Manuel de référence sur la sécurité

Allen-Bradley

Systèmes automates GuardLogix 5570

Références 1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT, 1756-L7SP, 1756-L7SPXT, 1756-L72EROMS, Applications Studio 5000 Logix Designer

Traduction des instructions d'origine

Informations importantes destinées à l'utilisateur

Avant d'installer, de configurer, d'exploiter ou d'entretenir ce produit, lisez le présent document et ceux répertoriés à la section Documentation connexe à propos de l'installation, de la configuration, et de l'exploitation de cet équipement. Les utilisateurs sont tenus de se familiariser avec les consignes d'installation et de câblage en plus des prescriptions stipulées dans toutes les règles, réglementations et normes en vigueur.

Les activités telles que l'installation, les réglages, la mise en service, l'utilisation, l'assemblage, le démontage et la maintenance doivent être effectuées par du personnel convenablement formé conformément aux règles de l'art en vigueur.

Si cet équipement n'est pas utilisé selon les recommandations du fabricant, la protection assurée par l'équipement risque d'être détériorée.

La société Rockwell Automation, Inc. ne saurait en aucun cas être tenue pour responsable ni être redevable des dommages indirects ou consécutifs à l'utilisation ou à l'application de cet équipement.

Les exemples et schémas contenus dans ce manuel sont présentés à titre indicatif seulement. En raison du nombre important de variables et d'impératifs associés à chaque installation, la société Rockwell Automation, Inc. ne saurait être tenue pour responsable ni être redevable des suites d'utilisation réelle basée sur les exemples et schémas présentés dans ce manuel.

La société Rockwell Automation, Inc. décline également toute responsabilité en matière de propriété intellectuelle et industrielle concernant l'utilisation des informations, circuits, équipements ou logiciels décrits dans ce manuel.

Toute reproduction totale ou partielle du présent manuel sans autorisation écrite de la société Rockwell Automation Inc. est interdite.

Des remarques sont utilisées tout au long de ce manuel pour attirer votre attention sur les mesures de sécurité à prendre en compte.

	AVERTISSEMENT : identifie des actions ou situations risquant de provoquer une explosion dans un environnement dangereux et d'entraîner des blessures pouvant être mortelles, des dégâts matériels ou des pertes financières.
	ATTENTION : identifie des actions ou situations risquant d'entraîner des blessures pouvant être mortelles, des dégâts matériels ou des pertes financières. Les messages « Attention » vous aident à identifier un danger, à éviter ce danger et en discerner les conséquences.
IMPORTANT	Informations particulièrement importantes dans le cadre de l'utilisation et de la compréhension du produit.

Des étiquettes peuvent être placées sur l'équipement ou à l'intérieur pour signaler des précautions particulières à prendre en compte.

	DANGER D'ÉLECTROCUTION : l'étiquette ci-contre, placée sur l'équipement ou à l'intérieur (un variateur ou un moteur, par ex.), signale la présence éventuelle de tensions électriques dangereuses.
	RISQUE DE BRÛLURE : l'étiquette ci-contre, placée sur l'équipement ou à l'intérieur (un variateur ou un moteur, par ex.), indique que certaines surfaces peuvent atteindre des températures particulièrement dangereuses.
	DANGER D'ÉCLAIR D'ARC : l'étiquette ci-contre, placée sur l'équipement ou à l'intérieur (un centre de commande de moteurs, par ex.), signale un risque d'éclair d'arc. L'éclair d'arc provoquera des blessures graves, voire mortelles. Portez un équipement de protection individuelle (ÉPI). Respectez TOUTES les prescriptions réglementaires concernant les pratiques de travail sûres et les équipements de protection individuelle (ÉPI).

Allen-Bradley, Armor, ArmorBlock, ArmorGuard, CompactBlock, CompactLogix, ControlFLASH, ControlLogix, ControlLogix-XT, FLEX, Guard I/O, GuardLogix, GuardLogix-XT, Kinetix, Logix5000, POINT Guard I/O, Rockwell Automation, Rockwell Software, RSLogix, SLC, SmartGuard, Studio 5000, Studio 5000 Automation Engineering & Design Environment sont des marques commerciales de Rockwell Automation, Inc.

ControlNet, DeviceNet et EtherNet/IP sont des marques commerciales d'ODVA. Les marques commerciales n'appartenant pas à Rockwell Automation sont la propriété de leurs sociétés respectives.

Ce manuel comporte des informations nouvelles et actualisées.

Informations nouvelles et actualisées

Ce tableau décrit les modifications apportées à la présente version.

Sujet	Page
Remplacement des renvois aux modules d'E/S de sécurité par des renvois aux dispositifs d'E/S de sécurité plus généraux, le cas échéant	Ensemble du manuel
Ajout à la première de couverture de la référence Armor™ GuardLogix®, 1756-L72ERDMS	Première de couverture
Ajout d'informations sur les servovariateurs Kinetix® 5500 à la liste des composants certifiés SIL-3	16
Ajout du module 1756-EN2TRXT à la liste des modules d'interface de communication	23
Ajout d'une remarque indiquant que le projet n'est pas valide en présence de doublons dans les combinaisons de SNN et d'adresse de station	35
Ajout d'un renvoi au manuel utilisateur des servovariateurs Kinetix 5500 pour des informations sur l'utilisation des commandes directes de mouvement dans les applications de sécurité	72
Ajout de données de sécurité actualisées (CEI 61508, édition 2, 2010) pour les modules Guard I/O™	Annexe E
Ajout de données de sécurité pour les modules 1734-IB8S, Série B et 1734-OB8S, Série B	Annexe E
Mise à jour des données PFH pour les modules 1734-IE4S	Annexe E

Notes :

Préface

Environnement Studio 5000 9
Terminologie 10
Documentation connexe 10

Chapitre 1

Concept de niveau d'intégrité de sécurité (SIL)

Certification SIL 3 13
Tests de vérification 14
Architecture GuardLogix pour les applications SIL 3 15
Composants du système GuardLogix 16
Certifications GuardLogix 18
Spécifications PFD et PFH de GuardLogix 18
Répartition et poids de la conformité au niveau d'intégrité de sécurité (SIL) 19
Temps de réponse du système 19
- Temps de réponse de la tâche de sécurité 20
- Période de la tâche de sécurité et chien de garde de la tâche de sécurité 20

Qui contacter en cas de défaillance du dispositif 20

Chapitre 2

Système automate GuardLogix

Configuration matérielle d'un automate GuardLogix 5570 21
- Automate principal 22
- Partenaire de sécurité 22
- Châssis 22
- Alimentations 22

Protocole CIP Safety 22
Dispositifs d'E/S de sécurité 23
Passerelles de communication 23
Présentation de la programmation 25

Chapitre 3

E/S CIP Safety pour le système de commande GuardLogix

Présentation 27
Fonctions de sécurité typiques des dispositifs d'E/S CIP Safety 27
- Diagnostics 28
- Données d'état 28
- Voyants d'état 28
- Temporisation à l'enclenchement ou au déclenchement 28

Temps de réponse 28
Conditions de sécurité des dispositifs d'E/S CIP Safety 29
- Propriété 29
- Signature de configuration des E/S de sécurité 29
- Remplacement des dispositifs d'E/S de sécurité 29

Chapitre 4

CIP Safety et numéro de réseau de sécurité

Système de commande CIP Safety routable 33
Référence de station unique 34
Numéro de réseau de sécurité 34
Remarques sur l'attribution du numéro de réseau de sécurité (SNN) 35
Numéro de réseau de sécurité (SNN) pour points de sécurité consommés 35
Numéro de réseau de sécurité (SNN) pour dispositifs en configuration d'usine 36
Numéro de réseau de sécurité (SNN) pour dispositif de sécurité avec un propriétaire de configuration différent 36
Numéro de réseau de sécurité (SNN) lors de la copie d'un projet de sécurité 36

Chapitre 5

Caractéristiques des points de sécurité, de la tâche de sécurité et des programmes de sécurité

Différence entre composants standard et de sécurité 37
Applications de sécurité SIL 2 38
Commande de sécurité SIL 2 dans la tâche de sécurité 38
Commandes de sécurité SIL 2 dans des tâches standard 40
Sécurité SIL 3 – tâche de sécurité 41
Limites de la tâche de sécurité 41
Détails de l'exécution de la tâche de sécurité 42
Utilisation d'interfaces homme-machine 43
Précautions 43
Accès à des systèmes dédiés à la sécurité 44
Programmes de sécurité 45
Sous-programmes de sécurité 45
Points de sécurité 46
Points standard dans des sous-programmes de sécurité (adressage des points) 47

Chapitre 6

Développement d'une application de sécurité

Principes du concept de sécurité 49
Principes de base du développement et du test d'une application 50
Organigramme de la mise en service 51
Définition de la fonction de commande 52
Création du projet 53
Tester le programme d'application 53
Génération de la signature de la tâche de sécurité 53
Test de vérification du projet 54
Confirmation du projet 55
Validation de la sécurité 56
Verrouillage de l'automate GuardLogix 56
Chargement du programme de l'application de sécurité 57
Transfert du programme de l'application de sécurité 57
Modification en ligne 57
Stockage et chargement d'un projet à partir de la mémoire non volatile 58

Forçage des données 58
Inhiber un dispositif 58
Modification de votre application de sécurité 59
Modifications hors ligne 60
Modifications en ligne 60
Test d'impact des modifications 60

Chapitre 7

Surveillance de l'état et gestion des défauts

Surveillance d'état du système 63
Données de CONNECTION_STATUS 63
Diagnostic des entrées et des sorties 64
Etat des connexions du dispositif d'E/S 64
Système de déclenchement par mise hors tension 65
Instructions GSV et SSV 65
Défauts du système GuardLogix 66
Défauts d'automate irrécupérables 66
Défauts de sécurité irrécupérables 66
Défauts récupérables 67

Annexe A

Instructions de sécurité

Annexe B

Instructions complémentaires de sécurité

Créer et utiliser une instruction complémentaire de sécurité 73
Créer un projet de test pour une instruction complémentaire 75
Créer l'instruction complémentaire de sécurité 75
Générer la signature d'instruction 75
Charger et générer la signature d'instruction de sécurité 76
Test de qualification d'instruction complémentaire SIL 3 76
Confirmer le projet 76
Valider l'instruction complémentaire de sécurité 77
Créer l'entrée d'historique de signature 77
Exporter et importer l'instruction complémentaire de sécurité 77
Vérifier les signatures d'instructions complémentaires de sécurité 78
Tester le programme d'application 78
Test de vérification du projet 78
Valider le projet de sécurité 78
Documentation connexe 78

Annexe C

Temps de réponse

Temps de réponse du système 79
Temps de réponse du système Logix 79
Chaîne Entrée-Programme-Sortie simple 80
Chaîne logique utilisant des points de sécurité produits/consommés 81
Facteurs affectant les composants du temps de réponse Logix 82
Accès aux réglages de délai d'un module d'entrée Guard I/O 82

Accès au temps de réponse max. des connexions d'entrée et de sortie de sécurité 83
Configuration de la période de la tâche de sécurité et du chien de garde 84
Accès aux données de point produit/consommé 85

Annexe D

Listes de contrôle pour applications de sécurité GuardLogix

Liste de contrôle pour le système automate GuardLogix 88
Liste de contrôle pour les entrées de sécurité 89
Liste de contrôle pour les sorties de sécurité 90
Liste de contrôle pour le développement d'un programme d'application de sécurité 91

Annexe E

Données de sécurité des systèmes GuardLogix

Valeurs de PFD 93
Valeurs de PFH 94

Annexe F

Logiciel RSLogix 5000, version 14 et ultérieure ; instructions pour applications de sécurité

Système à déclenchement par mise hors tension 95
Utilisation des données d'état de connexion pour générer un défaut par programmation 95

Annexe G

Utilisation de modules d'E/S FLEX I/O 1794 et d'entrées/sorties 1756 SIL 2 avec des automates GuardLogix 1756, conformément à la norme EN 50156

Entrées double voie SIL 2 (partie standard des automates GuardLogix) 101
Sorties SIL 2 utilisant des modules de sortie SIL 3 Guard I/O 103
Sorties SIL 2 utilisant des modules de sortie SIL 2 1756 ou 1794 103
Fonctions de sécurité dans la tâche de sécurité de l'automate GuardLogix 1756 104

Glossaire

Index

Sujet	Page
Environnement Studio 5000	9
Terminologie	10
Documentation connexe	10

Ce manuel a pour objet la présentation du système d'automate GuardLogix 5570, qui fait l'objet d'une **homologation de type** et d'une certification pour une utilisation dans les applications de sécurité jusqu'au niveau SIL CL 3 inclus conformément aux normes CEI 61508 et CEI 62061, et jusqu'au niveau de performance PLe (Catégorie 4) inclus selon la norme ISO 13849-1.

Utilisez ce manuel si vous êtes en charge du développement, de l'exploitation ou de la maintenance d'un système de sécurité à base d'automate GuardLogix 5570, utilisant l'application Studio 5000® Logix Designer en version 21.000 ou supérieure. Veuillez lire et bien assimiler les concepts et prescriptions de sécurité qui sont présentés dans ce manuel avant d'utiliser un système de sécurité à base d'automate GuardLogix 5570.

Pour les prescriptions de sécurité applicables aux automates GuardLogix 5570 dans le cadre de projets RSLogix™ 5000, reportez-vous à la publication 1756-RM093, « Systèmes automates GuardLogix Manuel de référence sur la sécurité ».

Environnement Studio 5000

Le progiciel Studio 5000 Automation Engineering and Design Environment™ regroupe des éléments d'ingénierie et de conception dans un environnement logiciel commun. Le premier élément de l'environnement Studio 5000 est l'application Logix Designer. L'application Logix Designer est la nouvelle dénomination commerciale du logiciel RSLogix™ 5000, qui continue d'être le produit destiné à programmer les automates Logix5000™ pour les solutions de commande discrète, de procédés, de traitement par lots, de mouvement, de sécurité et à base de variateurs.

L'environnement Studio 5000 constitue la base pour les futurs outils et possibilités que va offrir Rockwell Automation® en matière d'ingénierie et de conception. C'est une plate-forme unique au service des ingénieurs d'étude pour le développement de l'ensemble des composants de leurs systèmes de commande.

Terminologie

Vous trouverez dans le tableau suivant les termes utilisés dans ce manuel.

Tableau 1 – Termes et définitions

Abréviation	Description	Définition
1oo2	One Out of Two (un parmi deux)	Définit l'architecture de l'automate électronique programmable.
CIP	Common Industrial Protocol (protocole industriel commun)	Protocole de communication industriel utilisé par les systèmes d'automatisation basés sur la technologie Logix5000, sur des réseaux de communication Ethernet/IP™, ControlNet™ et DeviceNet™.
CIP Safety	Common Industrial Protocol – Safety Certified (protocole industriel commun – certifié sécurité)	Version homologuée SIL 3 du protocole CIP.
DC	Taux de couverture des tests de diagnostic	Rapport entre le taux de défaillances détectées et le taux de défaillances totales.
EN	European Norm (norme européenne)	Norme européenne de référence
GSV	Lire la valeur système	Instruction de logique à relais qui récupère les informations d'état de l'automate spécifiées et les place dans un point de destination.
PC	Personal Computer (ordinateur personnel)	Ordinateur utilisé pour assurer l'interface et la commande d'un système de type Logix par l'intermédiaire de l'environnement Studio 5000.
PFD	Probability of Failure on Demand (probabilité de défaillance sur sollicitation)	Probabilité moyenne d'échec d'un système opérationnel dans l'exécution d'une fonction sollicitée.
PFH	Probability of Failure per Hour (probabilité de défaillance par heure)	Probabilité de survenue d'une panne dangereuse par heure sur un système opérationnel.
PL	Niveau de performance	Classification de sécurité selon l'ISO 13849-1.
SNN	Numéro de réseau de sécurité	Numéro unique qui identifie une section d'un réseau de sécurité.
SSV	Définir la valeur système	Instruction de logique à relais qui définit les données du système automate.
--	Standard	Tout objet, tâche, point, programme ou composant de votre projet autre qu'un élément de sécurité (par exemple, « automate standard » renvoie génériquement à un automate ControlLogix® ou CompactLogix™).

Documentation connexe

Ces documents contiennent des informations détaillées sur des produits connexes de Rockwell Automation.

Ressource	Description
Automates GuardLogix 5570 – Manuel utilisateur, publication 1756-UM022	Fournit des informations sur l'installation, la configuration, la programmation et l'utilisation des automates GuardLogix 5570 dans les projets Studio 5000 Logix Designer
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Fournit des informations sur le jeu d'instructions pour application de sécurité GuardLogix.
Guard I/O DeviceNet Safety Modules User Manual, publication 1791DS-UM001	Fournit des informations sur l'utilisation des modules de sécurité Guard I/O sur DeviceNet
Guard I/O EtherNet/IP Safety Modules User Manual, publication 1791ES-UM001	Fournit des informations sur l'utilisation des modules de sécurité Guard I/O sur EtherNet/IP
Modules de sécurité POINT Guard I/O – Notice d'installation et manuel utilisateur, publication 1734-UM013	Fournit des informations sur l'installation et l'utilisation des modules POINT Guard I/O™
Servovariateurs Kinetix 5500 Manuel utilisateur, publication 2198-UM001	Fournit des informations sur l'installation et l'utilisation des servovariateurs Kinetix 5500
Using ControlLogix in SIL 2 Applications Safety Reference Manual, publication 1756-RM001	Décrit les exigences relatives à l'utilisation des automates ControlLogix et de la tâche standard GuardLogix dans les applications de commande de sécurité SIL 2.
Automates Logix5000 – Jeu d'instructions – Manuel de référence, publication 1756-RM003	Fournit des informations sur le jeu d'instructions des automates Logix5000.
Logix Common Procedures Programming Manual, publication 1756-PM001	Fournit des informations sur la programmation des automates Logix5000, y compris sur la gestion des fichiers de projet, l'organisation des points, la programmation et le test des sous-programmes, ainsi que le traitement des défauts
Automates Logix5000 – Instructions complémentaires Manuel de programmation, publication 1756-PM010	Fournit des informations sur la création et l'utilisation d'instructions complémentaires standard et de sécurité dans les applications Logix.
Manuel utilisateur des systèmes ControlLogix, publication 1756-UM001	Fournit des informations sur l'utilisation des automates ControlLogix dans des applications non liées à la sécurité

Ressource	Description
DeviceNet Modules in Logix5000 Control Systems User Manual, publication DNET-UM004	Fournit des informations sur l'utilisation du module 1756-DNB dans un système de commande Logix5000.
EtherNet/IP Modules in Logix5000 Control Systems User Manual, publication ENET-UM001	Fournit des informations sur l'utilisation du module 1756-ENBT dans un système de commande Logix5000.
ControlNet Modules in Logix5000 Control Systems User Manual, publication CNET-UM001	Fournit des informations sur l'utilisation du module 1756-CNB dans un système de commande Logix5000.
Logix5000 Controllers Execution Time and Memory Use Reference Manual, publication 1756-RM087	Informations sur l'estimation du temps d'exécution des instructions et de la mémoire utilisée.
Logix Import Export Reference Manual, publication 1756-RM084	Fournit des informations sur l'utilisation de l'utilitaire d'importation/exportation de Logix Designer
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Fournit des recommandations générales pour l'installation d'un système industriel Rockwell Automation
Site Internet Product Certifications (homologations produits), http://www.ab.com	Fournit des déclarations de conformité, des certificats et autres détails relatifs aux homologations

Vous pouvez visualiser ou télécharger ces documentations à l'adresse http://www.rockwellautomation.com/literature/. Pour commander des exemplaires imprimés de documentation technique, contactez votre distributeur Allen-Bradley® ou votre représentant Rockwell Automation local.

Notes :

Concept de niveau d'intégrité de sécurité (SIL)

Sujet	Page
Certification SIL 3	13
Tests de vérification	14
Architecture GuardLogix pour les applications SIL 3	15
Composants du système GuardLogix	16
Certifications GuardLogix	18
Spécifications PFD et PFH de GuardLogix	18
Répartition et poids de la conformité au niveau d'intégrité de sécurité (SIL)	19
Temps de réponse du système	19
Période de la tâche de sécurité et chien de garde de la tâche de sécurité	20
Qui contacter en cas de défaillance du dispositif	20

Certification SIL 3

Les systèmes d'automates GuardLogix 5570 font l'objet d'une homologation de type et sont certifiés pour une utilisation dans les applications de sécurité jusqu'au niveau SIL CL3 inclus, conformément aux normes CEI 61508 et CEI 62061, et dans les applications de sécurité jusqu'au niveau de performance PLe (catégorie 4) selon la norme ISO 13849-1. Les critères SIL sont basées sur les normes en vigueur au moment de la certification.

IMPORTANT	Quand l'automate GuardLogix se trouve en mode Exécution (Run) ou Programmation (Program) et que vous n'avez pas validé le programme d'application, vous êtes responsable du maintien des conditions de sécurité.

De plus, les tâches standard des automates GuardLogix peuvent être utilisées aussi bien dans des applications standard que dans des applications de sécurité SIL 2, telles que décrites dans la publication 1756-RM001, « Using ControlLogix in SIL 2 Applications Reference Manual ». Dans tous les cas, ne pas utiliser de tâches et de variables SIL 2 ou standard pour réaliser des boucles de sécurité d'un niveau supérieur. La tâche de sécurité est la seule tâche qui est certifiée pour les applications SIL 3.

Utilisez l'application Studio 5000 Logix Designer pour créer des programmes pour les automates GuardLogix 5570.

Le TÜV Rheinland a homologué l'utilisation des systèmes automates GuardLogix 5570 dans les applications de sécurité jusqu'au niveau SIL 3, dans lesquelles l'état hors tension est considéré comme étant l'état de sécurité. Dans tous les exemples qui se rapportent aux E/S présentées dans ce manuel, l'état hors tension est considéré comme étant l'état de sécurité pour les systèmes de sécurité machine et d'arrêt d'urgence (ESD) typiques.

IMPORTANT En tant qu'utilisateur du système, vous êtes responsable :

- de l'installation, de l'évaluation du niveau SIL et de la validation de tous les capteurs ou actionneurs qui sont connectés au système GuardLogix ;
- de la gestion du projet et du test fonctionnel ;
- du contrôle des accès au système de sécurité, y compris de la gestion des mots de passe ;
- de la programmation de l'application et de la configuration des dispositifs conformément aux informations contenues dans le présent manuel de référence pour la sécurité, ainsi que dans la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur »

Lorsque vous appliquez la sécurité fonctionnelle, limitez l'accès à un personnel qualifié et autorisé, dûment formé et expérimenté. La fonction de verrouillage de sécurité par mot de passe est fournie dans l'application Logix Designer.

Pour toute information sur les modalités d'utilisation de la fonction de verrouillage de sécurité, reportez-vous à la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur ».

Tests de vérification

La norme CEI 61508 impose l'exécution de différents tests de vérification des équipements utilisés dans le système. Ces tests sont effectués selon une fréquence définie par l'utilisateur. Ils peuvent par exemple être exécutés une fois par an, une fois tous les 15 ans ou selon n'importe périodicité appropriée.

Les automates GuardLogix 5570 requièrent une périodicité des tests de vérification pouvant aller jusqu'à 20 ans. D'autres composants du système, comme les dispositifs d'E/S de sécurité, les capteurs et les actionneurs peuvent faire l'objet de tests de vérification plus fréquents. L'automate doit être inclus dans la procédure des tests de vérification fonctionnelle des autres composants du système de sécurité.

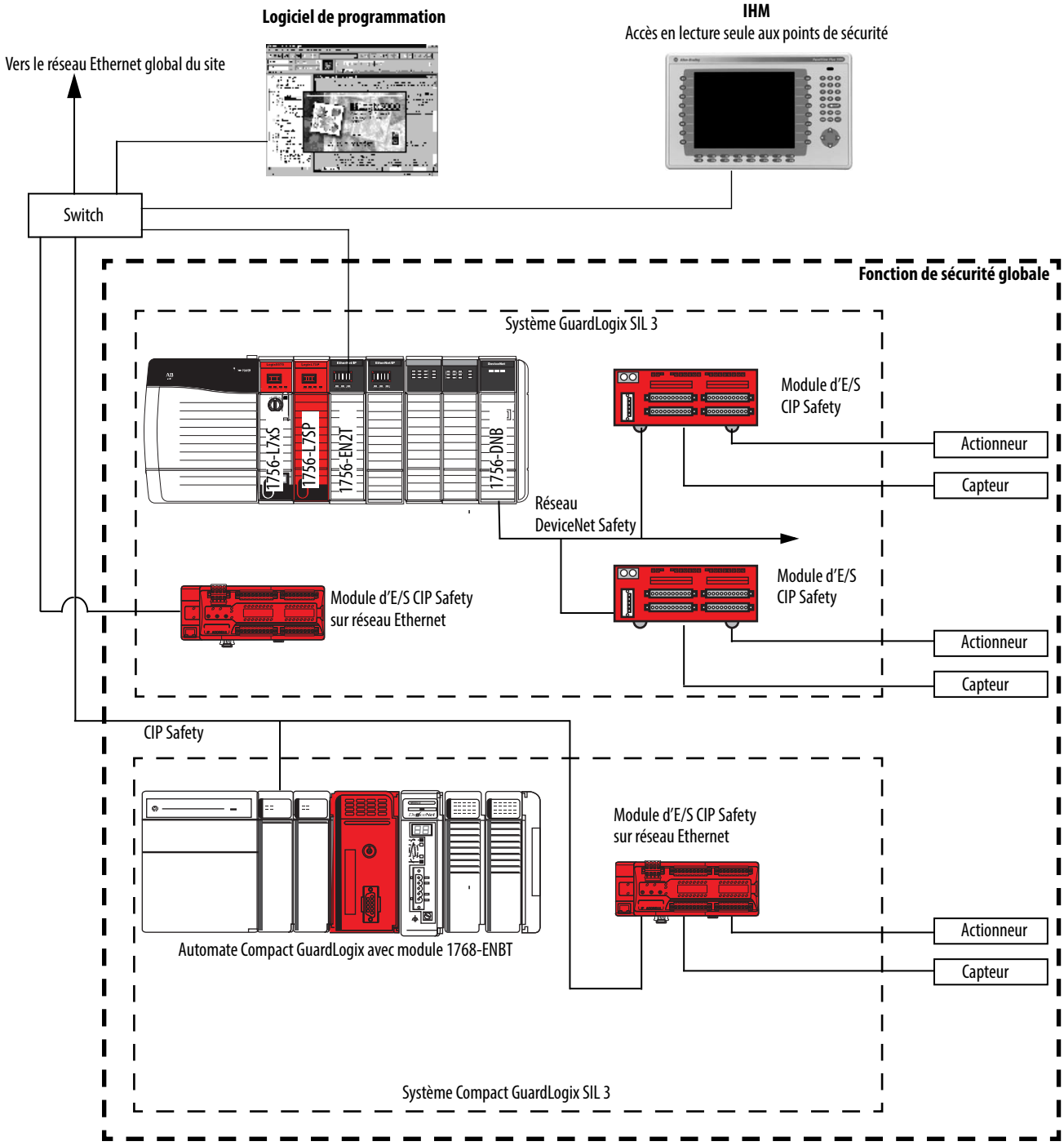
IMPORTANT La fréquence à laquelle les tests de vérification doivent être effectués est fonction de la spécificité de vos applications. Toutefois, elle est principalement déterminée par les dispositifs d'E/S de sécurité et l'instrumentation de terrain.

Architecture GuardLogix pour les applications SIL 3

L'illustration ci-dessous présente une fonction SIL typique, incluant les éléments suivants :

- la fonction de sécurité globale ;
- la partie GuardLogix de cette fonction de sécurité globale ;
- le mode de raccordement des autres dispositifs (comme les IHM) utilisés à l'extérieur de la fonction.

Figure 1 – Fonction SIL typique



Composants du système GuardLogix

Les tableaux présentés dans ce paragraphe répertorient les composants GuardLogix certifiés SIL 3, ainsi que les composants non certifiés SIL 3 qui peuvent être utilisés avec des systèmes GuardLogix SIL 3.

Pour obtenir la toute dernière liste des séries certifiées et des versions de firmware des automates GuardLogix et des dispositifs d'E/S CIP Safety, allez à l'adresse http://www.rockwellautomation.com/products/certification/safety/. Les versions de firmware sont disponibles à l'adresse http://support.rockwellautomation.com/ControlFLASH™/.

Tableau 2 – Composants GuardLogix certifiés SIL 3

Type d'équipement	Référence	Description	Documentation[3] connexe	
			Notice d'installation	Manuel utilisateur
Automate principal 1756 GuardLogix (ControlLogix5570S)	1756-L71S	Automate avec 2 Mo de mémoire standard et 1 Mo de mémoire de sécurité	–[4]	• Avec environnement Studio 5000 en version 21 ou supérieure : 1756-UM022 • Avec logiciel RSLogix 5000 en version 20 ou supérieure : 1756-UM020
	1756-L72S	Automate avec 4 Mo de mémoire standard et 2 Mo de mémoire de sécurité		
	1756-L73S	Automate avec 8 Mo de mémoire standard et 4 Mo de mémoire de sécurité		
	1756-L73SXT	Automate (XT) avec 8 Mo de mémoire standard et 4 Mo de mémoire de sécurité		
Partenaire de sécurité GuardLogix 1756 (ControlLogix557SP)	1756-L7SP	Partenaire de sécurité		
	1756-L7SPXT	Partenaire de sécurité (XT)		
Automate principal 1756 GuardLogix (ControlLogix5560S)[1]	1756-L61S	Automate avec 2 Mo de mémoire standard et 1 Mo de mémoire de sécurité	–[4]	1756-UM020
	1756-L62S	Automate avec 4 Mo de mémoire standard et 1 Mo de mémoire de sécurité		
	1756-L63S	Automate avec 8 Mo de mémoire standard et 3,75 Mo de mémoire de sécurité		
Partenaire de sécurité GuardLogix 1756 (ControlLogix55SP)[1]	1756-LSP	Partenaire de sécurité		
Automate Compact GuardLogix 1768 (CompactLogix4xS)[2]	1768-L43S	Automate prenant en charge deux modules 1768	–[4]	1768-UM002
	1768-L45S	Automate prenant en charge quatre modules 1768		
Modules d'E/S CIP Safety sur réseaux DeviceNet	Pour une liste à jour des séries certifiées et des versions de firmware, consultez le certificat de sécurité à l'adresse http://www.rockwellautomation.com/products/certification/safety/		1791DS-IN001 1791DS-IN002 1732DS-IN001	1791DS-UM001
Modules d'E/S CIP Safety sur réseaux EtherNet/IP			1791ES-IN001	1791ES-UM001
Modules d'E/S POINT Guard I/O			–[4]	1734-UM013
Servovariateurs Kinetix 5500 (références qui se terminent par -ERS2)	Pour une liste à jour des séries certifiées et des versions de firmware, consultez le certificat de sécurité à l'adresse http://www.rockwellautomation.com/products/certification/safety/		2198-IN001	2198-UM001

(1) Certifié pour une utilisation avec le logiciel RSLogix 5000 en versions 14, 16 et supérieure.
(2) Certifié pour une utilisation avec le logiciel RSLogix 5000 en version 18 et supérieure.
(3) Ces documentations peuvent être obtenues sur le site Rockwell Automation http://www.rockwellautomation.com/literature.
(4) Reportez-vous au manuel utilisateur pour les instructions d'installation.

Tableau 3 – Composants utilisables avec les systèmes de sécurité basés sur l'automate GuardLogix 1756

Type d'équipement	Référence	Description	Série[1]	Révision[1]	Documentation[3] connexe	
					Notice d'installation	Manuel utilisateur
Châssis	1756-A4 1756-A7 1756-A10 1756-A13 1756-A17	Châssis à 4 logements Châssis à 7 logements Châssis à 10 logements Châssis à 13 logements Châssis à 17 logements	B	–	1756-IN005	–
	1756-A4LXT 1756-A5XT 1756-A7XT 1756-A7LXT	Châssis XT à 4 logements Châssis XT à 5 logements Châssis XT à 7 logements Châssis XT à 7 logements	B	–		
Alimentation	1756-PA72	Alimentation c.a.	C	–	1756-IN005	–
	1756-PB72	Alimentation c.c.	C			
	1756-PA75	Alimentation c.a.	B			
	1756-PB75	Alimentation c.c.	B			
	1756-PAXT	Alimentation c.a. type XT	B			
	1756-PBXT	Alimentation c.c. type XT	B			
Modules de communication	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR 1756-EN3TR	Passerelle Ethernet/IP	A A A C B	3.006 2.005 2.005 10.007 10.007	ENET-IN002	ENET-UM001
	1756-EN2TXT 1756-EN2TRXT	Passerelle EtherNet/IP XT (câblage cuivre)	C C	5.007 10.006		
	1734-AENT	Adaptateur Ethernet POINT I/O	A	3.001	1734-IN590	1734-UM011
	1756-DNB	Passerelle DeviceNet	A	6.002	DNET-IN001	DNET-UM004
	1756-CN2	Passerelle ControlNet	A	12.001	CNET-IN005	CNET-UM001
	1756-CN2R	Passerelle ControlNet, redondante	A	12.001		
	1756-CN2RXT	Passerelle ControlNet XT, redondante	B	20.020		
Logiciel de programmation	9324-*xxxx*	Logiciel RSLogix 5000 pour automates GuardLogix 5560	–	14[2]	–	Consulter l'aide en ligne.
		Logiciel RSLogix 5000 pour automates GuardLogix 5570 (XT)		20		
	9324-*xxxx*	Environnement Studio 5000 pour automates GuardLogix 5570 (XT)		21		
Cartes mémoire	1784-CF128	Carte CompactFlash 128 Mo pour automates GuardLogix 5560	–	–	–	–
	1784-SD1	Carte SD (Secure Digital) 1 Go pour automates GuardLogix 5570				
	1784-SD2	Carte SD (Secure Digital) 2 Go pour automates GuardLogix 5570				

(1) Cette version ou une version ultérieure.
(2) La version 15 du logiciel RSLogix 5000 ne prend pas en charge les automates de sécurité GuardLogix.
(3) Ces documentations peuvent être obtenues sur le site Rockwell Automation http://www.rockwellautomation.com/literature.

Les logements de châssis d'un système SIL 3 qui ne sont pas utilisés par le système GuardLogix SIL 3 peuvent être occupés par d'autres modules ControlLogix (1756) conformes aux Directives Basse Tension et CEM.

IMPORTANT Les composants d'un système ControlLogix-XT™ sont compatibles avec des conditions environnementales extrêmes seulement lorsqu'ils sont utilisés de manière appropriée avec d'autres composants système Logix-XT. L'utilisation de composants ControlLogix-XT avec des composants système ControlLogix ou GuardLogix conventionnels annule l'homologation pour les environnements extrêmes.

Pour trouver les certificats applicables à la famille des produits ControlLogix, consultez la rubrique « Programmable Control-ControlLogix Product Family » sur la page http://www.rockwellautomation.com/products/certification/ce/.

Certifications GuardLogix

La publication 1756-TD001, « ControlLogix Controllers Technical Data », répertorie les caractéristiques techniques des produits ainsi que les organismes de certification par lesquels ces produits sont approuvés. Si un produit a été certifié par l'un de ces organismes, son étiquette en porte la marque. Pour les déclarations de conformité, les certificats et autres informations de certification, consultez le lien Product Certification (homologation produit) à l'adresse http://www.rockwellautomation.com/products/certification/.

Spécifications PFD et PFH de GuardLogix

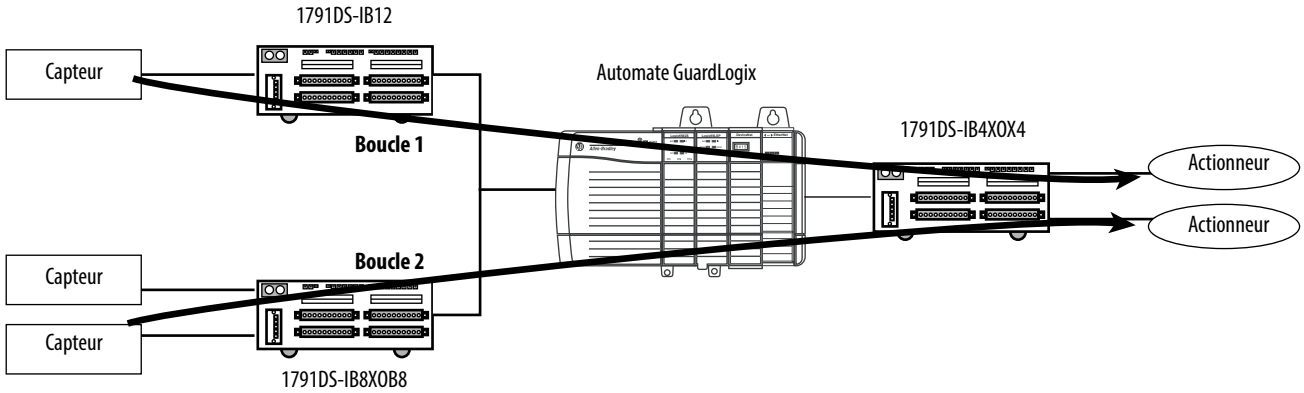
Les systèmes de sécurité peuvent être différenciés selon qu'ils fonctionnent en mode de faible sollicitation ou en mode de forte sollicitation/mode continu. La norme CEI 61508 quantifie cette classification en définissant la fréquence des sollicitations de fonctionnement du système de sécurité : moins d'une par an en mode de faible sollicitation ou plus d'une par an pour le mode de forte sollicitation/continu.

La valeur du niveau d'intégrité de sécurité (SIL) d'un système de sécurité de faible sollicitation est directement liée aux plages d'ordre de grandeur de sa probabilité moyenne de défaillance au cours de l'exécution correcte de sa fonction de sécurité sur sollicitation ou, plus simplement, de sa probabilité de défaillance sur sollicitation (PFD). La valeur SIL pour les systèmes de sécurité fonctionnant en mode de forte sollicitation/continu est directement liée à sa probabilité de défaillance dangereuse par heure (PFH).

Les valeurs PFD et PFH sont associées aux trois principaux éléments qui constituent un système de sécurité (les détecteurs, l'élément logique et les actionneurs). Dans l'élément logique, il y a également les entrées, le processeur et les sorties.

Pour les valeurs PFD et PFH ainsi que les intervalles entre les tests de vérification pour les modules d'E/S Guard I/O, voir Annexe E, Données de sécurité des systèmes GuardLogix.

Figure 2 – Exemple de PFH



Pour déterminer la valeur PFH de l'élément logique pour chaque boucle de sécurité dans l'exemple de système simple qui est présenté dans la section Exemple de PFH, additionnez les valeurs PFH de chaque composant de la boucle. Le tableau Équations PFH par boucle de sécurité fournit un exemple simplifié de calcul du PFH pour chacune des boucles de sécurité qui sont présentées dans le schéma d'exemple de PFH.

Tableau 4 – Équations PFH par boucle de sécurité

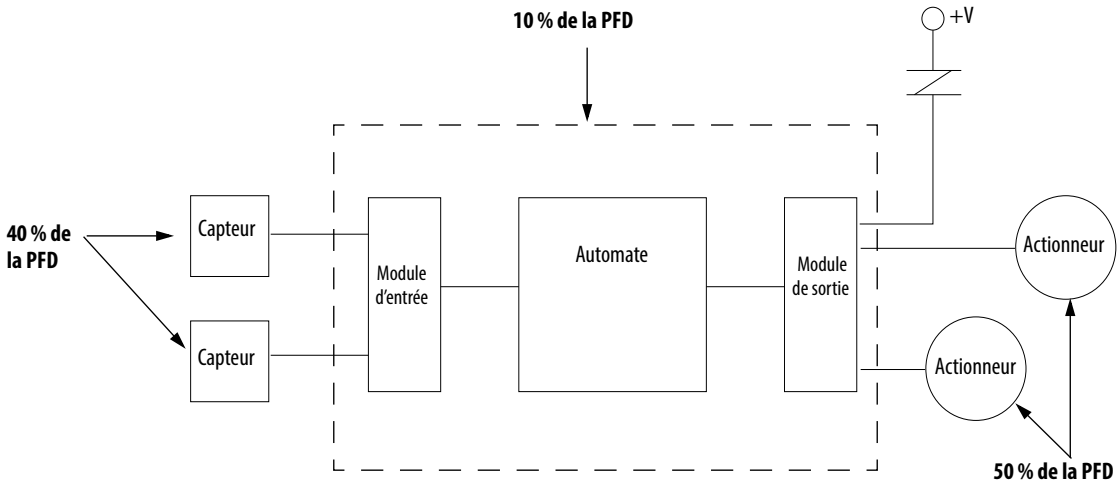
Pour cette boucle	Additionner les valeurs PFH de ces composants
PFH totale de la boucle 1 =	1791DS-IB12 + automate GuardLogix + 1791DS-IB4X0X4
PFH totale de la boucle 2 =	1791DS-IB8X0B8 + automate GuardLogix + 1791DS-IB4X0X4

Lors du calcul des valeurs PFH, vous devez prendre en compte les impératifs propres à votre application, y compris la périodicité des tests.

Répartition et poids de la conformité au niveau d'intégrité de sécurité (SIL)

On peut raisonnablement considérer que l'automate GuardLogix et le système d'E/S contribuent pour 10 % à la charge de fiabilité. Un système SIL 3 peut requérir l'incorporation de plusieurs entrées pour les détecteurs et les dispositifs d'entrées critiques, ainsi que des sorties doubles connectées en série à deux actionneurs, selon le niveau SIL évalué pour le système de sécurité.

Figure 3 – Charge de fiabilité



Temps de réponse du système

Le temps de réponse du système est le laps de temps qui s'écoule entre le moment où un événement relatif à la sécurité intervient au niveau d'une entrée du système et le moment où le système bascule les sorties correspondantes à leur état de sécurité. Les défauts présents dans le système peuvent également influer sur le temps de réponse du système. Le temps de réponse du système correspond à la somme des temps de réponse suivants.

Temps de réponse du détecteur + Temps de réponse de l'entrée + Temps de réponse de la tâche de sécurité + Temps de réponse de la sortie + Temps de réponse de l'actionneur

Chaque temps de réponse dépend de facteurs tels que le type de dispositif d'E/S et les instructions qui sont utilisées dans le programme.

Temps de réponse de la tâche de sécurité

Le temps de réponse de la tâche de sécurité correspond au délai le plus long entre la modification d'une entrée qui est présentée à l'automate et l'activation de la sortie traitée par le producteur de sortie. Il est inférieur ou égal à la somme de la période de la tâche de sécurité et du chien de garde de la tâche de sécurité.

Période de la tâche de sécurité et chien de garde de la tâche de sécurité

La période de la tâche de sécurité est l'intervalle auquel la tâche de sécurité est exécutée.

La durée du chien de garde de la tâche de sécurité est la durée maximale autorisée pour le traitement de la tâche de sécurité. Si le temps de traitement de la tâche de sécurité dépasse la durée du chien de garde de la tâche de sécurité, un défaut de sécurité irrécupérable se produit dans l'automate et les sorties passent automatiquement en état de sécurité (désactivées).

C'est vous qui définissez la durée du chien de garde de la tâche de sécurité, laquelle doit être inférieure ou égale à la période de la tâche de sécurité.

La temporisation du chien de garde de la tâche de sécurité est définie dans la fenêtre des propriétés de tâche de l'application Logix Designer. Cette valeur peut être modifiée en ligne, quel que soit le mode de l'automate, mais ne peut pas être changée une fois qu'il est verrouillé en sécurité ou lorsqu'une signature de tâche de sécurité est créée.

Qui contacter en cas de défaillance du dispositif

Si vous constatez un défaut sur n'importe quel dispositif certifié SIL 3, contactez votre distributeur local Allen-Bradley pour engager les actions suivantes :

- retour du dispositif à Rockwell Automation afin que le défaut soit enregistré de façon appropriée en regard de la référence produit concernée ;
- demande (si nécessaire) d'une analyse de ce défaut pour essayer d'en déterminer la cause.

Système automate GuardLogix

Sujet	Page
Configuration matérielle d'un automate GuardLogix 5570	21
Protocole CIP Safety	22
Dispositifs d'E/S de sécurité	23
Passerelles de communication	23
Présentation de la programmation	25

Pour obtenir une liste succincte des composants utilisables dans les applications de niveau SIL 3, reportez-vous au tableau de la page 16. Pour des informations plus détaillées et à jour, allez à l'adresse http://www.rockwellautomation.com/products/certification/safety/.

Lors de l'installation d'un automate GuardLogix 5570, suivez les instructions de la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur ».

Configuration matérielle d'un automate GuardLogix 5570

L'automate GuardLogix se compose d'un automate principal (ControlLogix 557*x*S) et de son partenaire de sécurité (ControlLogix 557SP). Ces deux modules sont organisés entre eux selon une architecture « 1oo2 », de façon à constituer un automate compatible SIL 3. Ils sont décrits dans les sections suivantes.

L'automate principal et le partenaire de sécurité exécutent des tests de diagnostic fonctionnel sur tous les composants de sécurité de l'automate lors de la mise sous tension et pendant le fonctionnement.

Pour plus d'informations sur le fonctionnement des voyants d'état, reportez-vous à la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur ».

IMPORTANT	Les voyants d'état ne sont pas des indicateurs fiables en ce qui concerne les fonctions de sécurité. Ne les utilisez que pour des diagnostics généraux pendant la mise en service ou le dépannage. Ne tentez pas d'utiliser les voyants pour déterminer l'état de fonctionnement.

Pour la liste des références des automates de sécurité GuardLogix, reportez-vous au Tableau 2, page 16. Pour la liste des composants ControlLogix standard compatibles avec les applications de sécurité, voir le Tableau 3, page 17.

Automate principal

L'automate principal est le processeur qui exécute les fonctions de commande standard et de sécurité et qui communique avec le partenaire de sécurité pour les fonctions de sécurité du système automate GuardLogix. L'automate principal comprend un processeur central, une interface d'E/S et une mémoire.

Partenaire de sécurité

Pour satisfaire aux exigences SIL 3, le partenaire de sécurité doit être installé dans le logement situé immédiatement à droite de l'automate principal. Le partenaire de sécurité est un coprocesseur qui assure une redondance pour les fonctions de sécurité du système.

L'automate principal configure le partenaire de sécurité. Un seul chargement du programme utilisateur vers l'automate principal est nécessaire. Le mode de fonctionnement du partenaire de sécurité est commandé par l'automate principal.

Châssis

Le châssis assure les connexions physiques entre les modules et le système GuardLogix 1756. Dans le cas improbable d'une défaillance, celle-ci sera détectée par un ou plusieurs composants actifs du système. C'est pourquoi, le châssis n'est pas pris en compte dans les questions relatives à la sécurité.

Les automates GuardLogix-XT™ doivent utiliser un châssis ControlLogix-XT pour satisfaire aux exigences d'environnement extrême.

Alimentations

Aucune configuration ou câblage supplémentaire n'est requis pour le fonctionnement des alimentations ControlLogix dans des applications SIL 3. Dans le cas d'une défaillance, celle-ci sera détectée par un ou plusieurs composants actifs du système GuardLogix. C'est pourquoi l'alimentation n'est pas prise en compte dans les questions relatives à la sécurité.

Les automates GuardLogix-XT doivent utiliser une alimentation ControlLogix-XT pour satisfaire aux exigences d'environnement extrême.

Protocole CIP Safety

Les communications de sécurité entre les automates GuardLogix s'effectuent par des points de sécurité produits et consommés. Ces points de sécurité utilisent le protocole CIP Safety, conçu pour préserver l'intégrité des données pendant la communication.

Pour de plus amples informations sur les points de sécurité, reportez-vous au Chapitre 5, Caractéristiques des points de sécurité, de la tâche de sécurité et des programmes de sécurité.

Dispositifs d'E/S de sécurité

Pour de plus amples informations sur les dispositifs d'E/S CIP Safety utilisables avec les automates GuardLogix, reportez-vous au Chapitre 3.

Passerelles de communication

Le Tableau 5 récapitule les modules d'interface de communication disponibles pour faciliter les communications en réseau EtherNet/IP, DeviceNet ou ControlNet au moyen du protocole CIP Safety.

Tableau 5 – Modules d'interface de communication par système

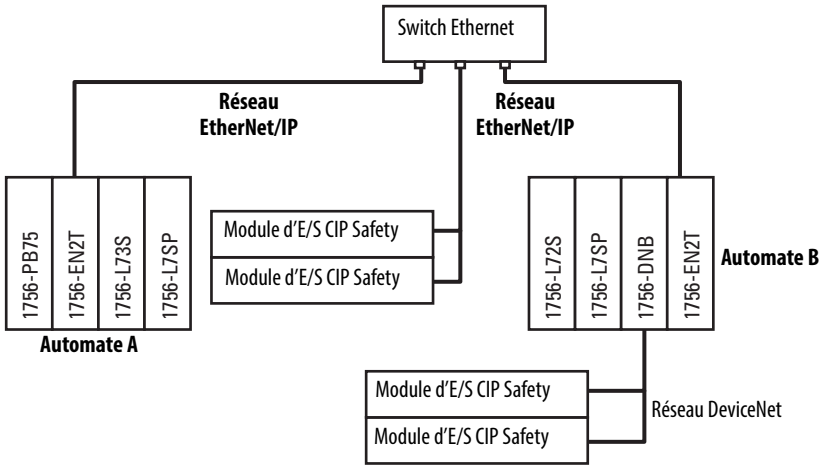
Système GuardLogix	Modules de communication
1756	• Passerelle EtherNet/IP 1756-ENBT, 1756-EN2T(R), 1756-EN2F ou 1756-EN3TR • Adaptateur Ethernet POINT I/O 1734-AENT • Passerelle DeviceNet 1756-DNB • Passerelle ControlNet 1756-CN2 • Passerelle ControlNet 1756-CN2R redondante
1756 -XT	• Passerelle EtherNet/IP 1756-EN2TXT 1756EN2TRXT – XT (câblage cuivre) • Passerelle ControlNet XT redondante 1756-CN2RXT
1768	• 1768-ENBT • Adaptateur Ethernet POINT I/O 1734-AENT • 1768-CNB • 1768-CNBR

IMPORTANT En raison de la conception du système de commande CIP Safety, il n'est pas nécessaire que les passerelles CIP Safety, telles que celles répertoriées dans le tableau, soient certifiées SIL 3.

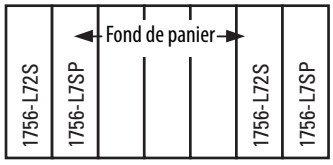
Réseau EtherNet/IP

Les communications de sécurité d'égal à égal entre automates GuardLogix sont réalisables en réseau EtherNet/IP grâce à l'utilisation de passerelles EtherNet/IP. Une passerelle EtherNet/IP permet à l'automate GuardLogix de contrôler et d'échanger des données de sécurité avec les dispositifs d'E/S CIP Safety sur un réseau EtherNet/IP.

Figure 4 – Communications d'égal à égal au moyen de passerelles EtherNet/IP et d'un réseau EtherNet/IP



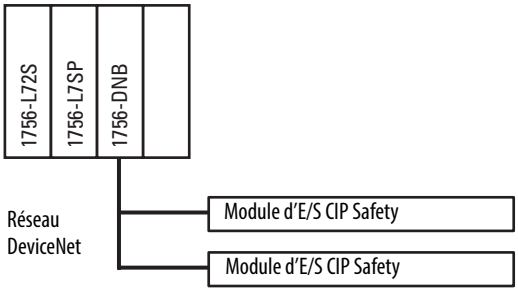
CONSEIL Des communications de sécurité d'égal à égal entre deux automates GuardLogix montés dans un même châssis sont également possibles par l'intermédiaire du bus intermodules.



Réseau DeviceNet Safety

Les passerelles DeviceNet permettent à un automate GuardLogix de contrôler et d'échanger des données de sécurité avec des modules d'E/S CIP Safety sur un réseau DeviceNet.

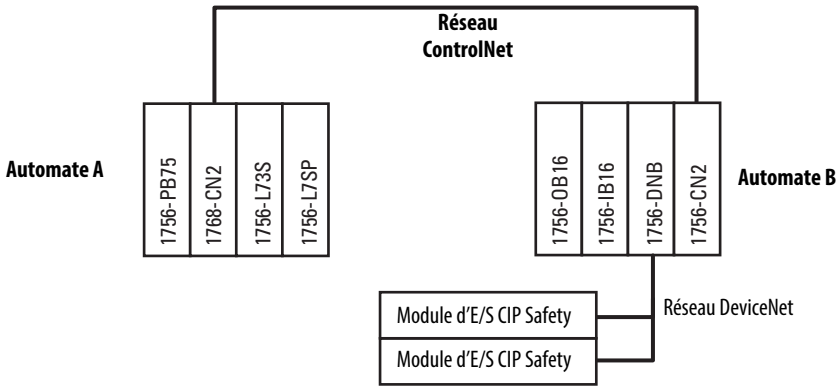
Figure 5 – Communications par l'intermédiaire d'une passerelle DeviceNet



Réseau ControlNet

Les passerelles ControlNet permettent à un automate GuardLogix de produire et de consommer à travers des réseaux ControlNet des points de sécurité en direction d'autres automates GuardLogix ou de réseaux d'E/S CIP Safety distants.

Figure 6 – Communications par l'intermédiaire d'une passerelle ControlNet



Présentation de la programmation

La programmation des automates GuardLogix 5570 s'effectue au moyen de l'application Logix Designer de Studio 5000.

Utilisez l'application Logix Designer pour définir l'emplacement, les règles de propriété et la configuration des dispositifs d'E/S et des automates, ou pour créer, tester et déboguer un programme logique. Seul le langage en logique à relais est pris en charge pour la tâche de sécurité GuardLogix.

Se reporter à l'Annexe A pour plus d'informations sur le jeu d'instructions logiques utilisables dans les projets de sécurité.

Le personnel habilité peut modifier un programme de sécurité, à condition d'utiliser l'une des procédures décrites au paragraphe Modification de votre application de sécurité, page 59.

Notes :

E/S CIP Safety pour le système de commande GuardLogix

Sujet	Page
Présentation	27
Fonctions de sécurité typiques des dispositifs d'E/S CIP Safety	27
Temps de réponse	28
Conditions de sécurité des dispositifs d'E/S CIP Safety	29

Présentation

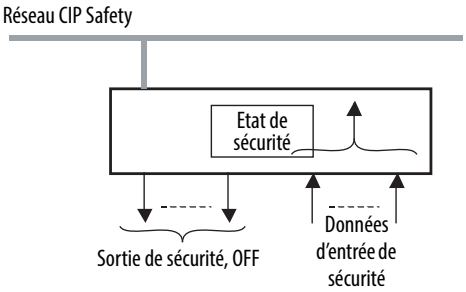
Avant d'utiliser un système de sécurité GuardLogix 5570 qui contient des dispositifs d'E/S CIP Safety, veuillez lire, assimiler et suivre les recommandations d'installation, d'exploitation et de sécurité qui sont formulées dans les documentations citées dans les tableaux Composants GuardLogix certifiés SIL 3, page 16.

Les dispositifs d'E/S CIP Safety peuvent être connectés à des dispositifs d'entrées et de sorties de sécurité, tels que des capteurs et actionneurs, qui permettent à ces dispositifs d'être surveillés et commandés par l'automate GuardLogix. Concernant les données de sécurité, les communications d'E/S utilisent le protocole CIP Safety par l'intermédiaire de connexions de sécurité. Le programme de sécurité est exécuté par l'automate GuardLogix.

Fonctions de sécurité typiques des dispositifs d'E/S CIP Safety

Ce qui suit est considéré comme l'état de sécurité par les dispositifs d'E/S CIP Safety :

- sorties de sécurité : OFF (désactivées) ;
- données d'entrées de sécurité dans l'automate : OFF (désactivées)



Les dispositifs d'E/S CIP Safety sont à utiliser dans les applications prévues pour passer à l'état de sécurité lorsque la sortie de sécurité passe à OFF.

Diagnostics

Les dispositifs d'E/S CIP Safety exécutent des autodiagnostics à la mise sous tension et à intervalles réguliers pendant le fonctionnement. En cas de détection d'une défaillance lors d'un diagnostic, les données d'entrées de sécurité (vers l'automate) et les sorties de sécurité locales sont réglées sur leur état de sécurité (OFF).

Données d'état

Outre les données d'entrée et de sortie de sécurité, les dispositifs d'E/S CIP Safety gèrent les données d'état pour surveiller l'état des circuits d'E/S et des dispositifs. Pour connaître les spécificités du produit, reportez-vous à la documentation de votre dispositif.

Voyants d'état

Les dispositifs d'E/S CIP Safety comportent des voyants d'état. Pour de plus amples informations sur le fonctionnement de ces voyants, reportez-vous à la documentation de votre dispositif.

Temporisation à l'enclenchement ou au déclenchement

Certains dispositifs d'E/S CIP Safety peuvent prendre en charge les fonctions de temporisation à l'enclenchement ou au déclenchement pour les signaux d'entrée. Selon votre application, vous devrez peut-être inclure une temporisation au déclenchement, à l'enclenchement ou les deux lorsque vous calculez le temps de réponse du système.

Pour des informations sur le temps de réponse du système, reportez-vous à l'Annexe C.

Temps de réponse

Le temps de réponse de l'entrée est le laps de temps qui s'écoule entre le moment où le signal change au niveau d'une borne d'entrée et le moment où les données de sécurité sont envoyées à l'automate GuardLogix.

Le temps de réponse de la sortie est le laps de temps qui s'écoule entre le moment où les données de sécurité sont reçues de l'automate GuardLogix et le moment où la borne de sortie change d'état.

Pour de plus amples informations sur le calcul des temps de réponse des entrées et des sorties, reportez-vous à la documentation de votre dispositif d'E/S CIP Safety.

Pour des informations sur le calcul du temps de réponse du système, reportez-vous à l'Annexe C.

Conditions de sécurité des dispositifs d'E/S CIP Safety

Vous devez définir l'adresse de station ou l'adresse IP et, s'il y a lieu, la vitesse de transmission de chaque dispositif avant de les installer sur un réseau de sécurité.

Propriété

Chaque dispositif d'E/S CIP Safety dans un système GuardLogix est géré par un automate GuardLogix. Plusieurs automates GuardLogix et plusieurs dispositifs d'E/S CIP Safety peuvent être utilisés sans restriction dans un châssis ou sur des réseaux, le cas échéant. Lorsqu'un automate est propriétaire d'un dispositif d'E/S, il stocke les données de configuration de ce dernier, telles que définies par l'utilisateur. Ceci détermine le mode de fonctionnement des dispositifs dans le système.

En termes de commande, les dispositifs de sortie de sécurité ne peuvent être commandés que par un seul automate. Chaque dispositif d'entrée de sécurité est également géré par un seul automate. Néanmoins, les données d'entrée de sécurité peuvent être partagées (consommées) par plusieurs automates GuardLogix.

Signature de configuration des E/S de sécurité

La signature de configuration définit la configuration du dispositif. Elle peut être lue et surveillée. La signature de configuration sert à identifier de façon unique la configuration d'un dispositif. Lorsque vous utilisez un automate GuardLogix, vous n'avez pas besoin de surveiller cette signature. L'automate GuardLogix surveille automatiquement la signature.

Remplacement des dispositifs d'E/S de sécurité

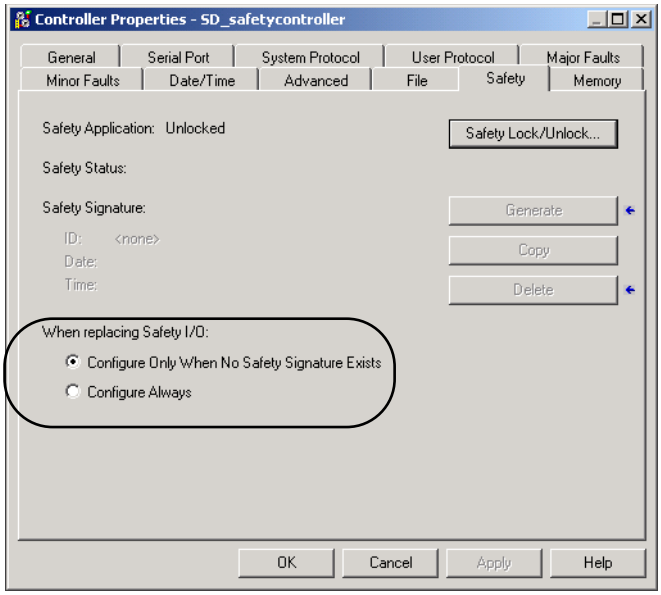
Le remplacement des dispositifs de sécurité requiert que le dispositif de remplacement soit correctement configurer et que son fonctionnement soit vérifié par l'utilisateur.

ATTENTION : pendant le remplacement ou le test fonctionnel d'un dispositif, la sécurité du système ne doit pas reposer sur une quelconque partie du dispositif en cause.

Deux options sont proposées pour le remplacement d'un dispositif d'E/S dans l'onglet Safety (Sécurité) de la boîte de dialogue Controller Properties (Propriétés de l'automate) de l'application Logix Designer :

- Configure Only When No Safety Signature Exists (Configurer uniquement lorsqu'il n'existe pas de signature de sécurité)
- Configure Always (Toujours configurer)

Figure 7 – Options de remplacement d'E/S de sécurité



Configurer uniquement lorsqu'il n'existe pas de signature de sécurité

Ce réglage indique à l'automate GuardLogix qu'il doit configurer un dispositif de sécurité seulement si la tâche de sécurité n'a pas de signature de tâche de sécurité, et si le dispositif de rechange est dans sa configuration d'usine, c'est-à-dire qu'il n'existe pas de numéro de réseau de sécurité dans le dispositif de sécurité.

Si la tâche de sécurité possède une signature de tâche de sécurité, l'automate GuardLogix configure uniquement le dispositif d'E/S CIP Safety de rechange si les conditions suivantes sont remplies :

- le dispositif possède déjà un numéro de réseau de sécurité conforme ;
- le détrompage électronique du dispositif est conforme ;
- l'adresse de station ou l'adresse IP est conforme.

Toujours configurer

L'automate GuardLogix tente toujours de configurer un dispositif d'E/S CIP Safety de rechange si le dispositif est dans sa configuration d'usine, c'est-à-dire qu'il ne possède pas de numéro de réseau de sécurité et que le numéro de station ainsi que le détrompage du dispositif d'E/S correspondent à la configuration de l'automate.

ATTENTION : activez la fonction Configure Always (Toujours configurer) seulement si l'ensemble du système de commande CIP Safety routable n'est pas chargé de maintenir la sécurité SIL 3 pendant le remplacement et le test fonctionnel d'un dispositif.

Si d'autres parties du système de commande CIP Safety sont chargées de maintenir le niveau SIL 3, assurez-vous que l'option Configure Always (Toujours configurer) de l'automate est désactivée.

Il vous incombe de mettre en œuvre un processus afin de veiller à ce que la fonction de sécurité appropriée soit maintenue pendant le remplacement d'un dispositif.

ATTENTION : n'incorporez pas de dispositifs sortant directement de leur emballage dans un réseau CIP Safety lorsque la fonctionnalité Configure Always (Toujours configurer) est active, à moins de respecter scrupuleusement la procédure de remplacement de dispositif décrite dans la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur ».

Notes :

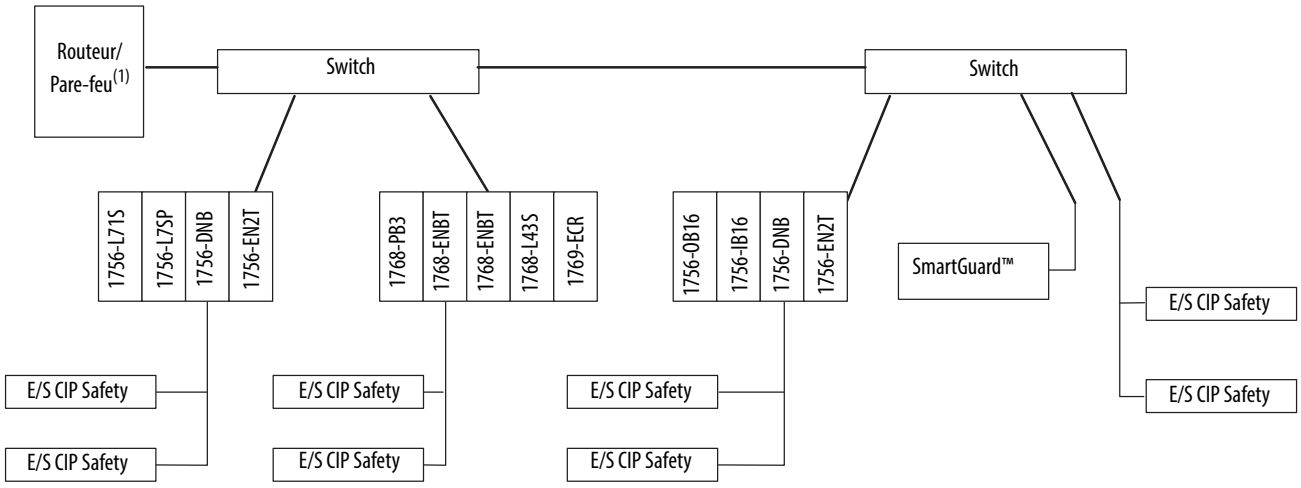
CIP Safety et numéro de réseau de sécurité

Sujet	Page
Système de commande CIP Safety routable	33
Remarques sur l'attribution du numéro de réseau de sécurité (SNN)	35

Système de commande CIP Safety routable

Pour comprendre les prescriptions de sécurité d'un système de commande CIP Safety et notamment le numéro de réseau de sécurité (SNN pour Safety Network Number), vous devez d'abord comprendre comment les informations sont acheminées dans les systèmes de commande CIP. Le système de commande CIP Safety est constitué d'un ensemble de dispositifs CIP Safety interconnectés. Le système routable représente le volume d'erreurs potentielles d'acheminement de trames d'un équipement source vers une cible dans le système de commande CIP Safety. Le système est isolé de manière à ce qu'il n'y ait aucune autre connexion. Vous trouverez à la Figure 8 l'exemple d'un système qui ne peut pas être interconnecté à un autre système CIP Safety par une infrastructure Ethernet plus vaste couvrant tout le site, et qui illustre la portée d'un système CIP Safety routable.

Figure 8 – Exemple de système CIP Safety



(1) Le routeur ou le pare-feu est configuré pour limiter le trafic.

Référence de station unique

Le protocole CIP Safety est un protocole de sécurité entre stations terminales. Il permet l'échange de messages CIP Safety entre dispositifs CIP Safety via des passerelles, des switchs et des routeurs non certifiés.

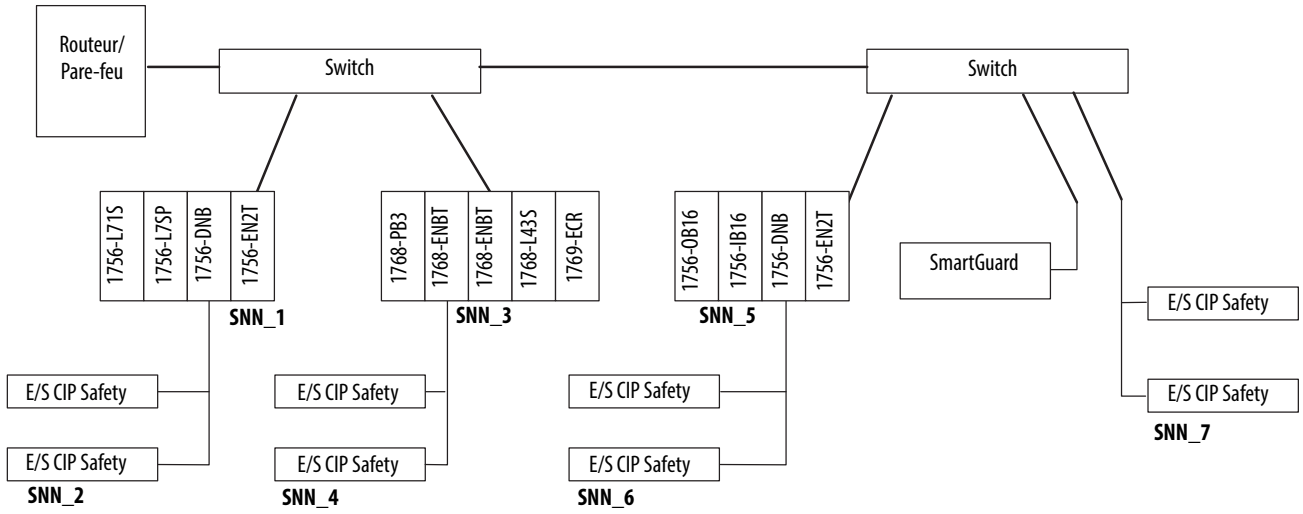
Pour éviter que les erreurs dans les passerelles, les switchs ou les routeurs non certifiés mettent en danger le système, chaque station terminale d'un système de commande CIP Safety routable doit avoir une référence de station unique. La référence de station unique regroupe un numéro de réseau de sécurité (SNN) et l'adresse de station de l'équipement sur le réseau.

Numéro de réseau de sécurité

Le numéro de réseau de sécurité (SNN) est attribué automatiquement par le logiciel ou manuellement par l'utilisateur. Chaque réseau CIP Safety qui contient des stations d'E/S de sécurité doit avoir au moins un SNN unique. Chaque châssis qui contient un ou plusieurs dispositifs de sécurité doit avoir au moins un SNN unique. Les numéros de réseau de sécurité qui sont attribués à chaque réseau ou sous-réseau de sécurité doivent être uniques.

CONSEIL Plusieurs numéros SNN peuvent être attribués à un sous-réseau CIP Safety ou à un châssis qui contient de multiples dispositifs de sécurité. Néanmoins, pour des raisons de simplicité, il est conseillé que chaque sous-réseau CIP Safety ait un, et un seul, SNN unique. Cette recommandation s'applique également à chaque châssis.

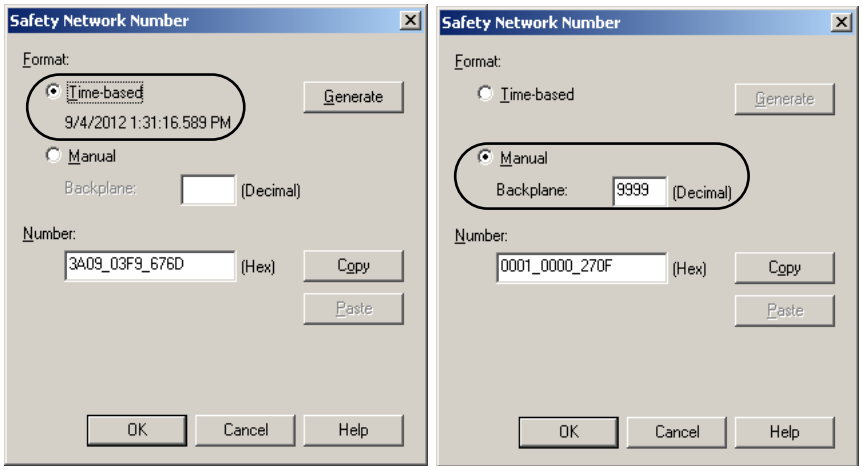
Figure 9 – Exemple de réseau CIP Safety ayant plusieurs SNN



Chaque dispositif CIP Safety doit être configuré avec un SNN. Tout dispositif qui établit une connexion de sécurité avec un autre dispositif de sécurité doit être configuré avec le SNN du dispositif cible. Si le système CIP Safety est en cours de démarrage avant que le test de sécurité fonctionnelle du système ne soit exécuté, le dispositif source peut être utilisé pour définir la référence de station unique du dispositif.

Le SNN utilisé par le système est un numéro hexadécimal à six octets. Le SNN peut être défini et affiché dans deux formats : temporel ou manuel. Si vous sélectionnez le format temporel, le SNN indique la date et l'heure locales. Si vous sélectionnez le format manuel, le SNN indique un type de réseau et une valeur hexadécimale comprise entre 1 et 9999.

Figure 10 – Formats de SNN



L'attribution d'un SNN temporel se fait automatiquement lorsque vous créez un projet d'automate de sécurité GuardLogix et que vous ajoutez de nouveaux dispositifs E/S de sécurité.

La définition manuelle d'un SNN est nécessaire dans les cas suivants :

- lorsque vous utilisez des points de sécurité consommés ;
- lorsque le projet consomme des données d'entrée de sécurité à partir d'un dispositif dont la configuration est gérée par un autre dispositif de sécurité ;
- lorsqu'un projet de sécurité est copié dans une installation matérielle différente à l'intérieur d'un même système CIP Safety routable.

IMPORTANT	Si vous attribuez manuellement un SNN, assurez-vous tout particulièrement que l'extension du système n'entraîne pas de doublons dans les combinaisons de SNN et d'adresse de station. La présence de doublons dans les combinaisons de SNN et d'adresse de station donne lieu à une erreur de vérification.

Remarques sur l'attribution du numéro de réseau de sécurité (SNN)

L'attribution du SNN dépend de facteurs tels que la configuration de l'automate ou du dispositif d'E/S CIP Safety.

Numéro de réseau de sécurité (SNN) pour points de sécurité consommés

Lorsque vous ajoutez un automate de sécurité contenant des points de sécurité produits à l'arborescence de configuration des E/S, vous devez entrer le SNN de l'automate producteur. Vous pouvez copier le SNN à partir du projet de l'automate producteur et le coller dans le nouvel automate ajouté à la configuration des E/S.

Reportez-vous à la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur », pour toute information sur la manière de copier/coller un SNN.

Numéro de réseau de sécurité (SNN) pour dispositifs en configuration d'usine

Les dispositifs d'E/S CIP Safety en configuration d'usine n'ont pas de SNN. Le SNN est défini lorsqu'une configuration est transmise au dispositif par l'automate GuardLogix qui gère le dispositif.

IMPORTANT	Pour ajouter un dispositif d'E/S CIP Safety à un système GuardLogix configuré (un SNN étant présent dans l'automate GuardLogix), ce nouveau dispositif CIP Safety doit recevoir le SNN conforme avant de pouvoir être intégré au réseau CIP Safety.

Numéro de réseau de sécurité (SNN) pour dispositif de sécurité avec un propriétaire de configuration différent

Lorsqu'un dispositif d'E/S CIP Safety appartenant à un automate GuardLogix différent (automate B) est ajouté à un autre projet GuardLogix (projet d'automate A), l'application Logix Designer attribue le SNN en fonction du projet actif. Le projet actif (projet de l'automate A) n'étant pas le véritable propriétaire de la configuration, vous devrez alors copier le SNN original (celui du projet de l'automate B) dans la configuration du projet de l'automate A. Cela se fait facilement grâce aux commandes copier-coller standard. Il en résulte que le dispositif d'E/S CIP Safety produit simultanément des données vers deux automates GuardLogix. Vous pouvez effectuer un copier/coller pour 16 automates au maximum.

Reportez-vous à la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur », pour toute information sur la manière de modifier, copier et coller des numéros de réseau de sécurité.

Numéro de réseau de sécurité (SNN) lors de la copie d'un projet de sécurité

ATTENTION : si vous copiez un projet de sécurité pour l'utiliser dans un autre projet avec du matériel différent ou dans un autre endroit physique et si le nouveau projet se trouve dans le même système CIP Safety routable, vous devez modifier chaque SNN dans le deuxième système. Les valeurs SNN ne doivent pas être répétées.

Reportez-vous à la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur », pour toute information sur la modification d'un SNN.

Caractéristiques des points de sécurité, de la tâche de sécurité et des programmes de sécurité

Sujet	Page
Différence entre composants standard et de sécurité	37
Applications de sécurité SIL 2	38
Sécurité SIL 3 – tâche de sécurité	41
Utilisation d'interfaces homme-machine	43
Programmes de sécurité	45
Sous-programmes de sécurité	45
Points de sécurité	46

Différence entre composants standard et de sécurité

Comme il s'agit d'un automate appartenant à la famille Logix, des composants standard (sans fonction de sécurité) et des composants dédiés à la sécurité peuvent cohabiter dans un système de commande GuardLogix.

Vous pouvez exécuter des commandes d'automatisation standard à partir de tâches standard dans un projet GuardLogix. Les automates GuardLogix offrent les mêmes fonctionnalités que les automates des autres séries ControlLogix. Mais les automates GuardLogix se différencient des automates standard par le fait qu'ils proposent une tâche de sécurité compatible SIL 3.

Toutefois, il faut faire une distinction logique et visible entre les parties standard et les parties dédiées à la sécurité de l'application. L'application Logix Designer permet d'effectuer cette différenciation en définissant une tâche de sécurité, des programmes de sécurité, des sous-programmes de sécurité, des points de sécurité et des dispositifs d'E/S de sécurité. Vous pouvez mettre en œuvre les niveaux de sécurité SIL 2 et SIL 3 avec la tâche de sécurité de l'automate GuardLogix.

Applications de sécurité SIL 2

Vous pouvez réaliser un système de commande de sécurité de niveau SIL 2 en utilisant la tâche de sécurité de l'automate GuardLogix.

Comme les automates GuardLogix appartiennent à la famille des processeurs ControlLogix, vous pouvez réaliser un système de commande de sécurité SIL 2 avec un automate GuardLogix en utilisant des tâches standard ou la tâche de sécurité. Cette possibilité offre des options de commande de sécurité uniques et souples. La majorité des applications comporte en effet un pourcentage de fonctions de sécurité SIL 2 supérieur à celui des fonctions de sécurité SIL 3.

Commande de sécurité SIL 2 dans la tâche de sécurité

La tâche de sécurité d'un GuardLogix peut être utilisée pour assurer des fonctions de sécurité SIL 2 et SIL 3. Si des fonctions de sécurité SIL 3 doivent être réalisées en même temps que des fonctions de sécurité SIL 2, vous devez respecter les exigences définies dans les sections Sécurité SIL 3 – tâche de sécurité, Programmes de sécurité et Sous-programmes de sécurité de ce chapitre, ainsi que les exigences SIL 2 répertoriées dans cette section.

Programme de sécurité SIL 2

Du point de vue de la commande de sécurité GuardLogix, la principale différence entre les dispositifs de niveau SIL 2 et de niveau SIL 3 tient au fait que le niveau SIL 2 est généralement à simple voie, alors que le niveau SIL 3 est généralement à double voie. Lorsque des E/S de sécurité Guard I/O (modules rouges) sont utilisées, ce qui est obligatoire pour la tâche de sécurité, les entrées de sécurité SIL 2 peuvent être mono voie. Ceci contribue à limiter la complexité du système et le nombre de modules nécessaires.

Il appartient au concepteur du système de sécurité de mettre correctement en œuvre l'ensemble des fonctions de sécurité. Les facteurs suivants doivent être pris en compte :

- choix des dispositifs de terrain (sélection appropriée, identification et prévention de tous les défauts susceptibles d'affecter ces dispositifs) ;
- détermination du niveau d'exigence de sécurité (faible/CEI 61511 ou élevé/ISO 13849) ;
- détermination des intervalles de test (diagnostics et essais de vérification nécessaires pour satisfaire aux exigences de l'application) ;
- identification et justification par une documentation appropriée de toutes les éventuelles exclusions de défaut retenues.

IMPORTANT	En cas d'utilisation simultanée d'une combinaison de fonctions de sécurité SIL 2 et SIL 3 dans la tâche de sécurité, vous devez empêcher les signaux d'entrée SIL 2 de commander directement les fonctions de sécurité SIL 3. Utilisez des programmes ou des sous-programmes de tâche de sécurité spécifiques pour séparer les fonctions de sécurité SIL 2 et SIL 3.

Au niveau de la tâche de sécurité, l'application Logix Designer permet d'inclure un ensemble d'instructions de sécurité en logique à relais. Les automates GuardLogix comportent également des instructions de sécurité de niveau SIL 3 spécifiques aux applications. Toutes ces instructions logiques sont utilisables dans les fonctions de sécurité de Cat 1 à 4 et SIL 1 à 3.

La sécurité limitée au niveau SIL 2 ne requiert pas de signature de tâche de sécurité. En revanche, si des fonctions de sécurité SIL 3 sont mises en œuvre dans la tâche de sécurité, une signature de tâche de sécurité devient nécessaire.

Pour les applications SIL 2, le verrouillage de sécurité de la tâche de sécurité est recommandé à l'issue des tests. Le verrouillage de la tâche de sécurité active davantage de fonctions de sécurité. Vous pouvez également utiliser la protection de source des sous-programmes dans FactoryTalk® Security et Logix Designer pour limiter l'accès au programme de sécurité.

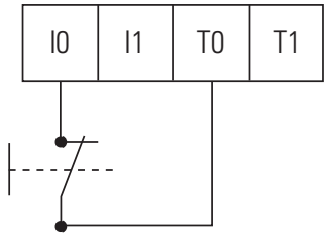
Pour plus d'informations sur la génération d'une signature de tâche de sécurité et le verrouillage de sécurité de cette tâche de sécurité, reportez-vous à la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur ».

Entrées de sécurité SIL 2

Les modules d'entrée de sécurité CompactBlock™ Guard I/O (Série 1791), ArmorBlock® Guard I/O (Série 1732) et POINT Guard I/O (Série 1734) acceptent les circuits d'entrée mono voie SIL 2. Ces modules étant également prévus pour un fonctionnement SIL 3, la combinaison de circuits de types SIL 2 et SIL 3 au niveau d'un même module est autorisée, à condition de respecter les recommandations ci-après.

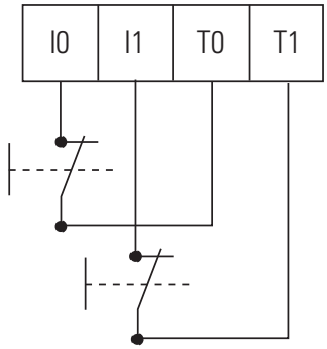
Ces deux exemples de câblage illustrent comment raccorder les circuits de sécurité SIL 2 aux modules d'entrée de sécurité Guard I/O. Ces exemples font appel à des sources de test intégrées (T0 à T*x*) qui résident sur tous les modules d'entrée de sécurité 1791 et 1732.

Figure 11 – Câblage des entrées



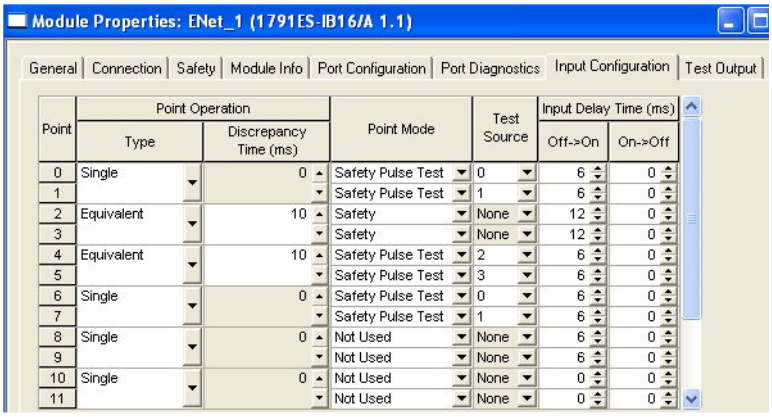
Les modules Guard I/O regroupent les entrées par paires afin de faciliter les fonctions de sécurité Cat. 3, Cat. 4 et SIL 3. Pour une mise en œuvre dans les fonctions de sécurité Cat. 1, Cat. 2 et SIL 2, les entrées de module doivent également être employées par paires comme illustré. Deux fonctions de sécurité SIL 2 sont présentées câblées aux entrées I0 et I1 en utilisant respectivement les sources de test T0 et T1.

Figure 12 – Câblage des entrées par paires



Concernant les fonctions de sécurité Cat. 1, Cat. 2, et SIL 2, les modules de sécurité Guard I/O ont besoin de configurations spécifiques dans le projet GuardLogix. Dans cet exemple, les entrées 0, 1, 6, 7, 8, 9, 10 et 11 font partie de la fonction de sécurité Cat. 1, Cat. 2 ou SIL 2. Les entrées 2 et 3, ainsi que les entrées 4 et 5, sont rattachées à la fonction de sécurité Cat. 3, Cat. 4 ou SIL 3.

Figure 13 – Configuration des entrées



Champ	Valeur
Type	Single (Simple)
Discrepancy Time (Temps d'écart)	–
Point Mode (Mode point)	Safety Pulse Test (Test par impulsion de sécurité)
Test Source (Source de test)	Définissez les valeurs en fonction du branchement physique du dispositif de terrain au module. Pour vous assurer que la source de test est activée correctement, accédez aux paramètres de l'onglet Test Output (Sortie de test).
Input Delay Time (Délai d'entrée)	Saisie utilisateur basée sur les caractéristiques du dispositif de terrain.

IMPORTANT Les sorties de test par impulsion intégrées (T0 à Tx) sont généralement employées avec des dispositifs de terrain dotés de contacts mécaniques. En cas d'utilisation d'un dispositif de sécurité avec des sorties électroniques (alimentant des entrées de sécurité), celles-ci doivent avoir le niveau de sécurité approprié.

IMPORTANT Si vous envisagez d'utiliser les instructions d'application de sécurité GuardLogix, configurez impérativement vos modules d'entrée de sécurité sur simple et non sur équivalent ou complémentaire. Ces instructions fournissent toutes les fonctionnalités de double voie nécessaires pour les fonctions de sécurité PLd (Cat. 3) ou PLe (Cat. 4).

Reportez-vous à la publication 1756-RM095, « GuardLogix Safety Application Instruction Set Reference Manual ».

Commandes de sécurité SIL 2 dans des tâches standard

En raison de la qualité et du nombre de diagnostics intégrés aux automates de la famille ControlLogix, vous pouvez exécuter des fonctions de sécurité SIL 2 au sein de tâches standard. Ceci est également vrai pour les automates GuardLogix.

Pour exécuter une commande de sécurité SIL 2 dans une tâche standard GuardLogix, vous devez vous conformer aux exigences définies dans la publication 1756-RM001, « Using ControlLogix in SIL 2 Applications Safety Reference Manual ».

Sécurité SIL 3 – tâche de sécurité

La création d'un projet GuardLogix génère automatiquement une tâche de sécurité unique. La tâche de sécurité présente les caractéristiques supplémentaires suivantes :

- les automates GuardLogix sont les seuls à prendre en charge la tâche de sécurité ;
- la tâche de sécurité ne peut pas être supprimée ;
- les automates GuardLogix prennent en charge une seule tâche de sécurité ;
- à l'intérieur de la tâche de sécurité, vous pouvez utiliser plusieurs programmes de sécurité comportant plusieurs sous-programmes de sécurité ;
- vous ne pouvez pas planifier ou exécuter de sous-programmes standard dans la tâche de sécurité.

La tâche de sécurité est une tâche périodique temporisée, dont la priorité et le chien de garde sont sélectionnés par l'utilisateur. La plupart du temps, elle est la première priorité de l'automate et le chien de garde du programme défini par l'utilisateur doit être réglé pour s'adapter aux variations dans l'exécution de la tâche de sécurité.

Limites de la tâche de sécurité

Vous pouvez préciser la période et le chien de garde de la tâche de sécurité. La période de la tâche de sécurité est l'intervalle auquel la tâche de sécurité est exécutée. Le chien de garde de la tâche de sécurité correspond à la durée maximale autorisée entre le début et la fin de l'exécution planifiée de la tâche de sécurité.

Pour de plus amples informations sur le chien de garde de la tâche de sécurité, reportez-vous à l'Annexe C, Temps de réponse.

La périodicité de la tâche de sécurité est limitée à 500 ms au maximum et ne peut pas être modifiée en ligne. Assurez-vous que la tâche de sécurité dispose d'assez de temps pour terminer son exécution avant qu'elle ne soit à nouveau déclenchée. Le timeout du chien de garde de la tâche de sécurité, qui est un défaut de sécurité irrécupérable dans l'automate GuardLogix, se produit si la tâche de sécurité est déclenchée alors que sa précédente exécution est toujours en cours.

Pour de plus amples informations, reportez-vous au Chapitre 7, Surveillance de l'état et gestion des défauts.

Détails de l'exécution de la tâche de sécurité

La tâche de sécurité s'exécute de la même manière qu'une tâche périodique standard, avec les exceptions suivantes :

- l'exécution de la tâche de sécurité ne commence pas tant que l'automate principal et le partenaire de sécurité n'ont pas établi leur partenariat de commande et que le temps système coordonné (CST) n'est pas synchronisé. Toutefois, les tâches standard commencent à s'exécuter dès que l'automate passe en mode Exécution ;
- bien que la plage de réglage de l'intervalle entre trames requis (RPI) pour les entrées de sécurité et les points de sécurité consommés soit comprise entre 6 et 500 ms, les points d'entrée de sécurité et les points de sécurité consommés sont mis à jour uniquement au début de l'exécution de la tâche de sécurité. Autrement dit, même si le RPI des E/S est plus court que la période de la tâche de sécurité, les données ne changent pas pendant l'exécution de la tâche de sécurité. Les données ne sont lues qu'une fois au début de l'exécution de la tâche de sécurité ;
- les valeurs d'entrée de sécurité sont figées au début de l'exécution de la tâche de sécurité. En conséquence, les instructions de temporisation, comme les instructions TON et TOF, ne seront pas mises à jour pendant une seule exécution de la tâche de sécurité. Elles prennent en compte de façon précise l'intervalle entre l'exécution de deux tâches, mais le temps cumulé ne changera pas au cours de l'exécution de la tâche de sécurité ;

ATTENTION : ce comportement est différent de l'exécution d'une tâche Logix standard, mais il est similaire à celui d'un PLC ou d'un SLC™.

- pour les points standard adressés vers des points de sécurité, leurs valeurs sont copiées dans la mémoire de sécurité au début de la tâche de sécurité et ne changent pas pendant l'exécution de la tâche de sécurité ;
- les valeurs des points de sortie de sécurité (points de sortie et produits) sont mises à jour à la fin de l'exécution de la tâche de sécurité ;
- la tâche de sécurité répond aux changements de mode (par exemple, d'Exécution à Programme ou de Programme à Exécution) à intervalles réguliers. Par conséquent, la tâche de sécurité peut utiliser plus d'une période de la tâche, mais toujours moins de deux, pour effectuer un changement de mode.

IMPORTANT	Lorsque la sécurité est déverrouillée et en l'absence d'une signature de tâche de sécurité, l'automate empêche l'accès en écriture simultané à la mémoire de sécurité à partir de la tâche de sécurité et des commandes de communication. Ainsi, la tâche de sécurité peut être suspendue jusqu'à la mise à jour des communications. Le temps nécessaire à cette mise à jour varie en fonction de la taille du point. Par conséquent, des timeouts de connexion de sécurité et de chien de garde peuvent se produire. (Par exemple, si vous procédez à des modifications en ligne lorsque la fréquence de la tâche de sécurité est réglée sur 1 ms, la durée du chien de garde risque d'être dépassée.) Pour compenser le temps d'interruption dû à la mise à jour des communications, ajoutez 2 ms à la durée du chien de garde. Lorsque l'automate est en état de verrouillage de sécurité ou en présence d'une signature de tâche de sécurité, la situation décrite dans cette remarque ne peut pas se produire.

Utilisation d'interfaces homme-machine

Respectez les précautions et consignes suivantes pour l'utilisation de dispositifs d'IHM dans des systèmes GuardLogix classés SIL.

Précautions

Vous devez prendre toutes précautions et mettre en place des procédures de protection particulières pour les dispositifs d'IHM. Ces précautions incluent, de façon non restrictive, les mesures suivantes :

- limitation et sécurité des accès ;
- établissement de spécifications, test et validation ;
- restrictions sur les données et leur d'accès ;
- limitations sur l'étendue des données et des paramètres accessibles.

Pour plus d'informations sur la façon d'intégrer des dispositifs d'IHM dans une boucle SIL classique, voir la Figure 1, page 15.

Utilisez une méthodologie pertinente pour développer les programmes d'application de l'IHM et de l'automate.

Accès à des systèmes dédiés à la sécurité

Les fonctions d'une IHM se résument à deux actions principales : la lecture et l'écriture de données.

Lecture de paramètres dans les systèmes dédiés à la sécurité

La lecture des données ne comporte aucune restriction car cette action n'affecte pas le comportement du système de sécurité. Néanmoins, le nombre, la fréquence et la taille des données lues peuvent avoir une incidence sur la disponibilité de l'automate. Pour éviter tout déclenchement intempestif de la fonction de sécurité, respectez les bonnes pratiques de communication afin de limiter les incidences du traitement de ces communications sur l'automate. Ne configurez pas la fréquence de lecture sur la valeur la plus rapide possible.

Modification de paramètres dans des systèmes classés SIL

La modification de paramètres dans une boucle dédiée à la sécurité par un dispositif externe (c'est-à-dire, situé à l'extérieur de cette boucle de sécurité ; par exemple, une IHM) n'est autorisée qu'avec les restrictions suivantes :

- Seul le personnel habilité et formé spécialement (opérateurs) peut modifier les paramètres d'un système dédié à la sécurité par l'intermédiaire d'une IHM.
- L'opérateur réalisant des modifications dans un système dédié à la sécurité par l'intermédiaire d'une IHM est responsable des effets de ces modifications sur la boucle de sécurité.
- Les variables modifiées doivent faire l'objet d'un enregistrement documentaire précis.
- Une procédure opérateur claire, complète et explicite doit être utilisée pour réaliser des modifications à caractère de sécurité par l'intermédiaire d'une IHM.
- De telles modifications d'un système dédié à la sécurité ne peuvent être validées que par la réalisation de la séquence d'actions suivante :

  a. La nouvelle variable doit être envoyée deux fois à deux points différents ; c'est-à-dire que les deux valeurs ne doivent pas être écrites par une même commande.
  b. Le programme dédié à la sécurité, exécuté dans l'automate, doit vérifier l'équivalence des deux points et s'assurer qu'ils se trouvent bien dans la tolérance (contrôle de limites).
  c. Les deux nouvelles variables doivent pouvoir être relues et affichées sur le dispositif d'IHM.
  d. Des opérateurs qualifiés doivent contrôler visuellement que les deux variables sont identiques et ont bien la bonne valeur.
  e. Ces opérateurs qualifiés doivent confirmer manuellement que les valeurs affichées sur l'écran de l'IHM sont correctes. Cela envoie alors une commande au programme de sécurité qui va autoriser l'utilisation de ces nouvelles valeurs dans la fonction de sécurité.

Dans tous les cas, l'opérateur doit confirmer la validité des modifications avant qu'elles puissent être acceptées et appliquées dans la boucle de sécurité.

- Testez toutes les modifications dans le cadre de la procédure de validation de sécurité.
- Documentez de façon suffisante toutes les modifications à caractère de sécurité apportées par l'intermédiaire de l'IHM en indiquant notamment :
  - les autorisations ;
  - l'analyse d'impact ;
  - l'exécution ;
  - les informations relatives aux tests ;
  - les informations de révision.
- Les modifications apportées au système dédié à la sécurité doivent être conformes à la norme CEI 61511 relative à la sécurité des procédés, paragraphe 11.7.1 « Exigences relatives à l'interface opérateur ».
- Les modifications apportées au système dédié à la sécurité doivent également être conformes à la norme CEI 62061 relative à la sécurité des machines.
- Le développeur doit respecter les mêmes méthodes et procédures de développement pertinentes que celles utilisées pour les autres développements de logiciel d'application, y compris la vérification et le test de l'interface opérateur et de ses accès aux autres parties du programme. Dans le logiciel d'application de l'automate, créez un tableau accessible par l'IHM et limitez l'accès aux données ponctuelles nécessaires seulement.
- De la même façon que le programme de l'automate, le logiciel de l'IHM a besoin d'être protégé et maintenu de façon à garantir la conformité au niveau SIL une fois que le système a été validé et testé.

Programmes de sécurité

Un programme de sécurité possède toutes les caractéristiques d'un programme standard, excepté qu'il ne peut être planifié que dans une tâche de sécurité. Un programme de sécurité peut également définir des points de sécurité d'accès programme. Il peut être planifié ou non.

Un programme de sécurité ne peut contenir que des composants de sécurité. Tous les sous-programmes d'un programme de sécurité sont des sous-programmes de sécurité. Un programme de sécurité ne peut pas contenir de sous-programmes standard ni de points standard.

Sous-programmes de sécurité

Les sous-programmes de sécurité possèdent toutes les caractéristiques des sous-programmes standard, hormis le fait qu'ils ne peuvent figurer que dans des programmes de sécurité. Un sous-programme de sécurité peut être désigné comme sous-programme principal. Un autre sous-programme de sécurité peut être désigné comme sous-programme de gestion des défauts. Seules les instructions certifiées pour la sécurité peuvent être utilisées dans les sous-programmes de sécurité.

Pour la liste des instructions de sécurité, reportez-vous à l'Annexe A.

ATTENTION : pour maintenir la conformité SIL 3, vous devez vous assurer que votre logique de sécurité ne tente pas de lire ou d'écrire des points standard.

Points de sécurité

Le système de commande GuardLogix accepte l'utilisation de points standard et de points de sécurité dans le même projet. Cependant, le logiciel de programmation fait une différence fonctionnelle entre les points standard et les points de sécurité.

Les points de sécurité ont tous les attributs des points standard avec, en plus, les mécanismes permettant d'assurer une intégrité des données de niveau SIL 3.

Tableau 6 – Types de données valables pour les points de sécurité

- AUX_VALVE_CONTROL
- BOOL
- CAM_PROFILE
- CAMSHAFT_MONITOR
- CB_CONTINUOUS_MODE
- CB_CRANKSHAFT_POS_MONITOR
- CB_INCH_MODE
- CB_SINGLE_STROKE_MODE
- CONFIGURABLE_ROUT
- CONNECTION_STATUS
- CONTROL
- COUNTER
- DCA_INPUT
- DCI_MONITOR
- DCI_START
- DCI_STOP
- DCI_STOP_TEST
- DCI_STOP_TEST_LOCK
- DCI_STOP_TEST_MUTE
- DINT
- DIVERSE_INPUT
- EIGHT_POS_MODE_SELECTOR
- EMERGENCY_STOP
- ENABLE_PENDANT
- EXT_ROUTINE_CONTROL
- EXT_ROUTINE_PARAMETERS
- FBD_BIT_FIELD_DISTRIBUTE
- FBD_CONVERT
- FBD_COUNTER
- FBD_LOGICAL
- FBD_MASK_EQUAL
- FBD_MASKED_MOVE
- FBD_TIMER
- FIVE_POS_MODE_SELECTOR
- INT
- LIGHT_CURTAIN
- MAIN_VALVE_CONTROL
- MANUAL_VALVE_CONTROL
- MUTING_FOUR_SENSOR_BIDIR
- MUTING_TWO_SENSOR_ASYM
- MUTING_TWO_SENSOR_SYM
- MOTION_INSTRUCTION
- PHASE
- PHASE_INSTRUCTION
- REAL
- REDUNDANT_INPUT
- REDUNDANT_OUTPUT
- SAFETY_MAT
- SERIAL_PORT_CONTROL
- SFC_ACTION
- SFC_STEP
- SFC_STOP
- SINT
- STRING
- THRS_ENHANCED
- TIMER
- TWO_HAND_RUN_STATION

L'application Logix Designer empêche la création directe de points non valides dans un programme de sécurité. Si des points non valides sont importés, ils ne peuvent pas être vérifiés.

IMPORTANT Créer des alias entre points standard et de sécurité n'est pas autorisé dans les applications de sécurité.

Les points qui sont classés comme points de sécurité sont soit des points d'accès automate, soit des points d'accès programme. Les points de sécurité en accès automate peuvent être lus par le programme standard ou celui de sécurité, ou encore par d'autres dispositifs de communication. Mais seul le programme de sécurité ou un autre automate de sécurité GuardLogix peut les écrire (modifier). En ce qui concerne les points de sécurité en accès programme, seules les sous-programmes de sécurité locaux peuvent y accéder. Il s'agit de sous-programmes qui résident dans le programme de sécurité.

Les points qui sont associés aux E/S de sécurité et les données de sécurité produites ou consommées doivent être des points de sécurité d'accès automate.

IMPORTANT Un point de sécurité d'accès automate peut être lu par n'importe quelle sous-programme standard, mais sa fréquence de mise à jour est basée sur l'exécution de la tâche de sécurité. Cela signifie que les points de sécurité sont mis à jour selon la fréquence d'exécution de la tâche de sécurité, ce qui est différent du comportement des points standard.

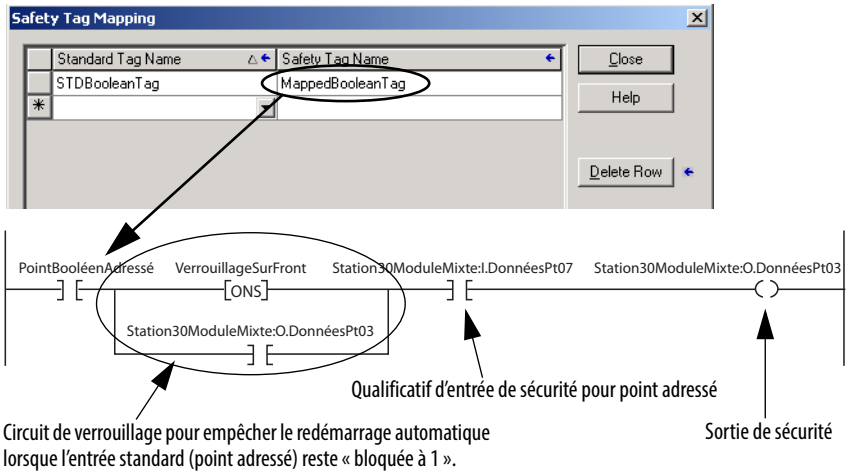
Points standard dans des sous-programmes de sécurité (adressage des points)

Les points standard d'accès automate peuvent être adressés vers des points de sécurité : vous pouvez ainsi synchroniser les actions standard et de sécurité.

ATTENTION : lorsque vous utilisez des données standard dans un sous-programme de sécurité, vous devez assurer un moyen fiable pour garantir que les données sont utilisées comme il convient. L'utilisation de données standard dans un point de sécurité n'en fait pas des données de sécurité. Il ne faut pas commander directement une sortie de sécurité avec des données de point standard.

Cet exemple montre comment qualifier les données standard avec des données de sécurité.

Figure 14 – Qualification de données standard avec des données de sécurité



Notes :

Développement d'une application de sécurité

Sujet	Page
Principes du concept de sécurité	49
Principes de base du développement et du test d'une application	50
Organigramme de la mise en service	51
Chargement du programme de l'application de sécurité	57
Transfert du programme de l'application de sécurité	57
Modification en ligne	57
Stockage et chargement d'un projet à partir de la mémoire non volatile	58
Forçage des données	58
Inhiber un dispositif	58
Modification de votre application de sécurité	59

Principes du concept de sécurité

Le concept de sécurité suppose que :

- si vous êtes responsable de la création, du fonctionnement et de la gestion de l'application, vous devez être parfaitement qualifié, spécifiquement formé et expérimenté dans le domaine des systèmes de sécurité ;
- vous utilisez correctement le langage de programmation, c'est-à-dire que les erreurs de programmation peuvent être détectées. Les erreurs de programmation peuvent être détectées si les spécifications et règles de programmation et de dénomination sont scrupuleusement observées ;
- vous effectuez une analyse critique de votre application et vous utilisez tous les moyens possibles pour détecter une défaillance ;
- vous confirmez tous les chargements de l'application par une vérification manuelle des signatures de tâche de sécurité ;
- vous effectuez une vérification de l'ensemble du système par un test fonctionnel complet avant le démarrage d'un système de sécurité.

Tableau 7 – Modes de l'automate

Mode de l'automate	État de la tâche de sécurité	Niveau de sécurité[1] (maximum possible)	Commentaires (Un programme valide a été chargé dans l'automate).
Programme	Déverrouillé Pas de signature		• Connexions d'E/S établies • Le programme de la tâche de sécurité n'est pas scruté.
Run (exécution)	Déverrouillé Pas de signature	(pour les besoins du développement uniquement)	• Forçage autorisé • Modifications en ligne autorisées • La mémoire de sécurité est isolée, mais n'est pas protégée (en lecture/écriture). • Le programme de la tâche de sécurité est scruté. L'automate principal et son partenaire de sécurité exécutent le programme et comparent de façon croisée leurs sorties logiques. Les sorties du programme sont écrites dans les sorties de sécurité.
Run (exécution)	Verrouillée Pas de signature	PLd/Cat. 3 Fiabilité de commande SIL CL2	• De nouveaux forçages ne sont pas autorisés. Les forçages existants sont maintenus. • Les modifications en ligne ne sont pas autorisées • La mémoire de sécurité est protégée (lecture seule). • Le programme de la tâche de sécurité est scruté. • L'automate principal et son partenaire de sécurité exécutent le programme et comparent de façon croisée leurs sorties logiques. Les sorties du programme sont écrites dans les sorties de sécurité.
Run (exécution)	Déverrouillé Avec signature	Ple/Cat. 4 Fiabilité de commande SIL CL3	• Les forçages ne sont pas autorisés (ils doivent être supprimés pour pouvoir générer une signature de tâche de sécurité). • Les modifications en ligne ne sont pas autorisées • La mémoire de sécurité est protégée (lecture seule). • Le programme de la tâche de sécurité est scruté. • L'automate principal et son partenaire de sécurité exécutent le programme et comparent de façon croisée leurs sorties logiques. Les sorties du programme sont écrites dans les sorties de sécurité. • La signature de la tâche de sécurité n'est pas protégée et peut être effacée par toute personne ayant accès à l'automate.
Run (exécution)	Verrouillée Avec signature	Ple/Cat. 4 Fiabilité de commande SIL CL3	• Les forçages ne sont pas autorisés (ils doivent être supprimés pour pouvoir générer une signature de tâche de sécurité). • Les modifications en ligne ne sont pas autorisées • La mémoire de sécurité est protégée (lecture seule). • Le programme de la tâche de sécurité est scruté. • L'automate principal et son partenaire de sécurité exécutent le programme et comparent de façon croisée leurs sorties logiques. Les sorties du programme sont écrites dans les sorties de sécurité. • La signature de la tâche de sécurité est protégée. Les utilisateurs doivent saisir le mot de passe pour déverrouiller l'automate avant de pouvoir effacer la signature de la tâche de sécurité.

(1) Pour obtenir ce niveau de sécurité, vous devez respecter les prescriptions de sécurité définies dans le présent document.

Principes de base du développement et du test d'une application

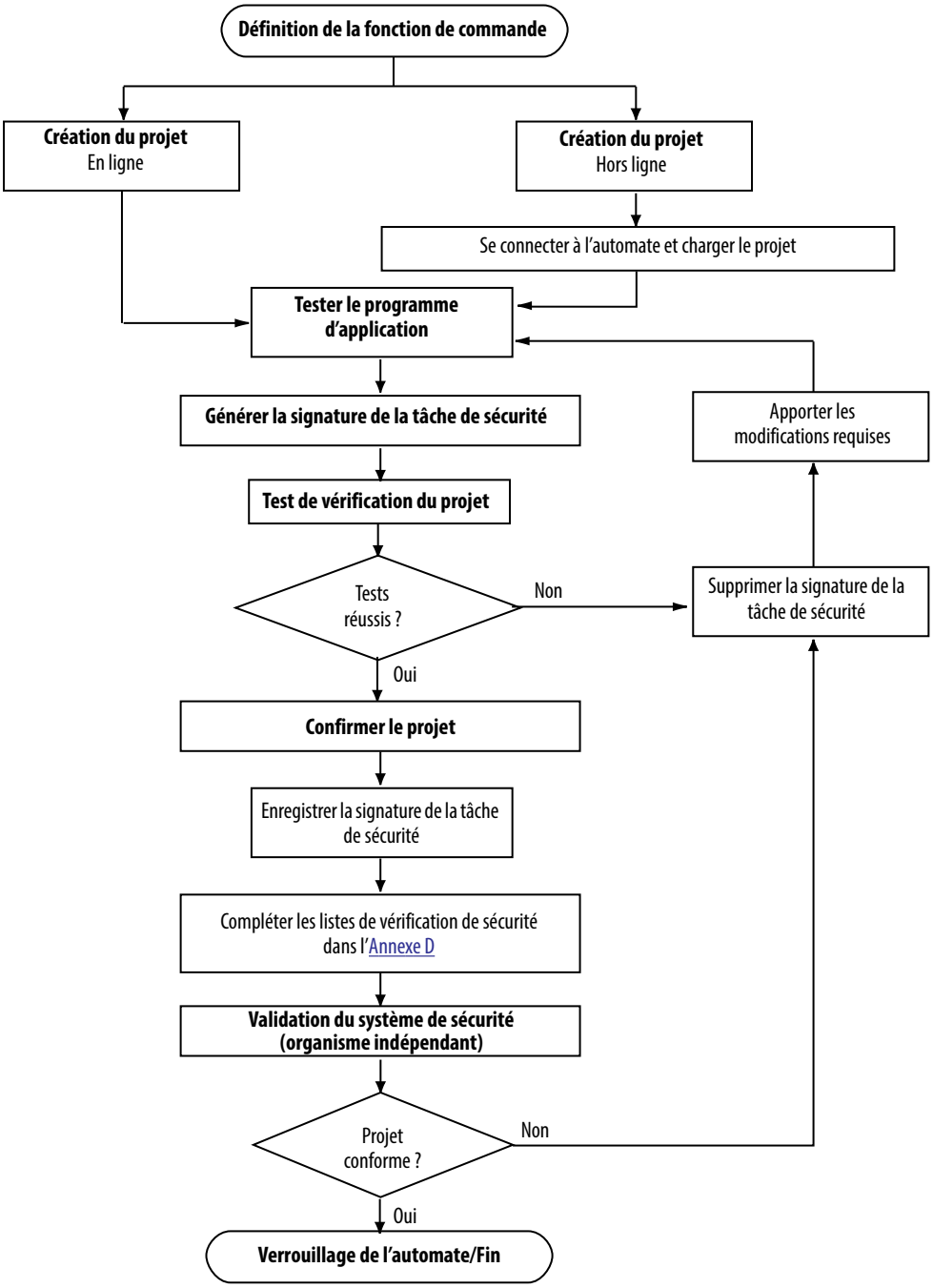
Nous vous recommandons de faire développer le programme d'application destiné au système SIL CL3 projeté par votre intégrateur système ou une personne de votre entreprise formée et expérimentée en matière d'applications de sécurité. Le développeur doit observer les bonnes pratiques de conception, à savoir :

- Utiliser des spécifications fonctionnelles, notamment des organigrammes, des chronogrammes et des graphes séquentiels.
- Effectuer un examem du programme logique de la tâche de sécurité.
- Réaliser une validation de l'application.

Organigramme de la mise en service

L'organigramme ci-dessous indique les étapes nécessaires à la mise en service d'un système GuardLogix. Les éléments en gras sont expliqués dans les sections suivantes.

Figure 15 – Mise en service du système



Définition de la fonction de commande

Vous devez créer une spécification pour votre fonction de commande. Utilisez cette spécification pour vérifier que le programme logique répond correctement et pleinement aux impératifs de fonctionnement et de commande de sécurité de votre application. La spécification peut être présentée dans différents formats, en fonction de votre application. Cependant, cette spécification doit comporter une description détaillée regroupant les éléments suivants (lorsque applicable) :

- l'ordre des opérations ;
- les organigrammes et les chronogrammes ;
- les graphes séquentiels ;
- la description du programme ;
- une impression du programme ;
- la description écrite des différentes étapes avec les conditions à respecter pour chacune d'elle et les actionneurs à commander, incluant :
  - la définition des entrées,
  - la définition des sorties,
  - les schémas et les références du câblage des E/S,
  - les principes de fonctionnement ;
- la matrice ou le tableau des conditions pour chaque étape, ainsi que les actionneurs à commander, y compris les graphes séquentiels et les chronogrammes ;
- la définition des conditions marginales, par exemple les modes de fonctionnement et l'arrêt d'urgence.

La partie E/S de la spécification doit contenir l'analyse électrique des circuits de terrain, c'est-à-dire le type des détecteurs et des actionneurs.

- Détecteurs (TOR ou analogiques) :
  - signal en fonctionnement normal (principe du courant dormant pour les détecteurs TOR, si le détecteur est sur OFF, il n'y a pas de signal) ;
  - détermination des redondances requises pour les niveaux SIL ;
  - surveillance et visualisation des écarts, incluant votre programme de diagnostic.
- Actionneurs :
  - position et activation en fonctionnement normal (normalement OFF) ;
  - réaction/position de sécurité en cas de mise hors tension ou de coupure de courant ;
  - surveillance et visualisation des écarts, incluant votre programme de diagnostic.

Création du projet

La logique et les instructions utilisées pour la programmation de l'application doivent être :

- faciles à comprendre ;
- faciles à suivre ;
- faciles à modifier ;
- faciles à tester.

Effectuez un examen et un test de tous les programmes. Séparez bien le programme de sécurité du programme standard.

Dénomination du programme

Le programme de l'application est clairement identifié par l'un des éléments suivants :

- le nom ;
- la date ;
- le numéro de révision ;
- n'importe quelle autre identification de l'utilisateur.

Tester le programme d'application

Cette étape consiste à tester toutes les combinaisons des modes d'exécution et de programmation, les modifications en ligne ou hors ligne, les transferts et les chargements de projet, ainsi qu'à effectuer tous les tests informels nécessaires pour s'assurer que l'application fonctionne correctement, en anticipation des essais de validation du projet.

Génération de la signature de la tâche de sécurité

La signature de la tâche de sécurité identifie de façon unique chaque projet, notamment son programme, ses données et sa configuration. La signature de la tâche de sécurité se compose d'un numéro d'identification (ID), de la date et de l'heure.

Vous pouvez générer la signature de la tâche de sécurité si toutes les conditions suivantes sont réunies :

- l'application Logix Designer est en ligne avec l'automate ;
- l'automate est en mode Programme ;
- la sécurité est déverrouillée sur l'automate ;
- l'automate n'a pas de forçage de sécurité, ni de modifications de la sécurité en cours ;
- l'état de la tâche de sécurité est OK.

Une fois le test du programme d'application terminé, vous devez générer la signature de la tâche de sécurité. Une fois la signature de la tâche de sécurité générée, le logiciel de programmation la transfère automatiquement.

IMPORTANT Pour vérifier l'intégrité de chaque chargement, vous devez enregistrer manuellement la signature de la tâche de sécurité après sa création initiale et la vérifier après chaque chargement pour vous assurer qu'elle correspond bien à la signature d'origine.

Vous pouvez supprimer la signature de la tâche de sécurité uniquement lorsque la sécurité de l'automate GuardLogix est déverrouillée et, si en mode en ligne, lorsque le commutateur à clé est en position REM ou PROG.

En présence d'une signature de tâche de sécurité, les actions suivantes ne sont pas autorisées dans la tâche de sécurité :

- programmation ou modification en ligne ou hors ligne des composants de sécurité ;
- forçage des E/S de sécurité ;
- manipulation des données (sauf par la logique d'un sous-programme ou un autre automate GuardLogix).

Test de vérification du projet

Pour vérifier que votre programme d'application est bien conforme à la spécification, vous devez réaliser un ensemble adapté de tests couvrant toutes les situations possibles pour votre application. Cet ensemble de tests doit être enregistré et stocké en tant que spécification de test.

Vous devez inclure un ensemble de tests pour prouver la validité des calculs (formules) utilisés dans votre programme. Les tests de plages équivalentes sont acceptés. Il s'agit de tests effectués à l'intérieur des plages de valeurs définies, aux limites de ces plages, ou dans des plages de valeurs non valables. Le nombre de tests nécessaires dépend des formules utilisées et doit comprendre des paires de valeurs critiques.

Une simulation active avec les sources (dispositifs de terrain) doit également être effectuée. C'est en effet la seule façon de vérifier que les détecteurs et les actionneurs du système sont correctement câblés. Vérifiez le fonctionnement des opérations programmées en manipulant manuellement les détecteurs et les actionneurs.

Vous devez également inclure des tests pour vérifier la réaction aux défauts de câblage et de communication réseau.

La vérification du projet comporte les tests des sous-programmes de gestion des défauts ainsi que des voies d'entrée et de sortie, afin de s'assurer du bon fonctionnement du système de sécurité.

Pour réaliser un test de vérification du projet sur l'automate GuardLogix, vous devez effectuer le test complet de votre application. Vous devez désactiver puis activer chaque détecteur et actionneur utilisé dans chacune des fonctions de sécurité. Du point de vue d'un automate, cela signifie désactiver et activer le point d'E/S allant dans l'automate, pas nécessairement les actionneurs eux-mêmes.

Assurez-vous que toutes les fonctions d'arrêt de l'installation ont bien été testées. Ces fonctions ne sont en effet pas habituellement utilisées en fonctionnement normal. N'oubliez pas qu'un test de vérification du projet n'est valable que pour l'application spécifiquement testée. Si l'automate est déplacé dans une autre application, vous devrez également réaliser des tests de démarrage et de vérification du projet sur cet automate dans le cadre du nouveau programme d'application.

Confirmation du projet

Vous devez imprimer ou contrôler à l'écran le projet. Comparez les E/S de sécurité, les configurations de l'automate, les données de sécurité et le programme de la tâche de sécurité qui ont été chargés sur l'automate afin de vous assurer que les composants de sécurité adéquats ont bien été chargés, testés et retenus dans le programme de l'application de sécurité.

Si votre programme d'application contient une instruction complémentaire de sécurité qui a été scellée avec une signature d'instruction, vous devez aussi comparer la signature d'instruction, la date/l'heure et la signature d'instruction de sécurité avec les valeurs que vous avez enregistrées quand vous avez scellé l'instruction complémentaire.

Pour de plus amples informations sur la création et l'utilisation d'instructions complémentaires de sécurité dans des applications SIL 3, reportez-vous à l'Annexe B, Instructions complémentaires de sécurité.

Les étapes ci-dessous indiquent une méthode pour confirmer le projet :

1. Avec l'automate en mode Programme, enregistrez le projet.
2. Répondez « Oui » au message vous demandant si vous souhaitez transférer la valeur des points.
3. L'application Logix Designer se trouvant hors ligne, enregistrez le projet sous un nouveau nom, par exemple « Nomduprojethorsligne.ACD », « Nomduprojet » correspondant au nom de votre projet.

   Il s'agit du nouveau fichier de projet maître testé.
4. Fermez le projet.
5. Déplacez le fichier d'archive du projet original hors de son répertoire habituel.
   Vous pouvez supprimer ce fichier ou le conserver dans un emplacement d'archivage. Cette étape est nécessaire car, si l'application Logix Designer trouve le fichier « Nomduprojet.ACD » dans ce répertoire, elle établira une corrélation avec le projet de l'automate et n'effectuera pas le transfert effectif.
6. L'automate toujours en mode Programme, transférez le projet à partir de l'automate.
7. Enregistrez le projet transféré sous le nom « Nomduprojetenligne.ACD », Nomduprojet correspondant au nom de votre projet.
8. Répondez « Oui » au message vous demandant si vous souhaitez transférer la valeur des points.

9. Utilisez l'utilitaire Compare du programme Logix Designer pour réaliser les comparaisons suivantes :
   - comparaison de toutes les propriétés de l'automate GuardLogix et des dispositifs d'E/S CIP Safety ;
   - comparaison de toutes les propriétés de la tâche de sécurité, des programmes de sécurité et des sous-programmes de sécurité ;
   - comparaison de tous les programmes logiques des sous-programmes de sécurité.

Validation de la sécurité

Une validation du système de sécurité par un organisme externe indépendant peut être requise avant de décréter ce système apte au fonctionnement. Une certification par un organisme indépendant extérieur est requise pour le niveau SIL 3 selon la norme CEI 61508.

Verrouillage de l'automate GuardLogix

Un verrouillage de sécurité de l'automate GuardLogix est réalisable de façon à empêcher toute modification des composantes de commande de sécurité. Toutefois, ce verrouillage de sécurité de l'automate n'est pas obligatoire pour les applications SIL 3. La fonction de verrouillage de sécurité s'applique uniquement aux composants de sécurité, notamment la tâche de sécurité, les programmes de sécurité, les sous-programmes de sécurité, les points de sécurité, les instructions complémentaires de sécurité, les E/S de sécurité et la signature de la tâche de sécurité. Toutefois, la fonction de verrouillage de sécurité à elle seule ne satisfait pas aux exigences SIL 3.

Aucun aspect de la sécurité ne peut être modifié lorsque la sécurité est verrouillée sur l'automate. Dans ce cas, les actions suivantes ne sont pas autorisées dans la tâche de sécurité :

- programmation ou modification en ligne/hors ligne ;
- forçage des E/S de sécurité ;
- manipulation des données (sauf par la logique d'un sous-programme ou un autre automate GuardLogix) ;
- création ou modification des instructions complémentaires de sécurité ;
- génération ou suppression de la signature de la tâche de sécurité.

Par défaut, la sécurité est déverrouillée sur l'automate. Vous pouvez verrouiller l'application de sécurité, que vous soyez en ligne ou non, et que vous disposiez ou non du programme source d'origine. Il ne doit cependant y avoir aucun forçage de sécurité ni aucune édition de sécurité en attente. Il n'est pas possible de modifier l'état verrouillé ou déverrouillé de la sécurité lorsque le commutateur à clé est en position RUN.

Pour ajouter un niveau de protection supplémentaire, vous pouvez utiliser des mots de passe distincts pour le verrouillage et le déverrouillage de la sécurité de l'automate. Les mots de passe ne sont pas obligatoires.

Chargement du programme de l'application de sécurité

Au cours du chargement, un test complet de l'application est nécessaire, à moins qu'une signature de tâche de sécurité soit présente.

IMPORTANT Pour vérifier l'intégrité de chaque chargement, vous devez enregistrer manuellement la signature de la tâche de sécurité après sa création initiale et la vérifier après chaque chargement pour vous assurer qu'elle correspond bien à la signature d'origine.

Les chargements de projet sur un automate GuardLogix dont la sécurité est verrouillée ne sont possibles que si la signature de la tâche de sécurité, la série du matériel et la version du système d'exploitation du projet hors ligne correspondent intégralement à celles de l'automate GuardLogix cible, et que si la tâche de sécurité de cet automate est à l'état OK.

IMPORTANT Si la signature de la tâche de sécurité ne correspond pas et si la sécurité de l'automate est verrouillée, vous devez le déverrouiller pour effectuer un chargement. Dans ce cas, le chargement d'un projet sur l'automate effacera la signature de la tâche de sécurité. En conséquence, vous serez obligé(e) de revalider l'application.

ATTENTION : le port USB n'est prévu que pour effectuer ponctuellement des programmations locales. Il n'est pas conçu pour une connexion permanente.

Transfert du programme de l'application de sécurité

Si l'automate GuardLogix contient une signature de tâche de sécurité, celle-ci sera transférée avec le projet. Cela signifie que toute modification apportée aux données de sécurité hors ligne sera écrasée suite au transfert.

Modification en ligne

S'il n'y a pas de signature de tâche de sécurité et si la sécurité de l'automate est déverrouillée, vous pouvez apporter des modifications en ligne à vos sous-programmes de sécurité.

CONSEIL Vous ne pouvez pas modifier des instructions complémentaires de sécurité ou standard lorsque vous êtes en ligne.

Il ne peut pas y avoir d'éditions en attente lorsque la sécurité de l'automate est verrouillée ou en présence d'une signature de tâche de sécurité. En revanche, vous pouvez effectuer des modifications en ligne lorsque la sécurité de l'automate est verrouillée, mais dans ce cas, vous ne pouvez ni les assembler ni les annuler.

CONSEIL Les modifications en ligne dans les sous-programmes standard ne sont pas affectées par l'état verrouillé ou déverrouillé de la sécurité.

Pour de plus amples informations sur les modifications de votre programme d'application, reportez-vous à la page 59.

Stockage et chargement d'un projet à partir de la mémoire non volatile

Les automates GuardLogix 5570 permettent la mise à jour de firmware ainsi que le stockage et la restauration d'un programme utilisateur au moyen d'une carte mémoire. Dans un système GuardLogix, seul l'automate principal utilise une carte mémoire comme mémoire non volatile.

Lors de la sauvegarde d'un projet de sécurité sur une carte mémoire, Rockwell Automation recommande de sélectionner Remote Program (Programmation à distance) pour le mode de chargement (Load Mode), c'est-à-dire pour le comportement qu'adoptera l'automate après le chargement. Avant le fonctionnement effectif de la machine, une intervention de l'opérateur est nécessaire pour démarrer la machine.

Vous ne pourrez lancer le chargement à partir de la mémoire non volatile que dans les conditions suivantes :

- le type d'automate spécifié dans le projet stocké en mémoire non volatile correspond à celui de votre automate ;
- les révisions majeure et mineure du projet en mémoire non volatile correspondent à celles de votre automate ;
- votre automate n'est pas en mode Exécution (Run).

Le chargement d'un projet vers un automate dont la sécurité est verrouillée est autorisé uniquement lorsque la signature de la tâche de sécurité du projet sauvegardé dans la mémoire non volatile correspond au projet présent dans l'automate. Si les signatures ne concordent pas ou si la sécurité de l'automate est verrouillée sans signature de tâche de sécurité, vous devez d'abord déverrouiller l'automate avant d'essayer de mettre à jour l'automate via la mémoire non volatile.

IMPORTANT Si vous déverrouillez l'automate et lancez un chargement à partir de la mémoire non volatile, l'état de verrouillage de la sécurité, les mots de passe et la signature de la tâche de sécurité adopteront les valeurs contenues dans la mémoire non volatile une fois le chargement terminé.

Forçage des données

Toutes les données contenues dans un point de sécurité d'E/S produit ou consommé, notamment CONNECTION_STATUS, peuvent être forcées lorsque la sécurité du projet est déverrouillée et en l'absence d'une signature de tâche de sécurité. Toutefois, pour qu'il soit possible de verrouiller la sécurité d'un projet ou de générer une signature de tâche de sécurité, les forçages doivent être désinstallés, et pas simplement désactivés, sur tous les points de sécurité. Vous ne pouvez pas forcer les points de sécurité lorsque la sécurité du projet est verrouillée ou en la présence d'une signature de tâche de sécurité.

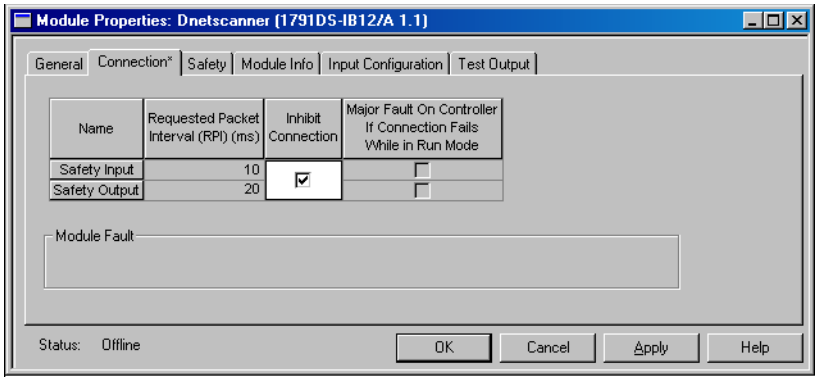
CONSEIL Vous pouvez installer et désinstaller les forçages sur les points standard que la sécurité soit verrouillée ou non.

Inhiber un dispositif

Vous ne pouvez pas inhiber ou désinhiber des dispositifs d'E/S de sécurité ou des automates producteurs si le programme d'application fait l'objet d'un verrouillage de sécurité ou en présence d'une signature de tâche de sécurité.

Pour inhiber un dispositif d'E/S de sécurité particulier, procédez comme suit.

1. Dans l'application Logix Designer, cliquez sur le dispositif avec le bouton droit de la souris et sélectionnez Properties (Propriétés).
2. Dans la boîte de dialogue Module Properties (Propriétés du module), cliquez sur l'onglet Connection (Connexion).
3. Cochez Inhibit Connection (Inhiber la connexion) et cliquez sur Apply (Appliquer).



Lorsque cette case est cochée, le dispositif est inhibé. Si un dispositif de communication est inhibé, tous les dispositifs en aval sont également inhibés.

Modification de votre application de sécurité

Les règles suivantes s'appliquent à toute modification de votre programme de sécurité dans l'application Logix Designer :

- seul le personnel autorisé et spécialement formé peut modifier le programme. Ces personnes doivent appliquer toutes les méthodes de supervision disponibles à l'aide, par exemple, du commutateur à clé de l'automate ou des protections par mot de passe du logiciel ;
- lorsqu'une personne autorisée et spécialement formée apporte des modifications au programme, elle assume la responsabilité de la sécurité pendant que les changements sont en cours. Cette personne doit également assurer le fonctionnement de l'application en toute sécurité ;
- lors d'une modification en ligne, vous devez utiliser une méthode de protection alternative pour préserver la sécurité du système ;
- vous devez renseigner de façon suffisamment précise toutes les modifications du programme, notamment :
  - les autorisations ;
  - l'analyse d'impact ;
  - l'exécution ;
  - les informations relatives aux tests ;
  - les informations de révision.
- si les modifications en ligne portent seulement sur les sous-programmes standard, il n'est pas nécessaire qu'elles soient validées pour revenir au fonctionnement normal ;
- vous devez vous assurer que les modifications apportées programme standard sont acceptables pour votre application de sécurité en termes de temps d'exécution et d'adressage des points ;
- vous **pouvez** modifier la partie logique de votre programme en ligne ou hors ligne, comme indiqué dans les sections suivantes.

Modifications hors ligne

Si vous modifiez hors ligne des éléments du programme standard seulement et si la signature de la tâche de sécurité correspond suite à un chargement, vous pouvez reprendre le fonctionnement.

Si des modification hors ligne sont effectuées sur le programme de sécurité, vous devez revalider tous les éléments concernés de l'application identifiés par l'analyse d'impact avant de reprendre le fonctionnement.

L'organigramme de la page 61 illustre le processus de modification hors ligne.

Modifications en ligne

Si des modification en ligne sont effectuées sur le programme de sécurité, vous devez revalider tous les éléments concernés de l'application identifiés par l'analyse d'impact avant de reprendre le fonctionnement. L'organigramme de la page 61 illustre le processus de modification en ligne.

CONSEIL Limitez les modifications en ligne à des modifications mineures du programme, comme des changements de point de consigne ou des ajouts, suppressions et modifications limitées d'éléments de ce programme.

Les modifications en ligne sont concernées par le verrouillage de la sécurité et par la signature de la tâche de sécurité de l'automate GuardLogix.

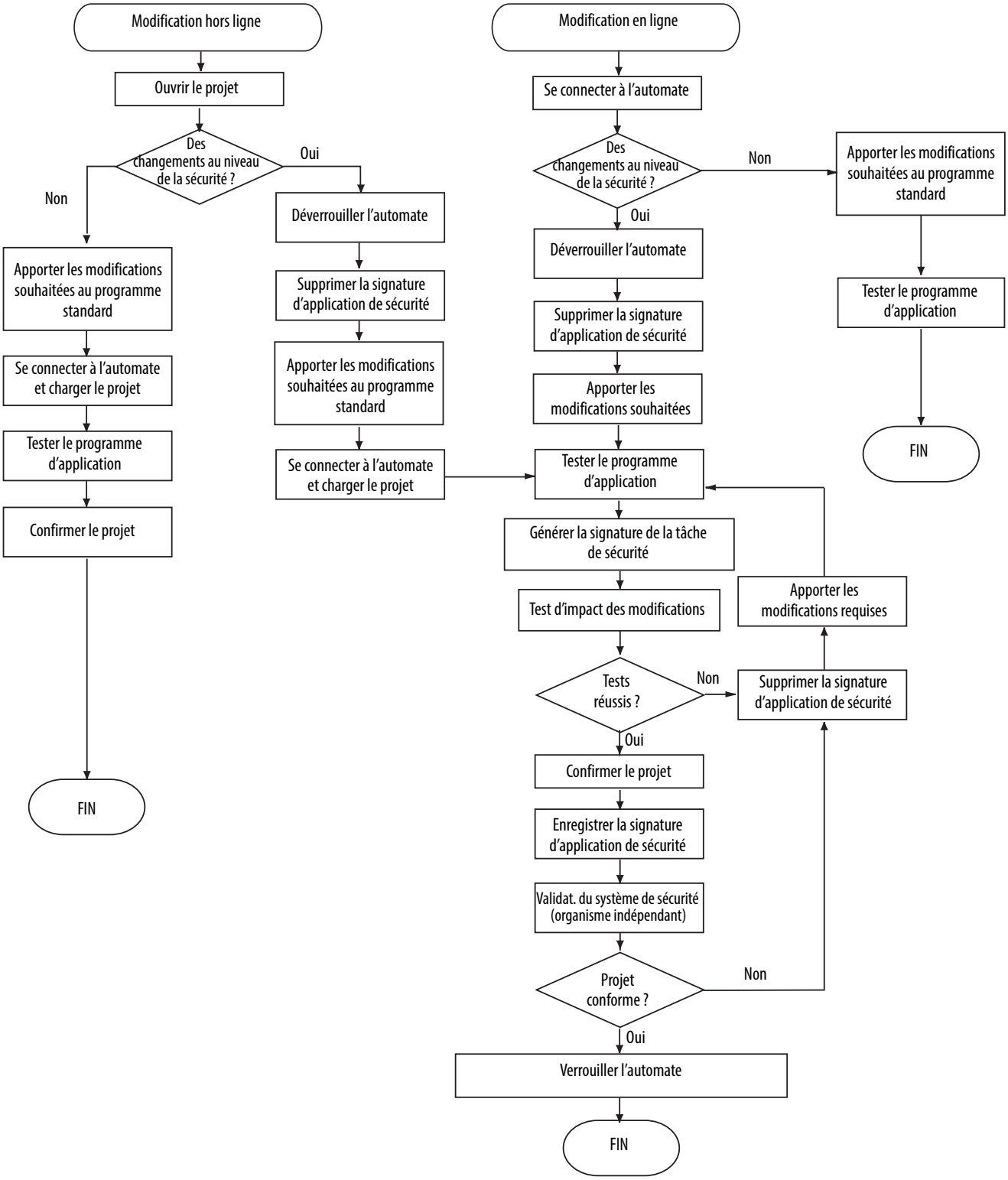
Pour de plus amples informations, reportez-vous à la section Génération de la signature de la tâche de sécurité, page 53, et à la section Verrouillage de l'automate GuardLogix, page 56.

Pour des informations détaillées sur la modification en ligne d'un programme en logique à relais dans l'application Logix Designer, reportez-vous à la publication 1756-QS001, « Logix5000 Controllers Quick Start ».

Test d'impact des modifications

Toute modification, amélioration ou adaptation d'un programme utilisateur validé doit être planifiée et tous les impacts potentiels sur le système de sécurité fonctionnelle doivent être analysés. Toutes les phases concernées du cycle de sécurité de ce programme doivent être testées comme indiqué par l'analyse d'impact. Un test fonctionnel minimum de tous les éléments de programme concernés doit être effectué. Toutes les modifications apportées aux spécifications de votre programme doivent être documentées. Les résultats des tests doivent également être consignés. Se reporter à la norme CEI 61508-3, paragraphe 7.8 « Modifications du logiciel », pour des informations plus détaillées.

Figure 16 – Procédure de modification en ligne et hors ligne



Notes :

Surveillance de l'état et gestion des défauts

Sujet	Page
Surveillance d'état du système	63
Défauts du système GuardLogix	66

L'architecture GuardLogix offre de nombreuses solutions de détection et de traitement des défauts dans le système. La première consiste à s'assurer que les listes de contrôle de l'application ont bien été suivies (voir l'Annexe D).

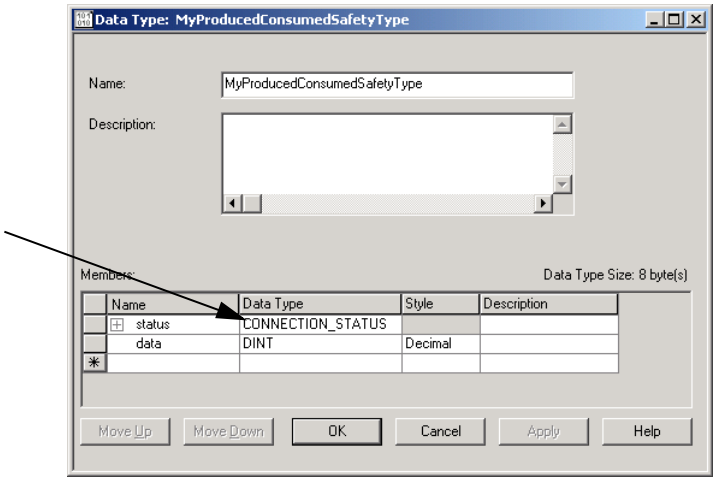
Surveillance d'état du système

Vous pouvez visualiser l'état des connexions de points de sécurité. Vous pouvez également déterminer l'état de fonctionnement en cours en interrogeant divers objets de dispositif. Il vous incombe de déterminer quelles sont les données les plus appropriées pour lancer une séquence d'arrêt.

Données de CONNECTION_STATUS

Le premier élément de la structure du point associé aux données d'entrée de sécurité et aux points de données de sécurité produits/consommés contient l'état de la connexion. Cet élément est un type de donnée prédéfini appelé CONNECTION_STATUS.

Figure 17 – Boîte de dialogue Data Type (type de donnée)



Les deux premiers bits du type de donnée CONNECTION_STATUS correspondent aux bits d'état RunMode (mode Exécution) et ConnectionFaulted (Défaut de connexion) du périphérique. Le tableau suivant décrit les combinaisons des états RunMode et ConnectionFaulted.

Tableau 8 – Etat de la connexion de sécurité

Etat RunMode	Etat ConnectionFaulted	Fonctionnement de la connexion de sécurité
1 = Exécution	0 = Correcte	Les données sont activement commandées par le dispositif producteur. Ce dernier est en mode Exécution.
0 = Inactif	0 = Correcte	La connexion est active et le dispositif producteur est inactif. Les données de sécurité sont remises à zéro.
0 = Inactif	1 = En défaut	La connexion de sécurité présente un défaut. L'état du dispositif producteur est inconnu. Les données de sécurité sont remises à zéro.
1	1	Etat non valable.

ATTENTION : les connexions d'E/S de sécurité, ainsi que les connexions produites/consommées ne peuvent pas être configurées automatiquement de façon à placer l'automate en défaut en cas de perte de connexion ou si le système passe en état de sécurité. En conséquence, si vous avez besoin de détecter un défaut éventuel au niveau d'un dispositif pour garantir que le système reste bien conforme au niveau SIL 3, vous devez surveiller les bits CONNECTION_STATUS des E/S de sécurité et prévoir le déclenchement du défaut par le programme logique.

Diagnostic des entrées et des sorties

Les modules d'E/S Guard I/O proposent des tests par impulsion et des fonctionnalités de surveillance. Si le module détecte une défaillance, il met l'entrée ou la sortie en cause en état de sécurité et informe l'automate de la défaillance. La défaillance est indiquée par l'état de l'entrée ou de la sortie et cette indication est maintenue pendant une certaine durée (configurable) après la réparation de la défaillance.

IMPORTANT Il vous incombe de fournir un programme d'application pour verrouiller ces défaillances d'E/S et vérifier que le système redémarre correctement.

Etat des connexions du dispositif d'E/S

Le protocole CIP Safety fournit un état de chaque dispositif d'E/S du système de sécurité. Si une défaillance de connexion d'entrée est détectée, le système d'exploitation désactive (met en sécurité) toutes les entrées du dispositif et passe leur état d'entrée associé sur défaut. Si une défaillance est détectée au niveau d'une connexion de sortie, le système d'exploitation met la sortie associée en défaut. Le dispositif de sortie désactive les sorties.

IMPORTANT Il vous incombe de fournir un programme d'application pour verrouiller ces défaillances d'E/S et vérifier que le système redémarre correctement.

Système de déclenchement par mise hors tension

Les automates GuardLogix font partie des systèmes à déclenchement par mise hors tension. Cela signifie que la valeur logique zéro correspond à leur état de sécurité. Certains défauts (mais pas tous) des dispositifs d'E/S de sécurité provoquent la mise à zéro (état de sécurité) des entrées ou des sorties du dispositif concerné. Les défauts associés à une voie d'entrée particulière occasionneront la mise à zéro de cette voie particulière. Par exemple, un défaut sur test par impulsion affectant spécifiquement la voie 0 se traduira par le passage à l'état de sécurité (0) des données d'entrée de cette voie 0. Si un défaut affecte le dispositif globalement et non une voie en particulier, le bit d'état combiné affiche l'état de défaut et toutes les données du dispositif sont placées en état de sécurité (0).

Pour toute information sur l'utilisation des instructions pour application de sécurité GuardLogix, reportez-vous à l'Annexe F de ce manuel, ainsi qu'à la publication 1756-RM095, « GuardLogix Safety Application Instructions Safety Reference Manual ».

Instructions GSV et SSV

Les instructions GSV et SSV vous permettent de lire (GSV) et de définir (SSV) les données système de l'automate stockées dans les objets de dispositif. Lorsque vous entrez une instruction GSV/SSV, le logiciel de programmation affiche les classes d'objets valables, le nom des objets et le nom des attributs pour chaque instruction. L'utilisation des instructions GSV et SSV avec des composants de sécurité est soumise à des restrictions.

IMPORTANT	La tâche de sécurité ne peut pas exécuter des opérations GSV ou SSV sur des attributs standard. Les attributs des objets de sécurité pouvant être écrits par la tâche standard servent uniquement au diagnostic et n'affectent pas l'exécution de la tâche de sécurité.

Pour de plus amples informations sur les attributs de sécurité accessibles par les instructions GSV et SSV, reportez-vous à la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur ».

Pour des informations générales sur l'utilisation des instructions GSV et SSV, reportez-vous à la publication 1756-RM003, « Automates Logix5000 – Instructions – Manuel de référence ».

Défauts du système GuardLogix

Les défauts du système GuardLogix se divisent en trois catégories :

- défauts d'automate irrécupérables
- défauts de sécurité irrécupérables
- défauts récupérables.

Pour toute information sur la gestion des défauts, reportez-vous à la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur ».

Défauts d'automate irrécupérables

Un défaut d'automate irrécupérable se produit en cas d'échec des diagnostics internes de l'automate. Le partenariat est perdu lorsqu'un défaut d'automate irrécupérable se produit dans l'automate principal ou dans le partenaire de sécurité ; dans ce cas, l'autre équipement génère un défaut de timeout du chien de garde irrécupérable. L'exécution de la tâche standard et de la tâche de sécurité s'arrête et les E/S de sécurité passent en état de sécurité.

Pour corriger un défaut d'automate irrécupérable, il faut recharger le programme d'application.

Défauts de sécurité irrécupérables

Dans le cas d'un défaut de sécurité irrécupérable, l'automate enregistre le défaut dans le gestionnaire de défauts de niveau automate et arrête la tâche de sécurité, y compris les E/S de sécurité et le programme de sécurité.

Pour corriger un défaut de sécurité irrécupérable, il faut réinitialiser la mémoire de sécurité à partir de la signature de tâche de sécurité (se fait automatiquement lorsque vous effacez le défaut), ou, en l'absence d'une signature de tâche de sécurité, en rechargeant le projet de sécurité.

Vous pouvez contourner le défaut de sécurité en effaçant l'entrée du journal des défauts via le gestionnaire de défauts de sécurité de niveau automate. Ceci permet de ne pas stopper l'exécution des tâches standard.

ATTENTION : le fait de contourner le défaut de sécurité ne l'efface pas. Si vous contournez le défaut de sécurité, vous devez vous assurer que la conformité SIL 3 est maintenue.

Défauts récupérables

Lorsque des défauts d'automate sont provoqués par des erreurs de programmation de l'utilisateur dans un programme de sécurité, l'automate exécute la logique contenue dans le gestionnaire de défauts du programme de sécurité du projet. Le gestionnaire de défauts du programme de sécurité permet à l'application de corriger la cause du défaut, puis de redémarrer.

ATTENTION : vous devez fournir à votre organisme de certification la preuve que la correction automatique suite à des défauts récupérables maintient la conformité SIL 3.

Lorsqu'il n'y a pas de gestionnaire de défauts du programme de sécurité, ou lorsqu'il ne peut pas corriger le défaut, l'automate exécute le programme du gestionnaire de défauts de niveau automate, ce qui stoppe l'exécution du programme de sécurité et laisse les connexions d'E/S de sécurité actives mais en attente.

IMPORTANT Lorsque l'exécution du programme de sécurité est arrêtée suite à un défaut récupérable non géré par le gestionnaire de défauts du programme de sécurité, les connexions des E/S de sécurité sont fermées puis rouvertes pour être réinitialisées.

Si le programme utilisateur s'arrête suite à un défaut récupérable non corrigé, les sorties de sécurité passent en état de sécurité et le producteur de points de sécurité consommés commande aux consommateurs de les placer en état de sécurité.

CONSEIL Lorsque des E/S de sécurité sont utilisées dans des applications standard, elles passent en état de sécurité si le programme utilisateur est stoppé en raison d'un défaut récupérable non corrigé.

Si un défaut de sécurité récupérable est contourné dans le gestionnaire de défauts de niveau automate, seules les tâches standard continuent à être exécutées. Si le défaut n'est pas contourné, les tâches standard sont également arrêtées.

ATTENTION : le fait de contourner le défaut de sécurité ne l'efface pas. Si vous contournez le défaut de sécurité, vous devez vous assurer que la conformité SIL 3 est maintenue.

Notes :

Instructions de sécurité

Pour obtenir les toutes dernières informations, reportez-vous à nos certifications de sécurité, à l'adresse http://www.rockwellautomation.com/products/certification/safety/.

Le Tableau 9 et le Tableau 10 récapitulent les instructions pour application de sécurité certifiées pour une utilisation dans des les applications SIL 3.

Tableau 9 – Instructions générales pour application de sécurité

Mnémonique	Nom	Fonction	Certification
CROUT	Sortie redondante configurable	Commande et surveille les sorties redondantes.	• BG • TÜV
DCA	Entrée double voie – analogique (version nombre entier)	Surveille les variations et la tolérance de plage de deux valeurs analogiques.	TÜV
DCAF	Entrée double voie – analogique (version virgule flottante)		
DCS	Entrée double voie – Arrêt	Surveille les dispositifs de sécurité à double entrée chargés principalement de fournir une fonction d'arrêt, par exemple un arrêt d'urgence, une barrière immatérielle ou un interrupteur de porte.	• BG • TÜV
DCST	Entrée double voie – Arrêt avec test	Surveille les dispositifs de sécurité à double entrée chargés principalement de fournir une fonction d'arrêt, par exemple un arrêt d'urgence, une barrière immatérielle ou un interrupteur de porte. Inclut la capacité supplémentaire de déclencher un test fonctionnel du dispositif d'arrêt.	• BG • TÜV
DCSTL	Entrée double voie – Arrêt avec test et verrouillage	Surveille les dispositifs de sécurité à double entrée chargés principalement de fournir une fonction d'arrêt, par exemple un arrêt d'urgence, une barrière immatérielle ou un interrupteur de porte. Inclut la capacité supplémentaire de déclencher un test fonctionnel du dispositif d'arrêt. Surveille un signal de retour provenant d'un dispositif de sécurité et émet une demande de verrouillage en direction d'un dispositif de sécurité.	• BG • TÜV
DCSTM	Entrée double voie – Arrêt avec test et inhibition	Surveille les dispositifs de sécurité à double entrée chargés principalement de fournir une fonction d'arrêt, par exemple un arrêt d'urgence, une barrière immatérielle ou un interrupteur de porte. Inclut la capacité supplémentaire de déclencher un test fonctionnel du dispositif d'arrêt et la possibilité d'inhiber le dispositif de sécurité.	TÜV
DCM	Entrée double voie – Surveillance	Surveille les dispositifs de sécurité à double entrée.	• BG • TÜV
DCSRT	Entrée double voie – Démarrage	Active les dispositifs de sécurité à double entrée chargés principalement du démarrage d'une machine en toute sécurité, par exemple une poignée homme mort.	• BG • TÜV
SMAT	Tapis de sécurité	Indique la présence d'une personne sur le tapis de sécurité.	TÜV
THRSe	Station bimanuelle – Évoluée	Surveille deux entrées de sécurité complémentaires, l'une à partir d'un bouton-poussoir main droite et l'autre à partir d'un bouton-poussoir main gauche, pour commander une seule sortie. Fournit un temps d'écart entre voies configurable et une capacité évoluée de contournement de station bimanuelle.	• BG • TÜV
TSAM	Inhibition asymétrique au moyen de deux capteurs	Désactive automatiquement et à titre provisoire la fonction de protection d'une barrière immatérielle, au moyen de deux capteurs d'inhibition qui sont disposés asymétriquement.	TÜV
TSSM	Inhibition symétrique au moyen de deux capteurs	Désactive automatiquement et à titre provisoire la fonction de protection d'une barrière immatérielle, au moyen de deux capteurs d'inhibition qui sont disposés symétriquement.	TÜV
FSBM	Inhibition bidirectionnelle au moyen de quatre capteurs	Désactive automatiquement et à titre provisoire la fonction de protection d'une barrière immatérielle, au moyen de quatre capteurs qui sont disposés les uns à la suite des autres à l'amont et à l'aval du champ de détection de la barrière immatérielle.	TÜV

Tableau 10 – Instructions pour applications de sécurité concernant le formage des métaux

Mnémonique	Nom	Fonction	Certification
CBCM	Mode continu d'embrayage/de freinage	Utilisé pour les applications de presse où un fonctionnement continu est souhaité.	• BG • TÜV
CBIM	Mode pas à pas d'embrayage/de freinage	Utilisé sur les presses nécessitant des ajustements mineurs de course, notamment le réglage de la presse.	• BG • TÜV
CBSSM	Mode coup par coup d'embrayage/de freinage	Utilisé dans les applications de presse à cycle unique.	• BG • TÜV
CPM	Surveillance de position de vilebrequin	Sert à déterminer la position de la glissière d'une presse.	• BG • TÜV
CSM	Surveillance d'arbre à cames	Surveille les opérations de démarrage, d'arrêt et de fonctionnement d'un arbre à cames.	• BG • TÜV
EPMS	Commutateur-sélecteur à huit positions	Surveille huit entrées de sécurité pour commander l'une des huit sorties qui correspond à l'entrée active.	• BG • TÜV
AVC	Commande de vanne auxiliaire	Commande une vanne auxiliaire qui est utilisée avec une vanne principale.	TÜV
MVC	Commande de vanne principale	Commande et surveille une vanne principale.	• BG • TÜV
MMVC	Commande manuelle de maintenance de vanne	Sert à commander manuellement une vanne pendant les opérations de maintenance.	• BG • TÜV

Les sous-programmes dans la tâche de sécurité peuvent utiliser ces instructions de sécurité en logique à relais.

Tableau 11 – Instructions de sécurité en logique à relais

Type	Mnémonique	Nom	Fonction
Tableau (fichier)	FAL[1]	Fichier arithmétique et logique	Exécute des opérations arithmétiques, logiques, de copie et de fonction sur des données qui sont stockées dans un tableau
	FLL[1]	Remplissage de fichier	Remplit les éléments d'un tableau avec des valeurs source, tout en laissant ces valeurs source inchangées
	FSC[1]	Recherche et comparaison de fichier	Compare les valeurs d'un tableau élément par élément
	SIZE[1]	Taille en éléments	Mesure la taille d'une dimension d'un tableau
Bit	XIC	Examine si contact fermé	Active les sorties lorsqu'un bit est activé
	XIO	Examine si contact ouvert	Active les sorties lorsqu'un bit est désactivé
	OTE	Activation de sortie	Active un bit
	OTL	Verrouillage de sortie	Active un bit (rémanent)
	OTU	Déverrouillage de sortie	Désactive un bit (rémanent)
	ONS	Exécution sur front	Déclenche un événement qui ne se produit qu'une fois
	OSR	Impulsion front montant	Déclenche un événement unique sur le front (montant) faux à vrai du changement d'état
	OSF	Impulsion front descendant	Déclenche un événement unique sur le front (descendant) vrai à faux du changement d'état
Temporisateur	TON	Temporisateur à l'enclenchement	Mesure la durée d'activation du temporisateur
	TOF	Temporisateur au déclenchement	Mesure la durée de désactivation du temporisateur
	RTO	Temporisateur rémanent	Cumule le temps
	CTU	Comptage progressif	Comptage progressif
	CTD	Comptage régressif	Comptage régressif
	RES	Remise à zéro	Réinitialise un temporisateur ou un compteur

Tableau 11 – Instructions de sécurité en logique à relais

Type	Mnémonique	Nom	Fonction
Comparaison	CMP[1][2]	Comparaison	Effectue une comparaison sur des opérations arithmétiques spécifiées dans une expression
	EQU	Egal à	Teste si deux valeurs sont égales
	GEQ	Supérieur ou égal à	Teste si une valeur est supérieure ou égale à une deuxième valeur
	GRT	Supérieur à	Teste si une valeur est supérieure à une deuxième valeur
	LEQ	Inférieur ou égal à	Teste si une valeur est inférieure ou égale à une deuxième valeur
	LES	Inférieur à	Teste si une valeur est inférieure à une deuxième valeur
	MEQ	Égalité par comparaison avec masque	Passe la source et compare les valeurs au travers d'un masque, et teste si elles sont égales
	NEQ	Différent de	Teste si une valeur est différente d'une deuxième valeur
	LIM	Test sur limites	Teste si une valeur figure dans une plage donnée
Transfert	CLR	Effacer	Efface une valeur
	COP[3]	Copie de fichier	Copie une valeur
	MOV	Transfert	Copie une valeur
	MVM	Transfert avec masque	Copie une partie spécifique d'un nombre entier
	SWPB[1]	Permutation d'octets	Réorganise les octets d'une valeur
Logique	AND	ET sur bits	Exécute une opération ET sur bits
	NOT	COMPLEMENT sur bits	Exécute une opération COMPLEMENT sur bits
	OR	OU sur bits	Exécute une opération OU sur bits
	XOR	OU exclusif sur bits	Exécute une opération OU exclusif sur bits
Commande de programme	JMP	Saut vers étiquette	Saute une portion de logique qui n'a pas besoin d'être systématiquement exécutée (passe à l'instruction Etiquette référencée)
	LBL	Etiquette	Attribue un nom d'étiquette à une instruction afin qu'elle puisse être référencée par une instruction JMP
	JSR	Saut vers un sous-programme	Passe à un sous-programme séparé
	RET	Retour	Renvoie les résultats d'un sous-programme
	SBR	Sous-programme	Passe des données à un sous-programme
	TND	Fin temporaire	Marque une fin temporaire qui arrête l'exécution du programme
	MCR	Relais de contrôle maître	Désactive toutes les lignes d'une portion de logique
	AFI	Toujours faux	Désactive une ligne
	NOP	Pas d'opération	Insère un marqueur dans la logique
	EVENT	Déclenchement d'une tâche événementielle	Déclenche l'exécution unique d'une tâche événementielle[5]
Mathématique/ Calcul	ADD	Addition	Additionne deux valeurs
	CPT[1]	Traitement	Exécute l'opération arithmétique qui est définie dans l'expression
	SUB	Soustraction	Soustrait deux valeurs
	MUL	Multiplication	Multiplie deux valeurs
	DIV	Division	Divise deux valeurs
	MOD	Modulo	Détermine le reste lorsqu'une valeur est divisée par une autre
	SQR	Racine carrée	Calcule la racine carrée d'une valeur
	NEG	Négation	Change le signe (+ ou -) d'une valeur
	ABS	Valeur absolue	Prend la valeur absolue d'une valeur
E/S	GSV[4]	Lire la valeur système	Lit les informations sur l'état de l'automate
	SSV[4]	Définir la valeur système	Définit les informations sur l'état de l'automate

(1) Prise en charge uniquement par les automates 1756-L7*x*S et 1756-L7*x*SXT. Pour les données de type REAL, un format à virgule flottante est pris en charge pour les programmes de sécurité par les automates 1756-L7*x*S et 1756-L7*x*SXT.

(2) Des opérandes évolués comme SIN, COS et TAN ne sont pas pris en charge dans les programmes de sécurité.

(3) L'opérande de longueur doit être une constante lorsque l'instruction COP est utilisée dans un programme de sécurité. La longueur de la source et celle de la destination doivent être identiques.

(4) Consultez la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur », pour les précautions particulières à respecter pour l'utilisation des instructions GSV et SSV.

(5) L'instruction événementielle déclenche la scrutation de la tâche standard.

IMPORTANT Si vous utilisez des commandes directes de mouvement avec un servovariateur Kinetix 5500, consultez la publication 2198-UM001, « Servovariateurs Kinetix 5500 Manuel utilisateur » pour des informations sur les modalités d'utilisation de cette fonction dans des applications de sécurité.

Pour des informations complémentaires, consultez les publications ci-après.

Tableau 12 – Documentation connexe

Ressource	Description
« GuardLogix Safety Application Instruction Set Reference Manual », publication 1756-RM095	Fournit des informations sur les instructions pour applications de sécurité.
Automates Logix5000 – Instructions – Manuel de référence, publication 1756-RM003	Contient des informations plus détaillées sur le jeu d'instructions Logix.

Instructions complémentaires de sécurité

Sujet	Page
Créer et utiliser une instruction complémentaire de sécurité	73
Documentation connexe	78

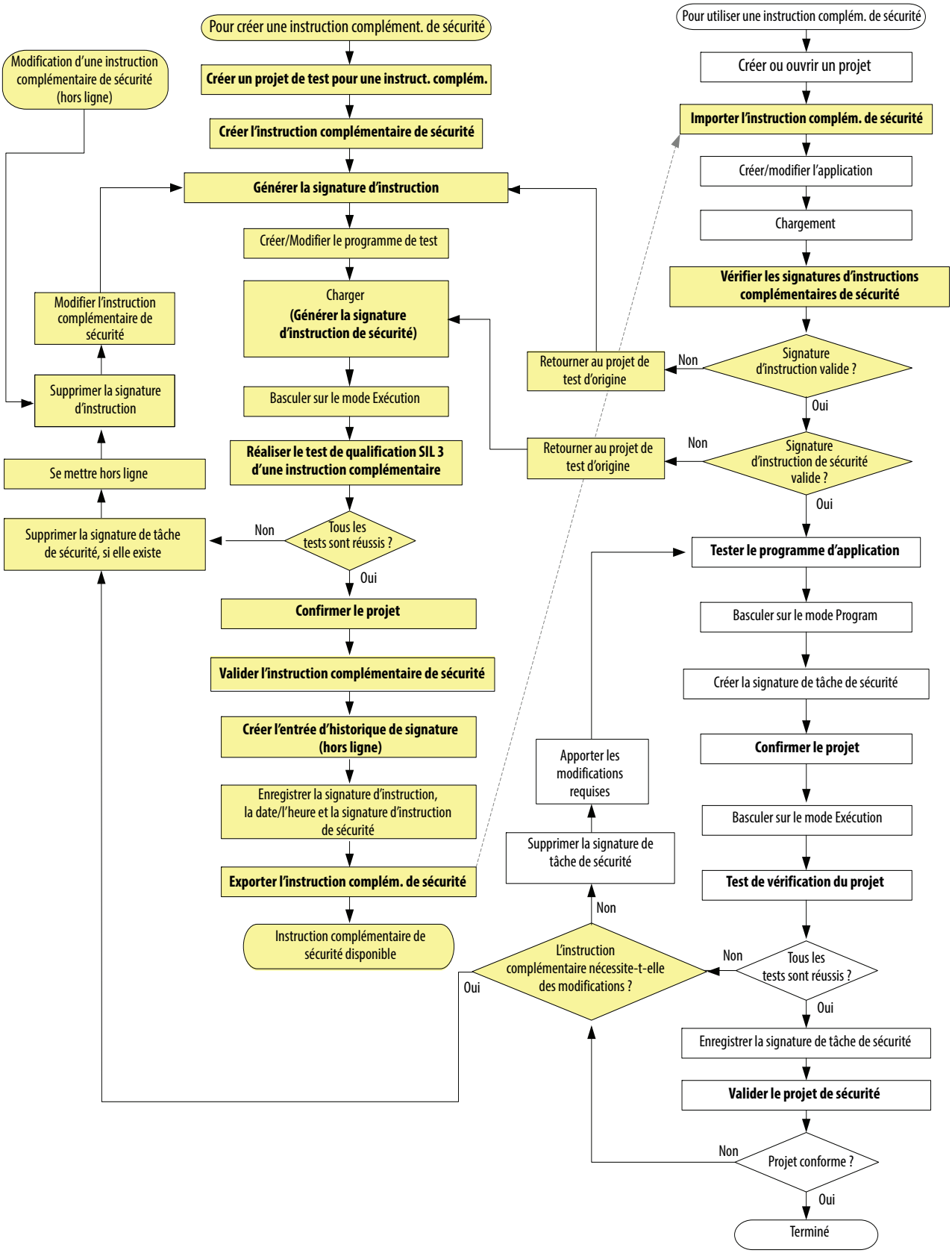
Avec l'application Logix Designer, vous pouvez créer des instructions complémentaires de sécurité. Celles-ci vous permettent d'encapsuler un programme de sécurité courant dans une instruction unique, ce qui le rend donc modulaire et réutilisable.

Les instructions complémentaires de sécurité utilisent la signature d'instruction des instructions complémentaires à haute intégrité et également une signature d'instruction de sécurité SIL 3 pour une utilisation dans les fonctions liées à la sécurité jusqu'au niveau SIL 3 inclus.

Créer et utiliser une instruction complémentaire de sécurité

L'organigramme de la page 74 affiche les étapes qui sont nécessaires pour créer une instruction complémentaire de sécurité, puis l'utiliser dans un programme d'application de sécurité SIL 3. Les éléments grisés constituent des étapes spécifiques aux instructions complémentaires. Les éléments en gras sont expliqués dans les pages qui suivent l'organigramme.

Figure 18 – Organigramme de création et d'utilisation des instructions complémentaires de sécurité



Créer un projet de test pour une instruction complémentaire

Vous devez créer un projet de test unique, dans le seul but de créer et de tester l'instruction complémentaire de sécurité. Il doit s'agir d'un projet dédié distinct, afin de réduire au minimum les influences imprévues.

Respectez les consignes relatives aux projets qui sont présentées à la section Création du projet, page 53.

Créer l'instruction complémentaire de sécurité

Pour en savoir plus sur la création d'instructions complémentaires, reportez-vous à la publication 1756-PM010, « Automates Logix5000 – Instructions complémentaires Manuel de programmation ».

Générer la signature d'instruction

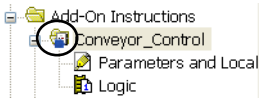
La signature d'instruction vous permet de déterminer rapidement si l'instruction a été modifiée. Chaque instruction complémentaire doit avoir sa propre signature. La signature d'instruction est requise en cas d'utilisation d'une instruction complémentaire dans des fonctions liées à la sécurité et peut parfois être exigée pour les industries réglementées. Utilisez-la lorsque votre application exige un niveau d'intégrité renforcé.

La signature d'instruction est constituée d'un identifiant (ID) et d'un horodatage servant à identifier le contenu de l'instruction complémentaire à un instant donné.

Une fois générée, la signature d'instruction scelle l'instruction complémentaire, ce qui empêche sa modification tant que la signature est valide. Cette protection s'applique aux commentaires des lignes, aux descriptions des points et à toute documentation d'instruction éventuellement créée. Une fois l'instruction scellée, vous pouvez uniquement effectuer les actions suivantes :

- copier la signature d'instruction ;
- créer ou copier l'entrée d'historique d'instruction ;
- créer des instances de l'instruction complémentaire ;
- charger l'instruction ;
- supprimer la signature d'instruction ;
- imprimer des rapports.

Lorsqu'une signature d'instruction a été générée, l'application Logix Designer affiche la définition de cette instruction avec une icône scellée.



IMPORTANT	Si vous envisagez de protéger votre instruction complémentaire au moyen de la fonction de protection de source de l'application Logix Designer, vous devez activer cette protection de source avant de générer la signature d'instruction.

Charger et générer la signature d'instruction de sécurité

Lorsqu'une instruction complémentaire de sécurité scellée est chargée pour la première fois, une signature d'instruction de sécurité SIL 3 est générée automatiquement. Cette signature est un identifiant qui détermine les caractéristiques d'exécution de l'instruction complémentaire de sécurité.

Test de qualification d'instruction complémentaire SIL 3

Les tests d'instruction complémentaire de sécurité SIL 3 doivent être réalisés dans une application distincte dédiée, afin de réduire au minimum les influences imprévues. Vous devez suivre un plan de test conçu avec soin et tester l'instruction complémentaire de sécurité qui suit tous les chemins d'exécution possibles dans le programme, notamment les plages valides et non valides de tous les paramètres d'entrée.

Le développement de toutes les instructions complémentaires de sécurité doit être conforme à la norme CEI 61508 – « Exigences relatives aux tests des modules logiciels », qui fournit des critères détaillés pour les tests.

Confirmer le projet

Vous devez imprimer ou afficher le projet et comparer manuellement les E/S de sécurité transférées et les configurations de l'automate, les données de sécurité, les définitions d'instructions complémentaires de sécurité et le programme de la tâche de sécurité pour vous assurer que les composants de sécurité adéquats ont été chargés, testés et retenus dans le programme de l'application de sécurité.

Reportez-vous à la section Confirmation du projet, page 55 pour la description d'une méthode de confirmation d'un projet.

Valider l'instruction complémentaire de sécurité

Une évaluation de l'instruction complémentaire de sécurité par un organisme indépendant peut s'avérer nécessaire pour que l'instruction soit homologuée en vue de son utilisation. Une validation par un organisme indépendant est requise pour le niveau SIL 3 selon la norme CEI 61508.

Créer l'entrée d'historique de signature

L'historique de la signature fournit un enregistrement utile pour les consultations futures. Une entrée d'historique de signature est constituée de la signature d'instruction, du nom de l'utilisateur, de la valeur d'horodatage et d'une description définie par l'utilisateur. Un maximum de six entrées d'historique peuvent être stockées. Il faut être hors ligne pour créer une entrée d'historique de signature.

CONSEIL La fonction d'édition de rapport Signature Listing (Liste des signatures) de l'application Logix Designer permet d'imprimer la signature d'instruction, l'horodatage et la signature d'instruction de sécurité. Pour imprimer le rapport, cliquez avec le bouton droit de la souris sur Add-On Instruction (Instruction complémentaire) dans la fenêtre Controller Organizer (Arborescence de l'automate) et sélectionnez Print>Signature Listing (Imprimer>Liste des signatures).

Exporter et importer l'instruction complémentaire de sécurité

Lorsque vous exportez une instruction complémentaire de sécurité, sélectionnez l'option appropriée pour inclure l'ensemble des instructions complémentaires référencées et des types définis par l'utilisateur dans le même fichier d'exportation. L'inclusion des instructions complémentaires référencées facilite la préservation des signatures.

Lors de l'importation d'instructions complémentaires, tenez compte des contraintes suivantes :

- vous ne pouvez pas importer une instruction complémentaire de sécurité dans un projet standard ;
- vous ne pouvez pas importer une instruction complémentaire de sécurité dans un projet de sécurité qui a été verrouillé ou qui comporte une signature de tâche de sécurité ;
- vous ne pouvez pas importer une instruction complémentaire de sécurité lorsque vous êtes en ligne ;
- si vous importez une instruction complémentaire avec une signature d'instruction dans un projet ne comportant pas d'instructions complémentaires référencées ou de types définis par l'utilisateur, il faudra peut-être supprimer la signature.

Vérifier les signatures d'instructions complémentaires de sécurité

Après le chargement du projet d'application contenant l'instruction complémentaire de sécurité importée, vous devez comparer les valeurs de la signature d'instruction, de la date, de l'heure et de la signature d'instruction de sécurité aux valeurs originales enregistrées avant l'exportation de l'instruction complémentaire de sécurité. Si les valeurs concordent, l'instruction complémentaire de sécurité est valable et vous pouvez poursuivre la validation de votre application.

Tester le programme d'application

Cette étape porte sur toute combinaison des modes Exécution et Programme, les modifications du programme en ligne ou hors ligne, les transferts et chargements, ainsi que les tests informels requis pour que l'application fonctionne correctement.

Test de vérification du projet

Effectuez un test technique de l'application, notamment du système de sécurité.

Voir Test de vérification du projet, page 54 pour plus d'informations sur les impératifs.

Valider le projet de sécurité

Une validation du système de sécurité par un organisme externe indépendant peut être requise avant de décréter ce système apte au fonctionnement. Une validation par un organisme indépendant est requise pour le niveau SIL 3 selon la norme CEI 61508.

Documentation connexe

Pour plus d'informations sur l'utilisation des instructions complémentaires, reportez-vous aux documentations suivantes :

Ressource	Description
« Automates Logix5000 – Instructions complémentaires Manuel de programmation », publication 1756-PM010	Fournit des informations sur la manière de planifier, créer, utiliser, importer, et exporter des instructions complémentaires dans les applications RSLogix 5000
« Importation/exportation de composants de projet – Manuel de programmation », publication 1756-PM019	Contient des informations détaillées sur la manière d'importer et d'exporter des composants de projet

Temps de réponse

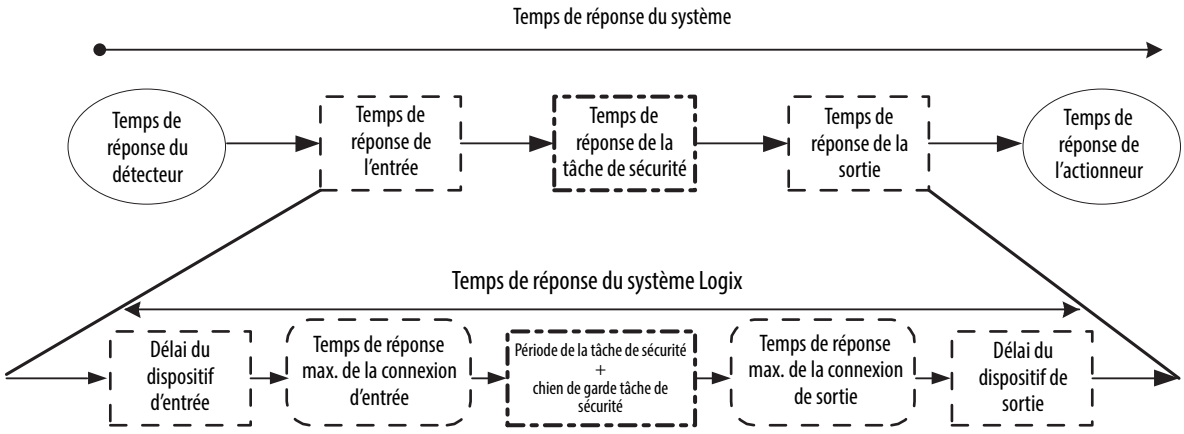
Sujet	Page
Temps de réponse du système	79
Temps de réponse du système Logix	79

Temps de réponse du système

Pour déterminer le temps de réponse du système pour n'importe quelle chaîne de commande, vous devez additionner les temps de réponse de tous les composants de la chaîne de sécurité.

Temps de réponse du système = Temps de réponse du détecteur + Temps de réponse du système Logix + Temps de réponse de l'actionneur

Figure 19 – Temps de réponse du système

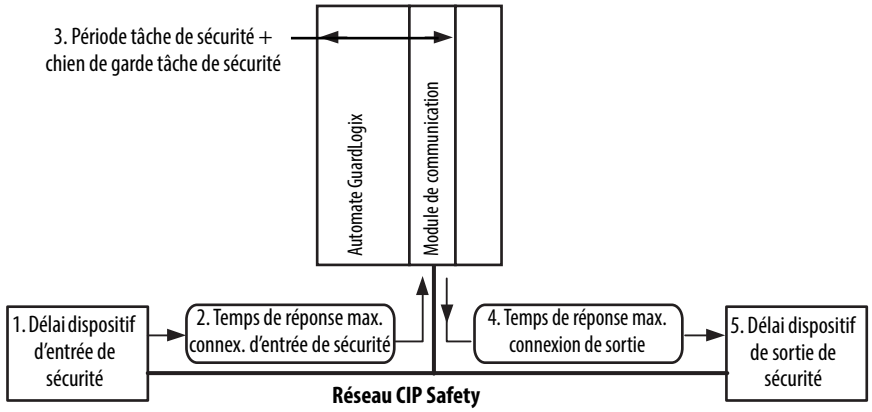


Temps de réponse du système Logix

Les sections qui suivent donnent des informations sur le calcul du temps de réponse du système Logix pour une chaîne Entrée-Programme-Sortie simple et pour une application plus complexe utilisant des points de sécurité produits/consommés dans la chaîne logique.

Chaîne Entrée-Programme-Sortie simple

Figure 20 – Temps de réponse du système Logix pour une chaîne Entrée-Programme-Sortie simple dans le cas le plus défavorable



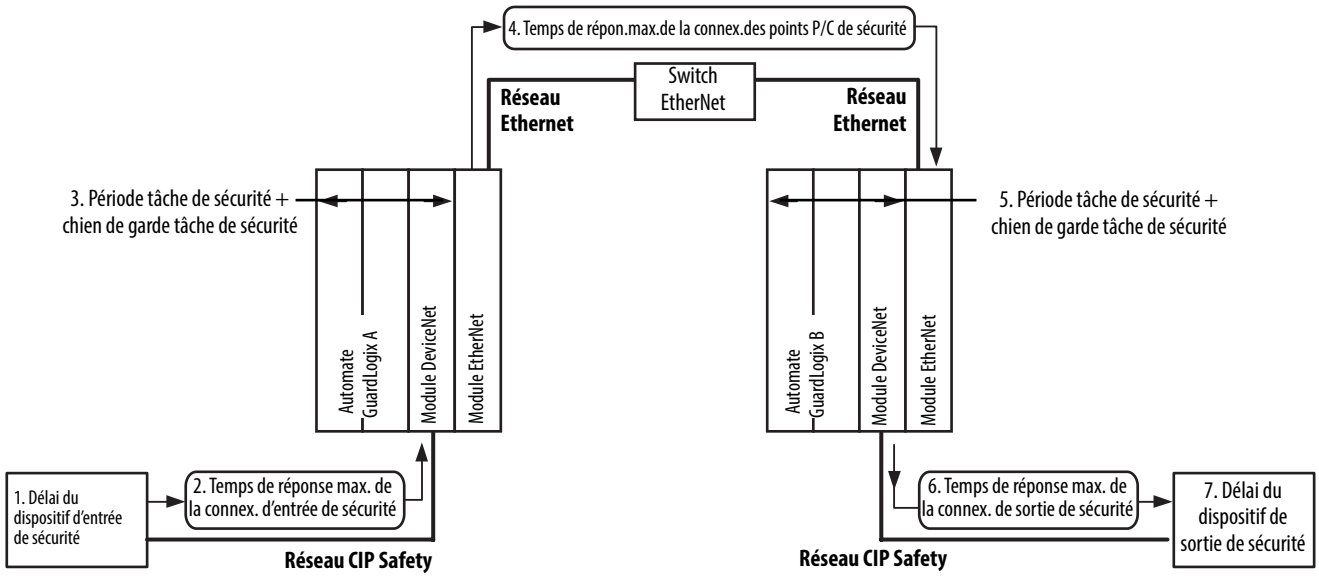
Le temps de réponse d'un système Logix pour une chaîne Entrée-Programme-Sortie simple est composé des cinq éléments suivants :

1. Temps de réponse du dispositif d'entrée de sécurité (plus délai d'entrée, le cas échéant)
2. Temps de réponse max. de la connexion d'entrée de sécurité (lu dans la boîte de dialogue Module Properties (Propriétés du module) de l'application Logix Designer – cette valeur est un multiple du RPI de la connexion du dispositif d'entrée de sécurité)
3. Période de la tâche de sécurité + temps du chien de garde de la tâche de sécurité
4. Temps de réponse max. de la connexion de sortie de sécurité (lu dans la boîte de dialogue Propriétés du module de l'application Logix Designer – cette valeur est un multiple de la période de la tâche de sécurité)
5. Temps de réponse du dispositif de sortie de sécurité

Pour vous aider à déterminer le temps de réponse de votre boucle de commande spécifique, une feuille de calcul Microsoft Excel est disponible dans le dossier Tools (outils) du DVD de l'environnement Studio 5000.

Chaîne logique utilisant des points de sécurité produits/consommés

Figure 21 – Temps de réponse du système Logix pour une chaîne Entrée-Programme automate A-Programme automate B-Sortie



Le temps de réponse du système Logix pour une chaîne Entrée-Programme automate A-Programme automate B-Sortie se compose des sept éléments suivants :

1. Temps de réponse du dispositif d'entrée de sécurité (plus délai d'entrée, le cas échéant)
2. Temps de réponse max. de la connexion d'entrée de sécurité
3. Période de la tâche de sécurité plus temps du chien de garde de la tâche de sécurité de l'automate A
4. Temps de réponse max. de la connexion de points produits/consommés de sécurité
5. Période de la tâche de sécurité plus temps du chien de garde de la tâche de sécurité de l'automate B
6. Temps de réponse max. de la connexion de sortie de sécurité
7. Temps de réponse du dispositif de sortie de sécurité.

Pour vous aider à déterminer le temps de réponse de votre boucle de commande spécifique, une feuille de calcul Microsoft Excel est disponible dans le dossier Tools (outils) du DVD de l'environnement Studio 5000.

Facteurs affectant les composants du temps de réponse Logix

Les composants du temps de réponse Logix décrits dans les sections précédentes peuvent être influencés par différents facteurs.

Tableau 13 – Facteurs affectant le temps de réponse du système Logix

Ces composants du temps de réponse	Sont influencés par les facteurs suivants
Délai du dispositif d'entrée	Temps de réponse du dispositif d'entrée
	Réglages de temporisation ON-OFF et OFF-ON pour chaque voie d'entrée, le cas échéant
Temps de réponse max. de la connexion d'entrée de sécurité	Réglages du dispositif d'entrée pour : • l'intervalle entre trames requis (RPI) ; • le multiplicateur de timeout ; • le multiplicateur de délai.
	Le volume du trafic de communication réseau
	L'environnement CEM du système
Période de la tâche de sécurité et chien de garde de la tâche de sécurité	Réglage de la période de la tâche de sécurité
	Réglage du chien de garde de la tâche de sécurité
	Nombre et temps d'exécution des instructions de la tâche de sécurité
	Tâches de priorité supérieure pouvant préempter l'exécution de la tâche de sécurité
Temps de réponse max. de la connexion de points produits/consommés de sécurité	Réglages du point consommé pour : • le RPI ; • le multiplicateur de timeout ; • le multiplicateur de délai.
	Le volume du trafic de communication réseau
	L'environnement CEM du système
Temps de réponse max. de la connexion de sortie	Réglage de la période de la tâche de sécurité
	Réglages du dispositif de sortie pour : • le multiplicateur de timeout ; • le multiplicateur de délai.
	Le volume du trafic de communication réseau
	L'environnement CEM du système
Délai du module de sortie	Temps de réponse du module de sortie

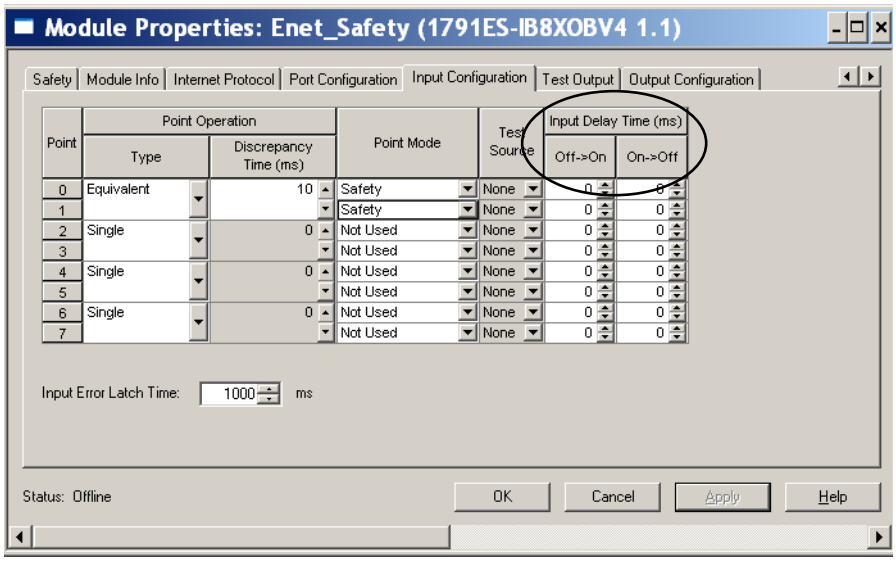
Les paragraphes suivants décrivent les procédures d'accès aux données ou aux paramètres de réglage d'une grande partie de ces facteurs.

Accès aux réglages de délai d'un module d'entrée Guard I/O

Pour configurer le délai d'un module d'entrée dans l'application Logix Designer, suivez ces étapes.

1. Dans l'arborescence de configuration, cliquez avec le bouton droit de la souris sur votre module Guard I/O et sélectionnez Properties (Propriétés).
2. Cliquez sur l'onglet Input Configuration (Configuration des entrées).

3. Réglez le délai d'entrée selon les besoins de votre application.



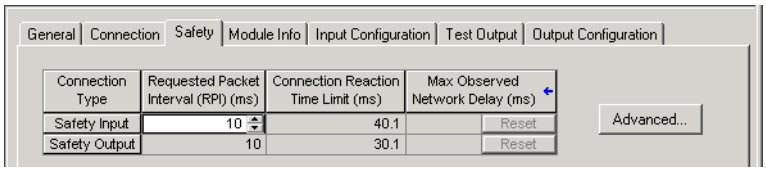
Accès au temps de réponse max. des connexions d'entrée et de sortie de sécurité

Le temps de réponse max. d'une connexion est défini par les trois paramètres suivants :

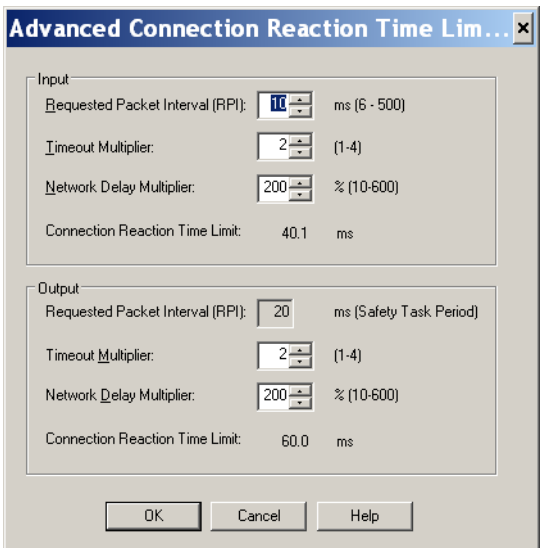
Valeur	Description
Intervalle entre trames requis (RPI)	Fréquence à laquelle les paquets d'entrée et de sortie sont envoyés sur le circuit (réseau).
Multiplicateur de timeout	Le multiplicateur de timeout représente essentiellement le nombre d'essais de reconnexion avant le timeout.
Multiplicateur de délai réseau	Le multiplicateur de délai réseau prend en compte toutes les sources de retards identifiées sur le réseau. Lorsque ces retards se produisent, des timeouts peuvent être évités grâce à ce paramètre.

En ajustant ces valeurs, vous pouvez définir le temps de réponse max. de la connexion. Pour visualiser ou configurer ces paramètres, suivez ces étapes.

1. Dans l'arborescence de configuration, cliquez avec le bouton droit de la souris sur votre dispositif d'E/S de sécurité et sélectionnez Properties (Propriétés).
2. Cliquez sur l'onglet Safety (Sécurité).



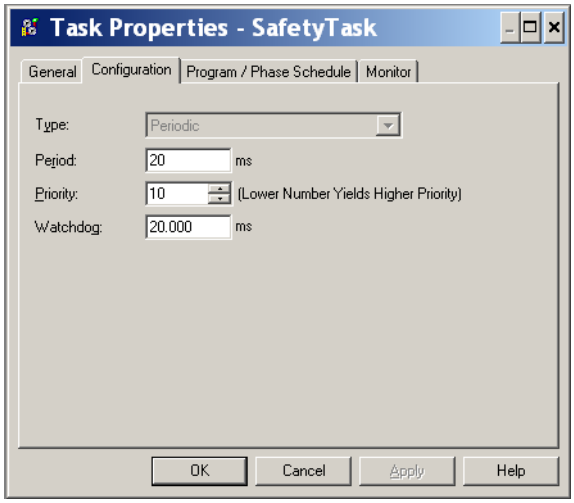
3. Cliquez sur Advanced (Avancé) pour ouvrir la boîte de dialogue Advanced Connection Reaction Time Limit (temps de réponse max. de connexion avancé).



Configuration de la période de la tâche de sécurité et du chien de garde

La tâche de sécurité est une tâche périodique temporisée. Vous pouvez choisir la priorité et le temps du chien de garde de cette tâche par l'intermédiaire de la boîte de dialogue Task Properties – Safety Task (Propriétés de tâche – Tâche de sécurité) dans votre projet Logix Designer.

Pour accéder aux réglages de la période et de temps du chien de garde de la tâche de sécurité, cliquez avec le bouton droit de la souris sur Safety Task (Tâche de sécurité) et sélectionnez Properties (Propriétés).

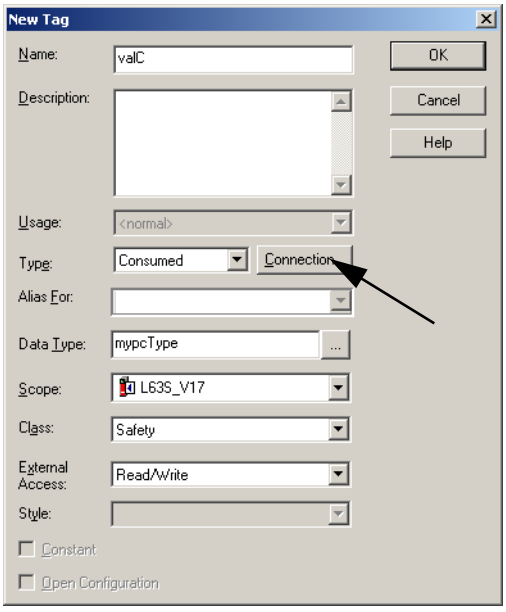


La priorité de la tâche de sécurité n'a pas un caractère de sécurité. Le chien de garde de cette tâche de sécurité se charge en effet de surveiller si elle est interrompue par une tâche de priorité plus élevée.

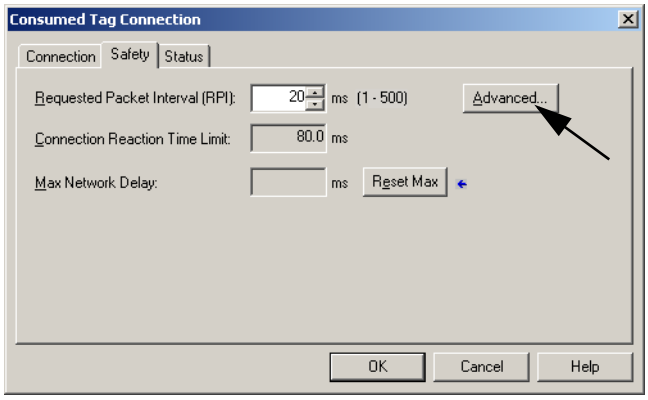
Accès aux données de point produit/consommé

Pour visualiser ou configurer les données des connexions de points de sécurité, suivez ces étapes.

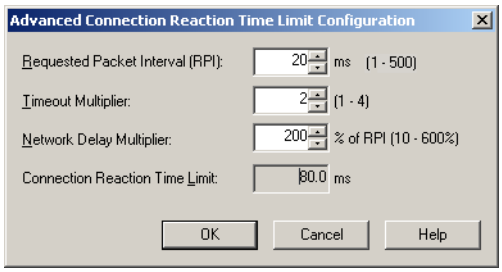
1. Dans l'arborescence de configuration, cliquez avec le bouton droit de la souris sur Controller Tags (Points d'automate) et choisissez Edit tags (Modifier les points).
2. Dans l'éditeur de points (Tag Editor), cliquez avec le bouton droit de la souris sur le nom du point et sélectionnez Edit Properties (Modifier les propriétés).
3. Cliquez sur Connection (Connexion).



4. Cliquez sur l'onglet Safety (Sécurité).



5. Cliquez sur Advanced (avancé) pour visualiser ou modifier les paramètres actuels.



Reportez-vous à la publication 1756-UM022, « Automates GuardLogix 5570 Manuel utilisateur », pour plus d'informations.

Listes de contrôle pour applications de sécurité GuardLogix

Sujet	Page
Liste de contrôle pour le système automate GuardLogix	88
Liste de contrôle pour les entrées de sécurité	89
Liste de contrôle pour les sorties de sécurité	90
Liste de contrôle pour le développement d'un programme d'application de sécurité	91

Les listes de contrôle présentées dans cette annexe sont nécessaires pour planifier, programmer et démarrer une application GuardLogix certifiée SIL 3. Elles peuvent être utilisées à titre de guides de planification et pendant le test de vérification du projet. Si vous les utilisez comme guides de planification, vous pouvez les enregistrer pour garder une trace de la planification.

Les listes de contrôle des pages suivantes sont des exemples de conditions de sécurité et non des listes exhaustives des éléments à vérifier. Votre application de sécurité peut avoir des exigences de sécurité supplémentaires que vous pouvez ajouter dans les espaces prévus à cet effet dans les listes de contrôle.

CONSEIL Faites des copies des listes de contrôle et gardez ces pages pour un usage ultérieur.

Liste de contrôle pour le système automate GuardLogix

Liste de contrôle pour le système GuardLogix				
Société				
Site				
Définition de la fonction de sécurité				
Numéro	**Impératifs du système**	**Effectué**		**Commentaires**
		Oui	**Non**	
1	Utilisez-vous uniquement les composants répertoriés au paragraphe Composants GuardLogix certifiés SIL 3, page 16 et sur le site http://www.rockwellautomation.com/products/certification/safety/ avec la version de firmware correspondante ?	☐	☐	
2	Avez-vous calculé le temps de réponse de sécurité du système pour chaque chaîne de sécurité ?	☐	☐	
3	Le temps de réponse du système inclut-il le chien de garde du programme de la tâche de sécurité défini par l'utilisateur (chien de garde du logiciel) et la fréquence/période de la tâche de sécurité ?	☐	☐	
4	Le temps de réponse du système est-il adapté au temps de tolérance du processus ?	☐	☐	
5	Les valeurs de probabilité (PFD/PFH) ont-elles été calculées en fonction de la configuration du système ?	☐	☐	
6	Avez-vous effectué tous les tests de vérification de projet adéquats ?	☐	☐	
7	Avez-vous déterminé de quelle manière le système gérera les défauts ?	☐	☐	
8	Chaque réseau du système de sécurité a-t-il un SNN unique ?	☐	☐	
9	Chaque dispositif CIP Safety est-il configuré avec le SNN approprié ?	☐	☐	
10	Avez-vous généré une signature de tâche de sécurité ?	☐	☐	
11	Avez-vous transféré et enregistré la signature de tâche de sécurité pour pouvoir la comparer par la suite ?	☐	☐	
12	Après un chargement, avez-vous vérifié que la signature de la tâche de sécurité de l'automate correspondait bien à la signature de la tâche de sécurité enregistrée ?	☐	☐	
13	Avez-vous mis en place un mécanisme de substitution pour protéger l'intégrité de la sécurité du système en cas de modifications en ligne ?	☐	☐	
14	Avez-vous tenu compte des listes de contrôle données aux pages 89 et 90 quant à l'utilisation des entrées et des sorties SIL ?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

Liste de contrôle pour les entrées de sécurité

Pour la programmation ou la mise en service, vous pouvez remplir une liste de contrôle individuelle pour chaque voie d'entrée SIL d'un système. C'est la seule façon de vous assurer que les impératifs sont clairement et pleinement respectés. Cette liste de contrôle peut également servir de documentation sur le raccordement du câblage externe au programme de l'application.

Liste de contrôle des entrées pour système GuardLogix				
Société				
Site				
Définition de la fonction de sécurité				
Voies d'entrée SIL				
Numéro	**Impératifs des dispositifs d'entrées**	**Effectué**		**Commentaires**
		Oui	**Non**	
1	Avez-vous suivi la notice d'installation ainsi que les consignes pour être conforme aux normes de sécurité en vigueur ?	☐	☐	
2	Avez-vous effectué les tests de vérification de projet sur le système et les dispositifs ?	☐	☐	
3	Les fonctions de commande, de diagnostic et d'alarme sont-elles exécutées séquentiellement dans le programme d'application ?	☐	☐	
4	Avez-vous transféré et comparé la configuration de chaque dispositif avec la configuration envoyée par l'outil de configuration ?	☐	☐	
5	Les dispositifs sont-ils câblés conformément au niveau PLe/Cat. 4 selon la norme ISO 13849-1 ?(1)	☐	☐	
6	Avez-vous vérifié si les caractéristiques électriques du détecteur et de l'entrée étaient compatibles ?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) Pour de plus amples informations sur le câblage de votre dispositif d'E/S CIP Safety, reportez-vous à la documentation de votre dispositif.

Liste de contrôle pour les sorties de sécurité

Pour la programmation ou la mise en service, vous pouvez remplir une liste de contrôle individuelle pour chaque voie de sortie SIL d'un système. C'est la seule façon de vous assurer que les impératifs sont clairement et pleinement respectés. Cette liste de contrôle peut également servir de documentation sur le raccordement du câblage externe au programme de l'application.

Liste de contrôle des sorties pour système GuardLogix				
Société				
Site				
Définition de la fonction de sécurité				
Voies de sortie SIL				
Numéro	**Impératifs des dispositifs de sorties**	**Effectué**		**Commentaires**
		Oui	**Non**	
1	Avez-vous suivi la notice d'installation ainsi que les consignes pour être conforme aux normes de sécurité en vigueur ?	☐	☐	
2	Avez-vous effectué les tests de vérification de projet sur les dispositifs ?	☐	☐	
3	Avez-vous transféré et comparé la configuration de chaque dispositif avec la configuration envoyée par l'outil de configuration ?	☐	☐	
4	Vous êtes vous assuré que les sorties de test ne sont pas utilisées comme sorties de sécurité ?	☐	☐	
5	Les dispositifs sont-ils câblés conformément au niveau PLe/Cat. 4 selon la norme ISO 13849-1 ?(1)	☐	☐	
6	Avez-vous vérifié si les caractéristiques électriques de la sortie et de l'actionneur étaient compatibles ?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) Pour de plus amples informations sur le câblage de votre dispositif d'E/S de sécurité, reportez-vous à la documentation de votre dispositif.

Liste de contrôle pour le développement d'un programme d'application de sécurité

Utilisez la liste de contrôle suivante pour vous aider à maintenir la sécurité lorsque vous créez ou modifiez un programme d'application de sécurité.

Liste de contrôle pour le développement d'un programme d'application GuardLogix				
Société				
Site				
Définition du projet				
Numéro	**Impératifs du programme d'application**	**Effectué**		**Commentaires**
		Oui	**Non**	
1	Utilisez-vous la version 21 ou ultérieure de l'application Logix Designer, l'outil de programmation des systèmes GuardLogix ?	☐	☐	
2	Avez-vous suivi les consignes de programmation présentées au Chapitre 6 lors de la création de votre programme d'application de sécurité ?	☐	☐	
3	Le programme de l'application de sécurité contient-il uniquement de la logique à relais ?	☐	☐	
4	Le programme de l'application de sécurité contient-il uniquement les instructions indiquées à l'Annexe A, adaptées à la programmation d'une application de sécurité ?	☐	☐	
5	Le programme d'application de sécurité fait-il clairement la distinction entre les points standard et les points de sécurité ?	☐	☐	
6	Est-ce que seuls des points de sécurité sont utilisés pour les sous-programmes de sécurité ?	☐	☐	
7	Vous êtes-vous assuré que les sous-programmes de sécurité ne tentent pas de lire ou d'écrire dans des points standard ?	☐	☐	
8	Vous êtes-vous assuré qu'aucun point de sécurité n'est l'alias d'un point standard ou vice-versa ?	☐	☐	
9	Chaque point de sortie de sécurité est-il correctement configuré et connecté à une voie de sortie physique ?	☐	☐	
10	Vous êtes-vous assuré que tous les points adressés ont été conditionnés dans le programme de l'application de sécurité ?	☐	☐	
11	Avez-vous défini les paramètres du procédé surveillés par les sous-programmes de gestion des défauts ?	☐	☐	
12	Avez-vous scellé des instructions complémentaires de sécurité avec une signature d'instruction et enregistré la signature d'instruction de sécurité ?	☐	☐	
13	Le programme a-t-il été revu par un organisme de sécurité indépendant (s'il y a lieu) ?	☐	☐	
14	Cette révision a-t-elle été documentée et signée ?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

Notes :

Données de sécurité des systèmes GuardLogix

Sujet	Page
Valeurs de PFD	93
Valeurs de PFH	94

Les exemples suivants présentent des valeurs de probabilité de défaillance sur sollicitation (PFD) et de probabilité de défaillance par heure (PFH) pour des systèmes GuardLogix 1oo2 SIL 3 qui utilisent des modules Guard I/O.

Le temps de mission des automates GuardLogix et des modules Guard I/O est de 20 ans.

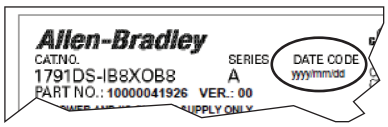
Valeurs de PFD

Tableau 14 – PFD calculée selon la périodicité des tests de vérification

Référence	Description	PFD calculée			
		2 ans (17 520 heures)	5 ans (43 800 heures)	10 ans (87 600 heures)	20 ans (175 200 heures)
1756-L7*x*S et 1756-L7SP	Automate GuardLogix	5,7E-06	1,5 E-05	3,5 E-05	8,9 E-05
1756-L73SXT et 1756-L7SPXT	Automate GuardLogix XT	5,7E-06	1,5 E-05	3,5 E-05	8,9 E-05
1791DS-IB12	Module de 12 entrées CIP Safety	4,73E-07	1,18E-06	2,35E-06	4,71E-06(2)
1791DS-IB16	Module 16 entrées CIP Safety	4,11E-06	1,03E-05	2,06E-05	4,11E-05
1791DS-IB8XOB8	Module 8 entrées/8 sorties CIP Safety	4,73E-07	1,18E-06	2,35E-06	4,71 E-06(2)
1791DS-IB4XOW4	Module 4 entrées/4 sorties relais CIP Safety	2,21E-05	7,05E-05	1,92E-04	5,88 E-04(2)
1791DS-IB8XOBV4	Module 8 entrées/4 sorties bipolaires CIP Safety	4,16E-06	1,04E-05	2,08E-05	4,16E-05
1732DS-IB8XOBV4					
1732DS-IB8	Module 8 entrées CIP Safety	4,11E-06	1,03E-05	2,06E-05	4,11E-05
1791ES-IB16	Module 16 entrées CIP Safety	4,13E-06	1,03E-05	2,06E-05	—
1791ES-IB8XOBV4	Module 8 entrées/4 sorties bipolaires CIP Safety	4,17E-06	1,04E-05	2,09E-05	—
1734-IB8S, Série A	Module 8 entrées CIP Safety	4,23E-06	1,06E-05	2,11E-05	4.23-05
1734-IB8S, Série B(1)	Module 8 entrées CIP Safety	4,36E-06	1,09E-05	2,18E-05	4,36E-05
1734-OB8S, Série A	Module 8 sorties CIP Safety	4,27E-06	1,07E-05	2,13E-05	4,27E-05
1734-OB8S, Série B	Module 8 sorties CIP Safety	4,32E-06	1,08E-05	2,16E-05	4,32E-05
1734-IE4S	Module de 4 entrées analogiques CIP Safety, fonctionnement mono voie	4,7E-07	1,2E-06	2,4E-06	4,8E-06
1734-IE4S	Module de 4 entrées analogiques CIP Safety, fonctionnement double voie	3,2 E-07	8,1 E-07	1,6 E-06	3,3 E-06

(1) Ces données correspondent à un fonctionnement mono voie et double voie.

(2) Ces caractéristiques de PFD sur 20 ans s'appliquent uniquement aux produits ayant un code de date de fabrication égal ou ultérieur à 2009/01/01 (1er janvier 2009). Consultez l'étiquette du produit pour le code de date.



Valeurs de PFH

Les données ci-après s'appliquent aux périodicités de test de vérification jusqu'à 20 ans inclus.

Tableau 15 – Calcul du PFH

Référence	Description	PFH (1/heure)
1756-L7xS et 1756-L7SP	Automate GuardLogix	1,2 E-09
1756-L7xSXT et 1756-L7SPXT	Automate GuardLogix-XT	1,2 E-09
1791DS-IB12	Module 12 entrées CIP Safety	5,77E-11(1)
1791DS-IB16	Module 16 entrées CIP Safety	4,96E-10
1791DS-IB8XOB8	Module 8 entrées/8 sorties CIP Safety	5,77 E-11(1)
1791DS-IB4XOW4	Module 4 entrées/4 sorties relais CIP Safety	9,03 E-09(1)
1791DS-IB8XOBV4	Module 8 entrées/4 sorties bipolaires CIP Safety	5,02E-10
1732DS-IB8XOBV4		
1732DS-IB8	Module 8 entrées CIP Safety	4,96E-10
1791ES-IB16	Module 16 entrées CIP Safety	4,98E-10
1791ES-IB8XOBV4	Module 8 entrées/4 sorties bipolaires CIP Safety	5,04E-10
1734-IB8S, Série A	Module 8 entrées CIP Safety	5,10E-10
1734-IB8S, Série B	Module 8 entrées CIP Safety	5,27E-10
1734-OB8S, Série A	Module 8 sorties CIP Safety	5,14E-10
1734-OB8S, Série B	Module 8 sorties CIP Safety	5,20E-10
1734-IE4S	Module 4 entrées analogiques CIP Safety, fonctionnement mono voie Module 4 entrées analogiques CIP Safety, fonctionnement double voie	5,6E-11 3,9 E-11

(1) Ces caractéristiques de PFH s'appliquent uniquement aux produits ayant un code de date de fabrication égal ou ultérieur à 2009/01/01 (1er janvier 2009). Consultez l'étiquette du produit pour le code de date.

Logiciel RSLogix 5000, version 14 et ultérieure ; instructions pour applications de sécurité

Sujet	Page
Système à déclenchement par mise hors tension	95
Utilisation des données d'état de connexion pour générer un défaut par programmation	95

Système à déclenchement par mise hors tension

Lorsque les instructions pour application de sécurité du logiciel RSLogix 5000 en version 14 sont utilisées, toutes les entrées et les sorties sont remises à zéro quand un défaut est détecté. Par conséquent, toutes les entrées qui sont surveillées par une des instructions d'entrées complémentaires (entrées complémentaires ou station bimanuelle) doivent avoir des entrées normalement fermées conditionnées par une logique similaire à celle de la ligne 4 de l'Exemple de logique à relais 2 et de l'Exemple de logique à relais 3, aux pages 98 et 99. La logique précise exigée dépend à la fois de l'application et du dispositif d'entrée. Cependant, la logique doit créer un état de sécurité de 1 pour l'entrée normalement fermée des instructions d'entrées complémentaires.

Utilisation des données d'état de connexion pour générer un défaut par programmation

Les schémas suivants sont des exemples du programme logique nécessaire pour verrouiller et réinitialiser les défaillances d'E/S. Ces exemples montrent la logique nécessaire pour les modules d'entrée uniquement, ainsi que pour les modules mixtes d'entrée/sortie. Ils utilisent une fonction Combined Status (Etat combiné) des modules d'E/S, qui présente l'état de toutes les voies d'entrée dans une seule variable booléenne. Une autre variable booléenne représente l'état de toutes les voies de sortie. Cette approche réduit la quantité de logique de conditionnement d'E/S nécessaire et force la logique à arrêter toutes les voies d'entrée ou de sortie du module concerné.

Utilisez l'Organigramme de verrouillage et de réinitialisation du défaut d'une entrée, page 96, pour déterminer les lignes de logique nécessaires selon les différentes situations d'application. L'Exemple de logique à relais 1 montre une logique qui écrase les variables réelles du point d'entrée en présence d'une condition de défaut. Si l'état réel de l'entrée est nécessaire pour le dépannage alors que le défaut d'entrée est verrouillé, utilisez la logique illustrée dans l'Exemple de logique à relais 2. Cette logique se sert des points internes qui représentent les entrées à employer dans la logique de l'application. Lorsque la défaillance de l'entrée est verrouillée, les points internes sont réglés sur leur état de sécurité. Lorsque la défaillance de l'entrée n'est pas verrouillée, les valeurs de l'entrée réelle sont copiées dans les points internes.

Utilisez l'Organigramme de verrouillage et de réinitialisation du défaut d'une sortie pour déterminer quelles lignes du programme d'application de l'Exemple de logique à relais 3, page 99, sont nécessaires.

Figure 22 – Organigramme de verrouillage et de réinitialisation du défaut d'une entrée

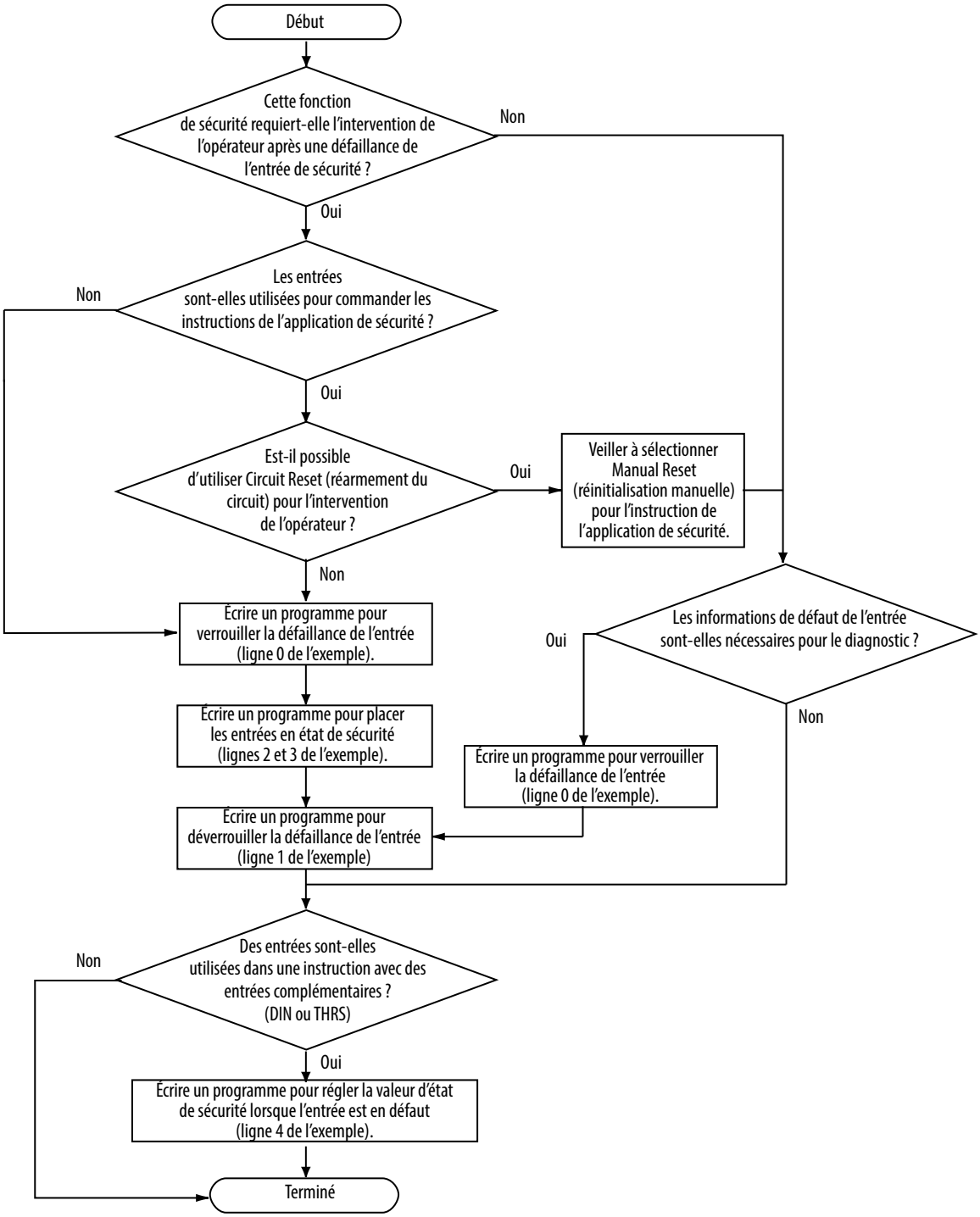


Figure 23 – Exemple de logique à relais 1

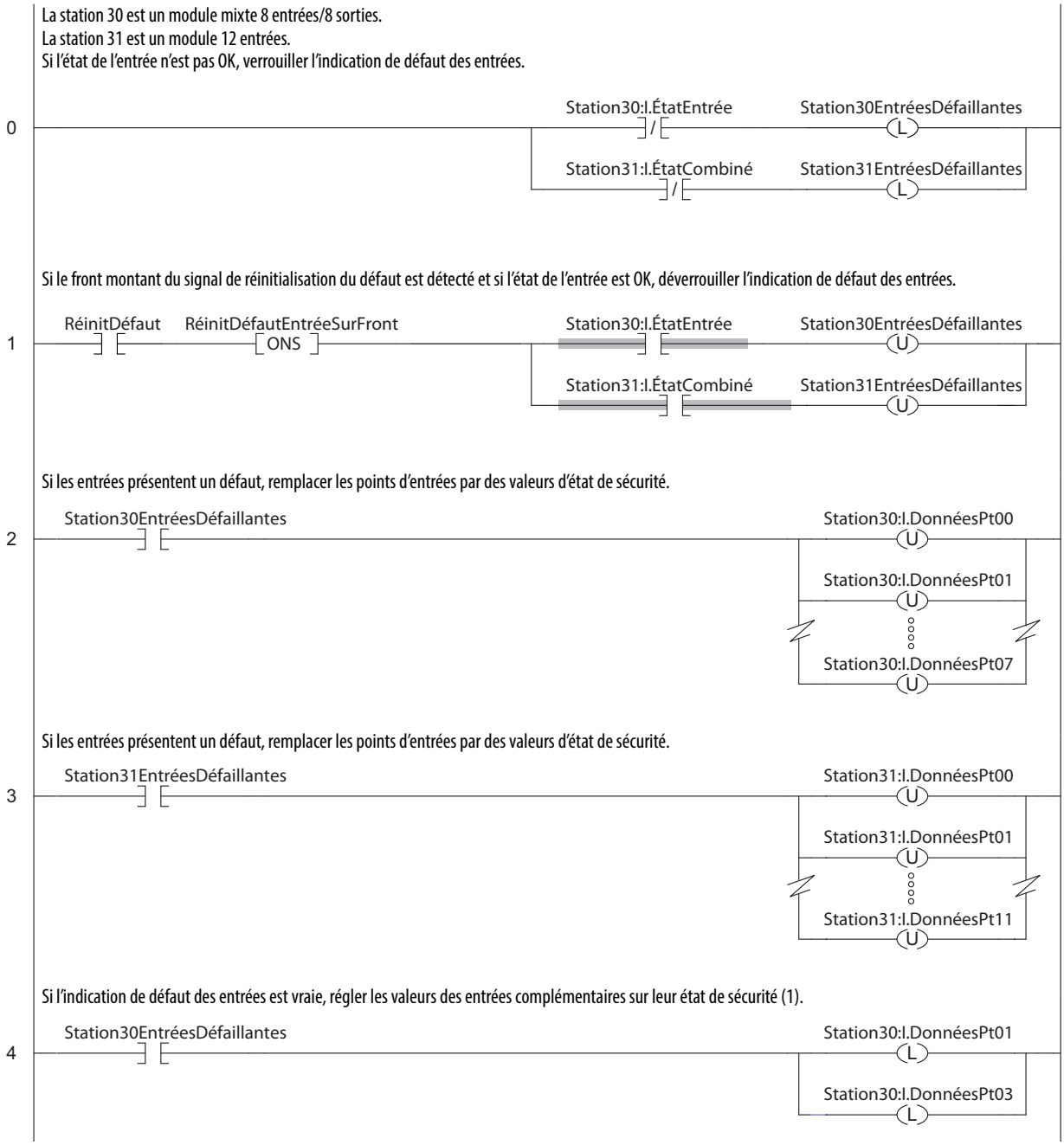


Figure 24 – Exemple de logique à relais 2

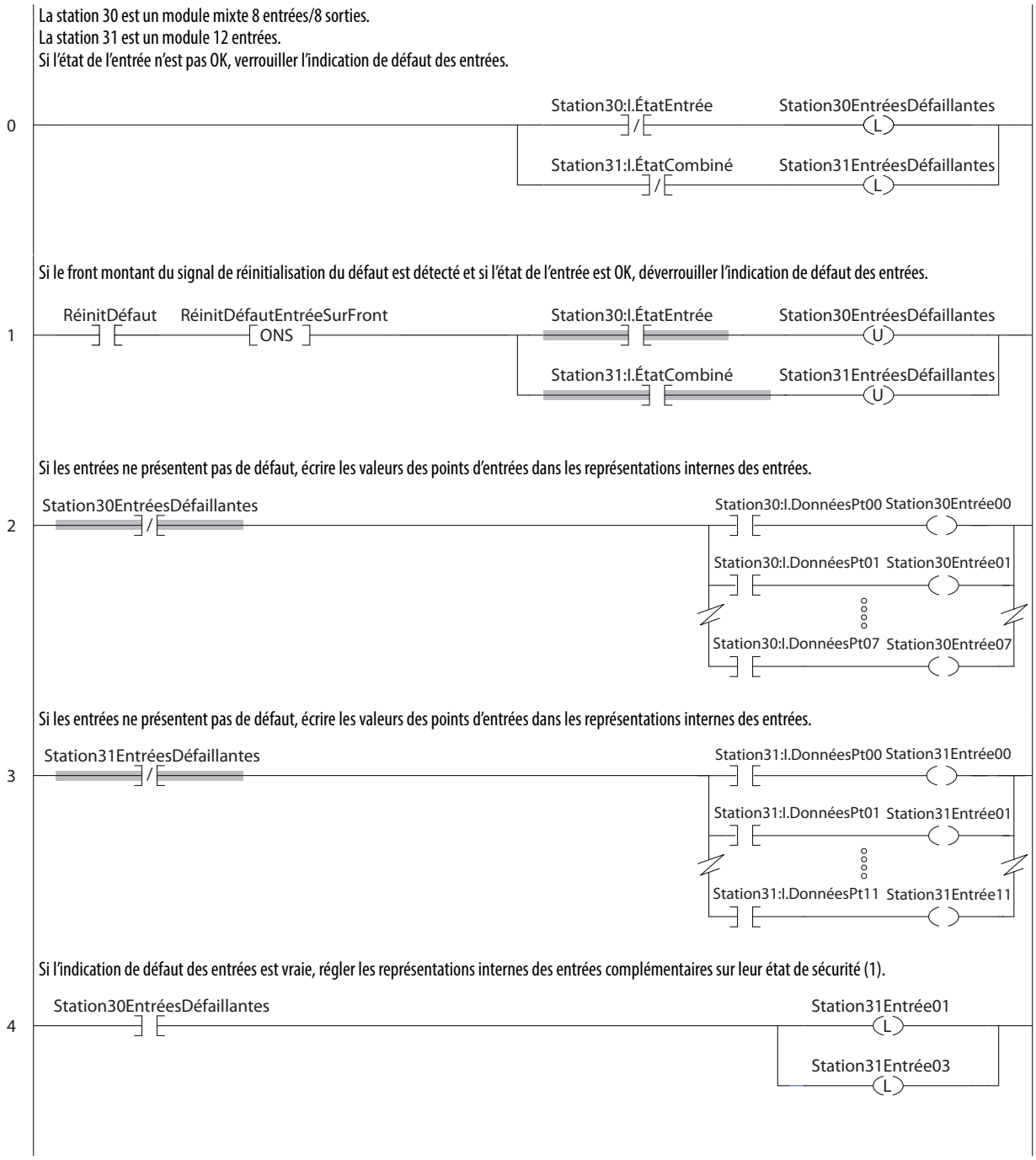


Figure 25 – Organigramme de verrouillage et de réinitialisation du défaut d'une sortie

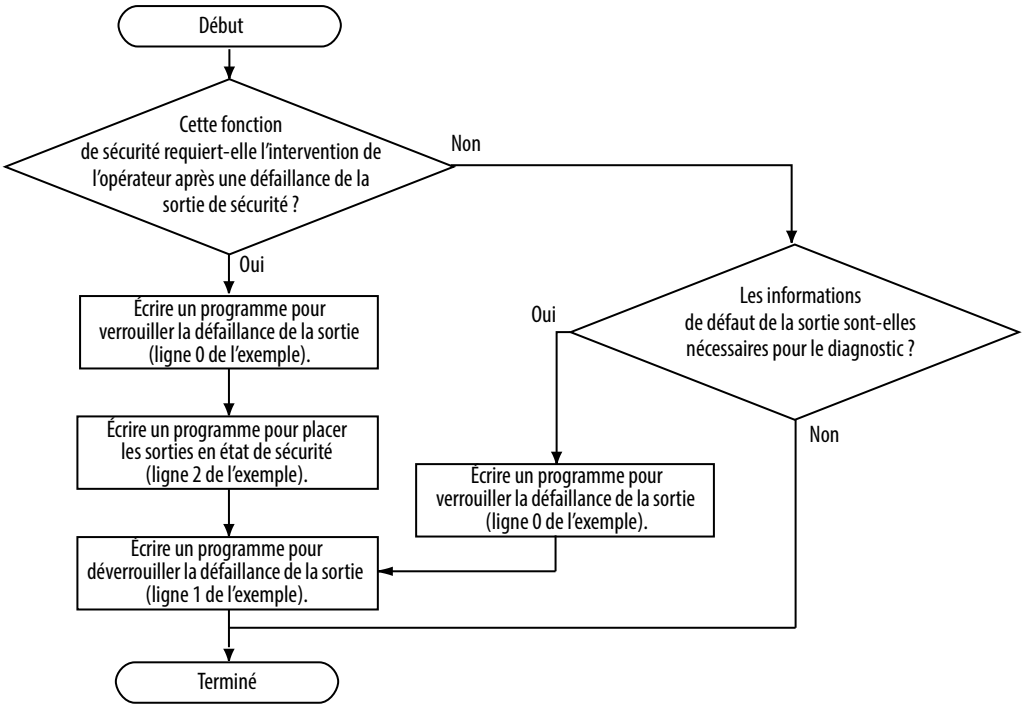
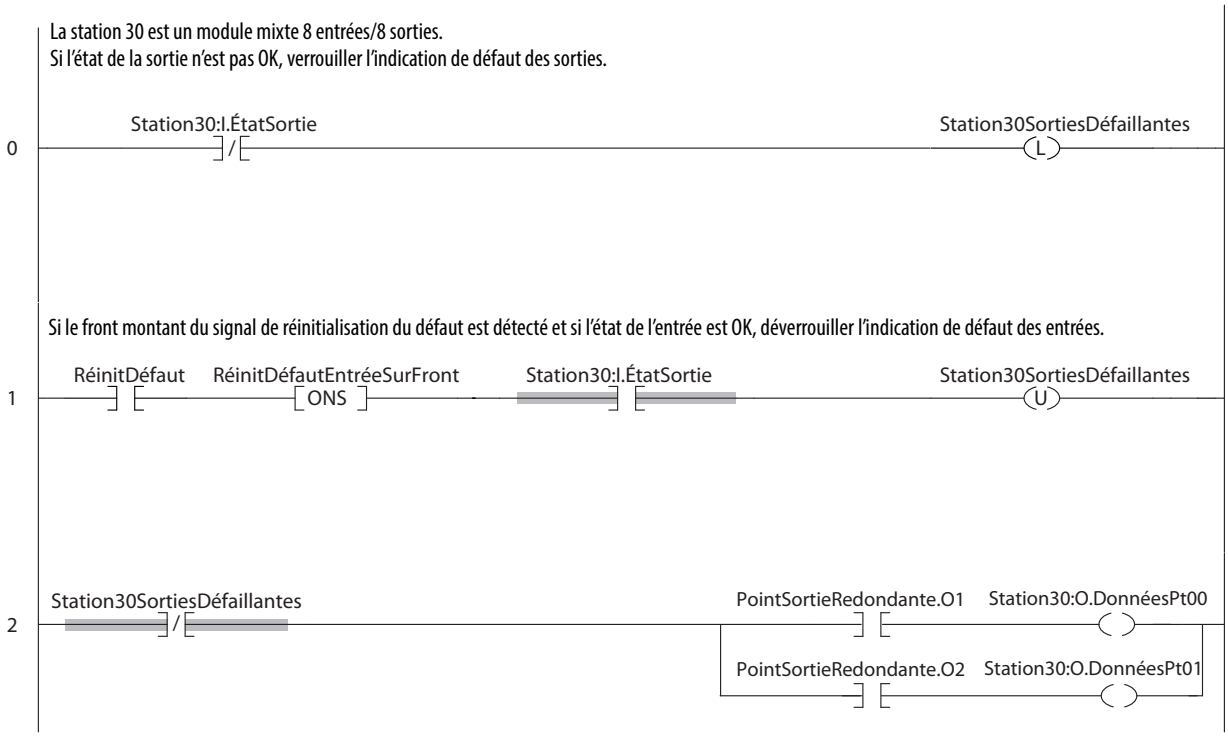


Figure 26 – Exemple de logique à relais 3



Notes :

Utilisation de modules d'E/S FLEX I/O 1794 et d'entrées/sorties 1756 SIL 2 avec des automates GuardLogix 1756, conformément à la norme EN 50156

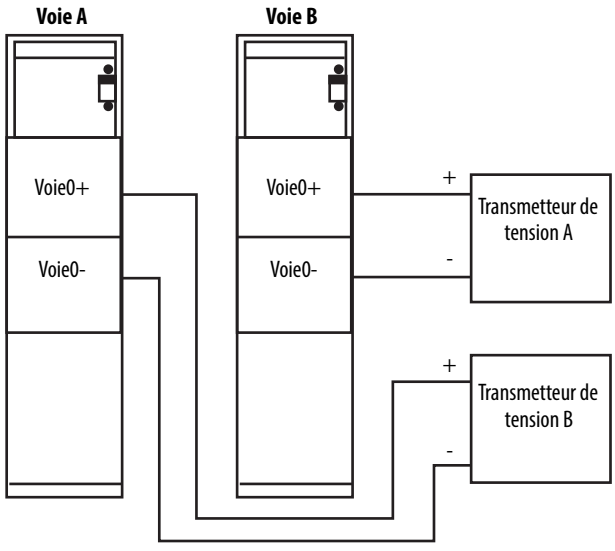
Sujet	Page
Entrées double voie SIL 2 (partie standard des automates GuardLogix)	101
Sorties SIL 2 utilisant des modules de sortie SIL 3 Guard I/O	103
Sorties SIL 2 utilisant des modules de sortie SIL 2 1756 ou 1794	103
Fonctions de sécurité dans la tâche de sécurité de l'automate GuardLogix 1756	104

Une configuration à double voie est nécessaire pour garantir la conformité de certaines applications de sécurité, notamment les -sécurités d'interruption d'alimentation de brûleurs. Les exemples suivants fournissent des recommandations pour se conformer aux exigences de double voie SIL 2 avec intervalles entre les tests de vérification de 1 et 2 ans, de la norme EN50156 .

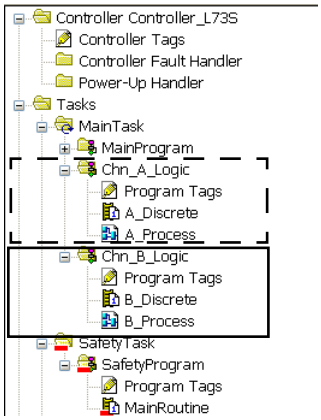
Entrées double voie SIL 2 (partie standard des automates GuardLogix)

Vous devez instaurer une séparation claire et facilement identifiable entre les deux voies d'entrées et respecter toutes les exigences SIL 2 existantes, telles que définies dans la publication 1756-RM001, « Using ControlLogix in SIL 2 Applications ».

Figure 27 – Exemple F d'entrées double voie SIL 2



Données d'entrées SIL 2



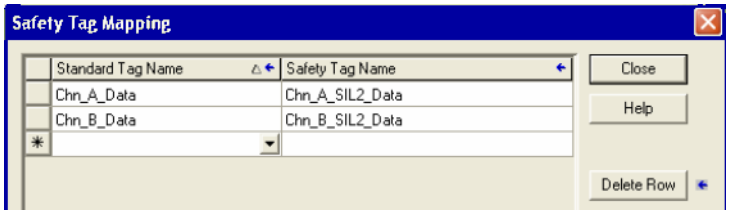
Maintenez toujours la séparation entre les données d'entrée de la voie A et de la voie B. Cet exemple illustre une méthode de séparation des données de la voie A et de la voie B dans votre application.

Conformez-vous à l'ensemble des règles définies pour les modules d'E/S 1756 et les modules d'E/S FLEX™ I/O 1794 dans la publication 1756-RM001, « Using ControlLogix in SIL 2 Applications Safety Reference Manual ».

IMPORTANT N'exécutez pas de fonctions spécifiques à la sécurité dans ces sous-programmes. L'évaluation de la sécurité doit être gérée dans la tâche de sécurité de l'automate GuardLogix 1756.

Transfert des données SIL 2 dans la tâche de sécurité

Pour transférer les données SIL 2 des voies A et B vers la tâche de sécurité GuardLogix, utilisez la fonction d'adressage des points de sécurité de l'application Logix Designer. Les noms de points utilisés ici ont uniquement valeur d'exemple. Mettez en œuvre et respectez les conventions de dénomination pertinentes pour votre application.



CONSEIL Pour accéder à la fonction d'adressage des points de sécurité, sélectionnez Map Safety Tags (Adressage des points de sécurité) dans le menu Logic (Programme) de l'application Logix Designer.

Sorties SIL 2 utilisant des modules de sortie SIL 3 Guard I/O

Respectez les consignes suivantes pour les sorties SIL 2 :

- les modules de sorties Guard I/O qui sont utilisés pour les sorties de sécurité SIL 2 doivent être configurés pour le fonctionnement double voie ;
- tous les modules de sorties Guard I/O sont homologués pour une utilisation dans des applications SIL 2.
  - 1732DS-IB8XOBV4
  - 1791ES-IB8XOBV4
  - 1791DS-IB8XOBV4, 1791ES-IB8XOBV4
  - 1791DS-IB4XOW4
  - 1791DS-IB8XOB8
  - 1734-OB8S

Sorties SIL 2 utilisant des modules de sortie SIL 2 1756 ou 1794

Lorsque vous utilisez ces modules de sortie homologués SIL 2, vous êtes tenus de configurer vos sorties de sécurité SIL 2 comme des points de sécurité produits par GuardLogix pour respecter les exigences de double voie de la norme EN 50156.

Créez les points de sécurité produits avec les sorties SIL 2 dont votre application a besoin. Les points de sécurité produits/consommés GuardLogix nécessitent que leur premier membre soit réservé aux diagnostics. Le premier élément d'une connexion de sécurité produite/consommée doit donc être constitué par une donnée appelée CONNECTION_STATUS (Etat de la connexion). L'exemple ci-dessous montre un point SIL 2 composé de deux éléments INT et deux éléments BOOL. Ces points de sécurité SIL 2 sont utilisés pour commander directement les sorties SIL 2 1756 ou 1794.

Name	Alias For	Base Tag	Data Type	Class	Description	External Access	Constant	Style
-SIL2_Outputs			SIL_2_Produced	Safety		Read/Write	☐	
+ SIL2_Outputs.Connection_Status			CONNECTION_STA	Safety		Read/Write		
+ SIL2_Outputs.SIL2_TempA			INT	Safety		Read/Write		Decimal
+ SIL2_Outputs.SIL2_TempB			INT	Safety		Read/Write		Decimal
SIL2_Outputs.SIL2_Valve1			BOOL	Safety		Read/Write		Binary
SIL2_Outputs.SIL2_Valve2			BOOL	Safety		Read/Write		Binary

CONSEIL Dans cet exemple, il n'est pas indiqué de consommateur pour le point produit. L'état de la connexion affiche un défaut si vous ne configurez pas ce consommateur. Néanmoins, dans ce type de configuration, vous n'êtes pas obligé(e) de surveiller l'état de la connexion du point produit. Ce défaut ne tirera donc pas à conséquence.

Conformez-vous à l'ensemble des règles définies pour les modules d'E/S 1756 et les modules d'E/S FLEX™ I/O 1794 dans la publication 1756-RM001, « Using ControlLogix in SIL 2 Applications Safety Reference Manual ».

Fonctions de sécurité dans la tâche de sécurité de l'automate GuardLogix 1756

Respectez les consignes suivantes pour l'utilisation des fonctions de sécurité SIL 2 et SIL 3 dans la tâche de sécurité :

- toutes les instructions d'application de sécurité disponibles peuvent être utilisées ;
- les modules d'entrée de sécurité SIL (autrement dit, les modules Guard I/O) peuvent être utilisés avec la configuration à simple voie pour les fonctions de sécurité SIL 2 ;
- l'utilisation de la signature de tâche de sécurité et le verrouillage de sécurité de l'application sont recommandés.

IMPORTANT Vous ne devez pas employer les données SIL 2 pour commander directement une sortie SIL 3.

Les termes et abréviations définis à la suite sont utilisés tout au long de ce manuel. Pour la définitions des termes qui ne sont pas mentionnés dans cette liste, reportez-vous au glossaire Allen-Bradley de l'automation industriel, publication AG-7.1.

Adressage symbolique Méthode d'adressage permettant une interprétation en ASCII du nom du point.

Annuler les éditions Action effectuée pour rejeter toute modification en ligne non assemblée.

Assembler les éditions Vous assemblez les éditions lorsque vous avez apporté des modifications en ligne dans le programme de l'automate et que vous souhaitez rendre ces modifications permanentes afin de pouvoir les tester, désactiver leur test ou les annuler.

Automate principal Processeur d'un automate à deux processeurs, qui exécute les fonctions d'un automate standard et communique avec le partenaire de sécurité pour l'exécution des fonctions de sécurité.

Automate standard Dans le présent manuel, un automate standard désigne généralement un automate ControlLogix.

Chevauchement Il y a chevauchement lorsqu'une tâche (périodique ou événementielle) est déclenchée alors que sa précédente exécution est toujours en cours.

Chien de garde de la tâche de sécurité Durée maximale autorisée entre le début et la fin de l'exécution de la tâche de sécurité. Le dépassement de la durée définie dans le chien de garde de la tâche de sécurité entraîne un défaut de sécurité irrécupérable.

Composant de sécurité Tout objet, tâche, programme, sous-programme, point ou module, marqué comme élément dédié à la sécurité.

Composant standard Tout objet, tâche, point, programme, etc., **non** marqué comme élément dédié à la sécurité.

Connexion valable Connexion de sécurité ouverte et active, sans aucune erreur.

Défaut d'automate irrécupérable Défaut qui entraîne l'arrêt de tous les traitements et requiert la remise sous tension de l'automate. Le programme utilisateur n'est pas protégé et doit être rechargé.

Défaut de sécurité irrécupérable Défaut qui, même s'il est correctement géré par les systèmes de gestion des défauts qui sont fournis par l'automate de sécurité et mis en œuvre par l'utilisateur, arrête tous les traitements de la tâche de sécurité et requiert une intervention externe de l'utilisateur pour redémarrer la tâche de sécurité.

Défaut récupérable Défaut qui, s'il est correctement géré par les systèmes de gestion des défauts qui sont fournis par l'automate, n'entraîne pas l'arrêt de l'exécution du programme utilisateur.

E/S de sécurité Les E/S de sécurité présentent la plupart des caractéristiques des E/S standard, mais elles intègrent en plus des mécanismes certifiés SIL 3 qui garantissent l'intégrité de leurs données.

Édition en attente Modification apportée à un programme dans l'application Logix Designer, mais non encore communiquée à l'automate par l'acceptation de cette modification.

En ligne Situation dans laquelle se trouve l'utilisateur lorsqu'il surveille/modifie le programme présent dans l'automate.

Instruction complémentaire Une instruction que vous créez en tant que complément au jeu d'instructions Logix. Une fois définie, une instruction complémentaire peut être employée comme n'importe quelle autre instruction Logix dans différents projets. Une instruction complémentaire est constituée de paramètres, de points locaux, d'un programme logique et de sous-programmes de scrutation facultatifs.

Instruction complémentaire de sécurité Une instruction complémentaire pouvant utiliser des instructions d'application de sécurité. Outre la signature d'instruction utilisée pour les instructions complémentaires à haute intégrité, les instructions complémentaires de sécurité comportent une signature d'instruction de sécurité SIL 3 pour une utilisation dans les fonctions liées à la sécurité.

Instructions pour application de sécurité Instructions de sécurité offrant des fonctionnalités à caractère de sécurité. Elles ont été certifiées SIL 3 pour une utilisation dans des programmes de sécurité.

Intervalle entre trames requis (RPI) Lors de la communication sur un réseau, durée maximale entre les productions successives de données d'entrée.

Multiplicateur de timeout Cette valeur détermine le nombre de messages susceptibles d'être perdus avant l'apparition d'une erreur de connexion.

Numéro de réseau de sécurité (SNN) Numéro identifiant de façon unique un réseau parmi tous les autres réseaux d'un système de sécurité. L'utilisateur final est tenu d'attribuer un numéro unique à chaque réseau de sécurité ou sous-réseau de sécurité d'un système. Le numéro de réseau de sécurité constitue une partie de l'identifiant de station unique (UNID).

Partenaire de sécurité Processeur d'un automate à deux processeurs qui travaille avec l'automate principal pour exécuter les fonctions de sécurité.

Partenariat L'automate principal et le partenaire de sécurité doivent être présents simultanément et leur matériel et firmware respectifs être compatibles pour qu'un partenariat soit possible.

Programme Jeu d'instructions logiques dans un même langage de programmation, comme la logique à relais. Les programmes fournissent un code exécutable pour le projet d'un automate. Chaque programme possède un programme principal. Vous pouvez également spécifier des programmes facultatifs.

Période de la tâche de sécurité Fréquence à laquelle la tâche de sécurité est exécutée.

Points de sécurité Un point de sécurité possède toutes les caractéristiques d'un point standard, hormis le fait que l'automate GuardLogix lui applique des mécanismes certifiés SIL 3 qui permettent de protéger l'intégrité des données qui lui sont associées. Il peut s'agir d'un point d'accès programme ou d'un point d'accès automate.

Programme de sécurité Un programme de sécurité possède toutes les caractéristiques d'un programme standard, hormis le fait qu'il ne peut être planifié que dans le cadre d'une tâche de sécurité. Le programme de sécurité peut comprendre plusieurs sous-programmes de sécurité ou aucun. Il ne peut pas contenir de sous-programmes standard ni de points standard.

Protocole CIP Safety Mode de communication réseau conçu et certifié pour le transport des données à haute intégrité.

Signature d'instruction La signature d'instruction est composée d'un numéro d'identification et d'un horodatage permettant d'identifier le contenu de la définition de l'instruction complémentaire à un instant donné.

Signature d'instruction de sécurité Cette signature est un identifiant qui détermine les caractéristiques d'exécution de l'instruction complémentaire de sécurité. Elle sert à vérifier l'intégrité du programme de l'instruction complémentaire de sécurité lors des chargements sur l'automate.

Signature de configuration Numéro unique identifiant la configuration d'un dispositif. La signature de configuration est composée d'un numéro d'identification, d'une date et d'une heure.

Signature de tâche de sécurité Valeur, calculée par le firmware, qui identifie de façon unique la logique et la configuration du système de sécurité. Elle sert à vérifier l'intégrité du programme de l'application de sécurité lors des chargements sur l'automate.

Sous-programme de sécurité Un programme de sécurité possède toutes les caractéristiques d'un programme standard, hormis le fait qu'il n'est valide que dans un programme de sécurité et qu'il se compose d'une ou plusieurs instructions adaptée(s) à des applications de sécurité. (Voir l'Annexe A pour une liste d'instructions spécifiquement destinées aux applications de sécurité et d'instructions standard Logix qui peuvent être utilisées dans la logique d'un programme de sécurité).

Tâche Système de planification pour l'exécution d'un programme. Une tâche fournit des informations de planification et de priorité pour un ou plusieurs programmes qui s'exécutent en fonction de certains critères. Une fois la tâche déclenchée (activée), tous les programmes attribués à cette tâche (planifiés) s'exécutent dans leur ordre d'affichage dans l'arborescence de l'automate.

Tâche de sécurité Une tâche de sécurité possède toutes les caractéristiques d'une tâche standard, hormis le fait qu'elle n'est valable que dans un automate GuardLogix et qu'elle ne peut planifier que des programmes de sécurité. Une seule tâche de sécurité peut exister dans un automate GuardLogix. La tâche de sécurité doit être une tâche périodique/temporisée.

Tâche périodique Tâche déclenchée par le système d'exploitation de façon périodique. Chaque fois que le durée paramétrée arrive à échéance, la tâche est déclenchée et ses programmes sont exécutés. Les données et les sorties qui sont définies par les programmes dans la tâche conservent leurs valeurs jusqu'à l'exécution suivante de la tâche ou jusqu'à ce qu'elles soient traitées par une autre tâche. Les tâches périodiques interrompent systématiquement la tâche continue.

Temps de réponse de la tâche de sécurité Somme de la période de la tâche de sécurité et de son chien de garde. Ce temps correspond au délai le plus long entre le changement d'une entrée présenté à l'automate GuardLogix et la disponibilité de la sortie traitée pour la connexion de production.

Temps de réponse du système Délai le plus long entre un événement de sécurité considéré comme une entrée ou comme un défaut dans le système et le moment où le système passe en état de sécurité. Le temps de réponse du système comprend les temps de réponse du détecteur et de l'actionneur, et le temps de réponse de l'automate.

Numériques

1734-AENT 17, 23
1756-A10 17
1756-A13 17
1756-A17 17
1756-A4 17
1756-A5XT 17
1756-A7 17
1756-A7XT 17
1756-CN2 17, 23
1756-CN2R 17, 23
1756-CN2RXT 17, 23
1756-DNB 17, 23
1756-EN2F 17, 23
1756-EN2T 17, 23
1756-EN2TR 23
1756-EN2TXT 17, 23
1756-EN3TR 23
1756-ENBT 17, 23
1756-PB72 17
1756-PB75 17
1768-CNB 23
1768-CNBR 23
1768-ENBT 23
1784-CF128 17
1784-SD1 17
1784-SD2 17

A

adressage des points 47
alimentations 17
  présentation du matériel 22
automate principal
  définition 105
  présentation du matériel 22

C

carte mémoire 17
carte Secure Digital (SD) 17
CEI 61508
  certification de niveau d'intégrité de sécurité SIL 3 9, 13, 76
certification de niveau d'intégrité de sécurité SIL 3 9, 13, 76
  composants Logix 16
  responsabilités de l'utilisateur 14
  TÜV Rheinland 14
certifications 18
certifications et conformités aux normes de sécurité 18
charge de fiabilité 19
châssis
  présentation du matériel 22
  références 17
chevauchement
  définition 105
chien de garde de la tâche de sécurité 20
  définition 105
  modifier 20
  présentation 20
  réglage 20
  timeout 41
communication d'égal à égal 23
composants Logix
  certifiés SIL 3 16
composants XT 17
concept de sécurité
  principes 49
CONNECTION_STATUS
  type de donnée 63

D

défauts
  contourner 66
  défauts d'automate irrécupérables 66
  défauts de sécurité irrécupérables 66
  récupérables 67, 105
défauts d'automate irrécupérables 66, 105
défauts de sécurité irrécupérables 66, 105
  redémarrer la tâche de sécurité 66
défauts matériels
  correction 66
défauts récupérables 67, 105
DeviceNet Safety
  présentation des communications 24

E

éditions en attente 57
en ligne
  définition 106
EN 954-1
  CAT 4 9, 13
EN50156 101
environnement Studio 5000 17
état de la connexion 64
EtherNet/IP
  présentation des communications 23

F

fonction de commande
  spécification 52
fonctions de sécurité
  E/S CIP Safety 27
  sortie de sécurité 28
forçage 58

H

historique de signature 77

I

inhibition d'un module 58
installation d'un automate 21
instruction complémentaire
certification 73
signature d'instruction 75
signature d'instruction de sécurité 76
instruction définir la valeur système (SSV) 65
instruction GSV 65
instructions de sécurité en logique à relais 70
instructions pour application de sécurité
définition 106
interface
utilisation et applications d'IHM 43–45
interfaces homme-machine
utilisation et applications 43–45
intervalle entre trames requis
plage 42
intervalle entre trames requis (RPI)
définition 106
ISO 13849-1 9, 13

L

lire une valeur système (GSV)
définition 10
liste de contrôle
développement du programme 91
entrées SIL 3 89
sorties SIL 3 90
système automate GuardLogix 25, 88
logiciel
modification de votre programme d'application 59
logiciel RSLogix 5000 17

M

modification de votre programme d'application 59
modification en ligne 57, 60
modifications hors ligne 60
module d'interface de communication EtherNet/IP
présentation du matériel 23
module d'interface scrutateur DeviceNet
présentation du matériel 23
module passerelle ControlNet
présentation du matériel 23
modules d'E/S
remplacement 29–31
modules de communication
présentation du matériel 23
références 17
modules Guard I/O
applications SIL 2 103
multiplicateur de timeout 82
définition 106

N

niveau d'intégrité de sécurité (SIL)
concept 13–20
exemple de fonction 16
répartition et poids de la conformité 19
niveau de performance
définition 10
norme européenne
définition 10
numéro de réseau de sécurité 34
attribution manuelle 34
définition 106
modules en configuration d'usine 36
points de sécurité consommés 35

O

organigramme de la mise en service 51
organismes de certification 18

P

partenaire de sécurité
définition 106
emplacement 22
présentation du matériel 22
partenariat
définition 106
période de la tâche de sécurité 20
définition 107
limites 41
présentation 20
PLe 9, 13
points
données de sécurité produites/consommées 46
E/S de sécurité 46
voir aussi points de sécurité
points de sécurité 46
définition 107
types de données valables 46
points de sécurité consommés
numéro de réseau de sécurité 35
principes de base du développement d'une application 50
probabilité de défaillance par heure (PFH) 18–19
définition 10
probabilité de défaillance sur sollicitation (PFD) 18–19
définition 10
programme
chargement 57
identification 53
liste de contrôle 91
modification en ligne 60
modification hors ligne 60
organigramme de la modification 61
transfert 57
vérification 54
programme d'application
modification 59
voir programme
programme de sécurité 45
définition 107

projet
confirmation 55
propriété 29
protocole CIP
définition 10
protocole CIP Safety
définition 107
présentation 22
système routable 33

Q

qualification des données standard 47

R

référence de station unique
définition 34
révisions de firmware 17

S

sécurités d'interruption d'alimentation de brûleurs 101
signature d'instruction 75
définition 107
signature d'instruction de sécurité 76
définition 107
signature de configuration 29
signature de la tâche de sécurité
création 53
opérations non autorisées 54
supprimer 54
signature de tâche de sécurité
définition 107
SIL 2
EN50156 101
sous-programme de sécurité 45
définition 107

T

tâche de sécurité
définition 108
exécution 42
présentation 41
priorité 84
temps de réponse 20, 108
temps du chien de garde 84
tâche périodique
définition 108
taux de couverture des tests de diagnostic
définition 10
temps de réponse
calcul pour le système 79
système 19, 108
tâche de sécurité 20
temps de réponse de la sortie 28
temps de réponse du système 19
calcul 79
temps de réponse du système Logix
calcul 80
temps du chien de garde 84
terminologie 10
test de vérification du projet 54, 78
tests de vérification 14

V

verrouillage de sécurité 56
mots de passe 56
opérations non autorisées 56
par défaut 56

Assistance Rockwell Automation

Rockwell Automation fournit des informations techniques sur Internet pour vous aider à utiliser ses produits. Sur le site http://www.rockwellautomation.com/support vous trouverez des notes techniques et des profils d'application, des exemples de code et des liens vers des mises à jours de logiciels (service pack). Rendez-vous également sur notre Centre d'Assistance, à l'adresse https://rockwellautomation.custhelp.com/, pour des mises à jour de logiciels, chats d'assistance et forums, informations techniques, foires aux questions, et pour vous enregistrer afin d'être informé des mises à jour de produit.

Nous proposons en outre de nombreux programmes d'aide à l'installation, à la configuration et au dépannage. Pour de plus amples informations, contactez votre distributeur ou votre représentant Rockwell Automation local, ou allez sur le site http://www.rockwellautomation.com/services/online-phone.

Aide à l'installation

En cas de problème dans les 24 heures suivant l'installation, consultez les informations données dans le présent manuel. Vous pouvez également appeler le Centre d'Assistance pour obtenir une aide pour la mise en service de votre produit.

Pour les États-Unis ou le Canada	1.440.646.3434
Pour les autres pays	Utilisez la rubrique Worldwide Locator sur la page http://www.rockwellautomation.com/rockwellautomation/support/overview.page, ou contactez votre représentant Rockwell Automation local.

Procédure de retour d'un nouveau produit

Rockwell Automation teste tous ses produits pour en garantir le parfait fonctionnement à leur sortie d'usine. Cependant, si votre produit ne fonctionne pas et doit être retourné, suivez les procédures ci-après.

Pour les États-Unis	Contactez votre distributeur. Vous devrez lui fournir le numéro de dossier que le Centre d'Assistance vous aura communiqué (voir le numéro de téléphone ci-dessus), afin de procéder au retour.
Pour les autres pays	Contactez votre représentant Rockwell Automation pour savoir comment procéder.

Commentaires

Vos commentaires sur ce document nous aident à mieux vous servir. Si vous avez des suggestions sur la façon d'améliorer ce document, remplissez le formulaire de la publication RA-DU002, disponible sur le site http://www.rockwellautomation.com/literature/.

Rockwell Automation tient à jour des données environnementales sur ses produits, sur son site Internet à l'adresse http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

www.rockwellautomation.com

Siège des activités « Power, Control and Information Solutions »

Amériques : Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 Etats-Unis, Tél: +1 414.382.2000, Fax : +1 414.382.4444
Europe / Moyen-Orient / Afrique : Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgique, Tél: +32 2 663 0600, Fax : +32 2 663 0640
Asie Pacifique : Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tél: +852 2887 4788, Fax : +852 2508 1846

Canada : Rockwell Automation, 3043 rue Joseph A. Bombardier, Laval, Québec, H7P 6C5, Tél: +1 (450) 781-5100, Fax: +1 (450) 781-5101, www.rockwellautomation.ca
France : Rockwell Automation SAS – 2, rue René Caudron, Bât. A, F-78960 Voisins-le-Bretonneux, Tél: +33 1 61 08 77 00, Fax : +33 1 30 44 03 09
Suisse : Rockwell Automation AG, Av. des Baumettes 3, 1020 Renens, Tél: 021 631 32 32, Fax: 021 631 32 31, Customer Service Tél: 0848 000 278

Publication 1756-RM099B-FR-P – Novembre 2014

Copyright © 2014 Rockwell Automation, Inc. Tous droits réservés. Imprimé aux États-Unis.