

CONTRÔLEUR DE SÉCURITÉ

Type SC22-3

Utilisable avec boutons d'arrêt d'urgence, interrupteurs de sécurité, rideaux lumineux de sécurité y compris mono ou multi-faisceaux, commandes bimanuelles, Commutateurs auxiliaires, tapis et bords de sécurité, capteurs d'inhibition, interrupteurs Bypass et mains courantes de sécurité

Manuel d'instructions

Version européenne, française



BANNER[®]
more sensors, more solutions

Tous droits réservés.

Cette publication ne peut être reproduite ou transmise, en tout ou en partie, sous quelque forme ou par quelque moyen que ce soit sans autorisation écrite préalable.

© - Banner Engineering Corp., 9714 10th Avenue North, Minneapolis, MN 55441, USA.

135453 rév. A 01.07.08

Page blanche

Table des matières

1 SÉCURITÉ GÉNÉRALE. 1

1.1 AUTOCOLLANTS DE SÉCURITÉ 1

 1.1.1 Avertissements 1

 1.1.2 Précautions 1

 1.1.3 Remarques 1

1.2 INFORMATIONS CONCERNANT LES ÉTIQUETTES DE SÉCURITÉ SUR LES PRODUITS 2

1.3 NORMES DE SÉCURITÉ 2

1.4 TAUX DE PROTECTION À L'ACCÈS 2

1.5 SÉCURITÉ ÉLECTRIQUE 3

1.6 CONDITIONS D'UTILISATION DE L'ÉQUIPEMENT 3

 1.6.1 Interface du contrôleur de sécurité SC22-3. 3

1.7 PROTOCOLE DE SÉCURITÉ 4

1.8 PERSONNES DÉSIGNÉES ET QUALIFIÉES 4

 1.8.1 Personne désignée 4

 1.8.2 Personne qualifiée. 4

1.9 ENTRÉES DE SÉCURITÉ 4

 1.9.1 États des signaux de fonctionnement et d'arrêt 4

1.10 RÉARMEMENTS 5

 1.10.1 Réarmement manuel. 5

 1.10.2 Réarmement du système 5

1.11 INHIBITION. 5

1.12 INFORMATION DE DÉNI DE RESPONSABILITÉ. 5

1.13 NIVEAUX DE PARASITE DE L'ÉQUIPEMENT 5

1.14 NIVEAUX DE VIBRATION 5

1.15 NIVEAUX D'IRRADIATION 5

 1.15.1 Niveaux d'immunité électromagnétique. 5

1.16 CONCEPTION ET TESTS 6

1.17 DISTANCES DE SÉCURITÉ 6

 1.17.1 Distance de sécurité des détecteurs optiques. 6

 1.17.2 Distance de sécurité pour des commandes bimanuelles 6

 1.17.3 Distances de sécurité pour des tapis de sécurité 6

1.18 SURVEILLANCE DES COMMUTATEURS EXTERNES 6

2 VUE GÉNÉRALE 7

2.1 CARACTÉRISTIQUES 7

2.2 APPLICATIONS 7

2.3 INFORMATIONS SUPPLÉMENTAIRES SUR LE RÉARMEMENT 7

 2.3.1 Entrées de réarmement manuel et automatique assignées à une même sortie de sécurité. 7

 2.3.2 Entrées de sécurité avec réarmement manuel commun assigné à la même sortie de sécurité 8

2.4 ENTRÉES DE SÉCURITÉ ET ENTRÉES AUXILIAIRES. 8

 2.4.1 Logique interne 8

 2.4.2 Commande bimanuelle 8

 2.4.2.1 Activation d'une commande bimanuelle à la mise sous tension 8

 2.4.3 Dispositif de commande 9

 2.4.3.1 Limite de temps du dispositif de commande 9

 2.4.4 Fonctions d'inhibition (Muting). 9

Table des matières (suite)

| | |
|--|-----------|
| 2.4.4.1 Inhibition | 9 |
| 2.4.4.2 Limite de temps d'inhibition (temporisateur de porte arrière) | 9 |
| 2.4.4.3 Fonction d'inhibition à la mise sous tension | 10 |
| 2.4.5 Fonction du bouton de Bypass | 10 |
| 2.4.5.1 Limite de temps de l'interrupteur de bypass | 11 |
| 2.4.5.2 Bypass avec inhibition | 11 |
| 2.4.6 EDM | 11 |
| 2.4.6.1 Surveillance simple voie | 11 |
| 2.4.6.2 Surveillance double voies | 11 |
| 2.5 CONFIGURATION DU CONTRÔLEUR DE SÉCURITÉ | 12 |
| 2.5.1 Sorties de sécurité | 12 |
| 2.5.1.1 Arrêts fonctionnels selon IEC 60204-1 | 13 |
| 2.5.1.2 Raccordement des sorties OSSD | 13 |
| 2.5.1.3 Retard à l'enclenchement et au déclenchement des sorties de sécurité | 14 |
| 2.5.2 Sorties d'état | 15 |
| 2.5.2.1 Sorties d'état de lampe d'inhibition | 15 |
| 2.5.3 Assignation des E/S et relation de commande des E/S | 16 |
| 2.5.3.1 Entrées de sécurité et entrées auxiliaires assignées aux sorties | 16 |
| 2.5.3.2 Entrées assignées à des entrées | 16 |
| 2.6 PARAMÈTRES SYSTÈME | 16 |
| 2.6.1 Décomposition des paramètres | 16 |
| 2.6.1.1 Nom de la configuration | 16 |
| 2.6.1.2 Nom de l'auteur | 16 |
| 2.6.1.3 Mode à la mise sous tension | 17 |
| 2.6.2 Inhibition à la mise sous tension | 17 |
| 2.6.3 Réarmement surveillé | 17 |
| 2.7 LOGIQUE INTERNE | 17 |
| 2.7.1 Autres fonctions logiques | 17 |
| 2.8 VUE GÉNÉRALE DU MOT DE PASSE | 17 |
| 2.9 CONFIRMATION D'UNE CONFIGURATION | 18 |
| 2.10 VUE GÉNÉRALE DE L'INTERFACE PC | 18 |
| 2.11 VUE GÉNÉRALE DE L'INTERFACE EMBARQUÉE | 18 |
| 3 INFORMATIONS GÉNÉRALES | 21 |
| 3.1 PRODUIT | 21 |
| 3.1.1 Marquage CE/plaque d'identification du produit | 21 |
| 3.1.2 Certificat de conformité | 21 |
| 3.1.3 Déclaration de conformité | 21 |
| 3.2 FICHE TECHNIQUE | 21 |
| 3.2.1 Spécifications | 21 |
| 3.2.2 Type n° | 23 |
| 3.2.2.1 Modèle et type du contrôleur de sécurité SC22-3 | 23 |
| 3.2.3 Dimensions du contrôleur de sécurité SC22-3 | 24 |
| 3.3 INFORMATIONS DES CLIENTS | 24 |

Table des matières (suite)

4 INSTALLATION - SYSTÈME 25

4.1 INTERFAÇAGE DU CONTRÔLEUR DE SÉCURITÉ SC22-3 25

4.2 COMPOSANTS 25

4.3 RACCORDEMENT DU CONTRÔLEUR DE SÉCURITÉ SC22-3 26

4.3.1 Raccordement électrique 26

4.3.2 Connexions USB 26

4.3.3 Outil de programmation SC-XMP 26

4.3.4 Carte SC-XM1 mémoire externe XM 26

4.4 EXPLICATIONS SUR LA CONNEXION DES DISPOSITIFS DE SÉCURITÉ 27

4.5 PROPRIÉTÉS DES DISPOSITIFS D'ENTRÉE DE SÉCURITÉ 27

4.5.1 Généralités 28

4.5.2 Désignation 28

4.5.3 Type de circuit 28

4.5.4 Logique de réarmement 28

4.5.5 Bornes d'entrée 28

4.5.6 Assigné à : 28

4.5.7 Réglages avancés 29

4.5.7.1 Changement d'état du signal (simultanéité) 29

4.5.7.2 Temps d'anti-rebond fermé à ouvert / temps d'anti-rebond ouvert à fermé 30

4.5.8 Test au démarrage 30

4.5.9 Temps limite du dispositif 30

4.5.10 Paire de capteurs d'inhibition 30

4.5.11 Interrupteur de bypass 30

4.6 PROPRIÉTÉS DES DISPOSITIFS D'ENTRÉES AUXILIAIRES 30

4.6.1 Dispositifs de réarmement manuel 30

4.6.2 Interrupteur marche / arrêt 30

4.6.3 Interrupteur d'inhibition 30

4.7 CONFIGURATION DU CONTRÔLEUR DE SÉCURITÉ 31

4.7.1 OBI 31

4.7.2 Interface PC 33

4.7.3 Définition de l'application de protection 33

4.7.4 Construction de la configuration 33

4.7.5 Confirmation de la configuration 33

4.8 RACCORDEMENT DES EDM, OSSD SORTIE DE SÉCURITÉ ET FSD 34

4.8.1 EDM 34

4.8.1.1 Surveillance simple voie 34

4.8.1.2 Surveillance double voies 34

4.8.1.3 Pas de surveillance 34

4.8.2 Raccordement d'interface FSD 34

4.8.2.1 Circuits d'arrêt de sécurité (de protection) 34

4.8.2.2 Connexion du contrôleur de sécurité aux modules d'interface 35

4.8.3 Installation du fil commun en courant continu 35

4.9 SORTIES D'ÉTAT 35

4.9.1 Conventions pour les signaux d'état des sorties 35

4.10 VÉRIFICATION DE MISE EN SERVICE 35

Table des matières (suite)

| | |
|--|-----------|
| 4.11 INSTALLATION DU LOGICIEL | 36 |
| 4.11.1 Installation du logiciel PCI | 36 |
| 4.11.1.1 Prescriptions du système | 36 |
| 4.11.1.2 Installation du logiciel | 36 |
| 5 INSTRUCTIONS DE FONCTIONNEMENT - PCI | 37 |
| 5.1 TRAVAILLER AVEC LE PROGRAMME PCI | 37 |
| 5.1.1 Installation du logiciel PCI | 37 |
| 5.1.2 Démarrage du programme PCI | 37 |
| 5.1.2.1 Diagrammes et résumés | 38 |
| 5.1.3 Outils de configuration | 39 |
| 5.1.4 Création d'une nouvelle configuration | 40 |
| 5.1.5 Ajout de dispositifs d'entrée de sécurité et d'entrée auxiliaire | 40 |
| 5.1.6 Sélection des entrées de sécurité | 41 |
| 5.1.6.1 Ajouter un arrêt d'urgence | 41 |
| 5.1.6.2 Ajout d'un interrupteur pour porte | 43 |
| 5.1.6.3 Ajout d'un capteur optique | 43 |
| 5.1.6.4 Ajout d'une commande bimanuelle | 44 |
| 5.1.6.5 Ajout d'une paire de capteurs d'inhibition | 44 |
| 5.1.6.6 Ajout d'une surveillance de dispositif externe | 45 |
| 5.1.7 Ajouter des dispositifs d'entrée auxiliaire | 46 |
| 5.1.7.1 Ajouter un interrupteur ON/OFF | 46 |
| 5.1.7.2 Ajout d'un interrupteur d'inhibition | 46 |
| 5.1.8 Assignation des sorties de sécurité | 47 |
| 5.1.9 Configurer les sorties d'état | 47 |
| 5.1.10 Confirmation de la configuration | 48 |
| 5.1.10.1 Validation de la configuration | 48 |
| 5.1.10.2 Modification de la configuration | 49 |
| 5.1.11 Réarmement du système | 49 |
| 5.1.12 Modification d'une configuration existante | 49 |
| 5.1.13 Réception d'une configuration depuis un contrôleur de sécurité SC22-3 | 50 |
| 5.1.14 Envoi d'une configuration au contrôleur de sécurité SC22-3 | 50 |
| 5.1.15 Ouvrir une configuration à partir de la carte XM | 50 |
| 5.1.16 Envoi d'une configuration à la carte XM | 50 |
| 5.1.17 Verrouillage de la carte XM | 50 |
| 5.1.18 Changement du mot de passe en utilisant le PCI | 50 |
| 5.1.19 Exportation de documents | 51 |
| 5.1.20 Impression | 51 |
| 5.1.21 Accès au registre d'erreurs | 51 |
| 5.1.22 Capture programmée du registre d'erreurs | 52 |
| 5.1.23 Affichage live | 52 |

Table des matières (suite)

6 INSTRUCTIONS DE FONCTIONNEMENT - OBI 53

6.1 MODE RUN (FONCTIONNEMENT) 53

6.1.1 Écran de diagnostic d'erreurs 53

6.1.2 Résumé de la configuration 54

6.1.2.1 Assignement des terminaux 54

6.1.2.2 Liaison entrée / sortie 54

6.1.2.3 Paramètres états des sorties 54

6.1.2.4 Voir les temps de réponse 54

6.1.3 Numéro du modèle 54

6.1.4 Régler le contraste de l'écran 55

6.1.5 Enregistrer la configuration 55

6.2 ENTRÉE DANS LE MODE DE CONFIGURATION 55

6.2.1 Entrer le mot de passe du contrôleur 55

6.3 MODE DE CONFIGURATION 56

6.3.1 Fichier de configuration 56

6.3.1.1 Modifier la configuration 56

6.3.1.2 Envoyer un fichier à XM 63

6.3.1.3 Recevoir fichier de l'XM 63

6.3.1.4 Effacer la configuration 64

6.3.2 Confirmer la configuration 64

6.3.2.1 Confirmer la configuration des entrées 64

6.3.2.2 Confirmer la configuration des sorties 65

6.3.2.3 Confirmer la configuration des paramètres du système 65

6.3.2.4 Étape de confirmation finale 65

6.3.3 Options du système 66

6.3.3.1 Changer le mot de passe 66

6.3.3.2 Sélectionner le langage 66

6.3.4 Sortir du mode de configuration 66

7 INSTRUCTIONS DE FONCTIONNEMENT — GÉNÉRALITÉS 67

7.1 AFFICHAGE DES INFORMATIONS DU CONTRÔLEUR — PCI 67

7.2 AFFICHAGE DES INFORMATIONS DU CONTRÔLEUR — OBI 68

7.2.1 Mode Run (fonctionnement) 68

7.2.1.1 Nom de la configuration 68

7.2.1.2 État de la sortie de sécurité 68

7.2.1.3 État de l'entrée 68

7.2.1.4 État du système 69

7.2.1.5 État OBI de la carte XM 69

7.3 RÉARMEMENT MANUEL 69

7.4 RÉARMEMENT SYSTÈME ET CONDITIONS DE BLOCAGE 70

7.5 PARAMÈTRES DU SIGNAL DE RÉARMEMENT 70

7.5.1 Reset contrôlé 70

7.5.2 Réarmement non surveillé 70

Table des matières (suite)

| | |
|--|-----------|
| 8 ENTRETIEN | 71 |
| 8.1 MAINTENANCE PRÉVENTIVE | 71 |
| 8.2 VÉRIFICATION DU SYSTÈME | 71 |
| 8.2.1 Planning des vérifications | 71 |
| 8.2.2 Vérification de mise en service | 71 |
| 8.2.3 Vérifications périodiques (tous les 6 mois) | 71 |
| 8.2.4 Vérifications opérationnelles journalières | 71 |
| 8.2.5 Procédure d'installation | 71 |
| 8.2.5.1 Pré vérifications de mise en service | 71 |
| 8.2.5.2 Vérification du fonctionnement du système | 72 |
| 8.2.5.3 Procédure | 72 |
| 8.2.6 Mise en service et configuration initiale – vérifications périodiques | 72 |
| 8.2.6.1 Vérification du système de sécurité et des dispositifs de protection | 72 |
| 8.2.6.2 Fonctions de mise sous tension et de réarmement | 73 |
| 8.2.6.3 Fonctions d'une commande bimanuelle | 73 |
| 8.2.6.4 Fonctions d'arrêt d'urgence et interrupteur à câble | 74 |
| 8.2.6.5 Autres fonctions de dispositifs d'arrêt | 74 |
| 8.2.6.6 Fonctions d'inhibition | 74 |
| 8.2.6.7 Option d'inhibition à la mise sous tension | 74 |
| 8.2.6.8 Fonction d'interrupteur de bypass (avec inhibition) | 75 |
| 8.2.6.9 Fonction d'interrupteur de bypass (sans inhibition) | 75 |
| 8.2.6.10 Fonction de dispositif de commande | 75 |
| 8.2.6.11 Vérification (finale) du système | 75 |
| 8.3 MAINTENANCE CORRECTRICE | 76 |
| 8.3.1 Nettoyage | 76 |
| 8.3.2 Réparations et service sous garantie | 76 |
| 8.3.3 Recherche de pannes | 77 |
| 8.3.3.1 Récupération suite à un blocage | 79 |
| 8.3.3.2 Diagnostic d'erreur par le PCI | 79 |
| 8.3.3.3 Diagnostic d'erreurs par OBI | 80 |
| 8.4 PIÈCES DE RECHANGE, OUTILS SPÉCIAUX ET ACCESSOIRES | 82 |
| 8.4.1 Pièces détachées | 82 |
| 8.4.1.1 Kit de démarrage du contrôleur de sécurité | 82 |
| 8.4.1.2 Relais de sécurité | 83 |
| 8.4.1.3 Contacts reliés mécaniquement | 84 |
| 8.4.2 Documentation | 84 |

Table des matières (suite)

A1 SCHÉMAS DE CÂBLAGE 85

A2 Dispositif d'entrée et catégorie de sécurité REFERENCE 89

A2.1 INTÉGRITÉ DU CIRCUIT DE SÉCURITÉ ET ISO 13849-1 (EN954-1) PRINCIPES DE CIRCUIT DE SÉCURITÉ 89

 A2.1.1 Niveaux d'intégrité des circuits de sécurité 89

 A2.1.2 Exclusion des défauts 89

A2.2 ARRÊTS DE PROTECTION (SÉCURITÉ) 91

 A2.2.1 Conditions 91

 A2.2.2 Possibilités de connexions 91

 A2.2.2.1 Canal simple, 1 borne – canal simple, 2 borne – canal simple, contact PNP 91

 A2.2.2.2 Double canal, 2 bornes – Double canal, 3 bornes 91

 A2.2.2.3 Double canal, PNP 91

 A2.2.2.4 Double canal, 4 bornes 91

 A2.2.2.5 Complémentaire, 2 bornes – Complémentaire, 3 bornes 91

 A2.2.2.6 complémentaire, contact PNP 91

A2.3 INTERRUPTEURS POUR PORTE (OU PROTECTION VERROUILLÉE) 92

 A2.3.1 Niveaux d'intégrité des circuits de sécurité 92

 A2.3.2 Conditions 92

 A2.3.2.1 Interrupteurs de verrouillage de sécurité à ouverture positive 92

 A2.3.2.2 Interrupteurs de verrouillage de sécurité à fonctionnement magnétique 92

 A2.3.2.3 Surveillance des interrupteurs de verrouillage de sécurité raccordés en série 93

 A2.3.2.4 Connexions en série et considérations sur l'intégrité du circuit de sécurité 93

 A2.3.2.5 Catégorie 2 93

 A2.3.2.6 Catégorie 3 93

 A2.3.2.7 Catégorie 4 93

 A2.3.3 Interrupteurs pour portes (ou protections interverrouillées) possibilités de connexions 94

 A2.3.3.1 Canal simple, 1 borne – canal simple, 2 borne – canal simple, contact PNP 94

 A2.3.3.2 Double canal, 2 bornes – Double canal, 3 bornes 94

 A2.3.3.3 Double canal, PNP 94

 A2.3.3.4 Double canal, 4 bornes 94

 A2.3.3.5 Complémentaire, 2 bornes – Complémentaire, 3 bornes 94

 A2.3.3.6 Complémentaire, contact PNP 95

 A2.3.3.7 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes 95

 A2.3.3.8 2 complémentaires, contact PNP 95

A2.4 CAPTEURS OPTIQUES (BARRIÈRE IMMATÉRIELLE) 96

 A2.4.1 Niveaux d'intégrité des circuits de sécurité 96

 A2.4.2 Exigences 96

 A2.4.3 Distance de sécurité 96

 A2.4.4 Connexion générique 97

 A2.4.4.1 Canal simple, 1 borne – canal simple, 2 borne – canal simple, contact PNP 97

 A2.4.4.2 Double canal, 2 bornes – Double canal, 3 bornes 97

 A2.4.4.3 Double canal, PNP 97

 A2.4.4.4 Complémentaire, 2 bornes – Complémentaire, 3 bornes 97

Table des matières (suite)

| | |
|--|-----|
| A2.4.4.5 Complémentaire, contact PNP | 97 |
| A2.5 COMMANDE BIMANUELLE | 98 |
| A2.5.1 Distance de sécurité | 99 |
| A2.5.2 Possibilités de connexions | 99 |
| A2.5.2.1 Canal double, 2 bornes – Canal double, 3 bornes – Canal double, 4 bornes | 99 |
| A2.5.2.2 Double canal, PNP | 100 |
| A2.5.2.3 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes | 100 |
| A2.5.2.4 2 complémentaires, contact PNP | 100 |
| A2.6 TAPIS DE SÉCURITÉ (BORDURES DE SÉCURITÉ) | 101 |
| A2.6.1 Conditions | 101 |
| A2.6.1.1 Conception et construction d'un système de tapis de sécurité | 101 |
| A2.6.2 Possibilités de connexions | 102 |
| A2.6.3 Installation | 102 |
| A2.6.4 Distance de sécurité | 103 |
| A2.7 ARRÊTS D'URGENCE | 104 |
| A2.7.1 Niveaux d'intégrité des circuits de sécurité | 104 |
| A2.7.2 Conditions | 104 |
| A2.7.2.1 Niveaux d'intégrité des circuits de sécurité avec plusieurs boutons d'arrêt d'urgence | 105 |
| A2.7.2.2 Catégorie 2 | 105 |
| A2.7.2.3 Catégorie 3 | 105 |
| A2.7.2.4 Catégorie 4 | 105 |
| A2.7.3 Possibilités de connexions | 105 |
| A2.7.3.1 Canal simple, 1 borne – canal simple, 2 borne – canal simple, contact PNP | 105 |
| A2.7.3.2 Double canal, 2 bornes – Double canal, 3 bornes | 105 |
| A2.7.3.3 Double canal, PNP | 106 |
| A2.7.3.4 Double canal, 4 bornes | 106 |
| A2.8 INTERRUPTEUR À CÂBLE | 107 |
| A2.8.1 Instructions d'installation | 107 |
| A2.8.2 Possibilités de connexions | 107 |
| A2.8.2.1 Canal simple, 1 borne – canal simple, 2 borne – canal simple, contact PNP | 107 |
| A2.8.2.2 Double canal, 2 bornes – Double canal, 3 bornes | 107 |
| A2.8.2.3 Double canal, PNP | 107 |
| A2.8.2.4 Double canal, 4 bornes | 107 |
| A2.8.2.5 Complémentaire, 2 bornes – Complémentaire, 3 bornes | 108 |
| A2.8.2.6 complémentaire, contact PNP | 108 |
| A2.9 DISPOSITIF D'ACTIVATION (SIMULTANÉ) | 109 |
| A2.9.1 Instructions d'installation | 109 |
| A2.9.2 Possibilités de connexions | 109 |
| A2.9.2.1 Double canal, 2 bornes – Double canal, 3 bornes | 109 |
| A2.9.2.2 Double canal, PNP | 109 |
| A2.9.2.3 Double canal, 4 bornes | 109 |
| A2.9.2.4 Complémentaire, 2 bornes – Complémentaire, 3 bornes | 110 |

Table des matières (suite)

| | |
|--|------------|
| A2.9.2.5 complémentaire, contact PNP | 110 |
| A2.9.2.6 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes | 110 |
| A2.9.2.7 2 complémentaires, contact PNP | 110 |
| A2.10 INTERRUPTEUR DE BYPASS (BYPASSANT LES PROTECTIONS) | 111 |
| A2.10.1 Conditions | 111 |
| A2.10.1.1 Procédures de sécurité d'exploitation et de formation | 111 |
| A2.10.1.2 Consignations | 111 |
| A2.10.2 Possibilités de connexions | 111 |
| A2.10.2.1 Double canal, 2 bornes – Double canal, 3 bornes | 111 |
| A2.10.2.2 Double canal, PNP | 112 |
| A2.10.2.3 Double canal, 4 bornes | 112 |
| A2.10.2.4 Complémentaire, 2 bornes – Complémentaire, 3 bornes | 112 |
| A2.10.2.5 complémentaire, contact PNP | 112 |
| A2.10.2.6 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes | 112 |
| A2.10.2.7 2 complémentaires, contact PNP | 112 |
| A2.11 CAPTEUR D'INHIBITION (PAIRE) | 113 |
| A2.11.1 Fonction d'inhibition | 113 |
| A2.11.2 Exigences | 113 |
| A2.11.2.1 Généralités | 113 |
| A2.11.2.2 Exemples de détecteurs et de contacteurs d'inhibition (muting) | 114 |
| A2.11.3 Possibilités de connexions | 114 |
| A2.11.3.1 Double canal, 2 bornes – Double canal, 3 bornes | 114 |
| A2.11.3.2 Double canal, PNP | 114 |
| A2.11.3.3 Double canal, 4 bornes | 114 |
| A2.11.3.4 Complémentaire, 2 bornes – Complémentaire, 3 bornes | 114 |
| A2.11.3.5 complémentaire, contact PNP | 115 |
| A2.11.4 Inhibition (ME), | 115 |
| A2.11.4.1 Fonction de réarmement du contrôleur de simultanéité | 115 |
| A2.11.5 Sortie de voyant d'inhibition (ML) | 115 |
| A2.11.6 Limite de temps d'inhibition (temporisateur de porte arrière) | 115 |
| A2.11.7 Inhibition à la mise sous tension | 116 |
| A2.11.8 Miroirs d'angle, systèmes optiques de sécurité et inhibition | 116 |
| A2.11.9 Dispositifs de sécurité de détection de présence multiples | 116 |
| A2.11.10 Séquences dans le temps de l'inhibition | 117 |
| A3 DÉCLARATION DE CONFORMITÉ | 119 |
| A3.1 DÉCLARATION DE CONFORMITÉ | 119 |
| A4 GLOSSAIRE ET ABRÉVIATIONS | 121 |
| A4.1 LISTE DES ABRÉVIATIONS | 121 |
| A4.2 GLOSSAIRE | 121 |
| A5 INFORMATION COMMERCIALES | 125 |

Liste des figures

| | |
|--|-----|
| Figure 1 Logique dans le temps des entrées de sécurité de réarmement manuel Auto et manuel surveillé assignées à la même sortie de sécurité (la sortie de sécurité n'a pas de délai) | 7 |
| Figure 2 Logique dans le temps des entrées de sécurité avec un réarmement manuel surveillé commun, assigné à la même sortie de sécurité | 8 |
| Figure 3 Logique dans le temps d'un dispositif de commande bimanuelle et réarmement manuel des entrées de sécurité. | 8 |
| Figure 4 Dispositif de commande et logique de temps du mode actif | 9 |
| Figure 5 Diagramme de temps pour une paire de détecteurs d'inhibition avec inhibition activée | 9 |
| Figure 6 Logique de temps d'une barrière immatérielle avec détecteurs d'inhibition et interrupteur de bypass | 10 |
| Figure 7 Évolution dans le temps de l'état EDM à canal simple par rapport à la sortie de sécurité. | 11 |
| Figure 8 Évolution dans le temps de EDM canal double entre les canaux | 11 |
| Figure 9 État EDM canal double par rapport à la sortie de sécurité. | 11 |
| Figure 10 Logique de temps de la sortie de sécurité avec temporisation OFF | 14 |
| Figure 11 Sorties de sécurité | 14 |
| Figure 12 Assignation de l'entrée et de la sortie | 16 |
| Figure 13 Options de configuration de OBI | 19 |
| Figure 14 Marquage CE et plaque d'identification du contrôleur de sécurité SC22-3 | 21 |
| Figure 15 Dimensions du contrôleur de sécurité SC22-3. | 24 |
| Figure 16 Composants du kit du Contrôleur de sécurité SC22-3. | 25 |
| Figure 17 Connexion du PC au port USB du contrôleur de sécurité | 26 |
| Figure 18 Raccordement du PC à l'outil de programmation SC-XMP | 26 |
| Figure 19 Contrôleur de sécurité SC22-3 Raccordement à SC-XM1 carte de mémoire externe (carte XM) | 26 |
| Figure 20 Détail des propriétés des entrées de sécurité | 27 |
| Figure 21 Interface embarqué avec boutons, écran d'affichage à LCD et indicateurs d'état. | 31 |
| Figure 22 Options du mode Run OBI du Contrôleur de sécurité SC22-3. | 53 |
| Figure 23 Options du mode de configuration OBI du contrôleur de sécurité SC22-3 | 56 |
| Figure 24 Modifier OBI sorties d'état - Options | 62 |
| Figure 25 Bornier des sorties de sécurité. | 71 |
| Figure 26 Connexion EDM à Canal simple | 85 |
| Figure 27 Raccordement EDM à canal double. | 85 |
| Figure 28 Connexion générique illustrant les options canal simple, canal double et pas de EDM | 85 |
| Figure 29 Connexion EDM canal simple au module d'interface SC-IM9A | 86 |
| Figure 30 Raccordement EDM à canal double au module d'interface IM-T-9A | 86 |
| Figure 31 raccordement EDM canal simple au module d'interface IM-T-9A | 87 |
| Figure 32 Installation du fil courant continu commun | 87 |
| Figure 33 Circuit catégorie 2 - Interrupteur de porte | 87 |
| Figure 34 Circuit catégorie 3 - Interrupteur de porte | 87 |
| Figure 35 Circuit catégorie 4 Circuit - Interrupteur de porte | 88 |
| Figure 36 Circuit d'arrêt d'urgence de catégorie 2 | 88 |
| Figure 37 Circuit d'arrêt d'urgence de catégorie 3 | 88 |
| Figure 38 Circuit d'arrêt d'urgence de catégorie 4 | 88 |
| Figure 39 Détermination de la distance de sécurité (S) pour le tapis de sécurité | 103 |

Liste des figures (suite)

| | |
|---|-----|
| Figure 40 Diagramme de temps d'inhibition avec une paire de détecteurs d'inhibition, inhibition activée, barrière immatérielle et temps d'inhibition limité par un dispositif de sécurité pouvant être inhibé configuré pour réarmement automatique | 117 |
| Figure 41 Diagramme de temps d'inhibition avec quatre détecteurs d'inhibition, inhibition activée, barrière immatérielle et temps d'inhibition limité par un dispositif de sécurité pouvant être inhibé configuré pour réarmement automatique | 117 |
| Figure 42 Diagramme de temps d'inhibition avec une paire de détecteurs d'inhibition, inhibition activée, commande bimanuelle et temps d'inhibition limité | 118 |
| Figure 43 Déclaration de conformité | 119 |
| Figure 44 Déclaration de conformité - Traduction | 120 |

Liste des tableaux

| | |
|---|----|
| Tableau 1 Présentation des avis de sécurité | 1 |
| Tableau 2 Autocollant d'identification du contrôleur de sécurité SC22-3 | 2 |
| Tableau 3 Logique interne de l'entrée de sécurité | 8 |
| Tableau 4 Contrôleur de sécurité SC22-3 Spécifications générales | 21 |
| Tableau 5 Contrôleur de sécurité SC22-3 | 23 |
| Tableau 6 Dispositif d'entrée de sécurité du Contrôleur de sécurité et présentation de la surveillance du type de circuit | 28 |
| Tableau 7 Types de changement d'état de signal (COS)(simultanéité). | 29 |
| Tableau 8 Dispositifs d'entrée auxiliaire | 30 |
| Tableau 9 Détail de l'indicateur d'état de l'interface embarqué | 32 |
| Tableau 10 Convention pour les signaux | 35 |
| Tableau 11 Dispositifs des Entrées de sécurité & Entrées auxiliaires configurables | 40 |
| Tableau 12 Décomposition des dispositifs supplémentaires d'entrée de sécurité | 59 |
| Tableau 13 Présentation des dispositifs d'Entrée de sécurité supplémentaires | 61 |
| Tableau 14 Présentation des messages d'état de la sortie de sécurité | 68 |
| Tableau 15 Présentation des messages d'état des dispositifs d'entrée | 68 |
| Tableau 16 Présentation des messages d'état de la carte XM | 69 |
| Tableau 17 Explications des indications de diagnostic | 77 |
| Tableau 18 Informations sur le kit et les accessoires du contrôleur de sécurité SC22-3 | 82 |
| Tableau 19 Modules d'interface Série SC-IM9 | 83 |
| Tableau 20 Modules d'interface Série IM-T-9 | 83 |
| Tableau 21 Contacts reliés mécaniquement | 84 |
| Tableau 22 Références de la documentation | 84 |
| Tableau 23 dispositifs d'entrée, options des circuits et leurs catégories de sécurité possibles | 90 |

1 SÉCURITÉ GÉNÉRALE

AVERTISSEMENT AVANT DE CONTINUER, LIRE CE CHAPITRE DE SÉCURITÉ GÉNÉRALE EN ENTIER

Ce chapitre couvre toutes les informations de sécurité concernant le Contrôleur de sécurité SC22-3 et son utilisation.

 **AVERTISSEMENT**

C'EST DE LA RESPONSABILITÉ DE CELUI PERSONNE QUALIFIÉE QUI CONFIGURE, INSTALLE OU ENTRETIEN LE CONTRÔLEUR DE SÉCURITÉ SC22-3 DE :

- LIRE AVEC ATTENTION, BIEN COMPRENDRE ET SUIVRE LES INFORMATIONS DE CE MANUEL
- EFFECTUER UNE ÉVALUATION DES RISQUES DE L'APPLICATION DE PROTECTION SPÉCIFIQUE À LA MACHINE
- DÉTERMINER LES DISPOSITIFS DE PROTECTION ET LES MÉTHODES APPROPRIÉES SELON LES EXIGENCES DE ISO 13849-1 ET DE EN 945-1 ET QUI SONT RÉFÉRENCÉS DANS LE MANUEL DU CONTRÔLEUR DE SÉCURITÉ SC22-3
- CRÉER ET CONFIRMER CHAQUE CONFIGURATION DU CONTRÔLEUR DE SÉCURITÉ SC22-3 PUIS VÉRIFIER QUE LA TOTALITÉ DU SYSTÈME DE PROTECTION (Y COMPRIS LES DISPOSITIFS D'ENTRÉE ET CEUX DE SORTIE) SONT OPÉRATIONNELS ET FONCTIONNENT COMME PRÉVU
- REVÉRIFIER PÉRIODIQUEMENT QUE L'ENSEMBLE DU SYSTÈME DE PROTECTION FONCTIONNE COMME PRÉVU

NE PAS SUIVRE UN DE CES RECOMMANDATIONS PEUT CRÉER UNE SITUATION POTENTIELLEMENT DANGEREUSE QUI PEUT ENTRAÎNER DES BLESSURES GRAVES, VOIRE MORTELLES.

1.1 AUTOCOLLANTS DE SÉCURITÉ

Pour monter et faire fonctionner le produit de façon sûre et efficace, des avis de sécurité sont affichés sur le produit et tout au long de ce manuel d'instructions.

Les autocollants de sécurité sont conformes à ISO 7010 et à ISO 3864-2.

Tous les signes de précaution et d'avertissement comportent des mots signalétiques qui attirent l'attention sur les messages de sécurité et correspondent au degré de risque encouru.

Tableau 1 en Page 1 présente les différents autocollants de sécurité qui sont utilisés dans ce document.

Tableau 1 Présentation des avis de sécurité

| Description | Exemple | Définition |
|-----------------------|--|---|
| AVERTISSEMENT |  AVERTISSEMENT | Un mot accompagné d'un triangle de sécurité indique une situation qui peut être dangereuse. Si on n'évite pas cette situation, l'action pourrait provoquer des blessures graves, voire la mort. Un AVERTISSEMENT est surligné en jaune. |
| PRÉCAUTION |  PRÉCAUTION | Un mot accompagné d'un triangle de sécurité indique une situation qui peut être dangereuse ou une pratique non sûre. Si on n'évite pas cette situation, l'action peut entraîner des blessures mineures à moyennes ou des dégâts aux équipements. Une PRÉCAUTION est surlignée en jaune. |
| PRÉCAUTION | PRÉCAUTION | Un mot qui indique une situation ou une pratique non sûre qui peut engendrer des dégâts aux équipements. Une PRÉCAUTION est surlignée en jaune. |
| Avertissement général |  | Indique un risque général. Des précisions sur ce risque apparaissent dans l'explication de la remarque de sécurité. |
| Haute tension |  | Indique un risque de haute tension. |

1.1.1 Avertissements

Ce type d'indication  **AVERTISSEMENT** est posté de préférence avant ou aussi près que possible de l'information à laquelle il se rapporte dans l'ensemble du manuel (voir le [Tableau 1 en Page 1](#)). Au cas où des indications identiques sont reproduites, une référence croisée est postée à l'endroit correspondant du texte ou du graphique pour renvoyer le lecteur à l'indication applicable.

Ils sont de deux ordres différents :

- Un  **AVERTISSEMENT** général est indiqué par le symbole  (voir exemple [AVERTISSEMENT, page 3](#))
- Un  **AVERTISSEMENT** de risque d'électrocution est indiqué par le symbole  (voir exemple [AVERTISSEMENT, page 4](#))

L'utilisateur doit lire l' **AVERTISSEMENT** correspondant avant de continuer.

1.1.2 Précautions

Ces types d'indication  **PRÉCAUTION** **PRÉCAUTION** sont postés de préférence avant ou aussi près que possible de l'information à laquelle ils se rapportent dans l'ensemble du manuel (voir le [Tableau 1 en Page 1](#)). Au cas où des indications identiques sont reproduites, une référence croisée est postée à l'endroit correspondant du texte ou du graphique pour renvoyer le lecteur à l'indication applicable.

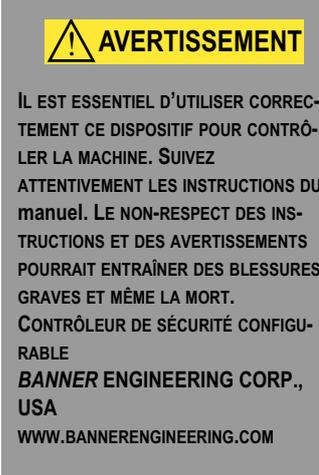
1.1.3 Remarques

 Une remarque est postée quand l'information est uniquement informative et non obligatoire. Elle est écrite et positionnée à proximité de l'information à laquelle elle s'applique.

1.2 INFORMATIONS CONCERNANT LES ÉTIQUETTES DE SÉCURITÉ SUR LES PRODUITS

Tableau 2 en Page 2 donne la liste des étiquettes de sécurité utilisées sur le produit ainsi que leurs descriptions et leurs emplacements.

Tableau 2 Autocollant d'identification du contrôleur de sécurité SC22-3

| SYMBOLE | EMPLACEMENT/SIGNIFICATION |
|---|--|
| <p>Fond jaune</p>  <p>AVERTISSEMENT</p> | <p>Situé sur le côté gauche du contrôleur de sécurité SC22-3.</p> <p>Indique les informations importantes suivantes :</p>   <p>IL EST ESSENTIEL D'UTILISER CORRECTEMENT CE DISPOSITIF POUR CONTRÔLER LA MACHINE. SUIVEZ ATTENTIVEMENT LES INSTRUCTIONS DU manuel. LE NON-RESPECT DES INSTRUCTIONS ET DES AVERTISSEMENTS POURRAIT ENTRAÎNER DES BLESSURES GRAVES ET MÊME LA MORT. CONTRÔLEUR DE SÉCURITÉ CONFIGURABLE BANNER ENGINEERING CORP., USA WWW.BANNERENGINEERING.COM</p> |

1.3 NORMES DE SÉCURITÉ

☛ La liste des normes ci-après est fournie aux utilisateurs de ce produit Banner. L'inclusion de ces normes ne signifie pas que le produit est spécifiquement conforme à d'autres normes que celles répertoriées dans les Spécifications (Paragraphe 3.2.1 en page 21) et la déclaration de conformité (Annexe A3.1 en page 119) de ce manuel.

ISO 7010 (2003)

Symboles graphiques – Couleurs de sécurité et signes de sécurité – Signes de sécurité utilisés sur les lieux de travail et les emplacements publics.

ISO 3864-2 (2004)

Symboles graphiques – Couleurs de sécurité et signes de sécurité – Partie 2 : Principes de conception des autocollants de sécurité pour les produits.

ISO 12100-1 (2003) & -2 (2003)(EN 292-1 & -2)

Sécurité des machines – Notions fondamentales, principes généraux de conception

ISO 13849-1 (2006)(EN 954-1)

Parties des systèmes de commande relatives à la sécurité

ISO 13850 (2006) (EN418)

Équipement d'arrêt d'urgence, aspects fonctionnels – Principes de conception

ISO 13851 (2002)(EN 574)

Dispositifs de commande bimanuelle – Aspects fonctionnels – Principes de conception

ISO 13852 (1996)(EN 294)

Distances de sécurité – membres supérieurs

ISO 13853 (1998) (prEN 811)

Distances de sécurité – Membres inférieurs

ISO 13855 (2002)(EN 999)

Positionnement des équipements de protection en fonction de la vitesse d'approche des parties du corps

ISO 14119 (1998) (EN 1088)

Dispositifs de verrouillage associés à des protecteurs – Principes de conception et de choix

ISO 14121-1 (2007)(EN 1050)

Principes d'appréciation du risque

IEC 60204-1 (2005-10)

Équipements électriques des machines – partie 1 : règles générales

IEC 61496-1 (2004-02), & IEC 61496-2 (2006-04)

Équipements de protection électrosensibles

IEC 60529 (2001-02)

Degrés de protection procurés par les enveloppes (Code IP)

IEC 60947-5-1 (2003-11)

Appareillage à basse tension – Appareils électromécaniques 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 60947-1 (2004-03)

Disjoncteur basse tension – Règles générales

2006/42/EC

Sécurité des machines

1.4 TAUX DE PROTECTION À L'ACCÈS

Le contrôleur de sécurité SC22-3 est conforme aux normes suivantes de protection contre l'intrusion IP selon IEC 60529 :

- IEC IP20*

*Le contrôleur de sécurité SC22-3 doit être installé à l'intérieur d'une armoire conforme à IEC l'IEC IP54 au minimum pour l'IP20.

1.5 SÉCURITÉ ÉLECTRIQUE



AVERTISSEMENTS

RISQUE D'ÉLECTROCUTION – DÉBRANCHER L'ALIMENTATION ÉLECTRIQUE

COUPER SYSTÉMATIQUEMENT L'ALIMENTATION ÉLECTRIQUE DU CONTRÔLEUR DE SÉCURITÉ ET DE LA MACHINE PROTÉGÉE AVANT DE FAIRE UN RACCORDEMENT OU DE REMPLACER UN COMPOSANT.

RACCORDEMENTS ÉLECTRIQUES

LES RACCORDEMENTS ÉLECTRIQUES DOIVENT ÊTRE EFFECTUÉS PAR UNE [Personnes qualifiées](#) ET CONFORMES AUX NORMES ÉLECTRIQUES. NE RACCORDER AU SYSTÈME AUCUN ÉLÉMENT AUTRE QUE CE QUI EST DÉCRIT EN [Chapitre 4](#) DE CE MANUEL, SOUS PEINE DE PROVOQUER DES BLESSURES GRAVES, VOIRE MORTELLES.

Le contrôleur de sécurité SC22-3 a été conçu pour répondre aux normes de sécurité électriques listées en [DOC](#).

1.6 CONDITIONS D'UTILISATION DE L'ÉQUIPEMENT

Important:

Lire ceci avant de continuer !

LE CONCEPTEUR DE LA MACHINE, L'INGÉNIEUR DE COMMANDE, LE CONSTRUCTEUR ET L'ÉLECTRICIEN D'ENTRETIEN ONT LA RESPONSABILITÉ DE CONCEVOIR ET D'ENTREtenir CE PRODUIT CONFORMÉMENT À TOUTES LES NORMES ET RÉGLEMENTS APPLICABLES. LE PRODUIT NE PEUT FOURNIR LA FONCTION DE PROTECTION VOULUE QUE S'IL EST CORRECTEMENT INSTALLÉ, UTILISÉ ET ENTRETENU SELON LES INSTRUCTIONS. CE MANUEL FOURNIT DES INSTRUCTIONS COMPLÈTES D'INSTALLATION, DE FONCTIONNEMENT ET D'ENTRETIEN. IL EST FORTEMENT RECOMMANDÉ DE LIRE LE MANUEL EN ENTIER. VEUILLEZ TRANSMETTRE TOUTE QUESTION CONCERNANT L'APPLICATION OU L'UTILISATION DE CE PRODUIT AU DÉPARTEMENT ENGINEERING APPLICATIONS DE [BANNER](#) AU NUMÉRO DE TÉLÉPHONE OU À L'ADRESSE INDIQUÉS AU DOS DE LA COUVERTURE. POUR PLUS D'INFORMATIONS SUR LES INSTITUTIONS AMÉRICAINES ET INTERNATIONALES QUI PEUVENT FOURNIR LES NORMES D'APPLICATION DES PROTECTIONS ET DES PERFORMANCES DES PRODUITS DE PROTECTION, VOIR LA LISE EN TROISIÈME DE COUVERTURE.

UTILISATION DES AVERTISSEMENTS

LES AVERTISSEMENTS SONT LÀ POUR RAPPELER AU CONCEPTEUR DE LA MACHINE, À L'INGÉNIEUR DE COMMANDE, AU CONSTRUCTEUR DE LA MACHINE, À L'ÉLECTRICIEN D'ENTRETIEN OU À L'UTILISATEUR FINAL LES FAÇONS D'ÉVITER UNE MAUVAISE UTILISATION DE CE PRODUIT ET D'UTILISER EFFICACEMENT LE CONTRÔLEUR DE SÉCURITÉ POUR RÉPONDRE AUX DIFFÉRENTES EXIGENCES D'APPLICATION DES PROTECTIONS. IL EST FORTEMENT RECOMMANDÉ DE LIRE ET DE RESPECTER LES AVERTISSEMENTS.



AVERTISSEMENTS

LIRE CE [PARAGRAPHE 1.6 EN PAGE 3](#) AVEC ATTENTION AVANT D'INSTALLER LE SYSTÈME

Le contrôleur de sécurité SC22-3 de [BANNER](#) EST UN DISPOSITIF ACCESSOIRE GÉNÉRALEMENT UTILISÉ EN ASSOCIATION AVEC UN OU PLUSIEURS DISPOSITIF(S) DE PROTECTION DE LA MACHINE. SA CAPACITÉ À RÉALISER CETTE FONCTION DÉPEND DU CARACTÈRE APPROPRIÉ DE L'APPLICATION ET DE L'INSTALLATION MÉCANIQUE ET ÉLECTRIQUE CORRECTE DU CONTRÔLEUR DE SÉCURITÉ SC22-3 ET DE L'INTERFACE AVEC LA MACHINE À PROTÉGER. SI TOUTES LES PROCÉDURES DE MONTAGE, D'INSTALLATION, D'INTERFACE ET DE VÉRIFICATION NE SONT PAS SUIVIES À LA LETTRE, LE CONTRÔLEUR DE SÉCURITÉ SC22-3 NE PEUT PAS ASSURER LA PROTECTION POUR LAQUELLE IL A ÉTÉ CONÇU. L'UTILISATEUR A DONC LA RESPONSABILITÉ DE S'ASSURER QUE L'ENSEMBLE DES LOIS, RÉGLEMENTS, CODES ET NORMES LOCALES, DE L'ÉTAT ET NATIONALES APPLICABLES À L'APPLICATION SONT RESPECTÉS. IL FAUT ÊTRE TRÈS ATTENTIF À RESPECTER TOUTES LES EXIGENCES LÉGALES ET TOUTES LES INSTRUCTIONS TECHNIQUES D'INSTALLATION ET D'ENTRETIEN DE CE MANUEL. LIRE ATTENTIVEMENT [Informations de sécurité au chapitre 1](#) DE CE MANUEL AVANT D'INSTALLER LE SYSTÈME. LE NON-RESPECT DE CETTE CONSIGNE PEUT ENTRAÎNER DES BLESSURES GRAVES, VOIRE MORTELLES. L'UTILISATEUR EST SEUL RESPONSABLE DE L'INSTALLATION ET DE L'INTERFACE DU CONTRÔLEUR DE SÉCURITÉ SC22-3 DE [BANNER](#) SUR LA MACHINE PROTÉGÉE PAR UNE [Personne qualifiée selon spécification du paragraphe 1.8.2 en page 4](#) CONFORMÉMENT À CE MANUEL ET AUX RÉGLEMENTATIONS APPLICABLES EN MATIÈRE DE SÉCURITÉ.

PAS UN DISPOSITIF DE PROTECTION AUTONOME D'UN POINT DE FONCTIONNEMENT

LE CONTRÔLEUR DE SÉCURITÉ SC22-3 N'EST PAS UN DISPOSITIF DE PROTECTION AUTONOME D'UN POINT DE FONCTIONNEMENT SELON LA DÉFINITION DES NORMES DE SÉCURITÉ EUROPÉENNES. IL EST DONC NÉCESSAIRE D'INSTALLER UN OU PLUSIEURS DISPOSITIF(S) DE PROTECTION DU POINT DE FONCTIONNEMENT, COMME DES BARRIÈRES IMMATÉRIELLES DE SÉCURITÉ OU DES PROTECTIONS FIXES POUR PROTÉGER LE PERSONNEL DES DANGERS DE LA MACHINE. LA NON-INSTALLATION DE PROTECTION DU POINT DE FONCTIONNEMENT SUR UNE MACHINE DANGEREUSE ET LE NON-RESPECT DES INSTRUCTIONS DES MANUELS D'INSTALLATION CORRESPONDANTS PEUVENT CRÉER UNE SITUATION DANGEREUSE ET ENTRAÎNER DES BLESSURES GRAVES, VOIRE MORTELLES.

RESPONSABILITÉ DE L'UTILISATEUR POUR LA SÉCURITÉ DE L'APPLICATION

LES EXEMPLES D'APPLICATION DÉCRITS EN [Annexe A3](#) REPRÉSENTENT DES SITUATIONS DE PROTECTION GÉNÉRALES. CHAQUE APPLICATION DE PROTECTION A DES EXIGENCES SPÉCIFIQUES. IL FAUT VEILLER À CE QUE TOUTES LES EXIGENCES LÉGALES SOIENT REMPLIES ET LES INSTRUCTIONS D'INSTALLATION SUIVIES. EN OUTRE, TOUTE QUESTION CONCERNANT LA PROTECTION DOIT ÊTRE DIRIGÉE VERS LE [Bureaux du siège social en page 125](#).

1.6.1 Interface du contrôleur de sécurité SC22-3

L'interface du contrôleur de sécurité SC22-3 dépend du type de machine et des protections qu'il faut interfacé avec le contrôleur. Le contrôleur est normalement interfacé avec des protections qui ne doivent être utilisées que sur des machines capables d'arrêter immédiatement leur mouvement à la réception d'un signal d'arrêt quelque soit le point de son cycle machine. L'utilisateur a la responsabilité de vérifier que la protection correspond à l'application et est installée conformément aux instructions des manuels appropriés.

S'il existe un doute quant à la compatibilité d'une machine et de ce contrôleur, contacter [Bureaux du siège social en page 125](#).

1.7 PROTOCOLE DE SÉCURITÉ

Le contrôleur de sécurité SC22-3 doit être monté à l'intérieur d'un boîtier ou d'une armoire IP conforme à l'IP54 ou plus, pour protéger le contrôleur des conditions environnementales mais aussi pour empêcher tout accès au personnel non autorisé, si les normes applicables le requièrent.

La clé (ou la combinaison) de l'armoire doit rester en possession d'une [Personne qualifiée selon spécification du paragraphe 1.8.2 en page 4](#) ; elle seule doit avoir accès aux interrupteurs de configuration.

1.8 PERSONNES DÉSIGNÉES ET QUALIFIÉES

1.8.1 Personne désignée

Une **personne désignée** ([Personne désignée en page 122](#)) est identifiée et désignée par l'employeur, par écrit, comme ayant suivi la formation et la qualification nécessaires pour effectuer les procédures de vérification spécifiées sur le contrôleur de sécurité SC22-3.

1.8.2 Personne qualifiée

Une **personne qualifiée** ([Personne qualifiée en page 122](#)) qui possède un niveau ou un certificat reconnu de formation professionnelle ou qui, de par l'étendue de ses connaissances, de sa formation et de son expérience, a démontré sa capacité à résoudre les problèmes associés à la mise en œuvre de ce système de sécurité.

1.9 ENTRÉES DE SÉCURITÉ



AVERTISSEMENT

ERREURS ET DÉFAILLANCES

LE CONTRÔLEUR DE SÉCURITÉ SC22-3 PEUT ÊTRE INTERFACÉ AVEC DES dispositifs d'entrée À DIFFÉRENTS NIVEAUX D'INTÉGRITÉ COMME CELA EST DÉCRIT EN [Annexe A2](#). L'UTILISATEUR DOIT EFFECTUER UNE ÉVALUATION DES RISQUES POUR DÉTERMINER LE NIVEAU D'INTÉGRATION CORRESPONDANT. L'UTILISATEUR DOIT AUSSI ÉLIMINER OU MINIMISER LE RISQUE DE DÉFAILLANCES ET D'ERREURS QUI PEUVENT SE PRODUIRE À LA SUITE DE LA PERTE DES FONCTIONS DE SÉCURITÉ.

Les entrées de sécurité entraînent l'arrêt du mouvement, pour éviter une situation dangereuse, en contrôlant la sortie de sécurité du contrôleur de sécurité SC22-3. Une sortie de sécurité en état OFF entraîne l'arrêt de tout mouvement et la coupure d'alimentation des actionneurs de la machine (en supposant que ceci n'entraîne pas de risques supplémentaires).

Pour qu'une sortie de sécurité passe sur ON, il faut que toutes les entrées de sécurité la contrôlant soient en état Run de fonctionnement. Certaines fonctions spéciales d'entrée de sécurité peuvent, dans des circonstances prédéfinies, suspendre temporairement le signal d'arrêt de l'entrée de sécurité pour conserver la sortie de sécurité en état ON (par ex. inhibition et shuntage).

Selon le type, les configurations d'entrée du contrôleur de sécurité SC22-3, sont capables de détecter les défaillances et les erreurs qui entraîneraient une perte de cette commande de la fonction de sécurité. Si une de ces défaillances ou erreurs est détectée, le contrôleur de sécurité SC22-3 se verrouille jusqu'à ce que le problème soit réglé.

D'autres configurations d'entrée n'ont pas cette capacité de détection. Il est recommandé que, dans toutes les circonstances, l'installation du contrôleur de sécurité SC22-3, de ses sécurités associées et des dispositifs de protection soient installés pour éliminer ou minimiser le risque de défaillances ou d'erreurs qui pourraient entraîner la perte de la fonction de sécurité.

Les méthodes d'élimination ou de minimisation du risque de ce type de défaillance sont les 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 des commandes d'interconnexion dans des tubes, des passages ou des chemins de câbles différents.
- Regrouper tous les éléments (modules, interrupteurs et contacteurs des commandes) dans une seule armoire, les uns à côté des autres, et les relier directement par des fils courts.
- Installer des raccords à réducteur de tension sur les câbles à plusieurs conducteurs (trop serrer un réducteur de tension peut entraîner des courts-circuits à cet endroit).
- Utiliser des composants à ouverture positive ou à conduite directe, installés et montés positivement.

Pour plus d'informations, voir [Paragraphe 2.4 en page 8](#)

1.9.1 États des signaux de fonctionnement et d'arrêt

Les entrées de sécurité à double voie ont deux lignes de signaux séparées. Les signaux double voie de certains dispositifs sont tous les deux positifs (+24 Vcc) quand le dispositif est en état Run de fonctionnement. D'autres ont une structure de circuit complémentaire dans laquelle un simple voie est sur 24 Vcc et l'autre sur 0 Vcc quand le dispositif est en état Run de fonctionnement. Dans un but de clarification, au lieu de se référer à une entrée de sécurité comme étant ON (par ex. 24 Vcc) ou OFF (par ex. 0 Vcc), ce manuel adopte la convention de l'état Run / état Stop.

1.10 RÉARMEMENTS

PRÉCAUTION

EMPLACEMENT DE L'INTERRUPTEUR DE RÉARMEMENT

Le bouton de réarmement du système ne doit être accessible que de l'extérieur et en pleine vue de la zone dangereuse. Les interrupteurs de réarmement manuel doit aussi être hors de portée de l'intérieur de la zone protégée et doit être protégé contre une utilisation non autorisée ou par inadvertance (par ex. utilisation de bagues ou de protections). Si des endroits ne sont pas visibles depuis les boutons de réarmement manuel, d'autres moyens de protection doivent être utilisés. Ne pas le faire peut provoquer des blessures graves, voire mortelles.

Deux types de RAZ manuel existent :

1.10.1 Réarmement manuel

Utilisé pour réarmer manuellement une sortie de sécurité qui est passée sur OFF en réponse à un signal d'arrêt d'une entrée de sécurité configurée pour (mode verrouillage) réarmement manuel. Le type de signal de réarmement manuel peut être configuré pour être soit surveillé soit non surveillé (le réglage par défaut est surveillé). Pour plus d'informations, voir [Paragraphe 2.3.1 en page 7](#) et [Paragraphe 7.3 en page 69](#).

1.10.2 Réarmement du système

Est utilisé pour récupérer après une erreur ou pour redémarrer le contrôleur quand une nouvelle configuration a été modifiée. Ce dispositif de réarmement manuel (bouton ou interrupteur) se raccorde à un borne d'entrée dédié du contrôleur de sécurité, intitulé SR & Sys Res. Le type de signal de réarmement manuel peut être configuré pour être surveillé ou pas (le réglage par défaut est surveillé). Pour plus d'informations, voir [Paragraphe 2.3.1 en page 7](#) et [Paragraphe 7.4 en page 70](#).

1.11 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 risque d'accès ou quand l'accès à la zone à risque est protégé.

Les détecteurs d'inhibition peuvent être assignés à une ou plusieurs entrées de sécurité "mutable" suivantes :

- Interrupteurs pour porte (Verrouillage)
- Détecteurs optiques
- Commande bimanuelle
- Tapis de sécurité

(boutons d'arrêt d'urgence, Interrupteurs par câble, arrêts de protection, dispositifs de commande, Surveillance des commutateurs externes, et interrupteurs de bypass sont dits « non-d'inhibition » dispositifs ou fonctions.)

Au moins deux détecteurs d'inhibition sont nécessaires pour chaque opération d'inhibition. Une ou deux paires de détecteurs d'inhibition peuvent être assignés à une ou plusieurs entrées de sécurité de façon à ce que leur sortie de sécurité assignée puisse rester ON pour achever l'opération (voir [Paragraphe 2.4.4 en page 9](#) et [Annexe A2.11 en page 113](#) pour plus d'informations).

1.12 INFORMATION DE DÉNI DE RESPONSABILITÉ

AVERTISSEMENT

IMPORTANT... LIRE CE PARAGRAPHE AVANT DE CONTINUER !

LA CONFORMITÉ D'UNE INSTALLATION PARTICULIÈRE D'UN CONTRÔLEUR DE SÉCURITÉ À TOUTES LES EXIGENCES APPLICABLES DÉPEND DE FACTEURS QUI SONT HORS DU CONTRÔLE DE **BANNER ENGINEERING CORP.** CES FACTEURS INCLUENT LA FAÇON DONT LES CONTRÔLEURS DE SÉCURITÉ SONT APPLIQUÉS, INSTALLÉS, CÂBLÉS, UTILISÉS ET ENTRETENUS. L'ACHETEUR ET L'UTILISATEUR SONT RESPONSABLES DE L'UTILISATION DES CONTRÔLEURS DE SÉCURITÉ SELON L'ENSEMBLE DES NORMES ET DES RÈGLEMENTS APPLICABLES. LES CONTRÔLEURS DE SÉCURITÉ NE PEUVENT PROTÉGER DES ACCIDENTS QUE S'ILS SONT CORRECTEMENT MONTÉS ET INTÉGRÉS À LA MACHINE, CORRECTEMENT UTILISÉS ET ENTRETENUS. **BANNER ENGINEERING CORP.** ESSAYE DE FOURNIR DES INSTRUCTIONS D'APPLICATION, D'INSTALLATION, DE FONCTIONNEMENT ET D'ENTRETIEN COMPLÈTES.

L'UTILISATEUR A LA RESPONSABILITÉ DE S'ASSURER QUE L'ENSEMBLE DES LOIS, RÈGLEMENTS, CODES ET RÉGULATIONS CONCERNANT L'UTILISATION DE CE SYSTÈME DE PROTECTION DANS UNE APPLICATION PARTICULIÈRE SONT RESPECTÉS. NOUS INSISTONS PARTICULIÈREMENT SUR LE FAIT QUE LES EXIGENCES LÉGALES DOIVENT ÊTRE RESPECTÉES ET LES INSTRUCTIONS D'INSTALLATION ET DE MAINTENANCE DE CE MANUEL SUIVIES.

LA LISTE DES NORMES EUROPÉENNES ET INTERNATIONALES QUI S'APPLIQUENT À CET ÉQUIPEMENT EST INDIQUÉE AU [DOC](#).

1.13 NIVEAUX DE PARASITE DE L'ÉQUIPEMENT

Le contrôleur de sécurité ne génère pas de bruit de fond et est donc conforme aux normes :

- IEC 61000-6-1
- EN 55011 (CISPR11)

1.14 NIVEAUX DE VIBRATION

En ce qui concerne les niveaux de chocs et de vibrations, le contrôleur de sécurité SC22-3 est conforme aux normes :

- IEC 61496-1

1.15 NIVEAUX D'IRRADIATION

1.15.1 Niveaux d'immunité électromagnétique

Le contrôleur de sécurité SC22-3 est conforme à la norme IEC 61496 concernant les niveaux électromagnétiques.

1.16 CONCEPTION ET TESTS

Le contrôleur de sécurité a été conçu pour des applications de protection jusqu'à la catégorie 4 PL (niveau de performances) "e" (ISO 13849-1) et SIL (niveau d'intégrité de sécurité; SIL) 3 (IEC 61508 et IEC 62061). Il a été complètement testé pour s'assurer qu'il correspond aux conditions de performances IEC et ISO en ce qui concerne sa fonction de sécurité aussi bien que sa fiabilité opérationnelle. Ce contrôleur de sécurité avec auto vérification comprend :

- Des microcontrôleurs redondants
- Un circuit de détection du signal d'entrée redondant
- Un circuit de contrôle de la sortie de sécurité redondant

Il faut remarquer que les performances du circuit de sécurité (par ex., les catégories) d'une entrée ou d'une sortie de sécurité sont principalement déterminées par les dispositifs et leurs interconnexions au contrôleur de sécurité SC22-3. Voir [Annexe A2](#) pour plus d'informations.

1.17 DISTANCES DE SÉCURITÉ

☛ *Les informations suivantes ne sont applicables qu'à des installations certifiées CE.*

1.17.1 Distance de sécurité des détecteurs optiques

Ces informations sont détaillées en [Annexe A2.4.3](#).

1.17.2 Distance de sécurité pour des commandes bimanuelles

Ces informations sont détaillées en [Annexe A2.5.1](#).

1.17.3 Distances de sécurité pour des tapis de sécurité

Ces informations sont détaillées en [Annexe A2.6.4](#).

1.18 SURVEILLANCE DES COMMUTATEURS EXTERNES



PRECAUTION

Configuration EDM

Si l'application ne fait pas appel à cette fonction, il est de la responsabilité de l'utilisateur de s'assurer que cela ne crée pas de situation dangereuse.

REMARQUE concernant les raccordements de la surveillance des commutateurs externes

Il est fortement recommandé de raccorder au moins un contact de surveillance normalement fermé, à guidage forcé, de chaque MPCE ou dispositif externe pour surveiller l'état des MPCEs (comme illustré aux [Figure 28](#), [Figure 29](#), [Figure 29](#), [Figure 30](#) et [Figure 31](#)). Dans ce cas, le fonctionnement des MPCE est vérifié. Les contacts de surveillance des MPCE doivent être utilisés pour conserver la fiabilité de la commande.

La sortie de sécurité du contrôleur de sécurité peut commander des relais, des contacteurs externes ou d'autres dispositifs ayant un jeu de contacts normalement fermés (NF) guidés en force (reliés mécaniquement) qui peuvent servir à surveiller l'état des contacts d'alimentation de la machine. Les contacts de surveillance sont NF quand le dispositif est sur OFF. Cette capacité permet au contrôleur de sécurité de détecter si les dispositifs sous tension répondent à la sortie de sécurité ou si les contacts normalement ouverts (NO) risquent d'être soudés entre eux ou bloqués sur ON.

La fonction de surveillance de dispositifs externes (EDM) est une méthode de surveillance d'erreurs et permet de s'assurer de l'intégrité fonctionnelle d'un système à double canaux, y compris les MPCE et les FSD.

Une entrée de surveillance de dispositifs externes ne peut être assignée qu'à une seule sortie de sécurité.

Les entrées de surveillance de dispositifs externes peuvent être configurées de trois façon différentes : simple voie, double voie ou pas de surveillance. La surveillance de dispositifs externes à simple voie ou double voie est utilisée quand les sorties du dispositif de commutation du signal de sortie (OSSD) commandent directement la coupure d'alimentation des MPCE ou des dispositifs externes.

Pour de plus amples informations, voir [Paragraphe 2.4.6 en page 11](#) et [Paragraphe 4.8.1 en page 34](#).

2 VUE GÉNÉRALE

Le contrôleur de sécurité SC22-3 de *Banner* (le contrôleur de sécurité ou le contrôleur) est un module de sécurité facile d'utilisation, configurable, fonctionnant en 24 Vcc et conçu pour surveiller des entrées de sécurité multiples des entrées auxiliaires et pour commander jusqu'à trois éléments de commande primaires indépendants d'une machine (MPCE). Il comprend les fonctions d'arrêt et de démarrage de sécurité de machines dont les mouvements internes sont dangereux. Le contrôleur de sécurité peut remplacer plusieurs modules de sécurité à relais dans des applications qui comprennent des entrées de sécurité comme des boutons d'arrêt d'urgence, des interrupteurs de verrouillage de sécurité, des barrières immatérielles de sécurité et autres dispositifs de protection. Il peut aussi être utilisé à la place de PLC (contrôleurs à logique programmable) ou d'autres dispositifs de sécurité avec logique quand ils deviennent excessifs dans l'application.

Les configurations sont créées en utilisant une interface à LCD (affichage à cristaux liquides) et un bouton ou en utilisant un PC raccordé au contrôleur de sécurité par un port USB (Universal Serial Bus).

2.1 CARACTÉRISTIQUES

Le contrôleur de sécurité SC22-3 de *Banner* dispose des caractéristiques suivantes :

- Un contrôleur facile d'utilisation avec des entrées et des sorties entièrement configurables
- Connexion de dispositifs d'entrée selon ISO 13849-1 fiabilité des commandes de catégorie 2, catégorie 3 ou catégorie 4
- Gère plusieurs fonctions de sécurité liées entre elles
- Vingt-deux entrées de dispositifs ou fonctions de sécurité et auxiliaires
- Trois sorties de sécurité double canal avec délai ON et OFF au choix
- Dix sorties d'état suivent l'état des entrées et des sorties, l'état d'inhibition, les conditions d'erreurs et les réarmements nécessaires
- Procédure de configuration simple en utilisant l'interface d'un PC (PCI) ou l'interface d'un contrôleur embarqué (OBI) assigne chaque dispositif d'entrée à une des trois sorties de sécurité
- Configurations protégées par mot de passe et confirmées avant usage, pour garantir l'intégrité de la sécurité
- Configurations transférables à plusieurs contrôleurs de sécurité SC22-3 et peuvent être envoyées par e-mail sous forme de pièce jointe
- Fonctionnement 24 Vcc.
- Conforme à SIL 3 (niveau d'intégrité de sécurité) selon IEC 62061, IEC 61508, et niveau de performance "e" catégorie 4 selon ISO 13849-1
- L'affichage en temps réel et le registre d'erreurs procurent une information de l'état "en temps réel" et un suivi de l'historique des erreurs
- Les diagrammes de raccordement, les diagrammes logiques Ladder et les résumés des configurations peuvent être imprimés et exportés sous forme de fichiers .pdf ou .dxf

2.2 APPLICATIONS

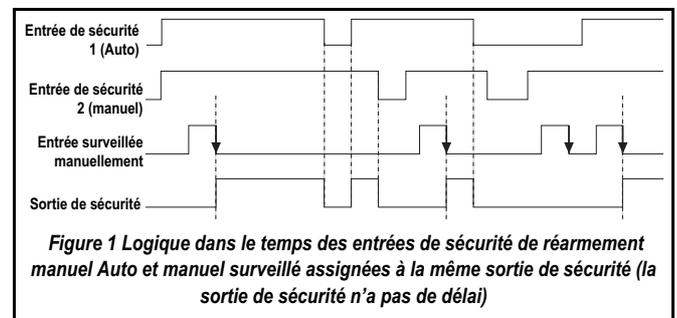
Le contrôleur de sécurité SC22-3 peut être utilisé à chaque fois qu'il faut utiliser des modules de sécurité. Le contrôleur de sécurité est particulièrement adapté à de nombreux types d'applications, dont :

- Commande bimanuelle avec fonction d'inhibition
- Cellules de traitement ou de soudage robotique avec inhibition de double zone
- Opérations de manutention de matériaux qui nécessitent plusieurs fonctions d'entrées et de bypass
- Stations de chargement manuel de carrousel
- Applications à plusieurs stations de commande bimanuelles
- Stations de fabrication

2.3 INFORMATIONS SUPPLÉMENTAIRES SUR LE RÉARMEMENT

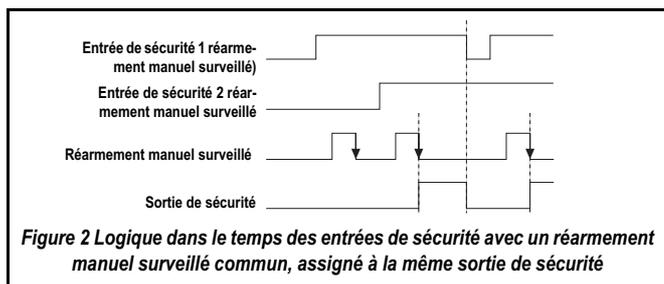
2.3.1 Entrées de réarmement manuel et automatique assignées à une même sortie de sécurité

Les dispositifs d'entrée de sécurité peuvent être configurés pour un réarmement manuel (mode manuel) ou automatique (mode automatique) et les deux types peuvent être assignés à la même sortie de sécurité. Pour qu'une sortie de sécurité passe sur ON, toutes les entrées de sécurité associées doivent être en état Run. Si une ou plusieurs entrées de sécurité sont configurées pour un réarmement manuel et qu'une ou plusieurs change de l'état d'arrêt à l'état Run, la sortie a alors besoin d'un signal de réarmement manuel avant de repasser sur ON (voir [Figure 1 en page 7](#)).



2.3.2 Entrées de sécurité avec réarmement manuel commun assigné à la même sortie de sécurité

Si deux entrées de sécurité, configurées toutes les deux pour un réarmement manuel, sont assignées à la même sortie de sécurité, alors seulement une opération de réarmement manuel est nécessaire pour réarmer manuellement la sortie de sécurité. Une opération de réarmement manuel est valable quand toutes les entrées de sécurité assignées à la sortie de sécurité sont en état Run et que le réarmement manuel est effectué. Si un réarmement manuel est effectué avant qu'une entrée de sécurité est en état Run, le signal de réarmement manuel est ignoré (sauf dans le cas d'une commande bimanuelle et d'une entrée ON/OFF) (voir [Figure 2 en page 8](#)).



Voir [Paragraphe 7.3 en page 69](#) pour avoir plus d'informations sur les réarmements.

2.4 ENTRÉES DE SÉCURITÉ ET ENTRÉES AUXILIAIRES

Le contrôleur de sécurité dispose de 22 bornes d'entrée qui peuvent être utilisés pour surveiller des dispositifs d'entrée de sécurité ou d'entrée auxiliaire. Ces dispositifs peuvent comporter des sorties transistorisées ou à contacts. Chacune de ces 22 bornes d'entrée peuvent soit surveiller un signal d'entrée ou fournir 24 Vcc. La fonction de chaque circuit d'entrée dépend du type de dispositif qui lui est raccordé. Cette fonction est établie à la configuration du contrôleur.

Se référer au [Chapitre 4](#) et à [Annexe A2](#) pour ce qui suit :

- Informations générales et particulières concernant les dispositifs d'entrée — les règles
- Options de connexions et avertissements et précautions appropriés
- Informations d'installation complémentaires (par ex. distances de sécurité)

[Annexe A2](#) comporte les connexions et autres informations utilisées pour intégrer les dispositifs suivants :

- Arrêt de protection (sécurité) — [Annexe A2.2 en page 91](#)
- Détecteur optique — [Annexe A2.4 en page 96](#)
- Interrupteur de sécurité (ou verrouillage de protection) — [Annexe A2.3 en page 92](#)
- Commande bimanuelle — [Annexe A2.5 en page 98](#)
- Tapis de sécurité (Bords) — [Annexe A2.6 en page 101](#)
- Arrêt d'urgence — [Annexe A2.7 en page 104](#)
- Interrupteur par câble (Câble) — [Annexe A2.8 en page 107](#)
- Dispositif d'activation (simultané) — [Annexe A2.9 en page 109](#)
- Interrupteur de bypass — [Annexe A2.10 en page 111](#)
- Capteur d'inhibition — [Annexe A2.11 en page 113](#)

Pour obtenir d'autres informations sur le raccordement de dispositifs au contrôleur de sécurité, contacter [Bureaux du siège social en page 125](#).

2.4.1 Logique interne

La logique interne du contrôleur est conçue pour qu'une sortie de sécurité ne puisse passer sur ON que si tous les signaux d'entrée de sécurité et les signaux d'auto vérification du contrôleur sont en état Run et indiquent qu'il n'y a pas d'erreur. [Tableau 3 en Page 8](#) illustre la logique interne.

Tableau 3 Logique interne de l'entrée de sécurité

| Entrée de sécurité 1 | Entrée de sécurité 2 | Sortie de sécurité 1 |
|----------------------|----------------------|----------------------|
| Stop | Stop | ARRÊT |
| Stop | Run | ARRÊT |
| Run | Stop | ARRÊT |
| Run | Run | ON |

[Tableau 3 en Page 8](#) illustre la logique pour deux entrées de sécurité qui sont assignées à la commande de la sortie de sécurité 1. Si une des entrées de sécurité est en état d'arrêt, la sortie de sécurité est OFF. Quand les deux entrées de sécurité et que le contrôleur sont en état Run, la sortie de sécurité 1 passe sur ON.

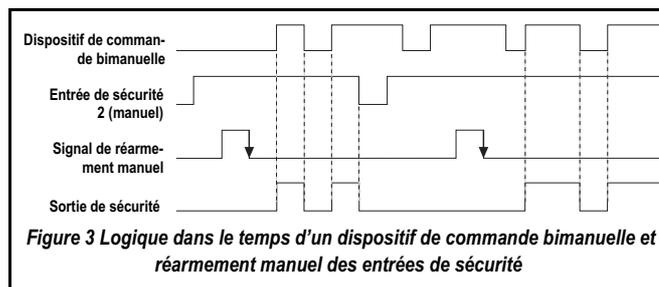
2.4.2 Commande bimanuelle

La fonction d'une commande bimanuelle nécessite que chaque actionnement de la commande se fasse en moins de 0,5 seconde l'une de l'autre pour produire un signal Run qui démarre un cycle machine. Les dispositifs de commande bimanuelle sont toujours les dernières entrées (dans le temps) à faire passer la sortie de sécurité sur ON. Si une ou plusieurs des autres dispositifs contrôlant la sortie de sécurité sont configurés pour un réarmement manuel et sont utilisés pour arrêter la machine, un réarmement manuel doit être effectué avant que le dispositif de commande bimanuelle puisse faire démarrer à nouveau le cycle de la machine. [Annexe A2.5 en page 98](#) pour plus d'informations.

2.4.2.1 Activation d'une commande bimanuelle à la mise sous tension

La logique de commande bimanuelle du contrôleur ne permet pas à la sortie de sécurité de passer sur ON quand la machine est initialement mise sous tension alors que chaque commande bimanuelle est en état Run. Chaque actionneur de commande bimanuelle doit d'abord passer par l'état d'arrêt puis revenir à l'état Run avant que la sortie de sécurité puisse passer sur ON (voir [Figure 3 en page 8](#)).

Un dispositif de commande bimanuelle n'a pas de possibilité de réarmement manuel.



2.4.3 Dispositif de commande

Le dispositif de commande commande activement la suspension d'un signal d'arrêt pendant une partie de l'opération de la machine dans laquelle un risque peut se produire. Le dispositif de commande permet à une partie dangereuse de la machine de fonctionner, mais ne peut pas la démarrer. Un signal de commande séparé d'un autre dispositif est nécessaire pour démarrer le déplacement dangereux.

Ce dispositif de commande doit avoir une autorité permettant de mettre le danger sur OFF ou sur arrêt quand il est utilisé. Le dispositif de commande est quelques fois appelé le 'simultanéité de l'homme vivant.'

Un dispositif de commande peut être assigné à une ou plusieurs sorties de sécurité. Quand le signal de commande passe de l'état d'arrêt à celui de Run, le contrôleur passe en mode actif. Dans ce mode, les sorties de sécurité associées passent sur ON si une des entrées de surveillance des dispositifs externes est fermée (elle peut néanmoins s'ouvrir quand les sorties sont passées sur ON) et que tous les dispositifs de contrôle arrêt d'urgence ou interrupteur par câble sont en état Run. À l'exception des dispositifs d'arrêt d'urgence et d'interrupteur par câble, tous les autres signaux d'entrée de sécurité (Run ou arrêt) sont ignorés tant que le contrôleur est en mode actif. La commande d'activation de la sortie de sécurité réside dans la fonction de la poignée d'assentiment pendant le mode actif. Pour sortir du mode actif, le dispositif de commande doit être dans l'état OFF et il faut effectuer un réarmement système. Voir [Annexe A2.9 en page 109](#) pour plus d'informations.

2.4.3.1 Limite de temps du dispositif de commande

La limite de temps d'activation du dispositif de commande peut être réglée entre 1 seconde et 30 minutes et ne peut être désactivée. Quand la limite de temps expire, les sorties de sécurité associées passent sur OFF. Pour démarrer un nouveau cycle de mode actif avec la limite de temps du réarmement manuel réglé à sa valeur d'origine, le dispositif de commande doit passer de ON à OFF et de nouveau sur ON (voir [Figure 4](#)).

Tous les temps de retard ON et OFF associés à la sortie de sécurité qui sont contrôlés par la fonction du dispositif de commande sont honorés pendant le mode actif.

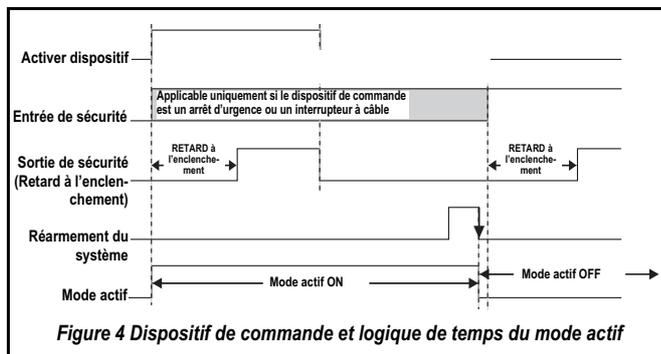


Figure 4 Dispositif de commande et logique de temps du mode actif

2.4.4 Fonctions d'inhibition (Muting)

2.4.4.1 Inhibition

La fonction inhibition activée ME 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 inhibition activée a été assigné à une entrée de sécurité que l'on peut inhiber, cette entrée de sécurité ne peut être inhibée que si l'interrupteur d'inhibition activée est en état activé (24 cc) au moment où le cycle d'inhibition est initié. Quand le cycle d'inhibition a démarré, l'entrée d'inhibition activée peut être mise sur OFF. Un dispositif d'entrée d'inhibition activée peut être assigné à une ou plusieurs sorties de sécurité que l'on peut inhiber (voir [Figure 5](#)).

Pour plus d'informations concernant les conditions d'inhibition activée, se référer à [Annexe A2.11 en page 113](#).

☛ L'activation de l'inhibition n'est pas une fonction de protection mais plutôt une fonction logique de la machine.

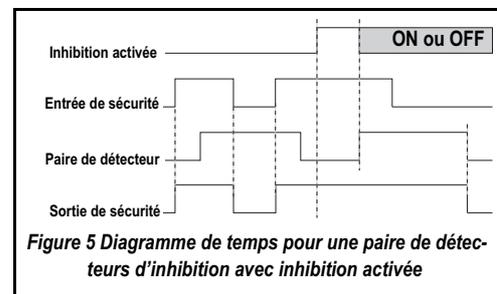


Figure 5 Diagramme de temps pour une paire de détecteurs d'inhibition avec inhibition activée

2.4.4.2 Limite de temps d'inhibition (temporisateur de porte arrière)

Une limite de temps peut être établie pour limiter la durée pendant laquelle le cycle d'inhibition est autorisé. La limite de temps peut être réglée entre 1 seconde et 30 minutes. Une différente limite de temps peut être réglée pour chaque entrée de sécurité à inhiber. Les autres dispositifs d'entrées de sécurité qui sont aussi inhibés ne sont affectés que par leur propre limite de temps d'inhibition. La limite de temps d'inhibition peut être désactivée. Si elle est désactivée, la limite de temps de la fonction d'inhibition de ce dispositif d'entrée de sécurité est infinie.

2.4.4.3 Fonction d'inhibition à la mise sous tension

⚠ AVERTISSEMENT

INHIBITION À LA MISE SOUS TENSION

LA FONCTION D'INHIBITION À LA MISE SOUS TENSION NE DOIT ÊTRE UTILISÉE QUE DANS LES APPLICATIONS SUIVANTES :

- L'INHIBITION DU SYSTÈME (M1 ET M2 FERMÉES) EST NÉCESSAIRE À LA MISE SOUS TENSION ET
- SON UTILISATION NE DOIT, EN AUCUN CAS, EXPOSER LE PERSONNEL À UN DANGER

Quand elle est configurée, la fonction d'inhibition à la mise sous tension initie un cycle d'inhibition dès que la tension est appliquée au contrôleur de sécurité SC22-3 à condition que les entrées de sécurité inhibées soient actives (état Run ou fermé) et que soit M1-M2, soit M3-M4, (mais pas les quatre à la fois) signalent une condition d'inhibition (par ex. état Run ou fermé) (voir **IMPORTANT** ci-dessus).

Inhibition à la mise sous tension

Quand l'option inhibition à la mise sous tension est activée, le contrôleur passe en cycle d'inhibition si les conditions d'un cycle d'inhibition sont satisfaites à la mise sous tension. Les conditions spécifiques pour un signal d'inhibition valide pour un cycle d'inhibition doivent être présentes pour être initiées et conservées.

Si une mise en service manuelle est configurée et que toutes les autres conditions sont satisfaites, le premier RAZ système après que les entrées de sécurité inhibées sont actives (état Run ou fermé) donne un cycle d'inhibition.

La fonction inhibition à la mise sous tension ne doit être utilisée que si la sécurité est assurée quand le cycle d'inhibition se présente et l'utilisation de cette fonction est le résultat d'une évaluation de risque et est demandée par le fonctionnement de cette machine particulière.

2.4.5 Fonction du bouton de Bypass

⚠ AVERTISSEMENTS

INTERRUPTEUR D'INHIBITION ET DE BYPASS

LES OPÉRATIONS D'INHIBITION ET DE BYPASS DOIVENT ÊTRE EFFECTUÉES DE FAÇON À MINIMISER LE RISQUE AU PERSONNEL. LES RÉGLES ET MÉTHODES SUIVANTES DOIVENT ÊTRE MISES EN ŒUVRE LORS DE LA CRÉATION D'APPLICATIONS D'INHIBITION ET DE BYPASS :

- SE PROTÉGER CONTRE UNE SUSPENSION NON VOULUE DU SIGNAL D'ARRÊT EN UTILISANT UNE OU PLUSIEURS PAIRES DE CAPTEUR D'INHIBITION REDONDANTES OU UN INTERRUPTEUR DE BYPASS À CLÉ À DOUBLE CANAL
- RÉGLER DES LIMITES DE TEMPS DE LA FONCTION D'INHIBITION ET DE BYPASS RAISONNABLES (PAS PLUS LONGUES QUE NÉCESSAIRE)

UTILISATION DES FONCTIONS DE L'INTERRUPTEUR D'INHIBITION ET DE BYPASS

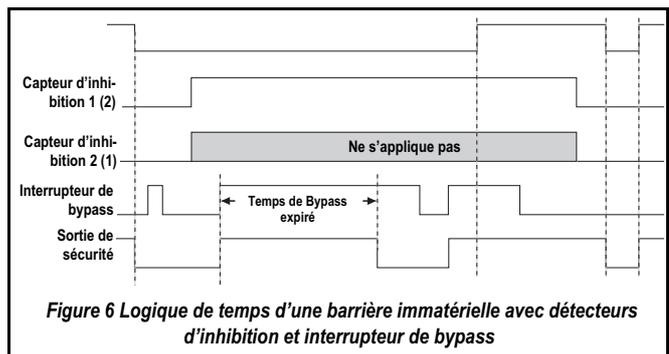
NE PAS RESPECTER CES RÉGLES PEUT ENTRAÎNER UNE SITUATION NON SÛRE QUI PEUT PROVOQUER DES BLESSURES GRAVES, VOIRE MORTELLES. SE RÉFÉRER À [Annexe A2.10 en page 111](#) ET À [Annexe A2.11 en page 113](#) POUR PLUS D'INFORMATIONS.

Le dispositif de sécurité interrupteur de bypass est une suspension temporaire activée manuellement d'un ou plusieurs signaux d'arrêt pour les entrées de sécurité quand il n'y a pas de risque immédiat. Les interrupteurs de bypass peuvent être assignés à une ou plusieurs entrées de sécurité suivantes :

- Interrupteurs pour porte (verrouillage)
- Dispositifs de commande bimanuelle
- Détecteurs optiques
- Tapis de sécurité

Quand le signal de l'interrupteur de bypass change vers l'état de bypass (Run), il fait passer sur ON ou rester sur ON toutes les sorties de sécurité qui sont contrôlées par les entrées de sécurité bypassées seulement si tous les autres dispositifs d'entrée de sécurité non bypassés assignés à ces sorties de sécurité sont en état Run (voir [Figure 6 en page 10](#)).

Pour obtenir plus d'informations concernant la fonction de l'interrupteur de bypass, voir [Annexe A2.10 en page 111](#).



2.4.5.1 Limite de temps de l'interrupteur de bypass.

Une limite de temps de la fonction de l'interrupteur de bypass peut être établie tant que le bypass de l'entrée de sécurité est actif. La limite de temps peut être réglée entre 1 seconde et 30 minutes et ne peut être désactivée. Une seule limite de temps peut être définie et cette limite s'applique à tous les dispositifs d'entrées de sécurité qui sont bypassés. À la fin de la limite de temps, l'autorité de la commande de la sortie de sécurité repasse aux entrées de sécurité bypassées.

2.4.5.2 Bypass avec inhibition.

Si un détecteur inhibé est assigné à une entrée de sécurité et que l'entrée de sécurité est en état d'arrêt, au moins un des détecteurs inhibés doit être dans l'état inhibé (Run) pour commencer un nouveau cycle bypassé. Si les conditions sont remplies pour le bypass, l'indicateur de sortie de l'état inhibé (s'il est configuré) commence à clignoter à 1 Hz.

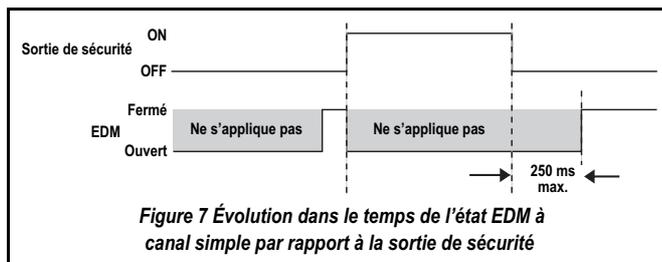
2.4.6 EDM

Pour plus d'informations, voir aussi [Paragraphe 1.18 en page 6](#) et [Paragraphe 4.8.1 en page 34](#).

2.4.6.1 Surveillance simple voie

Pour les informations sur le minutage, voir la [Figure 7 en page 11](#).

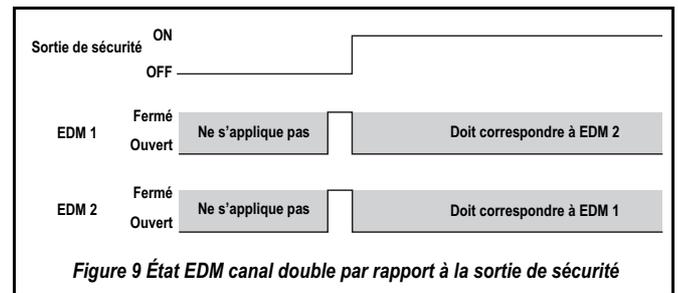
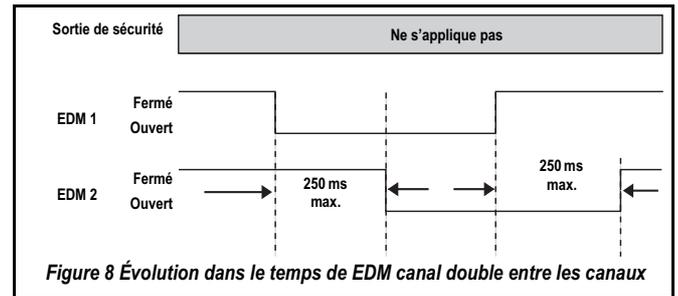
Un raccordement en série de contacts de surveillance fermés qui sont guidés en force (reliés mécaniquement) de chaque dispositif contrôlé par le contrôleur de sécurité. Les contacts de surveillance doivent être fermés avant que les sorties du contrôleur de sécurité puisse être RAZ système (manuellement ou automatiquement). Après qu'un RAZ système soit exécuté et qu'une sortie de sécurité (OSSD) passe sur ON, l'état des contacts de surveillance ne sont plus surveillés et peuvent changer d'état. Cependant, les contacts de surveillance doivent être fermés dans l'intervalle de temps de 250 ms à partir du moment où les OSSD sorties passent de ON à OFF.



2.4.6.2 Surveillance double voies

Pour les informations sur le minutage, voir la [Figure 8 en page 11](#) et la [Figure 9 en page 11](#).

Raccordement indépendant de contacts fermés surveillés, à guidage forcé (liés mécaniquement) depuis chaque dispositif contrôlé par le contrôleur de sécurité. Les deux entrées EDM doivent être fermées avant de pouvoir réarmer le contrôleur de sécurité et faire passer sur ON les OSSD. Lorsque les OSSD sont ON, les entrées peuvent changer d'état (ouvertes toutes les deux ou fermées toutes les deux). Si les entrées restent dans des états opposés pendant plus de 250 ms, un blocage se produit.



2.5 CONFIGURATION DU CONTRÔLEUR DE SÉCURITÉ

La configuration du contrôleur de sécurité peut s'effectuer au moyen d'une des deux interfaces :

- Boutons et affichage de OBI sur le contrôleur lui-même
- ou

- Logiciel PCI (inclus dans le CD livré, réf. 134534)

La procédure comprend trois étapes principales :

Définition de l'application de protection (évaluation des risques)

- Détermination des dispositifs nécessaires
- Détermination du niveau de sécurité nécessaire

Construction de la configuration

- Sélection des types d'entrée de sécurité et des connexions des circuits
- Assignation de chaque entrée de sécurité et entrée auxiliaire à une ou plusieurs sorties de sécurité ou à d'autres dispositifs d'entrée de sécurité ou d'entrée auxiliaire
- Réglage des temporisations ON ou OFF des sorties de sécurité
- Sélection des types d'entrées auxiliaires et des connexions des circuits, le cas échéant
- Assignation des signaux de sortie d'états, le cas échéant
- Création du nom de la configuration, du nom de fichier, de la date, du nom de l'auteur et des remarques

Confirmation de la configuration

- Vérification par le contrôleur de sécurité que la configuration choisie est valide
- Confirmation par l'utilisateur que la configuration est bien celle voulue

2.5.1 Sorties de sécurité



AVERTISSEMENTS

INTERFACE OSSD

POUR QUE LE CONTRÔLEUR DE SÉCURITÉ FONCTIONNE CORRECTEMENT, SES PARAMÈTRES DE SORTIE ET CEUX D'ENTRÉE DE LA MACHINE DOIVENT ÊTRE PRIS EN CONSIDÉRATION AU MOMENT DE LA CRÉATION DE L'INTERFACE DES SORTIES TRANSISTORISÉES DE SÉCURITÉ VERS LES ENTRÉES DE LA MACHINE. LES CIRCUITS DE CONTRÔLE DE LA MACHINE DOIVENT ÊTRE CONÇUS DE LA FAÇON SUIVANTE :

- LA VALEUR DE RÉSISTANCE MAXIMALE DU CÂBLE ENTRE LES SORTIES DE SÉCURITÉ TRANSISTORISÉES DU CONTRÔLEUR DE SÉCURITÉ ET LES ENTRÉES DE LA MACHINE N'EST PAS DÉPASSÉE.
 - LA TENSION D'ÉTAT OFF MAXIMUM DE LA SORTIE DE SÉCURITÉ TRANSISTORISÉE DU CONTRÔLEUR DE SÉCURITÉ N'ENTRAÎNE PAS DE CONDITION ON ET
 - 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.
- UNE DÉFAILLANCE DANS L'INTERFACE DES SORTIES DE SÉCURITÉ VERS LA MACHINE PROTÉGÉE PEUT ENTRAÎNER DES BLESSURES GRAVES, VOIRE MORTELLES.

INTERFACE DES DEUX OSSD

LES DEUX SORTIES DES DISPOSITIFS DE COMMUTATION DES SIGNAUX DE SORTIE (OSSD) DOIVENT ÊTRE RACCORDÉES À LA COMMANDE DE LA MACHINE DE SORTE QUE LE SYSTÈME DE COMMANDE DE LA SÉCURITÉ DE LA MACHINE INTERROMPE LE CIRCUIT DES ÉLÉMENTS PRINCIPAUX DE COMMANDE, AFIN D'ÉVITER UNE SITUATION DANGEREUSE. NE JAMAIS RACCORDER UN DISPOSITIF INTERMÉDIAIRE (PAR EX. PLC, PES OU PC) QUI PERMETTE DE SUSPENDRE, DE PASSER OUTRE OU DE FAIRE ÉCHOUER LA FONCTION DE SÉCURITÉ SAUF SI CELA APPORTE UN NIVEAU DE SÉCURITÉ ÉQUIVALENT OU SUPÉRIEUR.

UTILISATION DE SUPPRESSEURS D'ARCS

IL EST RECOMMANDÉ D'UTILISER DES SUPPRESSEURS D'ARCS. ILS DOIVENT ÊTRE INSTALLÉS SUR LES BOBINES DES FDS. NE JAMAIS INSTALLER DE SUPPRESSEURS D'ARCS DIRECTEMENT SUR LES BORNES DES FSD. IL EST POSSIBLE QU'ILS CRÉENT UN COURT-CIRCUIT. S'IL EST INSTALLÉ DIRECTEMENT SUR LES CONTACTS DU FSD, UN SUPPRESSEUR EN COURT-CIRCUIT CRÉE UNE SITUATION DANGEREUSE.

RÉSISTANCE DES FILS DE LA SORTIE DE SÉCURITÉ

POUR QU'ELLE FONCTIONNE CORRECTEMENT, LA RÉSISTANCE DES FILS D'UNE SORTIE DE SÉCURITÉ NE DOIT PAS EXCÉDER 10 OHMS. UNE RÉSISTANCE SUPÉRIEURE À 10 OHMS PEUT MASQUER UN COURT-CIRCUIT ENTRE LES SORTIES DE SÉCURITÉ D'UN CANAL DOUBLE ET CRÉER UNE SITUATION NON SÛRE QUI PEUT PROVOQUER DES BLESSURES GRAVES, VOIRE MORTELLES.

CONNEXION DES CONTRÔLEURS DE SÉCURITÉ EN SÉRIE

LA SORTIE DE SÉCURITÉ D'UN CONTRÔLEUR DE SÉCURITÉ PEUT ÊTRE RACCORDÉE À L'ENTRÉE DE SÉCURITÉ D'UN SECOND CONTRÔLEUR DE SÉCURITÉ. CEPENDANT, LE SECOND CONTRÔLEUR DE SÉCURITÉ DOIT ÊTRE LE SEUL DISPOSITIF AUQUEL LA SORTIE DU PREMIER CONTRÔLEUR DE SÉCURITÉ EST RACCORDÉE. SI UN TROISIÈME DISPOSITIF EST AUSSI RACCORDÉ À LA MÊME SORTIE DE SÉCURITÉ (UTILISÉE MAINTENANT EN TANT QU'ENTRÉE DE SÉCURITÉ DU SECOND CONTRÔLEUR DE SÉCURITÉ), PENDANT UNE TRANSITION DE PUISSANCE DU SECOND CONTRÔLEUR DE SÉCURITÉ, L'ENTRÉE PEUT ÊTRE LA SOURCE MOMENTANÉE D'UN COURANT QUI CRÉE UN FAUX SIGNAL ON (RUN) À L'ENTRÉE DU TROISIÈME DISPOSITIF. NE PAS RACCORDER PLUSIEURS CONTRÔLEUR DE SÉCURITÉS CORRECTEMENT PEUT CRÉER UNE SITUATION NON SÛRE QUI PEUT ENTRAÎNER DES BLESSURES GRAVES, VOIRE MORTELLES

CÂBLAGE

LE SCHÉMA DE CÂBLAGE GÉNÉRAL ILLUSTRÉ SERT UNIQUEMENT À DÉMONSTRER L'IMPORTANCE D'UNE INSTALLATION CORRECTE. LE RACCORDEMENT DU CONTRÔLEUR DE SÉCURITÉ À UNE MACHINE DÉTERMINÉE EST SOUS L'ENTIÈRE RESPONSABILITÉ DE L'INSTALLATEUR ET DE L'UTILISATEUR FINAL.

**PRECAUTIONS****RETARD AU DÉCLENCHEMENT**

Le temps de retard au déclenchement d'une sortie de sécurité sera honoré même si l'entrée de sécurité qui a déclenché le minuteur de retard rebasculé en état Run avant que le temps du retard ait expiré.

Cependant, en cas de panne d'alimentation, le temps du retard au déclenchement peut se terminer immédiatement. Si une telle situation d'arrêt immédiat de la machine peut créer un danger potentiel, il faut prendre des mesures de protection supplémentaires pour éviter les blessures.

REMARQUE : LES sorties de sécurité SO1, SO2 ET SO3 SONT DES sorties À canal double

Une sortie de sécurité individuelle (par ex. SO1) n'est pas capable, en elle-même, de répondre aux applications de catégorie 4 (selon ISO13849-1). Quand l'évaluation des risques ou les règlements applicables nécessitent un haut niveau d'intégrité de sécurité

(Par ex. catégorie 4), les deux sorties OSSD doivent être raccordées à la commande de la machine pour que celle-ci puisse interrompre le circuit ou l'alimentation aux MPCE, pour créer une situation non dangereuse.

Ceci est normalement effectué par les dispositifs de commutation finaux (FSD) quand les OSSD passent à l'état OFF. (Voir Figure 28 en page 85 à Figure 31 en page 87).

Les sorties de sécurité (voir Figure 11 en page 14) sont conçues pour commander les dispositifs finaux d'interruption (FSD) et les MPCE qui sont les derniers de la chaîne de commande à contrôler le déplacement dangereux. Ces éléments de commande comprennent des relais, des contacteurs, des solénoïdes, des commandes de moteurs et autres dispositifs incorporant des contacts de surveillance guidés en force (reliés mécaniquement) ou des signaux de commande fiables dont les surveillances de dispositifs externes ont besoin.

Le contrôleur de sécurité a trois sorties de sécurité transistorisées, commandées indépendamment et redondantes, chacune état capable de fournir 750 mA. L'algorithme d'auto vérification du contrôleur de sécurité s'assure que les sorties passent sur ON et sur OFF au bon moment, en réponse aux signaux d'entrée assignés et aux signaux de test du système auto vérification

Les sorties de sécurité, SO1, SO2 et SO3, peuvent être commandées par les dispositifs d'entrée de sécurité qui disposent d'un réarmement automatique comme d'un réarmement manuel.

Le contrôleur de sécurité SC22-3 a trois paires de sorties de sécurité transistorisées (SO1 a et b, SO2 a et b et SO3 a et b). Chaque paire consiste en deux OSSD (voir Figure 14 en page 21). Les sorties de sécurité transistorisées sont surveillées activement pour détecter les courts-circuits de la tension d'alimentation, entre eux et vers d'autres sources d'énergie électrique. Si une défaillance est constatée, les sorties basculent en état OFF. Pour les circuits qui ont besoin du plus haut niveau de sécurité et de fiabilité, chaque OSSD doit être capable d'arrêter le mouvement de la machine protégée par une sortie de sécurité, en cas d'urgence.

2.5.1.1 Arrêts fonctionnels selon IEC 60204-1

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

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

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

2.5.1.2 Raccordement des sorties OSSD

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

Les FSD accomplissent normalement cela quand les sorties de sécurité passent en état OFF. Voir Figure 14 en page 21.

Se référer aux spécifications des sorties (Tableau 4 en Page 21) et **IMPORTANT** ci-dessus à gauche avant de raccorder OSSD et d'interfacer le contrôleur de sécurité à la machine.

2.5.1.3 Retard à l'enclenchement et au déclenchement des sorties de sécurité

AVERTISSEMENT

MISE EN MARCHÉ OU ARRÊT D'UNE TEMPORISATION

SI UNE ENTRÉE ASSIGNÉE À UNE SORTIE DE SÉCURITÉ IMMÉDIATE EST AUSSI ASSIGNÉE À UNE SORTIE DE SÉCURITÉ TEMPORISÉE S'OUVRE PUIS SE REFERME AVANT QUE LA TEMPORISATION AIT EXPIRÉE, LA SORTIE DE SÉCURITÉ IMMÉDIATE PASSE SUR OFF ET RESTE SUR OFF PENDANT QUE LA TEMPORISATION COURT. À LA FIN DE LA TEMPORISATION, LA SORTIE RETARDÉE PASSE AUSSI SUR OFF. LES DEUX SORTIES RESTENT SUR OFF PENDANT ENVIRON 500 MS, AVANT DE REVENIR SUR ON. CECI SE PRODUIT AUTOMATIQUEMENT, SI LA CONFIGURATION PRÉVOIT UN RÉARMEMENT AUTOMATIQUE, OU APRÈS UN SIGNAL DE RÉARMEMENT MANUEL VALIDE, SI LA CONFIGURATION PRÉVOIT UN RÉARMEMENT MANUEL.

Chaque sortie de sécurité peut être configurée pour fonctionner avec un retard à l'enclenchement ou au déclenchement (voir Figure 11 en page 14), dans laquelle la sortie passe sur ON ou sur OFF seulement après que la limite de temps se soit écoulée. Une sortie ne peut pas avoir un retard à l'enclenchement et au déclenchement en même temps. La durée du retard à l'enclenchement comme au déclenchement est de 100 ms à 5 minutes, par incréments de 100 ms.

Le fonctionnement en cours est d'utiliser le retard au déclenchement pour les erreurs internes et système, chaque fois que cela est possible.

Le retard à l'enclenchement de la sortie de sécurité est quelques fois utilisé quand le fonctionnement d'une machine doit être retardé avant d'autoriser un démarrage de la machine en toute sécurité. Un exemple serait une cellule de soudage robotisée. Voir [Paragraphe 2.5.1 en page 12](#) pour plus d'informations.

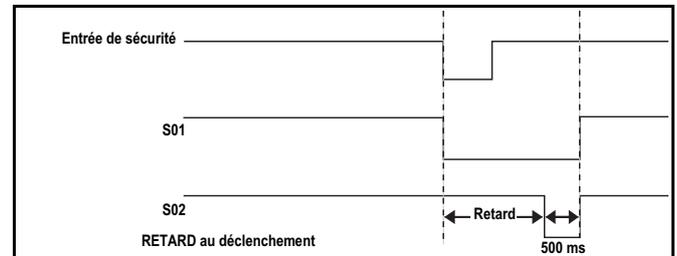


Figure 10 Logique de temps de la sortie de sécurité avec temporisation OFF

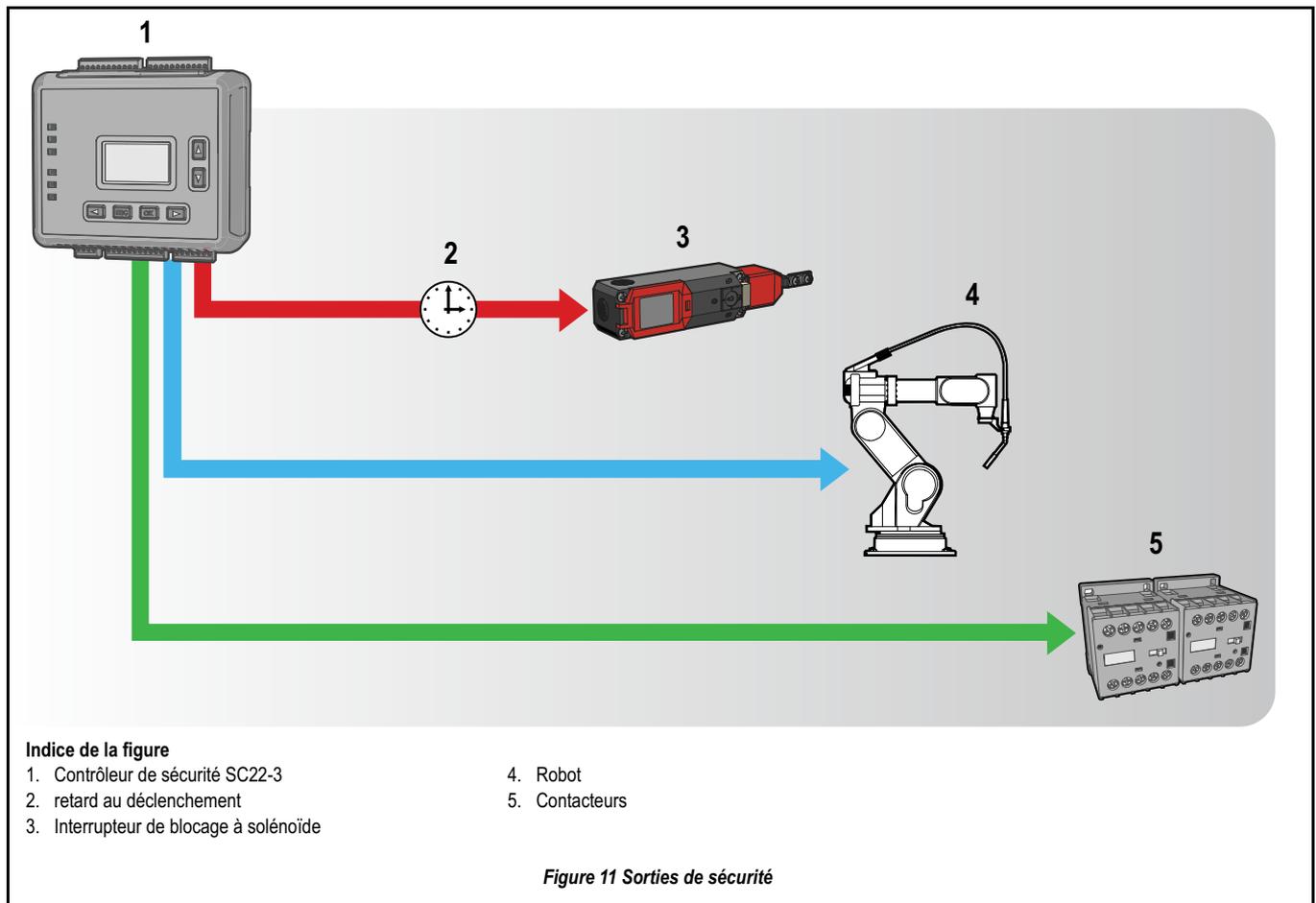


Figure 11 Sorties de sécurité

2.5.2 Sorties d'état

AVERTISSEMENT

SORTIES D'ÉTAT

LES SORTIES D'ÉTAT NE SONT PAS DES SORTIES DE SÉCURITÉ ET PEUVENT ÊTRE DÉFAILLANTES EN ÉTAT ON OU EN ÉTAT OFF. ELLES NE DOIVENT PAS ÊTRE UTILISÉES POUR COMMANDER DES APPLICATIONS CRITIQUES POUR LA SÉCURITÉ. SI UNE SORTIE D'ÉTAT EST UTILISÉE POUR COMMANDER UNE APPLICATION CRITIQUE POUR LA SÉCURITÉ, UNE DÉFAILLANCE EST POSSIBLE QUI PEUT ENTRAÎNER DES BLESSURES GRAVES, VOIRE MORTELLES.

Le contrôleur de sécurité a dix sorties d'état configurables qui servent à :

- Envoyer des signaux d'état auxiliaires aux PLC

ou

- Vers les HMI (interfaces homme machine)

ou

- Elles peuvent servir à alimenter des voyants

Ces sorties peuvent être configurées pour signaler l'état de dispositifs d'entrée de sécurité ou d'entrées auxiliaires, des sorties de sécurité ou du contrôleur lui-même. Voir [Paragraphe 4.9 en page 35](#) pour plus d'informations.

Convention du signal

La convention du signal de sortie d'état peut être configurée pour être 24 Vcc ou 0 Vcc pour indiquer que :

- Une entrée est dans l'état Run
- Une sortie de sécurité est dans l'état ON (voir [Remarque * en page 15](#))
- Le système est en Blocage
- Une erreur d'E/S est présente (voir [Remarque en page 15](#))
- Un réarmement système est nécessaire
- Une sortie de sécurité nécessite un réarmement (voir [Remarque en page 15](#))
- Une entrée de sécurité est inhibée
- Une Sorties de sécurité est ON ou DÉLAI À L'ENCLenchement (le statut logique)

- ☛ *Seules les sorties de sécurité dont les entrées leur sont assignées peuvent être assignées à une sortie d'état.*

Une erreur d'E/S est une défaillance d'une ou plusieurs entrées de sécurité, sorties de sécurité ou sorties d'état.

Seules les sorties de sécurité assignées aux entrées configurées avec une logique de réarmement manuel peuvent avoir une sortie d'état configurée pour indiquer qu'un réarmement est nécessaire.

2.5.2.1 Sorties d'état de lampe d'inhibition

Les sorties d'état **O9** et **O10** peuvent être configurées pour créer une fonction d'état de lampe d'inhibition pour une opération d'inhibition. Quand la lampe d'inhibition est ON, le contrôleur recherche un court-circuit dans la charge. Quand la lampe est OFF, le contrôleur recherche une coupure de circuit dans la charge. Si une coupure de circuit se produit avant le départ d'un cycle d'inhibition, le cycle d'inhibition suivant sera interdit. Si une coupure de circuit se produit pendant un cycle d'inhibition, ce cycle d'inhibition se termine, mais le cycle d'inhibition suivant sera interdit. Si un court-circuit se produit avant ou pendant une inhibition, ce cycle d'inhibition commencera et se terminera, mais le cycle d'inhibition suivant sera interdit. Si elles ne servent pas à surveiller une lampe d'inhibition, ces sorties peuvent être utilisées de la même façon que les sorties O1–O8.

IMPORTANT : Seuls les bornes **O9** et **O10** disposent du circuit supplémentaire de surveillance nécessaire pour surveiller une lampe d'inhibition. Si le monitoring d'une lampe d'inhibition n'est pas nécessaire (en fonction des normes applicables), n'importe quelle sortie d'état (O1–O10) peut être utilisée pour indiquer une condition d'inhibition.

- ☛ *À cause de cette caractéristique, ces sorties d'état apparaissent toujours ON sans charge (voir les spécifications, [Paragraphe 3.2.1 en page 21](#)).*

2.5.3 Assignment des E/S et relation de commande des E/S

Le terme **Assignment** implique une relation de logique de commande entre une entrée et une sortie ou entre une entrée et une autre entrée, quand l'état de la première entrée détermine l'état de la sortie ou de la seconde entrée (voir [Figure 12 en page 16](#)).

2.5.3.1 Entrées de sécurité et entrées auxiliaires assignées aux sorties

Les dispositifs suivants peuvent être assignés directement à une sortie de sécurité :

- Boutons d'arrêt d'urgence
- Interrupteurs de sécurité
- Détecteurs optiques
- Dispositifs de commande bimanuelle
- Tapis de sécurité
- Interrupteurs d'arrêt de protection
- Interrupteurs par câble
- Dispositifs d'activation
- Surveillance des commutateurs externes
- MARCHE/ARRET

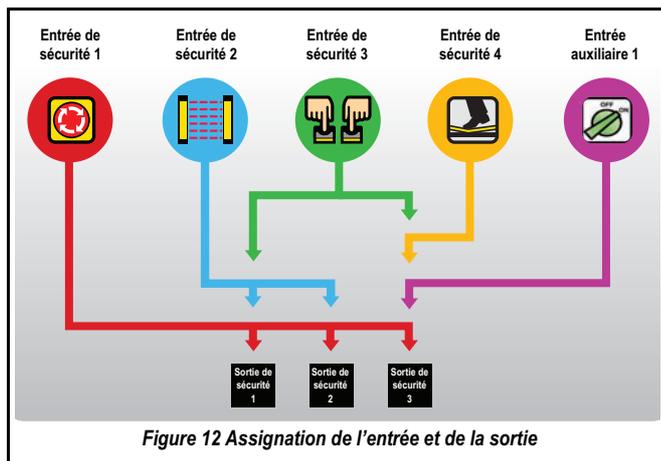


Figure 12 Assignment de l'entrée et de la sortie

2.5.3.2 Entrées assignées à des entrées

Les capteurs d'inhibition et les boutons de shuntage fonctionnent en conjonction avec certaines entrées de sécurité pour suspendre temporairement le signal d'arrêt d'une entrée de sécurité. Ces capteurs et boutons sont assignés directement aux entrées de sécurité ; ils sont indirectement assignés à la sortie de sécurité que les entrées de sécurité commandent (voir [Paragraphe 1.11 en page 5](#)).

2.6 PARAMÈTRES SYSTÈME

⚠ PRECAUTIONS

MISE SOUS TENSION AUTOMATIQUE

Quand le contrôleur est configuré en mode de réarmement automatique du système à la mise sous tension, le contrôleur agit comme si tous les dispositifs d'entrée sont configurés sur réarmement Auto. Chaque sortie de sécurité passe sur ON immédiatement à la mise sous tension à condition que tous les dispositifs d'entrée assignés soient en état Run, même si un ou plusieurs dispositifs d'entrée sont configurés pour un réarmement manuel. Si l'application nécessite qu'un réarmement manuel soit effectué avant que la sortie de sécurité passe sur ON, alors il faut utiliser la configuration soit du mode manuel soit du mode normal de mise sous tension. Ne pas s'y conformer peut faire que la machine fonctionne d'une façon inattendue à la mise sous tension ou après une interruption temporaire d'alimentation électrique.

FONCTIONNEMENT DU CONTRÔLEUR À LA MISE SOUS TENSION

Il est de la responsabilité de la personne qui configure, installe et entretient le contrôleur d'évaluer que les dispositifs et les méthodes de protection sont appropriés à une machine ou une application particulière et d'être conscient que le comportement du contrôleur à la mise sous tension n'est pas forcément évident pour l'opérateur de la machine.

Les paramètres système du contrôleur définissent les paramètres du fichier de configuration ainsi que du contrôleur. Ces paramètres sont les suivants :

- Nom de la configuration
- Nom de l'auteur
- Mode à la mise sous tension
- Inhibition à la mise sous tension activée
- Réarmement surveillé

2.6.1 Décomposition des paramètres

2.6.1.1 Nom de la configuration

Le nom de la configuration identifie la configuration qui sera utilisée dans une application du contrôleur de sécurité. Le nom de la configuration peut être affiché sur le contrôleur, ce qui est pratique pour s'assurer que la configuration d'un contrôleur est la bonne.

2.6.1.2 Nom de l'auteur

Le nom de l'auteur peut aussi être utile quand des questions se posent à propos des paramètres de configuration.

2.6.1.3 Mode à la mise sous tension

Utilisé pour les caractéristiques opérationnelles à la mise sous tension

Le contrôleur dispose de trois modes à la mise sous tension au choix qui déterminent la façon dont le contrôleur se comportera immédiatement à la mise sous tension. Ces modes à la mise sous tension sont : Normal, automatique et manuel.

À la mise sous tension, si le mode Normal est utilisé (par défaut) :

- Seulement les sorties de sécurité qui n'ont que des entrées à réarmements automatiques passent sur ON
- Les sorties de sécurité qui ont une ou plusieurs entrées à réarmement manuel passent sur ON seulement quand une opération de réarmement (verrouillé) manuel est effectuée
- Exception : **Les entrées** des commandes bimanuelles, les entrées de shuntage et les entrées du dispositif d'activation doivent être à l'état d'arrêt à la mise sous tension, quelle que soit la sélection du mode de mise sous tension. Si elles sont en état Run à la mise sous tension, les sorties restent sur OFF

À la mise sous tension, si le mode automatique est utilisé :

- Toutes les sorties de sécurité passent immédiatement sur ON si les entrées qui sont assignées à ces sorties sont toutes en l'état Run
Exception: Les entrées des commandes bimanuelles, les entrées de shuntage et les entrées du dispositif d'activation doivent être à l'état d'arrêt à la mise sous tension, quelle que soit la sélection du mode de mise sous tension. Si elles sont en état Run à la mise sous tension, les sorties restent sur OFF

À la mise sous tension, si le mode manuel est utilisé :

- Les sorties de sécurité passent sur ON seulement si toutes les entrées assignées à cette sortie sont en état Run et un réarmement système a été effectué (un réarmement pour un verrouillage manuel n'est pas nécessaire)
Exception: Les entrées des commandes bimanuelles, les entrées de shuntage et les entrées du dispositif d'activation doivent être à l'état d'arrêt à la mise sous tension, quelle que soit la sélection du mode de mise sous tension. Si elles sont en état Run à la mise sous tension, les sorties restent sur OFF

2.6.2 Inhibition à la mise sous tension

Si elle est configurée, la fonction d'inhibition à la mise sous tension initie un cycle d'inhibition quand la tension est appliquée au contrôleur de sécurité SC22-3 si les entrées de sécurité inhibées sont actives (Run ou fermées) et soit M1-M2 soit M3-M4 (mais pas tous les quatre à la fois) signalent une condition d'inhibition (par ex. active ou fermée). Voir aussi [Paragraphe 1.11 en page 5](#).

2.6.3 Réarmement surveillé

Un réarmement système surveillé est activé par défaut et nécessite un signal OFF-ON-OFF à l'entrée du réarmement système, dans lequel la durée du ON doit se situer entre 0,3 s et 2 s (réarmement système de bord de fuite), pour réarmer le système.

S'il n'est pas sélectionné (réarmement système surveillé désactivé), l'entrée du réarmement système ne nécessite qu'un signal OFF à ON (réarmement système de bord d'attaque), pour réarmer le système.

2.7 LOGIQUE INTERNE

Voir aussi [Paragraphe 2.4.1 en page 8](#).

2.7.1 Autres fonctions logiques

Les autres fonctions logiques sont des variations légères de la règle logique générale AND comme suit :

- **Commande bimanuelle** Le signal d'initiation de la machine incorporant une activation à 0,5 seconde une limite de simultanéité et une logique anti fixation permanente, conçue pour éviter le fonctionnement de la machine par une activation unique
- **Dispositif de sécurité inhibition activée** La suspension d'une ou plusieurs entrées de sécurité pour les signaux d'arrêt pendant une partie du fonctionnement de la machine quand il n'y a pas de danger ou quand l'accès au danger est protégé autrement
- **Dispositif de sécurité bouton de shuntage** La suspension temporaire, actionnée manuellement, d'une ou plusieurs entrées de sécurité pour les signaux d'arrêt quand le danger est protégé autrement

- **Commande du dispositif d'activation** La suspension manuelle activement contrôlée d'un signal d'arrêt pendant une partie du fonctionnement de la machine quand un danger peut être présent

Les règles qui s'appliquent à ces cas spéciaux sont expliquées en [Annexe A2](#).

2.8 VUE GÉNÉRALE DU MOT DE PASSE

Par mesure de sécurité, le contrôleur de sécurité nécessite l'utilisation d'un mot de passe dans certains cas. Les informations permettant de changer le mot de passe du contrôleur de sécurité se trouvent au [Paragraphe 5.1.18 en page 50](#) (PCI) et au [Paragraphe 6.3.3 en page 66](#) (OBI).

☛ *Si le mot de passe est perdu, contacter [Bureaux du siège social en page 125](#).*

Pour créer une configuration :

- Par l'intermédiaire du PC utilisant le programme SC22-3 PCI (pas besoin de mot de passe)
- Par l'intermédiaire de OBI du contrôleur de sécurité protégé par mot de passe

Confirmer une configuration :

- Par l'intermédiaire de PCI protégé par mot de passe, en utilisant le PC raccordé au contrôleur sous tension
- Par l'intermédiaire de OBI protégé par mot de masse sur un Contrôleur sous tension

Envoi d'une configuration confirmée au contrôleur de sécurité :

- Par l'intermédiaire d'une connexion directe entre le PC et le contrôleur, en utilisant le câble SC-USB1 et le PCI protégé par mot de passe
- Par l'intermédiaire de PCI PC, l'outil de programmation de la carte XM et la carte XM

2.9 CONFIRMATION D'UNE CONFIGURATION

Bien qu'un contrôleur de sécurité puisse accepter une configuration non confirmée, il ne l'activera (adoptera la configuration et fonctionnera selon ses paramètres) qu'après que la configuration soit confirmée, par l'intermédiaire de OBI.

IMPORTANT : Si une modification est introduite dans une configuration confirmée ou si une configuration est modifiée pendant la confirmation, le PCI et le OBI du contrôleur de sécurité reconnaîtra cette configuration modifiée comme une nouvelle et nécessitera qu'elle soit confirmée avant de pouvoir l'activer et l'utiliser.

Une fois confirmée, une configuration peut être sauvegardée et réutilisée sans reconfirmation. La code de confirmation sera validé automatiquement à chaque fois qu'elle est téléchargée vers un contrôleur de sécurité et chaque fois que le contrôleur de sécurité sera mis sous tension. Les configurations, confirmées ou non, peuvent être envoyées par mail. L'envoi (téléchargement) d'une nouvelle configuration confirmée à un contrôleur de sécurité nécessite l'entrée du mot de passe du contrôleur de sécurité.

2.10 VUE GÉNÉRALE DE L'INTERFACE PC

L'interface PC (PCI) est un programme informatique avec affichage en temps réel et outils de diagnostic qui peut servir à :

- Créer, confirmer, modifier, enregistrer, envoyer et recevoir une configuration
- Afficher les informations en temps réel en mode Run
- Enregistrer et afficher le registre d'erreurs

Le programme PCI utilise des icônes des dispositifs d'entrée et des symboles de circuit pour faciliter la sélection des bons dispositifs. Au fur et à mesure que les propriétés des différents dispositifs et les relations de commande des E/S sont établies, le programme construit automatiquement les diagrammes de raccordement et les diagrammes logiques Ladder. Ces schémas indiquent le détail de câblage des dispositifs d'E/S à l'installateur et une représentation symbolique de la logique de protection du contrôleur de sécurité que le concepteur de la machine et l'ingénieur de contrôle peuvent utiliser. Voir [Paragraphe 5.1 en page 37](#), pour avoir plus d'instructions sur l'utilisation de cette interface.

2.11 VUE GÉNÉRALE DE L'INTERFACE EMBARQUÉE

L'interface embarquée du contrôleur de sécurité SC22-3 (OBI) consiste en un affichage et six boutons qui servent à :

- Sélectionner une langue
- Créer, confirmer, modifier, effacer, envoyer et recevoir une configuration
- Afficher les informations en temps réel en mode Run
- Afficher les erreurs de données, le registre d'erreurs et à effacer le registre d'erreurs
- Afficher le numéro de modèle du contrôleur de sécurité
- Établir un mot de passe

La configuration est utilisée pour définir les dispositifs d'entrée qui seront connectés au contrôleur de sécurité et pour établir les relations entre les dispositifs d'entrée eux-mêmes aussi bien qu'entre les dispositifs d'entrée et les sorties.

[Figure 13 en Page 19](#) donne une décomposition de l'ensemble du mode Run et des options de mode de configuration disponibles en utilisant l'OBI.

Pour se déplacer dans les menus, dans la plupart des cas, il faut appuyer sur le bouton **OK** pour effectuer une sélection ou se déplacer plus loin dans l'arbre des menus. Le fait appuyer sur le bouton **ESC** fait remonter dans la hiérarchie des menus. Quand une liste d'options verticale apparaît à l'écran, les boutons des flèches vers le haut et vers le bas servent à surligner l'option sélectionnée. L'option surlignée est sélectionnée en appuyant sur **OK**. Quand une option unique apparaît à l'écran (par exemple, un dispositif d'entrée) avec une flèche en travers du haut de l'écran, les boutons des flèches gauche et droite servent à passer d'une sélection à l'autre. L'option affichée à l'écran est sélectionnée quand on appuie sur **OK**.

Voir [Chapitre 6](#), pour d'autres instructions sur l'utilisation de cet interface.

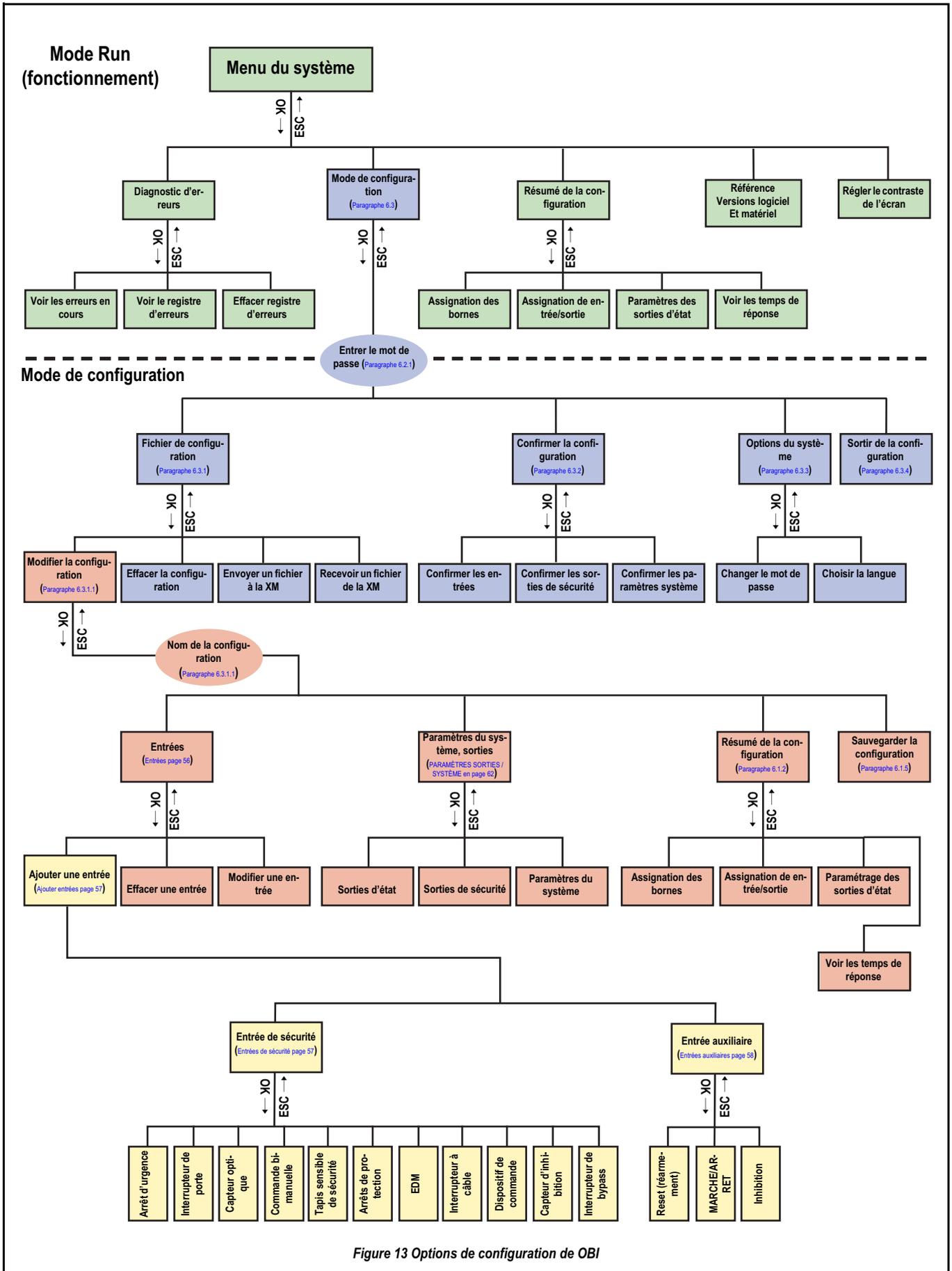


Figure 13 Options de configuration de OBI

Page blanche

3 INFORMATIONS GÉNÉRALES

Ce chapitre donne des informations générales sur cet équipement.

3.1 PRODUIT

Ce sous-chapitre donne des informations sur le produit comme les plaques d'identification CE et de produit et leur emplacement.

3.1.1 Marquage CE/plaque d'identification du produit

Les informations CE se trouvent avec celles d'identification comme le montre la [Figure 14 en page 21](#).

3.1.2 Certificat de conformité

Le manuel d'instructions du contrôleur de sécurité SC22-3 (réf. 135369 du 06.03.08) répond aux exigences de la: Directive machine 2006/42/EC, sécurité des machines, section 1.7.4 - Instructions.

3.1.3 Déclaration de conformité

Le Contrôleur de sécurité SC22-3 est livré avec une déclaration de conformité semblable à celle de la [Annexe A3.1 en page 119](#).

Cette déclaration certifie que le produit est conforme aux normes européennes.

3.2 FICHE TECHNIQUE

Ce sous-chapitre présente les principales données techniques du produit.

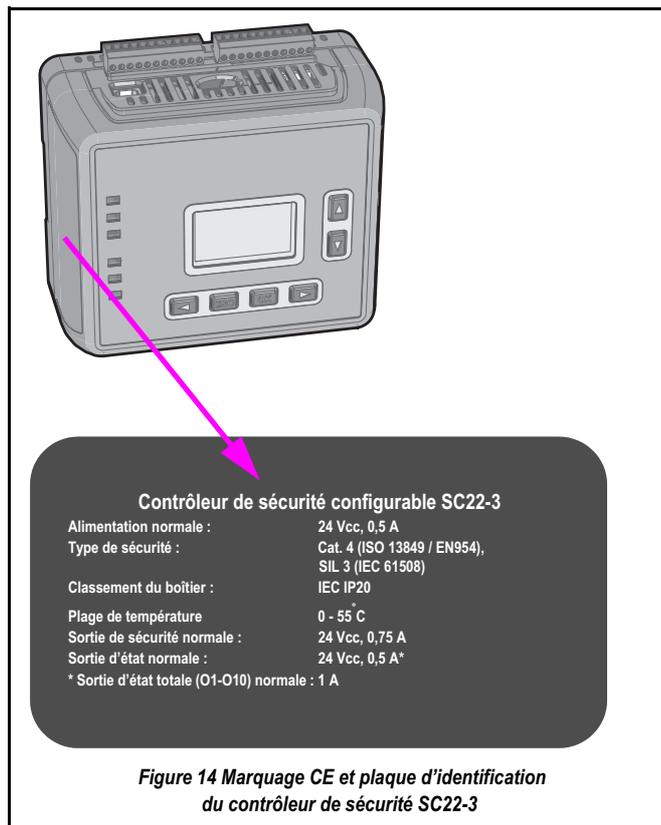


Figure 14 Marquage CE et plaque d'identification du contrôleur de sécurité SC22-3

3.2.1 Spécifications

[Tableau 4 en Page 21](#) présente les caractéristiques des Contrôleur de sécurité SC22-3.

Tableau 4 Contrôleur de sécurité SC22-3 Spécifications générales

| Nomenclature | Valeur/explication |
|---|--|
| Alimentation | 24 Vcc, ± 20% 0,4 A (Contrôleur de sécurité uniquement), 5,9 A (toutes les sorties ON à leur puissance maximale autorisée) Le contrôleur de sécurité ne doit être raccordé qu'à une alimentation SELV (« Safety Extra Low Voltage », pour les circuits électriques sans terre ou PELV (« Protected Extra Low Voltage », pour les circuits électriques avec la Terre) alimentation. |
| Entrée de sécurité et entrée auxiliaire (22 bornes) | Seuil d'entrée ON : > 15 Vcc (ON garanti), 30 Vcc max. Seuil d'entrée OFF : < 5 Vcc (OFF garanti avec n'importe quelle erreur), - 3 Vcc min. Intensité ON d'entrée : 8 mA normalement sous 24 Vcc, > 2 mA (garanti avec 1 erreur) Intensité de pointe de nettoyage de contact 50 mA sous 24 Vcc Intensité d'alimentation : 30 mA minimum continu (3 Vcc max. de chute) Résistance du fil d'entrée : 300 ohm max. (150 ohm par fil) |
| Sorties de sécurité (6 bornes, 3 sorties redondantes) | Intensité nominale de la sortie : 0,75 A max. sous 24 Vcc (1,0 Vcc max. de chute) Seuil de sortie OFF : 0,6 Vcc normal (1,2 Vcc max. garanti avec 1 erreur) 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 |
| Sorties d'état (10 bornes) | Intensité nominale de sortie : 0,5A sous 24 Vcc (individuellement), 1,0 A sous 24 Vcc (total de toutes les sorties) Tension OFF des sorties O1 à O8 (utilisation générale) : < 0,5 Vcc (à vide), 24 Vcc « pull down » à 0 V O9 et O10 (utilisation générale ou lampe d'inhibition surveillée) Tension OFF des sorties : 94 Kiloohms « pull up » à alimentation 24 Vcc Sortie ON / OFF seuil : 15 Vcc ± 4 Vcc sous alimentation 24 Vcc ☛ Pour O9 et O10, si un court-circuit ou une autre erreur fait que la sortie tombe en dessous de ce seuil alors que la sortie est ON, il se produit un blocage. Si une coupure de circuit ou une autre erreur fait que la sortie dépasse ce seuil alors que la sortie est OFF, il se produit un blocage. |

Tableau 4 Contrôleur de sécurité SC22-3 Spécifications générales

| Nomenclature | Valeur/explication | |
|---|---|--|
| Temps de réponse Et de réaction | Temps de réponse (ON vers OFF) : 10 ms max. (avec anti-anti-rebond normal de 6 ms ; il peut augmenter si le temps d'anti-anti-rebond augmente. Voir le résumé de la configuration pour avoir le temps de réponse réel. Temps de réaction (OFF vers ON) : 400 ms max. (avec l'option réarmement manuel) temps de réaction (OFF vers ON) : 400 ms max. plus temps d'anti-anti-rebond de l'entrée (réarmement automatique) | |
| Affichage embarqué sur LCD des informations — Utilisation du mot de passe | Le mot de passe n'est pas nécessaire : Mode Run (état des E/S) Erreur (détection d'erreur d'E/S et étapes de correction) Vérification des paramètres de configuration (propriétés et bornes des E/S) | Le mot de passe est nécessaire : Mode de configuration (configuration créer, modifier, confirmer, télécharger) |
| Indice de protection | IEC IP20, à utiliser dans une armoire de niveau IEC IP54 ou supérieur | |
| Environnement | Plage de température : 0° à +55° C | |
| Résistance mécanique | Chocs : 15 g pendant 11 ms, demi sinusoïde, 18 chocs au total (selon IEC 61131-2) Petits chocs répétés : 10 g pendant 16 ms, 6000 cycles au total (selon IEC 61496-1) Vibrations : 3,5 mm occasionnelle / 1,75 mm continue de 5 Hz à 9 Hz, 1,0 g occasionnelle et 0,5 g continue de 9 Hz à 150 Hz : (selon IEC 61131-2) et 0,35 mm d'amplitude unique / 0,70 mm de pic à pic de 10 Hz à 55 Hz (selon IEC 61496-1), tous sous 10 cycles de balayage par axe | |
| EMC | Répond ou dépasse toutes les exigences EMC de IEC 61131-2, IEC 61496-1 (Type 4), et IEC 62061 Annexe E, Tableau E.1 (niveaux d'immunité accrus) | |
| Bornier débrochable | Bornier à vis Dimension des fils : 0,20 mm ² – 1,31 mm ² Longueur de dénudement des fils : 5,00 mm Couple de serrage : 0,23 Nm nominal Couple de serrage : 0,34 Nm maximum auto vérification à pinces Dimension des fils : 0,20 mm ² – 1,31 mm ² Longueur de dénudement des fils : 9,00 mm IMPORTANT : Bornes à pinces ne sont conçues que pour 1 seul fil. Si on raccorde plus de 1 fil à une borne, un fil peut se desserrer ou se déconnecter de la borne, provoquant un court-circuit. | |
| Normes de performances du produit | <ul style="list-style-type: none"> • SIL 3 selon IEC 62061 Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et programmables liés à la sécurité • SIL 3 selon IEC 61508 Sécurité fonctionnelle des systèmes électriques, électroniques, programmables liés à la sécurité • Exigences de catégorie 4 de la norme européenne ISO 13849-1 (EN954-1) Sécurité des machines, Parties de systèmes de commande relatives à la sécurité • Niveau de performances (PL) selon ISO 13849-1 • IEC 61131-2 Contrôleurs programmables, Part 2 : Prescriptions et tests des équipements • IEC 60204-1 Équipement électrique des machines : Prescriptions générales • Norme européenne 954-1 Sécurité des machines. Parties de systèmes de commande relatives à la sécurité. Principes généraux de conception. • ISO 13851 (EN574) Sécurité des machines – Dispositifs de commande bimanuelle – Aspects fonctionnels – Principes de conception et d'aspect • ISO 13850 (EN418) Dispositifs d'arrêt d'urgence Voir aussi en DOC la liste des autres normes internationales applicables. | |
| Déclaration de conformité (DOC) |  | |

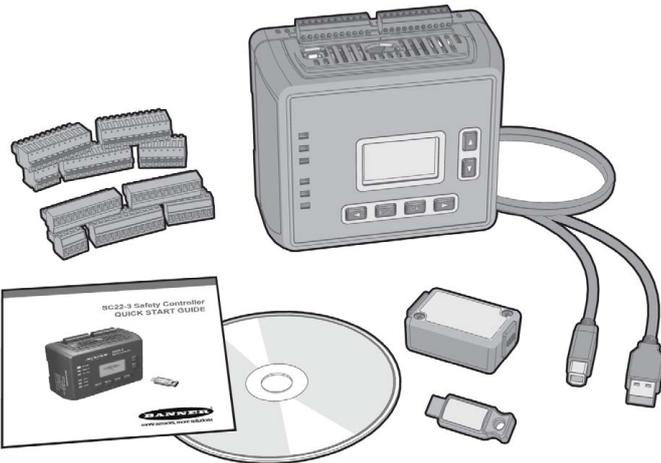
3.2.2 Type n°

Les documents suivants accompagnent le Contrôleur de sécurité SC22-3 (la référence de commande se trouve en [Tableau 5 en Page 23](#)) :

- Manuel européen d'instructions (ce document-ci ; pour une décomposition plus détaillée, voir [Paragraphe 8.4.2 en page 84](#))
- Guide de démarrage rapide (pour référence de commande, voir [Paragraphe 8.4.2 en page 84](#))

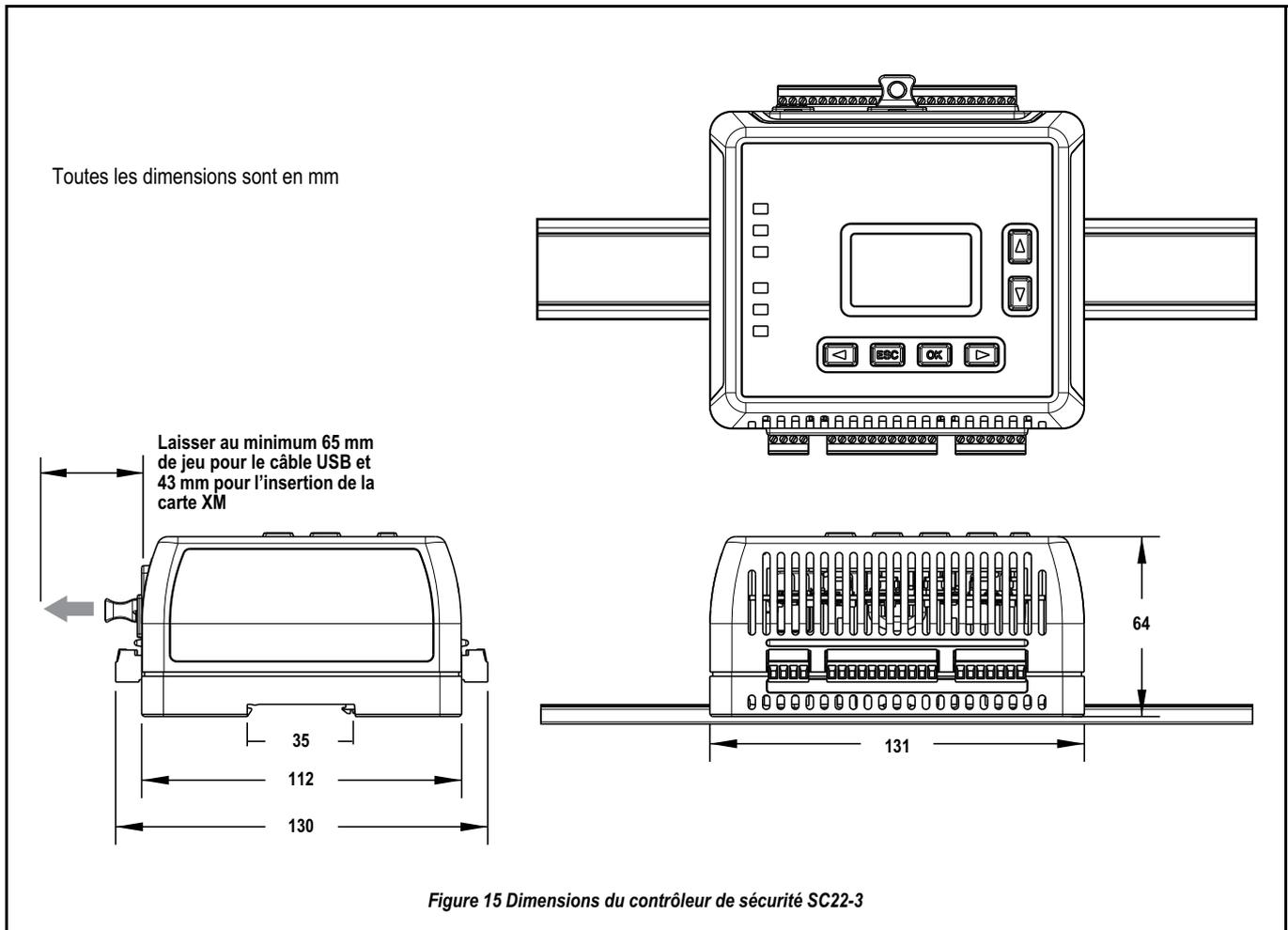
3.2.2.1 Modèle et type du contrôleur de sécurité SC22-3

Tableau 5 Contrôleur de sécurité SC22-3

| Modèle | Description | Référence de commande | Modèle |
|----------|-------------------------------|-----------------------|---|
| SC22-3-C | Contrôleur de sécurité en kit | 30 779 13 |  |
| SC22-3 | Contrôleur de sécurité seul | 30 797 15 |  |

3.2.3 Dimensions du contrôleur de sécurité SC22-3

Figure 15 en page 24 donne les dimensions du contrôleur de sécurité SC22-3.



3.3 INFORMATIONS DES CLIENTS

Les informations relatives au service client se trouvent en [Annexe A5](#) en page 125.

4 INSTALLATION - SYSTÈME

AVERTISSEMENT

AVANT D'INSTALLER LE CONTRÔLEUR DE SÉCURITÉ SC22-3, LIRE LES INFORMATIONS DE SÉCURITÉ DU Chapitre 1.

4.1 INTERFAÇAGE DU CONTRÔLEUR DE SÉCURITÉ SC22-3

l'interfaçage du contrôleur de sécurité SC22-3 dépend du type de machine et des protections qui doivent être interfacées avec le contrôleur. En général, le contrôleur est interfacé avec les protections qui sont utilisées sur des machines qui peuvent arrêter immédiatement leur mouvement à réception d'un signal d'arrêt en n'importe quel point du cycle machine. L'utilisateur a la responsabilité de vérifier si la protection correspond à l'application et est installée selon les instructions des manuels d'installation appropriés.

S'il existe un doute quant à la compatibilité d'une machine et de ce contrôleur, contacter [Bureaux du siège social en page 125](#).

4.2 COMPOSANTS

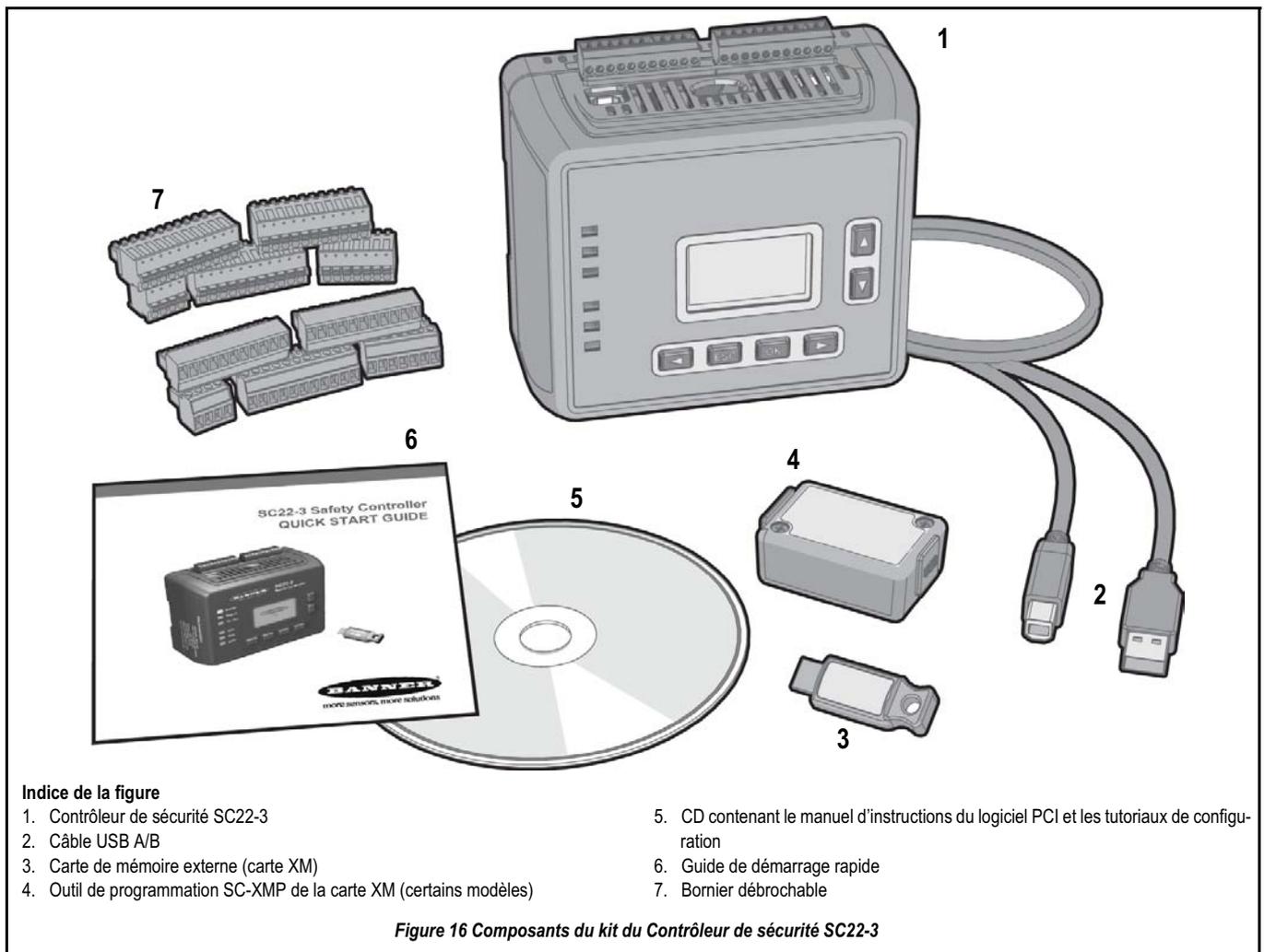
Le kit de démarrage du contrôleur de sécurité SC22-3 (voir au [Paragraphe 8.4.1 en page 82](#) une décomposition plus complète et la liste des pièces de rechange) comprend ce qui suit (voir [Figure 16 en page 25](#)):

- 1 Contrôleur de sécurité SC22-3
- 1 jeu de bornier débrochable (choisir entre bornier à vis ou à pince)
- 1 carte de mémoire externe SC-XM1 (carte XM)
- 1 câble USB A/B (certains modèles)
- 1 outil de programmation de la SC-XMP carte XM (certains modèles)
- 1 CD contenant le logiciel PCI, le manuel d'instructions et les tutoriaux de configuration (réf. 134534)
- 1 guide de démarrage rapide (réf. 133485)
- Manuel standard en anglais d'Amérique (réf. 133487)*
- Kit en langues européennes **



* Veuillez noter que le manuel (133487) n'est PAS celui qu'il faut utiliser à l'intérieur de EU. Les utilisateurs européens du contrôleur de sécurité doivent utiliser la version anglaise européenne (ce manuel 135369) ou une traduction équivalente.

** Pour les détails, contacter votre [Bureaux du siège social en page 125](#).



Indice de la figure

- | | |
|--|--|
| <ul style="list-style-type: none"> 1. Contrôleur de sécurité SC22-3 2. Câble USB A/B 3. Carte de mémoire externe (carte XM) 4. Outil de programmation SC-XMP de la carte XM (certains modèles) | <ul style="list-style-type: none"> 5. CD contenant le manuel d'instructions du logiciel PCI et les tutoriaux de configuration 6. Guide de démarrage rapide 7. Bornier débrochable |
|--|--|

Figure 16 Composants du kit du Contrôleur de sécurité SC22-3

4.3 RACCORDEMENT DU CONTRÔLEUR DE SÉCURITÉ SC22-3

4.3.1 Raccordement électrique

- 1) En se référant aux instructions d'installation du fournisseur en conjonction avec les informations de configuration du contrôleur de sécurité SC22-3 fournies dans ce manuel d'instructions, raccorder le bornier du contrôleur de sécurité SC22-3 (illustré [Figure 16 en page 25](#)) à l'alimentation électrique, aux sorties d'état, aux Sorties de sécurité et aux entrées.

4.3.2 Connexions USB

Le contrôleur de sécurité est raccordé à un PC par l'intermédiaire d'un câble USB A/B ([Figure 17 en page 26](#)). Ce câble sert aussi à raccorder le PC à l'outil de programmation SC-XMP (voir [Figure 18 en page 26](#)) pour télécharger une configuration sur la carte XM.

- 1) En se référant à la [Figure 17 en page 26](#), raccorder le câble USB A/B au contrôleur de sécurité et au PC avec le logiciel PCI chargé et configuré.

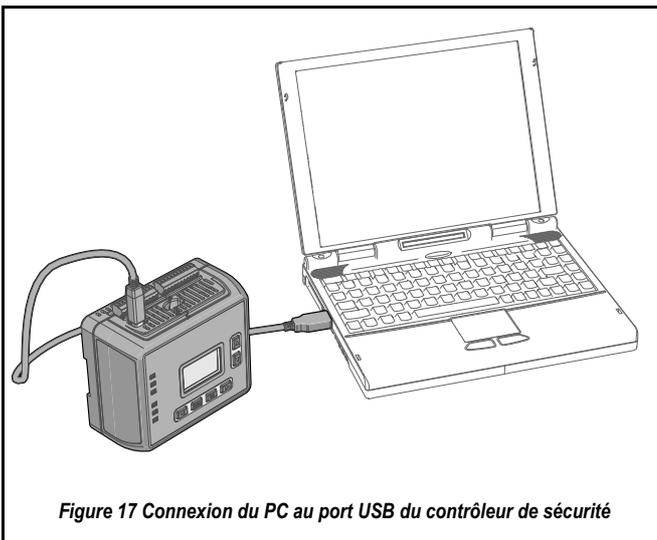


Figure 17 Connexion du PC au port USB du contrôleur de sécurité

4.3.3 Outil de programmation SC-XMP

L'outil de programmation SC-XMP est pratique pour transférer une configuration d'un PC (utilisant le logiciel PCI) à une carte XM ou d'une carte XM au PC, sans avoir besoin de se servir du contrôleur de sécurité SC22-3. Il se raccorde au PC par l'intermédiaire du câble USB A/B et du port USB du PC (voir [Figure 18 en page 26](#)).

- 1) En se référant à [Figure 18 en page 26](#), raccorder l'outil de programmation SC-XMP.
 - 2) Enficher la carte XM.
- ☛ Pour plus d'informations sur le chargement de la configuration sur la carte XM, se référer à [Paragraphe 5.1.16 en page 50](#).

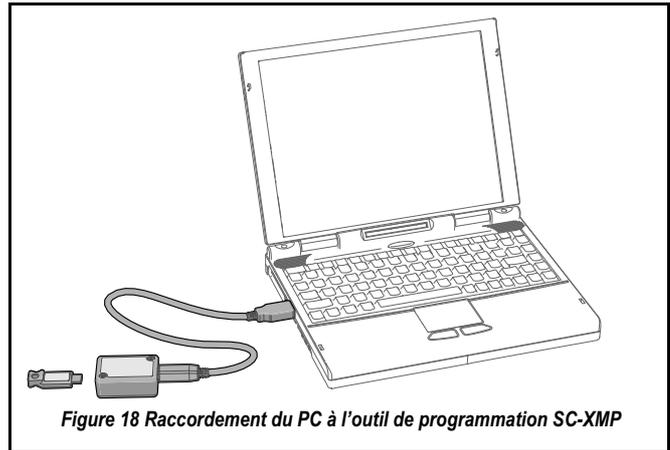


Figure 18 Raccordement du PC à l'outil de programmation SC-XMP

4.3.4 Carte SC-XM1 mémoire externe XM

La prise SC-XM1 mémoire externe XM est un module de mémoire amovible qui peut enregistrer ou servir à transférer une configuration. La carte XM dispose sur son envers d'un autocollant où on peut écrire le nom d'une configuration ou l'identification d'une machine. La carte XM est illustrée raccordée au contrôleur de sécurité SC22-3 dans la [Figure 18 en page 26](#).

La carte XM peut servir à :

- Conserver une copie de sauvegarde d'une configuration du contrôleur de sécurité (pour minimiser le temps de panne en cas d'une défaillance matérielle qui nécessiterait le remplacement du contrôleur)
- Transférer une configuration d'un contrôleur de sécurité à un autre contrôleur de sécurité
- Envoyer (télécharger) des configurations identiques à plusieurs contrôleurs de sécurité
- Transférer des configurations entre le contrôleur de sécurité et un ordinateur personnel

Enregistrer une configuration sur la carte XM selon l'une des deux façons suivantes :

- Envoyer une copie de la carte XM en utilisant l'interface du PC (PCI) et l'outil de programmation SC-XMP (voir [Paragraphe 5.1.16 en page 50](#))
- Envoyer une copie du contrôleur de sécurité à la carte XM ou vice versa, en utilisant OBI (voir [Paragraphe 6.3.1.2 en page 63](#) ou [Paragraphe 6.3.1.3 en page 63](#))

☛ Une configuration peut être enregistrée de façon permanente dans une carte XM, si on utilise la fonction « verrouillage ».

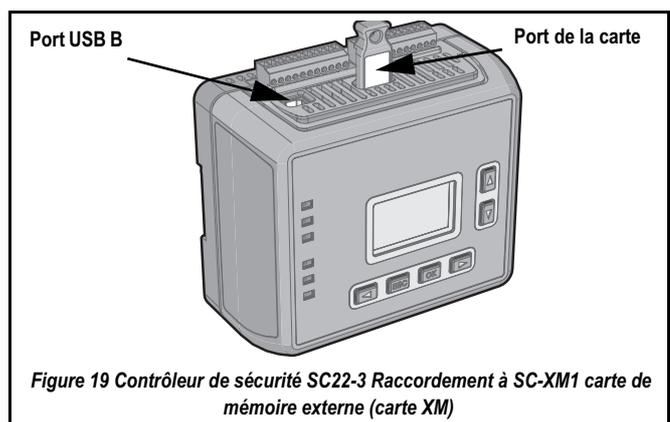


Figure 19 Contrôleur de sécurité SC22-3 Raccordement à SC-XM1 carte de mémoire externe (carte XM)

4.4 EXPLICATIONS SUR LA CONNEXION DES DISPOSITIFS DE SÉCURITÉ

AVERTISSEMENT

L'UTILISATEUR A LA RESPONSABILITÉ DE S'ASSURER QUE TOUTES LES LOIS, RÉGLES, CODES ET RÉGLEMENTS LOCAUX, D'ÉTAT ET NATIONAUX S'APPLIQUANT À L'UTILISATION DU CONTRÔLEUR DE SÉCURITÉ DANS UNE APPLICATION PARTICULIÈRE SONT RESPECTÉES. IL FAUT FAIRE TRÈS ATTENTION À RESPECTER TOUTES LES EXIGENCES LÉGALES ET TOUTES LES INSTRUCTIONS D'INSTALLATION, DE FONCTIONNEMENT ET D'ENTRETIEN DU MANUEL DU CONSTRUCTEUR DU DISPOSITIF DE SÉCURITÉ ET DE CE MANUEL SONT RESPECTÉES.

Les entrées du contrôleur de sécurité SC22-3 peuvent être configurées pour s'interfacer avec de nombreux types de dispositifs de sécurité, dont les dispositifs de protection (par ex. barrières immatérielles), les équipements de protection supplémentaire (par ex. boutons d'arrêt d'urgence) et les autres dispositifs qui entrent dans la sécurité d'utilisation d'une machine (par ex. protection des équipements).

La façon dont des dispositifs s'interconnectent joue sur la façon dont ils excluent ou détectent les erreurs qui peuvent provenir d'une perte de la fonction de sécurité. Il y a de nombreuses normes, règles et spécifications qui exigent un certain niveau d'un circuit de sécurité.

4.5 PROPRIÉTÉS DES DISPOSITIFS D'ENTRÉE DE SÉCURITÉ

Figure 20 en page 27 explique les propriétés du menu des entrées de sécurité.

Sert à taper un nom d'un dispositif d'entrée de sécurité

Sert à sélectionner le type de circuit dans un menu déroulant

Sert à sélectionner la logique de réarmement dans un menu déroulant

Montre le type de circuit et les assignations des bornes d'entrée sélectionnées

"+" indique une borne qui fournit +24 Vcc au dispositif d'entrée de sécurité

Ces menus déroulants servent à changer l'assignation des bornes d'entrée

Le fait de cliquer sur le bouton INFO renvoie à plus d'informations.
Astuce : Cliquer sur le bouton INFO renvoie à [Annexe A2](#) de ce manuel donnant plus d'informations sur un dispositif et le niveau de sécurité que donne chaque type de circuit.

Permet à chaque dispositif d'être assigné à 1, 2 ou 3 sorties de sécurité

Paramètres avancés utilisés pour la suite de la configuration du type de dispositif (par ex. simultanément, temps d'anti-rebond de fermé à ouvert ou temps d'anti-rebond d'ouvert à fermé)

Figure 20 Détail des propriétés des entrées de sécurité

4.5.1 Généralités

Le contrôleur peut être configuré pour correspondre à de nombreux types d'entrées de sécurité. Cependant, un certain nombre de propriétés des dispositifs doivent être établies (soit en utilisant l'OBI ou le PCI) pour que le contrôleur puisse suivre correctement leurs signaux.

Le détail des propriétés configurables des dispositifs d'entrée de sécurité est présenté dans le [Tableau 6 ci-dessous](#) et les [Paragraphe 4.5.2](#) à [Paragraphe 4.5.11](#).

4.5.2 Désignation

Cette propriété sert à configurer automatiquement la désignation du dispositif par le contrôleur et peut être modifiée par l'utilisateur.

4.5.3 Type de circuit

Cette propriété sert à configurer le circuit et les options de convention du signal qui peuvent être sélectionnées pour définir le dispositif d'entrée de sécurité. [Tableau 6 ci-dessous](#) donne une sélection des dispositifs d'entrée de sécurité et des types de circuits que le contrôleur de sécurité peut surveiller. Il indique aussi les propriétés qui peuvent être configurées et pour quels dispositifs. Ces aspects sont étudiés plus en détail dans les paragraphes suivants.

☛ *Tous les types de circuits ne correspondent pas à la classification de catégorie 4 selon ISO 13849-1 ; se référer à [Annexe A2](#) pour plus d'informations sur les niveaux d'intégrité des circuits de sécurité.*

Tableau 6 Dispositif d'entrée de sécurité du Contrôleur de sécurité et présentation de la surveillance du type de circuit

| | Arrêt d'urgence | Interrupteur pour porte | Détecteur optique | Commande bimanuelle | Interrupteur à câble | Arrêt de protection | Tapis sensible de sécurité | Dispositif de commande | Capteur d'inhibition | Interrupteur de bypass | Surveillance des commutateurs externes |
|---|-----------------|-------------------------|-------------------|---------------------|----------------------|---------------------|----------------------------|------------------------|----------------------|------------------------|--|
| Propriétés configurables | | | | | | | | | | | |
| Types de circuits : | 7 | 13 | 10 | 7 | 10 | 10 | 1 | 10 | 7 | 10 | 2 |
| Logique de réarmement : | Auto/Manuel | Auto/Manuel | Auto/Manuel | Auto | Auto/Manuel | Auto/Manuel | Auto/Manuel | Auto | Auto | Auto | — |
| Assigné à : | E/S | E/S | E/S | E/S | E/S | E/S | E/S | E/S | I/I | I/I | E/S |
| COS* (Simultanéité): Simultanément (S) / L'un après l'autre (C) | S/C | S/C | S/C | S | S/C | S/C | — | S/C | S | S/C | S |
| Anti-rebond | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Non |
| Test de démarrage | — | Oui | Oui | — | — | — | — | — | — | — | — |
| Limite de temps de la fonction | — | — | — | — | — | — | — | Oui | Oui | Oui | — |
| Peut être inhibé | — | Oui | Oui | Oui | — | — | Oui | — | — | — | — |
| Peut être bypassé | — | Oui | Oui | Oui | — | — | Oui | — | — | — | — |

* Changement d'état du signal ([paragraphe 4.5.7.1 en page 29](#))
S = Simultanéité
C = L'un après l'autre

4.5.4 Logique de réarmement

Cette propriété sert à configurer les deux réarmements automatique (mode automatique) ou manuel (mode manuel). Les entrées de sécurité peuvent être configurées pour exiger un réarmement manuel avant que la sortie de sécurité qu'elles contrôlent puissent repasser sur ON. On appelle quelles que fois ce mode de verrouillage parce que la sortie de sécurité se verrouille dans l'état OFF jusqu'à ce qu'on ait effectué un réarmement système. Si une entrée de sécurité est configurée pour un réarmement automatique ou mode automatique, les sorties de sécurité qu'elle contrôle repassent sur ON quand le dispositif d'entrée revient en l'état Run (à condition que toutes les autres entrées de contrôle soient aussi dans l'état Run). Les règles et les types de réarmement sont présentés au [Paragraphe 1.10 en page 5](#).

4.5.5 Bornes d'entrée

Cette propriété sert à configurer les bornes d'entrée qui raccordent les dispositifs d'entrée de sécurité et d'entrée auxiliaire. Le contrôleur de sécurité doit savoir quelles sont les lignes de signaux en provenance des dispositifs qui doivent être raccordés et à quels bornes afin de pouvoir appliquer les bonnes méthodes de surveillance du signal, les conventions Run et Stop, les règles de délais et les règles d'erreur. Bien que les bornes soient assignées automatiquement pendant le processus de configuration, il est possible de changer les assignations à la main, à l'aide de OBI ou de l'interface PCI.

4.5.6 Assigné à :

Cette propriété sert à configurer la relation de commande logique entre les entrées et les sorties ou entre les entrées

4.5.7 Réglages avancés

4.5.7.1 Changement d'état du signal (simultanéité)

Deux types COS (simultanéité voir [Simultanéité](#)) peuvent être utilisées pour surveiller la sécurité des signaux d'un dispositif d'entrée d'un double voie pour un double voie ; simultanément ou l'un après l'autre. Les règles pour chaque type de circuit sont énumérées dans le [Tableau 7](#) en Page 29.

Tableau 7 Types de changement d'état de signal (COS)(simultanéité)

| Type de circuit | Symbole du circuit | Règles de minutage du signal d'entrée COS (simultanéité) en état Stop | Règles de minutage du signal d'entrée COS (simultanéité) en état Run |
|----------------------------------|---|---|---|
| | | La sortie de sécurité passe sur OFF quand ¹ : | La sortie de sécurité passe sur ON quand ² : |
| Double voie A & B complémentaire | <p>Complémentaire, 2 bornes</p>  <p>Complémentaire, 3 bornes</p>  <p>complémentaire, contact PNP</p>  | <p>Au moins l'entrée d' 1 canal (A ou B) en état Stop.</p> | <p>Simultanéité A et B sont tous les deux en état Stop puis les deux en état Run en moins de 3 s avant que les sorties passent sur ON.</p> <p>L'un après l'autre A et B sont l'un après l'autre en état Stop puis tous les deux en état Run sans simultanéité, pour faire passer les sorties sur ON.</p> |
| Double voie A et B | <p>Canal double, 2 bornes</p>  <p>Canal double, 3 bornes</p>  <p>Canal double, 4 bornes 3 Bornes</p>  <p>Double canal, PNP</p>  | | |
| 2 complémentaires A et B | <p>2 complémentaires, 4 bornes</p>  <p>2 complémentaires, 5 bornes</p>  <p>2 complémentaires, contact PNP</p>  | <p>Au moins 1 canal (A ou B) dans une paire de contacts en état Stop.</p> | <p>Simultanéité A et B l'un après l'autre en état Stop, puis les contacts dans un canal en état Run en moins de 400 ms (150 ms pour une commande bimanuelle), les deux canaux en état Run en moins de 3 s (0,5 s pour une commande bimanuelle).</p> <p>L'un après l'autre A et B l'un après l'autre en état Stop, puis les contacts dans un canal en état Run en moins de 3 s. Les deux canaux en état Run sans simultanéité.</p> |
| 2 complémentaires A et B | <p>Tapis de sécurité 4 Bornes</p>  | <p>Des canaux d'entrée sont court-circuités ensemble, ou Au moins 1 des fils sont débranchés ou un des canaux normalement bas est détecté haut ou un des canaux normalement hauts est détecté bas</p> | <p>Chaque canal détecte ses propres impulsions.</p> |

¹ Les sorties de sécurité passent sur OFF quand une des entrées les contrôlant est en état Stop.

² Les sorties de sécurité ne passeront sur ON que quand toutes les entrées qui les contrôlent sont en état Run et seulement après avoir effectué un réarmement manuel, si une de ces entrées de sécurité est configurée pour réarmement manuel et était en état Stop.

4.5.7.2 Temps d'anti-rebond fermé à ouvert / temps d'anti-rebond ouvert à fermé

⚠ PRECAUTIONS

Temps de réponse et d'anti-rebond

Toute modification du temps d'anti-rebond de fermé à ouvert affectera le temps de réponse de la sortie de sécurité (passage sur OFF). Cette valeur est calculée et affichée pour chaque sortie de sécurité quand une configuration est créée. Les valeurs sont aussi indiquées dans les documents de OBI et du résumé de configuration de PCI. (Le réglage par défaut est de 6 ms.)

Temps de réponse

Le temps de réponse d'un dispositif complémentaire est basé sur l'ouverture des contacts fermés, pas sur la fermeture des contacts ouverts. Chacun déclenchera un signal d'arrêt, mais seulement un détermine le temps de réponse.

Toute modification du temps d'anti-rebond d'ouvert à fermé affecte le temps de réaction de la sortie de sécurité (passage sur ON).

L'anti-rebond configurable d'une entrée ON/OFF et l'entrée d'un dispositif d'actionnement ne font pas partie du temps de réponse calculé et confirmé.

Cette propriété sert à configurer le temps de transition d'état du signal

Temps d'anti-rebond de fermé à ouvert
De 6 ms à 100 ms par intervalles de 1 ms

Le temps d'anti-rebond fermé à ouvert est le temps limite que prend le signal pour passer de l'état élevé (24 Vcc) à l'état bas stabilisé (0 Vcc). Ce temps limite doit être accru quand des vibrations de forte amplitude, un choc d'impact ou des perturbations du dispositif nécessitent un temps de transition du signal plus élevé. Si le temps d'anti-rebond fermé à ouvert est trop court dans ces conditions difficiles, le système peut détecter une erreur de disparité du signal et se bloquer. (Le réglage par défaut est de 6 ms).

Temps d'anti-rebond ouvert à fermé
De 10 ms à 500 ms par intervalles de 1 ms

Le temps d'anti-rebond ouvert à fermé est le temps limite que prend le signal pour passer de l'état bas (0 Vcc) à l'état élevé stabilisé (24 Vcc). Ce temps limite doit être accru quand des vibrations de forte amplitude, un choc d'impact ou des perturbations du dispositif nécessitent un temps de transition du signal plus élevé. Si le temps d'anti-rebond de ouvert à fermé est trop court dans ces conditions difficiles, le système peut détecter une erreur de disparité du signal et se bloquer. (Le réglage par défaut est de 50 ms.)

Quand on utilise un tapis de sécurité, le calcul du temps de réponse du tapis dépend des temps d'anti-rebond Run (10 ms à 500 ms) et Stop (6 ms à 100 ms).

4.5.8 Test au démarrage

Cette propriété sert à configurer un test de l'entrée de sécurité de précaution en option après chaque mise sous tension.

4.5.9 Temps limite du dispositif

Cette propriété sert à configurer la limite de temps réglable pendant lequel une fonction doit se produire.

4.5.10 Paire de capteurs d'inhibition

Cette propriété sert à configurer si le dispositif peut être inhibé ou non.

4.5.11 Interrupteur de bypass

Cette propriété sert à configurer si le dispositif peut être bypassé ou non.

4.6 PROPRIÉTÉS DES DISPOSITIFS D'ENTRÉES AUXILIAIRES

Les propriétés configurables des dispositifs d'entrées auxiliaires sont présentées dans le [Tableau 8 ci-dessous](#) et [Paragraphe 4.6.1 à Paragraphe 4.6.3](#).

Tableau 8 Dispositifs d'entrée auxiliaire

| | Réarmement manuel | ON/OFF | Inhibition |
|---|---|---|---|
| Propriétés configurables |  |  |  |
| Types de circuits : | 3 | 3 | 3 |
| Assigné à : | E/S | E/S | E/S |
| Temps d'anti-anti-rebond fermé à ouvert / temps d'anti-anti-rebond ouvert à fermé | Fixé à 50 ms | Fermé à ouvert : 6 ms-100 ms Ouvert à fermé : 10 ms-500 ms | Fixé à 50 ms |
| Reset contrôlé | Oui | — | — |

4.6.1 Dispositifs de réarmement manuel

Le réarmement manuel sert à créer un signal de réarmement système quand une entrée de sécurité qui a été configurée pour nécessiter un réarmement manuel a été ouverte ou fermée. Après un réarmement manuel, toutes les sorties de sécurité contrôlées par cette entrée de sécurité peuvent passer sur ON. Voir [Mise en garde, page 5](#).

4.6.2 Interrupteur marche / arrêt

L'interrupteur ON/OFF sert à envoyer une commande ON ou OFF (marche ou arrêt) à la machine. Quand toutes les entrées de sécurité de commande sont en état Run, cette fonction permet à la sortie de sécurité de passer sur ON et OFF. C'est un signal de simple voie ; l'état Run est 24 Vcc et l'état Stop est 0 Vcc.

4.6.3 Interrupteur d'inhibition

L'interrupteur d'inhibition sert à signaler au contrôleur quand les capteurs d'inhibition sont autorisés à effectuer une fonction d'inhibition. Quand la fonction d'inhibition est configurée, les capteurs d'inhibition ne sont pas autorisés à effectuer une fonction d'inhibition jusqu'à ce que le signal soit en état Run. C'est un signal de simple voie ; le signal d'activation (Run) est 24 Vcc et celui de désactivation (Stop) est 0 Vcc.

4.7 CONFIGURATION DU CONTRÔLEUR DE SÉCURITÉ

L'établissement d'une configuration pour le contrôleur de sécurité est un processus simple, en utilisant une des deux interfaces suivantes :

- Les boutons et l'affichage du contrôleur de sécurité lui-même (OBI) ou
- Le logiciel PCI du CD (réf. 134534) inclus dans le kit du contrôleur de sécurité SC22-3.

La procédure comprend trois étapes principales :

4.7.1 OBI

Le contrôleur de sécurité peut être configuré en utilisant le OBI avec ses boutons et son écran LCD. L'affichage LCD donne des informations sur les dispositifs d'E/S et l'état du système pour chaque événement qui fait passer une des sorties de sécurité sur OFF. Voir [Figure 21 en page 31](#) et [Tableau 9 en Page 32](#) pour les explications de OBI .

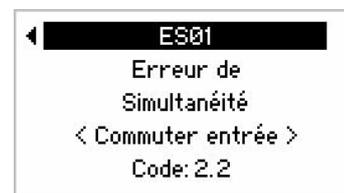
L'affichage est utilisé en conjonction avec les six boutons pour les opérations suivantes :

- Créer ou modifier des configurations protégées par mot de passe
- Retrouver les informations du registre d'erreurs
- Vérifier le détail de câblage des dispositifs et les relations logiques des E/S et
- Afficher les erreurs des dispositifs d'E/S et les étapes probables de récupération

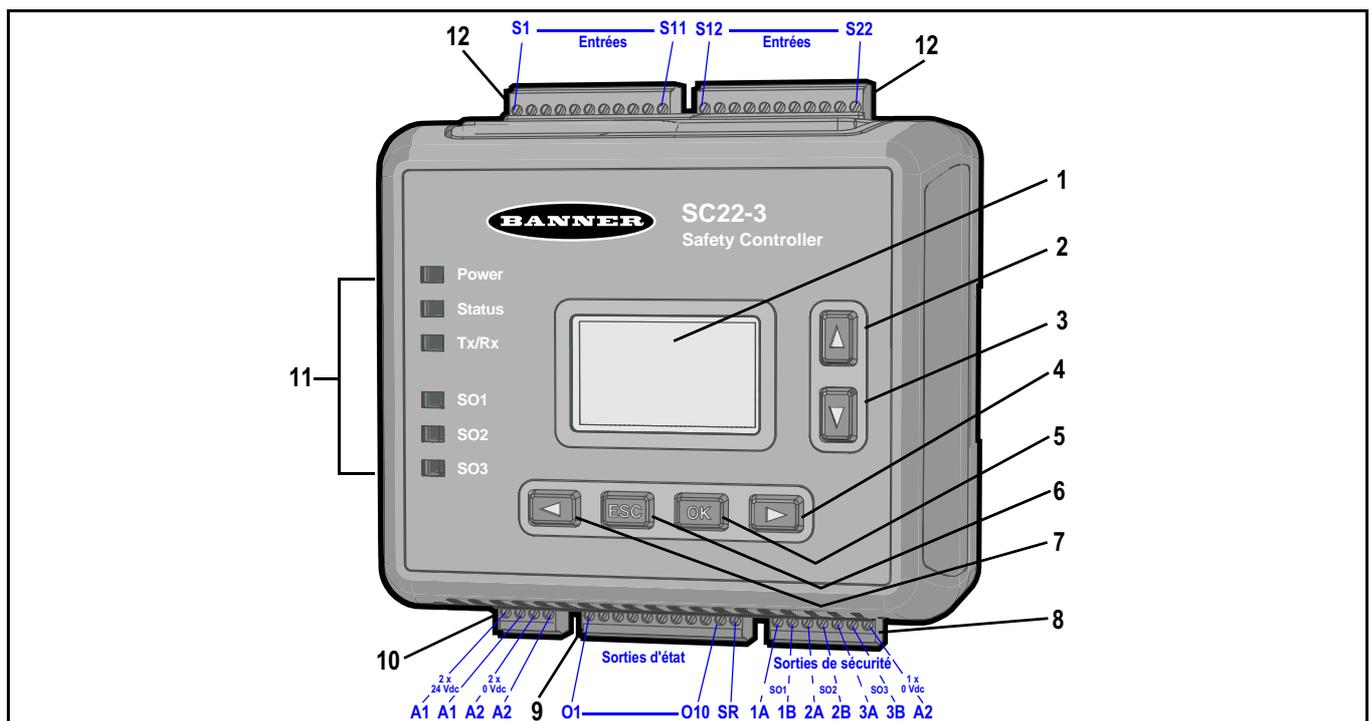
☛ Pour plus de détails sur les fonctions de l'OBI se référer au [Chapitre 6](#).

Accéder aux codes d'erreur

Les codes d'erreur sont affichés sur la dernière ligne du menu de diagnostic d'erreurs de l'OBI (voir [Screen 1](#)). Se référer au [Chapitre 6](#) et au [Paragraphe 8.3.3 en page 77](#) pour plus d'informations.



Screen 1



Indice de la figure

- | | | |
|---|---|---|
| <ol style="list-style-type: none"> 1. Affichage à cristaux liquides 2. Déplace le curseur vers le haut ou affiche des points dans une liste pendant que le curseur se déplace. Peut aussi servir à sélectionner des paramètres 3. Déplace le curseur vers le bas ou affiche des points dans une liste pendant que le curseur se déplace. Peut aussi servir à sélectionner des paramètres | <ol style="list-style-type: none"> 4. Déplace le curseur vers la droite ou sélectionne un paramètre. 5. Entrer ou définit le point de l'affichage en surbrillance en tant que sélection ou peut être utilisé pour faire basculer un paramètre 6. Déplace le curseur à un point pré-établi du programme pour redéfinir un point de référence du menu. | <ol style="list-style-type: none"> 7. Déplace le curseur vers la gauche ou sélectionne un paramètre. 8. Raccordement terminal de sorties de sécurité 9. Raccordement terminal de sorties d'état 10. Raccordement terminal de alimentation électrique 11. Indications des LED 12. Raccordement terminal de Entrées de sécurité |
|---|---|---|

Figure 21 Interface embarqué avec boutons, écran d'affichage à LCD et indicateurs d'état

Tableau 9 Détail de l'indicateur d'état de l'interface embarqué

| Indicateur d'état | Condition | Indique l'état du contrôleur de sécurité |
|---------------------------------------|--|--|
| Tous les indicateurs OFF | — | Mode d'initiation |
| Alimentation | ON Vert  OFF (ARRÊT)  | Alimentation ON Alimentation OFF |
| État (Mode du contrôleur de sécurité) | ON Rouge  Rouge clignotant  OFF (ARRÊT)  | Mode de configuration Mode de blocage Mode Run |
| Transmettre / recevoir Tx/Rx | Vert clignotant  OFF (ARRÊT)  | Émission ou réception de données (une liaison est établie avec le PC) Pas d'émission ni de réception de données |
| Sortie de sécurité SO1, SO2, SO3 | ON Vert  ON Rouge  Rouge clignotant  Vert clignotant  | Sortie de sécurité ON Sortie de sécurité OFF Sortie de sécurité erreur détectée Sortie de sécurité en attente d'un réarmement |

☛ Les fonctions de OBI sont expliquées au [Chapitre 6](#).

4.7.2 Interface PC

Le contrôleur de sécurité peut aussi être configuré à partir d'un ordinateur sous Windows® et le programme d'interface SC22-3 PC (PCI) (Écran 2). Cette interface conviviale utilise des icônes et des symboles de circuit pour simplifier la sélection des propriétés des dispositifs pendant la configuration. Le câblage de la configuration et les diagrammes logiques Ladder sont créés automatiquement au fur et à mesure de la progression de la configuration.

Quand la configuration est créée, elle peut être :

- Enregistrée dans un fichier informatique pour archivage et utilisation future

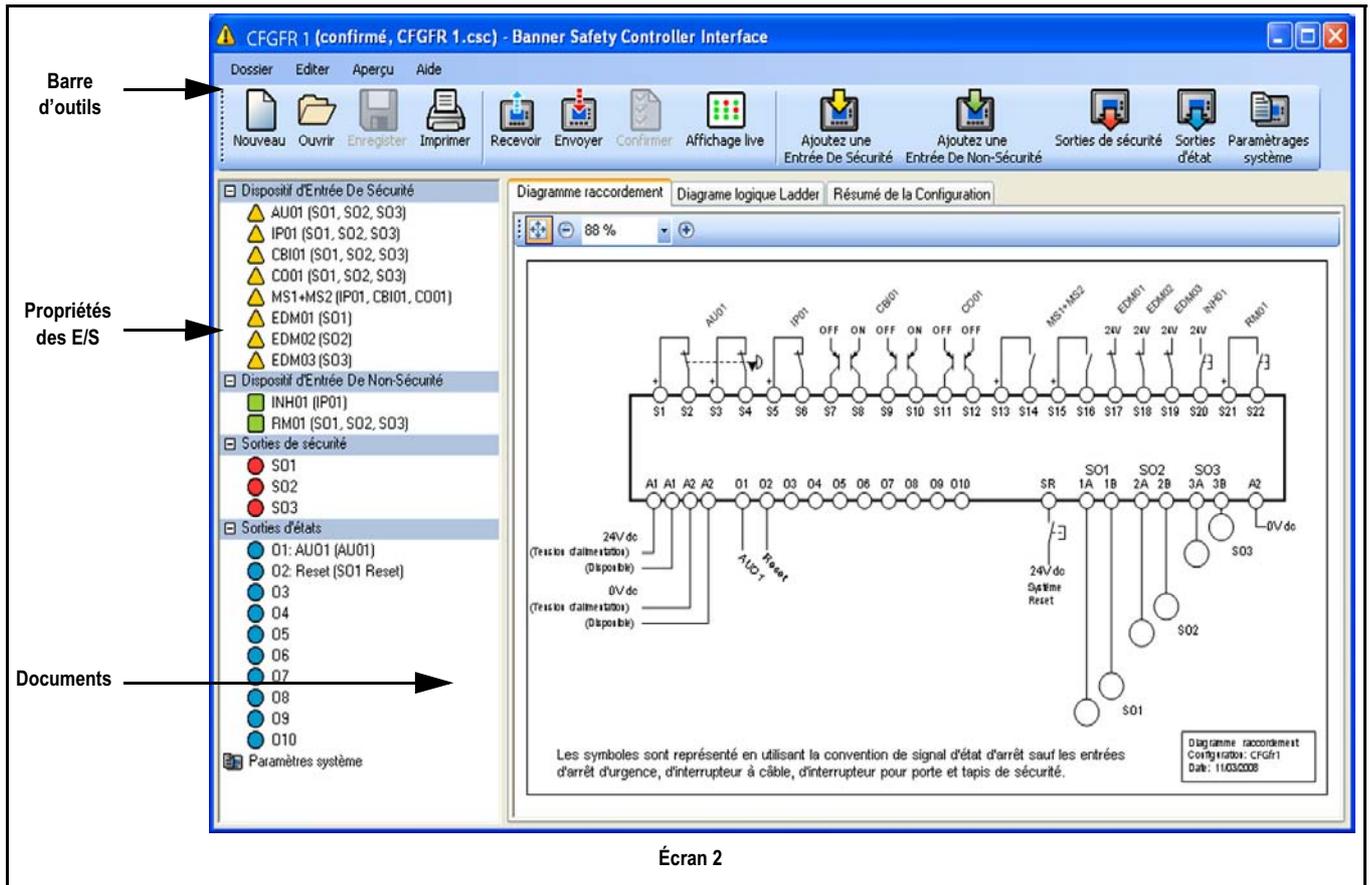
ou

- Envoyée par courriel sous forme de pièce jointe

ou

- Peut être envoyée directement à n'importe quel contrôleur de sécurité SC22-3 et à la carte mémoire externe enfichable

Le PCI peut servir à créer une configuration, la sauvegarder et l'envoyer comme cela est indiqué précédemment, mais aussi il peut surveiller le fonctionnement d'un contrôleur de sécurité en utilisant l'affichage en temps réel, ainsi que suivre le registre d'erreurs pour des besoins de dépannage. Le fonctionnement du PCI est couvert plus en détail dans le Chapitre 5.



Écran 2

4.7.3 Définition de l'application de protection

Évaluation des risques

Cela comprend :

- Détermination des dispositifs nécessaires
- Détermination du niveau de sécurité nécessaire

4.7.4 Construction de la configuration

Cela comprend :

- Sélection des types d'entrée de sécurité et des connexions des circuits
- Assignation de chaque entrée à une ou plusieurs sorties de sécurité ou à d'autres dispositifs d'entrée
- Établissement de retards à l'enclenchement ou au déclenchement des sorties de sécurité
- Sélection des types d'entrées auxiliaires et des connexions des circuits, le cas échéant
- Assignation des signaux de sortie d'états, le cas échéant
- Créer le nom de la configuration, le nom de l'auteur, le mode de mise sous tension et le réarmement système surveillé

4.7.5 Confirmation de la configuration

Cela comprend :

- Par l'intermédiaire du contrôleur de sécurité, vérifier que la configuration choisie est valide
- En tant qu'utilisateur, confirmer que la configuration est bien celle qu'on voulait

4.8 RACCORDEMENT DES EDM, OSSD SORTIE DE SÉCURITÉ ET FSD

4.8.1 EDM

4.8.1.1 Surveillance simple voie

Les informations de raccordement détaillées se trouvent en [Figure 26 en page 85](#).

4.8.1.2 Surveillance double voies

Les informations de raccordement détaillées se trouvent en [Figure 27 en page 85](#).

4.8.1.3 Pas de surveillance

Si on ne désire pas de surveillance, il ne faut pas choisir l'option simple voie ou double voie. **Si le contrôleur de sécurité n'utilise pas la fonction EDM dans des applications de catégorie 3 ou de catégorie 4, l'utilisateur doit s'assurer que toute défaillance unique ou accumulation de défaillances des dispositifs extérieure n'entraînent pas de condition dangereuse et que les cycles suivants de la machine sont interdits.**

4.8.2 Raccordement d'interface FSD

Les FSD (dispositifs de commutation finaux) peuvent prendre de nombreuses formes, la plus commune étant des relais de commande mécaniquement liés, à guidage forcé, ou des modules d'interface. La liaison mécanique entre les contacts permet de surveiller le contacteur par le circuit de surveillance des commutateurs externes pour certaines défaillances.

Selon l'application, l'utilisation des FSD peut permettre de contrôler la tension et l'intensité qui diffèrent des sorties OSSD du contrôleur de sécurité. Les FSD peuvent aussi servir à contrôler d'autres risques en créant plusieurs circuits d'arrêt d'urgence.

4.8.2.1 Circuits d'arrêt de sécurité (de protection)

Un arrêt d'urgence permet d'arrêter le mouvement pour des raisons de sécurité, ce qui interrompt le mouvement et coupe l'alimentation des MPCE (en supposant que cela n'entraîne pas de nouveaux risques). Un circuit d'arrêt d'urgence comporte normalement au moins deux contacts NO de relais à guidage forcé (liés mécaniquement), lesquels sont surveillés pour détecter certaines défaillances de façon à éviter la perte de la fonction de sécurité (soit la EDM). Ce circuit est appelé « point de commutation de sécurité. »

Normalement, les circuits d'arrêt de sécurité sont une connexion en série d'au moins deux contacts NO provenant de deux relais à guidage positif séparés, chacun étant commandé par une sortie de sécurité séparée du contrôleur de sécurité. La fonction de sécurité est basée sur l'utilisation de contacts redondants pour contrôler un risque unique, de façon à ce que, si un contact est défaillant sur ON, le second contact arrête le risque et empêche le 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 (voir les modèles au [Paragraphe 3.2.2 en page 23](#)) sont une connexion en série de contacts redondants qui forment des circuits d'arrêt de sécurité et peuvent servir dans des méthodes de commande à simple voie ou à double voies (voir [Figure 14 en page 21](#)).

Commande à double voie

La commande à double voies (ou deux canaux) est capable d'éteindre électriquement le point de commutation de sécurité au-delà des contacts FSD. Si la surveillance est bien faite (c'est-à-dire, EDM), cette méthode d'interfaçage peut détecter certaines défaillances dans le câblage de commande entre le circuit d'arrêt d'urgence et les MPCE. Par exemple, un court-circuit d'une voie vers une alimentation électrique secondaire ou la perte de la fonction de commutation d'une des sorties FSD dont l'effet serait une perte de redondance ou une perte complète de sécurité si elle n'était pas détectée et réparée.

Le risque d'une défaillance de câblage augmente :

- Avec la distance physique entre les circuits d'arrêt d'urgence FSD et les MPCE
- Avec la longueur des câbles d'interconnexion

ou

- 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 avec surveillance EDM si les FSD sont éloignés des MPCE.

Commande à simple voie

Une commande à simple voie (ou simple voie), comme déjà précisé, 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 ou une tension secondaire).

Cette méthode d'interfaçage ne doit donc être utilisée que si les circuits d'arrêt d'urgence FSD et les MPCE sont situés dans la même armoire de commande, à côté les uns des autres et directement raccordés, ou que si l'on peut exclure ce risque de défaillance. Dans le cas contraire, il faut utiliser une commande à double voie.

Les méthodes d'exclusion du risque de ce type de défaillance sont les 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 des commandes d'interconnexion dans des tubes, des passages ou des chemins de câbles différents
- Utilisation de faible tension ou de neutre pour les fils d'interconnexion qui ne peuvent générer de risques
- Montage de 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
- Montage correct de câbles à plusieurs conducteurs ou de fils multiples qui passent dans les presse-étoupes. Le fait de trop serrer le presse-étoupe peut créer des courts-circuits à cet endroit
- Utilisation de composants à ouverture positive ou à entraînement direct installés de façon positive

4.8.2.2 Connexion du contrôleur de sécurité aux modules d'interface

Pour la connexion du contrôleur de sécurité aux modules d'interface, se référer à la [Figure 29 en page 86](#), [Figure 30 en page 86](#) et [Figure 31 en page 87](#).

4.8.3 installation de fil de la terre

Le courant dans les charges crée une chute de tension due à la résistance de la ligne R_L du fil commun en courant continu. Plus la résistance du fil commun en courant continu est élevée (par ex., fil de section trop faible ou mauvaise connexion électrique), plus forte est la tension créée par la résistance de ce fil. Si la tension dépasse 0,6 V, une sortie de sécurité qui est passée sur OFF, peut apparaître comme étant en court-circuit avec la tension +. Cela crée une erreur au contrôleur et la sortie passe sur OFF ou reste sur OFF, provoquant un blocage ([voir le code d'erreur 1.2 page 77](#)).

Pour éviter cela, tous les câblages communs en courant continu des charges raccordées aux sorties de sécurité doivent toujours être de forte section et aussi courts que possible pour minimiser leur résistance (voir [Figure 32 en page 87](#)).

4.9 SORTIES D'ÉTAT

4.9.1 Conventions pour les signaux d'état des sorties

Il existe deux conventions pour les signaux d'état des sorties que l'on peut sélectionner. La convention par défaut envoie un signal en 24 Vcc quand l'entrée ou la sortie surveillée est active (fermée, élevée ou ON), quand le système est verrouillé, quand il y a une erreur d'E/S, quand le système attend un réarmement, quand la sortie attend un réarmement ou pendant un cycle d'inhibition actif. Si les conditions précédentes ne sont pas vraies, le signal de sortie doit être de 0 V.

La convention de signal 2 est l'inverse de la convention de signal 1, comme illustré dans le [Tableau 10 ci-dessous](#).

Tableau 10 Convention pour les signaux

| Fonction surveillée | État des sorties assignées | |
|--|---|------------------------------------|
| | Signal Convention 1 (défaut) 24 Vcc = Run (par défaut) | Signal Convention 2 0 Vcc = Run |
| Entrée Run Entrée Stop | 24 Vcc 0 Vcc | 0 Vcc 24 Vcc |
| Sortie ON Sortie OFF | 24 Vcc 0 Vcc | 0 Vcc 24 Vcc |
| Système en blocage Système en mode Run | 24 Vcc 0 Vcc | 0 Vcc 24 Vcc |
| Une erreur d'E/S existe Il n'existe pas d'erreur d'E/S | 24 Vcc 0 Vcc | 0 Vcc 24 Vcc |
| Réarmement système nécessaire Réarmement système non nécessaire | 24 Vcc 0 Vcc | 0 Vcc 24 Vcc |
| Réarmement sortie nécessaire Réarmement sortie non nécessaire | 24 Vcc 0 Vcc | 0 Vcc 24 Vcc |
| L'entrée est inhibée Pas d'inhibition | 24 Vcc 0 Vcc | 0 Vcc 24 Vcc |

4.10 VÉRIFICATION DE MISE EN SERVICE

Quand le contrôleur de sécurité est sous tension, que le EDM a été correctement configuré et que les sorties de sécurité ont été raccordées à la machine à protéger, le fonctionnement du contrôleur de sécurité doit être vérifié avec la machine protégée, avant de mettre l'ensemble du système en service. Pour ce faire, la [Personne qualifiée selon spécification du paragraphe 1.8.2 en page 4](#) doit effectuer une procédure de vérification de mise en service détaillée dans le [Paragraphe 8.2.5 en page 71](#).

4.11 INSTALLATION DU LOGICIEL

4.11.1 Installation du logiciel PCI

4.11.1.1 Prescriptions du système

Les prescriptions du système pour faire fonctionner le logiciel PCI sur l'ordinateur sont les suivantes :

| Prescriptions du système | |
|---------------------------|---|
| Système en fonctionnement | Windows® XP, Windows 2000® et Windows Vista (version 1.1 du logiciel PCI ou plus récente) |
| Espace sur le disque dur | 100 MB (plus jusqu'à 280 MB pour Microsoft .NET 2.0, s'il n'est pas déjà installé) |
| Logiciel de fournisseur | Microsoft .NET 2.0, inclus et installé avec le logiciel PC-GUI, s'il n'est pas déjà installé) Adobe® Reader® pour Windows® 7.0 ou une version plus récente n'est |
| Port USB | Port USB 1.1 ou 2.0 type A |

4.11.1.2 Installation du logiciel

☛ Le logiciel PCI peut être installé à partir du CD (fourni avec le contrôleur de sécurité) ou il peut être téléchargé à partir du site Internet de Banner Sales Force (<https://www.bannersalesforce.com/menu.php>).

Les instructions de démarrage sont aussi fournies avec le contrôleur de sécurité sous la forme du guide de démarrage rapide.



- 1) Insérer le CD dans le lecteur de CD de l'ordinateur.



- 2) Pour installer : Exécuter setup.exe, cliquer sur Install Software ou lancer le menu.
- 3) Redémarrer l'ordinateur pour activer toutes les fonctions.
- 4) Sortir le CD du lecteur

Au redémarrage du PC, l'icône *Banner* du contrôleur de sécurité



qui démarre le programme apparaît sur le plan de travail du PC.

5 INSTRUCTIONS DE FONCTIONNEMENT - PCI

5.1 TRAVAILLER AVEC LE PROGRAMME PCI

Le PCI du contrôleur de sécurité SC22-3 est l'outil principal pour créer et gérer les fichiers de configuration du contrôleur de sécurité. Il sert aussi à récupérer, afficher et enregistrer les E/S, l'état du système et les informations concernant les erreurs.

Les informations suivantes indiquent les étapes nécessaires à la création d'une configuration d'essai, en utilisant le PCI du contrôleur de sécurité. La configuration sert à définir les dispositifs d'entrées de sécurité et d'entrées auxiliaires à connecter au contrôleur de sécurité. Il sert aussi à établir les relations entre ces dispositifs d'entrées de sécurité/entrées auxiliaires et les Sorties de sécurité du contrôleur de sécurité.

5.1.1 Installation du logiciel PCI

Voir [Paragraphe 4.11.1 en page 36](#).

5.1.2 Démarrage du programme PCI

La procédure est la suivante :

- 1) Sur le bureau du PC, double cliquer sur l'icône *Banner* contrôleur de sécurité .
Ou bien
Dans le menu Démarrage, cliquer sur :
<Start> <All Programs> <Banner Engineering> <Banner Contrôleur de sécurité>
- 2)  Lire attentivement et comprendre les avertissements de la page de démarrage et cliquer sur **OK**.

Un nouveau fichier, sans nom, est créé comme illustré dans l'[Écran 3 en page 38](#).

5.1.2.1 Diagrammes et résumés

En cliquant sur chacun des trois documents de support, Diagramme de raccordement, Diagramme logique Ladder et Résumé de la configuration, on obtient les informations suivantes (voir l'Écran 3) :

- Diagramme de raccordement montre les bornes avec leur numéro, sans aucun élément du circuit logique en place. Seule la borne configurée par défaut est la borne du réarmement système (SR)
 - S1 à S22 pour les dispositifs d'entrée (à la fois de sécurité et auxiliaires)
 - A1 pour +24 Vcc et A2 pour 0 Vcc
 - O1 à O10 pour les indications du contrôleur et de l'état des E/S
 - SO1 (1A et 1B), SO2 (2A et 2B) et SO3 (3A et 3B) pour les connexions des sorties de sécurité
 - SR, le borne du réarmement système du contrôleur (indiqué par le symbole d'un bouton poussoir)
- Le diagramme logique Ladder montre les lignes verticales qui représentent +24 V et 0 Vcc et le circuit du réarmement système
- Résumé de la configuration ne montre que les réglages du système par défaut

The screenshot displays the 'Banner Safety Controller Interface' software with three main views:

- Diagramme de câblage (Wiring Diagram):** Shows a terminal block with terminals S1-S22, A1-A2, O1-O10, SR, SO1-SO3, and A2. It includes labels for 24Vdc and 0Vdc terminals and a note: "Les symboles sont représentés en utilisant la convention de signal d'état d'arrêt sauf les d'arrêt d'urgence, d'interrupteur à câble, d'interrupteur pour porte et tapis de sécurité." An arrow labeled '3' points to this view.
- Diagramme logique Ladder (Ladder Logic):** Shows a simple ladder logic circuit with a normally open contact and a coil. A note says: "Les symboles logiques ne s'affichent dans leur état normal." An arrow labeled '1' points to this view.
- Résumé de la Configuration (Configuration Summary):** Shows system parameters and the configuration name 'NEW FILE'. An arrow labeled '2' points to this view.

Index de l'écran

1. Diagramme logique Ladder
2. Résumé de la configuration
3. Diagramme de câblage

Écran 3

5.1.3 Outils de configuration

Écran 4 montre la barre d'outils qui sert à créer et à gérer les fichiers de configuration. En particulier, le bouton d'affichage live permet au PCI d'afficher en temps réel les données du mode Run d'un contrôleur de sécurité en fonctionnement par la connexion USB.

The screenshot displays the Banner Safety Controller Interface software. At the top, a toolbar contains seven numbered buttons: 1 (Receive), 2 (Send), 3 (Confirm), 4 (Add Security Entry), 5 (Add Non-Security Entry), 6 (Security Outputs), 7 (System Parameters). On the left, a sidebar lists 10 numbered items: 10 (Security Inputs), 11 (Non-Security Inputs), 12 (Security Outputs), and 13 (System Parameters). The main area shows a Ladder Logic diagram with 11 numbered components: 11 (Power supply), 12 (Reset), 13 (Security Outputs), 14 (Non-Security Outputs), 15 (Security Inputs), 16 (Non-Security Inputs), 17 (Security Outputs), 18 (Non-Security Outputs), 19 (Security Inputs), 20 (Non-Security Inputs), 21 (Security Outputs), and 22 (Non-Security Outputs). Below the diagram is a parameter table with 9 numbered sections: 9 (General), 10 (Security Inputs), 11 (Non-Security Inputs), 12 (Security Outputs), 13 (Non-Security Outputs), 14 (Security Inputs), 15 (Non-Security Inputs), 16 (Security Outputs), and 17 (Non-Security Outputs). To the right is a wiring diagram with 12 numbered components: 12 (Power supply), 13 (Reset), 14 (Security Outputs), 15 (Non-Security Outputs), 16 (Security Inputs), 17 (Non-Security Inputs), 18 (Security Outputs), 19 (Non-Security Outputs), 20 (Security Inputs), 21 (Non-Security Inputs), 22 (Security Outputs), and 23 (Non-Security Outputs).

Index de l'écran

| | | |
|---|---|--|
| 1. Les boutons envoyer, recevoir et confirmer passent en couleur quand un contrôleur de sécurité sous tension ou un outil de programmation est raccordé au PC | 4. Ajouter une entrée auxiliaire à la configuration | 9. Résumé de la configuration |
| 2. Accès à l'affichage live | 5. Accéder aux paramètres de la sortie de sécurité | 10. Propriétés des E/S – Double cliquer pour accéder aux paramètres de propriété |
| 3. Ajouter une entrée de sécurité à la configuration | 6. Accéder aux paramètres de la sortie d'état | 11. Chapitre documents |
| | 7. Accéder au paramètres du système | 12. Diagramme de câblage |
| | 8. Diagramme logique Ladder | |

Écran 4

5.1.4 Création d'une nouvelle configuration

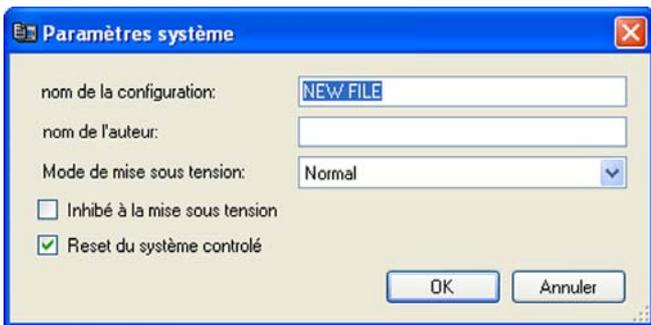
1) Double cliquer sur l'icône *Banner* Contrôleur de sécurité 

À ce point, on peut remplir le nom de la configuration et le nom de l'auteur ainsi que les paramètres du système.

2) Double cliquer sur l'icône des paramètres système



Écran 5 en page 40 est illustré.



Écran 5

3) Remplir le champ nom de la configuration au moyen de caractères alphanumériques (maximum 16).

4) Remplir le champ nom de l'auteur (10 caractères maximum).

5) Conserver ou modifier les paramètres du système par défaut :
 Mode de mise sous tension : Automatique, Manuel ou Normal (par défaut), voir [Paragraphe 2.5.3 en page 16](#)

Inhibé à la mise sous tension : Coché = ON ou décoché = OFF (par défaut), voir [Paragraphe 2.5.3 en page 16](#)

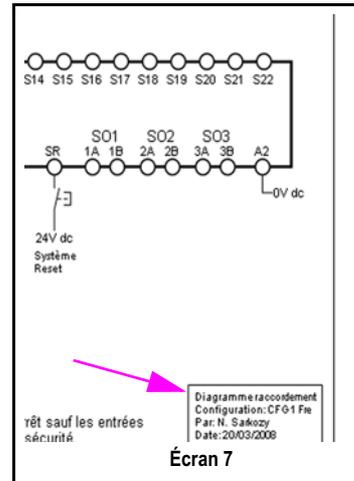
Reset du système contrôlé: Décoché = OFF ou coché = ON (par défaut), [Paragraphe 1.10 en page 5](#)



Écran 6

6) Puis cliquer sur **OK** ([Écran 6 en page 40](#)).

Les indications de nom apparaissent aussi maintenant dans l'écran principal ([Écran 7 en page 40](#)).



5.1.5 Ajout de dispositifs d'entrée de sécurité et d'entrée auxiliaire

[Tableau 11 en Page 40](#) indique les dispositifs d'entrée de sécurité et d'entrée auxiliaire qui peuvent être configurés avec le Contrôleur de sécurité SC22-3.

Tableau 11 Dispositifs des Entrées de sécurité & Entrées auxiliaires configurables

|  Entrées de sécurité |  Entrées auxiliaires |
|--|---|
| <ul style="list-style-type: none"> • Bouton d'arrêt d'urgence • Interrupteur à câble • Interrupteur pour porte (verrouillage) • Capteur optique – détecteurs mono ou multi-faisceaux, barrière immatérielle, scanners de zone, etc. • Dispositif de commande bimanuelle • Tapis sensible de sécurité • Arrêt de protection – dispositif divers • Dispositif de commande • Capteur d'inhibition • Interrupteur de bypass • EDM | <ul style="list-style-type: none"> • Interrupteur de réarmement manuel • Interrupteur ON/OFF • Interrupteur d'inhibition |

Se référer à [Annexe A2](#) pour plus d'informations sur les types de dispositifs d'entrée de sécurité.

Pour ajouter une entrée de sécurité:

- 1) Cliquer sur l'icône Ajouter dispositif d'entrée de sécurité



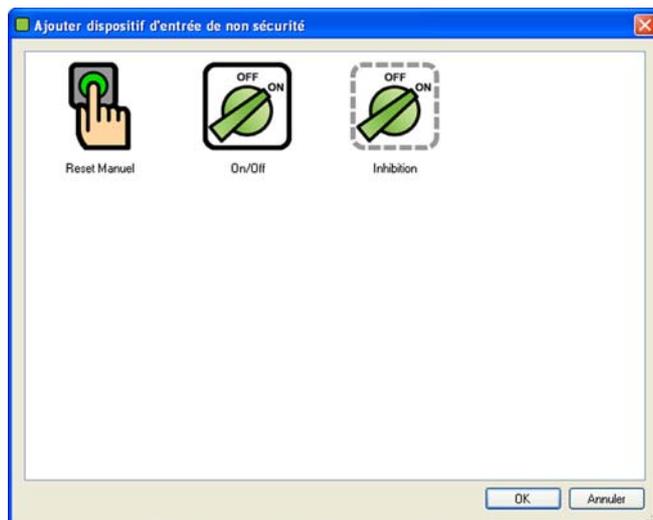
Écran 8

Écran 8 en page 41 affiche les types de dispositifs d'entrée de sécurité que le contrôleur de sécurité peut gérer.

- 2) Cliquer sur l'icône correspondant pour sélectionner le dispositif et cliquer sur **OK** (ou double cliquer sur l'icône).

Pour ajouter une entrée auxiliaire (entrée de non sécurité)

- 3) Cliquer sur l'icône Ajouter dispositif d'entrée de non sécurité



Écran 9

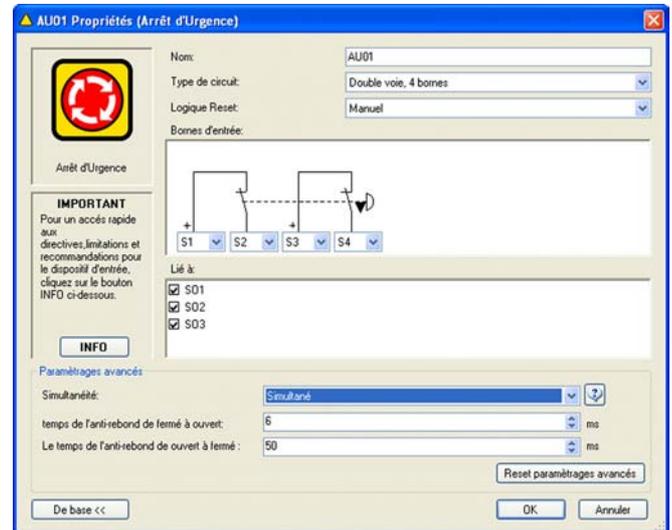
5.1.6 Sélection des entrées de sécurité

Pour le contexte et une explication des propriétés, se référer au [Paragraphe 1.9 en page 4](#) et [Paragraphe 4.5 en page 27](#).

Quand une entrée de sécurité est sélectionnée, le menu de ses propriétés s'affiche. Ce menu présente les propriétés qui doivent être établies pour chaque type d'entrée de sécurité.

5.1.6.1 Ajouter un arrêt d'urgence

- 1) Dans le menu Ajouter dispositif d'entrée de sécurité ([Écran 8 en page 41](#)) cliquer sur l'icône appropriée  et cliquer sur **OK** (ou double cliquer sur l'icône). [Écran 10 en page 41](#) est illustré.



Écran 10

Si on ne veut **PAS** utiliser les paramètres par défaut, procéder comme suit :

- 2) Entrer le nom : par ex. **ES01**.
Tout dispositif d'entrée de sécurité peut obtenir un nouveau nom pendant le processus de configuration.
- 3) Sélectionner le type de circuit correspondant au dispositif désigné : par ex. double voie, 4 bornes.

Le type de circuit sélectionné apparaît dans le diagramme des bornes des Entrées de sécurité qui assigne automatiquement les numéros de bornes. Les numéros des bornes peuvent être réassignés en utilisant le menu déroulant. Le signe plus de **S1** et de **S3** (voir [Écran 10 en page 41](#)) indique que ces bornes fournissent une source en +24 Vcc pour les contacts des dispositifs.

Pour plus d'informations sur les niveaux d'intégrité des circuits de sécurité et les capacités de chaque type de circuit voir [Annexe A2](#).

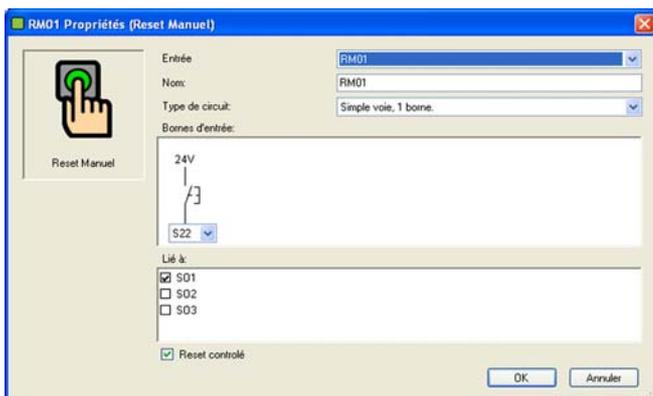
- 4) Configurer la logique de réarmement: par ex. manuelle.
- 5) Dans le menu déroulant, sélectionner bornes d'entrée: par ex. **S1**, **S2**, **S3** et **S4** (utiliser les champs des numéros des bornes déroulants pour changer l'assignation de la borne, le cas échéant).
- 6) Configurer assigné à : Cocher ou non les cases pour assigner chaque entrée de sécurité à une ou plusieurs sorties de sécurité, par ex. **SO1**, **SO2** et **SO3** (il faut au moins en choisir une).
- 7) Si on ne veut **PAS** utiliser les paramètres par défaut, cliquer sur : Paramètres avancés
 Cocher ou non la case Activer le test de démarrage
 Choisir Simultanéité:
 Choisir Temps de l'anti-rebond fermé à ouvert :
 Choisir Temps de l'anti-rebond ouvert à fermé :
- 8) Une fois terminé, cliquer sur **OK** pour sortir.

Parce qu'un signal de réarmement manuel a été choisi pour le bouton d'arrêt d'urgence, quand on clique sur OK et que le menu des propriétés **ES01** se ferme, l'écran de réarmement manuel des propriétés de **RS01** apparaît automatiquement (Écran 11 en page 42) pour ajouter un dispositif d'entrée de réarmement manuel à ce dispositif. Toute entrée de sécurité qui conserve la configuration manuelle de la logique de réarmement a besoin d'un réarmement manuel pour chaque sortie de sécurité assignée à ce dispositif. Un réarmement manuel séparé peut être assigné à chaque sortie de sécurité.

☛ Si l'entrée de sécurité est une paire de capteurs d'inhibition ou un interrupteur de bypass, ces entrées doivent être assignées à au moins une des autres entrées de sécurité.

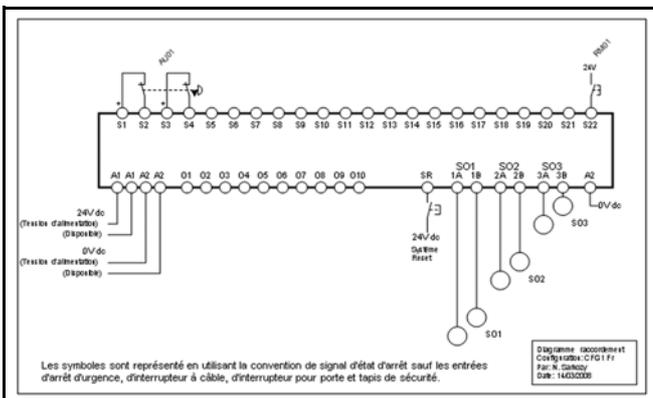
Si on ne veut **PAS** utiliser les paramètres par défaut, procéder comme suit :

- 9) Nom : par ex. **RS01**.
- 10) Sélectionner le type de circuit approprié : par ex. Simple voie, 2 bornes.
- 11) Dans le menu déroulant, sélectionner les bornes d'entrée : par ex. **S21** et **S22**.
- 12) Cocher ou non assigné à : par ex. **SO1**, **SO2** et **SO3**.
- 13) Cocher ou non Reset contrôlé.
- 14) Une fois terminé, cliquer sur **OK** pour sortir.

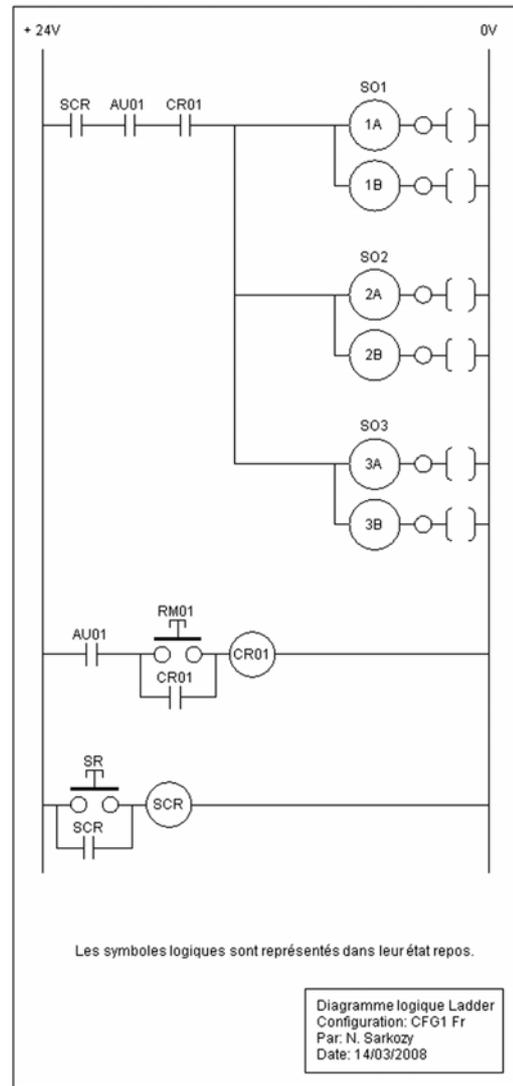


Écran 11

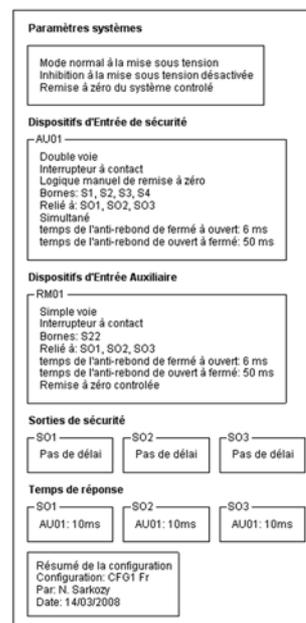
Au fur et à mesure que les propriétés sont sélectionnées, le diagramme de raccordement commence à se remplir (Écran 12 en page 42) avec les entrées de sécurité sélectionnées ainsi que le diagramme logique Ladder (Écran 13 en page 42) et le résumé de la configuration (Écran 14 en page 42).



Écran 12



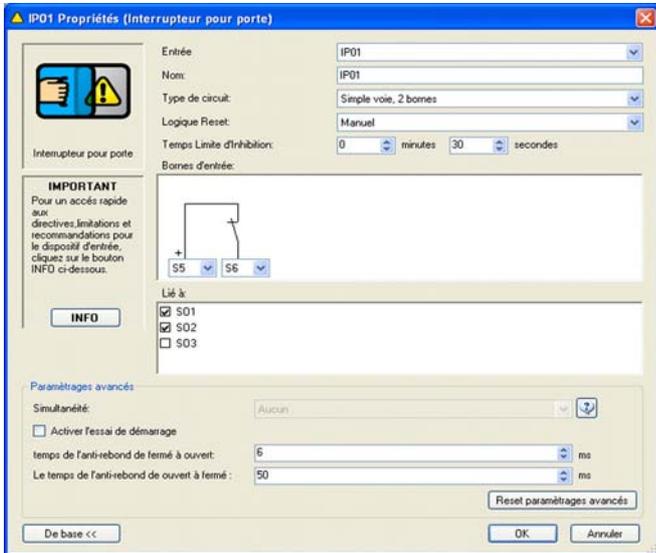
Écran 13



Écran 14

5.1.6.2 Ajout d'un interrupteur pour porte

- 1) Dans le menu Ajouter dispositif d'entrée de sécurité (Écran 8 en page 41) cliquer sur l'icône appropriée  et cliquer sur **OK** (ou double cliquer sur l'icône). Écran 15 en page 43 est illustré.



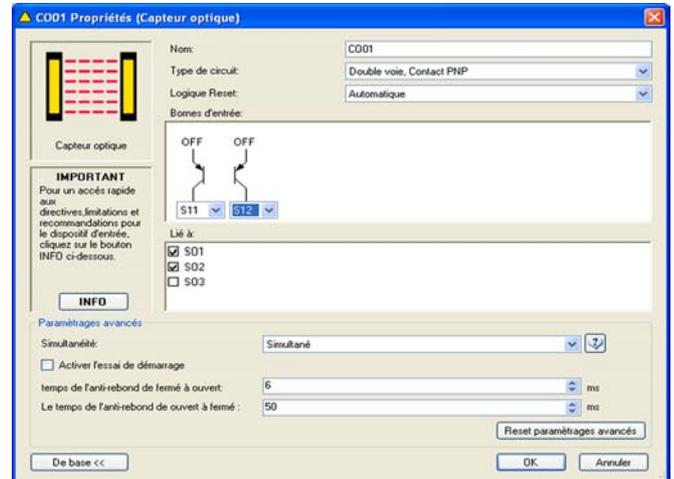
Écran 15

Si on ne veut **PAS** utiliser les paramètres par défaut, procéder comme suit :

- 2) Entrer un nom : par ex. **GS01**.
- 3) Sélectionner le type de circuit : simple voie, 2 bornes.
- 4) Configurer la logique de réarmement: par ex. manuelle.
- 5) Dans le menu déroulant, sélectionner les bornes d'entrée : par ex. **S5, S6**.
- 6) Configurer assigné à : par ex. **S01 et S02**.
- 7) Si on ne veut **PAS** utiliser les paramètres par défaut, cliquer sur : Paramètres avancés
Cocher ou non la case Activer le test de démarrage
Choisir Simultanéité:
Choisir Temps de l'anti-rebond fermé à ouvert :
Choisir Temps de l'anti-rebond ouvert à fermé :
- 8) Une fois terminé, cliquer sur **OK** pour sortir.

5.1.6.3 Ajout d'un capteur optique

- 1) Dans le menu Ajouter dispositif d'entrée de sécurité (Écran 8 en page 41) cliquer sur l'icône appropriée  et cliquer sur **OK** (ou double cliquer sur l'icône). Écran 16 en page 43 est illustré.



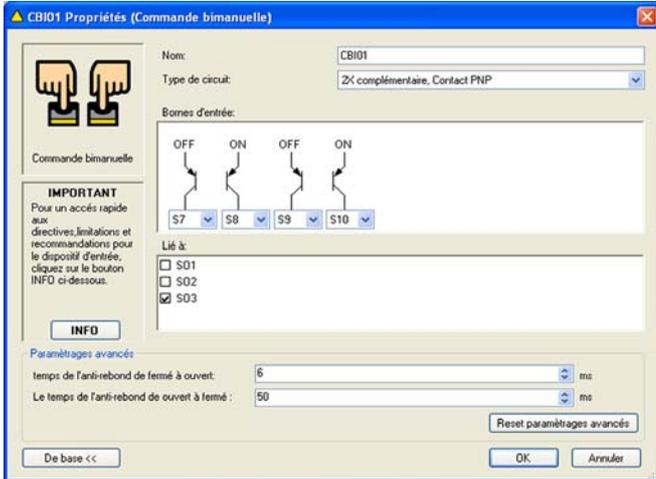
Écran 16

Si on ne veut **PAS** utiliser les paramètres par défaut, procéder comme suit :

- 2) Entrer un nom : par ex. **OS01**.
- 3) Sélectionner le type de circuit approprié : double voie, contact PNP.
- 4) Configurer la logique de réarmement : par ex. automatique.
- 5) Dans le menu déroulant, sélectionner les bornes d'entrée : par ex. **S11 et S12**.
- 6) Configurer assigné à : par ex. **S01 et S02**.
- 7) Si on ne veut **PAS** utiliser les paramètres par défaut, cliquer sur : Paramètres avancés
Cocher ou non la case Activer le test de démarrage
Choisir Simultanéité:
Choisir Temps de l'anti-rebond fermé à ouvert :
Choisir Temps de l'anti-rebond ouvert à fermé :
- 8) Une fois terminé, cliquer sur **OK** pour sortir.

5.1.6.4 Ajout d'une commande bimanuelle

- 1) Dans le menu Ajouter dispositif d'entrée de sécurité (Écran 8 en page 41) cliquer sur l'icône appropriée  et cliquer sur **OK** (ou double cliquer sur l'icône). Écran 17 en page 44 est illustré.



Écran 17

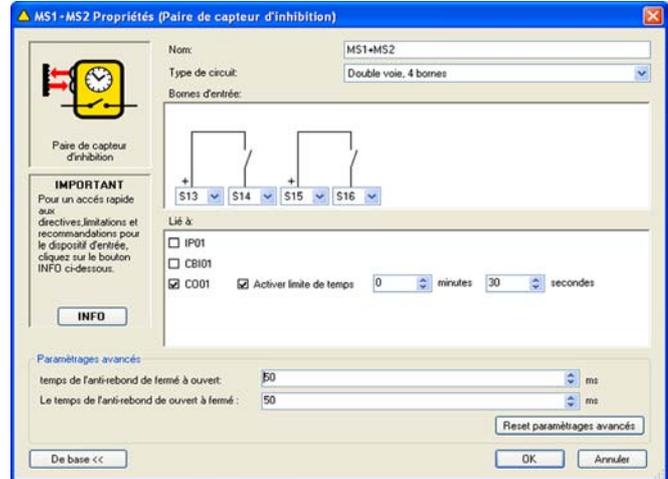
Si on ne veut **PAS** utiliser les paramètres par défaut, procéder comme suit :

- 2) Entrer un nom : par ex. **THC01**.
- 3) Sélectionner le type de circuit approprié : 2X complémentaire, contact PNP.
- 4) Dans le menu déroulant, sélectionner les bornes d'entrée : par ex. **S7, S8, S9 et S10**.
- 5) Configurer assigné à : par ex. **SO3**.
- 6) Si on n'utilise **PAS** les paramètres par défaut, cliquer sur : *Paramètres avancés*
Configurer le temps de l'anti-rebond de fermé à ouvert :
Configurer le temps de l'anti-rebond de ouvert à fermé :
- 7) Une fois terminé, cliquer sur **OK** pour sortir.

☛ La logique de réarmement est configurée sur automatique pour les dispositifs de commande bimanuelle. Il n'y a pas d'autre possibilité de réarmement.

5.1.6.5 Ajout d'une paire de capteurs d'inhibition

- 1) Dans le menu Ajouter dispositif d'entrée de sécurité (Écran 8 en page 41) cliquer sur l'icône appropriée  et cliquer sur **OK** (ou double cliquer sur l'icône). Écran 18 en page 44 est illustré.



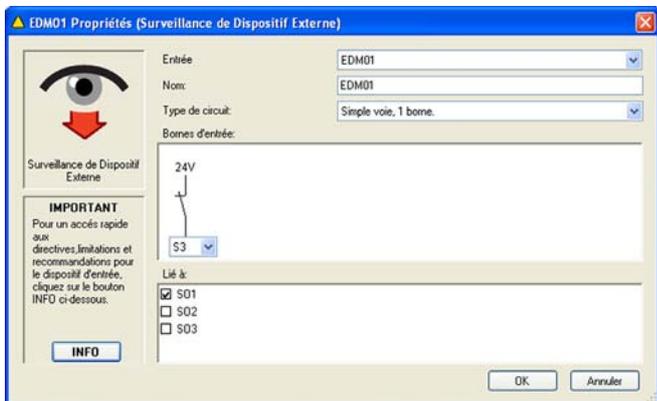
Écran 18

Si on ne veut **PAS** utiliser les paramètres par défaut, procéder comme suit :

- 2) Entrer un nom : par ex. **M1+M2**.
- 3) Sélectionner le type de circuit approprié : double voie, 4 bornes.
- 4) Dans le menu déroulant, sélectionner les bornes d'entrée : par ex. **S13, S14, S15 et S16**.
- 5) Configurer assigné à : par ex. **OSO1**.
- 6) Si on n'utilise **PAS** les paramètres par défaut, cliquer sur : *Paramètres avancés*
Configurer le temps de l'anti-rebond de fermé à ouvert :
Configurer le temps de l'anti-rebond de ouvert à fermé :
- 7) Une fois terminé, cliquer sur **OK** pour sortir.

5.1.6.6 Ajout d'une surveillance de dispositif externe

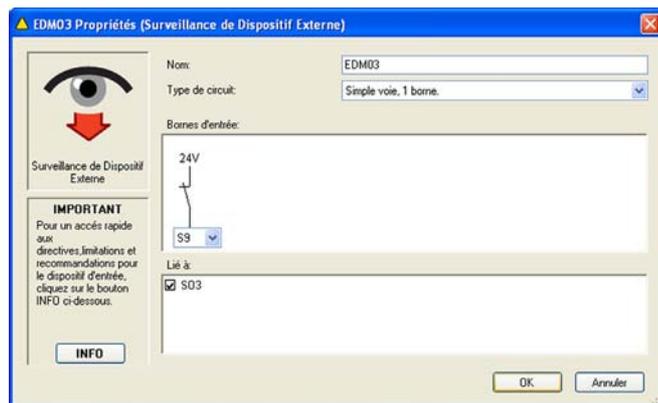
- 1) Dans le menu Ajouter dispositif d'entrée de sécurité (Écran 8 en page 41) cliquer sur l'icône appropriée  et cliquer sur **OK** (ou double cliquer sur l'icône). Écran 19 en page 45 est illustré.



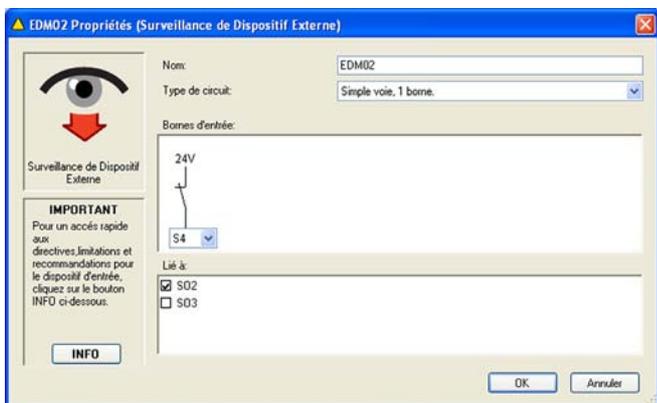
Écran 19

Si on ne veut **PAS** utiliser les paramètres par défaut, procéder comme suit :

- 2) Entrer un nom : par ex. **EDM01**.
- 3) Sélectionner le type de circuit approprié : simple voie, 1 borne.
- 4) Dans le menu déroulant, sélectionner les bornes d'entrée : par ex. **S17**.
- 5) Configurer assigné à : par ex. **SO1**.
- 6) Une fois terminé, cliquer sur **OK** pour sortir.
- 7) Ajouter deux entrées de sécurité de surveillances de dispositifs externes de plus, une pour chaque sortie de sécurité comme illustré en Écran 20 en page 45 et Écran 21 en page 45, comme suit :
 - Les appeler **EDM02** et **EDM03**
 - Utiliser les types de circuits simple voie, 1 borne pour chacune
 - Assigner les bornes d'entrée **S18** à **EDM02** et **S19** à **EDM03** assigné à **SO2** pour **EDM02** et à **SO3** pour **EDM03**



Écran 21



Écran 20

5.1.7 Ajouter des dispositifs d'entrée auxiliaire

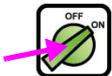
Pour l'explication des propriétés, se référer à [Paragraphe 4.6 en page 30](#).

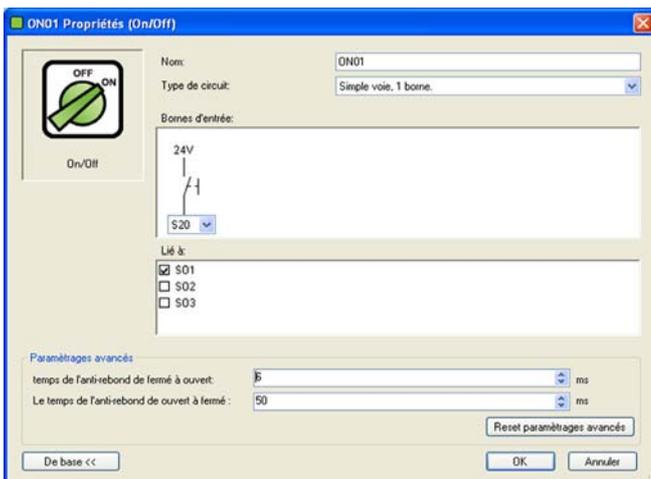
Quand un dispositif d'entrée auxiliaire est sélectionné, le menu des propriétés s'affiche ([Écran 22 en page 46](#)). Ce menu présente les propriétés qui doivent être établies pour chaque type d'entrée auxiliaire. Les propriétés définies par l'utilisateur, en fonction du dispositif, sont les suivantes :

- Nom — Le nom (ou la désignation du circuit) de chaque dispositif spécifique (pas le type de dispositif)
- Type de circuit — Une liste des types de contacts ou circuits intégrés qui peuvent être utilisés pour ce dispositif
- Assigné à — établit les relations entre les dispositifs d'entrée auxiliaire et les sorties

5.1.7.1 Ajouter un interrupteur ON/OFF

- 1) Dans le menu ajouter une entrée auxiliaire ([Écran 8 en page 41](#))

cliquer sur l'icône appropriée  et cliquer sur OK (ou double cliquer sur l'icône) comme illustré en [Écran 22 en page 46](#).



Écran 22

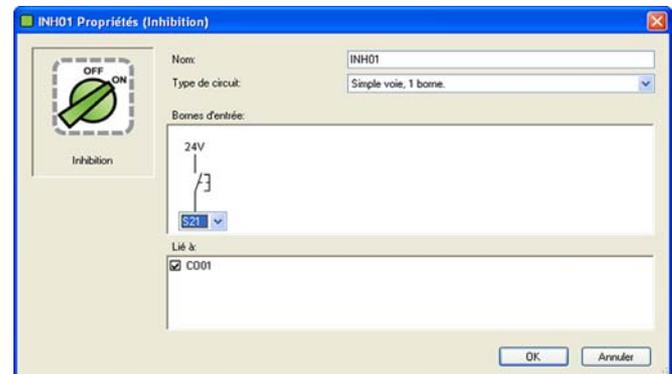
Si on n'utilise pas les paramètres par défaut, procéder comme suit :

- 2) Entrer un nom : par ex. ON01.
- *Tout dispositif d'entrée auxiliaire peut être renommé pendant le processus de configuration.*
- 3) Sélectionner le type de circuit approprié : au dispositif désigné. Le type de circuit sélectionné apparaît dans le diagramme de raccordement avec des numéros de bornes assignés automatiquement.
- *Voir Annexe A2 pour plus d'informations sur les niveaux d'intégrité des circuits de sécurité et les capacités de chaque type de circuit.*
- 4) Dans le menu déroulant, sélectionner les bornes d'entrée : par ex. **S20**.
- 5) Configurer assigné à : par ex. **SO1**.
- 6) Si on n'utilise pas les paramètres par défaut :
Paramètres avancés
Configurer le temps d'anti-rebond de fermé à ouvert :
Configurer le temps d'anti-rebond d'ouvert à fermé :
- 7) Une fois terminé, cliquer sur **OK** pour sortir.

5.1.7.2 Ajout d'un interrupteur d'inhibition

- 1) Dans le menu ajouter une entrée auxiliaire ([Écran 8 en page 41](#))

cliquer sur l'icône appropriée  et cliquer sur OK (ou double cliquer sur l'icône) comme illustré en [Écran 23 en page 46](#).



Écran 23

Si on n'utilise pas les paramètres par défaut, procéder comme suit :

- 2) Entrer le nom : par ex. **ME01**.
- *Tout dispositif d'entrée auxiliaire peut être renommé pendant le processus de configuration.*
- 3) Sélectionner le type de circuit approprié : simple voie, 1 borne. Le type de circuit sélectionné apparaît dans le diagramme de raccordement avec des numéros de bornes assignés automatiquement.
- 4) Dans le menu déroulant, sélectionner les bornes d'entrée : par ex. **S20**.
- *Voir Annexe A2 pour plus d'informations sur les niveaux d'intégrité des circuits de sécurité et les capacités de chaque type de circuit.*
- 5) Assigné à : Cocher ou non les cases pour assigner chaque entrée auxiliaire à une ou plusieurs Sorties de sécurité (il faut au moins en sélectionner une).
- 6) Une fois terminé, cliquer sur **OK** pour sortir.

5.1.8 Assignation des sorties de sécurité

Les sorties de sécurité sont assignées individuellement à chaque sortie de sécurité.

- 1) Cliquer sur l'icône sortie de sécurité . Écran 24 est illustré.
- 2) Dans le menu déroulant, sélectionner sortie de sécurité : par ex. **SO1**.
- 3) Entrer le nom : par ex. **SO1**.
- 4) Sélectionner le type de délai : Aucun, délai à l'enclenchement ou délai au déclenchement (pour les informations, se référer à [Paragraphe 2.5.1.3 en page 14](#)).
- 5) Une fois terminé, cliquer sur **OK** pour sortir.

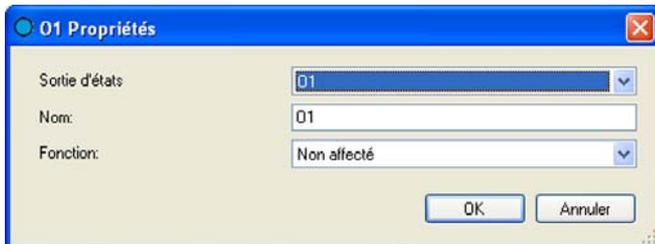


Écran 24

5.1.9 Configurer les sorties d'état

Le contrôleur de sécurité a 10 sorties d'état configurables (pour info, se référer à [Paragraphe 2.5.2 en page 15](#) et [Paragraphe 4.9.1 en page 35](#)).

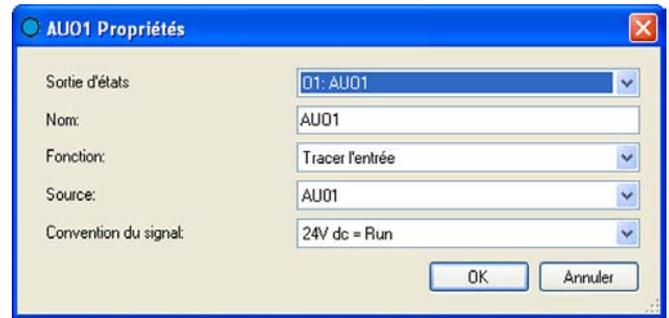
- 1) Cliquer sur l'icône sortie d'état . Écran 25 est illustré



Écran 25

- 2) Dans le menu déroulant, sélectionner sortie d'état : par ex. **O1**.
- 3) Entrer un nom : par ex. **ESO1**.
- 4) Sélectionner une fonction : Tracer l'entrée (pour info, se référer au [Paragraphe 2.5.2 en page 15](#) et [Paragraphe 4.9.1 en page 35](#)).
- 5) Sélectionner une source : par ex. **ESO1**.

- 6) Sélectionner une convention du signal...: par ex. 24 Vcc = Run. Écran 26 est illustré.



Écran 26

- 7) Une fois terminé, cliquer sur **OK** pour sortir.

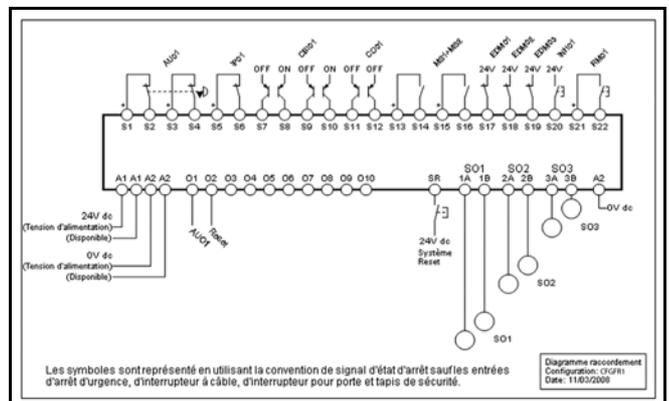
Ajouter une sortie d'état supplémentaire

- 8) Cliquer sur l'icône sortie d'état . Écran 27 est illustré.
- 9) Dans le menu déroulant, sélectionner sortie d'état : par ex. **O2**.
- 10) Entrer un nom : par ex. **Reset**.
- 11) Sélectionner une fonction : Sortie en attente de reset.
- 12) Sélectionner une source : par ex. **SO1**.
- 13) Sélectionner une convention du signal...: par ex. 24 Vcc = Run. Écran 27 est illustré.



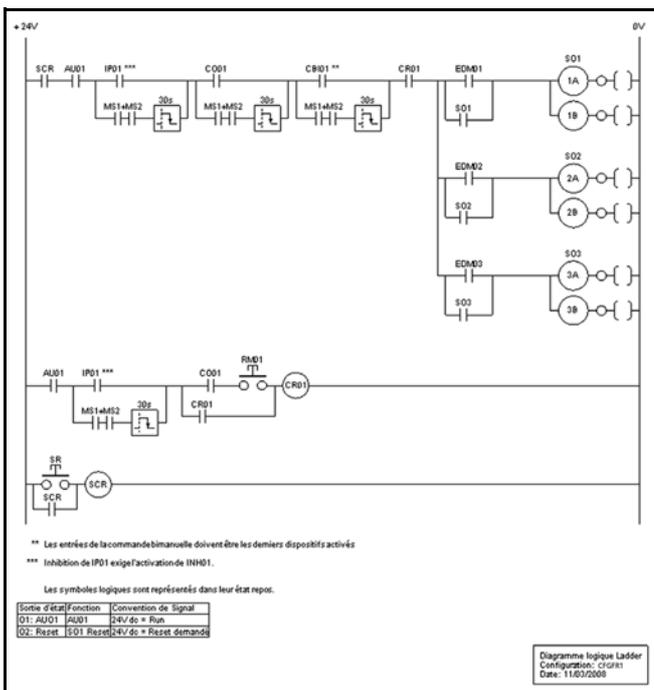
Écran 27

- 14) Une fois terminé, cliquer sur **OK** pour sortir.
- Le diagramme de raccordement doit être comme celui illustré en [Écran 28](#).



Écran 28

Le diagramme logique Ladder doit être comme celui illustré en Écran 29.



Écran 29

5.1.10 Confirmation de la configuration

La nouvelle configuration doit être confirmée avant de pouvoir l'utiliser dans une application de protection application et le contrôleur de sécurité SC22-3 doit être raccordé au PC par le câble USB.

Le processus de confirmation se fait en deux parties :

Validation de la configuration Le contrôleur de sécurité reçoit une copie de la configuration qu'il vérifie automatiquement pour s'assurer que tous les paramètres critiques de sécurité sont corrects.

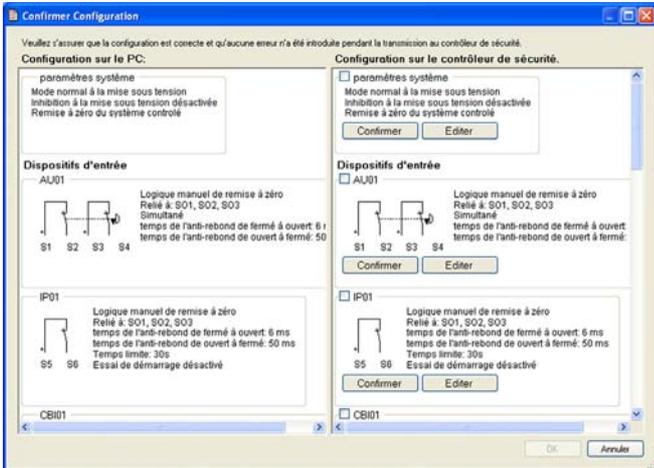
Vérification de la configuration Le contrôleur de sécurité renvoie une copie de la configuration au PC pour le processus de configuration manuel définitif.

5.1.10.1 Validation de la configuration

Pour confirmer une configuration **CFG1**, suivre les étapes suivantes :

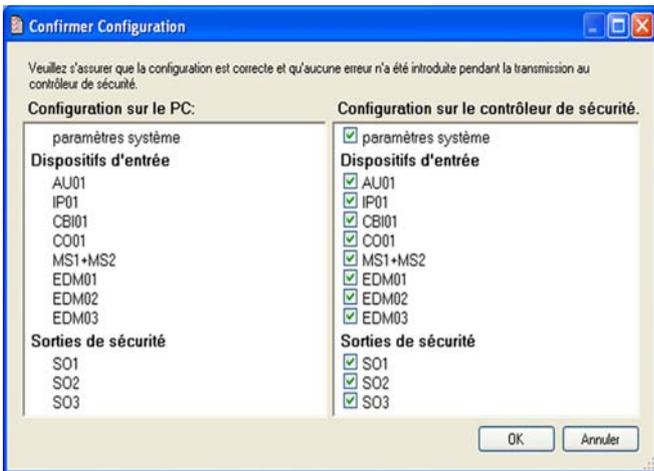
- 1) Enregistrer le fichier de la configuration sur le PC.
Cliquer sur fichier > Enregistrer.
Donner un nom au fichier de la configuration par ex. **CFG1** et sélectionner un emplacement de fichier sur l'ordinateur.
Cliquer sur enregistrer.
- 2) Utiliser le câble USB pour raccorder le contrôleur de sécurité SC22-3 au PC (voir [Paragraphe 4.3.2 en page 26](#)).
- 3) Mettre le Contrôleur de sécurité sous tension de 24 Vcc.
- 4) Vérifier que les boutons Recevoir, Envoyer et Confirmer () de la barre d'outil de PCI sont activés en changeant d'un niveau de gris à la couleur.
- 5) Cliquer sur le bouton Confirmer .
- 6) Le contrôleur utilisé pendant le processus de confirmation peut avoir déjà une configuration existante (soit par défaut d'usine, soit définie par l'utilisateur). Toute configuration déjà chargée dans le contrôleur est écrasée (et donc perdue) pendant le processus de confirmation. L'utilisateur a donc la responsabilité d'enregistrer les configurations existantes, le cas échéant.
- 6) Dans le menu déroulant enregistrer la configuration, sélectionner oui pour enregistrer la configuration ou Non pour écraser la configuration existant dans le contrôleur.
- 7) Dans le menu déroulant Confirmer la configuration (Écran 31), entrer le mot de passe (le mot de passe par défaut d'usine est 0000) et cliquer sur **OK**.
- 8) Un message d'avertissement apparaît pour demander si on veut continuer, sélectionner oui.

Attendre quelques secondes que le processus de validation de la configuration se termine. L'écran de vérification de la configuration apparaît alors (voir Écran 30).



Écran 30

- 9) Vérifier que les propriétés de la colonne de droite correspondent à celles de la colonne de gauche. Pour chaque dispositif, au fur et à mesure que l'on vérifie que les propriétés sont correctes, cliquer soit sur Confirmer soit dans la case correspondante. Une marque de coche apparaît dans la case et la section se comprime en une liste, comme illustré en Écran 31.



Écran 31

5.1.10.2 Modification de la configuration

Si les colonnes ne correspondent pas ou si on désire un circuit différent :

- 1) Sélectionner Modifier pour le dispositif à changer (Écran 30 est illustré).

Le menu des propriétés de ce dispositif s'ouvre (par ex. Écran 15).

- 2) Effectuer les modifications nécessaires.
- 3) Une fois terminé, cliquer sur **OK** pour sortir.
- 4) Au message demandant si d'autres dispositifs doivent être modifiés ou s'il faut continuer le processus de confirmation, cliquer ce qui convient.

☛ Si une propriété d'un dispositif est modifiée pendant l'étape de vérification manuelle, le contrôleur revalide le code.

Si les colonnes correspondent et qu'il n'y a plus de modification à faire :

- 5) Dans le Écran 30 sélectionner Confirmer pour chaque dispositif. L'écran de vérification (Écran 31) affiche le résumé qui est créé après que chaque propriété a été vérifiée.

Pour vérifier les propriétés d'un dispositif confirmé :

- 6) Dans le Écran 31, décocher la case et le menu déroulant des propriétés du dispositif apparaît. Effectuer les modifications nécessaires.
- 7) Quand la vérification manuelle est terminée, cliquer sur **OK** pour sortir.

À la fin du processus de vérification, le menu déroulant de Confirmer la configuration (Écran 31) s'affiche à nouveau

- 8) Cliquer sur fermer.
- 9) Effectuer un réarmement système (voir [Paragraphe 5.1.11 en page 49](#)).

Le contrôleur active la nouvelle configuration et fonctionne selon les nouveaux paramètres.

5.1.11 Réarmement du système

Dans certaines conditions, le contrôleur de sécurité nécessite un réarmement du système pour les raisons suivantes :

- Pour mettre le contrôleur en mode Run après sa configuration
- Pour récupérer après certaines conditions (par ex. Blocages)

Pour effectuer un réarmement du système, soit :

- 1) Envoyer un signal de 24 Vcc dans une entrée de réarmement du système (**SR**) (Écran 28 est illustré).

ou

- 2) Couper et rétablir l'alimentation électrique.

Quand la configuration est confirmée, le contrôleur passe en mode Run.

5.1.12 Modification d'une configuration existante

Pour modifier une configuration existante :

- 1) Dans le PC, double cliquer sur l'icône du programme contrôleur de sécurité *Banner* .

- 2) Dans le menu, cliquer sur fichier, puis sur ouvrir ou cliquer sur l'icône  pour faire défiler le fichier de configuration à modifier. Faire les modifications selon les instructions du [Paragraphe 5.1 en page 37](#).

5.1.13 Réception d'une configuration depuis un contrôleur de sécurité SC22-3

Pour recevoir une configuration d'un contrôleur de sécurité SC22-3 et l'afficher dans le PCI :

- 1) Raccorder le contrôleur de sécurité SC22-3 au PC.
- 2) Dans le PC double cliquer sur l'icône du programme du contrôleur de sécurité *Banner*. 
- 3) Appliquer une alimentation en 24 Vcc au contrôleur.
- 4) Dans la barre d'outils, cliquer sur le bouton recevoir .
- 5) Si la configuration n'est pas déjà confirmée, confirmer la configuration comme illustré dans [Écran 31](#).

5.1.14 Envoi d'une configuration au contrôleur de sécurité SC22-3

Pour envoyer une configuration depuis le PCI à un contrôleur de sécurité SC22-3 :

- 1) Avec le câble USB, raccorder le contrôleur de sécurité SC22-3 au PC.
- 2) Appliquer une alimentation en 24 Vcc au contrôleur.
- 3) Dans le PC double cliquer sur l'icône du programme du contrôleur de sécurité *Banner*. 

- 4) Dans la barre d'outil, cliquer sur le bouton envoyer .

5.1.15 Ouvrir une configuration à partir de la carte XM

Il est possible d'envoyer ou de recevoir des configurations, confirmées ou non, de ou vers la carte XM. Procéder comme suit :

- 1) Avec le câble USB, raccorder l'outil de programmation SC-XMP au PC.
- 2) Insérer la carte XM dans l'outil de programmation SC-XMP ([Figure 18 en page 26](#) est illustré).
- 3) Dans le PC, double cliquer sur l'icône du programme contrôleur de sécurité *Banner* .

- 4) Dans le menu, cliquer sur **fichier** puis sur **ouvrir** . Un message apparaît quand l'opération est terminée.

5.1.16 Envoi d'une configuration à la carte XM

Il est possible d'envoyer ou de recevoir des configurations, confirmées ou non, de ou vers la carte XM. Procéder comme suit :

- 1) Avec le câble USB, raccorder l'outil de programmation SC-XMP au PC ([Figure 18 en page 26](#) est illustré).
- 2) Insérer la carte XM dans l'outil de programmation SC-XMP ([Figure 19 en page 26](#)).
- 3) Dans le PC, double cliquer sur l'icône du programme contrôleur de sécurité *Banner* .

- 4) Dans le menu, cliquer sur **fichier**, ouvrir ou cliquer sur l'icône  pour faire défiler le fichier de configuration.

- 5) Dans le menu, cliquer sur **fichier** puis sur **envoyer à la carte XM**. Un message apparaît quand l'opération est terminée.

5.1.17 Verrouillage de la carte XM

PRÉCAUTION

Il est important de remarquer que cette opération ne peut pas être inversée. Quand la carte XM est verrouillée, on ne pourra jamais plus enregistrer une autre configuration dedans.

Cette opération est utilisée quand la carte XM et sa configuration sont utilisés sur un autre contrôleur de sécurité *Banner* ou pour sauvegarder et archiver une configuration.

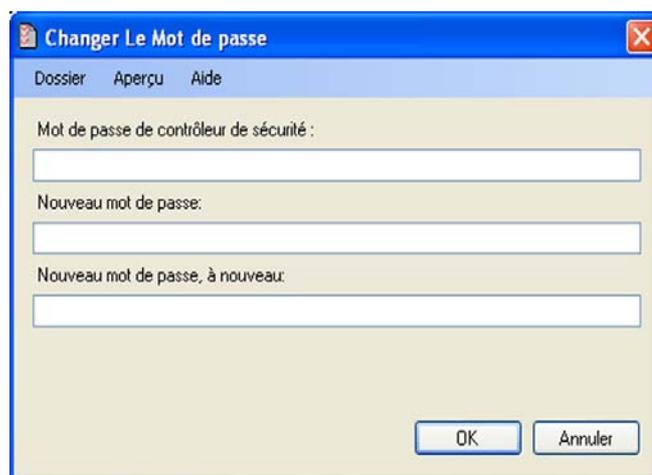
Pour verrouiller la carte XM de façon à ce que la configuration enregistrée ne puisse plus être modifiée :

- 1) Insérer la carte XM dans l'outil de programmation SC-XMP ([Figure 18 en page 26](#)).
- 2) Vérifier que le fichier enregistré sur la carte XM est le bon.
- 3) Dans le menu, cliquer sur **verrouiller la carte XM** (en haut à gauche de la barre d'outil).

Un message apparaît quand l'opération est terminée.

5.1.18 Changement du mot de passe en utilisant le PCI

- 1) Avec le câble USB, raccorder le PC au contrôleur de sécurité *Banner* ([Figure 19 en page 26](#)).
- 2) S'assurer que l'alimentation électrique du contrôleur de sécurité est **ON** (voyant vert .
- 3) Dans le PC, double cliquer sur l'icône du programme contrôleur de sécurité *Banner* .
- 4) Dans le menu, cliquer sur **fichier** puis sur **changer le mot de passe du contrôleur de sécurité**. [Écran 32](#) est illustré.



Écran 32

- 5) Renseigner les champs. Cliquer sur **OK**.

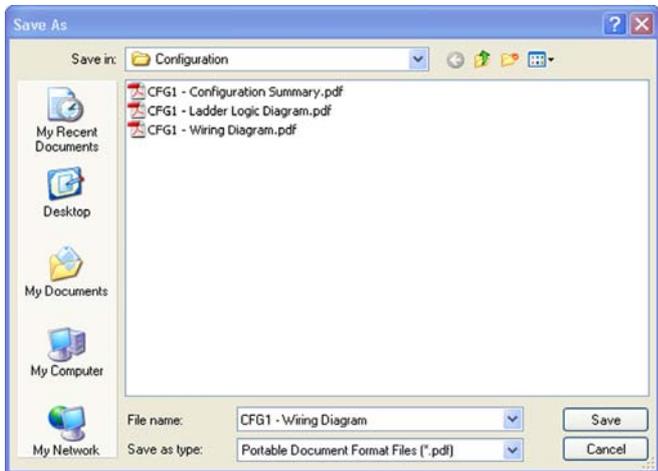
L'écran Entrée dans le mode de configuration s'affiche demandant "êtes-vous sûr ? Toutes les sorties de sécurité passeront sur off." Cliquer sur oui, toutes les sorties de sécurité passent sur OFF, en même temps que la machine ou le système qui est surveillé par le contrôleur de sécurité.

- 6) Cliquer sur **oui**. Écran 32 réapparaît.
- 7) Cliquer sur **fermer**. Le mot de passe est changé.
- 8) Noter le mot de passe de façon sûre.

☛ Si le mot de passe est perdu, contacter [Bureaux du siège social en page 125](#).

5.1.19 Exportation de documents

Les documents de configuration (diagramme de raccordement, diagramme logique Ladder et le résumé de la configuration) peuvent être sauvegardés sous forme de fichiers .pdf ou .dxf (voir Écran 33). Pour exporter un fichier de configuration :



Écran 33

- 1) Dans le PC, double cliquer sur l'icône du programme contrôleur de sécurité *Banner* .
- 2) Ouvrir le fichier de configuration à sauvegarder.
- 3) Dans le menu, cliquer sur fichier puis sur export.
- 4) Sélectionner le document de configuration à exporter.
- 5) Vérifier que le nom est correct et sélectionner l'option de fichier de type sauvegarder sous et l'option de type de fichier (.pdf ou .dxf).
- 6) Sélectionner Fait.

5.1.20 Impression

Pour imprimer un fichier de configuration :

- 1) Dans le PC, double cliquer sur l'icône du programme contrôleur de sécurité *Banner* .
 - 1) Ouvrir le fichier de configuration à imprimer.
 - 2) Dans le menu, cliquer sur fichier puis sur **imprimer**.
 - 3) Sélectionner le document de configuration (diagramme de raccordement, diagramme logique Ladder et Résumé de la configuration).
 - 4) Quand le menu Configuration des pages apparaît, choisir les pages et l'imprimante, puis cliquer sur **OK**.

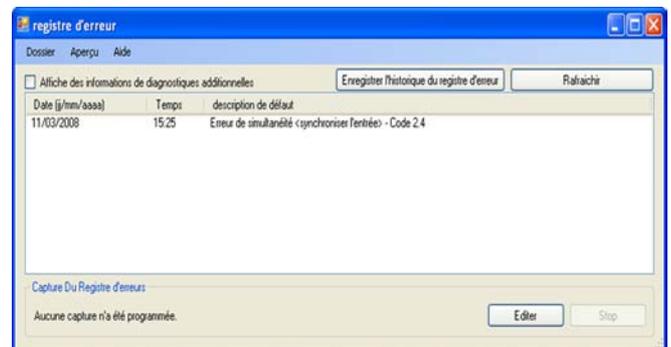
☛ Les diagrammes de raccordement, diagrammes logiques Ladder et résumé de la configuration sont plus faciles à mettre en page en format "paysage". Les autres documents sont tous au format "portrait."

5.1.21 Accès au registre d'erreurs

Pour accéder au registre d'erreurs interne au contrôleur en utilisant PCI:

- 1) Avec le câble USB, raccorder le PC au contrôleur de sécurité *Banner* (Figure 19 en page 26).
- 2) Mettre le contrôleur sous tension de 24 Vcc.
- 3) Cliquer sur le menu aperçu de la barre d'outils du PCI.
- 4) Sélectionner registre d'erreurs.

Écran 34 apparaît et affiche les erreurs d'E/S ou du système détectées par le contrôleur de sécurité.



Écran 34

5.1.22 Capture programmée du registre d'erreurs

Les informations d'erreurs des E/S et du système du contrôleur peuvent être enregistrées dans un fichier informatique. Pour configurer un délai de capture des données depuis un contrôleur de sécurité, depuis le menu registre d'erreurs.

- 1) Avec le câble USB, raccorder le PC au contrôleur de sécurité *Banner* (Figure 19 en page 26).
- 2) Appliquer une alimentation en 24 Vcc au contrôleur de sécurité.
- 3) Cliquer sur le menu aperçu.
- 4) Sélectionner registre d'erreurs.
- 5) Sélectionner le bouton modifier. Écran 35 est illustré.



Écran 35

- 6) Depuis les champs déroulants, configurer les temps de début et de fin.
- 7) Cliquer sur Passer en revue pour l'emplacement du fichier location.
- 8) Cliquer sur **OK**.

Les données d'erreurs sont enregistrées sous forme de fichier Excel file à cet emplacement.

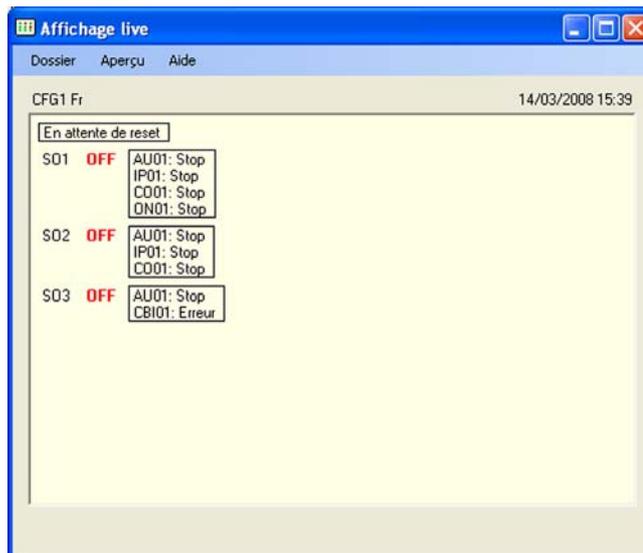
5.1.23 Affichage live

Pour accéder en live aux informations du contrôleur à partir du PCI:

- 1) Avec le câble USB, raccorder le PC au contrôleur de sécurité *Banner* (Figure 19 en page 26).
- 2) Appliquer une alimentation en 24 Vcc au contrôleur.
- 3) Dans la barre d'outil, cliquer sur le bouton affichage live

 ou ouvrir aperçu et sélectionner affichage live.

L'écran d'affichage live est illustré.



Écran 36

6 INSTRUCTIONS DE FONCTIONNEMENT - OBI

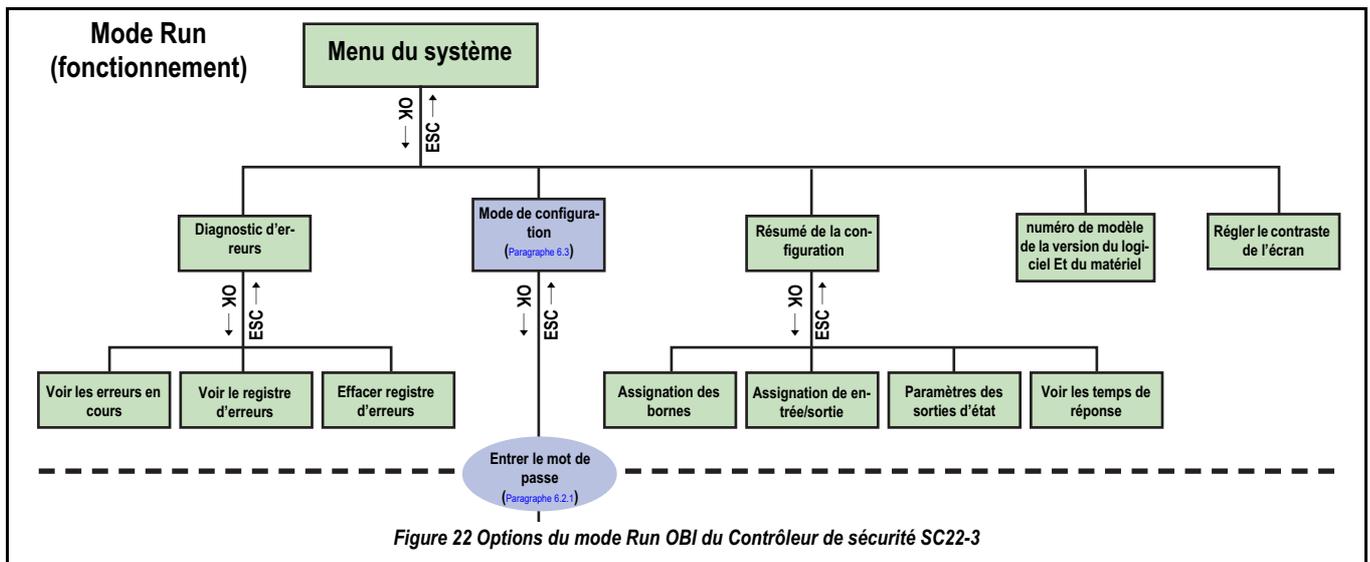
Pour avoir une vue générale de OBI, se référer au [Paragraphe 2.11 en page 18](#). L'OBI du contrôleur de sécurité SC22-3 est un outil de création et de gestion des fichiers de configuration du contrôleur de sécurité, utilisant les caractéristiques intrinsèques du contrôleur lui-même. L'OBI sert aussi à retrouver, afficher et enregistrer les E/S, l'état du système et les informations sur les erreurs.

Les informations suivantes détaillent les étapes nécessaires à la création d'une configuration type, en utilisant l'OBI du contrôleur de sécurité. La configuration sert à définir les dispositifs d'entrées de sécurité qui doivent être raccordés au contrôleur de sécurité et à établir les relations entre ces dispositifs d'entrées de sécurité et les sorties de sécurité du contrôleur.

☛ Pour entrer dans le mode Run, un mot de passe n'est **PAS** nécessaire. Pour entrer dans le mode de configuration en particulier, un mot de passe **EST** nécessaire.

6.1 MODE RUN (FONCTIONNEMENT)

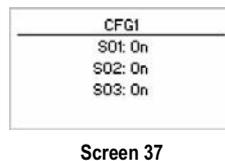
Une décomposition du mode Run est illustrée en [Figure 22 en page 53](#).



Pour entrer dans le mode Run du contrôleur de sécurité SC22-3 :

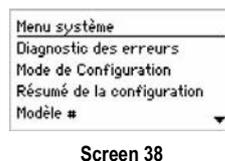
- 1) Raccorder le contrôleur de sécurité SC22-3 au système de sécurité comme convenu.
- 2) Appliquer une alimentation électrique de 24 Vcc au contrôleur de sécurité SC22-3.

Le contrôleur s'active sur l'[Screen 37](#) initial.



Screen 37

- 3) Dans le mode Run, appuyer sur **OK** pour voir le menu système ([Screen 38](#)).



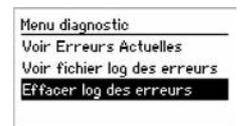
Screen 38

Ce menu permet de lire les informations de diagnostic d'erreurs, d'entrer dans le mode configuration pour créer ou modifier une configuration, de lire le résumé de la configuration, de lire le numéro de modèle du contrôleur de sécurité et de régler le contraste de l'écran lui-même.

- 4) Avec les boutons des flèches vers la haut et vers le bas, mettre en surbrillance la sélection choisie et appuyer sur **OK** pour la sélectionner.

6.1.1 Écran de diagnostic d'erreurs

- 1) Dans le menu système ([Screen 38](#)) sélectionner diagnostic d'erreurs. [Screen 39](#) est illustré.
- 2) Utiliser l'[Screen 39](#), pour voir erreurs actuelles, voir fichier log des erreurs ou effacer log des erreurs. Pour plus d'informations, se référer au [Paragraphe 8.3.3.3 en page 80](#).



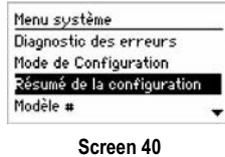
Screen 39

6.1.2 Résumé de la configuration

Le résumé de la configuration permet de consulter uniquement les écrans suivants :

- L'assignement des terminaux de chaque dispositif d'entrée de la configuration en cours.
- La liaison entrée / sortie entre les dispositifs d'entrée et entre les dispositifs d'entrée et les sorties de sécurité
- Les paramètres états des sorties (pour modifier les paramètres, voir le **PARAMÈTRES SORTIES / SYSTÈME** en page 62)
- Le temps de réponse de la sortie de sécurité de chaque entrée assignée à la sortie (voir **Paragraphe 6.1.2.4** en page 54)

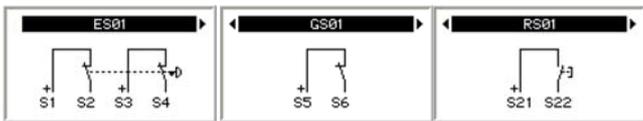
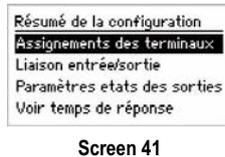
- 1) Dans le **Screen 40**, faire défiler le menu vers le bas et choisir le résumé de la configuration puis appuyer sur **OK**. **Screen 41** est illustré.



6.1.2.1 Assignement des terminaux

La description générale se trouve au **Paragraphe 4.5.4** en page 28.

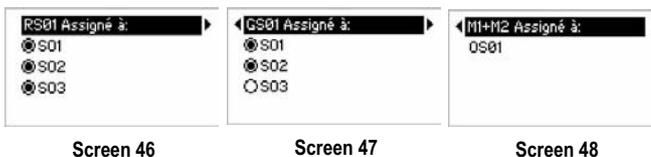
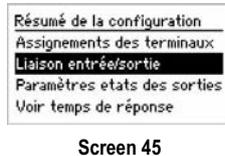
- 1) Dans le **Screen 41**, faire défiler le menu vers le bas et choisir assignement des terminaux puis appuyer sur **OK**. **Screen 42** affiche alors l'assignement des terminaux de la première entrée.
- 2) Utiliser les boutons des flèches droite et gauche pour visionner les assignements des terminaux des autres entrées (**Screen 43** et **Screen 44**). Une fois terminé, appuyer sur **OK** ou sur **ESC** pour sortir.



6.1.2.2 Liaison entrée / sortie

La description générale se trouve au **Paragraphe 4.5.6** en page 28.

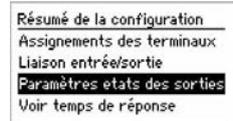
- 1) Dans le **Screen 45**, faire défiler le menu vers le bas et choisir liaison entrée / sortie puis appuyer sur **OK**. **Screen 46** affiche alors la liaison entrée / sortie de la première entrée.
- 2) Utiliser les boutons des flèches droite et gauche pour visionner la liaison entrée / sortie des autres entrées (**Screen 47** et **Screen 48**). Une fois terminé, appuyer sur **OK** ou sur **ESC** pour sortir.



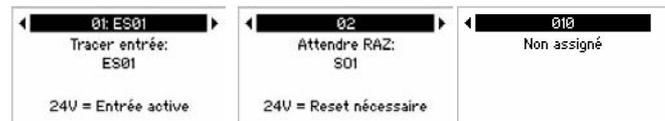
6.1.2.3 Paramètres états des sorties

Cette ligne sert à afficher les états des sorties configurées. Procéder comme suit :

- 1) Dans le **Screen 49**, faire défiler le menu vers le bas et choisir paramètres états des sorties puis appuyer sur **OK**. **Screen 50** affiche alors les paramètres état des sorties de la première entrée.
- 2) Utiliser les boutons des flèches droite et gauche pour visionner les paramètres états des sorties des autres entrées (**Screen 51** et **Screen 52**). Une fois terminé, appuyer sur **OK** ou sur **ESC** pour sortir.



Screen 49



Screen 50

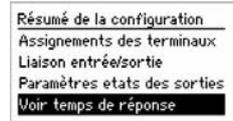
Screen 51

Screen 52

6.1.2.4 Voir les temps de réponse

Cette ligne permet de visionner les temps de réponse de chaque entrée assignée à la sortie. Les temps de réponse servent à calculer les distances de sécurité (voir **Annexe A2.4.2** en page 96 pour plus d'informations). Pour voir cette ligne :

- 1) Dans le **Screen 53**, faire défiler le menu vers le bas et choisir voir temps de réponse puis appuyer sur **OK**. **Screen 54** affiche alors les assignements des terminaux de la première entrée.
- 2) Utiliser les boutons des flèches droite et gauche pour visionner les temps de réponse des sorties de sécurité (**Screen 54**). Une fois terminé, faire défiler vers le bas jusqu'à **< Fait >** pour sortir.



Screen 53



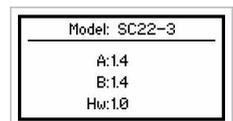
Screen 54

6.1.3 Numéro du modèle

Sélectionner cet écran pour voir le numéro du modèle du contrôleur et les versions du logiciel et du matériel. Cela peut être utile si l'on doit appeler l'assistance aux applications.

- 1) Dans le menu système (**Screen 38**), sélectionner numéro modèle. **Screen 55** est illustré.

Les détails du numéro du modèle sont illustrés dans le **Screen 55**.



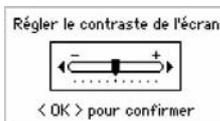
Screen 55

- 2) Avec les flèches haut et bas, mettre la sélection voulue en surbrillance et appuyer sur **OK** pour la sélectionner.

6.1.4 Régler le contraste de l'écran

Cet écran sert à régler la brillance d'arrière plan de l'écran d'affichage du contrôleur et les images en fonction des conditions ambiantes.

- 1) Dans le menu système (Screen 38), sélectionner régler le contraste de l'écran. Screen 56 est illustré.



Screen 56

- 2) Dans le Screen 56, sélectionner cet écran pour régler la brillance de fond de l'écran d'affichage du contrôleur et les images en fonction des conditions ambiantes.
- 3) Avec les flèches droite et gauche, régler le niveau du contraste (à gauche plus clair, à droite plus foncé). Quand le contraste est correct, appuyer sur **OK**.

6.1.5 Enregistrer la configuration

Les modifications de la configuration d'origine sont enregistrées dans une mémoire temporaire. Pour que les modifications soient permanentes (enregistrer la configuration dans une mémoire non volatile) :

- 1) Sélectionner enregistrer la configuration et appuyer sur **OK**.
Il n'est pas nécessaire d'enregistrer les modifications tant qu'on est dans le menu modifier la configuration:

- 2) Appuyer sur le bouton **ESC** et sélectionner **oui**.

Quand la configuration est enregistrée ou si on a appuyé sur **ESC**, l'affichage revient au menu de mode de configuration.

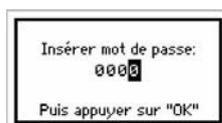
6.2 ENTRÉE DANS LE MODE DE CONFIGURATION

6.2.1 Entrer le mot de passe du contrôleur

Avant de pouvoir accéder au mode de configuration, il faut entrer un mot de passe. Le mot de passe par défaut est 0000.

Les instructions pour changer de mot de passe se trouvent au [Paragraphe 6.3.3.2 en page 66](#).

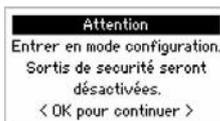
- 1) Dans le Screen 57, en utilisant les boutons des flèches gauche et droite, sélectionner la position du caractère du mot de passe.



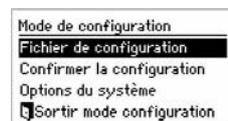
Screen 57

- 2) Avec les flèches haut et bas, sélectionner le caractère (sa valeur) de chaque position (choix 0-9).
- 3) Quand le mot de passe est entré, appuyer sur **OK** pour entrer dans le mode de configuration. Screen 57 est illustré.
- 4) Après avoir lu l'attention illustrée dans l'Screen 58 appuyer sur **OK**.

Screen 59 s'affiche alors.



Screen 58



Screen 59

6.3 MODE DE CONFIGURATION

Le mode de configuration sert à créer ou à modifier une configuration.

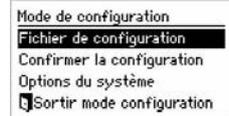
Un détail du mode de configuration est illustré en Figure 23 en page 56.

Pour entrer dans le mode de configuration :

- 1) Dans l’affichage du mode Run (Screen 37), appuyer sur **OK** pour afficher le menu système (Screen 38).
- 2) Dans le menu système, appuyer sur la flèche vers le bas jusqu’à ce que le mode de configuration soit en surbrillance à l’écran (Screen 38), puis appuyer sur **OK**. Screen 60 est illustré.

- 3) Dans l’Screen 60, utiliser cette sélection pour entrer dans les menus suivants :

- Fichier de configuration (pour modifier la configuration)
- Confirmer la configuration
- Options du système
- Sortir du mode de configuration



Screen 60

On trouvera plus d’informations au Paragraphe 8.3.3 en page 77.

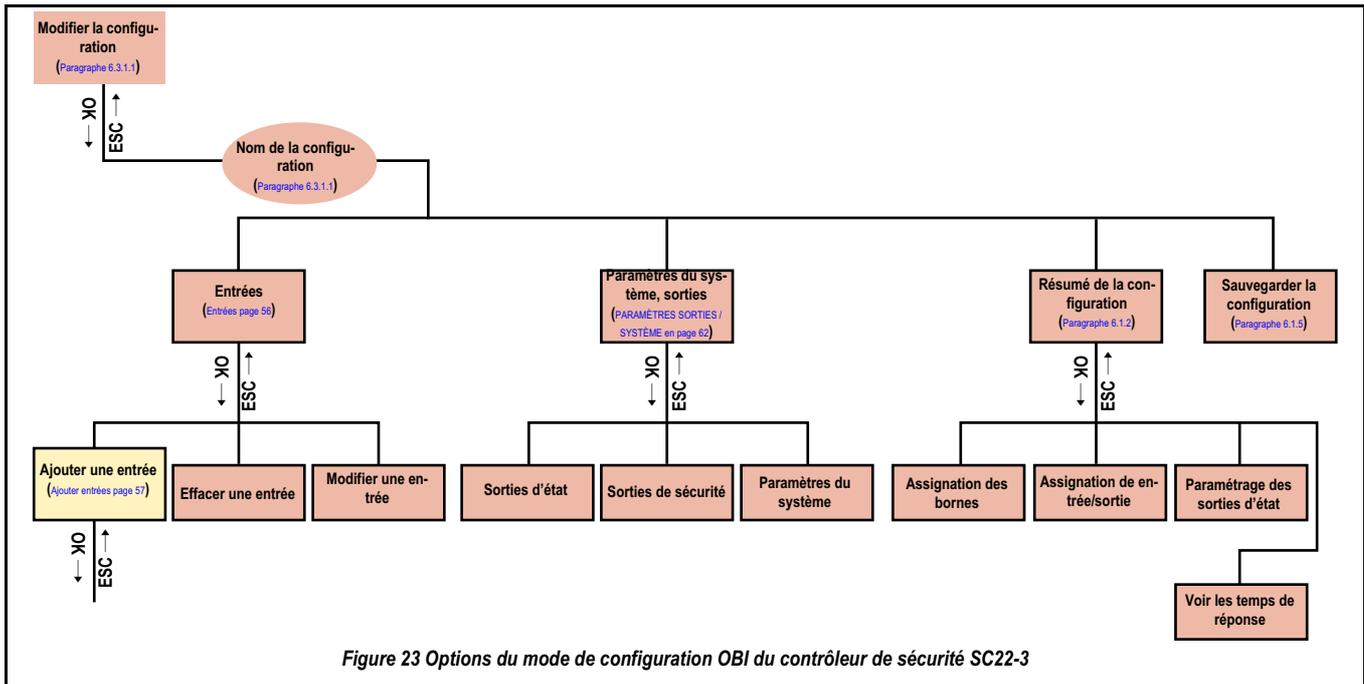


Figure 23 Options du mode de configuration OBI du contrôleur de sécurité SC22-3

6.3.1 Fichier de configuration

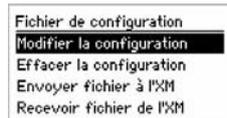
- 1) Dans le mode de configuration (Screen 59), sélectionner le fichier de configuration. Screen 61 est illustré.

Dans le menu du fichier de configuration se trouvent les fonctions suivantes :

- Modifier la configuration
- Effacer la configuration
- Envoyer fichier à l’ XM
- Recevoir fichier de l’ XM

6.3.1.1 Modifier la configuration

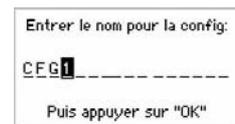
- 1) Dans le Screen 61, avec les boutons des flèches haut et bas, mettre en surbrillance modifier la configuration voulue puis appuyer sur **OK** pour le sélectionner. Screen 62 est illustré.



Screen 61

DONNER UN NOM À LA CONFIGURATION

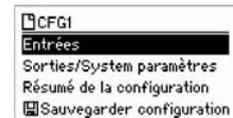
- 2) Dans le Screen 62, entrer le nom pour la configuration. Avec les boutons des flèches haut et bas, sélectionner le caractère à modifier (jusqu’à 16 caractères, avec au choix A-Z, 0-9, -, +, ou espace). Appuyer sur **OK**. Screen 63 est illustré.



Screen 62

Entrées

- 3) Dans le Screen 63, utiliser les flèches haut et bas pour sélectionner les entrées. Appuyer sur **OK**. Screen 64 est illustré.



Screen 63

Dans le menu des entrées, il est possible de sélectionner ajouter entrée, effacer entrée ou modifier entrée comme suit :

AJOUTER ENTRÉE

On peut sélectionner une entrée de sécurité ou une entrée auxiliaire dans ce menu.

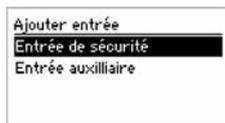
Entrées de sécurité

- 4) Dans le **Screen 64**, utiliser les boutons des flèches haut et bas pour sélectionner ajouter entrée. Appuyer sur **OK**. **Screen 65** est illustré.



Screen 64

- 5) Dans le **Screen 65**, utiliser les boutons des flèches haut et bas pour sélectionner entrée de sécurité. Appuyer sur **OK**. **Screen 66** est illustré.



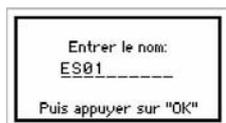
Screen 65

Arrêt d'urgence (ES01) Décomposition d'un exemple de menu

- 6) Dans le **Screen 66**, utiliser les boutons des flèches gauche et droit pour sélectionner une entrée de sécurité, par ex. EStop. Appuyer sur **OK**. **Screen 67** est illustré.
- 7) Dans le **Screen 67**, entrer le nom ; utiliser les boutons des flèches pour sélectionner le caractère à modifier (jusqu'à 16 caractères, choix de A-Z, 0-9, -, +, ou espace). Appuyer sur **OK**. **Screen 68** est illustré.



Screen 66

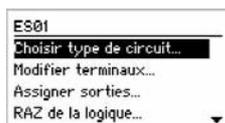


Screen 67

< Choisir type de circuit... >

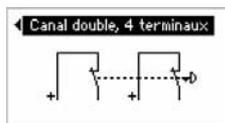
La description générale se trouve au **Paragraphe 4.5.3 en page 28**.

- 8) Dans le **Screen 68**, utiliser les boutons des flèches haut et bas pour sélectionner choisir type de circuit... Appuyer sur **OK**. **Screen 69** est illustré.



Screen 68

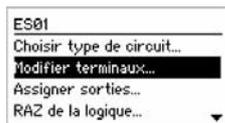
- 9) Dans le **Screen 69**, utiliser les boutons des flèches gauche et droite pour sélectionner, par ex. voie double, 4 bornes. Appuyer sur **OK**. **Screen 70** est illustré.



Screen 69

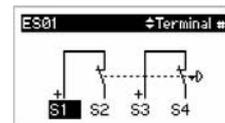
< Modifier terminaux >

- 10) Dans le **Screen 70**, utiliser les boutons des flèches haut et bas pour sélectionner modifier terminaux. Appuyer sur **OK**. **Screen 71** est illustré.



Screen 70

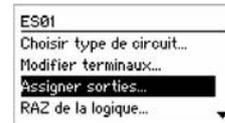
- 11) dans le **Screen 71**, pour modifier les terminaux, utiliser les boutons des flèches gauche et droite pour sélectionner l'assignement du terminal à modifier. Utiliser les boutons des flèches haut et bas pour changer les assignements des terminaux. appuyer sur **OK**. **Screen 72** est illustré.



Screen 71

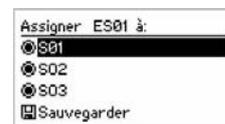
< Assigner sorties >

- 12) Dans le **Screen 72**, utiliser les boutons des flèches haut et bas pour sélectionner assigner sorties. Appuyer sur **OK**. **Screen 73** est illustré.



Screen 72

- 13) dans le **Screen 73**, pour assigner les sorties, utiliser les boutons des flèches haut et bas pour mettre en surbrillance une sortie.



Screen 73

- 14) Effacer ou ajouter l'assignement d'une entrée en sélectionnant sortie et en appuyant sur **OK**.

Un cercle noir à côté d'une sortie indique que l'entrée est assignée à cette sortie. Un cercle blanc indique que l'entrée n'est pas assignée à cette sortie.

- 15) Assigner E-Stop à toutes les trois sorties de sécurité et, en utilisant les boutons des flèches haut et bas, sélectionner enregistrer puis appuyer sur **OK**. **Screen 74** est illustré.

< Logique du réarmement.. >

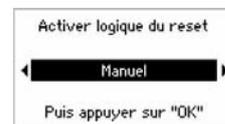
La description générale se trouve au **Paragraphe 4.5.4 en page 28**.

- 16) Dans le **Screen 74**, utiliser les boutons des flèches haut et bas pour sélectionner logique du réarmement... Appuyer sur **OK**. **Screen 75** est illustré.



Screen 74

- 17) Dans le **Screen 75**, paramétrer la logique du réarmement en utilisant les boutons des flèches gauche et droite pour sélectionner manuel à partir du choix manuel ou Auto. Appuyer sur **OK**. **Screen 76** est illustré.



Screen 75

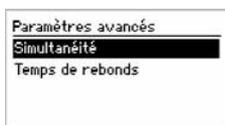
<Paramètres avancés...>

- 18) Dans le **Screen 76**, utiliser les boutons des flèches haut et bas pour sélectionner paramètres avancés.... Appuyer sur **OK**. **Screen 77** est illustré.



Screen 76

- 19) Si nécessaire, dans le **Screen 77**, choisir dans paramètres avancés... en utilisant les boutons des flèches haut et bas entre simultanéité ou temps d'anti-rebond (voir les informations concernant ces réglages en [Paragraphe 4.5.7 en page 29](#)). Appuyer sur **ESC** pour revenir au ES01 **Screen 78**.

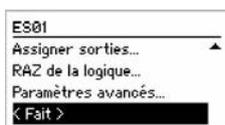


Screen 77

< Enregistrer les paramètres >

Cette fonction sert à sauvegarder les paramètres configurés. Procéder comme suit :

- 20) Dans le **Screen 78**, utiliser les boutons de flèches haut et bas pour faire défiler jusqu'à < fait >. Appuyer sur **OK**. **Screen 79** est illustré.



Screen 78

- 21) Dans le **Screen 79**, appuyer sur **OK** pour revenir à l'écran entrées (**Screen 64**).



Screen 79

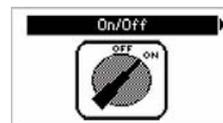
Entrées auxiliaires

- 22) Dans le **Screen 80**, utiliser les boutons des flèches haut et bas pour sélectionner entrée auxiliaire. Appuyer sur **OK**. **Screen 81** est illustré.



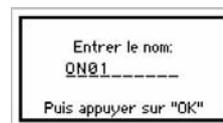
Screen 80

- 23) Dans le **Screen 81**, utiliser les boutons des flèches gauche et droite pour sélectionner une entrée auxiliaire par ex. interrupteur ON/OFF. Appuyer sur **OK**. **Screen 82** est illustré.



Screen 81

- 24) Dans le **Screen 82**, entrer le nom ; utiliser les boutons des flèches pour sélectionner le caractère à modifier (jusqu'à 16 caractères, choix de A-Z, 0-9, -, +, ou espace). Appuyer sur **OK**. **Screen 83** est illustré.



Screen 82

Les écrans de **Étape n° 8** à **Étape n° 21**) sont pratiquement identiques.

- 25) Recommencer **Étape n° 8**) à **Étape n° 21**).

Ajout de dispositifs d'ENTRÉE DE SÉCURITÉ supplémentaire

Les étapes pour ajouter d'autres dispositifs d'Entrée de sécurité sont semblables à celles qui viennent d'être faites.

- Créer les dispositifs d'Entrée de sécurité suivants, avec les propriétés indiquées dans le [Tableau 12 en Page 59](#) :
 Interrupteur de porte, GS01
 Commande bimanuelle, THC01
 Entrée de réarmement, RS01
 Barrière immatérielle, OS01
 Surveillance des dispositifs externes ; EDM01, EDM02 et EDM03
 Paire de capteurs d'inhibition, M1+M2

Tableau 12 Décomposition des dispositifs supplémentaires d'entrée de sécurité

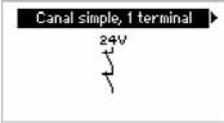
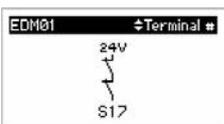
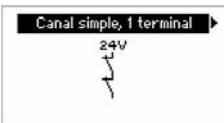
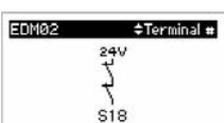
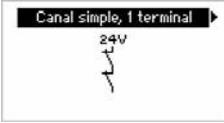
| Fonction | Écran |
|---|---|
| surveillance des commutateurs externes (EDM)  | |
| Type de circuit : Canal simple, 1 terminal |  Screen 83 |
| Terminaux : S17 |  Screen 84 |
| Assigné à : SO1 | Sélectionner sortie:  Puis appuyer sur "OK" Screen 85 |
| Surveillance des commutateurs externes - EDM02  | |
| Type de circuit : Canal simple, 1 terminal |  Screen 86 |
| Terminaux : S18 |  Screen 87 |
| Assigné à : SO2 | Sélectionner sortie:  Puis appuyer sur "OK" Screen 88 |
| Surveillance des commutateurs externes – EDM03  | |
| Type de circuit : Canal simple, 1 terminal |  Screen 89 |

Tableau 12 Décomposition des dispositifs supplémentaires d'entrée de sécurité

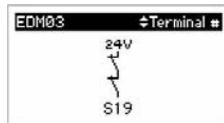
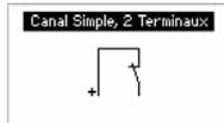
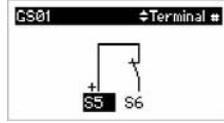
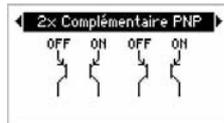
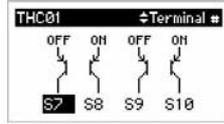
| Fonction | Écran |
|--|--|
| Terminaux : S19 |  Screen 90 |
| Assigné à : SO3 | Sélectionner sortie:  Puis appuyer sur "OK" Screen 91 |
| Interrupteur de porte – GS01  | |
| Type de circuit : Canal simple, 2 terminaux |  Screen 92 |
| Terminaux : S5 & S6 |  Screen 93 |
| Assigné à : SO1, SO2 | Assigner GS01 à: <input checked="" type="radio"/> SO1 <input checked="" type="radio"/> SO2 <input type="radio"/> SO3 <input type="checkbox"/> Sauvegarder Screen 94 |
| Auto Logique de réarmement : | Activer logique du reset  Puis appuyer sur "OK" Screen 95 |
| Commande bimanuelle – THC01  | |
| Type de circuit : 2X complémentaire, contact PNP |  Screen 96 |
| Terminaux : S7, S8, S9 & S10 |  Screen 97 |

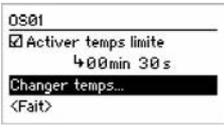
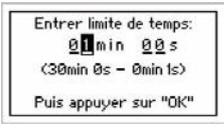
Tableau 12 Décomposition des dispositifs supplémentaires d'entrée de sécurité

| Fonction | Écran |
|--|-------------------|
| Assigné à : SO3 | <p>Screen 98</p> |
| Barrière immatérielle – OS01 | |
| Type de circuit : Canal double, contact PNP | <p>Screen 99</p> |
| Modifier terminaux : S11 & S12 | <p>Screen 100</p> |
| Assignés à : SO1 & SO2 | <p>Screen 101</p> |
| Auto Logique de réarmement : | <p>Screen 102</p> |
| Capteur d'inhibition – M1 + M2 | |
| L'entrée suivante est différente des entrées précédentes et est donc couverte plus en détail. | |
| 1) Après avoir sélectionné ajouter un capteur d'inhibition et avoir entré son nom, choisir le type de circuit et les assignements de terminaux comme suit: | |
| Type de circuit : Canal double, 4 terminaux | <p>Screen 103</p> |
| Modifier les terminaux : 13, 14, 15 & 16 | <p>Screen 104</p> |

Tableau 12 Décomposition des dispositifs supplémentaires d'entrée de sécurité

| Fonction | Écran |
|---|-------------------|
| <p>Au lieu d'être assignées à une sortie, les entrées d'un capteur d'inhibition sont assignées aux entrées qu'elles inhibent. Seuls certains types de dispositifs d'entrée peuvent être inhibés. Le contrôleur de sécurité crée une liste des entrées dans la configuration en cours qui sont susceptibles d'inhibition.</p> <p>2) Dans le menu des propriétés du capteur d'inhibition, sélectionner assigner les entrées et appuyer sur OK. Screen 105 est illustré.</p> <p>3) Dans le Screen 105, en utilisant les boutons des flèches haut et bas, sélectionner OS01 dans la liste des entrées et appuyer sur OK. Le cercle à gauche de OS01 se noircit pour indiquer que la paire de capteurs d'inhibition M1+M2 est assignée à OS01.</p> <p>☛ Dans ce cas, la paire de capteurs d'inhibition n'est assignée qu'à OS01, mais la paire de capteurs d'inhibition peut être assignée à plusieurs entrées.</p> <p>4) Sélectionner sauvegarder et appuyer sur OK pour terminer le processus d'assignation de l'entrée.</p> | <p>Screen 105</p> |
| <p>Paramétrage des temps limites d'inhibition</p> <p>Fixer un temps limite d'inhibition définit la durée maximale de temps qu'une entrée peut être inhibée.</p> <p>5) Dans le Screen 106, le menu des propriétés de M1+M2, sélectionner fixer temps limite d'inhibition et appuyer sur OK. Screen 107 est illustré.</p> | <p>Screen 106</p> |
| <p>6) Dans le Screen 107, sélectionner entrée, et appuyer sur OK. Screen 108 est illustré.</p> | <p>Screen 107</p> |

Tableau 12 Décomposition des dispositifs supplémentaires d'entrée de sécurité

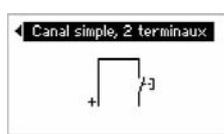
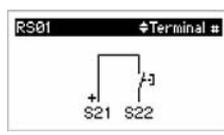
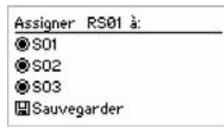
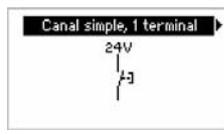
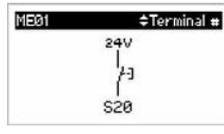
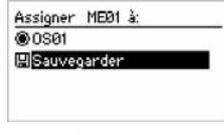
| Fonction | Écran |
|---|--|
| <p>☛ Si la case devant activer temps limite n'est pas cochée, le faire et appuyer sur OK pour activer le temps limite.</p> <p>7) Dans le Screen 108, en utilisant les boutons des flèches haut et bas, sélectionner changer temps... et appuyer sur OK. Screen 109 est illustré.</p> <p>8) Dans le Screen 109, modifier la valeur à 1 minute. Utiliser les boutons des flèches gauche et droite pour sélectionner le chiffre à changer et les boutons des flèches haut et bas pour modifier le chiffre (0-9) puis appuyer sur OK.</p> <p>9) Dans le Screen 108, sélectionner <Fait> et appuyer sur OK.</p> |  <p>Screen 108</p>  <p>Screen 109</p> |
| <p>Quand toutes les entrées de sécurité nécessaires ont été ajoutées l'une après l'autre, appuyer sur ESC pour revenir au Screen 63.</p> | |

AJOUT DE DISPOSITIFS D'ENTRÉES AUXILIAIRES SUPPLÉMENTAIRES

Les étapes pour ajouter d'autres dispositifs d'entrée auxiliaire sont semblables à celles qui viennent juste d'être faites.

- Créer les dispositifs d'entrée suivants, avec les propriétés du **Tableau 12 en Page 59** :
 - Entrée de réarmement, RS01
 - Inhibition

Tableau 13 Présentation des dispositifs d'Entrée de sécurité supplémentaires

| Fonction | Écran |
|---|---|
| <p>Réarmement – RS01 </p> | |
| Type de circuit : Canal simple, 2 terminaux |  <p>Screen 110</p> |
| Terminaux : S21 et S22 |  <p>Screen 111</p> |
| Assignés à : S01, S02 et S03 |  <p>Screen 112</p> |
| <p>Activation du muting (ME) – ME01 </p> | |
| Type de circuit : canal simple, 1 terminal |  <p>Screen 113</p> |
| Terminaux : S20 |  <p>Screen 114</p> |
| Assignés à : S01, S02 et S03 |  <p>Screen 115</p> |
| <p>Quand toutes les entrées auxiliaires nécessaires ont été rajoutées une par une, appuyer sur ESC pour sortir vers le Screen 63.</p> | |

Paramètres sorties / système

SORTIES DE SÉCURITÉ

Cette option sert à modifier les sorties de sécurité le cas échéant.

1) Dans le **Screen 63**, sélectionner paramètres sorties / système. **Screen 117** est illustré.

2) Dans le **Screen 116**, en utilisant les boutons des flèches haut et bas, sélectionner sorties de sécurité et appuyer sur **OK**. **Screen 117** est illustré.



3) Dans le **Screen 117**, sélectionner la sortie de sécurité à modifier et appuyer sur **OK**. **Screen 118** est illustré.



4) Dans le **Screen 118**, modifier changer nom..., type de délai et temps du délai selon le besoin. Quand cela est terminé, sélectionner < Fait >.



Cette option sert à configurer individuellement les sorties d'état.

1) Dans le **Screen 116**, sélectionner sorties d'état. **Screen 119** est illustré.

2) Dans le **Screen 119**, en utilisant les boutons des flèches gauche et droite, sélectionner chaque sortie d'état à tour de rôle pour la modifier (O1 à O10) et appuyer sur **OK**. **Screen 120** est illustré.



Le menu des propriétés de la sortie d'état apparaît et sert à modifier les indications suivantes :

Changer le nom...

Sélectionner une fonction...

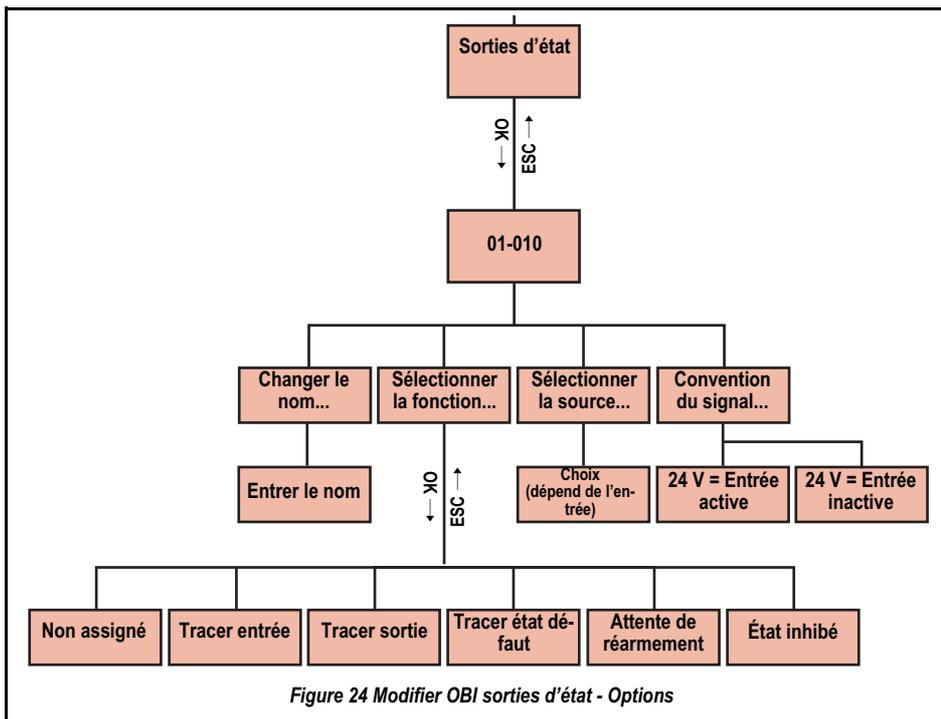
Sélectionner une source...

Convention des signaux...



Une présentation plus détaillée de ces indications se trouve en **Figure 24** en page 62.

SORTIES D'ÉTAT



Changer le nom...

3) Dans le **Screen 120**, faire défiler le menu vers le bas pour sélectionner changer le nom... et appuyer sur **OK**. **Screen 121** est illustré.

4) Dans le **Screen 121**, en utilisant les boutons des flèches gauche et droite, passer d'un caractère à l'autre (jusqu'à 10 caractères).

5) Dans le **Screen 121**, en utilisant les boutons des flèches haut et bas, modifier les caractères (possibilités : A-Z, 0-9, -, +, ou espace). Appuyer sur **OK** une fois terminé.



Quand l'affichage revient au menu des propriétés d'entrée d'état, la ligne du haut de l'affichage affiche le nouveau nom.

Sélectionner une fonction...

- 6) Dans le **Screen 120**, faire défiler le menu vers le bas jusqu'à sélectionner une fonction...
- 7) Utiliser les boutons des flèches gauche et droite pour sélectionner une fonction, puis appuyer sur **OK**.

L'affichage revient au menu des propriétés d'entrée d'état.

Sélectionner une source...

- 8) Dans le **Screen 120**, faire défiler le menu vers le bas pour choisir sélectionner une source... et appuyer sur **OK**.
- 9) Utiliser les boutons des flèches gauche et droite pour sélectionner le dispositif et appuyer sur **OK**.

L'affichage revient au menu des propriétés d'entrée d'état.

Convention des signaux...

- 10) Dans le **Screen 120**, faire défiler le menu vers le bas pour choisir convention des signaux... et appuyer sur **OK**.
- 11) Utiliser les boutons des flèches gauche et droite pour basculer entre les choix et appuyer sur **OK**.
Les choix sont : 24V = Input Active et 24V = entrée inactive (par ex. si tracer entrée est sélectionné ; voir [Paragraphe 4.9.1 en page 35](#) pour plus d'informations).
- 12) Sélectionner **<Fait>** et appuyer sur **OK** pour enregistrer les paramètres de cette sortie.

L'affichage revient au menu des paramètres sorties / système.

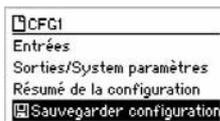
- 13) Recommencer **Étape n° 1)** à **Étape n° 12)** pour configurer les sorties d'état supplémentaires de la même façon.
- 14) Quand la dernière sortie d'état est configurée, appuyer sur **ESC** pour revenir au menu modifier la configuration.

PARAMÈTRES SYSTÈME

Ce menu sert à configurer le réarmement du système, le choix à la mise sous tension et l'inhibition à la mise sous tension.

Réarmement du système

- 1) Dans le **Screen 122**, faire défiler le menu vers le bas pour choisir réarmement du système et appuyer sur **OK**.



Screen 122

- 2) Utiliser les boutons des flèches gauche et droite pour basculer entre surveillé et non surveillé et appuyer sur **OK**.

Choix à la mise sous tension

- 3) Dans le **Screen 122**, faire défiler le menu vers le bas pour définir le choix à la mise sous tension et appuyer sur **OK**.

Utiliser les flèches gauche et droite pour sélectionner normal, auto, ou manuel et appuyer sur **OK**.

Inhibition à la mise sous tension

- 4) Dans le **Screen 122**, faire défiler le menu vers le bas pour choisir inhibition à la mise sous tension et appuyer sur **OK**.
- 5) Utiliser les flèches gauche et droite pour basculer entre OFF et ON et appuyer sur **OK**.

Résumé de la configuration

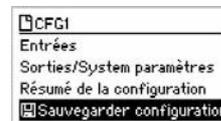
Les instructions détaillées se trouvent dans le [Paragraphe 6.1.2 en page 54](#).

Sauvegarder la configuration

Pendant que l'on modifie la configuration, les modifications sont enregistrées dans un emplacement de mémoire temporaire.

Pour faire que les modifications de la configuration soient permanentes :

- 1) Dans le **Screen 123**, sélectionner sauvegarder configuration et appuyer sur **OK**.



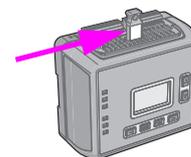
Screen 123

Il n'est pas nécessaire d'enregistrer les modifications dans le menu modifier configuration, appuyer sur **ESC** et sélectionner **oui** pour sortir sans enregistrer les modifications oui/non.

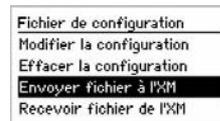
6.3.1.2 Envoyer un fichier à XM

Cette sélection sert à envoyer un fichier de configuration à la carte XM branchée dans le port XM du contrôleur. Le fichier peut alors être enregistré et, ou, transporté vers un autre contrôleur.

- 1) Insérer la carte XM dans le port XM du contrôleur comme illustré.



- 2) Dans le **Screen 124** du contrôleur, sélectionner envoyer fichier à l'XM et suivre les indications.



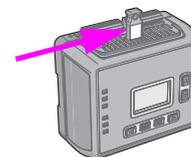
Screen 124

Si la carte XM n'est pas vide, le contrôleur demande s'il faut écraser la configuration déjà enregistrée sur la carte XM OUI/NON (sinon, envoyer d'abord la configuration existante vers une carte XM vide). Répondre oui, puis, il la carte XM n'est pas encore dans le port, l'y enfiler et appuyer sur **OK**.

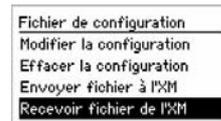
6.3.1.3 Recevoir fichier de l'XM

Cette sélection sert à recevoir une configuration depuis une carte XM.

- 1) Insérer la carte XM dans le port XM du Contrôleur.



- 2) Dans le **Screen 125** du contrôleur, sélectionner recevoir fichier de l'XM et suivre les indications.



Screen 125

Le contrôleur invite à écraser la configuration actuelle du contrôleur OUI/NON (sinon, envoyer d'abord la configuration existante vers une carte XM vide). Répondre oui, puis, si la carte XM n'est pas encore dans le port, l'y enfiler et appuyer sur **OK**. Si la nouvelle configuration n'est pas confirmée, le contrôleur permet de la confirmer à cet instant.

6.3.1.4 Effacer la configuration

Cette sélection sert à effacer la configuration courante du contrôleur de sécurité, pour pouvoir créer une nouvelle configuration (le contrôleur ne peut contenir qu'une seule configuration à la fois).

☛ Pour conserver le fichier existant, l'envoyer à une carte XM (comme expliqué en [Paragraphe 6.3.1.2 en page 63](#)) avant de l'effacer du contrôleur.

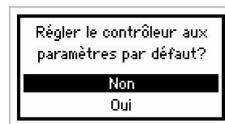
Pour effacer :

- 1) Dans le [Screen 126](#), en utilisant les boutons des flèches haut et bas, mettre en surbrillance effacer la configuration puis appuyer sur **OK**. [Screen 127](#) est illustré.



Screen 126

- 2) Dans le [Screen 127](#), en utilisant les boutons des flèches haut et bas, définir les paramètres par défaut, oui / non. Pour sortir, appuyer sur **OK**.

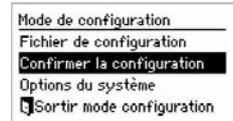


Screen 127

6.3.2 Confirmer la configuration

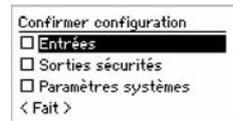
Avant de pouvoir utiliser une configuration dans une application de protection, il faut la confirmer. Pour confirmer la configuration:

- 1) Sélectionner confirmer la configuration et appuyer sur **OK**. [Screen 129](#) est illustré.



Screen 128

Les configurations critiques pour la sécurité des entrées, sorties de sécurité et des paramètres du système doivent maintenant être revues. Une case non cochée dans le menu confirmer la configuration indique que les paramètres critiques pour la sécurité n'ont pas encore été confirmés. [Screen 129](#) est illustré.

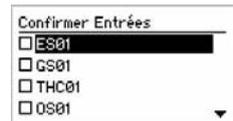


Screen 129

6.3.2.1 Confirmer la configuration des entrées

Dans le [Screen 129](#) menu confirmer la configuration, sélectionner entrées et appuyer sur **OK**. [Screen 130](#) est illustré.

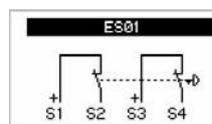
- 1) Dans le [Screen 130](#), confirmer en sélectionnant par ex. **E-Stop ES01**, puis appuyer sur **OK**. [Screen 131](#) est illustré.



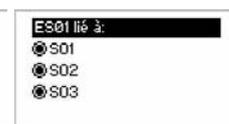
Screen 130

La série suivante de menus indique les configurations critiques pour la sécurité pour cette entrée.

- 2) Réviser les configurations critiques pour la sécurité de chaque paramètre de cette entrée dans les écrans suivants, [Screen 131](#), [Screen 132](#), [Screen 133](#), [Screen 134](#) et [Screen 135](#) puis appuyer sur **OK**:



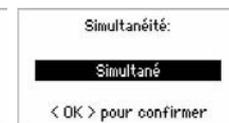
Screen 131



Screen 132



Screen 133



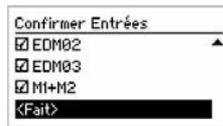
Screen 134



Screen 135

- Recommencer le processus de confirmation pour chacune des entrées.

Quand toutes les entrées sont confirmées, [Screen 136](#) s'affiche.

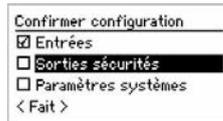


Screen 136

- Pour continuer confirmer la configuration, sélectionner **<Fait>** et appuyer sur **OK**.

6.3.2.2 Confirmer la configuration des sorties

- Dans le [Screen 129](#) sélectionner le menu confirmer la configuration et appuyer sur **OK**. [Screen 137](#) est illustré.



Screen 137

- Dans le [Screen 137](#), sélectionner sorties de sécurité puis appuyer sur **OK**. [Screen 138](#) est illustré.

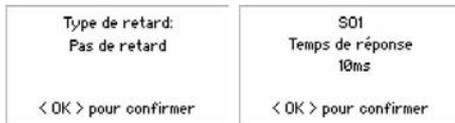
- Confirmer la configuration de la sortie de sécurité SO1 en sélectionnant **SO1** et en appuyant sur **OK**.



Screen 138

La série suivante de menus indique les configurations critiques de SO1.

- Réviser les configuration critiques pour la sécurité pour SO1 de cette sortie de sécurité dans les écrans suivants, [Screen 139](#), [Screen 140](#) et [Screen 141](#) puis appuyer sur **OK**.



Screen 139

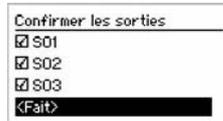
Screen 140



Screen 141

- Recommencer le processus de confirmation pour SO2 et SO3.

Quand toutes les sorties de sécurité sont confirmées, [Screen 142](#) s'affiche.

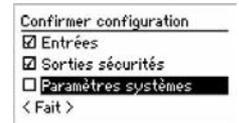


Screen 142

- Pour continuer confirmer la configuration, sélectionner **<Fait>** et appuyer sur **OK**.

6.3.2.3 Confirmer la configuration des paramètres du système

- Dans le [Screen 129](#) sélectionner le menu confirmer la configuration et appuyer sur **OK**. [Screen 143](#) est illustré.

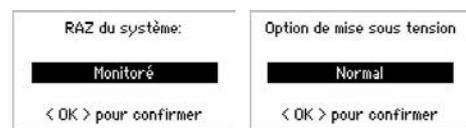


Screen 143

- Dans le [Screen 143](#), sélectionner paramètres système, puis appuyer sur **OK**. [Screen 138](#) est illustré.

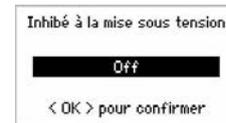
La série suivante de menus indique les paramètres système critiques pour la sécurité.

- Réviser les configurations critiques pour la sécurité des paramètres système dans les écrans suivants, [Screen 144](#), [Screen 145](#) et [Screen 146](#) puis appuyer sur **OK**.



Screen 144

Screen 145



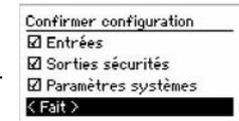
Screen 146

6.3.2.4 Étape de confirmation finale

Seulement quand tous les paramètres de configuration critiques pour la sécurité sont confirmés, et seulement à ce moment là, la configuration peut être utilisée dans une application de protection.

Si des modifications sont effectuées à la configuration, le processus de confirmation doit être recommencé.

- Dans le [Screen 147](#) sortir du menu confirmer la configuration en sélectionnant **<Fait >** et en appuyant sur **OK**.

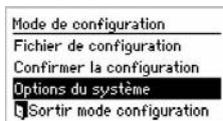


Screen 147

6.3.3 Options du système

Cette fonction sert à changer le mot de passe et à sélectionner le langage.

- 1) Dans le [Screen 148](#), sélectionner options du système. [Screen 149](#) est illustré.

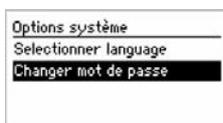


Screen 148

6.3.3.1 Changer le mot de passe

Cette fonction permet de sélectionner un mot de passe autre que celui par défaut. Le mot de passe peut être unique pour chaque contrôleur. La procédure est semblable à celle utilisée pour entrer initialement le mot de passe par défaut.

- 1) Dans le [Screen 149](#), sélectionner changer le mot de passe. [Screen 150](#) est illustré.



Screen 149

- 2) Dans le [Screen 150](#), en utilisant les boutons des flèches gauche et droite, sélectionner la position du caractère du mot de passe. Avec les flèches haut et bas, sélectionner la valeur du chiffre pour chaque position (choix 0-9).
- 3) Quand le mot de passe est entré, appuyer sur **OK** et noter le mot de passe dans un fichier pour le conserver en référence pour plus tard.



Screen 150

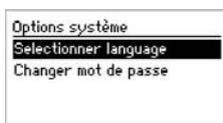
6.3.3.2 Sélectionner le langage

Cet écran sert à déterminer la langue qui apparaît dans l'affichage. Les choix sont les suivants :

| | | |
|----------|-----------|----------|
| Anglais | Français | Japonais |
| Allemand | Italien | |
| Espagnol | Portugais | |

Mettre en surbrillance la langue souhaitée et appuyer sur OK.

- 1) Dans le [Screen 151](#), sélectionner **sélectionner le langage**.



Screen 151

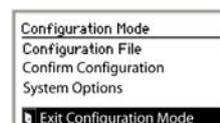
- 2) Sélectionner la langue et appuyer sur **OK**.

☛ *La langue peut aussi être modifiée immédiatement à la mise sous tension. Un écran apparaît automatiquement et le choix de la langue peut être fait à ce moment. Si rien n'est changé, l'écran disparaît après 5 secondes et passe en mode Run dans la langue qui était celle du contrôleur quand il a été éteint la dernière fois.*

6.3.4 Sortir du mode de configuration

Cette fonction permet de revenir en mode Run.

- 1) Dans le [Screen 152](#), sélectionner sortir du mode de configuration.



Screen 152

Le contrôleur demande s'il faut confirmer la configuration Oui/Non avant de sortir, puis retourne dans le menu système.

7 INSTRUCTIONS DE FONCTIONNEMENT — GÉNÉRALITÉS

7.1 AFFICHAGE DES INFORMATIONS DU CONTRÔLEUR — PCI

Pour afficher en temps réel les informations du mode Run sur le PC :

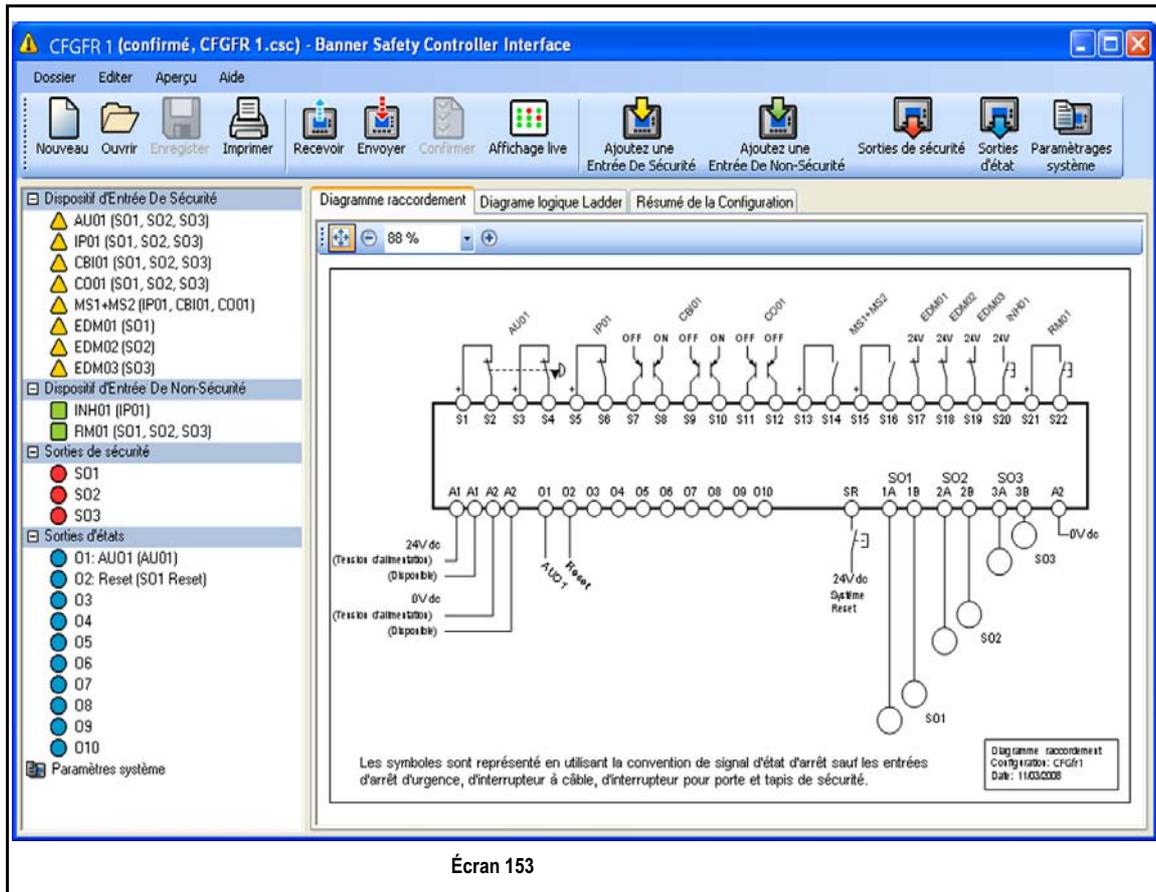
- 1) En se référant au paragraphe [Paragraphe 4.3.2 en page 26](#), raccorder le contrôleur au PC, par le câble USB.
- 2) Sur le bureau du PC, double cliquer sur l'icône *Banner* contrôleur de sécurité .

Ou bien

Dans le menu Démarrage, cliquer sur :

<Start> <All Programs> <Banner Engineering> <Banner Contrôleur de sécurité>

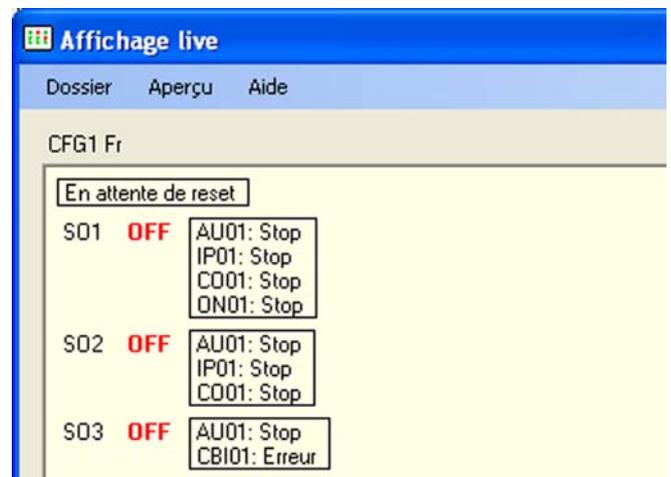
- 3)  Lire et comprendre les avertissements de la page de mise sous tension et cliquer sur **OK**. [Écran 153](#) est illustré.



- 4) Dans le [Écran 153 en page 67](#), cliquer sur l'icône affichage live 

[Écran 154 en page 67](#) est illustré.

L'affichage live ([Écran 154 en page 67](#)) met à jour en continu les données du mode Run et les affiche comme illustré. Il fournit les mêmes informations que celles qui peuvent être vues sur l'écran du contrôleur. Il indique l'état de chaque sortie de sécurité et informe sur chaque dispositif d'entrée ou événement système qui pourrait faire que la sortie de sécurité passe sur OFF.



Écran 154

Pour plus d'informations sur le PCI, se référer à [Chapitre 5](#).

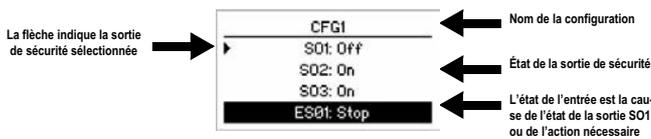
7.2 AFFICHAGE DES INFORMATIONS DU CONTRÔLEUR — OBI

7.2.1 Mode Run (fonctionnement)

Le détail du mode Run se trouve dans la [Figure 22 en page 53](#).

L'exemple du mode Run OBI du contrôleur ([Écran 155 en page 68](#)) affiche les informations courantes du contrôleur de sécurité, dont :

- Nom de la configuration
- État de la sortie de sécurité
- État de l'entrée
- État du système
- État de l'OBI de la carte XM



Écran 155

7.2.1.1 Nom de la configuration

La ligne du haut de l'affichage indique soit le nom de la configuration enregistrée dans le contrôleur de sécurité, si elle a été confirmée, soit, configuration non confirmée si elle ne l'est pas.

7.2.1.2 État de la sortie de sécurité

Les lignes 2, 3 et 4 de l'[Écran 155 en page 68](#) indiquent l'état des 3 sorties de sécurité. La sortie de sécurité sélectionnée est indiquée par un petit triangle noir, comme illustré ; (le triangle défile le long des sorties de sécurité qui sont OFF, selon un intervalle de 2 secondes). La ligne 5 de l'affichage indique les raisons de l'état de la sortie de sécurité sélectionnée. Le [Tableau 14 en Page 68](#) est un récapitulatif des messages d'état des sorties de sécurité.

Les erreurs de sortie sont récupérables grâce à un réarmement système (voir [Paragraphe 7.4 en page 70](#)).

La ligne 5 de l'affichage indique erreur de lampe d'inhibition s'il s'est produit une erreur de lampe d'inhibition.

Tableau 14 Présentation des messages d'état de la sortie de sécurité

| Message d'état de la sortie de sécurité | Cause et, ou, action requise |
|---|--|
| ON | La sortie de sécurité est sur ON. |
| Temporisation à l'enclenchement | La sortie de sécurité passe sur ON quand la temporisation à l'enclenchement expire. |
| OFF | La sortie de sécurité est sur OFF. La ligne 5 de l'affichage donne la raison pour laquelle la sortie de sécurité est sur OFF. |
| Temporisation au déclenchement | La sortie de sécurité passe sur OFF quand la temporisation au déclenchement expire. La ligne 5 de l'affichage donne la raison pour laquelle la sortie de sécurité est dans une temporisation au déclenchement. |
| Réarmement nécessaire | Un réarmement manuel est nécessaire. La ligne 5 de l'affichage indique le nom de l'entrée de réarmement manuel à utiliser. |

Tableau 14 Présentation des messages d'état de la sortie de sécurité

| Message d'état de la sortie de sécurité | Cause et, ou, action requise |
|---|--|
| Défaillance : | Un problème a été détecté au niveau de la sortie de sécurité. Voir le tableau de dépannage (Paragraphe 8.3.3 en page 77) pour obtenir d'avantage d'informations sur la défaillance. Si la défaillance est due à une erreur d'EDM, la ligne 5 de l'affichage indique le nom de l'EDM. |
| Mode actif | La ligne 5 de l'affichage indique mode actif si une sortie de sécurité est en mode actif. |

7.2.1.3 État de l'entrée

Si une sortie de sécurité est sur OFF ou passe sur OFF, la ligne 5 de l'affichage indique les informations sur l'entrée qui maintient la sortie sur OFF.

La ligne 5 indique aussi quand il faut effectuer un réarmement manuel.

La ligne 5 change pour indiquer chaque entrée quand il faut afficher l'état de plusieurs entrées.

Appuyer sur le bouton de la flèche haut pour figer l'écran sur l'entrée actuelle.

Appuyer sur le bouton de la flèche bas pour changer la dernière ligne vers l'entrée suivante (appuyer rapidement sur la flèche bas pour faire défiler les entrées).

Si plusieurs entrées sont sur OFF, un petit triangle noir indique la sortie de sécurité à laquelle correspond le message d'entrée (voir [Écran 155 en page 68](#)).

Il n'y a pas d'informations concernant les entrées quand la sortie de sécurité est sur ON, sauf si une entrée assignée est inhibée, bypassée ou en erreur.

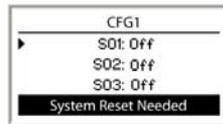
Le [Tableau 15 en Page 68](#) donne les détails des messages d'état des dispositifs d'entrée.

Tableau 15 Présentation des messages d'état des dispositifs d'entrée

| Message d'état des dispositifs d'entrée | Cause et, ou, action requise |
|---|---|
| Stop | L'entrée de sécurité est dans un état qui fait que la sortie de sécurité passe sur OFF. |
| Test | Un test de mise sous tension doit être effectué sur l'entrée de sécurité. Pour effectuer ce test, faire passer l'entrée alternativement sur (Run-Stop-Run) pour faire passer la sortie de sécurité sur ON. |
| Désactivé | L'entrée d'une commande bimanuelle ou un dispositif d'activation doit passer alternativement sur (Run-Stop-Run) avant que la sortie de sécurité passe sur ON. |
| Défaillance | Un problème a été détecté au niveau d'une entrée qui commande la sortie. |
| Temps dépassé | La sortie de sécurité est en mode actif et la limite du temps actif du dispositif d'activation est dépassée. Éteindre et rallumer le dispositif d'activation pour refaire passer la sortie sur ON, ou mettre le dispositif d'activation sur OFF et effectuer un réarmement système pour sortir du mode actif. |

7.2.1.4 État du système

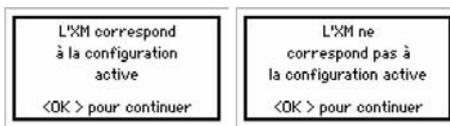
La ligne 5 de l'Screen 156 en page 69 affiche réarmement système nécessaire si un réarmement système est nécessaire pour faire passer les sorties de sécurité sur ON. Cependant, si une situation d'erreur existe, l'erreur doit être corrigée avant pour que le réarmement système puisse faire passer les sorties de sécurité sur ON.



Screen 156

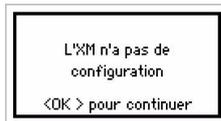
7.2.1.5 État OBI de la carte XM

L'état de la carte XM est affiché momentanément (Screen 157, Screen 158 et Screen 159) quand elle est insérée et que l'écran est en mode Run. La carte XM doit être enlevée ou remplacée le cas échéant.



Screen 157

Screen 158



Screen 159

Le Tableau 16 en Page 69 présente les messages d'état de la carte XM.

Tableau 16 Présentation des messages d'état de la carte XM

| Carte XM Message | Cause |
|--|---|
| XM correspond à la configuration active | La configuration enregistrée sur la carte XM est la même que la configuration du Contrôleur de sécurité |
| XM ne correspond pas à la configuration active | La configuration enregistrée sur la carte XM est différente de celle du contrôleur de sécurité. |
| XM n'a pas de configuration | La carte XM n'a aucune configuration enregistrée. |

7.3 RÉARMEMENT MANUEL

Un réarmement manuel est valide quand toutes les entrées de sécurité assignées aux sorties de sécurité sont en état Run quand le réarmement manuel est effectué. Voir les conditions de temps d'un réarmement au Paragraphe 1.10 en page 5.

Quand un dispositif unique de réarmement manuel est assigné à deux sorties de sécurité ou plus, dont une a une temporisation au déclenchement, le réarmement manuel n'est pas capable de faire passer une sortie de sécurité sur ON tant que la temporisation au déclenchement n'est pas écoulée.

Si un dispositif d'entrée de sécurité configuré pour un réarmement manuel passe de l'état Run à Stop puis de nouveau à Run, toutes les sorties de sécurité auxquelles est assigné ce dispositif passent sur OFF et restent sur OFF jusqu'à ce qu'un réarmement manuel soit effectué.

7.4 RÉARMEMENT SYSTÈME ET CONDITIONS DE BLOCAGE

AVERTISSEMENTS

RÉARMEMENT NON SURVEILLÉS

SI UN RÉARMEMENT NON SURVEILLÉ (RÉARMEMENT MANUEL OU DU SYSTÈME) EST CONFIGURÉ ET SI TOUTES LES AUTRES CONDITIONS POUR UN RÉARMEMENT SONT EN PLACE, UN COURT-CIRCUIT DE LA BORNE DE RÉARMEMENT À +24 V FAIT PASSER LES SORTIES DE SÉCURITÉ SUR ON IMMÉDIATEMENT.

VÉRIFICATION AVANT UN RÉARMEMENT

AU MOMENT D'EFFECTUER UN RÉARMEMENT DU SYSTÈME, L'UTILISATEUR A LA RESPONSABILITÉ DE S'ASSURER QUE TOUTS LES RISQUES POTENTIELS SONT ÉLIMINÉS ET QU'IL N'Y A PERSONNE NI MATÉRIELS INDÉSIRABLES (COMME DES OUTILS) QUI POURRAIENT ÊTRE EXPOSÉS AU DANGER. NE PAS S'Y CONFORMER PEUT ENTRAÎNER DES BLESSURES GRAVES, VOIRE MORTELLES.

EMPLACEMENT DU BOUTON DU SYSTÈME

LE BOUTON DE RÉARMEMENT MANUEL DU SYSTÈME DOIT ÊTRE ACCESSIBLE DE L'EXTÉRIEUR, ET EN PLEINE VUE, DE LA ZONE DANGEREUSE. LES INTERRUPTEURS DE RÉARMEMENT DOIVENT AUSSI ÊTRE HORS DE PORTÉE DE L'INTÉRIEUR DE LA ZONE PROTÉGÉE ET DOIVENT ÊTRE PROTÉGÉS CONTRE UNE UTILISATION NON AUTORISÉE OU ACCIDENTELLE (PAR EX. PAR L'UTILISATION DE BAGUES OU DE PROTECTIONS). SI DES ZONES NE SONT PAS VISIBLES DEPUIS LE BOUTON DE RÉARMEMENT, D'AUTRES MOYENS DE PROTECTION DOIVENT ÊTRE PRÉVUS. NE PAS S'Y CONFORMER PEUT ENTRAÎNER DES BLESSURES GRAVES, VOIRE MORTELLES.

7.5 PARAMÈTRES DU SIGNAL DE RÉARMEMENT

Les deux signaux réarmement manuel (verrouillé) et réarmement système peuvent être configurés pour être surveillés ou non surveillé, comme suit :

7.5.1 Reset contrôlé

Nécessite que le signal de réarmement passe de bas (0 Vcc) à élevé (24 Vcc) puis de nouveau à bas. Le temps de l'état élevé doit se situer entre 0,3 et 2 s. On l'appelle un événement de déclenchement de bord de fuite.

7.5.2 Réarmement non surveillé

Ne nécessite que le signal de réarmement passe de bas (0 Vcc) à élevé (24 Vcc) et qu'il reste élevé pendant au moins 0,3 seconde. Après le réarmement, le signal de réarmement peut être soit élevé, soit bas. On l'appelle un événement de déclenchement de bord d'attaque.

Un réarmement système est nécessaire dans les conditions suivantes :

- Récupération suite à une situation de blocage
- Mettre le contrôleur en service quand une nouvelle configuration a été téléchargée
- Récupération d'une erreur de sortie
- Entrer en mode Run après une mise sous tension, quand il est configuré pour une mise sous tension manuelle.
- Sortir du mode actif

Un réarmement système sert à effacer les conditions d'un blocage non liées aux entrées de sécurité. Une condition de blocage est la réponse quand le contrôleur passe toutes les sorties de sécurité affectées sur OFF si une erreur critique pour la sécurité est détectée. La récupération de cette situation nécessite que l'on répare toutes les erreurs et que l'on effectue un réarmement système. Un blocage se reproduira après un réarmement système si l'erreur qui a provoqué le blocage n'est pas corrigée.

Le dispositif de réarmement (un bouton ou un interrupteur) se raccorde à un terminal d'entrée dédié du contrôleur de sécurité, étiqueté SR. Le type de signal de réarmement peut être configuré pour un réarmement surveillé ou non surveillé (le réglage par défaut est surveillé). Voir les conditions de temps de réarmement au [Paragraphe 7.5 en page 70](#).

8 ENTRETIEN

8.1 MAINTENANCE PRÉVENTIVE

8.2 VÉRIFICATION DU SYSTÈME

⚠ AVERTISSEMENTS

VÉRIFICATIONS PÉRIODIQUES

LES VÉRIFICATIONS DE MISE EN SERVICE, PÉRIODIQUES ET QUOTIDIENNES DU SYSTÈME DE SÉCURITÉ DOIVENT ÊTRE EFFECTUÉES PAR DU PERSONNEL APPROPRIÉ AUX MOMENTS OPPORTUNS (COMME DÉCRIT DANS [Paragraphe 8.2.1 en page 71](#)) POUR S'ASSURER QUE LE SYSTÈME DE SÉCURITÉ FONCTIONNE COMME PRÉVU. NE PAS EFFECTUER CES VÉRIFICATIONS PEUT CRÉER UNE SITUATION POTENTIELLEMENT DANGEREUSE QUI PEUT ENTRAÎNER DES BLESSURES GRAVES, VOIRE MORTELLES.

NE PAS UTILISER LA MACHINE TANT QUE LE SYSTÈME NE FONCTIONNE PAS CORRECTEMENT

SI TOUTES CES CONDITIONS NE SONT PAS REMPLIES, NE PAS UTILISER LE SYSTÈME DE SÉCURITÉ QUI INCLUT LE CONTRÔLEUR DE SÉCURITÉ SC22-3 NI LA MACHINE AVANT D'AVOIR RÉSOLU LE PROBLÈME (VOIR [Chapitre 8](#)). L'UTILISATION DE LA MACHINE DANS DE TELLES CONDITIONS PEUT ENTRAÎNER DES DOMMAGES CORPORELS GRAVES, VOIRE MORTELS.

AVANT DE METTRE LA MACHINE SOUS TENSION

VÉRIFIER QUE LA ZONE PROTÉGÉE A ÉTÉ ÉVACUÉE PAR LE PERSONNEL ET QUE TOUS LES MATÉRIELS INUTILES (COMME LES OUTILS) ONT ÉTÉ RETIRÉS AVANT DE METTRE LA MACHINE PROTÉGÉE SOUS TENSION. NE PAS SE CONFORMER À CES PRÉSCRIPTIONS PEUT ENTRAÎNER DES BLESSURES GRAVES, VOIRE MORTELLES.

8.2.1 Planning des vérifications

La vérification de la configuration et le bon fonctionnement du contrôleur de sécurité comprend la vérification de chaque dispositif d'entrée de sécurité et d'entrée auxiliaire, ainsi que de chaque dispositif de sortie. Au fur et à mesure que les entrées basculent individuellement de l'état Run à l'état Stop, il faut vérifier les sorties de sécurité pour vérifier qu'elles passent sur ON et OFF comme prévu. Les autres entrées assignées aux mêmes sorties de sécurité que celle qui est testée, doivent être en état ON pendant le test.

Un test complet doit servir à vérifier le fonctionnement du contrôleur de sécurité et la fonctionnalité de la configuration utilisée. La liste de vérification du [Paragraphe 8.2.2 en page 71](#) est générique et sert à développer une liste de vérification personnalisée (en fonction de la configuration) pour chaque application. Cette liste personnalisée doit être mise à la disposition du personnel d'entretien au moment de la mise en service et des vérifications périodiques. Une liste de vérification journalière simplifiée doit être établie pour l'opérateur (ou la [Personne désignée selon spécification du paragraphe 1.8.1](#)). Il est fortement recommandé d'avoir sous la main des copies des diagrammes de connexion, des diagrammes logiques Ladder et du résumé de la configuration pour aider pendant les procédures de vérification.

8.2.2 Vérification de mise en service

Une [Personne qualifiée selon spécification du paragraphe 1.8.2 en page 4](#) doit effectuer la procédure de mise en service du système de sécurité avant l'utilisation de l'application sur une machine protégée et après chaque création ou modification de la configuration du contrôleur de sécurité.

8.2.3 Vérifications périodiques (tous les 6 mois)

Une [Personne qualifiée selon spécification du paragraphe 1.8.2 en page 4](#) doit aussi effectuer une remise en service du système de sécurité tous les 6 mois ou à intervalle régulier en fonction des règlements locaux et nationaux.

8.2.4 Vérifications opérationnelles journalières

Une [Personne désignée selon spécification du paragraphe 1.8.1](#) doit aussi vérifier l'efficacité des dispositifs de protection selon les recommandations du fabricant du dispositif chaque jour où la machine protégée est en service.

8.2.5 Procédure d'installation

Pour la partie initiale de la vérification de mise en service, le contrôleur et les systèmes de sécurité associés doivent être vérifiés sans alimentation de la machine protégée. Les raccordements finaux de l'interface à la machine protégée ne peuvent avoir lieu tant que ces systèmes n'ont pas été vérifiés.

8.2.5.1 Pré vérifications de mise en service

Effectuer les pré vérifications suivantes :

- 1) Vérifier que la machine est hors tension et que l'alimentation des commandes et des déclencheurs de la machine n'est pas branchée.
- 2) En se référant à la [Figure 25 en page 71](#), vérifier que le connecteur à 7 broches n'est pas branché au contrôleur de sécurité SC22-3 pour s'assurer que les sorties de sécurité SO1 (A et B), SO2 (A et B) et SO3 (A et B) ne sont pas raccordées à la machine.

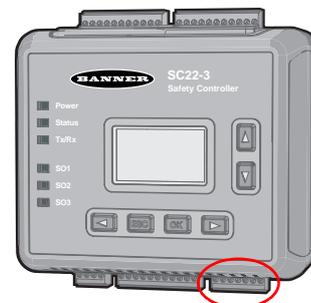


Figure 25 Bornier des sorties de sécurité

- ☛ Les raccordements permanents seront établis plus tard au cours de cette vérification.

8.2.5.2 Vérification du fonctionnement du système

La procédure de vérification de mise en service doit être effectuée par une [Personne qualifiée selon spécification du paragraphe 1.8.2 en page 4](#) (voir aussi le [AVERTISSEMENT, page 71](#)). Elle ne doit être effectuée qu'après la configuration du contrôleur et après l'installation et la configuration des systèmes de sécurité et le raccordement des dispositifs de protection à leurs entrées (selon l'annexe A et les normes applicables).

La vérification de mise en service s'effectue en deux occasions :

- Quand l'installation initiale du contrôleur a été effectuée correctement
- Après toute intervention de maintenance ou de modification du système ou de la machine protégée par le système, pour s'assurer du bon fonctionnement du contrôleur (voir en [Paragraphe 8.2.1 en page 71](#) la fréquence des vérifications)

8.2.5.3 Procédure

- 1) Vérifier que les fils de la sortie de sécurité sont isolés (c'est-à-dire qu'ils ne se court-circuitent pas et qu'ils ne sont pas reliés à la terre).
- 2) Vérifier que, si elles sont utilisées, les connexions, EDM sont raccordées à une source +24 Vcc par les contacts de surveillance N.F. du dispositif connecte aux sorties de sécurité selon les descriptions du [Paragraphe 4.8 en page 34](#) et [Figure 28 en page 85](#), [Figure 29 en page 86](#), [Figure 30 en page 86](#) et [Figure 31 en page 87](#).
- 3) Vérifier que le bon fichier de configuration du contrôleur correspondant à l'application a été téléchargé dans le contrôleur de sécurité SC22-3.
- 4) Vérifier que le contrôleur de sécurité SC22-3 a été raccordé aux systèmes de sécurité **uniquement** (ne **pas** le raccorder à la machine protégée à ce niveau) selon les instructions détaillées dans ce manuel et qu'il est conforme aux normes de sécurité et aux codes locaux de câblage.

Cette procédure permet de vérifier le contrôleur et les systèmes de sécurité associés de manière autonome avant qu'ils ne soient raccordés de façon permanente à la machine protégée.

8.2.6 Mise en service et configuration initiale – vérifications périodiques

☛ *Si une des sorties d'état est assignée à des fonctions dans la configuration, surveiller la fonction de chaque sortie d'état pendant que l'opération associée est testée.*

- 1) Configurer la machine pour que les indicateurs des sorties de sécurité (SO1, SO2 et SO3) du contrôleur de sécurité et des dispositifs de sortie associés puissent être observés et que leur fonctionnement puisse être vérifié sans risque de blessure.

Ne pas mettre le contrôleur de sécurité ni la machine protégée sous tension à ce stade.

8.2.6.1 Vérification du système de sécurité et des dispositifs de protection

- 1) Vérifier que le type et la conception de la machine protégée sont compatibles avec ce système de protection, selon le [Chapitre 2](#).
 - 2) Vérifier l'installation et effectuer les procédures de vérification des systèmes de sécurité et de protection externes raccordés aux entrées du contrôleur de sécurité SC22-3 selon les descriptions des manuels correspondants. **Ne pas continuer tant que les procédures de vérification ne sont pas terminées et que tous les problèmes sont résolus.**
 - 3) Vérifier que l'accès à toutes les parties dangereuses de la machine protégée est impossible pour toute approche non protégée par le système de protection, la protection fixe ou les protections supplémentaires et que les protections supplémentaires et les protections fixes décrites par les normes applicables sont en place et fonctionnent correctement.
 - 4) Vérifier que tous les interrupteurs de réarmement sont montés à l'extérieur de la zone protégée tout en étant visible, hors de portée d'une personne située dans la zone protégée et que le moyen d'éviter une utilisation non prévue est en place.
 - 5) Examiner les raccordements électriques entre les sorties OSSD du Contrôleur de sécurité SC22-3 et les commandes de la machine protégée pour vérifier que le câblage est conforme aux conditions exprimées au [Paragraphe 4.8 en page 34](#).
 - 6) Vérifier que tous les dispositifs de commande bimanuelle, dispositifs de commande, capteurs d'inhibition et interrupteurs de bypass sont en état inactif (Stop).
- ☛ *Dans tous les cas, les sorties associées à un dispositif de commande bimanuelle ne doit pas passer sur ON à la mise sous tension. De même, les interrupteurs de bypass ou les dispositifs de commande en état (Run) actif à la mise sous tension ne doivent pas pouvoir fonctionner tant qu'ils ne sont pas passés par un état OFF d'abord.*
- 7) S'assurer que les autres dispositifs d'entrée sont en état actif (Run).

8.2.6.2 Fonctions de mise sous tension et de réarmement

- 1) S'assurer qu'aucune personne n'est exposée à un déplacement ou une situation dangereuse de la machine protégée pendant la procédure de vérification.
- 2) Observer les indicateurs d'état SO ou les messages de l'affichage pour vérifier si la sortie de sécurité est sur ON ou sur OFF.
- 3) Mettre le contrôleur de sécurité et tous les dispositifs d'entrée sous tension, mais **PAS** la machine protégée.
- 4) Vérifier que le fichier de configuration (par ex. le niveau de révision) correspond bien à l'application. Au minimum, conserver une copie du résumé de la configuration du logiciel d'interface du PC sous la main en tant que référence pendant la procédure de vérification.
- 5) Vérifier que les sorties d'état configurées pour une lampe d'inhibition surveillée (le cas échéant) passe brièvement sur ON (c'est-à-dire clignote) à la mise sous tension.

CONFIGURATION DES OPTIONS DE MISE SOUS TENSION

 Avant d'effectuer les étapes 1, 2 et 3, se référer aux paramètres du système du résumé de la configuration.

- 1) **Si la configuration est normale (par défaut)**, vérifier que seules les sorties de sécurité associées aux dispositifs d'entrée configurés pour un réarmement automatique passent sur ON.*
- 2) **Si la configuration est automatique**, vérifier que toutes les sorties de sécurité passent sur ON* en moins de 5 secondes (les sorties configurées avec une temporisation à l'enclenchement peuvent allonger ce délai).
- 3) **Si la configuration est manuelle :**
 - Vérifier que toutes les sorties de sécurité restent sur OFF
 - Attendre au moins 10 s après la mise sous tension, puis effectuer un réarmement système (pour plus d'informations sur les réarmements voir [Paragraphe 7.3 en page 69](#) & [Paragraphe 1.10 en page 5](#))
 - Vérifier que les sorties de sécurité passent sur ON* même si une entrée auxiliaire associée est configurée pour un réarmement manuel

*Dans tous les cas, les sorties de sécurité associées à une commande bimanuelle ne passent pas sur ON à la mise sous tension. Les dispositifs de commande et les interrupteurs de bypass ne sont pas disponibles à la mise sous tension. Ils doivent commencer à l'état Stop (OFF).

CONFIGURATION DU RÉARMEMENT

- 1) **Si configuré pour réarmement automatique**, vérifier que l'indicateur de la sortie de sécurité du contrôleur est vert    indiquant que la sortie de sécurité est sur ON (en supposant que les autres entrées configurées pour réarmement manuel ne sont pas associées à la sortie de sécurité ; voir [Réarmement manuel](#)).
Si l'indicateur d'état du contrôleur commence à clignoter en rouge  quel que soit l'instant, se référer au [Paragraphe 8.3.3 en page 77](#) pour les informations de dépannage.
 - 2) **Si configuré pour réarmement manuel**,
 - Vérifier que le voyant d'état du contrôleur clignote en vert  pour indiquer qu'un réarmement est demandé et que le message réarmement système nécessaire apparaît dans l'affichage de diagnostic. Si l'indicateur d'état du contrôleur commence à clignoter en rouge  quel que soit l'instant, se référer au [Paragraphe 8.3.3 en page 77](#) pour les informations de dépannage
-  Si un "réarmement manuel surveillé" a été configuré, effectuer un réarmement en fermant l'entrée de réarmement pendant au moins 0,25 s, mais pas plus de 2 s, puis en rouvrant le contact. Vérifier que l'indicateur d'état du contrôleur passe sur ON en vert continu .
- 3) Vérifier que tous les interrupteurs de réarmement sont montés à l'extérieur de la zone protégée tout en étant visible, hors de portée d'une personne située dans la zone protégée et qu'un moyen pour éviter une utilisation non prévue est en place.
 - 4) Actionner chaque dispositif de réarmement manuel (entrée auxiliaire) pour faire passer sur ON les sorties restantes non associées à un dispositif de commande bimanuelle.
 - 5) Vérifier que toutes les sorties de sécurité non associées à un dispositif de commande bimanuelle sont maintenant sur ON (exception : Une sortie associée seulement à un dispositif de commande restera sur OFF).

Si une fonction ou un dispositif décrit au [Paragraphe 8.2.6.3](#), [Paragraphe 8.2.6.4](#) ou au [Paragraphe 8.2.6.5](#) ne fait pas partie de l'application, sauter ce paragraphe et passer à la vérification suivante ou au [Paragraphe 8.2.6.11 en page 75](#).

8.2.6.3 Fonctions d'une commande bimanuelle

- 1) S'assurer que toutes les entrées sont en état ON associées aux sorties de sécurité et activer chaque dispositif de commande bimanuelle pour faire passer sur ON les sorties restantes.
 - Si les deux boutons de la commande bimanuelle ne sont **PAS** actionnés en moins de 0,5 s l'un de l'autre, vérifier que la sortie de sécurité associée reste sur OFF
 - Vérifier que, quand une main est enlevée et replacée, la sortie de sécurité passe sur OFF et reste sur OFF

8.2.6.4 Fonctions d'arrêt d'urgence et interrupteur à câble

- 1) Alors que les sorties sont sur ON, actionner individuellement et réarmer chaque dispositif d'arrêt d'urgence et d'interrupteur à câble à tour de rôle.
 - Vérifier que chaque sortie de sécurité associée passe sur OFF avec la temporisation OFF correspondante, le cas échéant
- 2) Quand le dispositif d'arrêt d'urgence ou d'interrupteur à câble est revenu à l'état Run (armé) :

Si configuré pour un réarmement manuel ou associé à une commande bimanuelle, vérifier que la sortie de sécurité reste sur OFF.

Si configuré pour un réarmement automatique (en supposant qu'un autre dispositif ne le retient pas sur OFF), vérifier que la sortie de sécurité passe sur ON.
- 3) Appliquer un réarmement manuel ou activer un dispositif de commande bimanuelle pour refaire passer les sorties sur ON.
 - Vérifier que chaque sortie de sécurité associée passe sur ON avec la temporisation ON correspondante, le cas échéant.

8.2.6.5 Autres fonctions de dispositifs d'arrêt

- 1) Recommencer les [Étape n° 1](#), [Étape n° 2](#) et [Étape n° 3](#) du [Paragraphe 8.2.6.4 en page 74](#) pour chaque type de dispositif suivant, le cas échéant :
 - Vérifier le fonctionnement de tous les interrupteurs de portes.
 - Vérifier le fonctionnement de tous les capteurs optiques.
 - Vérifier le fonctionnement de tous les tapis de sécurité.
 - Vérifier le fonctionnement de tous les arrêts de protection (comme les autres dispositifs de sécurité ou de protection non listés).
 - Vérifier le fonctionnement de toutes les entrées ON/OFF.

Si des fonctions de capteurs d'inhibition, d'interrupteurs de bypass ou de dispositifs de commande ne sont pas utilisés, avancer au [Paragraphe 8.2.6.11 en page 75](#).

8.2.6.6 Fonctions d'inhibition

- 1) Pendant que les sorties sont sur ON, initier un cycle d'inhibition en activant l'entrée d'inhibition (le cas échéant) puis activer chaque détecteur d'inhibition d'une paire de détecteurs d'inhibition en moins de 3 s.
 - Vérifier que la lampe d'inhibition, s'il y en a une, passe sur ON
- 2) Envoyer un ordre d'arrêt depuis le dispositif de protection qui a été inhibé.
 - Vérifier que les sorties de sécurité associées restent sur ON (l'indicateur d'état du contrôleur reste sur ON vert)
 - Si une limite de temps d'inhibition (minuteur arrière) est associé à l'inhibition, vérifier que les sorties de sécurité associées passent sur OFF quand la limite de temps d'inhibition expire.
- 3) Recommencer [Étape n° 1](#) et [Étape n° 2](#) pour chaque paire de détecteurs d'inhibition.
 - Vérifier le fonctionnement de chaque détecteur d'inhibition de chaque paire de détecteur d'inhibition
- 4) Générer un ordre d'arrêt des non inhibés un par un.
 - Vérifier que les sorties de sécurité associées passent sur OFF pendant que l'entrée est inhibée.

*La fonction d'inhibition s'arrête quand une sortie associée passe sur OFF pour une raison quelconque. Pour terminer ce test avec les autres dispositifs de protection non inhibés, il faut initier un nouveau cycle d'inhibition pour chacun.

8.2.6.7 Option d'inhibition à la mise sous tension

- 1) Couper l'alimentation du contrôleur de sécurité SC22-3.
 - Activer les entrées inhibées (le cas échéant)
 - Activer une paire de détecteurs d'inhibition appropriée pour démarrer un cycle d'inhibition
 - S'assurer que tous les dispositifs d'entrée sont en état Run (actifs) (à l'exception des dispositifs de commande bimanuelle)
 - Vérifier que tous les dispositifs de commande et les interrupteurs de bypass sont en état Stop (inactifs)
- 2) Vérifier le bon fonctionnement à la mise sous tension.
- 3) Si la mise sous tension est configurée sur auto :
 - Vérifier que toutes les sorties de sécurité passent sur ON*
 - Vérifier que la sortie de l'état d'inhibition (le cas échéant) passe sur ON
- 4) Si la mise sous tension est configurée sur normal :
 - Vérifier que toutes les sorties de sécurité associées seulement aux dispositifs de réarmement automatique ou aux dispositifs de réarmement manuel à inhiber passent sur ON*
 - Vérifier que la sortie d'état inhibé (le cas échéant) passe sur ON
- 5) Si la mise sous tension est configurée sur manuel :
 - Vérifier que toutes les sorties de sécurité restent sur OFF
 - Attendre au moins 10 s après la mise sous tension puis appliquer un réarmement système (voir [Paragraphe 7.4 en page 70](#))
 - Vérifier que toutes les sorties de sécurité passent sur ON*
 - Vérifier que la sortie d'état inhibé (le cas échéant) passe sur ON

*Dans tous les cas, les sorties de sécurité associées à un dispositif de commande bimanuelle ne passe pas sur ON à la mise sous tension. La caractéristique d'inhibition à la mise sous tension ne s'applique pas aux dispositifs de commande bimanuelle que l'on peut inhiber.

- 6) Envoyer un ordre d'arrêt depuis le dispositif de protection qui a été inhibé.
 - Vérifier que les sorties de sécurité associées restent sur ON (c'est-à-dire que l'entrée est inhibée) et que le voyant d'état reste aussi ON sur vert

8.2.6.8 Fonction d'interrupteur de bypass (avec inhibition)

- 1) Vérifier que chaque entrée de sécurité, si elle peut être à la fois inhibée et bypassée, est en état Stop :
 - Si le contrôleur de sécurité SC22-3 active toujours l'inhibition, les sorties de sécurité associées doivent rester sur ON. Même si le minuteur expire et que les sorties passent sur OFF, passer au point suivant
- 2) Activer un ou les deux détecteurs d'inhibition d'une paire de détecteurs d'inhibition. S'il y a deux paires de détecteurs d'inhibition, au moins un détecteur de chaque paire doit être activé :
 - Vérifier que la lampe d'inhibition, si elle existe, clignote
- 3) Vérifier que, quand l'interrupteur de bypass est en état Run :
 - Les sorties de sécurité associées passent sur ON
 - La lampe d'inhibition, si elle existe, est maintenant ON en permanence
 - Les sorties de sécurité associées passent sur OFF quand le minuteur de l'interrupteur de bypass expire
- 4) Vérifier que, quand l'interrupteur de bypass est en état Stop et repasse en état Run :
 - Les sorties de sécurité passent sur ON
- 5) Vérifier que, quand les autres entrées auxiliaires associées à la même sortie sont en état Stop, l'une après l'autre :
 - Les sorties de sécurité associées passent sur OFF pendant que l'entrée est bypassée

8.2.6.9 Fonction d'interrupteur de bypass (sans inhibition)

- 1) Vérifier que, quand l'entrée de sécurité à bypasser est en état Stop :
 - Les sorties de sécurité associées sont OFF
- 2) Vérifier que, quand l'interrupteur de bypass est en état Run :
 - Les sorties de sécurité passent sur ON
 - Les sorties de sécurité associées passent sur OFF quand le minuteur de bypass (minuteur de porte arrière) expire
- 3) Vérifier que, quand l'interrupteur de bypass est en état Stop et repasse en état Run :
 - Les sorties de sécurité associées passent sur ON
- 4) Envoyer une commande d'arrêt depuis un non bypassé, une à la fois :
 - Vérifier que les sorties de sécurité associées passent sur OFF pendant que l'entrée est bypassée

8.2.6.10 Fonction de dispositif de commande

- 1) Vérifier que toutes les entrées associées à la même sortie pendant que le dispositif de commande est en état Run font passer les sorties sur ON. Le dispositif de commande doit rester en état Stop :
 - Vérifier que les sorties de sécurité associées sont sur ON
- 2) Vérifier que, quand le dispositif de commande est en état Run :
 - Les sorties de sécurité associées restent sur ON et l'écran affiche mode actif
- 3) Vérifier que, quand le dispositif de commande est en état Stop :
 - Les sorties de sécurité associées passent sur OFF

- 4) Vérifier que, quand le dispositif de commande est en état Run :
 - Les sorties de sécurité passent sur ON
 - Les sorties de sécurité passent sur OFF quand le minuteur du dispositif de commande expire
- 5) Vérifier que, quand le dispositif de commande est en état Stop et revient en état Run :
 - Les sorties de sécurité passent sur ON
- 6) Vérifier que, quand toutes les entrées d'arrêt d'urgence et de interrupteur à câble associés aux mêmes sorties sont en état Stop, à tour de rôle (recommencer l'étape pour chaque dispositif) :
 - Les sorties de sécurité associées passent sur OFF en mode actif
- 7) Vérifier que le dispositif de commande est en état Stop puis appliquer un réarmement système (voir [Paragraphe 7.4 en page 70](#)):
 - Vérifier que l'écran n'affiche plus le mode actif
 - Vérifier que le contrôleur de sécurité est revenu en fonctionnement normal

8.2.6.11 Vérification (finale) du système

NE PAS poursuivre l'opération tant que tous les problèmes n'ont pas été corrigés.

Il faut maintenant vérifier le fonctionnement du contrôleur de sécurité avec la machine protégée avant de pouvoir mettre l'ensemble en service. Pour ce faire, une [Personne qualifiée selon spécification du paragraphe 1.8.2 en page 4](#) doit effectuer les vérifications suivantes.

Couper l'alimentation électrique du contrôleur de sécurité.

- 1) Couper l'alimentation électrique du contrôleur de sécurité.
- 2) En se référant à la [Figure 25 en page 71](#), rebrancher le connecteur des terminaux à 7 broches de la sortie de sécurité aux Sorties de sécurité SO1 (A et B), SO2 (A et B) et SO3 (A et B) du contrôleur de sécurité SC22-3 pour activer le raccordement au circuit de commande de la machine. **Il s'agit d'une connexion permanente.**
- 3) Vérifier que tous les câblages sont conformes aux normes EU et aux codes locaux de câblages.
- 4) Démarrer la machine protégée et vérifier qu'elle ne démarre pas.
- 5) Mettre le contrôleur de sécurité sous tension et effectuer les réarmements (voir [Paragraphe 7.4 en page 70](#)) nécessaires pour faire passer les sorties sur ON.
- 6) Envoyer un ordre d'arrêt depuis chaque dispositif de sécurité ou protection raccordée aux bornes d'entrée du contrôleur de sécurité et vérifier pour chaque dispositif d'entrée les points suivants :
 - Les sorties de sécurité et les sorties de sécurité fonctionnent comme prévu (par ex. retard à l'enclenchement, retard au déclenchement, etc.). Utiliser le résumé de la configuration pour vérifier le bon fonctionnement.
 - Il n'est pas possible de mettre en marche la machine protégée.

- 7) Initier le mouvement de la machine protégée et, pendant qu'elle fonctionne, générer un ordre d'arrêt depuis chaque dispositifs de protection ou de sécurité. Ne pas essayer d'introduire quoi que ce soit dans les parties dangereuses de la machine. À l'exécution de chaque ordre d'arrêt, vérifier que les parties dangereuses de la machine s'arrêtent.
- 8) Au réarmement du dispositif de protection ou de sécurité ou du contrôleur, vérifier que la machine ne redémarre pas automatiquement et que les dispositifs de démarrage doivent être utilisés pour la redémarrer.
- 9) Tester le temps de réponse de la machine protégée à l'aide d'un instrument conçu à cet effet. Vérifier si le temps de réponse effectif correspond aux données du fabricant de la machine ([Bureaux du siège social en page 125](#) doit être capable de recommander un instrument adapté).

Si le module muting ne passe pas l'une de ces vérifications, ne pas l'utiliser avant d'avoir identifié et rectifié la ou les anomalies.

8.3 MAINTENANCE CORRECTRICE

8.3.1 Nettoyage

- 1) Couper l'alimentation du contrôleur.
- 2) Avec un chiffon non pelucheux humidifié d'une solution de détergent doux dans de l'eau tiède, nettoyer le boîtier en polycarbonate et l'écran.

8.3.2 Réparations et service sous garantie

Le contrôleur a été conçu et testé pour bien résister à une grande variété de parasites électriques que l'on trouve dans les installations industrielles. Cependant des sources de parasites électriques intenses qui produisent des EMI ou RFI au-delà de ces limites peuvent entraîner un déclenchement aléatoire ou un blocage.

Si des déclenchements ou des blocages aléatoires se produisent, vérifier ce qui suit :

- L'alimentation électrique est bien sous 24 Vcc +/- 20%
- Les borniers enfichables du contrôleur de sécurité sont bien insérés (voir la [Figure 25 en page 71](#))
- Les connexions de chaque borne individuelle sont bien faites
- Y a-t-il des sources de parasites sous haute tension, à haute fréquence ou des lignes à haute tension qui passent à proximité du contrôleur ou le long de câbles qui sont raccordés au contrôleur
- Une suppression de parasites est appliquée aux bornes des charges de sortie (voir [AVERTISSEMENT, page 12](#))

Le contrôleur de sécurité SC22-3 n'a pas de pièces internes qui peuvent être remplacés sur le site. Si le contrôleur ne fonctionne pas correctement, contacter [Bureaux du siège social en page 125](#). En cas d'erreur non récupérable, ne pas ouvrir le boîtier du contrôleur et ne pas essayer de démonter le contrôleur en aucune façon. Contacter [Bureaux du siège social en page 125](#).

Un ingénieur d'application essaiera de dépanner le contrôleur à distance en fonction du problème indiqué. S'il conclut que le contrôleur ou un de ses composants est défaillant et doit être renvoyé chez *Banner*, un numéro de RMA (autorisation de retour de marchandise) sera indiqué avec les instructions d'expédition. Le contrôleur doit être emballé soigneusement. Les dégâts qui se produiraient pendant l'expédition de renvoi ne sont pas couverts par la garantie.

8.3.3 Recherche de pannes

En fonction de la configuration, le contrôleur de sécurité est capable de détecter un certain nombre de panes d'entrée, de sortie et du système :

- 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 d'alimentation

Si une défaillance est détectée, un message décrivant la faute est affiché dans le menu de diagnostic d'erreur. Un message supplémentaire peut aussi être affiché pour aider à dépanner.

Le dépannage [Tableau 17 en Page 77](#) résume les défaillances et suggère des vérifications supplémentaires pour trouver la cause du problème. Les paragraphes suivants expliquent comment récupérer après un blocage et comment accéder aux informations de la défaillance, au moyen du PCI ou de l'OBI.

Tableau 17 Explications des indications de diagnostic

| Code d'erreur | Message affiché | Vérification initiale | Étapes et vérifications suivantes |
|---------------|------------------------|----------------------------------|---|
| 0.0 | Erreur d'entrée | Entrée de cycle | <ul style="list-style-type: none"> • Rechercher un signal d'entrée instable • Faire passer l'entrée sur OFF pour effacer l'indication d'erreur |
| 1.1 | Sortie/erreur | Rechercher les courts-circuits | <p>Il apparaît qu'une sortie de sécurité est ON à la mise sous tension alors qu'elle devrait être OFF.</p> <ul style="list-style-type: none"> • Rechercher un court-circuit de la source électrique extérieure • Vérifiez la taille du fil commun (DC) connectée aux charges de la sortie de sécurité. Le fil doit être de section suffisante et aussi court que possible pour réduire la résistance et la chute de tension. Au besoin, utilisez un fil commun (DC) séparé pour chaque paires de sorties et/ou évitez de partager le commun avec d'autres dispositifs (voir Paragraphe 4.8.3 en page 35) |
| 1.2 | Sortie/erreur | Rechercher les courts-circuits | <p>Une sortie de sécurité détecte une erreur d'une autre source de tension</p> <ul style="list-style-type: none"> • Rechercher un court-circuit entre les sorties de sécurité • Rechercher un court-circuit de la source électrique extérieure • Vérifier la compatibilité des dispositifs de charge (capacité trop élevée) • Vérifiez la taille du fil commun (DC) connectée aux charges de la sortie de sécurité. Le fil doit être de section suffisante et aussi court que possible pour réduire la résistance et la chute de tension. Au besoin, utilisez un fil commun (DC) séparé pour chaque paires de sorties et/ou évitez de partager le commun avec d'autres dispositifs (voir Paragraphe 4.8.3 en page 35) |
| 1.3 – 1.4 | Défaut interne | — | Défaut interne – Contacter Banner Bureaux du siège social en page 125. |
| 1.5 | Sortie/erreur | Vérifiez le câblage de rendement | <p>Une sortie de sécurité s'affiche à ON prématurément.</p> <ul style="list-style-type: none"> • Vérifiez la taille du fil commun (DC) connectée aux charges de la sortie de sécurité. Le fil doit être de section suffisante et aussi court que possible pour réduire la résistance et la chute de tension. Au besoin, utilisez un fil commun (DC) séparé pour chaque paires de sorties et/ou évitez de partager le commun avec d'autres dispositifs (voir Paragraphe 4.8.3 en page 35) |
| 1.6 | Défaut interne | — | Défaut interne – Contacter Banner Bureaux du siège social en page 125. |
| 1.7 | Sortie/erreur | Rechercher les courts-circuits | <p>Une surcharge est détectée aux sorties de sécurité.</p> <ul style="list-style-type: none"> • Rechercher un court-circuit à chaque borne de sortie à la masse ou une surcharge (un défaut sur une seule sortie peut faire que les autres sorties indiquent un défaut) • Comparer la puissance de l'alimentation du système aux besoins des charges |
| 1.8 | Défaut interne | — | Défaut interne – Contacter Banner Bureaux du siège social en page 125. |
| 2.1 | Défaut de séquence | Entrée de cycle | <p>Sur une entrée d'un canal double avec les deux entrées en état Run, une entrée est passée en état Stop puis de nouveau sur Run.</p> <ul style="list-style-type: none"> • Vérification du câblage • Vérifier les signaux d'entrée • Considérer le réglage des temps d'anti-rebond |
| 2.2 | Défaut de simultanéité | Entrée de cycle | <p>Sur une entrée d'un canal double, une entrée est passée en état Run mais l'autre n'a pas suivi dans les 3 secondes.</p> <ul style="list-style-type: none"> • Vérification du câblage • Vérifier la séquence de temps du signal d'entrée |

Tableau 17 Explications des indications de diagnostic

| Code d'erreur | Message affiché | Vérification initiale | Étapes et vérifications suivantes |
|---------------|------------------------|-----------------------|--|
| 2,3 ou 2,5 | Défaut de séquence | Entrée de cycle | Sur une paire complémentaire dont les deux entrées sont en état Run, une des entrées est passée sur Stop puis est revenue surRun. <ul style="list-style-type: none"> • Vérification du câblage • Vérifier les signaux d'entrée • Vérifier l'alimentation fournissant les signaux d'entrée • Considérer le réglage des temps d'anti-rebond |
| 2,4 ou 2,6 | Défaut de simultanéité | Entrée de cycle | Sur une paire complémentaire, une entrée est passée en état Run mais l'autre n'a pas suivi dans la limite de temps. <ul style="list-style-type: none"> • Vérification du câblage • Vérifier la séquence de temps du signal d'entrée |
| 2.7 | Défaut interne | Vérifier la borne xx | Défaut interne – Contacter Banner Bureaux du siège social en page 125 . |
| 2.8 – 2.9 | Erreur d'entrée | Vérifier la borne xx | L'entrée est bloquée sur élevée. <ul style="list-style-type: none"> • Rechercher des courts-circuits vers les autres entrées ou une autre source de tension • Vérifier la compatibilité des dispositifs d'entrée |
| 2.10 | Erreur d'entrée | Vérifier la borne xx | Rechercher un court-circuit entre les entrées. |
| 2.11 – 2.12 | Erreur d'entrée | Vérifier la borne xx | Rechercher un court-circuit avec la masse. |
| 2.13 | Erreur d'entrée | Vérifier la borne xx | L'entrée est bloquée sur bas. <ul style="list-style-type: none"> • Rechercher un court-circuit avec la masse. |
| 2.14 | Erreur d'entrée | Vérifier la borne xx | Impulsions de test manquantes. <ul style="list-style-type: none"> • Rechercher des courts-circuits vers les autres entrées ou une autre source de tension |
| 2.15 | Fil non branché | Vérifier la borne xx | Rechercher un fil non branché. |
| 2.16 – 2.18 | Erreur d'entrée | Vérifier la borne xx | Impulsions de test manquantes. <ul style="list-style-type: none"> • Rechercher des courts-circuits vers les autres entrées ou une autre source de tension |
| 2.19 | Fil non branché | Vérifier la borne xx | Rechercher un fil non branché. |
| 2.20 | Erreur d'entrée | Vérifier la borne xx | Impulsions de test manquantes. <ul style="list-style-type: none"> • Rechercher un court-circuit avec la masse. |
| 2.21 | Fil non branché | Vérifier la borne xx | Rechercher un fil non branché. |
| 2.22 – 2.23 | Erreur d'entrée | Vérifier la borne xx | Rechercher un signal instable à l'entrée. |
| 3.1 | Défaillance EDMxx | Vérifier la borne xx | Le contact EDM s'ouvre avant de faire passer les sorties de sécurité sur ON. <ul style="list-style-type: none"> • Rechercher un contacteur ou un relais bloqué sur ON • Rechercher un fil débranché |
| 3.2 | Défaillance EDMxx | Vérifier la borne xx | Les contacts EDM ne se sont pas fermés en moins de 200 ms après que les sorties de sécurité sont passées sur OFF. <ul style="list-style-type: none"> • Rechercher un contacteur ou un relais lent ou bloqué sur ON • Rechercher un fil débranché |
| 3.3 | Défaillance EDMxx | Vérifier la borne xx | Les contacts EDM s'ouvrent avant de faire passer les sorties de sécurité sur ON <ul style="list-style-type: none"> • Rechercher un contacteur ou un relais bloqué sur ON • Rechercher un fil débranché |
| 3.4 | Défaillance EDMxx | Vérifier la borne xx | La paire de contacts EDM n'est pas identique pendant plus de 200 ms. <ul style="list-style-type: none"> • Rechercher un contacteur ou un relais lent ou bloqué sur ON • Rechercher un fil débranché |
| 3.5 | Défaillance EDMxx | Vérifier la borne xx | Rechercher un signal instable à l'entrée. |
| 3.6 | Défaillance EDMxx | Vérifier la borne xx | Rechercher un court-circuit avec la masse. |
| 3.7 | Défaillance EDMxx | Vérifier la borne xx | Rechercher un court-circuit entre les entrées. |

Tableau 17 Explications des indications de diagnostic

| Code d'erreur | Message affiché | Vérification initiale | Étapes et vérifications suivantes |
|---------------|--|------------------------------------|--|
| 4.1 | Tension d'alimentation trop faible | Vérifier l'alimentation électrique | La tension d'alimentation est tombée sous la tension de référence pendant plus de 6 ms. <ul style="list-style-type: none"> • Vérifier la tension d'alimentation et la référence du courant • Rechercher une surcharge des sorties qui pourrait limiter le courant de l'alimentation |
| 4.2 | Défaut interne | — | Un paramètre de configuration est corrompu. Pour réparer la configuration : <ul style="list-style-type: none"> • Remplacer la configuration par une copie de sauvegarde en provenance de PCI ou de la carte XMou • Effacer et recréer la configuration avec OBI |
| 4.3 – 4.11 | Défaut interne | — | Défaut interne – Contacter Banner Bureaux du siège social en page 125 . |
| 4.12 | Limite de temps de la configuration dépassée | Vérifier la configuration | Le contrôleur de sécurité est resté en mode de configuration pendant plus d'une heure sans intervention sur les touches. |
| 4.13 | Limite de temps de la configuration dépassée | Vérifier la configuration | Le contrôleur de sécurité est resté en mode de configuration pendant plus d'une heure sans recevoir d'ordre de l'interface PC. |
| 4.14 | Configuration non confirmée | Vérifier la configuration | La configuration n'a pas été confirmée après avoir été modifiée. <ul style="list-style-type: none"> • Confirmer la configuration avec l'OBI ou le PCI |
| 4.15 – 4.19 | Défaut interne | — | Défaut interne – Contacter Banner Bureaux du siège social en page 125 . |
| 4.20 | Borne non assignée à l'usage | Vérifier la borne xx | Cette borne n'est pas assignée à un dispositif dans la configuration actuelle et ne devrait pas être active. <ul style="list-style-type: none"> • Vérification du câblage |
| 4.21 – 4.32 | Défaut interne | — | Défaut interne – Contacter Banner Bureaux du siège social en page 125 . |
| 5.1 | Défaillance de lampe d'inhibition | Vérifier la lampe et le câblage | La tension mesurée à la sortie d'état doit être basse quand la lampe est OFF et elle est mesurée élevée, indiquant un circuit interrompu de la lampe d'inhibition. |
| 5.2 | Défaillance de lampe d'inhibition | Rechercher les courts-circuits | La tension mesurée à la sortie d'état doit être élevée quand la lampe est ON et elle est mesurée basse, indiquant un court-circuit dans la lampe d'inhibition. |
| 5.3 | Défaut interne | — | Défaut interne – Contacter Banner Bureaux du siège social en page 125 . |
| 6xx | Défaut interne | — | Données de configuration invalides. Défaillance interne possible. <ul style="list-style-type: none"> • Essayer de charger une nouvelle configuration depuis le PCI, l'OBI ou la carte XM |

8.3.3.1 Récupération suite à un blocage

Pour récupérer suite à une situation de blocage effectuer une ou plusieurs des étapes suivantes :

- 1) Sur l'écran du contrôleur de sécurité, effectuer un affichage d'erreur À L'ÉCRAN (par ex. entrée de cycle).
- 2) Suivre les recommandations du dépannage [Tableau 17 en Page 77](#) sous étapes et vérifications suivantes.
- 3) Effectuer un réarmement système (voir [Paragraphe 7.4 en page 70](#)).
- 4) Couper l'alimentation et la rétablir et effectuer un réarmement système (voir [Paragraphe 7.4 en page 70](#)) si nécessaire.

Si ces mesures ne corrigent pas la situation de blocage, contacter Banner [Bureaux du siège social en page 125](#).

8.3.3.2 Diagnostic d'erreur par le PCI

Pour diagnostiquer des erreurs par l'intermédiaire du PCI:

- 1) S'assurer que le PC est raccordé au contrôleur de sécurité SC22-3 par le câble USB fourni, que le programme fourni avec le contrôleur de sécurité SC22-3 est chargé et que le matériel du contrôleur de sécurité a été reconnu par le PC.
- 2) En se référant aux instructions détaillées dans le [Paragraphe 5.1.2 en page 37](#), ouvrir le programme PCI .
- 3) En se référant à [Paragraphe 5.1.23 en page 52](#), ouvrir l'écran affichage live.

L'écran affichage live donne des informations en temps réel (voir [Écran 36 en page 52](#)) comme suit :

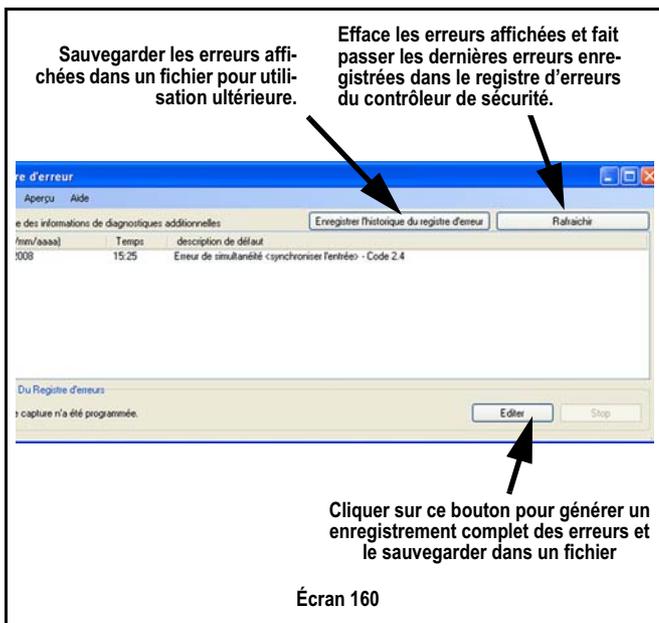
- État de chaque sortie de sécurité
- Le dispositif qui a mis la sortie sur OFF le cas échéant
- Des informations de base sur le modèle et la configuration du contrôleur

REGISTRE D'ERREURS — PCI

Pendant que le contrôleur est sous tension et relié au PC, toute erreur qui se produit est enregistrée dans le registre d'erreurs. Le PCI affiche en temps réel les informations concernant les erreurs dans l'écran du registre d'erreurs illustré en [Écran 160](#).

Pour accéder au registre d'erreurs :

- 1) Ouvrir le programme PCI
- 2) À partir du tableau, cliquer sur visionner et sur registre d'erreurs. [Écran 160](#) est illustré.



Le registre d'erreurs comprend les informations suivantes concernant chaque erreur (élargir la fenêtre pour voir toutes les erreurs).

- Date et heure de l'erreur
- Nom du dispositif
- Description générale de l'erreur et
- Le code d'erreur (pour la retrouver dans la table de référence)

Si l'assistance d'applications de l'usine est nécessaire, d'autres informations de codes peuvent s'afficher.

Capture du registre d'erreurs — PCI

Pour déterminer la cause d'une erreur persistante, un registre d'erreurs étendu peut être assemblé et sauvegardé dans un fichier

Pour accéder à cette fonction :

- 1) Ouvrir le registre d'erreurs comme décrit précédemment.
- 2) Dans le registre d'erreurs ([Écran 160](#)), cliquer sur le bouton modifier. Le menu de capture du registre d'erreurs [Écran 161](#) s'affiche alors.

Dans le [Écran 161](#), les paramètres du menu indiquent que toute erreur produite entre mardi 11 mars 2008 à 16 heures 34 et mardi 11 mars 2008 à 17 heures 34 sera enregistrée dans un fichier désigné par l'utilisateur pour utilisation ultérieure.

☛ Le temps de début et de fin doit être postérieur à l'instant auquel le choix est entré ; le registre d'erreurs ne peut pas capturer des erreurs passées.



Écran 161

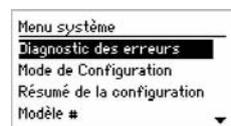
8.3.3.3 Diagnostic d'erreurs par OBI

Le diagnostic d'erreurs du contrôleur de sécurité SC22-3 et des dispositifs d'E/S associés peut aussi se faire en utilisant le OBI.

Tout événement qui fait qu'une sortie de sécurité passe sur OFF ou reste sur OFF (que ce soit une erreur ou des événements d'entrées d'arrêt) sera immédiatement détecté et affiché sur l'écran du contrôleur de sécurité. D'autres informations sur les erreurs en cours et passées peuvent être visionnées depuis le menu de diagnostic d'erreurs.

Pour accéder au menu de diagnostic d'erreurs du contrôleur de sécurité SC22-3 :

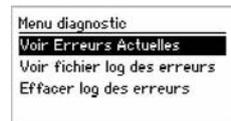
- 1) Dans le menu du mode Run, appuyer sur OK. [Screen 162](#) est illustré.
- 2) Dans le [Screen 162](#), sélectionner diagnostic d'erreurs et appuyer sur OK. [Screen 163](#) est affiché.



Screen 162

Dans le [Screen 163](#) le menu de diagnostic propose trois possibilités :

- Voir les erreurs actuelles
- Voir le registre des erreurs
- Effacer le registre des erreurs



Screen 163

Voir les erreurs actuelles

Pour voir les erreurs actuelles :

- 3) Avec les boutons des flèches haut et bas, sélectionner voir les erreurs actuelles et appuyer sur **OK**. L'écran affiche les conditions d'erreurs qui existent actuellement, une à la fois (Screen 164).
- 4) Utiliser les flèches gauche et droite pour voir les autres erreurs (Screen 165 et Screen 166) (astuce : Pour voir les erreurs en cours quand l'écran en mode Run est affiché, appuyer simplement sur **OK** trois fois).

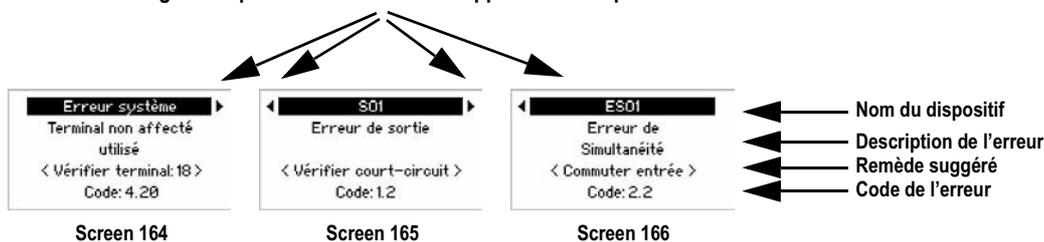
L'explication de voir les erreurs actuelles, illustré en Screen 164, Screen 165 et Screen 166, est la suivante :

- La ligne du haut indique le dispositif en erreur
- La seconde et la troisième lignes proposent une brève description de l'erreur
- La quatrième ligne suggère un moyen de corriger l'erreur
- La cinquième ligne donne le code d'erreur

Utiliser le code d'erreur et les informations du [Paragraphe 8.3.3 en page 77](#) et [Tableau 17 en Page 77](#) pour obtenir plus d'informations sur l'erreur et des suggestions supplémentaires pour la corriger.

- 5) Utiliser les boutons des flèches gauche et droite pour accéder aux informations des dispositifs défaillants.

La flèche désigne l'emplacement des écrans supplémentaires par défaut



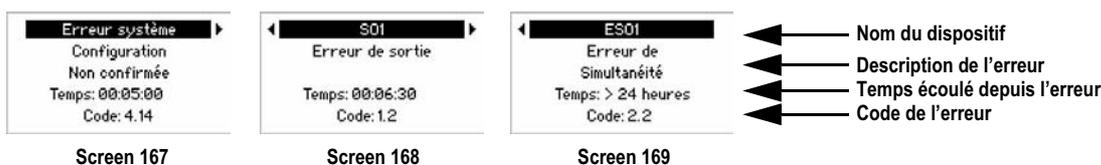
Voir le registre d'erreurs

Le contrôleur de sécurité conserve un enregistrement des dix dernières erreurs. Les erreurs peuvent être vues dans le menu voir le registre d'erreurs.

Pour voir le registre d'erreurs :

- 1) Dans le menu diagnostic (Screen 163), avec les boutons des flèches haut et bas, sélectionner voir le registre d'erreurs et appuyer sur **OK**. L'écran indique d'abord les erreurs enregistrées dans le registre d'erreurs (Screen 167).
- 2) Utiliser les flèches gauche et droite pour voir les autres erreurs du registre d'erreurs (Screen 168 et Screen 169).
 - La ligne du haut de l'écran du registre d'erreurs indique le dispositif en erreur
 - La seconde et la troisième lignes proposent une brève description de l'erreur
 - La quatrième ligne affiche depuis combien de temps s'est produite l'erreur. Par exemple, un temps de 01:30:23 indique que l'erreur s'est produite une heure, trente minutes et 23 secondes avant l'apparition du menu voir registre d'erreurs (si une erreur se rajoute au registre d'erreurs pendant qu'il est affiché, le temps est indiqué comme nouvelle erreur. Si une erreur s'est produite il y plus de vingt-quatre heures, le temps est affiché sous la forme > 24 heures)
 - La cinquième ligne indique le code d'erreur. Utiliser le code d'erreur et les informations du [Tableau 17 en Page 77](#) pour obtenir plus d'informations sur l'erreur et des suggestions supplémentaires pour la corriger

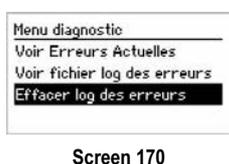
☛ Le fait de couper l'alimentation du contrôleur de sécurité efface le registre d'erreurs, en plus de la méthode décrite en [Effacer registre d'erreurs](#).



Effacer le registre d'erreurs

Pour effacer le registre d'erreurs :

- 1) Dans le menu diagnostic (Screen 170), sélectionner effacer le registre d'erreurs et appuyer sur **OK**. Screen 171 est affiché.



- 2) Quand l'erreur est corrigée, indiqué par Screen 171, appuyer sur **OK** pour revenir au menu diagnostic, puis appuyer deux fois sur **ESC** pour revenir au menu du mode Run.



8.4 PIÈCES DE RECHANGE, OUTILS SPÉCIAUX ET ACCESSOIRES

8.4.1 Pièces détachées

Ce paragraphe donne des informations sur les pièces de rechange du Contrôleur de sécurité SC22-3.

8.4.1.1 Kit de démarrage du contrôleur de sécurité

Le kit comprend le contrôleur de sécurité SC22-3 :

- Jeu de borniers amovibles (à vis ou à pinces selon le modèle)
- Câble USB A/B (pour un raccordement direct entre le PC et le contrôleur, inclus dans certains kits)
- Carte de mémoire non volatile externe (carte XM, avec étiquette pour écrire dessus à l'envers)
- Outil de programmation de la carte XM (inclus avec certains modèles)
- CD (inclus l'interface logiciel, le manuel en ligne et les tutoriaux de configuration)
- Guide de démarrage rapide

Tableau 18 en Page 82 donne des informations sur les kits.

Tableau 18 Informations sur le kit et les accessoires du contrôleur de sécurité SC22-3

| Type n° | Description | Référence | |
|---|--|-----------|--|
| Kit de démarrage du contrôleur de sécurité | | | |
| SC22-3-S | Bornes à vis, carte XM | 30 772 59 | |
| SC22-3-C | Bornes à pinces, carte XM | 30 779 13 | |
| SC22-3-SU1 | Bornes à vis, carte XM, outil de programmation de la carte XM et câble USB A/B inclus | 30 779 14 | |
| SC22-3-CU1 | Bornes à pinces, carte XM, outil de programmation de la carte XM et câble USB A/B inclus | 30 779 15 | |
| Pièces de rechange, accessoires | | | |
| SC22-3 | Contrôleur de rechange (sans bornes) | 30 797 15 | |
| SC-XM1 | Carte de mémoire externe (carte XM) | 30 761 77 | |
| SC-XM1-5 | Ensemble de 5 cartes de mémoire XM | ULT* | |
| SC-XMP | Outil de programmation USB des cartes XM | 30 777 08 | |
| SC-TS1 | Bornier à vis (1 jeu pour 1 contrôleur de sécurité) | 30 778 12 | |
| SC-TC1 | Bornier à pince (1 jeu pour 1 contrôleur de sécurité) | 30 778 13 | |
| SC-TC1SC-USB1 | Câble USB A/B | ULT* | |
| - | CD comprenant le programme PCI et le manuel d'instructions | 134534 | |

*Ultérieurement

8.4.1.2 Relais de sécurité

Série SC-IM9

Série SC-IM9 Modules d'interface à utiliser avec le contrôleur de sécurité SC22-3 qui ont :

- Des contacts secs à utiliser avec des tensions ac/dc supérieures et une sortie 10 A
- Boîtier à montage DIN
- Bornier amovible (à enficher) pour sorties OSSD (bornier à vis fourni)
- Mesure environ. 72 mm H, 170 mm P, et 45 mm, 90 mm, ou 140 mm L selon le modèle

☛ Il est nécessaire de câbler EDM séparément aux contacts N.F. pour être conforme à la fiabilité ISO 13849, catégorie 1 (voir [Paragraphe 4.8 en page 34](#)).

Tableau 19 en Page 83 donne des informations sur les différents modules.

Tableau 19 Modules d'interface Série SC-IM9

| Type n° | Description | Tension de service | Entrées (Sorties Contrôleur de sécurité) | Sorties de sécurité | Valeurs de sorties | Contacts EDM | Référence |
|---------|---|----------------------------|--|--------------------------------|--------------------|---|-----------|
| SC-IM9A | À utiliser avec une sortie de sécurité du contrôleur de sécurité SC22-3 | 24 Vcc (Contrôleur fourni) | x2 (SO1) | x3 N.O. | 10 A | 1 N.F. selon sortie (2 contacts en série) | 30 778 14 |
| SC-IM9B | À utiliser avec 2 sorties de sécurité du contrôleur de sécurité SC22-3 | | 4 (SO1 et SO2) | Total de 6 (3 N.O. par sortie) | | | 30 778 15 |
| SC-IM9C | À utiliser avec 3 Sorties de sécurité du contrôleur du SC22-3 | | x6 (SO1, SO2 & SO3) | Total de 9 (3 N.O. par sortie) | | | 30 778 23 |

Série IM-T-9

Les modules d'interface série IM-T-9 ont :

- Sortie 6 A
- Boîtier 22,5 mm à montage DIN
- Bornier amovible (enfichable)
- Courant bas de 1 V ac/dc sous 5 mA
- Courant fort de 250 V ac/dc sous 6A

☛ Il est nécessaire de câbler EDM séparément aux contacts N.F. pour être conforme à la fiabilité ISO 13849, catégorie 1 (voir [Paragraphe 4.8 en page 34](#)).

Tableau 20 en Page 83 donne des informations sur les différents modules.

Tableau 20 Modules d'interface Série IM-T-9

| Type n° | Tension d'alimentation | Entrées | Sorties de sécurité | Valeurs de sorties | Contacts EDM | Sorties auxiliaires non sécurisées | Référence |
|----------|------------------------|----------------------------|---------------------|--------------------|--------------|------------------------------------|-----------|
| IM-T-9A | 24V DC | 2 (double canal connexion) | x3 N.O. | 6:00 AM | x2 N.C. | — | 30 614 25 |
| IM-T-11A | | | x2 N.O. | | | x1 N.C. | 30 614 24 |

8.4.1.3 Contacts reliés mécaniquement

Fournit une capacité de transport supplémentaire de 10 A ou de 16 A vers un système de sécurité. Si on les utilise, deux contacts par paire de sorties de sécurité (par ex. 2 x SO1) sont nécessaires. Les contacts N.F. doivent être utilisés dans un circuit EDM (voir [Figure 28 en page 85](#)).

[Tableau 21 en Page 84](#) donne des informations sur les différentes versions.

Tableau 21 Contacts reliés mécaniquement

| Type n° | Tension d'alimentation | Entrées | Sorties | Valeurs de sorties | Référence |
|------------------|------------------------|----------------------------|-------------------------|--------------------|-----------|
| 11-BG00-31-D-024 | 24V DC | 2 (double canal connexion) | x3 N.O. + x1 N.C. | 10:00 AM | 30 696 82 |
| 11-BF16C01-024 | | | | 16 A | 30 696 87 |

8.4.2 Documentation

[Tableau 22 en Page 84](#) détaille la documentation applicable au contrôleur de sécurité SC22-3.

Tableau 22 Références de la documentation

| Référence | Description |
|-----------|---|
| 135369 | Notice d'utilisation (version européenne anglaise) |
| 135453 | Notice d'utilisation (version européenne française) |
| 135454 | Notice d'utilisation (version européenne allemande) |
| 135455 | Notice d'utilisation (version européenne italienne) |
| 133485 | Guide de mise en service rapide (anglais) |

A1 SCHÉMAS DE CÂBLAGE

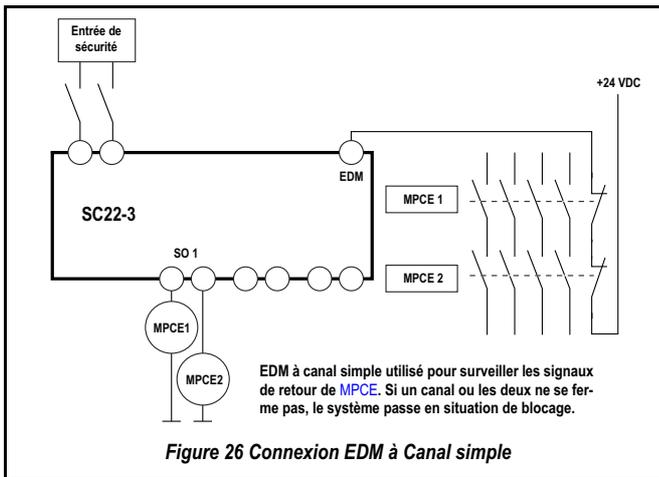


Figure 26 Connexion EDM à Canal simple

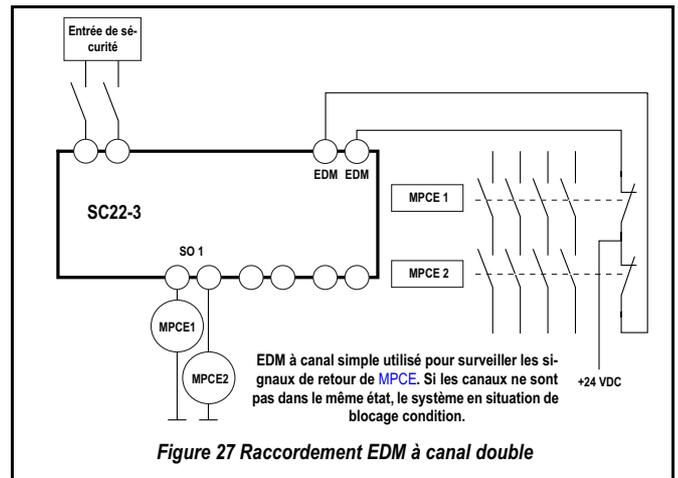


Figure 27 Raccordement EDM à canal double

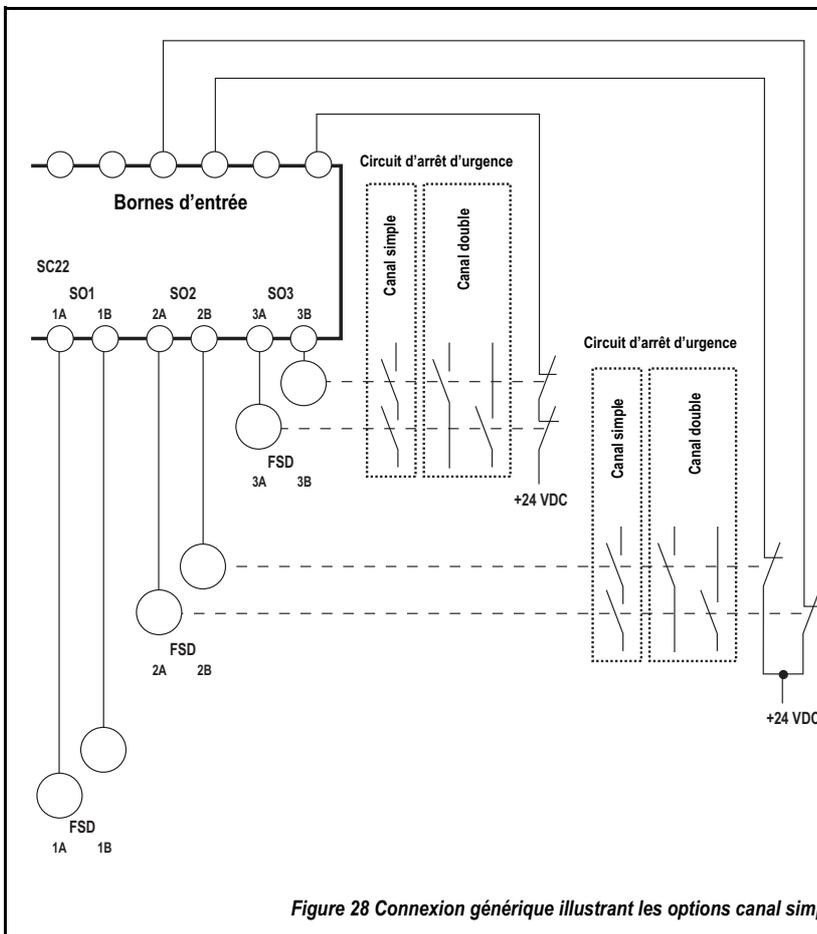


Figure 28 Connexion générique illustrant les options canal simple, canal double et pas de EDM

AVERTISSEMENTS

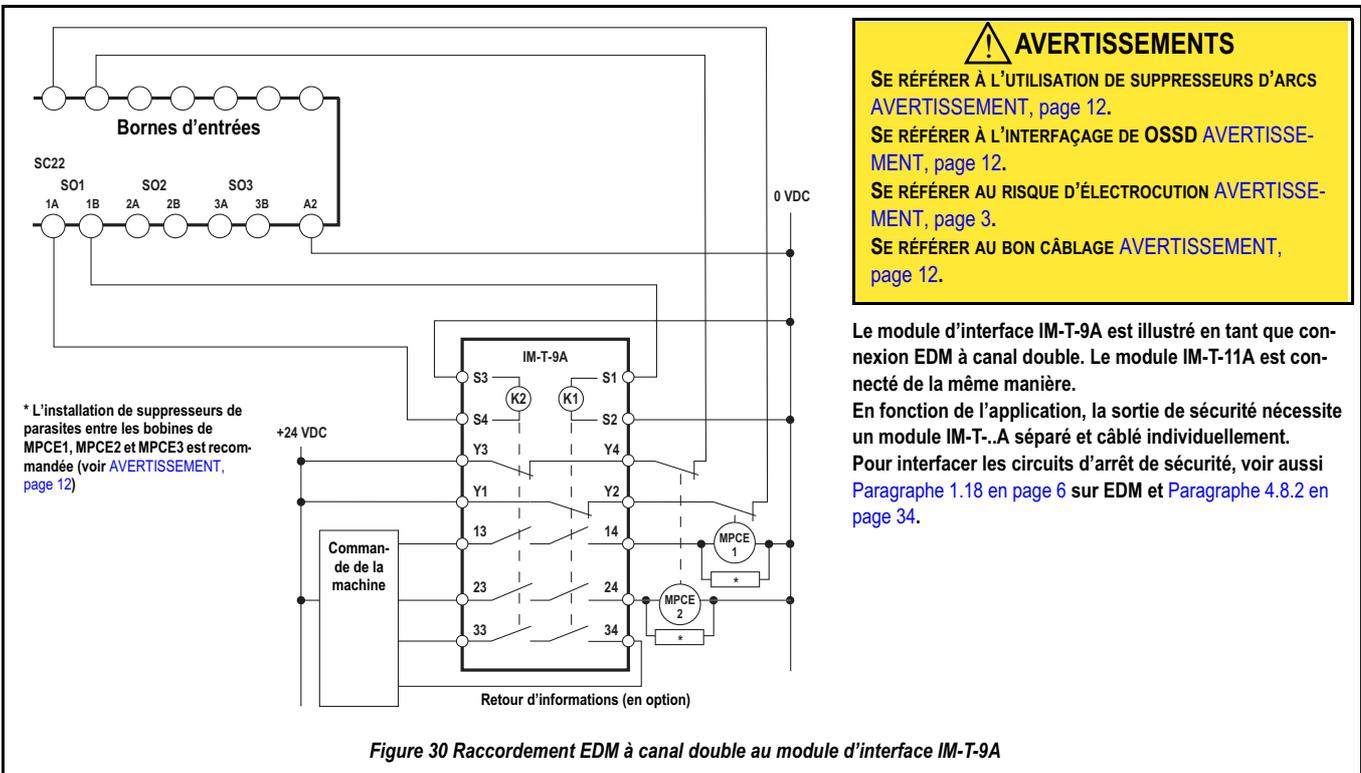
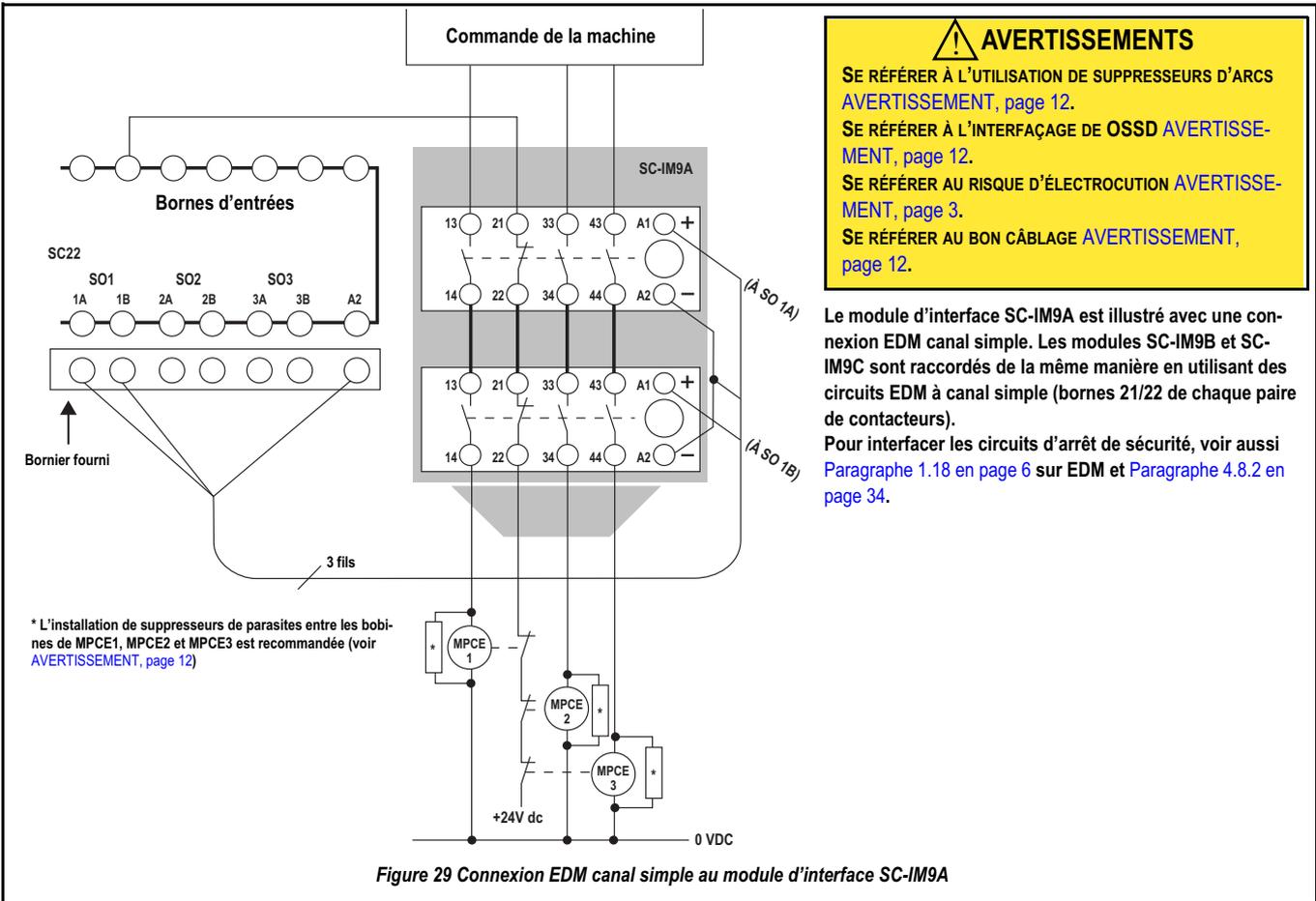
- SE RÉFÉRER À L'UTILISATION DE SUPPRESSEURS D'ARCS [AVERTISSEMENT](#), page 12.
- SE RÉFÉRER À L'INTERFAÇAGE DE OSSD [AVERTISSEMENT](#), page 12.
- SE RÉFÉRER AU RISQUE D'ÉLECTROCUTION [AVERTISSEMENT](#), page 3.
- SE RÉFÉRER AU BON CÂBLAGE [AVERTISSEMENT](#), page 12.

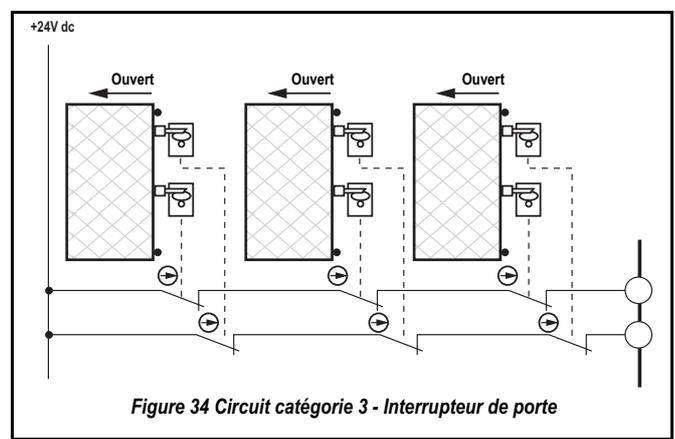
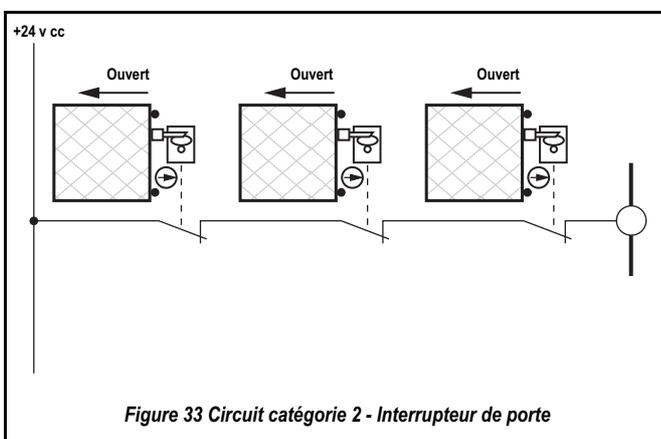
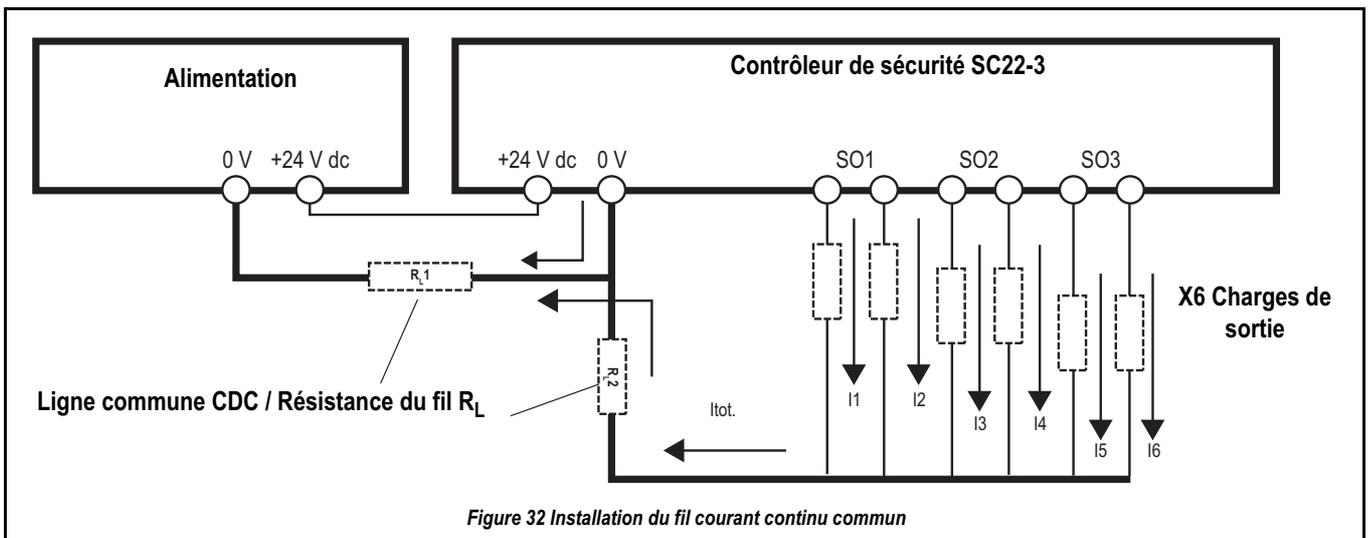
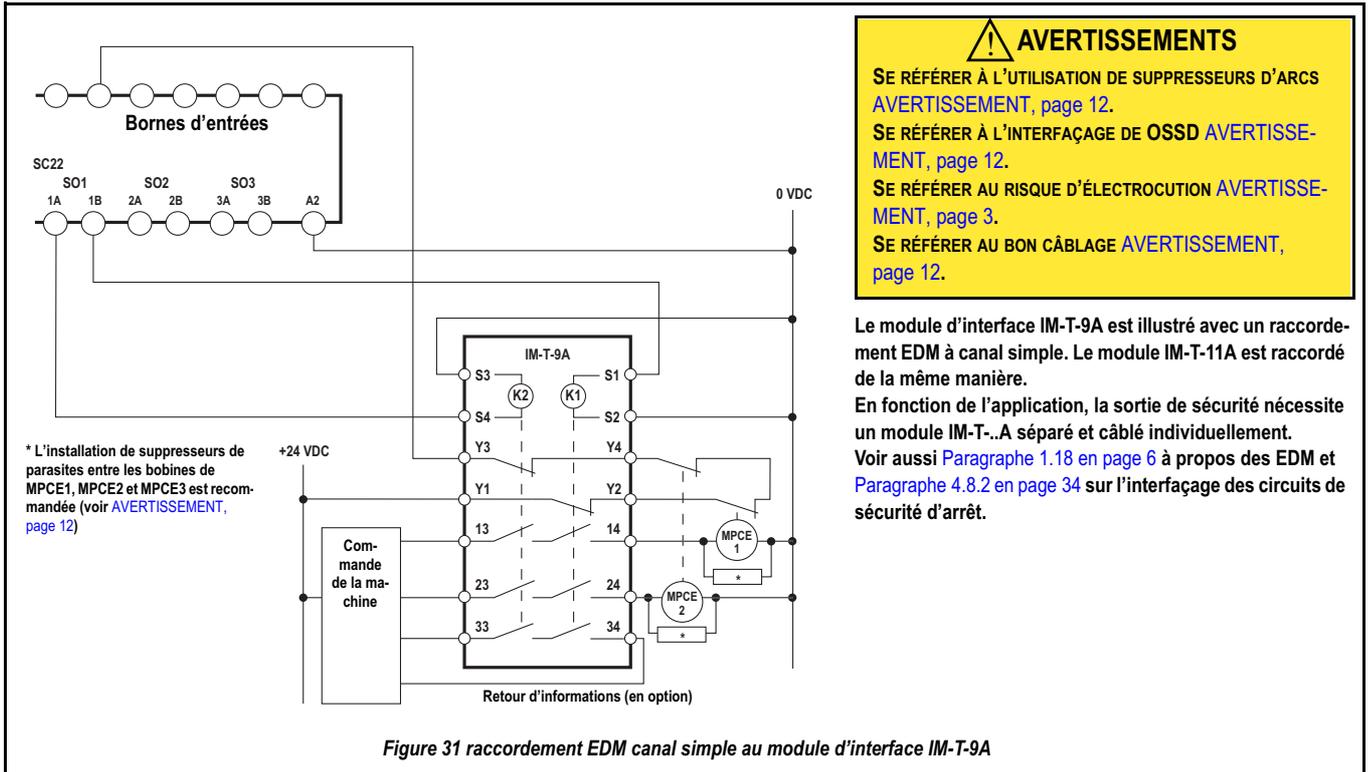
Cette illustration est générique et représente toutes les trois options EDM :

- La sortie de sécurité SO1 est illustrée SANS EDM configuré (utilisé normalement avec des dispositifs à auto surveillance)
- La sortie de sécurité SO2 est illustrée avec EDM à canal double configuré
- La sortie de sécurité SO3 est illustrée avec EDM à canal simple configuré

Toute configuration particulière du contrôleur de sécurité peut utiliser n'importe quelle combinaison d'options de surveillance des dispositifs externes en fonction de l'application.

Voir aussi [Paragraphe 1.18 en page 6](#) à propos des EDM et [Paragraphe 4.8.2 en page 34](#) sur l'interfaçage des circuits de sécurité d'arrêt.





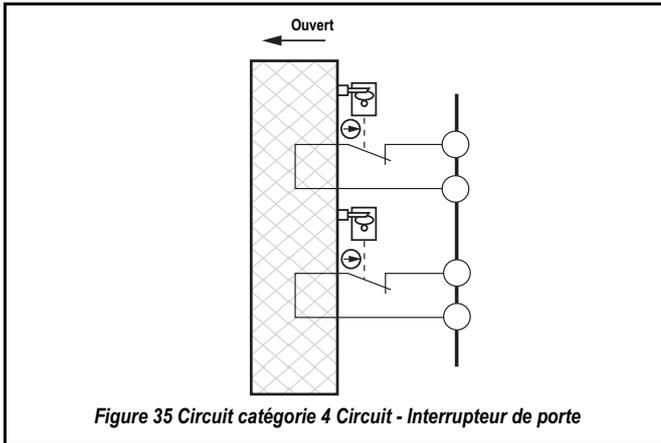


Figure 35 Circuit catégorie 4 Circuit - Interrupteur de porte

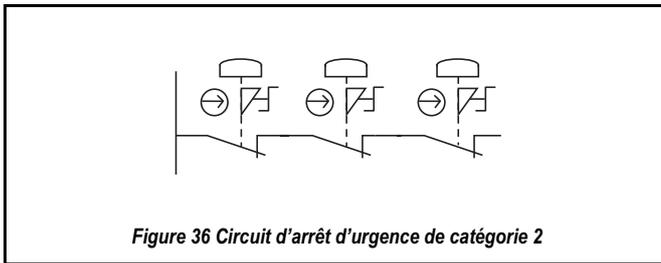


Figure 36 Circuit d'arrêt d'urgence de catégorie 2

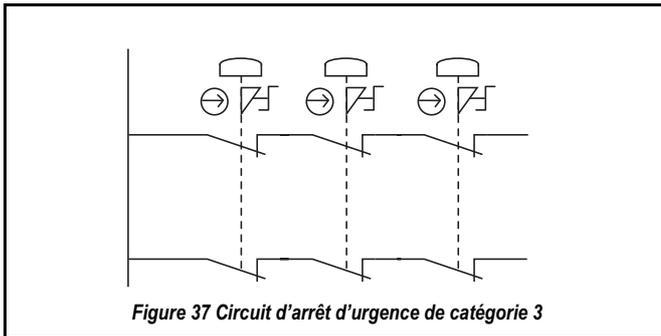


Figure 37 Circuit d'arrêt d'urgence de catégorie 3

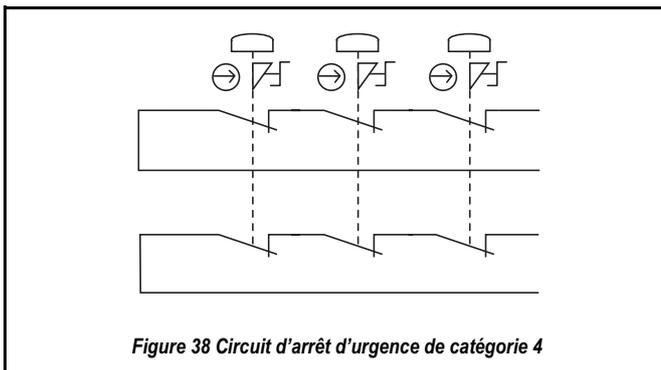


Figure 38 Circuit d'arrêt d'urgence de catégorie 4

A2 DISPOSITIF D'ENTRÉE ET CATÉGORIE DE SÉCURITÉ REFERENCE

A2.1 INTÉGRITÉ DU CIRCUIT DE SÉCURITÉ ET ISO 13849-1 (EN954-1) PRINCIPES DE CIRCUIT DE SÉCURITÉ



AVERTISSEMENTS

CATÉGORIES DE SÉCURITÉ

LE NIVEAU D'INTÉGRITÉ DU CIRCUIT DE SÉCURITÉ PEUT ÊTRE FORTEMENT ALTÉRÉ PAR LA CONCEPTION ET L'INSTALLATION DES DISPOSITIFS DE SÉCURITÉ ET LES MOYENS D'INTERFAÇAGE DE CES DISPOSITIFS. UNE ÉVALUATION DES RISQUES DOIT ÊTRE RÉALISÉE AFIN DE DÉTERMINER LE NIVEAU D'INTÉGRITÉ DU CIRCUIT DE SÉCURITÉ OU LA CATÉGORIE DE SÉCURITÉ APPROPRIÉE TEL QUE DÉFINI PAR L'ISO 13849-1 (EN 954-1), ET CE AFIN DE GARANTIR LA RÉDUCTION DES RISQUES ET DE FAÇON À CE QUE TOUTES LES RÉGLEMENTATIONS CORRESPONDANTES SOIENT RESPECTÉES.

DISPOSITIFS D'ENTRÉE AVEC RACCORDEMENTS DES SORTIES TRANSISTORISÉES

LE CONTRÔLEUR DE SÉCURITÉ NE DÉTECTE PAS LES COURTS-CIRCUITS ENTRE LES ENTRÉES OU ENTRE UNE ENTRÉE ET UNE ALIMENTATION EN +24 V SI LES SIGNAUX D'ENTRÉE DE CES BORNES PROVIENNENT DE DISPOSITIFS D'ENTRÉE AVEC DES SORTIES TRANSISTORISÉES.

IL EST DE LA RESPONSABILITÉ DE L'UTILISATEUR D'UTILISER UN DISPOSITIF QUI PEUT DÉTECTER CES COURTS-CIRCUITS (PAR EX. LA BARRIÈRE IMMATÉRIELLE EZ-SCREEN® DE BANNER QUI PEUT DÉTECTER UN COURT-CIRCUIT ENTRE SES DEUX SORTIES TRANSISTORISÉES OU ENTRE CHAQUE SORTIE ET +24 V).

COURT-CIRCUITS D'ENTRÉE DE CATÉGORIE 2 OU DE CATÉGORIE 3
LA DÉTECTION D'UN COURT-CIRCUIT ENTRE DEUX CANAUX D'ENTRÉE (CONTACTS D'ENTRÉE, MAIS PAS LES CONTACTS COMPLÉMENTAIRES), S'ILS SONT ALIMENTÉS PAR LA MÊME SOURCE (PAR EX. LA MÊME BORNE DU CONTRÔLEUR DANS UNE CONNEXION À CANAL DOUBLE, 3 BORNES OU DEPUIS UNE ALIMENTATION EXTERNE EN 24 V) N'EST PAS POSSIBLE, 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 2 SECONDES.

Les circuits de sécurité impliquent les fonctions associées à la sécurité d'une machine qui minimisent le niveau de risque de blessure. Ces fonctions de sécurité peuvent éviter l'initiation ou peuvent arrêter ou éliminer un danger. La défaillance d'une fonction de sécurité ou du circuit de sécurité associé entraîne généralement un plus haut risque de blessure.

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

En fonction du niveau de risque associé à la machine ou à son fonctionnement, un niveau de performance des circuits de sécurité approprié (par exemple l'intégrité) doit être intégré à la conception. Les normes européennes qui concernent les niveaux de performance de sécurité sont les normes ISO 13849-1 (EN 954-1) associées à la sécurité d'un système de surveillance.

A2.1.1 Niveaux d'intégrité des circuits de sécurité

Les circuits de sécurité dans les normes internationales et européennes ont été divisés en plusieurs catégories, en fonction de leur capacité à maintenir leur intégrité en cas de défaillance. La norme la plus reconnue, la norme ISO 13849-1 (EN 954-1), décrit les niveaux d'intégrité des circuits de sécurité. Elle définit cinq niveaux : les catégories B, 1, 2, 3 et la plus stricte, la catégorie 4.

Le niveau caractéristique d'intégrité du circuit de sécurité s'appelle la fiabilité de la commande. La fiabilité de la commande comprend normalement une commande redondante et un circuit à auto vérification qui correspond plus ou moins à ISO 13849-1 catégories 3 et 4.

Si les conditions décrites par la norme ISO 13849-1 (EN 954-1) doivent être appliquées en Europe, une évaluation des risques doit d'abord être réalisée pour déterminer la catégorie appropriée, afin de garantir la réduction du risque attendu. Cette évaluation des risques doit également prendre en compte les réglementations nationales telles que les normes européennes de niveau « C », afin de garantir que le niveau minimum de performance mandaté est respecté.

Les paragraphes suivants ([Annexe A2.2](#) à [Annexe A2.11](#)) ne traitent que des applications de la catégorie 2, la catégorie 3, et la catégorie 4, comme décrites par ISO 13849-1 (2006). [Tableau 23 en Page 90](#) donne une décomposition des catégories de sécurité possibles qui sont atteintes par chaque type de dispositif, en fonction de l'option de circuit choisie.

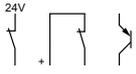
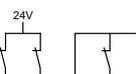
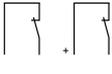
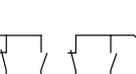
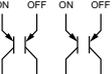
Pour plus d'informations, se référer à la partie restante de l'[Annexe A2](#) ainsi qu'aux normes applicables.

A2.1.2 Exclusion des défauts

Un concept important dans les conditions des catégories de l'ISO 13849-1 (EN 954-1) est la probabilité de survenue de la défaillance qui peut être réduite via une technique appelée exclusion des défauts. La justification (les raisons sous-jacentes) envisage la réduction de certaines défaillances bien définies à un niveau où le(s) défaut(s) résultants peuvent être, pour la plupart, écarté(s), c'est-à-dire exclu(s).

L'exclusion des défauts est un outil qu'un concepteur peut utiliser pendant le développement de la partie sécurisée du système de surveillance et le processus d'évaluation des défauts. L'exclusion des défauts permet de concevoir la possibilité de plusieurs défaillances et de la justifier par le processus d'évaluation des risques afin de répondre aux conditions d'alerte des catégories 2, catégories 3 ou catégories 4. Voir l'ISO 13849-1/-2 pour plus d'informations.

Tableau 23 dispositifs d'entrée, options des circuits et leurs catégories de sécurité possibles

| Exemples de symboles de circuits |  Arrêt d'urgence |  Interrupteur pour porte |  Détecteur optique |  Commande bimanuelle |  Interrupteur à câble |  Arrêt de protection |  Tapis sensible de sécurité |  Dispositif de commande |  Interrupteur de bypass |  Capteur d'inhibition |
|---|---|---|---|---|--|--|--|--|--|--|
|  | Catégorie 2 | Catégorie 2 | Catégorie 2 | — | Catégorie 2 | Catégorie 2 | — | — | — | — |
|  | Catégorie 3 | Catégorie 2 Catégorie 3 | Catégorie 2 Catégorie 3 | Type IIIa Cat. 1 Type IIIb Cat. 3 | Catégorie 3 | Cat. 2 Cat. 3 | — | Cat. 2 Cat. 3 | Cat. 2 Cat. 3 | Cat. 2 Cat. 3 |
|  | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | Type IIIa Cat. 1 | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | — | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 3 |
|  | Catégorie 4 | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | Type IIIa Cat. 1 Type IIIb Cat. 3 | Catégorie 4 | Cat. 2 Cat. 3 Cat. 4 | — | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 |
|  | — | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | — | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | — | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 |
|  | — | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | — | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | — | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 | Cat. 2 Cat. 3 Cat. 4 |
|  | — | Cat. 3 Cat. 4 | — | Type IIIc Cat. 4 | — | — | — | Cat. 3 Cat. 4 | Catégorie 4 | — |
|  | — | Cat. 3 Cat. 4 | — | Type IIIc Cat. 4 | — | — | — | Cat. 3 Cat. 4 | Catégorie 4 | — |
|  | — | — | — | — | — | — | Cat. 2 Cat. 3 | — | — | — |

☛ La catégorie B ou la catégorie 1 est supposée quand on n'utilise pas de dispositifs liés à la sécurité.
Tous les contacts de sécurité des dispositifs d'entrée sont illustrés en état ON, actif, (par ex. E-Stop en état armé, porte de sécurité fermée, barrière immatérielle sans obstruction, etc.).
La catégorie B/catégorie 1, la catégorie 2, la catégorie 3 et la catégorie 4 sont selon ISO 13849-1 (EN 954-1), sauf pour les commandes bimanuelles.
La catégorie de la commande bimanuelle est selon ISO 13851.

A2.2 ARRÊTS DE PROTECTION (SÉCURITÉ)



Un arrêt de protection (sécurité) est conçu pour raccorder différents dispositifs (non listés dans l'écran ajouter une entrée de sécurité) qui peut inclure des dispositifs de protection (protection) et des équipements complémentaires. Cette fonction d'arrêt est un type d'opération qui permet d'arrêter correctement le fonctionnement pour des raisons de protection. La fonction peut être activée manuellement ou automatiquement et réarmée manuellement ou automatiquement.

A2.2.1 Conditions

Le niveau voulu d'intégrité du circuit de sécurité est déterminé par une évaluation des risques qui indiquera le niveau de contrôle qui est acceptable (par ex. catégorie 4, fiabilité des commandes) (voir [Annexe A2.1 en page 89](#) et [Annexe A2.1.1 en page 89](#)). Le circuit d'arrêt de protection doit contrôler le risque protégé en provoquant un arrêt de la situation dangereuse et en coupant l'alimentation des actionneurs de la machine. C'est un arrêt fonctionnel typique de catégorie 0 ou de catégorie 1 selon IEC60204-1.

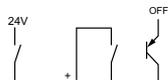
L'utilisateur doit suivre les instructions d'installation, de fonctionnement et d'entretien du fabricant et tous les règlements applicables. S'il demeure des questions au sujet des dispositifs à raccorder au contrôleur de sécurité SC22-3, appeler *Banner* Bureaux du siège social en page 125 pour obtenir une assistance.

A2.2.2 Possibilités de connexions

☛ **Toutes les figures montrent le dispositif d'entrée en état OFF (arrêt).**

A2.2.2.1 Canal simple, 1 borne – canal simple, 2 borne – canal simple, contact PNP

Ces circuits répondent normalement aux exigences de ISO 13849-1 catégorie 2, en fonction du niveau de sécurité des dispositifs de sortie. Au minimum, un dispositif de sécurité doit servir à atteindre la catégorie 2. Les circuits de dispositifs simple canal, 1 borne et simple canal, contact PNP ne peuvent pas détecter un court-circuit vers une autre alimentation. Les connexions simple canal, 2 bornes utilisent la surveillance des impulsions et peuvent détecter un court-circuit vers une autre alimentation. L'exclusion d'erreur doit être utilisée pour atteindre un niveau plus élevé d'intégrité de circuit de sécurité.



A2.2.2.2 Double canal, 2 bornes – Double canal, 3 bornes

Ce circuit répond normalement aux exigences de ISO 13849-1 catégorie 2 ou catégorie 3, en fonction du niveau de sécurité et de l'installation des dispositifs de sortie. Les connexions double canal, 3 bornes utilisent la surveillance d'impulsions et peuvent détecter un court-circuit vers une autre alimentation. Les connexions double canal, 2 bornes et double canal, 3 bornes peuvent détecter un court-circuit entre les canaux quand les contacts sont ouverts si le court-circuit dure plus de 2 secondes.



A2.2.2.3 Double canal, PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4 en fonction du niveau de sécurité, de l'installation et de la capacité de détection d'erreurs (par ex. court-circuit) du dispositif de sortie. Le contrôleur de sécurité SC22-3 ne fournit pas de détection de court-circuit dans cette configuration.



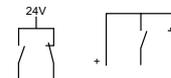
A2.2.2.4 Double canal, 4 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation du dispositif de sortie. Ce circuit peut détecter un court-circuit entre les canaux et vers une autre source d'alimentation.



A2.2.2.5 Complémentaire, 2 bornes – Complémentaire, 3 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4 en fonction du niveau de sécurité et de l'installation du dispositif de sortie. Ce circuit peut détecter un court-circuit entre les canaux. En situation activé (par ex. S1 ouvert / S2 fermé, voir le circuit ci-dessous), un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que spécifié, basé sur le temps d'anti-rebond (sélectionné) ([Paragraphe 4.5 en page 27](#)).



A2.2.2.6 complémentaire, contact PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4 en fonction du niveau de sécurité et de l'installation du dispositif de sortie. Ce circuit peut détecter un court-circuit entre les canaux. En situation activé (par ex. S1 OFF / S2 ON ci-dessous), un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que spécifié, basé sur le temps d'anti-rebond (sélectionné) ([Paragraphe 4.5 en page 27](#)).



A2.3 INTERRUPTEURS POUR PORTE (OU PROTECTION VERROUILLÉE)



Les entrées de sécurité du contrôleur de sécurité SC22-3 peuvent servir à surveiller des protections ou des portes verrouillées électriquement.

A2.3.1 Niveaux d'intégrité des circuits de sécurité

Les conditions du niveau de fiabilité de la commande ou de la catégorie de sécurité selon ISO 13849-1 (EN954-1) varient considérablement dans l'application des protections interverrouillées. Bien que *Banner Engineering* recommande toujours le niveau de sécurité le plus élevé pour toute application, l'utilisateur est seul responsable de la sécurité de l'installation, de l'utilisation et de l'entretien de chaque système de sécurité et de leur conformité avec les lois et règlements applicables.

La performance de sécurité (intégrité) doit réduire le risque de dangers identifiés tels qu'ils sont déterminés par l'évaluation des risques de la machine. Se reporter à [Annexe A2.1](#) pour savoir si les conditions décrites dans l'ISO 13849-1 doivent être appliquées.

Outre les conditions définies dans cette [Annexe A2.3.1](#), la conception et l'installation du dispositif de verrouillage doivent être conformes à l'ISO 14119.

A2.3.2 Conditions

Les conditions et considérations générales suivantes s'appliquent à l'installation de portes et de protections interverrouillées. En outre, l'utilisateur doit se référer aux règlements applicables pour s'assurer qu'il est conforme à toutes les conditions nécessaires.

Les dangers protégés par interverrouillage ne doivent pas pouvoir survenir tant que la protection est ouverte. Quand la protection s'ouvre en présence du danger, il faut qu'une commande d'arrêt de la machine protégée soit émise. Le fait de refermer la protection ne doit pas, en soi, lancer le mouvement dangereux ; il faut une procédure séparée pour redémarrer le mouvement. Les interrupteurs de sécurité ne doivent pas servir de fin de course ou d'arrêt mécanique.

La protection doit être située à une distance suffisante de la zone dangereuse (pour que le danger ait le temps d'être stoppé avant que la protection ne s'ouvre suffisamment pour permettre l'accès) et située soit latéralement soit éloignée du risque, mais pas dans la zone protégée. Il faut aussi que la protection ne puisse pas se refermer d'elle-même et activer le circuit d'interverrouillage. En outre, le personnel ne doit pas pouvoir atteindre le danger en passant par-dessus, en dessous, autour ou à travers la protection. Aucune ouverture dans la protection ne doit permettre un accès au danger (voir EN 294, ISO 14120 ou la norme qui s'applique). La protection doit être suffisamment solide pour protéger le personnel et restreindre les risques à la zone protégée, qu'ils soient éjectés, lâchés ou émis par la machine.

Les interrupteurs de verrouillage et déclencheurs de sécurité doivent être conçus de manière à ne pas pouvoir être facilement contournés. Ils doivent être fermement installés, de sorte que leur position ne puisse pas être modifiée, et ancrés par des fixations fiables qui nécessitent un outil pour être démontées.

A2.3.2.1 Interrupteurs de verrouillage de sécurité à ouverture positive

Les interrupteurs d'interverrouillage de sécurité doivent répondre à plusieurs exigences. Chaque interrupteur doit avoir des contacts isolés électriquement ; au minimum, un contact normalement fermé (N.C.) individuel par interrupteur monté. Les contacts doivent être à ouverture positive (directe), tel que décrit par la norme IEC 60947-5-1, avec un ou plusieurs contact(s) normalement fermés prévus pour la sécurité. Le fonctionnement par ouverture positive permet à l'interrupteur de s'ouvrir, sans avoir recours à des ressorts, quand l'actionneur de l'interrupteur est désengagé ou déplacé de sa position de base (voir les exemples dans le catalogue de sécurité de *Banner*).

En outre, les interrupteurs doivent être montés en mode positif, pour déplacer ou déverrouiller le déclencheur de sa position fermée et ouvrir le contact NF quand la protection s'ouvre.

A2.3.2.2 Interrupteurs de verrouillage de sécurité à fonctionnement magnétique

À un plus haut niveau de performances de sécurité, la conception de l'interrupteur magnétique à double canal utilise une commutation complémentaire, dans laquelle un canal est ouvert et un canal est fermé à tout instant. Cela permet la redondance (deux contacts) et la diversité (différents principes de fonctionnement) pour minimiser le risque de perte de la fonction de commutation par défaillance de mode commun (par ex. champs magnétiques secondaires). Le circuit du contrôleur de sécurité qui surveille l'interrupteur magnétique détecte et réagit à une erreur qui ferait perdre l'état complémentaire (par ex. un court-circuit entre les canaux ou un court-circuit vers d'autres sources d'alimentation).

Les interrupteurs magnétiques codés et non codés influencent la capacité de contourner l'interrupteur et à résister aux défaillances de mode commun. Les interrupteurs non codés sont facilement contournés par la présence d'un simple champ magnétique et ne doivent être installés que dans une position protégée. Un interrupteur magnétique codé qui utilise des pôles magnétiques alternants doit être utilisé dans les applications qui nécessitent des niveaux plus élevés de performances.

L'interrupteur et son aimant doivent être montés à une distance minimale de tout matériau magnétisé ou ferreux pour fonctionner correctement. Si l'interrupteur ou l'aimant est monté sur un matériau qui peut être magnétisé (métal ferreux, comme le fer), la distance de commutation en sera affectée. Cette distance est déterminée par le fabriquant.

A2.3.2.3 Surveillance des interrupteurs de verrouillage de sécurité raccordés en série

Quand on surveille individuellement deux interrupteurs de verrouillage de sécurité (comme illustré en [Figure 33 en page 87](#)), un interrupteur défaillant sera détecté s'il ne commute pas quand la protection s'ouvre. Dans ce cas, le contrôleur désactive ses sorties de sécurité ([OSSD en page 121](#)) et annule sa fonction de réarmement jusqu'à ce que les exigences d'entrées soient remplies (c'est-à-dire que l'interrupteur défaillant soit remplacé). Cependant, si plusieurs interrupteurs de verrouillage de sécurité sont montés en série, la défaillance d'un interrupteur dans le système peut être masquée ou ne pas être du tout détectée (voir [Figure 34 en page 87](#) et [Figure 35 en page 88](#)).

Les circuits des interrupteurs de verrouillage de sécurité peuvent ne pas correspondre aux exigences de ISO 13849 (EN954-1) catégorie de sécurité 4 à cause de la possibilité d'un réarmement inapproprié ou d'un risque de perte du signal d'arrêt de sécurité. Cela est dû à l'impossibilité d'exclure une défaillance de l'interrupteur de verrouillage de sécurité. Un raccordement multiple de ce type ne doit pas être utilisé dans des applications dans lesquelles la perte du signal d'arrêt de sécurité ou un réarmement inapproprié peut provoquer des blessures graves, voire mortelles. Les deux scénarios suivants supposent deux interrupteurs de verrouillage de sécurité à ouverture positive sur chaque protection, tous les deux raccordés en série aux interrupteurs de verrouillage de sécurité d'une seconde protection :

Exemple 1 – Défaillance cachée

Si une protection est ouverte, mais qu'un interrupteur de verrouillage de sécurité ne s'ouvre pas, l'interrupteur de verrouillage de sécurité redondant s'ouvre et fait que le contrôleur désactive ses sorties. Si la protection défaillante est maintenant fermée, les deux canaux d'entrée du contrôleur se ferment mais, parce que un canal ne s'est pas ouvert, le contrôleur ne réarme pas. Cependant, si l'interrupteur défaillant n'est pas remplacé et que la seconde protection en bon état est manipulée (ouverture et fermeture des deux canaux d'entrée du Contrôleur), le contrôleur considère que la défaillance a été corrigée. Comme les exigences d'entrée paraissent remplies, le contrôleur autorise un réarmement. Le système n'est plus redondant et si le deuxième interrupteur défaille, peut entraîner une situation non sûre (c'est-à-dire que l'accumulation de défaillance a entraîné une perte de la fonction de sécurité).

Exemple 2 – Non-détection d'une défaillance

Si une protection en bon état est ouverte, le contrôleur de sécurité désactive ses sorties (réponse normale). Mais si une protection défaillante est alors ouverte et refermée avant que la protection en bon état ne soit refermée, la défaillance de la porte n'est pas détectée. Ce système n'est plus redondant et peut entraîner une perte de sécurité si le second interrupteur de sécurité ne s'ouvre pas au moment où il le devrait.

Les systèmes de ces deux scénarios ne répondent pas de façon inhérente aux exigences des normes de sécurité concernant la détection des défaillances simples et l'interdiction du cycle suivant. Avec les systèmes de protections multiples utilisant des interrupteurs de sécurité en série, il est important de vérifier périodiquement le fonctionnement individuel de chaque interverrouillage. Les opérateurs, le personnel d'entretien et toutes les personnes associées à l'utilisation de la machine doivent être formés afin de reconnaître ces défaillances et de savoir les corriger immédiatement.

Chaque protection doit être ouverte et refermée séparément pendant que l'on vérifie que les sorties du contrôleur fonctionnent normalement. Chaque fois que l'on ferme une protection, il faut effectuer, le cas échéant, un réarmement manuel. Si un jeu de contacts est défaillant, le contrôleur n'autorise pas la fonction de réarmement. Si le contrôleur ne réarme pas, cela peut provenir d'un interrupteur défaillant qui doit être remplacé immédiatement.

Il faut procéder à cette vérification et réparer toutes les défaillances au moins pendant les vérifications périodiques. Si l'application ne peut exclure ce type de défaillance et qu'une défaillance peut entraîner des blessures sérieuses, voire mortelles, il ne faut pas utiliser le raccordement en série des interrupteurs de sécurité.

A2.3.2.4 Connexions en série et considérations sur l'intégrité du circuit de sécurité

A2.3.2.5 Catégorie 2

Une application de protection verrouillée à canal simple fournit généralement un niveau de performance des circuits de catégorie 2 car un court-circuit peut entraîner la perte de la fonction de sécurité. Le principe d'exclusion des défauts doit être intégré à la conception et à l'installation, afin d'éliminer ou de faire passer à un niveau de risque acceptable (minimum), la possibilité de défauts ou de défaillances non détectés susceptibles d'entraîner la perte de la fonction de sécurité. Le diagramme du circuit se trouve à la [Figure 33 en page 87](#).

A2.3.2.6 Catégorie 3

Une connexion à double canal connectant +24 Vcc est normalement une application de catégorie 3, parce qu'une défaillance unique n'entraîne pas une perte de sécurité. La perte de l'action de commutation d'un canal est détectée par l'action d'ouverture et de fermeture de la protection, permettant à la fonction de surveillance des entrées de sécurité de détecter la différence entre les canaux. Cependant, un court-circuit entre les canaux d'entrée ou les sorties de sécurité peut ne pas être détecté. Il faut remarquer qu'une accumulation de défaillances peut entraîner la perte de la fonction de sécurité. Le principe d'exclusion de défaillances doit être incorporé dans la conception et l'installation pour éliminer ou réduire à un niveau minimal (acceptable) le risque, la possibilité de défaillances non détectées ou de défaillances de mode commun ou catastrophique qui pourrait faire perdre la fonction de sécurité. Le diagramme du circuit se trouve à la [Figure 34 en page 87](#).

A2.3.2.7 Catégorie 4

Les entrées de sécurité à auto surveillance peuvent être interfacées pour atteindre le niveau de sécurité de catégorie 4. Le principe d'exclusion de défaillance doit être incorporé dans la conception et l'installation pour éliminer ou réduire à un niveau minimal (acceptable) le risque, la possibilité de défaillances non détectées ou de défaillances de mode commun ou catastrophique qui pourrait faire perdre la fonction de sécurité. Le diagramme du circuit se trouve à la [Figure 35 en page 88](#).

A2.3.3 Interrupteurs pour portes (ou protections interverrouillées) possibilités de connexions

Tous les schémas sont faits avec l'interrupteur pour porte (protection) en état FERMÉ ou RUN/ON. Le contact de sécurité est considéré comme étant un contact N.F. à ouverture positive (sauf indication contraire), marqué normalement

par le symbole .

A2.3.3.1 Canal simple, 1 borne – canal simple, 2 borne – canal simple, contact PNP

Ces circuits normalement sont conformes aux exigences de ISO 13849-1 catégorie 2, en fonction de la conception et de l'installation de l'interrupteur. Au minimum, l'interrupteur doit être un dispositif de sécurité de niveau de catégorie 2. Le canal simple, 1 borne et canal simple, contact PNP ne peut pas détecter un court-circuit vers une autre source d'alimentation. Le raccordement canal simple, 2 bornes utilise une surveillance d'impulsions et peut détecter un court-circuit vers une autre source d'alimentation. Il faut utiliser l'exclusion de défaillance pour obtenir un plus haut niveau d'intégrité du circuit de sécurité.



A2.3.3.2 Double canal, 2 bornes – Double canal, 3 bornes

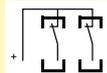
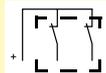
Ce circuit peut normalement répondre aux exigences de ISO 13849-1 catégorie 2 ou catégorie 3, en fonction de la conception et de l'installation des interrupteurs. Les connexions canal double, 3 bornes utilisent une surveillance d'impulsions qui peuvent détecter un court-circuit vers une autre source d'alimentation. Les connexions canal double, 2 bornes et canal double, 3 bornes peuvent détecter un court-circuit entre les canaux si les contacts sont ouverts pendant plus de 2 secondes.



Un interrupteur unique monté sur une seule protection est normalement une application de catégorie 2.



Deux interrupteurs montés sur une seule protection sont normalement une application de catégorie 3.



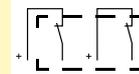
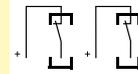
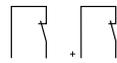
A2.3.3.3 Double canal, PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4 en fonction du niveau de sécurité, de l'installation et de la possibilité de détection de défaillance (par ex. court-circuit) des dispositifs. Le contrôleur de sécurité SC22-3 ne détecte pas les courts-circuits dans cette configuration.



A2.3.3.4 Double canal, 4 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction de la conception et de l'installation des interrupteurs. Ce circuit peut détecter un court-circuit entre canaux ou vers une autre source d'alimentation.



Deux interrupteurs montés individuellement sur une seule protection est techniquement une application de catégorie 4. Une connexion en série d'interrupteurs sur plusieurs protections est caractéristique d'une application de catégorie 3.

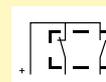
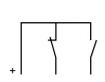
Un interrupteur monté sur une seule protection est normalement une application de catégorie 2.

A2.3.3.5 Complémentaire, 2 bornes – Complémentaire, 3 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction de la conception et de l'installation des interrupteurs. Ce circuit peut détecter un court-circuit entre canaux. Un interrupteur magnétique codé utilisera normalement ce style. En situation fermée (comme illustré) un court-circuit entre les contacts fermés peut augmenter le temps de réponse basé sur le temps d'anti-rebond (voir [Paragraphe 4.5 en page 27](#)).



Un interrupteur magnétique à un seul codage monté sur une seule protection peut répondre aux conditions de catégorie 3, ou catégories 4 en fonction de l'installation et de la fréquence d'utilisation de la protection (fermée-ouverte-fermée).



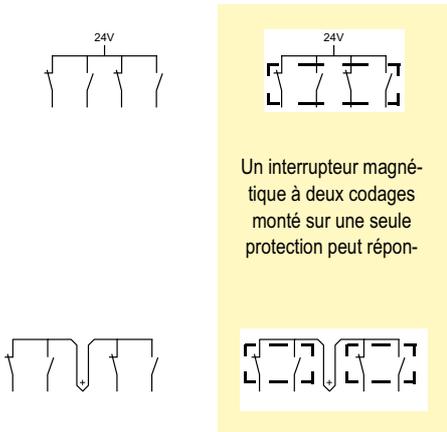
A2.3.3.6 Complémentaire, contact PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction de la conception et de l'installation des interrupteurs. Ce circuit peut détecter un court-circuit entre les canaux. Dans la position fermée de la protection (illustration) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que ce qui est spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.3.3.7 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 4, en fonction de la conception et de l'installation des interrupteurs. Un interrupteur magnétique codé utilisera normalement ce style. Dans la position fermée de la protection (illustration) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que ce qui est spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.3.3.8 2 complémentaires, contact PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 4 en fonction de la conception et de l'installation des interrupteurs. Dans la position fermée de la protection (illustration) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que ce qui est spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.4 CAPTEURS OPTIQUES (BARRIÈRE IMMATÉRIELLE)



Les dispositifs à capteurs optiques à Entrées de sécurité du contrôleur de sécurité SC22-3 utilisent la lumière comme moyen de détection.

A2.4.1 Niveaux d'intégrité des circuits de sécurité

Les conditions du niveau de fiabilité de la commande ou de la catégorie de sécurité selon ISO 13849-1 (EN954-1) varient considérablement dans l'application des protections optiques. Bien que *Banner Engineering* recommande toujours le niveau de sécurité le plus élevé pour toute application, l'utilisateur est seul responsable de la sécurité de l'installation, de l'utilisation et de l'entretien de chaque système de sécurité et de leur conformité avec les instructions du fabricant et les lois et règlements applicables.

Les performances de sécurité (intégrité) doivent réduire le risque des dangers identifiés en fonction de l'évaluation des risques de la machine. Suivre les indications de [Annexe A2.1](#) si les exigences de ISO 13849-1 (EN954-1) doivent être respectées. En plus des exigences de cet [Annexe A2.4.1](#), la conception et l'installation des dispositifs de protection optique doivent répondre à IEC 61496 (toutes pièces).

A2.4.2 Exigences

AVERTISSEMENT
INFORMATION INCOMPLÈTE

DE NOMBREUSES CONSIDÉRATIONS D'INSTALLATION NÉCESSAIRE À L'UTILISATION CORRECTE DE CES DISPOSITIFS NE SONT PAS COUVERTES PAR CE DOCUMENT. SE RÉFÉRER AUX INSTRUCTIONS D'INSTALLATION DU DISPOSITIF CORRESPONDANT POUR ASSURER UN APPLICATION SÛRE DU DISPOSITIF.

Utilisés en protection, ces dispositifs sont décrits par IEC 61496-1/-2/-3 en tant que dispositif de protection optronique actif (AOPD) et dispositif de protection optronique actif répondant à la réflexion diffuse (AOPDDR).

Les AOPD comprennent les écrans lumineux de sécurité et les systèmes de sécurité mono et multi faisceaux (dispositifs mono et multi faisceaux). Ces dispositifs sont décrits comme répondant aux exigences de conception de type 2 ou de type 4. Un dispositif de type 2 est autorisé dans une application de catégorie 2 selon ISO 13849-1 et un dispositif de type 4 peut être utilisé dans une application de catégorie 4. Les AOPDDR peuvent aussi être des scanners de surface ou à laser. La destination principale de ces dispositifs est une application de type 3, jusqu'à la catégorie 3.

Les dispositifs de sécurité optiques doivent aussi être placés à une distance de sécurité, selon les normes applicables.

Il faut tenir compte des normes applicables ainsi que de la documentation du fabricant spécifique au dispositif pour les calculs.

A2.4.3 Distance de sécurité

Les informations suivantes ne sont applicables qu'à des installations certifiées CE.

Pour le calcul de la distance de sécurité, le temps de réponse par défaut du contrôleur de sécurité est de 0,010 seconde, plus tout temps d'anti-rebond de fermé à ouvert supplémentaire. Si le temps d'anti-rebond est réglé, le temps en excès de 6 ms (=temps d'anti-rebond de fermé à ouvert par défaut) doit être ajouté à la réponse standard (voir les spécifications, [Paragraphe 3.2.1 en page 21](#)). Pour avoir un accès rapide aux temps de réponse spécifiques du contrôleur voir aussi [Paragraphe 6.1.2.4 en page 54](#).

Le calcul de la distance de sécurité prend en compte plusieurs facteurs, dont le calcul de la vitesse d'un humain, le temps d'arrêt total du système (qui comporte lui-même plusieurs éléments) et la distance supplémentaire due à l'intrusion de la main ou d'un objet vers la zone dangereuse avant que le dispositif de sécurité ne réagisse.

En tant qu'exemple, la distance de sécurité des barrières immatérielles de sécurité qui sont classées comme dispositifs de type 2 ou de type 4, peut être calculée par la formule générale indiquée dans ISO 13855 (EN 999) comme suit :

Formule générale

$S = K \times T + C$ dans laquelle :

S = Distance de sécurité exprimée en mm, de la zone dangereuse au centre de la zone de détection (voir [Zone de détection en page 123](#)). La distance de sécurité autorisée est de 100 mm (175 mm pour les applications hors industrie), indépendamment du résultat de la formule

K = Constante de vitesse de la main recommandée (en mm) dérivée des vitesses d'approche du corps ou de parties du corps définies en ISO/DIS 13855

T = temps de réponse total de la machine, à savoir le temps qui s'écoule entre l'activation du dispositif de sécurité et l'arrêt de la machine ou l'élimination de tout danger. Le temps de réponse peut être divisé entre T_s et T_r où $T = T_s + T_r$

T_s = Temps de réponse de la machine mesuré entre l'application du signal d'arrêt par la barrière immatérielle et l'arrêt de la machine ou la disparition du risque (y compris les temps d'arrêt de tous les éléments de commande mesurés à la vitesse maximale de la machine, par exemple, IM-T-Modules d'interface). T_s est mesuré normalement par un dispositif de mesure du temps

Si le temps d'arrêt spécifié est utilisé, il est conseillé de procéder à une majoration de 20 % de la valeur mesurée comme facteur de sécurité pour pallier une éventuelle détérioration du système de freinage.

T_r = temps de réponse de la barrière immatérielle

C = Distance supplémentaire exprimée en mm, fondée sur l'intrusion d'une main ou d'un objet vers la zone dangereuse avant l'activation du dispositif de sécurité. C est calculé à partir de la formule suivante : $C = 8 \times (d-14)$ où d est la résolution de l'appareil

☛ Cette mesure doit prendre en compte la plus lente des deux voies MPCE (voir MPCE en page 121) et le temps de réponse de tous les dispositifs et commandes (comme les modules d'interface) qui interviennent dans l'arrêt de la machine. Si tous les dispositifs ne sont pas inclus, la distance de sécurité (S) calculée sera trop courte et pourra entraîner des blessures graves.

L'utilisateur doit considérer tous les facteurs, y compris les capacités physiques de l'opérateur, pour déterminer la valeur de K.

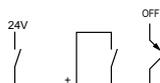
Il faut éviter d'accéder à la zone dangereuse par passage au-dessus ou autour de la barrière immatérielle en utilisant les valeurs indiquées dans les normes ISO 13852.

A2.4.4 Connexion générique

☛ Dans le [Annexe A2.4.4](#) le détecteur optique est actionné en état N.O. ou OFF.

A2.4.4.1 Canal simple, 1 borne – canal simple, 2 borne – canal simple, contact PNP

Ces circuits normalement sont conformes aux exigences de ISO 13849-1 catégorie 2, en fonction du niveau de sécurité des dispositifs d'entrée. Au minimum, un dispositif de sécurité doit arriver au niveau de catégorie 2. Le canal simple, 1 borne et canal simple, contact PNP ne peut pas détecter un court-circuit vers une autre source d'alimentation. Le raccordement canal simple, 2 borne utilise une surveillance d'impulsions et peut détecter un court-circuit vers une autre source d'alimentation. Il faut utiliser l'exclusion de défaillance pour obtenir un plus haut niveau d'intégrité du circuit de sécurité.



A2.4.4.2 Double canal, 2 bornes – Double canal, 3 bornes

Ce circuit peut normalement répondre aux exigences de ISO 13849-1 catégorie 2 ou catégorie 3, en fonction du niveau de sécurité des dispositifs d'entrée. Les connexions canal double, 3 bornes utilisent une surveillance d'impulsions qui peuvent détecter un court-circuit vers une autre source d'alimentation. Les connexions canal double, 2 bornes et canal double, 3 bornes peuvent détecter un court-circuit entre les canaux si les contacts sont ouverts pendant plus de 2 secondes.



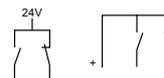
A2.4.4.3 Double canal, PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4 en fonction du niveau de sécurité, de l'installation et de la possibilité de détection de défaillance (par ex. court-circuit) du dispositif d'entrée. Le contrôleur de sécurité SC22-3 ne détecte pas les courts-circuits dans cette configuration.



A2.4.4.4 Complémentaire, 2 bornes – Complémentaire, 3 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation du dispositif d'entrée. Ce circuit peut détecter un court-circuit entre canaux. En situation activé (par ex. S1 ouvert / S2 fermé ci-dessous) un court-circuit entre les contacts fermés peut augmenter le temps de réponse basé sur le temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que ce qui est spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.4.4.5 Complémentaire, contact PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation du dispositif d'entrée. Ce circuit peut détecter un court-circuit entre les canaux. En situation activé (par ex. S1 OFF / S2 ON ci-dessous) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que ce qui est spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.5 COMMANDE BIMANUELLE

AVERTISSEMENT

PROTECTION DU POSTE DE TRAVAIL

INSTALLÉ CORRECTEMENT, LE DISPOSITIF DE COMMANDE BIMANUELLE NE PROTÈGE QUE LES MAINS DE L'OPÉRATEUR DE LA MACHINE. IL PEUT S'AVÉRER NÉCESSAIRE D'INSTALLER D'AUTRES PROTECTIONS SUR LE POSTE DE TRAVAIL COMME DES BARRIÈRES IMMATÉRIELLES DE SÉCURITÉ ET/OU DES CARTERS DE PROTECTION POUR PROTÉGER LE PERSONNEL DES MACHINES DANGEREUSES. LE FAIT DE NE PAS INSTALLER DES PROTECTIONS DU POSTE DE TRAVAIL SUR DES MACHINES DANGEREUSES PEUT PROVOQUER UN RISQUE QUI PEUT ENTRAÎNER DE SÉRIEUSES BLESSURES OU MÊME LA MORT.

PRÉCAUTIONS

COMMANDES MANUELLES

L'ENVIRONNEMENT DANS LEQUEL LES COMMANDES MANUELLES SONT INSTALLÉES NE DOIT PAS AFFECTER LES MOYENS DE MISE EN ACTION. DES CONTAMINATIONS OU AUTRES INFLUENCES SÉVÈRES DE L'ENVIRONNEMENT PEUVENT ENTRAÎNER UN RALENTISSEMENT DE LA RÉPONSE OU UNE MAUVAISE CONDITION LORS DE L'ACTIONNEMENT DES BOUTONS MÉCANIQUES OU ERGONOMIQUES. CECI PEUT PRÉSENTER UN RISQUE.

INSTALLER LES COMMANDES MANUELLES POUR ÉVITER UNE UTILISATION ACCIDENTELLE

UNE PROTECTION TOTALE CONTRE UNE UTILISATION « FRAUDULEUSE » DE LA COMMANDE BIMANUELLE N'EST PAS POSSIBLE. L'UTILISATEUR EST NÉANMOINS OBLIGÉ PAR LES RÈGLEMENTS EUROPÉENS D'ARRANGER ET DE PROTÉGER LES COMMANDES MANUELLES DE FAÇON À MINIMISER LE RISQUE D'UTILISATION FRAUDULEUSE OU ACCIDENTELLE.

LA COMMANDE DE LA MACHINE DOIT DISPOSER D'UNE COMMANDE D'ANTI-RÉPÉTITION

LA COMMANDE DE LA MACHINE DOIT DISPOSER D'UNE COMMANDE D'ANTI-RÉPÉTITION APPROPRIÉE, REQUISE PAR LES NORMES DES É.-U. ET INTERNATIONALES POUR LES MACHINES À SIMPLE COURSE ET À SIMPLE CYCLE.



Le contrôleur de sécurité SC22-3 peut servir d'actionneur pour la plupart des machines dont le cycle machine est commandé par un opérateur.

L'utilisation d'un système de commande bimanuelle de sécurité fait que l'opérateur devient alors « otage » en présence de risque, limitant ou éliminant ainsi l'exposition au risque. Les commandes bimanuelles doivent être situées de façon à ce 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 [Annexe A2.5.1](#) distance de sécurité).

Les entrées de sécurité du contrôleur de sécurité SC22-3 utilisées pour surveiller l'utilisation des deux mains pour la commande bimanuelle sont conformes aux exigences fonctionnelles de type III de IEC60204-1 et de ISO 13851 pour les commandes bimanuelles, ce qui inclut :

- Utilisation simultanée 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
- Utilisation continue pendant la situation dangereuse
- Arrêt immédiat de la situation dangereuse si une commande est relâchée
- Relâchement et réactualisation des deux commandes pour réinitialiser le mouvement ou la situation dangereuse (anti coincement)
- Le niveau de performances approprié de la fonction de sécurité (par ex. fiabilité des commandes, catégorie ou SIL) selon une évaluation des risques

Le niveau de sécurité atteint (par ex. ISO 13849-1 catégorie) dépend en partie du type de circuit choisi. Voir [Annexe A2.5.2](#).

L'installation des commandes manuelles doit considérer les points suivants :

- Modes de défaillance qui entraîneraient un court-circuit, un ressort cassé, un blocage mécanique, etc., qui empêcherait la détection du relâchement de la commande manuelle
- Contamination sévère ou autres influences de l'environnement qui peuvent ralentir la réponse à la relâche ou une fausse situation ON de la commande manuelle, par ex. le grippage d'une liaison mécanique
- La protection contre le déclenchement par accident ou par inadvertance. (Par ex., en choisissant leur position de montage ou en utilisant des protections comme des bagues, des gardes ou des grillages)
- En minimisant la possibilité de la contourner par ex., 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, selon ISO 13851
- La fiabilité fonctionnelle et l'installation de dispositifs logiques externes
- Installation électrique correcte selon IEC 60204

Si la machine est utilisée en mode simple cycle ou simple course, sa commande doit comporter une disposition de non-répétition pour que l'opérateur doive relâcher les actionneurs de commande bimanuelle à la fin de chaque cycle machine avant de pouvoir commencer un nouveau cycle. En outre, la fonction de non-répétition de la commande, les entrées du contrôleur de sécurité SC22-3 peuvent aussi servir à arrêter le cycle de la machine et aider à la non-répétition (voir [Mise en garde](#))

A2.5.1 Distance de sécurité



AVERTISSEMENT

EMPLACEMENT DES BOUTONS DE COMMANDE À CONTACT

LES BOUTONS DOIVENT ÊTRE INSTALLÉS À DISTANCE SUFFISANTE DES PARTIES MOBILES DE LA MACHINE. L'OPÉRATEUR OU TOUTE AUTRE PERSONNE NON COMPÉTENTE NE DOIT PAS POUVOIR LES DÉPLACER. LE NON-RESPECT DE LA DISTANCE DE SÉCURITÉ REQUISE PEUT PROVOQUER DES BLESSURES GRAVES OU MÊME LA MORT.

☛ *Les informations suivantes ne sont applicables qu'à des installations certifiées CE.*

ISO 13855 – Sécurité des machines – Positionnement des équipements de protection par rapport à la vitesse d'approche des pièces des parties du corps humain.

Les deux commandes manuelles 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 que le mouvement dangereux ne cesse. S'il n'existe pas d'autre norme de Type C, la distance minimale doit être calculée au moyen de la formule générale.

Formule générale

S = K x T + C dans laquelle :

S est la distance minimale en millimètres entre la zone dangereuse et le point, la ligne ou le plan de détection ;

K est une constante en millimètres par seconde, dérivée des données des vitesses d'approche du corps ou des parties du corps.

K = 1600 mm par seconde ;

T est le temps total de réaction en secondes ;

C est une distance supplémentaire en millimètres, basée sur l'intrusion vers la zone dangereuse avant l'activation ; **C = 250 mm.**

Si les normes européennes spécifiques aux machines spécifient une distance différente de la distance de sécurité calculée en utilisant cette norme, il faut utiliser la plus grande des deux valeurs comme distance minimale de sécurité.

☛ *Le temps de réaction total est le temps entre l'initiation physique du dispositif de sécurité et l'arrêt de la machine ou la fin du risque. Le temps de réaction total comprend au moins deux phases :*

T = T₁ + T₂ dans laquelle :

T₁ est le temps de réaction maximum du dispositif de sécurité entre l'initiation physique de la fonction de détection et la mise hors tension des dispositifs de commutation du signal de sortie

Le DUO-TOUCH avec boutons STB (module de sécurité AT-FM-10K interfacé avec les boutons STB) a un temps de réaction de sortie de 55 millisecondes.

T₂ est le temps de réaction de la machine, à savoir le temps nécessaire pour que la machine s'arrête ou que le risque disparaisse après avoir reçu le signal de sortie du dispositif de sécurité

☛ *Si le risque d'accrochage de tout ou partie du corps dans la zone de danger est éliminé quand le dispositif est activé, par exemple par une protection adéquate, C peut être égal à zéro, si la distance minimale de S est de 100 mm.*

Voir l'exemple du calcul de la distance de sécurité en face.

Exemple de calcul de la distance de sécurité (S)

L'exemple suivant illustre l'utilisation de la formule pour calculer la distance de sécurité :

K = 1600 mm par seconde

T₁ = 0,055 seconde

T₂ = 0,50 seconde (mesuré au chronomètre)

C = 250 mm

S = K x T + C (dans laquelle T = T₁ + T₂)

= 1600 x (0,055 + 0,50) + 250

= 1138 mm

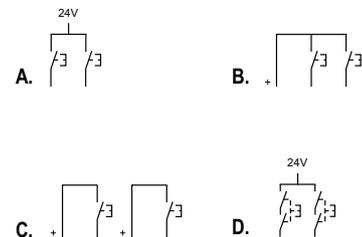
Dans cet exemple, les deux commandes manuelles ne doivent pas être situées à moins de 1138 mm du point dangereux le plus proche.

A2.5.2 Possibilités de connexions

☛ *Le dispositif est illustré non actionné ou en état OFF. Voir ISO 13851 pour une explication complète des désignations types et les exigences de ISO 13849 catégorie 1.*

A2.5.2.1 Canal double, 2 bornes – Canal double, 3 bornes – Canal double, 4 bornes

Les schémas des circuits ci-dessous sont de type IIIa commande bi-manuelle selon ISO 13851 et sont normalement conformes aux exigences de ISO 13849-1 EN 954-1) catégorie 1. Un type IIIb et une catégorie 3 peuvent être atteints si les contacts redondants de chaque commande manuelle sont utilisés par un canal chacun, à savoir, deux de chaque en série, comme illustré dans le schéma D ci-dessous ou avec des connexions de canal double, 3 bornes qui utilisent la surveillance d'impulsions pour détecter un court-circuit vers une autre source d'alimentation. Les deux connexions canal double, 2 bornes et canal double, 3 bornes peuvent détecter un court-circuit entre les canaux quand les contacts sont ouverts si le court-circuit dure plus de 2 secondes. Le circuit double canal, 4 bornes peut détecter un court-circuit entre les canaux ou vers une autre source d'alimentation (schéma C).



A2.5.2.2 Double canal, PNP

Le schéma ci-dessous est un circuit de Type IIIa pour commande bi-manuelle selon ISO 13851 et peut normalement respecter les exigences de ISO 13849-1 (EN 954-1) catégorie 1. Le contrôleur de sécurité SC22-3 ne fournit pas de détection de court-circuit entre les canaux dans cette configuration.

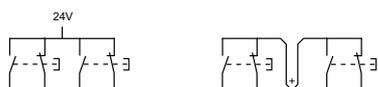


A2.5.2.3 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes

Le schéma ci-dessous est un circuit de type IIIc pour commande bi-manuelle selon ISO 13851 qui répond normalement aux exigences de ISO 13849-1

(EN 954-1) catégorie 4. En situation activée (par ex. S1 ouvert / S2 fermé ci-dessous) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).

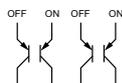
☛ Sélectionner cette option quand on utilise les boutons à autocontrôle Banner modèle STBVR81...



A2.5.2.4 2 complémentaires, contact PNP

Le schéma ci-dessous est un circuit de type IIIc pour commande bi-manuelle selon ISO 13851 qui répond normalement aux exigences de ISO 13849-1 (EN 954-1) catégorie 4. En situation activée (par ex. S1 ouvert / S2 fermé ci-dessous) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).

☛ Sélectionner cette option quand on utilise les boutons à autocontrôle Banner modèle STBVP6...



A2.6 TAPIS DE SÉCURITÉ (BORDURES DE SÉCURITÉ)



AVERTISSEMENT

APPLICATION DES TAPIS DE SÉCURITÉ

LES EXIGENCES VARIENT CONSIDÉRABLEMENT SELON LE NIVEAU DE FIABILITÉ DE COMMANDE OU LA CATÉGORIE ISO 13849-1 (EN954-1) DANS L'UTILISATION DES TAPIS DE SÉCURITÉ. L'UTILISATEUR A LA RESPONSABILITÉ D'INSTALLER, DE FAIRE FONCTIONNER ET D'ENTREtenir CHAQUE TAPIS DE SÉCURITÉ (OU BORDURE DE SÉCURITÉ) SELON LES RECOMMANDATIONS DU FABRICANT ET DE RESPECTER TOUTES LES LOIS ET RÈGLEMENTS APPLICABLES.

NE PAS UTILISER UN TAPIS DE SÉCURITÉ EN TANT QUE DISPOSITIF D'ACTIVATION POUR INITIER LE MOUVEMENT DE LA 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.

NE PAS UTILISER DE 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 EX. PERTE D'ALIMENTATION DU CONTRÔLEUR) PEUVENT ENTRAÎNER UN 'FAUX SIGNAL D'ACTIVATION.



Le contrôleur de sécurité SC22-3 peut aussi servir à surveiller des tapis de sécurité et des bordures de sécurité (détecteurs) sensibles à la pression.

L'objectif de l'entrée tapis de sécurité du contrôleur de sécurité est de vérifier que les tapis de sécurité à détection de présence à 4 fils fonctionnent bien (détecteurs). Plusieurs tapis de sécurité peuvent être raccordés en série à un contrôleur (voir [Annexe A2.6.2](#)).

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

La fonction est de surveiller les contacts (plaques de contact) et le câblage d'un ou plusieurs tapis de sécurité pour détecter une défaillance et empêcher la machine de redémarrer en cas de défaillance. Un réarmement après que l'opérateur ait marché sur le tapis de sécurité peut être fourni par le contrôleur de sécurité, ou, si le contrôleur est utilisé en mode de réarmement automatique, la fonction de réarmement/redémarrage doit être fournie par le système de commande de la machine. Ceci évite à la machine de redémarrer automatiquement quand le tapis de sécurité est dégagé.

A2.6.1 Conditions

Ce qui suit représente les exigences minimales de conception, construction et installation de détecteurs de tapis de sécurité à quatre fils à interfacer avec le contrôleur de sécurité. Ces exigences sont un résumé des informations contenues dans ISO 13856-1. L'utilisateur doit revoir tous les règlements et normes applicables et doit s'assurer que le contrôleur et tous les détecteurs associés sont entièrement compatibles.

A2.6.1.1 Conception et construction d'un système de tapis de sécurité

Le système de tapis de sécurité, le contrôleur de sécurité et tous les dispositifs supplémentaires doivent avoir un temps de réponse qui est 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, la sensibilité minimale du détecteur est, au minimum, d'un poids de 30 kg sur une pièce test en forme de disque de diamètre 80 mm, n'importe où sur la surface sensible du tapis de sécurité, y compris aux raccords. La surface sensible effective doit être identifiable et peut comprendre un ou plusieurs détecteurs. Le fournisseur du tapis de sécurité doit indiquer ce poids et ce diamètre minimum sous forme de sensibilité minimale du détecteur.

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

Les conditions d'utilisation du tapis doivent correspondre au minimum à IP54. Si le détecteur est prévu pour être immergé dans l'eau, l'enveloppe du détecteur doit être au minimum à 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. Le raccord de câblage peut devoir être situé dans une enveloppe qui a une condition d'utilisation appropriée.

Le détecteur ne doit pas être affecté par les conditions d'utilisation pour lesquelles le système est prévu ; c'est-à-dire que les effets sur le détecteur de liquides ou autres substances prévues doivent être pris en compte (par ex. une exposition à long terme à certains liquides peut dégrader ou faire gonfler le matériau d'enveloppe du détecteur, entraînant une situation non sûre).

La surface supérieure du détecteur doit être conçue comme non glissante à vie ou, les possibilités de ne pas répondre aux conditions attendues doivent être minimisées.

Le raccordement à quatre fils entre les câbles et le détecteur doit supporter le raclement et le support du détecteur par le câble sans défaillance (par ex. connexions cassées parce qu'on a tiré brutalement, régulièrement ou par pliage continu). Sinon, un autre moyen doit être employé pour éviter ce genre de défaillance, par exemple, un câble qui se déconnecte sans dégâts et conserve une situation sûre.

A2.6.2 Possibilités de connexions

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 ISO 13849-1 (EN 954-1).

Le tapis de sécurité, son contrôleur de sécurité et tous les systèmes de commutation du signal de sortie doivent répondre aux exigences de la catégorie de sécurité 1 au minimum. Pour répondre à ces exigences, le système doit au minimum répondre aux exigences de ISO 13856-1 (EN 1760-1) et aux exigences applicables de ISO 13849-1 (EN 954-1).

Le contrôleur de sécurité SC22-3 est conçu pour surveiller des tapis de sécurité à quatre fils, mais n'est pas compatible avec les dispositifs à deux fils (tapis, bordures sensibles, etc., à deux fils et une résistance de 'détection').

Ce circuit peut normalement répondre aux exigences de ISO 13849-1 catégorie 2 ou catégorie 3 en fonction du niveau de sécurité et de l'installation des tapis de sécurité ou autres détecteurs. Ce circuit peut détecter un court-circuit entre les canaux ou vers une autre source d'alimentation.



A2.6.3 Installation

La qualité de la surface d'installation et sa préparation pour le détecteur doivent répondre aux exigences indiquées par le fabricant du détecteur. Des irrégularités du sol (ou autres surfaces de montage) peuvent perturber le fonctionnement du détecteur et doivent donc être réduites au minimum acceptable.

La surface d'installation doit être plane et propre. Le drainage de fluides sous ou autour du capteur doit être évité. Le risque de défaillance du à l'accumulation de poussière, de copeaux ou d'autres matériaux sous le capteur ou les fixations doit être évité. Il faut particulièrement faire attention aux raccords entre les capteurs pour s'assurer que les matières étrangères ne s'accumulent pas sous ou dans le capteur.

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

Chaque capteur doit être régulièrement inspecté et testé selon les recommandations du fabricant. Il faut faire attention à ne pas dépasser les spécifications d'utilisation (par ex. le nombre maximum de commutations).

Chaque détecteur doit être solidement fixé pour éviter qu'il ne se déplace par inadvertance ou qu'il ne soit déplacé sans autorisation. On peut fixer les bords, utiliser des ancrages à un seul usage ou inviolables, surbaïsser le sol ou la surface de montage en plus de la taille et du poids des gros tapis.

Chaque capteur doit être installé pour minimiser le risque de trébucher (en particulier vers le risque de la machine). Un risque de trébucher peut exister si la différence de hauteur par rapport à la surface horizontale adjacente est de 4 mm ou plus. Les risques de trébucher doivent être minimisés aux raccords, aux jonctions et aux bords et si on utilise une couverture supplémentaire. On peut l'aligner par rapport au sol (sol enfoncé pour qu'il soit au même niveau que la surface environnante) ou utiliser une rampe qui ne doit pas dépasser 20° par rapport à l'horizontale. Utiliser des couleurs contrastées ou des marquages pour identifier les rampes et les bords.

Le système de tapis de sécurité doit être dimensionné et positionné de façon à ce que les personnes ne puissent pas entrer dans la zone dangereuse sans être détectées et ne puissent atteindre le danger avant que le risque de danger n'ait cessé. Des protections supplémentaires ou dispositifs de protection peuvent être nécessaire pour s'assurer que l'exposition au danger n'est pas possible en passant par-dessus, par-dessous ou autour de la surface sensible du dispositif.

L'installation d'un tapis de sécurité doit prendre en compte la possibilité de passer par-dessus la surface sensible sans être détecté. Les normes internationales 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 entre 750 mm et 1200 mm, en fonction de l'application et des normes applicables. La possibilité de monter sur les supports de la machine ou autres objets pour contourner ou enjamber le capteur doit aussi être évitée.

A2.6.4 Distance de sécurité

Les informations suivantes ne sont applicables qu'à des installations certifiées CE.

En tant que protection autonome, le capteur doit être installé à la distance de sécurité pour que le bord externe de la surface sensible soit au moins à la distance de sécurité, sauf s'il est utilisé uniquement pour éviter un démarrage ou un redémarrage ou utilisé uniquement comme dispositif de protection de dégagement.

La distance de sécurité prévue pour une application dépend de plusieurs facteurs, dont la vitesse de la main (ou de l'individu), du temps d'arrêt du système total (qui comprend plusieurs composants du temps de réponse) et le facteur de pénétration en profondeur. L'utilisateur doit se rapporter à la norme applicable pour déterminer la distance appropriée ou le moyen de s'assurer que personne ne peut être exposé au risques.

La distance de sécurité calculée est la distance horizontale minimale entre le bord externe de la zone de détection du tapis de sécurité et la partie la plus proche du danger. La formule générale pour des tapis de sécurité posés au sol est spécifiée dans ISO 13855 (EN 999).

Formule générale

$$S = [1600 \times (t_1 + t_2)] + (1200 - 0,4H)$$

S est la **distance de sécurité** en mm dans le plan horizontal de la **zone dangereuse** au bord de détection du dispositif le plus éloigné de la **zone dangereuse**

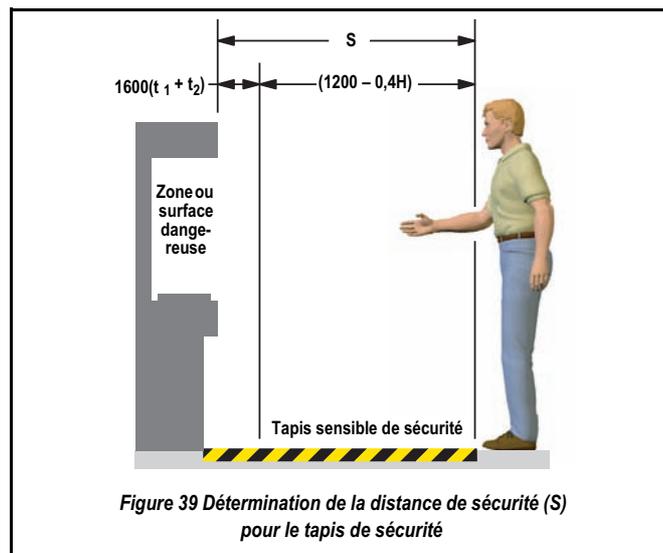
1600 est la constante de vitesse minimale basée sur le mouvement de la main ou du bras quand le corps est stationnaire
1600 mm/s

t₁ est le temps de réaction maximum entre l'initiation physique de la fonction de détection et la mise hors tension des dispositifs de commutation du signal de **sortie**

t₂ est le **temps de réponse** maximum de la machine, c'est-à-dire le temps nécessaire pour arrêter la machine ou annuler les risques après avoir reçu le signal de sortie de l'équipement de protection

1200 est le facteur de pénétration en profondeur qui est la distance maximale vers le danger sur la surface du **tapis de sécurité** qui peut se produire avant que l'arrêt soit signalé 1200 mm

H est la distance au dessus du plan de référence, par ex. le sol, en millimètres



Si une personne peut traverser le capteur complètement sans être détectée, des dispositifs de protection supplémentaires ou d'autres moyens doivent être utilisés pour éviter un démarrage non prévu et l'exposition au risque. Au minimum, le système de tapis de sécurité (ou la commande de la machine) doit être réarmé manuellement et nécessiter une réinitialisation des moyens normaux d'activation avant le démarrage ou redémarrage du cycle machine.

A2.7 ARRÊTS D'URGENCE



AVERTISSEMENTS

FONCTIONS D'ARRÊT D'URGENCE

NE PAS INHIBER OU BYPASSER DE DISPOSITIFS D'ARRÊT D'URGENCE. L'IEC 60204-1 EXIGE QUE LA FONCTION D'ARRÊT D'URGENCE RESTE ACTIVE À TOUT MOMENT. L'INHIBITION OU LE BYPASS DES SORTIES DE SÉCURITÉ DÉSACTIVE LA FONCTION D'ARRÊT D'URGENCE.

LA CONFIGURATION D'ARRÊT D'URGENCE DU CONTRÔLEUR DE SÉCURITÉ SC22-3 EMPÊCHE L'INHIBITION OU LE BYPASS DES ENTRÉES D'ARRÊT D'URGENCE. CEPENDANT, L'UTILISATEUR DOIT TOUJOURS S'ASSURER QUE LE DISPOSITIF D'ARRÊT D'URGENCE RESTE ACTIF À TOUT INSTANT.

SÉQUENCE DE RÉARMEMENT REQUISE

LES NORMES INTERNATIONALES REQUIÈRENT LA RÉALISATION D'UNE SÉQUENCE DE RÉARMEMENT APRÈS LE RETOUR DU BOUTON D'ARRÊT D'URGENCE SUR LA POSITION DE CONTACT FERMÉ (ARMEMENT DU BOUTON D'ARRÊT D'URGENCE). LORSQUE LE RÉARMEMENT AUTOMATIQUE EST UTILISÉ, UNE SOLUTION ALTERNATIVE DOIT POUVOIR EXIGER UNE SÉQUENCE DE RÉARMEMENT, APRÈS L'ARMEMENT DU BOUTON D'ARRÊT D'URGENCE. LE FAIT DE PERMETTRE À LA MACHINE DE REDÉMARRER LE BOUTON D'ARRÊT D'URGENCE DÈS QUE POSSIBLE CRÉE UNE CONDITION DANGEREUSE POUVANT ENTRAÎNER DES BLESSURES GRAVES VOIRE MORTELLES.



Les entrées de sécurité du contrôleur de sécurité SC22-3 peuvent servir à surveiller des boutons d'arrêt d'urgence.

A2.7.1 Niveaux d'intégrité des circuits de sécurité

Les conditions du niveau de fiabilité de la commande ou de la catégorie de sécurité selon ISO 13849-1 (EN954-1) varient considérablement dans l'application des arrêts d'urgence. Bien que *Banner Engineering* recommande toujours le niveau de sécurité le plus élevé pour toute application, l'utilisateur est seul responsable de la sécurité de l'installation, de l'utilisation et de l'entretien de chaque système de sécurité et de leur conformité avec les instructions du fabricant et les lois et règlements applicables.

La performance de sécurité (intégrité) doit réduire le risque de dangers identifiés tels qu'ils sont déterminés par l'évaluation des risques de la machine. Se reporter à [Annexe A2.1](#) pour savoir si les conditions décrites dans l'ISO 13849-1 (EN 954-1) doivent être appliquées.

Outre les conditions définies dans cette [Annexe A2.7.1](#), la conception et l'installation du dispositif d'arrêt d'urgence doivent être conformes à l'ISO 13850.

A2.7.2 Conditions

Le bouton d'arrêt d'urgence doit fournir un ou deux contacts de sécurité qui sont fermés lorsque l'interrupteur est armé comme indiqué sur [Figure 36](#), [Figure 37](#) et [Figure 38](#). Une fois activé, le bouton d'arrêt d'urgence doit ouvrir tous ses contacts de sécurité et doit nécessiter une action délibérée (retrait ou déverrouillage) pour repasser en position armée à contact fermé. L'interrupteur doit être à ouverture positive (ou ouverture directe), tel que décrit par la norme IEC 60947-5-1. Une force mécanique appliquée sur ce bouton (interrupteur) est transmise directement aux contacts, les forçant à s'ouvrir. Ceci pour garantir que les contacts de l'interrupteur s'ouvriront à chaque fois que l'interrupteur est actionné.

Les normes IEC 60204-1 et ISO 13850 spécifient les conditions supplémentaires du dispositif d'arrêt d'urgence, notamment les suivantes :

- Les dispositifs d'arrêt d'urgence doivent être installés sur chaque poste de commande à partir desquels un arrêt d'urgence peut s'avérer nécessaire
 - Les boutons d'arrêt d'urgence doivent pouvoir être utilisés en permanence et faciles d'accès depuis toutes les stations de commande où ils sont situés. Ne pas inhiber ou bypasser les boutons d'arrêt d'urgence
 - Les actionneurs des dispositifs d'arrêt d'urgence doivent être de couleur rouge. Le fond entourant l'actionneur du dispositif doit être jaune. L'actionneur d'un dispositif à bouton poussoir doit être de type bouton poussoir à paume ou champignon.
 - L'actionneur d'un arrêt d'urgence doit être de type « manuel »
- ☛ *Pour certaines applications, des exigences supplémentaires doivent être satisfaites. L'utilisateur doit se conformer à tous les règlements applicables.*

A2.7.2.1 Niveaux d'intégrité des circuits de sécurité avec plusieurs boutons d'arrêt d'urgence

⚠ AVERTISSEMENT

ARRÊTS D'URGENCE MULTIPLES

QUAND DEUX INTERRUPTEURS D'ARRÊT D'URGENCE, OU PLUS, SONT RACCORDÉS AU MEME CONTRÔLEUR:

- **LES CONTACTS DES PÔLES CORRESPONDANTS DE CHAQUE INTERRUPTEUR DOIVENT ÊTRE RACCORDÉS EN SÉRIE. NE JAMAIS RACCORDER PLUSIEURS INTERRUPTEURS D'ARRÊT D'URGENCE EN PARALLÈLE SUR UN CONTRÔLEUR. UN RACCORDEMENT EN PARALLÈLE PERTURBE LA FONCTION DE SURVEILLANCE DES CONTACTS DE L'INTERRUPTEUR PAR LE CONTRÔLEUR ET CRÉE UNE SITUATION NON SÛRE QUI PEUT ENTRAÎNER DES BLESSURES GRAVES, VOIRE MORTELLES.**
- **CHAQUE BOUTON DOIT ÊTRE ACTIONNÉ INDIVIDUELLEMENT (ENGAGÉ) PUIS RÉARMÉ, TOUT COMME LE CONTRÔLEUR. CELA PERMET AU CONTRÔLEUR DE VÉRIFIER INDIVIDUELLEMENT CHAQUE BOUTON ET SON CÂBLAGE POUR DÉTECTER DES DÉFAILLANCES.**

NE PAS TESTER CHAQUE INTERRUPTEUR INDIVIDUELLEMENT DE CETTE MANIÈRE PEUT RÉSULTER EN ERREURS NON DÉTECTÉES ET CRÉER UNE SITUATION NON SÛRE QUI PEUT PROVOQUER DES BLESSURES GRAVES, VOIRE MORTELLES. CETTE VÉRIFICATION DOIT ÊTRE EFFECTUÉE PENDANT LES VÉRIFICATION PÉRIODIQUES.

Dans le cadre de l'évaluation nécessaire des risques pour la machine, la norme IEC 60204-1 indique que la performance de sécurité (intégrité) doit réduire le risque dérivé des dangers identifiés tels qu'ils sont déterminés par l'évaluation des risques. Voir [Annexe A2.1 en page 89](#) pour savoir si les conditions décrites par l'ISO 13849-1 (EN 954-1) doivent être appliquées.

En plus des conditions indiquées plus haut, la conception et l'installation d'un dispositif d'arrêt d'urgence (par ex. interrupteur, bouton ou interrupteur à câble) doivent être tels que le risque d'une défaillance catastrophique du dispositif entraînant la perte de la fonction de sécurité doit être exclue (par conception). Le dispositif doit être conforme aux exigences de ISO 13850 pour que les exclusions de défaillance de ISO 13849-2 soient applicables. Les dispositifs électromécaniques dont les contacts sont conçus selon IEC 60947-5-1 Annexe K et sont installés selon les instructions du fabricant doivent s'ouvrir quand le dispositif d'arrêt d'urgence est actionné.

A2.7.2.2 Catégorie 2

Une application d'arrêt d'urgence à une voie fournit généralement un niveau de performance de circuit de catégorie 2 car un court-circuit peut provoquer la perte de la fonction de sécurité. Le principe d'exclusion des défauts doit être intégré à la conception et à l'installation, afin d'éliminer ou de faire passer à un niveau de risque acceptable (minimum), la possibilité de défauts ou de défaillances non détectés susceptibles d'entraîner la perte de la fonction de sécurité. Pour le diagramme, se reporter à [Figure 36 en page 88](#).

A2.7.2.3 Catégorie 3

Une commutation à deux voies +24 Vcc est généralement une application de catégorie 3 car une seule défaillance n'entraîne pas une perte de sécurité. La perte d'une action de commutation d'une voie est détectée par l'action du bouton d'arrêt d'urgence, l'ouverture de la deuxième voie et la fonction de surveillance des entrées de sécurité. Toutefois, un court-circuit entre les voies d'entrée ou les sorties de sécurité peut ne pas être détecté. Il convient de noter qu'une accumulation de défauts peut entraîner la perte de la fonction de sécurité. Pour le diagramme, se reporter à [Figure 37 en page 88](#).

Le principe d'exclusion des défauts doit être intégré à la conception et à l'installation, afin d'éliminer ou de faire passer à un niveau de risque acceptable (minimum), la possibilité de défauts ou de défaillances non détectés susceptibles d'entraîner la perte de la fonction de sécurité.

A2.7.2.4 Catégorie 4

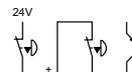
Les entrées de sécurité à auto surveillance peuvent être interfacées pour atteindre une application de catégorie 4. Le principe d'exclusion des défauts doit être intégré à la conception et à l'installation, afin d'éliminer ou de faire passer à un niveau de risque acceptable (minimum), la possibilité de défauts ou de défaillances non détectés susceptibles d'entraîner la perte de la fonction de sécurité. Pour le diagramme du circuit, se reporter à [Figure 38 en page 88](#).

A2.7.3 Possibilités de connexions

☛ **Le dispositif est illustré en état armé ou Run.**

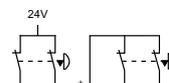
A2.7.3.1 Canal simple, 1 borne – canal simple, 2 borne – canal simple, contact PNP

Ces circuits normalement sont conformes aux exigences de ISO 13849-1 catégorie 2, en fonction de la conception et de l'installation de l'interrupteur. Au minimum, l'interrupteur doit être un dispositif de sécurité de niveau de catégorie 2. Le canal simple, 1 borne et canal simple, contact PNP ne peut pas détecter un court-circuit vers une autre source d'alimentation. Le raccordement canal simple, 2 bornes utilise une surveillance d'impulsions et peut détecter un court-circuit vers une autre source d'alimentation. Il faut utiliser l'exclusion de défaillance pour obtenir un plus haut niveau d'intégrité du circuit de sécurité.



A2.7.3.2 Double canal, 2 bornes – Double canal, 3 bornes

Ce circuit peut normalement répondre aux exigences de ISO 13849-1 catégorie 3, en fonction de la conception et de l'installation des interrupteurs. Les connexions canal double, 3 bornes utilisent une surveillance d'impulsions qui peuvent détecter un court-circuit vers une autre source d'alimentation. Les connexions canal double, 2 bornes peuvent détecter un court-circuit entre les canaux si les contacts sont ouverts pendant plus de 2 secondes.



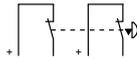
A2.7.3.3 Double canal, PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4 en fonction du niveau de sécurité, de l'installation et de la possibilité de détection de défaillance (par ex. court-circuit) des dispositifs. Le contrôleur de sécurité SC22-3 ne détecte pas les courts-circuits dans cette configuration.



A2.7.3.4 Double canal, 4 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 4, en fonction de la conception et de l'installation des interrupteurs. Ce circuit peut détecter un court-circuit entre canaux ou vers une autre source d'alimentation.



A2.8 INTERRUPTEUR À CÂBLE



Les interrupteurs d'arrêt d'urgence à câble utilisent un câble d'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 ont à peu près les mêmes exigences que les boutons d'arrêt d'urgence, comme un fonctionnement à ouverture positive (ou ouverture directe), selon IEC 60947-5-1. Voir [Annexe A2.7 en page 104](#) sur les boutons d'arrêt d'urgence pour les informations supplémentaires applicables.

Il est recommandé d'utiliser des interrupteurs d'arrêt d'urgence à câble qui sont capables de réagir à une traction dans tous les sens, mais aussi à une détente ou un cassure du câble. Normalement ceci est accompli par des contacts séparés dans l'interrupteur. Quand le câble est correctement tendu, les deux contacts de l'interrupteur sont fermés. Quand on tire sur le câble, les contacts à ouverture positive s'ouvrent. Si le câble se casse ou se détend, le second jeu de contacts s'ouvre. Voir [Annexe A2.8.2 en page 107](#) pour les possibilités de connexion.

Certains interrupteurs d'arrêt d'urgence à câble fournissent une fonction de verrouillage qui nécessite un réarmement manuel après utilisation. Si on utilise un interrupteur qui ne fournit pas de fonction de verrouillage quand le câble est relâché, un circuit de verrouillage séparé est nécessaire et ce circuit peut être fourni par le contrôleur de sécurité SC22-3.

A2.8.1 Instructions d'installation

Pour installer un interrupteur d'arrêt d'urgence à câble observer les instructions suivantes :

- Le câble doit être facilement accessible et visible sur toute sa longueur. Des marqueurs ou des drapeaux peut être fixés sur le câble pour augmenter sa visibilité
- Les points de montage, y compris les points d'ancrage, doivent être rigides
- Le câble ne doit pas frotter au niveau des supports. Il est recommandé d'utiliser des poulies
- Utiliser des poulies pour passer un angle ou si la direction change, même légèrement
- Ne pas faire passer le câble dans un conduit ou un tube quelconque
- Ne pas attacher de poids au câble
- La température influe sur la tension du câble. Le câble s'allonge quand la température augmente et se rétrécit quand elle décroît. Des variations importantes de température nécessitent des vérifications fréquentes du réglage de la tension
- Ne pas dépasser la longueur maximale de câble recommandée par le fabricant
- Monter l'interrupteur solidement sur une surface stable et fixe
- Les points d'ancrage du câble doivent être solides et stationnaires et pouvoir supporter la tension constante du câble
- Chaque installation d'arrêt d'urgence par câble doit être testée et inspecté à intervalle appropriés pour pouvoir fonctionner selon l'évaluation des risques de l'utilisateur, en se basant sur la sévérité de l'environnement de fonctionnement et la fréquence d'utilisation de l'interrupteur
- Les poulies et autres pièces mobiles associées au câble doivent être lubrifiées périodiquement

A2.8.2 Possibilités de connexions

Le dispositif est illustré en état armé ou Run.

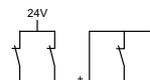
A2.8.2.1 Canal simple, 1 borne – canal simple, 2 borne – canal simple, contact PNP

Ces circuits normalement sont conformes aux exigences de ISO 13849-1 catégorie 2, en fonction de la conception et de l'installation de l'interrupteur. Au minimum, l'interrupteur doit être un dispositif de sécurité de niveau de catégorie 2. Le canal simple, 1 borne et canal simple, contact PNP ne peut pas détecter un court-circuit vers une autre source d'alimentation. Le raccordement canal simple, 2 bornes utilise une surveillance d'impulsions et peut détecter un court-circuit vers une autre source d'alimentation. Il faut utiliser l'exclusion de défaillance pour obtenir un plus haut niveau d'intégrité du circuit de sécurité.



A2.8.2.2 Double canal, 2 bornes – Double canal, 3 bornes

Ce circuit peut normalement répondre aux exigences de ISO 13849-1 catégorie 3, en fonction de la conception et de l'installation des dispositifs de sortie. Les connexions canal double, 3 bornes utilisent une surveillance d'impulsions qui peuvent détecter un court-circuit vers une autre source d'alimentation. Les connexions canal double, 2 bornes et canal double, 3 bornes peuvent détecter un court-circuit entre les canaux si les contacts sont ouverts pendant plus de 2 secondes.



A2.8.2.3 Double canal, PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4 en fonction du niveau de sécurité, de l'installation et de la possibilité de détection de défaillance (par ex. court-circuit) des dispositifs de sortie. Le contrôleur de sécurité SC22-3 ne détecte pas les courts-circuits dans cette configuration.



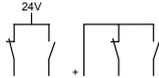
A2.8.2.4 Double canal, 4 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 4, en fonction du niveau de sécurité et de l'installation du dispositif de sortie. Ce circuit peut détecter un court-circuit entre canaux ou vers une autre source d'alimentation.



A2.8.2.5 Complémentaire, 2 bornes – Complémentaire, 3 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation du dispositif de sortie. Ce circuit peut détecter un court-circuit entre canaux. En situation activé (par ex. S1 fermé /S2 ouvert ci-dessous) un court-circuit entre les contacts fermés peut augmenter le temps de réponse basé sur le temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que ce qui est spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.8.2.6 complémentaire, contact PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation du dispositif de sortie. Ce circuit peut détecter un court-circuit entre les canaux. En situation activé (par ex. S1 ON / S2 OFF ci-dessous) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que ce qui est spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.9 DISPOSITIF D'ACTIVATION (SIMULTANÉ)



Un dispositif d'activation est une commande manuelle qui, parce qu'elle est actionnée en continu, permet à la machine d'initier son cycle en conjonction avec une commande de démarrage. Les normes qui couvrent la conception et l'application des dispositifs d'activation sont les suivantes :

ISO 12100-1/-2

IEC 60204-1

A2.9.1 Instructions d'installation

En fonction de l'application, l'utilisation d'un dispositif d'activation peut nécessiter une supervision et ne permettre qu'un fonctionnement limité de la machine quand la personne utilisant le dispositif est exposée à une situation dangereuse. Quand le dispositif d'activation est utilisé, la commande du mouvement de la machine doit être interdit à partir d'autres sources qui surclasseraient le fonctionnement du dispositif d'activation. Le simple fait d'actionner le dispositif d'activation ne doit pas créer un risque.

Un dispositif d'activation permet une situation dangereuse s'il est actionné en permanence dans une seule position. Dans toutes les autres positions, le risque doit être éliminé et la fonction de démarrage inhibée.

Étant donné que la réaction d'une personne en cas d'urgence peut être soit de relâcher soit de serrer la poignée, de nombreuses normes exigent l'utilisation d'un dispositif à trois positions :

- **Position 1** – La fonction OFF de l'interrupteur (l'actionneur n'est pas utilisé)
- **Position 2** – La fonction d'utilisation (l'actionneur est utilisé en son point milieu)
- **Position 3** – La fonction OFF de l'interrupteur (l'actionneur est utilisé au-delà de son point milieu)

Le relâchement ou l'utilisation au-delà de son point milieu de fonctionnement normal (position 2) du dispositif d'activation doit déclencher un arrêt immédiat du mouvement ou de la situation dangereuse. Il est nécessaire de relâcher le dispositif d'activation et de le réactiver avant que le mouvement de la machine puisse être réinitié.

S'ils sont autorisés, les dispositifs à deux positions utilisent les deux positions suivantes :

- **Position 1** – La fonction OFF de l'interrupteur (l'actionneur n'est pas utilisé)
- **Position 2** – Fonction d'activation (l'actionneur est utilisé)

La fonction d'arrêt doit être soit un arrêt fonctionnel de catégorie 0 ou de catégorie 1. La conception et l'installation du dispositif d'activation doit considérer les problèmes ergonomiques (force, posture, etc.) d'un actionnement permanent. Un moyen visuel d'indiquer que le dispositif est actif peut être demandé.

☛ *Seuls des individus formés et qualifiés (voir [Paragraphe 1.8.2 en page 4](#)) sont autorisés à utiliser un dispositif d'activation s'il bypass d'autres protections.*

La sécurité des procédures de travail doit inclure, sans y être limité, l'utilisation du dispositif d'activation, les risques associés et la tâche qui nécessite l'utilisation du dispositif d'activation.

Si plus d'une personne doivent être protégées par l'utilisation de dispositifs d'activation, chaque personne doit avoir son propre dispositif. Chaque dispositif d'activation doit être utilisé en même temps pour que la machine puisse être initiée.

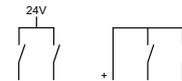
Le moyen de remettre la machine en mode de production doit être situé en dehors de la zone dangereuse, où il ne peut pas être atteint depuis l'intérieur de la zone et doit être protégé contre une utilisation non volontaire. En outre, l'opérateur de l'interrupteur de réarmement doit avoir une vue complète de toute la zone protégée et vérifier qu'aucune personne ne se trouve dans cette zone pendant la procédure de réarmement.

A2.9.2 Possibilités de connexions

☛ *Le dispositif est illustré en état position activée ou arrêté.*

A2.9.2.1 Double canal, 2 bornes – Double canal, 3 bornes

Ce circuit peut normalement répondre aux exigences de ISO 13849-1 catégorie 2 ou catégorie 3, en fonction du niveau de sécurité et de l'installation des dispositifs d'activation. Les connexions canal double, 3 bornes utilisent une surveillance d'impulsions qui peuvent détecter un court-circuit vers une autre source d'alimentation. Les connexions canal double, 2 bornes et canal double, 3 bornes peuvent détecter un court-circuit entre les canaux si les contacts sont ouverts pendant plus de 2 secondes.



A2.9.2.2 Double canal, PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4 en fonction du niveau de sécurité, de l'installation et de la possibilité de détection de défaillance (par ex. court-circuit) du dispositif d'activation. Le contrôleur de sécurité SC22-3 ne détecte pas les courts-circuits dans cette configuration.



A2.9.2.3 Double canal, 4 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation du dispositif d'activation. Ce circuit peut détecter un court-circuit entre canaux ou vers une autre source d'alimentation.



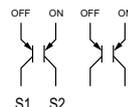
A2.9.2.4 Complémentaire, 2 bornes – Complémentaire, 3 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation du dispositif de sortie. Ce circuit peut détecter un court-circuit entre canaux. En situation activé (par ex. S1 ouvert / S2 fermé ci-dessous) un court-circuit entre les contacts fermés peut augmenter le temps de réponse basé sur le temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que ce qui est spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.9.2.7 2 complémentaires, contact PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 3 ou catégorie 4 en fonction de la conception et de l'installation du dispositif d'activation. Ce circuit peut détecter un court-circuit entre les canaux. En situation de protection fermée (par ex. S1 OFF / S2 ON) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que celui spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.9.2.5 complémentaire, contact PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation du dispositif de sortie. Ce circuit peut détecter un court-circuit entre les canaux. En situation activé (par ex. S1 OFF / S2 ON ci-dessous) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que ce qui est spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).

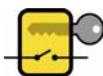


A2.9.2.6 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 3 ou catégorie 4 en fonction de la conception et de l'installation du dispositif d'activation. Ce circuit peut détecter un court-circuit entre les canaux. En situation de protection fermée (par ex. S1 ouvert / S2 fermé) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que celui spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.10 INTERRUPTEUR DE BYPASS (BYPASSANT LES PROTECTIONS)



Le Contrôleur de sécurité SC22-3 peut servir à surveiller des interrupteurs qui initient le bypass d'un dispositif de protection.

Bypasser ou passer outre un dispositif de protection est une interruption ou une suspension manuelle de la fonction normale de protection sous contrôle d'un superviseur. Cela se produit normalement en choisissant un mode de bypass utilisant un interrupteur à clé pour faciliter la configuration de la machine, l'alignement et les réglages des faisceaux, l'apprentissage d'un robot et la recherche de panne du processus.

A2.10.1 Conditions

Les conditions pour bypasser un dispositif de protection sont les suivantes* :

- La fonction de bypass doit être temporaire
- Le moyen de sélectionner et d'activer le bypass 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 pas à pas ou à vitesse lente). Le mode de bypass ne doit pas être utilisé en production.
- Des protections supplémentaires doivent être installées. Le personnel ne doit pas être exposé aux dangers
- Le moyeu de bypass doit être en pleine vue de la protection qui est bypassée
- L'initiation du mouvement ne doit être fait que par l'intermédiaire d'une commande de type maintenir pour fonctionner
- Tous les arrêts d'urgence doivent rester actifs
- Le moyen de bypasser doit être employé au même niveau de fiabilité que la protection
- Une indication visuelle que le dispositif de protection a été bypassé doit exister et être facilement visible de l'emplacement de la protection
- Le personnel doit être formé à l'utilisation de la protection et à l'utilisation du bypass
- Il faut effectuer une évaluation des risques et une réduction des risques (selon la norme applicable)
- Le réarmement, l'activation ou l'effacement du dispositif de protection ne doit pas initier de mouvement dangereux ni créer de situation dangereuse

* Ce résumé provient des sources suivantes, et d'autres sources : ISO 13849-1 (EN954-1) et IEC60204-1

Le fait de bypasser un dispositif de protection ne doit pas être confondu avec un inhibition qui est une suspension temporaire et automatique de la fonction de protection d'un dispositif de protection pendant une partie non dangereuse du cycle machine. L'inhibition permet d'alimenter manuellement ou automatiquement une machine ou un processus sans déclencher un ordre d'arrêt. Un autre terme est facilement confondu avec bypass est blanking, qui désensibilise une partie du champ sensible d'un dispositif optique de sécurité (par ex. désactiver un ou plusieurs faisceaux d'une barrière immatérielle pour qu'une intrusion dans un faisceau spécifique soit ignorée).

A2.10.1.1 Procédures de sécurité d'exploitation et de formation

L'utilisateur doit aussi traiter la possibilité qu'une personne puisse bypasser le dispositif de protection puis oublier de réarmer la protection ou oublier de prévenir les autres personnes de la situation bypassée du dispositif de protection ; dans les deux cas, on se trouve dans une situation non sûre. Une méthode possible pour éviter ceci est de développer une procédure de sécurité du travail et de s'assurer que le personnel est formé et suit correctement la procédure.

Les procédures de sécurité du travail sont un moyen pour des personnes de contrôler l'exposition aux risques en utilisant des procédures écrites pour certaines tâches particulières et leurs risques. Ces procédures fournissent aussi la documentation de base à un programme de formation. Encore une fois, le personnel doit être formé à l'utilisation des protections et à l'utilisation du bypass.

A2.10.1.2 Consignations

☛ *Il n'y a pas de norme européenne particulière qui couvre les consignations. Ce sujet est couvert dans les normes américaines OSHA 29CFR1910.147 "Le contrôle d'énergies dangereuses (consignations)" ou ANSI 2244.1 "consignations de sources d'énergie"*

L'intention est d'éviter que la machine ne puisse fonctionner quand elle est temporairement à l'arrêt ou en réparation. Des démarrages non prévus ont provoqué des blessures et des morts. Cette approche garantit que l'alimentation électrique est coupée à la machine en bloquant physiquement l'interrupteur d'alimentation en position OFF. De plus, une étiquette est rajoutée sur l'interrupteur qui identifie le processus en cours et le personnel impliqué.

Si une consignation doit être appliquée pendant des situations d'entretien ou de service d'une machine dans laquelle une mise en service non prévue, un démarrage ou le relâchement d'énergie stockée peuvent provoquer des blessures, les normes ci-dessus doivent être respectées. L'utilisateur doit se référer à ces normes pour s'assurer que le bypass d'un dispositif de protection n'entre pas en conflit avec les exigences de ces normes.

A2.10.2 Possibilités de connexions

☛ *Le dispositif est illustré non actionné ou en état OFF.*

A2.10.2.1 Double canal, 2 bornes – Double canal, 3 bornes

Ce circuit peut normalement répondre aux exigences de ISO 13849-1 catégorie 2 ou catégorie 3, en fonction du niveau de sécurité et de l'installation des interrupteurs de bypass. Les connexions canal double, 3 bornes utilisent une surveillance d'impulsions qui peuvent détecter un court-circuit vers une autre source d'alimentation. Les connexions canal double, 2 bornes et canal double, 3 bornes peuvent détecter un court-circuit entre les canaux si les contacts sont ouverts pendant plus de 2 secondes.



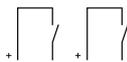
A2.10.2.2 Double canal, PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4 en fonction du niveau de sécurité, de l'installation et de la possibilité de détection de défaillance (par ex. court-circuit) des interrupteurs de bypass. Le contrôleur de sécurité SC22-3 ne détecte pas les courts-circuits dans cette configuration.



A2.10.2.3 Double canal, 4 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation des interrupteurs de bypass. Ce circuit peut détecter un court-circuit entre canaux ou vers une autre source d'alimentation.



A2.10.2.4 Complémentaire, 2 bornes – Complémentaire, 3 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation des interrupteurs de bypass. Ce circuit peut détecter un court-circuit entre canaux. En situation activé (par ex. S1 ouvert / S2 fermé ci-dessous) un court-circuit entre les contacts fermés peut augmenter le temps de réponse basé sur le temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que ce qui est spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.10.2.5 Complémentaire, contact PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation des interrupteurs de bypass. Ce circuit peut détecter un court-circuit entre les canaux. En situation activé (par ex. S1 OFF / S2 ON ci-dessous) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que ce qui est spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



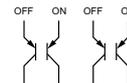
A2.10.2.6 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 4 en fonction de la conception et de l'installation des interrupteurs de bypass. Ce circuit peut détecter un court-circuit entre les canaux. En situation de protection fermée (par ex. S1 ouvert / S2 fermé) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que celui spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.10.2.7 2 complémentaires, contact PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 4 en fonction de la conception et de l'installation des interrupteurs de bypass. Ce circuit peut détecter un court-circuit entre les canaux. En situation de protection fermée (par ex. S1 OFF / S2 ON) un court-circuit entre les contacts fermés peut augmenter le temps de réponse sur la base du temps d'anti-rebond. Dans cette situation, le temps de réponse peut être plus long que celui spécifié, sur la base du temps d'anti-rebond (sélectionné) (voir [Paragraphe 4.5 en page 27](#)).



A2.11 CAPTEUR D'INHIBITION (PAIRE)

A2.11.1 Fonction d'inhibition

⚠ AVERTISSEMENTS

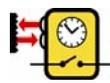
LIMITES DE L'INHIBITION

L'INHIBITION N'EST AUTORISÉE QUE PENDANT LA PARTIE NON DANGEREUSE DU CYCLE MACHINE.

UNE APPLICATION D'INHIBITION DOIT ÊTRE ÉTUDIÉE POUR QU'AUCUNE DÉFAILLANCE D'UN COMPOSANT UNIQUE N'EMPÊCHE LA COMMANDE D'ARRÊT DE LA MACHINE ET DE SES CYCLES SUCCESSIFS JUSQU'À CE QUE LA DÉFAILLANCE SOIT RÉPARÉE SELON ISO 13855.

LES ENTRÉES DE MUTING DOIVENT ÊTRE REDONDANTES

IL N'EST PAS ACCEPTABLE D'UTILISER UN CONTACTEUR, UN INTERRUPTEUR OU UN RELAIS UNIQUE AVEC DEUX CONTACTS NO. LES CONTACTS D'ENTRÉE DE MUTING D'UN CONTACTEUR UNIQUE, AVEC PLUSIEURS SORTIES, PEUVENT ÊTRE DÉFAILLANTS, ENTRAÎNANT UNE SÉQUENCE DE MUTING À UN MOMENT NON PROPICE. CELA PEUT ENTRAÎNER UNE SITUATION DANGEREUSE.



L'utilisateur est obligé de concevoir, installer et faire fonctionner le système de sécurité de façon à protéger le personnel et à minimiser le risque de contournement de la protection.

Pour que la protection puisse être inhibée, le système d'inhibition doit remplir les conditions suivantes :

- Identifier les parties du cycle machine qui sont sans risques,
- Sélectionner des bons dispositifs d'inhibition
- Monter et installer ces dispositifs d'inhibition correctement.

Le contrôleur de sécurité SC22-3 peut surveiller et répondre à des signaux redondants qui initie 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 ; par ex. cela permet à un objet ou à une personne de passer dans la zone définie d'une barrière immatérielle sans générer un ordre d'arrêt (à ne pas confondre avec blanking, qui désactive un ou plusieurs faisceaux d'une barrière immatérielle, augmentant ainsi sa résolution).

L'inhibition peut être déclenchée par plusieurs dispositifs externes. Ceci permet de choisir entre plusieurs options (voir la personnalisation du système en [Annexe A2.11.2 en page 113](#)) pour répondre aux besoins d'une application spécifique.

Deux dispositifs de dispositifs d'inhibition doivent se déclencher simultanément l'un l'autre (dans un délai de 3 secondes). Cela permet de réduire le risque de défaillance de mode commun ou de fraude.

A2.11.2 Exigences

Le commencement et la fin d'un cycle d'inhibition doivent être déclenchés par les sorties de l'une des paires de dispositifs d'inhibition, selon l'application. Les deux paires de dispositifs d'inhibition doivent avoir des contacts N.O. ou des sorties PNP, qui doivent répondre toutes les deux aux exigences du dispositif d'inhibition, décrites ci-dessous. Ces contacts doivent se fermer (conducteurs) quand l'interrupteur est activé pour initier l'inhibition et doivent s'ouvrir (non-conducteurs) quand l'interrupteur n'est pas activé et est en situation d'alimentation OFF.

Le contrôleur surveille les dispositifs d'inhibition pour vérifier que leurs sorties passent sur ON en moins de 3 s. Si les entrées ne répondent pas à cette condition de simultanéité une situation d'inhibition ne peut pas se produire.

On peut utiliser plusieurs types de dispositifs d'inhibition, dont, mais sans s'y limiter :

- Détecteurs de position
- Détecteurs photoélectriques
- Contacteurs de sécurité à ouverture positive
- Détecteurs de proximité à induction
- Interrupteurs à tige flexible

Voir [Annexe A2.11.2.1 en page 113](#) pour plus d'informations.

A2.11.2.1 Généralités

Les dispositifs d'inhibition (normalement des détecteurs et des commutateurs) doivent, au minimum, répondre aux conditions suivantes :

- Il doit y avoir un minimum de deux dispositifs d'inhibition câblés indépendamment l'un de l'autre
- Les dispositifs d'inhibition doivent avoir des contacts N.O. ou des sorties PNP (qui doivent répondre toutes les deux aux exigences des spécifications ([Paragraphe 3.2.1 en page 21](#))) ou de l'action commutation complémentaire. Au moins un de ces contacts doit se fermer quand l'interrupteur est activé pour initier l'inhibition et doivent s'ouvrir (non-conducteurs) quand l'interrupteur n'est pas activé et est en situation d'alimentation OFF.
- L'activation des entrées de la fonction muting doit provenir de sources séparées. Ces sources doivent être montées séparément pour éviter de déclencher un muting non intentionnel soit à cause d'une erreur ou d'un défaut d'alignement, soit suite à une défaillance de mode commun (Par exemple, un endommagement physique de la surface de montage peut désaligner les deux dispositifs d'inhibition, donnant de faux signaux d'entrée de muting.) Seule l'une de ces sources peut passer, ou être affectée, par un automate programmable (automate) ou un dispositif semblable
- Les dispositifs d'inhibition doivent être installés de façon à ce qu'il ne soit pas facile de les contourner
- Les dispositifs d'inhibition doivent être montés de façon à ce que leur position et leur alignement ne soient pas faciles à changer
- Il ne faut pas qu'une condition d'environnement puisse déclencher une condition de muting (contamination extrême de l'air par exemple)
- Les dispositifs d'inhibition ne doivent pas entraîner de retard ou d'autres perturbations temporelles sauf :
 - si ces fonctions sont accomplies de façon à ce qu'aucune défaillance unique d'un composant n'empêche la suppression du risque
 - l'arrêt des cycles machine suivants jusqu'à ce que la défaillance soit corrigée et
 - aucun nouveau risque ne provienne de l'allongement de la période de muting).

A2.11.2.2 Exemples de détecteurs et de contacteurs d'inhibition (muting)

⚠ AVERTISSEMENT

ÉVITER LES INSTALLATIONS DANGEREUSES

DEUX OU QUATRE INTERRUPTEURS DE POSITION INDÉPENDANTS (À M1-M2 OU M3-M4) DOIVENT ÊTRE POSITIONNÉS ET RÉGLÉS CORRECTEMENT POUR NE SE FERMER QUE LORSQUE LE RISQUE N'EXISTE PLUS ET NE SE ROUVRIRE QUE LORSQUE LE CYCLE EST TERMINÉ OU QUE LE RISQUE SE PRÉSENTE À NOUVEAU. S'ILS SONT MAL POSITIONNÉS OU MAL RÉGLÉS, DES BLESSURES GRAVES, VOIRE MORTELLES, PEUVENT EN DÉCOULER

L'UTILISATEUR A LA RESPONSABILITÉ DE S'ASSURER QUE L'ENSEMBLE DES LOIS, RÉGLEMENTS, CODES ET NORMES LOCALES, DE L'ÉTAT ET NATIONALES APPLICABLES À L'APPLICATION SONT RESPECTÉS. IL EST EXTRÊMEMENT 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.

Détecteurs photoélectriques (mode barrière)

Les détecteurs en mode barrière, qui initient la situation d'inhibition quand le faisceau est bloqué, doivent être configurés pour fonctionnement sombre (DO) et avoir des contacts de sortie ouverts (non conducteurs) en situation d'alimentation coupée OFF. L'émetteur et le récepteur de chaque paire doivent être alimentés par la même source pour réduire le risque de défaillances de mode commun.

Détecteurs optoélectroniques (mode rétro-réfléctif polarisé)

L'utilisateur doit s'assurer qu'un faux déclenchement « miroir » (activation par une surface brillante ou réfléchissante) n'est pas possible. Les détecteurs *Banner LP* à polarisation linéaire peuvent grandement réduire ou éliminer cet effet.

Utiliser un détecteur configuré pour fonctionnement clair (LO ou N.O.) pour initier une inhibition quand la cible ou la bande rétro-réfléchissante est détectée (par ex. position base). Utiliser un détecteur configuré pour fonctionnement sombre (DO ou N.F.) si la situation d'inhibition est déclenchée par le blocage d'un rayon (par ex. entrée/sortie). Les deux situations doivent avoir des contacts de sortie ouverts (non conducteurs) quand ils ne sont pas sous tension OFF.

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 pourrait entraîner une situation non sûre.

Détecteurs de proximité à induction

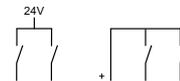
Normalement, les détecteurs de proximité à induction servent à initier un cycle d'inhibition quand une surface métallique est détectée. En raison de fuites de courant importantes entraînant de fausses situations ON, il ne faut pas utiliser de détecteurs à deux fils. On ne peut utiliser que des détecteurs à trois ou quatre fils avec des sorties digitales PNP, ou à contact dur qui sont séparés de l'alimentation d'entrée.

A2.11.3 Possibilités de connexions

Le contrôleur dispose de configurations différentes pour les dispositifs d'inhibition. Il faut utiliser une ou deux paires de dispositifs d'inhibition (normalement des détecteurs ou des interrupteurs) ; ces paires sont désignées M1-M2 et M3-M4. dans le diagramme ci-dessous, on suppose que chaque contact ou sortie est généré par un dispositif individuel pour la catégorie 3 et la catégorie 4.

A2.11.3.1 Double canal, 2 bornes – Double canal, 3 bornes

Ce circuit peut normalement répondre aux exigences de ISO 13849-1 catégorie 2 ou catégorie 3, en fonction de l'installation des dispositifs d'inhibition. Pour répondre aux conditions de catégorie 4, l'utilisateur doit éliminer par conception ou d'autres moyens la possibilité d'un court-circuit entre les canaux d'entrée (voir chapitre [Annexe A2.1.2 en page 89](#)). Les connexions canal double, 3 bornes utilisent une surveillance d'impulsions qui peuvent détecter un court-circuit vers une autre source d'alimentation. Les connexions canal double, 2 bornes et canal double, 3 bornes peuvent détecter un court-circuit entre les canaux si les contacts sont ouverts pendant plus de 2 secondes.



A2.11.3.2 Double canal, PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2 ou catégorie 3 en fonction de l'installation et de la possibilité de détection de défaillance (par ex. court-circuit) du dispositif d'inhibition. Pour répondre aux conditions de catégorie 4, l'utilisateur doit éliminer par conception ou d'autres moyens la possibilité d'un court-circuit entre les canaux d'entrée (voir chapitre [Annexe A2.1.2 en page 89](#)). Le contrôleur de sécurité SC22-3 ne détecte pas les courts-circuits dans cette configuration.



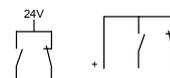
A2.11.3.3 Double canal, 4 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction de l'installation des dispositifs d'inhibition. Ce circuit peut détecter un court-circuit entre canaux ou vers une autre source d'alimentation.



A2.11.3.4 Complémentaire, 2 bornes – Complémentaire, 3 bornes

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation du dispositif d'inhibition. Ce circuit peut détecter un court-circuit entre canaux. Ce circuit peut détecter un court-circuit entre les canaux. La connexion complémentaire, 3 bornes peut détecter un court-circuit vers une autre source d'alimentation, quand le contact est fermé.



A2.11.3.5 complémentaire, contact PNP

Ce circuit peut répondre aux exigences de ISO 13849-1 catégorie 2, catégorie 3 ou catégorie 4, en fonction du niveau de sécurité et de l'installation du dispositif de sortie. Ce circuit peut détecter un court-circuit entre les canaux.



A2.11.4 Inhibition (ME),

L'entrée d'activation d'inhibition (ME) est une entrée non sécurisée. Quand l'entrée est fermée, le module autorise une action d'inhibition. L'ouverture de cette entrée pendant que le système est inhibé n'a pas d'influence.

Exemples typiques d'utilisation d'activation de l'inhibition:

- Permettre à la logique de commande de la machine de créer une "fenêtre" de commencement d'inhibition; Pour empêcher l'inhibition de se produire ou Pour réduire le risque de bypass non autorisé ou non voulu ou pour contourner le système de sécurité.

A2.11.4.1 Fonction de réarmement du contrôleur de simultanéité

L'entrée inhibition activée peut aussi servir à réarmer le contrôleur de simultanéité des entrées d'inhibition. Si une entrée est activée pendant plus de trois secondes avant que la seconde entrée ne s'active, le contrôleur de simultanéité empêche le cycle d'inhibition de se produire. Cela peut être dû à un arrêt normal de la ligne de montage qui peut bloquer un dispositif d'inhibition faire que le temps de simultanéité soit dépassé.

If the ME input is cycled (Closed-Open-Closed) while one Mute Input is active, the Simultaneity Timer is Reset and if the second Mute Input becomes active within three seconds, a normal Mute Cycle begins. The timing requirement for the Closed-Open-Closed is similar to the Manual Reset function. Initially, the input needs to be active (Closed) for longer than 0,25 second, then open for longer than 0,25 second, but not longer than 2 seconds, and then must Reclose to Reset the Simultaneity Timer. The function can Reset the timer only once per Mute Cycle (i.e. all Mute Inputs M1–M4 must open before another Reset can occur).

A2.11.5 Sortie de voyant d'inhibition (ML)

⚠ PRÉCAUTION

L'ÉTAT DE MUTING DOIT ÊTRE FACILEMENT OBSERVABLE

Une indication de l'inhibition du dispositif de sécurité doit être prévue et facilement observable.

Une défaillance de cette indication doit être détectable et éviter le muting suivant, ou le fonctionnement de cet indicateur doit être vérifié à intervalles appropriés.

La surveillance du voyant doit être sélectionnée si l'application doit être conforme à IEC 61496.

Certaines applications nécessitent qu'un voyant (ou un autre moyen) indique quand le dispositif de sécurité (par ex. la barrière immatérielle) est inhibée ; le contrôleur le fournit par les sorties d'état. Si un signal de sortie surveillé est nécessaire (voir [Mise en garde](#) plus haut), les sorties d'état O9 et O10 peuvent être configurées comme sortie surveillée. La sortie surveillée empêche l'initiation d'une inhibition si une défaillance du voyant est détectée. Si l'application nécessite la conformité à IEC 61496, il faut sélectionner surveillance de la lampe et le voyant utilisé doit répondre aux exigences applicables.

A2.11.6 Limite de temps d'inhibition (temporisateur de porte arrière)

⚠ AVERTISSEMENT

LIMITE DE TEMPS D'INHIBITION

UNE DURÉE INFINIE POUR LE MINUTEUR D'INHIBITION (LA DÉSACTIVATION PAR EXEMPLE) DOIT ÊTRE SÉLECTIONNÉE UNIQUEMENT SI LA POSSIBILITÉ D'UN CYCLE DE MUTING INAPPROPRIÉ OU IMPRÉVU EST RÉDUITE, TEL QUE DÉFINI ET AUTORISÉ PAR L'ÉVALUATION DES RISQUES DE LA MACHINE. IL EST DE LA RESPONSABILITÉ DE L'UTILISATEUR DE GARANTIR QUE CELA NE PROVOQUE PAS DE SITUATION DANGEREUSE.

Le temps limite d'inhibition (minuteur de porte arrière) permet de sélectionner une période maximale de temps pendant laquelle l'inhibition peut se situer. Cette caractéristique évite que l'on essaye volontairement de tricher avec le dispositif d'inhibition pour déclencher une inhibition non autorisée. Il sert aussi à détecter une défaillance de mode commun qui affecterait tous les dispositifs d'inhibition de l'application.

Le minuteur commence quand le second dispositif d'inhibition effectue la condition de simultanéité (en moins de 3 secondes du premier dispositif) et permet à l'inhibition de continuer pendant le temps prédéterminé – quelle que soit l'indication des signaux des dispositifs d'inhibition. Si le dispositif d'entrée inhibé est en état OFF, les sorties assignées aux OSSD passent sur OFF et doivent généralement être réarmées manuellement (si le dispositif d'entrée est configuré pour un réarmement manuel).

A2.11.7 Inhibition à la mise sous tension



AVERTISSEMENT

INHIBITION LA MISE SOUS TENSION

LA FONCTION d'inhibition à la mise sous tension NE DOIT ÊTRE UTILISÉE QUE DANS LES APPLICATIONS SUIVANTES :

- L'INHIBITION DU SYSTÈME (M1 ET M2 FERMÉES) EST NÉCESSAIRE À LA MISE SOUS TENSION ET
- SON UTILISATION NE DOIT, EN AUCUN CAS, EXPOSER LE PERSONNEL À UN DANGER

Quand elle est sélectionnée, la fonction Inhibition à la mise sous tension déclenche une inhibition lorsque le système est mis sous tension, l'entrée d'activation de l'inhibition est fermée (si elle est confirmée), les entrées du dispositif de sécurité sont activées (fermées) et soit M1-M2 soit M3-M4 (mais pas les quatre à la fois) sont fermées.

Si la configuration est pour un réarmement automatique, le contrôleur attend 2 secondes que les dispositifs d'entrée deviennent actifs (fermés) pour accommoder les systèmes qui ne seraient pas immédiatement actifs à la mise sous tension.

S'il est configuré sur réarmement manuel, le premier réarmement après l'activation (fermeture) des dispositifs de sortie déclenche un cycle d'inhibition si toutes les autres conditions sont remplies.

A2.11.8 Miroirs d'angle, systèmes optiques de sécurité et inhibition

Les miroirs sont normalement utilisés avec des barrières immatérielles 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 sur tous les côtés. Il est alors possible à un individu d'entrer dans la zone protégée sans être détecté et sans qu'un ordre d'arrêt n'ait été émis en direction de la commande de la machine. Cette protection supplémentaire est normalement fournie par un dispositif supplémentaire qui reste actif pendant que la protection primaire est inhibée. Par conséquent, les miroirs ne sont normalement pas autorisés pour les applications avec muting.

A2.11.9 Dispositifs de sécurité de détection de présence multiples



AVERTISSEMENT

PROTECTION DE PLUSIEURS ZONES

NE PAS PROTÉGER PLUSIEURS ZONES, AVEC DES MIROIRS OU PLUSIEURS CHAMPS DE DÉTECTION, SI LE PERSONNEL PEUT ENTRER DANS LA ZONE DANGEREUSE PENDANT QUE LE SYSTÈME EST EN MODE MUTING ET QU'IL NE PEUT PAS ÊTRE DÉTECTÉ PAR DES DISPOSITIFS DE PROTECTION SUPPLÉMENTAIRES QUI ENVOIENT UN ORDRE À LA MACHINE.

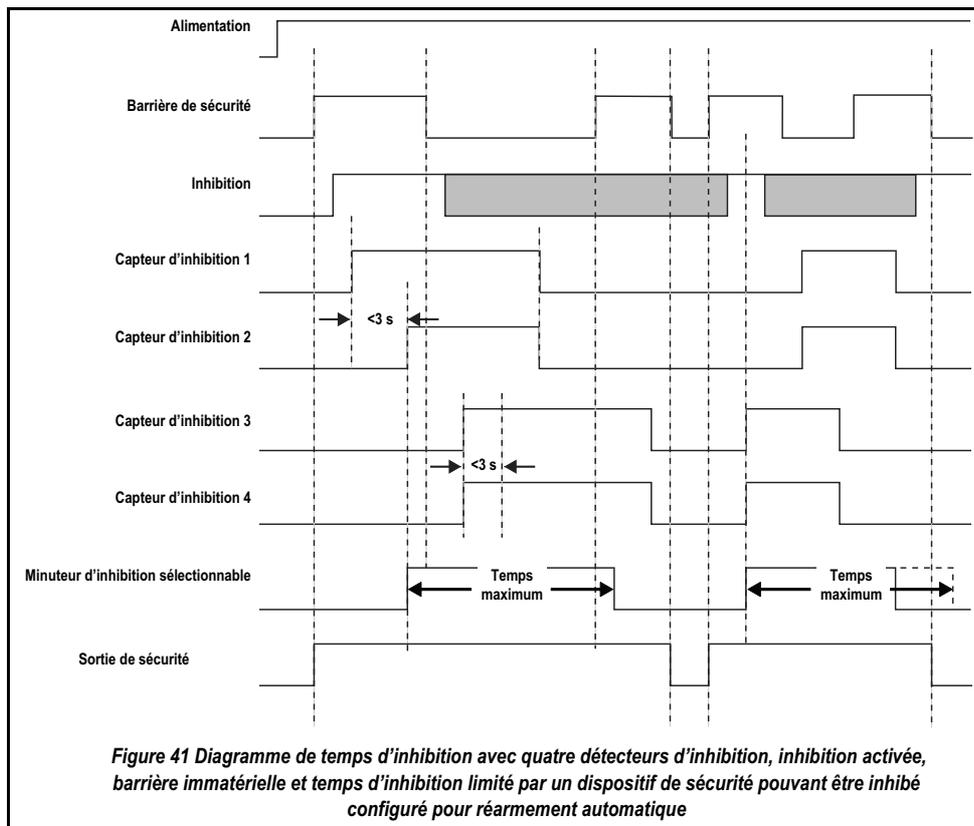
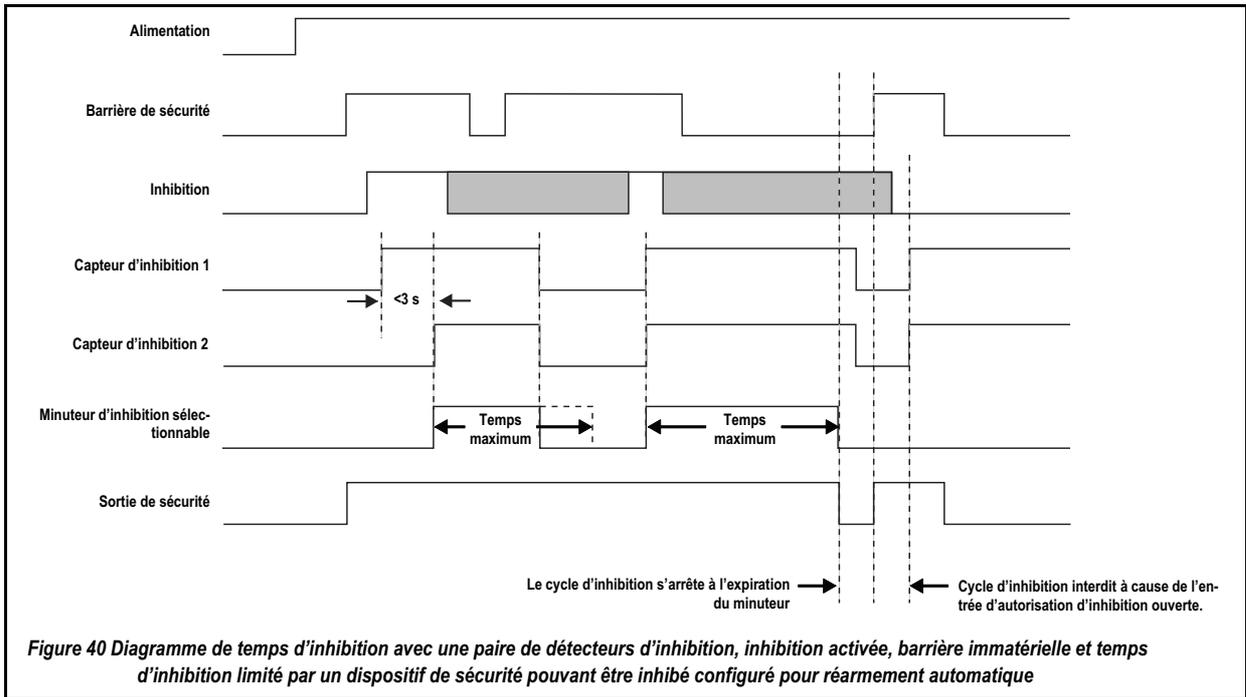
L'inhibition de plusieurs dispositifs de sécurité de détection de présence (PSSD) ou un PSSD avec plusieurs champs de détection n'est pas recommandé sauf s'il est impossible qu'un individu entre dans la zone protégée sans être détecté et sans qu'un ordre d'arrêt ne soit émis vers la commande de la machine.

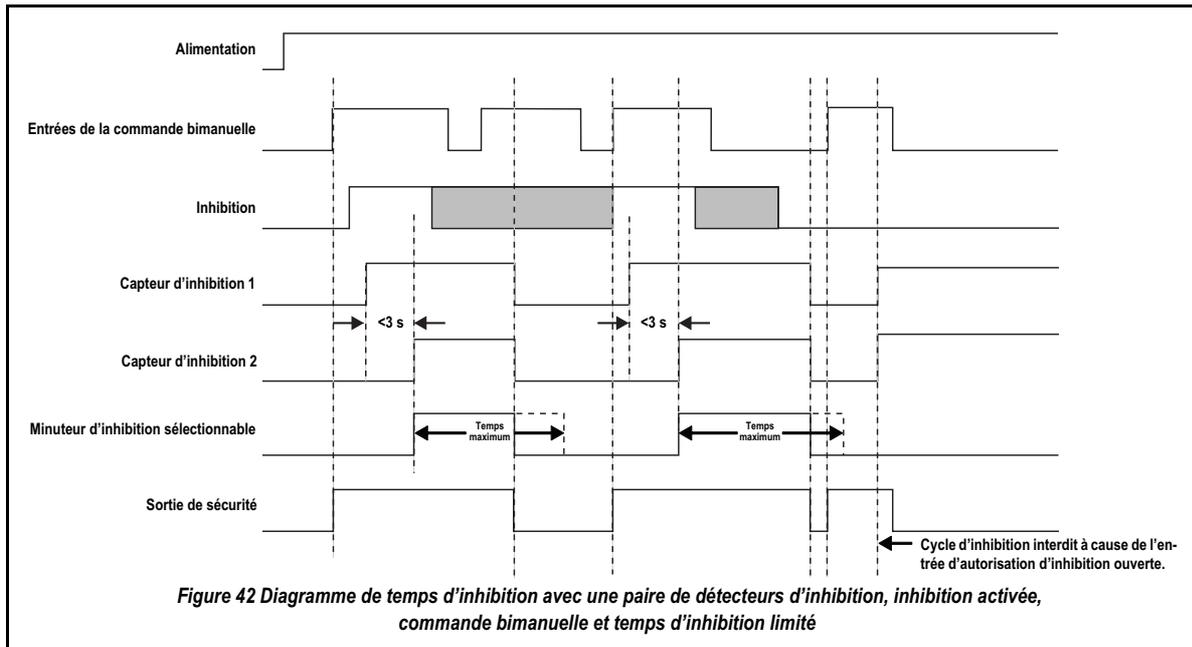
Comme dans le cas d'utilisation des miroirs d'angle (voir [Annexe A2.11.8](#)), si plusieurs champs de détection sont en muting, il est possible qu'une personne passe à travers une barrière ou un point d'accès en muting et entre dans la zone protégée sans être détectée.

Par exemple : une application utilise une palette pour déclencher le cycle d'inhibition en entrant dans le poste. Si l'entrée et la sortie PSSD sont inhibées, un individu peut entrer dans la zone protégée par la 'sortie' du poste. Une solution appropriée serait de mettre en muting l'entrée et la sortie avec des dispositifs de protection séparés.

A2.11.10 Séquences dans le temps de l'inhibition

Figure 40, Figure 41 et Figure 42 détaillent des séquences d'inhibition dans le temps.





A3 DÉCLARATION DE CONFORMITÉ

A3.1 DÉCLARATION DE CONFORMITÉ

| Declaration of Conformity | |
|--|--|
| <p>Manufacturer: Address:</p> <p>Herewith declares that:</p> <p style="padding-left: 20px;">- is in conformity with the provisions of the Machinery Directive (Directive 98/37/EC), and all Essential Health and Safety Requirements have been met.</p> <p style="padding-left: 20px;">- is in conformity with the provisions of the following other EEC Directives:</p> <p>and that:</p> <p style="padding-left: 20px;">- the following (parts/clauses of) harmonized standards, national technical standards and specifications have been used:</p> <p>EU Notified Body:</p> | <p>Banner Engineering Corp. 9714 10th Ave N. Minneapolis, MN 55441 USA</p> <p>SC22-3 (Safety Controller)</p> <p>(See attached schedule for list of models covered by this Declaration of Conformity)</p> <p>89/336/EEC, 73/23/EEC</p> <p>IEC61508-Part 1-7:2000 IEC 62061:2005 IEC 61131-2:2003 EN ISO 13849-1:2006 EN 50178:1997 EN 60204-1:2006 EN 574:1996 EN 61496-1:2004 Type 4 IEC 61508/IEC62061 (SIL CL: 3) ISO 13849-1 (Cat. 4, PL e) EN 574 (Type III C)</p> <p>TUV Rheinland Product Safety GmbH Certificate: #968/EL. 493.00/07</p> |
| <p>I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standard(s).</p> <p style="text-align: left;"> _____</p> <p style="text-align: left; font-size: small;">R. Eagle / Engineering Manager</p> <p style="text-align: right;">11 / 27 / 07</p> <p style="text-align: right; font-size: small;">Date</p> | |

| Declaration of Conformity | |
|--|---------------|
| <u>Attached Schedule</u> | |
| SAFETY CONTROLLER | |
| <p>Models covered by this Declaration of Conformity:</p> | <p>SC22-3</p> |

Figure 43 Déclaration de conformité

A4 GLOSSAIRE ET ABRÉVIATIONS

A4.1 LISTE DES ABRÉVIATIONS

| | |
|---------------|---|
| AOPD | Dispositif de protection optoélectronique actif |
| AOPDDR | Active Opto-Electronic Protective Device Responsive to Diffuse Reflection |
| COS | Changement d'état |
| EDM | Surveillance des commutateurs externes |
| EN | Norme d'ingénierie |
| ESPE | Équipement de protection électro-sensible |
| FMEA | Analyse du mode et des effets des défaillances |
| FSD | Dispositif de commutation final |
| HMI | Interface homme machine |
| IEC | Commission internationale technique électrique |
| IP... | Protection contre l'entrée (Classe) |
| ISO | Office international de normalisation |
| LCD | Affichage à cristaux liquides |
| LED | Diode électroluminescente |
| ME | Activation de l'inhibition |
| ML | Voyant d'inhibition |
| MSSI | Interfaces d'arrêt de sécurité pour inhibition |
| MPCE | Élément de contrôle primaire de la machine |
| N.O. | Normalement ouvert |
| N.F. | Normalement fermé |
| OBI | Interface embarquée |
| OSSD | Dispositif de commutation du signal de sortie |
| PCI | Interface PC |
| PL | Niveau de performances |
| PLC | Contrôleur logique programmable |
| prEN | Norme Européenne préliminaire |
| PSSD | Détection de présence |
| PSDI | Dispositif de détection de présence |
| QD | Raccord rapide |
| SIL | Niveau d'intégrité de sécurité |
| SSI | Interface d'arrêt de sécurité |
| USB | Bus de série universel |
| VAC | Tension en courant alternatif |
| VDC | Tension en courant continu |

A4.2 GLOSSAIRE

Les termes suivants sont souvent utilisés dans ce manuel. Chaque fois que cela est possible, ce manuel utilise les définitions des normes américaines et internationales de performances des produits qui s'appliquent à la conception du contrôleur de sécurité. D'autres définitions sont disponibles sur <http://www.bannerengineering.com/training>.

☛ *Quand un réarmement automatique est sélectionné, on peut dire que le dispositif d'entrée est configuré pour fonctionner en mode automatique.*

Arrêt d'urgence : Bouton poussoir spécial positionné à un endroit stratégique et utilisé pour couper l'alimentation électrique et le mouvement d'une machine en cas d'urgence.

Assigné à : Implique une relation logique de commande entre une entrée et une sortie ou entre une entrée et une autre entrée, dans laquelle l'état de la première entrée détermine l'état de la sortie ou de la seconde entrée.

Canal simple : Le fait de n'avoir qu'une ligne de signal pour une entrée de sécurité ou une sortie de sécurité.

Changement d'état : Le changement d'un signal d'entrée quand il bascule de Run à Stop ou de Stop à Run. Les signaux d'entrée canal double, ont deux paramètres configurables **COS** décrivant les limites de disparité du signal qui peuvent exister entre les canaux avant qu'une erreur soit enregistrée ; **Simultanéité** et **L'un après l'autre**.

☛ *Simultanéité par opposition à l'un après l'autre. Si la simultanéité est une condition ou une obligation pour l'application, l'utilisateur doit s'assurer que la bonne sélection a été faite pendant la configuration.*

Condition de blocage : Condition du système de barrière immatérielle automatiquement obtenue en réponse à certains signaux de défaillance (blocage interne). Lorsqu'une condition de blocage survient, les sorties de sécurité du système de barrière immatérielle **S'ÉTEIGNENT** et un réarmement manuel est requis pour replacer le système en mode RUN. Nécessite l'attention d'une **Personne qualifiée selon spécification du paragraphe 1.8.2 en page 4**.

Condition de verrouillage : Réponse des sorties de sécurité (OSSD par exemple) d'un système de barrière immatérielle lorsqu'un objet de taille égale ou supérieure au diamètre de la pièce test spécifiée entre dans la zone définie. Dans une condition de verrouillage, les sorties de sécurité désactivent et ouvrent simultanément leurs contacts. Les contacts sont maintenus (verrouillés) ouverts jusqu'à ce que l'objet soit retiré de la zone définie et qu'un réarmement manuel soit réalisé. Une sortie à réarmement manuel est utilisée le plus souvent dans le périmètre de protection des applications (voir **Réarmement automatique en page 123**).

Contacts à guidage forcé : Contacts de relais qui sont liés mécaniquement de façon à ce que tous les contacts se déplacent ensemble quand la bobine du relais est activée. Si un jeu de contacts du relais s'immobilise, les autres contacts du relais ne peuvent plus bouger. La fonction des contacts à guidage forcé est de permettre au circuit de sécurité de vérifier l'état du relais. Les contacts à guidage forcé s'appellent aussi « contacts à guidage positif », « contacts captifs », « contacts bloqués » ou « relais de sécurité ».

Défaillance face au danger : Défaillance qui retarde ou empêche le système de sécurité de la machine d'arrêter le mouvement dangereux de la machine.

Démarrage par dispositif de détection de présence (PSDI) : Application qui utilise un dispositif de détection de présence pour démarrer le cycle d'une machine. Avec ce type de dispositif, l'opérateur place une pièce à usiner dans la zone de fonctionnement de la machine. Lorsque l'opérateur s'est retiré de la zone dangereuse, le dispositif de détection de présence démarre la machine (aucun interrupteur de démarrage n'est utilisé). La machine fonctionne jusqu'à la fin de son cycle, puis s'arrête. L'opérateur peut alors placer une nouvelle pièce à usiner. Le dispositif de détection de présence contrôle la machine en permanence. Le mode « single break » est utilisé lorsque la pièce est automatiquement éjectée par la machine en fin de cycle. Le mode « double break » est utilisé lorsque la pièce est à la fois insérée et retirée par l'opérateur.

Dispositif de commutation du signal de sortie (OSSD) : La sortie de sécurité utilisée pour lancer un signal d'arrêt.

Dispositif de commutation final (FSD) : Le composant du système de commande lié à la sécurité 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.

Distance de sécurité minimale : Distance entre la zone de détection et les parties dangereuses de la machine les plus proches.

Dispositif lié à la sécurité : Un dispositif qui est conçu selon une norme de sécurité applicable et qui, bien utilisé, réduit le niveau du risque.

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.

Émetteur : Composant émetteur de lumière de la barrière immatérielle constitué d'une rangée de diodes (LED) infrarouges synchronisées. L'émetteur et le récepteur (placé en face) génèrent un « rideau lumineux » appelé zone définie.

État OFF : Le signal de la sortie de sécurité qui se produit quand au moins un de ses signaux associés de dispositifs d'entrée passe en état Stop. Dans ce manuel, la sortie de sécurité est OFF ou en état OFF quand le signal est de 0 Vcc.

État ON : Le signal de la sortie de sécurité qui se produit quand tous les signaux des dispositifs d'entrée associés passent en état Run. Dans ce manuel, la sortie de sécurité est ON ou en état ON quand le signal est de 24 Vcc.

État Run : Le signal d'entrée surveillé par le contrôleur qui, à détection, fait passer une ou plusieurs sorties de sécurité sur ON, si les autres signaux d'entrée associés sont aussi en état Run. Dans ce manuel, soit le dispositif d'entrée soit le signal du dispositif est présenté en état Run.

État Stop : Le signal d'entrée surveillé par le contrôleur qui, à détection, fait passer une ou plusieurs sorties de sécurité sur OFF. Dans ce manuel, le dispositif d'entrée ou son signal sont présentés en état Stop.

Fausse alarme : Activation des détecteurs en raison de surfaces brillantes ou réfléchissantes.

Fiabilité du contrôle : Méthode permettant d'assurer l'intégrité d'un système de contrôle. Les circuits de contrôle sont conçus pour qu'une simple défaillance ou erreur du système n'empêche pas le processus normal d'arrêt de la machine et n'entraîne pas de dysfonctionnement. Le problème devra cependant être résolu avant de pouvoir utiliser à nouveau la machine.

FMEA (Failure Mode et Effects Analysis, soit l'analyse des modes de défaillance et de leurs effets) : Analyse des modes de défaillance potentiels d'un système pour déterminer leurs effets et leurs conséquences. Les modes de défaillance sans incidence ou ceux entraînant un blocage du système sont permis. Les défaillances entraînant une condition d'insécurité sont interdites. Les produits de sécurité *Banner* sont testés selon cette méthode.

Inhibition : Suspension automatique de la fonction de protection d'un dispositif de sécurité pendant une partie non dangereuse du cycle machine.

Interrupteur à clé (réarmement manuel) : Interrupteur à clé utilisé pour réinitialiser un système de barrière immatérielle sur l'état ON suite à une condition de blocage. Se rapporte également à l'acte qui consiste à utiliser l'interrupteur pour réinitialiser un système de sécurité à partir d'une situation de verrouillage.

Interrupteur à ouverture positive : Terme utilisé pour les boutons d'arrêts d'urgence. Une force mécanique appliquée sur ce bouton est transmise directement aux contacts, les forçant à s'ouvrir sans intervention de ressorts. Cela garantit que les contacts de l'interrupteur s'ouvrent à chaque fois qu'il est utilisé même si un contact s'est soulevé en position fermée.

L'un après l'autre : Le réglage qui permet une disparité infinie de signaux entre les canaux, sans passer en situation d'erreur. Une situation d'erreur se crée si le signal Stop repasse sur Run avant que son signal allié passe en état Stop. Les deux signaux doivent changer de l'état Stop à l'état Run avant que le dispositif à double canal soit considéré en état Run.

Opérateur machine : Individu qui effectue un travail de production et qui contrôle le fonctionnement de la machine.

PELV : « Protected Extra Low Voltage », pour les circuits électriques avec la Terre alimentation (pour plus d'informations, se reporter à la norme internationale CEI 61140).

Personne désignée : Toute personne identifiée et désignée par écrit par l'employeur comme étant suffisamment compétente et expérimentée pour effectuer une procédure de vérification déterminée. Voir [Personne désignée selon spécification du paragraphe 1.8.1](#) (voir également [Personne qualifiée en page 122](#)).

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. Voir [Personne qualifiée selon spécification du paragraphe 1.8.2 en page 4](#) (voir aussi [Personne désignée en page 122](#)).

Point dangereux : Le point le plus proche que l'on peut atteindre dans la zone dangereuse.

Protection fixe ou rigide : Barrières, barres ou autres barrières mécaniques fixées à la structure de la machine prévues pour empêcher l'entrée du personnel dans les zones dangereuses d'une machine, tout en permettant la visualisation de la zone de fonctionnement. La taille maximum des ouvertures est déterminée par la norme applicable.

Protection supplémentaire : Protection supplémentaire ou fixe utilisée pour empêcher une personne de passer sur, sous, à travers ou autour de la protection primaire ou toute autre protection permettant d'accéder à la zone protégée.

Réarmement automatique : L'opération de commande du dispositif d'entrée de sécurité dans laquelle la sortie de sécurité assignée passera automatiquement sur ON quand tous les dispositifs d'entrée associés sont en état Run. Il n'est pas nécessaire d'effectuer un réarmement manuel pour qu'une sortie de sécurité passe sur ON quand elle n'est contrôlée que par des dispositifs d'entrée de sécurité configurés pour un réarmement automatique.

Réarmement du système : Le terme utilisé pour décrire une opération de réarmement manuel nécessaire pour qu'une ou plusieurs sorties de sécurité passent sur ON à la mise sous tension du contrôleur, s'il est configuré sur mise sous tension manuelle et dans les situations de blocage (détection d'erreur).

Réarmement manuel : L'opération de commande du dispositif d'entrée de sécurité assignée dans laquelle la sortie de sécurité assignée ne repassera sur ON qu'après un réarmement manuel et si les autres dispositifs d'entrée associés sont en état Run.

Réarmement (reset) : Utilisation d'un interrupteur manuel pour restaurer les sorties de sécurité à l'état ON suite à une situation de blocage ou de verrouillage.

Récepteur : Composant récepteur de lumière d'un système de barrière immatérielle, constitué d'une rangée de phototransistors synchronisés. Le récepteur et l'émetteur (placé en face) génèrent un « rideau lumineux » appelé zone définie.

SELV : « Safety Extra Low Voltage », pour les circuits électriques sans terre alimentation (pour plus d'informations, se reporter à la norme internationale CEI 61140).

Simultanéité : Le paramètre qui permet une disparité du signal entre les canaux à l'intérieur du dispositif d'entrée pendant un temps limité, sans passer en situation d'erreur. Si une disparité de signal existe pendant plus de 3 secondes, une situation d'erreur se produit.

Situation de blocage : Réponse des sorties de sécurité (OSSD par exemple) d'un système de barrière immatérielle lorsqu'un objet de diamètre supérieur ou égal au diamètre de la pièce de test spécifiée pénètre dans la zone définie. Dans une situation de blocage, les OSSD se désactivent simultanément. Une situation de blocage disparaît (se réarme) automatiquement lorsque l'objet est retiré de la zone définie. (Voir aussi [Réarmement manuel en page 121](#)).

Surveillance des commutateurs externes (EDM) : Moyen par lequel un dispositif de sécurité (une barrière immatérielle par exemple) surveille activement l'état (ou le statut) des dispositifs externes qui peuvent être surveillés par le dispositif de sécurité. Le dispositif se bloque si une situation dangereuse est détectée sur le dispositif externe. Le(s) dispositif(s) externe(s) peu(ven)t inclure mais sans limitation les éléments suivants : MPCE, contacteurs/relais liés mécaniquement et modules de sécurité.

Temps d'anti-rebond de fermé à ouvert : Le temps nécessaire pour laisser passer un signal d'entrée hésitant ou le rebond de contacts d'entrée pour éviter un déclenchement intempestif du contrôleur. Réglable entre 6 et 100 ms. Les détecteurs d'inhibition sont réglés par défaut à 50 ms et les autres dispositifs à 6 ms.

Un temps d'anti-rebond de fermé à ouvert augmente aussi le temps de réponse du système et le [Temps de réponse machine \(voir page 123\)](#)

Temps d'anti-rebond d'ouvert à fermé : Le temps nécessaire pour laisser passer un signal d'entrée hésitant ou le rebond de contacts d'entrée pour éviter un démarrage non souhaité de la machine. Réglable entre 10 et 500ms. La valeur par défaut est de 50ms.

Un temps d'anti-rebond d'ouvert à fermé affectera aussi le temps de réaction du contrôleur.

Temps de réponse de la machine : Temps qui s'écoule entre l'activation du dispositif d'arrêt d'une machine et l'instant où les parties dangereuses de la machine atteignent un état de sécurité en s'arrêtant.

☛ *Quand un réarmement manuel est sélectionné, on peut dire que le dispositif d'entrée est configuré pour fonctionner en mode manuel ; ce qui veut dire que la sortie contrôlée est bloquée en état OFF et nécessite un réarmement manuel pour revenir sur ON. Ce réarmement s'appelle parfois un réarmement de verrouillage manuel.*

Temps de réponse : Temps qui s'écoule entre l'activation du dispositif de sécurité et l'arrêt de la machine ou l'élimination de tout danger.

Test de démarrage : Pour certains dispositifs de sécurité comme les barrières immatérielles ou les interrupteurs de porte, il peut être intéressant de tester au moins une fois le dispositif à la mise sous tension pour vérifier son fonctionnement. Si le 'test de démarrage' a été sélectionné pour une barrière immatérielle et qu'il est concluant à la mise sous tension, il est nécessaire de cycler la barrière immatérielle une fois (de ON à OFF puis de nouveau sur ON), même si le contrôleur a été configuré pour une mise en service automatique.

TUV (Technischer Überwachungsverein) : Organisation de test et de certification indépendante fournissant des tests de sécurité des produits, la certification et les enregistrements des systèmes de gestion de la qualité EMC (compatibilité électromagnétique).

Validation de code : Le processus d'inspection du fichier de code de la configuration effectué automatiquement par le contrôleur pour vérifier que le code de configuration n'est pas corrompu ou altéré de quelque façon que ce soit.

Zone dangereuse : Zone qui présente un risque physique immédiat ou potentiel.

Zone de détection : Rideau optique généré par le système. Lorsqu'un objet opaque de diamètre ou de taille définie pénètre dans la zone de détection, il se produit un verrouillage du système en réarmement automatique ou manuel, selon le contrôleur.

Zone de fonctionnement : Zone de la machine surveillée où une pièce ou un produit est positionné pour être usiné.

Page blanche

A5 INFORMATION COMMERCIALES

La liste qui suit représente les adresses des représentants et distributeurs *Banner* en Europe :



CORPORATE OFFICES:

Banner Engineering Europe

Park Lane, Culliganlaan 2F
1831 Diegem,
Belgium

Tel.: +32 2 456 07 80

Fax: +32 2 456 07 89

e-mail : mail@bannereurope.com

<http://www.bannereurope.com>

Banner Engineering GmbH

Martin-Schmeißer-Weg 11
44227 Dortmund

Tel.: + 49 (0) 231 963 37 30

Fax: + 49 (0) 231 963 39 38

e-mail: info@bannerengineering.de

<http://www.bannerengineering.de>



AUSTRIA

Intermax GmbH

Josef-Moser-Gasse 1
A-1170 Vienna

Tel.: +431 48 615870

Fax: +431 48 6158723

e-mail: imax.office@intermax.at

<http://www.intermax.at>



BELGIUM

MULTIPROX N.V.

Lion d'Orweg, 12
B-9300 Aalst

Tel.: +32 53 766 566

Fax: +32 53 783 977

e-mail: mail@multiprox.be

<http://www.multiprox.be>



BULGARIA

Sensomat Ltd.

VH V, App 11
Dr. Ivan Penakov Str. 15
BG-9300 Dobrich

Tel.: +359 58 603 023

Fax: +359 58 603 033

e-mail: info@sensomat.info

<http://www.sensomat.info>



CZECH REPUBLIC

Turck s.r.o.

Hradecká 1151
CZ-50003 Hradec Králové 3

Tel.: +420 495 518 766

Fax: +420 495 518 767

e-mail: turck@turck.cz

<http://www.turck.cz>



DENMARK

Hans Folsgaard AS

Ejby Industrivej 30
Dk-2600 Glostrup

Tel.: +45 43 20 86 00

Fax: +45 43 96 88 55

e-mail: hf@hf.net

<http://www.hf.net>



ESTONIA

Osaühing «System Test»

Pirita tee 20
EE-10127 Tallinn

Estonia

Tel.: +372 6 405 423

Fax: +372 6 405 422

e-mail: systemtest@systemtest.ee



FINLAND

Sarlin Oy Ab

P.O. Box 750
SF-00101 Helsinki 10

Tel.: +358 9 50 44 41

Fax: +358 9 56 33 227

e-mail: sales.automation@sarlin.com

<http://www.sarlin.com>



FRANCE

Turck Banner S.A.S.

3, Rue de Courtalin
Magny - Le - Hongre
77703 Marne - La - Vallée Cedex 4

Tel.: +33 1 60 43 60 70

Fax: +33 1 60 43 10 18

e-mail: info@turckBanner.fr

<http://www.turckBanner.fr>



GERMANY

Hans Turck GmbH & Co KG

Witzlebenstrasse 7
45472 Mülheim an der Ruhr

Tel.: +49 208 49 520

Fax: +49 208 49 52 264

e-mail: turckmh@mail.turck-globe.de

<http://www.turck.com>



GREECE

2KAPPA LTD

Sofokli Venizelou 13, 54628 Menemeni

Tél. : 00 30 23 10 77 55 10

Fax : 00 30 23 10 77 55 14-15

e-mail: 2kappa@pel.forthnet.gr



HUNGARY

Turck Hungary Kft.

Könyves Kalman Krt. 76
H-1087 Budapest

Tel.: +36 1 477-0740 or 36-1-313-8221

Fax: +36 1 477-0741

e-mail: turck@turck.hu

<http://www.turck.hu>



ICELAND

K M Stáhl ehf.

Bíldshöfða 16
110 Reykjavík

Tel.: +354 56 78 939

Fax: +354 56 78-938

e-mail: kalli@krmstal.is



IRELAND

Tektron

Tramore House
Tramore Road
Cork

Tel.: +353 (0)21-431 33 31

Fax: +353 (0)21-431 33 71

e-mail: sales@tektron.ie

<http://www.tektron.ie>



ITALY

Turck Banner s.r.l.

Via Adamello, 9
20010 Bareggio
Milano

Tél. : +390 2 90 36 42 91

Fax: +390 2 90 36 48 38

e-mail: info@turckBanner.it

<http://www.turckBanner.it>



LATVIA

LASMA Ltd.

Aizkraukles 21-111
LV-1006 Riga

Tel.: +371 754 5217

Fax: +371 754 5217

e-mail: inga@lasma.lv

**LITHUANIA****Hidroteka**

Büro: Taikos 76-4
 LT-3031 Kaunas
 Post: P.O. Box 572
 LT-3028 Kaunas
 Tel.: +370 37 352195
 Fax: +370 37 351952
 e-mail: hidroteka@post.sonexco.com

**LUXEMBOURG****Sogel SA 1**

7, Rue de l'Industrie
 8399 Windhof
 Luxembourg
 Tel.: +352 40 05 05 331
 Fax: +352 40 05 05 305
 e-mail: sogel@sogel.lu

**NETHERLANDS/HOLLAND****Turck B.V.**

Ruiterlaan 7
 NL-8019 BN Zwolle
 Tel.: +31 38 42 27 750
 Fax: +31 38 42 27 451
 e-mail: info@turck.nl
<http://www.turck.nl>

**NORWAY****Danyko A.S.**

P.O. Box 48
 N-4891 Grimstad
 Tel.: +47 37 04 02 88
 Fax: +47 37 04 14 26
 e-mail: danyko@hf.net
<http://www.danyko.no>

**POLAND****Turck Sp. z o.o.**

ul Zeromskiego 1
 PL-50 053 Opole
 Tel.: +48-77 443 48 00
 Fax: +48-77 443 48 01
 e-mail: turck@turck.pl
<http://www.turck.pl>

**PORTUGAL****Salmon & Cia Lda.**

Rua Cova da Moura, 2-6º
 1399-033 Lisboa
 Tel.: +351 21 39 20 130
 Fax: +351 21 39 20 189
 e-mail: div8.salmon@mail.telepac.pt

**ROMANIA****TURCK Automation Romania SRL**

Str. Iuliu Tetrat nr. 18, Sector 1
 RO-011914 Bucharest
 Tél. : +40 21 230 02 79 ou 230 05 94
 Fax: +40 21 231 40 87
 e-mail: info@turck.ro
<http://www.turck.ro>

**RUSSIA ET CIS****Turck Office Minsk**

ul. Engelsa, 30
 BY-220030 Minsk
 Republic of Belarus
 Tel.: +375 172 105957
 Fax: +375 172 275313
 e-mail: turck@infonet.by
<http://www.turck.by>

Turck Office Moskwo

Volokolamskoe shosse 1 office 606A
 125080 Moskwo
 Tel.: +7 095 105 00 54
 Fax: +7 095 158 95 72
 e-mail: turck@turck.ru

**SLOVAK REPUBLIC****MARPEX s.r.o.**

Sportovcov 672
 018 41 Dubnica nad Váhom
 Tel.: +421 42 4426987
 Fax: +421 42 4426986
 e-mail: marpex@marpex.sk

**SLOVENIA****Tipteh d.o.o**

CESTA V GORICE 40
 SLO-1111 Ljubljana
 Tel.: +386 1 200 51 50
 Fax: +386 1 200 51 51
 e-mail: info@tipteh.si

**SPAIN****Elion, S.A.**

Farell, 5 - 08014 Barcelona
 Tél. : + 932 982 035
 Fax : + 934 314 133
 e-mail : elion@elion.es
<http://www.elion.es>

**SWEDEN****Thomas Winemar**

Technical Consulting Manager

Hans Turck GmbH & Co. KG

EA Rosengrensgata 32
 421 31 Västra Frölunda
 Tel.: +46 31 471605
 Fax: +46 31 471630
 Mobile: +46 707 471656
 e-mail: thomas.winemar@turck.com
 Web: www.turck.se

**SWITZERLAND****Bachofen AG**

Ackerstrasse 42
 8610 Uster
 Tél. : + 41 44 944 11 11
 Fax : + 41 44 944 12 33
 e-mail: info@bachofen.ch
<http://www.bachofen.ch>

**TURKEY****Dacel Muhendislik Elektrik,**

Elektronik, San. Ve Tic. Ltd.
 Perpa Elektrokent Is Merkezi
 A Blok Kat 2 No:38
 Okmedani/Istanbul
 TURKIYE
 Tel: 00 90 212 210 76 46
 Fax:00 90 212 220 50 45
 e-mail: Özer Özkurt <ozkurt@dacel.net

Gökhan Elektrik Malzemeleri San Tic Ltd. Sti

Perpa Elektrokent Ticaret Merkezi A Blok Kat 8
 No: 694
 80270 Okmeydani - ISTANBUL
 Tel.: +90 212 2213236
 Fax: +90 212 2213240
 e-mail: gokhan@gokhanelektrik.com
<http://www.gokhanelektrik.com>

**UNITED KINGDOM****Turck Banner Limited**

Blenheim House, Hurricane Way,
 Wickford,
 Essex, SS11 8YT
 Tel: +44 (0)1268 578888
 Fax: +44 (0)1268 763648
 e-mail: info@turckBanner.co.uk
<http://www.turckBanner.co.uk>

Cliquez sur une ligne de texte pour information

L'installation de supresseurs de parasites entre les bobines de MPCE1, MPCE2 et MPCE3 est recommandée (voir AVERTISSEMENT, page 12) 86
 L'installation de supresseurs de parasites entre les bobines de MPCE1, MPCE2 et MPCE3 est recommandée (voir AVERTISSEMENT, page 12) 86
 L'installation de supresseurs de parasites entre les bobines de MPCE1, MPCE2 et MPCE3 est recommandée (voir AVERTISSEMENT, page 12) 87
 Pour les détails, contacter votre Bureaux du siège social en page 125. 25
 "+" indique une borne qui fournir +24 Vcc au dispositif d'entrée de sécurité 27
 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes 100
 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes 110
 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes 112
 2 complémentaires, 4 bornes - 2 complémentaires, 5 bornes 95
 2 complémentaires, contact PNP 100
 2 complémentaires, contact PNP 110
 2 complémentaires, contact PNP 112
 2 complémentaires, contact PNP 95
 2 complémentaires
 24 V = Entrée active 62
 24 V = Entrée inactive 22

A

Accéder aux codes d'erreur 31
 Accès au registre d'erreurs 51
 Activation d'une commande bimanuelle à la mise sous tension 8
 Activation du muting (ME) – ME01 61
 Activer dispositif 9
 Affichage des informations du contrôleur — OBI 68
 Affichage des informations du contrôleur — PCI 67
 Affichage embarqué sur LCD des informations — Utilisation du mot de passe 22
 Affichage live 52
 Ajout d'un capteur optique 43
 Ajout d'un interrupteur d'inhibition 46
 Ajout d'un interrupteur pour porte 43
 Ajout d'une commande bimanuelle 44
 Ajout d'une paire de capteurs d'inhibition 44
 Ajout d'une surveillance de dispositif externe 45
 Ajout de dispositifs d'entrée de sécurité et d'entrée auxiliaire 40
 Ajout de dispositifs d'Entrée de sécurité supplémentaire 58
 Ajout de dispositifs d'entrées auxiliaires supplémentaires 61
 Ajouter des dispositifs d'entrée auxiliaire 46
 Ajouter entrée 57
 Ajouter un arrêt d'urgence 41
 Ajouter un interrupteur ON/OFF 46
 Ajouter une entrée 19, 53, 62
 Ajouter une entrée
 (Ajouter entrées page 57) 56
 Ajouter une sortie d'état supplémentaire 47
 Alimentation 21, 32, 117, 118
 Anti -rebond 28
 AOPD Dispositif de protection optoélectronique actif 121
 AOPDDR Active Opto-Electronic Protective Device Responsive to Diffuse Reflection 121
 Application des tapis de sécurité 101
 Applications 7
 Arrêt d'urgence (ES01) Décomposition d'un exemple de menu 57
 Arrêt d'urgence 19, 28, 53, 62, 90
 Arrêt de protection 28, 53, 62, 90
 Arrêts d'urgence 104
 Arrêts d'urgence multiples 105
 Arrêts de protection (sécurité) 91
 Arrêts de protection 19
 Arrêts fonctionnels selon IEC 60204-1 13
 Assignment de entrée/sortie 19, 53, 56, 62
 Assignment de l'entrée et de la sortie 16
 Assignment des bornes 19, 53, 56, 62
 Assignment des E/S et relation de commande des E/S 16
 Assignment des sorties de sécurité 47
 Assigné à : 28, 30
 Assignement des terminaux 54
 Attente de réarmement 62

auto vérification à pincés 22
 Autocollant d'indentification du contrôleur de sécurité SC22-3 2
 Autocollants de sécurité 1
 Autres fonctions de dispositifs d'arrêt 74
 Autres fonctions logiques 17
 Avant de mettre la machine sous tension 71
 Avertissement 1
 Avertissement général 1
 Avertissements 1

B

Barrière de sécurité 117
 Barrière immatérielle – OS01 60
 Bornes d'entrée 28
 Bornier à vis 22
 Bornier débouchable 22
 Bornier des sorties de sécurité 71
 Bornier fourni 86
 Bypass avec inhibition. 11

C

C'est de la responsabilité de celui personne qualifiée qui configure, installe ou entretien le contrôleur de sécurité sc22-3 de : 1
 Câblage 12
 Canal double 85
 Canal double, 2 bornes – Canal double, 3 bornes – Canal double, 4 bornes 99
 Canal simple 85
 Canal simple, 1 borne – canal simple, 2 borne – canal simple, contact PNP 91, 94, 97, 105, 107
 Capteur d'inhibition – M1 + M2 60
 Capteur d'inhibition (paire) 113
 Capteur d'inhibition 1 (2) 10
 Capteur d'inhibition 1 117
 Capteur d'inhibition 1 118
 Capteur d'inhibition 19
 Capteur d'inhibition 2 (1) 10
 Capteur d'inhibition 2 117
 Capteur d'inhibition 2 118
 Capteur d'inhibition 28
 Capteur d'inhibition 3 117
 Capteur d'inhibition 4 117
 Capteur d'inhibition 53, 62, 90
 Capteur optique 19
 Capteurs optiques (barrière immatérielle) 96
 Capture du registre d'erreurs — PCI 80
 Capture programmée du registre d'erreurs 52
 Caractéristiques 7
 Carte SC-XM1 mémoire externe XM 26
 Carte XM Message 69
 Catégorie 2 93, 105
 Catégorie 3 93, 105
 Catégorie 4 93, 105
 Catégories de sécurité 89
 Cause 69
 Cause et, ou, action requise 68
 Certificat de conformité 21
 Ces menus déroulants servent à changer l'assignation des bornes d'entrée 27
 Cette illustration est générique et représente toutes les trois options EDM : 85
 Changement d'état du signal (simultanéité) 29
 Changement du mot de passe en utilisant le PCI 50
 Changer le mot de passe 19, 53, 66
 Changer le nom... 62
 Choisir la langue 19, 53
 Choix à la mise sous tension 63
 Choix (dépend de l'entrée) 62
 Circuit catégorie 2 - Interrupteur de porte 87
 Circuit catégorie 3 - Interrupteur de porte 87
 Circuit catégorie 4 Circuit - Interrupteur de porte 88
 Circuit d'arrêt d'urgence 85
 Circuit d'arrêt d'urgence de catégorie 2 88
 Circuit d'arrêt d'urgence de catégorie 3 88
 Circuit d'arrêt d'urgence de catégorie 4 88

Circuits d'arrêt de sécurité (de protection) 34
 Cliquer sur ce bouton pour générer un enregistrement complet des erreurs et le sauvegarder dans un fichier 80
 Code d'erreur 77
 Code de l'erreur 81
 Commande à double voie 34
 Commande à simple voie 34
 Commande bimanuelle – THC01 59
 Commande bimanuelle 8, 19, 28, 53, 62, 90, 98
 Commande de la machine 86
 Commande de la machine 87
 Commandes manuelles 98
 Complémentaire, 2 bornes – Complémentaire, 3 bornes 91, 94, 97, 108, 110, 112, 114
 Complémentaire, contact PNP 91, 95, 97, 108, 110, 112, 115
 Composants 25
 Composants du kit du Contrôleur de sécurité SC22-3 25
 Conception et construction d'un système de tapis de sécurité 101
CONCEPTION ET TESTS 6
 Condition 32
 Conditions 91, 92, 101, 104, 111
 Conditions d'utilisation de l'équipement 3
 Configuration des options de mise sous tension 73
 Configuration du contrôleur de sécurité 12, 31
 Configuration du réarmement 73
 Configurer les sorties d'état 47
 Confirmation d'une configuration 18
 Confirmation de la configuration 12, 33, 48
 Confirmer la configuration 19, 53, 64
 Confirmer la configuration des entrées 64
 Confirmer la configuration des paramètres du système 65
 Confirmer la configuration des sorties 65
 Confirmer les entrées 19, 53
 Confirmer les paramètres système 19, 53
 Confirmer les sorties de sécurité 19, 53
 Confirmer une configuration : 17
 Connexion des contrôleurs de sécurité en série 12
 Connexion du contrôleur de sécurité aux modules d'interface 35
 Connexion du PC au port USB du contrôleur de sécurité 26
 Connexion EDM à Canal simple 85
 Connexion EDM canal simple au module d'interface SC-IM9A 86
 Connexion générique 97
 Connexion générique illustrant les options canal simple, canal double et pas de EDM 85
 Connexions en série et considérations sur l'intégrité du circuit de sécurité 93
 Connexions USB 26
 Consignations 111
 Construction de la configuration 12, 33
 Contacteurs de sécurité à ouverture positive 114
 Contacts EDM 83
 Contacts reliés mécaniquement 84
 Contrôleur de sécurité configurable SC22-3 21
 Contrôleur de sécurité SC22-3 23, 87
 Contrôleur de sécurité SC22-3 Raccordement à SC-XM1 carte de mémoire externe (carte XM) 26
 Contrôleur de sécurité SC22-3 Spécifications générales 21
 Convention des signaux... 63
 Convention du signal 15, 62
 Convention pour les signaux 35
 Conventions pour les signaux d'état des sorties 35
 COS Changement d'état 121
 COS* (Simultanéité): Simultanément (S) / L'un après l'autre (C) 28
 Court-circuits d'entrée de catégorie 2 ou de catégorie 3 89
 Création d'une nouvelle configuration 40
 Cycle d'inhibition interdit à cause de l'entrée d'autorisation d'inhibition ouverte. 117
 Cycle d'inhibition interdit à cause de l'entrée d'autorisation d'inhibition ouverte. 118

D

De 10 ms à 500 ms par intervalles de 1 ms 30
 De 6 ms à 100 ms par intervalles de 1 ms 30
 Déclaration de conformité - Traduction 120
 Déclaration de conformité (DOC) 22
 Déclaration de conformité 21, 119, 120
 Décomposition des dispositifs supplémentaires d'entrée de sécurité 59
 Décomposition des paramètres 16
 Défaillance : 68
 Définition 1
 Définition de l'application de protection (évaluation des risques) 12
 Définition de l'application de protection 33
 Démarrage du programme PCI 37
 Désactivé 68
 Description 1, 23, 82, 83, 84
 Description de l'erreur 81
 Désignation 28
 Détail de l'indicateur d'état de l'interface embarqué 32
 Détail des propriétés des entrées de sécurité 27
 Détecteur
 optique 28
 Détecteur optique 53, 62, 90
 Détecteurs de proximité à induction 114
 Détecteurs optoélectroniques (mode rétro-réfléctif polarisé) 114
 Détecteurs photoélectriques (mode barrière) 114
 Détermination de la distance de sécurité (S) pour le tapis de sécurité 103
 Diagnostic d'erreur par le PCI 79
 Diagnostic d'erreurs 19, 53
 Diagnostic d'erreurs par OBI 80
 Diagrammes et résumés 38
 Dimensions du contrôleur de sécurité SC22-3 24
 Dimensions du contrôleur de sécurité SC22-3 24
 Dispositif d'activation (simultané) 109
 Dispositif d'entrée de sécurité du Contrôleur de sécurité et présentation de la surveillance du type de circuit 28
 Dispositif d'entrée et catégorie de sécurité REFERENCE 89
 Dispositif de commande 9, 19, 28, 53, 62, 90
 Dispositif de commande bimanuelle 8
 Dispositif de commande et logique de temps du mode actif 9
 Dispositifs d'entrée auxiliaire 30
 Dispositifs d'entrée avec raccordements des sorties transistorisées 89
 dispositifs d'entrée, options des circuits et leurs catégories de sécurité possibles 90
 Dispositifs de commande bimanuelle – Aspects fonctionnels – Principes de conception 2
 Dispositifs de réarmement manuel 30
 Dispositifs de sécurité de détection de présence multiples 116
 Dispositifs des Entrées de sécurité & Entrées auxiliaires configurables 40
 Distance de sécurité 96, 99, 103
 Distance de sécurité des détecteurs optiques 6
 Distance de sécurité pour des commandes bimanuelles 6
 Distances de sécurité 6
 Distances de sécurité pour des tapis de sécurité 6
 Documentation 84
 Donner un nom à la configuration 56
 Double canal, 2 bornes – Double canal, 3 bornes 91, 94, 97, 105, 107, 109, 111, 114
 Double canal, 4 bornes 91, 94, 106, 107, 109, 112, 114
 Double canal, PNP 91, 94, 97, 100, 106, 107, 109, 112, 114,
 Double voie A & B complémentaire 29
 Double voie A et B 29

E

Écran 59, 61
 Écran de diagnostic d'erreurs 53
 EDM 11, 19, 34, 53, 62
 EDM à canal simple utilisé pour surveiller les signaux de retour de MPCE. Si un canal ou les deux ne se ferme pas, le système passe en situation de blocage. 85
 EDM Surveillance des commutateurs externes 121
 Efface les erreurs affichées et fait passer les dernières erreurs enregistrées dans le registre d'erreurs du contrôleur de sécurité. 80
 Effacer L'entrée 53, 62
 Effacer la configuration 19, 53, 64
 Effacer le registre d'erreurs 81
 Effacer registre d'erreurs 19, 81
 Effacer registre d'erreurs 53
 Effacer une entrée 19, 56
 EMC 22
 Emplacement de l'interrupteur de réarmement 5
 Emplacement des boutons de commande à contact 99
 Emplacement du bouton du système 70
 Emplacement/signification 2
 EN Norme d'ingénierie 121
 Enregistrer la configuration 55
 Entrée auxiliaire 1 16
 Entrée auxiliaire 19, 53, 62
 Entrée dans le mode de configuration 55
 Entrée de sécurité 1 (Auto) 7
 Entrée de sécurité 1 8, 16
 Entrée de sécurité 1 réarmement manuel surveillé) 8
 Entrée de sécurité 14, 19
 Entrée de sécurité 2 (manuel) 7, 8
 Entrée de sécurité 2 8, 16
 Entrée de sécurité 2 réarmement manuel surveillé 8
 Entrée de sécurité 3 16
 Entrée de sécurité 4 16
 Entrée de sécurité 9, 53, 62
 Entrée de sécurité et entrée auxiliaire (22 bornes) 21
 Entrée Run Entrée Stop 35
 Entrée surveillée manuellement réarmement manuel 7
 Entrées 19, 53, 56, 62, 83, 84
 Entrées assignées à des entrées 16
 Entrées auxiliaires 58
 Entrées de la commande bimanuelle 118
 Entrées de réarmement manuel et automatique assignées à une même sortie de sécurité 7
 Entrées de sécurité 4, 57
 Entrées de sécurité avec réarmement manuel commun assigné à la même sortie de sécurité 8
 Entrées de sécurité et entrées auxiliaires 8
 Entrées de sécurité et entrées auxiliaires assignées aux sorties 16
 Entrées (Entrées page 56) 56
 Entrer le mot de passe (Paragraphe 6.2.1) 19
 Entrer le mot de passe du contrôleur 55
 Entrer le mot de passe (Paragraphe 6.2.1) 53
 Entrer le nom 62
 Entretien 71
 Environnement 22
 Envoi d'une configuration à la carte XM 50
 Envoi d'une configuration au contrôleur de sécurité SC22-3 50
 Envoi d'une configuration confirmée au contrôleur de sécurité : 17
 Envoyer un fichier à la XM 19, 63
 Envoyer un fichier À la XM 53
 Erreurs et défaillances 4
 Espace sur le disque dur 36
 ESPE Équipement de protection électro-sensible 121
 Étape de confirmation finale 65
 Étapes et vérifications suivantes 77
 État (Mode du contrôleur de sécurité) 32
 État de l'entrée 68
 État de la sortie de sécurité 68
 État des sorties assignées 35
 État du système 69

État EDM canal double par rapport à la sortie de sécurité 11
 État inhibé 62
 État OBI de la carte XM 69
 États des signaux de fonctionnement et d'arrêt 4
 Évaluation des risques 33
 Éviter les installations dangereuses 114
 Évolution dans le temps de EDM canal double entre les canaux 11
 Évolution dans le temps de l'état EDM à canal simple par rapport à la sortie de sécurité 11
 Exclusion des défauts 89
 Exemple 1
 Exemple 1 – Défaillance cachée 93
 Exemple 2 – Non-détection d'une défaillance 93
 Exemples de détecteurs et de contacteurs d'inhibition (muting) 114
 Exemples de symboles de circuits 90
 Exigences 113
 Exigences 96, 113
 Explications des indications de diagnostic 77
 Explications sur la connexion des dispositifs de sécurité 27
 Exportation de documents 51

F

Fiche technique 21
 Fichier de configuration 19
 Fichier de configuration 53
 Fichier de configuration 56
 FMEA Analyse du mode et des effets des défaillances 121
 Fonction 59, 61
 Fonction d'inhibition 113
 Fonction d'inhibition à la mise sous tension 10
 Fonction d'interrupteur de bypass (avec inhibition) 75
 Fonction d'interrupteur de bypass (sans inhibition) 75
 Fonction de dispositif de commande 75
 Fonction de réarmement du contrôleur de simultanéité 115
 Fonction du bouton de Bypass 10
 Fonction surveillée 35
 Fonctionnement du contrôleur à la mise sous tension 16
 Fonctions d'arrêt d'urgence 104
 Fonctions d'arrêt d'urgence et interrupteur à câble 74
 Fonctions d'inhibition (Muting) 9
 Fonctions d'inhibition 74
 Fonctions d'une commande bimanuelle 73
 Fonctions de mise sous tension et de réarmement 73
 Formule générale 96, 99, 103
 FSDDispositif de commutation final 121

G

Généralités 28, 113
 Glossaire 121
 Glossaire et abréviations 121

H

Haute tension 1
 HMIInterface homme machine 121

I

IEC 60204-1 (2005-10) 2
 IEC 60529 (2001-02) 2
 IEC 60947-1 (2004-03) 2
 IEC 60947-5-1 (2003-11) 2
 IEC 60947-5-5 2
 IEC 61496-1 (2004-02), & IEC 61496-2 (2006-04) 2
 IEC Commission internationale technique électrique 121
 Important... Lire ce paragraphe avant de continuer ! 5
 Impression 51
 Indicateur d'état 32
 Indice de protection 22
 Indique l'état du contrôleur de sécurité 72
 Information commerciales 125
 Information de déni de responsabilité 5
 Information incomplète 96
 Informations concernant les étiquettes de sécurité sur les produits 2

Informations des clients 24
 Informations générales 21
 Informations supplémentaires sur le réarmement 7
 Informations sur le kit et les accessoires du contrôleur de sécurité SC22-3 82
 Inhibition (ME), 115
 Inhibition 5, 9, 19, 30, 117, 118
 Inhibition à la mise sous tension 10, 17, 63, 116
 Inhibition activée 9, 53, 62
 Inhibition la mise sous tension 116
 Installation - système 25
 Installation 102
 Installation du fil commun en courant continu 35
 Installation du fil courant continu commun 87
 Installation du logiciel 36
 Installation du logiciel PCI 36, 37
 Installer les commandes manuelles pour éviter une utilisation accidentelle 98
 Instructions d'installation 107, 109
 Instructions de fonctionnement — généralités 67
 Instructions de fonctionnement - OBI 53
 Instructions de fonctionnement - PCI 37
 Intégrité du circuit de sécurité et ISO 13849-1 (EN954-1) Principes de circuit de sécurité 89
 Interfaçage du Contrôleur de sécurité SC22-3 25
 Interface des deux OSSD 12
 Interface du contrôleur de sécurité SC22-3 3
 Interface embarqué avec boutons, écran d'affichage à LCD et indicateurs d'état 31
 Interface OSSD 12
 Interface PC 33
 Interrupteur à câble 19, 28, 53, 62, 90, 107
 Interrupteur d'inhibition 30
 Interrupteur d'inhibition et de bypass 10
 Interrupteur de bypass (Bypassant les protections) 111
 Interrupteur de bypass 10, 19, 28, 30, 53, 62, 90
 Interrupteur de porte – GS01 59
 Interrupteur de porte 19
 Interrupteur marche / arrêt 30
 Interrupteur pour porte 28, 53, 62, 90
 Interrupteurs de verrouillage de sécurité à fonctionnement magnétique 92
 Interrupteurs de verrouillage de sécurité à ouverture positive 92
 Interrupteurs pour porte (ou protection verrouillée) 92
 Interrupteurs pour portes (ou protections interverrouillées) possibilités de connexions 94
 IP...Protection contre l'entrée (Classe) 121
 ISO 12100-1 (2003) & -2 (2003)(EN 292-1 & -2) 2
 ISO 13849-1 (2006)(EN 954-1) 2
 ISO 13850 (2006) (EN418) 2
 ISO 13851 (2002)(EN 574) 2
 ISO 13852 (1996)(EN 294) 2
 ISO 13853 (1998) (prEN 811) 2
 ISO 13855 (2002)(EN 999) 2
 ISO 14119 (1998) (EN 1088) 2
 ISO 14121-1 (2007)(EN 1050) 2
 ISO 3864-2 (2004) 2
 ISO 7010 (2003) 2
 ISO Office international de normalisation 121

K

Kit de démarrage du contrôleur de sécurité 82

L

L'entrée est inhibée Pas d'inhibition 35
 L'état de muting doit être facilement observable 115
 La commande de la machine doit disposer d'une commande d'anti-répétition 98
 La configuration du contrôleur de sécurité peut s'effectuer au moyen d'une des deux interfaces : 12
 La liste qui suit représente les adresses des représentants et distributeurs Banner en Europe : 125
 La procédure comprend trois étapes principales : 12
 La sortie de sécurité passe sur OFF quand1 : 29
 La sortie de sécurité passe sur ON quand2 : 29
 Laisser au minimum 65 mm de jeu pour le câble USB et 43 mm pour l'insertion de la carte XM 24

LCD Affichage à cristaux liquides 121
 Le contrôleur de sécurité ne doit être raccordé qu'à une alimentation SELV ou PELV. 21
 Le cycle d'inhibition s'arrête à l'expiration du minuteur 117
 Le fait de cliquer sur le bouton INFO renvoie à plus d'informations. 27
 LED Diode électroluminescente 121
 Les entrées de muting doivent être redondantes 113
 Liaison entrée / sortie 54
 Limite de temps d'inhibition (temporisateur de porte arrière) 9, 115
 Limite de temps d'inhibition 115
 Limite de temps de l'interrupteur de bypass. 11
 Limite de temps de la fonction 28
 Limite de temps du dispositif de commande 9
 Limites de l'inhibition 113
 Lire ce Paragraphe 1.6 en page 3 avec attention avant d'installer le système 3
 Liste des abréviations 121
 Logiciel installé 36
 Logique dans le temps d'un dispositif de commande bimanuelle et réarmement manuel des entrées de sécurité 8
 Logique dans le temps des entrées de sécurité avec un réarmement manuel surveillé commun, assigné à la même sortie de sécurité 8
 Logique dans le temps des entrées de sécurité de réarmement manuel Auto et manuel surveillé assignées à la même sortie de sécurité (la sortie de sécurité n'a pas de délai) 7
 Logique de réarmement : 28
 Logique de temps d'une barrière immatérielle avec détecteurs d'inhibition et interrupteur de bypass 10
 Logique de temps de la sortie de sécurité avec temporisation OFF 14
 Logique interne 8, 17
 Logique interne de l'entrée de sécurité 8

M

Maintenance correctrice 76
 Maintenance préventive 71
 MARCHE/ARRET 19, 53, 62
 Marquage CE et plaque d'identification du contrôleur de sécurité SC22-3 21
 Marquage CE/plaque d'identification du produit 21
 ME Activation de l'inhibition 121
 Message affiché 77
 Message d'état de la sortie de sécurité 68
 Message d'état des dispositifs d'entrée 68
 Minuteur d'inhibition sélectionnable 117, 118
 Miroirs d'angle, systèmes optiques de sécurité et inhibition 116
 Mise en marche ou arrêt d'une temporisation 14
 Mise en service et configuration initiale – vérifications périodiques 72
 Mise sous tension automatique 16
 ML Voyant d'inhibition 121
 Mode à la mise sous tension 17
 Mode actif 9, 68
 Mode de configuration 19, 53, 56
 Mode Run (fonctionnement) 53, 68
 Modèle 23
 Modèle et type du contrôleur de sécurité SC22-3 23
 Modification d'une configuration existante 49
 Modification de la configuration 49
 Modifier L'entrée 53, 62
 Modifier la configuration 19, 53, 56
 Modifier OBI sorties d'état - Options 62
 Modifier une entrée 19, 56
 Modules d'interface Série IM-T-9 83
 Modules d'interface Série SC-IM9 83
 Montre le type de circuit et les assignations des bornes d'entrée sélectionnées 72
 MPCE Élément de contrôle primaire de la machine 121
 MSSl Interfaces d'arrêt de sécurité pour inhibition 121

N

N.F. Normalement fermé 121
 N.O. Normalement ouvert 121
 Ne pas mettre le contrôleur de sécurité ni la machine protégée sous tension à ce stade. 72
 NE PAS poursuivre l'opération tant que tous les problèmes n'ont pas été corrigés. 75
 Ne pas utiliser la machine tant que le système ne fonctionne pas correctement 71

Nettoyage 76
 Niveaux d'immunité électromagnétique 5
 Niveaux d'intégrité des circuits de sécurité 89, 92, 96, 104
 Niveaux d'intégrité des circuits de sécurité avec plusieurs boutons d'arrêt d'urgence 105
 Niveaux d'irradiation 5
 Niveaux de parasite de l'équipement 5
 Niveaux de vibration 5
 Nom de l'auteur 16
 Nom de la configuration 16, 19, 56, 68
 Nom du dispositif 81
 Nomenclature 21
 Nommer la configuration 53
 Non assigné 62
 Normes de performances du produit 22
 Normes de sécurité 2
 numéro de modèle de la version du logiciel Et du matériel 53
 Numéro du modèle 54

O

OBI 31
 OBI Interface embarquée 121
 OFF 68
 ON 68
 ON/OFF 30
 Option d'inhibition à la mise sous tension 74
 Options de configuration de OBI 19
 Options du mode de configuration OBI du contrôleur de sécurité SC22-3 56
 Options du mode Run OBI du Contrôleur de sécurité SC22-3 53
 Options du système 19, 53, 66
 OSSD Dispositif de commutation du signal de sortie 121
 Outil de programmation SC-XMP 26
 Outils de configuration 39
 Ouvrir une configuration à partir de la carte XM 50

P

Paire de capteurs d'inhibition 30
 Paire de détecteur d'inhibition 9
 Paramétrage des sorties d'état 19, 56
 Paramétrage des temps limites d'inhibition 60
 Paramètre de sortie d'état 53, 62
 Paramètres des sorties d'état 19, 53
 Paramètres du signal de réarmement 70
 Paramètres du système 19, 53, 56, 62
 Paramètres du système, sorties 19, 53, 62
 Paramètres du système, sorties (paramètres sorties / système en page 62) 56
 Paramètres états des sorties 54
 Paramètres sorties / système 62
 Paramètres système 16, 63
 Pas de surveillance 34
 PAS un dispositif de protection autonome d'un point de fonctionnement 3
 PCI Interface PC 121
 Permet à chaque dispositif d'être assigné à 1, 2 ou 3 sorties de sécurité 27
 Personne désignée 4
 Personne qualifiée 4
 Personnes désignées et qualifiées 4
 Peut être bypassé 28
 Peut être inhibé 28
 Pièces de rechange, outils spéciaux et accessoires 82
 Pièces détachées 82
 PL Niveau de performances 121
 Planning des vérifications 71
 PLC Contrôleur logique programmable 121
 Port de la carte XM 26
 Port USB 36
 Port USB B 26
 Possibilités de connexions 91, 99, 102, 105, 107, 109, 111, 114
 Pour ajouter une entrée auxiliaire (entrée de non sécurité) 41
 Pour ajouter une entrée de sécurité: 41
 Pour créer une configuration : 17
 Pré vérifications de mise en service 71
 Précaution 1

prEN Norme Européenne préliminaire 121
 Prescriptions du système 36
 Présentation des avis de sécurité 1
 Présentation des dispositifs d'Entrée de sécurité supplémentaires 61
 Présentation des messages d'état de la carte XM 69
 Présentation des messages d'état de la sortie de sécurité 68
 Procédure 72
 Procédure d'installation 71
 Procédures de sécurité d'exploitation et de formation 111
 Produit 21
 Propriétés configurables 28, 30
 Propriétés des dispositifs d'entrée de sécurité 27, 30
 Protection de plusieurs zones 116
 Protection du poste de travail 98
 Protocole de sécurité 4
 PSDI Dispositif de détection de présence 121
 PSSD Détection de présence 121

Q

QD Raccord rapide 121

R

Raccordement d'interface FSD 34
 Raccordement des EDM, ossd sortie de sécurité et fsd 34
 Raccordement des sorties OSSD 13
 Raccordement du contrôleur de sécurité SC22-3 26
 Raccordement du PC à l'outil de programmation SC-XMP 26
 Raccordement EDM à canal double 85
 Raccordement EDM à canal double au module d'interface IM-T-9A 86
 raccordement EDM canal simple au module d'interface IM-T-9A 87
 Raccordement électrique 26
 Raccordements électriques 3
 Réarmement – RS01 61
 Réarmement 53, 62
 Réarmement du système 49
 Réarmement du système 5, 9, 49, 63
 Réarmement manuel 5, 30, 69
 Réarmement manuel surveillé 8
 Réarmement nécessaire 68
 Réarmement non surveillé 70
 Réarmement sortie nécessaire Réarmement sortie non nécessaire 35
 Réarmement surveillé 17
 Réarmement système et conditions de blocage 70
 Réarmement système nécessaire Réarmement système non nécessaire 35
 Réarmements 5
 Réception d'une configuration depuis un contrôleur de sécurité SC22-3 50
 Recevoir fichier de l'XM 63
 Recevoir un fichier de la XM 19, 53
 Recherche de pannes 77
 Récupération suite à un blocage 79
 Référence 19, 82, 83, 84
 Référence de commande 23
 Références de la documentation 84
 Registre d'erreurs — PCI 80
 Réglages avancés 29
 Régler le contraste de l'écran 19, 53, 55
 Règles de minutage du signal d'entrée COS (simultanéité) en état Run 29
 Relais de sécurité 83
 Remarque : Les sorties de sécurité SO1, SO2 et SO3 sont des sorties à canal double 13
 Remarques 1
 Remède suggéré 81
 Réparations et service sous garantie 76
 Reset (réarmement) 19
 Reset contrôlé 30, 70
 Résistance des fils de la sortie de sécurité 12
 Résistance mécanique 22
 Responsabilité de l'utilisateur pour la sécurité de l'application 3
 Résumé de la configuration 19, 53, 54, 56, 62, 63
 Retard à l'enclenchement et au déclenchement des sorties de sécurité 14
 Retard au déclenchement 13
 Risque d'électrocution – débrancher l'alimentation électrique 3

S

Sauvegarder la configuration 19, 53, 56, 62, 63
 Sauvegarder les erreurs affichées dans un fichier pour utilisation ultérieure. 80
 Schémas de câblage 85
 Sécurité électrique 3
 Sécurité générale 1
 Sélection des entrées de sécurité 41
 Sélectionner la fonction... 62
 Sélectionner la source... 62
 Sélectionner le langage 66
 Sélectionner une fonction... 63
 Sélectionner une source... 63
 Séquence de réarmement requise 104
 Séquences dans le temps de l'inhibition 117
 Série IM-T-9 83
 Série SC-IM9 83
 Sert à sélectionner la logique de réarmement dans un menu déroulant 27
 Sert à sélectionner le type de circuit dans un menu déroulant 27
 Sert à taper un nom d'un dispositif d'entrée de sécurité 27
 Si le module muting ne passe pas l'une de ces vérifications, ne pas l'utiliser avant d'avoir identifié et rectifié la ou les anomalies. 76
 Signal Convention 1 24 Vcc = Run (par défaut) 35
 Signal Convention 2 0 Vcc = Run 35
 Signal de réarmement manuel 8
 SIL Niveau d'intégrité de sécurité 121
 Sortie de sécurité (Retard à l'enclenchement) 9
 Sortie de sécurité 1 8
 Sortie de sécurité 7, 8, 9, 10, 11, 117, 118
 Sortie de sécurité SO1, SO2, SO3 32
 Sortie de voyant d'inhibition (ML) 115
 Sortie Run Sortie Stop 35
 Sorties 84
 Sorties auxiliaires non sécurisées 83
 Sorties d'état 15, 19, 35, 53, 56, 62
 Sorties d'état de lampe d'inhibition 15
 Sorties d'état (10 bornes) 21
 Sorties de sécurité 12, 14, 19, 56, 62, 83
 Sorties de sécurité (6 bornes, 3 sorties redondantes) 21
 Sorties de sécurité. 53, 62
 Sortir de la configuration 19, 53
 Sortir du mode de configuration 66
 Spécifications 21
 SSI Interface d'arrêt de sécurité 121
 Stop 68
 Surveillance des commutateurs externes - EDM02 59
 Surveillance des commutateurs externes – EDM03 59
 surveillance des commutateurs externes (EDM) 59
 Surveillance des commutateurs externes 6, 28
 Surveillance des interrupteurs de verrouillage de sécurité raccordés en série 93
 Surveillance double voies 11, 34
 Surveillance simple voie 11, 34
 Symbole 2
 Symbole du circuit 29
 Système en blocage Système en mode Run 35
 Système en fonctionnement 36

T

Tapis de sécurité (bordures de sécurité) 101
 Tapis sensible de sécurité 19, 28, 53, 62, 90
 Taux de protection à l'accès 2
 Temporisation à l'enclenchement 68
 Temporisation au déclenchement 68
 Temps d'anti-anti-rebond fermé à ouvert / temps d'anti-anti-rebond ouvert à fermé 30
 Temps d'anti-rebond de fermé à ouvert 30
 Temps d'anti-rebond fermé à ouvert / temps d'anti-rebond ouvert à fermé 30
 Temps d'anti-rebond ouvert à fermé 30
 Temps de réponse Et de réaction 22
 Temps dépassé 68
 Temps écoulé depuis l'erreur 81
 Temps limite du dispositif 30

Temps maximum 117
 Tension d'alimentation 83, 84
 Tension de service 83
 Test 68
 Test de démarrage 28, 30
 Tous les indicateurs OFF 32
 Tracer entrée 62
 Tracer état défaut 62
 Tracer sortie 62
 Transmettre / recevoir Tx/Rx 32
 Travailler avec le programme PCI 37
 Type de circuit 28, 29
 Type n° 23, 82, 83, 84
 Types de changement d'état de signal (COS)(simultanéité) 29
 Types de circuits : 28, 30

U

Une erreur d'E/S existe Il n'existe pas d'erreur d'E/S 35
 USB Bus de série universel 121
 Utilisation de supprimeurs d'arcs 12
 Utilisation des avertissements 3
 Utilisation des fonctions de l'interrupteur d'inhibition et de bypass 10

V

VAC Tension en courant alternatif 121
 Valeur/explication 21
 Valeurs de sorties 83, 84
 Validation de la configuration 48
 VDC Tension en courant continu 121
 Vérification (finale) du système 75
 Vérification avant un réarmement 70
 Vérification de mise en service 35, 71
 Vérification du fonctionnement du système 72
 Vérification du système 71
 Vérification du système de sécurité et des dispositifs de protection 72
 Vérification initiale 77
 Vérifications opérationnelles journalières 71
 Vérifications périodiques (tous les 6 mois) 71
 Vérifications périodiques 71
 Verrouillage de la carte XM 50
 Versions logiciel et matériel 19
 Voir aussi Paragraphe 1.18 en page 6 à propos des EDM et Paragraphe 4.8.2 en page 34 sur l'interfaçage des circuits de sécurité d'arrêt. 85
 Voir le registre d'erreurs 19, 53, 81
 Voir les erreurs actuelles 81
 Voir les erreurs en cours 19, 53
 Voir les temps de réponse 19, 53, 54, 56
 Vue générale 7
 Vue générale de l'interface embarquée 18
 Vue générale de l'interface PC 18
 Vue générale du mot de passe 17

X

XM correspond à la configuration active 69
 XM n'a pas de configuration 69
 XM ne correspond pas à la configuration active 69