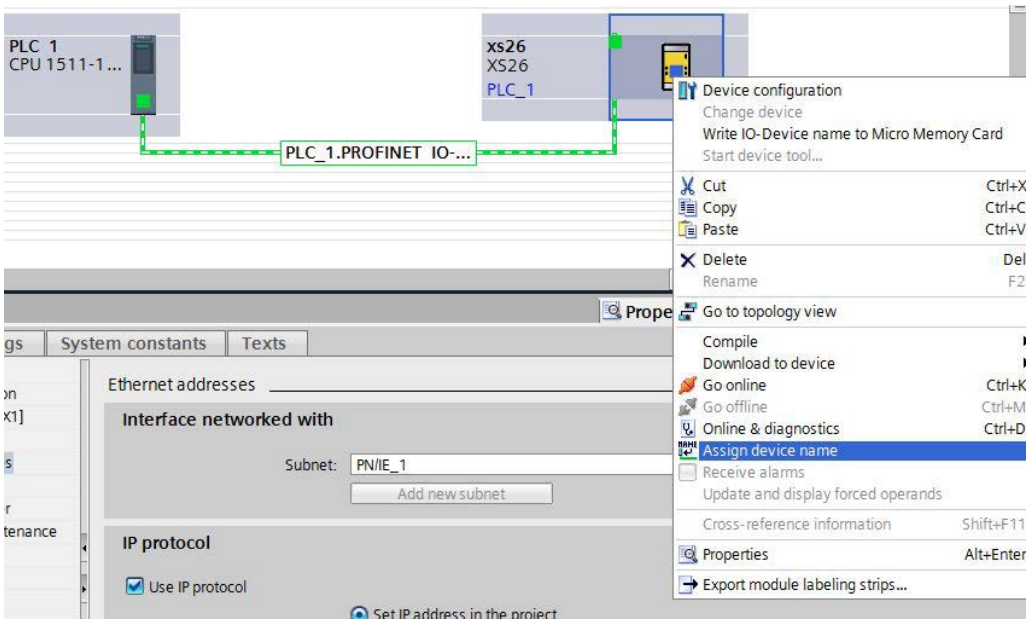
Illustration 289. Vue réseau



La vue **Network View** (Vue réseau) s'affiche.

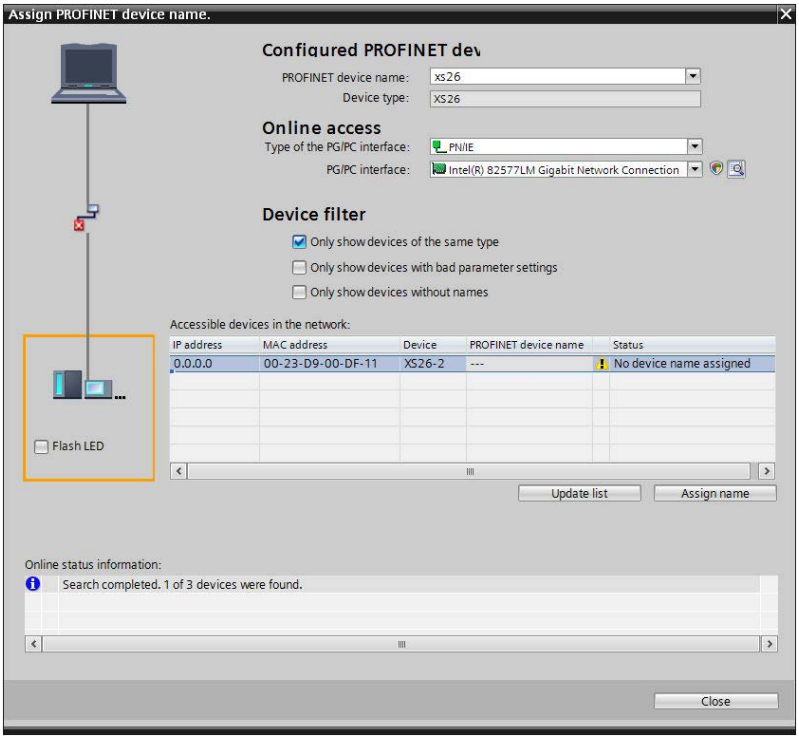
2. Cliquez avec le bouton droit sur l'icône Contrôleur de sécurité et sélectionnez **Assign device name** (Attribuer un nom au dispositif).

Illustration 290. Adresses Ethernet



La fenêtre **Assign PROFINET device name** (Attribuer un nom de dispositif PROFINET) s'affiche et le logiciel recherche des dispositifs du même type.

Illustration 291. Adresses Ethernet

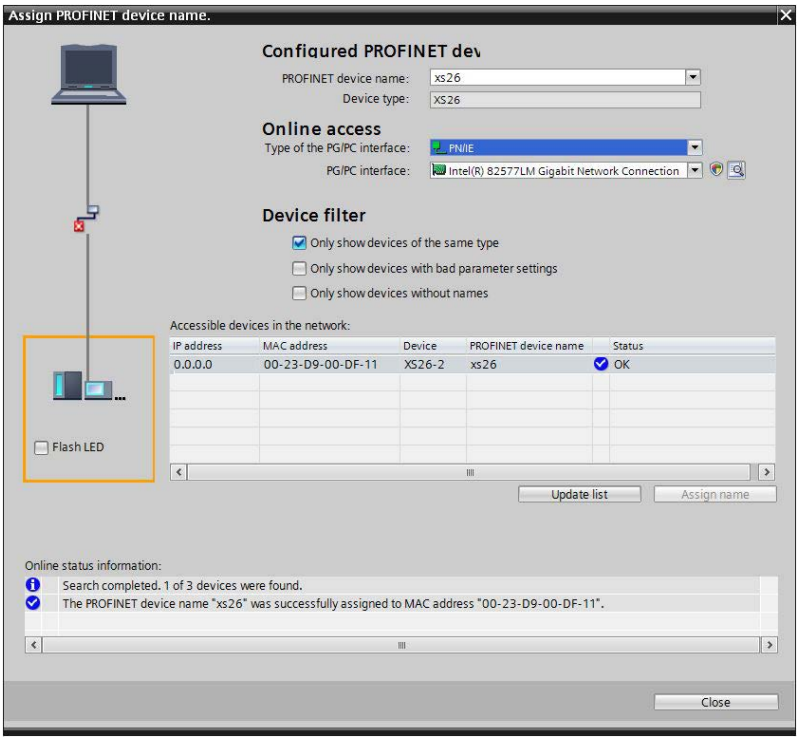


3. Indiquez le nom de votre choix dans le champ **PROFINET device name**.

Remarque: Chaque nom ne peut être utilisé qu'une seule fois.

4. Cliquez sur **Assign name** (Attribuer le nom).
   Le dispositif possède désormais un nom PROFINET.

Illustration 292. Adresses Ethernet



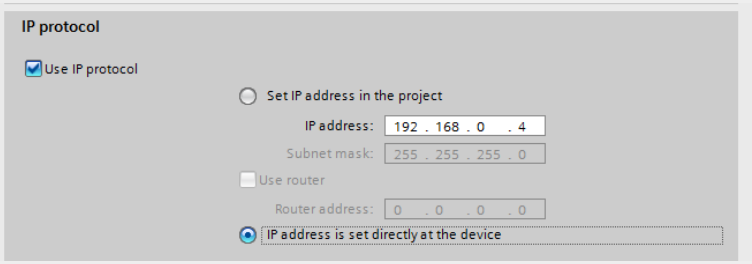
Changement de l’adresse IP du dispositif

Remarque: Les dispositifs PROFINET n'ont généralement pas d'adresse IP au démarrage (l'adresse IP ne contient que des zéros). Toutefois, les dispositifs du Contrôleur de sécurité ont besoin d’une adresse IP pour se connecter au logiciel Contrôleur de sécurité Banner et configurer le dispositif.

Par défaut, l'adresse IP 192.168.0.128 est attribuée à chaque dispositif Banner Engineering expédié de l'usine. L’adresse par défaut peut être modifiée à l’aide du logiciel Contrôleur de sécurité Banner.

Immédiatement après l’activation du protocole PROFINET dans le dispositif Banner Engineering, mais avant que l’API ne découvre et ne se connecte au dispositif Banner Engineering, le dispositif Banner Engineering conservera son adresse IP. Après la détection et la connexion de l'API au dispositif Banner Engineering, le comportement de l'adresse IP dépendra de la façon dont l'API a été configuré pour attribuer l'adresse IP du dispositif Banner Engineering. Deux options de configuration sont disponibles.

Illustration 293. Siemens TIA Portal (v15) : Options pour le protocole IP



- L'adresse IP est définie dans le projet : si l'API a pour instruction d'attribuer l'adresse IP du dispositif Banner Engineering (par exemple avec l'option **Set IP address in the project** (Définir l'adresse IP dans le projet) dans le logiciel Siemens TIA Portal), le dispositif Banner Engineering reçoit l'adresse spécifiée mais seulement après que le programme a été chargé dans l'API et est en cours d'exécution.

  Si le dispositif Banner Engineering est redémarré après sa détection et configuration par l'API, il a l'adresse IP 0.0.0.0 jusqu'à ce que l'API le redétecte et lui réattribue l'adresse IP spécifiée.

  Lorsque le dispositif Banner Engineering n’a pas d’adresse IP attribuée, il est toujours possible d’attribuer une adresse IP au dispositif Banner Engineering à l’aide du logiciel Contrôleur de sécurité Banner. Toutefois, si cette adresse diffère de celle spécifiée dans l'API, le dispositif Banner Engineering récupère l'adresse définie dans l'API dès la réactivation de ce dernier.

  Utilisez cette option pour un Contrôleur de sécurité avec FID 1–6.
- L'adresse IP est définie au niveau du dispositif : si l'API a pour instruction de laisser la configuration de l'adresse IP au dispositif Banner Engineering (par exemple à l'aide de l'option **IP address is set directly at the device** (Adresse IP définie directement au niveau du dispositif) dans le logiciel Siemens TIA Portal), le dispositif Banner Engineering conserve toujours l'adresse IP qui lui a été attribuée dans le logiciel Contrôleur de sécurité Banner.

  Il s’agit de la méthode préférée pour paramétrer l’adresse IP d’un Contrôleur de sécurité avec FID 7 ou supérieur.

Ces options de configuration respectent la norme PROFINET.

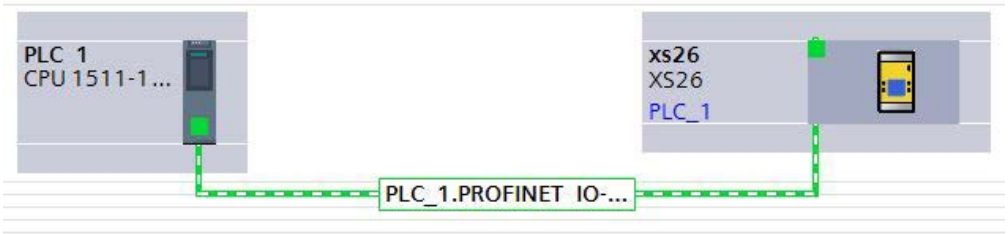
Paramétrage direct de l’adresse IP sur le dispositif

Suivez ces instructions pour modifier l’adresse IP du dispositif du Contrôleur de sécurité, via le logiciel Siemens TIA Portal (v15 illustré). Utilisez ces instructions à titre de référence si vous utilisez un autre contrôleur (API). Il s’agit de la méthode préférée pour paramétrer l’adresse IP d’un Contrôleur de sécurité avec FID 7 ou supérieur.

Configurez d’abord l’adresse IP à l’aide du logiciel Contrôleur de sécurité Banner.

1. Lancez le logiciel Siemens TIA Portal.
2. Cliquez sur **Open existing project** (Ouvrir un projet existant).
3. Sélectionnez un projet et ouvrez-le.
4. Cliquez sur **Devices & networks** (Dispositifs et réseaux) après le chargement du projet pour accéder à la vue **Network View** (Vue réseau).

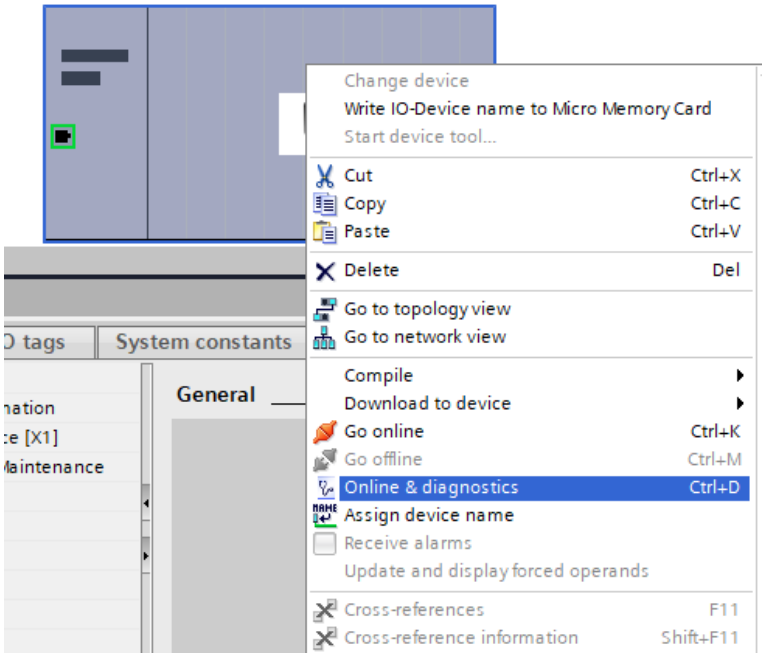
Illustration 294. Vue réseau



La vue **Network View** (Vue réseau) s'affiche.

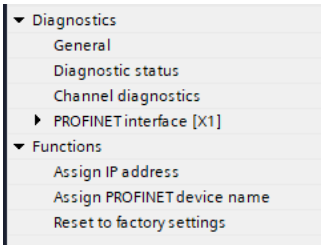
5. Double-cliquez sur l'icône du Contrôleur de sécurité pour ouvrir la vue **Device view** (Vue dispositif).
6. Cliquez sur l'icône du Contrôleur de sécurité dans la zone graphique de la vue **Device view** pour ouvrir la fenêtre **Module properties** (Propriétés du module).
   Le module peut désormais être configuré.
7. Cliquez avec le bouton droit sur l'icône du dispositif et sélectionnez **Online & diagnostics** (En ligne et diagnostic).

Illustration 295. Sélection de l'option Online & diagnostics



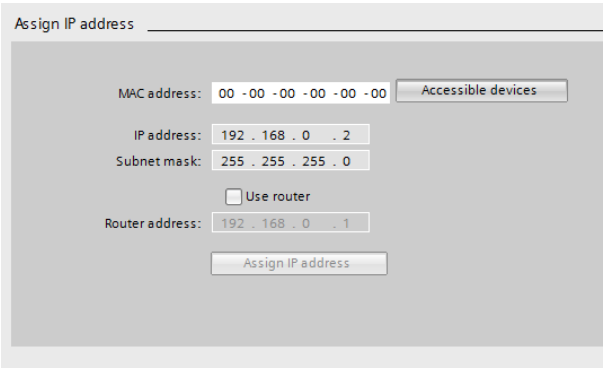
La fenêtre **Online & diagnostics** s'affiche.

Illustration 296. Online & diagnostics



8. Sélectionnez **Assign IP address** (Attribuer une adresse IP) sous **Functions** (Fonctions).
9. Cliquez sur **Accessible devices** (Dispositifs accessibles).

Illustration 297. Fenêtre Assign IP Address — Option Accessible Devices

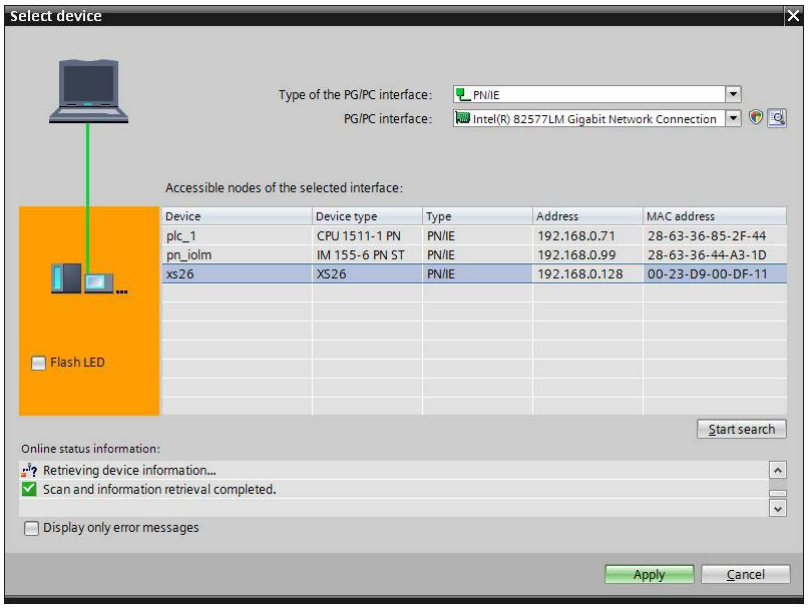


Dans la fenêtre **Select device** (Sélectionner un dispositif), le système recherche les dispositifs disponibles sur le réseau.

10. Identifiez le dispositif à modifier via l'adresse MAC et sélectionnez-le.

11. Cliquez sur **Appliquer**.

Illustration 298. Sélection du dispositif et application des modifications



L'adresse IP du dispositif est mise à jour.

12. Cliquez sur **Assign IP address** (Attribuer l'adresse IP) pour terminer l'étape.

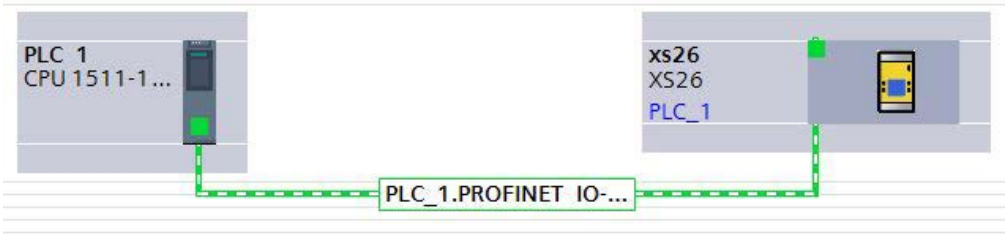
    Cette étape est effectuée pour chaque dispositif.

Sélectionnez Set IP address in the project (Définir l'adresse IP dans le projet)

Suivez ces instructions pour modifier l'adresse IP du dispositif du Contrôleur de sécurité, via le logiciel Siemens TIA Portal (v15 illustré). Utilisez ces instructions à titre de référence si vous utilisez un autre contrôleur (API). Utilisez cette option pour un Contrôleur de sécurité avec FID 1–6.

1. Lancez le logiciel Siemens TIA Portal.
2. Cliquez sur **Open existing project** (Ouvrir un projet existant).
3. Sélectionnez un projet et ouvrez-le.
4. Cliquez sur **Devices & networks** (Dispositifs et réseaux) après le chargement du projet pour accéder à la vue **Network View** (Vue réseau).

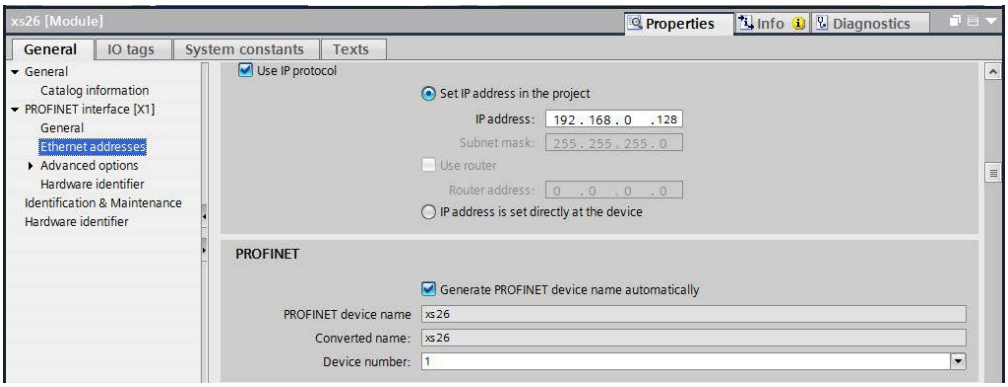
Illustration 299. Vue réseau



La vue **Network View** (Vue réseau) s'affiche.

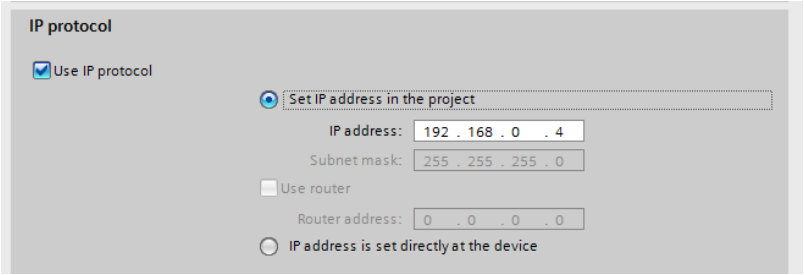
5. Double-cliquez sur l'icône du Contrôleur de sécurité pour ouvrir la vue **Device view**.
6. Cliquez sur l'icône du Contrôleur de sécurité dans la zone graphique de la vue **Device view** pour ouvrir la fenêtre **Module properties** (Propriétés du module).
   Le module peut désormais être configuré.
7. Cliquez sur **Properties** (Propriétés).
8. Cliquez sur **General** (Général).
9. Sélectionner **PROFINET Interface (Interface PROFINET)** > **Ethernet addresses (Adresses Ethernet)**.

Illustration 300. Adresses Ethernet



10. Sélectionnez **Set IP address in the project** (Définir l'adresse IP dans le projet).

Illustration 301. Définition de l'adresse IP



Le projet définit l'adresse IP du dispositif.

11. Indiquez l'adresse IP.
    L'adresse IP du dispositif est mise à jour.

13.8 EtherCAT®

EtherCAT® [57] est un protocole de communication de données pour les processus d'automatisation industriels. EtherCAT IO définit comment les contrôleurs (contrôleurs d'E/S) et les périphériques (dispositifs d'E/S) échangent les données en temps réel.

Le Contrôleur de sécurité Banner prend en charge EtherCAT IO. Le protocole EtherCAT suit la norme IEC 61158 ; le support de transmission de données est un fil de cuivre.

Remarque: Dans ce document, les sorties du dispositif Contrôleur de sécurité sont considérées comme des « entrées » vers le contrôleur (API). Les sorties du contrôleur (API) sont considérées comme des « entrées » vers le dispositif Contrôleur de sécurité.

13.8.1 EtherCAT® et les contrôleurs de sécurité

Cette section comporte des instructions pour les contrôleurs de sécurité XS/SC26 portant la désignation FID 6 ou ultérieure sur l'étiquette du produit.

La passerelle de communication EtherCAT, XSeCAT, doit être installée sur le contrôleur de sécurité.

Les données en temps réel EtherCAT sont transmises et reçues via des objets de données de processus (PDO).

Remarque: Le fichier ESI peut être téléchargé à l'adresse www.bannerengineering.com/safetycontroller.

Remarque: Avant de charger une nouvelle configuration dans un contrôleur actif sur un système EtherCAT, l'API doit basculer le module EtherCAT en état INIT ou PREOP. Cela permet d'éviter que le module ne passe en état d'erreur pendant le processus de téléchargement de la configuration qui nécessite une remise sous tension ou une autre action de l'API EtherCAT.

13.8.2 Fichier d'informations esclave EtherCAT® (ESI)

Le fichier d'informations esclave EtherCAT (ESI) contient des informations sur le module, par exemple :

57 EtherCAT® est une marque déposée et une technologie brevetée, sous licence de Beckhoff Automation GmbH, Allemagne.

- Données de configuration
- Informations de données (nombre de pièces acceptables, état du contrôle, etc.)
- Diagnostic

13.8.3 Modèle de données d'E/S EtherCAT®

Le modèle de données d'E/S EtherCAT repose sur un dispositif de terrain extensible normal équipé d'un fond de panier avec des logements.

Chaque logement est soit un Tx-PDO (objet de données de processus d'émission), soit un Rx-PDO (objet de données de processus de réception). Le Tx-PDO ou le Rx-PDO est divisé en structures de données. La majorité des données du XS/SC26 sont divisées en plusieurs PDO avec 4 octets de données. Les PDO ISD, RCD, Journal de défauts et Informations système ont des structures personnalisées.

- Un PDO est désigné comme un Tx (émission) ou un Rx (réception)
- Un PDO d'émission est utilisé pour envoyer des données au contrôleur (API)
- Un PDO de réception est utilisé pour recevoir des données du contrôleur (API)

13.8.4 Configuration du contrôleur de sécurité pour une connexion d'E/S EtherCAT®

1. Raccordez le contrôleur de sécurité au PC via le câble USB SC-USB2 ou via Ethernet (pour les modèles Ethernet XS/SC26 FID7 ou ultérieurs).
2. Ouvrez le logiciel Contrôleur de sécurité Banner et cliquez sur l'onglet **Ethernet industriel**.
3. Vérifiez que la passerelle de communication EtherCAT a été ajoutée dans l'onglet **Équipement** du fichier de projet.

   L'onglet **EtherCAT** doit s'afficher automatiquement car la passerelle de communication EtherCAT se trouve dans l'onglet **Équipement**.
4. Cliquez sur ✚ pour ajouter des informations à l'objet PDO EtherCAT. La fonction **Configuration auto** peut vous aider dans cette tâche.
5. Saisissez le mot de passe approprié pour modifier les paramètres de configuration et réseau du contrôleur de sécurité.
6. Vérifiez que le contrôleur de sécurité possède un fichier de configuration valide et confirmé.

Remarque: Si vous utilisez une séquence Reset virtuel ou Annulation de la temporisation, vous devez créer un code d'actionnement dans **Paramètres réseau**. Le code doit ensuite être envoyé au contrôleur de sécurité à l'aide du bouton **Envoyer** dans la fenêtre **Paramètres réseau**.

Remarque: L'adresse IP ClickSet n'est pas disponible pour EtherCAT.

13.8.5 Créer un fichier PLCopenXML pour EtherCAT® pour TwinCAT® 3.0

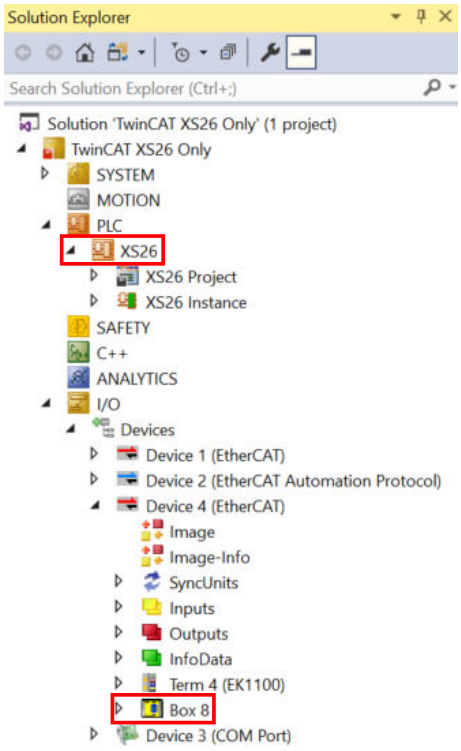
Deux éléments doivent être connus :

- Le nom du projet dans TwinCAT [62]
- Le nom du contrôleur de sécurité dans le système

Ces informations sont disponibles dans le logiciel de l'API. La figure suivante est un exemple du logiciel Beckhoff TwinCAT 3.0.

[62] TwinCAT® est une marque déposée sous licence de Beckhoff Automation GmbH, Allemagne.

Illustration 302. Explorateur de solutions



1. Dans le logiciel Contrôleur de sécurité Banner, sous l'onglet **Ethernet industriel**, assurez-vous que **EtherCAT** est sélectionné dans la liste de gauche.
2. Cliquez sur **Exporter**.
   La fenêtre **Exporter vers XML** s'ouvre.

*Illustration 303. **Exporter vers XML**— Aucune chaîne ISD*

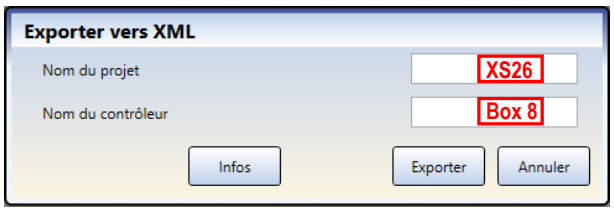
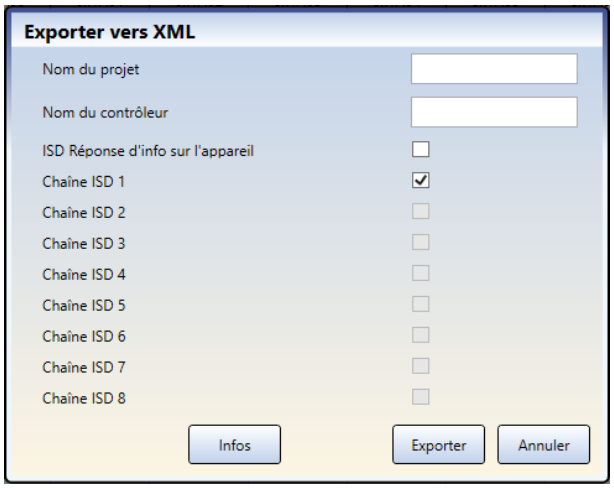


*Illustration 304. **Exporter vers XML**— avec chaînes ISD*



3. Entrez les informations dans la fenêtre.
   a) Dans le champ **Nom du projet**, saisissez le nom du projet dans le logiciel de l'API. Voir l'élément 1 dans la Illustration 303 à la page 301. Dans cet exemple, il s'agit de `XS26`.
   b) Dans le champ **Nom du contrôleur**, indiquez le nom du contrôleur de sécurité dans le logiciel de l'API. Voir l'élément 2 dans la Illustration 303 à la page 301. Dans cet exemple, il s'agit de `Box 8`.
4. Cliquez sur **Exporter**.

5. Enregistrez le fichier PLCopenXML à l'emplacement voulu.

Le fichier PLCopenXML est prêt à être directement importé dans le logiciel TwinCAT de Beckhoff ou à être ouvert avec n'importe quel logiciel capable de lire un fichier .xml.

13.8.6 Description des objets de données de processus (PDO)

Table 80. Affectation des PDO

Dans ce tableau, la direction d'E/S est envisagée à partir de l'API.

PDO	Nom	IO	Taille (octets)
1A00	VS définis par l'utilisateur TxPDO [1] 0×1A00	In	4
1A01	VS définis par l'utilisateur TxPDO [2] 0×1A01	In	4
1A02	Défauts VS TxPDO [1] 0×1A02	In	4
1A03	Défauts VS TxPDO [2] 0×1A03	In	4
1A04	Entrées VS TxPDO[1] 0×1A04	In	4
1A05	Entrées VS TxPDO[2] 0×1A05	In	4
1A06	Entrées VS TxPDO[3] 0×1A06	In	4
1A07	Entrées VS TxPDO[4] 0×1A07	In	4
1A08	Entrées VS TxPDO[5] 0×1A08	In	4
1A09	Sorties VS TxPDO[1] 0×1A09	In	4
1A0A	Sorties VS TxPDO[2] 0×1A0A	In	4
1A0B	Sorties VS TxPDO[3] 0×1A0B	In	4
1A0C	Retour d'infos sur le reset, annulation de la temporisation TxPDO 0×1A0C	In	4
1A10	Réponse à une demande d'information sur un dispositif ISD 0×1A10 [64]	In	56
1A20	État système de la chaîne ISD 1 TxPDO 0×1A20 [64]	In	32
1A3A	État du module ECAT TxPDO 0x1A3A	In	4
1600	On/Off, activation de l'inhibition VI RxPDO [1] 0×1600	Out	4
1601	On/Off, activation de l'inhibition VI RxPDO [2] 0×1601	Out	4
1602	Commande de reset et d'annulation de temporisation RxPDO 0×1610	Out	4
1610	Demande d'informations sur un dispositif ISD RxPDO 0×1610 [64]	Out	6

Bits d'état définis par l'utilisateur

PDO 1 et PDO 2 sont remplis d'objets de données de process de bits d'état définis par l'utilisateur (PDO). Ces PDO incluent 64 bits d'informations de sortie d'état virtuelle de tout type.

Table 81. VS définis par l'utilisateur TxPDO [1] 0×1A00

Nom des données d'entrée API	Type de données d'entrée
VS définis par l'utilisateur TxPDO [1] 0×1A00 Octet 0	OCTET
VS définis par l'utilisateur TxPDO [1] 0×1A00 Octet 1	OCTET
VS définis par l'utilisateur TxPDO [1] 0×1A00 Octet 2	OCTET
VS définis par l'utilisateur TxPDO [1] 0×1A00 Octet 3	OCTET

Table 82. VS définis par l'utilisateur TxPDO [2] 0×1A01

Nom des données d'entrée API	Type de données d'entrée
VS définis par l'utilisateur TxPDO [2] 0×1A01 Octet 0	OCTET

[64] Cette affectation PDO est désactivée par défaut.

Nom des données d'entrée API	Type de données d’entrée
VS définis par l’utilisateur TxPDO [2] 0×1A01 Octet 1	OCTET
VS définis par l’utilisateur TxPDO [2] 0×1A01 Octet 2	OCTET
VS définis par l’utilisateur TxPDO [2] 0×1A01 Octet 3	OCTET

Bits de défaut

Les objets PDO 3 et 4 sont remplis avec 64 bits d'informations de sortie d'état virtuelle de type Défaut envoyés par le contrôleur de sécurité.

Table 83. Défauts VS TxPDO [1] 0×1A02

Nom des données d'entrée API	Type de données d’entrée
Défauts VS TxPDO [1] 0×1A02 Octet 0	OCTET
Défauts VS TxPDO [1] 0×1A02 Octet 1	OCTET
Défauts VS TxPDO [1] 0×1A02 Octet 2	OCTET
Défauts VS TxPDO [1] 0×1A02 Octet 3	OCTET

Table 84. Défauts VS TxPDO [2] 0×1A03

Nom des données d'entrée API	Type de données d’entrée
Défauts VS TxPDO [2] 0×1A03 Octet 0	OCTET
Défauts VS TxPDO [2] 0×1A03 Octet 1	OCTET
Défauts VS TxPDO [2] 0×1A03 Octet 2	OCTET
Défauts VS TxPDO [2] 0×1A03 Octet 3	OCTET

Bits d'état d’entrée

Les PDO 5 à 9 sont toujours réservés pour 160 bits d'informations d'entrée du contrôleur de sécurité. Un contrôleur de sécurité extensible peut avoir jusqu'à 154 entrées, si les 8 cartes d'extension possibles sont utilisées comme entrées 16 voies (en plus des 26 entrées intégrées du contrôleur de base).

Table 85. Entrées VS TxPDO [1] 0×1A04

Nom des données d'entrée API	Type de données d’entrée
Entrées VS TxPDO [1] 0×1A04 Octet 0	OCTET
Entrées VS TxPDO [1] 0×1A04 Octet 1	OCTET
Entrées VS TxPDO [1] 0×1A04 Octet 2	OCTET
Entrées VS TxPDO [1] 0×1A04 Octet 3	OCTET

Table 86. Entrées VS TxPDO [2] 0×1A05

Nom des données d'entrée API	Type de données d’entrée
Entrées VS TxPDO [2] 0×1A05 Octet 0	OCTET
Entrées VS TxPDO [2] 0×1A05 Octet 1	OCTET
Entrées VS TxPDO [2] 0×1A05 Octet 2	OCTET
Entrées VS TxPDO [2] 0×1A05 Octet 3	OCTET

Table 87. Entrées VS TxPDO [3] 0×1A06

Nom des données d'entrée API	Type de données d’entrée
Entrées VS TxPDO [3] 0×1A06 Octet 0	OCTET
Entrées VS TxPDO [3] 0×1A06 Octet 1	OCTET
Entrées VS TxPDO [3] 0×1A06 Octet 2	OCTET
Entrées VS TxPDO [3] 0×1A06 Octet 3	OCTET

Table 88. Entrées VS TxPDO [4] 0×1A07

Nom des données d'entrée API	Type de données d'entrée
Entrées VS TxPDO [4] 0×1A07 Octet 0	OCTET
Entrées VS TxPDO [4] 0×1A07 Octet 1	OCTET
Entrées VS TxPDO [4] 0×1A07 Octet 2	OCTET
Entrées VS TxPDO [4] 0×1A07 Octet 3	OCTET

Table 89. Entrées VS TxPDO [5] 0×1A08

Nom des données d'entrée API	Type de données d'entrée
Entrées VS TxPDO [5] 0×1A08 Octet 0	OCTET
Entrées VS TxPDO [5] 0×1A08 Octet 1	OCTET
Entrées VS TxPDO [5] 0×1A08 Octet 2	OCTET
Entrées VS TxPDO [5] 0×1A08 Octet 3	OCTET

Bits d'état de sortie

Les PDO 10 à 12 sont réservés pour 96 bits de sortie d'état virtuel de type sortie du contrôleur de sécurité.

Table 90. Sorties VS TxPDO [1] 0×1A09

Nom des données d'entrée API	Type de données d'entrée
Sorties VS TxPDO [1] 0×1A09 Octet 0	OCTET
Sorties VS TxPDO [1] 0×1A09 Octet 1	OCTET
Sorties VS TxPDO [1] 0×1A09 Octet 2	OCTET
Sorties VS TxPDO [1] 0×1A09 Octet 3	OCTET

Table 91. Sorties VS TxPDO [2] 0×1A0A

Nom des données d'entrée API	Type de données d'entrée
Sorties VS TxPDO [2] 0×1A0A Octet 0	OCTET
Sorties VS TxPDO [2] 0×1A0A Octet 1	OCTET
Sorties VS TxPDO [2] 0×1A0A Octet 2	OCTET
Sorties VS TxPDO [2] 0×1A0A Octet 3	OCTET

Table 92. Sorties VS TxPDO [3] 0×1A0B

Nom des données d'entrée API	Type de données d'entrée
Sorties VS TxPDO [3] 0×1A0B Octet 0	OCTET
Sorties VS TxPDO [3] 0×1A0B Octet 1	OCTET
Sorties VS TxPDO [3] 0×1A0B Octet 2	OCTET
Sorties VS TxPDO [3] 0×1A0B Octet 3	OCTET

Retour d'informations sur le reset et l'annulation de la temporisation virtuels

Le PDO 13 contient le retour d'informations sur le code d'actionnement RCD ainsi que 16 entrées auxiliaires virtuelles. Ils sont utilisés dans la séquence de reset et d'annulation de la temporisation virtuels.

Référez-vous à la section Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64.

Table 93. Reset et annulation de la temporisation virtuels

Nom des données d'entrée API	Type de données d'entrée
Retour d'informations sur le code d'actionnement RCD	UINT
Retour d'informations sur le reset et l'annulation de la temporisation TxPDO [1] 0×1A0C Octet 0	OCTET

Nom des données d'entrée API	Type de données d'entrée
Retour d'informations sur le reset et l'annulation de la temporisation TxPDO [1] 0×1A0C Octet 1	OCTET

Réponse aux demandes d'informations sur un dispositif ISD

L'objet PDO 14 contient les données de réponse pour la communication avec un dispositif ISD individuel.

Voir aussi les sections Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52 et Description détaillée des données spécifiques à un dispositif ISD individuel à la page 214.

Table 94. Réponse aux demandes d'informations sur un dispositif ISD

Nom des données d'entrée API	Type de données d'entrée
Accusé de réception ISD	UINT
Accusé de réception de la chaîne ISD	UINT
Accusé de réception du dispositif ISD	UINT
Informations sur le dispositif ISD [66]	ARRAY[0..17] de BYTE (TABLEAU[0..17] d'OCTETS)
Dispositif détecté [0–15] dans une chaîne	ARRAY[0..15] de BYTE (TABLEAU[0..15] d'OCTETS)
Dispositif détecté [16–31] dans une chaîne	ARRAY[0..15] de BYTE (TABLEAU[0..15] d'OCTETS)

Description détaillée des données spécifiques à un dispositif ISD individuel

Indique le format de données pour le nom des données d'entrée API : Informations sur un dispositif ISD.

Référez-vous à la section Réponse aux demandes d'informations sur un dispositif ISD à la page 305.

Table 95. Données spécifiques à un dispositif ISD individuel

Informations	Byte.Word	Taille des données
Défaut d'entrée de sécurité	0.0	1 bit
réservé	0.1	1 bit
Capteur non couplé	0.2	1 bit
Erreur de données ISD	0.3	1 bit
Mauvais actionneur/État du bouton/État de l'entrée	0.4	1 bit
Portée marginale/État du bouton/État de l'entrée	0.5	1 bit
Actionneur détecté	0.6	1 bit
Erreur de sortie	0.7	1 bit
Entrée 2	1.0	1 bit
Entrée 1	1.1	1 bit
Reset local attendu	1.2	1 bit
Avertissement de tension de fonctionnement	1.3	1 bit
Erreur de tension de fonctionnement	1.4	1 bit
Sortie 2	1.5	1 bit
Sortie 1	1.6	1 bit
Remise sous tension requise	1.7	1 bit
Sorties à tolérance de panne	2.0	1 bit
Dispositif de reset local	2.1	1 bit
En cascade	2.2	1 bit
Niveau de codage élevé	2.3	1 bit

[66] Pour le format des données, voir Description détaillée des données spécifiques à un dispositif ISD individuel à la page 305.

Informations	Byte.Word	Taille des données
Apprentissages restants	2.7 à 2.4	4 bits
ID dispositif	3.4 à 3.0	5 bits
Nombre d'avertissements de portée	4.2 à 3.5	6 bits
Délai de désactivation de la sortie	4.7 à 4.3	5 bits
Nombre d'erreurs de tension	5	8 bits
Température interne	6	8 bits
Distance de l'actionneur	7	8 bits
Tension d'alimentation	8	8 bits
Nom de société attendu	9.3 à 9.0	4 bits
Nom de société reçu	9.7 à 9.4	4 bits
Code attendu	11 à 10	16 bits
Code reçu	13 à 12	16 bits
Erreur interne A	15 à 14	16 bits
Erreur interne B	17 à 16	16 bits

État système de la chaîne ISD – 8 chaînes

Les objets PDO 15 à PDO 22 couvrent les données spécifiques à une chaîne ISD individuelle. Chaque chaîne possède ses propres données.

Table 96. État de la chaîne ISD individuelle

Nom des données d'entrée API	Type de données d'entrée
Nombre d'entrées dans la chaîne n°	UDINT
État de la chaîne n° [67]	ARRAY[0..27] de BYTE (TABLEAU[0..27] d'OCTETS)

État de la chaîne n° - Description détaillée spécifique

Indique le format de données pour le nom des données d'entrée de l'API : État de la chaîne n°.

Référez-vous à la section État système de la chaîne ISD – 8 chaînes à la page 306.

Table 97. Données d'une chaîne individuelle ISD

Informations	Taille des données
Nombre de dispositifs Chaîne n°	32 bits
Dispositif On/Off Chaîne n° (voir Mots (word) d'état de système ISD à la page 218)	32 bits
État de défaut Chaîne n° (voir Mots (word) d'état de système ISD à la page 218)	32 bits
État marginal Chaîne n° (voir Mots (word) d'état de système ISD à la page 218)	32 bits
État d'alerte Chaîne n° (voir Mots (word) d'état de système ISD à la page 218)	32 bits
État de reset Chaîne n° (voir Mots (word) d'état de système ISD à la page 218)	32 bits
Actionneur Chaîne n° reconnu (voir Mots (word) d'état de système ISD à la page 218)	32 bits
État système Chaîne n° (voir État système de la chaîne ISD à la page 52)	32 bits

État du module EtherCAT

Nom des données d'entrée API	Type de données d'entrée
État du module ECAT	UINT
Mode de fonctionnement	UINT

[67] Pour le format des données, voir État de la chaîne n° - Description détaillée spécifique à la page 306.

Bits de marche/arrêt (on/off) et d'activation de l'inhibition virtuels

Le PDO 25 est occupé par 64 entrées auxiliaires de sécurité, à utiliser comme entrées de marche/arrêt (on/off) virtuelles (vers le contrôleur de sécurité) ou entrées d'activation de l'inhibition (ME) virtuelles (vers le contrôleur de sécurité).

Table 98. Bits de marche/arrêt (on/off) et d'activation de l'inhibition virtuels 0x1600

Nom des données de sortie API	Type de données de sortie
On/Off, activation de l'inhibition VI RxPDO [1] 0×1600 Octet 0	OCTET
On/Off, activation de l'inhibition VI RxPDO [1] 0×1600 Octet 1	OCTET
On/Off, activation de l'inhibition VI RxPDO [1] 0×1600 Octet 2	OCTET
On/Off, activation de l'inhibition VI RxPDO [1] 0×1600 Octet 3	OCTET

Table 99. Bits de marche/arrêt (on/off) et d'activation de l'inhibition virtuels 0x1601

Nom des données de sortie API	Type de données de sortie
On/Off, activation de l'inhibition VI RxPDO [2] 0×1601 Octet 0	OCTET
On/Off, activation de l'inhibition VI RxPDO [2] 0×1601 Octet 1	OCTET
On/Off, activation de l'inhibition VI RxPDO [2] 0×1601 Octet 2	OCTET
On/Off, activation de l'inhibition VI RxPDO [2] 0×1601 Octet 3	OCTET

Commande de reset et d'annulation de la temporisation virtuels

Le PDO 26 inclut le code d'actionnement RCD, un mot (word) de code important utilisé dans la séquence de reset et d'annulation de la temporisation virtuels.

Référez-vous à la section Séquence de reset manuel et d'annulation de la temporisation (RCD) virtuels à la page 64. Ce PDO contient également seize entrées auxiliaires virtuelles, à utiliser dans la séquence de reset et d'annulation de la temporisation virtuels.

Table 100. Commande RCD

Nom des données de sortie API	Type de données de sortie
Code d'actionnement RCD	UDINT
Commande de reset et d'annulation de temporisation RxPDO [1] 0×1602 octet 0	OCTET
Commande de reset et d'annulation de temporisation RxPDO [1] 0×1602 octet 1	OCTET

Demande d'informations sur un dispositif ISD individuel

PDO 27 contient les données de réponse pour la communication avec un dispositif ISD individuel.

Voir aussi les sections Demande d'informations d'état et de performance sur un dispositif individuel via ISD à la page 52 et Description détaillée des données spécifiques à un dispositif ISD individuel à la page 214.

Table 101. Demande d'informations sur un dispositif ISD individuel

Nom des données de sortie API	Type de données de sortie
Demande de lecture ISD	UINT
Chaîne ISD demandée	UINT
Dispositif ISD demandé	UINT

13.8.7 Instructions de configuration

Installation du fichier ESI

Suivez ces instructions pour installer le fichier ESI dans le logiciel Beckhoff TwinCAT 3.

1. Téléchargez le fichier ESI sur le site www.bannerengineering.com.
2. Accédez au dossier `TwinCAT/3.1/Config/Io/EtherCAT`.
3. Déplacez le fichier ESI dans ce dossier.
   Le fichier ESI sera disponible dans TwinCAT au prochain démarrage du programme.

Ajout du contrôleur de sécurité à un projet

Utilisez ces instructions pour ajouter un dispositif XS/SC26 à un projet TwinCAT.

1. Démarrez le logiciel TwinCAT 3.
2. Ouvrez un projet.
3. Développez la sélection des E/S.
4. Cliquez avec le bouton droit sur le dispositif dont le Contrôleur de sécurité Banner fera partie.
5. Sélectionnez l'option **Add New Item (Ajouter un nouvel élément)**.
   « Banner Engineering Corporation » sera repris dans la liste. Vous pouvez également utiliser la fonction de recherche et entrer `XS26` pour sélectionner rapidement l'ESI.
6. Sélectionnez le **module EtherCAT XS26**.
7. Modifiez le **nom** de la façon requise pour le système.
8. Cliquez sur **OK** pour ajouter le contrôleur de sécurité au système.

13.8.8 Modification du PDO EtherCAT®

Le PDO EtherCAT peut être modifié. Par défaut, seul un ensemble spécifique de données est activé.

Il est possible d'activer les PDO actuellement désactivés, tout comme il est possible de désactiver les PDO actuellement activés.. Le réglage du PDO permet d'envoyer et de recevoir uniquement les données nécessaires à l'application.

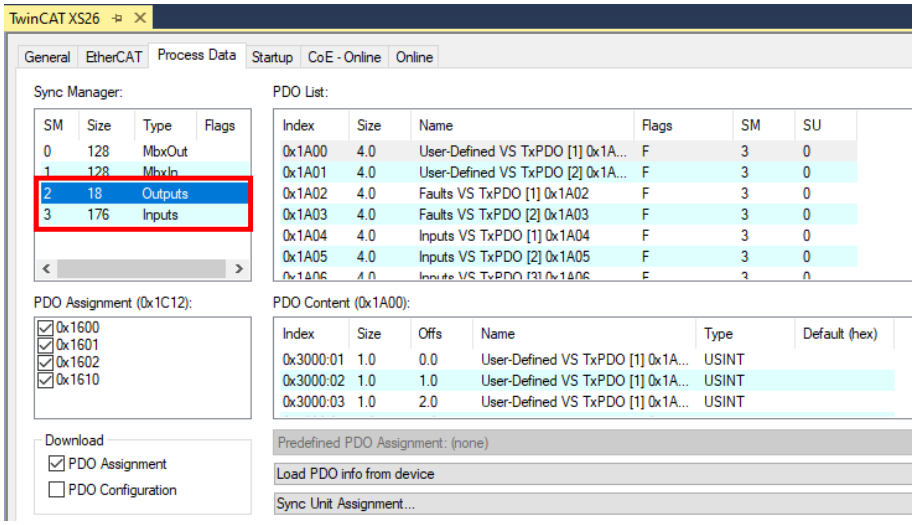
Plus le PDO est petit, plus il est facile de l'intégrer à la taille de paquet allouée à EtherCAT.

Suivez les instructions suivantes pour activer et désactiver les PDO selon les besoins.

Accès au menu PDO

1. Dans l'explorateur de solutions TwinCAT, double-cliquez sur le contrôleur de sécurité Banner dans l'arborescence d'E/S.
   Une nouvelle fenêtre s'ouvre. L'onglet **Général** est actif par défaut.
2. Cliquez sur l'onglet **Données de processus**.
   Il s'agit de l'onglet qui permet d'activer et de désactiver le PDO.
3. Notez les sorties et les entrées dans le volet **Sync Manager**.

Illustration 305. Sortie et entrées dans Sync Manager



Désactivation d'un PDO

Cet exemple de procédure désactive un PDO de sortie.

1. Dans le volet **Sync Manager** de TwinCAT, sélectionnez **Outputs** (Sorties) ou **Inputs** (Entrées).
2. Examinez le volet **PDO Assignment** (Affectation de PDO) pour les sorties.
3. Décochez la case de l'élément que vous souhaitez désactiver.
   Cet exemple désactive PDO 0×1610 (demande d'informations sur un dispositif ISD).

Illustration 306. PDO Assignment (Attribution PDO) — Toutes les sorties sélectionnées

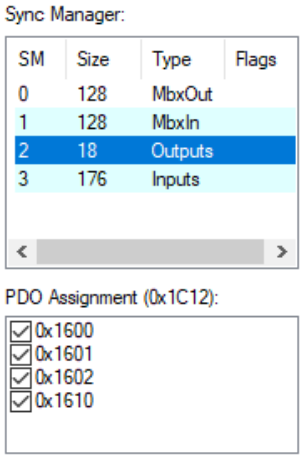
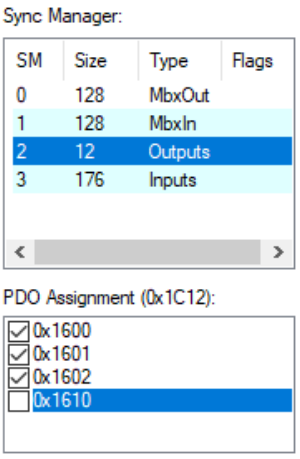


Illustration 307. PDO Assignment (Attribution PDO) — 0×1610 décoché



4. Répétez ce processus si nécessaire pour tous les éléments qui doivent être désactivés.

Activation d'un PDO

Cet exemple illustre la procédure d'activation d'un PDO (Process Data Object) d'entrée.

1. Dans le volet **Sync Manager** de TwinCAT, sélectionnez **Sorties** ou **Entrées**.
2. Examinez le volet **PDO Assignment** (Attribution de PDO) pour les entrées.
3. Cochez la case correspondant à l'élément ou aux éléments que vous souhaitez activer.
   Cet exemple active les PDO 0×1A20 et 0×1A21 (État ISD Chaîne 1 et État ISD Chaîne 2).

Illustration 308. Attribution de PDO — Toutes les entrées sont effacées

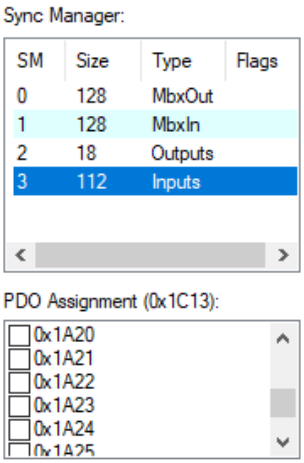
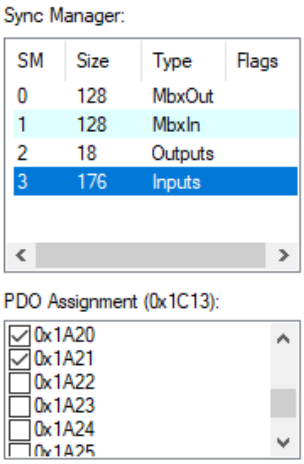


Illustration 309. Attribution de PDO — Deux entrées sont sélectionnées



13.9 ISD : Informations complémentaires

13.9.1 ISD : Informations sur la conversion de la distance, tension et température

Téléchargez un fichier AOI (Add-On Instruction) sur le site www.bannerengineering.com à insérer dans le programme de l'API pour effectuer la conversion des valeurs obtenues en valeurs réelles.

ISD : Tension d'alimentation

Pour obtenir la tension réelle à partir de la valeur de conversion analogique-numérique (ADC) envoyée à l'API, multipliez la valeur ADC par 0,1835.

Tension d'alimentation = Valeur ADC × 0,1835

ISD : Température interne

Commencez par décaler la valeur de conversion analogique-numérique (ADC) de 2 bits vers la gauche. Ensuite, convertissez la valeur binaire en nombre. Si le nombre correspond à une valeur ADC du tableau suivant, lisez la température. Si le nombre est compris entre les valeurs du tableau, utilisez la formule suivante pour obtenir la température réelle.

```
Température interne = ((A–L) / (H–L)) × 5 + T
```

A

Valeur ADC obtenue du contrôleur

L

Valeur ADC dans la table de recherche inférieure ou égale à A

H

Valeur ADC dans la table de recherche supérieure à A

T

Température associée à la valeur L

Table 102. Température

Valeur ADC	Température (°C)
41	-40
54	-35
69	-30
88	-25
110	-20
136	-15
165	-10
199	-5
237	0
278	5
321	10
367	15
414	20
461	25
508	30
554	35
598	40
640	45
679	50
715	55
748	60
778	65
804	70
829	75
850	80
869	85
886	90
901	95
914	100
926	105
936	110

ISD : Distance de l'actionneur

Convertissez la valeur binaire en nombre. Si le nombre correspond à une valeur de conversion analogique en numérique (ADC) du tableau suivant, lisez la distance. Si le nombre est compris entre les valeurs du tableau, utilisez la formule suivante pour obtenir la distance réelle.

```
Distance de l'actionneur = ((A-L) / (H-L)) + D
```

A

Valeur ADC obtenue du contrôleur

L

Valeur ADC dans la table de recherche inférieure ou égale à A

H

Valeur ADC dans la table de recherche supérieure à A

D

Distance associée à la valeur L

Table 103. Distance

Valeur ADC	Distance (mm)
<62	<7
62	7
65	8
77	9
110	10
133	11
148	12
158	13
163	14
169	15
172	16
176	17
180	18
>180	>18

14 Vérification du système

14.1 Planning des vérifications requises

La vérification de la configuration et le bon fonctionnement du contrôleur de sécurité consiste à contrôler chaque dispositif d'entrée de sécurité et d'entrée auxiliaire, ainsi que chaque dispositif de sortie. Au fur et à mesure de la commutation individuelle des entrées de l'état marche à l'état d'arrêt, il faut vérifier que les sorties de sécurité s'activent (ON) et se désactivent (OFF) comme prévu.

Banner Engineering recommande vivement d'effectuer les vérifications système de la façon décrite dans les procédures de vérification. Toutefois, une personne (ou équipe) qualifiée doit adapter ces recommandations génériques en fonction de l'application spécifique et déterminer la fréquence appropriée des vérifications. Cette dernière est généralement déterminée en menant une étude des risques, telle que celle incluse dans la norme ANSI B11.0. Le résultat de l'étude de risques détermine la fréquence et le contenu des procédures de vérification périodique à respecter.

AVERTISSEMENT:
- **N'utilisez pas le système tant que les vérifications ne sont pas terminées**
- Toute tentative d'utilisation de la machine surveillée/contrôlée avant l'exécution de ces vérifications peut entraîner des blessures graves, voire mortelles.
- Si toutes ces conditions ne sont pas remplies, n'utilisez pas le système de sécurité, qui inclut le dispositif Banner Engineering et la machine surveillée/contrôlée, avant d'avoir résolu le problème ou corrigé le défaut.

Il faut procéder à un test complet pour vérifier le fonctionnement du contrôleur de sécurité et les fonctionnalités de la configuration prévue. La section Configuration initiale, procédures de vérification à la mise en route et périodiques à la page 313 a pour but de vous aider à élaborer une liste de contrôle personnalisée (spécifique à la configuration) pour chaque application ou installation. Cette liste de contrôle personnalisée doit être mise à la disposition du personnel responsable de la maintenance et des vérifications de mise en route et périodiques. Une liste de contrôle journalier similaire et simplifiée doit être rédigée à l'intention de l'opérateur (ou de la personne désignée [70]). Il est vivement recommandé de conserver des copies des schémas logiques et de câblage pour faciliter les procédures de vérification.

AVERTISSEMENT:
- **Vérifications périodiques**
- Ne pas effectuer ces vérifications pourrait créer une situation potentiellement dangereuse susceptible de provoquer des blessures graves, voire mortelles.
- Les vérifications de mise en service, périodiques et quotidiennes du système de sécurité doivent être effectuées par le personnel approprié aux moments prévus pour s'assurer que le système de sécurité fonctionne comme prévu.

Vérification à la mise en route : une personne qualifiée [70] doit effectuer une procédure de mise en route du système de sécurité avant l'utilisation de l'application sur la machine protégée et lors de la création ou modification des configurations du contrôleur de sécurité.

Vérification périodique (semestrielle) : une personne qualifiée [70] doit également effectuer une remise en route du système de sécurité tous les 6 mois ou à intervalle régulier selon les réglementations locales ou nationales.

Vérifications opérationnelles journalières : une personne désignée [70] doit aussi vérifier l'efficacité des mesures de réduction du risque selon les recommandations du fabricant du dispositif chaque jour où la machine protégée est en service.

AVERTISSEMENT:
- **Dégagez la zone protégée avant de mettre le système sous tension ou d'effectuer un reset de celui-ci**
- Si vous ne dégagez pas la zone protégée avant la mise sous tension cela peut entraîner des blessures graves, voire mortelles.
- Vérifiez qu'aucune personne ne se trouve dans la zone protégée et que le matériel inutile a été enlevé avant de mettre la machine sous surveillance sous tension ou d'effectuer un reset du système.

14.2 Procédure de vérification à la mise en route

Avant de continuer, vérifiez les points suivants :

- Aucune borne de sortie de relais et transistorisée de l'ensemble du système du contrôleur de sécurité ne doit être raccordée à la machine. Il est recommandé de débrancher toutes les bornes enfichables de la sortie de sécurité du contrôleur de sécurité.
- La machine doit être hors tension et l'alimentation des commandes et des déclencheurs de la machine ne doit pas être branchée.

[70] Référez-vous à la section Glossaire à la page 362 pour consulter des définitions.

Les raccordements permanents seront effectués ultérieurement.

14.2.1 Vérification du fonctionnement du système

La procédure de vérification à la mise en route doit être effectuée par une personne qualifiée [71]. **Elle ne doit être effectuée qu'après la configuration du contrôleur de sécurité et après l'installation et la configuration correctes** des systèmes de sécurité et des dispositifs de protection connectés à ses entrées (voir Options des dispositifs d'entrée de sécurité à la page 38 et les normes appropriées).

La vérification à la mise en route s'effectue en deux occasions :

1. Lors de l'installation initiale du contrôleur, pour vérifier qu'il a été correctement installé.
2. Après toute intervention de maintenance ou modification du système ou de la machine protégée par le système, pour s'assurer du bon fonctionnement du contrôleur (voir Planning des vérifications requises à la page 312).

Pour la première partie de la vérification à la mise en route, le contrôleur de sécurité et les systèmes de sécurité associés doivent être vérifiés sans que la machine protégée soit sous tension. Les derniers raccordements des interfaces à la machine protégée ne doivent pas être effectués tant que ces systèmes n'ont pas été vérifiés.

Vérifiez les points suivants :

- **Les fils de la sortie de sécurité doivent être isolés** — ils ne se court-circuitent pas et ne sont pas reliés à l'alimentation ou à la terre.
- En cas d'utilisation de l'EDM (surveillance des commutateurs externe), les connexions de l'EDM doivent être raccordées à une source +24 Vcc par les contacts de surveillance normalement fermés (N.F.) du ou des dispositifs connectés aux sorties de sécurité, comme décrit dans la section Surveillance des commutateurs externes (EDM) à la page 74 et les schémas de câblage.
- Le fichier de configuration du contrôleur de sécurité correspondant à l'application doit avoir été installé sur le contrôleur de sécurité.
- Tous les raccordements effectués doivent être conformes aux dispositions NEC appropriées et aux codes de câblage locaux.

Cette procédure permet de vérifier le contrôleur de sécurité et les systèmes de sécurité associés de manière autonome avant qu'ils ne soient raccordés de façon permanente à la machine protégée.

14.2.2 Configuration initiale, procédures de vérification à la mise en route et périodiques

Il existe deux moyens de vérifier que les sorties de sécurité changent d'état au moment approprié au cours de l'étape de vérification de la configuration initiale (ouvrez la fenêtre **Résumé de la configuration** dans le logiciel pour afficher les paramètres de configuration de la mise sous tension et le test de démarrage) :

- Surveillez les LED associées aux entrées et sorties. Si la LED d'entrée est verte, l'entrée a le niveau haut (ou 24 V). Si la LED d'entrée est rouge, l'entrée a le niveau bas (ou 0 V). De même, si les contacts de sortie RO1 ou RO2 sont fermés, la LED correspondante est verte. Si les contacts sont ouverts, la LED est rouge.
- Démarrez le **Mode temps réel** dans le logiciel (le contrôleur de sécurité doit être sous tension et raccordé au PC à l'aide du câble SC-USB2).

Configuration au démarrage

Les sorties associées aux fonctions de commande bimanuelle, de dispositif de dérivation, de commande de presse ou d'activation ne s'activent pas à la mise sous tension. Après la mise sous tension, vous devez faire passer ces dispositifs à l'état d'arrêt puis à l'état marche afin de pouvoir activer les sorties de sécurité associées.

Pour la fonction de commande de presse, suivez le processus décrit dans la section Commande de presse à la page 165.

Si le système est configuré pour une mise sous tension normale

Si la fonction de verrouillage n'est pas utilisée, vérifiez que les sorties de sécurité s'activent après la mise sous tension.

Si les dispositifs d'entrée ou les sorties utilisent la fonction de verrouillage, vérifiez que les sorties de sécurité ne s'activent pas après la mise sous tension tant que les opérations de reset à verrouillage manuel spécifiques n'ont pas été effectuées.

Si le système est configuré pour un reset automatique à la mise sous tension

Vérifiez que toutes les sorties de sécurité s'activent dans les 7 secondes (les sorties pour lesquelles l'option de retard à l'enclenchement est activée peuvent avoir un délai d'activation plus long).

Si le système est configuré pour un reset manuel à la mise sous tension

Vérifiez que toutes les sorties de sécurité restent désactivées après la mise sous tension.

Attendez au moins 10 secondes après la mise sous tension puis effectuez un reset manuel.

Vérifiez que toutes les sorties de sécurité s'activent (les sorties avec l'option de retard à l'enclenchement activée peuvent avoir un délai d'activation plus long).

[71] Référez-vous à la section Glossaire à la page 362 pour consulter des définitions.

PRÉCAUTION: Vérification de la fonction d'entrée et de sortie

La personne qualifiée est chargée de soumettre les dispositifs d'entrée à un cycle complet (état Run et état Stop) pour vérifier que les sorties de sécurité s'activent et se désactivent pour remplir leur rôle de protection prévu dans des conditions de fonctionnement normales et des conditions d'erreur (défaut) prévisibles. Vérifiez et testez soigneusement chaque configuration du contrôleur de sécurité pour vous assurer qu'une perte d'alimentation d'un dispositif d'entrée de sécurité, du contrôleur de sécurité ou du signal d'entrée inversé d'un dispositif d'entrée de sécurité n'entraînera pas une activation, une inhibition ou une dérivation imprévue de la sortie de sécurité.

Remarque: Si un voyant d'entrée ou de sortie clignote en rouge, consultez la section Recherche de pannes à la page 344.

Fonctionnement d'un dispositif d'entrée de sécurité (arrêt d'urgence, interrupteur à câble, capteur optique, tapis de sécurité, arrêt de protection, interrupteur de porte, dispositif ISD de chaîne)

1. Lorsque les sorties de sécurité associées sont activées, actionnez chaque dispositif d'entrée de sécurité, les uns après les autres (y compris chaque dispositif dans une chaîne ISD ou une cascade).
2. Vérifiez que chaque sortie de sécurité associée se désactive (OFF) avec le retard au déclenchement approprié, dans les cas applicables.
3. Lorsque le dispositif de sécurité est en état marche :
   - **Si le dispositif d'entrée de sécurité est configuré avec une fonction de reset de verrouillage :**
     1. Vérifiez que la sortie de sécurité reste désactivée (OFF).
     2. Effectuez un reset de verrouillage pour activer les sorties.
     3. Vérifiez que toutes les sorties de sécurité associées s'activent (ON).
   - **Si aucune fonction de reset de verrouillage n'est utilisée :** vérifiez que la sortie de sécurité s'active.

Important: Testez toujours les dispositifs de protection conformément aux recommandations du fabricant du dispositif.

Dans les étapes de vérification ci-dessous, si une fonction ou un dispositif donné ne fait pas partie de l'installation, passez l'étape et vérifiez le point suivant ou passez à l'étape finale de la mise en route.

Fonction de commande bimanuelle sans inhibition

1. Vérifiez que les commandes bimanuelles sont en état d'arrêt.
2. Assurez-vous que toutes les autres entrées associées à la fonction de commande bimanuelle sont en état marche et enclenchez les deux actionneurs pour activer la sortie de sécurité associée.
3. Vérifiez que la sortie de sécurité associée reste désactivée sauf si les deux actionneurs sont activés à moins de 0,5 seconde d'intervalle.
4. Vérifiez que la sortie de sécurité se désactive et le reste lorsqu'une seule main est retirée et replacée (tout en maintenant l'autre actionneur en état marche).
5. Vérifiez que la sortie de sécurité est ou reste désactivée lorsque vous commutez l'entrée de sécurité qui lui est associée (autre qu'un actionneur de commande bimanuelle) en état d'arrêt.
6. Si vous utilisez plusieurs commandes bimanuelles, les actionneurs supplémentaires doivent être activés avant que la sortie de sécurité passe sur ON. Vérifiez que la sortie de sécurité se désactive et le reste lorsqu'une seule main est retirée et replacée (tout en maintenant les autres actionneurs en état de marche).

Fonction de commande bimanuelle avec inhibition

1. Suivez la procédure de vérification de la fonction de commande bimanuelle décrite ci-dessus.
2. Enclenchez les actionneurs de la commande bimanuelle puis activez la paire 1 de capteurs d'inhibition (MSP1).
3. Avec les capteurs MSP1 activés, retirez vos mains de la commande bimanuelle et vérifiez que la sortie de sécurité reste activée (ON).
4. Vérifiez que la sortie de sécurité se désactive (OFF) dans les cas suivants :
   - Les capteurs MSP1 sont commutés en état d'arrêt.
   - Le temps limite d'inhibition expire.
5. En présence de plusieurs commandes bimanuelles dont une au moins possède des actionneurs qui ne peuvent être inhibés, vérifiez que, lors d'un cycle d'inhibition actif, le retrait d'une ou des deux mains de chaque actionneur non inhibé entraîne la désactivation des sorties de sécurité.

Fonction d'inhibition bidirectionnelle (bilatérale) (aussi possible pour des fonctions d'inhibition de contrôle de zones)

1. Lorsque la protection inhibée est en état marche, activez l'entrée Inhibition activée (si vous l'utilisez) puis chaque capteur d'inhibition par ordre séquentiel dans les trois secondes qui suivent.
2. Générez une commande d'arrêt du dispositif de sécurité inhibé :
   a) Vérifiez que les sorties de sécurité associées restent activées.
   b) Si une limite de temps d'inhibition a été configurée, vérifiez que les sorties de sécurité associées se désactivent lorsque la limite de temps d'inhibition expire.
3. Répétez la procédure ci-dessus pour chaque paire de capteurs d'inhibition (MSP).
4. Vérifiez que chaque dispositif de sécurité inhibé fonctionne comme prévu.
5. Générez successivement une commande d'arrêt de tous les dispositifs de sécurité non inhibés pendant le cycle d'inhibition et vérifiez que les sorties de sécurité associées se désactivent.
6. Vérifiez le processus d'inhibition en sens inverse en répétant la procédure ci-dessus et en activant les capteurs d'inhibition dans l'ordre inverse.

Fonction d'inhibition unidirectionnelle

1. Lorsque les capteurs d'inhibition sont désactivés, que les dispositifs de sécurité inhibés sont en état marche et que les sorties de sécurité sont activées :
   a) Activez la paire de capteurs d'inhibition 1 (MSP1).
   b) Faites passer le dispositif de sécurité inhibé en état d'arrêt.
   c) Activez la paire de capteurs d'inhibition 2 (MSP2).
   d) Désactivez MSP1.
2. Vérifiez que la sortie de sécurité associée reste active pendant toute la procédure.
3. Répétez le test dans le *mauvais sens* (MSP2, puis dispositif de sécurité puis MSP1).
4. Vérifiez que le passage à l'état OFF de la protection entraîne la désactivation de la sortie de sécurité.

Si un temps limite d'inhibition a été configuré

Vérifiez que les sorties de sécurité se désactivent quand le temps limite d'inhibition expire.

Fonction d'inhibition à la mise sous tension (non applicable pour les commandes bimanuelles)

1. Mettez le contrôleur de sécurité hors tension.
2. Activez l'entrée Inhibition activée, le cas échéant.
3. Activez une paire de capteurs d'inhibition appropriée pour démarrer un cycle d'inhibition.
4. Vérifiez que tous les dispositifs de sécurité avec fonction d'inhibition sont en état marche.
5. Mettez le contrôleur de sécurité sous tension.
6. Vérifiez que la sortie de sécurité s'active et qu'un cycle d'inhibition démarre.
7. Répétez ce test lorsque le dispositif de sécurité avec fonction d'inhibition est en état d'arrêt.
8. Vérifiez que la sortie de sécurité reste désactivée.

Fonction d'inhibition avec neutralisation dépendante de l'inhibition

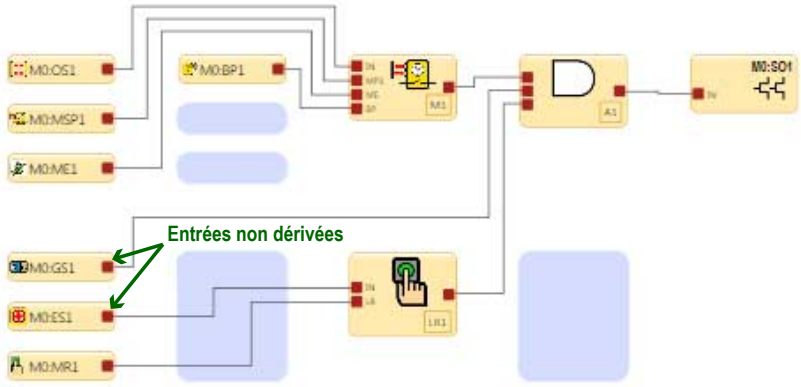
1. Vérifiez que les capteurs d'inhibition ne sont pas activés et que les dispositifs de sécurité inhibés sont en état marche.
2. Vérifiez que les sorties de sécurité sont activées.
3. Commutez le dispositif de sécurité en état d'arrêt.
4. Vérifiez que la sortie de sécurité se désactive.
5. Activez un des capteurs d'inhibition.
6. Vérifiez que le voyant d'inhibition en option clignote.
7. Démarrez la neutralisation dépendante de l'inhibition en activant l'interrupteur de dérivation.
8. Vérifiez que la sortie de sécurité s'active.
9. Vérifiez que la sortie de sécurité se désactive dans l'une des conditions suivantes :
   - Le temps limite de dérivation (neutralisation) expire.

- Les capteurs d'inhibition sont désactivés.
- Le dispositif de dérivation est désactivé.

Fonction d'inhibition avec dérivation

1. Vérifiez que chaque entrée de sécurité, si elle peut être à la fois inhibée et dérivée, est en état d'arrêt.
2. Vérifiez les éléments suivants lorsque l'interrupteur de dérivation est en état marche :
   a) Les sorties de sécurité associées s'activent.
   b) Les sorties de sécurité associées se désactivent quand la limite de temps de dérivation expire.
3. Commutez l'interrupteur de dérivation en état marche et vérifiez que les sorties de sécurité associées s'activent.
4. Commutez, un par un, les dispositifs d'entrée non dérivés associés en état d'arrêt et vérifiez que les sorties de sécurité associées se désactivent lorsque l'interrupteur de dérivation est en état marche.

Illustration 310. Fonction d'inhibition avec dérivation



Fonction de dérivation

1. Vérifiez que les sorties de sécurité associées sont désactivées lorsque les entrées de sécurité à dériver sont en état d'arrêt.
2. Vérifiez les éléments suivants lorsque l'interrupteur de dérivation est en état marche :
   a) Les sorties de sécurité associées s'activent.
   b) Les sorties de sécurité associées se désactivent quand la limite de temps de dérivation expire.
3. Commutez l'interrupteur de dérivation en état marche et vérifiez que les sorties de sécurité associées s'activent.
4. L'un après l'autre, commutez les dispositifs d'entrée non dérivés en état d'arrêt et vérifiez que les sorties de sécurité associées se désactivent lorsque l'interrupteur de dérivation est en état marche.

Fonction de temporisation d'arrêt (retard au déclenchement) de sortie de sécurité

1. Avec l'une des entrées de contrôle en état d'arrêt et la sortie de sécurité temporisée en état Retard au déclenchement, vérifiez que la sortie de sécurité se désactive à l'expiration du temps de temporisation.
2. Avec l'une des entrées de contrôle en état d'arrêt et le minuteur de temporisation d'arrêt actif, basculez l'entrée en état marche et vérifiez que la sortie de sécurité s'active et le reste.

Fonction de retard au déclenchement de sortie de sécurité - Entrée d'annulation de temporisation

Avec les entrées associées en état d'arrêt et la sortie de sécurité temporisée en état Retard au déclenchement, activez l'entrée d'annulation de temporisation et vérifiez que la sortie de sécurité se désactive immédiatement.

Fonction de temporisation d'arrêt (retard au déclenchement) de sortie de sécurité - Entrées de contrôle

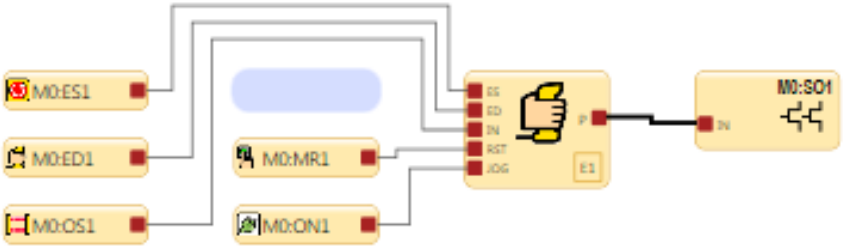
1. Avec l'une des entrées de contrôle en état d'arrêt et la sortie de sécurité temporisée en état Retard au déclenchement, basculez l'entrée en état marche.
2. Vérifiez que la sortie de sécurité est activée et le reste.

Fonction de temporisation d'arrêt (retard au déclenchement) de sortie de sécurité et reset de verrouillage

1. Vérifiez que les dispositifs d'entrée associés sont en état marche afin que la sortie de sécurité temporisée soit activée (ON).
2. Démarrez le temporisateur au déclenchement en basculant un dispositif d'entrée en état d'arrêt.
3. Rebasculez le dispositif d'entrée en état marche pendant le délai de retard au déclenchement et appuyez sur le bouton de reset.
4. Vérifiez que la sortie temporisée se désactive à la fin du délai de retard et reste désactivée (un signal de reset à verrouillage pendant le temps du retard est ignoré).

Fonction de dispositif de commande sans sortie d'approche secondaire

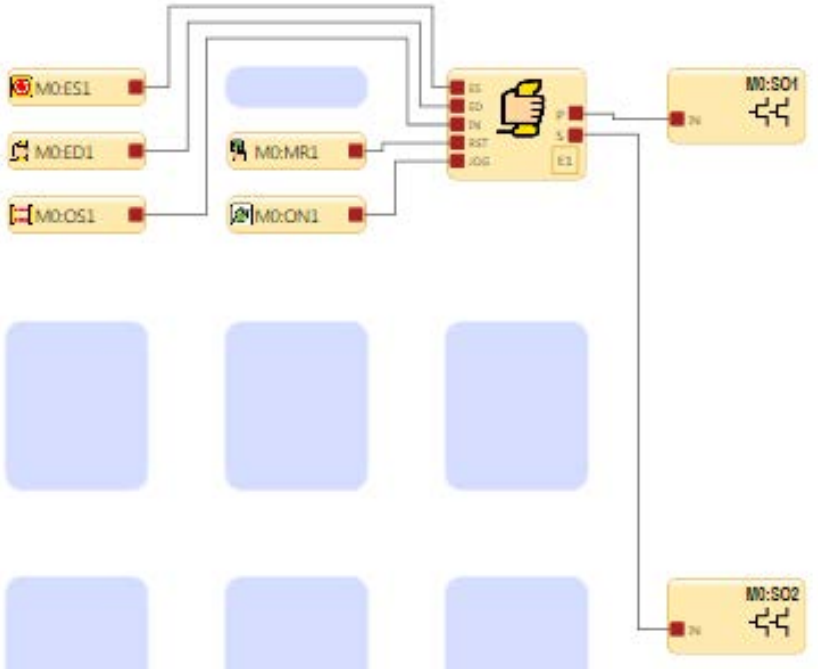
Illustration 311. Fonction de dispositif de commande sans sortie d'approche secondaire



1. Avec les entrées associées en état marche et le dispositif de commande en état d'arrêt, vérifiez que la sortie de sécurité est activée.
2. Avec le dispositif de commande toujours en état marche et la sortie de sécurité associée activée, vérifiez que la sortie de sécurité se désactive à l'expiration du minuteur du dispositif de commande.
3. Faites repasser le dispositif de commande en état d'arrêt puis en état marche et vérifiez que la sortie de sécurité s'active.
4. Commutez le dispositif de commande en état d'arrêt et vérifiez que les sorties de sécurité associées se désactivent.
5. Commutez les arrêts d'urgence et interrupteurs à câble associés au dispositif de commande en état d'arrêt et vérifiez pour chacun d'eux successivement que les sorties de sécurité associées sont activées (ON) et en mode d'activation (Enable).
6. Lorsque le dispositif de commande est en état d'arrêt, effectuez un reset.
7. Vérifiez que le contrôle ultime repose désormais sur les dispositifs d'entrée associés de la fonction du dispositif (appareil) de commande :
   a) Si un ou plusieurs dispositifs d'entrée sont en état d'arrêt, vérifiez que la sortie est désactivée.
   b) Si tous les dispositifs d'entrée sont en état marche, vérifiez que la sortie est activée.

Fonction de dispositif de commande — Avec fonction d'approche sur la sortie secondaire

Illustration 312. Fonction de dispositif de commande — Avec fonction d'approche sur la sortie secondaire



1. Lorsque le dispositif de commande et le bouton d'approche sont en état marche et qu'ils ont le contrôle de la sortie de sécurité principale, vérifiez que la sortie se désactive lorsque soit le dispositif de commande, soit le bouton d'approche bascule en état d'arrêt.
2. Lorsque le dispositif de commande a le contrôle de la sortie de sécurité principale et le bouton d'approche celui de la sortie de sécurité secondaire, vérifiez que la sortie principale :
   a) s'active lorsque le dispositif de commande est en état marche ;
   b) se désactive lorsque le dispositif de commande est en état d'arrêt et que le bouton d'approche est en état marche.
3. Vérifiez que la sortie s'active uniquement lorsque le dispositif de commande et le bouton d'approche sont en état marche.
4. Vérifiez que la sortie secondaire :
   a) s'active lorsque le dispositif de commande et le bouton d'approche sont en état marche ;
   b) se désactive lorsque soit le dispositif de commande, soit le bouton d'approche est en état d'arrêt.

Bloc fonction Commande de presse avec configuration d'une commande à actionneur unique

1. Assurez-vous que l'entrée de sécurité non inhibable, l'entrée d'arrêt d'urgence inhibable (si elle est configurée) et TOS sont activés.
2. Effectuez un cycle de reset.
3. Activez momentanément l'entrée GO. Vérifiez que le mouvement descendant démarre.
4. Utilisez une pièce de test pour bloquer l'entrée d'arrêt d'urgence inhibable. Vérifiez que le mouvement descendant s'arrête.
5. Supprimez l'entrée d'arrêt d'urgence inhibable et effectuez un cycle de reset.
6. Activez momentanément l'entrée GO. Vérifiez que le coulisseau monte jusqu'à la position TOS et s'arrête.
7. Activez momentanément l'entrée GO. Vérifiez que le coulisseau descend.
8. Lorsque le coulisseau atteint le point BOS et entame son mouvement ascendant, bloquez l'entrée d'arrêt d'urgence inhibable avec la pièce de test. Vérifiez que le coulisseau poursuit sa course montante jusqu'à la position TOS.

Bloc fonction Commande de presse avec configuration du paramétrage manuel Course montante

1. Assurez-vous que l'entrée de sécurité non inhibable, l'entrée de sécurité inhibable et TOS sont activés.
2. Effectuez un cycle de reset, activez PIP (s'il est utilisé), puis activez l'entrée GO. Vérifiez que la sortie Down (Descente) est activée.
3. Désactivez l'entrée GO. Vérifiez que la sortie Down (Descente) est désactivée.
4. Activez l'entrée GO. La sortie Down (Descente) devrait se réactiver.

5. Utilisez une pièce de test pour bloquer l'entrée d'arrêt d'urgence inhibable. Vérifiez que le mouvement descendant s'arrête.
6. Supprimez l'entrée d'arrêt d'urgence inhibable et effectuez un cycle de reset.
7. Activez l'entrée GO. Vérifiez que le coulisseau monte jusqu'à la position TOS et s'arrête.
8. Activez l'entrée GO. Une fois que le coulisseau atteint le point BOS, vérifiez que la sortie Down (Descente) se désactive et que la sortie Up (Montée) s'active.
9. Avec la pièce de test, bloquez l'entrée d'arrêt d'urgence inhibable. Vérifiez que le mouvement montant s'arrête.
10. Désactivez l'entrée GO.
11. Supprimez l'entrée d'arrêt d'urgence inhibable.
12. Effectuez un cycle de reset.
13. Activez l'entrée GO pour ramener le coulisseau à la position TOS.

Contrôles du bloc fonction Mode Commande de presse

Si le paramètre Double pression est sélectionné, vérifiez que toutes les sorties fonctionnent correctement. La sortie haute pression ne doit s'activer qu'en mode Run (Marche).

1. Assurez-vous que l'entrée NM safety (Arrêt d'urgence non inhibable), l'entrée M Safety (Arrêt d'urgence inhibable) et TOS sont activées (mais que toutes les entrées Mode sont désactivées).
2. Effectuez un cycle de reset, activez PIP (s'il est utilisé), puis activez l'entrée GO. Vérifiez qu'aucune sortie ne s'allume.
3. Désactivez l'entrée GO.
4. Sélectionnez l'état RUN, effectuez un cycle de reset, puis activez l'entrée GO. La sortie Down (Descente) devrait s'activer. (Effectuez un cycle complet puis arrêtez le processus, y compris la désactivation/réactivation de l'entrée PIP.)
5. Désactivez l'entrée Run et activez l'entrée Inch Down (Descente par à-coups).
6. Effectuez un cycle de reset, puis activez l'entrée GO. Vérifiez la sortie Down (Descente) est activée puis désactivée (et vérifiez que la vitesse du coulisseau est conforme aux spécifications d'approche).
7. Au point BOS du processus, désactivez l'entrée Inch Down (Descente par à-coups) et activez l'entrée Inch Up (Montée par à-coups).
8. Effectuez un cycle de reset, puis activez l'entrée GO. Vérifiez la sortie Up (Montée) est activée puis désactivée (et vérifiez que la vitesse du coulisseau est conforme aux spécifications d'approche).

Contrôles de l'arrêt séquentiel (SQS) de la commande de la presse (ou de SQS et PCMS)

Si le paramètre Double pression est sélectionné, vérifiez que la sortie haute pression ne s'active que lorsque le coulisseau passe de SQS au point BOS.

Voir Bloc fonction Entrées de commande de presse à la page 167 pour les configurations et comportements spécifiques GO, SQS et interrupteur au pied.

1. Assurez-vous que l'entrée de sécurité non inhibable, l'entrée de sécurité inhibable et TOS sont activés.
2. Effectuez un cycle de reset, activez PIP (s'il est utilisé), puis activez l'entrée GO. Vérifiez que la sortie Down (Descente) est activée.
3. Vérifiez que le coulisseau s'arrête au(x) capteur(s) SQS (ou aux capteurs SQS & PCMS).
4. Relâchez (désactivez) l'entrée GO. Vérifiez que l'écartement des outils est inférieur à 6 mm (sans danger pour les doigts). Vérifiez que l'entrée d'arrêt d'urgence inhibable est maintenant inhibée.
5. Activez l'entrée de l'interrupteur au pied. Vérifiez que le coulisseau se déplace du point SQS au point BOS puis s'arrête.
6. Relâchez l'entrée de l'interrupteur au pied.
7. Activez l'entrée GO. Vérifiez que le coulisseau retourne au point TOS puis s'arrête.
8. Désactivez l'entrée GO.

15 Informations d'état et de fonctionnement

Utilisez l'interface embarquée ou le logiciel du contrôleur de sécurité XS/SC26 pour surveiller l'état de fonctionnement.
Utilisez le logiciel du contrôleur de sécurité SC10-2 pour surveiller l'état de fonctionnement.

15.1 État des LED du XS/SC26

LED	État	Signification
Tous	OFF	Mode d'initialisation
	Séquence : Vert allumé pendant 0,5 s Rouge allumé pendant 0,5 s Éteint pendant 0,5 s minimum	Mise sous tension
Mise sous tension/ Défaut	OFF	Hors tension
	Vert : fixe	Mode RUN (marche)
	Vert : clignotant	Mode de configuration OU Mode manuel de mise sous tension
	Rouge : clignotant	Verrouillage non fonctionnel
USB (Contrôleur de base FID 2 ou antérieur)	OFF	Aucune liaison établie avec le PC
	Vert : fixe	Liaison avec le PC établie
	Vert : clignotant pendant 5 s, puis éteint	Correspondance avec la configuration de la carte SC-XM2/3
	Rouge : clignotant pendant 5 s, puis éteint	Non correspondance avec la configuration de la carte SC-XM2/3
USB (Contrôleur de base FID 3 ou ultérieur)	OFF	Aucune liaison établie et aucun contrôleur de sécurité configuré
	Vert : fixe	Câble USB connecté à un contrôleur de sécurité configuré
	Vert : clignotant	Aucune liaison établie et contrôleur de sécurité avec configuration d'usine OU Câble USB connecté et contrôleur de sécurité avec configuration d'usine
	Vert : clignotement rapide (contrôleur de base FID 7 ou ultérieur uniquement)	Unité connectée au logiciel via une connexion Ethernet
	Vert : clignotant pendant 4 s, puis fixe	Une carte SC-XM2/3 configurée (verrouillée ou non) contenant des informations créées avec le logiciel Contrôleur de sécurité Banner version 4.2 ou ultérieure, ou créées à partir d'un contrôleur de sécurité FID 3 ou ultérieur est enfichée dans un contrôleur de sécurité avec configuration d'usine
	Vert : clignotant pendant 5 s, puis éteint	Une carte SC-XM2/3 configurée et déverrouillée contenant des informations créées à l'aide du logiciel Contrôleur de sécurité Banner version 4.2 ou ultérieure, ou créées à partir d'un contrôleur de sécurité FID 3 ou ultérieur, est enfichée dans un contrôleur de sécurité configuré avec une configuration identique, des codes PIN/mots de passe identiques et des paramètres réseau identiques ou différents OU Une carte SC-XM2/3 contenant des informations créées avec le logiciel Contrôleur de sécurité Banner version 4.1 ou antérieure ou créées à partir d'un contrôleur de sécurité FID 2 ou antérieur est insérée dans un contrôleur FID 3 ou ultérieur (configuré ou avec réglages d'usine) et a une configuration identique
	Vert : clignotant pendant 5 s, puis rouge clignotant	Une carte SC-XM2/3 configurée et verrouillée contenant des informations créées à l'aide du logiciel Contrôleur de sécurité Banner version 4.2 ou ultérieure, ou créées à partir d'un contrôleur de sécurité FID 3 ou ultérieur, est enfichée dans un contrôleur de sécurité configuré avec une configuration et des codes PIN/mots de passe identiques, mais avec des paramètres réseau différents.

LED	État	Signification
	Rouge : clignotant	Une carte SC-XM2/3 configurée (verrouillée ou non) contenant des informations créées à l'aide du logiciel Contrôleur de sécurité Banner version 4.2 ou ultérieure, ou créées à partir d'un contrôleur de sécurité FID 3 ou ultérieur, est raccordée à un contrôleur de sécurité configuré avec une configuration différente et des codes PIN/mots de passe différents, ou une carte SC-XM2/3 vide est enfichée OU Carte SC-XM2/3 vide enfichée dans un contrôleur de sécurité avec configuration d'usine ou dans un contrôleur de sécurité configuré
	Rouge : clignotant pendant 5 s, puis éteint	Une carte SC-XM2/3 contenant des informations créées avec le logiciel Contrôleur de sécurité Banner version 4.1 ou antérieure ou créées à partir d'un contrôleur de sécurité FID 2 ou antérieur est insérée dans un contrôleur FID 3 ou ultérieur (configuré ou avec réglages d'usine) et a une configuration différente
Entrées	Vert : fixe	Aucun défaut d'entrée
	Rouge : clignotant	Une ou plusieurs entrées sont en mode verrouillage.
SO1, SO2	OFF	Sortie non configurée
	Vert : fixe	Sortie de sécurité activée
	Rouge : fixe	Sortie de sécurité désactivée
	Rouge : clignotant	Défaut de sortie de sécurité détecté ou défaut EDM ou AVM détecté

État de la LED pour les sorties divisées	Signification
Vert : fixe	Les deux sorties sont activées.
Rouge : fixe	SOxa et/ou SOxb désactivées
Rouge : clignotant	Défaut SOxa et/ou SOxb détecté

LED de diagnostic Ethernet		
LED jaune	**LED verte**	**Description**
ON	Varie selon le trafic	Liaison établie/fonctionnement normal
OFF	OFF	Défaillance matérielle

Clignotement simultané des LED jaune et verte	Description
5 clignotements suivis de plusieurs clignotements rapides	Mise sous tension normale
1 clignotement toutes les 3 secondes	Contactez Banner Engineering
Séquence répétée de 2 clignotements	Câble actif débranché au cours des 60 dernières secondes
Séquence répétée de 3 clignotements	Câble débranché
Séquence répétée de 4 clignotements	Réseau non activé dans la configuration
Séquence répétée de 5 clignotements ou plus	Contactez Banner Engineering

Commande Flash	Signification
LED du contrôleur de base clignotant pendant 4 secondes 	Le clignotement indique que le contrôleur de base est connecté. Il s'agit du résultat de la commande « Flash LED » du réseau PROFINET. Les LED clignotent lorsque vous cliquez sur  dans la fenêtre **Contrôleurs disponibles** du logiciel.

15.2 Indicateurs d'état du module d'entrées

Les informations suivantes concernent les modèles XS8si et XS16si.

LED	État	Signification
Tous	Séquence : Vert allumé pendant 0,5 s Rouge allumé pendant 0,5 s Éteint pendant 0,5 s minimum	Mise sous tension
	OFF	Mode d'initialisation
Voyant de mise sous tension	Vert : allumé	Mise sous tension
	OFF	Hors tension
	Rouge : clignotant	Verrouillage non fonctionnel
Indicateur de transmission / réception	Vert : allumé	Transmission ou réception de données
	Rouge : allumé	Pas de communication
	Rouge : clignotant	Défaut de communication détecté OU Problème de communication du bus de sécurité
Indicateur d'entrée	Vert : allumé	Aucun défaut d'entrée
	Rouge : clignotant	Défaut d'entrée détecté

15.3 LED d'état du module de sorties (électroniques ou relais)

Les informations suivantes concernent les modèles XS2so, XS4so, XS1ro, et XS2ro.

LED	État	Signification
Tous	Séquence : Vert allumé pendant 0,5 s Rouge allumé pendant 0,5 s Éteint pendant 0,5 s minimum	Mise sous tension
	OFF	Mode d'initialisation
Voyant de mise sous tension	OFF	Hors tension
	Vert : allumé	Mise sous tension
	Rouge : clignotant	Verrouillage non fonctionnel
Indicateur de transmission / réception	Vert : allumé	Transmission ou réception de données
	Rouge : allumé	Pas de communication
	Rouge : clignotant	Défaut de communication détecté OU Problème de communication du bus de sécurité
Indicateurs de sorties de sécurité	OFF	Sortie non configurée
	Vert : allumé	Deux sorties de sécurité simple voie (toutes deux activées) OU Sortie de sécurité double voie ou simple voie activée
	Rouge : allumé	Deux sorties de sécurité simple voie (une activée et l'autre désactivée)
	Rouge : allumé	Deux sorties de sécurité simple voie (toutes deux désactivées) OU Sortie de sécurité double voie ou simple voie désactivée (autre voie non utilisée)
	Rouge : clignotant	Défaut de sortie de sécurité détecté

15.4 Indicateurs d'état du module de la passerelle de communication EtherCAT®

Les informations suivantes concernent le modèle XSeCAT.

LED	État	Signification
Alimentation/Défaut (LED système) **Tx/Rx** (LED système)	OFF	Mode d'initialisation
	Séquence : Vert allumé pendant 0,5 s Rouge allumé pendant 0,5 s Éteint pendant 0,5 s minimum	Mise sous tension
Alimentation/défaut (LED système)	OFF	Hors tension
	Vert : allumé	Mise sous tension
	Vert : clignotant	Téléchargement de la nouvelle configuration (et une configuration précédente contenait EtherCAT)
	Rouge : clignotant	Verrouillage non fonctionnel
Tx/Rx (LED système)	Vert : allumé	Transmission ou réception de données
	Rouge : allumé	Pas de communication
RUN (LED EtherCAT)	OFF	Le dispositif est en état INIT
	Vert : clignotant 200 ms ON/200 ms OFF	Le dispositif est en état pré-opérationnel
	Vert : clignotement unique	Le dispositif est en état opérationnel sûr
	Vert : allumé	Le dispositif est en état opérationnel
ERREUR (LED EtherCAT)	OFF	Aucune erreur
	Rouge : clignotement double	Process Data Watchdog Timeout/EtherCAT Watchdog Timeout — Il est fort probable qu'un câble a été débranché pendant le fonctionnement du système
	Rouge : clignotement unique	Erreur locale — Il est fort probable qu'une nouvelle configuration est en cours de chargement dans le contrôleur de base
	Rouge : clignotant 200 ms ON/200 ms OFF	Configuration invalide
L/A IN (LED EtherCAT)	OFF	Aucune connexion EtherCAT détectée
	Vert : allumé	Raccordement du câble détecté, mais pas de communication détectée
	Vert : clignotant 50 ms ON/50 ms OFF	Raccordement du câble détecté et communication détectée
L/A OUT (LED EtherCAT)	OFF	Aucune connexion EtherCAT détectée
	Vert : allumé	Raccordement du câble détecté, mais pas de communication détectée
	Vert : clignotant 50 ms ON/ 50 ms OFF	Raccordement du câble détecté et communication détectée

15.5 État des LED du SC10-2

Utilisez le tableau suivant pour déterminer l'état du contrôleur de sécurité.

Les LED sont toujours allumées sauf si le contrôleur de sécurité est éteint.

LED	État	Signification
Tous	OFF	Mode d'initialisation

LED	État	Signification
	Séquence : Vert allumé pendant 0,5 s Rouge allumé pendant 0,5 s Éteint pendant 0,5 s minimum	Mise sous tension
Mise sous tension/Défaut (1)	Vert : fixe	24 Vcc connecté
	Vert : clignotant	Mode de configuration ou de reset manuel à la mise sous tension Configuration via SC-XM3 : coupez puis rétablissez l'alimentation
	Rouge : clignotant	Verrouillage non fonctionnel
USB (1)	Vert : fixe	Câble USB raccordé ou SC-XM3 connectée
	Vert : clignotant	Contrôleur de sécurité avec configuration par défaut, pas de câble USB ou de SC-XM3 connectée
	Vert : clignotement rapide pendant 3 s, puis fixe	SC-XM3 configurée (verrouillée ou déverrouillée) et raccordée à un contrôleur de sécurité configuré d'usine ; la configuration, les paramètres réseau et les mots de passe sont transférés de la SC-XM3 au contrôleur de sécurité.
	Vert : clignotant pendant 3 s, puis fixe	SC-XM3 configurée et déverrouillée, raccordée à un contrôleur de sécurité configuré avec une configuration et des codes PIN identiques **Remarque:** Si les paramètres réseau ne correspondent pas, ceux-ci sont transférés du contrôleur de sécurité vers une carte SC-XM3 déverrouillée. Les paramètres réseau ne sont pas transférés vers une carte SC-XM3 verrouillée.
	Vert : clignotant pendant 3 s, puis rouge clignotant	SC-XM3 configurée et déverrouillée, raccordée à un contrôleur de sécurité configuré avec une configuration et des codes PIN identiques mais des paramètres réseau différents
	Rouge : fixe	Contrôleur de sécurité configuré, pas de câble USB ou de SC-XM3 raccordé
	Rouge : clignotant	SC-XM3 configurée (verrouillée ou déverrouillée) raccordée à un contrôleur de sécurité configuré avec une configuration différente, un code PIN différent ou une SC-XM3 vide raccordée à un contrôleur de sécurité
Entrées (10)	Vert : fixe	Configurée comme un circuit d'entrée : 24 Vcc et pas de défaut
	Vert : fixe	Configurée comme une sortie d'état : active
	Rouge : fixe	Configurée comme un circuit d'entrée : 0 Vcc et pas de défaut
	Rouge : fixe	Configurée comme une sortie d'état : inactive
	Rouge : clignotant	Toutes les bornes d'une entrée défaillante (y compris les bornes partagées)
RO1, RO2 (2)	Vert : fixe	Active (contacts fermés)
	Rouge : fixe	Inactive (contacts ouverts) ou non configurée
	Rouge : clignotant	Défaut de sortie de sécurité détecté ou défaut EDM ou AVM détecté

LED de diagnostic Ethernet		
LED jaune	**LED verte**	**Description**
ON	Varie selon le trafic	Liaison établie/fonctionnement normal
OFF	OFF	Défaillance matérielle

Clignotement simultané des LED jaune et verte	**Description**
5 clignotements suivis de plusieurs clignotements rapides	Mise sous tension normale
1 clignotement toutes les 3 secondes	Contacter Banner Engineering
Séquence répétée de 2 clignotements	Câble actif débranché au cours des 60 dernières secondes
Séquence répétée de 3 clignotements	Câble débranché
Séquence répétée de 4 clignotements	Réseau non activé dans la configuration
Séquence répétée de 5 clignotements ou plus	Contacter Banner Engineering

Commande Flash	Signification
Toutes les LED clignotent pendant 4 secondes 	Le clignotement indique que le SC10-2 est connecté. Il s'agit du résultat de la commande « Flash LED » du réseau PROFINET.

15.6 Informations du mode temps réel : logiciel

Pour afficher les informations du mode marche (Run) en temps réel sur un PC, le contrôleur de sécurité doit être connecté à l'ordinateur via le câbleSC-USB2 ou via un câble Ethernet (modèles Ethernet XS/SC26 FID 7 ou ultérieurs). Cliquez sur **Mode temps réel** pour accéder à l'onglet **Mode temps réel**. Cette fonction effectue constamment des mises à jour et affiche des données dont les états marche, d'arrêt et Défaut de toutes les entrées et sorties ainsi que le tableau des codes de défaut. L'onglet **Équipement** et l'onglet **Vue fonctionnelle** proposent également une représentation visuelle des données spécifique au dispositif. Référez-vous à la section Mode temps réel à la page 140 pour en savoir plus.

L'onglet **Mode temps réel** fournit les mêmes informations que celles affichées sur l'écran du contrôleur de sécurité (modèles avec écran).

15.7 Informations du mode temps réel : interface embarquée

Pour afficher des informations du mode marche en temps réel dans l'interface embarquée du contrôleur de sécurité (modèles avec écran d'affichage uniquement), sélectionnez **État du système** [72] dans le menu **Système** (voir Interface embarquée du XS/SC26 à la page 176 pour une carte de navigation). L'écran **État du système** affiche les états des dispositifs d'entrée et des sorties de sécurité. L'écran **Diagnostic des défauts** affiche des informations sur les défauts actuels (courte description, mesures correctives et code de défaut) et permet d'accéder au **journal de défauts**. Pour plus d'informations, voir Interface embarquée du XS/SC26 à la page 176.

L'écran du contrôleur de sécurité affiche les mêmes informations que celles affichées dans le logiciel via la fonction **Mode temps réel**.

15.8 Verrouillage

Le verrouillage d'une entrée est généralement résolu en corrigeant le défaut et en désactivant puis en réactivant l'entrée.

Le verrouillage d'une sortie (dont les défaut EDM et AVM) est résolu en corrigeant le défaut puis en désactivant et réactivant l'entrée de reset connectée au nœud FR de la sortie de sécurité.

Les défauts système (tension électrique faible, surchauffe ou tension détectée sur des entrées non assignées ou défauts de la commande de presse) peuvent être résolus en désactivant puis en réactivant l'entrée de reset système (toute entrée de reset assignée au reset du système). Un seul bouton de réarmement, physique ou virtuel, peut être configuré pour effectuer cette opération.

Un reset système permet d'annuler un verrouillage non associé à des entrées ou des sorties de sécurité. Un verrouillage est une réponse du contrôleur de sécurité qui consiste à désactiver (OFF) toutes les sorties de sécurité affectées lorsqu'un défaut de sécurité critique est détecté. Pour récupérer d'une telle situation, tous les défauts doivent être corrigés et le système doit être réarmé. Un verrouillage se reproduira après un reset du système si le défaut à l'origine du verrouillage n'est pas résolu.

Un reset du système est nécessaire dans les conditions suivantes :

- Récupération suite à un verrouillage du système
- Démarrage du contrôleur de sécurité après le téléchargement d'une nouvelle configuration
- Récupération d'un défaut de la commande de presse

Lorsqu'il s'agit d'un défaut interne, il est probable qu'un reset du système ne fonctionnera pas. Il faut procéder à une mise hors tension puis sous tension avant toute tentative de remise en service.

[72] **État du système** est le premier écran qui s'affiche lorsque le contrôleur de sécurité est mis sous tension après un reset. Cliquer sur **ESC** pour voir le menu **Système**.

AVERTISSEMENT:
- **Reset non surveillé**
- Le non-respect de ces instructions pourrait entraîner des blessures graves, voire mortelles.
- Si un reset non surveillé (reset manuel ou du système) est configuré et si toutes les autres conditions d'un reset sont vérifiées, un court-circuit de la borne de reset à +24 V active immédiatement les sorties de sécurité.

AVERTISSEMENT:
- **Dégagez la zone protégée avant de mettre le système sous tension ou d'effectuer un reset de celui-ci**
- Si vous ne dégagez pas la zone protégée avant la mise sous tension cela peut entraîner des blessures graves, voire mortelles.
- Vérifiez qu'aucune personne ne se trouve dans la zone protégée et que le matériel inutile a été enlevé avant de mettre la machine sous surveillance sous tension ou d'effectuer un reset du système.

15.9 Récupération suite à un verrouillage

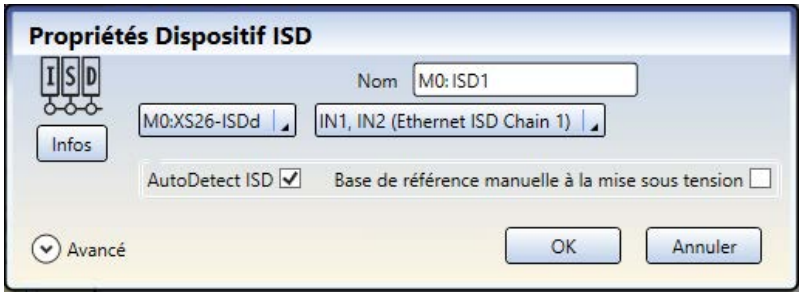
Pour sortir d'un verrouillage :
- Suivez les recommandations de l'écran des défauts (modèles avec écran).
- Suivez les étapes et les vérifications recommandées dans la section Tableaux des codes de défaut du XS/SC26 à la page 349 ou Tableau des codes de défaut du SC10-2 à la page 354
- Procédez au reset du système.
- Coupez l'alimentation puis rétablissez-la et effectuez un reset système si nécessaire.

Si ces mesures ne permettent pas de corriger la situation de blocage, contactez Banner Engineering (voir Réparations et service sous garantie à la page 359).

15.10 Option Détection auto ISD

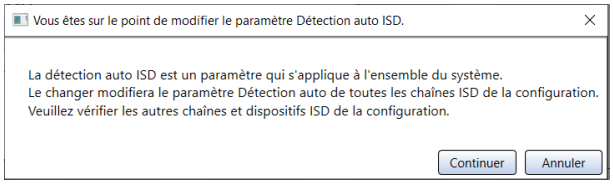
La fonction **Détection auto ISD** est disponible sur le XS26-ISD FID 5 ou ultérieur.

*Illustration 313. **Propriétés du dispositif ISD — Détection auto ISD sélectionnée***



La sélection **Détection auto ISD** est une sélection universelle. Elle modifie toutes les voies ISD en « Configuration automatique », pas seulement celle actuellement sélectionnée dans la zone **Propriétés du dispositif ISD**. Elle supprime également toutes les entrées déjà créées dans d'autres chaînes ISD. Le fait de décocher la case **Détection auto ISD** ne réinitialise **pas** ces entrées (le bouton Annuler peut réinitialiser des entrées précédentes). Lorsque vous activez **Détection auto ISD**, l'avertissement suivant s'affiche, vous permettant d'annuler la modification :

Illustration 314. Confirmation de changement en Détection auto



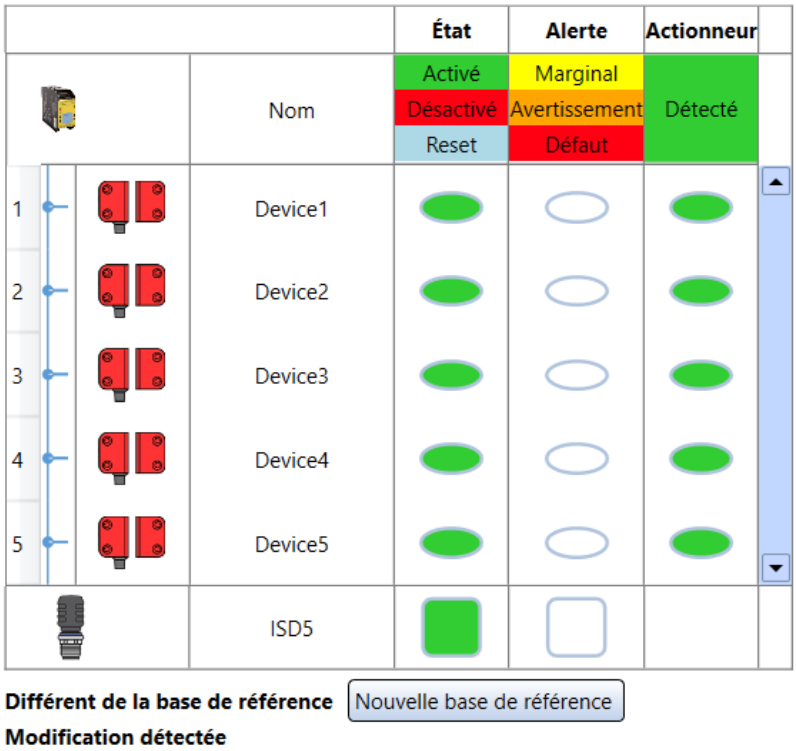
Le fait de cocher la case **Détection auto ISD** permet au contrôleur de sécurité de surveiller plus que la longueur et la composition des chaînes ISD. Lorsque **Détection auto ISD** est sélectionné, le contrôleur met à jour la configuration pour qu'elle corresponde aux nouvelles configurations des chaînes (modifications de chaîne). Le contrôleur transmet cette composition à un API afin qu'elle puisse être vérifiée comme une configuration valide. Les modifications s'affichent également dans la vue **Mode temps réel** du logiciel Contrôleur de sécurité Banner pour une vérification manuelle.

Remarque: La réponse de sécurité du contrôleur est basée sur l'état des OSSD des entrées ISD et non sur les informations ISD transportées sur les OSSD. Les informations ISD sont des informations d'état de la chaîne et/ou du dispositif non liées à la sécurité.

Lorsque **Détection auto ISD** est sélectionné, le contrôleur interroge chacune des chaînes d'entrée ISD configurées pour déterminer le nombre, la position et le type de dispositifs. Le contrôleur fournit ces informations au logiciel Contrôleur de sécurité Banner et/ou à l'API connecté pour vérifier qu'elles sont correctes pour le système donné.

- À la mise sous tension, le contrôleur interroge les chaînes ISD configurées pour déterminer le nombre, la position et le type de dispositifs et définit cette configuration comme étant la configuration de base de la chaîne. Il transmet ces informations au logiciel du contrôleur et/ou à un API connecté pour vérifier que les informations sont correctes. Le contrôleur n'informe pas l'utilisateur des modifications qui auraient pu être apportées lorsque l'alimentation était coupée.
- Lorsque **Détection auto ISD** est sélectionné, la case à cocher **Base de référence manuelle à la mise sous tension** est disponible. Si cette case est cochée, le contrôleur règle le bit « Nouvelle base de référence » sur le logiciel et/ou l'API connecté. Le bit « Accepter cette base de référence » doit être renvoyé au contrôleur pour définir la base de référence. Si la case est décochée, le contrôleur accepte automatiquement la configuration existante de toutes les chaînes ISD connectées. La fonction **Base de référence manuelle à la mise sous tension** est une sélection universelle. La sélection de cette option pour une chaîne s'applique à toutes les chaînes. N'oubliez pas que la réponse de sécurité du contrôleur est basée sur l'état des OSSD des entrées ISD et non sur les informations ISD.
- En cours de fonctionnement, le contrôleur avertit l'utilisateur qu'une modification a été détectée dans une chaîne ISD spécifique. En cas de connexion avec le contrôleur et en Mode temps réel, les éléments suivants s'affichent :

*Illustration 315. Bouton **Nouvelle base de référence** disponible*



Lorsque des modifications de chaîne sont détectées, la vue de la chaîne est automatiquement mise à jour vers la nouvelle configuration. En dessous de la chaîne modifiée, vous pouvez d'abord voir une notification indiquant que les données ISD sont retardées. Après la mise à jour des données, la notification de modification de la chaîne s'affiche pendant 15 secondes. Si la chaîne est différente de ce qu'elle était à la mise sous tension (base de référence), la notification indiquant que la configuration est différente de la base de référence s'affiche. Si le changement est acceptable, il peut être défini comme nouvelle base de référence en cliquant sur **Nouvelle base de référence**. Le contrôleur avertit également l'API connecté qu'une chaîne a été modifiée. Le bit Changement de chaîne détecté des données cycliques pour la chaîne concernée est paramétré sur 1. Il est effacé en accusant réception du changement

Comme le contrôleur ne sait pas si la chaîne ISD connectée à une paire d'entrées est correcte, il incombe à l'utilisateur de s'assurer que la chaîne de dispositifs ISD détectée est correcte. Pour ce faire, il suffit de :

- Vérifier physiquement le nombre de dispositifs par rapport à la documentation
- Vérifier l'affichage ISD en Mode temps réel par rapport à la documentation
- Lire les données dans l'API et les comparer avec les informations chargées pour la structure spécifique de la machine

Il faut parfois quelques secondes au contrôleur pour détecter une modification du nombre de dispositifs ISD dans une chaîne. Le contrôleur détecte le retrait du connecteur de terminaison et/ou la perte des informations ISD (par exemple, lorsque la chaîne est interrompue entre les unités). Ces informations font partie des données cycliques transmises entre le contrôleur et l'API.

Remarque: Les OSSD de la chaîne ISD se désactivent rapidement dans l'une de ces situations (dans le délai de réponse de la chaîne ISD).

Dans la plupart des cas, le contrôleur ne peut pas détecter un changement de longueur de chaîne tant que la chaîne n'est pas terminée (par exemple, le connecteur de terminaison est retiré, des dispositifs sont ajoutés, puis le connecteur de terminaison est réinstallé). Les sorties OSSD peuvent être remises en état ON (marche) après la réinstallation du connecteur de terminaison. Il faut quelques secondes pour commencer une nouvelle transmission des informations ISD car le dispositif de démarrage a peut-être changé.

La façon la plus simple de s'assurer que la machine ne peut pas démarrer après un changement de configuration de la chaîne consiste à mapper la chaîne à un bloc de reset manuel (ou à une sortie avec un nœud LR (reset à verrouillage) sélectionné) dans la configuration. L'opérateur doit donc réarmer le système de sécurité chaque fois que les sorties OSSD de la chaîne passent sur OFF puis sur ON. L'opérateur doit alors redémarrer la machine. Toutefois, ce processus n'exige pas que l'opérateur (ou autre) vérifie que la nouvelle structure de la chaîne ISD est correcte.

Si un utilisateur souhaite maintenir la machine en état OFF (arrêt) jusqu'à ce que l'opérateur ait vérifié que la longueur de la chaîne est correcte pour la structure actuelle de la machine, configurez l'API pour qu'il exige une action spécifique de l'opérateur chaque fois que le drapeau Connecteur de terminaison manquant est activé pour une chaîne. Cette action de l'opérateur consiste à vérifier manuellement que la configuration est correcte ou à sélectionner une fonction sur l'API pour vérifier que la configuration est correcte.

Remarque: Il incombe au constructeur de la machine (à l'utilisateur) de s'assurer que le câblage ne peut pas être facilement manipulé par un opérateur pour contourner la ou les fonctions de sécurité ; par exemple, rendre impossible le retrait d'un interrupteur du système.

Pour un système dans lequel les chaînes ISD ne doivent pas changer, c'est-à-dire que les chaînes ISD sont programmées lors de l'installation de la machine, le constructeur de la machine (utilisateur) doit s'assurer que le câblage ne puisse pas être facilement manipulé par un opérateur pour contourner la ou les fonction(s) de sécurité des dispositifs ISD.

Pour un système dans lequel les chaînes ISD peuvent changer en cours de fonctionnement (par exemple, ajouter et retirer des chariots), le constructeur de la machine (utilisateur) doit s'assurer que les seules modifications qui peuvent être apportées au câblage sont celles impliquées dans l'ajout ou le retrait des sections appropriées de la machine. Il faut effectuer une vérification du système après chaque changement de machine soit automatiquement via un API, soit manuellement par un opérateur.

Remarque: Si un contrôleur est réglé avec le mode Configuration automatique et que la configuration est lue dans le logiciel, le fait de décocher la case **Détection auto ISD** supprime toutes les entrées ISD reçues. Pour créer une configuration permanente à partir d'une configuration réglée sur Configuration automatique, lisez la configuration à partir du contrôleur, puis imprimez-la. Une nouvelle configuration peut alors être créée à partir de l'impression (les chaînes ISD peuvent être recréées une fois que la case **Détection auto ISD** est décochée).

Remarque: Lorsque **Détection auto ISD** est sélectionné, le dispositif 1 est positionné le plus près du contrôleur. Les numéros des dispositifs augmentent à mesure qu'ils s'éloignent du contrôleur, vers le connecteur de terminaison. Lorsque les dispositifs ISD sont entrés manuellement, le dispositif 1 est positionné le plus près du connecteur de terminaison. Les numéros des dispositifs augmentent à mesure qu'ils se rapprochent du contrôleur.

15.11 SC10-2 - Utilisation de l'optimisation automatique des bornes

Procédez comme suit pour un exemple de configuration utilisant la fonction d'optimisation automatique des bornes (ATO).

Remarque: Cette procédure est donnée à titre d'exemple uniquement.

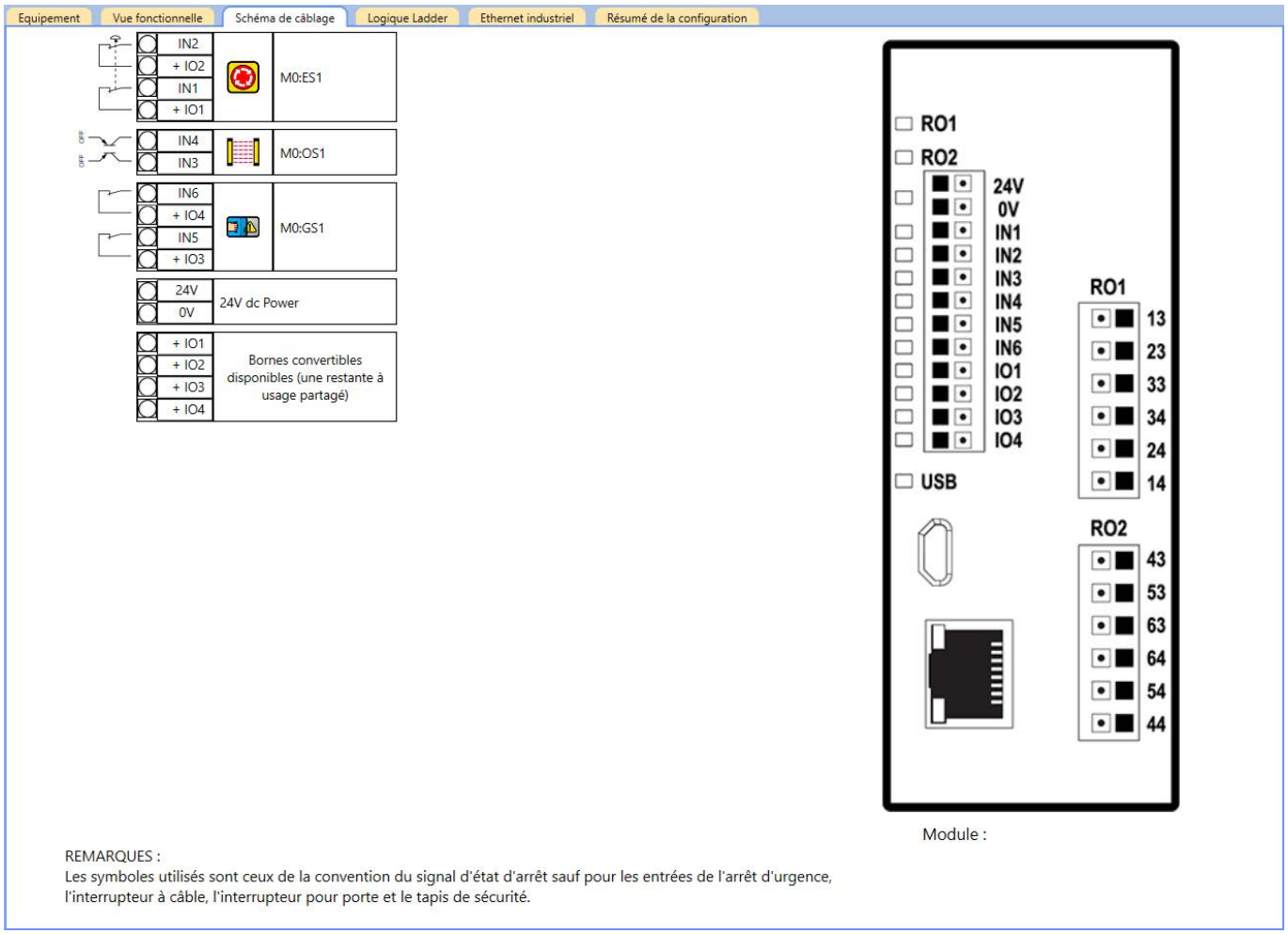
1. Cliquez sur **Nouveau projet** pour commencer un nouveau projet.
2. Sélectionnez SC10-2 **SC10-2**.
3. Définissez les paramètres du projet et cliquez sur **OK**.

Remarque: Vérifiez que la case à cocher **Désactiver la fonction d'optimisation automatique des bornes** est désactivée.

Le projet est créé.

4. Dans l'onglet **Équipement**, cliquez sur ✚ sous le contrôleur de sécurité.
   La fenêtre **Ajouter un équipement** s'affiche.
5. Ajoutez un bouton d'arrêt d'urgence et cliquez sur **OK** pour accepter les paramètres par défaut.
6. Cliquez sur ✚.
7. Ajoutez un capteur optique et cliquez sur **OK** pour accepter les paramètres par défaut.
8. Cliquez sur ✚.
9. Ajoutez un interrupteur de porte et cliquez sur **OK** pour accepter les paramètres par défaut.
10. Accédez à l'onglet **Schéma de câblage** et observez les bornes utilisées.

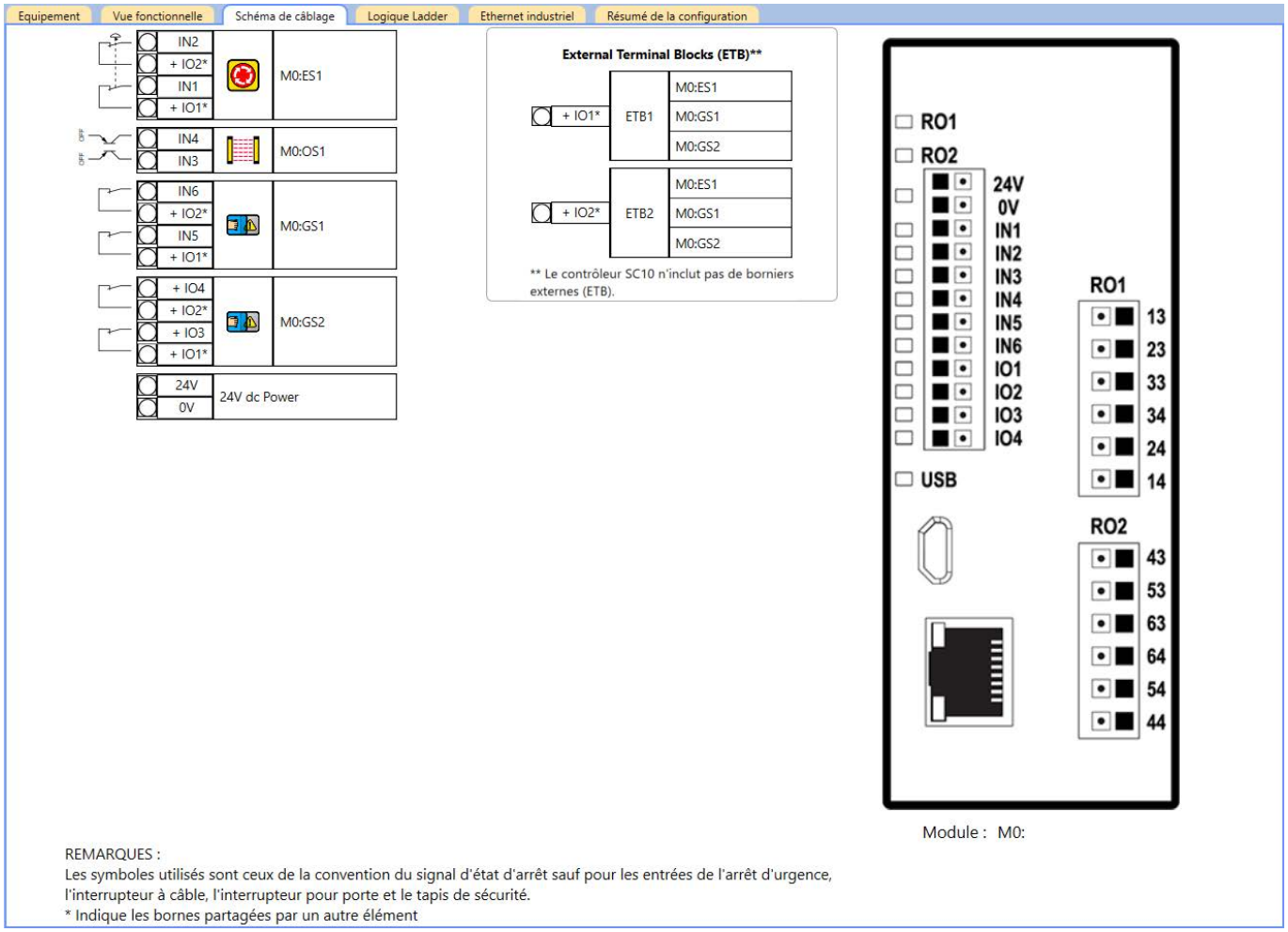
*Illustration 316. Onglet **Schéma de câblage** avec bouton d'arrêt d'urgence, capteur optique et interrupteur de porte*



11. Accédez à l'onglet **Équipement** et cliquez sur ✚.
12. Ajoutez un second interrupteur de porte et cliquez sur **OK** pour accepter les paramètres par défaut.
13. Accédez à l'onglet **Schéma de câblage** et remarquez que des borniers externes (ETB) ont été ajoutés pour prendre en compte le second interrupteur de porte.

Remarque: Les borniers externes sont fournis par l'utilisateur.

*Illustration 317. Onglet **Schéma de câblage** avec trois boutons d'arrêt d'urgence et des borniers externes*



15.12 Exemple de configuration du SC10-2 sans optimisation automatique des bornes

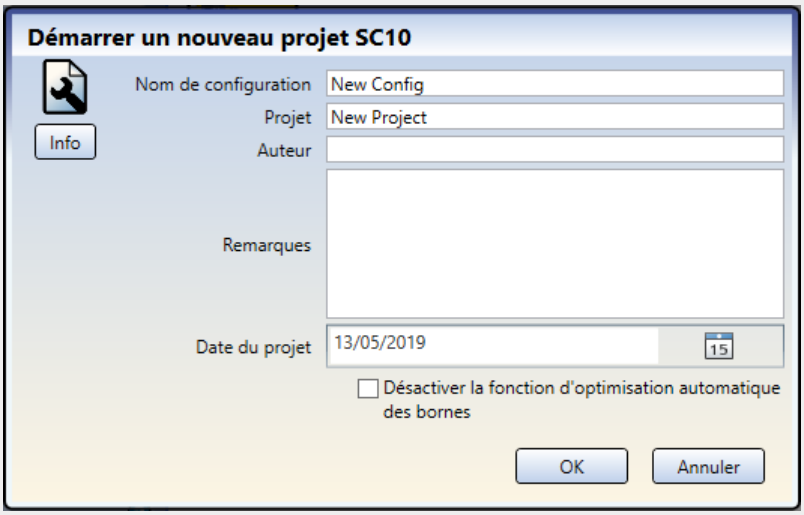
Procédez comme suit pour un exemple de configuration où la fonction d'optimisation automatique des bornes (ATO) est désactivée.

Remarque: Cette procédure est donnée à titre d'exemple uniquement.

1. Cliquez sur **Nouveau projet** pour commencer un nouveau projet.
2. Sélectionnez SC10-2 **SC10-2**.
3. Définissez les paramètres du projet, activez la case à cocher **Désactiver la fonction d'optimisation automatique des bornes**, et cliquez sur **OK**.

Remarque: Vérifiez que la case à cocher **Désactiver la fonction d'optimisation automatique des bornes** est activée.

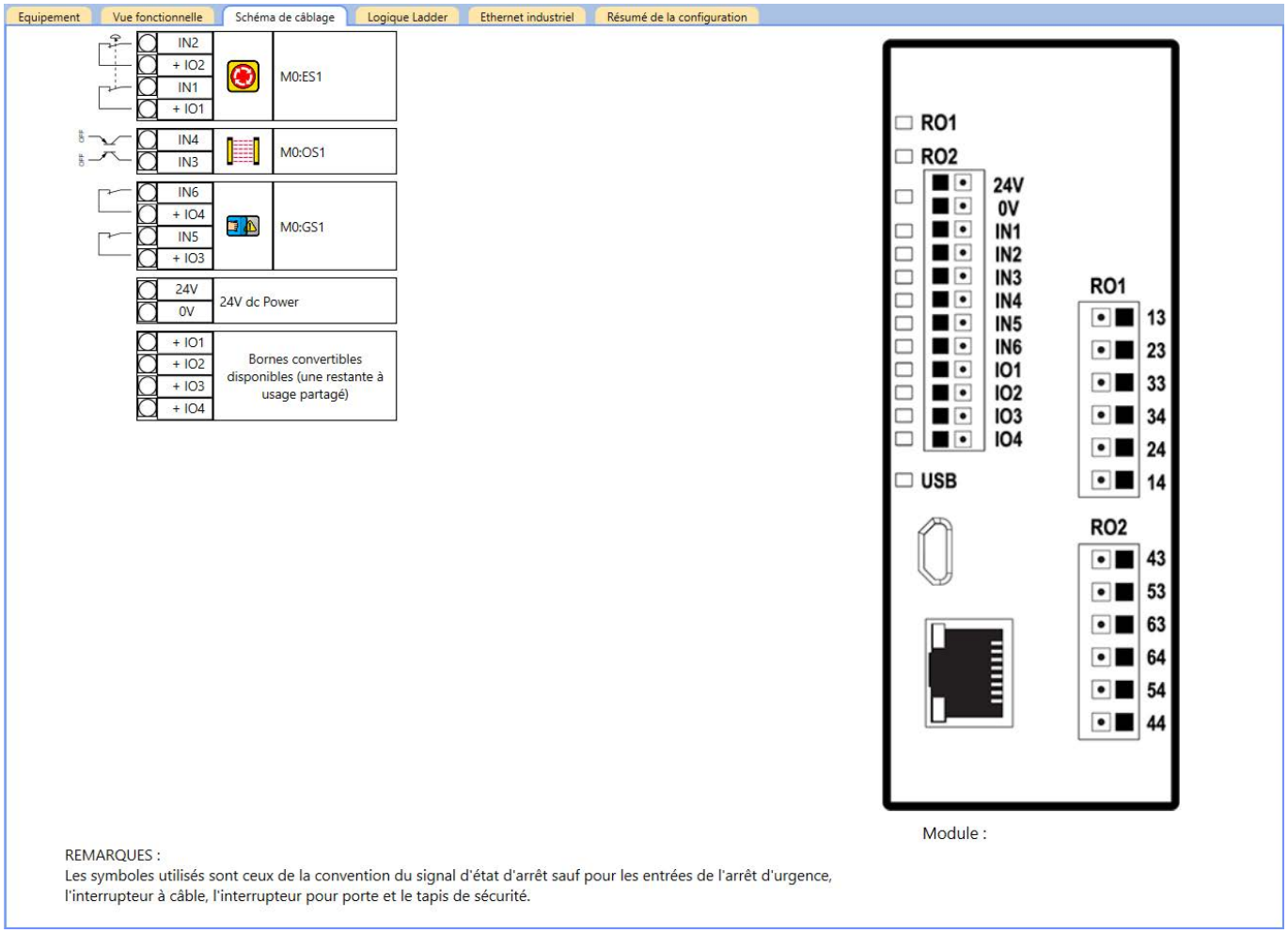
*Illustration 318. Option **Désactiver la fonction d'optimisation automatique des bornes** sélectionnée*



Le projet est créé.

4. Dans l'onglet **Équipement**, cliquez sur ✚ sous le contrôleur de sécurité.
   La fenêtre **Ajouter un équipement** s'affiche.
5. Ajoutez un bouton d'arrêt d'urgence et cliquez sur **OK** pour accepter les paramètres par défaut.
6. Cliquez sur ✚.
7. Ajoutez un capteur optique et cliquez sur **OK** pour accepter les paramètres par défaut.
8. Cliquez sur ✚.
9. Ajoutez un interrupteur de porte et cliquez sur **OK** pour accepter les paramètres par défaut.
10. Accédez à l'onglet **Schéma de câblage** et observez les bornes utilisées.

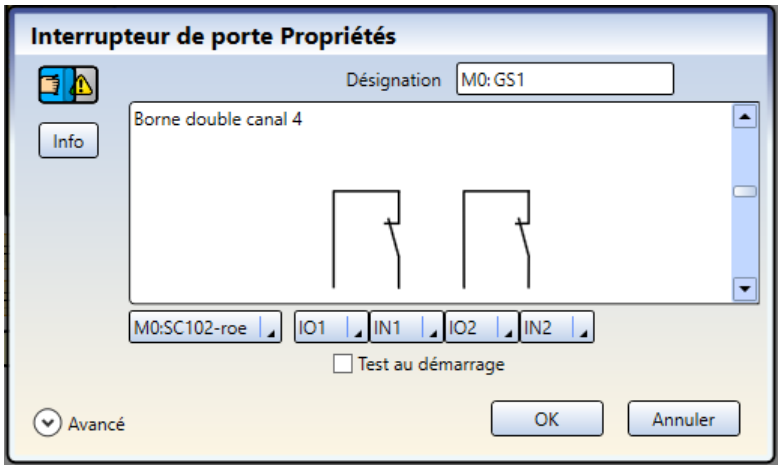
*Illustration 319. Onglet **Schéma de câblage** avec bouton d'arrêt d'urgence, capteur optique et interrupteur de porte*



11. Accédez à l'onglet **Équipement** et essayez d'ajouter un autre interrupteur de porte.

    Il est impossible d'ajouter un autre équipement (n'apparaît pas) car la fonction ATO est désactivée et il n'y a plus suffisamment de bornes pour prendre en charge d'autres équipements.
12. Accédez à l'onglet **Vue fonctionnelle** et essayez d'ajouter un autre interrupteur de porte.
    Aucun autre équipement ne peut être ajouté ici non plus car la fonction ATO est désactivée.
13. Cliquer sur **Annuler**.
14. Dans l'onglet **Vue fonctionnelle**, cliquez sur l'interrupteur de porte puis cliquez sur **Modifier** pour changer les propriétés.
    a) Remplacez respectivement les bornes IO3 et IO4 par IO1 et IO2.

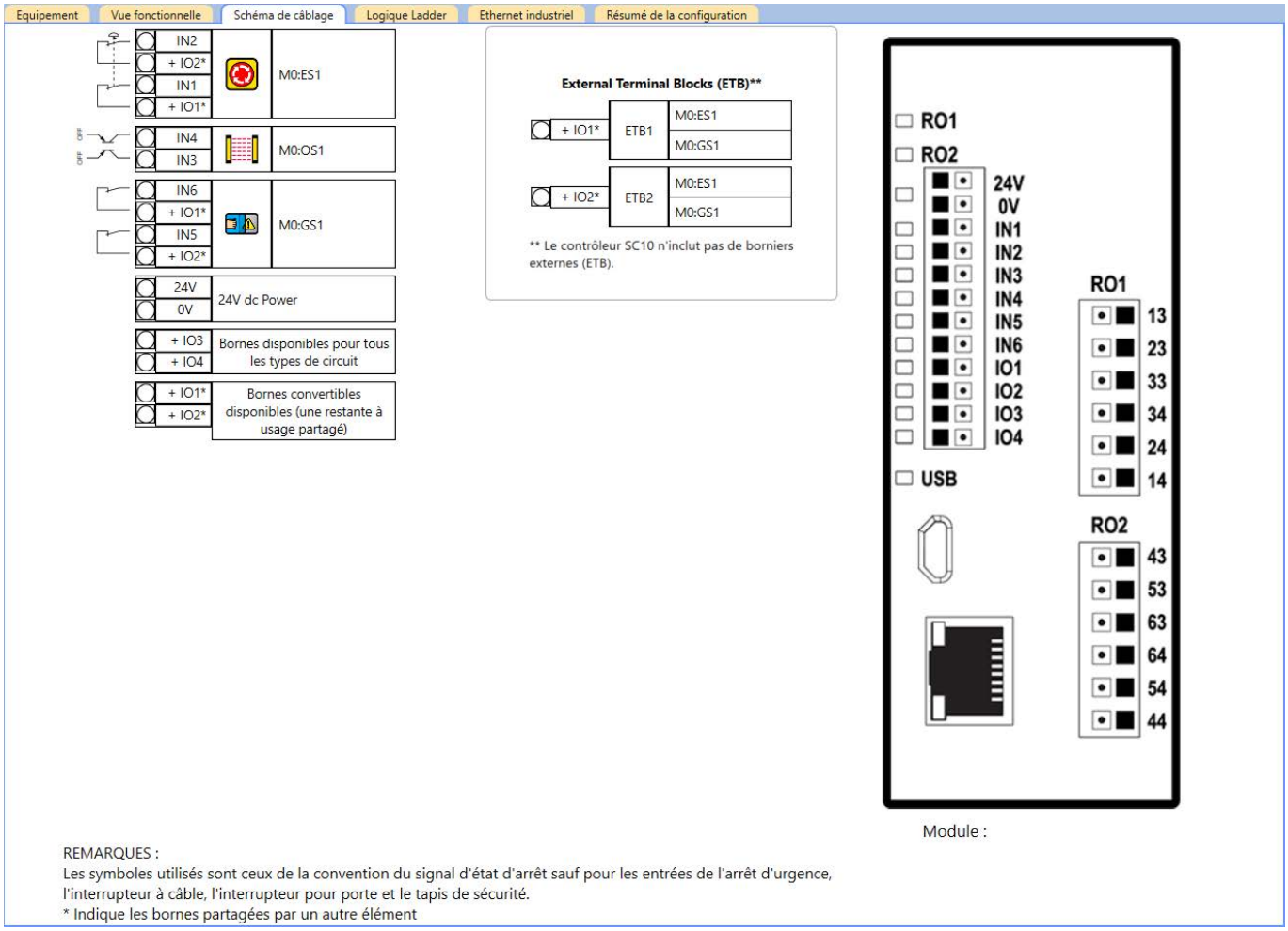
Illustration 320. Propriétés de l'interrupteur de porte



    b) Cliquez sur **OK**.
15. Accédez à l'onglet **Schéma de câblage** et remarquez que des borniers externes (ETB) ont été ajoutés pour prendre en compte la modification des assignations des bornes de l'interrupteur de porte.

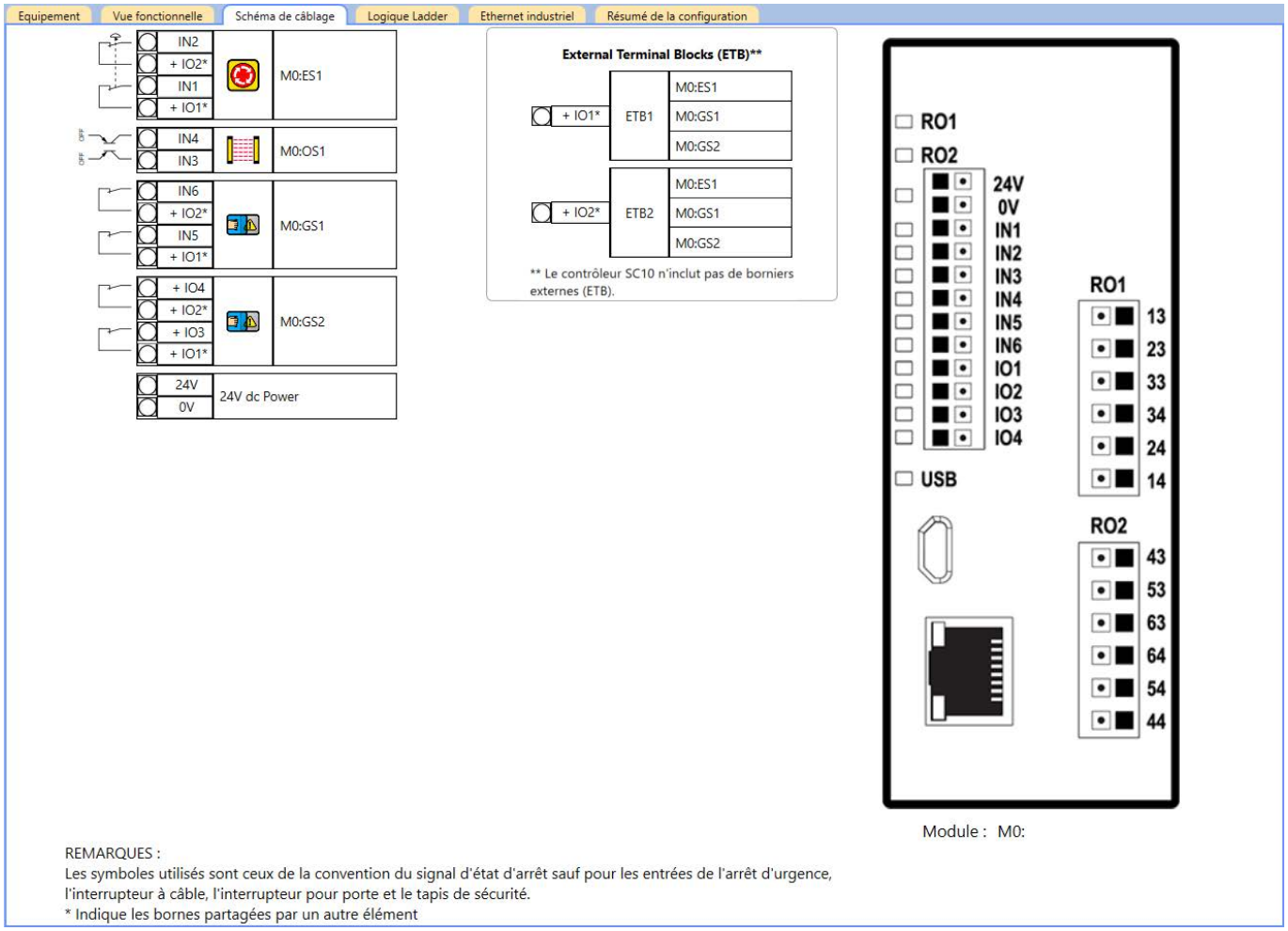
Remarque: Les borniers externes sont fournis par l'utilisateur.

*Illustration 321. Onglet **Schéma de câblage** avec bouton d'arrêt d'urgence, capteur optique, interrupteur de porte et borniers externes*



16. Accédez à l'onglet **Vue fonctionnelle** et essayez d'ajouter un autre interrupteur de porte.
    Il est désormais possible d'ajouter un autre interrupteur de porte car l'optimisation des bornes a été effectuée manuellement.
17. Ajoutez un second interrupteur de porte et cliquez sur **OK** pour accepter les paramètres par défaut.
18. Accédez à l'onglet **Schéma de câblage** et remarquez que le second interrupteur de porte a été ajouté sans bornier externe supplémentaire.

*Illustration 322. Onglet **Schéma de câblage** avec bouton d'arrêt d'urgence, capteur optique, interrupteurs de porte et borniers externes*



15.13 Modèles XS/SC26 sans interface embarquée : utilisation de la carte mémoire SC-XM2/3

Cette procédure concerne les modèles XS/SC26 et XS/SC26-2e.

Utilisez une carte SC-XM2 ou SC-XM3 pour :

- stocker une configuration confirmée ;
- configurer rapidement plusieurs contrôleurs de sécurité XS/SC26 avec la même configuration (FID 3 et ultérieur) ;
- remplacer un contrôleur de sécurité XS/SC26 par un autre au moyen de la carte SC-XM2/3 (FID 3 et ultérieur)

Remarque: Il faut disposer de l'outil de programmation de Banner (SC-XMP2) et du logiciel Contrôleur de sécurité Banner pour écrire une configuration confirmée sur une carte SC-XM2/3. De cette façon, l'accès est limité au personnel autorisé.

1. Créez la configuration voulue avec le logiciel.
   L'utilisation de la dernière version du logiciel est recommandée. Toutefois, certaines fonctions ne seront pas disponibles sur les contrôleurs de sécurité plus anciens. La liste de contrôle à gauche de l'écran du logiciel vous fournira des informations supplémentaires au fur et à mesure de la création de la configuration.
2. Vérifiez et confirmez la configuration en la chargeant sur le XS/SC26.
   Après examen et approbation de la configuration, cette dernière peut être enregistrée et utilisée par le contrôleur de sécurité.
3. Écrivez la configuration confirmée sur la carte SC-XM2/3 avec l'outil de programmation.

Remarque: Seule une configuration confirmée peut être stockée sur la carte SC-XM2/3. Référez-vous à la section Écrivez une configuration confirmée sur la carte SC-XM2/3 avec l'outil de programmation. à la page 94.

4. Utilisez une étiquette pour désigner la configuration stockée sur la carte SC-XM2/3.
5. Installez et/ou raccordez l'alimentation au XS/SC26 voulu (nouveau contrôleur de sécurité avec réglages d'usine ou contrôleur de sécurité configuré).

- **Contrôleurs FID 1 ou FID 2 :** la LED USB est éteinte.
- **Contrôleurs FID 3 ou ultérieur :** la LED USB clignote en vert si le XS/SC26 est un contrôleur de sécurité avec réglages d'usine. La LED USB est éteinte si le contrôleur de sécurité est un contrôleur configuré.

Remarque: Le réglage d'usine par défaut est basé sur les microprocesseurs de sécurité. La modification de l'adresse IP par défaut ne modifie pas ce paramètre. La configuration d'une telle unité avec la carte SC-XM2/3 écrasera les paramètres réseau.

6. Insérez la carte SC-XM2/3 dans le port micro USB du XS/SC26.

Remarque: Pour des informations complémentaires concernant les LED, voir État des LED du XS/SC26 à la page 320.

Contrôleur de sécurité FID 1 ou FID 2

- Si la LED USB clignote en vert pendant 5 secondes, la configuration sur le contrôleur de sécurité et sur la carte SC-XM2/3 est identique.
- Si la LED USB clignote en rouge pendant 5 secondes, la configuration sur le contrôleur de sécurité et sur la carte SC-XM2/3 est différente.

Contrôleur de sécurité avec réglages d'usine FID 3 ou ultérieur

- Si la LED USB clignote en vert pendant 4 secondes, puis reste fixe, la configuration, les paramètres réseau et les codes PIN/mots de passe sont automatiquement téléchargés sur le contrôleur de sécurité.
- Si la LED USB clignote en rouge pendant 5 secondes, la configuration sur la carte SC-XM2/3 a été créée avec une version plus ancienne du logiciel (4.1 ou antérieure) ou avec un contrôleur de sécurité FID 2 ou antérieur, et la carte est insérée dans un contrôleur de sécurité FID 3 ou ultérieur. Dès lors, la configuration ne peut pas être chargée automatiquement sauf si la configuration de la carte SC-XM2/3 est recréée avec la version 4.2 ou une version ultérieure du logiciel ou à l'aide d'un contrôleur de sécurité FID 3 avec écran.

Contrôleur de sécurité FID 3 ou ultérieur configuré

- Si une carte SC-XM2/3 avec une configuration contenant des informations créées avec le logiciel Contrôleur de sécurité Banner version 4.1 ou antérieure, ou créées à partir d'un contrôleur de sécurité FID 2 ou antérieur est insérée et :
  - La LED USB clignote en vert pendant 5 secondes, la configuration sur le contrôleur de sécurité et sur la carte SC-XM2/3 est identique.
  - La LED USB clignote en rouge pendant 5 secondes, la configuration sur la carte SC-XM2/3 est différente.
- Si une carte SC-XM2/3 avec une configuration contenant des informations créées avec le logiciel Contrôleur de sécurité Banner version 4.2 ou ultérieure, ou créées à partir d'un contrôleur de sécurité FID 3 ou ultérieur est insérée et :
  - La LED USB clignote en vert pendant 5 secondes, la configuration et les codes PIN/mots de passe sur le contrôleur de sécurité et sur la carte SC-XM2/3 sont identiques. Par ailleurs, si les paramètres réseau sont différents (modèles XS/SC26-2e), les paramètres réseau du contrôleur de sécurité sont transférés vers la carte SC-XM2/3, pour autant que cette carte SC-XM2/3 ne soit pas verrouillée. Si la carte SC-XM2/3 est verrouillée, la LED USB clignote en rouge pendant 5 secondes et si la carte SC-XM2/3 n'est pas retirée pendant ce délai, le contrôleur de sécurité se verrouille.
  - La LED USB clignote en rouge, la configuration ou les codes/PIN mots de passe sur le contrôleur de sécurité et sur la carte SC-XM2/3 sont différents. Si la carte SC-XM2/3 n'est pas retirée dans les 5 secondes, la LED d'alimentation/défaut clignote en rouge et le contrôleur de sécurité se verrouille.

7. Si le contrôleur de sécurité se verrouille, retirez la carte SC-XM2/3 et mettez le système hors tension puis sous tension ou effectuez un reset système.
8. Pour les contrôleurs de sécurité FID 3 ou ultérieur avec réglages d'usine : lorsque la LED USB arrête son clignotement rapide, mettez le système hors tension puis sous tension ou effectuez un reset système.

Le contrôleur de sécurité est prêt pour la mise en service. Référez-vous à la section Procédure de vérification à la mise en route à la page 312.

Remarque: Si le protocole industriel PROFINET était utilisé sur le contrôleur remplacé, utilisez l'API pour attribuer le même nom PROFINET au contrôleur de remplacement.

15.14 Modèles XS/SC26 avec interface embarquée : Utilisation de la carte mémoire SC-XM2/3

Les procédures suivantes concernent les modèles XS/SC26-2d, XS/SC26-2de et XS26-ISDd.

Utilisez une carte SC-XM2 ou SC-XM3 pour :

- stocker une configuration confirmée ;
- configurer rapidement plusieurs contrôleurs de sécurité XS/SC26 avec la même configuration ;

- remplacer un contrôleur de sécurité XS/SC26 par un autre au moyen de la carte SC-XM2/3 (fonction FID 3 ou ultérieur).

Remarque: Il faut disposer de l'outil de programmation de Banner (SC-XMP2) et du logiciel Contrôleur de sécurité Banner pour écrire une configuration confirmée sur une carte SC-XM2/3. De cette façon, l'accès est limité au personnel autorisé. Il est également possible d'écrire une configuration sur une carte SC-XM2/3 à l'aide d'un contrôleur de sécurité avec interface embarquée (modèles XS/SC26-2d, -2de et -ISDd).

Remarque: Le comportement des LED est le même avec ou sans interface embarquée (pour plus d'infos, voir la section Modèles XS/SC26 sans interface embarquée : utilisation de la carte mémoire SC-XM2/3 à la page 334). Toutefois, la procédure suivante se concentre sur ce qui se passe à l'écran.

15.14.1 XS/SC26 FID 1 ou FID 2 avec interface embarquée : Utilisation de la carte mémoire SC-XM2/3

Cette procédure est destinée aux modèles XS/SC26-2d et XS/SC26-2de.

1. Créez la configuration voulue avec le logiciel.
   L'utilisation de la dernière version du logiciel est recommandée. Toutefois, certaines fonctions ne seront pas disponibles sur les contrôleurs de sécurité plus anciens. La liste de contrôle à gauche de l'écran du logiciel vous fournira des informations supplémentaires au fur et à mesure de la création de la configuration.
2. Vérifiez et confirmez la configuration en la chargeant sur un XS/SC26.
   Après examen et approbation de la configuration, cette dernière peut être enregistrée et utilisée par le contrôleur de sécurité.
3. Écrivez la configuration confirmée sur la carte SC-XM2/3 avec l'outil de programmation ou l'interface embarquée (modèles XS/SC26-2d/2de).

   Remarque: Seule une configuration confirmée peut être stockée sur la carte SC-XM2/3.
4. Utilisez une étiquette pour désigner la configuration stockée sur la carte SC-XM2/3.
5. Installez et/ou raccordez l'alimentation au XS/SC26 voulu (nouveau contrôleur de sécurité avec réglages d'usine ou contrôleur de sécurité configuré).
   La LED USB est éteinte.
6. Insérez la carte SC-XM2/3 dans le port micro USB du XS/SC26.
   - Si une carte SC-XM2/3 avec une configuration
     - créée avec le logiciel Contrôleur de sécurité Banner version 4.1 ou antérieure, ou créée à partir d'un contrôleur de sécurité FID 2 ou antérieur
     - créée avec le logiciel Contrôleur de sécurité Banner version 4.2 ou antérieure, ou créée à partir d'un contrôleur de sécurité FID 3 ou ultérieur

     est enfichée dans un contrôleur de sécurité FID 1 ou FID 2 configuré, un des écrans suivants s'affiche selon que la configuration est identique ou non à celle du contrôleur de sécurité :

Illustration 323. Correspondance



Illustration 324. Configuration différente



Pour des instructions sur l'importation de données à partir de la carte mémoire SC-XM2/3, voir la section Mode de configuration du XS/SC26 à la page 177.

- Si une carte SC-XM2/3 vide est enfichée dans un contrôleur de sécurité FID 1 ou FID 2 configuré, l'écran indique le problème suivant :

Illustration 325. Carte SC-XM2/3 vide



Le contrôleur de sécurité est prêt pour la mise en service. Référez-vous à la section Procédure de vérification à la mise en route à la page 312.

Remarque: Si le protocole industriel PROFINET était utilisé sur le contrôleur remplacé, utilisez l'API pour attribuer le même nom PROFINET au contrôleur de remplacement.

15.14.2 Contrôleurs XS/SC26 FID 3 à FID 6 avec interface embarquée : Utilisation des modèles SC-XM2/3

Cette procédure concerne les modèles XS/SC26-2d, XS/SC26-2de et XS26-ISDd.

1. Créez la configuration voulue avec le logiciel.

   L'utilisation de la dernière version du logiciel est recommandée. Toutefois, certaines fonctions ne seront pas disponibles sur les contrôleurs de sécurité plus anciens. La liste de contrôle à gauche de l'écran du logiciel vous fournira des informations supplémentaires au fur et à mesure de la création de la configuration.
2. Vérifiez et confirmez la configuration en la chargeant sur un XS/SC26.
   Après examen et approbation de la configuration, cette dernière peut être enregistrée et utilisée par le contrôleur de sécurité.
3. Écrivez la configuration confirmée sur la carte SC-XM2/3 avec l'outil de programmation ou l'interface embarquée (modèles XS/SC26-2d et -2de et modèles XS26-ISDd).

   Remarque: Seule une configuration confirmée peut être stockée sur la carte SC-XM2/3.
4. Utilisez une étiquette pour désigner la configuration stockée sur la carte SC-XM2/3.
5. Installez et/ou raccordez l'alimentation au XS/SC26 voulu (nouveau contrôleur de sécurité avec réglages d'usine ou contrôleur de sécurité configuré).
   - La LED USB clignote en vert si le XS/SC26 est un contrôleur de sécurité avec réglages d'usine.
   - La LED USB est éteinte si le contrôleur de sécurité est un contrôleur configuré.

   Remarque: La configuration d'usine par défaut est basée sur les micros de sécurité. La modification de l'adresse IP par défaut ne modifie pas ce paramètre. La configuration d'une telle unité avec la carte SC-XM2/3 écrasera les paramètres réseau.
6. Insérez la carte SC-XM2/3 dans le port micro USB du XS/SC26.

   Contrôleur de sécurité avec réglages d'usine
   - Si le FID de la configuration ne correspond pas au FID du contrôleur de sécurité, la configuration ne correspondra pas. L'écran signale le problème et commence le décompte jusqu'au verrouillage du système :

     Illustration 326. Non-concordance FID

   - Si la configuration inclut ISD mais que le contrôleur de sécurité n'est pas un XS26-ISD, la configuration est rejetée. L'écran signale le problème et commence le décompte jusqu'au verrouillage du système :

     Illustration 327. Non-concordance ISD

   - Si une carte SC-XM2/3 avec une configuration contenant des informations créées à l'aide du logiciel Contrôleur de sécurité Banner version 4.2 ou ultérieure, ou créées à partir d'un contrôleur de sécurité FID 3 ou ultérieur est enfichée dans un contrôleur de sécurité FID 3 ou ultérieur avec réglages d'usine, la configuration, les paramètres réseau et les codes PIN/mots de passe sont téléchargés automatiquement dans le contrôleur de sécurité. L'écran signale le chargement automatique :

Illustration 328. État de chargement automatique



Après le chargement automatique, l'écran indique que la configuration a été reçue et qu'il faut effectuer une remise sous tension ou un reset système.

- Si une carte SC-XM2/3 contenant des informations créées avec le logiciel Contrôleur de sécurité Banner version 4.1 ou antérieure ou créées à partir d'un contrôleur de sécurité FID 2 ou antérieur est enfichée dans un contrôleur de sécurité FID 3 ou ultérieur avec réglages d'usine, la configuration ne correspondra pas :

Illustration 329. Configuration différente



- Si une carte SC-XM2/3 vide est enfichée dans un contrôleur de sécurité FID 3 ou ultérieur avec réglages d'usine, l'écran signale le problème et commence le décompte jusqu'au verrouillage du système :

Illustration 330. Erreur SC-XM2/3



Si la carte SC-XM2/3 n'est pas retirée du contrôleur de sécurité dans les 3 secondes, le contrôleur de sécurité se verrouille :

Illustration 331. Verrouillage du système



Contrôleur de sécurité configuré

- Si une carte SC-XM2/3 avec une configuration contenant des informations créées avec le logiciel Contrôleur de sécurité Banner version 4.1 ou antérieure ou créées à partir d'un contrôleur de sécurité FID 2 ou antérieur est enfichée dans un contrôleur de sécurité FID 3 ou ultérieur configuré, un des écrans suivants s'affiche selon que la configuration correspond ou non à celle du contrôleur de sécurité :

Illustration 332. Correspondance



Illustration 333. Configuration différente



Pour des instructions sur l'importation de données à partir de la carte mémoire SC-XM2/3, voir la section Mode de configuration du XS/SC26 à la page 177.

- Si une carte SC-XM2/3 avec une configuration contenant des informations créées à l'aide du logiciel Contrôleur de sécurité Banner version 4.2 ou ultérieure, ou créées à partir d'un contrôleur de sécurité FID 3 ou ultérieur est enfichée dans un contrôleur de sécurité FID 3 ou ultérieur configuré et que la configuration et les codes PIN/mots de passe correspondent, un des écrans suivants s'affiche :

Illustration 334. Modèles XS/SC26-2d : écran indiquant que les paramètres réseau sont ignorés



Illustration 335. Modèles XS/SC26-2de et XS26-ISDd : les paramètres réseau correspondent



Par ailleurs, si les paramètres réseau sont différents (modèles XS/SC26-2de), les paramètres réseau du contrôleur de sécurité sont transférés vers la carte SC-XM2/3. Une fois cette opération terminée, l'écran affiche ce qui suit :

Illustration 336. Mise à jour du réseau



Cliquez sur **OK**. Si la mise à jour échoue (par exemple si la carte SC-XM2/3 est verrouillée), l'écran affiche le motif de l'échec et démarre le décompte jusqu'au verrouillage du système :

Illustration 337. Échec de la mise à jour du réseau



Si la carte SC-XM2/3 n'est pas retirée du contrôleur de sécurité dans les 3 secondes, le contrôleur de sécurité se verrouille :

Illustration 338. Verrouillage du système



- Si une carte SC-XM2/3 avec une configuration contenant des informations créées à l'aide du logiciel Contrôleur de sécurité Banner version 4.2 ou ultérieure, ou créées à partir d'un contrôleur de sécurité FID 3 ou ultérieur est enfichée dans un contrôleur de sécurité FID 3 ou ultérieur configuré, mais que la configuration et les codes PIN/mots de passe ne correspondent pas, l'écran signale le problème et commence le décompte jusqu'au verrouillage du système :

Illustration 339. Modèles XS/SC26-2d : configuration différente



Illustration 340. Modèles XS/SC26-2de : configuration différente



Si la carte SC-XM2/3 n'est pas retirée du contrôleur de sécurité dans les 3 secondes, le contrôleur de sécurité se verrouille :

Illustration 341. Modèles XS/SC26-2d : verrouillage du système



Illustration 342. Modèles XS/SC26-2de : verrouillage du système



Pour des instructions sur l'importation de données à partir de la carte mémoire SC-XM2/3, voir la section Mode de configuration du XS/SC26 à la page 177.

- Si une carte SC-XM2/3 vide est enfichée dans un contrôleur de sécurité FID 3 ou ultérieur configuré, l'écran signale le problème et commence le décompte jusqu'au verrouillage du système :

Illustration 343. Erreur SC-XM2/3



Si la carte SC-XM2/3 n'est pas retirée du contrôleur de sécurité dans les 3 secondes, le contrôleur de sécurité se verrouille :

Illustration 344. Verrouillage du système



7. Si le contrôleur de sécurité se verrouille, retirez la carte SC-XM2/3 et mettez le système hors tension puis sous tension ou effectuez un reset système.
8. Pour les contrôleurs de sécurité avec réglages d'usine : lorsque la LED USB arrête son clignotement rapide, mettez le système hors tension puis sous tension ou effectuez un reset système.

Le contrôleur de sécurité est prêt pour la mise en service. Référez-vous à la section Procédure de vérification à la mise en route à la page 312.

Remarque: Si le protocole industriel PROFINET a été utilisé sur le contrôleur remplacé, utilisez l'API pour attribuer le même nom PROFINET au contrôleur de remplacement.

15.14.3 Contrôleurs XS/SC26 FID 7 et ultérieurs avec interface embarquée : Utilisation de la carte mémoire SC-XM2/3

Cette procédure est destinée aux modèles XS/SC26-2d, XS/SC26-2de et XS26-ISDd.

Voir Contrôleurs XS/SC26 FID 3 à FID 6 avec interface embarquée : Utilisation des modèles SC-XM2/3 à la page 337 pour la procédure.

La différence réside dans le fait que les contrôleurs FID 7 et ultérieurs stockent également les paramètres Configuration via le réseau et Surveillance en temps réel via les paramètres réseau ainsi que les mots de passe réseau.

15.15 SC10-2 : Utilisation de la carte mémoire SC-XM3

Utilisez une carte mémoire SC-XM3 pour :

- configurer rapidement plusieurs contrôleurs de sécurité SC10-2; avec la même configuration ;
- remplacer un contrôleur de sécurité SC10-2 par un autre avec la carte SC-XM3 de l'ancien contrôleur de sécurité.

Remarque: Il faut disposer de l'outil de programmation de Banner (SC-XMP2) et du logiciel pour écrire une configuration confirmée sur une carte SC-XM3. De cette façon, l'accès est limité au personnel autorisé.

1. Créez la configuration voulue avec le logiciel.
2. Vérifiez et confirmez la configuration en la chargeant sur un SC10-2.
   Après examen et approbation de la configuration, cette dernière peut être enregistrée et utilisée par le contrôleur de sécurité.
3. Écrivez la configuration confirmée sur la carte SC-XM3 avec l'outil de programmation.

   Remarque: Seule une configuration confirmée peut être stockée sur la carte SC-XM3. Référez-vous à la section Écrivez une configuration confirmée sur la carte SC-XM2/3 avec l'outil de programmation. à la page 94.
4. Utilisez une étiquette pour désigner la configuration stockée sur la carte SC-XM3.
5. Installez et/ou raccordez l'alimentation au SC10-2 voulu (nouveau contrôleur de sécurité avec réglages d'usine ou contrôleur de sécurité configuré).
   - Si le contrôleur de sécurité SC10-2 n'est pas configuré (réglages d'usine), le voyant d'alimentation/défaut est vert fixe et le voyant USB clignote en vert pour indiquer que le contrôleur de sécurité est en attente d'une configuration.
   - Si le SC10-2 est un contrôleur de sécurité configuré, le voyant d'alimentation/défaut est vert fixe et le voyant USB rouge fixe.

   Remarque: Le réglage d'usine par défaut est basé sur les microprocesseurs de sécurité. La modification de l'adresse IP par défaut ne modifie pas ce paramètre. La configuration d'une telle unité avec la carte SC-XM2/3 écrasera les paramètres réseau.
6. Insérez la carte SC-XM3 dans le port micro USB du SC10-2.

   Contrôleur de sécurité avec réglages d'usine
   - Le voyant USB clignote rapidement pendant 3 secondes puis reste allumé et la configuration, les paramètres réseau et les codes PIN sont automatiquement téléchargés sur le contrôleur de sécurité. Ensuite, le voyant d'alimentation/défaut clignote en vert pour indiquer que le contrôleur de sécurité attend une mise hors tension suivie d'une remise sous tension.

   Contrôleur de sécurité configuré
   - Si la configuration et les codes PIN sur le contrôleur de sécurité et sur la carte SC-XM3 correspondent, le voyant USB clignote en vert pendant 3 secondes, puis reste allumé. Par ailleurs, si les paramètres réseau ne correspondent pas, les paramètres réseau du contrôleur de sécurité sont transférés vers la carte SC-XM3 après 3 secondes, pour autant que cette carte SC-XM3 ne soit pas verrouillée. Si la carte SC-XM3 est verrouillée, le contrôleur passe en état de verrouillage.
   - Si la configuration et les codes PIN sur le contrôleur de sécurité et sur la carte SC-XM3 ne correspondent pas, le voyant USB clignote en rouge. Si la carte SC-XM3 n'est pas retirée du contrôleur de sécurité dans les 3 secondes, les voyants USB et d'alimentation/défaut clignotent en rouge et le contrôleur bascule alors en état de verrouillage.
7. Coupez puis rétablissez l'alimentation électrique.
   Le voyant d'alimentation/défaut est vert, le voyant USB est vert (si la carte SC-XM3 est toujours enfichée) ou rouge (pas de carte SC-XM3 ou de câble USB connecté), et les voyants d'entrée et de sortie affichent l'état d'entrée réel.

Le contrôleur de sécurité est prêt pour la mise en service. Référez-vous à la section Procédure de vérification à la mise en route à la page 312.

15.16 Réinitialisation des réglages d'usine pour le contrôleur

Pour réinitialiser le contrôleur de sécurité XS/SC26 FID 3 ou ultérieur ou SC10-2 aux réglages d'usine, procédez comme suit.

Remarque: Le contrôleur XS/SC26 FID 1 ou FID 2 utilisant la version logicielle 4.2 ou ultérieure affiche l'option **Réinitialiser les réglages d'usine** en grisé.

Le contrôleur de sécurité doit être mis sous tension et connecté au PC via le câble SC-USB2 ou via un câble Ethernet (modèles Ethernet XS/SC26 FID 7 ou ultérieur).

1. Cliquez sur .
2. Cliquez sur **Réinitialisation des réglages d'usine**.
   L'avertissement qui s'affiche vous signale que tous les réglages vont être rétablis aux valeurs par défaut.
3. Cliquez sur **Continuer**.
   L'écran **Entrer le mot de passe** s'affiche.
4. Entrez le code PIN Utilisateur1 s'il est connecté via USB ou le mot de passe s'il est connecté via Ethernet et cliquez sur **OK**.
   Le contrôleur de sécurité est mis à jour avec les réglages d'usine et une fenêtre de confirmation s'affiche.
5. Cliquez sur **OK**.
6. Coupez puis rétablissez l'alimentation électrique.
   La réinitialisation des réglages d'usine est terminée.

15.17 Réglages d'usine

Le tableau suivant répertorie certains des paramètres, ou réglages, par défaut du contrôleur de sécurité et du logiciel.

Réglage	Valeur par défaut	Produit applicable
Fonction AVM	50 ms	XS/SC26, SC10-2
Temps d'anti-rebond fermé à ouvert	6 ms	XS/SC26, SC10-2
EDM	Pas de surveillance	XS/SC26, SC10-2
Bloc fonction : Bloc de dérivation — Nœuds par défaut	IN, BP	XS/SC26, SC10-2
Bloc fonction : Dérivation — Limite de temps	1 s	XS/SC26, SC10-2
Bloc fonction : Bloc de temporisation — Nœuds par défaut	IN	XS/SC26, SC10-2
Bloc fonction : Bloc de temporisation — Temporisation de sortie	100 ms	XS/SC26, SC10-2
Bloc fonction : Bloc dispositif de commande — Nœuds par défaut	ED, IN, RST	XS/SC26, SC10-2
Bloc fonction : Bloc dispositif de commande — Limite de temps	1 s	XS/SC26, SC10-2
Bloc fonction : Bloc de reset à verrouillage — Nœuds par défaut	IN, LR	XS/SC26, SC10-2
Bloc fonction : Bloc d'inhibition — Nœuds par défaut	IN, MP1	XS/SC26, SC10-2
Bloc fonction : Bloc d'inhibition — Limite de temps	30 s	XS/SC26, SC10-2
Bloc fonction : Bloc de commande bimanuel — Nœuds par défaut	TC	XS/SC26, SC10-2
Bloc fonction : Bloc 1 impulsion — Nœuds par défaut	IN	XS/SC26
Bloc fonction : Bloc 1 impulsion — Limite de temps	100 ms	XS/SC26
Ethernet industriel : Chaîne (protocoles EtherNet/IP et PCCC)	32 bits	XS/SC26, SC10-2
Paramètres réseau : Adresse de passerelle	0.0.0.0	XS/SC26, SC10-2
Paramètres réseau : Adresse IP	192.168.0.128	XS/SC26, SC10-2
Paramètres réseau : Vitesse de liaison et mode duplex	Négociation auto	XS/SC26, SC10-2
Paramètres réseau : Masque de sous-réseau	255.255.255.0	XS/SC26, SC10-2

Réglage	Valeur par défaut	Produit applicable
Paramètres réseau : Port TCP	502	XS/SC26, SC10-2
Temps anti-rebond ouvert à fermé	50 ms	XS/SC26, SC10-2
Code PIN Utilisateur1	1901	XS/SC26, SC10-2
Code PIN Utilisateur2	1902	XS/SC26, SC10-2
Code PIN Utilisateur3	1903	XS/SC26, SC10-2
Mot de passe Ethernet Utilisateur1	1901@Banner	XS/SC26
Mode à la mise sous tension	Normal	SC10-2
Sorties de sécurité	Reset automatique	XS/SC26, SC10-2
Sorties de sécurité : Mode à la mise sous tension	Normal	XS/SC26
Sorties de sécurité : Diviser (sorties de sécurité)	Fonctionnement par paires	XS/SC26
Mode simulation : Vitesse de simulation	1	XS/SC26, SC10-2
Optimisation automatique des bornes	Activé(e)	SC10-2
Conventions pour les signaux d’état des sorties	Actif = PNP On	XS/SC26, SC10-2
Fréquence de clignotement de la sortie d'état	Aucune	XS/SC26

16 Recherche de pannes

Le contrôleur de sécurité a été conçu et testé pour bien résister aux parasites électriques produits par les environnements industriels. Toutefois, des sources de parasites électriques intenses qui produisent des interférences électromagnétiques (EMI) ou des interférences radioélectriques (RFI) au-delà de ces limites peuvent entraîner un déclenchement ou un verrouillage aléatoire.

Si des déclenchements ou des verrouillages aléatoires se produisent, vérifiez ce qui suit :

- La tension d'alimentation est dans la plage 24 Vcc +/- 20 %.
- Les borniers enfichables du contrôleur de sécurité sont correctement insérés.
- Les raccordements des bornes individuelles sont bons.
- Aucune source de parasites à haute tension, à haute fréquence ni aucune ligne à haute tension ne passe à proximité du contrôleur de sécurité ou le long de câbles raccordés au contrôleur de sécurité.
- Une suppression de parasites est appliquée aux charges de sortie.
- La température autour du contrôleur de sécurité fait partie de la plage de température ambiante admise (voir Spécifications et exigences à la page 21).

16.1 Logiciel : recherche de pannes

Le bouton Mode temps réel n'est pas accessible (grisé)

1. Vérifiez que le câble SC-USB2 est enfiché dans l'ordinateur et le contrôleur de sécurité.

   Remarque: Il est préférable d'utiliser le câble Banner de SC-USB2. Si vous utilisez d'autres câbles USB, assurez-vous que le câble inclut une ligne de communication. De nombreux câbles de charge de téléphones mobiles ne possèdent pas de ligne de communication.
2. Vérifiez que le contrôleur de sécurité est correctement installé — Voir la section Vérification de l'installation des pilotes à la page 347.
3. Quittez le logiciel.
4. Débranchez le contrôleur de sécurité et rebranchez-le.
5. Lancez le logiciel.

Impossible de lire la configuration sur le contrôleur de sécurité ou d'envoyer la configuration au contrôleur de sécurité (boutons grisés)

1. Vérifiez que le **Mode temps réel** est désactivé.
2. Vérifiez que le câble SC-USB2 est enfiché dans l'ordinateur et le contrôleur de sécurité.

   Remarque: Il est préférable d'utiliser le câble Banner de SC-USB2. Si vous utilisez d'autres câbles USB, assurez-vous que le câble inclut une ligne de communication. De nombreux câbles de charge de téléphones mobiles ne possèdent pas de ligne de communication.
3. Vérifiez que le contrôleur de sécurité est correctement installé — Voir la section Vérification de l'installation des pilotes à la page 347.
4. Quittez le logiciel.
5. Débranchez le contrôleur de sécurité et rebranchez-le.
6. Lancez le logiciel.

Impossible de déplacer un bloc vers un autre emplacement

Tous les blocs ne peuvent pas être déplacés. Certains blocs peuvent être uniquement déplacés au sein de certaines sections.

- Les **sorties de sécurité** sont statiques et ne peuvent pas être déplacées. Les **sorties de sécurité de référence** peuvent être déplacées n'importe où dans les sections de gauche et du milieu.
- Les **entrées de sécurité** et les **entrées auxiliaires** peuvent être déplacées n'importe où au sein des sections de gauche et du milieu.
- Les **blocs fonction** et les **blocs logiques** peuvent être déplacés n'importe où au sein de la colonne du milieu.

Le bouton SC-XM2/3 n'est pas accessible (grisé)

1. Vérifiez que tout est bien raccordé — De l'outil SC-XMP2 au port USB de l'ordinateur et à la carte mémoire SC-XM2 ou SC-XM3.
2. Vérifiez que l'outil de programmation SC-XMP2 est correctement installé — voir la section Vérification de l'installation des pilotes à la page 347.
3. Quittez le logiciel.
4. Débranchez et rebranchez tous les raccordements — De l'outil SC-XMP2 au port USB et à la carte SC-XM2 ou SC-XM3.
5. Lancez le logiciel.

Remarque: Contactez Banner Engineering si vous avez besoin d'une assistance supplémentaire.

16.2 Logiciel : codes d'erreur

Le tableau suivant répertorie les codes d'erreur que vous pouvez rencontrer lorsque vous configurez une connexion non valide entre les blocs dans l'onglet **Vue fonctionnelle**.

AVERTISSEMENT:

- **Configuration conforme aux normes applicables**
- Le fait de ne pas vérifier l'application peut entraîner des blessures graves, voire mortelles.
- Le logiciel Contrôleur de sécurité Banner vérifie principalement la configuration logique pour détecter des erreurs de connexion. Il incombe à l'utilisateur de vérifier que l'application répond aux exigences de l'évaluation des risques et qu'elle est conforme à toutes les normes applicables.

Code du logiciel	Erreur
A.1	Cette connexion crée une boucle.
A.2	Il existe déjà une connexion à partir de ce bloc.
A.3	La connexion d'un bloc à lui-même n'est pas autorisée.
B.2	Ce bloc de dérivation est connecté au nœud **TC** d'un bloc Commande bimanuelle. Vous ne pouvez connecter qu'une entrée de commande bimanuelle au nœud **IN** de ce bloc Dérivation.
B.3	Ce bloc de dérivation est déjà connecté à un autre bloc.
B.4	Ce bloc de dérivation est connecté au nœud **TC** d'un bloc de commande bimanuelle et ne peut pas être connecté à d'autres blocs.
B.5	Impossible de connecter cette entrée de commande bimanuelle au nœud **IN** de ce bloc Dérivation car l'option « La sortie se désactive quand les deux entrées (**IN** et **BP**) sont activées » est désactivée.
B.6	Le nœud **IN** d'un bloc Dérivation ne peut pas être connecté aux entrées d'arrêt d'urgence et d'interrupteur à câble.
B.7	Le nœud **IN** d'un bloc Dérivation ne peut pas être connecté aux entrées d'arrêt d'urgence et d'interrupteur à câble via d'autres blocs.
C.1	Seule une entrée d'annulation de temporisation peut être connectée à un nœud **CD**.
C.2	Une entrée d'annulation de temporisation peut être uniquement connectée à un nœud **CD** d'une sortie de sécurité, d'un bloc fonction 1 impulsion ou d'un bloc fonction Temporisation.
D.1	Cette entrée EDM est configurée pour un circuit à 2 bornes double canal et peut être uniquement connectée au nœud **EDM** d'une sortie de sécurité.
E.1	Les nœuds de sortie du bloc Dispositif d'activation (**P** ou **S**) peuvent être uniquement connectés au nœud **IN** d'une sortie de sécurité.
E.2	Le nœud **IN** d'un bloc appareil de commande ne peut pas être connecté aux entrées arrêt d'urgence et interrupteur à câble.
E.3	Le nœud **ED** d'un bloc appareil de commande peut être uniquement connecté à une entrée d'appareil de commande.
E.4	Le nœud **ED** d'un bloc appareil de commande ne peut pas être connecté aux entrées arrêt d'urgence et interrupteur à câble via d'autres blocs.
E.5	Un bloc Dispositif de commande dont un bloc de commande bimanuelle est connecté au nœud **IN** ne peut pas être connecté à une sortie de sécurité dont l'option *Temporisation de sortie de sécurité* est configuré sur « Retard au déclenchement ».
F.1	Les entrées d'arrêt d'urgence et d'interrupteur à câble ne peuvent pas être inhibées, et ne peuvent donc pas être connectées au nœud **IN** d'un bloc fonction Inhibition ou à l'entrée **M Safety** du bloc fonction Entrées de commande de presse.
F.2	Les entrées arrêt d'urgence et interrupteur à câble ne peuvent pas être connectées à un bloc de reset à verrouillage connecté à un bloc d'inhibition.
F.3	Un bloc de reset à verrouillage connecté à une entrée arrêt d'urgence ou interrupteur à câble ne peut pas être connecté à un bloc d'inhibition.
G.1	**XS/SC26 FID 1, 2, & 3 et SC10-2:** seule une sortie de reset manuel peut être connectée au nœud **FR** d'une sortie de sécurité. **XS/SC26 FID 4 ou ultérieur :** seule une entrée de reset manuel ou un nœud de sortie d'un bloc OR (OU) désigné de reset peut être connecté au nœud **FR** d'une sortie de sécurité.
G.2	**XS/SC26 FID 1, 2, & 3 et SC10-2 :** seule une entrée de reset manuel peut être connectée au nœud **LR** d'un bloc Reset à verrouillage ou d'une sortie de sécurité. **XS/SC26 FID 4 ou ultérieur :** seule une entrée de reset manuel ou le nœud de sortie d'un bloc OR (OU) désigné de reset peut être connecté au nœud **LR** d'un bloc Reset à verrouillage ou d'une sortie de sécurité.

Code du logiciel	Erreur
G.3	**XS/SC26 FID 1, 2, & 3 et SC10-2 :** seule une entrée de reset manuel peut être connectée au nœud **RST** d'un bloc Dispositif d'activation. **XS/SC26 FID 4 ou ultérieur :** seule une entrée de reset manuel ou un nœud de sortie d'un bloc OR (OU) désigné de reset peut être connecté au nœud **RST** d'un bloc Dispositif d'activation.
G.4	**XS/SC26 FID 1, 2, & 3 et SC10-2 :** une entrée de reset manuel peut être uniquement connectée aux nœuds **LR** et **FR** d'une sortie de sécurité, à un nœud **LR** d'un bloc Reset à verrouillage, à un nœud **RST** d'un bloc Dispositif d'activation et aux nœuds **SET** et **RST** des blocs Bascule. **XS/SC26 FID 4 ou ultérieur :** une entrée de reset manuel peut être uniquement connectée aux nœuds **LR** et **FR** d'une sortie de sécurité, à un nœud **LR** d'un bloc Reset à verrouillage, à un nœud **RST** d'un bloc Dispositif d'activation, aux nœuds **SET** et **RST** des blocs Bascule, au nœud **RST** d'un bloc Commande de presse et à un nœud d'entrée d'un bloc OR désigné de reset.
G.5	Le nœud d'entrée d'un bloc OR désigné de reset ne peut être connecté qu'à une entrée de reset manuel, à une entrée de reset manuel virtuel et au nœud de sortie d'un bloc OR désigné de reset.
G.6	Le noeud de sortie d'un bloc OR désigné de reset peut être uniquement connecté aux nœuds **LR** et **FR** d'une sortie de sécurité, à un nœud **LR** d'un bloc Réarmement à verrouillage, à un nœud **RST** d'un bloc Dispositif d'activation, aux nœuds **SET** et **RST** des blocs Bascule et à un nœud d'entrée d'un bloc OR désigné de reset.
H.1	Un bloc de reset à verrouillage déjà connecté à un bloc fonction ne peut pas être connecté à un bloc Inhibition.
H.2	Un bloc reset à verrouillage déjà connecté à un bloc Inhibition ne peut pas être connecté à un autre bloc fonction.
I.1	Seules les entrées de capteur d'inhibition, Capteur optique, interrupteur de porte, tapis de sécurité ou arrêt de protection peuvent être connectés aux nœuds **MP1** et **MP2** d'un bloc d'inhibition ou au nœud **MP1** d'un bloc de commande bimanuelle.
I.2	Les nœuds **MP1** et **MP2** d'un bloc d'inhibition et le nœud **MP1** d'un bloc de commande bimanuelle peuvent être connectés aux entrées qui utilisent seulement les circuits double canal.
I.3	Une entrée paire de capteurs d'inhibition peut être uniquement connectée aux nœuds **MP1** et **MP2** d'un bloc d'inhibition ou au nœud **MP1** d'un bloc de commande bimanuelle.
J.1	**XS/SC26 FID 1, 2, & 3 et SC10-2 FID 1 :** un bloc Commande bimanuelle ne peut être connecté qu'au nœud **IN** d'un bloc Dispositif d'activation ou au nœud **IN** d'une sortie de sécurité. **XS/SC26 FID 4 ou ultérieur ou SC10-2 FID 2 ou ultérieur :**un bloc Commande bimanuelle peut être connecté uniquement à un bloc logique (à l'exclusion des blocs Bascule), au nœud **IN** d'un bloc Dispositif d'activation ou au nœud **IN** d'une sortie de sécurité.
J.3	Seules les entrées de commande bimanuelle ou les blocs Dérivation avec entrées de commande bimanuelle qui leur sont connectés peuvent être connectés au nœud **TC** d'un bloc Commande bimanuelle. Un bloc Dérivation avec une entrée de commande bimanuelle connectée à son nœud **IN** ne peut être connecté qu'au nœud **TC** d'un bloc Commande bimanuelle.
K.1	**XS/SC26 FID 1, 2, & 3 et SC10-2 FID 1 :** une entrée de commande bimanuelle ne peut être connectée qu'à un bloc de commande bimanuelle (nœud **TC**) ou à un bloc de dérivation (nœud **IN**). **XS/SC26 FID 4 ou ultérieur ou SC10-2 FID 2 ou ultérieur :** une entrée de commande bimanuelle ne peut être connectée qu'à un bloc Commande bimanuelle (nœud **TC**), à un bloc Dérivation (nœud **IN**), à un bloc logique (à l'exception des blocs Bascule), à un bloc Commande de presse (nœud **GO**) ou à une sortie avec retard au déclenchement.
K.2	**XS/SC26 FID 1, 2, & 3 et SC10-2 FID 1 :** une sortie de sécurité dont l'option *Temporisation de sortie de sécurité* est configurée en « Retard au déclenchement » ne peut pas être connectée à un bloc Commande bimanuelle. **XS/SC26 FID 4 ou ultérieur ou SC10-2 FID 2 ou ultérieur :** une sortie de sécurité dont l'option *Temporisation de sortie de sécurité* est configurée en « Retard au déclenchement » ne peut pas être directement connectée à un bloc Commande bimanuelle.
K.3	Une sortie de sécurité dont l'option *Temporisation de sortie de sécurité* est configurée en « Retard au déclenchement » ne peut pas être connectée à un bloc Commande bimanuelle via un bloc Dispositif d'activation.
L.1	Cette sortie de sécurité est désactivée parce qu'une sortie d'état utilise ses bornes.
L.2	Le nœud **IN** d'une sortie de sécurité ne peut pas être connecté à des entrées EDM, AVM, paire de capteurs d'inhibition, interrupteur de dérivation, reset manuel, inhibition activée ou annulation de l'entrée de temporisation.
L.3	Une sortie de sécurité dont la fonction *LR* est activée ne peut pas être connectée à des blocs de commande bimanuelle ou à des blocs appareil de commande.
L.4	**XS/SC26 FID 1, 2 & 3 et SC10-2 FID 1 :** une sortie de sécurité dont la fonction *Mode à la mise sous tension* est configurée en « Reset manuel » ne peut pas être connectée à des blocs Commande bimanuelle ou à des blocs Dispositif d'activation. **XS/SC26 FID 4 ou ultérieur ou SC10-2 FID2 ou ultérieur :** un bloc Sortie de sécurité dont la fonction *Mode à la mise sous tension* est configurée en « Reset manuel » ne peut pas être connecté à des entrées de commande bimanuelle, à des blocs Commande bimanuelle ou à des blocs Dispositif d'activation.
P.1	Seules les entrées ON/OFF physiques ou virtuelles peuvent être connectées aux nœuds **RUN**, **INCH UP** et **INCH DOWN** du bloc fonction Mode de commande de la presse.
P.2	Seule une entrée physique ON/OFF peut être connectée aux nœuds **TOS** et **BOS** du bloc fonction Commande de presse et au nœud **PIP** du bloc fonction Entrées de commande de presse.
P.3	Seule une entrée **SQS** peut être connectée au nœud d'entrée **SQS** du bloc fonction Entrées de commande de presse.
P.4	La seule entrée qui peut être connectée à l'entrée **M Sensor** du bloc fonction Entrées de commande de presse est un dispositif d'entrée Capteur d'inhibition de commande de presse (PCMS).

Code du logiciel	Erreur
P.5	Lorsque le bloc Commande de presse est configuré pour une commande à actionneur unique, le nœud d'entrée **GO** ne peut être connecté qu'à une entrée de démarrage de cycle, une entrée de pédale ou une entrée de commande bimanuelle. Lorsque le bloc Commande de presse est configuré pour le paramétrage manuel Course montante, le nœud d'entrée **GO** ne peut être connecté qu'à une entrée de pédale ou de commande bimanuelle.
P.6	Si la commande à actionneur unique est sélectionnée dans le bloc fonction Commande de presse, alors l'arrêt séquentiel (**SQS**) et la course montante ne sont pas autorisés.
P.7	Seule une entrée ON/OFF physique ou une entrée de pédale peut être connectée à l'entrée **Interrupteur au pied** du bloc fonction Entrées de la commande de presse.
P.8	Les nœuds de sortie du bloc fonction Commande de presse (**U**, **D**, **H** et **L**) ne peuvent être connectés qu'au nœud **IN** d'une sortie de sécurité.
P.9	Lorsque l'entrée du capteur d'inhibition de la commande de la presse n'est pas sélectionnée, seule une entrée SQS à deux voies peut être connectée au nœud d'entrée **SQS** du bloc fonction Entrées de commande de presse.

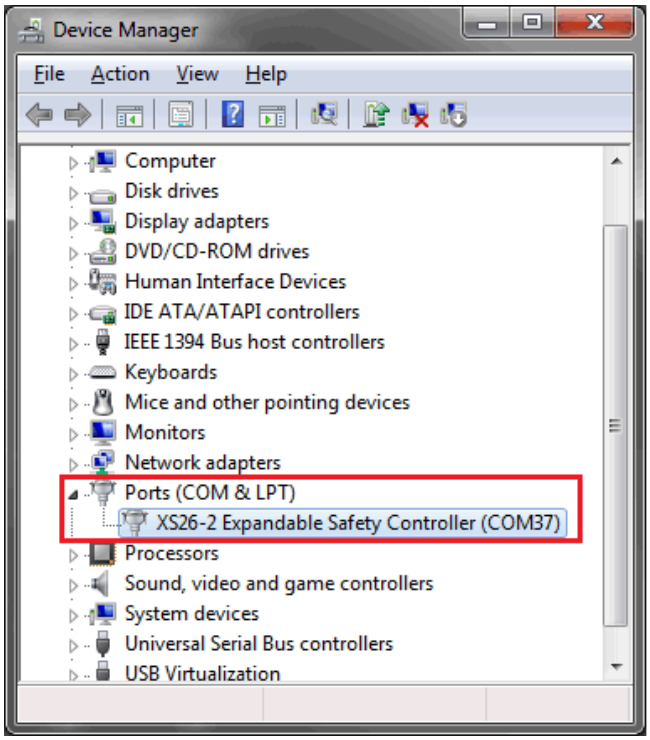
16.3 Vérification de l'installation des pilotes

Cette section s'applique au XS/SC26 et au SC10-2.

Pilotes du contrôleur de sécurité — Windows 7, 10 et 11

1. Ouvrez le **Gestionnaire de périphériques**.
2. Développez le menu déroulant **Ports (COM & LPT)**.
3. Localisez le **Contrôleur de sécurité extensible XS26-2** suivi d'un numéro de port COM (par exemple COM3). L'entrée ne doit pas comporter de point d'exclamation, croix rouge ou flèche vers le bas. Si aucun de ces symboles n'est affiché, votre périphérique est correctement installé. Si l'un des symboles apparaît, suivez les instructions ci-dessous pour résoudre ces problèmes.

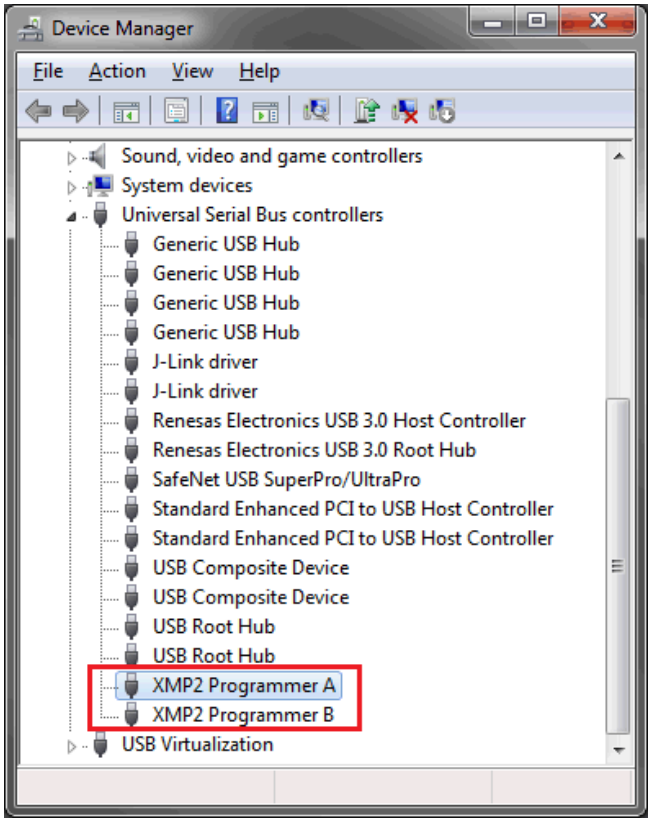
Illustration 345. Pilotes du contrôleur de sécurité XS/SC26 correctement installés



Pilotes SC-XMP2 — Windows 7, 10 et 11

1. Ouvrez le **Gestionnaire de périphériques**.
2. Développez le menu déroulant **Contrôleurs de bus USB**.
3. Localisez **XMP2 Programmer A** et **XMP2 Programmer B**. Ces entrées ne peuvent pas comporter de point d'exclamation, croix rouge ou flèche vers le bas. Si aucun de ces symboles n'est affiché, votre périphérique est correctement installé. Si l'un des symboles apparaît, suivez les instructions ci-dessous pour résoudre ces problèmes.

Illustration 346. Pilotes SC-XMP2 correctement installés



Résoudre un problème lié à la présence d'un point d'exclamation, d'une croix rouge ou d'une flèche vers le bas

1. Vérifiez que votre périphérique est activé :
    a. Double-cliquez sur l'entrée comportant un indicateur.
    b. Si l'option **Désactiver** s'affiche, le périphérique est activé. Si l'option **Activer** s'affiche, le périphérique est désactivé.
        - Si le périphérique est activé passez à l'étape de dépannage suivante.
        - Si le périphérique est désactivé, cliquez sur **Activer**. Si cela ne supprime pas l'indicateur, passez à l'étape suivante.
2. Débranchez le câble USB du contrôleur de sécurité ou de l'ordinateur, patientez quelques secondes puis rebranchez-le. Si cela ne supprime pas l'indicateur, passez à l'étape suivante.
3. Essayez de brancher le contrôleur de sécurité ou la carte SC-XMP2 dans un autre port USB. Si cela ne supprime pas l'indicateur, passez à l'étape suivante.
4. Redémarrez votre ordinateur. Si cela ne supprime pas l'indicateur, passez à l'étape suivante.
5. Désinstallez et réinstallez le logiciel à l'aide des options **Ajout/Suppression de programmes** ou **Programmes et fonctionnalités** du **Panneau de configuration**. Si cela ne supprime pas l'indicateur, passez à l'étape suivante.
6. Contactez Banner Engineering.

Résoudre un problème lié au contrôleur de sécurité répertorié dans le Gestionnaire de périphériques comme un « périphérique USB générique »

1. Cliquez avec le bouton droit sur le port de périphérique USB générique représentant le contrôleur de sécurité Banner Engineering.
2. Cliquez sur **Mettre à jour le pilote**.
3. Cliquez sur **Rechercher un pilote sur mon ordinateur**.
4. Cliquez sur le bouton **Parcourir** à droite du champ **Rechercher les pilotes à cet emplacement**. Une nouvelle fenêtre s'ouvre.
5. Sélectionnez **Disque local (C:)** > **Programmes (x86)** > **Banner Engineering** > **Banner Safety Controller** > **Pilote**.
6. Cliquez sur **OK** pour fermer cette fenêtre.
7. Dans la boîte de mise à jour du pilote, cliquez sur **Suivant**. Le pilote doit avoir été mis à jour.

Vous devrez peut-être fermer le logiciel Contrôleur de sécurité Banner et le rouvrir. Les ports USB doivent désormais lier les contrôleurs de sécurité Banner Engineering au logiciel.

16.4 Détection et correction des défauts

Selon la configuration, le contrôleur de sécurité est capable de détecter un certain nombre de défauts, ou défaillances, d'entrée, de sortie et du système.

I s'agit notamment des éléments suivants :

- Un contact bloqué
- Un contact ouvert
- Un court-circuit entre canaux
- Un court-circuit avec la masse
- Un court-circuit avec une source de tension
- Un court-circuit avec une autre entrée
- Une connexion desserrée ou débranchée
- Une limite de temps de fonctionnement dépassée
- Une chute de tension
- Une surchauffe

En cas de détection d'un défaut, un message décrivant celui-ci s'affiche dans le menu **Diagnostic des défauts** (modèles avec écran). Pour les modèles non équipés d'un écran, utilisez l'onglet **Mode temps réel** du logiciel sur un PC connecté au contrôleur de sécurité avec le câble SC-USB2 ou via un câble Ethernet (modèles EthernetXS/SC26 FID 7 ou ultérieur). La fonction de diagnostic des défauts est également disponible via le réseau. Un message supplémentaire expliquant comment corriger le défaut est parfois affiché.

Remarque: Le journal des défauts est effacé lorsque vous coupez puis rétablissez l'alimentation du contrôleur de sécurité.

16.4.1 Tableaux des codes de défaut du XS/SC26

Le tableau suivant répertorie les différents codes de défaut du contrôleur de sécurité et le message associé, d'éventuels messages supplémentaires, ainsi que la procédure à suivre pour corriger le défaut.

Le code d'erreur plus le code d'erreur avancé constituent le code de défaut du contrôleur de sécurité. Le format du code de défaut est `Error Code 'dot' Advanced Error Code`. Par exemple le code de défaut 2.1 du contrôleur de sécurité est composé du code d'erreur `2` et du code d'erreur avancé `1`. La valeur d'index du message d'erreur est constituée du code d'erreur et du code d'erreur avancé, lequel peut être précédé d'un zéro non significatif, le cas échéant. Par exemple, le code de défaut 2.1 du contrôleur de sécurité est représenté par l'index de message d'erreur `201`. La valeur d'index du message d'erreur offre un moyen pratique d'obtenir le code de défaut complet en lisant uniquement un registre 16 bits.

Remarque: Un code d'erreur 1.1 est différent d'un code d'erreur 1.10 (le zéro est important).

Code de défaut	Message affiché	Message complémentaire	Procédure de résolution
1.1	Défaut de sortie	**Contrôleur de base ou module transistorisé** Vérification des courts-circuits **Module relais** N/A	**Contrôleur de base ou module transistorisé** Une sortie de sécurité semble activée (ON) alors qu'elle devrait être désactivée (OFF) : • Recherchez un court-circuit vers la source électrique externe. • Vérifiez la section du fil commun CC connecté aux charges de la sortie de sécurité. Le fil doit avoir une section plus épaisse ou être aussi court que possible pour minimiser la résistance et la perte de tension. Le cas échéant, utilisez un fil commun CC distinct pour chaque paire de sorties et/ou évitez de partager le canal de retour de ce fil avec d'autres dispositifs (voir Installation du fil commun à la page 71). **Module relais** • Remplacez le module relais.

Code de défaut	Message affiché	Message complémentaire	Procédure de résolution
1.2	Défaut de sortie	**Contrôleur de base ou module transistorisé** Vérification des courts-circuits **Module relais** N/A	**Contrôleur de base ou module transistorisé** Une sortie de sécurité détecte un défaut vers une autre source de tension alors que la sortie est activée : • Recherchez un court-circuit entre les sorties de sécurité. • Recherchez un court-circuit vers la source électrique externe. • Vérifiez la compatibilité des dispositifs de charge. • Vérifiez la section du fil commun CC connecté aux charges de la sortie de sécurité. Le fil doit avoir une section plus épaisse ou être aussi court que possible pour minimiser la résistance et la perte de tension. Le cas échéant, utilisez un fil commun CC distinct pour chaque paire de sorties et/ou évitez de partager le canal de retour de ce fil avec d'autres dispositifs (voir Installation du fil commun à la page 71). **Module relais** • Remplacez le module relais.
1.3 – 1.8	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
1.9	Défaut de sortie	Défaut interne du relais	• Remplacez le module relais.
1.10	Défaut de sortie	Vérification des délais d'entrée	Erreur de séquence de temps : • Effectuez un reset du système pour annuler le défaut.
2.1	Défaut de séquence	Cycle d'entrée	Sur une entrée double voie, ou une entrée complémentaire, avec les deux entrées en état de marche, une entrée est passée en état d'arrêt puis de nouveau en état de marche. Sur une entrée double voie-complémentaire avec les deux paires d'entrées en état de marche, une paire d'entrées est passée en état d'arrêt puis de nouveau en état de marche. • Vérifiez le câblage. • Vérifiez les signaux d'entrée. • Envisagez de modifier les temps anti-rebond.
2.2	Défaut de simultanéité	Cycle d'entrée	Sur une entrée double voie, ou une entrée complémentaire, une entrée est passée en état de marche mais l'autre n'a pas suivi dans les 3 secondes. Sur une entrée double voie-complémentaire, une paire d'entrées est passée en état de marche mais l'autre paire n'a pas suivi dans les 3 secondes. • Vérifiez le câblage. • Vérifiez la séquence de temps du signal d'entrée.
2.3 ou 2.5	Défaut de séquence	Cycle d'entrée	Sur une entrée double voie-complémentaire avec les deux entrées d'une paire complémentaire en état de marche, une entrée de cette paire complémentaire est passée en état d'arrêt puis de nouveau en état de marche : • Vérifiez le câblage. • Vérifiez les signaux d'entrée. • Vérifiez la source d'alimentation des signaux d'entrée. • Envisagez de modifier les temps anti-rebond.
2.4 ou 2.6	Défaut de simultanéité	Cycle d'entrée	Sur une entrée double voie-complémentaire, une entrée d'une paire complémentaire est passée en état marche mais l'autre entrée de la même paire n'a pas suivi dans le délai imparti. • Vérifiez le câblage. • Vérifiez la séquence de temps du signal d'entrée.
2.7	Défaut interne		Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
2.8 – 2.9	Défaut d'entrée	Vérification de la borne xx	L'entrée est bloquée sur haut : • Recherchez des courts-circuits vers les autres entrées ou d'autres sources de tension. • Vérifiez la compatibilité des dispositifs d'entrée. • Recherchez des bornes mal câblées (borne de sortie câblée à la mauvaise borne d'entrée)
2.10	Défaut d'entrée	Vérification de la borne xx	• Recherchez un court-circuit entre les entrées.
2.11 – 2.12	Défaut d'entrée	Vérification de la borne xx	• Recherchez un court-circuit avec la masse.
2.13	Défaut d'entrée	Vérification de la borne xx	L'entrée est bloquée sur bas : • Recherchez un court-circuit avec la masse.

Code de défaut	Message affiché	Message complémentaire	Procédure de résolution
2.14	Défaut d'entrée	Vérification de la borne xx	Impulsions de test manquantes : • Recherchez un court-circuit vers d'autres entrées ou sources de tension.
2.15	Fil non branché	Vérification de la borne xx	• Recherchez un fil non branché.
2.16 – 2.18	Défaut d'entrée	Vérification de la borne xx	Impulsions de test manquantes : • Recherchez un court-circuit vers d'autres entrées ou sources de tension.
2.19	Fil non branché	Vérification de la borne xx	• Recherchez un fil non branché.
2.20	Défaut d'entrée	Vérification de la borne xx	Impulsions de test manquantes : • Recherchez un court-circuit avec la masse.
2.21	Fil non branché	Vérification de la borne xx	• Recherchez un fil non branché.
2.22 – 2.23	Défaut d'entrée	Vérification de la borne xx	• Recherchez un signal instable à l'entrée.
2.24	Entrée activée pendant qu'elle était dérivée	Exécution du démarrage système	Une entrée de commande bimanuelle a été activée (ON) pendant qu'elle était dérivée.
2.25	Défaut d'entrée	Expiration du délai de surveillance avant la fermeture de l'AVM	Après que la sortie de sécurité qui lui est associée a été désactivée (Off), l'entrée AVM ne s'est pas fermée avant l'expiration du délai de surveillance de l'AVM : • L'AVM peut être déconnecté. Vérifiez le raccordement de l'AVM. • Soit l'AVM est déconnecté, soit son temps de réponse à une désactivation de la sortie de sécurité est trop lent. • Vérifiez le raccordement de l'AVM. • Vérifiez le paramètre de temps et modifiez-le le cas échéant. • Contactez Banner Engineering
2.26	Défaut d'entrée	AVM non fermé lorsque les sorties s'activent	L'entrée AVM était ouverte mais aurait dû être fermée lorsque la sortie de sécurité associée a été activée (ON) : • L'AVM peut être déconnecté. Vérifiez le raccordement de l'AVM.
3.1	Défaut EDMxx	Vérification de la borne xx	Le contact EDM s'est ouvert avant l'activation (ON) des sorties de sécurité : • Recherchez un contacteur ou un relais bloqué en position ON. • Recherchez un fil non branché.
3.2	Défaut EDMxx	Vérification de la borne xx	Les contacts EDM ne se sont pas fermés en moins de 250 ms après que les sorties de sécurité ont été désactivées (OFF) : • Recherchez un contacteur ou un relais lent ou bloqué en position ON. • Recherchez un fil non branché.
3.4	Défaut EDMxx	Vérification de la borne xx	La paire de contacts EDM n'a pas eu le même comportement pendant plus de 250 ms : • Recherchez un contacteur ou un relais lent ou bloqué en position ON. • Recherchez un fil non branché.
3.5	Défaut EDMxx	Vérification de la borne xx	• Recherchez un signal instable à l'entrée.
3.6	Défaut EDMxx	Vérification de la borne xx	• Recherchez un court-circuit avec la masse.
3.7	Défaut EDMxx	Vérification de la borne xx	• Recherchez un court-circuit entre les entrées.
3.8	Défaut AVMxx	Exécution du démarrage système	Après la désactivation de cette sortie de sécurité, l'entrée AVM qui lui est associée ne s'est pas fermée avant l'expiration du délai de surveillance de l'AVM : • Soit l'AVM est déconnecté, soit son temps de réponse à une désactivation de la sortie de sécurité est trop lent. • Vérifiez l'entrée AVM puis effectuez un reset du système pour annuler le défaut.

Code de défaut	Message affiché	Message complémentaire	Procédure de résolution
3.9	Défaut d'entrée	AVM non fermé lorsque les sorties s'activent	L'entrée AVM était ouverte mais aurait dû être fermée lorsque la sortie de sécurité associée a été activée (ON) : • L'AVM peut être déconnecté. Vérifiez le raccordement de l'AVM.
3.10	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.x	-	-	Voir le tableau suivant.
5.1 – 5.3	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
6.xx	Défaut interne	-	Données de configuration non valides. Défaillance interne possible : • Essayez d'enregistrer une nouvelle configuration sur le contrôleur de sécurité.
7.1	Défaut de la commande de presse	Vérification des entrées TOS et BOS	Les entrées TOS et BOS sont activées en même temps • Vérifiez les court-circuits sur les entrées TOS et BOS • Vérifiez les problèmes de fonctionnement des dispositifs TOS et BOS
7.2	Défaut de la commande de presse	Vérification des entrées TOS et SQS	Les entrées TOS et SQS sont activées en même temps • Vérifiez les court-circuits sur les entrées TOS et SQS • Vérifiez les problèmes de fonctionnement des dispositifs TOS et SQS
7.3	Défaut de la commande de presse	Vérification des entrées TOS et PCMS	Les entrées TOS et PCMS sont activées en même temps • Vérifiez les court-circuits sur les entrées TOS et PCMS • Vérifiez les problèmes de fonctionnement des dispositifs TOS et PCMS
7.4	Défaut de la commande de presse	Vérification de SQS et BOS	Erreur de séquencement entre SQS et BOS (BOS activé avant SQS) • Vérifiez le câblage des capteurs SQS et BOS • Vérifiez les problèmes fonctionnels et d'emplacement des capteurs SQS et BOS
7.5	Défaut de la commande de presse	Vérification de TOS	Erreur d'expiration du délai TOS (pour la course montante automatique, le délai interne de 30 secondes a été dépassé) • Vérifiez le câblage du système TOS • Vérifiez les problèmes fonctionnels et d'emplacement du capteur TOS
7.6	Défaut de la commande de presse	Vérification de BOS	Erreur d'expiration du délai BOS (pour la course descendante automatique, le délai interne de 30 secondes a été dépassé) • Vérifiez le câblage du système BOS • Vérifiez les problèmes fonctionnels et d'emplacement du capteur BOS
7.7	Défaut de la commande de presse	Vérification des entrées de sélection de mode	Erreur de sélection de mode (plusieurs entrées de sélection de mode activées en même temps) • Vérifiez le câblage des entrées d'état de mode • Vérifiez que le sélecteur de mode ne présente pas de défauts
7.8	Défaut de la commande de presse	-	Erreur d'index (erreur de configuration interne) Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
7.9	Défaut de la commande de presse	Vérifiez l'entrée de l'interrupteur au pied	Erreur de l'interrupteur au pied (lorsqu'il a été configuré avec un SQS, le nœud d'entrée de l'interrupteur au pied s'est activé au lieu du nœud d'entrée GO) • Erreur de séquencement • Si elle persiste, vérifiez le câblage des entrées Commande bimanuelle (THC) et Pédale (Ft Pedal)
7.10	Défaut de la commande de presse	Vérification Cylindre Descendant	Erreur AVM Descendant (État incorrect de l'AVM Descendant par rapport à l'état attendu) • Vérifiez le câblage de l'AVM Descendant • Vérifiez le capteur AVM Descendant et le système Course descendante

Code de défaut	Message affiché	Message complémentaire	Procédure de résolution
7.11	Défaut de la commande de presse	Vérification Cylindre Montant	Erreur AVM Montant (État incorrect de l'AVM Montant par rapport à l'état attendu) • Vérifiez le câblage de l'AVM Montant • Vérifiez le capteur AVM Montant et le système Course montante
7.12	Défaut de la commande de presse	Vérification Cylindre Haut	Erreur AVM Haut (État incorrect de l'AVM Haut par rapport à l'état attendu) • Vérifiez le câblage de l'AVM Haut • Vérifiez le capteur AVM Haut et le système Course haute
7.13	Défaut de la commande de presse	Vérification Cylindre Bas	Erreur AVM Bas (État incorrect de l'AVM Bas par rapport à l'état attendu) • Vérifiez le câblage de l'AVM Bas • Vérifiez le capteur AVM Bas et le système Course basse
7.14	Défaut de la commande de presse	Simultanéité entre SQS et PCMS	Erreur de simultanéité entre SQS et PCMS (dépassement du délai de 3 secondes entre les entrées) • Vérifiez le câblage SQS/PCMS • Vérifiez l'emplacement SQS/PCMS en tenant compte de la vitesse du coulisseau
7.15	Défaut de la commande de presse	Vérification de l'état SQS	Erreur d'état SQS (niveau d'état SQS imprévu pendant le cycle de la presse) • Vérifiez le câblage de l'entrée SQS • Vérifiez l'emplacement du capteur SQS et ses fonctions
7.16	Défaut de la commande de presse	Vérification de l'état PCMS	Erreur d'état PCMS (niveau d'état PCMS imprévu pendant le cycle de la presse) • Vérifiez le câblage de l'entrée PCMS • Vérifiez l'emplacement du capteur PCMS et ses fonctions
7.17	Défaut de la commande de presse	Vérification de l'état TOS	Erreur d'état TOS (niveau d'état TOS imprévu pendant le cycle de la presse) • Vérifiez le câblage de l'entrée TOS • Vérifiez l'emplacement du capteur TOS et ses fonctions
7.18	Défaut de la commande de presse	Vérification de l'état BOS	Erreur d'état BOS (niveau d'état BOS imprévu pendant le cycle de la presse) • Vérifiez le câblage de l'entrée BOS • Vérifiez l'emplacement du capteur BOS et ses fonctions
10.xx	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)

Pour les codes de défaut 4.x, consultez le journal de défauts afin de déterminer le module spécifique dans lequel le défaut original est survenu.

Code de défaut	Message affiché	Message complémentaire	Procédure de résolution
4.1	Tension d'alimentation trop faible	Vérification de l'alimentation électrique	La tension d'alimentation est tombée sous la tension de référence pendant plus de 6 ms : • Vérifiez la tension d'alimentation et l'intensité. • Recherchez une surcharge des sorties qui pourrait limiter le courant de l'alimentation.
4.2	Défaut interne		Un paramètre de configuration est corrompu. Pour corriger la configuration : • Remplacez la configuration en utilisant une copie de sauvegarde de la configuration. • Recréez la configuration à l'aide du logiciel et enregistrez-la dans le contrôleur de sécurité.
4.3 – 4.11	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.12	Limite de temps de la configuration dépassée	Vérification de la configuration	Le contrôleur de sécurité est resté en mode de configuration pendant plus d'une heure sans saisie clavier. • Coupez puis rétablissez l'alimentation électrique. • Procédez au reset du système.

Code de défaut	Message affiché	Message complémentaire	Procédure de résolution
4.13	Limite de temps de la configuration dépassée	Vérification de la configuration	Le contrôleur de sécurité est resté en mode de configuration pendant plus d'une heure sans recevoir de commandes du logiciel. • Coupez puis rétablissez l'alimentation électrique. • Procédez au reset du système.
4.14	Configuration non confirmée	Confirmation de la configuration	La configuration n'a pas été confirmée après avoir été modifiée : • Confirmez la configuration à l'aide du logiciel.
4.15 – 4.19	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.20	Borne non assignée à l'usage	Vérification de la borne xx	Cette borne n'est pas assignée à un dispositif dans la configuration actuelle et ne devrait pas être active : • Vérifiez le câblage.
4.21 – 4.34	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.35	Surchauffe	-	Surchauffe interne. Vérifiez que les conditions ambiantes et de chargement de sortie sont conformes aux spécifications du contrôleur de sécurité.
4.36 – 4.39	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.40 – 4.41	Échec de communication du module	Vérification de l'alimentation du module	Perte de contact entre un module d'extension de sorties et le contrôleur de base
4.42	Non-correspondance de module	-	Le ou les modules détectés ne correspondent pas à la configuration du contrôleur de sécurité.
4.43	Échec de communication du module	Vérification de l'alimentation du module	Perte de contact entre un module d'extension et le contrôleur de base
4.44 - 4.45	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.46 – 4.47	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.48	Sortie inutilisée	Vérification du câblage de la sortie	Une tension a été détectée sur une borne non confirmée.
4.49 – 4.55	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.56	Échec de communication avec l'écran	-	Échec de communication avec l'écran (interface embarquée) : • Mettez le contrôleur de sécurité hors tension puis sous tension. Si le code de défaut persiste, contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.57 – 4.59	Défaut interne	-	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.60	Défaut de sortie	Vérification des courts-circuits	Une borne de sortie a détecté un court-circuit. Vérifiez le défaut de la sortie pour plus d'informations.
4.61	Non correspondance avec la configuration	-	Une fonctionnalité (par exemple, les entrées ISD, les entrées virtuelles, les modules d'extension) contenue dans la configuration chargée n'est pas prise en charge par ce modèle de contrôleur. La configuration est maintenant confirmée et peut être sauvegardée en tant que configuration confirmée et/ou écrite sur une carte SC-XM2/3. La configuration ne sera pas exécutée sur ce modèle. • Supprimez les fonctionnalités non prises en charge par ce modèle • Chargez la configuration sur un modèle qui prend en charge les fonctionnalités sélectionnées.

16.4.2 Tableau des codes de défaut du SC10-2

Le tableau suivant répertorie les différents codes de défaut du contrôleur de sécurité et le message associé, d'éventuels messages supplémentaires, ainsi que la procédure à suivre pour corriger le défaut.

Le code d'erreur plus le code d'erreur avancé constituent le code de défaut du contrôleur de sécurité. Le format du code de défaut est `Error Code 'dot' Advanced Error Code`. Par exemple le code de défaut 2.1 du contrôleur de sécurité est composé du code d'erreur `2` et du code d'erreur avancé `1`. La valeur d'index du message d'erreur est constituée du code d'erreur et du code d'erreur avancé, lequel peut être précédé d'un zéro non significatif, le cas échéant. Par

exemple, le code de défaut 2.1 du contrôleur de sécurité est représenté par l'index de message d'erreur `201`. La valeur d'index du message d'erreur offre un moyen pratique d'obtenir le code de défaut complet en lisant uniquement un registre 16 bits.

Remarque: Un code d'erreur 1.1 est différent d'un code d'erreur 1.10 (le zéro est important).

Code de défaut	Description du code de défaut	Procédure de résolution
1.1 – 1.2	Défaut de sortie	Remplacez le contrôleur de sécurité.
1.3 – 1.8	Défaut interne	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
1.9	Défaut de sortie	Remplacez le contrôleur de sécurité.
1.10	Défaut de sortie	Erreur de séquence de temps : • Effectuez un reset du système pour annuler le défaut.
2.1	Défaut de séquence	Sur une entrée double voie, ou une entrée complémentaire, avec les deux entrées en état de marche, une entrée est passée en état d'arrêt puis de nouveau en état de marche. Sur une entrée double voie-complémentaire avec les deux paires d'entrées en état de marche, une paire d'entrées est passée en état d'arrêt puis de nouveau en état marche. • Vérifiez le câblage. • Vérifiez les signaux d'entrée. • Envisagez de modifier les temps anti-rebond. • Cycle d'entrée
2.2	Défaut de simultanéité	Sur une entrée double voie, ou une entrée complémentaire, une entrée est passée en état de marche mais l'autre n'a pas suivi dans les 3 secondes. Sur une entrée double voie-complémentaire, une paire d'entrées est passée en état de marche mais l'autre paire n'a pas suivi dans les 3 secondes. • Vérifiez le câblage. • Vérifiez la séquence de temps du signal d'entrée. • Cycle d'entrée
2.3 ou 2.5	Défaut de séquence	Sur une entrée double voie-complémentaire avec les deux entrées d'une paire complémentaire en état marche, une entrée de cette paire complémentaire est passée en état d'arrêt puis de nouveau en état marche. • Vérifiez le câblage. • Vérifiez les signaux d'entrée. • Vérifiez la source d'alimentation des signaux d'entrée. • Envisagez de modifier les temps anti-rebond. • Cycle d'entrée
2.4 ou 2.6	Défaut de simultanéité	Sur une entrée double voie-complémentaire, une entrée d'une paire complémentaire est passée en état marche mais l'autre entrée de la même paire n'a pas suivi dans le délai imparti. • Vérifiez le câblage. • Vérifiez la séquence de temps du signal d'entrée. • Cycle d'entrée
2.7	Défaut interne	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
2.8 – 2.9	Défaut d'entrée	L'entrée est bloquée sur haut : • Recherchez des courts-circuits vers les autres entrées ou d'autres sources de tension. • Vérifiez la compatibilité des dispositifs d'entrée. • Recherchez des bornes mal câblées (borne de sortie câblée à la mauvaise borne d'entrée)
2.10	Défaut d'entrée	• Recherchez un court-circuit entre les entrées.
2.11 – 2.12	Défaut d'entrée	• Recherchez un court-circuit avec la masse.
2.13	Défaut d'entrée	L'entrée est bloquée sur bas : • Recherchez un court-circuit avec la masse.
2.14	Défaut d'entrée	Impulsions de test manquantes : • Recherchez un court-circuit vers d'autres entrées ou sources de tension.
2.15	Fil non branché	• Recherchez un fil non branché.
2.16 – 2.18	Défaut d'entrée	Impulsions de test manquantes : • Recherchez un court-circuit vers d'autres entrées ou sources de tension.

Code de défaut	Description du code de défaut	Procédure de résolution
2.19	Fil non branché	• Recherchez un fil non branché.
2.20	Défaut d’entrée	Impulsions de test manquantes : • Recherchez un court-circuit avec la masse.
2.21	Fil non branché	• Recherchez un fil non branché.
2.22 – 2.23	Défaut d’entrée	• Recherchez un signal instable à l’entrée.
2.24	Entrée activée pendant qu'elle était dérivée	Une entrée de commande bimanuelle a été activée (ON) pendant qu'elle était dérivée.
2.25	Défaut d’entrée	Après que la sortie de sécurité qui lui est associée a été désactivée (Off), l'entrée AVM ne s'est pas fermée avant l'expiration du délai de surveillance de l'AVM : • L'AVM peut être déconnecté. Vérifiez le raccordement de l'AVM. • Soit l'AVM est déconnecté, soit son temps de réponse à une désactivation de la sortie de sécurité est trop lent. • Vérifiez le raccordement de l'AVM. • Vérifiez le paramètre de temps et modifiez-le le cas échéant. • Contactez Banner Engineering
2.26	Défaut d’entrée	L'entrée AVM était ouverte mais aurait dû être fermée lorsque la sortie de sécurité associée a été activée (ON) : • L'AVM peut être déconnecté. Vérifiez le raccordement de l'AVM.
3.1	Défaut EDMxx	Le contact EDM s’est ouvert avant l'activation (ON) des sorties de sécurité : • Recherchez un contacteur ou un relais bloqué en position ON. • Recherchez un fil non branché.
3.2	Défaut EDMxx	Les contacts EDM ne se sont pas fermés en moins de 250 ms après que les sorties de sécurité ont été désactivées (OFF) : • Recherchez un contacteur ou un relais lent ou bloqué en position ON. • Recherchez un fil non branché.
3.4	Défaut EDMxx	La paire de contacts EDM n'a pas eu le même comportement pendant plus de 250 ms. • Recherchez un contacteur ou un relais lent ou bloqué en position ON. • Recherchez un fil non branché.
3.5	Défaut EDMxx	• Recherchez un signal instable à l’entrée.
3.6	Défaut EDMxx	• Recherchez un court-circuit avec la masse.
3.7	Défaut EDMxx	• Recherchez un court-circuit entre les entrées.
3.8	Défaut AVMxx	Après la désactivation de cette sortie de sécurité, l'entrée AVM qui lui est associée ne s'est pas fermée avant l'expiration du délai de surveillance de l'AVM : • Il est possible que l’AVM soit déconnecté ou que son temps de réponse à une désactivation de la sortie de sécurité soit trop lent. • Vérifiez l'entrée AVM puis effectuez un reset du système pour annuler le défaut.
3.9	Défaut d’entrée	L'entrée AVM était ouverte mais aurait dû être fermée lorsque la sortie de sécurité associée a été activée (ON) : • L'AVM peut être déconnecté. Vérifiez le raccordement de l'AVM.
3.10	Défaut interne	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.1	Tension d’alimentation trop faible	La tension d’alimentation est tombée sous la tension de référence pendant plus de 6 ms : • Vérifiez la tension d’alimentation et l'intensité. • Recherchez une surcharge des sorties qui pourrait limiter le courant de l’alimentation.
4.2	Défaut interne	Un paramètre de configuration est corrompu. Pour corriger la configuration : • Remplacez la configuration en utilisant une copie de sauvegarde de la configuration. • Recréez la configuration à l'aide du logiciel et enregistrez-la dans le contrôleur de sécurité.
4.3 – 4.12	Défaut interne	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)

Code de défaut	Description du code de défaut	Procédure de résolution
4.13	Limite de temps de la configuration dépassée	Le contrôleur de sécurité est resté en mode de configuration pendant plus d'une heure sans recevoir de commandes du logiciel. • Coupez puis rétablissez l'alimentation électrique. • Effectuez un reset du système.
4.14	Configuration non confirmée	La configuration n'a pas été confirmée après avoir été modifiée : • Confirmez la configuration à l'aide du logiciel.
4.15 – 4.19	Défaut interne	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.20	Borne non assignée à l'usage	Cette borne n'est pas assignée à un dispositif dans la configuration actuelle et ne devrait pas être active : • Vérifiez le câblage.
4.21 – 4.34	Défaut interne	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.35	Surchauffe	Surchauffe interne. Vérifiez que les conditions ambiantes et de chargement de sortie sont conformes aux spécifications du contrôleur de sécurité.
4.36 – 4.47	Défaut interne	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.48	Sortie inutilisée	Une tension a été détectée sur une borne non confirmée.
4.49 – 4.59	Défaut interne	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
4.60	Défaut de sortie	Une borne de sortie a détecté un court-circuit. Vérifiez le défaut de la sortie pour plus d'informations.
5.1 – 5.3	Défaut interne	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)
6.xx	Défaut interne	Données de configuration non valides. Défaillance interne possible : • Essayez d'enregistrer une nouvelle configuration sur le contrôleur de sécurité.
10.xx	Défaut interne	Erreur interne — Contactez Banner Engineering (voir Réparations et service sous garantie à la page 359)

17 Composants et accessoires

17.1 Pièces de rechange et accessoires

Modèle	Description	Produit applicable
SC-USB2	Câble USB	XS/SC26, SC10-2
SC-XMP2	Outil de programmation pour la carte SC-XM2/3	XS/SC26, SC10-2
DIN-SC	Bride terminale DIN	XS/SC26, SC10-2
SC-XM2	Carte mémoire externe pour le XS/SC26	XS/SC26
SC-XM3	Carte mémoire externe pour le SC10-2	XS/SC26, SC10-2
SC-TS2	Bornier à vis contrôleur	XS/SC26
SC-TS3	Bornier à vis module d'extension	XS/SC26
SC-TC2	Bornier à ressort contrôleur	XS/SC26
SC-TC3	Bornier à ressort module d'extension	XS/SC26

17.2 Câbles Ethernet

Câbles blindés Cat5e	Câbles croisés blindés Cat5e	Longueur
STP07	**STPX07**	2,1 m
STP25	**STPX25**	7,62 m
STP50	**STPX50**	15,2 m
STP75	**STPX75**	22,9 m

17.3 Modules d'interface

Référez-vous aux fiches techniques réf. 62822 et 208873 ainsi qu'à la section Raccordement EDM et FSD à la page 74 pour plus d'informations.

Modèle	Tension d'entrée	Entrées	Sorties de sécurité	Aux. Sorties	Caractéristiques des sorties	Contacts EDM
IM-T-9A	24 Vcc	2 (raccordement à deux voies)	3 N.O.	—	6 A	2 N.F.
IM-T-11A			2 N.O.	1 N.F.		
SR-IM-9A			3 N.O.	—	Voir la fiche technique pour les spécifications	
SR-IM-11A			2 N.O.	1 N.F.		

17.3.1 Contacts reliés mécaniquement

Ces contacts fournissent une capacité de transport supplémentaire de 10 A ou de 18 A vers un système de sécurité.

En cas d'utilisation, deux contacteurs par paire de sorties de sécurité sont nécessaires pour la catégorie 4. Une seule sortie OSSD (dispositif de commutation du signal de sortie) avec 2 contacteurs peut atteindre la catégorie 3. Les contacts N.F. doivent être utilisés dans un circuit de surveillance des commutateurs (EDM) externes.

Référez-vous à la section Raccordement EDM et FSD à la page 74 pour en savoir plus.

Modèle	Tension d'alimentation	Entrées	Sorties	Caractéristiques des sorties
11-BG00-31-D-024	24 Vcc	2 (raccordement à deux voies)	3 N.O., 1 N.F.	10 A
BF1801L-024				18 A

18 Assistance et maintenance du produit

18.1 Nettoyage

1. **Coupez l'alimentation du contrôleur de sécurité.**
2. Nettoyez le boîtier en polycarbonate et l'écran (modèles avec écran) avec un chiffon doux préalablement imprégné d'eau tiède additionnée de détergent doux.

18.2 Réparations et service sous garantie

Pour plus d'informations sur le dépannage du produit, contactez Banner Engineering. **Ne tentez pas de réparer ce dispositif Banner. Il ne contient aucun composant ou pièce qui puisse être remplacé sur place.** Si un ingénieur de Banner conclut que le dispositif ou l'une de ses pièces ou composants est défectueux, il vous informera de la procédure à suivre pour le retour des produits (RMA).

Important: Si vous devez retourner le dispositif, emballez-le avec soin. Les dégâts occasionnés pendant le transport de retour ne sont pas couverts par la garantie.

Pour aider Banner Engineering à résoudre un problème, lorsque le PC est connecté au contrôleur de sécurité, allez dans le menu **Aide** du logiciel puis cliquez sur **Informations de support**. Cliquez sur **Enregistrer le diagnostic du contrôleur** pour générer un fichier contenant des informations d'état. Ces informations peuvent s'avérer utiles pour l'équipe de support d'Banner. Envoyez le fichier à Banner en suivant les instructions affichées à l'écran.

18.3 Nous contacter

Le siège social de Banner Engineering Corp. a son adresse à :

9714 Tenth Avenue North Minneapolis, MN 55441, USA Téléphone : + 1 888 373 6767

Pour une liste des bureaux et des représentants locaux dans le monde, visitez la page www.bannerengineering.com.

18.4 Garantie limitée de Banner Engineering Corp.

Banner Engineering Corp. garantit ses produits contre tout défaut lié aux matériaux et à la main d'oeuvre pendant une durée de 1 an à compter de la date de livraison. Banner Engineering Corp. s'engage à réparer ou à remplacer, gratuitement, tout produit défectueux, de sa fabrication, renvoyé à l'usine durant la période de garantie. La garantie ne couvre en aucun cas la responsabilité ou les dommages résultant d'une utilisation inadaptée ou abusive, ou d'une installation ou application incorrecte du produit Banner.

CETTE GARANTIE LIMITÉE EST EXCLUSIVE ET PRÉVAUT SUR TOUTES LES AUTRES GARANTIES, EXPRESSES OU IMPLICITES (Y COMPRIS, MAIS SANS S'Y LIMITER, TOUTE GARANTIE DE QUALITÉ MARCHANDE OU D'ADÉQUATION À UN USAGE PARTICULIER), QUE CE SOIT DANS LE CADRE DE PERFORMANCES, DE TRANSACTIONS OU D'USAGES DE COMMERCE.

Cette garantie est exclusive et limitée à la réparation ou, à la discrétion de Banner Engineering Corp., au remplacement du produit. **EN AUCUNE CIRCONSTANCE, BANNER ENGINEERING CORP. NE SERA TENU RESPONSABLE VIS-À-VIS DE L'ACHETEUR OU TOUTE AUTRE PERSONNE OU ENTITÉ, DES COÛTS SUPPLÉMENTAIRES, FRAIS, PERTES, PERTE DE BÉNÉFICES, DOMMAGES CONSÉCUTIFS, SPÉCIAUX OU ACCESSOIRES RÉSULTANT D'UN DÉFAUT OU DE L'UTILISATION OU DE L'INCAPACITÉ À UTILISER LE PRODUIT, EN VERTU DE TOUTE THÉORIE DE RESPONSABILITÉ DÉCOULANT DU CONTRAT OU DE LA GARANTIE, DE LA RESPONSABILIÉ JURIDIQUE, DÉLICTUELLE OU STRICTE, DE NÉGLIGENCE OU AUTRE.**

Banner Engineering Corp. se réserve le droit de modifier ou d'améliorer la conception du produit sans être soumis à une quelconque obligation ou responsabilité liée à des produits précédemment fabriqués par Banner Engineering Corp. Toute utilisation ou installation inappropriée, abusive ou incorrecte du produit ou toute utilisation à des fins de protection personnelle alors que le produit n'est pas prévu pour cela annule la garantie. Toute modification apportée à ce produit sans l'autorisation expresse de Banner Engineering annule les garanties du produit. Toutes les spécifications publiées dans ce document sont susceptibles d'être modifiées. Banner se réserve le droit de modifier à tout moment les spécifications du produit ou la documentation. En cas de différences entre les spécifications et informations produits publiées en anglais et dans une autre langue, la version anglaise prévaut. Pour obtenir la dernière version d'un document, rendez-vous sur notre site : www.bannerengineering.com.

Pour des informations sur les brevets, voir www.bannerengineering.com/patents.

18.5 Avis de copyright du logiciel Banner Engineering Corp.

© Banner Engineering Corp. Tous droits réservés.

https://www.bannerengineering.com/us/en/company/terms-and-conditions.html

Exclusion de garantie. Ce logiciel est fourni tel quel. Dans les limites prévues par la loi en vigueur, Banner, ses sociétés affiliées et ses partenaires excluent toute garantie explicite ou implicite, y compris toute garantie quant à l'adéquation du logiciel à un usage particulier, titre, qualité marchande, perte de données, non ingérence ou non infraction à tous les droits de propriété intellectuelle ou relative à la précision, fiabilité, qualité ou contenu liés aux services. Banner, ses sociétés affiliées et ses partenaires ne garantissent pas que les services sont sûrs, sans bogues, virus, erreurs et qu'il ne feront pas l'objet d'interruption, vol ou destruction. Si les exclusions de garanties implicites ne s'appliquent pas à vous, toute garantie implicite est limitée à 60 jours à compter de la date de la première utilisation de ce logiciel.

Limitation de responsabilité et indemnisation. Banner, ses sociétés affiliées et ses partenaires ne peuvent être tenus responsables de tout dommage indirect, spécial, accessoire, punitif ou consécutif lié à la corruption, sécurité, vol ou perte de données, virus, spyware, perte de contrats, de revenus, de bénéfices ou d'investissement, ou à une utilisation du logiciel ou du matériel non conforme aux exigences système minimum de Banner. Les limitations ci-dessous sont d'application même si Banner, ses sociétés affiliées et ses partenaires ont été avertis de la possibilité de tels dommages. Le présent Accord stipule l'entière responsabilité de Banner, ses sociétés affiliées et ses partenaires et votre seul recours quant à l'utilisation du logiciel.

19 Normes et réglementations

La liste des normes ci-dessous est fournie à titre indicatif aux utilisateurs de ce dispositif Banner. L'inclusion de ces normes ne signifie pas que le dispositif est conforme à des normes autres que celles répertoriées dans la section Spécifications de ce manuel.

19.1 Normes américaines en vigueur

ANSI B11.0 Sécurité des machines, Principes généraux et d'appréciation du risque

ANSI B11.1 Presses mécaniques

ANSI B11.2 Presses mécaniques hydrauliques

ANSI B11.3 Presses plieuses mécaniques

ANSI B11.4 Cisailles

ANSI B11.5 Produits sidérotechniques

ANSI B11.6 Tours

ANSI B11.7 Machines à frapper et à former à froid

ANSI B11.8 Machines à percer, laminer et forer

ANSI B11.9 Meuleuses

ANSI B11.10 Scies à métaux

ANSI B11.11 Machines à tailler les engrenages

ANSI B11.12 Machines à laminer et couder les profilés

ANSI B11.13 Machines de serrage et vis/bar - Automatiques, monobroches et multibroches

ANSI B11.14 Machines/équipement à refendre

ANSI B11.15 Machines à couder les tuyaux et conduites

ANSI B11.16 Presses de compactage de poudre métallique

ANSI B11.17 Extrudeuses hydrauliques horizontales

ANSI B11.18 Machines et systèmes pour le traitement des bandes, feuilles et plaques enroulées

ANSI B11.19 Machines-outils, protection

ANSI B11.20 Systèmes/éléments de fabrication

ANSI B11.21 Machines-outils équipées de lasers

ANSI B11.22 Tours à commande numérique

ANSI B11.23 Centres d'usinage

ANSI B11.24 Machines transferts

ANSI/RIA R15.06 Exigences de sécurité pour les robots et systèmes robotisés industriels

NFPA 79 Norme électrique pour les machines industrielles

ANSI/PMMI B155.1 Machines de conditionnement et machines de conversion pour le conditionnement - Normes de sécurité

19.2 Réglementations de l'OSHA applicables

OSHA Documents listed are part of: Code of Federal Regulations Title 29, Parts 1900 to 1910 (Les documents de l'OSHA répertoriés font partie du : Code of Federal Regulations (Code des réglementations fédérales) Titre 29, Parties 1900 à 1910)

OSHA 29 CFR 1910.212 General Requirements for (Guarding of) All Machines (OSHA 29 CFR 1910.212 Exigences générales en matière de protection de toutes les machines)

OSHA 29 CFR 1910.147 The Control of Hazardous Energy (lockout/tagout) (OSHA 29 CFR 1910.147 Maîtrise des énergies dangereuses (verrouillage/étiquetage))

OSHA 29 CFR 1910.217 (Guarding of) Mechanical Power Presses (OSHA 29 CFR 1910.217 (Protection des) presses mécaniques)

19.3 Normes européennes et internationales applicables

EN ISO 12100 Sécurité des machines – Notions fondamentales, principes généraux de conception — Évaluation et réduction des risques

ISO 13857 Sécurité des machines — Distances de sécurité empêchant d'atteindre les zones dangereuses

ISO 13850 (EN 418) Dispositifs d'arrêt d'urgence – Aspects fonctionnels – Principes de conception

ISO 13851 Dispositifs de commande bimanuelle – Aspects fonctionnels – Principes de conception et de choix

IEC 62061 Sécurité fonctionnelle des systèmes de commande électriques, électroniques et programmables liés à la sécurité

EN ISO 13849-1:2015 Parties des systèmes de commande relatives à la sécurité

EN 13855 (EN 999) Positionnement des équipements de protection en fonction de la vitesse d'approche des parties du corps

ISO 14119 (EN 1088) Dispositifs de verrouillage associés à des protecteurs – Principes de conception et de choix

EN 60204-1 Équipement électrique des machines — Partie 1 : Prescriptions générales

IEC 61496 Équipement de protection électrosensible

IEC 60529 Degrés de protection procurés par les boîtiers

IEC 60947-1 Appareillage à basse tension – Règles générales

IEC 60947-5-1 Appareillage à basse tension – Appareils et éléments de commutation pour circuits de commande

IEC 60947-5-5 Appareillage à basse tension - Dispositifs d'arrêt d'urgence électriques avec fonction de réarmement manuel mécanique

IEC 61508 Sécurité fonctionnelle des systèmes électriques, électroniques, programmables liés à la sécurité

IEC 62046 Sécurité des machines – Application des équipements de protection à la détection de la présence de personnes

ISO 16092-1 Sécurité des machines-outils — Presses — Partie 1 : Exigences générales de sécurité

ISO 16092-3 Sécurité des machines-outils — Presses — Partie 3 : Exigences de sécurité pour les presses hydrauliques

ISO 16092-4 Sécurité des machines outils — Presses — Partie 4 : Exigences de sécurité pour les presses pneumatiques

ISO 4413 Transmissions hydrauliques — Règles générales et exigences de sécurité relatives aux systèmes et leurs composants

ISO 4414 Transmissions pneumatiques — Règles générales et exigences de sécurité pour les systèmes et leurs composants

20 Glossaire

A

Reset automatique

Fonction opérationnelle du module d'entrée de sécurité qui permet d'activer automatiquement la sortie de sécurité assignée lorsque tous les dispositifs d'entrée associés à celle-ci ont l'état marche.

C

Changement d'état (COS, Change of State)

Changement d'un signal d'entrée quand il bascule de l'état marche à l'état d'arrêt ou de l'état d'arrêt à l'état marche.

Temps anti-rebond fermé à ouvert

Temps pendant lequel un signal d'entrée instable ou un rebond des contacts d'entrée est ignoré afin d'éviter le déclenchement inopiné du contrôleur. Sa valeur est réglable entre 6 et 100 ms. La valeur par défaut est 6 ms (50 ms pour les détecteurs d'inhibition).

Contacts complémentaires

Deux jeux de contacts qui ont constamment des états opposés.

Concurrent (Concurrence)

Paramétrage exigeant un état d'arrêt simultané pour les deux canaux avant de pouvoir repasser à l'état marche. Si cette condition n'est pas satisfaite, l'entrée passe en condition de défaut.

D

Personne désignée

Toute personne identifiée et désignée par écrit par l'employeur comme étant suffisamment compétente et dûment formée pour effectuer une procédure de vérification déterminée.

Redondance multiple

Pratique consistant à utiliser des composants, des circuits, des modes de fonctionnement de différentes conceptions, architectures ou fonctions pour garantir la redondance et limiter le risque de défaillances de mode commun.

Double voie

Existence de lignes de signal redondantes pour chaque entrée ou sortie de sécurité.

F

Défaut

État d'un dispositif caractérisé par son incapacité à exécuter une fonction requise, sauf au cours d'une maintenance préventive ou d'autres opérations planifiées ou si cette incapacité résulte d'un manque de ressources externes. Un défaut résulte souvent d'une défaillance du dispositif lui-même mais il peut apparaître sans défaillance préalable.

Dispositif de commutation final (FSD)

Composant du système de commande lié à la sécurité de la machine qui interrompt le circuit de l'élément de contrôle primaire de la machine (MPCE) quand le dispositif de commutation du signal de sortie (OSSD) passe à l'état désactivé.

H

Protection rigide (fixe)

Grilles, barres ou autres barrières mécaniques fixées à la structure de la machine et prévues pour empêcher l'entrée du personnel dans la ou les zone(s) dangereuse(s) d'une machine, tout en permettant de voir la zone de fonctionnement. La taille maximale des ouvertures est déterminée par la norme applicable (Tableau O-10 de la norme OSHA 29CFR1910.217), également appelée dispositif de surveillance fixe.

I

ISD

Le protocole de communication ISD (In-Series Diagnostics) fournit des informations de performance et d'état des différents dispositifs d'une chaîne à l'API ou à l'IHM (interface homme-machine). Une notification est envoyée pour l'ouverture ou la fermeture d'une porte, des actionneurs ou capteurs désynchronisés ou mal alignés, et toute une série d'attributs de fonctionnement du système supplémentaires.

M

Élément de contrôle primaire de la machine (MPCE)

Élément électrique, externe au système de sécurité, qui contrôle directement le fonctionnement normal de la machine. Cet élément est le dernier à fonctionner lors du démarrage ou de l'arrêt de la machine.

Temps de réponse de la machine

Délai entre l'activation du dispositif d'arrêt d'une machine et l'instant où les éléments dangereux de la machine ne posent plus de risque puisqu'ils ont été mis à l'arrêt.

Reset manuel

Fonction opérationnelle du dispositif d'entrée de sécurité qui ne permet d'activer la sortie de sécurité assignée qu'après un reset manuel et si les autres dispositifs d'entrée associés à celle-ci sont en état marche.

O

Signal OFF (désactivation)

Signal de la sortie de sécurité qui se produit quand au moins un des signaux des dispositifs d'entrée associés passe en état d'arrêt. Dans ce manuel, la sortie de sécurité est dite désactivée ou en état OFF quand le signal est de 0 V CC.

Signal ON (activation)

Signal de la sortie de sécurité qui se produit quand tous les signaux des dispositifs d'entrée associés passent en état marche. Dans ce manuel, la sortie de sécurité est dite active ou en état ON quand le signal est de 24 V CC.

Temps anti-rebond ouvert à fermé

Temps pendant lequel un signal d'entrée instable ou un rebond des contacts d'entrée est ignoré afin d'éviter un démarrage non souhaité de la machine. Sa valeur est réglable entre 10 et 500 ms. La valeur par défaut est de 50 ms.

P

Risque d'enfermement

Un risque d'enfermement existe quand une personne passe un dispositif de protection (qui envoie une commande d'arrêt pour supprimer le risque), puis continue d'avancer dans la zone protégée, à l'intérieur du périmètre surveillé par exemple. Par la suite, sa présence n'est plus détectée et le danger réside dans un (re)démarrage imprévu de la machine alors que la personne est toujours dans la zone protégée.

Protection très basse tension (PELV ou Protection extra-low voltage)

Alimentation à très basse tension de protection destinée aux circuits mis à la terre. Selon la norme IEC 61140 : « Un système PELV est un dispositif électrique dans lequel la tension ne peut pas dépasser le niveau minimum ELV (25 V CA efficaces ou 60 V CC sans ondulation) dans des conditions normales et en condition de défaut unique, à l'exception de défauts de masse dans d'autres circuits ».

Q

Personne qualifiée

Toute personne titulaire d'un diplôme reconnu ou d'un certificat de formation professionnelle, ou toute personne ayant démontré, par ses connaissances approfondies et son expérience, sa capacité à résoudre les problèmes relevant de son domaine de spécialité.

R

Signal marche

Signal d'entrée surveillé par le contrôleur qui, lorsqu'il est détecté, entraîne l'activation (état On) d'une ou de plusieurs sorties de sécurité si les signaux d'entrée qui leur sont associés sont également en état marche.

S

Très basse tension de sécurité (SELV ou Security Extra Low Voltage)

Alimentation à très basse tension de sécurité ou distincte, destinée aux circuits sans mise à la terre. Selon la norme IEC 61140 : « Un système SELV est un dispositif électrique dans lequel la tension ne peut pas dépasser le niveau ELV (25 V CA efficaces ou 60 V CC sans ondulation) dans des conditions normales et en condition de défaut unique, y compris les défauts à la terre dans d'autres circuits ».

Simultané (Simultanéité)

Paramétrage exigeant un état d'arrêt simultané pour les deux voies ET que celles-ci repassent à l'état marche avec un décalage de 3 secondes maximum. Si les deux conditions ne sont pas satisfaites, l'entrée passe en condition de défaut.

Circuit

Fait de n'avoir qu'une ligne de signal pour une entrée ou une sortie de sécurité.

Test de démarrage

Pour certains dispositifs de protection, notamment les barrières immatérielles ou les portes de sécurité, il peut être utile de tester au moins une fois le dispositif à la mise sous tension pour s'assurer qu'il fonctionne correctement.

Pour tester l'appareil, il convient de désactiver les sorties, puis de les réactiver.

Signal d'arrêt

Signal d'entrée surveillé par le contrôleur qui, en cas de détection, entraîne la désactivation (OFF) d'une ou de plusieurs sorties de sécurité. Dans ce manuel, le dispositif d'entrée ou le signal du dispositif peut avoir l'état d'arrêt

Reset du système

Reset configurable d'une ou de plusieurs sorties de sécurité afin qu'elles s'activent à la mise sous tension du contrôleur, s'il est configuré pour une mise sous tension manuelle, et dans les situations de blocage (détection de défaut).

L'index

A

abréviations 111
accessoires
  SC10-2 358
  XS/SC26 358
activation
  de l’inhibition 161
ADC 309
Adresse IP 180
afficher les données du contrôleur 137
ajouter
  entrée 86
  entrée de sécurité 86
  sortie d'état 90
AND (ET) 119
annulation de la temporisation 64, 316
approche 317
arrêt de protection 41, 314
arrêt de sécurité 41
arrêt séquentiel 58
arrêts fonctionnels 14, 19
ATO 15, 19, 328, 330
autoconfiguration 125
AVM 50

B

Bascule RS 120
Bascule SR 120
bits d’état 302
bloc 1 impulsion 164
bloc commande bimanuelle 171
bloc commande de presse 165
bloc d’inhibition 156
bloc de dérivation 150
bloc de reset à verrouillage 153
bloc dispositif de commande 152
bloc fonction
  1 impulsion 164
  commande bimanuelle 171, 175
  commande de presse 165
  dispositif de commande 152
  inhibition 156
  reset à verrouillage 153
  temporisation 151
bloc fonction Commande bimanuelle 175
blocs fonction 9, 121, 150
blocs logiques 9, 118
bordure de sécurité 45
bordure, sécurité 45
bouton arrêt d’urgence 39
bouton d’arrêt d'urgence 314
bouton d’arrêt d’urgence 39
Byte 181

C

capteur
  inhibition 59
capteur d’inhibition 48
capteur d’inhibition de la commande de presse 59
capteur optique 42, 314
circuits d'arrêt d'urgence 77
circuits d'arrêt de sécurité 77
code PIN 10, 135, 136
codes d’erreur 345
codes de défaut
  SC10-2 354
  XS/SC26 349
commande bimanuelle
  avec inhibition 314
  sans inhibition 314
commande de presse 57, 83, 97
conditions de fonctionnement 25
configuration
  exemple 95
configuration au démarrage 313
Configuration PC requise 28
confirmation d’une configuration 92
connecté manuellement 107
Connecté par USB 107
contraste de l’écran 176
contraste interface embarquée 176
Contrôle de redondance cyclique 64, 280
Conversion analogique-numérique 309
CRC 64, 280
CSV 132, 183

D

DAP 271
défauts 349
démarrage de cycle 57
dérivation 162, 316
désactivées 107
Détection auto ISD 326
Device Access Point
  DAP
diagnostic
  enregistrer contrôleur de sécurité 359
diagnostic des défauts 176, 349
diagnostic en série 19
dimensions 28
disponibles 107
dispositif d’entrée
  sécurité 33
dispositif d’entrée de sécurité 33
dispositif de commande 41, 317
Dispositif non trouvé 107
dispositifs d'entrée
  auxiliaires 60
dispositifs d'entrée auxiliaire virtuelle 64
dispositifs d'entrée auxiliaires 60
distance de sécurité
  commande bimanuelle 43
  tapis de sécurité 46
distance minimale
  commande bimanuelle 43
  tapis de sécurité 46
données du contrôleur
  lire 137
  visualiser 138
données du contrôleur de sécurité
  affichage 138
Données spécifiques à un dispositif ISD 54, 214, 268, 282
données spécifiques au dispositif ISD 255
DWORD 181

E

EDM 74
enregistrer
  configuration 92
  diagnostic du contrôleur de sécurité 359
  projet 92
entrées de contrôle 316
ESI
  installation 307
état des LED 323
état du système 176
état LED 320–323
EtherCAT 299
Ethernet 9
EtherNet/IP™ 183
étiquetage 150
exemple de configuration 95, 97

F

fichier d’étiquettes 132
Fichier XML 132
FID 12, 18
fil commun 71
fonctionnement d'un dispositif d'entrée de sécurité 314

G

garantie 359
General Station Description
  GSD
gestionnaire de mots de passe 10
gestionnaire des mots de passe 135, 136
GSD
  installation 286

H

Hex 181

I

impression de la configuration 134
imprimer 134
impulsion de test 19, 328
indicateur
  état 320, 321, 323
indicateur d'état 320–323
indicateur d’état 323
Informations esclave EtherCAT 299
informations sur le module 139
inhibition
  bidirectionnelle 315
  dérivation 316
  limite de temps 162
  temps limite 315
  unidirectionnelle 315
  unilatérale 315
inhibition bidirectionnelle 315
inhibition bilatérale 315
inhibition unidirectionnelle 315
inhibition unilatérale 315
installation
  électrique 31
installation des pilotes
  vérification 347
installation électrique 31
interface
  embarquée 176, 325

PC 8, 111
interface de bus de terrain 130
interface embarquée 176, 325
interrupteur
dérivation 49
interrupteur à câble 40, 314
interrupteur au pied 60
interrupteur de dérivation 49
ISD 19, 51, 132

J

journal
configuration 139
défaut 138
journal de configuration 139
journal de défauts 138

L

L5X 132, 183, 184
langue
sélection 112
LED 320–323
limite de temps
inhibition 162
lire les données du contrôleur 137
logiciel 8, 111
Logiciel 30, 112
logique de contrôle 91
logique interne 9

M

ME 161
Menu PDO 308
Modbus TCP 241
mode
configuration 176
temps réel 325
mode de configuration 177
mode simulation 142
mode temps réel 140, 325, 344
modèle de données 271, 300
modèle n° 176
modèles
SC10-2 17
XS/SC26 11
modules d’extension
XS/SC26 11
montage du contrôleur de sécurité 30
mot de passe 10, 135, 136

N

NAND (NON-ET) 120
nettoyage 359
neutralisation
dépendante de l'inhibition 315
neutralisation dépendante de l'inhibition 315
niveaux d’intégrité des circuits de sécurité 39
nom
contrôleur 129
nom du contrôleur 129
NOR (NON-OU) 120
NOT (NON) 120
nouveau projet 115
nouvelle configuration 91

O

objets assemblés 133
Octet 181
onglet
Accès réseau 129
bus de terrain 129
Équipement 116
Ethernet industriel 125
ISD 123
Logique Ladder 122
Mode simulation 142
Mode temps réel 140
Résumé de la configuration 133
Schéma de câblage 121
Vue fonctionnelle 117
Onglet Accès réseau 129
onglet bus de terrain 129
onglet Équipement 116
onglet Ethernet industriel 125
Onglet ISD 123
onglet Logique Ladder 122
onglet Mode simulation 142
onglet Résumé de la configuration 133
onglet Schéma de câblage 121
onglet Vue fonctionnelle 117
optimisation automatique des bornes 15, 328
Optimisation automatique des bornes 19, 330
OR (OU) 119

P

paramètres
projet 115
réseau 128, 129
paramètres du projet 115
paramètres projet 115
paramètres réseau
EtherCAT 131
Modbus TCP, Ethernet/IP, PCCC 130
PROFINET 130
PCCC 256
PDO
activation 309
désactiver 308
pièces de rechange
SC10-2 358
XS/SC26 358
PLCopenXML 300
porte à verrouillage 41
porte, à verrouillage 41
PROFINET 271

R

raccourci 110
RCD 64
récupérer les informations actuelles du contrôleur 137
redémarrage 107
réglages d'usine 342
régler
contraste de l’écran 176
contraste interface embarquée 176
réparations 359
réseau connecté 107
reset à verrouillage 317
reset du système 325
reset manuel virtuel 64
résumé
configuration 176
retard au déclenchement 316, 317

S

SC-USB2 8
SC-XM2 8, 10, 334–337, 341
SC-XM3 8, 10, 334–337, 341
SC-XMP2 10
sortie
fonctionnalité 83
voyant d’inhibition 162
sortie d'approche 317
sortie d’état 81, 82
sortie de sécurité
retard au déclenchement 316, 317
temporisation d'arrêt 316
sortie de voyant d’inhibition 162
sortie secondaire 317
sorties d'état
virtuelles 84
sorties d'état virtuelles 84
sorties d’état
SC10-2 19
XS/SC26 14
sorties d’état virtuelles
SC10-2 19
XS/SC26 14
sorties de relais de sécurité 19
sorties de sécurité 13, 67
spécifications
SC10-2 25
XS/SC26 21
SQS 58
String 181
surveillance de vanne réglable 50
surveillance des commutateurs externes 74
système de protection 41
système de protection à verrouillage 41

T

tags
API 132
tags d’API 132
tapis de sécurité 45, 314
tapis, sécurité 45
temporisation
annulation 64
annuler 316
bloc 151
temporisation d'arrêt 316
temps anti-rebond 37
temps anti-rebond fermé à ouvert 37
temps limite
inhibition 315
THC
commande bimanuelle

U

UDINT 181
UINT 181
USB 8

V

valeurs par défaut 342
vérification 312, 313
vérification à la mise en route 312, 313
vérification de l’installation des pilotes 347
vérification journalière 312
vérification périodique 312
vérification semestrielle 312
vérification système 312
verrouillage 150, 325, 326

visualiser les données du contrôleur
138

W

Word 181

X

XM2
SC-XM2
XM3
SC-XM3
XML 272
XOR (OU exclusif) 120