Manuel utilisateur

Allen-Bradley

Automates GuardLogix

Références 1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP, 1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP, 1756-L73SXT, 1756-L7SPXT

Informations importantes destinées à l'utilisateur

Les équipements électroniques possèdent des caractéristiques de fonctionnement différentes de celles des équipements électromécaniques. La publication SGI-1.1 « Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls », disponible auprès de votre agence locale Rockwell Automation ou sur le site http://www.rockwellautomation.com/literature/) décrit certaines de ces différences. En raison de ces différences et de la grande diversité des utilisations des équipements électroniques, les personnes qui en sont responsables doivent s'assurer de l'acceptabilité de chaque application.

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

Les exemples et schémas contenus dans ce manuel sont fournis qu'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 les 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 des situations susceptibles de provoquer une explosion dans un environnement dangereux et pouvant entraîner des blessures graves voire mortelles, des dégâts matériels ou des pertes financières.
	**ATTENTION :** identifie des actions ou des situations risquant d'entraîner des blessures allant jusqu'à la mort, des dégâts matériels ou des préjudices financiers. Les messages « Attention » vous aident à identifier un danger ; éviter ce danger et en discerner les conséquences.
	**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.
IMPORTANT	Informations particulièrement importantes pour la compréhension et l'utilisation du produit.

Les informations ci-dessous résument les modifications apportées à ce manuel depuis sa dernière publication.

Sujet	Pages
Information sur les automates 1756-L71S	11, 18, 21, 26, 47
Conseils pour l'installation du module de stockage d'énergie	45

Notes :

Chapitre 3

Configuration de l'automate

Chapitre 4

Communications en réseaux

Chapitre 5

Ajout, configuration, surveillance et remplacement d'E/S de sécurité CIP Safety

Chapitre 6

Développement d'applications de sécurité

Chapitre 7

Mise en ligne de l'automate

Chapitre 8

Stockage et chargement des projets dans la mémoire non volatile

Chapitre 9

Surveillance de l'état et gestion des défauts

Annexe A

Voyants d'état

Annexe B

Maintenance de la pile

Annexe C

Changement du type d'automate dans un projet RSLogix 5000

Annexe D

Historique des modifications

Index

Notes :

Ce manuel est destiné à vous guider dans l'utilisation des automates GuardLogix™. Il décrit les procédures de configuration, d'exploitation et de dépannage propres à votre automate GuardLogix.

Utilisez ce manuel si vous êtes responsable de la conception, de l'installation, de la programmation ou du dépannage de systèmes de commande comprenant des automates GuardLogix.

Vous devez avoir des notions élémentaires sur les circuits électriques et bien connaître la logique à relais. Vous devez également avoir une formation et une expérience dans la création, l'utilisation et la maintenance de systèmes de sécurité.

Pour plus d'informations sur des sujets connexes comme la programmation de votre automate
GuardLogix, les exigences SIL 3/PLe ou les composants Logix standard, reportez-vous à la liste des Informations connexes, page 13.

À propos des automates GuardLogix 1756

Il existe deux familles d'automates GuardLogix™ 1756. Ces automates partagent de nombreuses fonctionnalités, mais ont également quelques différences. Le Tableau 1 fournit un bref aperçu de ces différences.

Tableau 1 – Différences entre les automates 1756-L7*x*S et 1756-L6*x*S

Fonctionnalité	**1756-L7*x*S** (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT)	**1756-L6*x*S** (1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP)
Prise en charge de l'horloge et sauvegarde de la mémoire à la mise hors tension	Module de stockage d'énergie (ESM)	Pile
Ports de communication ports (intégrés)	USB	Série
Connexions, automate	500	250
Mémoire non volatile	Carte Secure Digital (SD)	Carte CompactFlash
Voyants d'état	Afficheur d'état défilant et voyants d'état DEL	Voyants d'état DEL

Les automates GuardLogix pour environnements extrêmes, références 1756-L73SXT et 1756-L7SPXT, offrent les mêmes fonctionnalités que les automates 1756-L73S, mais sont conçus pour supporter des températures allant de –25 à 70 °C .

IMPORTANT Les composants système Logix-XT sont qualifiés pour des contions environnementales extrêmes uniquement quand ils sont utilisés correctement avec d'autres composants système Logix-XT. L'utilisation de composants Logix-XT avec des composants système Logix standard annule les classifications pour environnement extrême.

Terminologie

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

Tableau 2 – Termes et définitions

Abréviation	Signification	Définition
1oo2	One Out of Two (un sur deux)	Fait référence au principe de fonctionnement d'un système de sécurité à plusieurs processeurs.
CIP	Common Industrial Protocol (protocol industriel commun)	Protocole de communication conçu pour les applications d'automatisation industrielle.
CIP Safety	Common Industrial Protocol – Safety Certified (CIP – Certification de sécurité)	Version SIL 3/PLe du protocole CIP.
DC	Diagnostic Coverage (taux de couverture des tests de diagnostic)	Proportion des défaillances de composants détectées dans le taux de défaillance global.
EN	Norme européenne	Norme européenne de référence.
ESM	Module de stockage d'énergie (Energy Storage Module)	Utilisé comme alimentation de secours de l'horloge interne et sauvegarde de la mémoire en cas de coupures de courant sur les automates 1756-L7*xS* et 1756-L73SXT .
GSV	Lecture d'une valeur système (Get System Value)	Instruction destinée à récupérer une information d'état spécifique de l'automate et à la placer dans un point (tag) de destination.
–	Multicast (multidiffusion)	La transmission d'informations par un expéditeur pour plusieurs destinataires.
PFD	Probability of Failure on Demand (probabilité de défaillance sur sollicitation)	Probabilité moyenne de défaillance d'un système dans l'exécution de ses fonctions lorsque la demande lui en est faite.
PFH	Probability of Failure per Hour (probabilité de défaillance horaire)	Probabilité de survenue d'une panne dangereuse sur une heure de temps dans un système opérationnel.
PL	Niveau de performance de sécurité (Performance Level)	Classification de sécurité ISO 13849-1.
RPI	Intervalle entre trames requis (Requested Packet Interval)	Fréquence de transmission attendue des trames de données pour les communications en réseau.
SNN	Numéro de réseau de sécurité (Safety Network Number)	Numéro unique qui identifie une section d'un réseau de sécurité.
SSV	Set System Value (définir la valeur système)	Une instruction qui définit une donnée système de l'automate.
–	Standard	Objet, tâche, point, programme ou composant de votre projet qui n'est pas un composant de sécurité.
–	Unicast (envoi individuel)	La transmission d'informations par un expéditeur pour un destinataire.

Informations connexes

Les documentations suivantes contiennent des informations complémentaires sur des produits Rockwell Automation en rapport.

Tableau 3 – Publications relatives aux automates et systèmes GuardLogix

Pour plus d'informations sur…	Se reporter à la documentation…	Description
Impératifs d'application (sécurité)	« GuardLogix Controller Systems Safety Reference Manual », publication 1756-RM093	Fournit des informations détaillées sur les contraintes à respecter pour réaliser et entretenir un niveau de sécurité SIL 3/PLe dans un système de commande GuardLogix.
Piles	« Guidelines for Handling Lithium Batteries », publication AG-5.4	Fournit des informations sur le stockage, la manipulation, le transport et l'élimination des piles au lithium.
	Références des piles pour les automates programmables, http://www.ab.com/programmablecontrol/batteries.html	Donne accès aux fiches techniques de sécurité (MSDS) pour le remplacement individuel des piles.
CIP Sync (synchronisation temporelle)	« Integrated Architecture and CIP Sync Configuration Application Technique », publication IA-AT003	Fournit des informations détaillées et complètes sur la manière d'appliquer la technologie CIP Sync pour synchroniser les horloges dans un système de commande Logix.
Conception et choix du système	« Logix5000 Controllers Design Considerations Reference Manual », publication 1756-RM094	Fournit aux utilisateurs avancés des recommandations pour l'optimisation du système, ainsi que des informations destinées à guider leurs choix en matière de conception du système.
	« ControlLogix Selection Guide », publication 1756-SG001	Propose une méthode de sélection évoluée des composants d'un système ControlLogix®, des informations sur les points critiques à connaître pour prendre les bonnes décisions initiales, ainsi que des liens vers les spécifications techniques de ces composants.
Guard I/O	Manuel utilisateur des modules de sécurité Guard I/O DeviceNet, publication 1791DS-UM001	Fournit des informations sur l'utilisation des modules de sécurité Guard I/O DeviceNet.
	« Guard I/O DeviceNet Safety Modules User Manual », publication 1791ES-UM001	Fournit des informations sur l'utilisation des modules de sécurité Guard I/O EtherNet/IP.
	Modules de sécurité POINT Guard I/O – Manuel utilisateur, publication 1734-UM013	Fournit des informations sur l'installation, la configuration et l'utilisation des modules de sécurité Point Guard I/O™.
Installation du matériel	« ControlLogix Chassis and Power Supplies Installation Instructions », publication 1756-IN005	Décrit comment installer et mettre à la terre les châssis et les alimentations ControlLogix.
	« Industrial Automation Wiring and Grounding Guidelines », publication 1770-4.1	Fournit des informations approfondies sur la mise à la terre et le câblage des automates programmables.
Instructions (programmation)	« GuardLogix Safety Application Instruction Set Reference Manual », publication 1756-RM095	Fournit des informations sur le jeu d'instructions pour applications de sécurité GuardLogix.
	« Logix5000 Controllers General Instructions Reference Manual », publication 1756-RM003	Fournit aux programmeurs une description détaillée des instructions utilisables avec les automates Logix5000.
	Automates Logix5000 – Instructions de mouvement – Manuel de référence, publication MOTION-RM002	Fournit aux programmeurs la description des instructions de commande de mouvement disponibles avec un automate Logix5000.
Commande de mouvement	« SERCOS Motion Configuration and Startup User Manual », publication MOTION-UM001	Fournit des détails sur la configuration d'un système pour une application de mouvement SERCOS.
	« Motion Coordinated Systems User Manual », publication MOTION-UM002	Fournit les détails sur la création et la configuration d'un système pour une application de mouvement coordonné.
	« CIP Motion Configuration and Startup User Manual », publication MOTION-UM003	Fournit des détails sur la configuration d'un système pour une application de mouvement intégré sur les réseaux EtherNet/IP.
	« CIP Motion Reference Manual », publication MOTION-RM003	Informations détaillées sur les modes et attributs de commande d'axe pour la commande de mouvement intégrée sur les réseaux EtherNet/IP.
Réseaux (ControlNet, DeviceNet, EtherNet/IP)	« EtherNet/IP Modules in Logix5000 Control Systems User Manual », publication ENET-UM001	Explique comment configurer et utiliser des modules EtherNet/IP dans un système de commande Logix5000™.
	« ControlNet Modules in Logix5000 Control Systems User Manual », publication CNET-UM001	Décrit comment configurer et exploiter des modules ControlNet dans un système de commande Logix5000.
	« DeviceNet Modules in Logix5000 Control Systems User Manual », publication DNET-UM004	Décrit comment configurer et exploiter des modules DeviceNet dans un système de commande Logix5000.
PhaseManager™	« PhaseManager User Manual », publication LOGIX-UM001	Fournit une méthodologie et des exemples pour organiser et programmer un automate Logix5000 pour utiliser les phases d'équipement.

Tableau 3 – Publications relatives aux automates et systèmes GuardLogix

Pour plus d'informations sur…	Se reporter à la documentation…	Description
Programmation des tâches et des procédures	« Logix5000 Controllers Common Procedures Programming Manual », publication 1756-PM001	Permet d'accéder aux guides de programmation des automates Logix5000 relatifs à la gestion des fichiers projet, à l'organisation des points, à la programmation en logique à relais, aux sous-programmes de test, à la création des instructions complémentaires, aux informations d'état de l'automate, à la gestion des défauts, à l'importation et l'exportation d'éléments de projet et plus encore.
	« Logix5000 Controllers Execution Time and Memory Use Reference Manual », publication 1756-RM087	Aide à l'estimation de la mémoire utilisée et du temps d'exécution de la logique programmée, et à choisir parmi diverses options de programmation.
Redondance	« ControlLogix Redundancy System User Manual », publication 1756-UM523	Recommandations pour la conception, le développement et la mise en œuvre d'un système ControlLogix à redondance standard.
	« ControlLogix Enhanced Redundancy System User Manual », publication 1756-UM535	Recommandations pour la conception, le développement et la mise en œuvre d'un système ControlLogix à redondance évoluée.

Ces publications peuvent être consultées ou téléchargées sur le site http://www.rockwellautomation.com/literature. Pour commander des versions imprimées de documentation technique, contactez votre distributeur local Allen-Bradley® ou votre agence commerciale Rockwell Automation.

Présentation du système

Impératifs de l'application de sécurité

L'automate GuardLogix est homologué pour une utilisation dans des applications de sécurité classées jusqu'au niveau d'intégrité de sécurité SIL 3 ou de performance de sécurité PLe, dans lesquelles l'état de sécurité correspond à l'absence de tension. Les impératifs des applications de sécurité incluent l'évaluation de la probabilité de défaillance (PFD et PFH), les réglages du temps de réponse du système et les tests de vérification fonctionnelle, conformément aux exigences SIL 3/PLe.

Pour en savoir plus sur les exigences relatives aux systèmes de sécurité SIL 3 et PLe, notamment en ce qui concerne les intervalles entre les tests de validation fonctionnelle, le temps de réaction du système et les calculs de PFD et de PFH, reportez-vous à la publication 1756-RM093, « Systèmes automates GuardLogix – Manuel de référence sur la sécurité ». Il est impératif d'avoir lu, assimilé et pris en compte ces exigences préalablement à toute mise en œuvre d'un système de sécurité SIL 3/PLe GuardLogix.

Les applications de sécurité SIL 3/PLe GuardLogix requièrent l'utilisation d'au moins un numéro de réseau de sécurité (SNN) et une signature de tâche de sécurité. Tous deux affectent la configuration de l'automate et des E/S ainsi que les communications réseau.

Pour plus de détails, reportez-vous à la publication 1756-RM093, « Systèmes automates GuardLogix – Manuel de référence sur la sécurité ».

Numéro de réseau de sécurité (SNN)

Le numéro de réseau de sécurité (SNN) est un numéro unique qui identifie les sous-réseaux de sécurité. Chaque sous-réseau de sécurité utilisé par l'automate pour les communications de sécurité doit avoir son propre SNN. Chaque composant CIP de sécurité doit également être configuré avec le SNN de son sous-réseau de sécurité. Le SNN peut être attribué automatiquement ou manuellement.

Pour de plus amples informations sur la configuration du numéro SNN, voir Gestion du numéro de réseau de sécurité (SNN), page 53.

Signature de tâche de sécurité

Une signature de tâche de sécurité est constituée d'un numéro d'identification, d'une date et d'une heure qui identifient de façon unique la partie sécurité d'un projet. Elle s'applique au programme, aux données et à la configuration de ce système de sécurité. Le système GuardLogix utilise la signature de tâche de sécurité pour authentifier l'intégrité du projet et vous permettre de vérifier que le bon projet est chargé dans l'automate cible. La création, l'enregistrement et la vérification de la signature de tâche de sécurité constituent une étape obligatoire du processus de développement d'une application de sécurité.

Voir Génération d'une signature de tâche de sécurité, page 106 pour plus d'informations.

Distinction entre composants standard et de sécurité

Les logements de châssis d'un système GuardLogix qui ne sont pas utilisés par la fonction de sécurité peuvent être occupés par d'autres modules ControlLogix répondant aux Directives Basse Tension et CEM de l'Union européenne. Pour consulter le certificat CE de la gamme d'automates programmables ControlLogix et savoir quels modules sont certifiés, rendez-vous sur le site http://ab.com/certification/ce.

Vous devez créer et documenter les parties standard et de sécurité de l'application en les distinguant de façon claire, logique et visible. Pour favoriser cette distinction, le logiciel de programmation RSLogix 5000 comporte des icônes d'identification de sécurité permettant de reconnaître la tâche de sécurité, les programmes de sécurité, les sous-programmes de sécurité et les composants de sécurité. En outre, le logiciel RSLogix 5000 utilise un attribut de classe sécurité qui est rappelé à chaque fois que vous affichez les propriétés de la tâche de sécurité, des programmes et sous-programmes de sécurité, d'un point de sécurité ou d'une instruction complémentaire de sécurité.

L'automate n'autorise pas l'écriture de données dans les points de sécurité depuis des terminaux d'IHM externes ou via des messages provenant d'instructions d'automates homologues. Le logiciel RSLogix 5000 peut écrire dans des points de sécurité lorsque la sécurité de l'automate GuardLogix est déverrouillée, qu'il ne possède pas de signature de tâche de sécurité et qu'il fonctionne sans défauts de sécurité.

Le Manuel utilisateur des systèmes ControlLogix, publication 1756-UM001, apporte des informations sur l'utilisation d'éléments système ControlLogix dans des applications standard (non à caractère de sécurité).

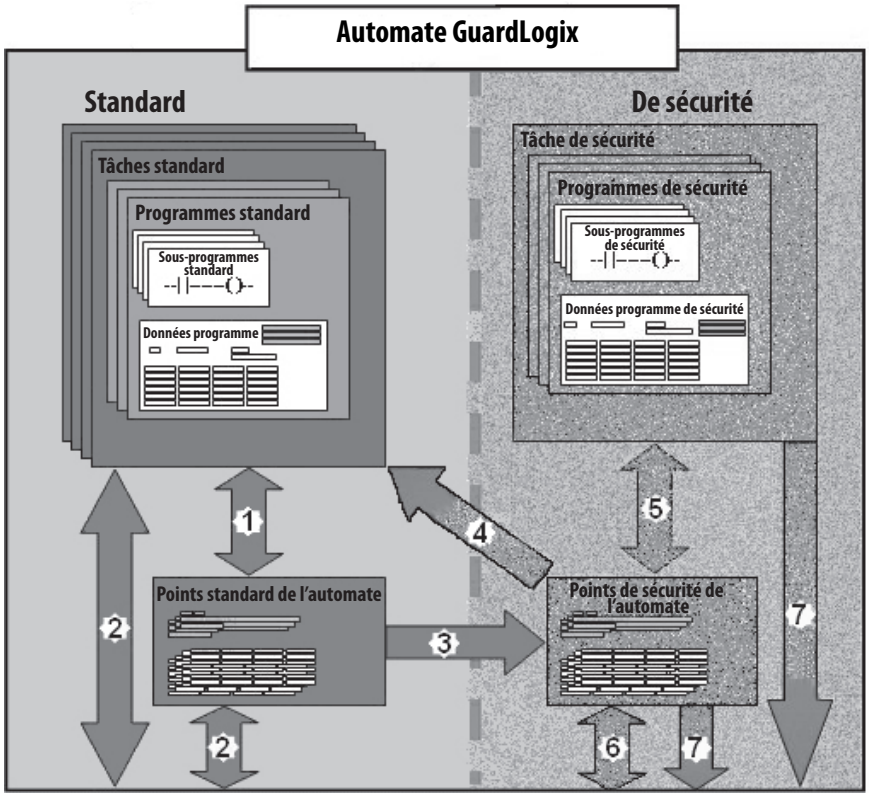
Terminaux d'IHM

Vous pouvez utiliser des terminaux d'interface opérateur (IHM) avec les automates GuardLogix. Ces IHM permettent l'accès aux points standard tout comme avec un automate standard. Mais elles ne peuvent pas écrire dans les points de sécurité. Ceux-ci sont en lecture seule.

Traitement des flux d'information dans un automate

Le schéma suivant illustre la circulation des données standard et de sécurité à l'intérieur de l'automate GuardLogix.

Figure 1 – Circulation des données



N°	Description	
1	Les points et le programme standard se comportent de la même façon qu'ils le feraient sur une plate-forme Logix standard.	
2	Les données de points standard, qu'ils soient en accès programme ou automate, peuvent être échangées avec des IHM externes, des PC et d'autres automates.	
3	Les automates GuardLogix sont de type intégré. Ils ont la propriété de pouvoir transférer (« mapper ») des données de point standard dans des points de sécurité de façon à permettre leur utilisation dans la tâche de sécurité.	
		**ATTENTION :** ces données ne doivent cependant pas être utilisées pour commander directement une sortie SIL 3/PLe.
4	Les points de sécurité en accès automate peuvent être lus directement par un programme standard.	
5	Les points de sécurité ne peuvent être lus ou écrits que par un programme de sécurité.	
6	Les points de sécurité peuvent être échangés par l'intermédiaire de réseaux Ethernet ou ControlNet entre des automates de sécurité, notamment les modèles GuardLogix 1756 et 1768.	
7	Les données de points de sécurité, en accès programme ou automate, peuvent être lus par des dispositifs externes comme des IHM, des PC ou d'autres automates standard.	
	IMPORTANT	Une fois lue, ces données sont considérées comme standard et non plus comme données de type SIL 3/PLe.

Sélection des composants système

Le système GuardLogix prend en charge les applications de sécurité SIL 3 et PLe. L'automate GuardLogix est composé d'un automate principal et d'un partenaire de sécurité qui fonctionnent ensemble dans une architecture 1oo2. Le Tableau 4 répertorie les références des automates principaux et des partenaires de sécurité.

Le partenaire de sécurité doit être installé dans le logement immédiatement à droite de l'automate principal. Les révisions majeures et mineures du firmware de l'automate principal et du partenaire de sécurité doivent correspondre parfaitement pour établir le partenariat de commande nécessaire aux applications de sécurité.

Tableau 4 – Références de l'automate principal et du partenaire de sécurité correspondant

Automate principal	Partenaire de sécurité
1756-L61S, 1756-L62S, 1756-L63S	1756-LSP
1756-L71S, 1756-L72S, 1756-L73S	1756-L7SP
1756-L73SXT	1756-L7SPXT

Automate principal

L'automate principal est le processeur qui exécute les fonctions standard et les fonctions de sécurité. Il communique également avec le partenaire de sécurité pour les fonction liées à la sécurité dans le système de commande du GuardLogix. Les fonctions standard comprennent :

- la commande des E/S ;
- le programme ;
- les temporisations ;
- le comptage ;
- la génération de rapports ;
- les communications ;
- les calculs arithmétiques ;
- les manipulations de fichiers de données.

L'automate principal comprend un processeur central, une interface d'E/S et une mémoire.

Tableau 5 – Capacité mémoire

Référence	Mémoire utilisateur (capacité de la RAM)	
	Tâches et composants standard	Tâches et composants de sécurité
1756-L61S	2 Mo	1 Mo
1756-L62S	4 Mo	1 Mo
1756-L63S	8 Mo	3,75 Mo
1756-L71S	2 Mo	1 Mo
1756-L72S	4 Mo	2 Mo
1756-L73S,1756-L73SXT	8 Mo	4 Mo

À partir de la version 18 du logiciel RSLogix 5000, il est possible de gérer les mises à jour du système d'exploitation de l'automate GuardLogix ou l'enregistrement et la restauration du programme utilisateur à l'aide d'une carte mémoire. Avec les versions 16 et 17 du logiciel RSLogix 5000, vous ne pouvez

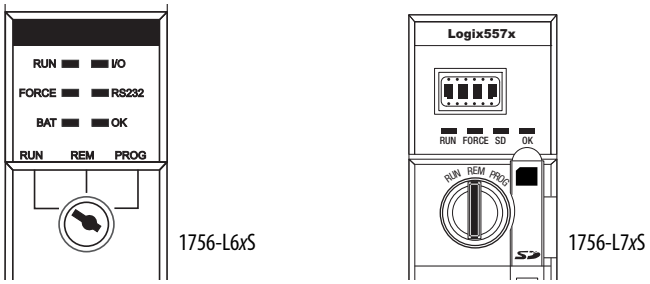
visualiser le contenu d'une carte mémoire que si celle-ci est montée dans l'automate principal. Dans les versions antérieures à la version 16, les cartes mémoire ne sont pas prises en charge.

Pour de plus amples informations, voir le Chapitre 8, Stockage et chargement des projets dans la mémoire non volatile.

Un commutateur à clé à trois positions, situé sur la face avant de l'automate principal, commande les modes de fonctionnement de l'automate. Les modes de fonctionnement possibles sont les suivants :

- RUN (exécution)
- PROG (programmation)
- REM (à distance) : ce mode de pilotage logiciel peut correspondre à Programmation, Exécution ou Test

Figure 2 – Positions du commutateur à clé



Partenaire de sécurité

Le partenaire de sécurité fonctionne en coprocesseur assurant la redondance des fonctions de sécurité du système.

Le partenaire de sécurité ne comporte pas de commutateur à clé, ni de port de communication. Sa configuration et son fonctionnement sont déterminés par l'automate principal.

Châssis

Le châssis ControlLogix fournit des connexions physiques entre les modules et l'automate GuardLogix.

Alimentation

Les alimentations ControlLogix répertoriées Page 27 sont compatibles avec une utilisation dans des applications SIL 3. Aucune configuration ni câblage supplémentaires ne sont nécessaires pour utiliser ces alimentations dans des applications SIL 3.

Sélection des modules d'E/S de sécurité

Des périphériques d'entrée et de sortie de sécurité peuvent être connectés aux E/S CIP Safety en réseau DeviceNet ou EtherNet/IP. Ceci permet la commande de dispositifs de sortie par l'automate GuardLogix par l'intermédiaire de communications DeviceNet ou EtherNet/IP.

Pour connaître les informations les plus récentes sur les références des E/S de sécurité CIP disponibles, ainsi que celles des séries et révisions de firmware certifiées, allez sur le site http://ab.com/certification/safety.

Sélection des réseaux de communication

L'automate GuardLogix prend en charge des communication qui lui permettent :

- de relier et commander des E/S de sécurité en réseau DeviceNet ou EtherNet/IP ;
- de relier et commander des E/S de sécurité décentralisées en réseau DeviceNet, EtherNet/IP ou ControlNet ;
- de produire et consommer des données de points de sécurité entre des automates GuardLogix 1756 et 1768 en réseau Ethernet/IP ou ControlNet, ou au sein d'un même châssis ControlLogix ;
- de relier et commander des E/S standard décentralisées en réseau EtherNet, ControlNet ou DeviceNet.

Utilisez les modules de communication suivants pour assurer l'interface entre les automates GuardLogix et des périphériques en réseau.

Tableau 6 – Modules de communication

Pour assurer l'interface entre	Utilisez le module	Reportez-vous aux notices d'installation suivantes
un automate GuardLogix et des dispositifs DeviceNet	1756-DNB	DNET-IN001
un automate GuardLogix et des dispositifs EtherNet/IP	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR, 1756-EN3TR 1756-EN2TXT	ENET-IN002
des automates en réseau ControlNet	1756-CN2, 1756-CN2R 1756-CN2RXT	CNET-IN005

L'automate GuardLogix peut communiquer avec le logiciel de programmation RSLogix 5000 par l'intermédiaire d'une connexion série ou USB, d'un module EtherNet ou ControlNet.

Les automates 1756-L6*x*S possèdent un port série. Les automates 1756-L7*x*S possèdent un port USB.

Pour des informations complémentaires sur l'utilisation des modules de communication réseau, reportez-vous à Informations connexes, page 13.

Critères de programmation

Le logiciel RSLogix 5000 est l'outil de programmation destiné aux applications de commande GuardLogix.

Utilisez le Tableau 7 pour identifier les numéros de version minimum des logiciels compatibles avec vos automates GuardLogix. Le logiciel RSLogix 5000 en version 15 ne prend pas en charge le niveau de sécurité SIL 3.

Tableau 7 – Versions de logiciel

Référence	Version du logiciel RSLogix 5000(1)	Version du logiciel RSLinx® Classic(1)
1756-L61S, 1756-L62S	14	Toutes versions
1756-L63S	16	
1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT	20	2.59

(1) ou ultérieure.

Les sous-programmes de sécurité comprennent des instructions de sécurité qui constituent un sous-ensemble du jeu d'instructions en logique à relais standard, ainsi que des instructions d'application de sécurité. Les programmes définis pour la tâche de sécurité ne peuvent être réalisés qu'en logique à relais.

Tableau 8 – Fonctions prises en charge par les différentes versions du logiciel RSLogix 5000

Fonction	Version 14		Version 16		Version 17		Version 18		Version 19		Version 20	
	Tâche de sécurité	Tâche standard	Tâche de sécurité	Tâche standard	Tâche de sécurité	Tâche standard	Tâche de sécurité	Tâche standard	Tâche de sécurité	Tâche standard	Tâche de sécurité	Tâche standard
Instructions complémentaires				X		X	X	X	X	X	X	X
Alarmes et événements				X		X		X		X		X
Journalisation de l'automate					X	X	X	X	X	X	X	X
Contrôle d'accès aux données							X	X	X	X	X	X
Sous-programmes de phase d'équipement				X		X		X		X		X
Tâches événementielles				X		X		X		X		X
Firmware Supervisor				X		X	X	X	X	X	X	X
Diagrammes de blocs fonctionnels (FBD)				X		X		X		X		X
Commande d'axe intégrée				X		X		X		X		X
Logique à relais	X	X	X	X	X	X	X	X	X	X	X	X
Commutation de langue					X	X	X	X	X	X	X	X
Carte mémoire							X	X	X	X	X	X
Importation et exportation en ligne d'éléments de programme						X		X		X		X
Sous-programmes en graphe de fonctionnement séquentiel (SFC)				X		X		X		X		X
Texte structuré				X		X		X		X		X
Connexions d'envoi individuel pour des points de sécurité produits et consommés									X	X	X	X
Connexions d'envoi individuel pour des modules d'E/S de sécurité sur les réseaux EtherNet/IP											X	X

Pour de plus amples informations sur l'utilisation de ces fonctions, reportez-vous à la publication 1756-PM001, « Automates Logix5000 – Procédures générales – Manuel de programmation », aux publications mentionnées au paragraphe Informations connexes, page 13 et à l'aide en ligne du logiciel RSLogix 5000.

Notes :

Installation de l'automate

Précautions

Lisez et suivez ces précautions d'utilisation.

Environnement et armoire de protection

ATTENTION : cet équipement est prévu pour fonctionner en environnement industriel avec une pollution de niveau 2, dans des applications de surtension de catégorie II (telles que définies dans la publication 60664-1 de la CEI) et à une altitude maximum de 2000 m sans déclassement.

Cet équipement fait partie des équipements industriels de Groupe 1, Classe A selon la publication 11 de la CEI/CISPR. A défaut de précautions suffisantes, il se peut que la compatibilité électromagnétique ne soit pas garantie dans les environnements résidentiels et autres, en raison de perturbations par conduction et par rayonnement.

Cet équipement est fourni en tant qu'équipement de type « ouvert ». Il doit être installé à l'intérieur d'une armoire fournissant une protection adaptée aux conditions d'utilisation ambiantes et suffisante pour éviter toute blessure corporelle pouvant résulter d'un contact direct avec des composants sous tension. L'armoire doit posséder des propriétés ignifuges capables d'empêcher ou de limiter la propagation des flammes, conformément à un indice de propagation de 5 VA, ou être homologuée pour l'application si elle n'est pas de type métallique. L'accès à l'intérieur de l'armoire ne doit être possible qu'à l'aide d'un outil. Certaines sections de la présente publication peuvent comporter des recommandations supplémentaires portant sur les degrés de protection spécifiques à respecter pour maintenir la conformité à certaines normes de sécurité.

En complément de cette publication, consultez :

- la publication 1770-4.1, « Industrial Automation Wiring and Grounding Guidelines », pour d'autres critères d'installation ;
- les normes NEMA 250 ou CEI 60529, selon le cas, pour la description des niveaux de protection fournis par les différents types d'armoires.

Systèmes électroniques programmables (PES)

ATTENTION : le personnel en charge de la mise en œuvre de systèmes électroniques programmables de sécurité doivent avoir connaissance des contraintes de sécurité spécifiques à l'application de ces systèmes et doivent être formées à leur utilisation.

Retrait et insertion sous tension (RIUP)

AVERTISSEMENT : lorsque vous insérez ou retirez le module alors que le bus intermodules est sous tension, un arc électrique peut se produire, susceptible de provoquer une explosion dans les installations en environnement dangereux.

Assurez-vous que l'alimentation est coupée ou que l'environnement est classé non dangereux avant de poursuivre. Des arcs électriques répétés provoquent une usure excessive des contacts, à la fois sur le module et sur le connecteur de raccordement. Des contacts détériorés peuvent créer une résistance électrique qui affectera le bon fonctionnement du module.

Homologation Environnements dangereux pour l'Amérique du Nord

The following information applies when operating this equipment in hazardous locations:	**Informations sur l'utilisation de cet équipement en environnements dangereux :**
Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	Les produits marqués « CL I, DIV 2, GP A, B, C, D » ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.
WARNING: EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**AVERTISSEMENT :** RISQUE D'EXPLOSION • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles.

Homologation environnements dangereux pour l'Europe

Informations relatives aux produits marqués Ex.

Cet équipement est destiné à être utilisé dans des atmosphères potentiellement explosives telles que définies par la directive 94/9/CE de l'Union européenne. Il a été testé comme étant conforme aux exigences essentielles de santé ainsi qu'aux normes de sécurité relatives à la conception et à la fabrication d'équipements de Catégorie 3 destinés à être utilisés dans des atmosphères potentiellement explosibles de Zone 2, selon l'annexe II de cette directive.

La conformité aux exigences essentielles de santé et de sécurité découle de la conformité aux normes EN 60079-15 et EN 60079-0.

ATTENTION : cet équipement n'est pas protégé contre le rayonnement solaire direct ni les autres sources de rayonnement UV.

AVERTISSEMENT :

- Cet équipement doit être monté dans une armoire assurant au minimum une protection IP54 lorsqu'il est utilisé dans un environnement en Zone 2.
- Cet équipement doit être utilisé dans les limites nominales définies par Rockwell Automation.
- Cet équipement ne doit être utilisé qu'avec les bus intermodules homologués ATEX de Rockwell Automation.
- Raccordez de façon sûre tous les branchements externes sur cet équipement au moyen de vis, de dispositifs de verrouillage coulissants, de connecteurs filetés ou de tous autres accessoires fournis avec le produit.
- Ne déconnectez l'équipement que lorsque son alimentation a été préalablement coupée et que la zone est réputée non dangereuse.

Prévention des décharges électrostatiques

ATTENTION : cet équipement est sensible aux décharges électrostatiques, lesquelles peuvent entraîner des dommages internes et nuire au bon fonctionnement. Respectez les recommandations suivantes lorsque vous manipulez l'équipement :

- touchez un objet mis à la terre pour vous décharger de toute électricité statique éventuelle ;
- portez au poignet un bracelet antistatique homologué ;
- ne touchez pas les connecteurs ni les broches placés sur les cartes électroniques ;
- ne touchez pas les circuits internes de l'équipement ;
- utilisez si possible un poste de travail antistatique ;
- lorsque vous n'utilisez pas l'équipement, stockez-le dans un emballage antistatique adapté.

Assurez-vous que vous disposez de tous les composants

Avant de commencer, vérifiez que vous disposez de tous les composants dont vous aurez besoin.

IMPORTANT Vous devez utiliser un automate principal **et** un partenaire de sécurité pour obtenir un niveau SIL 3/PLe.

Automates 1756-L6*x*S

Une clé 1747-KY et une pile 1756-BA2 sont livrées avec les automates 1756-L6*x*S. Les partenaires de sécurité 1756-LSP sont livrés avec une pile 1756-BA2 .

Pour connecter un périphérique (par exemple, un ordinateur) au port série de l'automate, utilisez un câble série 1756-CP3.

En ce qui concerne la mémoire non volatile, une carte CompactFlash 1784-CF128 peut être utilisée avec les automates GuardLogix 1756-L6*x*S à partir du firmware révision 18 ou ultérieure.

Automates 1756-L7*x*S

Les accessoires suivants sont fournis avec les automates principaux et leurs partenaires de sécurité :

Référence	Description	Livré avec
1756-L71S 1756-L72S 1756-L73S	Automate principal	• Module de stockage d'énergie (ESM) à condensateur 1756-ESMCAP • Carte SD (Secure Digital) 1784-SD1, 1 Go • Clé 1747-KY
1756-L7SP	Partenaire de sécurité	• Module de stockage d'énergie (ESM) 1756-SPESMNSE
1756-L73SXT	Automate principal pour températures extrêmes	• Module de stockage d'énergie (ESM) à condensateur 1756-ESMCAPXT • Clé 1747-KY
1756-L7SPXT	Partenaire de sécurité pour températures extrêmes	• Module de stockage d'énergie (ESM) à condensateur 1756-SPESMNSXT

Les équipements optionnels suivants peuvent être utilisés.

Si votre application nécessite…	Utilisez le composant suivant…
une mémoire non volatile	1784-SD1 (1 Go) ou 1784-SD2 (2 Go)
que le niveau d'énergie résiduelle dans le module ESM présent dans l'appareil soit en dessous de 200 µJ avant que celui-ci puisse être installé ou retiré de votre application(1)	1756-ESMNSE pour l'automate principal 1756-SPESMNSE pour le partenaire de sécurité(2) Cet ESM n'effectue pas de sauvegarde de l'heure. En outre, vous ne pouvez utiliser cet ESM qu'avec un automate 1756-L73S (8 Mo) ou de capacité mémoire inférieure.
un module ESM qui protège l'automate en empêchant l'utilisation de la connexion USB et de la carte SD(1)	1756-ESMNRM pour l'automate principal 1756-SPESMNRM pour le partenaire de sécurité(3) Ce module ESM apportera à votre application un niveau de sécurité renforcé.

(1) Pour plus d'informations sur la durée de sauvegarde d'alimentation des modules ESM, reportez-vous à la rubrique Estimer le temps de maintien de l'horloge interne par le module ESM, page 124.

(2) Pour les températures extrêmes l'automate principal et le partenaire de sécurité utilisent respectivement des 1756-ESMNSEXT et 1756-SPESMNSEXT.

(3) Pour les températures extrêmes l'automate principal et le partenaire de sécurité utilisent respectivement des 1756-ESMNRMXT et 1756-SPESMNRMXT.

Installation d'un châssis et d'une alimentation

Avant d'installer un automate, vous devez installer un châssis et une alimentation.

1. Installez un châssis ControlLogix selon les instructions d'installation correspondantes.

Référence	Logements disponibles	Série	Reportez-vous aux notices d'installation suivantes
1756-A4	4	B	1756-IN005
1756-A7	7		
1756-A10	10		
1756-A13	13		
1756-A17	17		
1756-A4LXT	4	B	
1756-A5XT	5	B	
1756-A7XT	7	B	
1756-A7LXT	7	B	

   Les automates pour environnement extrême (XT) requièrent un châssis XT.

2. Installez une alimentation ControlLogix selon les instructions d'installation correspondantes.

Référence	Description	Série	Reportez-vous aux notices d'installation suivantes
1756-PA72	Alimentation c.a.	C	1756-IN005
1756-PB72	Alimentation c.c.		
1756-PA75	Alimentation c.a.	B	
1756-PB75	Alimentation c.c.		
1756-PAXT	Alimentation c.a. XT	B	
1756-PBXT	Alimentation c.c. XT		

   Les automates pour environnement extrême (XT) requièrent une alimentation XT.

Montage de la pile (automates 1756-L6*x*S uniquement)

Les automates 1756-L6*x*S et leurs partenaires de sécurité 1756-LSP contiennent une pile au lithium dont le remplacement est normalement nécessaire pendant la durée de vie de ces produits.

AVERTISSEMENT : lorsque vous branchez ou débranchez la pile, un arc électrique peut se produire, susceptible de provoquer une explosion dans un environnement dangereux. Assurez-vous que l'alimentation est coupée ou que l'environnement est classé non dangereux avant de poursuivre.

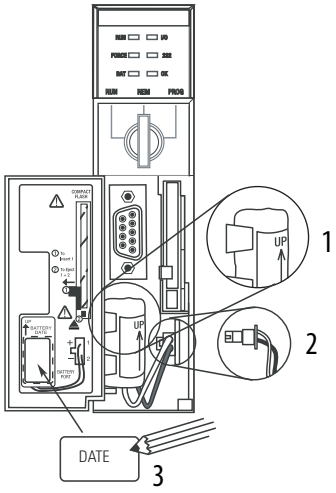
Pour toutes informations relatives à la sécurité concernant la manipulation des piles au lithium, notamment la manutention et l'élimination des piles qui fuient, reportez-vous à la publication AG 5-4, « Guidelines for Handling Lithium Batteries ».

Pour éviter de perdre le contenu de la mémoire de l'automate lorsque celui-ci est hors tension, installez une pile. Suivez cette procédure pour l'automate 1756-L6*x*S et le partenaire de sécurité 1756-LSP.

IMPORTANT Montez uniquement des piles 1756-BA2 dans l'automate. Si vous installez tout autre type de pile, vous risquez d'endommager l'automate.

Effectuez la procédure suivante pour mettre en place une pile 1756-BA2 neuve.

1. Insérez la pile comme indiqué.
2. Connectez la pile :
   + Rouge
   – Noir
3. Inscrivez sur l'étiquette de la pile la date à laquelle vous l'avez installée et fixez cette étiquette sur la face interne de la porte de l'automate.



Reportez-vous à l'Annexe B pour plus d'informations sur la maintenance des piles.

Installation de l'automate dans le châssis

Vous pouvez installer ou retirer un automate même lorsque le châssis est sous tension et que le système est en fonctionnement.

AVERTISSEMENT : lorsque vous insérez ou retirez le module alors que le bus intermodules est sous tension, un arc électrique peut se produire, susceptible de provoquer une explosion dans les installations en environnement dangereux.

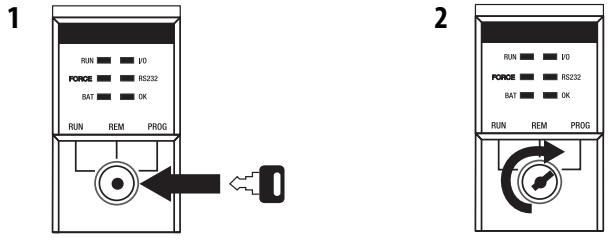
Assurez-vous que l'alimentation est coupée ou que l'environnement est classé non dangereux avant de poursuivre. Des arcs électriques répétés provoquent une usure excessive des contacts, à la fois sur le module et sur le connecteur de raccordement. Des contacts détériorés peuvent créer une résistance électrique qui affectera le bon fonctionnement du module.

IMPORTANT Pour les automates 1756-L7*x*S et leurs partenaires de sécurité 1756-L7SP, la charge du module ESM commence dès qu'une des actions suivantes se produit :

- l'automate et l'ESM sont installés dans un châssis sous tension ;
- l'alimentation est appliquée à un châssis contenant un automate avec un module ESM installé ;
- un module ESM est monté dans un automate sous tension.

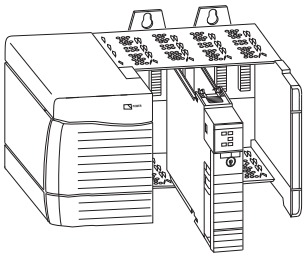
Une fois le système sous tension, le module ESM se charge pendant deux minutes au maximum, comme indiqué par le voyant CHRG ou le message « ESM Charging » (ESM en charge) sur l'afficheur d'état.

1. Insérez la clé dans l'automate principal.
2. Tournez la clé en position PROG.



Le partenaire de sécurité ne possède pas de clé.

3. Aligner le circuit imprimé sur les guides supérieur et inférieur du châssis.



4. Glissez l'automate à l'intérieur du châssis.

   L'automate est complètement installé quand il est de niveau avec l'alimentation ou d'autres modules adjacents et que les loquets supérieur et inférieur sont engagés.

IMPORTANT Le partenaire de sécurité doit être installé dans le logement immédiatement à droite de l'automate principal. Répétez les étapes 3 et 4 ci-dessus pour installer le partenaire de sécurité.

Après avoir inséré l'automate dans le châssis, reportez-vous au Chapitre 9 pour les informations d'interprétation des signaux des voyants d'état de l'automate principal et du partenaire de sécurité.

Insertion et retrait d'une carte mémoire

AVERTISSEMENT : quand vous insérez ou retirez la carte mémoire sous tension, un arc électrique peut se produire, susceptible de provoquer une explosion dans les installations en environnement dangereux. Assurez-vous que l'alimentation est coupée ou que l'environnement est classé non dangereux avant de poursuivre.

ATTENTION : si vous n'êtes **pas** sûr des contenus de la carte mémoire **avant** de l'installer, tournez le commutateur à clé de l'automate sur la position PROG. Selon le contenu de la carte, une remise sous tension ou un défaut pourrait provoquer le chargement par la carte d'un projet ou d'un système d'exploitation différent dans l'automate.

Les automates 1756-L7*x*S utilisent des cartes SD (Secure Digital). Voir Page 30.

Les automates 1756-L6*x*S utilisent des cartes CompactFlash (CF). Voir Page 32.

Carte SD (automates 1756-L7*x*S)

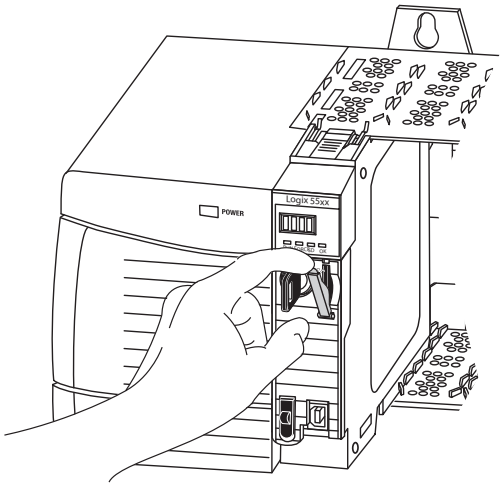
Les automates 1756-L7*x*S sont livrés avec une carte SD installée. Nous recommandons que vous laissiez une carte SD installée.

Retrait de la carte SD

Pour retirer la carte SD d'un automate 1756-L7*x*S, procédez de la façon suivante :

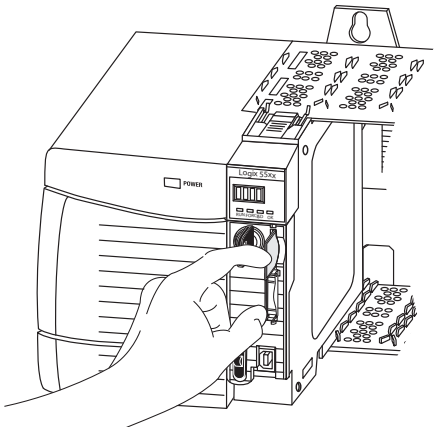
IMPORTANT Vérifier que le voyant d'état de la carte SD est éteint et que cette carte n'est pas en cours d'utilisation avant de la retirer.

1. Tournez le commutateur à clé en position PROG.
2. Ouvrez la trappe pour accéder à la carte SD.



32015-M

3. Pousser et relâcher la carte SD pour l'éjecter.



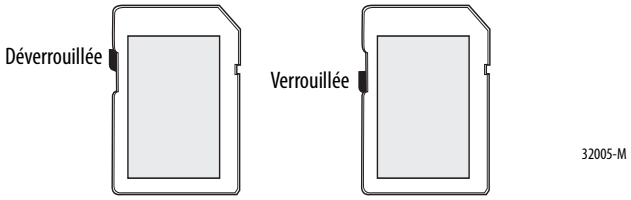
32004-M

4. Retirer la carte SD et refermer la trappe.

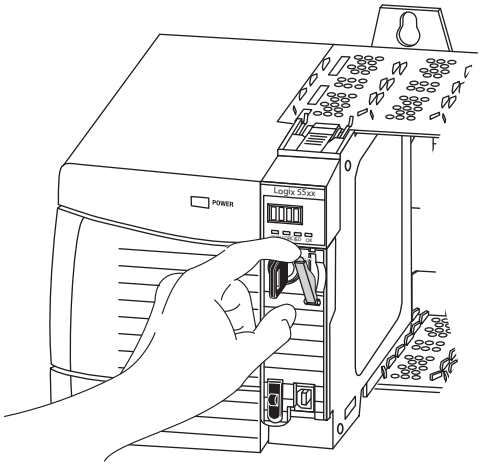
Installation de la carte SD

Procédez de la façon suivante pour mettre en place la carte SD sur un automate 1756-L7*x*S.

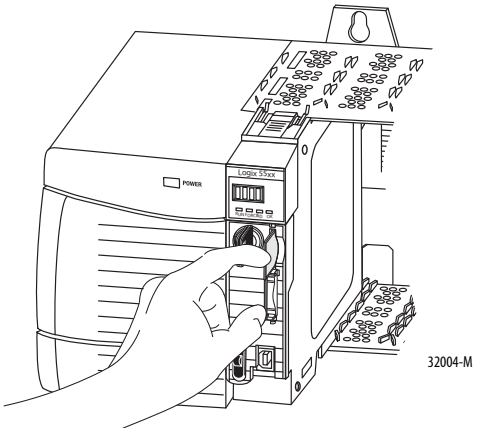
1. Vérifiez que la carte SD est verrouillée ou déverrouillée, selon votre préférence.



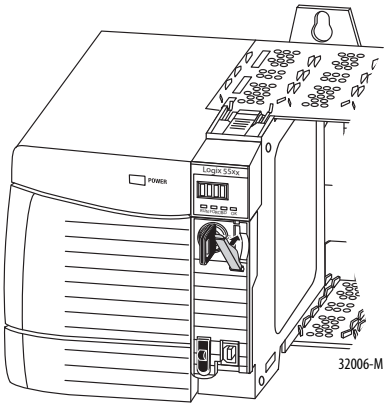
2. Ouvrez la trappe du logement de la carte SD.



3. Insérez la carte SD dans son logement.
4. Appuyez doucement sur la carte jusqu'à ce qu'elle s'enclenche en position.



5. Fermez la trappe du logement de la carte SD.



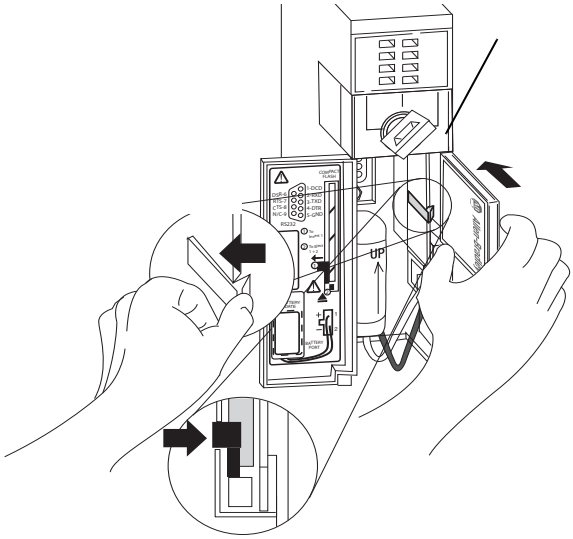
Carte CompactFlash (automates 1756-L6*x*S)

Dans le cas des automates 1756-L6xS, la carte CompactFlash n'est pas livrée montée.

Mise en place d'une carte CF

Suivez ces étapes pour mettre en place la carte mémoire.

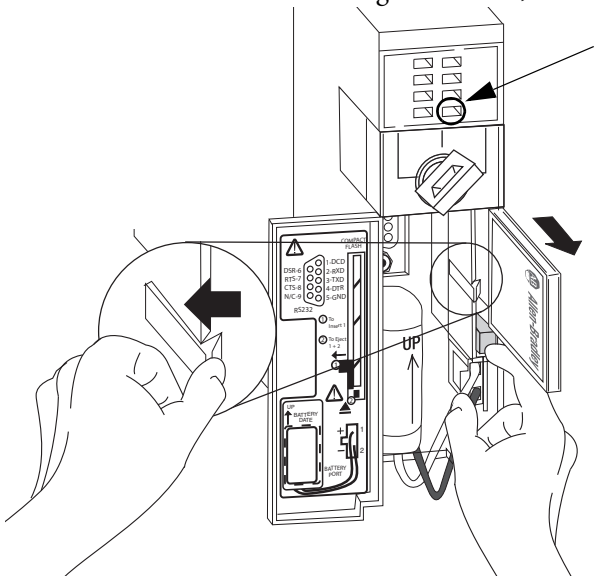
1. Tournez le commutateur à clé en position PROG.
2. Ouvrez la porte de l'automate.
3. Repoussez la griffe de maintien vers la gauche.
4. Insérez la carte mémoire avec le logo Allen-Bradley orienté vers la gauche.
5. Relâchez la griffe de maintien et vérifiez qu'elle vient bien bloquer la carte mémoire.



Retrait d'une carte CF

Suivez ces étapes pour retirer la carte mémoire.

1. Si l'indicateur d'état OK clignote en vert, attendez qu'il passe en vert fixe.



2. Ouvrez la porte de l'automate.
3. Repoussez la griffe de maintien vers la gauche et maintenez-la dans cette position.
4. Appuyez sur le bouton d'éjection et retirez la carte.
5. Relâchez la griffe de maintien.

Établir les connexions de communication

Les automates 1756-L7*x*S sont équipés d'un port USB. Voir Connexion au port USB d'un automate 1756-L7xS.

Les automates 1756-L6*x*S sont équipés d'un port série. Voir Connexion au port série d'un automate 1756-L6xS, page 36.

Connexion au port USB d'un automate 1756-L7*x*S

L'automate possède un port USB qui utilise une prise de type B. Le port est compatible USB 2.0 et fonctionne à 12 Mbits/s.

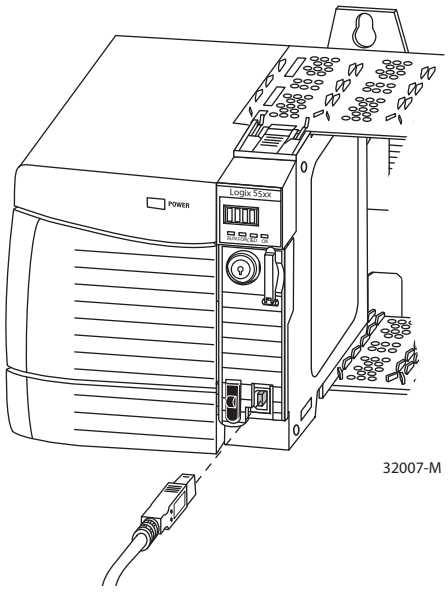
Pour utiliser le port USB de l'automate, vous devez avoir installé le logiciel RSLinx en version 2.59 ou ultérieure sur votre poste de travail. Utilisez un câble USB pour connecter votre poste de travail au port USB de l'automate. Au moyen de cette connexion, vous pourrez mettre à jour le firmware et charger des programmes sur l'automate directement depuis votre ordinateur.

ATTENTION : le port USB est prévu uniquement pour une utilisation temporaire, afin d'effectuer la programmation localement, et non pour une connexion permanente.

Le câble USB ne doit pas dépasser 3,0 m ni être branché sur un concentrateur.

AVERTISSEMENT : n'utilisez pas le port USB dans des environnements dangereux.

Figure 3 – Connexion USB



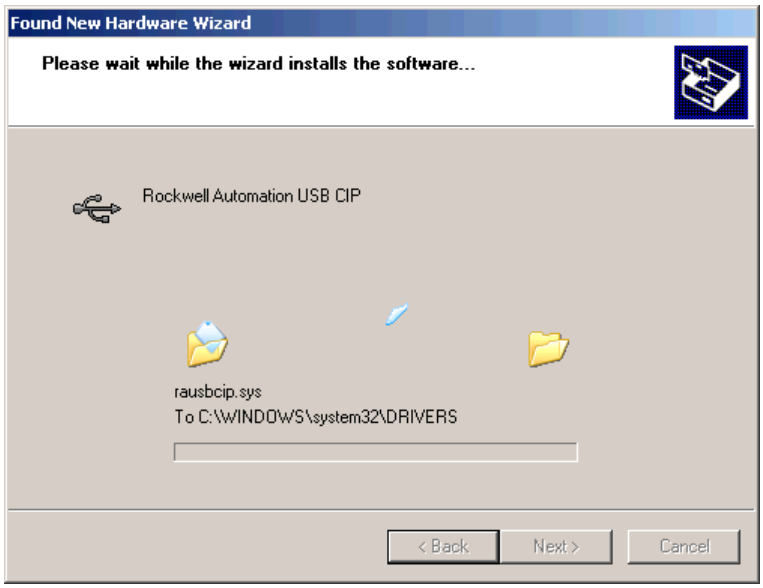
Pour configurer le logiciel RSLinx pour l'utilisation d'un port USB, vous devez d'abord installer un driver USB. Pour installer un driver USB, effectuez cette procédure.

1. Raccordez votre automate et votre poste de travail au moyen d'un câble USB.
2. Dans le boîte de dialogue de l'assistant « Found New Hardware » (Recherche de nouveau matériel), cliquez sur l'une des options de connexion de mise à jour Windows et cliquez sur Next (Suivant).

CONSEIL Si le logiciel fournissant le driver USB est introuvable et que l'installation est annulée, vérifiez que vous avez bien installé la version 2.59 ou supérieure du logiciel RSLinx Classic.

3. Cliquez sur « Install the software automatically » (Installer le logiciel automatiquement) – procédure recommandée – puis sur Next (Suivant).

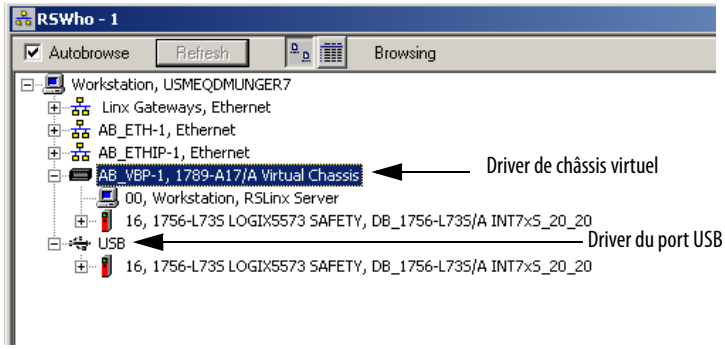
   Le logiciel est installé.



4. Cliquez sur Finish (Terminer) pour installer votre driver USB.

5. Pour accéder à votre automate par l'intermédiaire du logiciel RSLinx, cliquez sur RSWho  .

Dans l'organisateur de la station de travail RSLinx, votre automate apparaît sous deux drivers différents, un châssis virtuel et le port USB. Vous pouvez utiliser l'un ou l'autre de ces drivers pour atteindre votre automate.



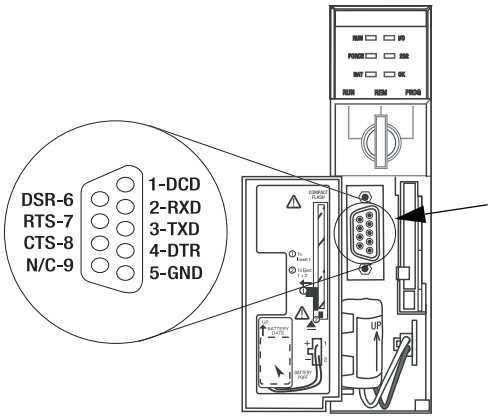
Connexion au port série d'un automate 1756-L6*x*S

AVERTISSEMENT : si vous connectez ou déconnectez le câble série au/du module alors que ce dernier ou tout autre périphérique série raccordé à son autre extrémité est sous tension, un arc électrique peut se produire, susceptible de provoquer une explosion dans les installations en environnement dangereux.

Assurez-vous que l'alimentation est coupée ou que l'environnement est classé non dangereux avant de poursuivre.

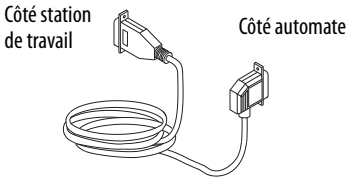
Utilisez le port série de l'automate 1756-L6*x*S pour les communications RS-232.

Figure 4 – Port série



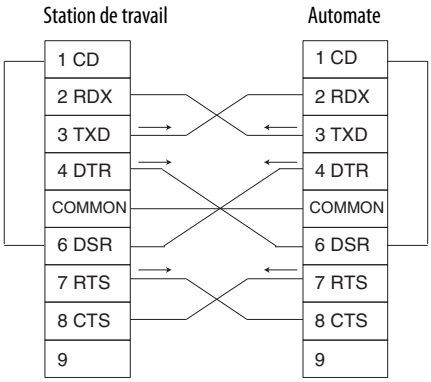
Pour connecter une station de travail au port série de l'automate, utilisez l'un des câbles suivants :

- un câble série 1756-CP3 ;
- un câble 1747-CP3 de la famille des produits SLC (si vous utilisez ce type câble, il se peut que vous ayez du mal à refermer la porte de l'automate).



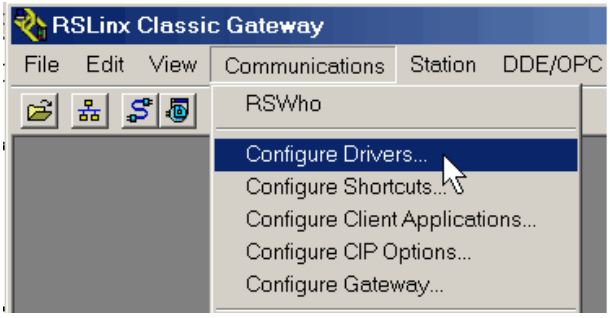
Tenez compte des consignes suivantes si vous choisissez de fabriquer vous-même votre câble série :

- Limitez la longueur à 15,2 m.
- Câblez les connecteurs conformément au schéma ci-contre.
- Raccordez le blindage aux deux connecteurs.

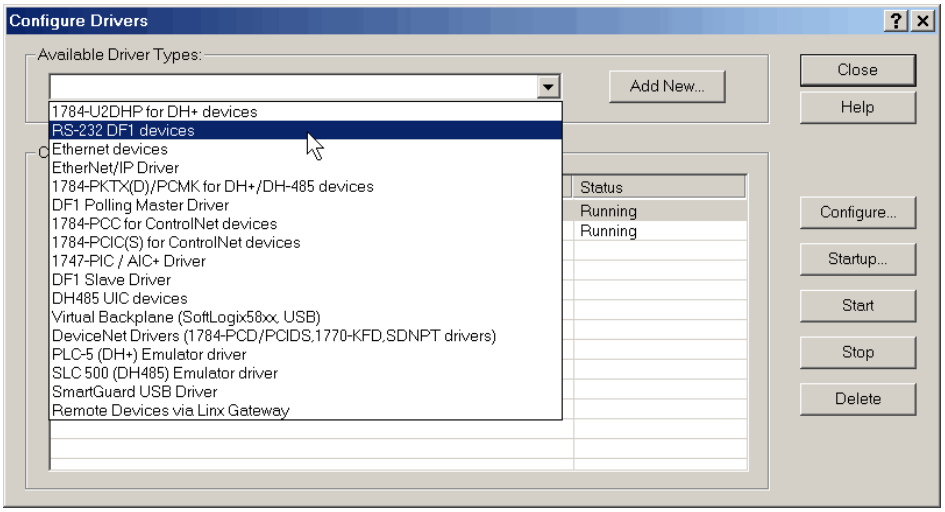


Pour configurer le driver de communication série RS-232 DF1 au moyen du logiciel RSLinx, procédez de la façon suivante.

1. Dans le menu Communications du logiciel RSLinx, sélectionnez « Configure Drivers » (Configuration des drivers).

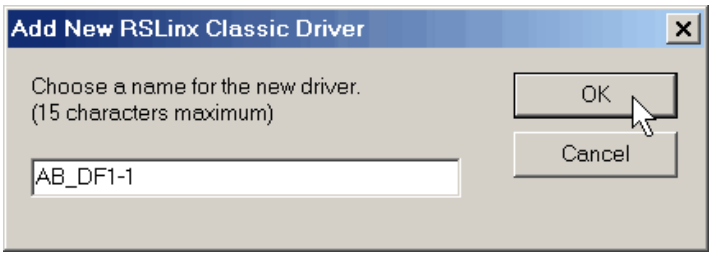


La boîte de dialogue de configuration de driver apparaît.

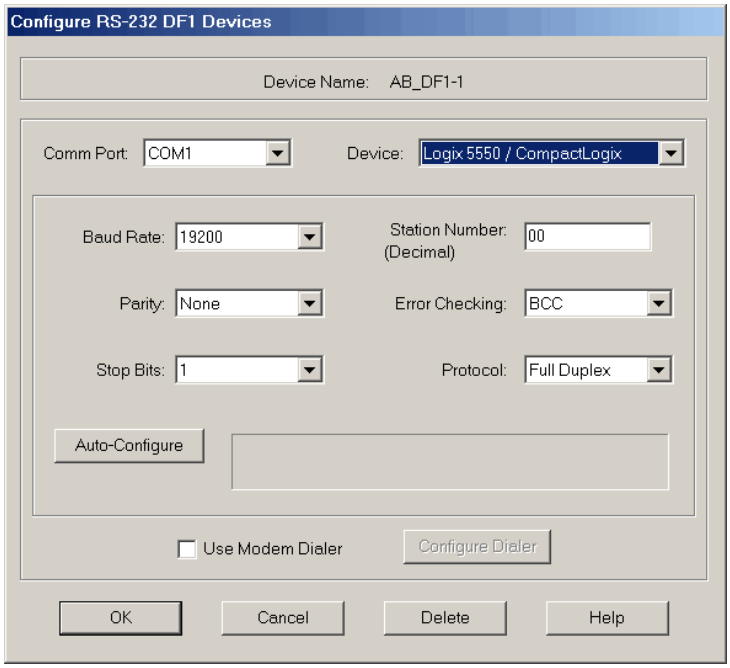


2. Dans la liste déroulante « Available Driver Types » (Types de drivers disponibles), sélectionnez le driver RS-232 DF1.
3. Cliquez sur « Add New » (Ajouter nouveau).

La boîte de dialogue « Add New RSLinx Driver » (Ajouter un nouveau driver RSLinx) apparaît.



4. Tapez le nom de ce driver et cliquez sur OK.
5. Spécifiez les paramètres du port série.
   a. Dans le menu déroulant « Comm Port » (Port de communication), sélectionnez le port série de la station de travail auquel le câble est raccordé.
   b. Dans le menu déroulant « Device » (Périphérique), sélectionnez « Logix 5550/CompactLogix ».
   c. Cliquez sur « Auto-Configure » (Configuration automatique).



6. Si la configuration automatique a été réalisée correctement, cliquez sur OK.

   Si la configuration automatique a échoué, vérifiez que le bon port Comm a été sélectionné.
7. Cliquez sur Close (Fermer).

Mise à jour de l'automate

Les automates sont livrés sans firmware. Le firmware de l'automate est inclus avec le logiciel de programmation RSLogix 5000. Par ailleurs, le firmware de l'automate est également disponible en téléchargement depuis le site Internet de l'Assistance Technique de Rockwell Automation à l'adresse : http://www.rockwellautomation.com/support/.

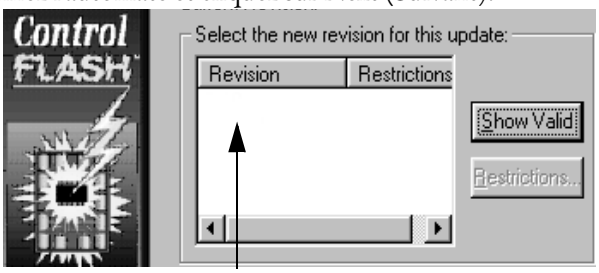
Vous pouvez mettre à jour le firmware de votre automate soit au moyen de l'utilitaire ControlFLASH™ fourni avec le logiciel RSLogix 5000, soit en utilisant la fonction AutoFlash de ce même logiciel RSLogix 5000.

Utilisation du logiciel ControlFLASH pour mettre à jour le firmware

Avec l'utilitaire ControlFLASH en version 8 ou ultérieure (à partir de la version 18 du logiciel RSLogix 5000), le partenaire de sécurité est mis à jour automatiquement à chaque fois que l'automate principal est mis à jour.

IMPORTANT Sur les automates 1756-L7*x*S, lorsque la carte SD est verrouillée et que l'option « Stored Project's Load Image » (Chargement de l'image projet enregistrée) est définie sur « On Power Up » (à la mise sous tension), le firmware de l'automate ne sera pas mis à jour au terme de la procédure. Tout firmware et projets précédemment enregistrés seront rechargés à la place.

1. Vérifiez qu'il existe une connexion réseau appropriée et que le driver pour ce réseau a été bien configuré dans le logiciel RSLinx.
2. Lancez le logiciel ControlFLASH.
3. Cliquez sur Next (Suivant).
4. Sélectionnez la référence de l'automate et cliquez sur Next (Suivant).
5. Développez le réseau jusquà ce que vous voyez l'automate.
6. Sélectionnez l'automate et cliquez sur Next (Suivant).



7. Sélectionnez le niveau de révision auquel vous voulez mettre à jour l'automate et cliquez sur Next (Suivant).
8. Pour commencer la mise à jour de l'automate, cliquez sur Finish (Terminer) et ensuite sur Yes (Oui).

   Après la mise à jour de l'automate, la boîte de dialogue d'état affiche « Update complete » (Mise à jour terminée).

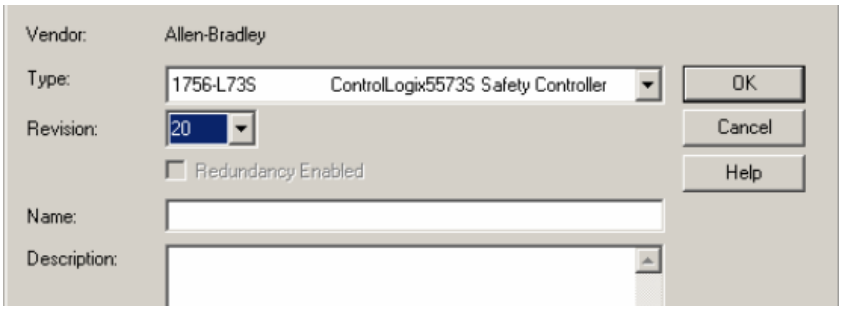
   IMPORTANT Laissez la mise à jour du firmware s'achever complètement avant de couper/rétablir l'alimentation ou d'interrompre de quelque façon le processus.

   CONSEIL Si sa mise à jour par ControlFLASH est interrompue, l'automate 1756-L7*x*S revient au firmware initial (c'est à dire, celui dont le numéro de révision est de la forme 1.*xxx*).
9. Cliquez sur OK.
10. Fermez le logiciel ControlFLASH.

Utilisation d'AutoFlash pour la mise à jour du firmware

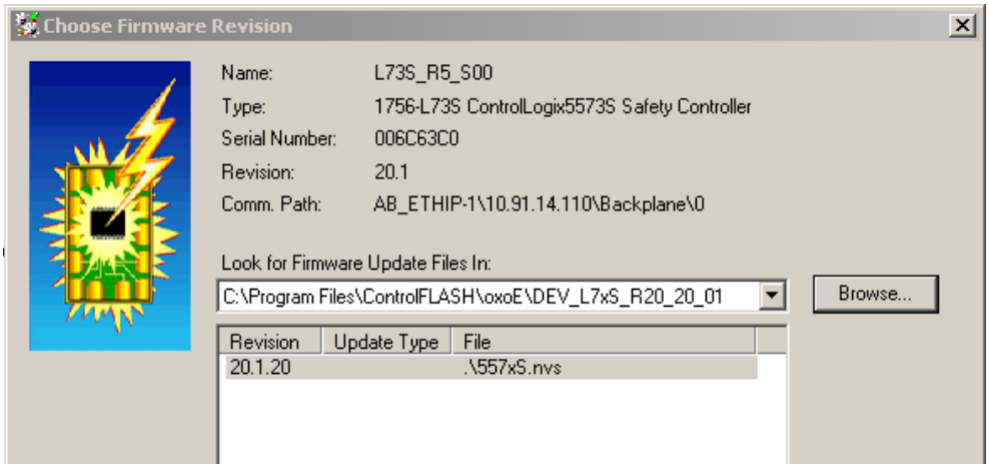
Pour mettre à jour le firmware de votre automate à l'aide de la fonction AutoFlash du logiciel RSLogix 5000, procédez de la façon suivante.

1. Vérifiez qu'il existe une connexion réseau appropriée et que votre driver réseau a été bien configuré dans le logiciel RSLinx.
2. Utilisez le logiciel de programmation RSLogix 5000 pour créer un projet d'automate utilisant la version que vous souhaitez.



3. Cliquez sur RSWho pour spécifier le chemin d'accès à l'automate.

4. Sélectionnez votre automate et cliquez sur Update Firmware (Mettre à jour le firmware).
5. Sélectionnez la version (numéro de révision) du firmware à laquelle vous voulez mettre à jour l'automate.



6. Cliquez sur Update (Mise à jour).
7. Cliquez sur Yes (oui).

Laissez la mise à jour du firmware se dérouler sans l'interrompre. Une fois la mise à niveau de firmware terminée, la boîte de dialogue Who Active (Qui est actif) s'ouvre. Elle vous permet d'effectuer d'autres tâches au moyen du logiciel RSLogix 5000.

Choisir le mode de fonctionnement de l'automate

Servez-vous de ce tableau comme référence pour définir le mode de fonctionnement de votre automate.

Tableau 9 – Mode de fonctionnement de l'automate

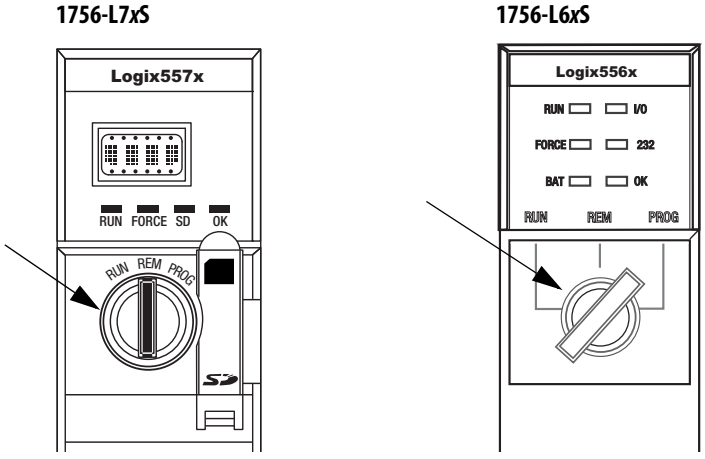
Si vous voulez	Sélectionnez l'un de ces modes				
	Run	À distance			Programmation
		Run	Test	Program-mation	
Ramener les sorties dans l'état commandé par le programme du projet	X	X			
Ramener les sorties dans l'état configuré pour le mode Programmation			X	X	X
Exécuter (scruter) les tâches	X	X	X		
Changer le mode de l'automate par le logiciel		X	X	X	
Télécharger un projet		X	X	X	X
Planifier un réseau ControlNet				X	X
Modifier le projet lorsque vous êtes en ligne		X	X	X	X
Envoyer des messages	X	X	X		
Envoyer et recevoir des données en réponse à un message provenant d'un autre automate	X	X	X	X	X
Produire et consommer des points	X	X	X	X	X

Utiliser le commutateur à clé pour changer le mode de fonctionnement

Le commutateur à clé situé en façade de l'automate peut être utilisé pour placer l'automate dans l'un des modes de fonctionnement suivants :

- Programmation (PROG)
- A distance (REM)
- Exécution (RUN)

Figure 5 – Commutateur à clé de l'automate



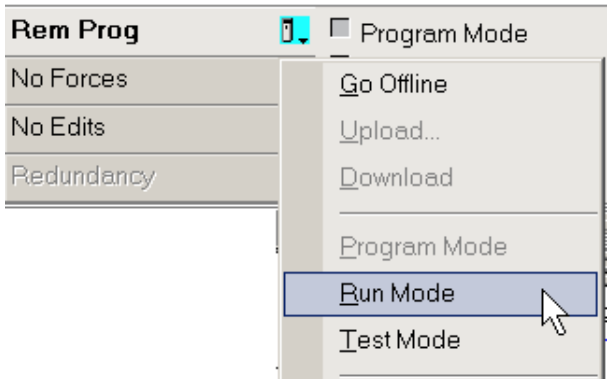
Utilisation du logiciel RSLogix 5000 pour changer de mode de fonctionnement

Selon la position dans laquelle se trouve le commutateur à clé de l'automate, vous pouvez changer le mode de fonctionnement de celui-ci à l'aide du logiciel RSLogix 5000.

Une fois que vous avez établi la communication avec l'automate et que son commutateur à clé est placé sur REM (à distance), c'est-à-dire en position centrale, vous pouvez utiliser le menu « Controller Status » (État de l'automate) situé dans le coin supérieur gauche de la fenêtre du logiciel RSLogix 5000 pour définir l'un des modes de fonctionnement suivants :

- Remote Program (programmation à distance)
- Remote Run (exécution à distance)
- Remote Test (test à distance)

Figure 6 – Accès au mode de fonctionnement par l'intermédiaire du logiciel RSLogix 5000



CONSEIL Pour cet exemple, le commutateur à clé de l'automate est réglé sur le mode à distance. Si le commutateur à clé de votre automate est réglé sur le mode Exécution (Run) ou Programmation (Prog), les options du menu seront différentes.

Démontage d'un module de stockage d'énergie (ESM)

Les automates 1756-L7*x*S sont livrés avec un module ESM installé.

Automate	Réf. de l'ESM installé
Automate 1756-L7*x*S	1756-ESMCAP
Automate pour températures extrêmes 1756-L7*x*SXT	1756-ESMCAPXT
Partenaire de sécurité 1756-L7SP	1756-SPESMNSE
Partenaire de sécuirté pour températures extrêmes 1756-L7SPXT	1756-SPESMNSEXT

Tenez compte des points suivants avant de procéder à la dépose du module ESM :

- Une fois qu'un automate 1756-L7*x*S n'est plus alimenté, soit parce que l'alimentation de son châssis a été coupée, soit parce qu'il a été retiré d'un châssis sous tension, ne démontez pas son module ESM immédiatement.

  Attendez que le voyant d'état OK de cet automate passe du vert au rouge fixe puis s'éteigne avant de procéder à la dépose de son module ESM.

- Utilisez le module 1756-ESMNSE lorsque votre application nécessite que le module de stockage d'énergie en place soit capable de se vider de l'énergie résiduelle qu'il contient jusqu'en dessous d'un seuil de 40 µJ avant d'être transporté dans ou hors de votre application.

- Une fois installé, vous ne pourrez plus retirer le module 1756-ESMNRM d'un automate 1756-L7*x*S.

IMPORTANT Avant de déposer le module ESM, effectuez les ajustements nécessaires dans votre programme pour anticiper les modifications potentielles de l'attribut WallClockTime.

Suivez ces étapes pour retirer un module 1756-ESMCAP(XT), 1756-ESMNSE(XT), ou 1756-SPESMNSE(XT).

AVERTISSEMENT : si votre application nécessite que le module ESM soit déchargé de son énergie résiduelle jusqu'à un niveau de 40 µJ ou inférieur avant de pouvoir être transporté dans ou hors de l'application, utiliser uniquement le module 1756-ESMNSE(XT) pour l'automate principal et le 1756-SPESMNSE(XT) pour le partenaire de sécurité. Dans ce cas, les actions suivantes seront à effectuer pour pouvoir retirer le module ESM :

a. Couper l'alimentation du châssis.

   Une fois l'alimentation du châssis coupée, le voyant d'état OK de l'automate passe du vert au rouge fixe puis s'éteint.

b. Attendez **au moins 20 minutes** pour que le niveau d'énergie résiduelle redescende en dessous de 40 µJ avant de retirer l'ESM.

   Aucun témoin visuel n'indique que ce délai 20 minutes est écoulé. **Vous devez donc contrôler cette durée vous-même**.

AVERTISSEMENT : quand vous insérez ou retirez un module de stockage d'énergie alors que le bus intermodules est sous tension, un arc électrique peut se produire, susceptible de provoquer une explosion dans les installations en environnement dangereux.

Assurez-vous que l'alimentation est coupée ou que l'environnement est classé non dangereux avant de poursuivre. Des arcs électriques répétés provoquent une usure excessive des contacts, à la fois sur le module et sur le connecteur de raccordement.

1. Retirez la clé du commutateur à clé.

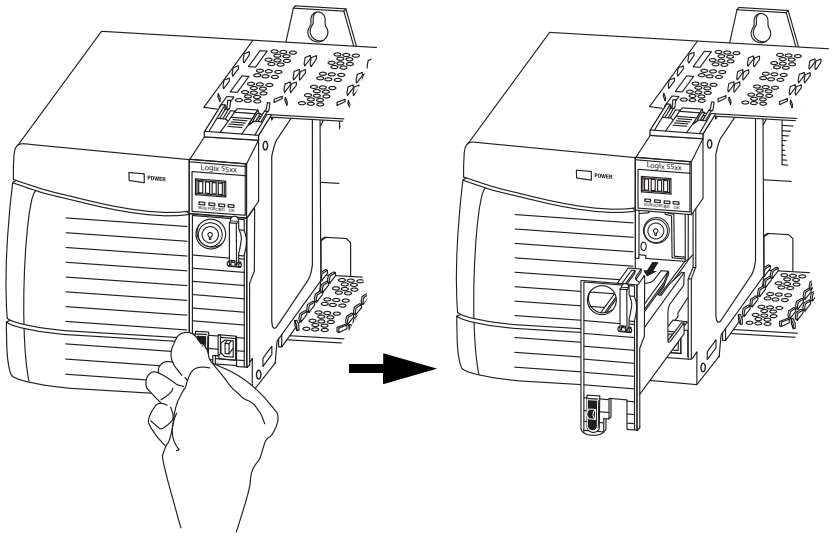
IMPORTANT L'étape suivante dépend de la situation de votre application.

- Si vous procédez à la dépose du module ESM d'un automate 1756-L7*x*S(XT) sous tension, vous pouvez passer à l'étape 2.
- Si vous procédez à la dépose du module ESM d'un automate 1756-L7*x*S(XT) qui n'est plus alimenté, soit parce que l'alimentation de son châssis a été coupée, soit parce qu'il a été retiré d'un châssis sous tension, **ne démontez pas** le module ESM immédiatement.

  Attendez que le voyant d'état OK de cet automate passe du vert au rouge fixe puis s'éteigne avant de procéder à la dépose de son module ESM.

  Après que le voyant d'état OK se soit éteint, passez à l'étape 2.

2. Appuyer sur le bouton de déblocage noir avec le pouce et extraire le module ESM de l'automate.



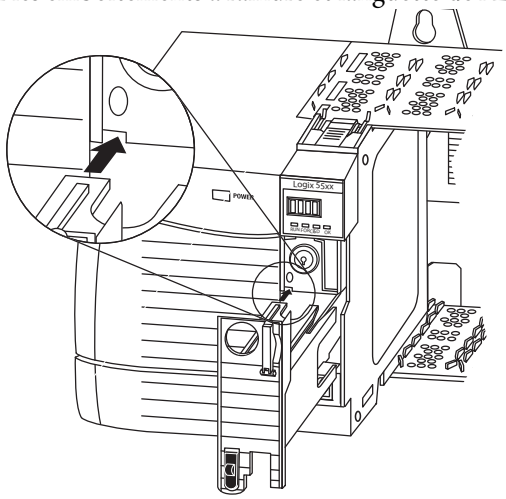
Installation d'un module de stockage d'énergie (ESM)

Tableau 10 – Modules de stockage d'énergie compatibles

Référence	ESM compatibles
1756-L7*x*S	1756-ESMCAP, 1756-ESMNSE, 1756-ESMNRM
1756-L7*x*SXT	1756-ESMCAPXT, 1756-ESMNSEXT, 1756-ESMNRMXT
1756-L7SP	1756-SPESMNSE, 1756-SPESMNRM
1756-L7SPXT	1756-SPESMNSEXT, 1756-SPESMNRMXT

Pour installer un ESM, effectuez ces étapes. Suivez les mêmes étapes pour le partenaire de sécurité.

1. Alignez les emboîtements à rainure et languette de l'ESM et de l'automate.



2. Glissez l'ESM dans le châssis jusqu'à ce qu'il s'enclenche en position.

ATTENTION : pour éviter tout risque de dommage au produit lors de la mise en place de l'ESM, bien l'aligner sur la glissière et le faire coulisser vers l'avant en lui appliquant une force minimum, jusqu'à ce qu'il s'enclenche en position.

L'ESM commence sa charge dès qu'il est installé. L'état de la charge est indiqué par l'un des messages suivants :

- « ESM Charging » (ESM en charge)
- CHRG

Après la mise en place de l'ESM, il peut s'écouler jusqu'à 15 secondes avant que les messages d'état de la charge ne commencent à s'afficher.

IMPORTANT Laisser l'ESM achever sa charge avant de couper l'alimentation de l'automate. Pour confirmer la charge complète du module ESM, vérifiez l'afficheur d'état et assurez-vous que les messages « CHRG » ou « ESM charging » n'apparaissent plus.

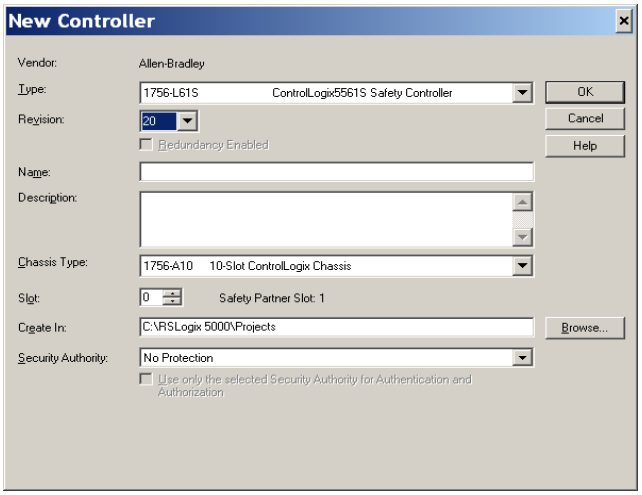
CONSEIL Contrôlez les attributs de l'objet WallClockTime après l'installation d'un ESM afin de vérifier que l'heure de l'automate est correcte.

Configuration de l'automate

Création d'un projet automate

Pour configurer et programmer votre automate, utilisez le logiciel RSLogix 5000 afin de créer et de gérer un projet pour cet automate.

1. Créez un projet dans le logiciel RSLogix 5000 en cliquant sur le bouton New (Nouveau) sur la barre d'outils principale.
2. À partir du menu déroulant Type, sélectionnez un automateGuardLogix :
   - Automate 1756-L61S ControlLogix5561S
   - Automate 1756-L62S ControlLogix5562S
   - Automate 1756-L63S ControlLogix5563S
   - Automate 1756-L71S ControlLogix5571S
   - Automate 1756-L72S ControlLogix5572S
   - Automate 1756-L73S ControlLogix5573S



3. Entrez le numéro de révision majeure du firmware de cet automate.

4. Entrez un nom pour l'automate.

   Lorsque vous créez un projet, son nom par défaut est identique à celui de l'automate. Cependant, vous avez la possibilité de renommer le projet ou l'automate.

5. Sélectionnez la taille du châssis.
6. Entrez le numéro de logement de l'automate.

   La boîte de dialogue New Controller (Nouvel automate) affiche le numéro de logement du partenaire de sécurité en fonction du numéro saisi pour l'automate principal.

   Si vous sélectionnez pour l'automate principal un numéro de logement qui ne corresponde pas à la position située immédiatement à gauche de celle du partenaire de sécurité, un message vous notifiera de ressaisir un numéro valide.

7. Indiquez le dossier dans lequel sera stocké le projet d'automate de sécurité.
8. Dans RSLogix 5000 à partir de la version 20, vous devez sélectionner une option « Security Authority » (Contrôle de sécurité).

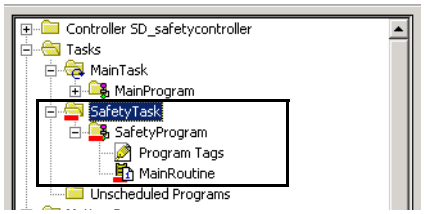
   Pour des informations complémentaires sur la sécurité, reportez-vous à la publication 1756-PM016, « Sécurité des automates Logix5000 – Manuel de programmation ».

9. Cliquez sur OK.

Le logiciel RSLogix 5000 crée automatiquement une tâche de sécurité et un programme de sécurité.

Un sous-programme principal de sécurité en logique à relais, appelé « MainRoutine », est également créé dans le programme de sécurité.

Figure 7 – Tâche de sécurité dans la fenêtre d'organisation de l'automate



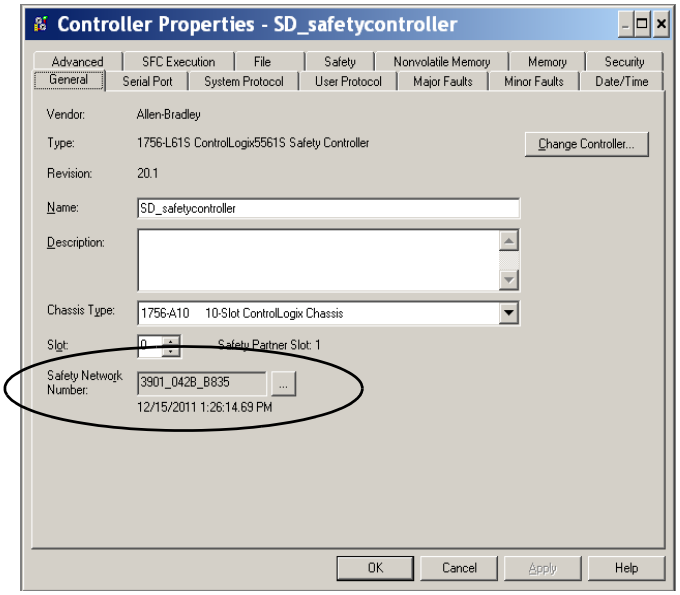
Un trait rouge sous l'icône permet de différencier les programmes et sous-programmes de sécurité des composants de projet standard dans la fenêtre d'organisation de l'automate de RSLogix 5000.

Lorsque vous créez un nouveau projet de sécurité, le logiciel RSLogix 5000 génère également automatiquement un numéro de réseau de sécurité (SNN) temporel.

Ce numéro SNN définit le bus intermodules du châssis local comme sous-réseau de sécurité. Vous pouvez le visualiser et le modifier dans l'onglet « General » (Général) de la boîte de dialogue « Controller Properties » (Propriétés de l'automate).

Ce SNN temporel créé automatiquement est suffisant pour la plupart des applications. Cependant, dans certains cas, vous pourrez être amené à entrer un SNN particulier.

Figure 8 – Numéro de réseau de sécurité (SNN)



CONSEIL

Vous pouvez utiliser la boîte de dialogue « Controller Properties » (Propriétés de l'automate) pour transformer un automate standard en automate de sécurité et vice-versa, en cliquant sur « Change Controller » (Changer l'automate). Mais cette action a une incidence importante sur les projets standard et de sécurité enregistrés.

Pour de plus amples informations sur les répercutions d'un changement de type d'automate, reportez-vous à l'Annexe C, « Changement du type d'automate dans un projet RSLogix 5000 ».

Tableau 11 – Informations connexes

Ressource	Description
Chapitre 6, Développement d'applications de sécurité.	Contient des informations complémentaires sur la tâche de sécurité, les programmes et sous-programmes de sécurité
Chapitre 4, Communications en réseaux	Contient des informations complémentaires sur la gestion du numéro SNN

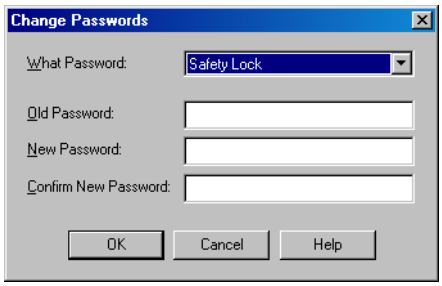
Définition des mots de passe pour le verrouillage et le déverrouillage de la sécurité

Verrouiller la sécurité de l'automate permet d'empêcher la modification des composants de commande de sécurité. Ce verrouillage porte uniquement sur les composants de sécurité, tels que la tâche de sécurité, les programmes de sécurité, les sous-programmes de sécurité et les points de sécurité. Les composants standard ne sont pas concernés. Vous pouvez verrouiller ou déverrouiller la sécurité du projet avec l'automate en ligne ou hors ligne.

La fonction de verrouillage et de déverrouillage de la sécurité utilise deux mots de passe distincts, qui sont facultatifs.

Pour définir ces mots de passe, procédez comme suit.

1. Choisissez Tools > Safety > Change Password (Outils > Sécurité > Modifier le mot de passe).
2. Dans la liste déroulante What Password (Quel mot de passe), sélectionnez Safety Lock (Verrouiller la sécurité) ou Safety Unlock (Déverrouiller la sécurité).

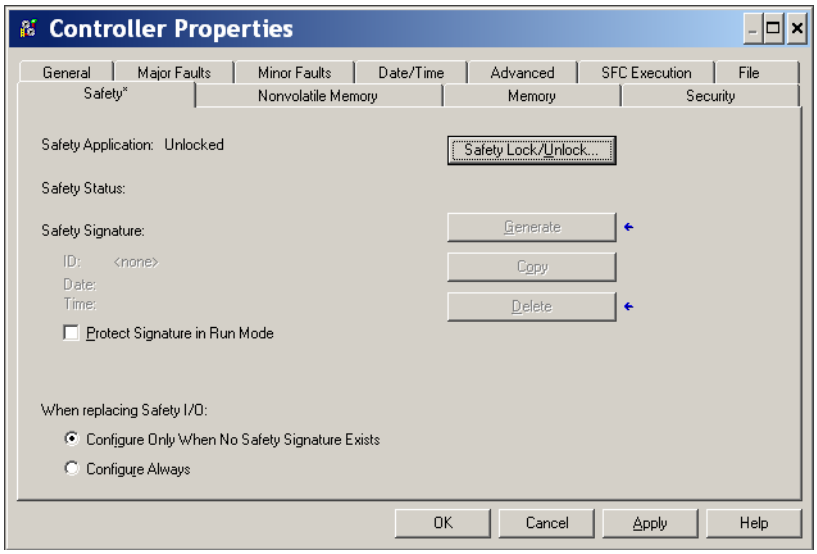


3. Entrez l'ancien mot de passe s'il en existe un.
4. Entrez et confirmez le nouveau mot de passe.
5. Cliquez sur OK.

   Les mots de passe peuvent contenir de 1 à 40 caractères et ne sont pas sensibles à la casse. Les lettres, les chiffres, ainsi que les symboles suivants peuvent être utilisés : ' ~ ! @ # $ % ^ & * ( ) _ + , – = { } | [ ] \ : ; ? / .

Protection de la signature de tâche de sécurité en mode exécution

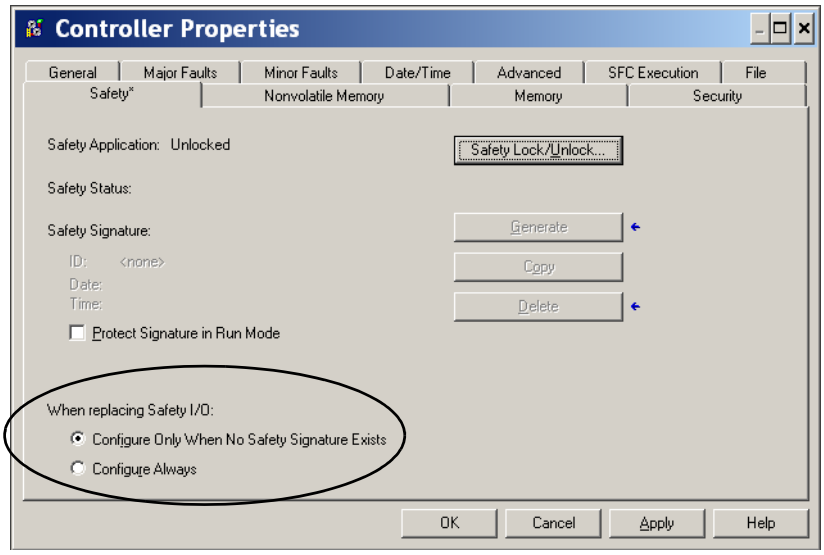
Vous pouvez empêcher la création ou la suppression de la signature de tâche de sécurité en mode Run (Exécution) ou en mode REM RUN (Exécution à distance), que l'application de sécurité soit verrouillée ou non, en cochant Protect Signature in Run Mode (Protéger la signature en mode Exécution) dans l'onglet Security (Sécurité) de la boîte de dialogue Controller Properties (Propriétés de l'automate).



Gestion du remplacement d'un module d'E/S

L'onglet « Safety » (Sécurité) de la boîte de dialogue « Controller Properties » (Propriétés de l'automate) vous permet de définir la façon dont l'automate va gérer le remplacement d'un module d'E/S dans le système. Cette option permet de choisir si l'automate doit assigner le numéro SNN à un module d'E/S auquel il est connecté et pour lequel il possède des informations de configuration lorsqu'une signature de tâche[1] de sécurité existe.

Figure 9 – Options de remplacement de modules d'E/S



ATTENTION : n'activez la fonction « Configure Always » (Toujours configurer) que si vous n'avez pas besoin de faire appel à la totalité du système de commande de sécurité (CIP Safety) routable pour maintenir le niveau d'intégrité de sécurité SIL 3 pendant le remplacement et le test fonctionnel d'un module.

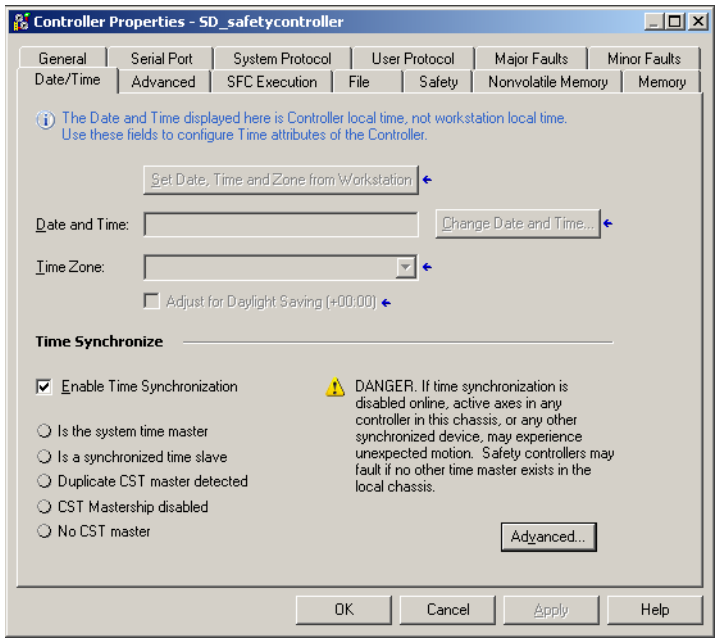
Voir Chapitre 5, Ajout, configuration, surveillance et remplacement d'E/S de sécurité CIP Safety pour des informations complémentaires.

Activation de la synchronisation temporelle

Dans un système automate GuardLogix, un dispositif présent dans le châssis local doit être défini comme horloge maître pour le temps système coordonné (CST). Pour permettre à l'automate de devenir l'horloge maître CST, activez la fonction « Time Synchronization » (Synchronisation temporelle) dans l'onglet « Date/Time » (Horodatage) de la boîte de dialogue « Controller Properties » (Propriétés de l'automate). La synchronisation temporelle offre une procédure standard de synchronisation des horloges des périphériques distribués sur un réseau.

(1) La signature de tâche de sécurité est un numéro utilisé par le système GuardLogix pour identifier de manière unique chaque programme, donnée et éléments de configuration d'un projet. Elle protège ainsi le niveau d'intégrité de sécurité (SIL) du système. Pour de plus amples informations, voir Signature de tâche de sécurité, page 16 et Génération d'une signature de tâche de sécurité, page 106.

Figure 10 – Onglet Date/Time



Pour des informations complémentaires sur la synchronisation temporelle, reportez-vous à la publication IA-AT003, « Integrated Architecture™ and CIP Sync Configuration Application Solution ».

Configuration d'un automate de sécurité homologue

Vous pouvez ajouter un automate de sécurité homologue au dossier de configuration des E/S de votre projet de sécurité pour autoriser la consommation de points standard ou de sécurité. Le partage de données de sécurité entre automates homologues consiste à produire et à consommer des points de sécurité à accès automate.

Pour des détails sur la configuration des automates de sécurité homologues, la production et la consommation des points de sécurité, voir Points de sécurité produits/consommés, page 97.

Communications en réseaux

Réseau de sécurité

Le protocole CIP Safety est un protocole de communication entre stations terminales d'un réseau, dédié à la sécurité. Il permet l'échange de messages de sécurité entre des périphériques CIP Safety par l'intermédiaire de passerelles, switchs et routeurs.

Pour garantir un niveau d'intégrité maximum durant l'acheminement des messages à travers les passerelles, switchs ou routeurs standard, chaque station terminale appartenant à un système de commande CIP Safety routable doit être référencée de façon unique. Cette référence unique regroupe un numéro de réseau de sécurité (SNN) et l'adresse du dispositif sur le réseau.

Gestion du numéro de réseau de sécurité (SNN)

Le numéro SNN affecté aux périphériques de sécurité situés sur un même segment de réseau doit être unique. Vous devez vous assurer qu'un numéro SNN unique est attribué à :

- chaque réseau de type CIP Safety contenant des dispositifs de sécurité ;
- chaque châssis contenant un ou plusieurs automates GuardLogix.

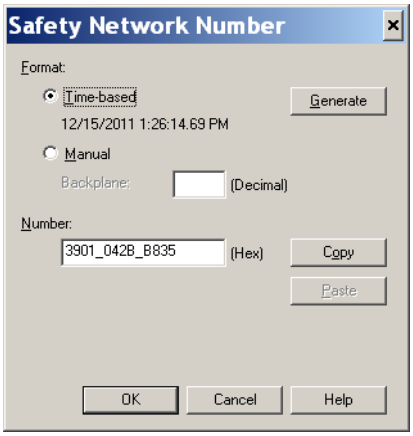
CONSEIL Plusieurs numéros SNN peuvent être attribués à un sous-réseau CIP Safety ou à un châssis ControlBus contenant plusieurs dispositifs de sécurité. **Cependant, pour plus de simplicité, nous recommandons l'attribution d'un numéro SNN unique à chaque sous-réseau CIP Safety.**

Le numéro SNN peut être attribué par le logiciel (chronologiquement) ou par l'utilisateur (manuellement). Ces deux formats de numéro SNN sont décrits à la suite.

Numéro de réseau de sécurité chronologique

Si le format chronologique est sélectionné, la valeur du numéro SNN généré correspond à la date et à l'heure de sa création. Celles-ci sont déterminées par l'ordinateur qui exécute le logiciel de configuration.

Figure 11 – Format chronologique



Numéro de réseau de sécurité manuel

Si le format manuel est sélectionné, le numéro SNN doit être constitué d'une valeur décimale comprise entre 1 et 9999 saisie manuellement.

Figure 12 – Saisie manuelle

Attribution du numéro de réseau de sécurité (SNN)

Vous pouvez laisser le logiciel RSLogix 5000 attribuer automatiquement un numéro SNN ou l'attribuer vous-même manuellement.

Attribution automatique

Quand un nouvel automate ou un nouveau module est crée, un numéro SNN chronologique est automatiquement attribué par le logiciel de configuration. Les nouveaux modules de sécurité ajoutés par la suite au même réseau CIP Safety seront affectés du même numéro SNN que celui correspondant à l'adresse la plus basse de ce réseau.

Attribution manuelle

L'option manuelle est destinée aux systèmes CIP Safety routables n'ayant qu'un petit nombre de sous-réseaux et de réseaux interconnectés. Il permet aux utilisateurs qui le souhaitent de gérer et attribuer un numéro SNN selon une méthode logique propre à leur application.

Voir Modification du numéro de réseau de sécurité (SNN), page 55.

IMPORTANT	Si vous attribuez manuellement un numéro SNN, assurez-vous que l'extension du système n'entraîne pas de doublons dans les combinaisons SNN/adresse de station déjà enregistrées.

Choix de l'attribution automatique ou manuelle

Pour la plupart des utilisateurs, l'attribution automatique d'un numéro SNN sera suffisante. Toutefois, une définition manuelle du SNN est nécessaire si :

- vous utilisez des points de sécurité consommés ;
- le projet consomme des données d'entrée de sécurité produites par un module dont la configuration est gérée par un autre équipement ;
- vous copiez un projet de sécurité dans une installation matérielle différente au sein du même système CIP Safety routable.

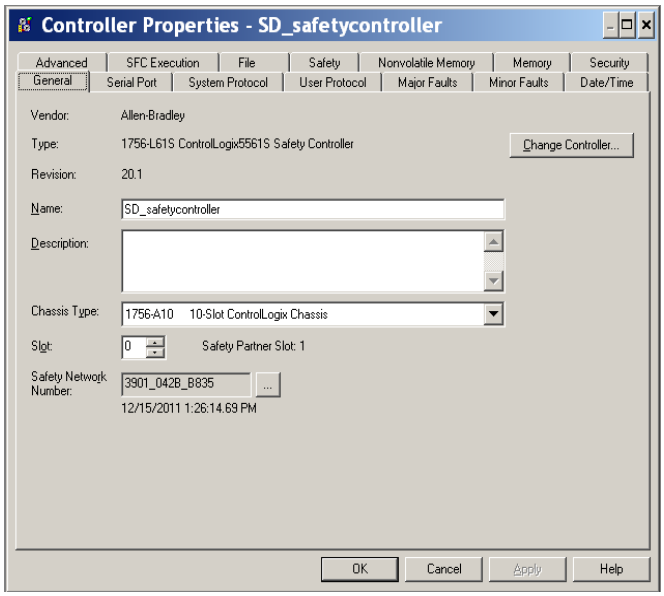
Modification du numéro de réseau de sécurité (SNN)

Avant de modifier le SNN vous devez :

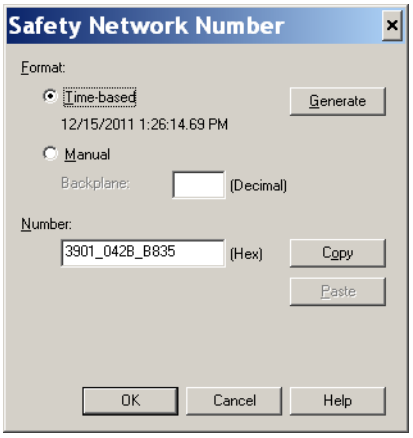
- déverrouiller le projet, si la sécurité est verrouillée (voir Verrouillage de sécurité de l'automate, page 105) ;
- supprimer la signature de tâche de sécurité s'il en existe une (voir Supprimer la signature de tâche de sécurité, page 108).

Modification du numéro de réseau de sécurité (SNN) de l'automate

1. Dans l'arborescence de l'automate, cliquez sur l'automate concerné avec le bouton droit de la souris et sélectionnez « Properties » (Propriétés).
2. Dans l'onglet General (Général) de la boîte de dialogue des propriétés de l'automate, cliquez sur le bouton ... situé à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro SNN).



3. Sélectionnez « Time-based » (Chronologique) et cliquez sur « Generate » (Générer).



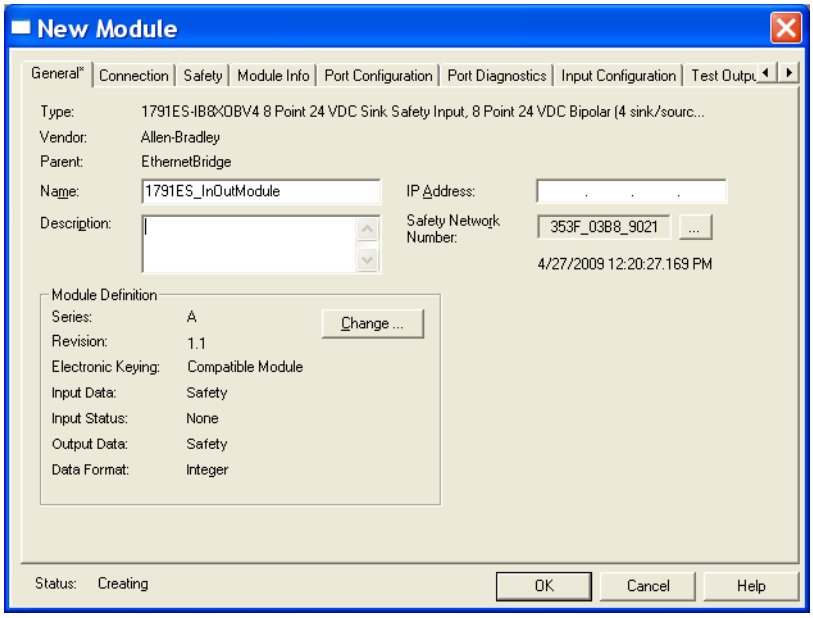
4. Cliquez sur OK.

Modification du numéro SNN des modules d'E/S de sécurité sur un réseau CIP Safety

Cet exemple est basé sur un réseau EtherNet/IP.

1. Trouvez le premier module de communication EtherNet/IP dans l'arborescence de configuration des E/S.

2. Développez la liste des modules d'E/S de sécurité disponibles via ce module de communication EtherNet/IP.
3. Cliquez deux fois sur le premier module d'E/S de sécurité pour afficher l'onglet General (Général).

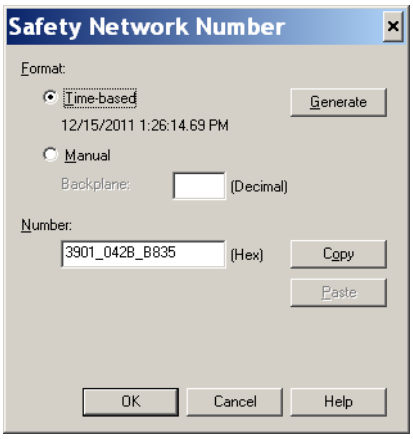


4. Cliquez sur le bouton ... situé à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro SNN).
5. Sélectionnez « Time-based » (Chronologique) et cliquez sur « Generate » (Générer) pour générer un nouveau numéro SNN pour ce réseau EtherNet/IP.
6. Cliquez sur OK.
7. Cliquez sur Copy (Copier) pour copier le nouveau numéro SNN dans le presse-papiers de Windows.
8. Ouvrez l'onglet General (Général) de la boîte de dialogue des propriétés du module pour le module d'E/S de sécurité suivant dans la liste du module EtherNet/IP.
9. Cliquez sur le bouton ... situé à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro SNN).
10. Sélectionnez Time-based (chronologique) et cliquez sur Paste (Coller) pour coller le numéro SNN du réseau EtherNet/IP dans les propriétés de cet équipement.
11. Cliquez sur OK.
12. Répétez les étapes 8 à 10 pour les autres modules d'E/S de sécurité figurant dans la liste du module de communication EtherNet/IP.
13. Répétez les étapes 2 à 10 pour tous les modules de communication en réseau présents dans l'arborescence de configuration des E/S.

Copier-coller un numéro SNN

Si la configuration du module est la propriété d'un autre automate, vous devrez copier le numéro SNN du propriétaire de cette configuration et le coller dans le module apparaissant dans votre arborescence de configuration d'E/S.

1. Dans l'utilitaire de configuration logicielle du propriétaire de la configuration du module, ouvrez la boîte de dialogue Safety Network Number (Numéro SNN).



2. Cliquez sur Copy (Copier).
3. Ouvrez l'onglet General (Général) de la boîte de dialogue des propriétés du module d'E/S figurant dans l'arborescence de configuration des E/S du projet de l'automate consommateur.
   Cet automate consommateur n'est pas le propriétaire de la configuration.
4. Cliquez sur le bouton ... situé à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro SNN).
5. Cliquez sur Paste (Coller).
6. Cliquez sur OK.

Communications EtherNet/IP

Pour les communications réseau EtherNet/IP dans un système GuardLogix, vous avez le choix entre plusieurs modules.Pour les communications CIP Safety, y compris la commande de modules d'E/S de sécurité, choisissez l'un des modules répertoriés dans le Tableau 12, à l'exception du module 1756-EWEB qui ne prend pas en charge les communications CIP Safety.

Le Tableau 12 répertorie les modules et leurs fonctionnalités principales.

Tableau 12 – Modules de communication EtherNet/IP et fonctionnalités

Module	Fonctionnalités
1756-ENBT	• Connecte des automates à des modules d'E/S (nécessite un adaptateur pour les E/S distribuées). • Communique avec d'autres dispositifs EtherNet/IP (messagerie). • Sert de chemin d'accès pour le partage de données entre automates Logix5000 (production/consommation). • Relie des stations EtherNet/IP pour le routage de messages à des périphériques sur d'autres réseaux.
1756-EN2T	• Mêmes fonctions qu'un module 1756-ENBT, mais avec deux fois plus de capacité pour des applications plus exigeantes. • Fourniture d'une connexion temporaire de configuration par l'intermédiaire du port USB. • Configuration rapide d'adresses IP grâce à l'utilisation de sélecteurs rotatifs.
1756-EN2F	• Mêmes fonctions qu'un module 1756-EN2T. • Raccordement d'une liaison fibre au module au moyen d'un connecteur LC pour fibre optique.
1756-EN2TXT	• Mêmes fonctions qu'un module 1756-EN2T. • Fonctionnement dans des environnements extrêmes présentant des températures de –25 à 70 °C.
1756-EN2TR	• Mêmes fonctions qu'un module 1756-EN2T. • Prise en charge des communications en topologie d'anneau pour un réseau DLR (Device Level Ring/anneau de niveau dispositif) à tolérance de défaut unique.
1756-EN3TR	• Mêmes fonctions que le module 1756-EN2TR. • Trois ports pour connexion DLR.
1756-EWEB	• Utilisation de pages Internet personnalisables pour un accès externe aux informations de l'automate. • Fournit un accès à distance aux points d'un automate ControlLogix local par l'intermédiaire d'un navigateur Internet. • Communique avec d'autres dispositifs EtherNet/IP (messagerie). • Relie des stations EtherNet/IP pour le routage de messages à des périphériques sur d'autres réseaux. • Prise en charge de périphériques Ethernet qui ne sont pas de type EtherNet/IP au moyen d'un connecteur logiciel d'interface. Ce module ne permet pas la gestion des E/S ni des points produits/consommés et ne prend pas en charge la communication CIP Safety.

Les modules de communication EtherNet/IP offrent les fonctionnalités suivantes :

- gestion de la messagerie, des points produits/consommés, des IHM et des E/S distribuées ;
- gestion des messages encapsulés selon un protocole TCP/UDP/IP standard ;
- couche application commune avec les réseaux ControlNet et DeviceNet ;
- communiquent via un câble à paire torsadée non blindé de catégorie 5 à connecteur RJ45 ;
- prise en charge des communications en duplex intégral et semi-duplex à 10 ou 100 Mbits/s ;
- fonctionne avec des switchs standard ;
- ne requièrent pas de planification du réseau ;
- pas de tables de routage nécessaires.

Les logiciels suivants sont disponibles pour les réseaux EtherNet/IP.

Tableau 13 – Logiciels pour la gestion des modules EtherNet/IP

Logiciel	Fonction	Requis
Logiciel de programmation RSLogix 5000	Ce logiciel est nécessaire pour configurer le projet de l'automate et pour définir les communications EtherNet/IP.	Oui
Utilitaire BOOTP/DHCP	Cet utilitaire est fourni avec le logiciel RSLogix 5000. Vous pouvez l'utiliser pour assigner des adresses IP aux dispositifs d'un réseau EtherNet/IP.	Non
Logiciel RSNetWorx™ for EtherNet/IP	Vous pouvez utiliser les logiciels suivants pour configurer l'adresse IP et/ou le nom d'hôte de périphériques EtherNet/IP.	Non
Logiciel RSLinx	Vous pouvez utiliser ce logiciel pour configurer des périphériques, établir une communication entre ces périphériques et réaliser des diagnostics.	Oui

Production et consommation de données via un réseau EtherNet/IP

L'automate prend en charge la production (émission) et la consommation (réception) de points sur un réseau Ethernet/IP. Chaque point produit et consommé requiert des connexions. Le nombre total de points pouvant être produit et consommé est limité par le nombre de connexions disponibles.

Connexions sur le réseau EtherNet/IP

Vous déterminez indirectement le nombre des connexions utilisées par l'automate de sécurité lorsque vous le configurez pour communiquer avec d'autres équipements du système. Les connexions sont des allocations de ressources qui apportent des communications plus fiables entre les équipements que le principe des messages sans connexion (instructions de message).

Les connexions EtherNet/IP sont non prioritaires. Une connexion non prioritaire pour la commande d'E/S est déterminée par l'intervalle RPI ou par le programme (par le biais d'une instruction MSG, par exemple). Le système de messagerie non prioritaire vous permet d'envoyer ou recevoir des données selon les besoins.

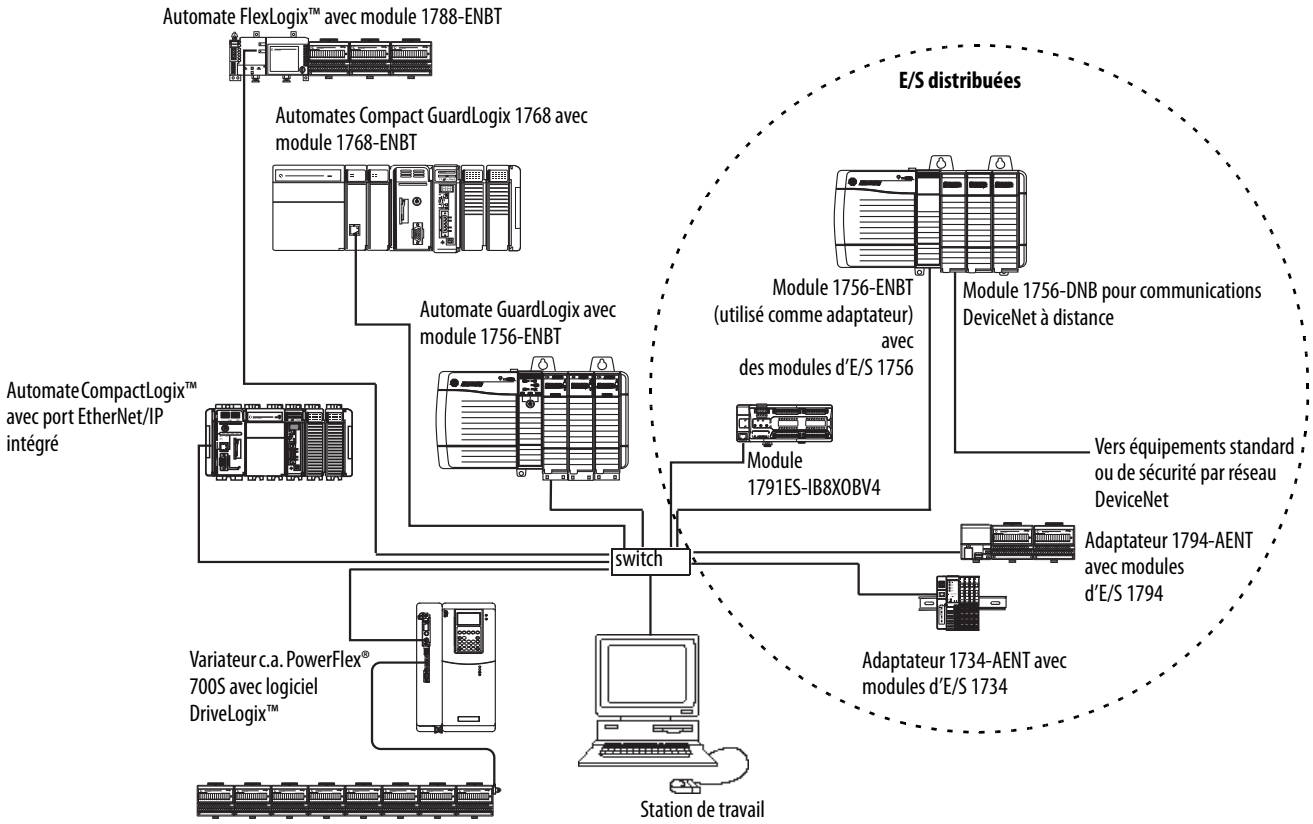
Les modules de communication EtherNet/IP peuvent gérer jusqu'à 128 connexions CIP (Common Industrial Protocol) sur un réseau EtherNet/IP.

Exemple de communications EtherNet/IP

Cet exemple démontre ce qui suit :

- les automates peuvent produire et consommer des points standard ou de sécurité entre eux ;
- les automates peuvent générer des instructions MSG pour échanger des données standard ou configurer des équipements ;(1)
- le module de communication EtherNet/IP est utilisé comme passerelle, ce qui permet à l'automate de sécurité de produire et de consommer des données standard et de sécurité ;
- le PC peut transférer et télécharger des projets dans les automates ;
- le PC peut configurer les dispositifs du réseau EtherNet/IP.

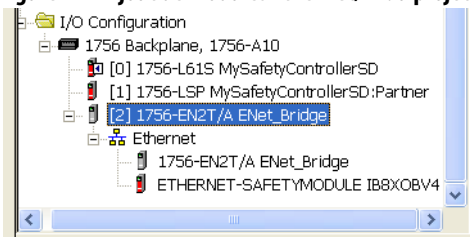
Figure 13 – Exemple de communications EtherNet/IP



Connexions EtherNet/IP pour modules d'E/S CIP Safety

Les modules d'E/S CIP Safety en réseaux EtherNet/IP sont ajoutés au projet sous le module de communication EtherNet/IP, comme décrit au Chapitre 5, Ajout, configuration, surveillance et remplacement d'E/S de sécurité CIP Safety. Lorsque vous ajoutez un module d'E/S CIP Safety, le logiciel RSLogix 5000 crée automatiquement les points de données de sécurité à accès automate pour ce module.

Figure 14 – Ajout de modules EtherNet/IP au projet



Connexions EtherNet/IP standard

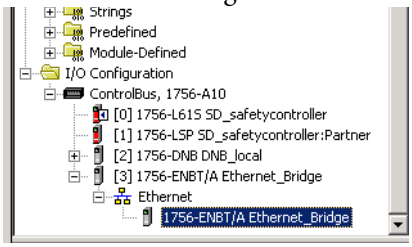
Pour utiliser un module EtherNet/IP standard avec l'automate de sécurité, ajoutez ce module au projet de l'automate de sécurité et téléchargez le projet dans l'automate GuardLogix.

(1) Les automates GuardLogix ne prennent pas en charge les instructions MSG pour les données de sécurité.

1. Pour configurer le module, vous devez définir l'adresse IP, le masque de sous-réseau et la passerelle.

Paramètre EtherNet/IP	Description
Adresse IP	L'adresse IP identifie le module de manière unique. L'adresse IP est au format *xxx.xxx.xxx.xxx.*, où chaque groupe de xxx est un nombre entre 0 et 255. Cependant, vous ne pouvez pas utiliser certaines valeurs dans le premier octet de l'adresse : • 000.*xxx.xxx.xxx* • 127.*xxx.xxx.xxx* • 223 à 255.*xxx.xxx.xxx*
Masque de sous-réseau	L'adressage de sous-réseau est une extension du système d'adresse IP. Il permet à un site d'utiliser un seul identifiant réseau pour plusieurs réseaux physiquement différents. L'acheminement hors du site se fait en subdivisant l'adresse IP en un identifiant réseau et un identifiant hôte en fonction de la classe. A l'intérieur du site, le masque de sous-réseau sert à rediviser l'adresse entre les parties identifiant réseau et identifiant hôte prédéfinies. Ce champ est réglé par défaut sur 0.0.0.0. Si vous modifiez le masque de sous-réseau d'un module déjà configuré, vous devrez redémarrer le module pour que les modifications soient prises en compte.
Passerelle	Une passerelle relie des réseaux physiquement différents en un même système. Lorsqu'une station d'un réseau doit communiquer avec une station d'un autre réseau, une passerelle transfère les données entre les deux réseaux. Ce champ est réglé par défaut sur 0.0.0.0.

2. Après avoir installé physiquement un module EtherNet/IP et défini son adresse IP, ajoutez ce module dans la fenêtre d'organisation de votre projet d'automate GuardLogix.



3. Utilisez le logiciel RSLogix 5000 pour charger le projet.

Communications ControlNet

Pour les communications ControlNet standard, choisissez un module 1756-CNB ou 1756-CNBR ou un module 1756-CN2, 1756CN2R ou 1756CN2RXT pour les communications de sécurité.

Tableau 14 – Modules ControlNet

Si votre application…	Choisissez la référence…
• commande des modules d'E/S standard ; • requiert un adaptateur pour des E/S distribuées sur un réseau ControlNet ; • communique avec d'autres dispositifs ControlNet (par messages) ; • partage (produit et consomme) des données standard avec d'autres automates Logix5000 ; • ponte des liaisons ControlNet pour acheminer des messages vers des équipements situés sur d'autres réseaux.	1756-CNB
• exécute les mêmes fonctions qu'un module 1756-CNB ; • doit en plus prendre en charge des systèmes ControlNet redondants.	1756-CNBR
• exécute les mêmes fonctions prises en charge par le module 1756-CNB avec de meilleures performances ; • prend en charge des communications CIP Safety.	1756-CN2
• exécute les mêmes fonctions qu'un module 1756-CN2 ; • doit en plus prendre en charge des systèmes ControlNet redondants.	1756-CN2R
• exécute les mêmes fonctions qu'un module 1756-CN2R ; • fonctionne dans des environnements extrêmes présentant des températures de –25 à 70 °C.	1756-CN2RXT

Ces logiciels sont disponibles pour les réseaux ControlNet.

Tableau 15 – Logiciels pour la gestion des modules ControlNet

Logiciel	Fonction	Requis
Logiciel de programmation RSLogix 5000	Ce logiciel est nécessaire pour configurer le projet GuardLogix et pour définir les communications ControlNet.	Oui
Logiciel RSNetWorx for ControlNet	Ce logiciel est nécessaire pour configurer le réseau ControlNet, définir le temps de rafraîchissement du réseau (Network Update Time/NUT) et pour planifier le réseau ControlNet.	Oui
Logiciel RSLinx	Vous pouvez utiliser ce logiciel pour configurer des périphériques, établir une communication entre ces périphériques et réaliser des diagnostics.	Oui

Les modules de communication ControlNet procurent ce qui suit :

- prennent en charge la messagerie, les points produits/consommés de sécurité et standard et les E/S distribuées ;
- acceptent l'utilisation de répéteurs coaxiaux ou à fibre optique pour garantir l'isolement et permettre des distances de transmission plus longues.

Production et consommation de données via un réseau ControlNet

L'automate GuardLogix prend en charge la production (émission) et la consommation (réception) de points sur les réseaux ControlNet. Le nombre total de points pouvant être produits et consommés est limité par le nombre de connexions disponibles dans l'automate GuardLogix.

Connexions sur un réseau ControlNet

Le nombre de connexions que l'automate utilise est déterminé par la façon dont vous configurez l'automate pour qu'il communique avec d'autres dispositifs dans le système. Les connexions sont des allocations de ressources qui fournissent des communications plus fiables entre les dispositifs que des messages sans connexion.

Les connexions ControlNet peuvent être prioritaires ou non.

Tableau 16 – Connexions ControlNet

Type de connexion	Description
Prioritaire (spécifique au réseau ControlNet)	Une connexion prioritaire est propre aux communications ControlNet. Une connexion prioritaire permet d'envoyer et de recevoir des données de façon répétée selon un intervalle prédéfini correspondant à la valeur du RPI. Par exemple, une connexion à un module d'E/S est une connexion prioritaire parce que vous recevez des données d'un module de façon répétée à intervalle défini. Autres connexions prioritaires : • avec les dispositifs de communication ; • de transmission des points produits/consommés. Pour un réseau ControlNet, vous devez utiliser le logiciel RSNetWorx for ControlNet pour activer les connexions prioritaires et définir un temps de rafraîchissement du réseau (NUT). L'établissement d'une connexion prioritaire réserve une partie de la bande passante du réseau pour le traitement spécifique de cette connexion.
Non prioritaire	Une connexion non prioritaire consiste en un transfert de message entre automates qui est déclenché par l'intervalle entre trames requis (RPI) ou par le programme (au moyen d'une instruction MSG). Le système de messagerie non prioritaire vous permet d'envoyer ou recevoir des données selon les besoins. Les connexions non prioritaires utilisent le restant de la bande passante du réseau, lorsque la partie réservée aux connexions prioritaires a été allouée. Les connexions de sécurité produites/consommées sont non prioritaires.

Les modules de communication 1756-CNB et 1756-CNBR prennent en charge jusqu'à 64 connexions CIP sur un réseau ControlNet. Toutefois, nous vous conseillons de ne pas configurer plus de 48 connexions pour maintenir des performances optimales.

Le module 1756-CN2 prend en charge jusqu'à 128 connexions CIP sur un réseau ControlNet.

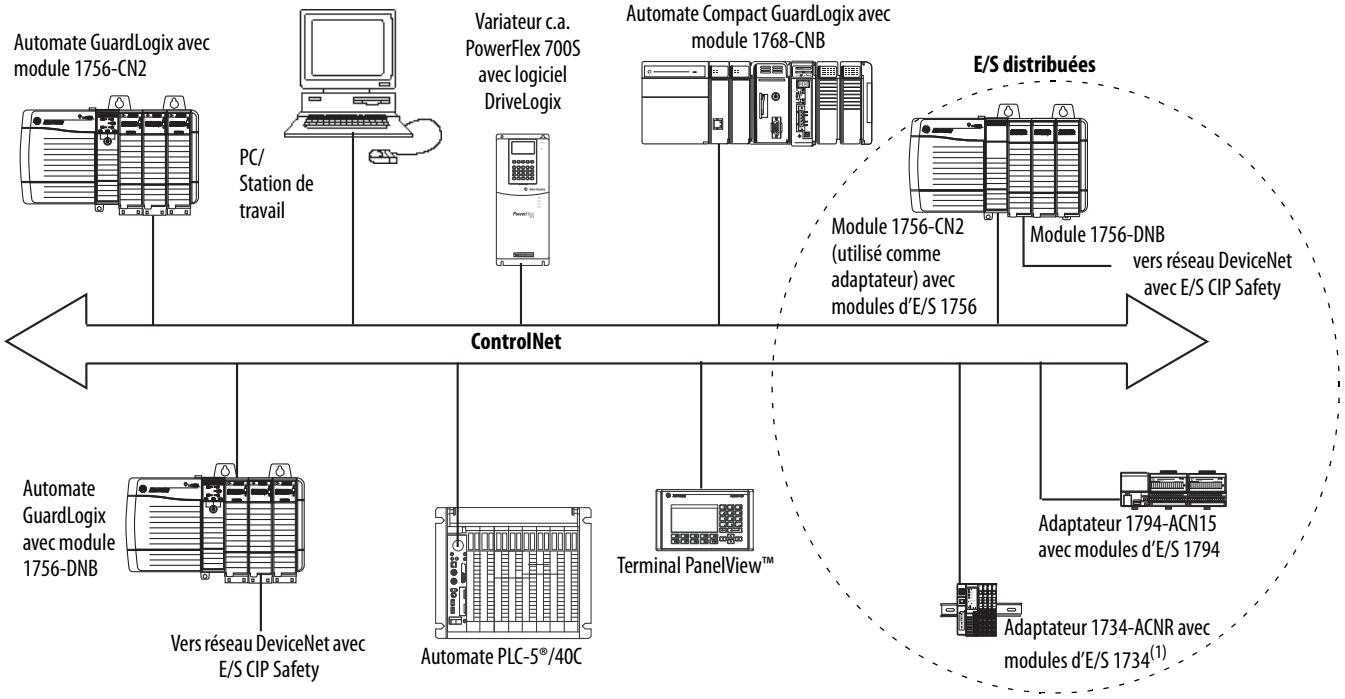
Exemple de communication ControlNet

Cet exemple démontre ce qui suit :

- les automates GuardLogix peuvent produire et consommer des points standard ou de sécurité entre eux ;
- les automates GuardLogix peuvent déclencher des instructions MSG pour échanger des données standard ou configurer des équipements ;(1)
- Le module 1756-CN2 peut être utilisé comme passerelle, pour permettre à l'automate GuardLogix de produire et de consommer des données standard et de sécurité vers et depuis des dispositifs d'E/S.
- le PC peut transférer et télécharger des projets dans les automates ;
- le PC peut configurer les dispositifs présents sur le réseau ControlNet et le réseau lui-même également.

(1) Les automates GuardLogix ne prennent pas en charge les instructions MSG pour les données de sécurité.

Figure 15 – Exemple de communication ControlNet



(1) L'adaptateur 1734-ACN ne prend pas en charge les modules d'E/S de sécurité POINT Guard.

Connexions ControlNet pour les E/S distribuées

Pour communiquer avec des modules d'E/S distribuées en réseau ControlNet, ajoutez une passerelle ControlNet, un adaptateur ControlNet et des modules d'E/S dans le dossier « I/O Configuration » (Configuration des E/S) de l'automate.

Communications DeviceNet

Pour communiquer et échanger des données avec des modules d'E/S CIP Safety sur des réseaux DeviceNet, vous avez besoin d'un module 1756-DNB dans le châssis local.

Pour de plus amples informations sur l'installation de votre module 1756-DNB, reportez-vous à la publication 1756-IN566, « ControlLogix DeviceNet Scanner Module Installation Instructions ».

Le module 1756-DNB accepte les communications avec des périphériques DeviceNet de sécurité aussi bien que standard. Vous pouvez donc utiliser ces deux types de périphériques.

Les produits logiciels suivants peuvent être utilisés avec les réseaux DeviceNet et le module 1756-DNB.

Tableau 17 – Logiciels utilisables avec les réseaux DeviceNet

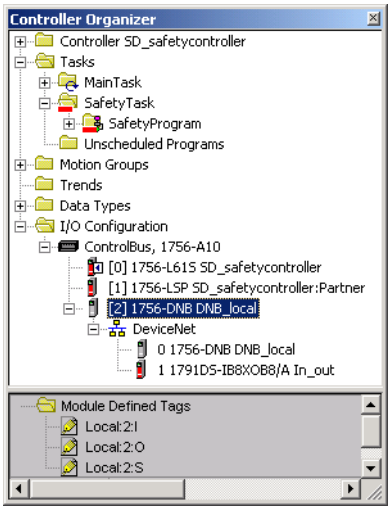
Logiciel	Est utilisé pour…	Nécessaire/Facultatif
RSLogix 5000	• Configurer des projets ControlLogix. • Définir une communication DeviceNet.	Nécessaire
RSNetWorx™ for DeviceNet	• Configurer des dispositifs DeviceNet. • Définir une liste de scrutation pour ces dispositifs.	
RSLinx Classic ou RSLinx Enterprise	• Configurer des dispositifs de communication. • Effectuer des diagnostics. • Établir la communication entre les périphériques.	

Connexions DeviceNet pour modules d'E/S CIP Safety

Pour accéder aux dispositifs CIP Safety en réseau DeviceNet, ajoutez un module 1756-DNB à l'arborescence de configuration des E/S du projet de l'automate GuardLogix.

Les modules d'E/S CIP Safety pour réseaux DeviceNet sont ajoutés au projet sous le module 1756-DNB, comme indiqué au Chapitre 5, Ajout, configuration, surveillance et remplacement d'E/S de sécurité CIP Safety. Lorsque vous ajoutez un module d'E/S CIP Safety, le logiciel RSLogix 5000 crée automatiquement les points de données de sécurité à accès automate pour ce module.

Figure 16 – Module DeviceNet de l'automate dans l'arborescence de configuration des E/S



Connexions DeviceNet standard

Si vous utilisez des E/S DeviceNet standard avec votre automate GuardLogix, vous devrez allouer deux connexions pour chaque module 1756-DNB. Une connexion sera réservée à la configuration et aux informations d'état du module. L'autre sera une connexion native pour rack pour les données d'E/S DeviceNet.

Pour utiliser le module 1756-DNB afin d'accéder aux données standard via le réseau DeviceNet, vous avez besoin du logiciel RSNetWorx for DeviceNet pour :

- créer un fichier de configuration du réseau ;
- configurer chaque dispositif standard du réseau ;
- configurer le module 1756-DNB ;
- ajouter des dispositifs d'E/S standard à la liste de scrutation du module 1756-DNB.

Lorsque vous ajoutez un module 1756-DNB à la configuration des E/S de l'automate, le logiciel RSLogix 5000 crée automatiquement un jeu de points standard pour les données d'entrée, de sortie et d'état du réseau.

Communications série

Pour utiliser l'automate GuardLogix sur un réseau série, il vous faut :

- une station de travail dotée d'un port série ;
- le logiciel RSLinx pour configurer le driver de communication série ;
- le logiciel RSLogix 5000 pour configurer le port série de l'automate.

Pour que l'automate puisse communiquer par le réseau série avec une station de travail ou tout autre matériel, vous devez :

1. Configurer le driver de communication série pour la station de travail.
2. Configurer le port série de l'automate.

Tableau 18 – Modes de communication série

Utilisez ce mode…	Pour…
DF1 point à point	Communiquer entre l'automate et un autre équipement compatible avec le protocole DF1. Il s'agit du mode système par défaut. Il est généralement utilisé pour la programmation de l'automate via son port série.
DF1 maître	Commander l'appel et la transmission de messages entre des stations maître et esclave. Les communications en mode maître/esclave mettent en œuvre un automate configuré comme station maître et jusqu'à 254 stations esclaves. Reliez les stations esclaves en utilisant des modems ou des amplificateurs de ligne. Dans un tel réseau, les stations auront un numéro compris entre 0 et 254. Chaque station devra par ailleurs avoir une adresse unique. En outre, il faut qu'il y ait au moins 2 stations (1 maître et 1 esclave) pour définir une liaison comme étant un réseau .
DF1 esclave	Utiliser un automate comme station esclave dans un réseau de communication série de type maître/esclave. Lorsque le réseau comporte plusieurs stations esclaves, reliez-les à la station maître à l'aide de modems ou d'amplificateurs de ligne. Lorsque le réseau ne comporte qu'une seule station esclave, vous n'avez pas besoin de modem pour connecter cette station esclave à la station maître. Vous pouvez configurer les paramètres de commande sans établissement de liaison. Vous pouvez connecter de 2 à 255 stations sur une même liaison. En mode DF1 esclave, l'automate utilise le protocole DF1 half-duplex. Une station est assignée comme maître et commande l'accès à la liaison. Toutes les autres stations sont des stations esclaves. Elles doivent attendre l'autorisation du maître avant de transmettre.
DH-485	Communiquer avec un autre réseau à passage de jeton multimaître comportant des équipements DH-485, et permettre la programmation et la messagerie d'égal à égal.

Informations connexes

Ressource	Description
« EtherNet/IP Modules in Logix5000 Control Systems User Manual », Publication ENET-UM001	Comporte des informations détaillées sur la configuration et l'utilisation de modules de communication EtherNet/IP dans un système de commande Logix5000
« ControlNet Modules in Logix5000 Control Systems User Manual », Publication CNET-UM001	Comporte des informations détaillées sur la configuration et l'utilisation de modules de communication ControlNet dans un système de commande Logix5000
« DeviceNet Modules in Logix5000 Control Systems User Manual », Publication DNET-UM004	Informations détaillées sur la configuration et l'utilisation des modules 1756-DNB dans un système de commande Logix5000

Ajout, configuration, surveillance et remplacement d'E/S de sécurité CIP Safety

Pour de plus amples informations sur l'installation, la configuration et le fonctionnement des modules d'E/S CIP Safety, veuillez vous reporter aux publications suivantes :

- « Guard I/O DeviceNet Safety Modules User Manual », Publication 1791DS-UM001
- « Guard I/O EtherNet/IP Safety Modules User Manual », Publication 1791ES-UM001
- « Modules de sécurité POINT Guard I/O Notice d'installation et manuel utilisateur », Publication 1734-UM013
- Aide en ligne du logiciel RSLogix 5000

Ajout de modules d'E/S CIP Safety

Lorsque vous ajoutez un module au système, vous devez définir la configuration de ce module, notamment :

- L'adresse de station pour les réseaux DeviceNet

  Vous ne pouvez pas utiliser le logiciel RSLogix 5000 pour définir l'adresse de station d'un module d'E/S CIP Safety sur les réseaux DeviceNet. Les adresses de station des modules sont définies par les sélecteurs rotatifs des modules.

- L'adresse IP pour les réseaux EtherNet/IP

  Pour définir l'adresse IP, vous pouvez utiliser les sélecteurs rotatifs du module, le logiciel DHCP disponible auprès de Rockwell Automation ou récupérer l'adresse par défaut enregistrée en mémoire non volatile.

- Le numéro de réseau de sécurité (SNN)

  Pour de plus amples informations sur la configuration du numéro SNN, voir page 71.

- La signature de configuration

  Voir page 75 pour vérifier dans quels cas la signature de configuration est définie automatiquement ou doit l'être manuellement.

- La limite de temps de réponse

  Pour de plus amples informations sur la configuration de la limite de temps de réponse, voir page 71.

- Les paramètres d'entrées/sorties et de test de sécurité

Vous pouvez configurer les modules d'E/S CIP Safety via l'automate GuardLogix, à l'aide du logiciel RSLogix 5000.

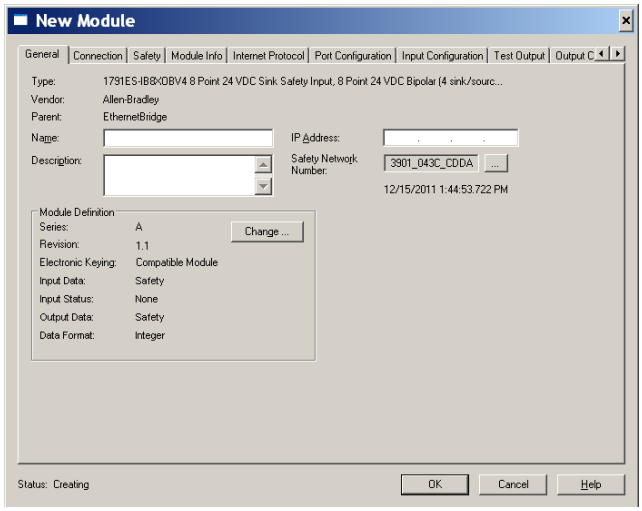
CONSEIL Les modules d'E/S acceptent des données standard et de sécurité. La configuration du module définit les types de données disponibles.

Configuration de modules d'E/S CIP Safety via le logiciel RSLogix 5000

Ajoutez le module d'E/S de sécurité CIP Safety au module de communication dans le dossier de configuration des E/S (I/O Configuration) du projet RSLogix 5000.

CONSEIL Vous ne pouvez ni ajouter ni supprimer un module d'E/S CIP Safety lorsque vous êtes en ligne.

1. Cliquez sur le réseau approprié avec le bouton droit de la souris et sélectionnez New Module (Nouveau module).
2. Développez la catégorie Safety (Sécurité) et choisissez un module d'E/S CIP Safety.
3. Précisez les propriétés du module.



   a. S'il y a lieu, modifiez les paramètres du module en cliquant sur le bouton Change (Modifier).

   b. Entrez un nom pour le nouveau module.

   c. Entrez l'adresse de station ou l'adresse IP de ce module selon le réseau auquel il est connecté.

      Seuls les numéros de station non utilisés apparaissent dans le menu déroulant.

d. Si nécessaire, modifiez le numéro SNN en cliquant sur le bouton ....

   Pour de plus amples informations, voir page 71.

e. Définissez les paramètres de configuration du module dans les onglets Input Configuration (Configuration des entrées), Test Output (Sorties de test) et Output Configuration (Configuration des sorties).

   Pour de plus amples informations sur la configuration des modules d'E/S CIP Safety, reportez-vous à l'aide en ligne de RSLogix 5000.

f. Définissez la limite de temps de réponse de la connexion à l'aide de l'onglet Safety (Sécurité).

   Pour de plus amples informations, voir page 71.

Configuration du numéro de réseau de sécurité (SNN)

L'attribution d'un numéro SNN chronologique est automatique lorsque vous ajoutez un nouveau module d'E/S de sécurité. Les modules de sécurité ajoutés par la suite au même réseau CIP Safety recevront le même numéro SNN que l'adresse la plus basse de ce réseau.

Un numéro SNN chronologique créé automatiquement est suffisant dans la plupart des applications. Il s'avère cependant parfois nécessaire de le modifier.

Voir Attribution du numéro de réseau de sécurité (SNN), page 55.

Utilisation des connexions d'envoi individuel sur les réseaux EtherNet/IP

Dans le logiciel RSLogix 5000 à partir de la version 20, vous pouvez configurer les modules d'E/S EtherNet/IP pour utiliser des connexions d'envoi individuel. Les connexions d'envoi individuel sont des connexions point à point entre une station source et une station de destination. Pour ce type de connexion vous n'avez par besoin de saisir une plage minimum ou maximum de RPI ou une valeur par défaut.

Pour configurer des connexions d'envoi individuel, choisissez l'onglet Connection et cochez Use Unicast Connection over Ethernet/IP (Utiliser la connexion d'envoi individuel sur EtherNet/IP).

Définir la limite de temps de réponse de la connexion

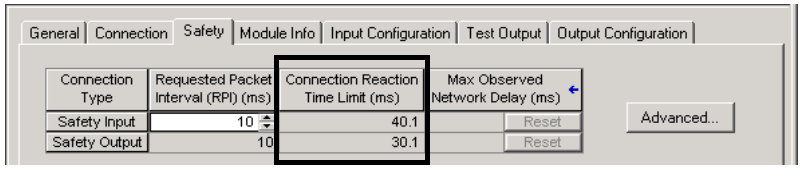
La limite de temps de réponse d'une connexion correspond à la rémanence maximale des paquets de sécurité sur la connexion en question. Si l'âge des données utilisées par l'équipement consommateur dépasse la limite de temps de réponse de la connexion, une erreur de connexion se produit. La limite de temps de réponse de la connexion se calcule à l'aide des équations suivantes :

Limite de temps de réponse de la connexion en entrée =
RPI des entrées x [Multiplicateur de timeout + Multiplicateur de délai du réseau]

Limite de temps de réponse de la connexion en sortie =
Fréquence de la tâche de sécurité x [Multiplicateur de timeout + Multiplicateur de délai du réseau – 1]

La limite de temps de réponse de la connexion apparaît dans l'onglet Safety (Sécurité) de la boîte de dialogue Module Properties (Propriétés du module).

Figure 17 – Limite de temps de réponse de la connexion



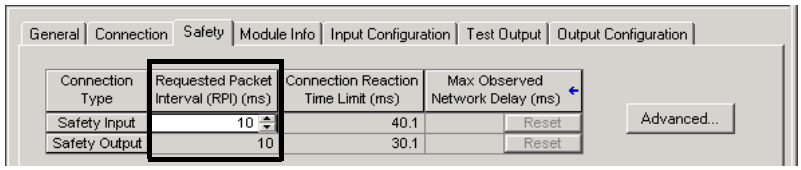
Définir l'intervalle entre trames requis (RPI)

L'intervalle RPI indique la fréquence de rafraîchissement des données sur une connexion. Par exemple, un module d'entrée produira des données selon la valeur RPI que vous lui aurez assignée.

Pour les connexions d'entrées de sécurité, vous pouvez définir l'intervalle RPI dans l'onglet Safety (Sécurité) de la boîte de dialogue Module Properties (Propriétés du module). L'intervalle RPI est défini par incréments de 1 ms dans une plage de 1 à 100 ms. La valeur RPI par défaut est de 10 ms.

La limite de temps de réponse de la connexion se trouve immédiatement ajustée en cas de modification de l'intervalle RPI par le logiciel RSLogix 5000.

Figure 18 – Intervalle entre trames requis



Pour les connexions de sorties de sécurité, le RPI est égal à la fréquence de la tâche de sécurité. Si la valeur limite du temps de réponse de la connexion correspondante n'est pas satisfaisante, vous pouvez ajuster la fréquence de connexion dans la boîte de dialogue Safety Task Properties (Propriétés de la tâche de sécurité).

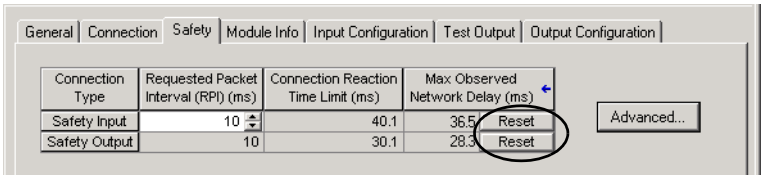
Pour de plus amples informations sur la période de la tâche de sécurité, voir Spécification de la période de la tâche de sécurité, page 90.

Pour les applications courantes, la valeur RPI par défaut est généralement suffisante. Pour des configurations plus complexes, utilisez le bouton Advanced (Avancé) pour modifier les paramètres de limite de temps de réponse de la connexion comme indiqué page 73.

Afficher le délai réseau maximum observé

Lorsque l'automate GuardLogix reçoit un paquet de sécurité, le logiciel enregistre le délai de transmission maximum observé sur le réseau. Pour les entrées de sécurité, le délai réseau maximum observé (Maximum Observed Network Delay) indique le temps total nécessaire pour la transmission d'un paquet de données depuis un module d'entrée jusqu'à l'automate et le retour de l'accusé de réception de ce dernier au module. Pour les sorties de sécurité, il indique le temps total nécessaire pour la transmission d'un paquet de données depuis l'automate jusqu'au module de sortie et pour le retour de l'accusé de réception de ce dernier à l'automate. Le délai réseau maximum observé apparaît dans l'onglet Safety (Sécurité) de la boîte de dialogue Module Properties (Propriétés du module). Lorsque vous êtes en ligne, vous pouvez remettre à zéro ce paramètre en cliquant sur Reset (Réinitialiser).

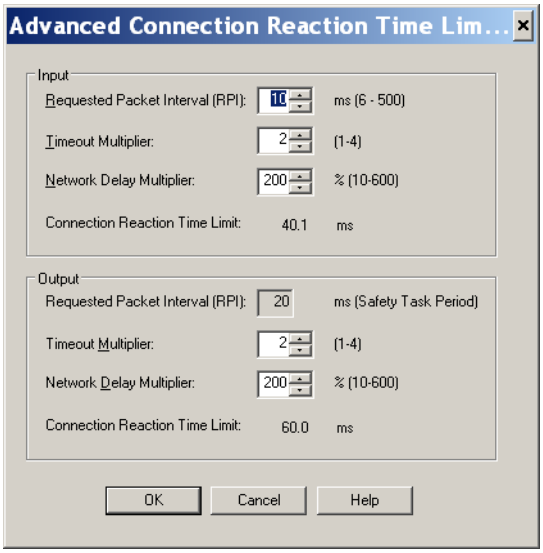
Figure 19 – Réinitialisation du délai réseau maximum observé



IMPORTANT Le délai réseau maximum réel entre le producteur et le consommateur d'une donnée est inférieur à la valeur affichée dans le champ Maximum Network Delay (Délai réseau maximum) de l'onglet Safety (Sécurité). En général, le délai maximum de transmission réel d'un message est égal à environ la moitié de la valeur de délai réseau maximum indiquée.

Réglage des paramètres avancés de limite de temps de réponse de la connexion

Figure 20 – Configuration évoluée



Multiplicateur de timeout

Le multiplicateur de timeout (Timeout Multiplier) de la connexion définit la durée de réception maximum d'un paquet de données en nombre d'intervalles RPI, au delà de laquelle la connexion sera déclarée expirée. Ceci se traduit par le nombre de messages susceptibles d'être perdus avant qu'une erreur de connexion ne soit déclarée.

Par exemple, un multiplicateur de timeout de 1 indique que les messages doivent être reçus pendant chaque intervalle RPI. Un multiplicateur de timeout de 2 indique qu'un message peut être perdu tant qu'un message au moins est reçu dans un intervalle équivalent à 2 fois la valeur RPI (2 x RPI).

Multiplicateur de délai réseau

Le multiplicateur de délai réseau (Network Delay Multiplier) définit le temps d'acheminement d'un message conformément aux exigences du protocole CIP Safety. Il indique le temps total de transmission d'une trame du producteur au consommateur et de retour de l'accusé de réception au producteur. Vous pouvez utiliser le multiplicateur de délai réseau pour réduire ou augmenter la limite de temps de réponse de la connexion dans les cas où le temps de transfert des messages en vigueur est sensiblement inférieur ou supérieur à la valeur RPI. Par exemple, il peut s'avérer utile d'ajuster le multiplicateur de délai réseau lorsque le RPI d'une connexion de sortie est identique à une longue période de tâche de sécurité.

Dans les cas où le RPI des entrées ou le RPI des sorties est relativement long ou court par rapport au temps de transport des messages appliqué, vous pouvez estimer le multiplicateur de délai réseau à l'aide de l'une des deux méthodes suivantes.

1ère méthode : utilisation du rapport entre le RPI des entrées et la période de la tâche de sécurité. Utilisez cette méthode uniquement dans les conditions suivantes :

- Lorsque le trajet ou le temps d'acheminement correspondent sensiblement à ceux des sorties.
- Lorsque l'intervalle RPI des entrées a été configuré de telle façon que le temps d'acheminement réel des messages d'entrée se trouve être inférieur à cette valeur.
- Lorsque la période de la tâche de sécurité est faible par rapport à l'intervalle RPI des entrées.

Dans ces conditions, le multiplicateur de délai réseau des sorties peut être estimé de la façon suivante :

Multiplicateur de délai réseau des entrées x [RPI des entrées ÷ période de la tâche de sécurité]

EXEMPLE **Calcul approximatif du multiplicateur de délai réseau des sorties**

Si :

RPI des entrées = 10 ms
Multiplicateur de délai réseau des entrées = 200 %
Période de la tâche de sécurité = 20 ms

Alors le multiplicateur de délai réseau des sorties est égal à :

200 % x [10 ÷ 20] = 100 %

2ème méthode : utilisation du délai réseau maximum observé. Si le système fonctionne longtemps dans des conditions de charge les plus défavorables, le multiplicateur de délai réseau peut être défini à partir du délai réseau maximum observé. Cette méthode peut être utilisée pour les connexions d'entrée ou de sortie. Après que le système ait fonctionné longtemps dans les conditions de charge les plus défavorables, enregistrez le délai réseau maximum observé.

Le multiplicateur de délai réseau peut alors être estimé à l'aide de la formule suivante :

[Délai réseau maximum observé + Facteur de marge] ÷ valeur RPI

EXEMPLE **Calcul du multiplicateur de délai réseau à partir du délai réseau maximum observé**

Si :

Intervalle RPI = 50 ms
Délai réseau maximum observé = 20 ms
Facteur de marge = 10

Le coefficient de délai réseau sera alors égal à :

[20 + 10] ÷ 50 = 60 %

Tableau 19 – Informations connexes

Ressource	Description
Systèmes de commande GuardLogix – Manuel de référence sur la sécurité (publication 1756-RM093)	Fournit des informations pour le calcul des temps de réponse.
« Guard I/O DeviceNet Safety Modules User Manual », Publication 1791DS-UM001	
« Guard I/O EtherNet/IP Safety Modules User Manual », Publication 1791ES-UM001	

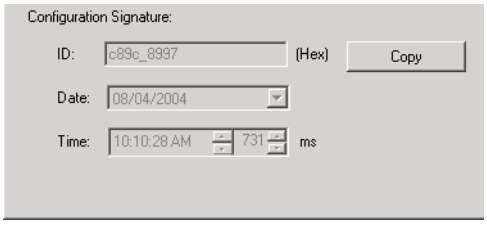
Utilité de la signature de configuration

Chaque dispositif de sécurité possède une signature de configuration unique qui définit la configuration du module. La signature de configuration est composée d'un numéro d'identification (ID number), d'une date et d'une heure. Cette signature est utilisée pour vérifier la configuration d'un module.

Configuration via le logiciel RSLogix 5000

Lorsqu'un module d'E/S est configuré à l'aide du logiciel RSLogix 5000, sa signature de configuration est générée automatiquement. Vous pouvez afficher et copier cette signature de configuration par l'intermédiaire de l'onglet Safety (Sécurité) de la boîte de dialogue Module Properties (Propriétés du module).

Figure 21 – Visualiser et copier la signature de configuration



Propriétaire de la configuration différent (connexion en écoute seule)

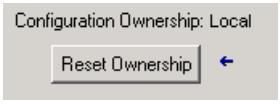
Quand la configuration d'un module d'E/S appartient à un automate différent, vous devez copier la signature de configuration de ce module dans le projet de son propriétaire et la coller dans l'onglet Safety (Sécurité) de la boîte de dialogue Module Properties (Propriétés du module).

CONSEIL Si le module est configuré pour les entrées uniquement, vous pouvez copier et coller la signature de configuration. Si le module possède des sorties de sécurité, elles appartiennent à l'automate qui est propriétaire de la configuration et la zone de texte de la signature de configuration n'est pas disponible.

Réinitialisation du propriétaire des modules d'E/S de sécurité

Lorsque le logiciel RSLogix 5000 est en ligne, l'onglet Safety (sécurité) de la boîte de dialogue Module Properties (Propriétés du module) affiche la propriété de configuration actuelle. Lorsque le projet ouvert est propriétaire de la configuration, Local est affiché. Lorsqu'un second équipement est propriétaire de la configuration, Remote (Distant) s'affiche, ainsi que le numéro de réseau de sécurité (SNN) et l'adresse de station ou le numéro de logement du propriétaire de la configuration. Communication error (Erreur de communication) s'affiche en cas d'échec de la lecture du module.

En ligne, vous pouvez rétablir la configuration par défaut du module en cliquant sur le bouton Reset Ownership (Réinitialiser la propriété).



CONSEIL Vous ne pouvez pas réinitialiser le propriétaire d'un module lorsque des modifications de ses propriétés sont en cours, ou lorsqu'une signature de tâche de sécurité est présente ou encore lorsque la sécurité est verrouillée.

Adressage des données d'E/S de sécurité

Lorsque vous ajoutez un module au dossier de configuration des E/S, le logiciel RSLogix 5000 crée automatiquement des points d'accès automate pour le module.

Les informations d'E/S sont représentées sous la forme d'un ensemble de points. Chaque point utilise une certaine structure de données selon le type et les caractéristiques du module d'E/S. La dénomination d'un point est basée sur le nom du module dans le système.

L'adresse d'un dispositif d'E/S CIP Safety est au format suivant :

Nomdumodule:Type.Membre

Tableau 20 – Format d'adresse d'un module d'E/S CIP Safety

Dans lequel	Désigne	
Nomdumodule	Le nom du module d'E/S CIP Safety	
Type	Le type de donnée	
	Entrée : I	
	Sortie : O	
Membre	Données spécifiques au module d'E/S	
	Module d'entrées seules :	Nomdumodule:I.ModeRun Nomdumodule:I.ConnectionFaulted Nomdumodule:I.Input Members
	Module de sortie uniquement :	Nomdumodule:I.RunMode Nomdumodule:I.ConnectionFaulted Nomdumodule:O.Output Members
	Module d'E/S mixte :	Nomdumodule:I.RunMode Nomdumodule:I.ConnectionFaulted Nomdumodule:I.Input Members Nomdumodule:O.Output Members

Tableau 21 – Informations connexes

Ressource	Description
Chapitre 9, Surveillance de l'état et gestion des défauts	Contient des informations sur la surveillance des points de données de sécurité
Données d'E/S et de point des automates Logix5000, publication 1756-PM004	Fournit des informations sur l'adressage des modules d'E/S standard

Surveillance de l'état des modules d'E/S de sécurité

Vous pouvez surveiller l'état d'un module d'E/S de sécurité grâce à la messagerie explicite ou aux voyants d'état situés sur les modules.

Ces publications fournissent des informations de dépannage des modules d'E/S :

- « Guard I/O DeviceNet Safety Modules User Manual », publication 1791DS-UM001
- « Guard I/O EtherNet/IP Modules User Manual », publication 1791ES-UM001
- Modules de sécurité POINT Guard I/O Notice d'installation et manuel utilisateur, publication 1734-UM013

Tableau 22 – Fonctionnement des voyants d'état

Voyant	État	Description		
		Modules Guard I/O DeviceNet	**Modules Guard I/O EtherNet/IP**	**Modules POINT Guard I/O**
État du module (MS)	Éteint	Module hors tension.		
	Vert, fixe	Fonctionnement normal.		
	Vert, clignotant	Module en attente.		
	Rouge, clignotant	Une erreur récupérable s'est produite.	Une erreur récupérable s'est produite ou une mise à jour du firmware est en cours.	
	Rouge, fixe	Une erreur irrécupérable s'est produite.		
	Rouge/vert, clignotant	Auto-tests en cours.	Auto-tests en cours ou le module n'est pas configuré correctement. Pour plus de précisions, vérifier le voyant d'état du réseau.	
État du réseau (NS)	Éteint	Le module n'est pas en ligne ou n'est peut être pas sous tension.		
	Vert, fixe	Le module est en ligne et les connexions sont établies.		
	Vert, clignotant	Le module est en ligne mais les connexions ne sont pas établies.		
	Rouge, clignotant	Timeout de la communication.	Timeout de la communication ou une mise à jour du firmware est en cours.	
	Rouge, fixe	Échec de la communication. Le module a détecté une erreur qui a empêché la communication avec le réseau.		
	Rouge/vert, clignotant	Le module est en état de défaut de communication ou le numéro SNN est en cours de définition.	Auto-test en cours.	–
Points d'entrée (IN*x*)	Éteint	Entrée de sécurité désactivée.		
	Jaune, fixe	Entrée de sécurité activée.		
	Rouge, fixe	Erreur dans le circuit d'entrée.		
	Rouge, clignotant	Quand le fonctionnement en double voie est sélectionné, une erreur s'est produite dans le circuit d'entrée du partenaire.		
Points de sortie (O*x*)	Éteint	Sortie de sécurité désactivée.		
	Jaune, fixe	Sortie de sécurité activée.		
	Rouge, fixe	Erreur dans le circuit de sortie.		
	Rouge, clignotant	Quand le fonctionnement en double voie est sélectionné, une erreur s'est produite dans le circuit de sortie du partenaire.		
Points de sortie de test (T*x*)	Éteint	–	La sortie est désactivée.	–
	Jaune, fixe		La sortie est activée.	
	Rouge, fixe		Erreur dans le circuit de sortie.	
LOCK (verrouillage)	Jaune, fixe	La configuration du dispositif est verrouillée.	Le logiciel RSLogix 5000 ne prend pas en charge cette fonction.	
	Jaune, clignotant	La configuration du dispositif est valable mais le module n'est pas verrouillé.		
	Jaune, éteint	Données de configuration incorrectes ou absentes, ou le dispositif a été configuré par le logiciel RSLogix 5000.		
IN PWR	Vert, éteint	Pas de tension d'entrée.		–
	Vert, fixe	La tension d'entrée est conforme aux spécifications.		
	Jaune, fixe	La tension d'entrée est hors spécifications.		
OUT PWR	Vert, éteint	Pas de tension de sortie.		
	Vert, fixe	La tension de sortie est conforme aux spécifications.		
	Jaune, fixe	La tension de sortie est hors spécifications.		
PWR	Vert, éteint	–		Module hors tension.
	Vert, fixe			La tension d'alimentation est conforme aux spécifications.
	Jaune, fixe			La tension d'alimentation est hors spécifications.

Réinitialisation d'un module en condition d'origine

Si un module Guard I/O était utilisé précédemment, effacez la configuration existante avant de l'installer dans un réseau de sécurité, en le réinitialisant en condition d'origine.

Lorsque le logiciel RSLogix 5000 est en ligne avec l'automate, l'onglet Safety (Sécurité) de la boîte de dialogue Module Properties (Propriétés du module) affiche le propriétaire actuel de la configuration. Lorsque le projet ouvert est propriétaire de la configuration, Local est affiché. Lorsqu'un second équipement est propriétaire de la configuration, Remote (Distant) s'affiche, ainsi que le numéro de réseau de sécurité (SNN) et l'adresse de station ou le numéro de logement du propriétaire de la configuration. Communication error (Erreur de communication) s'affiche en cas d'échec de la lecture du module.

Si la connexion est locale, vous devez inhiber la connexion du module avant de réinitialiser la propriété. Suivez ces étapes pour inhiber le module.

1. Cliquez avec le bouton droit de la souris sur le module et choisissez Properties (Propriétés).
2. Cliquez sur l'onglet Connection (Connexion).
3. Cliquez sur Inhibit Connection (Inhiber la connexion).
4. Cliquez sur Apply (Appliquer), puis sur OK.

Suivez ces étapes pour réinitialiser le module dans sa configuration d'origine lorsque vous êtes en ligne.

1. Cliquez avec le bouton droit de la souris sur le module et choisissez Properties (Propriétés).
2. Cliquez sur l'onglet Safety (Sécurité).
3. Cliquez sur Reset Ownership (Réinitialiser la propriété).

CONSEIL Vous ne pouvez pas réinitialiser le propriétaire d'un module lorsque des modifications de ses propriétés sont en cours, ou lorsqu'une signature de tâche de sécurité est présente ou encore lorsque la sécurité est verrouillée.

Remplacement d'un module à l'aide du logiciel RSLogix 5000

Vous pouvez utiliser le logiciel RSLogix 5000 pour remplacer un module Guard I/O sur un réseau Ethernet. Pour remplacer un module Guard I/O sur un réseau DeviceNet, le choix du logiciel dépend du type de ce module.

Tableau 23 – Logiciel

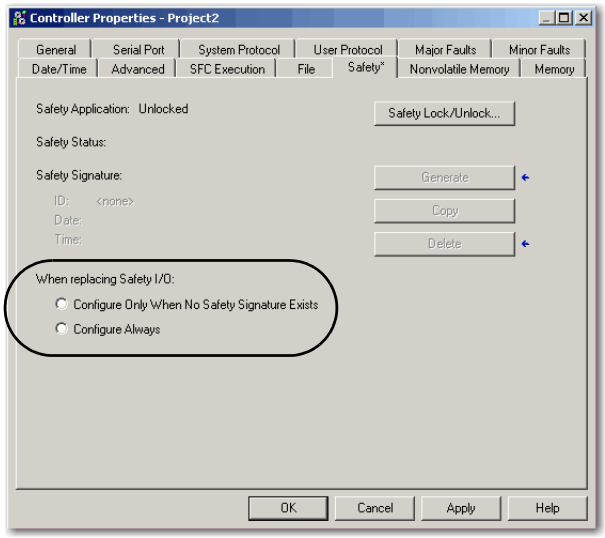
Si vous utilisez un…	Utilisez le logiciel…	Voir…
module Guard I/O 1791DS avec un adaptateur 1756-DNB	RSLogix 5000	ci-dessous
module Guard I/O 1734 avec un adaptateur 1734-PDN	logiciel RSNetWorx for DeviceNet	Remplacement d'un module POINT Guard I/O à l'aide du logiciel RSNetWorx for DeviceNet, page 86

Si vous comptez sur une partie du système CIP Safety pour maintenir un comportement SIL3 pendant le remplacement et le test fonctionnel d'un module, l'utilisation de la fonctionnalité Configure Always (Toujours configurer) est déconseillée. Passez à Remplacement avec « Configure Only When No Safety Signature Exists » validé, page 80.

Si vous ne comptez pas sur la totalité du système de commande CIP Safety routable pour maintenir le niveau SIL 3/PLe pendant le remplacement et le test fonctionnel du module, la fonctionnalité Configure Always (Toujours configurer) peut être utilisée. Allez à Remplacement avec « Configure Always » validé, page 84.

Le module de remplacement est configuré dans l'onglet Safety (Sécurité) de l'automate GuardLogix.

Figure 22 – Remplacement de module d'E/S de sécurité



Remplacement avec « Configure Only When No Safety Signature Exists » validé

Quand un module est remplacé, la configuration sera téléchargée depuis l'automate de sécurité si le DeviceID (ID de dispositif) du nouveau module correspond à l'ancien. L'identifiant DeviceID est une combinaison de l'adresse IP de la station et du numéro de réseau de sécurité (SNN) qui est mise à jour quand le SNN est établi.

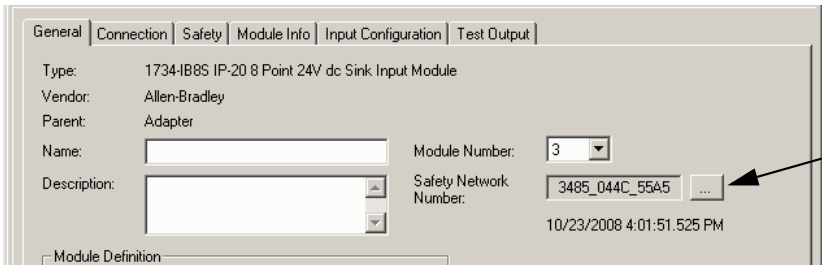
Si le projet est configuré selon « Configure Only When No Safety Signature Exists » (Configurer seulement en absence de signature de sécurité), suivez les étapes appropriées du Tableau 24 pour remplacer un module POINT Guard I/O en fonction de votre scénario. Une fois que vous avez terminé les étapes correctement, le DeviceID correspondra à l'original, ce qui permet à l'automate de sécurité de télécharger la configuration de module correcte et de rétablir la connexion de sécurité.

Tableau 24 – Remplacement d'un module

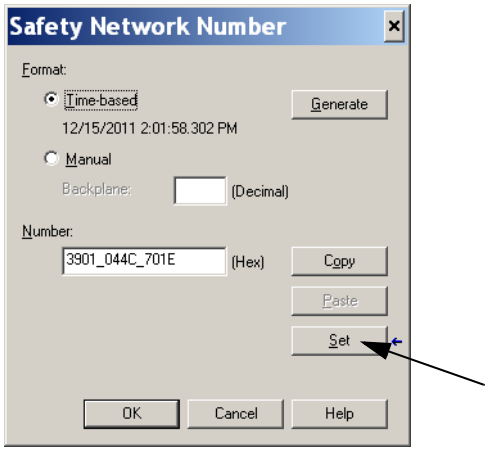
La signature de sécurité GuardLogix existe	Condition du module de remplacement	Action requise
Non	Pas de SNN (matériel neuf)	Aucune. Le module est prêt pour l'emploi.
Oui ou non	Même SNN que dans la configuration de la tâche de sécurité originale	Aucune. Le module est prêt pour l'emploi.
Oui	Pas de SNN (matériel neuf)	Voir Scénario 1 – Le module de remplacement est neuf et la signature de sécurité existe, page 81.
Oui	SNN différent de la configuration de la tâche de sécurité originale	Voir Scénario 2 – Le SNN du module de remplacement est différent de l'original et une signature de sécurité existe, page 82.
Non		Voir Scénario 3 – Le SNN du module de remplacement est différent de l'original et aucune signature de sécurité n'existe, page 84.

Scénario 1 – Le module de remplacement est neuf et la signature de sécurité existe

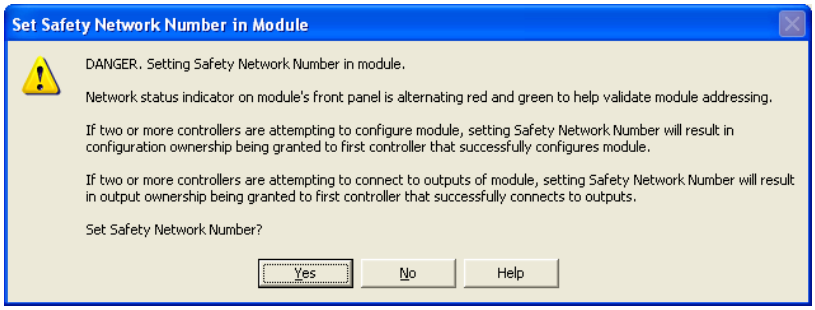
1. Retirez l'ancien module d'E/S et installez le nouveau.
2. Cliquez avec le bouton droit de la souris sur le module POINT Guard I/O de remplacement et choisissez Properties (Propriétés).
3. Cliquez sur le bouton ... situé à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro SNN).



4. Cliquez sur Set (Définir).



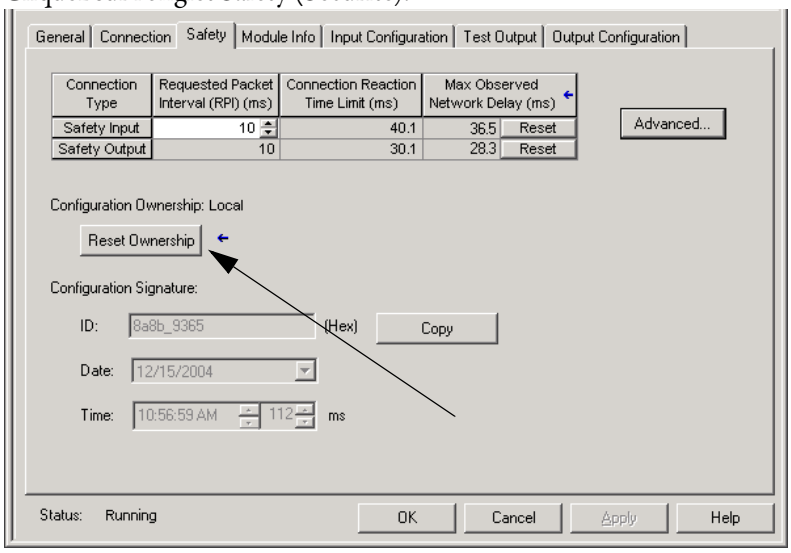
5. Vérifiez que le voyant d'état du réseau (NS) clignote alternativement en vert et rouge sur le module concerné avant de cliquer sur Yes (Oui) dans la boîte de dialogue Set Safety Network Number in Module (Définir le numéro SNN dans le module) pour confirmer le numéro SNN et valider le module de remplacement.



6. Suivez les procédures définies dans votre société pour la réalisation des tests fonctionnels du nouveau module d'E/S et du système et la revalidation de ce système.

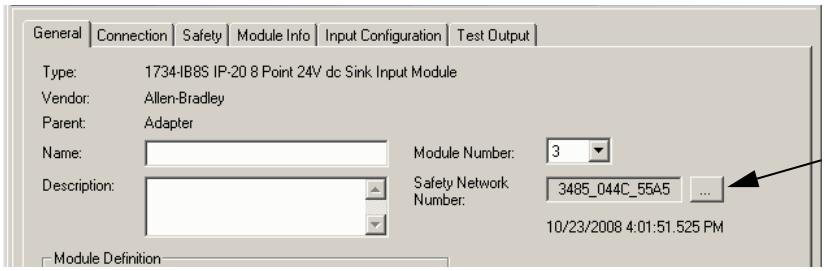
Scénario 2 – Le SNN du module de remplacement est différent de l'original et une signature de sécurité existe

1. Retirez l'ancien module d'E/S et installez le nouveau.
2. Cliquez avec le bouton droit de la souris sur le module POINT Guard I/O et choisissez Properties (Propriétés).
3. Cliquez sur l'onglet Safety (Sécurité).

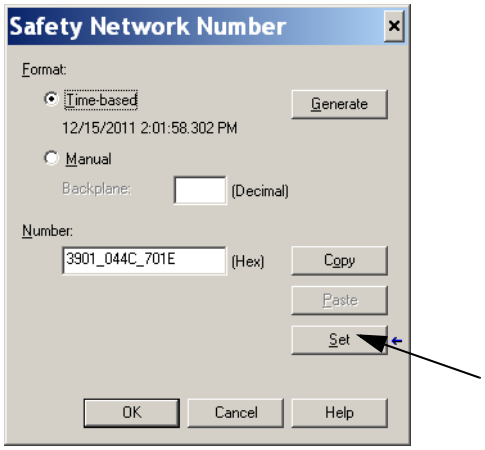


4. Cliquez sur Reset Ownership (Réinitialiser la propriété).
5. Cliquez sur OK.
6. Cliquez avec le bouton droit de la souris sur l'automate et choisissez Properties (Propriétés).

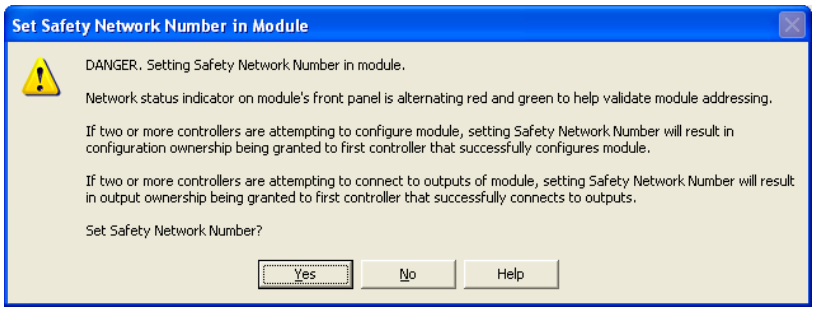
7. Cliquez sur le bouton ... situé à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro SNN).



8. Cliquez sur Set (Définir).



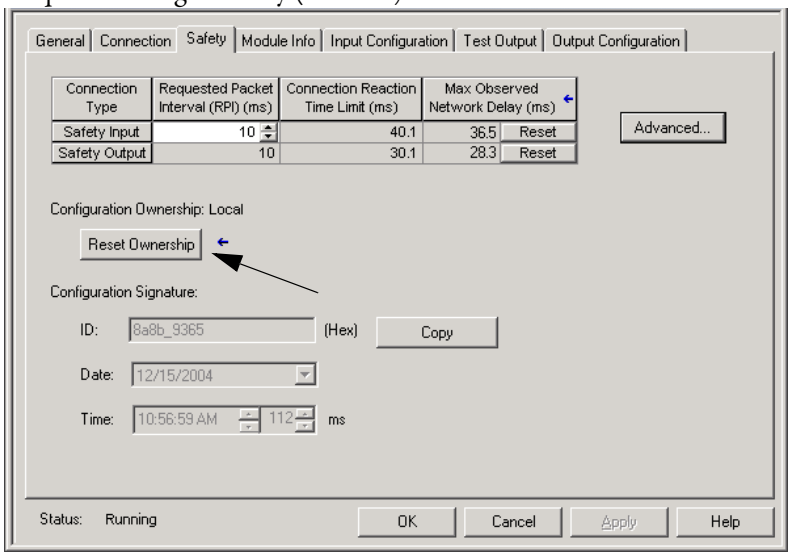
9. Vérifiez que le voyant d'état du réseau (NS) clignote alternativement en vert et rouge sur le module concerné avant de cliquer sur Yes (Oui) dans la boîte de dialogue de confirmation pour affecter le numéro SNN et valider le module de remplacement.



10. Suivez les procédures définies dans votre société pour la réalisation des tests fonctionnels du nouveau module d'E/S et du système et la revalidation de ce système.

Scénario 3 – Le SNN du module de remplacement est différent de l'original et aucune signature de sécurité n'existe

1. Retirez l'ancien module d'E/S et installez le nouveau.
2. Cliquez avec le bouton droit de la souris sur le module POINT Guard I/O et choisissez Properties (Propriétés).
3. Cliquez sur l'onglet Safety (Sécurité).



4. Cliquez sur Reset Ownership (Réinitialiser la propriété).
5. Cliquez sur OK.
6. Suivez les procédures définies dans votre société pour la réalisation des tests fonctionnels du nouveau module d'E/S et du système et la revalidation de ce système.

Remplacement avec « Configure Always » validé

ATTENTION : n'activez la fonction « Configure Always » (Toujours configurer) que si vous n'avez **pas** besoin de faire appel à une quelconque partie du système de commande CIP Safety pour maintenir un comportement SIL 3 pendant le remplacement et le test fonctionnel d'un module.

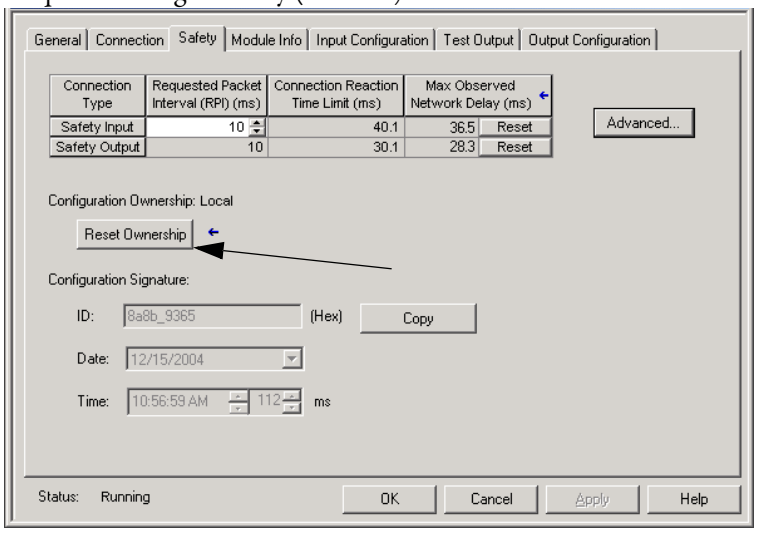
N'introduisez pas sur un réseau CIP Safety des modules dans leur configuration d'origine lorsque la fonctionnalité Configure Always (Toujours configurer) est activée, sauf en suivant cette procédure de remplacement.

Si la fonction « Configure Always » (Toujours configurer) est activée dans le logiciel RSLogix 5000, l'automate vérifiera automatiquement la présence et connectera un module de remplacement satisfaisant à l'ensemble des exigences suivantes :

- L'automate contient déjà des informations de configuration pour un module de même type à cette adresse réseau.
- Le module est dans la condition d'origine ou possède un SNN qui correspond à la configuration.

Si le projet est configuré pour « Configure Always », suivez les étapes appropriées pour remplacer un module POINT Guard I/O.

1. Retirez l'ancien module d'E/S et installez le nouveau.
   a. Si le module est en condition d'origine, allez à l'étape 6.
   Aucune action n'est nécessaire pour que l'automate GuardLogix acquiert la propriété du module.
   b. Si une erreur de discordance de SNN se produit, passez à l'étape suivante pour réinitialiser le module en condition d'origine.
2. Cliquez avec le bouton droit de la souris sur le module POINT Guard I/O et choisissez Properties (Propriétés).
3. Cliquez sur l'onglet Safety (Sécurité).



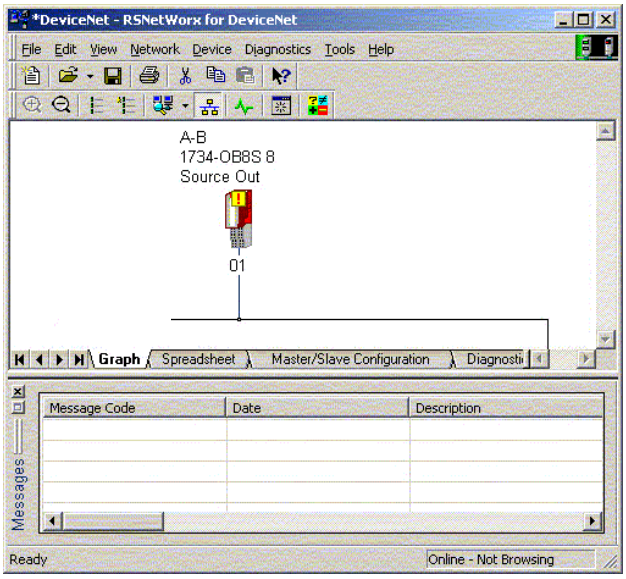
4. Cliquez sur Reset Ownership (Réinitialiser la propriété).
5. Cliquez sur OK.
6. Suivez les procédures prescrites par votre entreprise pour réaliser les tests fonctionnels du nouveau module d'E/S et du système, et revalider ce système.

Remplacement d'un module POINT Guard I/O à l'aide du logiciel RSNetWorx for DeviceNet

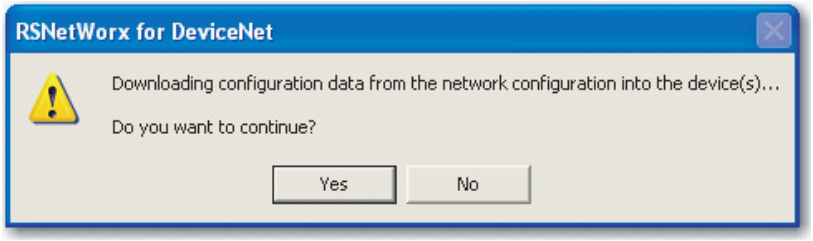
Suivez ces étapes pour remplacer un module POINT Guard I/O quand le module et l'automate sont sur un réseau DeviceNet.

1. Remplacez le module et réglez le numéro de station pour qu'il corresponde à celui du module original.
2. Ouvrez votre projet dans le logiciel RSNetWorx for DeviceNet.

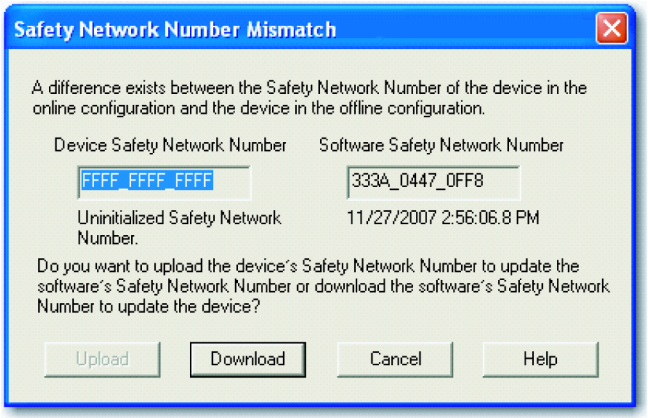
   Si le module de remplacement est neuf ou a un SNN qui ne correspond pas au module d'origine, le module apparaît avec un point d'exclamation.



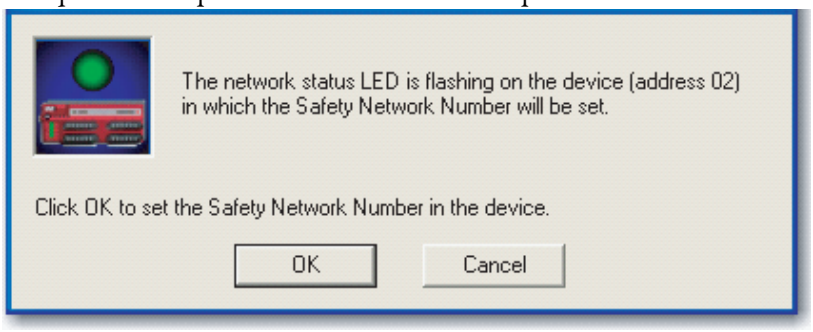
3. Cliquez avec le bouton droit de la souris sur le module et choisissez Download to Device (Télécharger le dispositif).



4. Cliquez sur Yes (Oui) pour confirmer.
5. Dans la boîte de dialogue Safety Network Number Mismatch (Discordance de SNN), cliquez sur Download (Télécharger) pour établir le SNN dans le module de remplacement.

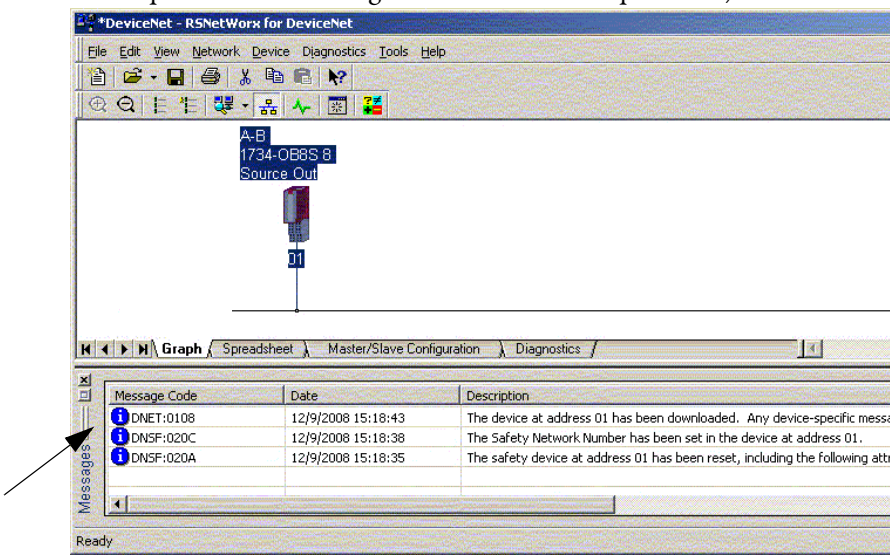


6. Vérifiez que le voyant d'état du réseau (NS) clignote sur le module correct et cliquez sur OK pour établir le SNN sur ce dispositif.



Le logiciel RSNetWorx for DeviceNet confirme que le SNN a été établi.

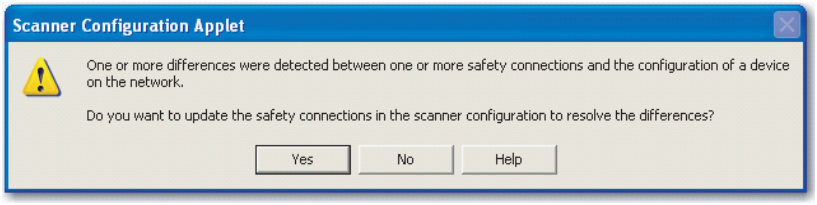
Une fois que le téléchargement s'est terminé avec succès, la vue principale du projet affiche ce message : « The device at address *xx* has been downloaded » (Le dispositif à l'adresse [xx] a été téléchargé). « Any device-specific messages related to the download operation displayed separately » (Tous les messages spécifiques au périphérique en relation avec l'opération de téléchargement sont affichés séparément).



En supposant que c'est la configuration correcte provenant du fichier DNT original, le SNN et la signature de configuration correspondent maintenant à l'original. Si vous êtes déjà connecté à l'automate, une connexion est établie. Il est inutile de passer l'automate hors du mode Exécution pour télécharger le module de remplacement.

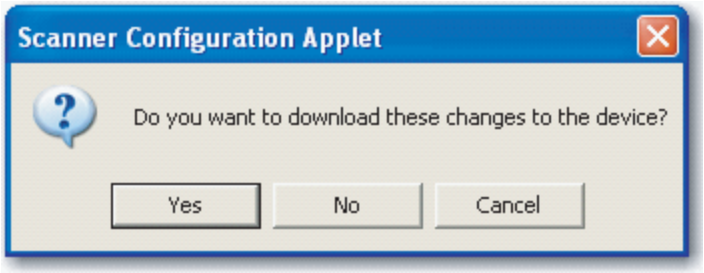
Si vous téléchargez cette configuration dans un agencement temporaire, placez le module sur le réseau et il se connecte automatiquement à l'automate.

Si la configuration téléchargée dans le module ne provenait pas du fichier DNT original, la signature de configuration ne correspondra pas à l'originale. Même si vous créez les mêmes paramètres dans un nouveau fichier DNT, les parties de temps et de date de la signature seront différentes et par conséquent la connexion avec l'automate ne sera pas réalisée. Si cela se produit, cliquez sur l'onglet Safety Connection (Connexion de sécurité) de l'automate qui vous a indiqué que la signature de configuration est différente et qui vous offre l'option de faire correspondre la nouvelle signature de configuration. Toutefois, vous devriez d'abord revalider le système de sécurité, car il n'utilise pas le fichier DNT original.



7. Cliquez sur Yes (oui).

   Ceci sort l'automate du mode Exécution et vous invite à télécharger les modifications.



8. Cliquez sur Yes (Oui) pour télécharger la nouvelle configuration de connexion dans l'automate SmartGuard.

   Quand le téléchargement est terminé, remettez l'automate en mode Exécution et la connexion avec le module de remplacement est établie.

9. Suivez les procédures prescrites par votre entreprise pour réaliser les tests fonctionnels du nouveau module d'E/S et du système, et revalider ce système.

Développement d'applications de sécurité

Ce chapitre présente les composants d'un projet de sécurité et informe sur l'utilisation de fonctions permettant de garantir l'intégrité des applications de sécurité, comme la signature de tâche de sécurité et le verrouillage de sécurité.

Pour connaître les directives et les conditions à respecter pour le développement et la mise en service d'applications de sécurité SIL 3 et PLe, reportez-vous à la publication 1756-RM093, « Systèmes automates GuardLogix – Manuel de référence sur la sécurité ».

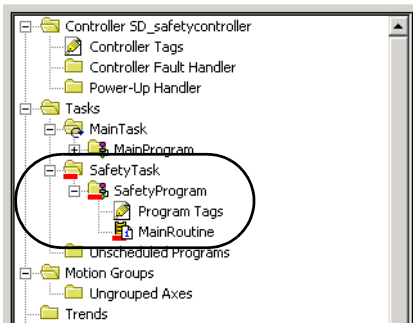
Ce manuel de référence sur la sécurité traite des sujets suivants :

- création d'une spécification détaillée pour un projet ;
- écriture, documentation et test de l'application ;
- création d'une signature de tâche de sécurité pour l'identification et la protection du projet ;
- validation du projet transféré à partir de son impression ou de son affichage en comparant manuellement les configurations, les données de sécurité et la logique du programme de sécurité ;
- vérification du projet à l'aide de tests types, de simulations, de tests de vérification fonctionnelle ; et s'il y a lieu, un examen de conformité des fonctions de sécurité par un organisme indépendant ;
- verrouillage de l'application de sécurité ;
- calcul du temps de réaction du système.

La tâche de sécurité

Lorsque vous créez un projet d'automate de sécurité, le logiciel RSLogix 5000 constitue automatiquement une tâche de sécurité comprenant un programme de sécurité et un sous-programme principal (de sécurité).

Figure 23 – Tâche de sécurité dans la fenêtre d'organisation de l'automate



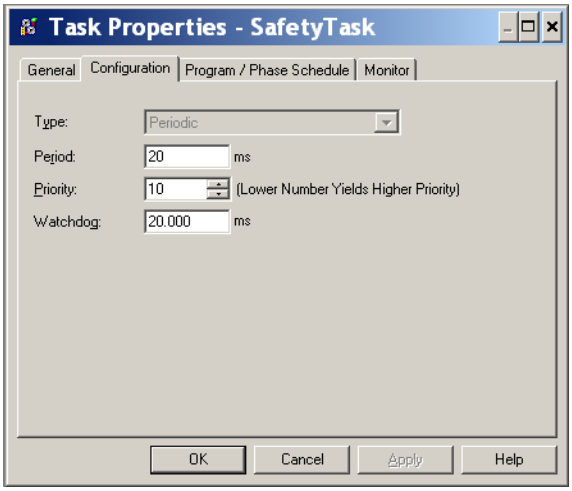
Dans le cadre de cette tâche de sécurité, vous pouvez utiliser plusieurs programmes de sécurité eux-même composés de divers sous-programmes de sécurité. L'automate GuardLogix prend en charge une tâche de sécurité. La tâche de sécurité ne peut pas être supprimée.

Vous ne pouvez pas planifier des programmes standard ou exécuter des sous-programmes standard au sein de la tâche de sécurité.

Spécification de la période de la tâche de sécurité

La tâche de sécurité est une tâche périodique. Vous devez sélectionner la priorité de la tâche et un temps de chien de garde via les Task Properties (Propriétés de la tâche) de la boîte de dialogue Safety Task (Tâche de sécurité). Pour ouvrir cette boîte de dialogue, cliquez sur la tâche de sécurité avec le bouton droit de la souris et sélectionnez Properties (Propriétés).

Figure 24 – Configuration de la période de la tâche de sécurité



La tâche de sécurité doit avoir une priorité élevée. Vous devez définir la période de la tâche de sécurité (en ms) et le chien de garde de la tâche de sécurité (en ms). La période de la tâche de sécurité est la périodicité à laquelle elle s'exécute. Le chien de garde de la tâche de sécurité correspond à la durée maximale autorisée entre le début et la fin de son exécution.

La période de la tâche de sécurité est limitée à 500 ms maximum et ne peut pas être modifiée en ligne. Assurez-vous que la tâche de sécurité dispose d'assez de temps pour terminer l'exécution de la logique avant qu'elle ne soit à nouveau déclenchée. Si un timeout du chien de garde de la tâche de sécurité se produit, un défaut de sécurité irrécupérable est généré dans l'automate de sécurité.

La période de la tâche de sécurité influe directement sur le temps de réaction du système.

Vous trouverez des informations détaillées sur le calcul du temps de réaction du système dans la publication 1756-RM093, « Systèmes d'automates GuardLogix – Manuel de référence sur la sécurité ».

Exécution de la tâche de sécurité

La tâche de sécurité s'exécute de la même façon qu'une tâche périodique standard, à l'exception des caractéristiques suivantes :

- La tâche de sécurité ne démarre pas tant que l'automate principal et son partenaire de sécurité n'ont pas établi leur partenariat de commande. Toutefois, les tâches standard commenceront à s'exécuter dès que l'automate sera passé en mode RUN (Exécution).
- Tous les points d'entrée de sécurité (entrées, points consommés et mappés) sont mis à jour et gelés au début de l'exécution de la tâche de sécurité.

  Pour de plus amples informations sur le mappage des points de sécurité, voir page 102.
- Les valeurs des point de sortie de sécurité (sorties et points produits) sont mises à jour à la fin de l'exécution de la tâche de sécurité.

Programmes de sécurité

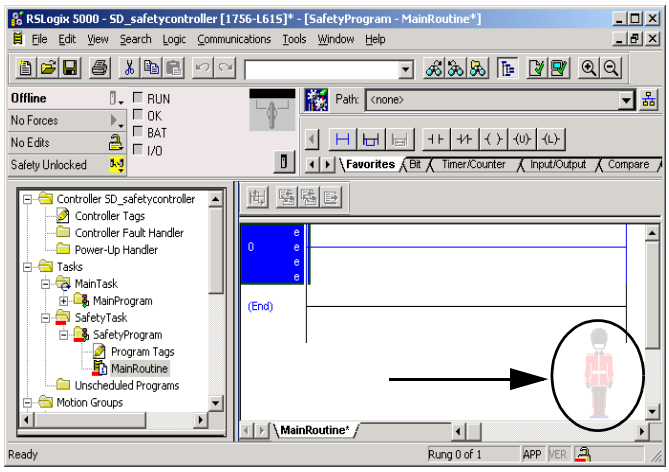
Les programmes de sécurité possèdent toutes les caractéristiques des programmes standard, excepté qu'ils ne peuvent être planifiés qu'à l'intérieur d'une tâche de sécurité et ne peuvent contenir que des composants de sécurité. Les programmes de sécurité ne peuvent contenir que des sous-programmes de sécurité, l'un d'eux devant être défini comme sous-programme principal et un autre comme sous-programme de gestion des défauts.

Les programmes de sécurité ne peuvent pas contenir de sous-programmes standard ou de points standard.

Sous-programmes de sécurité

Les sous-programmes de sécurité possèdent tous les attributs des sous-programmes standard, hormis le fait qu'ils ne peuvent exister que dans un programme de sécurité. Pour l'instant, seule la logique à relais est prise en charge pour la programmation des sous-programmes de sécurité.

CONSEIL Le logiciel RSLogix 5000 utilise un filigrane permettant de distinguer visuellement un sous-programme de sécurité d'un sous-programme standard.



Points de sécurité

Un point est une zone de la mémoire d'un automate dans laquelle des données sont stockées. Les points constituent le mécanisme de base pour l'allocation de la mémoire, le référencement des données à partir de la logique et la surveillance des données. Les points de sécurité possèdent tous les attributs des points standard. Ils utilisent de plus des mécanismes normalisés leur permettant de garantir une intégrité SIL 3 de leurs données.

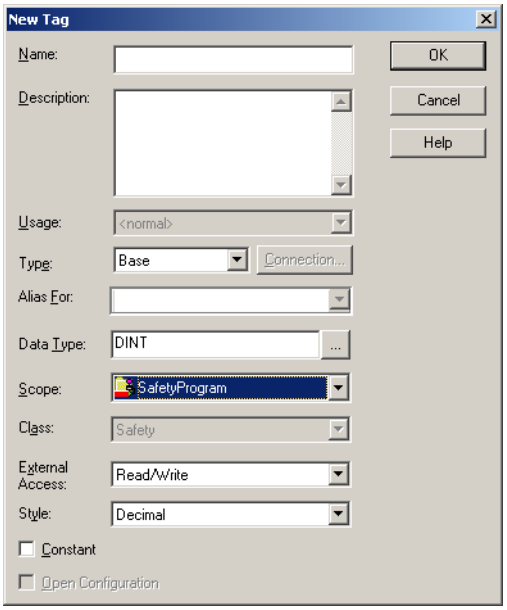
Lorsque vous créez un point, vous lui attribuez les propriétés suivantes :

- Nom
- Description (facultative)
- Type de point
- Type de données
- Accès
- Classe
- Style
- Accès externe

Vous pouvez également définir si la valeur du point doit être une constante.

Pour créer un point de sécurité, ouvrez la boîte de dialogue New Tag (Nouveau point) en cliquant avec le bouton droit de la souris sur Controller Tags (Points automate) ou sur Program Tags (Points programme), puis choisissez New Tag (Nouveau point).

Figure 25 – Création d'un nouveau point



Type de point

Le Tableau 25 définit les quatre types de points : de base, alias, produit et consommé.

Tableau 25 – Quatre types de point

Type de point	Description
De base	Ces points stockent des valeurs qui seront utilisées par le programme au sein du projet.
Alias	Point faisant référence à un autre point. Un alias de point peut faire référence à un autre alias de point ou à un point de base. Un alias de point peut également faire référence à un composant d'un autre point en renvoyant à un membre d'une structure, à un élément de tableau ou à un bit dans un point ou un membre. **IMPORTANT :** la création d'un alias entre des points standard et de sécurité est interdite dans les applications de sécurité. Les points standard peuvent plutôt être mappés sur les points de sécurité en utilisant le mappage de points de sécurité. Voir Mappage de points de sécurité, page 102.
Produit	Point qu'un automate met à la disposition d'autres automates. 15 automates au maximum peuvent consommer (recevoir) simultanément des données. Un point produit envoie ses données à un point consommateur ou plus sans intervention du programme. Les données du point produit sont transmises selon l'intervalle RPI du point consommateur.
Consommé	Point qui reçoit les données d'un point produit. Le type de donnée du point consommé doit correspondre à celui du point produit. L'intervalle RPI du point consommé détermine la fréquence de mise à jour des données.

Type de données

Le type de donnée définit la forme sous laquelle le point stocke les données, comme un bit ou un nombre entier.

Les types de données peuvent être combinés pour former des structures. Une structure définit un type de données spécifique répondant à un usage particulier. À l'intérieur d'une structure, chaque type de données est appelé « membre ». Tout comme les points, les membres possèdent un nom et un type de données. Vous pouvez créer vos propres structures sous forme de types de données utilisateur.

Les automates Logix contiennent des types de données prédéfinis utilisables avec des instructions spécifiques.

Seuls les types de données suivants sont autorisés pour les points de sécurité :

Tableau 26 – Types de données applicables aux points de sécurité

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

Les types de données REAL sont compatibles avec les projets pour les automates 1756-L7*x*S, mais ils ne le sont pas avec les projets pour les automates 1756-L6*x*S ou 1768-L4*x*S.

IMPORTANT Cette restriction est extensible aux types de données utilisateur comportant des types de données prédéfinis.

Accès

L'accès d'un point détermine où vous pouvez accéder aux données du point. Lorsque vous créez un point, vous le définissez en tant que point d'accès automate (données globales) ou en tant que point d'accès programme pour un programme de sécurité ou standard particulier (données locales). Les points de sécurité peuvent être en accès automate ou programme de sécurité.

Points d'accès automate

Lorsque les points de sécurité sont en accès automate, tous les programmes ont accès aux données de sécurité. Les points doivent être en accès automate s'ils sont utilisés :

- par plusieurs programmes du projet ;
- pour produire ou consommer des données ;
- pour communiquer avec un terminal d'IHM PanelView ;
- pour le mappage d'un point de sécurité.
  Reportez-vous à Mappage de points de sécurité, page 102 pour plus d'informations.

Les points de sécurité en accès automate peuvent être lus, mais pas écrits, par des sous-programmes standard.

IMPORTANT	Les points de sécurité en accès automate peuvent être lus par n'importe quel sous-programme standard. La fréquence d'actualisation du point de sécurité est basée sur la période de la tâche de sécurité.

Les points associés aux E/S de sécurité et aux données de sécurité produites ou consommées doivent être des points de sécurité en accès automate. Pour les points de sécurité produits ou consommés, vous devrez créer un type de données utilisateur. Le premier membre de la structure du point sera réservé à l'état de la connexion. Il utilisera le type de données prédéfini CONNECTION_STATUS.

Tableau 27 – Informations connexes

Ressource	Description
Connexions de sécurité, page 127	Contient des informations supplémentaires sur le membre CONNECTION_STATUS
« Données d'E/S et de point des automates Logix5000 », publication 1756-PM004	Fournit des recommandations pour la création de types de données utilisateur

Points d'accès programme

Lorsque les points sont en accès programme, leurs données sont isolées des autres programmes. Vous pouvez réutiliser les noms des points d'accès programme dans différents programmes.

Seul un sous-programme de sécurité figurant dans le même programme de sécurité que les points de sécurité d'accès programme peut les lire ou y écrire des données.

Classe

Les points peuvent être classés en catégorie standard ou sécurité. Les points classés en catégorie sécurité doivent utiliser un type de données compatible.

Lorsque vous créez des points d'accès programme, leur classe est automatiquement définie en fonction du type du programme, standard ou de sécurité, pour lequel ils ont été créés.

Lorsque vous créez des points d'accès automate, vous devrez choisir leur classe manuellement.

Valeur constante

Lorsque vous assignez une valeur constante à un point, il ne peut pas être modifié par le programme de l'automate ni par une application externe telle qu'une IHM. Les points à valeur constante ne peuvent pas être forcés.

Si aucune signature de tâche de sécurité n'est présente, le logiciel RSLogix 5000 peut modifier des points standard à valeur constante et des points de sécurité. Les points de sécurité ne peuvent pas être modifiés en présence d'une signature de sécurité.

Accès externe

L'accès externe définit le niveau d'autorisation donné à des dispositifs externes telle qu'une IHM, pour afficher ou modifier des valeurs de point. Les accès par le logiciel RSLogix 5000 ne sont pas concernés par ce réglage. La valeur par défaut est lecture/écriture.

Tableau 28 – Niveaux de l'accès externe

Réglage de l'accès externe	Description
Aucun	Les points ne sont pas accessibles depuis l'extérieur de l'automate.
Lecture seule	Les points peuvent être parcourus ou lus, mais pas écrits depuis l'extérieur de l'automate.
Lecture/écriture	Les points standard peuvent être parcourus, lus et écrits depuis l'extérieur de l'automate.

Pour les points d'alias, le type d'accès externe correspond à celui configuré pour le point de base associé.

Points de sécurité produits/consommés

Pour transférer des données de sécurité entre des automates GuardLogix de tous types, vous devez utiliser des points de sécurité produits et consommés. Les points produits et consommés nécessitent des connexions. À partir de la version 19 du logiciel RSLogix 5000, le type de connexion par défaut pour les points produits et consommés est envoi individuel (unicast).

Tableau 29 – Connexions produites et consommées

Point	Description de la connexion
Produit	Un automate GuardLogix peut produire (envoyer) des points de sécurité à destination d'autres automates GuardLogix 1756 ou 1768. L'automate producteur utilise une connexion unique avec chaque consommateur.
Consommé	Les automates GuardLogix peuvent consommer (recevoir) des points de sécurité en provenance d'autres automates GuardLogix 1756 ou 1768. Chaque point consommé utilise une connexion.

Les points de sécurité produits et consommés sont soumis aux restrictions suivantes :

- seuls les points d'accès automate peuvent être partagés ;
- les points de sécurité produits et consommés sont limités à 128 octets ;
- les paires de points produits/consommés doivent utiliser le même type de données utilisateur ;
- le premier membre de ce type de données utilisateur doit être du type prédéfini CONNECTION_STATUS ;
- l'intervalle RPI du point de sécurité consommé doit correspondre à la période de la tâche de sécurité de l'automate GuardLogix producteur.

Pour configurer correctement des points de sécurité produits et consommés et partager des donnés entre les automates de sécurité homologues, vous devez correctement configurer les automates de sécurité homologues, produire un point de sécurité, et consommer un point de sécurité, en suivant la description ci-dessous.

Configuration des numéros de réseau de sécurité des automates de sécurité homologues

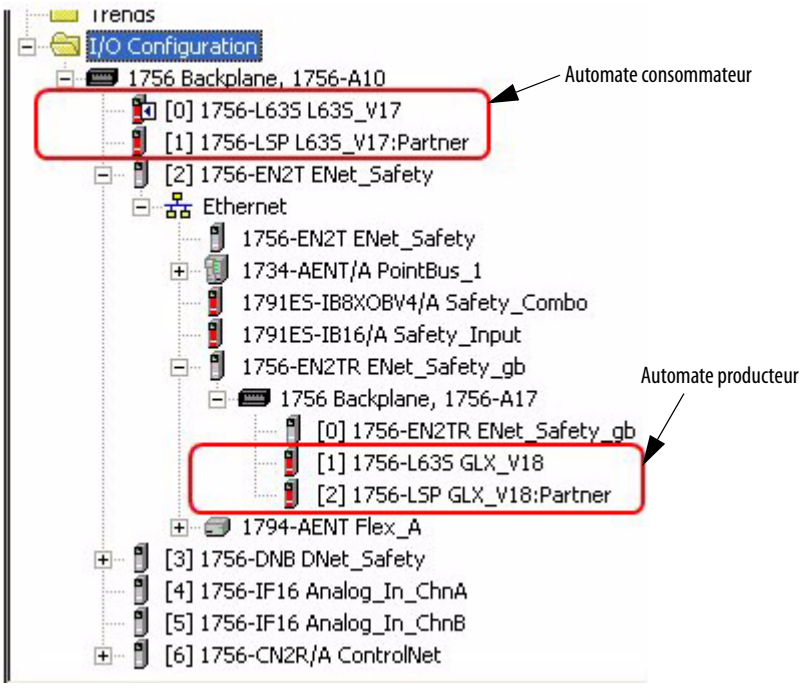
L'automate de sécurité homologue est assujetti aux mêmes caractéristiques de configuration que l'automate de sécurité local. L'automate de sécurité homologue doit également avoir un numéro SNN. Ce numéro SNN dépend de sa position dans le système.

Tableau 30 – SNN et position de l'automate

Emplacement de l'automate de sécurité homologue	SNN
Placé dans le châssis local	Les automates GuardLogix situés dans un même châssis doivent avoir le même numéro SNN.
Placé dans un autre châssis	L'automate doit avoir un numéro SNN spécifique.

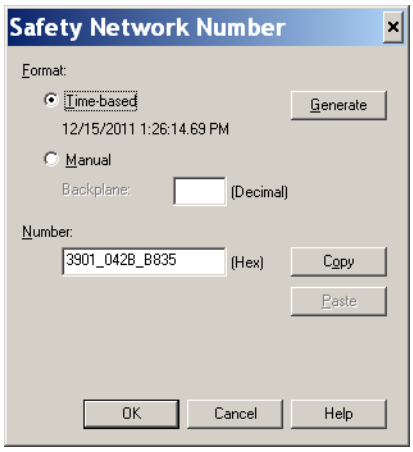
Suivez ces étapes pour copier et coller le SNN.

1. Ajoutez l'automate producteur à l'arborescence des E/S de l'automate consommateur.



2. Dans la fenêtre d'organisation de l'automate, cliquez sur l'automate concerné avec le bouton droit de la souris et sélectionnez Properties (Propriétés).
3. Copiez le SNN de l'automate producteur.

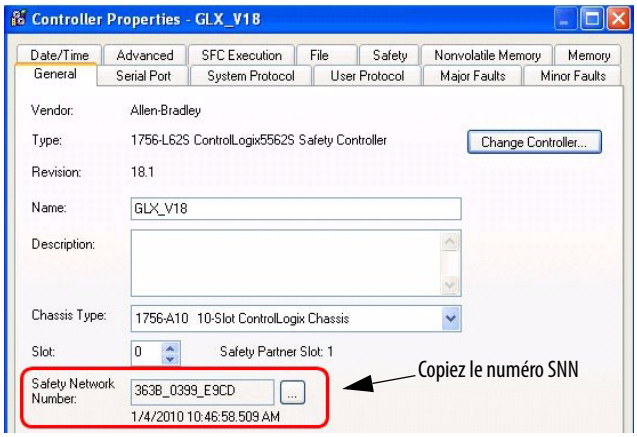
CONSEIL Vous pouvez copier et coller un numéro SNN à l'aide des boutons de la boîte de dialogue Safety Network Number (Numéro de réseau de sécurité). Ouvrez les boîtes de dialogue Safety Network Number respectives en cliquant sur le bouton ... situé à droite du champ SNN de la boîte de dialogue des propriétés.



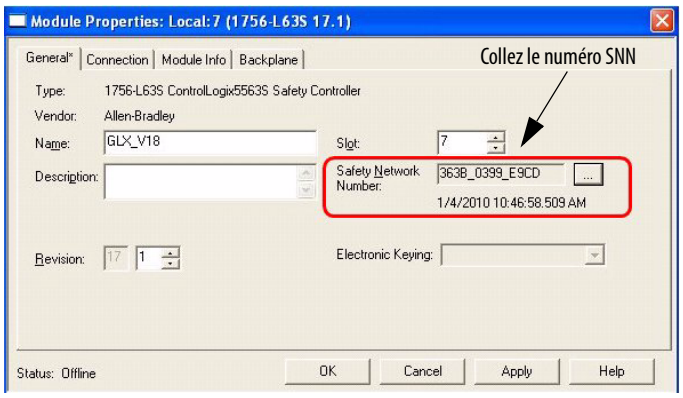
4. Dans la fenêtre d'organisation de l'automate, cliquez sur l'automate concerné avec le bouton droit de la souris et sélectionnez Properties (Propriétés).

5. Collez le numéro SNN de l'automate producteur dans le champ SNN.

Boîte de dialogue des propriétés de l'automate producteur dans le projet producteur



Boîte de dialogue des propriétés du module dans le projet consommateur



Production d'un point de sécurité

Pour permettre la production d'un point de sécurité procédez de la façon suivante.

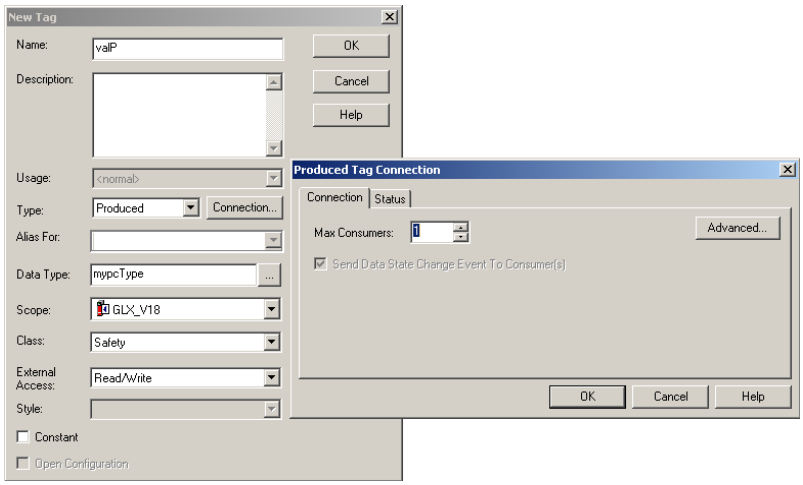
1. Dans le projet des automates producteurs, créez un type de données utilisateur pour définir la structure des données à produire.

   Vérifiez que le premier membre de données est bien du type CONNECTION_STATUS.

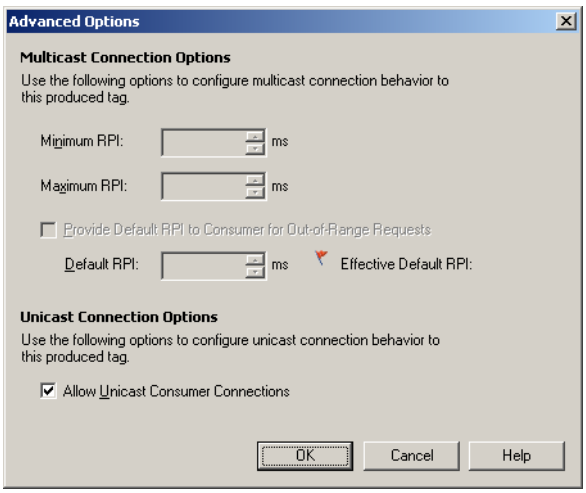
2. Cliquez avec le bouton droit sur Controller Tags (Points automate) et sélectionnez New Tag (Nouveau point).

3. Définissez le type comme Produced (Produit), la classe comme Safety (Sécurité) et le type de données (Data Type) comme le type utilisateur que vous avez créé à l'étape 1.

4. Cliquez sur Connection (Connexion) et entrez le nombre de consommateurs.



5. Cliqué sur Advanced (Avancé) si vous souhaitez modifier le type de connexion en désélectionnant « Allow Unicast Consumer Connections » (Autoriser les connexions consommateur en envoi individuel).



6. Cliquez sur OK.

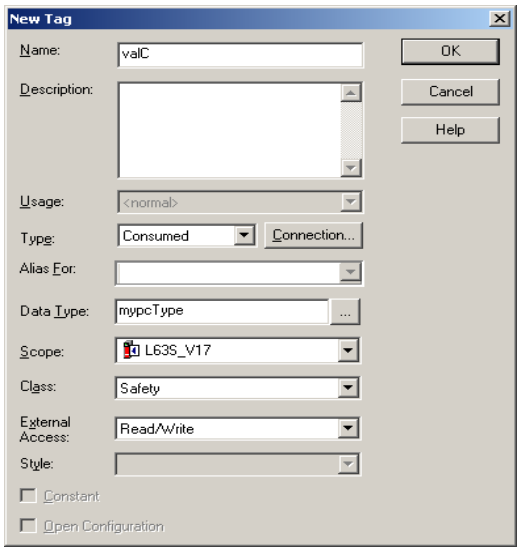
Consommation de points de données de sécurité

Pour autoriser la consommation de données produites par un autre automate, procédez de la façon suivante.

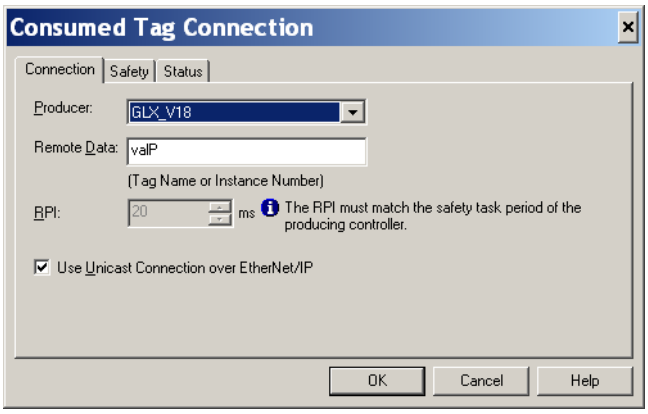
1. Dans le projet d'automate consommateur, créez un type de données utilisateur identique à celui créé dans le projet producteur.

   CONSEIL Le type de données utilisateur peut être copié à partir du projet producteur et collé dans le projet consommateur.

2. Cliquez avec le bouton droit sur Controller Tags (Points automate) et sélectionnez New Tag (Nouveau point).
3. Définissez le type comme Consumed (Consommé), la classe comme Safety (Sécurité) et le type de données (Data Type) comme étant le type de données utilisateur que vous avez créé à l'étape 1.



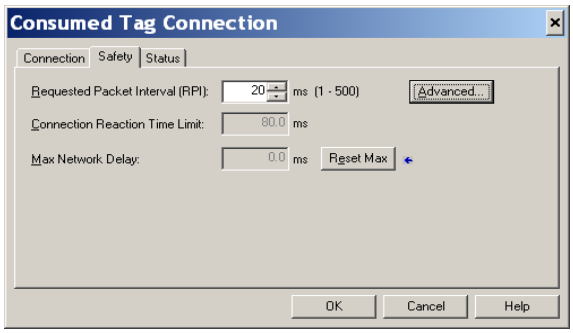
4. Cliquez sur Connection (Connexion) pour ouvrir la boîte de dialogue Consumed Tag Connection (Connexion de point consommé).



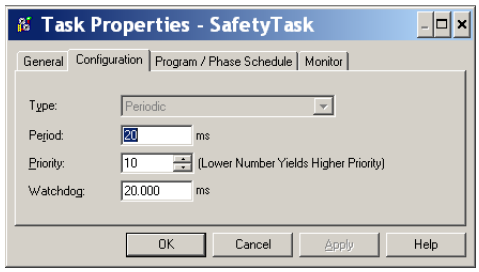
5. Sélectionnez l'automate producteur des données.
6. Entrez le nom du point produit.
7. Cliquez sur l'onglet Safety (Sécurité).
8. Saisissez l'intervalle entre trames requis (RPI) pour la connexion par incréments de 1 ms.

   La valeur par défaut est de 20 ms.

Projet consommateur



Projet producteur

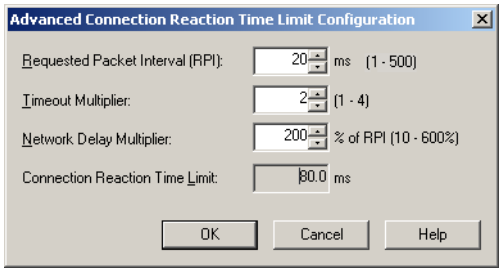


L'intervalle RPI indique la période de rafraîchissement des données sur une connexion. Le RPI du point de sécurité consommé doit correspondre à la période de la tâche de sécurité du projet de sécurité producteur.

La limite de temps de réponse d'une connexion correspond à la rémanence maximale des paquets de sécurité sur la connexion en question. Pour les contraintes de temps simples, il suffit généralement d'ajuster la valeur RPI pour obtenir une limite acceptable du temps de réponse de la connexion.

Le délai réseau maximum (Max Network Delay) est le délai de transport maximum observé entre la production des données et leur réception. Lorsque vous êtes en ligne, vous pouvez remettre à zéro ce délai réseau maximum en cliquant sur Reset Max.

9. Si la limite de temps de réponse de la connexion vous paraît acceptable, cliquez sur OK. Dans le cas d'une configuration plus complexe, utilisez le bouton Advanced (Avancé) pour accéder aux paramètres avancés de limite de temps de réponse de la connexion (Advanced Connection Reaction Time Limit).



Le multiplicateur de timeout (Timeout Multiplier) de la connexion définit la durée de réception maximum d'un paquet de données en nombre d'intervalles RPI, au terme de laquelle la connexion sera déclarée expirée.

Le multiplicateur de délai réseau (Network Delay Multiplier) définit le temps d'acheminement d'un message conformément aux exigences du protocole CIP Safety. Il indique le temps de transfert aller et retour entre le producteur et le consommateur. Vous pouvez utiliser le multiplicateur de délai réseau pour augmenter ou diminuer la limite du temps de réponse de la connexion.

Tableau 31 – Informations connexes

Ressource	Description
Pages 71…75	Fournit des informations supplémentaires sur le réglage du RPI ainsi que sur l'incidence du délai réseau maximum, du multiplicateur de timeout et du multiplicateur de délai réseau sur le temps de réponse de la connexion
Chapitre 9	Contient des Informations sur le type de donnée prédéfini CONNECTION_STATUS.
« Points produits et consommés des automates Logix5000 – Manuel de programmation », publication 1756-PM011	Fournit des informations détaillées sur l'utilisation de points produits et consommés

Mappage de points de sécurité

Un sous-programme de sécurité ne peut pas accéder directement à des points standard d'accès automate. Pour permettre l'utilisation de données de points standard dans des sous-programmes de la tâche de sécurité, les automates GuardLogix disposent d'une fonction de mise en correspondance de points de sécurité qui permet de copier des valeurs de point standard dans la mémoire de la tâche de sécurité.

Restrictions

Le mappage de points de sécurité est soumis aux restrictions suivantes :

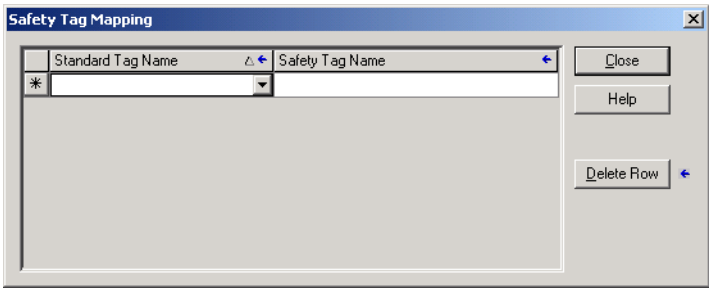
- la paire point de sécurité/point standard doit être en accès automate ;
- les types de données de la paire point de sécurité/point standard doivent correspondre ;
- les alias de points ne sont pas autorisés ;
- le mappage doit être applicable à l'ensemble du point. Par exemple, « myTimer.pre » ne sera pas autorisé si « myTimer » est un point de type TIMER ;
- une paire mappée est constituée d'un point standard mis en correspondance avec un point de sécurité ;
- vous ne pouvez pas mapper un point standard avec un point de sécurité défini comme constante ;
- vous ne pouvez pas modifier le mappage de points lorsque :
  - la sécurité du projet est verrouillée ;
  - il existe une signature de tâche de sécurité ;
  - le commutateur à clé de l'automate est en position RUN (Exécution) ;
  - une erreur de sécurité irrécupérable existe ;
  - le partenariat entre l'automate principal et son partenaire de sécurité est incorrect.

ATTENTION : Lorsque vous utilisez des données standard dans un sous-programme de sécurité, vous devez définir une procédure rigoureuse pour garantir que leur traitement soit effectué de manière conforme. L'utilisation de données standard dans un point de sécurité n'en fait pas des données de sécurité. Vous ne devez pas commander directement une sortie de sécurité SIL 3/PLe avec des données provenant d'un point standard.

Pour plus d'informations, reportez-vous à la publication 1756-RM093, « Systèmes automates GuardLogix – Manuel de référence sur la sécurité ».

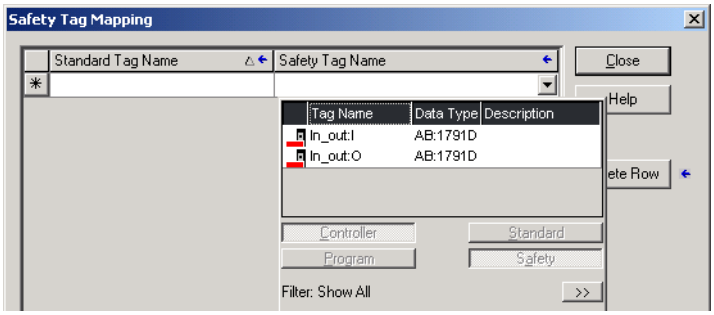
Création de paires de points mappées

1. Sélectionnez Map Safety Tags (Mapper des points de sécurité) dans le menu Logic (Programme) pour ouvrir la boîte de dialogue Safety Tag Mapping (Mappage d'un point de sécurité).



2. Ajoutez un point existant au Standard Tag Name (Nom de point standard) ou à la colonne Safety Tag Name (Nom de point de sécurité) en entrant le nom de point dans la cellule, ou en choisissant un point à partir du menu déroulant.

   Cliquez sur la flèche pour afficher la liste filtrée des points dans une boîte de dialogue d'explorateur de points. Dans la colonne Standard Tag Name (Nom des points standard), l'explorateur affiche uniquement les points standard en accès automate. Dans la colonne Safety Tag Name (Nom des points de sécurité), l'explorateur affiche les points de sécurité en accès automate.



3. Ajoutez un point existant à la colonne Standard Tag Name (Nom de point standard) ou Safety Tag Name (Nom de point de sécurité) en cliquant avec le bouton droit de la souris dans la cellule vide, en sélectionnant New Tag (Nouveau point) et en entrant le nom du point dans la cellule.
4. Cliquez dans la cellule avec le bouton droit de la souris et sélectionnez New tagname (Nouveau nom de point). Le nouveau nom de point sera celui que vous venez de saisir.

Surveillance de l'état du mappage des points

La colonne la plus à gauche de la boîte de dialogue Safety Tag Mapping (Mappage des points de sécurité) indique l'état des paires mappées.

Tableau 32 – Icônes d'état du mappage des points

Contenu de la cellule	Description
Vide	Le mappage de points est correct.
	Lorsque vous êtes hors ligne, l'icône X indique que le mappage des points est incorrect. Vous pouvez passer à une autre ligne ou fermer la boîte de dialogue Safety Tag Mapping.(1) En ligne, un adressage incorrect de point génère un message d'erreur expliquant pourquoi cet adressage n'est pas valable. Vous ne pouvez pas passer à une autre ligne ni fermer la boîte de dialogue Safety Tag Mapping tant que subsiste cette erreur de mappage.
	Indique la ligne actuellement sélectionnée.
	Indique la ligne de création d'une nouvelle paire mappée.
	Indique une modification en cours.

(1) Le mappage des points est également vérifié lors de la vérification du projet. Un mappage de points incorrect entraîne une erreur de vérification du projet.

Pour plus d'informations, reportez-vous aux restrictions de mappage des points, page 103.

Protection de l'application de sécurité

Vous pouvez protéger votre programme d'application de modifications non autorisées en verrouillant la sécurité sur l'automate puis en générant et en enregistrant une signature de tâche de sécurité.

Verrouillage de sécurité de l'automate

Il est possible de verrouiller la sécurité sur un automate GuardLogix de façon à empêcher toute modification des éléments de commande relatifs à la sécurité. La fonction de verrouillage de la sécurité ne s'applique qu'aux composants de sécurité, tels que la tâche de sécurité, les programmes et les sous-programmes de sécurité, les instructions complémentaires de sécurité, les points de sécurité, les E/S de sécurité et la signature de tâche de sécurité.

Lorsque la sécurité de l'automate est verrouillée, les actions suivantes ne sont pas autorisées sur la partie sécurité de l'application :

- programmation ou modifications en ligne et hors ligne (notamment des instructions complémentaires de sécurité) ;
- forçage des E/S de sécurité ;
- changement de l'état d'inhibition des E/S de sécurité ou des connexions produites ;
- manipulation des données de sécurité (sauf par un sous-programme de sécurité) ;
- génération ou suppression de la signature de tâche de sécurité.

CONSEIL Le texte du bouton d'état de la sécurité de la barre En ligne indique si la sécurité est verrouillée ou non.

La barre d'applications affiche également les icônes suivantes pour indiquer si les fonctions de sécurité sont verrouillées ou non sur l'automate de sécurité.

- = automate verrouillé
- = automate déverrouillé

Vous pouvez sécuriser le projet d'automate, que vous soyez en ligne ou non et que vous disposiez ou non de la source originale du programme. Des forçages de sécurité ou des modifications de sécurité en ligne ne doivent cependant pas être en cours.

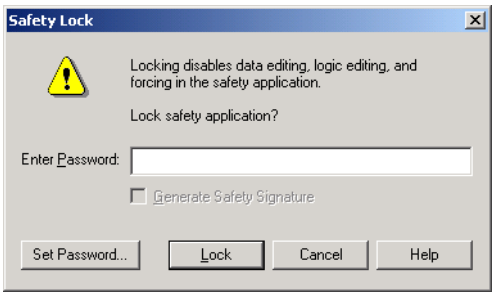
Vous ne pouvez pas verrouiller ou déverrouiller la sécurité lorsque le commutateur à clé est en position RUN (Exécution).

CONSEIL Les actions de verrouillage ou de déverrouillage de la sécurité sont enregistrées dans le journal de l'automate.

Pour plus d'informations sur la façon d'accéder au journal de l'automate, reportez-vous à la publication 1756-PM015, « Informations et états des automates Logix5000 – Manuel de programmation ».

Vous pouvez verrouiller ou déverrouiller la sécurité de l'automate soit depuis l'onglet Safety (Sécurité) de la boîte de dialogue Controller Properties (Propriétés de l'automate), soit en sélectionnant Tools>Safety>Safety Lock/Unlock (Outils > Sécurité > Verrouiller/Déverrouiller la sécurité).

Figure 26 – Verrouillage de la sécurité de l'automate



Si vous avez défini un mot de passe pour la fonction de verrouillage de la sécurité, vous devez le saisir dans le champ Enter Password (Entrer le mot de passe). Dans le cas contraire, cliquez sur Lock (Verrouiller).

Vous pouvez également définir ou modifier le mot de passe à partir de la boîte de dialogue Safety Lock (Verrouillage de la sécurité). Voir page 49.

La fonction de verrouillage de sécurité décrite dans la présente section, ainsi que les fonctions de sécurité standard de RSLogix, concernent les applications à base d'automate GuardLogix.

Pour plus d'informations sur les fonctions de sécurité de RSLogix 5000, reportez-vous à la publication 1756-PM016, « Logix5000 Controllers Security Programming Manual ».

Génération d'une signature de tâche de sécurité

Avant d'entreprendre les tests de vérification, vous devez générer la signature de tâche de sécurité. Vous ne pouvez générer cette signature de sécurité que lorsque l'automate GuardLogix est en ligne, en mode programmation, sécurité déverrouillée, sans forçage de sécurité, sans modifications de sécurité en ligne en attente et sans défaut de sécurité. L'indication d'état de la sécurité doit être Safety Task OK (Tâche de sécurité OK).

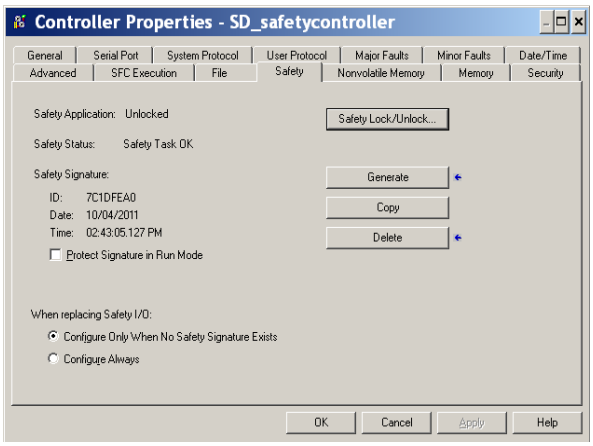
De plus, vous ne pouvez pas générer une signature de tâche de sécurité si l'automate est en mode Execution et la protection du mode exécution activée.

CONSEIL Vous pouvez visualiser l'état de la sécurité par l'intermédiaire du bouton situé sur la barre Online (En ligne) – voir page 126) – ou dans l'onglet Safety (Sécurité) de la boîte de dialogue Controller Properties (Propriétés de l'automate), comme indiqué page 107.

Vous pouvez générer la signature de tâche de sécurité à partir de l'onglet Safety (Sécurité) de la boîte de dialogue Controller Properties (Propriétés de l'automate) en cliquant sur le bouton Generate (Générer). Vous pouvez

également sélectionner Tools>Safety>Generate Signature (Outils>Sécurité>Générer la signature).

Figure 27 – Onglet Sécurité



Si une signature existe déjà, la confirmation de son remplacement vous est demandée.

CONSEIL La création et la suppression d'une signature de tâche de sécurité sont enregistrées dans le journal de l'automate.

Pour de plus amples informations sur la façon d'accéder au journal de l'automate, reportez-vous à la publication 1756-PM015, « Informations et états des automates Logix5000 Manuel de programmation ».

Lorsqu'une signature de tâche de sécurité est présente, les actions suivantes ne sont pas autorisées dans la partie sécurité de l'application :

- programmation ou modifications en ligne et hors ligne (notamment des instructions complémentaires de sécurité) ;
- forçage des E/S de sécurité ;
- changement de l'état d'inhibition des E/S de sécurité ou des automates producteurs ;
- manipulation des données de sécurité (sauf par un sous-programme de sécurité).

Copier la signature de tâche de sécurité

Vous pouvez utiliser le bouton Copy (Copier) pour créer un enregistrement de la signature de tâche de sécurité qui sera utilisable pour la documentation, la comparaison et la validation du projet de sécurité. Cliquez sur Copy (Copier) pour copier les composants d'identification, de date et d'heure dans le presse-papiers de Windows.

Supprimer la signature de tâche de sécurité

Cliquez sur Delete (Supprimer) pour effacer la signature de tâche de sécurité. La signature de tâche de sécurité ne peut pas être supprimée lorsque :

- la sécurité de l'automate est verrouillée ;
- l'automate est en mode Run (Exécution) avec le commutateur à clé dans la position RUN ;
- l'automate est en mode Run (Exécution) ou en mode Remote Run (Exécution à distance) et la protection en mode d'exécution est activée.

ATTENTION : Si vous supprimez la signature de tâche de sécurité, vous devrez tester et valider à nouveau la conformité SIL 3/PLe de votre système.

Pour de plus amples informations sur les impératifs SIL 3, reportez-vous à la publication 1756-RM093, « Systèmes automates GuardLogix – Manuel de référence sur la sécurité ».

Restrictions au niveau du logiciel

Des restrictions d'accès à certaines options de menu et fonctions (telles que Couper, Coller, Supprimer, Rechercher et Remplacer) sont imposées par le logiciel de programmation pour empêcher la modification des éléments de sécurité dans les situations suivantes :

- la sécurité de l'automate est verrouillée ;
- il existe une signature de sécurité ;
- il existe des défauts de sécurité ;
- l'état de la sécurité indique :
  - partenaire manquant ;
  - partenaire indisponible ;
  - matériel incompatible ;
  - firmware incompatible.

Si une seule de ces conditions est présente, vous ne pourrez pas :

- créer ou modifier des objets de sécurité, notamment les programmes, les sous-programmes, les points, les instructions complémentaires et les modules d'E/S de sécurité ;

IMPORTANT Les temps de scrutation de la tâche de sécurité ainsi que les programmes de sécurité peuvent être réinitialisés lorsque l'automate est en ligne.

- appliquer des forçages de points de sécurité ;
- créer de nouveaux mappages de point de sécurité ;
- modifier ou supprimer des mappages de points ;
- modifier ou supprimer des types de données utilisateur utilisés par des points de sécurité ;
- modifier le nom de l'automate, sa description, le type du châssis, l'emplacement, ainsi que le numéro de réseau de sécurité ;
- modifier ou supprimer la signature de tâche de sécurité lorsque la sécurité est verrouillée.

Mise en ligne de l'automate

Connexion de l'automate au réseau

Si ce n'est pas déjà fait, connectez l'automate au réseau.

Tableau 33 – Connexions de communication

Pour ce type de connexion	Utiliser…	Voir…
Série	câble 1756-CP3 ou 1747-CP3	Connexion au port série d'un automate 1756-L6xS, page 36
USB	câble USB 2.0	Connexion au port USB d'un automate 1756-L7xS, page 34
EtherNet/IP	Un module EtherNet/IP monté dans un logement libre dans le même châssis que l'automate	Connexion entre un périphérique EtherNet/IP et votre ordinateur, page 110
DeviceNet	Un module 1756-DNB monté dans un logement libre dans le même châssis que l'automate.	Connexion entre un module de communication ControlNet ou un scrutateur DeviceNet et votre ordinateur, page 110
ControlNet	Un module 1756-CN2 monté dans un logement libre dans le même châssis que l'automate	

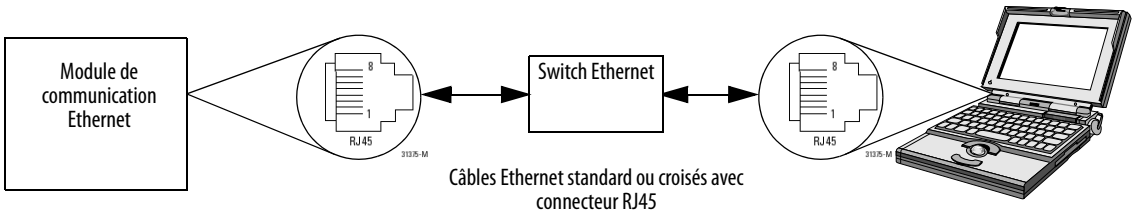
Connexion entre un périphérique EtherNet/IP et votre ordinateur

AVERTISSEMENT : si vous branchez ou débranchez le câble de communication avec le module ou tout autre périphérique du réseau sous tension, un arc électrique peut se produire, susceptible de provoquer une explosion dans les installations en environnement dangereux.

Assurez-vous que l'alimentation est coupée ou que l'environnement est classé non dangereux avant de poursuivre.

Raccordez votre dispositif EtherNet/IP au PC au moyen d'un câble Ethernet.

Figure 28 – Connexions Ethernet



Connexion entre un module de communication ControlNet ou un scrutateur DeviceNet et votre ordinateur

Pour accéder à un réseau ControlNet ou DeviceNet , vous pouvez procéder de l'une des deux manières suivantes :

- vous connecter directement au réseau ;
- vous connecter à un réseau série ou EtherNet/IP et naviguer (par passerelle) jusqu'au réseau souhaité. Cette procédure ne nécessite pas de programmation supplémentaire.

Configuration d'un driver EtherNet/IP, ControlNet ou DeviceNet

Pour plus d'informations sur la configuration d'un driver, veuillez vous reporter à la publication appropriée :

- « EtherNet/IP Modules in Logix5000 Control Systems », Publication ENET-UM001
- « ControlNet Modules in Logix5000 Control Systems User Manual », Publication CNET-UM001
- « DeviceNet Modules in Logix5000 Control Systems », Publication DNET-UM004

Compréhension des facteurs affectant la mise en ligne

Le logiciel RSLogix 5000 détermine si une liaison peut être établie avec l'automate cible en s'assurant que le projet hors ligne est nouveau ou qu'il a été modifié. Si le projet est nouveau, vous devez d'abord le télécharger dans l'automate. S'il a été modifié, un message d'invite vous demandera de le transférer ou le télécharger. Si aucune modification n'a été apportée, vous pouvez vous mettre directement en ligne avec l'automate pour surveiller l'exécution du projet.

Un certain nombre de facteurs peuvent néanmoins influer sur ces processus. C'est notamment le cas de la fonction Project to Controller Match (Correspondance projet/automate), de l'état et des défauts de sécurité, de la présence d'une signature de tâche de sécurité ainsi que de l'état du verrouillage de la sécurité du projet et de l'automate.

Correspondance Projet/Automate

La fonction de Project to Controller Match (Correspondance projet/automate) concerne les processus de téléchargement, de transfert et de mise en ligne de projets standard et de sécurité.

Si la fonction « Project to Controller Match » (Correspondance projet/automate) a été activée dans le projet hors ligne, le logiciel RSLogix 5000 comparera le numéro de série de l'automate enregistré dans ce projet hors ligne à celui de l'automate connecté. S'ils ne correspondent pas, vous devrez annuler le téléchargement ou le transfert ou vous connecter au bon automate. À moins que vous ne confirmiez que vous êtes bien connecté à l'automate approprié. Ceci mettra à jour le numéro de série dans le projet afin qu'il corresponde à celui de l'automate cible.

Correspondance de la révision du firmware

La correspondance de révision du firmware a une incidence sur le processus de téléchargement. Si la révision de l'automate ne correspond pas à celle enregistrée dans le projet, un message vous invite à mettre à jour le firmware de l'automate. Le logiciel RSLogix 5000 vous permet d'effectuer cette mise à jour au cours de la séquence de téléchargement.

IMPORTANT Pour mettre à jour le firmware de l'automate, commencez par installer un kit de mise à niveau du firmware. Ce kit de mise à niveau est fourni sur un CD-ROM supplémentaire avec le logiciel RSLogix 5000.

CONSEIL Vous pouvez également mettre à jour le firmware en sélectionnant l'utilitaire ControlFLASH™ dans le menu Tools (Outils) du logiciel RSLogix 5000.

État et défauts de la sécurité

Le transfert du programme logique et la mise en ligne sont autorisés quel que soit l'état de la sécurité. L'état et les défauts de sécurité affectent uniquement le processus de téléchargement.

Vous pouvez visualiser l'état de la sécurité dans l'onglet Safety (Sécurité) de la boîte de dialogue Controller Properties (Propriétés de l'automate).

Signature de tâche de sécurité et état du verrouillage de la sécurité

La présence d'une signature de tâche de sécurité et l'état du verrouillage de la sécurité de l'automate affectent les processus de transfert et de téléchargement.

Lors d'un transfert

Si l'automate possède une signature de tâche de sécurité, celle-ci ainsi que l'état du verrouillage de cette tâche de sécurité sont transférés avec le projet. Par exemple, si la sécurité du projet est déverrouillée au niveau de l'automate, la sécurité du projet hors ligne reste déverrouillée à la suite du transfert, même si elle était verrouillée avant le transfert.

Au terme du transfert, la signature de tâche de sécurité du projet hors ligne correspondra à celle de l'automate.

Lors d'un téléchargement

La présence d'une signature de tâche de sécurité ainsi que l'état du verrouillage de la sécurité de l'automate déterminent si le téléchargement peut être effectué ou non.

Tableau 34 – Effets du verrouillage de la sécurité et de la signature de tâche de sécurité sur l'exécution du chargement

État du verrouillage de la sécurité	État de la signature de tâche de sécurité	Fonctionnalité du chargement
Automate déverrouillé	La signature de tâche de sécurité dans le projet hors ligne correspond à celle de l'automate.	Tous les composants de projet standard sont chargés. Les points de sécurité sont réinitialisés sur les valeurs qu'ils avaient à la création de la signature de tâche de sécurité. La tâche de sécurité n'est pas chargée. L'état du verrouillage de la sécurité est aligné sur celui du projet hors ligne.
	Les signatures de tâche de sécurité ne correspondent pas.	Si l'automate avait une signature de tâche de sécurité, elle est automatiquement supprimée et le projet est entièrement chargé. L'état du verrouillage de la sécurité est aligné sur celui du projet hors ligne.
Automate verrouillé	Les signatures de tâche de sécurité correspondent.	Si la sécurité est verrouillée dans le projet hors ligne et dans l'automate, tous les composants de projet standard sont chargés et la tâche de sécurité est réinitialisée sur les valeurs qu'elle avait à la création de la signature de tâche de sécurité. Si la sécurité est déverrouillée dans le projet hors ligne mais qu'elle est verrouillée dans l'automate, le chargement est bloqué. Vous devrez d'abord déverrouiller l'automate pour permettre son exécution.
	Les signatures de tâche de sécurité ne correspondent pas.	Vous devez d'abord déverrouiller l'automate pour permettre le chargement. Si l'automate avait une signature de tâche de sécurité, elle est automatiquement supprimée et le projet est entièrement chargé. L'état du verrouillage de la sécurité est aligné sur celui du projet hors ligne.

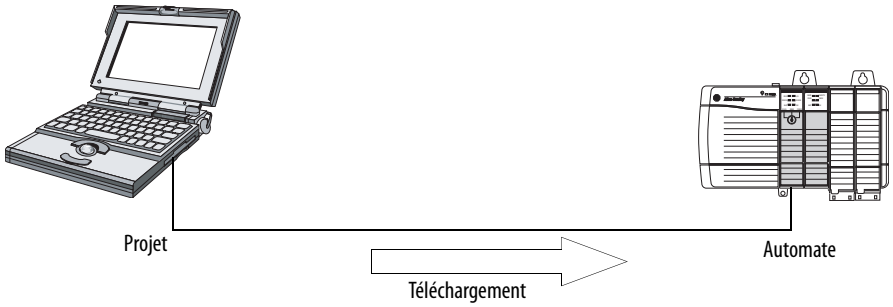
IMPORTANT Lors d'un téléchargement vers un automate dont la sécurité est déverrouillée, si le firmware de l'automate est différent de celui enregistré dans le projet hors ligne, vous pouvez soit :

- mettre à jour l'automate afin qu'il corresponde avec celui enregistré dans le projet hors ligne. Une fois cette mise à jour terminée, le projet sera chargé entièrement ;
- mettre à jour le projet en fonction de la version de l'automate.

Si vous mettez à jour le projet, la signature de tâche de sécurité sera effacée et il sera nécessaire de revalider le système.

Téléchargement

Procédez de la façon suivante pour transférer votre projet de l'ordinateur vers l'automate.



1. Tournez le commutateur à clé de l'automate sur REM.
2. Ouvrez le projet RSLogix 5000 à télécharger.
3. Spécifiez le chemin vers l'automate.
   a. Cliquez sur le bouton Who Active (Qui est actif)  .
   b. Sélectionnez l'automate.
   Pour développer un niveau, cliquez sur le signe +. Si un automate est déjà sélectionné, assurez-vous qu'il s'agit bien de celui que vous souhaitez.
4. Cliquez sur Download (Télécharger).

   Le logiciel compare les informations suivantes entre le projet hors ligne et la mémoire de l'automate :
   - le numéro de série de l'automate (si la fonction Project to Controller Match – correspondance Projet/Automate – est sélectionnée) ;
   - les révisions majeures et mineures du firmware ;
   - l'état de la sécurité ;
   - la signature de tâche de sécurité (s'il y en a une) ;
   - l'état du verrouillage de la sécurité.

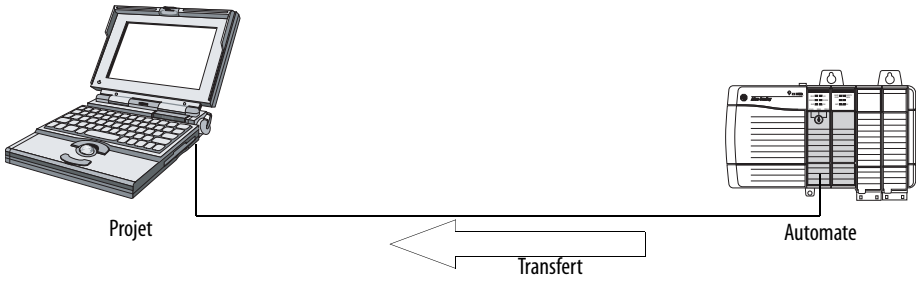
5. Suivez les instructions figurant dans le tableau ci-dessous selon le message retourné par le logiciel pour effectuer le téléchargement.

Si le logiciel indique	Alors
Download to the controller (Télécharger sur l'automate).	Sélectionnez Download (Télécharger). Le projet est téléchargé dans l'automate et le logiciel RSLogix 5000 se met en ligne.
Unable to download to the controller (Impossible de télécharger sur l'automate). Mismatch between the offline project and the controller serial number (Discordance entre le numéro de série du projet hors ligne et celui de l'automate). Selected controller may be the wrong controller (L'automate sélectionné n'est peut-être pas le bon).	Connectez-vous au bon automate ou vérifiez qu'il s'agit bien de l'automate approprié. Si c'est le cas, cochez la case Update project serial number (Mettre à jour le numéro de série du projet) pour permettre le téléchargement. Le numéro de série du projet sera alors modifié de façon à correspondre à celui de l'automate.
Unable to download to the controller (Impossible de télécharger sur l'automate). The major revision of the offline project and the controller's firmware are not compatible (Le numéro de révision majeure enregistré dans le projet hors ligne n'est pas compatible avec celui du firmware de l'automate).	Sélectionnez Update Firmware (Mettre à jour le firmware). Choisissez la version correcte puis cliquez sur Update (Mettre à jour). Cliquez sur Yes (Oui) pour confirmer votre choix.
Unable to download to controller (Impossible de télécharger sur l'automate). The safety partner is missing or unavailable (Le partenaire de sécurité est absent ou indisponible).	Annulez le processus de téléchargement. Installez un partenaire de sécurité compatible avant de tenter à nouveau l'opération.
Unable to download to controller (Impossible de télécharger sur l'automate). The firmware revision of the safety partner is not compatible with the primary controller (La version de firmware du partenaire de sécurité n'est pas compatible avec celle de l'automate principal).	Mettez à jour la version du firmware du partenaire de sécurité. Sélectionnez Update Firmware (Mettre à jour le firmware). Choisissez la version correcte puis cliquez sur Update (Mettre à jour). Cliquez sur Yes (Oui) pour confirmer votre choix.
Unable to download to controller (Impossible de télécharger sur l'automate). Safety partnership has not been established (Le partenariat de sécurité n'est pas établi).	Annulez le processus de chargement en cours puis relancez-le.
Unable to download to controller (Impossible de télécharger sur l'automate). Incompatible safety task signature cannot be deleted while the project is safety-locked (La signature de tâche de sécurité non conforme ne peut pas être supprimée tant que la sécurité du projet est verrouillée).	Annulez le téléchargement. Pour pouvoir télécharger le projet, vous devez préalablement déverrouiller la sécurité du projet hors ligne et effacer sa signature de tâche de sécurité. **IMPORTANT :** le système de sécurité devra être revalidé.
Cannot download in a manner that preserves the safety task signature (Impossible de procéder au téléchargement en préservant la signature de tâche de sécurité). Controller's firmware minor revision is not compatible with safety task signature in offline project (Le numéro de révision mineure du firmware de l'automate n'est pas compatible avec celui de la signature de la tâche de sécurité dans le projet hors ligne).	• En cas d'incompatibilité d'une révision mineure du firmware, mettez à jour celui-ci dans l'automate afin qu'il corresponde exactement à la révision enregistrée dans le projet hors ligne. Cela permettra de préserver la signature de tâche de sécurité existante. Téléchargez ensuite le projet hors ligne. • Pour procéder au téléchargement malgré l'incompatibilité, cliquez sur Download (Télécharger). La signature de la tâche de sécurité est effacée. **IMPORTANT :** le système de sécurité devra être revalidé.
Unable to download to controller (Impossible de télécharger sur l'automate). Controller is locked (L'automate est verrouillé). Controller and offline project safety task signatures do not match (La signature de la tâche de sécurité de l'automate ne correspond pas avec celle du projet hors ligne).	Sélectionnez Unlock (Déverrouiller). La boîte de dialogue Safety Unlock for Download (Déverrouiller la sécurité pour le téléchargement) apparaît. Si la case Delete Signature (Supprimer la signature) est cochée et si vous choisissez Unlock (Déverrouiller), vous devrez cliquer sur Yes (Oui) pour confirmer cette suppression.
A nonrecoverable safety fault will occur in the safety controller (Un défaut de sécurité non récupérable va se produire dans l'automate de sécurité). No designated coordinated system time (CST) master exists (Il n'y a pas d'horloge maître définie pour la coordination du temps système).	Cochez Enable Time Synchronization (Activer la synchronisation temporelle) et cliquez sur Download (Télécharger) pour poursuivre l'opération.

Une fois le projet téléchargé avec succès, l'état du verrouillage de la sécurité et la signature de tâche de sécurité de l'automate seront les mêmes que ceux du projet importé. Les données de sécurité seront réinitialisées sur les valeurs qu'elles avaient à la création de la signature de tâche de sécurité.

Transfert

Suivez la procédure ci-dessous pour transférer un projet depuis l'automate vers votre ordinateur.



1. Spécifiez le chemin vers l'automate.
   a. Cliquez sur le bouton Who Active (Qui est actif)  .
   b. Sélectionnez l'automate.
   Pour développer un niveau, cliquez sur le signe +. Si un automate est déjà sélectionné, assurez-vous qu'il s'agit bien de celui que vous souhaitez.
2. Cliquez sur Upload (Transférer).
3. Si le fichier projet n'existe pas, sélectionnez File>Select>Yes (Fichier>Sélectionner>Oui).
4. Si le fichier projet existe déjà, sélectionnez-le.

   Si la fonction Project to Controller Match (Correspondance Projet/Automate) est sélectionnée, le logiciel RSLogix 5000 vérifie si le numéro de série du projet ouvert correspond à celui de l'automate.

   Si les numéros de série de l'automate ne correspondent pas, vous pouvez procéder de l'une des manières suivante :
   - annuler le transfert et vous connecter à un automate qui correspond. La procédure de transfert pourra alors être relancée ;
   - sélectionner un nouveau projet à transférer ou choisir un autre projet avec Select File (Sélectionner un fichier) ;
   - mettre à jour le numéro de série du projet afin qu'il corresponde à celui de l'automate. Cocher pour cela la case Update Project Serial Number (Mettre à jour le numéro de série du projet) avant de sélectionner Upload (Transférer).
5. Le logiciel vérifie si le projet ouvert correspond bien à celui de l'automate.
   a. Si ces projets ne correspondent pas, vous devrez sélectionner un fichier approprié ou annuler le transfert.
   b. Si les projets correspondent, le logiciel recherchera les éventuelles variations existant dans le projet hors ligne (ouvert).

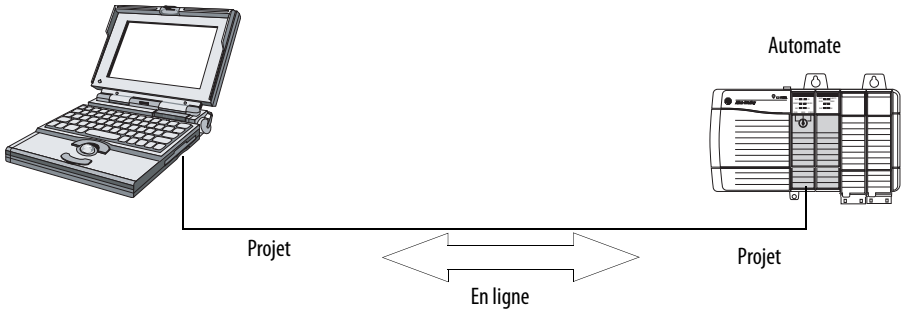
6. Le logiciel recherche les éventuelles modifications du projet hors ligne.
   a. En l'absence de modifications apportées au projet hors ligne, vous pourrez passer en ligne sans effectuer de transfert. Cliquez sur Go Online (Passer en ligne).
   b. Si le projet ouvert comporte des modifications non retranscrites dans l'automate, vous pouvez choisir de transférer ce projet, d'annuler le transfert ou de sélectionner un autre fichier.

   Si vous choisissez Upload (Transférer), les applications standard et de sécurité seront transférées. S'il existe une signature de tâche de sécurité, elle sera également transférée. L'état du verrouillage de la sécurité du projet correspondra à l'état d'origine du projet en ligne (de l'automate).

   CONSEIL Si, préalablement au transfert, il existe une signature de tâche de sécurité hors ligne ou si la sécurité du projet hors ligne est verrouillée alors qu'elle est déverrouillé sur l'automate, ou encore si ce dernier ne possède pas de signature de tâche de sécurité, la signature de tâche de sécurité et l'état du verrouillage de la sécurité enregistrés dans le projet hors ligne seront alors remplacés par les valeurs utilisées en ligne (sécurité déverrouillée et pas de signature de tâche de sécurité). Si vous ne souhaitez pas que ces modifications deviennent définitives, n'enregistrez pas le projet hors ligne après le transfert.

Passer en ligne

Suivez la procédure ci-dessous pour vous mettre en ligne avec l'automate afin de surveiller l'exécution du projet.



1. Spécifiez le chemin vers l'automate.
   a. Cliquez sur le bouton Who Active (Qui est actif)  .
   b. Sélectionnez l'automate.
      Pour développer un niveau, cliquez sur le signe +. Si un automate est déjà sélectionné, assurez-vous qu'il s'agit bien de celui que vous souhaitez.
2. Cliquez sur Go Online (Passer en ligne).

   Le logiciel vérifie si :
   - le numéro de série du projet hors ligne correspond à celui de l'automate (si la fonction Project to Controller Match – Correspondance Projet/Automate – a été sélectionnée) ;
   - le projet hors ligne comporte des modifications par rapport à celui de l'automate ;

- les révisions du firmware indiquées dans le projet hors ligne correspondent à celles de l'automate ;
- la sécurité dans le projet hors ligne ou l'automate est verrouillée ;
- le projet hors ligne et l'automate ont une signature de tâche de sécurité compatible.

3. Suivez les instructions figurant dans le tableau ci-dessous pour vous connecter à l'automate.

Tableau 35 – Connexion à l'automate

Si le logiciel indique	Alors
Unable to connect to controller (Impossible de se connecter à l'automate). Mismatch between the offline project and the controller serial number (Discordance entre le numéro de série du projet hors ligne et celui de l'automate). Selected controller may be the wrong controller (L'automate sélectionné n'est peut-être pas le bon).	Connectez-vous au bon automate, sélectionnez un autre fichier projet ou cochez la case Update project serial number (Mettre à jour le numéro de série du projet), puis sélectionnez Go Online (Passer en ligne) pour vous connecter à l'automate et mettre à jour le numéro de série du projet hors ligne de façon à ce qu'il corresponde à celui de l'automate.
Unable to connect to controller (Impossible de se connecter à l'automate). The revision of the offline project and the controller's firmware are not compatible (Le numéro de révision du projet hors ligne et celui du firmware de l'automate ne sont pas compatibles).	Choisissez l'une des options suivantes : • Sélectionnez Update Firmware (Mettre à jour le firmware). Choisissez la version correcte puis cliquez sur Update (Mettre à jour). Cliquez sur Yes (Oui) pour confirmer votre choix. **IMPORTANT :** le projet en ligne sera supprimé. • Pour préserver le projet en ligne, annulez le processus de mise en ligne et installez une version du logiciel RSLogix 5000 compatible avec la révision du firmware de votre automate.
You need to upload or download to go online by using the open project (Vous devez choisir d'effectuer un transfert ou un téléchargement pour passer en ligne en utilisant le projet ouvert).	Choisissez l'une des options suivantes : • Effectuez un transfert pour mettre à jour le projet hors ligne. • Effectuez un téléchargement pour mettre à jour le projet de l'automate. • Sélectionnez un autre projet hors ligne dans File (Fichier).
Unable to connect in a manner that preserves safety task signature (Impossible de se connecter en préservant la signature de la tâche de sécurité). Controller's firmware minor revision is not compatible with safety task signature in offline project (Le numéro de révision mineure du firmware de l'automate n'est pas compatible avec celui de la signature de la tâche de sécurité dans le projet hors ligne).	• Pour préserver la signature de tâche de sécurité en cas d'incompatibilité d'une révision mineure de firmware, mettez à jour le firmware de l'automate afin que son numéro de révision corresponde exactement à celui du projet hors ligne. Passez ensuite en ligne avec l'automate. • Pour procéder au téléchargement malgré l'incompatibilité, cliquez sur Download (Télécharger). La signature de la tâche de sécurité est effacée. **IMPORTANT :** le système de sécurité devra être revalidé.
Unable to connect to controller (Impossible de se connecter à l'automate). Incompatible safety task signature cannot be deleted while project is safety-locked (La signature de tâche de sécurité non conforme ne peut pas être supprimée tant que la sécurité du projet est verrouillée).	Annulez le processus de mise en ligne. Vous devrez déverrouiller la sécurité du projet hors ligne avant de tenter à nouveau l'opération.

Lorsque l'automate et le logiciel RSLogix 5000 sont en ligne, l'état du verrouillage de la sécurité et la signature de tâche de sécurité de l'automate correspondent à ceux du projet de l'automate. L'état du verrouillage de la sécurité et la signature de tâche de sécurité du projet hors ligne sont remplacés par ceux de l'automate. Si vous ne souhaitez pas que les modifications apportées au projet hors ligne deviennent définitives, n'enregistrez pas le fichier projet après le passage en ligne.

Notes :

Stockage et chargement des projets dans la mémoire non volatile

Utilisation des cartes mémoires comme mémoire non volatile

À partir de leur version 18, les automates GuardLogix, acceptent une carte de mémoire non volatile. La mémoire non volatile vous permet de conserver une copie de votre projet dans l'automate. L'automate n'a pas besoin d'alimentation ou de pile pour conserver cette copie.

Vous pouvez recharger dans la mémoire d'application de l'automate le projet sauvegardé dans sa mémoire non volatile :

- à chaque mise sous tension ;
- chaque fois qu'il n'y a pas de projet dans l'automate lors de la mise sous tension ;
- à n'importe quel moment au moyen du logiciel RSLogix 5000.

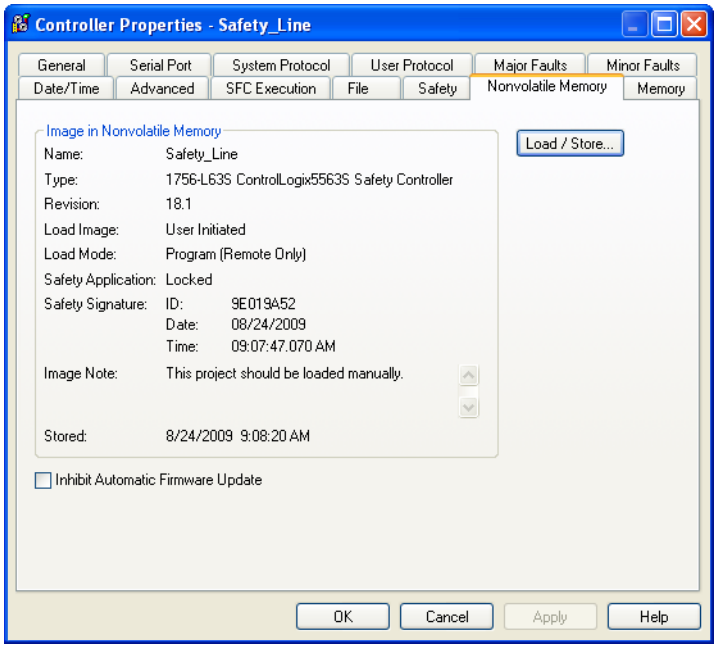
IMPORTANT La mémoire non volatile enregistre le contenu de la mémoire utilisateur au moment où vous sauvegardez le projet :

- Les modifications effectuées après cet enregistrement du projet ne seront pas retranscrites dans la mémoire non volatile.
- Si vous apportez des modifications au projet mais que vous ne les sauvegardez pas, elles seront écrasées lorsque vous rechargerez le projet à partir de la mémoire non volatile. Si cela se produit, vous devrez transférer ou télécharger le projet pour passer en ligne.
- Si vous voulez conserver des changements tels que des modifications en ligne, des valeurs de points ou une planification de réseau ControlNet, sauvegardez à nouveau le projet après avoir effectué ces changements.

Si une carte mémoire est installée, vous pouvez visualiser son contenu dans l'onglet Nonvolatile Memory (Mémoire non volatile) de la boîte de dialogue Controller Properties (Propriétés de l'automate). Si une application de sécurité est enregistrée sur cette carte, l'état du verrouillage de la sécurité et la signature de tâche de sécurité sont indiqués.

ATTENTION : ne retirez pas la carte mémoire quand l'automate effectue une opération de lecture ou d'écriture sur cette carte, comme l'indique le clignotement en vert du voyant d'état OK . Cela pourrait corrompre les données présentes sur la carte ou dans l'automate, ainsi que corrompre le firmware le plus récent dans l'automate. Laissez la carte dans l'automate jusqu'à ce que le voyant d'état OK passe au vert fixe.

Figure 29 – Onglet Mémoire non volatile



Pour de plus amples informations sur l'utilisation de la mémoire non volatile, reportez-vous à la publication 1756-PM017, « Logix5000 Controllers Nonvolatile Memory Programming Manual ».

Enregistrement d'un projet de sécurité

Vous ne pouvez pas enregistrer un projet de sécurité si l'état de la tâche de sécurité indique Safety Task Inoperable (Tâche de sécurité inexploitable). Lorsque vous enregistrez un projet de sécurité, le firmware de l'automate principal et celui de son partenaire de sécurité sont enregistrés sur la carte mémoire.

Si aucune application n'est présente dans l'automate, vous ne pourrez sauvegarder que le firmware de l'automate de sécurité, à condition qu'un partenariat valable soit établi. Le chargement du firmware seul n'annule pas une condition Safety Task Inoperable (Tâche de sécurité inexploitable) pré-existante.

Si une signature de tâche de sécurité existe lorsque vous enregistrez un projet, les opérations suivantes se produisent :

- les points de sécurité sont enregistrés avec la valeur qu'ils avaient à la création de la signature de sécurité ;
- les points standard sont mis à jour ;
- la signature de tâche de sécurité actuelle est sauvegardée.

Lorsque vous sauvegardez le projet d'une application de sécurité sur une carte mémoire, il est recommandé de choisir Program (Remote Only) (Programmation – à distance seulement) pour le mode de chargement (Load mode), c'est-à-dire le mode de fonctionnement dans lequel repassera l'automate au terme du chargement.

Chargement d'un projet de sécurité

Vous ne pouvez lancer le chargement depuis la mémoire non volatile que dans les conditions suivantes :

- le type d'automate défini dans le projet enregistré dans la mémoire non volatile correspond à celui de l'automate cible ;
- les révisions majeures et mineures du projet enregistré dans la mémoire non volatile correspondent à celles de l'automate cible ;
- l'automate ne se trouve pas en mode RUN (Exécution).

Vous disposez de plusieurs options (en fonction des circonstances) pour charger un projet dans la mémoire utilisateur de l'automate.

Tableau 36 – Options pour le chargement d'un projet

Si vous souhaitez charger ce projet	Alors sélectionnez cette option de chargement d'image	Remarques
Chaque fois que vous mettez ou remettez sous tension	On Power Up (À la mise sous tension)	• Lors d'un remise sous tension, vous perdrez toutes les modifications effectuées en ligne ainsi que les valeurs de point et les planification réseau qui n'auront pas été sauvegardées dans la mémoire non volatile. • L'automate charge le projet et le firmware enregistrés à chaque remise sous tension, quel que soit le firmware ou l'application contenu dans l'automate. Ce chargement est effectué que la sécurité de l'automate soit verrouillée ou non ou qu'il possède une signature de tâche de sécurité ou non. • Vous pouvez toujours utiliser le logiciel RSLogix 5000 pour charger le projet.
Lorsqu'il n'y a pas de projet dans l'automate et que vous mettez ou remettez le châssis sous tension.	On Corrupt Memory (Sur corruption de la mémoire)	• Par exemple, si la pile est déchargée et que l'alimentation de l'automate est coupée, le projet est effacé de la mémoire. Quand l'alimentation est rétablie, cette option recharge le projet dans l'automate. • Le système met à jour le firmware de l'automate principal ou celui du partenaire de sécurité, le cas échéant. L'application enregistrée dans la mémoire non volatile est également chargée et l'automate se met dans le mode sélectionné, Programmation (PROG) ou Exécution (RUN). • Vous pouvez toujours utiliser le logiciel RSLogix 5000 pour charger le projet.
Uniquement avec le logiciel RSLogix 5000	User Initiated (À l'initiative de l'utilisateur)	• Si le type d'automate, ainsi que les révisions majeure et mineure du projet présentes dans la mémoire non volatile correspondent à ceux de l'automate cible, vous pouvez lancer le chargement quel que soit l'état de la tâche de sécurité. • Le chargement sur un automate dont la sécurité est verrouillée n'est autorisé que lorsque la signature de tâche de sécurité du projet enregistré dans la mémoire non volatile correspond à celle du projet actif dans l'automate. • Si les signatures ne correspondent pas ou si la sécurité de l'automate est verrouillée mais qu'il n'existe pas de signature de tâche de sécurité, vous êtes invité à déverrouiller préalablement l'automate. **IMPORTANT :** quand vous déverrouillez l'automate et que vous lancez le chargement du projet depuis la mémoire non volatile, l'état du verrouillage de sécurité, les mots de passe et la signature de tâche de sécurité se trouveront définis sur les valeurs enregistrées dans cette mémoire au terme de l'opération. • Si le numéro de révision du firmware de l'automate principal correspond bien à celui enregistré dans la mémoire non volatile, seul le firmware du partenaire de sécurité sera mis à jour lorsque nécessaire. L'application enregistrée dans la mémoire non volatile sera chargée de façon à ce que l'état de la tâche de sécurité repasse sur Safety Task Operable (Tâche de sécurité opérationnelle). L'automate basculera alors dans le mode de fonctionnement sélectionné, programmation (Program) ou exécution (Run).

IMPORTANT Avant d'utiliser le logiciel ControlFLASH, assurez-vous que la carte SD est déverrouillée si elle est paramétrée pour le transfert à la mise sous tension. Sinon les données mises à jour seront écrasées par le firmware sur la carte mémoire.

Utilisation de modules de stockage d'énergie (automates 1756-L7*x*S uniquement)

Vous pouvez utiliser des modules ESM GuardLogix pour réaliser les opérations suivantes :

- Fournir l'alimentation nécessaire aux automates 1756-L7*x*S pour sauvegarder leur programme dans leur mémoire de stockage non volatile (NVS) intégrée en cas de coupure de l'alimentation du châssis ou lorsque l'automate est retiré d'un châssis sous tension ;

IMPORTANT	Lorsque vous utilisez le module ESM pour sauvegarder le programme dans la mémoire NVS intégrée, vous ne pouvez **pas** sauvegarder ce programme sur la carte SD installée dans l'automate.

- Effacer le programme de la mémoire NVS intégrée aux automates 1756-L7*x*S. Pour plus d'information, voir Effacement du programme de la mémoire NVS intégrée

Le tableau suivant décrit les différents modèles de module ESM.

Tableau 37 – Modules de stockage d'énergie

Référence	Description
1756-ESMCAP(XT)	Module ESM à condensateur Les automates 1756-L7*x*S sont livrés avec ce module ESM monté.
1756-ESMNSE(XT)	Module ESM à condensateur sans sauvegarde de l'horloge Utilisez ce module ESM lorsque votre application nécessite que le module de stockage d'énergie en place puisse se vider de l'énergie résiduelle qu'il contient jusqu'en dessous d'un seuil de 200 µJ avant de pouvoir être transporté dans ou hors de cette application. En outre, vous ne pouvez utiliser ce module ESM qu'avec un automate 1756-L73S (8 Mo) ou de capacité mémoire inférieure.
1756-ESMNRM(XT)	Module ESM à condensateur de sécurité (inamovible) Ce module ESM apporte à votre application un niveau de sécurité renforcé en empêchant tout accès physique au connecteur USB et à la carte SD.
1756-SPESMNSE(XT)	Module ESM à condensateur sans sauvegarde de l'horloge pour le partenaire de sécurité. Utilisez ce module ESM lorsque votre application nécessite que le module de stockage d'énergie en place puisse se vider de l'énergie résiduelle qu'il contient jusqu'en dessous d'un seuil de 200 µJ avant de pouvoir être transporté dans ou hors de cette application. Le partenaire de sécurité pour température extrême 1756-L7SPXT est livré avec le 1756-SPESMNSEXT installé.
1756-SPESMNRM(XT)	Module ESM à condensateur de sécurité (inamovible) pour le partenaire de sécurité.

Sauvegarde du programme dans la mémoire NVS intégrée

Suivez ces étapes pour sauvegarder le programme en mémoire NVS lorsque l'automate n'est plus sous tension.

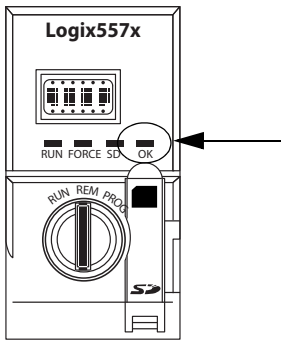
1. Coupez l'alimentation de l'automate.

   Cette opération peut être réalisée de deux façons :

   - en coupant l'alimentation du châssis alors que l'automate est encore dedans ;
   - en retirant l'automate de son châssis sous tension.

Dès que l'automate n'est plus alimenté, le voyant d'état OK passe en rouge fixe et reste dans cet état le temps nécessaire à la sauvegarde du programme.

Figure 30 – Voyant d'état OK.



2. Laisser le module ESM dans l'automate jusqu'à ce que le voyant d'état OK soit éteint.

3. Si nécessaire, retirez l'ESM de l'automate après que le voyant OK se soit éteint.

Effacement du programme de la mémoire NVS intégrée

Si votre application le permet, procédez de la façon suivante pour effacer le programme de la mémoire NVS intégrée à l'automate 1756-L7*x*S.

1. Retirez l'ESM de l'automate.

2. Mettez l'automate hors tension en coupant l'alimentation du châssis quand l'automate y est installé ou en retirant l'automate du châssis lorsque ce dernier est alimenté.

3. Remontez le module ESM dans l'automate.

4. Remettez l'automate sous tension.
   a. Si l'automate est déjà monté dans le châssis, remettez ce châssis sous tension.
   b. Si l'automate n'est pas installé dans le châssis, remettez le en place et remettez le châssis sous tension.

Estimer le temps de maintien de l'horloge interne par le module ESM

Le module ESM assure le maintien de l'horloge interne de l'automate lorsque son alimentation est coupée. Servez-vous de ce tableau pour estimer le temps de maintien fourni par le module ESM en fonction de la température de l'automate et du type de module en place.

Tableau 38 – Temps de maintien

	Temps de maintien (en jours)		
Température	**1756-ESMCAP(XT)**	**1756-ESMNRM(XT) 1756-SPESMNRM(XT)**	**1756-ESMNSE(XT) 1756-SPESMNSE(XT)**
20 °C	12	12	0
40 °C	10	10	0
60 °C	7	7	0

Gestion du firmware avec Firmware Supervisor

A partir de la version 18 du logiciel RSLogix 5000, vous pouvez utiliser la fonction Firmware Supervisor pour gérer le firmware des automates . Firmware Supervisor permet aux automates de mettre automatiquement à jour les dispositifs :

- les modules locaux ou décentralisés peuvent être mis à jour en mode Programme ou Exécution ;
- le détrompage électronique doit être configuré sur « Exact Match » (Correspondance exacte) ;
- le kit de firmware pour le dispositif cible doit résider sur le carte mémoire de l'automate ;
- Les périphériques doivent être compatibles avec la mise à niveau de leur firmware par l'utilitaire ControlFLASH.

Firmware Supervisor prend en charge tous les équipements d'E/S distribués non modulaires raccordés directement au réseau sans adaptateur, y compris les modules d'E/S CIP Safety en réseau EtherNet/IP. Les modules d'E/S CIP Safety en réseau DeviceNet, ainsi que les modules d'E/S POINT Guard I/O, ne sont pas pris en charge pour l'instant.

Procédez de la façon suivante pour activer Firmware Supervisor.

1. Dans la boîte de dialogue Controller Properties (Propriétés de l'automate), cliquez sur l'onglet Nonvolatile Memory (Mémoire non volatile).
2. Cliquez sur Load/Store (Charger/sauvegarder).
3. Dans le menu déroulant Automatic Firmware Updates (Mises à jour automatiques du firmware), sélectionnez Enable and Store Files to Image (Activer l'enregistrement d'images des fichiers).

Le logiciel RSLogix 5000 transfère les kits firmware de votre ordinateur à la carte mémoire de l'automate afin que Firmware Supervisor puisse les utiliser.

CONSEIL Si vous désactivez Firmware Supervisor, vous désactivez seulement les mises à jour au moyen de cette fonction. Ceci ne comprend pas les mises à jour d'automate qui se produisent quand l'image de l'automate est rechargée à partir de la carte mémoire.

Surveillance de l'état et gestion des défauts

Reportez-vous à l'Annexe A, Voyants d'état pour plus d'information sur l'interprétation des signaux des voyants d'état de l'automate et des messages de l'afficheur.

Visualisation d'état via la barre En ligne

La barre en ligne affiche des informations sur l'automate et le projet, notamment l'état de l'automate, des forçages, des modifications en ligne et de la sécurité.

Figure 31 – Boutons d'état

Lorsque le bouton d'état de l'automate est sélectionné, comme dans la figure ci-dessus, la barre en ligne affiche le mode de fonctionnement de l'automate (RUN) et l'état (OK). Le voyant BAT représente l'état de l'automate principal et du partenaire de sécurité. Si l'un, l'autre ou les deux présentent un défaut de pile, le voyant d'état s'allume.Le voyant I/O renseigne sur l'état des E/S standard et de sécurité. Il se comporte exactement comme le voyant d'état situé sur l'automate. L'E/S présentant l'état d'erreur le plus significatif est affiché en regard du voyant.

Lorsque le bouton d'état de la sécurité est sélectionné, comme dans la figure ci-dessous, la barre de contrôle en ligne affiche la signature de tâche de sécurité.

Figure 32 – Visualisation en ligne de la signature de sécurité

Le bouton d'état de la sécurité lui-même indique si la sécurité de l'automate est verrouillée, déverrouillée ou en défaut. Ce bouton comporte également une icône qui montre l'état de la sécurité.

Tableau 39 – Icône d'état de la sécurité

Si l'état de la sécurité indique…	L'icône suivante est affichée
Tâche de sécurité OK	
Safety task inoperable (Tâche de sécurité non opérationnelle)	
Partenaire absent Partenaire indisponible Matériel incompatible Firmware incompatible	
Hors ligne	

Ces icônes sont de couleur verte lorsque la sécurité de l'automate est verrouillée, de couleur jaune lorsqu'elle est déverrouillée et de couleur rouge lorsque l'automate présente un défaut de sécurité. En présence d'une signature de tâche de sécurité, l'icône comporte une petite coche. 

Surveillance des connexions

Vous pouvez surveiller l'état des connexions standard et de sécurité.

Toutes les connexions

En l'absence d'une communication avec un dispositif présent dans la configuration des E/S de l'automate pendant 100 ms, le délai de communication expire et l'automate génère les alarmes suivantes :

- Le voyant I/O (E/S) en face avant de l'automate clignote en vert.
- Un symbole d'alerte  s'affiche sur le dossier de configuration des E/S et sur le périphérique dont le délai d'établissement de communication est expiré.
- Un défaut de module est produit, auquel vous pouvez accéder par l'onglet Connections (Connexions) de la boîte de dialogue Module Properties (Propriétés du module) pour le module ou via l'instruction GSV.

ATTENTION : il n'est pas possible de configurer les E/S de sécurité et les connexions produites/consommées de façon à mettre automatiquement l'automate en défaut en cas de perte de la connexion. Vous devez donc surveiller toute apparition de défaut de connexion afin de vous assurer que le système de sécurité maintient toujours son intégrité SIL 3/PLe.

Voir Connexions de sécurité.

Connexions de sécurité

Pour les points associés à des données de sécurité produites ou consommées, vous pouvez surveiller l'état des connexions de sécurité par l'intermédiaire du membre CONNECTION_STATUS. Pour surveiller les connexions d'entrées et de sorties, les points d'E/S de sécurité comportent un membre d'état de connexion appelé SafetyStatus. Pour chacun des deux types de donnée, deux bits sont utilisés : RunMode (Mode Exécution) et ConnectionFaulted (Connexion en défaut).

La valeur RunMode indique si les données consommées sont couramment actualisées par un périphérique en mode d'exécution (1) ou à l'état inactif (0). L'état inactif est indiqué lorsque la connexion est fermée, la tâche de sécurité est en défaut ou que l'automate ou le périphérique distant est en mode de programmation ou de test.

La valeur ConnectionFaulted (connexion en défaut) indique si la connexion de sécurité entre le producteur et le consommateur de sécurité est valable (0) ou en défaut (1). Si ConnectionFaulted passe en défaut (1) suite à une perte de la connexion physique, les données de sécurité sont remises à zéro.

Le tableau suivant décrit les combinaisons possibles entre les états des bits RunMode (Mode d'exécution) et ConnectionFaulted (Défaut de connexion).

Tableau 40 – État de la connexion de sécurité

État de RunMode	État de ConnectionFaulted	Fonctionnement de la connexion de sécurité
1 = Exécution	0 = Valable	Les données sont activement commandées par le dispositif producteur. Le producteur est en mode Exécution (Run).
0 = Inactif	0 = Valable	La connexion est active et le périphérique producteur est à l'état inactif. La donnée de sécurité est remise à zéro.
0 = Inactif	1 = En défaut	La connexion de sécurité est en défaut. L'état du dispositif producteur est inconnu. La donnée de sécurité est remise à zéro.
1 = Exécution	1 = En défaut	État non valide.

Si un module est inhibé, le bit ConnectionFaulted est mis en défaut (1) et le bit RunMode à l'état inactif (0) pour chaque connexion associée au module. En conséquence, les données de sécurité consommées sont remises à zéro.

Surveillance des indicateurs d'état

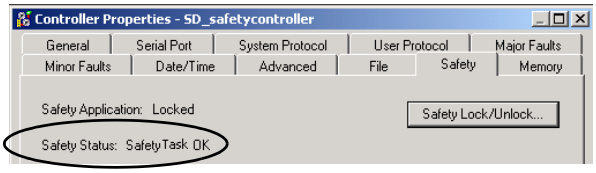
Les automates Logix et notamment les automates GuardLogix, prennent en charge des mots clés d'état que vous pouvez utiliser dans votre programme pour surveiller certains événements particuliers.

Pour de plus amples informations sur l'utilisation de ces mots clés, reportez-vous à la publication 1756-PM015, « Automates Logix5000 Informations et état de l'automate – Manuel de programmation ».

Surveillance de l'état de la sécurité

Vous pouvez visualiser l'état de la sécurité de l'automate sur le bouton d'état de la sécurité dans la barre en ligne et dans l'onglet Safety (Sécurité) de la boîte de dialogue Controller Properties (Propriétés de l'automate).

Figure 33 – État de la tâche de sécurité



Les états possibles de la sécurité sont les suivants :

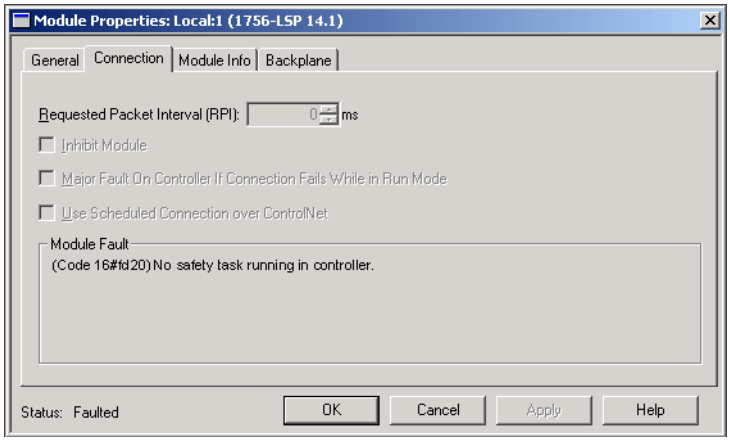
- Safety partner is missing or unavailable (le partenaire de sécurité est absent ou indisponible) ;
- Safety partner hardware is incompatible with primary controller (La configuration matérielle du partenaire de sécurité est incompatible avec celle de l'automate principal) ;
- Safety partner firmware is incompatible with the primary controller (Le firmware du partenaire de sécurité est incompatible avec celui de l'automate principal) ;
- Safety task inoperable (Tâche de sécurité non opérationnelle) ;
- Safety task OK (Tâche de sécurité OK).

A l'exception de Safety Task OK, tous les autres messages indiquent la présence de défauts de sécurité irrécupérables.

Pour la liste des codes de défaut et des actions correctives correspondantes, voir Défauts de sécurité majeurs (Type 14), page 130.

Vous pouvez visualiser l'état du partenaire de sécurité dans l'onglet Connections (Connexions) de sa boîte de dialogue Module Properties (Propriétés du module).

Figure 34 – État du partenaire de sécurité



Défauts de l'automate

Les défauts dans le système GuardLogix peuvent être des défauts irrécupérables de l'automate, des défauts de sécurité irrécupérables dans l'application de sécurité ou des défauts récupérables dans l'application de sécurité.

Défauts irrécupérables de l'automate

Ces défauts se produisent en cas d'échec des diagnostics internes de l'automate. Si un défaut irrécupérable de l'automate se produit, l'exécution de la tâche de sécurité est interrompue et les modules d'E/S CIP Safety sont placés en état de sécurité. La récupération nécessite que vous rechargiez le programme d'application.

Défauts de sécurité irrécupérables dans l'application de sécurité

Si un défaut irrécupérable se produit dans l'application de sécurité, le programme et le protocole de sécurité sont interrompus. Les défauts de chien de garde de la tâche de sécurité et de partenariat de commande font partie de cette catégorie.

Quand la tâche de sécurité rencontre un défaut de sécurité irrécupérable qui est effacé par programme dans le gestionnaire de défaut de l'automate, l'exécution de l'application standard se poursuit.

ATTENTION : ignorer un défaut de sécurité ne le supprime pas ! Si vous ignorez le défaut de sécurité, il est de votre responsabilité de prouver que le fonctionnement reste sûr.

Vous devez être en mesure de démontrer à votre organisme de certification que le fait d'autoriser une partie du système à continuer de fonctionner ne remet pas en cause sa sécurité de fonctionnement.

En présence d'une signature de tâche de sécurité, il vous suffit d'effacer le défaut pour permettre l'exécution de la tâche de sécurité. En l'absence de signature de tâche de sécurité, la tâche de sécurité ne peut pas reprendre tant que l'application n'a pas été rechargée en totalité.

Défauts récupérables dans l'application de sécurité

Si un défaut récupérable se produit dans l'application de sécurité, le système peut interrompre ou non l'exécution de la tâche de sécurité, selon que le défaut est géré ou non par le gestionnaire de défauts du programme dans l'application de sécurité.

Quand un défaut récupérable est acquitté par programme, la tâche de sécurité est autorisée à continuer sans interruption.

Quand un défaut récupérable dans l'application de sécurité n'est pas effacé par programme, un défaut de sécurité récupérable de type 14, code 2 se produit. L'exécution du programme de sécurité est arrêtée et les connexions du protocole de sécurité sont fermées et rouvertes afin d'être réinitialisées. Les sorties de sécurité sont placées en état de sécurité et le producteur des points de sécurité consommés commande aux consommateurs de les placer également en état de sécurité.

Les défauts récupérables vous permettent de modifier l'application standard et l'application de sécurité, selon le cas, afin de corriger la cause du défaut.

Cependant, en présence d'une signature de tâche de sécurité ou si l'automate est verrouillé, vous devez d'abord déverrouiller l'automate et supprimer la signature de tâche de sécurité pour pouvoir modifier l'application de sécurité.

Affichage des défauts

La boîte de dialogue Recent Faults (Défauts récents), dans l'onglet Major Faults (Défauts majeurs) de la boîte de dialogue Controller Properties (Propriétés de l'automate), contient deux sous-onglets : l'un pour les défauts standard et l'autre pour les défauts de sécurité.

L'afficheur d'état des automates 1756-L7*x*S indique également des codes de défaut avec un bref message d'état, comme indiqué page 137 et suivantes.

Codes de défaut

Le Tableau 41 montre les codes de défaut spécifiques aux automates GuardLogix. Le type et le code indiqués correspondent à ceux affichés dans l'onglet Major Faults (Défauts majeurs) de la boîte de dialogue des propriétés de l'automate ainsi que dans les attributs MAJORFAULTRECORD (ou MINORFAULTRECORD) de l'objet PROGRAM.

Tableau 41 – Défauts de sécurité majeurs (Type 14)

Code	Cause	État	Action corrective
01	Le chien de garde de la tâche a expiré. La tâche utilisateur ne s'est pas terminée dans le laps de temps spécifié. Un défaut de programme a provoqué une boucle infinie, le programme est trop complexe pour être exécuté aussi rapidement que prévu, une tâche de priorité supérieure empêche cette tâche de se terminer ou le partenaire de sécurité a été démonté.	Irrécupérable	Effacez l'erreur. Si une signature de tâche de sécurité est présente, la mémoire de sécurité sera réinitialisée et la tâche de sécurité recommencera son exécution. En l'absence de signature de tâche de sécurité, vous devrez recharger le programme dans l'automate pour permettre à nouveau l'exécution de la tâche de sécurité. Remettez en place le partenaire de sécurité (s'il a été démonté).
02	Une erreur est présente dans un sous-programme de la tâche de sécurité.	Récupérable	Rectifiez l'erreur dans la logique du programme utilisateur.
03	Le partenaire de sécurité est manquant.	Irrécupérable	Installez un partenaire de sécurité compatible.
04	Le partenaire de sécurité est indisponible.	Irrécupérable	Installez un partenaire de sécurité compatible.
05	Matériel du partenaire de sécurité incompatible.	Irrécupérable	Installez un partenaire de sécurité compatible.
06	Firmware du partenaire de sécurité incompatible.	Irrécupérable	Mettez à jour le partenaire de sécurité de sorte que les révisions majeure et mineure de son firmware correspondent à celles de l'automate principal.
07	Tâche de sécurité non opérationnelle. Ce défaut se produit lorsque le programme de sécurité est incorrect. Par exemple, lorsqu'une incompatibilité existe entre le programme de l'automate principal et celui du partenaire de sécurité, un timeout du chien de garde s'est produit ou lorsque la mémoire est corrompue.	Irrécupérable	Effacez l'erreur. Si une signature de tâche de sécurité est présente, elle permettra de réinitialiser la mémoire de sécurité et la tâche de sécurité reprendra son exécution. S'il n'y a pas de signature de sécurité, vous devrez recharger le programme dans l'automate pour permettre l'exécution de la tâche de sécurité.
08	Pas de temps système coordonné (CST) détecté.	Irrécupérable	Effacez l'erreur. Définissez un dispositif comme horloge maître CST.
09	Défaut irrécupérable de l'automate au niveau du partenaire de sécurité.	Irrécupérable	Effacez l'erreur et rechargez le programme dans l'automate. Si le problème persiste, remplacez le partenaire de sécurité.

Un défaut code 11, de type mineur récupérable (10), apparaît lorsque la pile du partenaire de sécurité 1756-LSP est absente ou nécessite d'être remplacée.

Pour plus d'informations sur le remplacement de la pile, reportez-vous à l'Annexe B.

La publication 1756-PM014, « Défauts majeurs et mineurs des automates Logix5000 – Manuel de programmation », contient la description des codes de défaut communs aux automates Logix.

Développement d'un sous-programme de traitement de défaut

Si une condition de défaut se produit et qu'elle soit suffisamment grave pour interrompre le fonctionnement de l'automate, ce dernier génère un défaut majeur et arrête l'exécution du programme.

Selon votre application, vous ne voudrez peut-être pas que tous les défauts de sécurité provoquent l'arrêt de l'ensemble de votre système. Dans ce cas, vous pouvez utiliser un sous-programme de gestion des défauts pour effacer un défaut spécifique et permettre à la partie de commande standard de votre système de continuer à fonctionner ou configurer certaines sorties pour qu'elles restent activées.

ATTENTION : vous devez être en mesure de démontrer à votre organisme de certification que le fait d'autoriser une partie du système à continuer de fonctionner ne remet pas en cause sa sécurité de fonctionnement.

L'automate prend en charge deux niveaux de gestion des défauts majeurs :

- le sous-programme de gestion des erreurs de programme ;
- le gestionnaire de défauts (Fault Handler) de l'automate.

Ces deux sous-programmes peuvent utiliser les instructions GSV et SSV, comme décrit à la page 132.

Sous-programme de gestion des erreurs de programme

Chaque programme peut posséder son propre sous-programme de gestion des défauts. L'automate exécute le sous-programme de gestion des défauts du programme en cas de défaut d'instruction. Si le sous-programme de gestion des défauts d'un programme n'efface pas le défaut, ou s'il n'existe pas de sous-programme de gestion des défauts de programme, l'automate continue d'exécuter le gestionnaire de défaut de l'automate, s'il en existe un.

Gestionnaire de défauts de l'automate

Le gestionnaire de défauts d'automate est un composant facultatif qui est exécuté quand le sous-programme de gestion des défauts de programme n'a pas pu effacer le défaut ou qu'il n'existe pas.

Vous ne pouvez créer qu'un seul programme pour le gestionnaire de défauts de l'automate. Après avoir créé ce programme, vous devez configurer un sous-programme comme sous-programme principal.

La publication 1756-PM014, « Défauts majeurs et mineurs des automates Logix5000 – Manuel de programmation », fournit des informations détaillées sur la création et le test d'un sous-programme de gestion de défaut.

Utilisation des instructions GSV et SSV

Les automates Logix stockent les données systèmes dans des objets, plutôt que dans des fichiers d'état. Vous pouvez utiliser des instructions GSV (Get System Value/Lire la valeur système) et SSV (Set System Value/Définir la valeur système) pour extraire et configurer les données de l'automate.

L'instruction GSV récupère les informations spécifiées et les place dans la destination définie. L'instruction SSV modifie l'attribut spécifié avec les données de la source de l'instruction. Lorsque vous saisissez une instruction GSV ou SSV, le logiciel de programmation affiche les classes d'objets, le nom des objets et le nom des attributs pour chaque instruction.

Pour les tâches standard, vous pouvez utiliser l'instruction GSV pour lire les valeurs de tous les attributs disponibles. Lorsque vous utilisez l'instruction SSV, le logiciel affiche uniquement les attributs que vous êtes autorisé à définir.

Pour la tâche de sécurité, les instructions GSV et SSV sont plus restreintes. Notez que les instructions SSV dans les tâches de sécurité et standard ne peuvent pas activer le bit 0 (défaut majeur sur erreur) dans l'attribut de mode d'un module d'E/S de sécurité.

Pour les objets de sécurité, le Tableau 42 montre les attributs dont vous pouvez lire les valeurs à l'aide de l'instruction GSV et ceux que vous êtes autorisé à définir à l'aide de l'instruction SSV dans les tâches de sécurité et standard.

ATTENTION : utilisez les instructions GSV et SSV avec précaution. La modification des objets peut entraîner un fonctionnement imprévu de l'automate, voire des blessures corporelles.

Tableau 42 – Accessibilité des instructions GSV et SSV

Objet de sécurité	Nom de l'attribut	Type de donnée	Description de l'attribut	Accessible à partir de la tâche de sécurité		Accessible à partir des tâches standard	
				GSV	SSV	GSV[4]	SSV
Tâche de sécurité	Instance	DINT	Fournit le numéro d'instance de cet objet de tâche. Les valeurs valables sont comprises entre 0 et 31.	✓		✓	
	MaximumInterval	DINT[2]	Intervalle de temps maximum entre les exécutions successives de cette tâche.			✓	✓
	MaximumScanTime	DINT	Temps d'exécution maximal enregistré (en ms) pour cette tâche.			✓	✓
	MinimumInterval	DINT[2]	Intervalle de temps minimum entre les exécutions successives de cette tâche.			✓	✓
	Priority	INT	Priorité relative de cette tâche par rapport aux autres tâches. Les valeurs valables sont comprises entre 0 et 15.	✓		✓	
	Rate	DINT	Période d'exécution de la tâche (en ms) ou timeout de la tâche (en ms).	✓		✓	
	Watchdog	DINT	Limite de temps (en ms) assignée à l'exécution de tous les programmes associés à cette tâche.	✓		✓	
Programme de sécurité	Instance	DINT	Fournit le numéro d'instance de cet objet programme.	✓		✓	
	MajorFaultRecord[1]	DINT[11]	Enregistre les défauts majeurs survenus dans ce programme.	✓	✓	✓	
	MaximumScanTime	DINT	Temps d'exécution maximal enregistré (en ms) pour ce programme.			✓	✓

Tableau 42 – Accessibilité des instructions GSV et SSV

Objet de sécurité	Nom de l'attribut	Type de donnée	Description de l'attribut	Accessible à partir de la tâche de sécurité		Accessible à partir des tâches standard	
				GSV	SSV	GSV[4]	SSV
Sous-programme de sécurité	Instance	DINT	Fournit le numéro d'instance de cet objet sous-programme. Les valeurs valables sont comprises entre 0 et 65 535.	✓			
Automate de sécurité	SafetyLocked	SINT	Indique si la sécurité de l'automate est verrouillée ou déverrouillée.	✓		✓	
	SafetyStatus[2]	INT	Définit l'état de la sécurité comme suit : • Tâche de sécurité OK. (1000000000000000) • Tâche de sécurité non opérationnelle. (1000000000000001) • Partenaire absent. (0000000000000000) • partenaire indisponible. (0000000000000001) • Configuration matérielle incompatible. (0000000000000010) • Firmware incompatible. (0000000000000011)			✓	
	SafetySignatureExists	SINT	Indique si une signature de tâche de sécurité est présente ou non.	✓		✓	
	SafetySignatureID	DINT	Numéro d'identification à 32 bits.			✓	
	SafetySignature	Chaîne[3]	Numéro d'identification à 32 bits.			✓	
	SafetyTaskFaultRecord[1][2]	DINT[11]	Enregistre les défauts de la tâche de sécurité.			✓	
Instruction complémentaire (de sécurité)	LastEditDate	LINT	Horodatage de la dernière modification de la définition d'instruction complémentaire.			✓	
	SignatureID	DINT	Numéro d'identification.			✓	
	SafetySignatureID	DINT	Numéro d'identification à 32 bits.			✓	

(1) Pour plus d'informations sur la façon d'accéder à cet attribut, voir Accès aux attributs FaultRecord, page 133.
(2) Pour plus d'informations sur la façon d'accéder à cet attribut, voir Saisie des informations de défaut, page 134.
(3) Longueur = 37.
(4) A partir de la tâche standard, l'accessibilité GSV aux attributs d'objets de sécurité est identique à celle des attributs d'objets standard.

Accès aux attributs FaultRecord

Créez une structure utilisateur pour simplifier l'accès aux attributs MajorFaultRecord et SafetyTaskFaultRecord.

Tableau 43 – Paramètres d'accès aux attributs FaultRecord

Nom	Type de donnée	Style	Description
TimeLow	DINT	Décimal	Les 32 bits inférieurs de la valeur d'horodatage du défaut
TimeHigh	DINT	Décimal	Les 32 bits supérieurs de la valeur d'horodatage du défaut
Type	INT	Décimal	Type de défaut (programme, E/S ou autre)
Code	INT	Décimal	Code unique attribué à un défaut particulier (dépend du type de défaut)
Info	DINT[8]	Hexadécimal	Information spécifique au défaut (dépend du type et du code de défaut)

Pour plus d'informations sur l'utilisation des instructions GSV et SSV, reportez-vous au chapitre relatif aux instructions d'entrée et de sortie de la publication 1756-RM003, « Automate Logix5000 – Instructions – Manuel de référence ».

Saisie des informations de défaut

Les attributs SafetyStatus et SafetyTaskFaultRecord peuvent saisir les informations relatives aux défauts irrécupérables. Utilisez une instruction GSV dans le gestionnaire de défaut de l'automate pour saisir et enregistrer les informations de défaut. L'instruction GSV peut être utilisée dans une tâche standard conjointement à un sous-progamme de gestion de défaut de l'automate qui efface le défaut et permet aux tâches standard de poursuivre leur exécution.

Voyants d'état

Indicateurs d'état des automates 1756-L6*x*S

L'état de l'automate principal et celui du partenaire de sécurité sont indiqués par des voyants lumineux à DEL.

Tableau 44 – Automate 1756-L6*x*S – Description des voyants d'état

Voyant	État	Description de l'automate principal	Description du partenaire de sécurité
RUN	Éteint	Aucune tâche utilisateur en cours. L'automate est en mode programmation (PROG).	–
	Vert	L'automate est en mode Exécution (RUN).	–
SAFE RUN	Éteint	–	La tâche de sécurité utilisateur ou les sorties de sécurité sont désactivées. L'automate est en mode de programmation (PROG) ou de test ; ou bien la tâche de sécurité est en défaut.
	Vert	–	La tâche de sécurité utilisateur et les sorties de sécurité sont actives. L'application de sécurité est en cours d'exécution. Une signature de tâche de sécurité est présente.
	Vert, clignotant	–	La tâche de sécurité utilisateur et les sorties de sécurité sont actives. L'application de sécurité est en cours d'exécution. La signature de tâche de sécurité est absente.
FORCE	Éteint	Aucun forçage, standard ou de sécurité, n'est actif dans l'automate.	–
	Orange	Des forçages standard et/ou de sécurité ont été activés.	–
	Orange, clignotant	Une ou plusieurs adresses d'E/S, standard et/ou de sécurité, ont été forcées à l'état activé ou désactivé, mais les forçages ne sont pas activés.	–
BAT	Éteint	Le niveau de charge de la pile est suffisant pour sauvegarder le contenu de la mémoire.	Le niveau de charge de la pile est suffisant pour sauvegarder le contenu de la mémoire.
	Rouge	Le niveau de charge de la pile est insuffisant pour sauvegarder le contenu de la mémoire.	Le niveau de charge de la pile est insuffisant pour sauvegarder le contenu de la mémoire.
OK	Éteint	Absence d'alimentation.	Absence d'alimentation.
	Vert	L'automate fonctionne sans défauts.	Le partenaire de sécurité fonctionne sans défauts.
	Rouge, clignotant	Défaut irrécupérable ou défaut récupérable pas pris en charge par le gestionnaire de défaut. Toutes les tâches utilisateur standard et de sécurité sont arrêtées.	–
	Rouge	Défaut à la mise sous tension ou défaut irrécupérable de l'automate.	Défaut à la mise sous tension ou défaut irrécupérable de l'automate.

Tableau 44 – Automate 1756-L6*x*S – Description des voyants d'état

Voyant	État	Description de l'automate principal	Description du partenaire de sécurité
I/O[1]	Éteint	Pas d'activité. Aucune E/S configurée.	–
	Vert	L'automate communique avec tous les dispositifs d'E/S configurés, standard et de sécurité.	–
	Vert, clignotant	Un ou plusieurs dispositifs d'E/S ne répondent pas.	–
	Rouge, clignotant	L'automate ne communique avec aucune des E/S configurées.	–
RS232	Éteint	Pas d'activité.	–
	Vert	Données en cours de réception ou de transmission.	–
SAFETY TASK	Éteint	–	Pas de partenariat établi. L'automate principal est absent, ne fonctionne pas correctement ou la révision de son firmware est incompatible avec celle du partenaire de sécurité.
	Vert	–	L'état de l'automate de sécurité est OK. Le temps système coordonné (CST) est synchronisé et les connexions d'E/S de sécurité sont établies.
	Vert, clignotant	–	L'état de l'automate de sécurité est OK. Le temps système coordonné (CST) n'est pas synchronisé dans l'automate principal ou le partenaire de sécurité.
	Rouge	–	Le partenariat a été perdu et un nouveau partenariat n'a pas pu être rétabli. L'automate principal est absent, ne fonctionne pas correctement ou la révision de son firmware est incompatible avec celle du partenaire de sécurité.
	Rouge, clignotant	–	Tâche de sécurité inexploitable.

(1) Les E/S incluent des points produits/consommés provenant d'autres automates.

Indicateurs d'état des automates 1756-L7*x*S

L'état de l'automate principal est indiqué à l'aide de quatre voyants d'état.

Tableau 45 – Description des indications d'état d'un automate principal 1756-L7*x*S

Voyant	État	Description
RUN	Éteint	Aucune tâche utilisateur en cours. L'automate est en mode programmation (PROG).
	Vert	L'automate est en mode Exécution (RUN).
FORCE	Éteint	Aucun forçage, standard ou de sécurité, n'est actif dans l'automate.
	Orange	Des forçages standard et/ou de sécurité ont été activés. **Soyez prudent lorsque vous installez (ajoutez) un forçage. Si vous installez un forçage, il prend effet immédiatement.**
	Orange, clignotant	Une ou plusieurs adresses d'E/S, standard et/ou de sécurité, ont été forcées à l'état activé ou désactivé, mais les forçages ne sont pas activés. **Soyez prudent lorsque vous activez des forçages d'E/S. Si vous activez des forçages d'E/S, tous les forçages d'E/S existants prendront également effet.**
SD	Éteint	Aucune activité existante sur la carte mémoire.
	Vert, clignotant	L'automate lit ou écrit dans la carte mémoire. Ne pas retirer la carte mémoire pendant que l'automate lit son contenu ou y enregistre des données.
	Vert	
	Rouge, clignotant	Le système de fichier de la carte mémoire est incorrect.
	Rouge	La carte mémoire n'est pas reconnue par l'automate.

Tableau 45 – Description des indications d'état d'un automate principal 1756-L7*x*S

Voyant	État	Description
OK	Éteint	Absence d'alimentation.
	Vert	L'automate fonctionne sans défauts.
	Rouge, clignotant	• Défaut irrécupérable ou défaut récupérable pas pris en charge par le gestionnaire de défaut. Toutes les tâches utilisateur standard et de sécurité sont arrêtées. • Il s'agit d'un nouvel automate qui vient d'être déballé, il nécessite une mise à niveau de son firmware. L'afficheur d'état indique qu'une installation de firmware est requise.
	Rouge	• L'automate est en train d'effectuer ses diagnostics pendant la mise sous tension. • Un défaut majeur irrécupérable s'est produit et le programme a été effacé de la mémoire. • La charge du condensateur du module de stockage d'énergie (ESM) est en cours de décharge suite à une mise hors tension. • L'automate est sous tension, mais il ne peut pas fonctionner. • L'automate est en train de charger un projet dans sa mémoire non volatile.

Le partenaire de sécurité 1756-L7SP ne possède qu'un indicateur d'état OK.

Tableau 46 – Voyant d'état du 1756-L7SP

Voyant	État	Description
OK	Éteint	Absence d'alimentation.
	Vert	Le partenaire de sécurité fonctionne sans défauts.
	Rouge	Défaut à la mise sous tension ou défaut irrécupérable de l'automate.

Afficheur d'état des automates 1756-L7*x*S

L'afficheur d'état des automates 1756-L7*x*S permet le défilement de messages fournissant des informations sur le numéro de révision du firmware de l'automate, l'état du module de stockage d'énergie (ESM), l'état du projet et les défauts majeurs.

Messages d'état de la sécurité

L'afficheur de l'automate principal peut afficher les messages suivants. Le partenaire de sécurité affiche « L7SP ».

Tableau 47 – Afficheur d'état de la sécurité

Message	Signification
No Safety Signature	La tâche de sécurité est en mode Exécution sans signature de tâche de sécurité.
Safety Partner Missing	Le partenaire de sécurité est absent ou indisponible.
Hardware Incompatible	Le matériel du partenaire de sécurité est incompatible avec l'automate principal.
Firmware incompatible	Les niveaux de révision de firmware du partenaire de sécurité et de l'automate principal sont incompatibles.
No CST Master	Un maître de temps système coordonné (CST) est introuvable.
Safety Task Inoperable	Le programme logique de sécurité est incorrect. Par exemple, lorsqu'une incompatibilité existe entre le programme de l'automate principal et celui du partenaire de sécurité, un timeout du chien de garde s'est produit ou lorsque la mémoire est corrompue.
Safety Unlocked	L'automate est en mode Exécution avec une signature de sécurité, mais la sécurité n'est pas verrouillée.

Messages d'état généraux

Les messages décrit dans le Tableau 48 sont habituellement affichés à la mise sous tension, à la mise hors tension et pendant la fonctionnement de l'automate. Ces messages indiquent l'état de l'automate et de l'ESM.

Tableau 48 – Afficheur d'état général

Message	Signification
Aucun message affiché	L'automate est hors tension ou un défaut majeur irrécupérable (MNRF) s'est produit. Contrôler le voyant OK pour vérifier si l'automate est sous tension et déterminer l'état de l'automate.
TEST	Les tests à la mise sous tension sont en cours d'exécution par l'automate.
PASS	Les tests à la mise sous tension ont été accomplis avec succès.
SAVE	Un projet est en cours d'enregistrement sur la carte SD à la mise hors tension. Vous pouvez également contrôler le voyant SD (voir page 136) pour obtenir des informations d'état supplémentaires. Laissez la sauvegarde se terminer avant de retirer la carte SD ou de déconnecter l'alimentation.
LOAD	Un projet est en cours de chargement depuis la carte SD à la mise sous tension de l'automate. Vous pouvez également contrôler le voyant SD (voir page 136) pour obtenir des informations d'état supplémentaires. Laissez le chargement se terminer avant de retirer la carte SD, de retirer le module ESM ou de déconnecter l'alimentation.
UPDT	Une mise à niveau du firmware est en cours d'exécution depuis la carte SD à la mise sous tension de l'automate. Vous pouvez également contrôler le voyant SD (voir page 136) pour obtenir des informations d'état supplémentaires. Si vous ne voulez pas que le firmware soit mis à jour à la mise sous tension, modifiez la propriété Load Image (chargement d'une image) de l'automate.
CHRG	Le module ESM à condensateur est en cours de charge.
1756-L7*x*/*X*	Référence et série de l'automate.
Rev *XX.xxx*	Numéros de révision majeure et mineure du firmware de l'automate.
No Project	Il n'y a pas de projet chargé sur l'automate. Pour charger un projet dans l'automate, utilisez le logiciel RSLogix 5000 ou une carte SD.
Project Name	Nom du projet en cours de chargement sur l'automate. Le nom indiqué correspond au nom du projet spécifié dans le logiciel RSLogix 5000.
BUSY	Les modules d'E/S associés à l'automate ne sont pas encore totalement mis sous tension. Laissez le temps à ces modules d'E/S de se mettre sous tension et d'effectuer leur auto-test.
Corrupt Certificate Received	Le certificat de sécurité associé au firmware est corrompu. Allez sur http://www.rockwellautomation.com/support/ et téléchargez la révision de firmware que vous essayez de mettre à niveau. Remplacez la version de firmware que vous avez précédemment installée par celle en provenance du site Internet de l'Assistance Technique.
Corrupt Image Received	Le fichier du firmware est corrompu. Allez sur http://www.rockwellautomation.com/support/ et téléchargez la révision de firmware que vous essayez de mettre à niveau. Remplacez la version de firmware que vous avez précédemment installée par celle en provenance du site Internet de l'Assistance Technique.
ESM Not Present	Il n'y a pas de module ESM dans l'automate et celui-ci ne peut pas sauvegarder l'application lors des coupures d'alimentation. Insérez un module ESM compatible et, s'il s'agit d'un module ESM à condensateur, ne coupez pas l'alimentation tant qu'il n'est pas chargé.
ESM Incompatible	Le module ESM est incompatible avec la capacité mémoire de l'automate. Remplacez ce module ESM incompatible par un ESM compatible.
ESM Hardware Failure	Une défaillance du module ESM s'est produite et l'automate n'est plus capable de sauvegarder son programme en cas de coupure d'alimentation. Remplacez le module ESM avant de couper l'alimentation de l'automate de façon à ce que son programme soit sauvegardé.
ESM Energy Low	Le module ESM à condensateur ne possède plus une réserve d'énergie suffisante pour permettre à l'automate de sauvegarder son programme en cas de coupure d'alimentation. Remplacez le module ESM.
ESM Charging	Le module ESM à condensateur est en cours de charge. Ne coupez pas l'alimentation tant que la charge n'est pas terminée.
Flash in Progress	Une mise à niveau de firmware par l'intermédiaire des utilitaires ControlFLASH ou AutoFlash est en cours. Laissez la mise à niveau du firmware se dérouler sans l'interrompre.
Firmware Installation Required	L'automate utilise le firmware d'initialisation (doté d'un numéro de révision en 1.*xxx*). Il nécessite une mise à niveau de ce firmware. Mettez à jour le firmware de l'automate.
SD Card Locked	Une carte SD verrouillée a été installée.

Messages de défaut

Si l'automate est en défaut, les messages suivants peuvent être indiqués par l'afficheur d'état :

Tableau 49 – Messages de défaut(1)

Message	Signification
Major Fault T*XX*:C*XX message*	Un défaut majeur de type *XX* et de Code *XX* a été détecté. Par exemple, si l'afficheur d'état indique Major Fault T04:C42 Invalid JMP Target, cela signifie qu'une instruction JMP a été programmée pour effectuer un saut à une instruction LBL non valide.
I/O Fault Local:*X #XXXX message*	Un défaut d'E/S s'est produit sur un module du châssis local. Les numéros de logement et de code de défaut sont indiqués avec une brève description. Par exemple, I/O Fault Local:3 #0107 Connection Not Found indique que la connexion au module d'E/S local situé dans le logement numéro trois n'est pas établie. Effectuez l'action corrective appropriée au type de défaut indiqué.
I/O Fault *ModuleName #XXXX message*	Un défaut d'E/S s'est produit sur un module d'un châssis décentralisé. Le nom du module en défaut est indiqué tel qu'il a été défini dans l'arborescence de configuration des E/S du logiciel RSLogix 5000, avec le code de défaut et une brève description de ce défaut. Par exemple, I/O Fault My_Module #0107 Connection Not Found indique que la connexion avec le module « My_Module » n'est pas établie. Effectuez l'action corrective appropriée au type de défaut indiqué.
I/O Fault *ModuleParent:X #XXXX message*	Un défaut d'E/S s'est produit sur un module d'un châssis décentralisé. Le nom du module parent est indiqué car il n'y a pas de nom défini pour ce module dans l'arborescence de configuration des E/S du logiciel RSLogix 5000. Le code du défaut est par ailleurs mentionné avec une brève description de ce défaut. Par exemple, I/O Fault My_CNet:3 #0107 Connection Not Found indique que la connexion avec un module situé dans le logement numéro 3 du châssis et associé au module de communication « My_CNet » n'est pas établie. Effectuez l'action corrective appropriée au type de défaut indiqué.
X I/O Faults	Des défauts d'E/S sont présents et *X* est le nombre de défauts actifs. Dans le cas de défauts d'E/S multiples, l'automate indique le premier défaut rapporté. Au fur et à mesure que ces défauts d'E/S sont rectifiés, le nombre affiché décroit et le défaut suivant rapporté est indiqué par le message de défaut d'E/S. Effectuez l'action corrective appropriée au type de défaut indiqué.

(1) Pour plus de détails sur les codes de défaut des E/S, reportez-vous à la publication 1756-PM014, « Défauts majeurs, mineurs et d'E/S des automates Logix5000 – Manuel de programmation ».

Messages de défaut majeur récupérable

Les défauts majeurs récupérables sont indiqués par Major Fault T*XX*:C*XX message* sur l'afficheur d'état de l'automate. Le Tableau 50, page 140 répertorie les types de défaut spécifiques, les codes et les messages associés tels qu'ils sont affichés sur l'afficheur d'état.

Pour une description détaillée de ces défauts majeurs récupérables et des méthodes correctives correspondantes recommandées, reportez-vous au manuel de programmation, Publication 1756-PM014, « Défauts majeurs, mineurs et d'E/S des automates Logix5000 ».

Tableau 50 – Messages de défaut d'état majeur récupérable

Type	Code	Message
1	1	Run Mode Powerup
1	60	Non-recoverable
1	61	Non-recoverable – Diagnostics Saved
1	62	Non-recoverable – Program Saved
3	16	I/O Connection Failure
3	20	Chassis Failure
3	21	
3	23	Connection Failure
4	16	Unknown Instruction
4	20	Invalid Array Subscript
4	21	Control Structure LEN or POS < 0
4	31	Invalid JSR Parameter
4	34	Timer Failure
4	42	Invalid JMP Target
4	82	SFC Jump Back Failure
4	83	Value Out of Range
4	84	Stack Overflow
4	89	Invalid Target Step
4	90	Invalid Instruction
4	91	Invalid Context
4	92	Invalid Action
4	990	User-defined
4	991	
4	992	
4	993	
4	994	
4	995	
4	996	
4	997	
4	998	
4	999	
6	1	Task Watchdog Expired
7	40	Save Failure
7	41	Bad Restore Type
7	42	Bad Restore Revision
7	43	Bad Restore Checksum
8	1	Keyswitch Change Ignored
11	1	Positive Overtravel Limit Exceeded
11	2	Negative Overtravel Limit Exceeded
11	3	Position Error Tolerance Exceeded
11	4	Encoder Channel Connection Fault
11	5	Encoder Noise Event Detected
11	6	SERCOS Drive Fault
11	7	Synchronous Connection Fault
11	8	Servo Module Fault
11	9	Asynchronous Connection Fault
11	10	Motor Fault
11	11	Motor Thermal Fault
11	12	Drive Thermal Fault
11	13	SERCOS Communications Fault
11	14	Inactive Drive Enable Input Detected
11	15	Drive Phase Loss Detected
11	16	Drive Guard Fault
11	32	Motion Task Overlap Fault
11	33	CST Reference Loss Detected
18	1	CIP Motion Initialization Fault
18	2	CIP Motion Initialization Fault Mfg
18	3	CIP Motion Axis Fault
18	4	CIP Motion Axis Fault Mfg
18	5	CIP Motion Fault
18	6	CIP Module Fault
18	7	Motion Group Fault
18	8	CIP Motion Configuration Fault
18	9	CIP Motion APR Fault
18	10	CIP Motion APR Fault Mfg
18	128	CIP Motion Guard Fault

Codes de défaut d'E/S

Les défaut d'E/S indiqués par l'automate apparaissent sur l'afficheur d'état sous l'une ou l'autre de ces formes :

- I/O Fault Local:*X #XXXX message*
- I/O Fault *ModuleName #XXXX message*
- I/O Fault *ModuleParent*:*X #XXXX message*

La première partie de la structure est utilisée pour indiquer l'emplacement du module en défaut. La façon dont cet emplacement est désigné est fonction de la configuration d'E/S et des propriétés de module que vous avez définies dans le logiciel RSLogix 5000.

Le second membre de la structure, #XXXX message, peut être utilisé pour le diagnostic du type de défaut d'E/S et une indication des actions correctives possibles. Pour plus de détails sur chaque code de défaut des E/S, reportez-vous à la publication 1756-PM014, « Défauts majeurs, mineurs et d'E/S des automates Logix5000 – Manuel de programmation ».

Tableau 51 – Messages de défaut des E/S

Code	Message
#0001	Connection Failure
#0002	Insufficient Resource
#0003	Invalid Value
#0004	IOI Syntax
#0005	Destination Unknown
#0006	Partial Data Transferred
#0007	Connection Lost
#0008	Service Unsupported
#0009	Invalid Attribute Value
#000A	Attribute List Error
#000B	State Already Exists
#000C	Object Mode Conflict
#000D	Object Already Exists
#000E	Attribute Not Settable
#000F	Permission Denied
#0010	Device State Conflict
#0011	Reply Too Large
#0012	Fragment Primitive
#0013	Insufficient Command Data
#0014	Attribute Not Supported
#0015	Data Too Large
#0100	Connection In Use
#0103	Transport Not Supported
#0106	Ownership Conflict
#0107	Connection Not Found
#0108	Invalid Connection Type
#0109	Invalid Connection Size
#0110	Module Not Configured
#0111	RPI Out of Range
#0113	Out of Connections
#0114	Wrong Module

Code	Message
#0115	Wrong Device Type
#0116	Wrong Revision
#0117	Invalid Connection Point
#0118	Invalid Configuration Format
#0119	Module Not Owned
#011A	Out of Connection Resources
#0203	Connection Timeout
#0204	Unconnected Message Timeout
#0205	Invalid Parameter
#0206	Message Too Large
#0301	No Buffer Memory
#0302	Bandwidth Not Available
#0303	No Bridge Available
#0304	ControlNet Schedule Error
#0305	Signature Mismatch
#0306	CCM Not Available
#0311	Invalid Port
#0312	Invalid Link Address
#0315	Invalid Segment Type
#0317	Connection Not Scheduled
#0318	Invalid Link Address
#0319	No Secondary Resources Available
#031E	No Available Resources
#031F	No Available Resources
#0800	Network Link Offline
#0801	Incompatible Multicast RPI
#0802	Invld Safety Conn Size
#0803	Invld Safety Conn Format
#0804	Invld Time Correct Conn Format
#0805	Invld Ping Intrvl EPI Multiplier
#0806	Time Coord Msg Min Multiplier

Messages de défaut des E/S (suite)

Code	Message
#0807	Time Expectation Multiplier
#0808	Timeout Multiplier
#0809	Invld Max Consumer Number
#080A	Invld CPCRC
#080B	Time Correction Conn ID Invld
#080C	Safety Cfg Signature Mismatch
#080D	Safety Netwk Num Not Set OutOfBx
#080E	Safety Netwk Number Mismatch
#080F	Cfg Operation Not Allowed
#0814	Data Type Mismatch
#FD01	Bad Backplane EEPROM
#FD02	No Error Code
#FD03	Missing Required Connection
#FD04	No CST Master
#FD05	Axis or GRP Not Assigned
#FD06	SERCOS Transition Fault
#FD07	SERCOS Init Ring Fault
#FD08	SERCOS Comm Fault
#FD09	SERCOS Init Node Fault
#FD0A	Axis Attribute Reject
#FD1F	Safety Data Fault
#FD20	No Safety Task Running
#FD21	Invld Safety Conn Parameter
#FE01	Invalid Connection Type
#FE02	Invalid Update Rate
#FE03	Invalid Input Connection
#FE04	Invalid Input Data Pointer
#FE05	Invalid Input Data Size
#FE06	Invalid Input Force Pointer
#FE07	Invalid Output Connection

Code	Message
#FE08	Invalid Output Data Pointer
#FE09	Invalid Output Data Size
#FE0A	Invalid Output Force Pointer
#FE0B	Invalid Symbol String
#FE0C	Invalid Scheduled P/C Instance
#FE0D	Invalid Symbol Instance
#FE0E	Module Firmware Updating
#FE0F	Invalid Firmware File Revision
#FE10	Firmware File Not Found
#FE11	Firmware File Invalid
#FE12	Automatic Firmware Update Failed
#FE13	Update Failed – Active Connection
#FE14	Searching Firmware File
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
–	

Maintenance de la pile

Les automates principaux GuardLogix 1756-L6*x*S et leurs partenaires de sécurité 1756-LSP contiennent une pile au lithium qui peut nécessiter un remplacement. Les automates GuardLogix 1756-L7*x*S et leurs partenaires de sécurité 1756-L7SP ne contiennent pas de pile.

Estimation de la durée de vie de la pile

L'autonomie de la pile dépend de la température du châssis, de la taille du projet et de la fréquence de mise hors/sous tension de l'automate. Elle ne dépend pas du fait que l'automate soit alimenté ou non.

Avant l'allumage du voyant BAT

Servez-vous de ce tableau pour estimer le temps disponible avant que le témoin BAT ne s'allume en rouge, dans le cas le plus défavorable.

Tableau 52 – Estimation du temps avant déclenchement de l'indication de pile faible (cas le plus défavorable)

Température mesurée à 2,54 cm sous le châssis	Nbre de cycles de remise sous tension par jour	Taille du projet			
		1 Mo	2 Mo	4 Mo	8 Mo
0 à 40 °C	3	3 ans	3 ans	26 mois	20 mois
	2 ou moins	3 ans	3 ans	3 ans	31 mois
41 à 45 °C	3	2 ans	2 ans	2 ans	20 mois
	2 ou moins	2 ans	2 ans	2 ans	2 ans
46 à 50 °C	3 ou moins	16 mois	16 mois	16 mois	16 mois
51 à 55 °C	3 ou moins	11 mois	11 mois	11 mois	11 mois
56 à 60 °C	3 ou moins	8 mois	8 mois	8 mois	8 mois

EXEMPLE Dans les conditions suivantes, la pile durera au moins 20 mois avant que le voyant BAT ne s'allume en rouge :

- La température maximale à 2,54 cm sous le châssis est de 45 °C.
- Le système est éteint et remis sous tension 3 fois par jour.
- l'automate contient un projet de 8 Mo.

Après allumage du voyant BAT

IMPORTANT Si le voyant BAT s'allume pour la première fois lors d'une mise sous tension de l'automate, l'autonomie de la pile peut être inférieure à celle indiquée dans le Tableau 53. Il se produit en effet en permanence une décharge légère de la pile. Il se peut donc qu'une partie de la charge de la pile ait été consommée alors que l'automate était hors tension et dans l'incapacité d'activer son voyant BAT.

Tableau 53 – Autonomie de la pile une fois que le voyant BAT est allumé (cas le plus défavorable)

Température mesurée à 2,54 cm sous le châssis	Cycles de remise sous tension	Taille du projet			
		1 Mo	2 Mo	4 Mo	8 Mo
0 à 20 °C	3 par jour	26 semaines	18 semaines	12 semaines	9 semaines
	1 par jour	26 semaines	26 semaines	26 semaines	22 semaines
	1 par mois	26 semaines	26 semaines	26 semaines	26 semaines
21 à 40 °C	3 par jour	18 semaines	14 semaines	10 semaines	8 semaines
	1 par jour	24 semaines	21 semaines	18 semaines	16 semaines
	1 par mois	26 semaines	26 semaines	26 semaines	26 semaines
41 à 45 °C	3 par jour	12 semaines	10 semaines	7 semaines	6 semaines
	1 par jour	15 semaines	14 semaines	12 semaines	11 semaines
	1 par mois	17 semaines	17 semaines	17 semaines	17 semaines
46 à 50 °C	3 par jour	10 semaines	8 semaines	6 semaines	6 semaines
	1 par jour	12 semaines	11 semaines	10 semaines	9 semaines
	1 par mois	12 semaines	12 semaines	12 semaines	12 semaines
51 à 55 °C	3 par jour	7 semaines	6 semaines	5 semaines	4 semaines
	1 par jour	8 semaines	8 semaines	7 semaines	7 semaines
	1 par mois	8 semaines	8 semaines	8 semaines	8 semaines
56 à 60 °C	3 par jour	5 semaines	5 semaines	4 semaines	4 semaines
	1 par jour	6 semaines	6 semaines	5 semaines	5 semaines
	1 par mois	6 semaines	6 semaines	6 semaines	6 semaines

Quand remplacer la pile

Quand la pile est déchargée à environ 95 %, l'automate déclenche les alarmes suivantes :

- le voyant BAT situé sur la face avant s'allume (rouge, fixe) ;
- un défaut mineur est généré (de type 10, code 10 au niveau de l'automate).

ATTENTION : pour éviter toute fuite des produits chimiques potentiellement dangereux contenus dans la pile, il est recommandé de la remplacer à la fréquence suivante, même si le voyant BAT est éteint.

Tableau 54 – Fréquence de remplacement de la pile

Si la température à 2,54 cm sous le châssis est de	Remplacez la pile tous les
–25 à 35 °C	Remplacement non requis
36 à 40 °C	3 ans
41 à 45 °C	2 ans
46 à 50 °C	16 mois
51 à 55 °C	11 mois
56 à 70 °C	8 mois

IMPORTANT L'automate GuardLogix étant un automate de type « 1oo2 » (à deux processeurs), nous vous recommandons vivement de remplacer ses deux piles en même temps.

Remplacement de la pile

Cet automate contient une pile au lithium qui est prévue pour être remplacée pendant la durée de vie du produit. Vous devez prendre certaines précautions pour la manipulation et la mise au rebut de cette pile.

ATTENTION : l'automate utilise une pile au lithium qui contient des substances chimiques potentiellement dangereuses.

Avant de manipuler ou de procéder à la mise au rebut d'une pile de ce type, veuillez vous référer à la publication AG-5.4, « Guidelines for Handling Lithium Batteries ».

AVERTISSEMENT : lorsque vous branchez ou débranchez la pile, un arc électrique peut se produire, susceptible de provoquer une explosion dans les installations en environnement dangereux. Assurez-vous que l'alimentation est coupée ou que l'environnement est classé non dangereux avant de poursuivre.

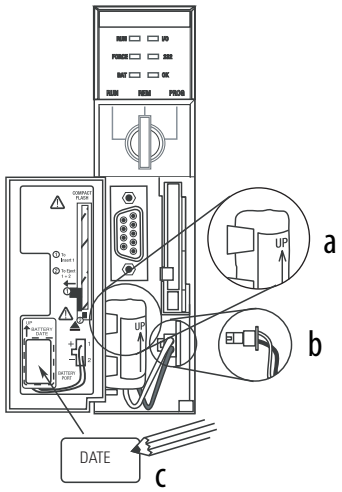
IMPORTANT Si vous enlevez la pile qu'une coupure d'alimentation se produit, le projet de l'automate sera perdu.

Pour remplacer la pile, procédez comme suit.

1. Mettez le châssis sous tension.
2. La pile présente-t-elle des signes de fuite ou semble-t-elle endommagée ?

Si	Alors
Oui	Avant de manipuler la pile, consultez la publication AG-5.4, « Guidelines for Handling Lithium Batteries ».
Non	Passez à l'étape suivante.

3. Démontez la pile usagée.
4. Installez une pile 1756-BA2 neuve.
   a. Insérez la pile comme indiqué.
   b. Connectez la pile :
      + Rouge
      – Noir
   c. Inscrivez sur l'étiquette de la pile la date à laquelle vous l'avez installée et fixez cette étiquette sur la face interne de la porte de l'automate.



ATTENTION : utilisez uniquement une pile 1756-BA2. Si vous utilisez une pile d'un autre modèle, vous risquez d'endommager l'automate.

5. Vérifiez que l'indicateur BAT situé en façade de l'automate est bien éteint.

Si	Alors
Oui	Passez à l'étape suivante.
Non	1. Vérifiez que la pile est correctement montée dans l'automate. 2. Si le voyant BAT reste allumé, installez une autre pile 1756-BA2. 3. Si le voyant BAT reste allumé après que vous ayez installé une nouvelle pile (Cf. étape 2), contactez votre représentant ou votre distributeur local Rockwell Automation.

6. Éliminez la pile usagée conformément aux réglementations locales.

AVERTISSEMENT : ne jetez pas au feu ni dans les ordures ménagères des piles au lithium. Elles risquent d'exploser ou d'éclater violemment. Respectez toutes les réglementations locales en vigueur relatives à la mise au rebut de ces matériaux. Vous êtes légalement responsable des dangers engendrés par la mise au rebut de votre pile.

ATTENTION : ce produit contient une pile au lithium étanche dont le remplacement peut s'avérer nécessaire pendant sa durée de vie.

A la fin de sa vie, la pile contenue dans ce produit devra être collectée séparément des déchets courants non soumis au tri sélectif.

La récupération et le retraitement des piles usagées permettent de protéger l'environnement et contribuent à la préservation des ressources naturelles par le recyclage des matériaux réutilisables industriellement.

Stockage des piles de rechange

ATTENTION : des substances chimiques potentiellement dangereuses peuvent s'écouler d'une pile si celle-ci n'est pas stockée convenablement. Stockez les piles dans un endroit sec et frais. Nous recommandons une température de 25 °C et une humidité relative comprise entre 40 et 60 %. Vous pouvez néanmoins conserver ces piles entre –45 et +85 °C pendant 30 jours maximum, le temps d'un transport par exemple. Pour éviter toute fuite éventuelle, ne stockez pas ces piles à une température supérieure à 60 °C pendant plus de 30 jours.

Informations connexes

Pour plus d'informations sur la manutention, le stockage et la mise au rebut des piles au lithium, reportez-vous à la publication AG-5.4, « Guidelines for Handling Lithium Batteries ».

Notes :

Changement du type d'automate dans un projet RSLogix 5000

Les automates de sécurité ont des caractéristiques spécifiques et ne prennent pas en charge certaines fonctions standard. Il est en conséquence important de bien comprendre les incidences sur le comportement du système d'une modification du type de l'automate de standard à sécurité (ou de sécurité à standard) dans un projet RSLogix 5000. Changer le type de l'automate affecte en effet :

- les fonctions prises en charge ;
- la configuration physique du projet, c'est-à-dire l'affectation du partenaire et des E/S de sécurité ;
- les propriétés de l'automate ;
- les éléments du projet, comme les tâches, les programmes, les sous-programmes et les points ;
- les instructions complémentaires de sécurité.

Transformation d'un système de commande standard en système de sécurité

Pour pouvoir transformer sans problème un automate standard en automate de sécurité principal, le logement de châssis situé immédiatement à sa droite doit être disponible pour son partenaire de sécurité.

Lors de la confirmation du passage d'un projet d'automate standard à un automate de sécurité, les composants de sécurité sont créés afin que la configuration minimale requise par un automate de sécurité soit respectée :

- la tâche de sécurité n'est créée que si le nombre maximal de tâches chargeables n'est pas atteint. La tâche de sécurité est initialisée avec ses valeurs par défaut ;
- les composants de sécurité sont créés (c'est-à-dire la tâche de sécurité, le programme de sécurité, etc.) ;
- un numéro de réseau de sécurité (SNN) temporel est généré pour le châssis local ;

- toutes les fonctions d'un automate standard, comme la redondance, qui ne sont pas prises en charge par l'automate de sécurité sont supprimées de la boîte de dialogue Controller Properties (Propriétés de l'automate), le cas échéant.

Transformation d'un automate de sécurité en automate standard

Lors de la confirmation du passage d'un projet d'automate de sécurité à un automate standard, certains composants sont modifiés et d'autres supprimés, comme indiqué ci-dessous :

- le partenaire de sécurité (1756-LSP) est supprimé du châssis des E/S ;
- les modules d'E/S de sécurité et leurs points sont supprimés ;
- la tâche, les programmes et les sous-programmes de sécurité sont modifiés en tâche, programmes et sous-programmes standard ;
- tous les points de sécurité, à l'exception de ceux consommés, sont transformés en points standard ; les points de sécurité consommés sont supprimés ;
- les mappages de points de sécurité sont supprimés ;
- le numéro de réseau de sécurité (SNN) est supprimé ;
- les mots de passe de verrouillage et de déverrouillage de la sécurité sont supprimés ;
- si l'automate standard doit gérer des fonctions qui n'étaient pas prises en compte dans l'automate de sécurité, ces nouvelles fonctions apparaissent dans la boîte de dialogue Controller Properties (Propriétés de l'automate) ;

CONSEIL Les automates de sécurité homologues ne sont pas supprimés, même s'ils n'ont plus aucune connexion.

- des instructions peuvent continuer à faire référence à des modules qui ont été supprimés et produiront des erreurs de vérification ;
- les points consommés sont supprimés lorsque le module producteur est supprimé ;
- suite aux modifications précédentes apportées au système, les instructions spécifiques à la sécurité et les points d'E/S de sécurité ne seront plus vérifiés.

Si le projet de l'automate de sécurité contenait des instructions complémentaires de sécurité, vous devrez les supprimer du projet ou changer leur classe en standard avant de modifier le type de l'automate.

Remplacement d'un automate GuardLogix 1756 par un automate Compact GuardLogix 1768, ou vice versa

Lorsque vous passez d'un type d'automate de sécurité à un autre, la classe des points, des sous-programmes et des programmes ne change pas. Les modules d'E/S qui ne sont pas compatibles avec le nouvel automate sont supprimés.

La représentation du partenaire de sécurité est mise à jour de façon à apparaître convenablement pour l'automate cible :

- Lors du remplacement par un automate GuardLogix 1756, le partenaire de sécurité est créé dans le logement *x* (correspondant au logement de l'automate principal + 1).
- Lors du remplacement par un automate Compact GuardLogix 1768, le partenaire de sécurité est supprimé car il est intégré dans un automate Compact GuardLogix.

CONSEIL Un automate GuardLogix 1756 autorise jusqu'à 100 programmes pour sa tâche de sécurité, alors que l'automate Compact GuardLogix 1768 n'en permet que 32.

Remplacement d'un automate 1756-L7*x*S par un automate 1756-L6*x*S ou 1768-L4*x*S

Les instructions à virgule flottante, telles que FAL, FLL, FSC, SIZE, CMP, SWPB, et CPT sont prises en charge par les automates GuardLogix 1756-L7*x*S, mais pas par les automates 1756-L6*x*S et 1768-L4*x*S. Si votre programme de sécurité contient de telles instructions, des erreurs de vérification se produiront lors du remplacement d'un automate 1756-L7*x*S par un automate 1756-L6*x*S ou 1768-L4*x*S.

Informations connexes

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

Notes :

Historique des modifications

En raison de l'apparition de nouveaux automates, modules et applications, ainsi que des nouvelles fonctionnalités du logiciel RSLogix 5000, le présent manuel a été révisé pour intégrer les dernières informations disponibles. Cette annexe reprend de façon synthétique les différentes modifications qui ont été apportées par chacune des versions antérieures de ce manuel.

Reportez-vous à cette annexe si vous avez besoin de connaître les modifications qui ont été apportées par rapport aux révisions antérieures. Il vous sera particulièrement utile de connaître les nouvelles informations introduites par chacune des révisions précédentes de ce manuel pour décider d'effectuer une mise à jour de vos composants matériels ou logiciels.

1756-UM020H-FR-P, Avril 2012

Modification de la liste des alimentations prises en charge.

1756-UM020G-FR-P, Février 2012

- Ajout des informations relatives aux automates 1756-L7*x*S et 1756-L73SXT
- Mise à jour de la liste des documentations complémentaires
- Ajout du chapitre sur l'installation de l'automate
- Ajout des informations relatives aux connexions en envoi individuel (unicast) pour les modules d'E/S de sécurité en réseau EtherNet/IP
- Ajout d'informations relatives à l'installation
- Ajout des informations relatives à la protection du mode d'exécution en ce qui concerne la signature de tâche de sécurité
- Mise à jour des procédures de remplacement des E/S incluant différents scénarios de remplacement
- Mise à jour de la valeur maximale d'intervalle entre trames requis
- Ajout des types de données DCA_INPUT et DCAF_INPUT à la liste des types de données utilisables par les points de sécurité
- Restructuration des informations sur les points de sécurité produits et consommés, ainsi que sur la configuration des automates de sécurité pairs de façon à regrouper toutes ces informations dans le chapitre 6
- Ajout des informations relatives à l'incidence d'une carte SD verrouillée sur la mise à jour du firmware
- Ajout des informations relatives à l'utilisation d'un module de stockage d'énergie (ESM) pour la mémoire non volatile
- Transfert des tableaux de description des indications d'état en annexe et ajout des informations de dépannage

- Mise à jour des informations sur la fréquence de remplacement de la pile sur les automates 1756-L6*x*S
- Ajout des informations relatives au remplacement par un automate 1756-L7*x*S
- Ajout de la présente annexe d'historique des modifications

1756-UM020F-FR-P, Août 2010

- Prise en charge des automates GuardLogix par RSLogix 5000 en version 19
- Le type de connexion par défaut pour les points de sécurité produits et consommés est l'envoi individuel (unicast)

1756-UM020E-FR-P, Janvier 2010

- Instructions complémentaires de sécurité et haute intégrité ajoutées à la liste des fonctions prises en charge par RSLogix 5000
- Activation de la synchronisation temporelle
- Mise à jour des exemples de modification du numéro SNN des modules d'E/S de sécurité en réseau CIP Safety de façon à introduire les modules d'E/S de sécurité EtherNet/IP
- Clarification des informations sur l'adressage Ethernet
- Connexions en réseau ControlNet pour modules d'E/S distribuées
- Définition d'un point comme constante
- Réglage du niveau d'accès extérieur pour les données de point
- Mise à jour des procédures pour la production et la consommation des points de sécurité
- Restriction pour le mappage des points à valeur constante
- Mise à jour du tableau des réponses du logiciel pendant le téléchargement
- Accessibilité GSV/SSV d'un objet AOI (Add-on Instruction/instruction complémentaire) de sécurité
- Stockage et chargement des projets dans la mémoire non volatile
- Mise à jour des informations sur la mise au rebut de la pile
- Remplacement d'un automate GuardLogix 1756 par un automate Compact GuardLogix 1768 ou vice versa

1756-UM020D-FR-P, Juillet 2008

- Mise à jour du tableau des documentations complémentaires afin d'y inclure de nouveaux manuels
- Informations sur l'automate 1756-L63S
- Informations générales sur la programmation à l'aide du logiciel RSLogix 5000 en version 17, y compris les versions logicielles et les améliorations prises en compte
- Utilisation d'un module 1756-EN2T dans un système à base d'automate GuardLogix
- Informations sur les modules de sécurité Guard I/O EtherNet/IP
- Mise à jour de la liste des types de données applicables aux points de sécurité
- Enregistrement dans le journal des actions de verrouillage ou de déverrouillage

- Enregistrement dans le journal de la création et de la suppression d'une signature de tâche de sécurité
- La procédure de téléchargement inclut maintenant la vérification de l'horloge maître pour la coordination du temps système (CST)
- Mise à jour de la description du code de défaut « Safety Task Inoperable » (Tâche de sécurité non opérationnelle)
- Possibilité d'accès à la valeur de la signature de sécurité via une instruction GSV
- Possibilité d'accès aux Informations de type de données pour les attributs via des instructions GSV et SSV
- Possibilité d'accès aux informations de défaut via une instruction GSV
- Mise à jour des informations d'homologation
- Mise à jour des informations sur l'estimation de la durée de vie de la pile
- Mise à jour des informations sur l'élimination réglementaire des piles

1756-UM020C-FR-P, Décembre 2006

- Présentation des possibilités de traitement des flux d'informations par un automate GuardLogix
- L'automate ne reconnaît pas les mises à jour du système d'exploitation au moyen de CompactFlash
- La tâche de sécurité ne reconnaît pas les instructions complémentaires ni le logiciel de gestion des alarmes et des événements FactoryTalk®
- Intervalle entre trames requis (RPI) maximum pour les connexions de sécurité ramené de 500 ms à 100 ms
- Remplacement de la liste des types de données non valides pour les programmes de sécurité a été par une liste des types de données valides
- Révision de la description des connexions de sécurité produites/ consommées
- Révision de la description des effets du verrouillage de la sécurité et de la signature de tâche de sécurité sur les téléchargements
- Ajout de la certification UL NRGF
- Ajout des valeurs de probabilité de défaillance sur sollicitation (PFD) et de probabilité de défaillance horaire (PFH) aux caractéristiques de l'automate

1756-UM020B-FR-P, Octobre 2005

Le logiciel de programmation RSLogix 5000 à partir de la version 14.01, ne compare plus les références du matériel entre le partenaire de sécurité et l'automate principal, ou entre l'automate et la signature de sécurité enregistrée dans le projet.

1756-UM020A-FR-P, Janvier 2005

1ère édition.

Numériques

A

B

C

D

E

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

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 manuels techniques, une foire aux questions, des notes techniques et des profils d'application, des exemples de code et des liens vers des mises à jour de logiciels (service pack). Vous y trouverez également la rubrique « MySupport », que vous pourrez personnaliser pour utiliser au mieux ces outils.

Pour une assistance technique supplémentaire par téléphone concernant l'installation, la configuration et le dépannage, nous vous proposons les programmes TechConnect^{SM}. Pour de plus amples informations, contactez votre distributeur ou représentant Rockwell Automation, ou allez sur le site http://www.rockwellautomation.com/support/.

Aide à l'installation

Si vous rencontrez un problème dans les 24 heures suivant l'installation du produit, consultez les informations contenues dans ce manuel. Vous pouvez également appeler l'Assistance clients pour obtenir de l'aide pour la mise en service de votre produit.

Pour les États-Unis et le Canada	1.440.646.3434
Pour les autres pays	Utilisez l'outil de recherche (Worldwide Locator) à l'adresse : http://www.rockwellautomation.com/support/americas/phone_en.html ou contactez votre représentant Rockwell Automation.

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 faire l'objet d'un retour, suivez la procédure ci-dessous.

Pour les États-Unis	Contactez votre distributeur. Vous devrez lui fournir un 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 nous sont utiles pour améliorer nos publications. Si vous avez des suggestions pour améliorer ce document, remplissez le formulaire de publication RA-DU002, disponible à l'adresse : http://www.rockwellautomation.com/literature/.

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-UM020I-FR-P – Août 2012