Manuel utilisateur

Traduction des instructions d'origine

Automates Compact GuardLogix® 5370

Références 1769-L30ERMS, 1769-L33ERMS, 1769-L33ERMOS, 1769-L36ERMS, 1769-L36ERMOS, 1769-L37ERMOS

Informations importantes destinées à l'utilisateur

Lire ce document et les documents répertoriés dans la section sur les ressources connexes relatifs à l'installation, la configuration et le fonctionnement de cet équipement avant d'installer, de configurer, de faire fonctionner ou de procéder à la maintenance du produit. Les utilisateurs doivent se familiariser avec les instructions traitant de l'installation et du câblage, en plus des exigences relatives à toutes les normes, réglementations et lois en vigueur.

Les opérations telles que l'installation, la mise au point, la mise en service, l'utilisation, l'assemblage, le désassemblage et la maintenance doivent être exécutées par des personnes qualifiées conformément au code de bonne pratique.

Si cet équipement est utilisé d'une façon non prévue par le fabricant, la protection qu'il fournit peut être altérée.

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

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

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

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

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

	**AVERTISSEMENT :** Actions ou situations susceptibles de provoquer une explosion en environnement dangereux et risquant d'entraîner des blessures pouvant être mortelles, des dégâts matériels ou des pertes financières.
	**ATTENTION :** Actions ou situations risquant d'entraîner des blessures pouvant être mortelles, des dégâts matériels ou des pertes financières. Ces mises en garde vous aident à identifier un danger, à éviter ce danger et à en discerner les conséquences.
IMPORTANT	Informations particulièrement importantes dans le cadre de l'utilisation du produit.

Des étiquettes peuvent également être placées à l'intérieur ou à l'extérieur d'un équipement pour avertir de dangers spécifiques.

	**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 élevées.
	**RISQUE D'ARC ÉLECTRIQUE :** L'étiquette ci-contre, placée sur l'équipement ou à l'intérieur (un centre de commande de moteur, par ex.) indique qu'un arc électrique eut se produire et provoquer des blessures graves pouvant être mortelles. Le personnel doit porter un équipement de protection individuelle (EPI) adapté et observer TOUTES les exigences réglementaires relatives à la sécurité au travail et à l'utilisation de l'équipement de protection individuelle (EPI).

Chapitre 7

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

Chapitre 8

Éléments d'une application de commande

Chapitre 9

Développement d'applications de sécurité

Chapitre 10

Développement d'applications de commande d'axe intégrée en réseau EtherNet/IP

Chapitre 11

Mise en ligne de l'automate

Chapitre 12

Surveillance de l'état et gestion des défauts

Chapitre 13

Enregistrement et chargement de programmes avec la carte Secure Digital

Cette publication contient des informations nouvelles et actualisées, comme indiqué dans le tableau suivant.

Sujet	Page
Références ajoutées 1769-L33ERMOS, 1769-L36ERMOS et 1769-L37ERMOS.	Partout
Ajout de la publication sur les automates Armor Compact GuardLogix au Tableau 2.	12
Ajout de trois paragraphes d'introduction au Chapitre 1.	15
Ajout de la mention « Accessible en tant que révision du firmware 30 » en note de bas de page relative à la référence 1769-L37ERMOS.	15, 19, 20, 25, 55, 71, 75, 81, 163
Déplacement du paragraphe d'introduction dans la section sur le système de commande Compact GuardLogix 5370 à la première page du Chapitre 1.	19
Les modifications suivantes ont été apportées au Tableau 1 : • Ajout de la rangée 1769-ERMOS • Ajout des informations sur l'alimentation secteur intégrée • Actualisation de la description du bouton de réinitialisation • Ajout des notes de bas de page 1 et 2	19
Ajout des rangées pour les nouvelles références et stations Ethernet correspondantes au Tableau 7.	71
Ajout du contenu du paragraphe d'introduction à la sous-section Correspondance des révisions du firmware.	168
Ajout de la note de bas de page au tableau dans la section Téléchargement.	171

Notes :

Ce manuel décrit les opérations à réaliser pour l'installation, la configuration, la programmation et l'utilisation d'un automate Compact GuardLogix® 5370. Ce manuel s'adresse à des automaticiens et des développeurs de systèmes de commande.

Les automates Compact GuardLogix 5370 constituent des solutions pour les petites et moyennes applications.

Terminologie

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

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 (protocole industriel commun)	Protocole de communication conçu pour les applications d'automatisation industrielle.
CIP Safety	Common Industrial Protocol – Safety Certified (CIP – certifié sécurité)	Version certifiée SIL 3/PLe du protocole CIP.
DC	Diagnostic Coverage (taux de couverture des tests de diagnostic)	Rapport entre le taux de défaillances détectées et le taux de défaillances totales.
DLR	Aneau de niveau dispositif	Protocole de communication qui permet à des appareils EtherNet/IP multi-port de fonctionner dans des topologies à anneau.
EN	European Norm (norme européenne)	Norme européenne de référence.
GSV	Get System Value (récupérer une valeur système)	Instruction destinée à récupérer une information d'état particulière de l'automate et à la placer dans un point de destination.
–	Multicast	Transmission d'informations par un expéditeur pour plusieurs destinataires.
NAT	Network Address Translation (traduction d'adresses réseau)	Traduction d'une adresse de protocole Internet (IP) à une adresse IP différente sur un autre réseau.
PFD	Probability of Failure on Demand (probabilité de défaillance sur sollicitation)	Probabilité moyenne de défaillance d'un système à exécuter sa fonction sur sollicitation.
PFH	Probability of Failure per Hour (probabilité de défaillance par heure)	Probabilité de survenue d'une panne dangereuse par heure sur un système opérationnel.
PL	Performance Level (niveau de performance)	Classification de sécurité ISO 13849-1.
RPI	Requested Packet Interval (intervalle entre trames requis)	Fréquence de transmission attendue des trames de données pour les communications en réseau.
SNN	Safety Network Number (numéro de réseau de sécurité)	Numéro unique qui identifie une section d'un réseau de sécurité.
SSV	Set System Value (définir une valeur système)	Instruction qui définit les données système d'un automate.
–	Standard	Objet, tâche, point, programme ou composant de votre projet qui n'est pas un composant de sécurité.
–	Unicast	Transmission d'informations par un expéditeur pour un destinataire.

Documentation connexe

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

Documentation	Description
GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual, publication 1756-RM099	Fournit des informations sur les exigences en matière d'application de sécurité pour les automates GuardLogix 5570 et Compact GuardLogix 5370 dans les applications Studio 5000 Logix Designer.
Instructions d'installation des automates Armor Compact GuardLogix, publication 1769-IN022	Fournit des informations sur l'installation, le montage et la connexion des automates Armor Compact GuardLogix à un réseau.
1769-SDN DeviceNet Scanner Module User Manual, publication 1769-UM009	Décrit l'utilisation du module scrutateur 1769-SDN avec les automates Compact GuardLogix.
ControlLogix High-speed Counter Module User Manual, publication 1769-UM006	Décrit le fonctionnement du module de comptage rapide autonome 1769-HSC avec les automates Compact GuardLogix.
Compact I/O™ DeviceNet Scanner Module Installation Instructions, publication 1769-IN060	Décrit l'installation des modules d'E/S Compact I/O.
Compact I/O Expansion Power Supplies Installation Instructions, publication 1769-IN028	Décrit le câblage du module d'alimentation Compact I/O 1769.
Compact I/O Modules Installation Instructions, publication 1769-IN088	Décrit l'installation des modules Compact I/O 1769 avec n'importe quel automate Compact GuardLogix.
CompactLogix™ Controllers Specifications Technical Data, publication 1769-TD005	Fournit les caractéristiques d'automate CompactLogix de tous les automates Compact GuardLogix.
CompactLogix System Selection Guide, publication 1769-SG001	Fournit des informations sur les produits utilisables dans les systèmes de commande Compact GuardLogix afin de vous aider dans la conception d'une solution de commande.
Ethernet Design Considerations Reference Manual, publication ENET-RM002	Décrit les notions nécessaires pour concevoir un système de commande incluant un réseau EtherNet/IP : • présentation d'EtherNet/IP ; • infrastructure Ethernet ; • protocole EtherNet/IP.
EtherNet/IP embedded Switch Technology Application Guide, publication ENET-AP005	Décrit l'utilisation d'une topologie de réseau à anneau de niveau dispositif.
EtherNet/IP Socket Interface Application Technique, publication ENET-AT002	Décrit les applications d'interface de connexion.
Execution Time and Memory Use for Logix5000™ Controller Instructions Reference Manual, publication 1756-RM087	Explique comment estimer l'utilisation de la mémoire et le temps d'exécution de la logique programmée, et comment sélectionner différentes options de programmation.
Integrated Architecture® and CIP Sync Configuration Application Technique, publication IA-AT003	Présente la technologie CIP Sync et le principe de synchronisation des horloges dans le système Integrated Architecture de Rockwell Automation®.
Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, publication MOTION-UM003	Décrit comment configurer une application de commande de mouvement intégrée sur EtherNet/IP et comment démarrer cette solution de commande de mouvement avec un système Logix5000.
Servovariateurs Kinetix® 5500 – Manuel utilisateur, publication 2198-UM001	Fournit des informations sur l'installation, la configuration, le démarrage, et le dépannage de votre système servovariateur Kinetix 5500. Inclut également les exigences pour l'utilisation des variateurs Kinetix 5500 dans des applications de sécurité.
Kinetix 5700 Servo Drives User Manual, publication 2198-UM002	Fournit des informations sur l'installation, la configuration, le démarrage, et le dépannage de votre système servovariateur Kinetix 5700. Inclut également les exigences pour l'utilisation des variateurs Kinetix 5700 dans des applications de sécurité.
Logix5000 Controllers Common Procedures Programming Manual, publication 1756-PM001	Guide les utilisateurs de tout niveau dans les procédures d'élaboration de projets pour les automates Logix5000 et fournit des liens vers des guides particuliers pour des compléments d'informations sur des sujets tels que l'importation/exportation, les messages, la sécurité et la programmation dans différents langages.
Logix5000 Controllers Design Considerations Reference Manual, publication 1756-RM094	Fournit aux utilisateurs expérimentés des recommandations sur l'optimisation du système ainsi que des informations système facilitant les choix en matière de conception du système.
Logix Controllers Instructions Reference Manual, publication 1756-RM009	Fournit des informations sur le jeu d'instructions Logix5000 qui inclut des instructions générales, des instructions de commande de mouvement et de process.
Logix5000 Controllers Motion Instructions Reference Manual, publication MOTION-RM002	Décrit comment programmer l'automate pour les applications de commande de mouvement.
Logix5000 Controllers Nonvolatile Memory Card Programming Manual, publication 1756-PM017	Décrit la mise sous tension de l'automate et les situations d'altération de la mémoire.
Logix5000 Controllers Process Control/Drives Instruction Set Reference Manual, publication 1756-RM006	Explique comment programmer l'automate pour les applications de process.

Documentation	Description
PowerFlex® 527 Adjustable Frequency AC Drive User Manual, publication 520-UM002	Fournit des informations sur l'installation, le démarrage, et le dépannage des variateurs de fréquence c.a. PowerFlex de la série 520.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Fournit des recommandations générales pour l'installation d'un système industriel Rockwell Automation®.
Site Internet sur les certifications de produit, http://www.rockwellautomation.com/rockwellautomation/certification/overview.page	Fournit des déclarations de conformité, des certificats et autres informations relatives aux homologations.

Vous pouvez visualiser et télécharger ces publications à l'adresse http://www.rockwellautomation.com/global/literature-library/overview.page.

Pour commander des exemplaires imprimés de documentation technique, contactez votre distributeur Allen-Bradley ou votre agence commerciale Rockwell Automation.

Notes :

Présentation du système

Les automates Compact GuardLogix 5370 proposent des composants de commande, de communication et d'E/S de pointe regroupés dans un système de commande distribuée. Cette gamme comprend les automates Compact GuardLogix suivants :

- 1769-L30ERMS
- 1769-L33ERMS
- 1769-L33ERMOS
- 1769-L36ERMS
- 1769-L36ERMOS
- 1769-L37ERMOS(1)

L'automate Armor™ Compact GuardLogix (1769-L33ERMOS, 1769-L36ERMOS, ou 1769-L37ERMOS(1)) combine un automate Compact GuardLogix avec une alimentation secteur dans un boîtier certifié IP67 destiné à être monté sur une machine. Pour de plus amples informations sur l'installation de l'automate Armor Compact GuardLogix, reportez-vous à la publication « Installation des automates Armor Compact GuardLogix », 1769-IN022.

Pour une description complète des composants et des fonctionnalités des systèmes de commande CompactLogix 5370, reportez-vous respectivement au Tableau 1 et au Tableau 2.

(1) Accessible en tant que révision du firmware 30.

Exigences de l'application de sécurité

Le système de commande Compact GuardLogix® 5370 est certifié pour une utilisation dans des applications de sécurité jusqu'au niveau d'intégrité de sécurité (SIL) 3 et au niveau de performance (PL)e inclus, pour lesquelles la condition de sécurité est l'état hors 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 les exigences relatives aux systèmes de sécurité SIL 3 et PLe, notamment les intervalles pour les tests de validation fonctionnelle, les temps de réponse du système et les calculs de PFD/PFH, reportez-vous à la publication 1756-RM099, « GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual ». Vous devez lire, comprendre et répondre à ces exigences préalablement à la mise en exploitation d'un système de sécurité Compact GuardLogix SIL 3, PLe.

Les applications de sécurité SIL 3/PLe requièrent 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 de plus amples informations, reportez-vous à la publication 1756-RM099, « GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual ».

Numéro de réseau de sécurité

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 dispositif CIP Safety doit également être configuré avec le SNN du sous-réseau de sécurité. Le SNN peut être attribué automatiquement ou manuellement.

Pour de plus amples informations sur l'attribution du numéro SNN, voir Gestion du numéro de réseau de sécurité (SNN), page 64.

Signature de tâche de sécurité

La signature de tâche de sécurité est constituée par un numéro d'identification, une date et une heure. Ces paramètres identifient de façon unique la partie sécurité d'un projet. Elle s'applique au programme, aux données et à la configuration de sécurité. Le système Compact 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.

Reportez-vous à Génération d'une signature de tâche de sécurité, page 158, pour plus d'informations.

Distinction entre composants standard et composants de sécurité

Les logements en fond de panier d'un système Compact GuardLogix qui ne sont pas utilisés par la sécurité peuvent être occupés par d'autres modules CompactLogix certifiés conformes aux Directives Basse Tension et CEM.

Reportez-vous à l'adresse http://www.rockwellautomation.com/global/certification/overview.page pour consulter le certificat CE de la gamme d'automates programmables CompactLogix et déterminer les modules qui sont certifiés.

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, l'application Logix Designer comporte des icônes d'identification de la sécurité permettant de reconnaître la tâche de sécurité, les programmes de sécurité, les sous-programmes de sécurité et les composants de sécurité. En outre, l'application Logix Designer utilise un attribut de classe sécurité qui apparaît dès que vous affichez les propriétés de la tâche de sécurité, des programmes de sécurité, d'un sous-programme 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 dispositifs d'interface homme-machine (IHM) externes ou via des instructions de message provenant d'automates homologues. L'application Logix Designer peut écrire dans des points de sécurité lorsque la sécurité de l'automate Compact GuardLogix est déverrouillée, qu'il ne possède pas de signature de tâche de sécurité et qu'il fonctionne sans défauts de sécurité.

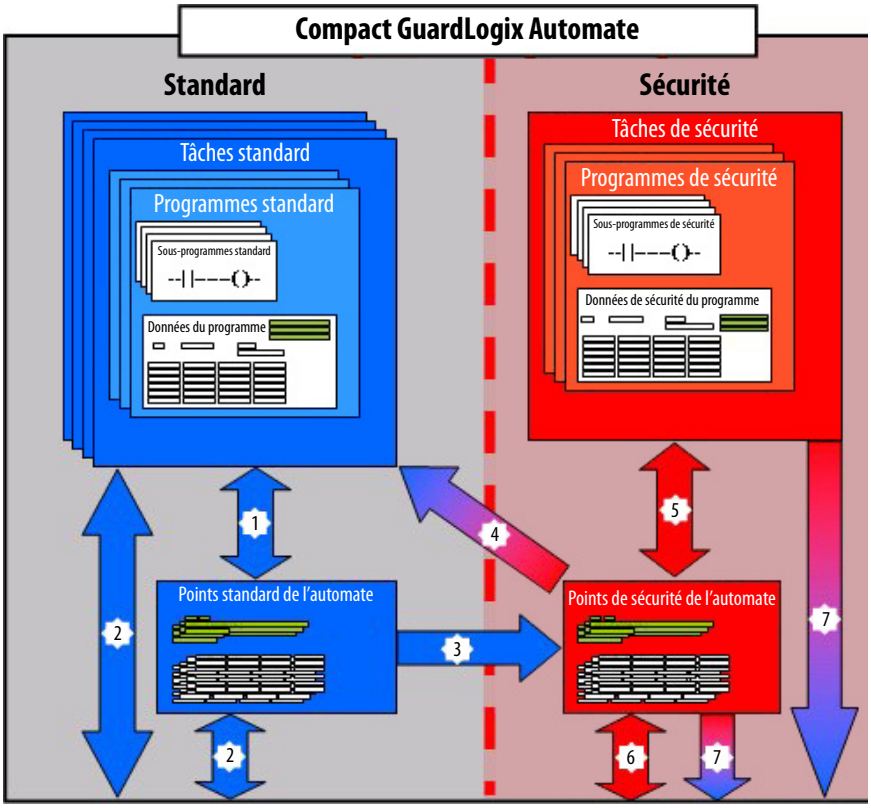
Dispositifs IHM

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

Capacités de flux de données de l'automate

La Figure 1 illustre les capacités de flux de données standard et de sécurité de l'automate Compact GuardLogix.

Figure 1 – Capacités de flux de données



N°	Description	
1	Les points et le programme standard se comportent comme 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	Compact GuardLogix Les automates intègrent la possibilité de déplacer (mapper) des données de points standard dans des points de sécurité de façon à permettre leur utilisation dans des tâches 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 entre des automates de sécurité sur un réseau Ethernet, notamment des automates GuardLogix 5570 et Compact GuardLogix 5370.	
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 que ces données sont lues, elles sont considérées comme standard et non plus comme données SIL 3/PLe.

Système de commande Compact GuardLogix 5370

Le Tableau 1 décrit les composants utilisés dans un système de commande Compact GuardLogix 5370 type.

Tableau 1 – Composants système

Composant système	Description
Automate	L'un des automates décrits dans ce document.
Alimentation	L'une des alimentations Compact I/O 1769 suivantes : • 1769-PA2 • 1769-PB2(2) • 1769-PA4 • 1769-PB4
Composants des réseaux de communication	L'un des supports de communication suivants : • Réseau EtherNet/IP utilisant les ports réseau EtherNet/IP intégrés (communications de sécurité et standard) • Réseau DeviceNet via un module 1769-SDN (uniquement pour communication standard)(3) • Connexion USB (uniquement pour la programmation ou les mises à jour du firmware)
Logiciel	• Application Logix Designer, version 28.00.00 ou ultérieure • Logiciel RSLinx® Classic, version 3.80.*xx* ou ultérieure • Logiciel RSNetWorx™ for DeviceNet, version 25.00.00 ou ultérieure
Carte Secure Digital (SD) pour stockage en mémoire non volatile externe	• Carte 1784-SD1 – Livrée avec l'automate Compact GuardLogix 5370 et fournissant 1 Go de mémoire • Carte 1784-SD2 – Livrable séparément et fournissant 2 Go de mémoire
Modules des E/S(1)	• Modules d'extension locaux – Modules Compact I/O 1769 • E/S distribuées – Plusieurs familles de modules des E/S en réseau DeviceNet et EtherNet/IP
Bouton de réinitialisation	Si ce bouton est enfoncé et maintenu enfoncé à la mise sous tension de l'automate, il efface le programme utilisateur de la mémoire interne de l'automate et du partenaire de sécurité interne.

(1) Les systèmes de commande Compact GuardLogix Armor ne prennent pas en charge les E/S dans leur boîtier certifié IP67. Pour obtenir les E/S, vous devez connecter EtherNet/IP aux E/S distribuées.
(2) Dans les systèmes de commande Compact GuardLogix Armor, cette alimentation secteur est intégrée à leur boîtier certifié IP67.
(3) Pour les communications de sécurité, un module passerelle Ethernet à DeviceNet est requis ; voir page 100.

Fonctionnalité de l'automate

Le Tableau 2 décrit les fonctionnalités disponibles sur les automates Compact GuardLogix 5370.

Tableau 2 – Fonctionnalités des automates CompactLogix 5370

N° réf.	Nombre de tâches automate gérées	Nombre de programmes gérés par tâche	Solution de stockage d'énergie interne	Prise en charge des réseaux EtherNet/IP	Distance nominale de l'alimentation	Taille de la mémoire utilisateur embarquée (Mo)		Prise en charge de modules Compact I/O locaux	Axes de mouvement
						Standard	Sécurité		
1769-L30ERMS	32(2)	100	Oui – Supprime la nécessité d'une pile	Accepte les topologies suivantes : • Anneau de niveau dispositif (DLR) • Linéaire • Étoile traditionnelle	4	1	0.5	Autant que 8	4
1769-L33ERMS						2	1	Autant que 16	8
1769-L33ERMOS								–	
1769-L36ERMS						3	1.5	Autant que 30	16
1769-L36ERMOS								–	
1769-L37ERMOS(1)									

(1) Accessible en tant que révision du firmware 30.
(2) Inclut une tâche de sécurité.

Exigences de programmation

Utilisez le Tableau 3 pour identifier l'outil de programmation et les versions à utiliser avec vos automates Compact GuardLogix 5370.

Tableau 3 – Versions des logiciels

N° réf.	Environnement Studio 5000®	Version du logiciel RSLinx Classic
1769-L30ERMS 1769-L33ERMS 1769-L33ERMOS 1769-L36ERMS 1769-L36ERMOS 1769-L37ERMOS(1)	28.00.00 ou ultérieure	3.80 ou ultérieure

(1) Accessible en tant que révision du firmware 30.

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 4 – Fonctions prises en charge

Fonction	Application Studio 5000 Logix Designer	
	Tâche de sécurité	Tâche standard
Alarmes et événements		X
Carte mémoire	X	
Commande d'axe intégrée		
Commutation de langues	X	
Connexions d'envoi individuel pour des points de sécurité produits et consommés		
Connexions standard et de sécurité		
Connexions unicast pour des modules des E/S de sécurité sur les réseaux EtherNet/IP		
Contrôle d'accès aux données		
Diagrammes de blocs fonctionnels (FBD)		
Firmware Supervisor	X	
Import et export en ligne d'éléments de programme		
Instructions complémentaires	X	
Journal automate		
Logique à relais		
Sous-programmes de phases d'équipement		
Sous-programmes en graphe de fonctionnement séquentiel (SFC)		
Tâches événementielles		
Texte structuré		
Traduction d'adresses réseau (NAT)	X	

Pour de plus amples informations sur l'utilisation de ces fonctions, reportez-vous à la publication 1756-PM001, « Logix5000™ Controllers Common Procedures Programming Manual », aux publications répertoriées au paragraphe Documentation connexe, page 12, ainsi qu'à l'aide en ligne.

Installation de l'automate

Précautions

ATTENTION : Environnement et armoire de protection

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 norme CEI 60664-1), et à une altitude maximum de 2000 m sans déclassement.

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, correspondant à un indice de propagation de 5 VA ou être approuvée pour l'application dans le cas d'une armoire non 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, il est recommandé de consulter :

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

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  II 3 G. De tels modules :

- Sont des équipements du groupe II, de catégorie 3, et sont conformes aux exigences essentielles en matière de santé et de sécurité relatives à la conception et à la fabrication de tels équipements, présentées à l'annexe II de la directive 94/9/CE. Pour plus de détails, consultez la Déclaration de conformité CE à l'adresse http://www.rockwellautomation.com/global/certification/overview.page. Le type de protection utilisé est « Ex nA IIC T5 Gc » conformément à la norme EN 60079-15. Le code de température spécifique est marqué sur le produit.
- Sont destinés à être utilisés dans des environnements dans lesquels des atmosphères explosives provoquées par des gaz, vapeurs, brouillards, ou mélanges d'air ou de poussière sont peu susceptibles de se produire, ou sont susceptibles de se produire uniquement en de rares occasions et pendant de brèves périodes. De tels emplacements correspondent à la classification en Zone 2 conformément à la directive ATEX 1999/92/CE.
- Peuvent avoir des références se terminant par la lettre 'K' pour indiquer la présence d'un revêtement de protection.
- Sont conformes aux normes EN60079-0:2002+A11:2013, EN 60079-15:2010, numéro de certificat de référence DEMKO 15ATEX1388X

AVERTISSEMENT : Conditions spéciales d'utilisation sûre :

- Cet équipement doit être monté dans une armoire homologuée ATEX présentant au minimum un indice de protection IP54 (conformément à la définition CEI 60529) et utilisé dans un environnement n'excédant pas le degré de pollution 2 (conformément à la définition CEI/EN 60664-1) lorsqu'il est implanté dans des environnements de Zone 2. L'enceinte doit utiliser un capot ou une porte amovible à l'aide d'un outil.
- Cet équipement doit être utilisé dans les limites nominales définies par Rockwell Automation.
- Des précautions doivent être prises afin d'éviter un dépassement de plus de 140 % de la tension nominale par les perturbations transitoires lors d'une utilisation dans des environnements de Zone 2.
- Cet équipement ne doit être utilisé qu'avec des bus intermodules Rockwell Automation homologués ATEX.
- Fixer de façon sûre tous les raccordements externes à cet équipement au moyen de bornes à vis ou à ressort, de connecteurs filetés ou de tout autre accessoire fourni avec le produit.
- Ne pas déconnecter l'équipement tant que son alimentation n'est pas coupée ou que l'environnement est réputé non dangereux.

Composants de l'automate Compact GuardLogix 5370

Les composants suivants sont inclus dans le carton de livraison de l'automate :

- L'automate proprement-dit (référence particulière selon votre commande) ;
- Une carte mémoire SD 1784-SD1 d'une capacité d'1 Go.

  Une carte mémoire SD 1784-SD2 d'une capacité de 2 Go, ainsi que des cartes SD 1784-SD1 supplémentaires peuvent également être fournies si vous avez besoin de plus de capacité de stockage.

IMPORTANT La durée de vie prévisible de la mémoire non volatile dépend du nombre de cycles d'écriture réalisés. Le support non volatile utilise une technique de répartition de l'usure afin de prolonger la durée de service, mais il convient d'éviter les écritures trop fréquentes.

Évitez des écritures fréquentes lors de l'enregistrement de données. Il est recommandé d'enregistrer les données dans une mémoire tampon de l'automate et de limiter le nombre des écritures de ces données sur le support mémoire amovible.

Installation de la carte SD

Les automates Compact GuardLogix® 5370 sont expédiés départ usine avec la carte SD 1784-SD1 installée.

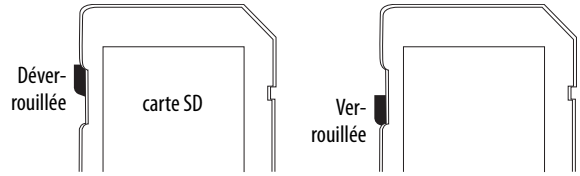
Suivez les étapes ci-dessous pour remonter dans l'automate une carte SD retiré ou pour installer une nouvelle carte SD dans l'automate.

Il est recommandé de laisser la carte SD dans l'automate, même lorsqu'elle n'est pas utilisée. Si un défaut majeur non récupérable se produit sur l'automate, les informations détaillées sur le défaut sont enregistrées sur la carte.

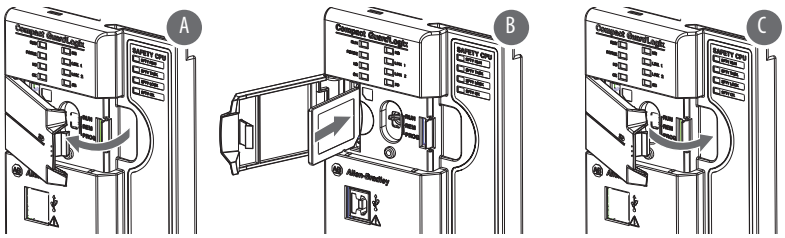
AVERTISSEMENT : Quand vous insérez ou retirez la carte SD alors que l'automate est sous tension un arc électrique peut se produire, susceptible de provoquer une explosion dans des installations en environnement dangereux.

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

1. Vérifiez que la carte SD est verrouillée ou déverrouillée, selon votre préférence. Lorsque vous décidez de verrouiller la carte avant de l'installer, tenez compte du point suivant :
   - Si la carte est déverrouillée, l'automate pourra y écrire ou lire les données.



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



3. Insérez la carte SD dans son logement.

   Vous ne pouvez monter la carte SD que dans un seul sens. Le coin biseauté se trouve en haut. Un repère est imprimé sur la carte.

   Si vous sentez une résistance lors de l'insertion de la carte SD, retirez-la et changez son orientation.

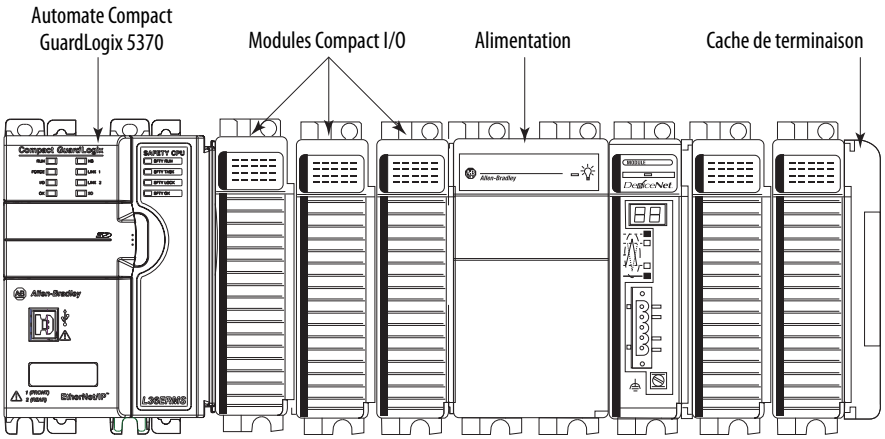
4. Appuyez doucement sur la carte jusqu'à ce qu'elle s'enclenche en position (B).
5. Fermez la trappe du logement de la carte SD (C).

Il est recommandé de maintenir la trappe du logement de carte SD fermée pendant le fonctionnement normal du système. Pour de plus amples informations sur la carte SD, reportez-vous au Chapitre 13.

Planification du système

Lorsque vous planifiez votre système de commande Compact GuardLogix 5370, tenez compte des points suivants :

- L'automate doit toujours être placé à l'extrême gauche du système.
- Un seul automate peut être utilisé sur un CompactBus 1769 local. L'automate prend en charge la rangée locale et jusqu'à deux rangées supplémentaires.
- La distance nominale de l'automate par rapport à l'alimentation est de quatre. Cette distance nominale signifie que l'automate doit être à moins de quatre emplacements de l'alimentation. Vous pouvez installer un maximum de trois modules entre l'alimentation et l'automate, comme illustré sur le graphique suivant.



- Les automates peuvent gérer, sur plusieurs rangées d'E/S, le nombre maximum de modules d'extension locaux suivant :

N° réf.	Nombre max. de modules d'extension locaux pris en charge
1769-L30ERMS	8
1769-L33ERMS	16
1769-L33ERMOS	–
1769-L36ERMS	30
1769-L36ERMOS 1769-L37ERMOS(1)	–

(1) Accessible en tant que révision du firmware 30.

- Chaque rangée d'E/S nécessite sa propre alimentation.
- Vous devez terminer l'extrémité de la dernière rangée d'un système de commande Compact GuardLogix 5370. Vous devez terminer une rangée à l'extrémité gauche ou droite de la rangée en fonction de la conception de votre système.

  Un cache de terminaison 1769-EC*x* est nécessaire pour terminer l'extrémité de la dernière rangée du système de commande.

  Par exemple, si un système de commande Compact GuardLogix 5370 n'utilise qu'une seule rangée, vous devez utiliser un cache de terminaison droit 1769-ECR pour terminer l'extrémité droite de la rangée.

  Reportez-vous à Implantation physique des modules des E/S, page 89, pour les exigences liées aux modules d'extension locaux Compact I/O.

Pour des exemples de systèmes de commande Compact GuardLogix 5370 qui utilisent une ou plusieurs rangées, voir Monter le système, page 27.

ATTENTION : Les systèmes de commande Compact GuardLogix 5370 ne permettent pas le retrait et l'insertion sous tension (RIUP). Les événements suivants se produisent pendant que le système de commande Compact GuardLogix 5370 est sous tension :

- toute coupure de la liaison entre l'alimentation et l'automate (par exemple le retrait de l'alimentation, de l'automate ou d'un module d'E/S) peut exposer le circuit logique à des transitoires dépassant les seuils prévus par conception et endommager les composants système ou entraîner un comportement imprévisible ;
- le retrait d'un cache de terminaison ou d'un module d'E/S met l'automate en défaut et peut également endommager les composants système.

Assembler le système

Vous pouvez relier un module Compact I/O™ ou une alimentation Compact I/O 1769 adjacent à l'automate Compact GuardLogix 5370 avant ou après son montage. Pour les instructions de montage, voir Dimensions du système, page 29 ou Montage de l'automate sur un panneau, page 30.

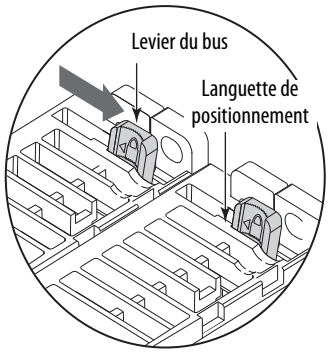
ATTENTION : Ne pas retirer ou remplacer le module quand le système est sous tension. L'interruption du bus intermodules peut provoquer un fonctionnement ou des mouvements imprévisibles de la machine.

AVERTISSEMENT : Couper l'alimentation avant d'insérer ou de retirer ce module. Si vous insérez ou retirez un module avec le bus intermodules sous tension un arc électrique peut se produire, susceptible de provoquer une explosion dans des installations en environnement dangereux.

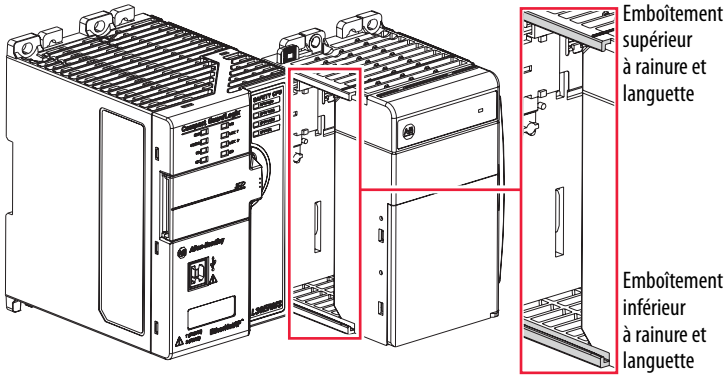
Assurez-vous que l'alimentation est coupée ou que l'environnement est classé non dangereux avant de poursuivre.

Suivez les étapes ci-dessous pour installer l'automate. L'exemple suivant explique comment attacher une alimentation Compact I/O 1769 à l'automate.

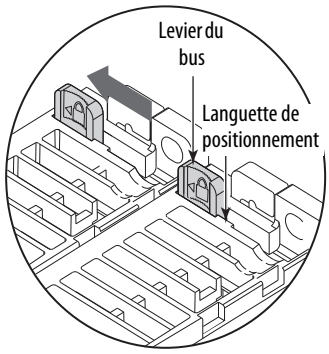
1. Assurez-vous que l'alimentation secteur est coupée.
2. Utilisez les doigts ou un petit tournevis pour repousser légèrement le levier de bus de l'alimentation Compact I/O afin de dégager la languette de positionnement.
3. Amenez le levier de bus sur la droite de la languette de positionnement pour le mettre en position déverrouillée.



4. Utilisez les emboîtements à rainure et languette supérieur et inférieur pour accoupler l'automate et l'alimentation.



5. Faites coulisser l'alimentation le long des rainures vers l'arrière jusqu'à ce que les connecteurs de bus soient alignés.
6. Utilisez les doigts ou un petit tournevis pour repousser légèrement le levier de bus de l'alimentation afin de dégager la languette de positionnement.
7. Amenez le levier de bus de l'alimentation vers la gauche de la languette de positionnement jusqu'à ce qu'il s'enclenche ; vérifiez qu'il est verrouillé.



8. Si votre système ne possède pas de modules d'extension locaux, utilisez le système d'emboîtement décrit précédemment pour fixer un cache de terminaison 1769-ECR Compact I/O sur le dernier module du système.

IMPORTANT	Vous devez installer un cache de terminaison sur le côté droit du système de commande Compact GuardLogix 5370 à l'extrémité de l'automate ou de tout module d'extension local éventuellement installé sur l'automate.

9. Câblez l'alimentation Compact I/O 1769 conformément aux instructions fournies dans la publication 1769-IN028, « Compact I/O Expansion Power Supplies Installation Instructions ».

   Si vous utilisez des modules d'extension locaux, reportez-vous à Modules d'extension locaux, page 81.

Monter le système

ATTENTION : L'automate doit être monté sur une surface avec une mise à la terre correcte, tel qu'un panneau métallique. Des connexions de mise à la terre supplémentaires à partir des pattes de fixation de l'alimentation ou du rail DIN (le cas échéant) ne sont pas nécessaires, sauf si le plan de montage ne peut pas être raccordé à la terre.

Reportez-vous à la publication de Rockwell Automation 1770-4.1, « Industrial Automation Wiring and Grounding Guidelines », pour de plus amples informations.

Vous pouvez monter un système de commande Compact GuardLogix 5370 sur un panneau ou un rail DIN.

ATTENTION : Pendant le montage des différents dispositifs sur le panneau ou le rail DIN, veillez à ce qu'aucun déchet (copeaux de métal ou brins de fil, par exemple) ne pénètre à l'intérieur de l'automate. Les débris tombés à l'intérieur de l'automate peuvent provoquer des dégâts lors de sa mise sous tension.

Un système de commande Compact GuardLogix 5370 doit être monté de façon à ce que les modules soient alignés horizontalement les uns par rapport aux autres. Si vous répartissez les modules sur plusieurs rangées, ces rangées peuvent être placées verticalement ou horizontalement les unes par rapport aux autres.

La Figure 2 illustre des exemples incluant des modules d'extension locaux.

Figure 2 – Exemple de rangées et de configurations système

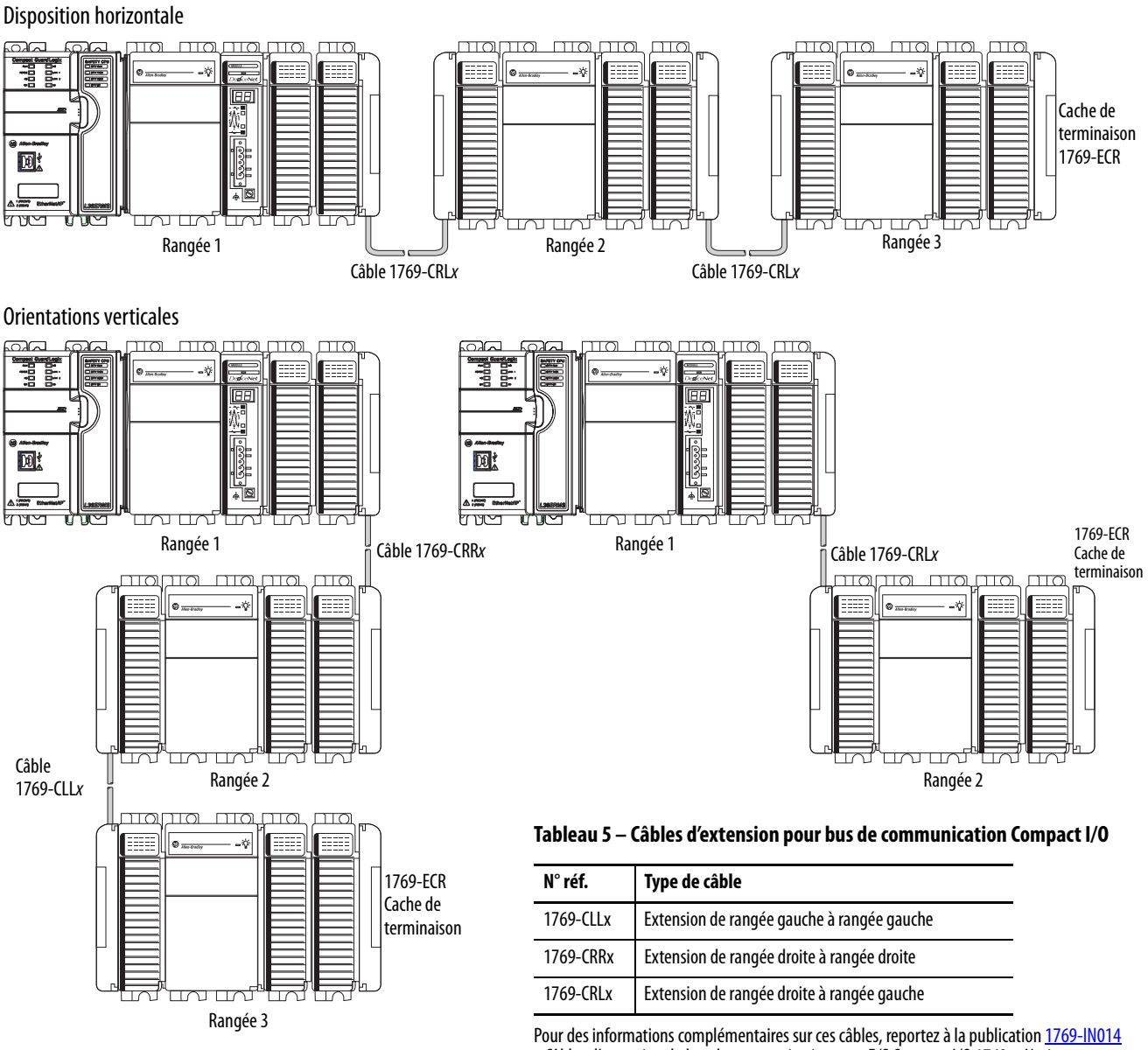


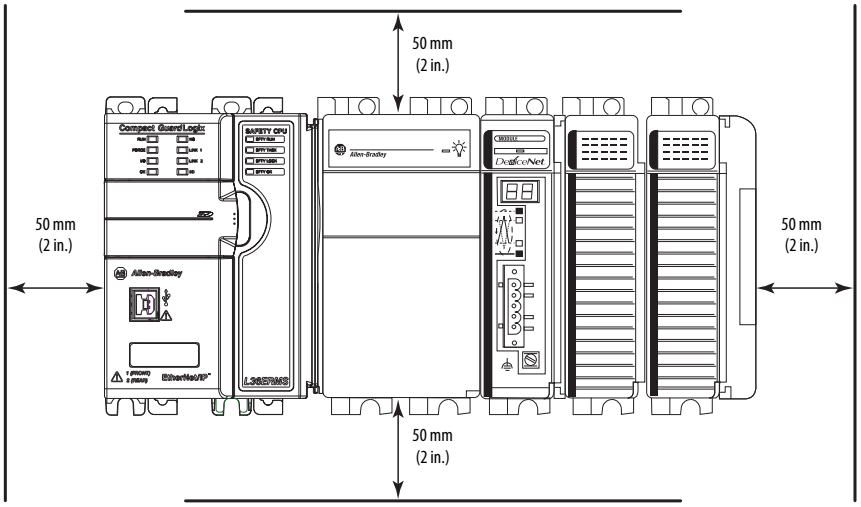
Tableau 5 – Câbles d'extension pour bus de communication Compact I/O

N° réf.	Type de câble
1769-CLLx	Extension de rangée gauche à rangée gauche
1769-CRRx	Extension de rangée droite à rangée droite
1769-CRLx	Extension de rangée droite à rangée gauche

Pour des informations complémentaires sur ces câbles, reportez à la publication 1769-IN014 « Câbles d'extension du bus de communication pour E/S Compact I/O 1769 – Notice d'installation ».

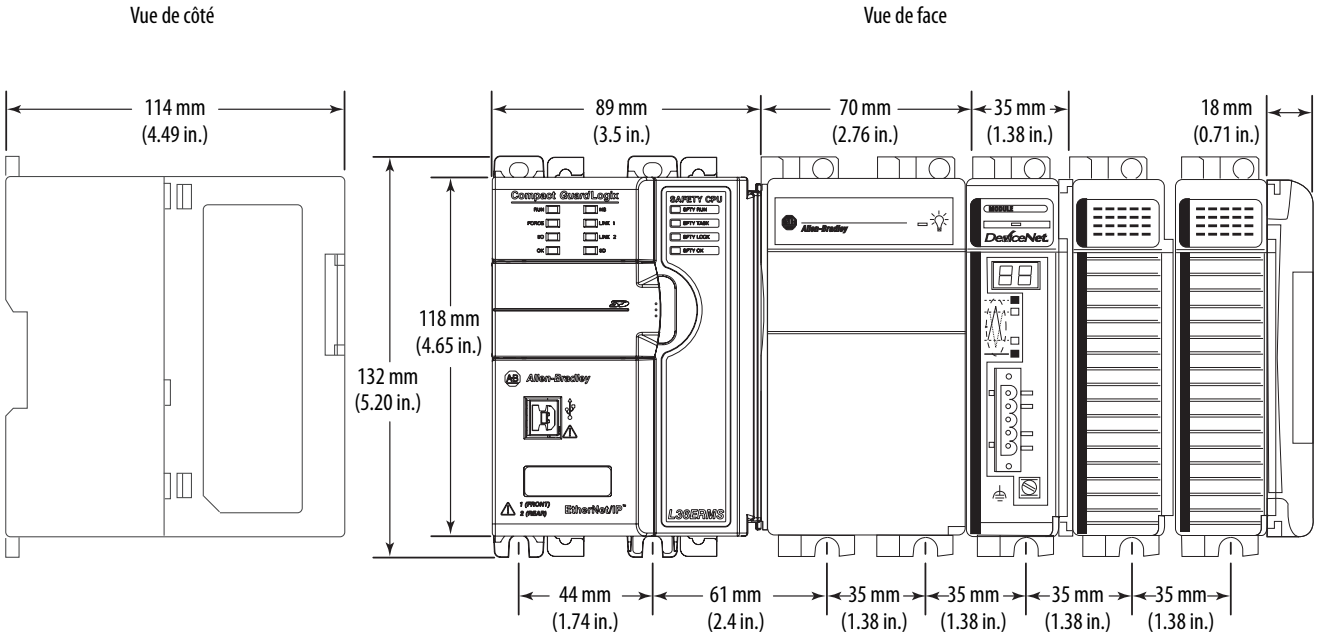
Dégagement minimum

Vous devez respecter une distance minimum par rapport aux parois de l'enceinte, chemins de câbles et équipements adjacents. Laissez un dégagement minimum de 50 mm de tous les côtés, comme illustré. Ce dégagement permet d'assurer la ventilation et l'isolation électrique.



Dimensions du système

La figure ci-dessous indique les dimensions d'un système.



Montage de l'automate sur un panneau

Utilisez deux vis M4 ou N° 8 à tête cylindrique bombée pour fixer l'automate. Des vis de montage sont nécessaires sur de nombreux modules. La procédure suivante consiste à utiliser un assemblage de modules comme gabarit pour le perçage du panneau.

IMPORTANT En raison de la tolérance permise pour l'espacement des trous de fixation du module, il est important de respecter la procédure suivante :

1. Assemblez trois modules maximum sur une surface de travail propre.
2. Utilisez les modules assemblés comme gabarit pour marquer avec soin le centre de tous les trous de montage sur le panneau.
3. Reposez les modules assemblés sur la surface de travail, ainsi que tout module précédemment monté.
4. Percez et taraudez les trous de montage pour les vis M4 ou n° 8 recommandées.
5. Repositionnez les modules sur le panneau et vérifiez si l'alignement des trous est correct.

   CONSEIL Lorsque le module est monté sur panneau, c'est la plaque de mise à la terre (à l'endroit où les vis de montage sont installées) qui met le module à la terre.

6. Utilisez les vis de montage pour fixer les modules au panneau.

   CONSEIL Si vous devez installer des modules supplémentaires, ne montez que le dernier module du groupe et laissez les autres de côté. Ceci réduira les temps de dépose/remontage lors du perçage et du taraudage des trous de fixation du groupe de modules suivant.

7. Répétez les étapes 1 à 6 pour les éventuels modules restants.

Montage de l'automate sur un rail DIN

Vous pouvez monter l'automate Compact GuardLogix 5370 sur les types de rails DIN suivants :

- EN 50 022 de 35 x 7,5 mm
- EN 50 022 de 35 x 15 mm

ATTENTION : Cet automate est relié à la terre du châssis par le rail DIN. Utilisez un rail DIN en acier zingué chromaté jaune pour garantir une bonne mise à la terre. L'utilisation de rails DIN en d'autres matières (par exemple, en aluminium ou en plastique) pouvant se corroder et s'oxyder ou présenter une mauvaise conduction, peut se traduire par une mise à la terre incorrecte ou intermittente. Fixez le rail DIN au plan de montage tous les 200 mm environ et utilisez des ancrages d'extrémité appropriés.

1. Avant d'installer l'automate sur le rail DIN, placez les loquets de fixation de l'automate sur le rail en position fermée.
2. Pressez la zone de contact de l'automate avec le rail DIN contre ce dernier.

   Les loquets s'ouvrent momentanément et se referment sur le rail pour verrouiller le module en place.

Raccordement de l'alimentation du système de commande

La façon de raccorder l'alimentation à votre système de commande Compact GuardLogix 5370 dépend de l'alimentation Compact I/O 1769 que votre application utilise. Pour de plus amples informations sur le raccordement de l'alimentation à votre système, reportez-vous à la publication 1769-IN028 « Compact I/O Expansion Power Supplies Installation Instructions ».

Raccordement à l'automate via un câble USB

L'automate Compact GuardLogix 5370 dispose d'un port USB équipé d'une fiche de type B. Le port est compatible USB 2.0 et fonctionne à 12 Mbit/s.

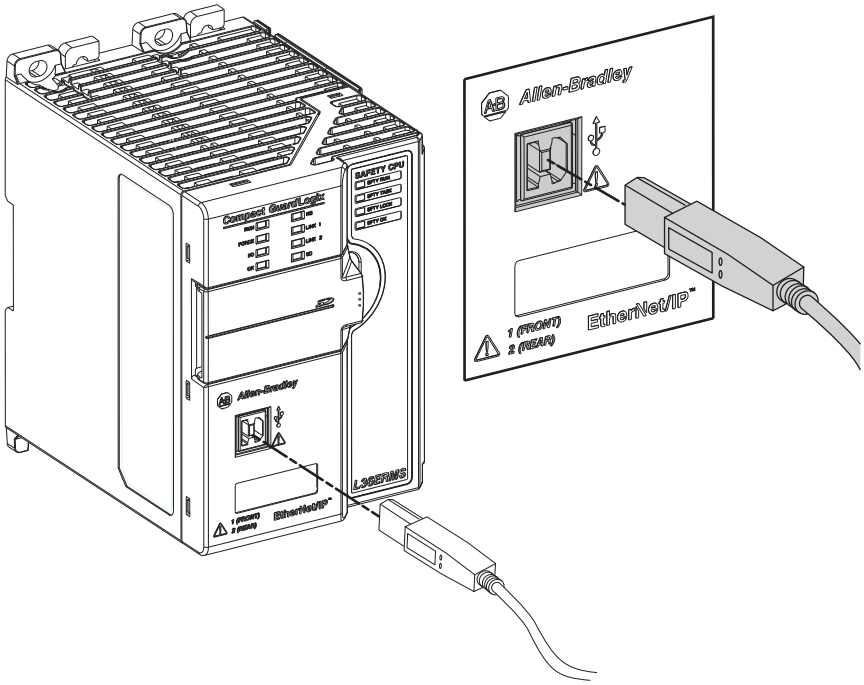
Utilisez un câble USB pour raccorder votre ordinateur au port USB. Avec cette connexion, vous pourrez mettre à jour le firmware et charger des programmes sur l'automate directement depuis votre ordinateur.

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

Le câble USB ne doit pas dépasser une longueur de 3,0 m (9,84 pieds) et il ne doit pas y avoir de concentrateurs.

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

Branchez le câble USB sur l'automate Compact GuardLogix 5370 comme illustré.



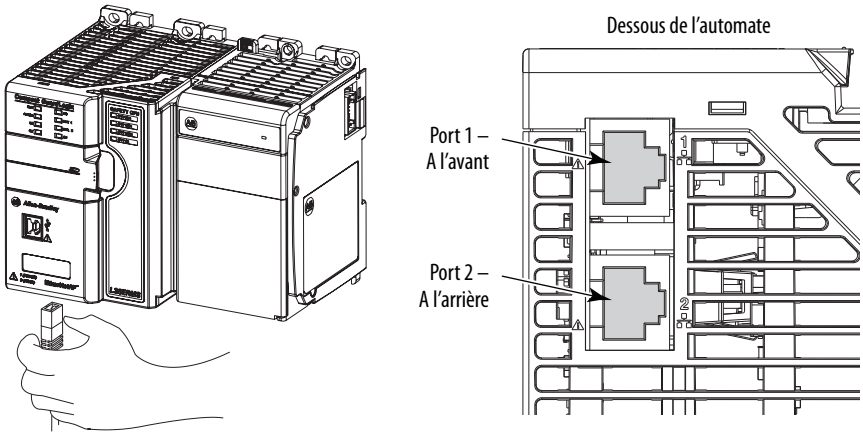
Raccordement de l'automate à un réseau EtherNet/IP

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

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

Branchez le connecteur RJ45 du câble Ethernet sur l'un des ports Ethernet de l'automate. Ces ports se trouvent en dessous de l'automate.

ATTENTION : Ne branchez pas de câble réseau DH-485 ou NAP sur ce port Ethernet. Ceci pourrait entraîner un comportement indésirable ou endommager le port.



IMPORTANT Cet exemple montre comment raccorder l'automate au réseau au moyen d'un de ses ports. Selon la topologie réseau Ethernet de votre application, vous pouvez raccorder les deux ports de l'automate au réseau EtherNet/IP.

Pour de plus amples informations sur les topologies réseau EtherNet/IP, voir Communication réseau EtherNet/IP, page 70.

Connexion à différentes topologies réseaux EtherNet/IP

Les automates Compact GuardLogix 5370 utilisent une technologie à switch embarqué et deux ports EtherNet/IP, ce qui leur permet de se monter dans les diverses topologies de réseau EtherNet/IP suivantes :

- Topologie en anneau de niveau dispositif (DLR) – Les deux ports de l'automate sont raccordés au réseau et les connexions doivent respecter certaines contraintes.
- Topologie linéaire – Les deux ports de l'automate sont raccordés au réseau et les connexions doivent respecter certaines contraintes.
- Topologie en étoile – Un seul port de l'automate est raccordé au réseau.

Pour de plus amples informations, voir Communication réseau EtherNet/IP, page 70.

Configuration de l'automate

Pour effectuer les tâches présentées dans ce chapitre, les logiciels ci-après doivent être installés sur votre ordinateur.

- RSLinx® Classic
- Environnement Studio 5000®
- Serveur BOOTP-DHCP (installé avec RSLinx Classic)
- ControlFLASH™ (installé avec l'environnement Studio 5000)

Les automates Compact GuardLogix® 5370 ont besoin d'une adresse réseau IP (Internet Protocol) pour fonctionner en réseau EtherNet/IP.

Paramétrage de l'adresse IP

L'adresse IP identifie l'automate de manière unique. L'adresse IP se présente sous la forme *xxx.xxx.xxx.xxx*, dans laquelle chaque groupe *xxx* représente un nombre entre 000 et 254, avec quelques exceptions correspondant à des valeurs réservées. Les nombres suivants sont des **exemples** de valeurs réservées qui ne peuvent pas être utilisées :

- 000.*xxx.xxx.xxx*
- 127.*xxx.xxx.xxx*
- 224 à 255.*xxx.xxx.xxx*

Certaines autres valeurs peuvent être réservées en fonction d'applications particulières.

Vous pouvez réaliser l'une de ces tâches en fonction des conditions du système :

- **Paramétrer** l'adresse IP d'un automate qui n'en possède pas.
- **Modifier** une adresse IP déjà attribuée à un automate.

IMPORTANT	Les automates Compact GuardLogix 5370 possèdent deux ports EtherNet/IP pour une connexion à un réseau EtherNet/IP ; vous ne pouvez pas installer de ports supplémentaires sur ces automates. Les ports Ethernet/IP peuvent véhiculer le même trafic réseau du fait de leur association au switch intégré de l'automate. L'automate n'utilise cependant qu'une seule adresse IP.

Vous devez paramétrer l'adresse IP de l'automate Compact GuardLogix 5370 lors de sa première mise sous tension, c'est-à-dire au moment de sa mise en service initiale. Il n'est pas nécessaire de reparamétrer l'adresse IP à chaque fois que l'automate est éteint et remis sous tension.

Vous pouvez utiliser les outils suivants pour **paramétrer** l'adresse IP d'un automate Compact GuardLogix 5370 :

- serveur BOOTP (Bootstrap Protocol)
- serveur DHCP (Dynamic Host Configuration Protocol)
- logiciel RSLinx Classic
- application Logix Designer
- carte SD

Utilisation du serveur BOOTP pour définir l'adresse IP

BOOTP (Bootstrap Protocol) est un protocole permettant à l'automate de communiquer avec un serveur BOOTP. Ce serveur peut être utilisé pour affecter une adresse IP. Vous pouvez utiliser le serveur BOOTP pour définir une adresse IP pour votre automate Compact GuardLogix 5370.

Les points suivants sont à connaître pour l'utilisation du serveur BOOTP :

- Le serveur BOOTP est installé automatiquement lorsque vous installez RSLinx Classic ou l'environnement Studio 5000 sur votre ordinateur. Le serveur BOOTP permet de définir l'adresse IP ainsi que les autres paramètres TCP (Transmission Control Protocol).
- L'automate est expédié départ usine sans adresse IP définie mais avec BOOTP activé.
- Cette section explique comment utiliser le serveur BOOTP/DHCP de Rockwell Automation. Si vous utilisez un serveur BOOTP/DHCP différent, contactez votre administrateur réseau pour vous assurer qu'il est compatible.
- Pour utiliser le serveur BOOTP, votre ordinateur et l'automate doivent être connectés par l'intermédiaire du même réseau EtherNet/IP.
- Si la fonctionnalité BOOTP est désactivée au niveau de l'automate, vous ne pourrez pas utiliser le serveur BOOTP pour définir l'adresse IP.

Il y a deux situations dans lesquelles l'automate Compact GuardLogix 5370 utilise les serveurs BOOTP pour définir l'adresse IP de l'automate :

- **Lors de la mise sous tension initiale** – Étant donné que l'automate Compact GuardLogix 5370 est livré avec BOOTP activé, lors de sa première mise sous tension, l'automate envoie une demande d'adresse IP au réseau EtherNet/IP. Vous pouvez alors utiliser le serveur BOOTP pour lui attribuer une adresse IP, comme décrit plus loin dans ce paragraphe.
- **Lors d'une remise sous tension après la mise en service de l'automate** – Si l'automate est éteint et remis sous tension alors qu'il était déjà en service, le serveur BOOTP/DHCP lui attribue une adresse IP si l'une des conditions suivantes est présente :
  - Le BOOTP est activé sur l'automate – Vous devrez alors définir l'adresse IP manuellement à l'aide du serveur BOOTP.
  - Le DHCP est activé sur l'automate – L'adresse IP sera définie automatiquement par le serveur DHCP.

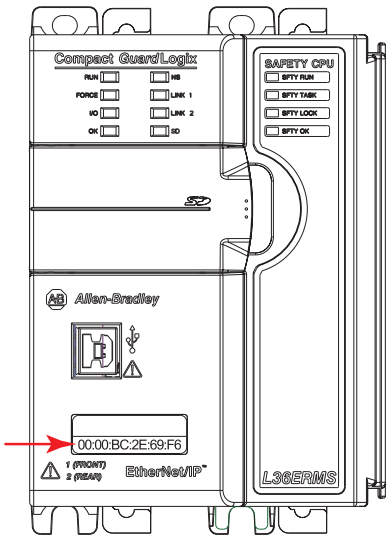
Vous pouvez accéder à l'utilitaire BOOTP/DHCP depuis l'un de ces emplacements :

- Start>Programs>Rockwell Software>BOOTP-DHCP Server (Démarrer>Programmes>Rockwell Software>Serveur BOOTP-DHCP)

  Si vous n'avez pas installé l'utilitaire, vous pouvez le télécharger et l'installer à partir de l'adresse suivante : http://www.rockwellautomation.com/global/support/tools.page.
- Le répertoire des outils (Tools) du CD d'installation du logiciel de programmation

IMPORTANT Avant de lancer l'utilitaire BOOTP/DHCP, vérifiez que vous disposez de l'adresse matérielle (MAC) de l'automate. Cette adresse matérielle se trouve en façade de l'automate et utilise un format du type :

00:00:BC:2E:69:F6



Utilisation du serveur DHCP pour définir l'adresse IP

Le serveur DHCP (Dynamic Host Configuration Protocol) attribue automatiquement des adresses IP aux stations clientes connectées en réseau TCP/IP. DHCP est basé sur BOOTP et maintient une certaine rétrocompatibilité. Leur principale différence est que BOOTP ne permet qu'une configuration manuelle (statique), alors que DHCP permet l'affectation statique et dynamique des adresses réseau et la configuration automatique des automates nouvellement raccordés.

Faites néanmoins attention lorsque vous utilisez le serveur DHCP pour configurer un automate. Un client BOOTP, tel qu'un automate CompactLogix, ne peut démarrer avec un serveur DHCP que si celui-ci est spécialement programmé pour gérer les requêtes BOOTP. Cette exigence dépend de la version du serveur DHCP utilisée. Consultez votre administrateur système pour savoir si votre version DHCP prend en charge les commandes BOOTP et l'affectation IP manuelle.

ATTENTION : Attribuez une adresse réseau fixe aux automates Compact GuardLogix 5370. L'adresse IP de ces automates ne doit pas être affectée dynamiquement.

L'inobservation de cette précaution peut entraîner des mouvements imprévus de la machine ou la perte de contrôle du procédé.

Si vous utilisez le serveur BOOTP ou DHCP de Rockwell Automation dans un sous-réseau à liaison montante sur lequel se trouve un serveur DHCP, l'automate risque de se voir attribuer une adresse par le serveur général de l'entreprise avant que l'utilitaire Rockwell Automation ne détecte cet automate. Débranchez la liaison montante pour définir l'adresse et configurer l'automate de manière à ce qu'il conserve son adresse statique ; reconnectez la liaison montante, si nécessaire.

Utilisation du logiciel RSLinx Classic pour définir l'adresse IP

Vous pouvez utiliser le logiciel RSLinx pour définir l'adresse IP de l'automate Compact GuardLogix 5370.

IMPORTANT Cette section explique comment attribuer une adresse IP à un automate Compact GuardLogix qui n'en possède pas encore.

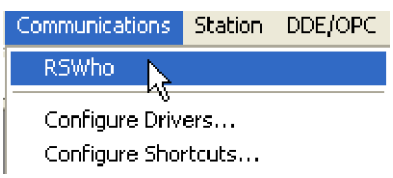
Pour attribuer une adresse IP à un automate Compact GuardLogix via le logiciel RSLinx, vous devez d'abord être connecté à votre automate via le port USB.

Suivez les étapes ci-dessous pour définir l'adresse IP de l'automate avec le logiciel RSLinx.

IMPORTANT Ces étapes font référence à un automate 1769-L36ERMS. La même procédure s'applique également aux autres automates de la famille Compact GuardLogix 5370 avec de légères variations au niveau des écrans.

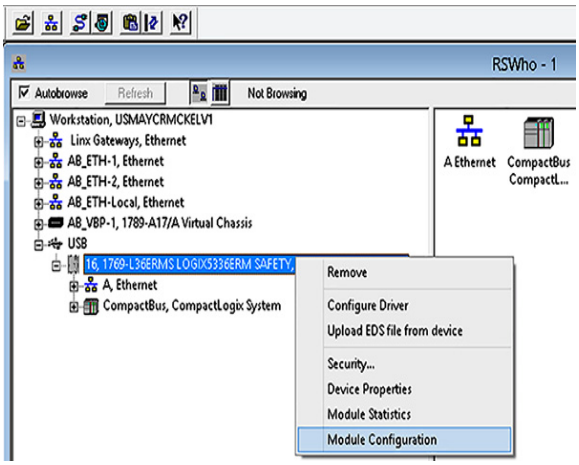
1. Assurez-vous que votre ordinateur et l'automate sont reliés par un câble USB.
2. Lancez le logiciel RSLinx.

   Après quelques secondes, la boîte de dialogue RSWho s'affiche.
3. Si ce n'est pas le cas, sélectionnez RSWho dans le menu déroulant Communications.



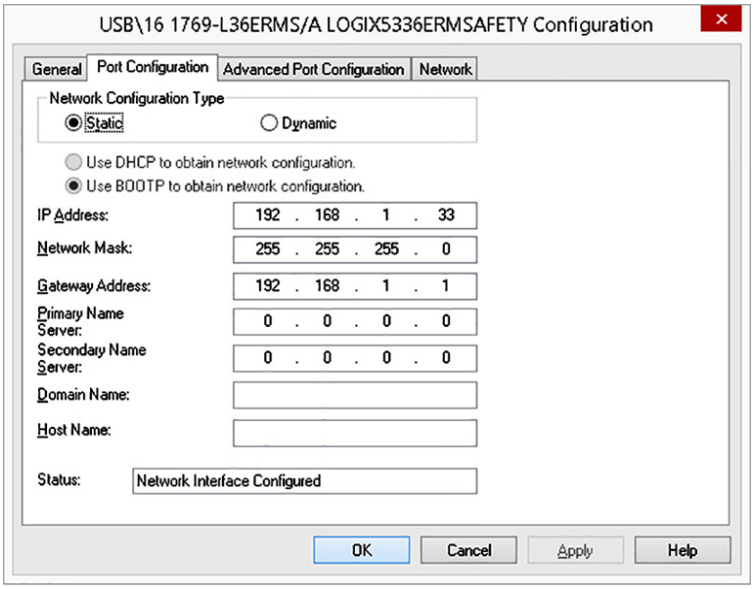
La boîte de dialogue RSWho qui apparaît inclut le driver USB.

4. Cliquez avec le bouton droit de la souris sur le module EtherNet/IP et choisissez Module Configuration (Configuration du module).



La boîte de dialogue Module Configuration (configuration du module) apparaît alors.

5. Cliquez sur l'onglet Port Configuration (configuration du port).



6. Définissez Network Configuration Type (Type de configuration réseau) sur Static (Statique) pour affecter cette configuration au port de manière permanente.

IMPORTANT	Si vous cliquez sur Dynamic (Dynamique), lors d'une remise sous tension, l'automate efface la configuration IP actuelle et reprend l'envoi de requêtes BOOTP.

7. Saisissez la nouvelle adresse IP et le masque du réseau.
8. Cliquez sur OK.

Comme pour toutes les modifications de configuration, assurez-vous que l'enregistrement sur la carte SD (si vous l'utilisez) est effectué d'une façon qui ne risque pas d'écraser l'adresse IP existante lors de la remise sous tension suivante de l'automate.

Pour de plus amples informations sur l'utilisation de la carte SD, reportez-vous au Chapitre 13.

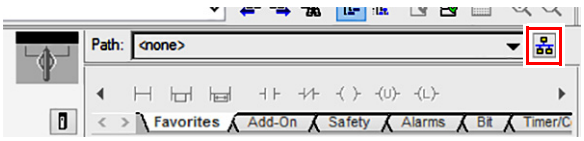
Utilisation de l'environnement Studio 5000 pour définir l'adresse IP

Vous pouvez utiliser l'application Logix Designer pour définir l'adresse IP d'un automate Compact GuardLogix 5370. Pour définir l'adresse IP via l'application, l'ordinateur doit être connecté à l'automate via le port USB.

Suivez les étapes ci-dessous pour définir l'adresse IP de l'automate.

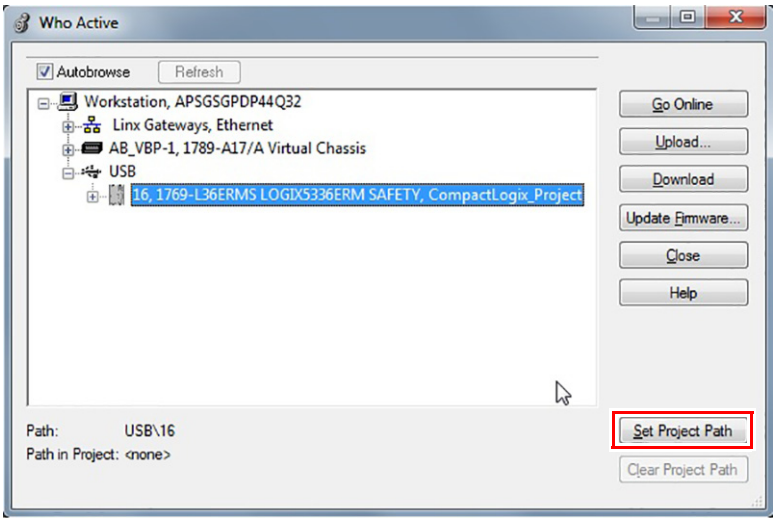
IMPORTANT Ces étapes font référence à un automate 1769-L36ERMS. La même procédure s'applique également aux autres automates de la famille Compact GuardLogix 5370 avec de légères variations au niveau des écrans.

1. Lancez l'application Logix Designer.
2. Cliquez sur RSWho pour spécifier le chemin d'accès au projet.

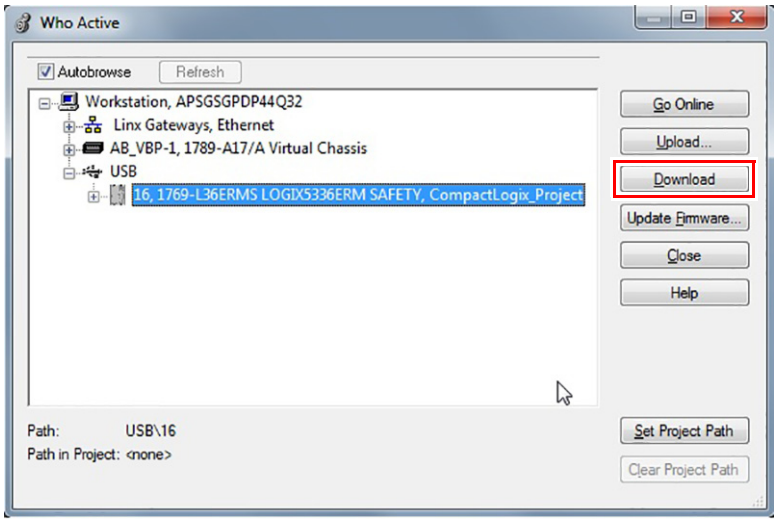


La boîte de dialogue Who Active (Qui est actif) s'affiche.

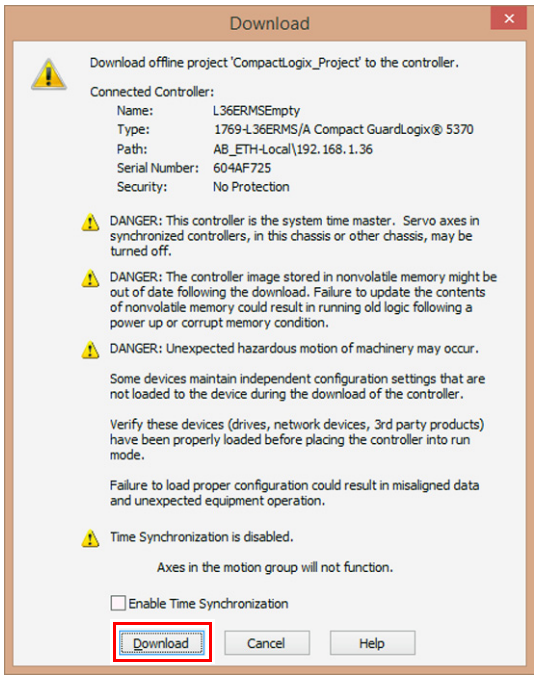
3. Naviguez sur le réseau USB et sélectionnez l'automate Compact GuardLogix.
4. Cliquez sur Set Project Path (Définir le chemin d'accès au projet).



5. Cliquez sur Download (Télécharger).

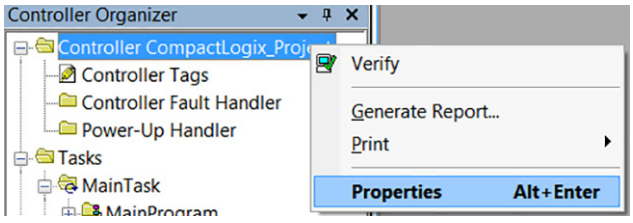


6. Cliquez à nouveau sur Download (Télécharger).



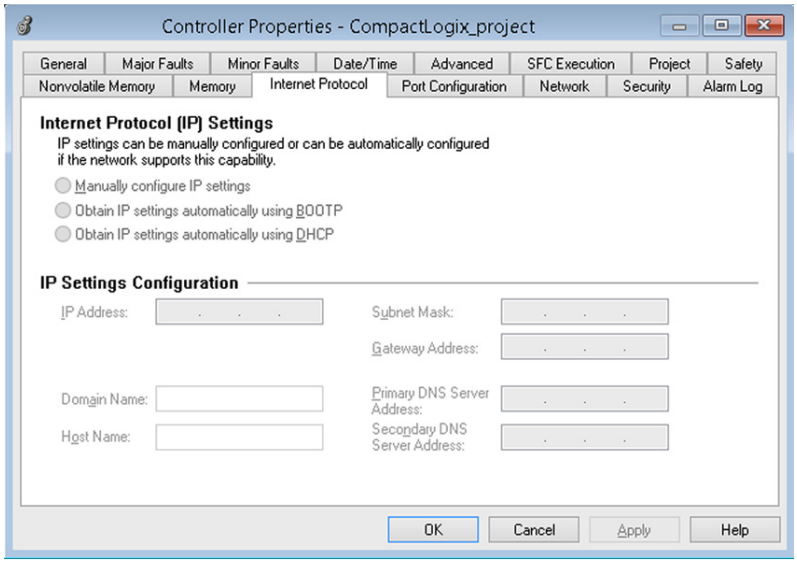
Le nouveau projet est téléchargé dans l'automate et mis en ligne, en mode Remote Program (Programmation à distance) ou Program (Programmation).

7. Cliquez avec le bouton droit sur le nom de l'automate et sélectionnez Properties (Propriétés).

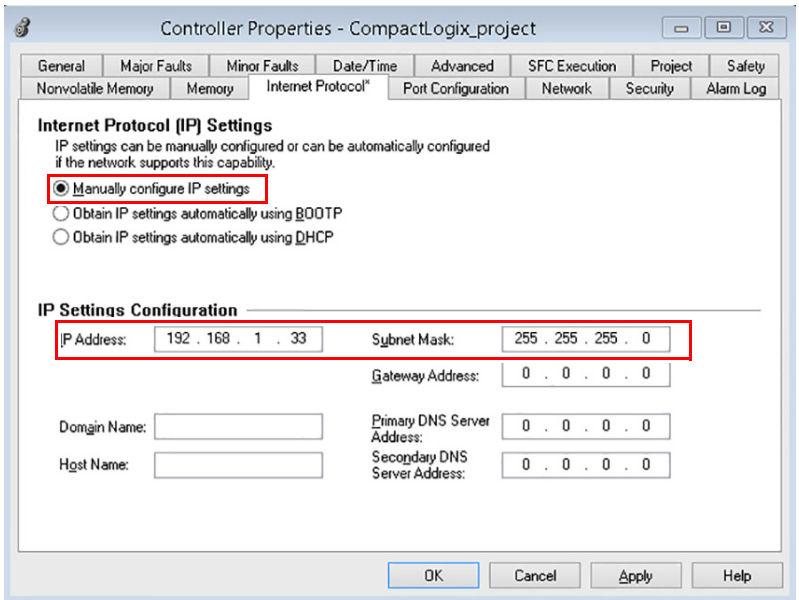


8. Dans la boîte de dialogue Controller Properties (Propriétés de l'automate), cliquez sur l'onglet Internet Protocol (Protocole Internet).

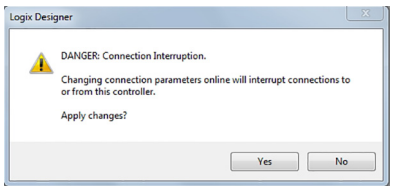
   Les valeurs apparaissant dans le champ IP Settings Configuration (Configuration des paramètres IP) indiquent que l'automate n'a pas d'adresse IP affectée.



9. Cliquez sur Manually configure IP settings (Configurer les paramètres IP manuellement).
10. Saisissez l'adresse IP souhaitée ainsi que les autres informations de configuration, puis cliquez sur OK.



11. Lorsque le logiciel vous demande de confirmer les valeurs d'adresse IP saisies, cliquez sur Yes (Oui).



L'automate utilise désormais l'adresse IP qui vient d'être définie.

Utilisation de la carte SD pour définir l'adresse IP

Vous pouvez utiliser la carte SD pour définir l'adresse IP d'un automate Compact GuardLogix 5370. L'utilisation de la carte SD pour définir l'adresse IP supprime le besoin d'un logiciel pour réaliser cette opération.

IMPORTANT	La définition de l'adresse IP à partir d'une carte SD évite de recourir à un logiciel lors du processus de mise sous tension. Cependant, le projet doit avoir été enregistré au préalable sur la carte SD. L'adresse IP de l'automate Compact GuardLogix 5370 est automatiquement configurée à la mise sous tension dans la mesure où vous avez configuré une adresse IP, enregistré le programme sur un automate, et réglé la carte SD avec le paramètre de chargement d'image défini sur à la mise sous tension. La définition de l'adresse IP d'un automate Compact GuardLogix 5370 par le biais de la carte SD à la mise sous tension n'est qu'une partie du processus de chargement de l'ensemble d'un projet sur l'automate depuis la carte SD. Utilisez cette option avec précaution. La carte SD peut en effet contenir l'adresse IP souhaitée, mais dans le cadre d'un projet inadapté ; par exemple, un projet plus ancien que celui actuellement utilisé sur l'automate.

Les règles suivantes s'appliquent à l'utilisation de la carte SD pour définir l'adresse IP d'un automate Compact GuardLogix 5370 :

- Il faut qu'un projet ait été stocké au préalable sur la carte SD.
- Ce projet doit être configuré avec le paramètre Load Image (Chargement de l'image) défini sur On Power Up (À la mise sous tension).

Des règles supplémentaires s'appliquent aux projets de sécurité. Voir le Chapitre 13 et la publication 1756-RM099, « GuardLogix 5570 and Compact GuardLogix 5370 Controllers Safety Reference Manual ».

Modification de l'adresse IP

Vous pouvez modifier l'adresse IP d'un automate Compact GuardLogix 5370 après que le système a commencé à fonctionner. Dans ce cas, l'automate possédera déjà une adresse IP valide mais vous aurez besoin de la modifier.

Vous pouvez utiliser les outils suivants pour modifier l'adresse IP d'un automate :

- logiciel RSLinx Classic
- application Studio 5000 Logix Designer
- carte SD

IMPORTANT Vous **ne pouvez pas** utiliser l'un des outils suivants pour **modifier** l'adresse IP d'un automate :

- serveur BOOTP (Bootstrap Protocol)
- serveur DHCP (Dynamic Host Configuration Protocol)

Tenez compte des facteurs ci-après pour déterminer comment modifier au mieux l'adresse IP d'un automate :

- Le fait que le réseau soit indépendant ou qu'il soit intégré au réseau général de l'usine/de l'entreprise.
- La taille du réseau – Pour des réseaux indépendants de grande taille, il peut s'avérer plus pratique et plus sûr d'utiliser un serveur BOOTP/DHCP plutôt que l'environnement Studio 5000 ou le logiciels RSLinx Classic. Un serveur BOOTP/DHCP limite en effet le risque d'affectation d'adresses IP en double.

  Cependant, vous ne pouvez utiliser le serveur BOOTP/DHCP que pour **définir** l'adresse IP de l'automate, non pour la modifier. Si vous décidez de modifier l'adresse IP de l'automate et que vous souhaitiez utiliser un serveur BOOTP/DHCP pour limiter les risques d'attribution d'adresses IP en double, vous devez commencer par effacer l'adresse IP existante.

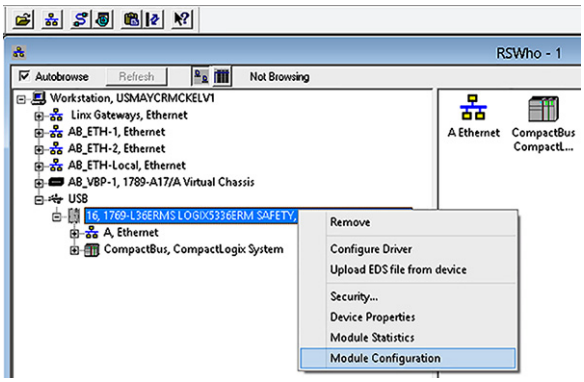
  Après avoir effacé cette adresse IP, suivez les étapes décrites à la section Utilisation du serveur BOOTP pour définir l'adresse IP, page 34, ou Utilisation du serveur DHCP pour définir l'adresse IP, page 35, pour définir l'adresse IP de l'automate.
- Le règlement et les procédures de l'entreprise concernant l'installation et la maintenance du réseau d'usine.
- Le degré d'implication du personnel informatique dans l'installation et la maintenance des réseaux utilisés en production.
- Le niveau de la formation dispensée aux automaticiens et au personnel de maintenance.

Modification de l'adresse IP avec le logiciel RSLinx

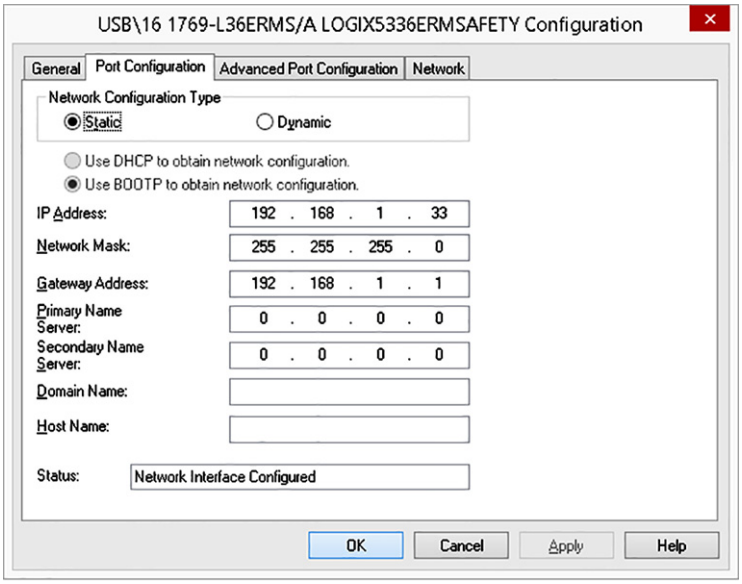
Suivez les étapes ci-dessous pour modifier l'adresse IP de l'automate.

IMPORTANT Ces étapes font référence à un automate 1769-L36ERMS. La même procédure s'applique également aux autres automates de la famille Compact GuardLogix 5370 avec de légères variations au niveau des écrans.

1. Assurez-vous que votre ordinateur et l'automate sont reliés par un câble USB.
2. Cliquez avec le bouton droit sur l'automate et choisissez l'option Module Configuration (Configuration du module).



3. Cliquez sur l'onglet Port Configuration (configuration du port).



L'automate doit avoir une adresse IP et un type de configuration réseau (Network Configuration Type) valides.

4. Saisissez la nouvelle adresse IP et le masque du réseau.
5. Définissez Network Configuration Type (Type de configuration réseau) sur Static (Statique) pour affecter cette configuration au port de manière permanente.

IMPORTANT Si vous cliquez sur Dynamic (Dynamique), lors d'une remise sous tension, l'automate efface la configuration IP actuelle et reprend l'envoi de requêtes BOOTP.

6. Cliquez sur OK.

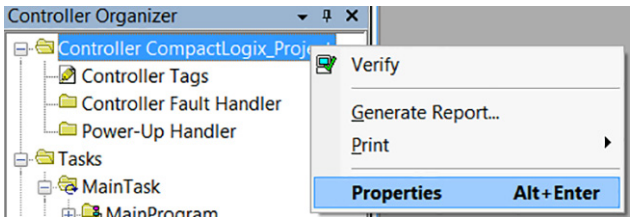
Modification de l'adresse IP réseau avec le logiciel Logix Designer

Vous pouvez modifier l'adresse IP d'un automate Compact GuardLogix 5370 via l'application Logix Designer sur une connexion USB ou en réseau EtherNet/IP.

Suivez les étapes ci-dessous pour modifier l'adresse IP de l'automate.

IMPORTANT Ces étapes font référence à un automate 1769-L36ERMS. La même procédure s'applique également aux autres automates de la famille Compact GuardLogix 5370 avec de légères variations au niveau des écrans.

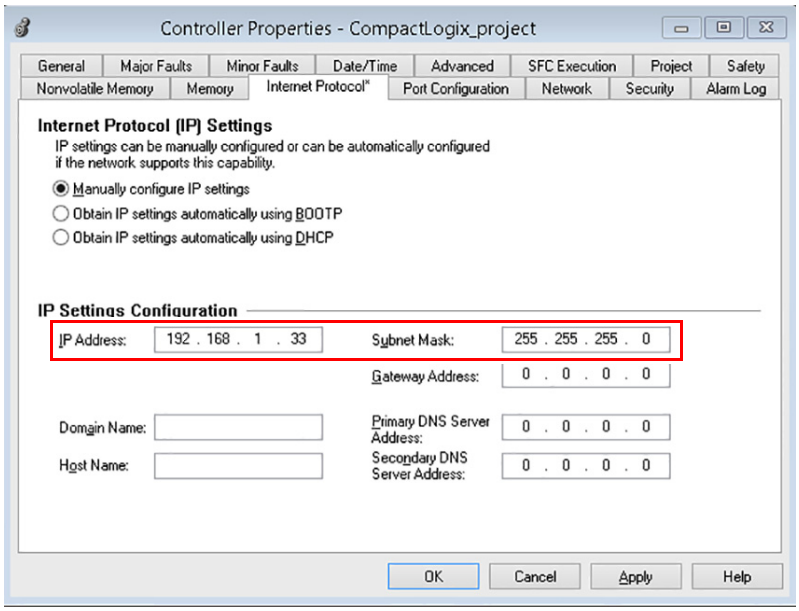
1. Vérifiez que votre ordinateur est connecté à l'automate.
2. Vérifiez que votre projet est en ligne.
3. Cliquez avec le bouton droit sur le nom de l'automate et sélectionnez Properties (Propriétés).



CONSEIL Vous pouvez également cliquer avec le bouton droit de la souris sur la station Ethernet dans la section I/O Configuration (Configuration des E/S) et choisir Properties (Propriétés).

La boîte de dialogue Controller Properties (Propriétés de l'automate) apparaît dans l'onglet Internet Protocol (protocole Internet).

4. Modifiez l'adresse IP de l'automate.
5. Apportez les autres modifications nécessaires.



6. Cliquez sur OK.

Modification de l'adresse IP avec une carte SD

Vous pouvez utiliser une carte SD pour modifier l'adresse IP d'un automate Compact GuardLogix 5370 lors d'une remise sous tension de l'automate. L'utilisation de la carte SD pour modifier l'adresse IP supprime le besoin d'un logiciel pour réaliser cette opération.

IMPORTANT	La définition de l'adresse IP à partir d'une carte SD évite de recourir à un logiciel lors du processus de mise sous tension. Cependant, le projet doit avoir été enregistré au préalable sur la carte SD.

Les règles suivantes s'appliquent à l'utilisation d'une carte SD pour modifier l'adresse IP d'un automate Compact GuardLogix 5370 :

- Un projet est stocké sur la carte SD.
- Ce projet doit comporter une adresse IP destinée à l'automate Compact GuardLogix 5370 qui héberge physiquement la carte SD, différente de celle actuellement utilisée par cet automate.
- Ce projet doit être configuré avec le paramètre Load Image (Chargement de l'image) défini sur On Power Up (À la mise sous tension).
- L'automate doit être remis sous tension avec la carte SD installée.

Des règles supplémentaires s'appliquent aux projets de sécurité. Voir le Chapitre 13 et la publication 1756-RM099, « GuardLogix 5570 and Compact GuardLogix 5370 Controllers Safety Reference Manual ».

Chargement du firmware sur l'automate

Vous devez télécharger la version la plus récente du firmware avant de pouvoir utiliser l'automate Compact GuardLogix 5370.

IMPORTANT	N'interrompez pas une mise à jour de firmware en cours. L'interruption de la mise à jour du firmware peut faire en sorte que la version du firmware de l'automate Compact GuardLogix revienne à sa -version d'origine, soit 1.*xxx*.

Pour charger ce firmware sur l'automate, vous pouvez utiliser :

- l'utilitaire ControlFLASH, qui est installé avec l'application Logix Designer ;
- l'utilitaire AutoFlash, qui est lancé automatiquement par l'application lorsque vous chargez un projet dont la version de firmware ne correspond pas à celle de l'automate ;
- une carte SD (référence 1784-SD1 ou 1784-SD2) comportant une image du projet préalablement enregistrée.

Si vous utilisez les utilitaires ControlFLASH ou AutoFlash, vous avez besoin d'une connexion USB ou en réseau EtherNet/IP avec l'automate.

IMPORTANT La version du firmware d'automate qui est chargée via le logiciel ControlFLASH ou l'option AutoFlash peut être écrasée lors de remises sous tension futures de l'automate en présence des conditions décrites au paragraphe Utilisation de la carte SD pour charger le firmware, page 52.

Le firmware est disponible avec l'application ou vous pouvez le télécharger depuis le site Web de Rockwell Automation, à la page Support, via le centre Product Compatibility and Download Center (PCDC), à l'adresse http://www.rockwellautomation.com/global/support/pcdc.page.

Utilisation de l'utilitaire ControlFLASH pour charger le firmware

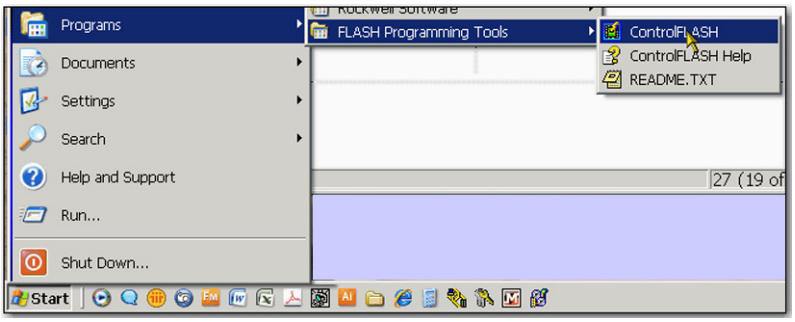
Vous pouvez employer l'utilitaire ControlFLASH pour charger le firmware par l'intermédiaire d'une connexion USB ou en réseau EtherNet/IP. Nous recommandons de procéder de la façon suivante pour charger un firmware via l'utilitaire ControlFLASH :

- utilisez une connexion USB pour effectuer l'opération ;
- si une carte SD est installée dans l'automate, retirez-la.

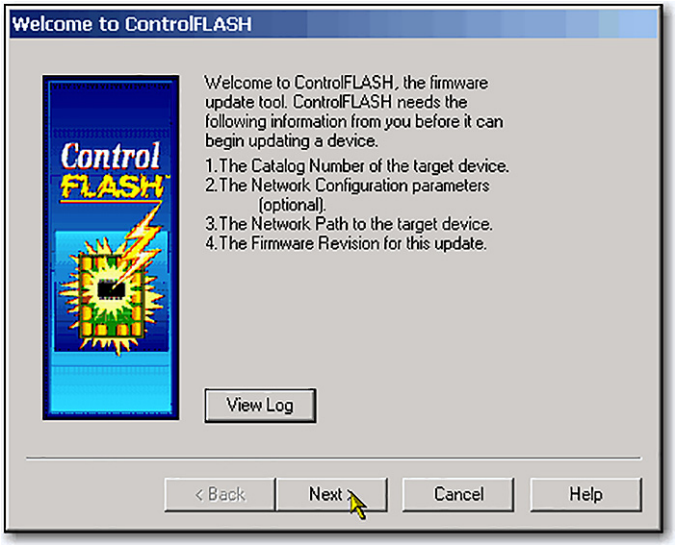
Suivez les étapes ci-dessous pour charger le firmware au moyen de l'utilitaire ControlFLASH.

IMPORTANT Ces étapes font référence à un automate 1769-L36ERMS. La même procédure s'applique également aux autres automates de la famille Compact GuardLogix 5370 avec de légères variations au niveau des écrans.

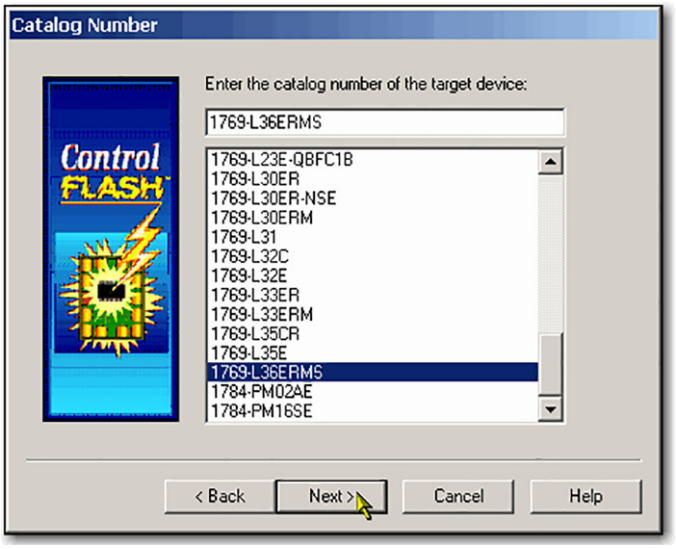
1. Vérifiez qu'il existe une connexion entre votre ordinateur et l'automate Compact GuardLogix 5370.
2. Sélectionnez Start>Programs>FLASH Programming Tools>ControlFLASH (Démarrer>Programmes>Outils de programmation FLASH>ControlFLASH).



3. Lorsque la boîte de dialogue de bienvenue s'affiche, cliquez sur Next (suivant).

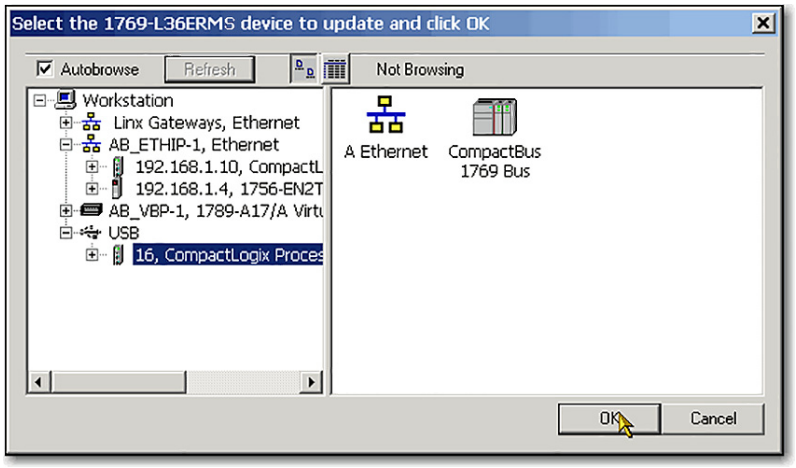


4. Choisissez la référence d'automate appropriée et cliquez sur Next (Suivant).

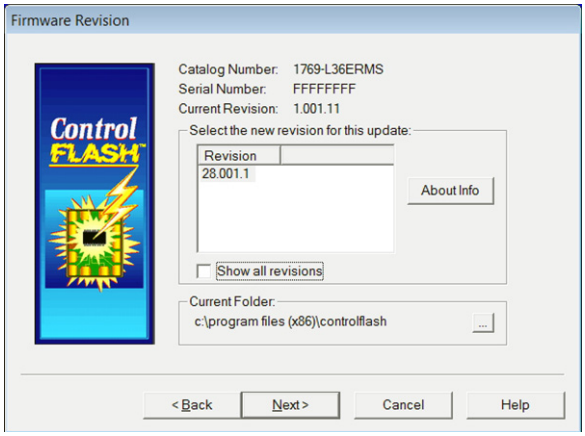


5. Développez l'arborescence du réseau jusqu'à vous voyiez apparaître votre automate.

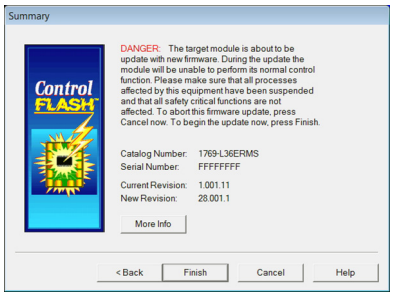
6. Sélectionnez la première instance de l'automate qui s'affiche, comme illustré ci-dessous, et cliquez sur OK.

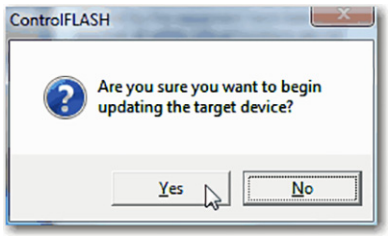


7. Choisissez le niveau de version auquel vous souhaitez mettre à jour l'automate et cliquez sur Next (Suivant).

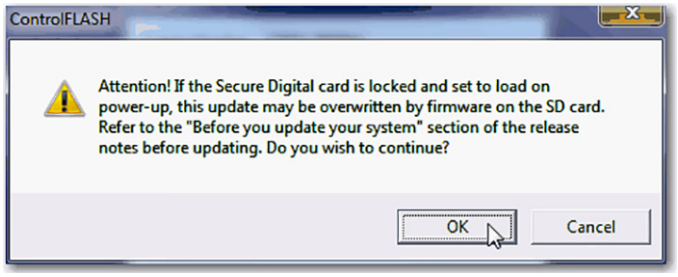


8. Pour lancer la mise à jour de l'automate, cliquez sur Finish (Terminer), puis sur Yes (Oui).

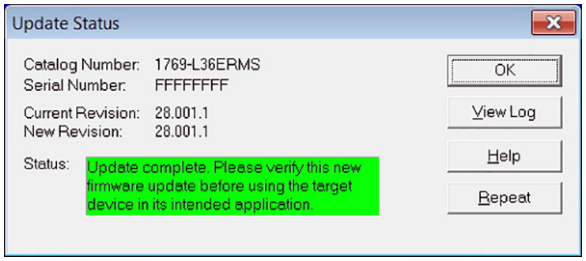




Avant que ne commence cette mise à jour du firmware, la boîte de dialogue suivante s'affiche : Prenez les mesures nécessaires en fonction de votre application. Dans l'exemple présenté, la mise à jour se poursuivra après avoir cliqué sur OK.



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



9. Cliquez sur OK.
10. Pour fermer l'utilitaire ControlFLASH, cliquez sur Cancel (Annuler), puis sur Yes (Oui).

Utilisation de l'utilitaire AutoFlash pour charger le firmware

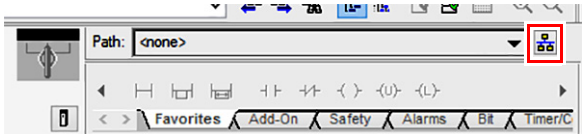
Vous pouvez employer l'utilitaire AutoFlash pour charger le firmware par l'intermédiaire d'une connexion USB ou en réseau EtherNet/IP.

Laissez la mise à jour se terminer sans l'interrompre. Si vous interrompez une mise à jour de firmware, vous êtes averti(e) qu'une erreur s'est produite. Dans ce cas, coupez et remettez l'automate sous tension. Le firmware revient alors à sa version de base 1.*xxx* et vous pouvez recommencer le processus de mise à jour.

Suivez les étapes ci-dessous pour charger le firmware au moyen de l'utilitaire AutoFlash.

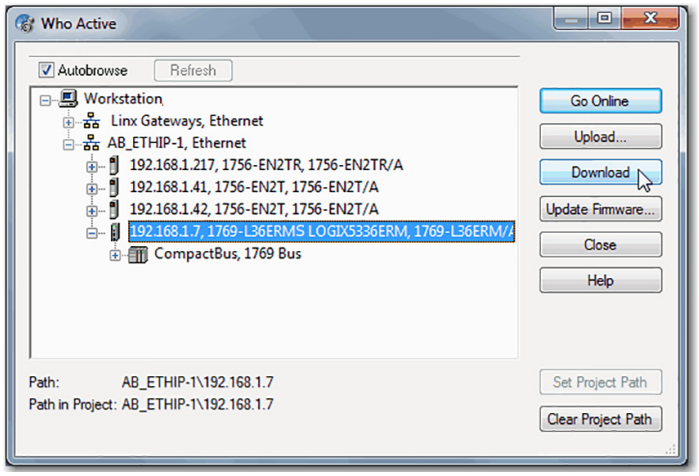
IMPORTANT Ces étapes font référence à un automate 1769-L36ERMS. La même procédure s'applique également aux autres automates de la famille Compact GuardLogix 5370 avec de légères variations au niveau des écrans.

1. Vérifiez qu'il existe une connexion réseau appropriée et que le driver pour ce réseau est configuré dans le logiciel RSLinx Classic.
2. Créez un projet d'automate.
3. Cliquez sur RSWho pour spécifier le chemin d'accès à l'automate.



La boîte de dialogue Who Active (Qui est actif) s'affiche.

4. Naviguez sur le réseau Ethernet et sélectionnez l'automate Compact GuardLogix.

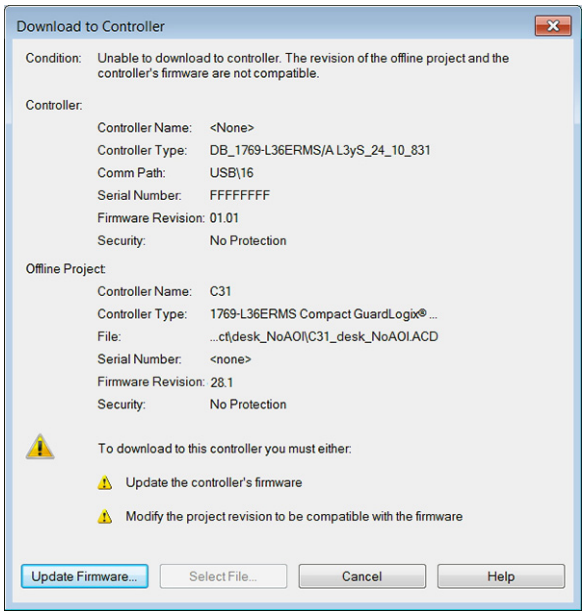


5. Cliquez sur Download (Télécharger).

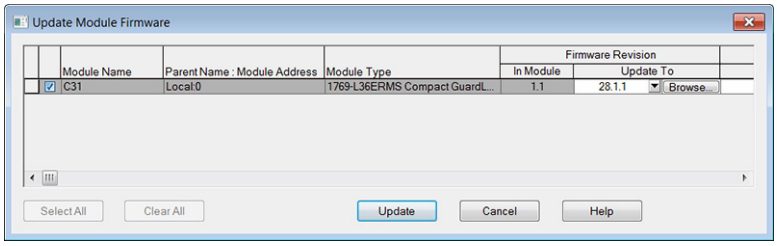
CONSEIL Pour terminer ce processus, vous pouvez cliquez sur Update Firmware (Mettre à jour firmware) au lieu de Download (Télécharger). Si tel est le cas, allez à étape 6.

Une boîte de dialogue apparaît pour vous notifier que les niveaux de version du firmware de l'automate et de celui du projet sont différents.

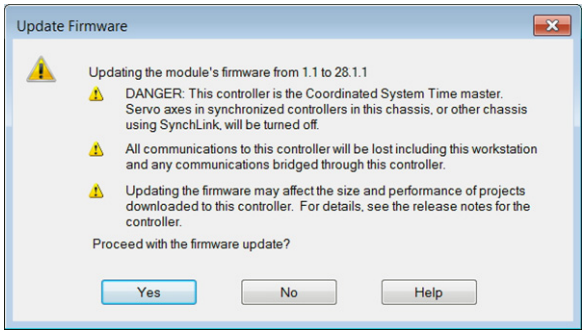
6. Cliquez sur Update Firmware (Mettre à jour le firmware).



7. Utilisez la case à cocher et le menu déroulant pour sélectionner votre automate et la version du firmware.
8. Cliquez sur Update (Mettre à jour).



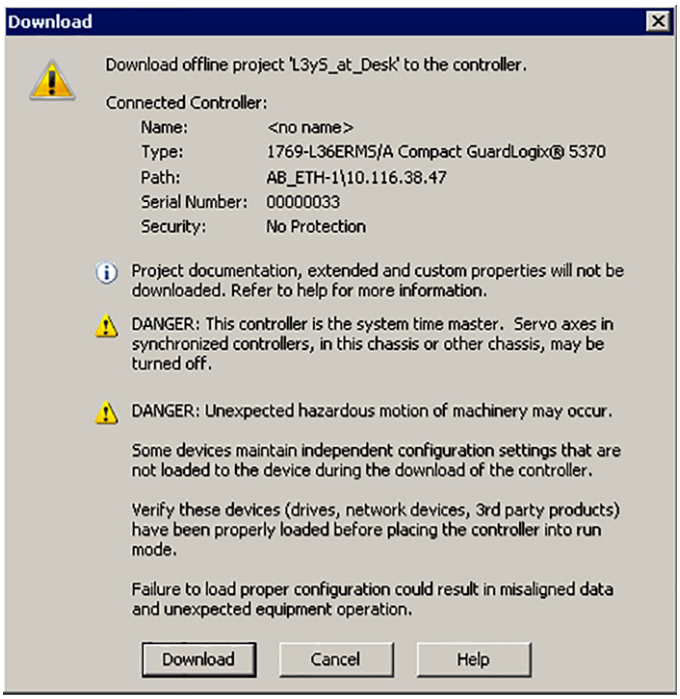
9. Lorsque la boîte de dialogue Update Firmware (Mettre à jour le firmware) apparaît, cliquez sur Yes (Oui).



Avant que la mise à jour du firmware ne démarre, il se peut que vous soyez averti(e) de l'absence de la carte SD dans votre automate. Prenez les mesures appropriées et cliquez sur OK.

La mise à niveau du firmware commence.

10. Une fois la mise à jour du firmware terminée, la boîte de dialogue Download (Télécharger) s'affiche. Dans cet exemple, le téléchargement du projet sur l'automate se poursuit après avoir cliqué sur Download.



Utilisation de la carte SD pour charger le firmware

Vous pouvez utiliser une carte SD installée pour charger le firmware sur un automate Compact GuardLogix 5370. L'utilisation de la carte SD pour charger le firmware supprime le besoin d'un logiciel pour réaliser cette opération.

IMPORTANT	Une carte SD installée met automatiquement à jour le firmware de l'automate Compact GuardLogix 5370, si elle a été configurée avec le paramètre de chargement d'image défini sur à la mise sous tension.

Pour charger le firmware à partir d'une carte SD au démarrage, les conditions suivantes doivent être remplies :

- Vous devez avoir enregistré le projet sur la carte SD avant la remise sous tension.
- La version du firmware du projet stocké sur la carte SD est différente de celle de l'automate Compact GuardLogix 5370.

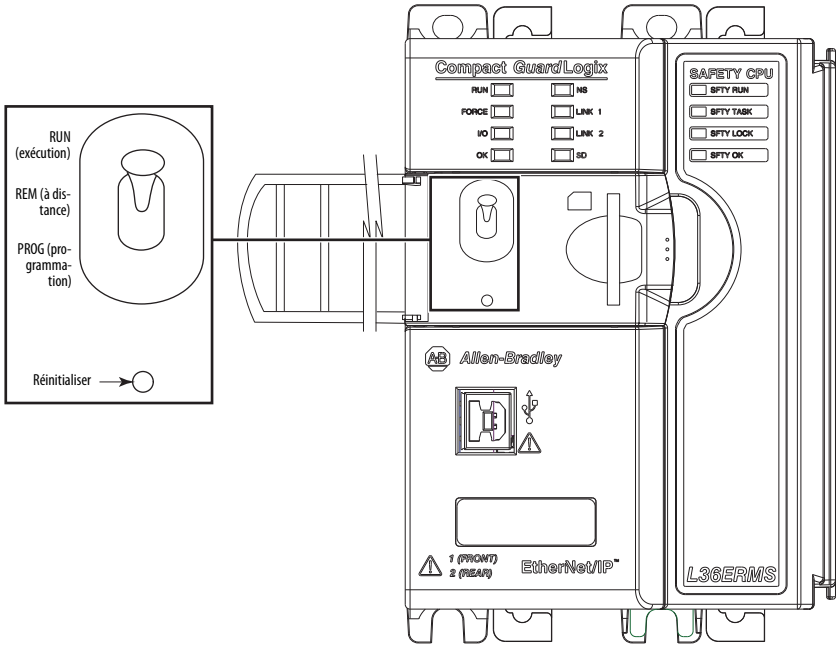
Des règles supplémentaires s'appliquent aux projets de sécurité. Voir le Chapitre 13 et la publication 1756-RM099, « GuardLogix 5570 and Compact GuardLogix 5370 Controllers Safety Reference Manual ».

Choix du mode de fonctionnement de l'automate

AVERTISSEMENT : lorsque vous changez le commutateur de position sous tension, un arc électrique peut se produire susceptible de provoquer une explosion dans des installations en environnement dangereux.

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

La figure ci-dessous illustre le sélecteur de mode sur un automate Compact GuardLogix 5370. Utilisez le sélecteur de mode sur l'automate pour définir le mode de fonctionnement.



IMPORTANT Des restrictions s'appliquent aux applications de sécurité. Reportez-vous au Chapitre 9, Développement d'applications de sécurité, et à la publication 1756-RM099, « GuardLogix 5570 and Compact GuardLogix 5370 Safety Reference Manual », pour des informations détaillées sur les restrictions de programmation.

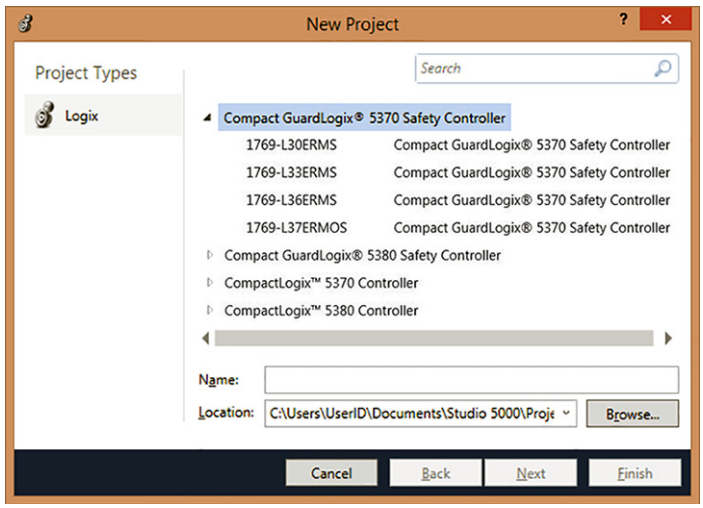
Position du commutateur de mode	Description	
RUN (exécution)	Vous pouvez exécuter les tâches suivantes : • Transférer des projets. • Exécuter le programme et activer les sorties. Vous ne pouvez pas exécuter les tâches suivantes : • Mise à jour du firmware de l'automate. • Créer ou supprimer des tâches, des programmes ou des sous-programmes. • Créer ou supprimer des points ou les modifier en ligne. • Importer un programme dans l'automate. • Modifier la configuration du port de l'automate, la configuration de port avancée ou les paramètres de configuration du réseau. • Modifier les paramètres de configuration d'un automate définis directement pour fonctionner dans une topologie réseau DLR (anneau de niveau dispositif).	
Prog (programmation)	Vous pouvez exécuter les tâches suivantes : • Mise à jour du firmware de l'automate. • Désactiver des sorties. • Transférer/charger des projets. • Créer, modifier et supprimer des tâches, des programmes ou des sous-programmes. • Modifier la configuration du port de l'automate, la configuration de port avancée ou les paramètres de configuration du réseau. Vous ne pouvez pas exécuter les tâches suivantes : • Utiliser l'automate pour exécuter (scruter) des tâches.	
Rem (à distance)	Vous pouvez exécuter les tâches suivantes : • Transférer/charger des projets. • Modifier la configuration du port de l'automate, la configuration de port avancée ou les paramètres de configuration du réseau. • Sélectionner le mode de programmation à distance (Remote Program), de test à distance (Remote Test) ou d'exécution à distance (Remote Run) au moyen de l'application.	
	Remote Run (exécution à distance)	• Exécution (scrutation) des tâches par l'automate. • Activation des sorties. • Modification en ligne.
	Remote Program (programmation à distance)	• Mise à jour du firmware de l'automate. • Désactiver des sorties. • Créer, modifier et supprimer des tâches, des programmes ou des sous-programmes. • Transfert/chargement de projets. • Modification en ligne. • L'automate n'exécute pas (ne scrute pas) les tâches.
	Remote Test (test à distance)	• Exécution des tâches avec les sorties désactivées. • Modification en ligne.

Configuration de l'automate

Création d'un projet d'automate

Pour configurer et programmer votre automate, suivez les étapes ci-dessous qui expliquent comment créer et gérer un projet pour l'automate avec l'application Logix Designer.

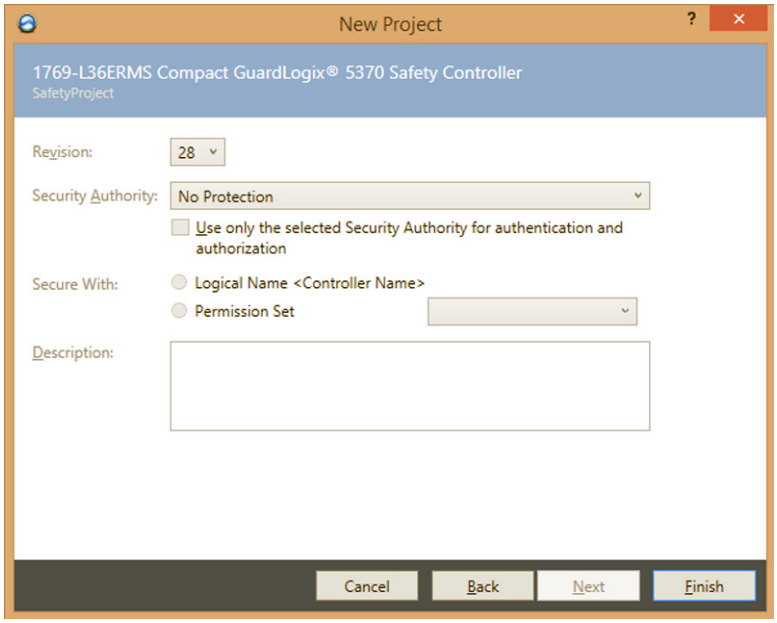
1. Cliquez sur le bouton New (Nouveau) de la barre d'outils principale pour créer un projet.
2. Cliquez deux fois sur la ligne Compact GuardLogix® 5370 pour développer la liste des options d'automate.
3. Choisissez un automate Compact GuardLogix 5370 :
   - 1769-L30ERMS
   - 1769-L33ERMS
   - 1769-L36ERMS
   - 1769-L37ERMOS(1)



4. Dans le champ Name (Nom), tapez le nom du projet.

(1) Accessible en tant que révision du firmware 30.

5. Cliquez sur Browse (Parcourir) pour indiquer le dossier dans lequel le projet automate de sécurité sera stocké.
6. Cliquez sur Next (Suivant).
7. Dans le menu déroulant Revision, choisissez la version majeure du firmware pour l'automate.

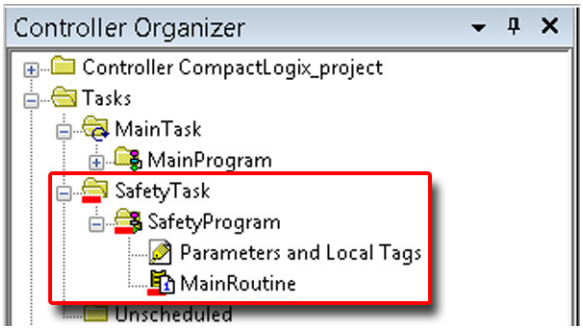


8. Dans le menu déroulant Security Authority (Autorité de sécurité), choisissez une option d'autorité de sécurité.

   Pour des informations complémentaires sur la sécurité, reportez-vous à la publication 1756-PM016 « Sécurité des automates Logix5000™ – Manuel de programmation ».
9. Cochez la case sous Security Authority si vous souhaitez utiliser la protection sélectionnée pour l'authentification et l'autorisation.
10. Dans le champ Description, entrez une description du projet.
11. Cliquez sur Finish (Terminer).

L'application Logix Designer crée une tâche de sécurité et un programme de sécurité. Un sous-programme de sécurité principal en logique à relais appelé « MainRoutine » est également créé dans le programme de sécurité.

Figure 3 – 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.

Lorsque vous créez un nouveau projet de sécurité, l'application Logix Designer génère également automatiquement un numéro de réseau de sécurité (SNN) temporel.

Ce SNN définit le réseau EtherNet/IP dans lequel réside l'automate comme un sous-réseau de sécurité. Vous pouvez le visualiser et le modifier dans l'onglet General 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 devez saisir un SNN particulier.

Figure 4 – Numéro de réseau de sécurité

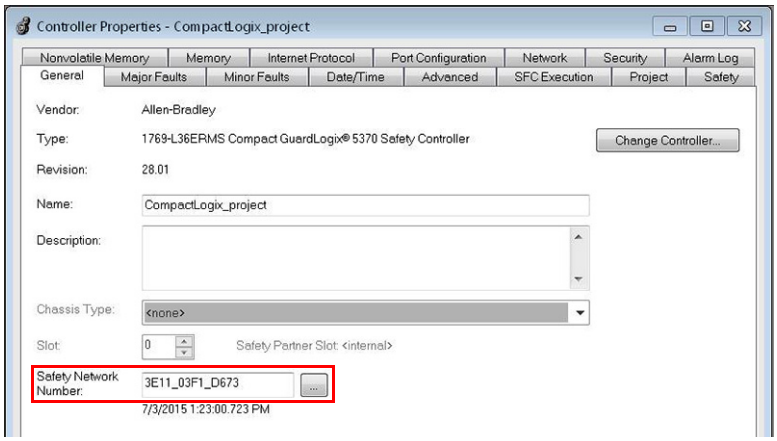


Tableau 6 – documentation connexe

Documentation	Description
Chapitre 9, Développement d'applications de sécurité	Informations complémentaires sur la tâche de sécurité, les programmes et sous-programmes de sécurité.
Chapitre 5, Communications en réseaux	Contient des informations complémentaires sur la gestion du numéro SNN.

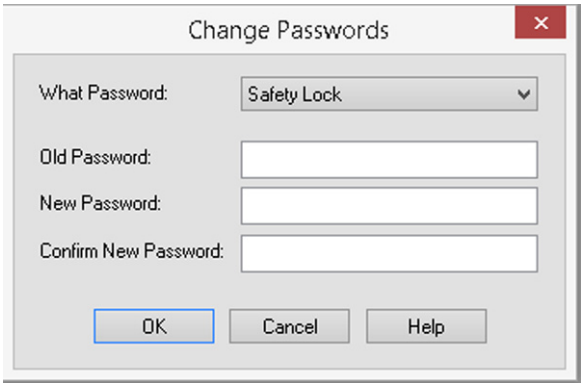
Définition des mots de passe pour le verrouillage et le déverrouillage de la sécurité

Le verrouillage de la sécurité de l'automate vous permet de protéger 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. Cliquez sur Tools > Safety > Change Passwords (Outils > Sécurité > Changer les mots de passe).
2. Dans la liste déroulante What Password (Quel mot de passe), sélectionnez Safety Lock ou Safety Unlock (Verrouillage ou Déverrouillage de 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.

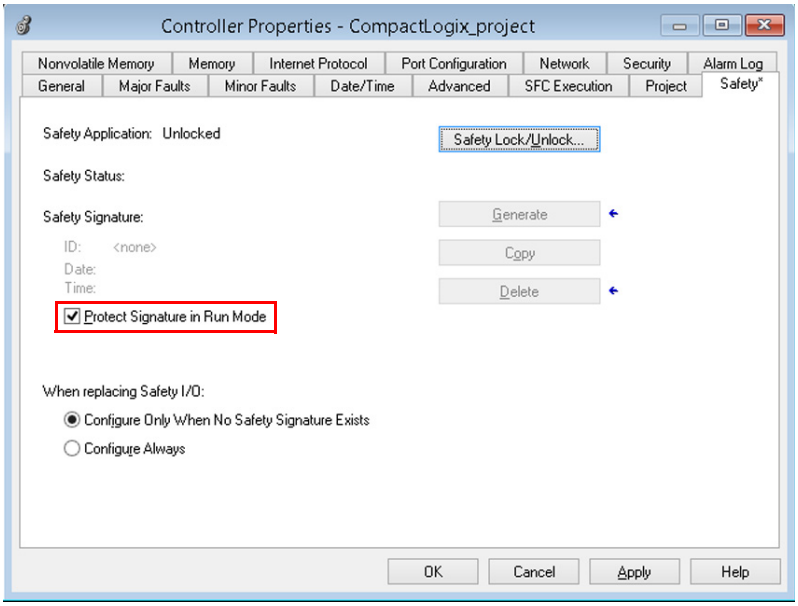
   Les mots de passe peuvent contenir de 1 à 40 caractères et ne sont pas sensibles à la casse. Les lettres, les chiffres, ainsi que les symboles suivants peuvent être utilisés : ‘ ~ ! @ # $ % ^ & * ( ) _ + , – = { } | [ ] \ : ; ? /.

Protection de la signature de tâche de sécurité en mode d'exécution

Vous pouvez empêcher la création ou la suppression de la signature de tâche de sécurité en mode Run (Exécution) ou en mode Remote Run (exécution à distance), que l'application de sécurité soit verrouillée ou non.

Suivez la procédure ci-dessous pour protéger la signature de la tâche de sécurité :

1. Ouvrez la boîte de dialogue Controller Properties (Propriétés de l'automate).
2. Cliquez sur l'onglet Safety (Sécurité).
3. Cochez la case Protect Signature in Run Mode (Protéger la signature en mode Exécution).
4. Cliquez sur OK.



Détrompage électronique

Le détrompage électronique réduit la possibilité d'utiliser le mauvais dispositif dans un système de commande. Il compare le dispositif défini dans votre projet au dispositif installé. En cas d'échec du détrompage, un défaut se produit. Les attributs suivants sont alors comparés.

Caractéristique	Description
Vendor	Le fabricant du dispositif.
Device Type	Le type général du dispositif, par exemple, un module d'E/S TOR.
Code produit	Le type spécifique du produit. Ce code produit correspond à une référence.
Major Revision	Un numéro qui représente les capacités fonctionnelles d'un dispositif.
Minor Revision	Un numéro qui représente les changements de comportement du dispositif.

Les options de détrompage électronique suivantes sont disponibles.

Option de détrompage	Description
Module compatible	Permet au dispositif installé d'accepter la clé du dispositif défini dans le projet lorsque le dispositif installé peut émuler le dispositif défini. Grâce à cette option, vous pouvez généralement remplacer un dispositif par un autre avec les caractéristiques suivantes : • Même référence • Version majeure de même niveau ou de niveau plus élevé • Version mineure comme suit : – si Version majeure est du même niveau, Version mineure doit être identique ou de niveau plus élevé ; – si Version majeure est de niveau plus élevé, Version mineure peut prendre toute valeur.
Concordance exacte	Indique que tous les attributs de détrompage doivent correspondre pour établir la communication. Si un attribut ne correspond pas, la communication avec le dispositif ne se produit pas. Exact Match (Correspondance exacte) est nécessaire si vous utilisez le Firmware Manager (Gestionnaire de firmware).

Considérez soigneusement les incidences de chaque option de détrompage pour toute sélection.

IMPORTANT La modification des paramètres de détrompage électronique en ligne interrompt les connexions au dispositif et à tous les dispositifs connectés au moyen de ce dispositif. Les connexions à partir d'autres automates peuvent être également coupées.

L'interruption de connexion d'E/S à un dispositif peut entraîner une perte de données.

Pour plus d'informations sur le détrompage électronique, reportez-vous à la publication LOGIX-AT001, « Logix5000 Control Systems Application Technique ».

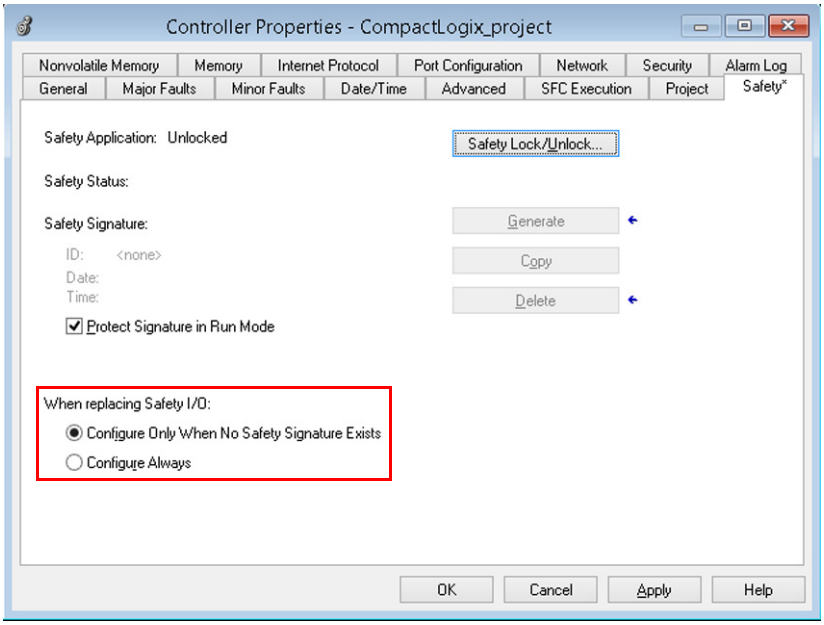
Options de remplacement de dispositifs d'E/S

L'onglet Safety (Sécurité) de la boîte de dialogue Controller Properties (Propriétés de l'automate) vous permet de définir la manière dont l'automate va gérer le remplacement d'un dispositif d'E/S dans le système. Cette option détermine si l'automate définit le numéro de réseau de sécurité (SNN) d'un dispositif d'E/S auquel il est connecté et dispose des données de configuration lorsqu'une signature de tâche de sécurité(1) existe.

Suivez la procédure ci-dessous pour configurer la manière dont l'automate gère le remplacement d'un dispositif d'E/S dans le système.

1. Ouvrez la boîte de dialogue Controller Properties (Propriétés de l'automate).
2. Cliquez sur l'onglet Safety (Sécurité).
3. Sélectionnez l'option de configuration pour l'automate à utiliser lors du remplacement de l'E/S de sécurité.
4. Cliquez sur OK.

Figure 5 – Options de remplacement de dispositifs d'E/S



ATTENTION : Activez uniquement la fonction Configure Always (Toujours configurer) si vous ne comptez pas sur l'ensemble du système de commande CIP Safety routable pour garantir la sécurité SIL 3 pendant le remplacement et le test fonctionnel d'un dispositif.

Pour de plus amples informations, voir Chapitre 5, Communications en réseaux, page 63.

(1) La signature de tâche de sécurité est un numéro utilisé par le système GuardLogix pour identifier de manière unique chaque programme, donnée et configuration d'un projet. Elle protège ainsi le niveau d'intégrité de sécurité (SIL) du système. Reportez-vous à Signature de tâche de sécurité, page 16 et Génération d'une signature de tâche de sécurité, page 158 pour plus d'informations.

Activation de la synchronisation temporelle

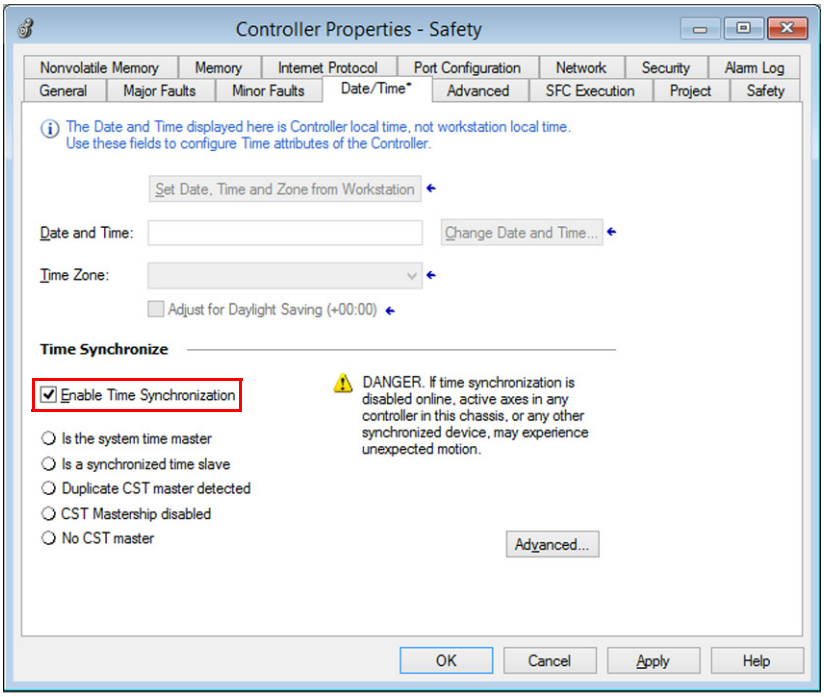
Dans un système de commande Compact GuardLogix 5370, l'automate doit être défini comme horloge maître pour le temps système coordonné (CST). La synchronisation temporelle propose une procédure standard de synchronisation des horloges des dispositifs répartis sur un réseau.

IMPORTANT	La synchronisation temporelle est exigée pour les applications de commande de mouvement.

Suivez la procédure ci-après pour configurer l'automate en horloge maître pour le CST.

1. Ouvrez la boîte de dialogue Controller Properties (Propriétés de l'automate).
2. Cliquez sur l'onglet Date/Time (Date/Heure).
3. Cochez la case Enable Time Synchronization (Valider la synchronisation temporelle).
4. Cliquez sur OK.

Figure 6 – Onglet Date/Time



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. Pour partager des données de sécurité entre automates homologues, vous produisez et consommez 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 et consommés, page 146.

Communications en réseaux

Tous les automates Compact GuardLogix® 5370 sont capables de réaliser les tâches suivantes en réseau EtherNet/IP :

- gestion des E/S distribuées de commande pour connexions standard et de sécurité ;
- émission/réception de messages vers/depuis des périphériques du même réseau ou d'un autre réseau ;
- production/consommation de données (verrouillage) entre automates ;
- interface de connexion.

Les automates Compact GuardLogix 5370 prennent en charge les tâches suivantes en réseau DeviceNet :

- gestion des E/S distribuées de commande pour les connexions standard uniquement ;
- envoi de messages vers des périphériques du même réseau (mais l'automate ne peut pas recevoir de messages provenant d'autres périphériques du réseau).

Tous les automates Compact GuardLogix 5370 prennent aussi en charge des communications temporaires avec votre ordinateur par l'intermédiaire d'une connexion USB.

Réseau de sécurité

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

Pour maintenir un niveau d'intégrité élevé lors de l'acheminement de messages via des passerelles, des switchs ou des routeurs standard, chaque station terminale d'un système de commande CIP Safety routable doit avoir une référence 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 attribué aux dispositifs de sécurité pour un segment de réseau donné doit être unique. Vous devez vous assurer qu'un numéro SNN unique est attribué à chaque réseau CIP Safety contenant des dispositifs de sécurité.

Le numéro SNN attribué aux dispositifs de sécurité pour un segment de réseau donné doit être unique. Vous devez vous assurer qu'un numéro SNN unique est attribué à chaque réseau CIP Safety contenant des dispositifs de sécurité.

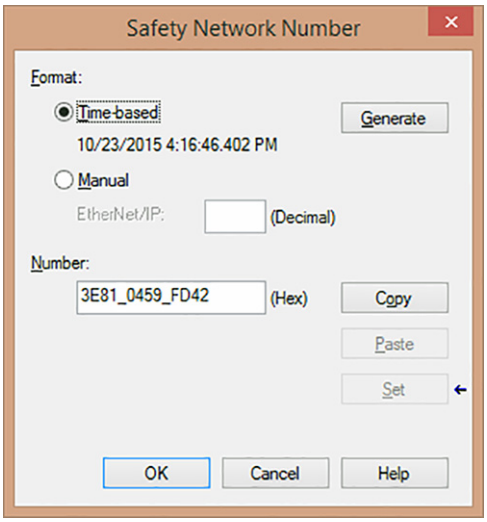
CONSEIL Plusieurs numéros de réseau de sécurité peuvent être attribués à un sous-réseau CIP Safety ou à un châssis ControlBus™ contenant plusieurs dispositifs de sécurité.

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

SNN temporel

Si le format temporel 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.

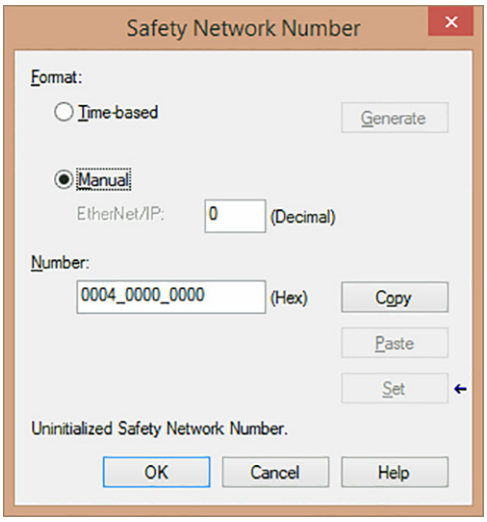
Figure 7 – Format SNN temporel



SSN 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 8 – Format SNN manuel



Attribution du numéro de réseau de sécurité (SNN)

Vous pouvez laisser l'application Logix Designer 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 66.

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

Un avertissement s'affiche si votre projet contient des doublons de combinaisons de SNN et d'adresse de station. Vous pouvez toujours vérifier le projet mais Rockwell Automation vous recommande de résoudre les combinaisons en double.

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.

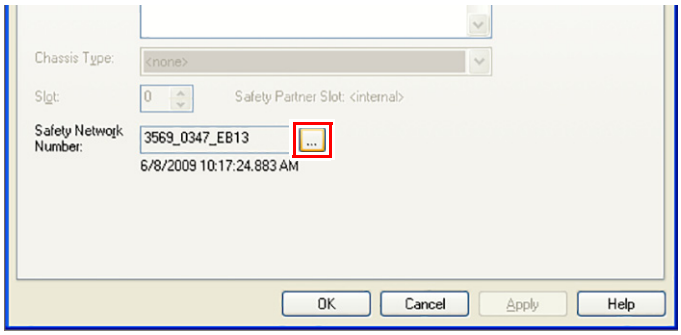
Modification du numéro de réseau de sécurité (SNN)

Avant de modifier le SNN vous devez faire ce qui suit :

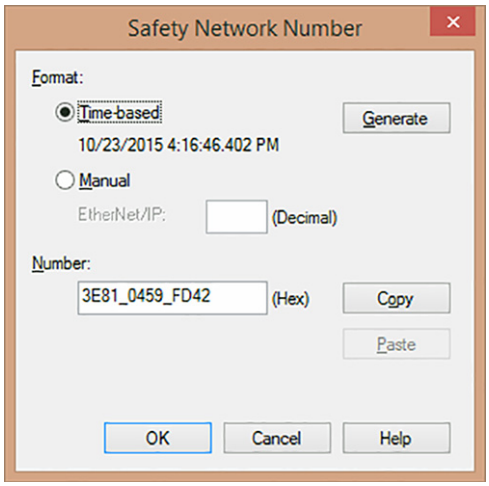
- Déverrouiller le projet, si la sécurité est verrouillée.
  Voir Verrouillage de sécurité de l'automate, page 156.
- Supprimer la signature de tâche de sécurité, s'il en existe une.
  Voir Suppression de la signature de tâche de sécurité, page 159.

Modification du numéro SNN de l'automate

1. Dans la fenêtre d'organisation de l'automate, cliquez sur l'automate concerné avec le bouton droit de la souris et sélectionnez Properties (Propriétés).
2. Dans l'onglet General de la boîte de dialogue Controller Properties (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 de réseau de sécurité).



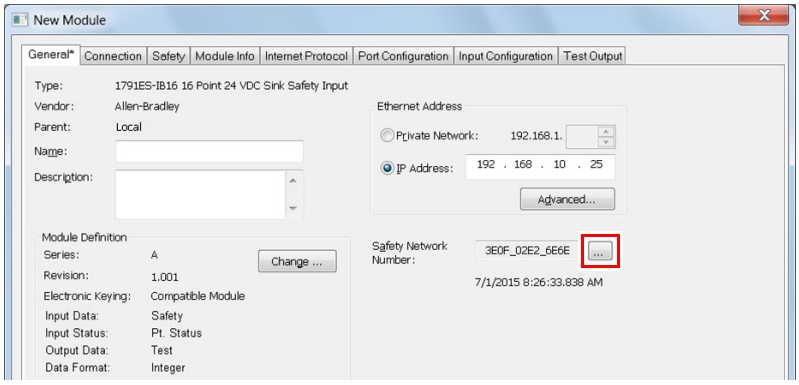
3. Sélectionnez Time-based (Temporel) et cliquez sur Generate.



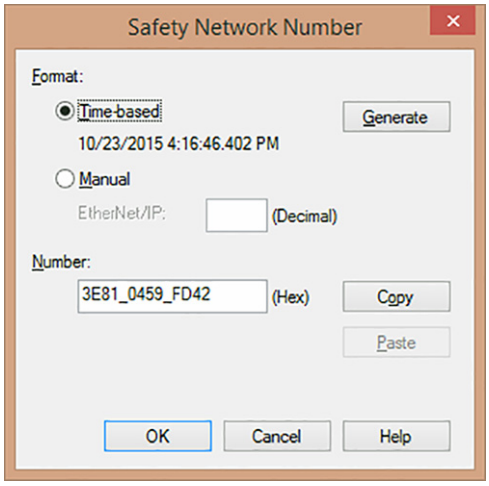
4. Cliquez sur OK.

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

1. Dans la fenêtre d'organisation de l'automate, cliquez deux fois sur le premier module d'E/S de sécurité sous le réseau Ethernet pour afficher l'onglet General.
2. Cliquez sur le bouton ... situé à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro de réseau de sécurité).



3. Sélectionnez Time-based (Temporel) et cliquez sur Generate pour générer un nouveau numéro SNN pour ce réseau EtherNet/IP.

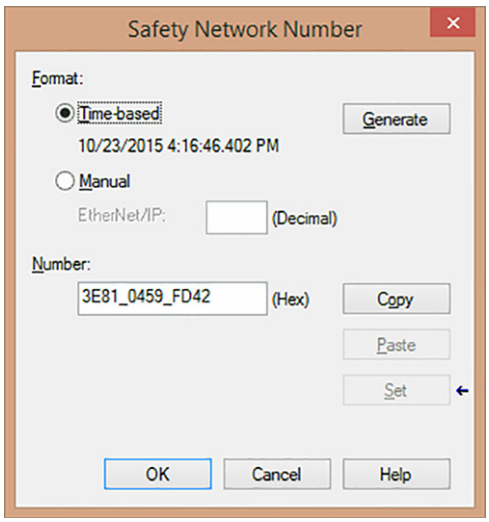


4. Cliquez sur OK.
5. Cliquez sur Copy pour copier le nouveau numéro SNN dans le presse-papiers de Windows.
6. Ouvrez l'onglet General (Général) de la boîte de dialogue des propriétés du module pour le module d'E/S de sécurité suivant dans la liste de ce module EtherNet/IP.
7. Cliquez sur le bouton ...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

Communication réseau EtherNet/IP

Le réseau EtherNet/IP propose un ensemble complet de services de commande, de configuration et de collecte des données en superposant le protocole CIP par dessus les protocoles Internet standard, tels que TCP/IP et UDP. Cette combinaison de standards reconnus fournit les capacités requises pour la prise en charge de l'échange d'informations et des applications de commande.

Les automates Compact GuardLogix 5370 utilisent des transactions par interface de connexion et des communications classiques sur le réseau EtherNet/IP pour communiquer avec les dispositifs Ethernet qui ne prennent pas en charge le protocole d'application EtherNet/IP.

Pour de plus amples informations sur ces transactions par interface de connexion, voir Interface de connexion, page 75.

Logiciels disponibles

Les applications logicielles répertoriées dans le tableau suivant sont utilisées avec un automate Compact GuardLogix 5370 en réseau EtherNet/IP.

Logiciel	Version requise	Fonctions	Requis
Environnement Studio 5000®	28.00.00 ou ultérieure	• Configurer le projet CompactLogix™ • Définir la communication EtherNet/IP • Modifier l'adresse IP des périphériques du réseau, y compris l'automate Compact GuardLogix 5370	Oui
RSLinx® Classic	3.80 ou ultérieure	• Attribuer ou modifier les adresses IP des périphériques d'un réseau EtherNet/IP • Configurer des dispositifs de communication • Fournir des diagnostics • Établir la communication entre les dispositifs	
Utilitaire BOOTP/DHCP	La version la plus récente est installée avec le logiciel RSLinx Classic	Attribution d'adresses IP aux dispositifs d'un réseau EtherNet/IP	Non

Fonctionnalités EtherNet/IP

Les automates Compact GuardLogix 5370 offrent les fonctionnalités réseau EtherNet/IP suivantes :

- Double port EtherNet/IP intégré
- Prise en charge des topologies réseau EtherNet/IP suivantes :
  - Topologie réseau en anneau de niveau dispositif (DLR)
  - Topologie réseau linéaire
  - Topologie réseau en étoile
- Prise en charge du protocole CIP Safety
- Prise en charge de la commande d'axe intégrée en réseau EtherNet/IP
- Interface de connexion pour communiquer avec les dispositifs Ethernet ne prenant pas en charge le protocole d'application EtherNet/IP

- Détection d'adresses IP en double
- Communications unicast et multicast multidiffusion
- Prise en charge de la messagerie, des points produits/consommés, des IHM et des E/S distribuées
- Interface RJ45 pour câbles à paire torsadée
- Prise en charge des communications half et full duplex à 10 ou 100 Mbits/s
- Compatible avec les switchs standard
- Planification de réseau non requise
- Tables de routage non requises

Stations d'un réseau EtherNet/IP

Lorsque vous configurez votre système de commande Compact GuardLogix 5370, vous devez tenir compte du nombre de stations Ethernet à inclure dans la section de configuration des E/S de votre projet. Les automates Compact GuardLogix 5370 sont limités en nombre de stations qu'ils peuvent prendre en charge dans la section de configuration des E/S.

Tableau 7 – Recommandations sur les stations Ethernet des automates Compact GuardLogix 5370

N° réf.	Stations Ethernet gérées
1769-L30ERMS	16
1769-L33ERMS 1769-L33ERMOS	32
1769-L36ERMS 1769-L36ERMOS	48
1769-L37ERMOS(1)	64

(1) Accessible en tant que révision du firmware 30.

IMPORTANT Bien que les automates Compact GuardLogix 5370 offrent la possibilité d'optimiser la conception du système de commande par un recensement précis des stations Ethernet, ils n'en sont pas moins limités en terme de nombre de connexions à un réseau EtherNet/IP.

Pour de plus amples informations sur la conception d'un réseau EtherNet/IP pour votre système de commande Compact GuardLogix 5370, vous pouvez utiliser les outils et documents suivants :

- L'outil EtherNet/IP Capacity Tool, disponible à l'adresse http://www.rockwellautomation.com/global/products-technologies/integrated-architecture/tools/overview.page.
  Cet outil facilite la conception initiale de votre réseau EtherNet/IP.
- Publication ENET-RM002, « Ethernet Design Considerations Reference Manual ».

Périphériques exclus du décompte des stations

Pour calculer le nombre total de stations Ethernet gérables par un automate Compact GuardLogix 5370, vous n'avez pas besoin de compter les périphériques Ethernet qui sont présents physiquement sur le réseau EtherNet/IP mais ne sont pas inclus dans la section de configuration des E/S du projet.

Les périphériques suivants ne sont pas inclus dans la section de configuration des E/S de votre projet et ne sont pas comptés dans le nombre total de stations :

- Ordinateur
- Terminaux d'IHM n'entrant pas dans la section de configuration des E/S, comme les terminaux PanelView™ Plus
- Instructions MSG
- Périphériques avec lesquels les automates Compact GuardLogix 5370 utilisent une interface de connexion pour communiquer.

  Par exemple, les périphériques suivants nécessitent une interface de connexion pour pouvoir communiquer :

  – Dispositifs TCP/IP Modbus
  – Lecteurs de codes-barres

Topologies réseau EtherNet/IP

Les automates Compact GuardLogix 5370 acceptent les types de réseau EtherNet/IP suivants :

- Topologie réseau en anneau de niveau dispositif (DLR)
- Topologie réseau linéaire
- Topologie réseau en étoile

Chacune de ces topologies réseau EtherNet/IP est compatible, si nécessaire, avec les applications comprenant une commande d'axe intégrée sur EtherNet/IP.

Topologie réseau en anneau de niveau dispositif (DLR)

Une topologie réseau DLR correspond à un réseau en boucle à tolérance de défaut unique, destiné à l'interconnexion de composants d'automatisme. Un tel réseau est constitué de stations de supervision (actives et de sauvegarde) et de stations de raccordement à l'anneau.

Les topologies réseau DLR se transforment automatiquement en topologies réseau linéaires lorsqu'un défaut est détecté. Cette conversion dans la nouvelle topologie maintient le transfert des données sur le réseau. La condition de défaut est généralement facile à détecter et à rectifier.

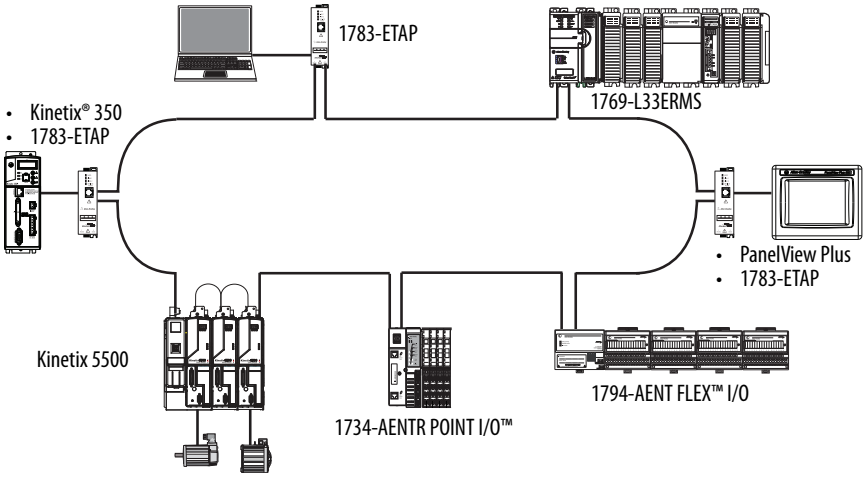
Les automates Compact GuardLogix 5370 se connectent directement en topologie réseau DLR, c'est-à-dire sans avoir besoin de passer par un module de connexion 1783-ETAP. Les automates peuvent jouer n'importe quel rôle sur un réseau DLR : station de supervision active, station de supervision de sauvegarde ou station de raccordement à l'anneau.

IMPORTANT	Les exemples de topologie présentés dans les figures de cette section font référence à des applications en topologie réseau DLR uniquement. Nous vous recommandons d'être prudent(e) dans le cas où vous envisageriez une application incluant l'interconnexion d'un réseau DLR avec un réseau linéaire ou en étoile.

Pour de plus amples informations sur les réseaux DLR, voir la publication ENET-AP005, « Technologie de switch EtherNet/IP embarqué – Guide d'application ».

La Figure 9 illustre un exemple de système de commande 1769-L33ERMS utilisant la topologie réseau DLR.

Figure 9 – Exemple de système de commande 1769-L33ERMS utilisant la topologie réseau DLR

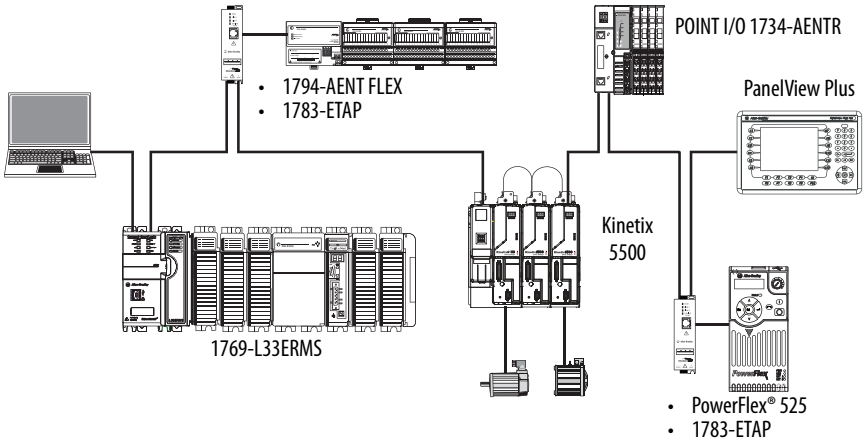


Topologie réseau linéaire

Une topologie linéaire consiste en un ensemble de périphériques raccordés en série sur un réseau EtherNet/IP. Les périphériques susceptibles de se connecter selon la topologie réseau linéaire utilisent un switch embarqué, ce qui évite d'avoir recours à un switch séparé comme dans le cas des topologies de réseau en étoile.

La Figure 10 illustre un exemple de système de commande 1769-L33ERMS utilisant la topologie réseau linéaire.

Figure 10 – Exemple de système de commande 1769-L33ERMS utilisant la topologie réseau linéaire

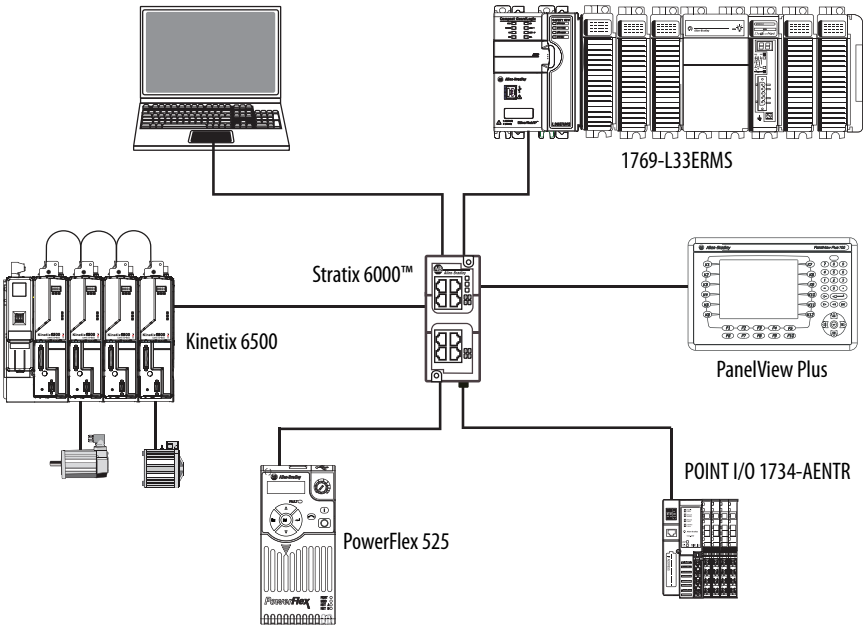


Topologie réseau en étoile

Une topologie réseau en étoile est un réseau EtherNet/IP traditionnel incluant plusieurs périphériques raccordés les uns aux autres via un switch Ethernet.

La Figure 11 illustre un exemple de système de commande 1769-L33ERMS utilisant la topologie réseau en étoile.

Figure 11 – Exemple de système de commande 1769-L33ERMS utilisant la topologie réseau en étoile



Connexions en réseau EtherNet/IP

Les automates Compact GuardLogix 5370 utilisent des connexions pour gérer les communications en réseau EtherNet/IP. Une connexion est un système de communication point à point permettant de transférer des données entre un émetteur et un récepteur. Les connexions peuvent être logiques ou physiques.

Vous définissez indirectement le nombre de connexions utilisées par l'automate lorsque vous le configurez pour communiquer avec les autres périphériques du système. Les connexions sont des affectations de ressources permettant des communications entre périphériques plus fiables que les messages sans connexion.

Toutes les connexions EtherNet/IP sont de type asynchrone. Une connexion non prioritaire consiste en un transfert de message entre automates, déclenché par l'intervalle entre trames requis (RPI) ou par le programme, par exemple par une instruction MSG. Ce système de messagerie non planifiée vous permet d'envoyer et de recevoir des données à la demande.

Tableau 8 – Caractéristiques du port réseau EtherNet/IP d'un automate Compact GuardLogix 5370

N° réf.	Connexions			Message sans connexion CIP (bus intermodules + Ethernet)	Capacité de transfert de paquets (en paquets/seconde)(2)		Prise en charge SNMP (mot de passe nécessaire)	Câble	Points produits/consommés	
	Automate	TCP	CIP		E/S	IHM/MSG			Nombre de points multicast (max.)(3)	Envoi individuel possible
1769-L30ERMS	256	120	256	256	6000 (paquets de 500 octets)	400 messages/s dans une portion du temps de comm. de 20 %	Oui	Paire torsadée	• 32 points produits multidiffusés • 128 points produits monodiffusés	Oui
1769-L33ERMS										
1769-L33ERMOS										
1769-L36ERMS										
1769-L36ERMOS										
1769-L37ERMOS(1)										

(1) Accessible en tant que révision du firmware 30.

(2) Capacité totale de transfert de paquets = points d'E/S produits, max + IHM/MSG, débit max. de transfert de paquets varie en fonction de la taille des paquets. Pour de plus amples informations, reportez-vous à la section relative à la capacité du fichier EDS pour le produit concerné.

(3) Nombre de connexions CIP d'E/S (max.)

Interface de connexion

L'automate Compact GuardLogix 5370 peut utiliser des interfaces de connexion pour communiquer avec des périphériques Ethernet qui ne prennent pas en charge le protocole d'application EtherNet/IP.

Exemples de périphériques ne prenant pas en charge le protocole d'application EtherNet/IP mais pouvant être utilisés dans une application d'automate Compact GuardLogix 5370 :

- Dispositifs TCP/IP Modbus ;
- Lecteurs de codes-barres ;
- Lecteurs RFID

Une interface de connexion est mise en œuvre à l'aide d'un objet Socket. Les automates Compact GuardLogix 5370 communiquent avec cet objet Socket au moyen d'instructions MSG. Tous les automates Compact GuardLogix 5370 doivent utiliser des instructions MSG déconnectées avec des interfaces de connexion.

Pour de plus amples informations sur les services de connexion, voir :

- La publication 1769-UM021, « Automates GuardLogix 5370 – Manuel utilisateur »
- La publication ENET-AT002, « EtherNet/IP Socket Interface Application Technique »

Qualité du service (QoS) et connexions au module d'E/S

Les automates Compact GuardLogix 5370 sont compatibles avec la technologie QoS (qualité du service). QoS permet à l'automate d'établir des priorités dans le trafic sur le réseau EtherNet/IP. Par défaut, les automates Compact GuardLogix 5370 ont la fonctionnalité QoS activée. La fonctionnalité QoS peut être désactivée en configurant une instruction de message dans l'application Logix Designer.

Certains périphériques EtherNet/IP ne prennent pas en charge la technologie QoS à moins que leur firmware ne soit mis à jour à un niveau de version compatible. Par exemple, le module de communication ControlLogix ™ 1756-ENBT doit utiliser le firmware de version 4.005 ou supérieure pour pouvoir prendre en charge la technologie QoS.

Afin de garantir le bon fonctionnement de la communication entre l'automate Compact GuardLogix 5370 et les modules des E/S, vérifiez que les périphériques EtherNet/IP utilisent bien le niveau de firmware minimum requis pour qu'ils puissent prendre en charge la technologie QoS.

Pour des informations complémentaires sur les points ci-après, consultez la note technique 66325 sur la base de connaissances de Rockwell Automation® (disponible à la page https://rockwellautomation.custhelp.com/):

- Niveaux minimum de version de firmware des périphériques EtherNet/IP afin de prendre en charge la technologie QoS
- Activation/désactivation de la fonctionnalité QoS

Communication en réseau DeviceNet

Les automates Compact GuardLogix 5370 peuvent communiquer avec d'autres périphériques en réseau DeviceNet par l'intermédiaire d'un module scrutateur DeviceNet Compact I/O 1769-SDN. Les réseaux DeviceNet utilisent le protocole CIP pour assurer des fonctions de commande, de configuration et de collecte de données avec des équipements industriels.

IMPORTANT	Les automates Compact GuardLogix acceptent des connexions standard au réseau DeviceNet. Les réseaux CIP Safety sur DeviceNet ne sont pas pris en charge.

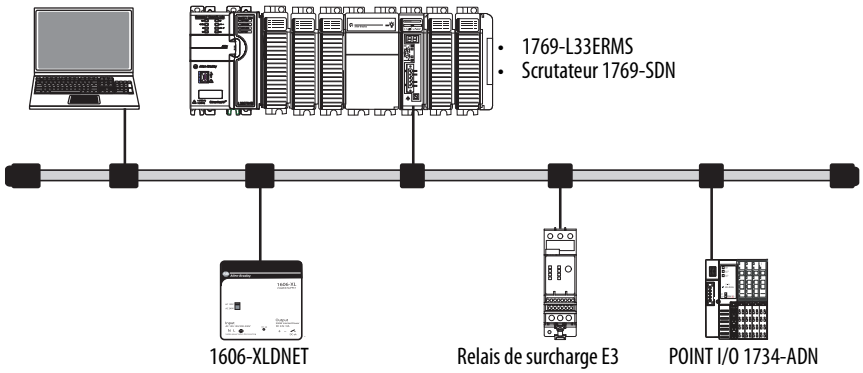
Logiciels disponibles

Les logiciels énumérés dans le tableau ci-dessous sont nécessaires pour pouvoir utiliser un automate Compact GuardLogix 5370 en réseau DeviceNet.

Logiciel	Version requise	Fonctions
Environnement Studio 5000	28.00.00 ou ultérieure	Configurer le projet CompactLogix.
RSLinx Classic	3.80 ou ultérieure	• Configurer des dispositifs de communication. • Fournir des diagnostics. • Établir la communication entre les dispositifs.
RSNetWorx™ for DeviceNet	25.00.00 ou ultérieure si utilisé avec les versions ci-dessus de l'environnement Studio 5000	• Configurer les dispositifs DeviceNet. • Définir la liste de scrutation pour le réseau DeviceNet.

La Figure 12 illustre un exemple de système de commande 1769-L33ERMS en réseau DeviceNet.

Figure 12 – Exemple de système de commande 1769-L33ERMS en réseau DeviceNet



Module scrutateur DeviceNet Compact I/O 1769-SDN

Pour raccorder un automate Compact GuardLogix 5370 à un réseau DeviceNet, il est nécessaire d'utiliser un module scrutateur DeviceNet Compact I/O 1769-SDN pour communication **standard**.

IMPORTANT CIP Safety n'est pas pris en charge sur un réseau DeviceNet avec le scrutateur 1769-SDN. Les modules d'E/S de sécurité DeviceNet ne peuvent pas être connectés à un système de commande Compact GuardLogix 5370 via le scrutateur 1769-SDN.

Points à prendre en compte

Avant d'installer ce module scrutateur, prenez note des points suivants :

- Vous pouvez raccorder le module scrutateur à un automate, une alimentation ou un module d'E/S contigu.
- Vous devez tenir compte de ces deux contraintes combinées :
  - Distance nominale par rapport à l'alimentation, voir page 78
  - Capacité électrique dans les systèmes de commande Compact GuardLogix, voir page 80
- Le module scrutateur, en tant que maître, peut gérer jusqu'à 63 stations d'E/S esclaves maximum.
- Un autre maître DeviceNet peut posséder un scrutateur qui joue alors simultanément le rôle de maître et d'esclave.

Fonctionnalités du scrutateur

Le scrutateur possède les fonctionnalités suivantes :

- gestion de la messagerie en direction des dispositifs (mais pas entre automates) ;
- gestion de l'interface réseau entre le niveau automate et le niveau dispositifs pour la programmation, la configuration, la commande et la collecte de données ;
- partage d'une couche applications commune avec les réseaux EtherNet/IP ;
- fourniture des diagnostics permettant d'améliorer la collecte des données et la détection des défauts.

Distance nominale par rapport à l'alimentation

Les systèmes de commande Compact GuardLogix 5370 vous permettent d'installer des scrutateurs 1769-SDN en tant que modules d'extension locaux. Afin d'installer le module scrutateur 1769-SDN, il faut tenir compte de sa distance nominale par rapport à l'alimentation.

La distance nominale par rapport à l'alimentation correspond au nombre maximum d'emplacements auquel le module scrutateur 1769-SDN peut être installé par rapport à l'alimentation. La module scrutateur 1769-SDN est défini par une distance nominale de quatre. Par conséquent, votre système de commande Compact GuardLogix 5370 peut comporter jusqu'à trois modules entre le module scrutateur 1769-SDN et l'alimentation.

Les systèmes de commande Compact GuardLogix 5370 ne possèdent pas de modules des E/S embarqués. Le dénombrement des emplacements d'extension locaux commence avec le premier module Compact I/O installé près de l'alimentation lorsqu'il s'agit de déterminer l'endroit où installer un module scrutateur 1769-SDN tout en satisfaisant à ses exigences en matière de distance nominale par rapport à l'alimentation.

Dans les systèmes de commande Compact GuardLogix 5370, vous pouvez installer les modules scrutateurs 1769-SDN à gauche ou à droite de l'alimentation. Vous pouvez utiliser à la fois la rangée locale et des rangées supplémentaires dans un système de commande Compact GuardLogix 5370, chacune d'elles permettant d'inclure un module scrutateur 1769-SDN.

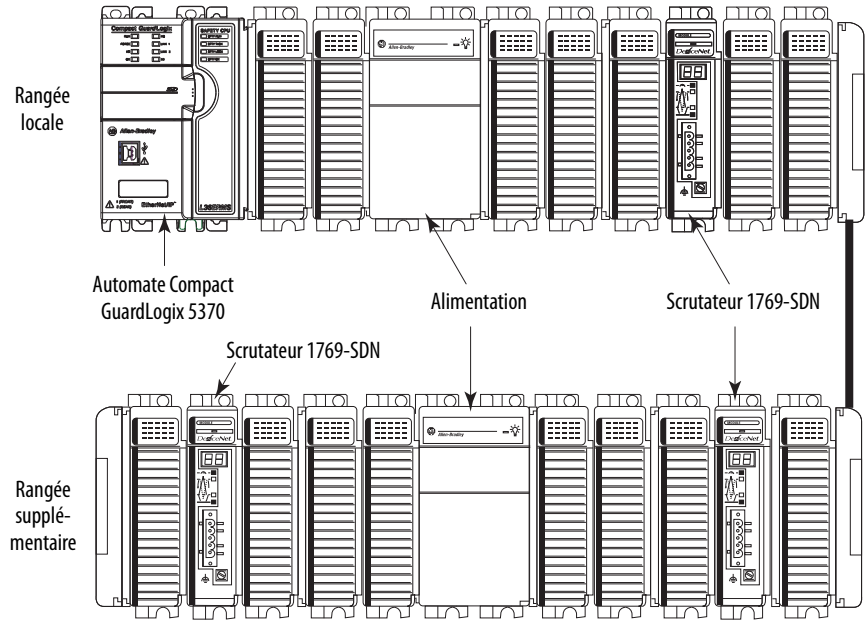
Dans la rangée locale, l'automate doit être le dispositif le plus à gauche du système et vous pouvez uniquement installer un maximum de trois modules entre l'automate et l'alimentation. Par conséquent, tout module scrutateur 1769-SDN installé à la gauche de l'alimentation dans la rangée locale, se trouve à un emplacement qui satisfait aux exigences du module en matière de distance nominale par rapport à l'alimentation.

Les systèmes de commande Compact GuardLogix 5370 prennent également en charge des rangées supplémentaires pour les modules d'extension locaux du système. Chaque rangée supplémentaire exige une alimentation Compact I/O 1769. La rangée peut être conçue avec des modules d'extension locaux de part et d'autre de l'alimentation.

Dans ce cas, vous devez installer le module scrutateur 1769-SDN de sorte qu'il est séparé de l'alimentation d'au plus trois modules Compact I/O, que les modules soient installés à gauche ou à droite de l'alimentation.

La Figure 13, page 79 illustre des modules scrutateurs 1769-SDN installés dans un système de commande 1769-L36ERMS qui satisfait aux exigences des modules en matière de distance nominale par rapport à l'alimentation.

Figure 13 – Exemple de distance nominale par rapport à l'alimentation d'un module scrutateur 1769-SDN



Capacité électrique dans les systèmes de commande Compact GuardLogix 5370

Dans une rangée locale ou supplémentaire, les modules installés de part et d'autre de l'alimentation ne peuvent pas consommer plus de courant que l'alimentation ne peut en fournir. Cette contrainte détermine en partie l'implantation des modules dans une rangée.

Par exemple, si une rangée utilise une alimentation Compact I/O 1769-PA2, chaque côté de la rangée doit avoir une capacité électrique de 1 A sous 5 V c.c. et de 0,4 A sous 24 V c.c. Puisqu'un module scrutateur 1769-SDN consomme 440 mA sous 5 V c.c. et 0 mA sous 24 V c.c., vous ne pouvez installer dans ce cas qu'un maximum de deux modules scrutateurs de part et d'autre de l'alimentation dans la rangée.

Pour de plus amples informations sur la capacité électrique maximale des alimentations Compact I/O 1769 et sur les calculs que vous pouvez effectuer pour déterminer l'implantation des modules dans une rangée locale ou supplémentaire, voir la section Calcul de la consommation électrique du système, page 87.

Ajout et configuration de modules d'E/S standard

Choix des modules des E/S

Les systèmes de commande Compact GuardLogix® 5370 offrent les options suivantes pour les modules d'E/S standard :

- Modules d'extension locaux
- Modules d'E/S distribuées standard en réseau EtherNet/IP
- Modules d'E/S distribuées standard en réseau DeviceNet

Modules d'extension locaux

Les systèmes de commande Compact GuardLogix 5370 permettent d'utiliser des modules Compact I/O™ raccordés au bus intermodules CompactBus comme modules d'extension locaux.

Les points suivants sont à prendre en compte pour l'utilisation de modules d'extension locaux :

- Les automates peuvent gérer autant de modules Compact I/O locaux qu'indiqué dans le tableau suivant, sur trois rangées d'E/S au maximum, c'est-à-dire la rangée locale et deux rangées supplémentaires.

N° réf.	Nombre max. de modules d'extension locaux pris en charge
1769-L30ERMS	8
1769-L33ERMS	16
1769-L33ERMOS	–
1769-L36ERMS	30
1769-L36ERMOS 1769-L37ERMOS(1)	–

(1) Accessible en tant que révision du firmware 30.

- Chaque fois que possible, utilisez des modules Compact I/O spécialisés pour répondre aux besoins spécifiques de votre application.
- Pour chaque module d'E/S, vous pouvez utiliser un système de câblage 1492 en alternative au bornier livré avec le module.
- Utilisez des modules et des câbles PanelConnect™ 1492 pour raccorder les modules d'entrées aux capteurs.

Installation des modules d'extension locaux

Suivez les étapes ci-dessous pour installer des modules d'extension locaux dans votre système de commande Compact GuardLogix 5370.

1. Assemblez les modules Compact 1769 de communication et d'E/S restants comme décrit dans les publications suivantes :
   - Publication 1769-IN088, « Instructions d'installation des modules Compact I/O »
   - Publication 1769-IN060, « Module scrutateur d'E/S Compact DeviceNet – Notice d'installation »
2. Si votre système n'utilise qu'une seule rangée locale, suivez la procédure ci-dessous.
   a. Utilisez le système d'emboîtement pour fixer un cache de terminaison Compact I/O 1769-ECR sur le dernier module du système.
   b. Déplacez le levier du cache de terminaison à fond sur la gauche jusqu'à ce qu'il s'enclenche et verrouille le cache.
3. Si votre système utilise des rangées supplémentaires, suivez cette procédure.
   a. Branchez un câble d'extension du bus de communication Compact I/O 1769-CR*x* à l'extrémité droite de la rangée locale.
   b. Raccordez ce câble 1769-CR*x* à la rangée supplémentaire de la façon appropriée.

      Autrement dit, la manière dont vous effectuez le raccordement à la première rangée supplémentaire – à droite ou à gauche de la rangée – détermine le câble d'extension qui est installé à l'extrémité de la rangée locale. Voir page 91 pour un exemple de raccordement d'une rangée locale à des rangées supplémentaires.
   c. Terminez le montage des rangées restantes de votre système.

IMPORTANT	N'oubliez pas de placer un cache de terminaison à l'extrémité de la dernière rangée du système.

La Figure 2, page 28 illustre des exemples de système comportant des modules d'extension locaux.

Câblage des modules d'extension locaux

Câblez chaque module Compact I/O utilisé en tant que module d'extension local conformément à la documentation technique portant sur le module en question.

Modules d'E/S distribuées standard en réseau EtherNet/IP

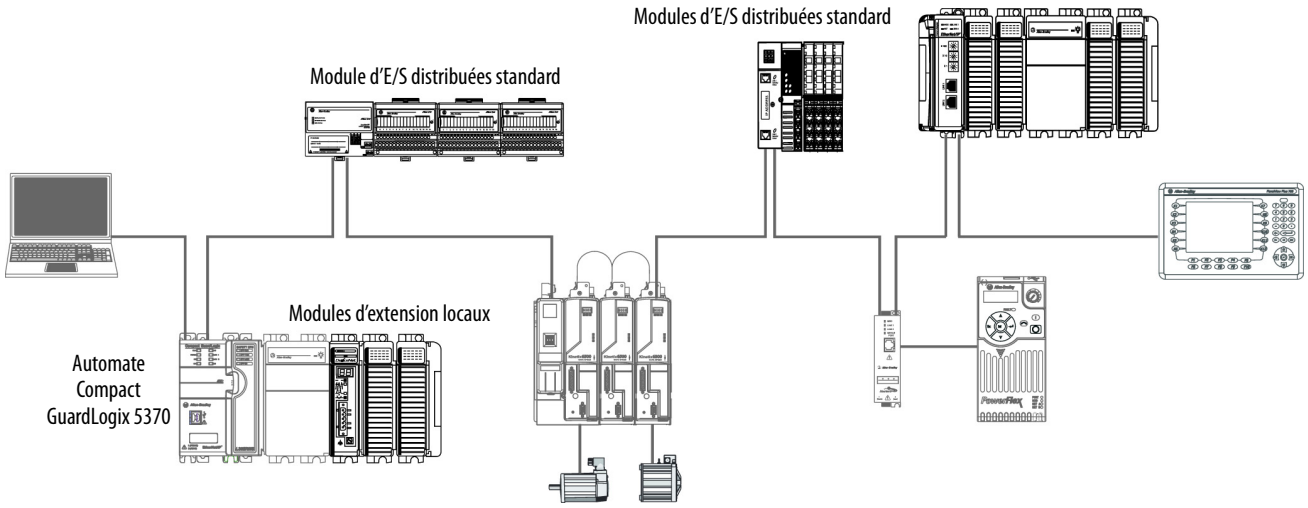
Vous pouvez inclure des modules des E/S distribuées standard en réseau EtherNet/IP dans votre système de commande Compact GuardLogix 5370. Tenez compte des points suivants lorsque vous utilisez des modules des E/S distribuées en réseau EtherNet/IP :

- Chaque adaptateur EtherNet/IP décentralisé faisant partie du système doit être pris en compte dans le calcul du nombre maximum autorisé de stations EtherNet/IP pour l'automate.

  Pour de plus amples informations sur le nombre maximum autorisé de stations EtherNet/IP, voir Stations d'un réseau EtherNet/IP, page 71.
- Les réglages de configuration du RPI varient selon les modules des E/S distribuées utilisés dans le système.

La Figure 14 présente un exemple de système de commande 1769-L33ERMS utilisant des modules d'extension locaux et des modules des E/S distribuées standard en réseau EtherNet/IP.

Figure 14 – Exemple de système de commande 1769-L33ERMS avec modules en réseau EtherNet/IP



Modules d'E/S distribuées standard en réseau DeviceNet

Vous pouvez inclure des modules des E/S distribuées standard en réseau DeviceNet dans votre système de commande Compact GuardLogix 5370.

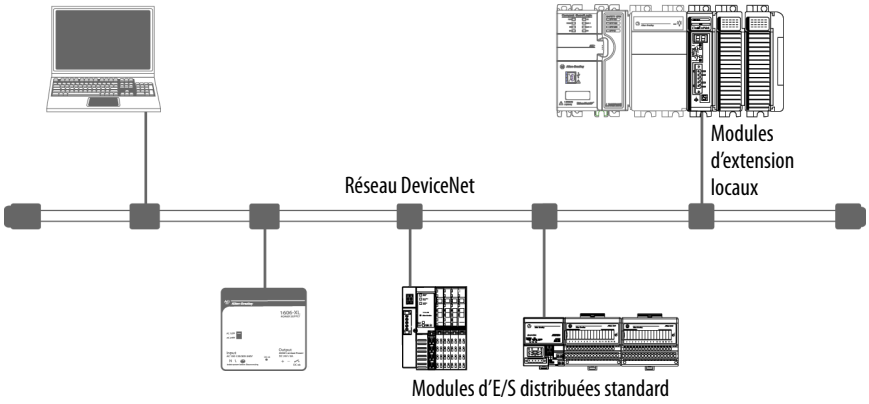
IMPORTANT	CIP Safety n'est pas pris en charge sur un réseau DeviceNet avec le module 1769-SDN. Les modules d'E/S de sécurité DeviceNet ne peuvent pas être connectés à un système Compact GuardLogix via le module 1769-SDN.

Tenez compte des points suivants lorsque vous utilisez des modules des E/S distribuées en réseau DeviceNet :

- Environnement Studio 5000® – Pour plus d'informations, voir Configuration des modules des E/S distribuées standard en réseau EtherNet/IP, page 96.
- Logiciel RSNetWorx™ for DeviceNet – Pour plus d'informations, voir Communication en réseau DeviceNet, page 76.
- Pour de plus amples informations sur l'ajout de modules des E/S distribuées à un système de commande Compact GuardLogix 5370, voir Configuration de modules des E/S distribuées standard en réseau DeviceNet, page 98.

La Figure 15 présente un exemple de système de commande 1769-L33ERMS utilisant des modules d'extension locaux et des modules des E/S distribuées standard en réseau DeviceNet.

Figure 15 – Exemple de système de commande 1769-L33ERMS avec modules en réseau DeviceNet



Validation de l'agencement des E/S

Une fois que vous avez choisi vos modules des E/S, vous devez valider la conception du système que vous voulez réaliser. Les points suivants sont à prendre en compte pour valider cette organisation des E/S :

- Estimation de l'intervalle entre trames requis
- Défauts de module liés aux estimations de RPI
- Calcul de la consommation électrique du système
- Distance nominale de l'alimentation
- Implantation physique des modules des E/S

Estimation de l'intervalle entre trames requis

L'intervalle entre trames requis (RPI) définit la fréquence à laquelle l'automate envoie des données aux modules des E/S et en reçoit de ces mêmes modules. Vous pouvez définir le RPI de chaque module d'E/S de votre système.

Les automates Compact GuardLogix 5370 essaient toujours de scruter un module d'E/S selon sa fréquence RPI configurée. Dans le cas de modules des E/S individuels, un défaut mineur de type Module RPI Overlap (Chevauchement de RPI du module) se produira lorsqu'au moins un de ces module d'E/S ne peut être traité dans le délai imparti par son RPI.

Les paramètres de configuration spécifiques à un système donné ont une incidence sur les fréquences RPI réelles. Les paramètres de configuration suivants peuvent avoir un impact sur la fréquence de scrutation réelle de n'importe quel module individuel :

- fréquences RPI définies pour les autres modules Compact I/O ;
- nombre de modules Compact I/O dans le système ;
- types de modules Compact I/O dans le système ;
- priorités des tâches d'utilisation de l'application.

Tableau 9 – Recommandations relatives à l'intervalle entre trames requis

Type de module	Recommandations[1]
Tout numérique	Les principes suivants sont à retenir : • 1 à 2 modules peuvent être scrutés en 0,5 ms. • 3 à 4 modules peuvent être scrutés en 1 ms. • 5 à 30 modules peuvent être scrutés en 2 ms.
Mélange de numérique et d'analogique ou tout analogique	Les principes suivants sont à retenir : • 1 à 2 modules peuvent être scrutés en 0,5 ms. • 3 à 4 modules peuvent être scrutés en 1 ms. • 5 à 13 modules peuvent être scrutés en 2 ms. • 14 à 30 modules peuvent être scrutés en 3 ms.
Spécialisé	Les règles suivantes s'appliquent : • Pour chaque module 1769-SDN présent dans le système, augmentez le RPI de chacun des autres modules de 2 ms. • Pour chaque module 1769-HSC présent dans le système, augmentez le RPI de chacun des autres modules de 1 ms. • Pour chaque module 1769-ASCII présent dans le système, augmentez le RPI de chacun des autres modules de 1 ms. • Pour chaque module 1769-SM2 présent dans le système, augmentez le RPI de chacun des autres modules de 2 ms.

(1) Les recommandations présentées dans le tableau ne tiennent pas compte des éléments suivants, qui influent sur la charge du processeur de l'automate Compact GuardLogix 5370 :

- Le fait que les temps RPI d'E/S n'affectent pas la priorité des tâches. Les tâches événementielles et périodiques ont une priorité plus élevée que les tâches d'E/S et les tâches utilisateur.
- IOT (instruction de Sortie Immédiate)
- Messagerie
- L'exploration CompactBus telle que l'accès réseau DeviceNet via 1769-SDN avec connexion Ethernet ou USB du Compact GuardLogix 5370.

Les recommandations de RPI de module peuvent nécessiter des ajustements (augmentation de 1 ms ou plus) si l'application automate Compact GuardLogix 5370 comporte un ou plusieurs des éléments répertoriés dans ce tableau. Surveillez les défauts mineurs d'automate pour déterminer la présence de chevauchements de RPI.

Vous pouvez définir les fréquences RPI de modules Compact I/O individuels à des valeurs supérieures aux fréquences indiquées dans le Tableau 9. Le RPI indique la rapidité à laquelle les modules peuvent être scrutés, mais il ne présume pas de la rapidité avec laquelle l'application est capable de traiter les données. Le RPI est asynchrone par rapport à la scrutation du programme. D'autres facteurs, comme la durée d'exécution du programme, affectent le débit des E/S.

Défauts de module liés aux estimations de RPI

Si vous suivez les recommandations du Tableau 9, la plupart des systèmes automates Compact GuardLogix 5370 fonctionneront de façon satisfaisante. Malgré le respect de ces recommandations, certains systèmes pourront cependant rencontrer les défauts mineurs de chevauchement de RPI du module, décrits dans le Tableau 10.

Tableau 10 – Chevauchement de RPI du module détecté

Nom	Information du défaut	Condition de survenue du défaut
Module RPI Overlap (Chevauchement de RPI du module)	(Type 03) défaut d'E/S (Code 94) chevauchement de RPI du module détecté Module Slot (Emplacement module) = *x*, dans lequel *x* correspond au numéro d'emplacement du module d'E/S tel que spécifié à la section de configuration des E/S	Ce défaut est consigné lorsque la mise à jour de RPI actuelle d'un module d'E/S chevauche la mise à jour de RPI précédente. Le module dont le RPI présentant un chevauchement est indiqué dans l'onglet Minor Faults (défauts mineurs) de la boîte de dialogue Controller Properties (Propriétés de l'automate). Si plusieurs modules des E/S présentent ce défaut, l'application n'indiquera que le premier module d'E/S sur lequel s'est produit le défaut. Il s'agira généralement d'un module d'E/S ayant une grande capacité d'entrées/sorties. Comme exemple de modules offrant une grande capacité d'entrées/sorties, on peut citer les modules 1769-SDN et 1769-HSC. Dans ces cas, nous vous recommandons d'ajuster le RPI du module pour éliminer le défaut. Une fois que le défaut est effacé du premier module d'E/S, l'application indique le module suivant sur lequel survient le défaut. Ce processus se poursuit jusqu'à ce que le défaut ait été supprimé de tous les modules d'E/S affectés. Pour éviter ce défaut, réglez le RPI des modules d'E/S à des valeurs numériques plus élevées. Il est recommandé d'utiliser une valeur de fréquence RPI qui ne puisse pas être un multiple commun des RPI des autres modules, comme 2,5 ms, 5,5 ms ou 7 ms. • Il est recommandé de ne pas faire fonctionner un système de commande Compact GuardLogix 5370 présentant des défauts de chevauchement de RPI sur ses modules. • Un système présentant plusieurs défauts de chevauchement de RPI (Module RPI Overlap) sur ses modules peut ne pas fonctionner de façon optimale car les données d'E/S ne sont pas échantillonnées à la fréquence de RPI prévue dans la configuration. • Lorsque le projet est chargé sur l'automate ou que la valeur de RPI d'un module d'E/S est redéfinie, on peut s'attendre à l'apparition d'un défaut mineur. Les défauts survenant dans ces circonstances ont un caractère transitoire. Acquittez le défaut et vérifiez qu'il ne réapparaît plus avant de régler la valeur du RPI ou les priorités de la tâche.

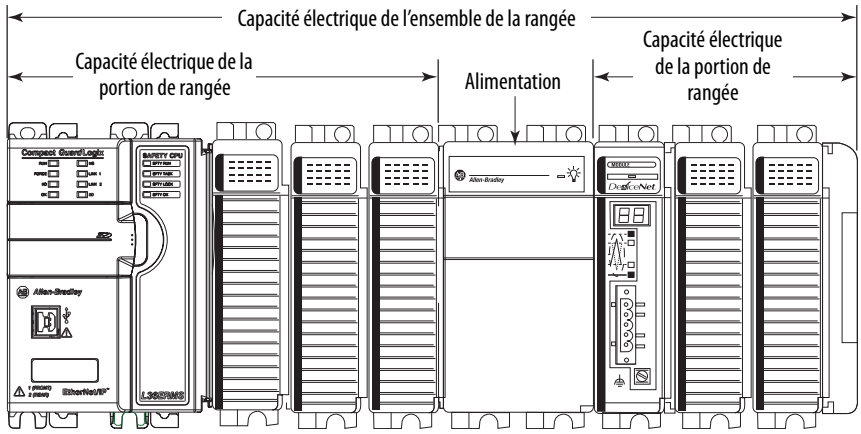
Calcul de la consommation électrique du système

Des alimentations Compact I/O 1769 sont utilisées pour alimenter la rangée Compact GuardLogix locale et chaque rangée supplémentaire. Le courant fourni par cette alimentation détermine la capacité électrique du système.

Les points suivants sont à prendre en compte pour concevoir les rangées de votre système de commande Compact GuardLogix 5370 :

- Les alimentations Compact I/O 1769 sont soumises à deux contraintes de capacité électrique maximale qui influent toutes deux sur la conception et la configuration de chaque rangée.

  Ces contraintes de capacité électrique maximale sont les suivantes :
  - la capacité électrique maximale de l'ensemble de la rangée ;
  - la capacité électrique maximale de chaque côté de l'alimentation.



- Les contraintes de capacité électrique maximale varient selon l'alimentation utilisée pour la rangée.

N° cat. d'alimentation	Capacité électrique max. pour l'ensemble de la rangée	Capacité électrique max. pour chaque portion de rangée[1]
1769-PA2	2 A sous 5 V c.c. et 0,8 A sous 24 V c.c.	1 A sous 5 V c.c. et 0,4 A sous 24 V c.c.
1769-PB2		
1769-PA4	4 A sous 5 V c.c. et 2 A sous 24 V c.c.	2 A sous 5 V c.c. et 1 A sous 24 V c.c.
1769-PB4		

(1) Caractéristiques applicables aux rangées présentant des dispositifs à gauche et à droite de l'alimentation.

Calcul de la consommation électrique d'une rangée simple

IMPORTANT Une rangée exige que l'automate Compact GuardLogix 5370 réside dans l'emplacement le plus à gauche. Vous devez donc au minimum calculer la consommation électrique de cet automate sur la portion de rangée située à gauche de l'alimentation.

Si d'autres modules sont présents à gauche de l'alimentation, vous devez également calculer leur consommation électrique.

Si des modules additionnels sont présents à droite de l'alimentation, vous devez calculer la consommation électrique de cette portion de rangée séparément.

Ce tableau permet de calculer la consommation électrique d'une rangée simple.

Tableau 11 – Calcul de la consommation électrique des modules d'une rangée simple

Côté de l'alimentation	N° réf.	Nombre de modules[3]	Intensité nominale du module		Intensité totale = (nombre de modules) x (intensité nominale du module)	
			sous 5 V c.c. (en mA)	sous 24 c.c. (en mA)	sous 5 V c.c. (en mA)	sous 24 c.c. (en mA)
Gauche – Obligatoire	1769-L30ERMS 1769-L33ERMS 1769-L36ERMS	1	500	225	500	225
À gauche – Facultatif	Propre au module d'E/S	Jusqu'à 3	Propre au module	Propre au module		
				Intensité totale nécessaire[2] :		
À droite	Propre au module d'E/S **IMPORTANT** : Utilisez une ligne distincte pour chaque module d'E/S entrant dans le calcul.	Jusqu'à 8	Propre au module	Propre au module		
				Intensité totale nécessaire[2] :		
				Intensité totale nécessaire pour une rangée simple lorsque les modules sont installés de chaque côté de l'alimentation[1] :		

(1) Ce nombre ne doit pas dépasser la capacité électrique de l'alimentation pour l'ensemble de la rangée.

(2) Ce nombre ne doit pas dépasser la capacité électrique de l'alimentation pour cette portion de la rangée.

(3) Dans la rangée locale, vous ne pouvez installer qu'un maximum de trois modules à gauche de l'alimentation car l'automate Compact GuardLogix 5370 a une distance nominale par rapport à l'alimentation de quatre et doit donc se trouver à quatre emplacements maximum de l'alimentation Compact I/O. Du côté droit de l'alimentation sur la rangée locale et des deux côtés de l'alimentation sur des rangées supplémentaires, vous pouvez installer jusqu'à huit modules si les valeurs de distance nominale des modules par rapport à l'alimentation le permettent.

Calcul de la consommation électrique d'une rangée supplémentaire

IMPORTANT Dans les rangées supplémentaires, vous pouvez installer les modules des E/S à gauche, à droite ou de part et d'autre de l'alimentation.

La conception du système détermine le mode d'utilisation du tableau ci-dessous.

Le Tableau 12 permet de calculer la consommation électrique d'une rangée supplémentaire.

Tableau 12 – Calcul de la consommation électrique des modules pour une rangée supplémentaire

Côté de l'alimentation	N° réf.	Nombre de modules[3]	Intensité nominale du module		Intensité totale = (nombre de modules) x (intensité nominale du module)	
			sous 5 V c.c. (en mA)	sous 24 c.c. (en mA)	sous 5 V c.c. (en mA)	sous 24 c.c. (en mA)
À gauche – Facultatif dans une rangée supplémentaire	modules des E/S **IMPORTANT** : Utilisez une ligne distincte pour chaque module d'E/S entrant dans le calcul.	Jusqu'à 8	Propre au module	Propre au module		
	Intensité totale nécessaire[2] :					
À droite – Facultatif dans une rangée simple	modules des E/S **IMPORTANT**: Utilisez une ligne distincte pour chaque module d'E/S.	Jusqu'à 8	Propre au module	Propre au module		
	Intensité totale nécessaire[2] :					
Intensité totale nécessaire pour une rangée lorsque les modules sont installés de chaque côté de l'alimentation[1] :						

(1) Ce nombre ne doit pas dépasser la capacité électrique de l'alimentation pour l'ensemble de la rangée.
(2) Ce nombre ne doit pas dépasser la capacité électrique de l'alimentation pour cette portion de la rangée.
(3) Vous pouvez installer jusqu'à huit modules dans les rangées supplémentaires si les valeurs de distance nominale des modules par rapport à l'alimentation le permettent.

Implantation physique des modules des E/S

Selon leur référence, les automates Compact GuardLogix 5370 peuvent gérer de 8 à 30 modules des E/S. Pour de plus amples informations sur les références, voir Modules d'extension locaux, page 81.

Les facteurs suivants doivent être pris en considération pour déterminer l'implantation physique des modules des E/S :

- Vous pouvez monter des modules des E/S dans la rangée locale et les rangées supplémentaires.
- Vous pouvez installer des modules des E/S à gauche et à droite de l'alimentation.
- Lorsqu'un système nécessite plus d'une rangée, vous pouvez disposer les rangées supplémentaires horizontalement ou verticalement, comme illustré à la Figure 2, page 28.
- Chaque module d'E/S est également défini par une distance nominale par rapport à l'alimentation et une consommation électrique maximum spécifique. La combinaison de ces caractéristiques de distance nominale et de consommation électrique détermine le positionnement de ces modules des E/S et leurs possibilités de montage dans une rangée donnée.

  Pour de plus amples informations sur la distance nominale des modules par rapport à l'alimentation, voir la section Distance nominale par rapport à l'alimentation, page 91. Pour de plus amples informations sur la consommation électrique d'un système, voir la section Calcul de la consommation électrique du système, page 87.

Rangée locale

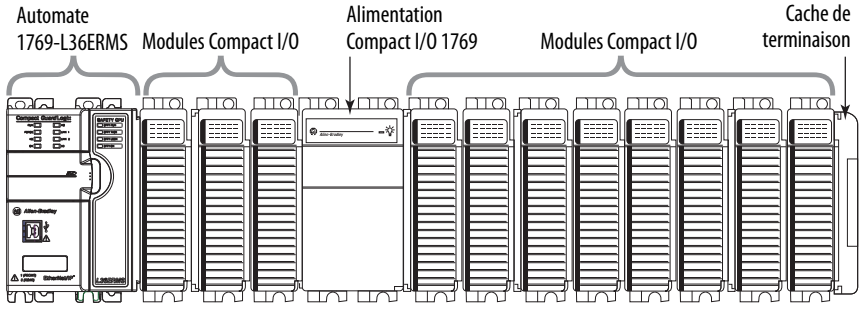
Pour valider l'agencement d'une rangée locale, vérifiez qu'il respecte les règles suivantes :

- L'automate est placé le plus à gauche dans cette rangée locale.
- Pas plus de trois modules sont montés entre l'automate et le côté gauche de l'alimentation.
- Pas plus de huit modules sont montés à droite de l'alimentation.
- La consommation électrique des modules de chaque côté de l'alimentation ne dépasse pas la capacité de l'alimentation pour le côté en question.
- La consommation électrique totale de tous les modules présents dans la rangée ne dépasse pas la capacité de l'alimentation pour l'ensemble de la rangée.
- Les modules sont placés de telle façon que toutes les contraintes de distance nominale par rapport à l'alimentation et de consommation électrique du système sont respectées.

  Par exemple, un module scrutateur 1769-SDN est défini par une distance nominale de quatre par rapport à l'alimentation. Si vous avez monté un module de scrutation 1769-SDN avec plus de trois autres modules entre lui et l'alimentation, cet agencement n'est pas acceptable.

IMPORTANT En ce qui concerne la distance nominale par rapport à l'alimentation, si vous montez un module sans respecter sa distance nominale par rapport à l'alimentation, le système pourra sembler fonctionner normalement pendant un certain temps, mais il risquera tôt ou tard de rencontrer des problèmes de fonctionnement, comme des défauts d'E/S.

La figure ci-dessous représente une rangée locale.



Rangées supplémentaires

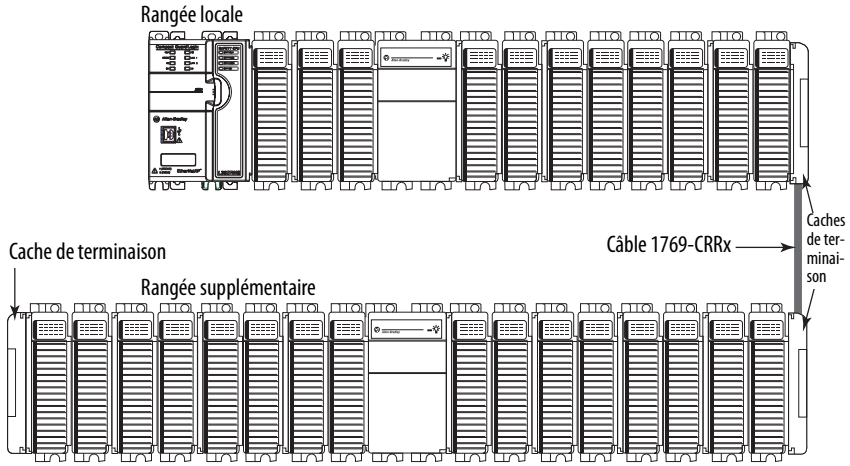
Si votre application nécessite douze modules des E/S ou plus, vous devrez répartir ces modules sur plusieurs rangées supplémentaires. Les conditions de chaque application déterminent le nombre de rangées supplémentaires.

Une fois validée la configuration de la rangée locale, vous devez valider la configuration de toutes les rangées supplémentaires. Pour cela, vérifiez que ces rangées supplémentaires respectent bien les règles suivantes :

- Les câbles d'extension de bus de communication Compact I/O sont utilisés correctement.

  CONSEIL Les câbles d'extension Compact I/O présentent les mêmes caractéristiques par rapport aux caches de terminaison, qu'ils soient montés à gauche ou à droite du bus de communication.

- Pas plus de huit modules sont installés d'un côté ou de l'autre de l'alimentation.
- La consommation électrique des modules de chaque côté de l'alimentation ne dépasse pas la capacité de l'alimentation pour le côté en question.
- Ces modules sont placés de façon à ce que toutes les contraintes de distance nominale par rapport à l'alimentation soient respectées.
- Les caches de terminaison sont correctement installés, comme illustré sur la figure ci-dessous.



Distance nominale par rapport à l'alimentation

Les systèmes de commande Compact GuardLogix 5370 ne possèdent pas de modules des E/S embarqués. Le dénombrement des emplacements d'extension locaux commence avec le premier module Compact I/O installé près de l'alimentation lorsqu'il s'agit de déterminer l'endroit où installer un module Compact I/O tout en satisfaisant à ses exigences en matière de distance nominale par rapport à l'alimentation.

Dans les systèmes de commande Compact GuardLogix 5370, vous pouvez installer les modules Compact I/O à gauche ou à droite de l'alimentation. Vous pouvez utiliser à la fois la rangée locale et des rangées supplémentaires d'un système de commande Compact GuardLogix 5370, chacune d'elles permettant d'inclure des modules Compact I/O.

Rangée locale

Dans la rangée locale, l'automate doit être le dispositif le plus à gauche du système et vous pouvez uniquement installer un maximum de trois modules entre l'automate et l'alimentation. Par conséquent, tout module Compact I/O installé à la gauche de l'alimentation dans la rangée locale, se trouve à un emplacement qui satisfait aux exigences du module en matière de distance nominale par rapport à l'alimentation.

Rangées supplémentaires

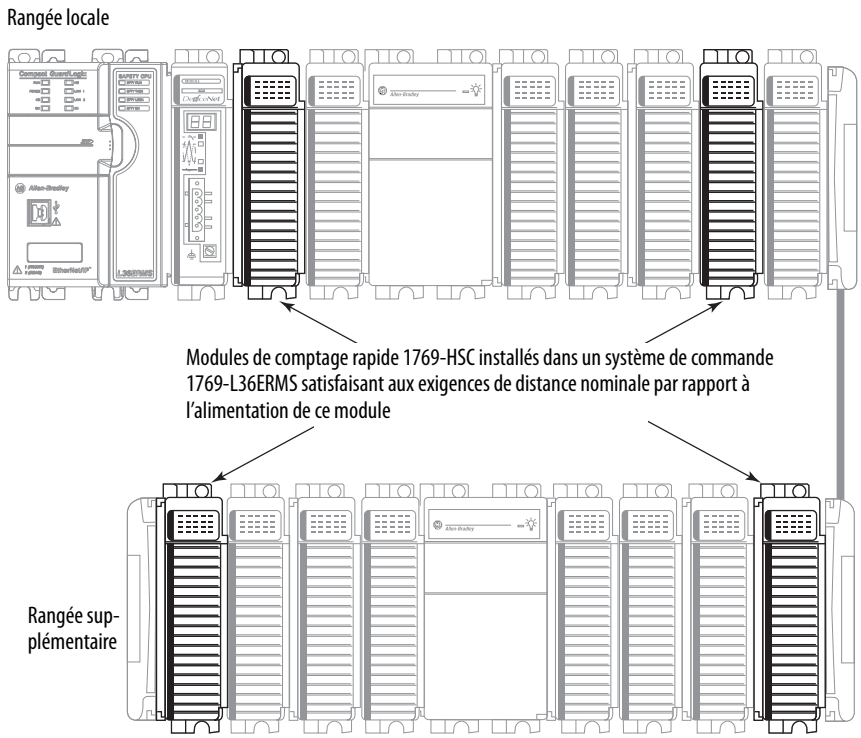
Les systèmes de commande Compact GuardLogix 5370 prennent également en charge des rangées supplémentaires pour les modules d'extension locaux du système. Chaque rangée supplémentaire exige une alimentation Compact I/O 1769. La rangée peut être conçue avec des modules d'extension locaux de part et d'autre de l'alimentation.

La plupart des modules Compact I/O ont des valeurs de distance nominale par rapport à l'alimentation qui permettent de les installer dans des rangées supplémentaires à n'importe quel emplacement de part et d'autre de l'alimentation. Certains modules Compact I/O ont des distances nominales par rapport à l'alimentation qui influent sur l'endroit où vous pouvez les installer dans le système de commande Compact GuardLogix 5370.

Par exemple, les module compteurs rapides Compact 1769-ASCII et Compact 1769-HSC possèdent chacun une distance nominale de quatre par rapport à l'alimentation. Ces modules peuvent être installés dans les emplacements 1 à 3 de module d'extension local.

Dans ce cas, vous devez installer le module 1769-ASCII et le module compteur rapide 1769-HSC de sorte que chacun d'eux est séparé de l'alimentation d'au plus trois modules Compact I/O, que les modules soient installés à gauche ou à droite de l'alimentation.

La figure ci-dessous illustre des modules compteurs rapides 1769-HSC installés dans un système de commande 1769-L36ERMS qui satisfait aux exigences des modules en matière de distance nominale.

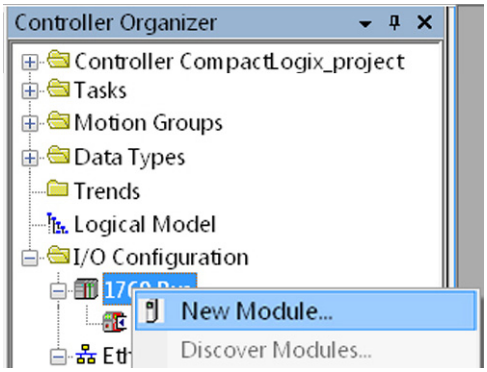


Pour de plus amples informations sur la distance nominale des modules Compact I/O par rapport à l'alimentation, voir la publication 1769-SG001 « Guide de sélection CompactLogix™ ».

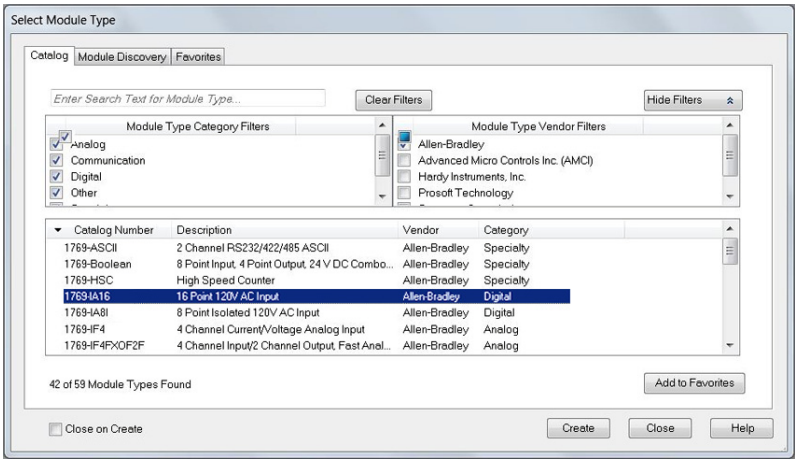
Configuration d'E/S standard

Suivez les étapes ci-dessous pour ajouter un module Compact I/O à votre système de commande Compact GuardLogix 5370 et le configurer.

1. Dans la fenêtre d'organisation de l'automate, sélectionnez 1769 Bus sous la configuration des E/S (I/O Configuration) et faites un clic droit ; choisissez New Module (Nouveau module).

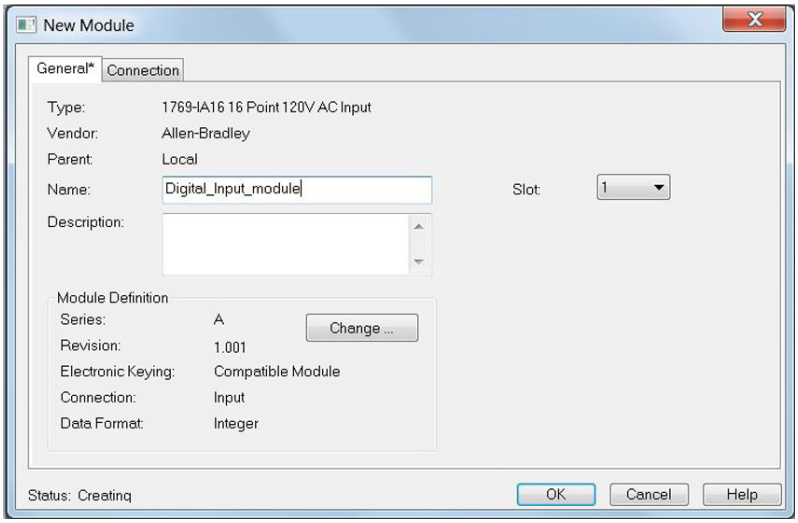


2. Sélectionnez le module d'E/S désiré et cliquez sur Create (Créer).



La boîte de dialogue New Module (Nouveau module) apparaît.

3. Configurez le nouveau module d'E/S comme souhaité et cliquez sur OK.



Paramètres de configuration communs

Bien que les options de configuration varient d'un module à l'autre, il existe un tronc commun d'options qui sont normalement à configurer lorsqu'on utilise des modules Compact I/O dans un système de commande Compact GuardLogix 5370. Elles sont décrites dans le Tableau 13.

Tableau 13 – Paramètres de configuration communs

Option de configuration	Description
Requested packet interval – RPI (intervalle entre trames requis)	Le RPI définit l'intervalle auquel les données sont transmises ou reçues sur une connexion. Pour les modules Compact I/O 1769 locaux, les données sont transmises à l'automate selon le RPI. Pour la scrutation des modules d'entrée sur le bus local ou sur le réseau EtherNet/IP, le RPI défini dans la configuration de ces modules est utilisé. Habituellement, le RPI est défini en millisecondes (ms). Pour les modules des E/S, la plage va de 0,5 à 750 ms. En réseau DeviceNet, les modules d'entrées distribuées sont scrutés à la fréquence utilisée par l'adaptateur DeviceNet qui relie ces modules d'entrées au réseau. Par exemple, la fréquence de scrutation de POINT I/O™ 1734 distribué sur DeviceNet ne pourra pas être supérieure à la vitesse de transmission des données de l'adaptateur DeviceNet 1734-ADN.
Module definition (Définition du module)	Ensemble de paramètres de configuration déterminant la transmission des données entre l'automate et le module d'E/S. Ces paramètres incluent : • Série – Série matérielle du module. • Version – Numéros de version majeure et mineure du firmware utilisés pour le module. • Détrompage électronique – Voir LOGIX-AT001 pour des informations sur le détrompage électronique. • Connexion – Type de connexion entre l'automate qui définit la configuration et le module d'E/S ; par exemple, de sortie (Output). • Format de données – Type des données qui sont transférées entre l'automate et le module d'E/S et points qui sont générés lorsque la configuration est terminée.
Major Fault on Controller If Connection Fails While in Run Mode (défaut majeur sur l'automate si la connexion échoue en mode d'exécution)	Cette option définit la façon dont l'automate doit se comporter au cas où la connexion avec un module d'E/S échouerait en mode d'exécution. Vous pouvez configurer votre projet de façon à ce que cet échec de la connexion entraîne ou non la génération d'un défaut majeur sur l'automate. Par défaut, l'option est réglée sur activée (enabled), c'est-à-dire que si la connexion à un module d'E/S échoue en mode d'exécution, un défaut majeur est déclenché sur l'automate.

Connexions d'E/S

Un système Logix5000™ utilise des connexions pour transmettre les données d'E/S. Ces connexions sont décrites dans le Tableau 14.

Tableau 14 – Connexions au module d'E/S

Connexion	Description
Directe	Une connexion directe est une liaison de transfert de données en temps réel entre l'automate et un module d'E/S. L'automate maintient et surveille la connexion. Toute coupure de cette connexion, en cas de défaut du module par exemple, entraîne l'activation par l'automate des bits de défaut dans la zone de données associée au module. Généralement, les modules des E/S analogiques, les modules des E/S de diagnostic et les modules spécialisés nécessitent des connexions directes.
Native pour rack	Vous pouvez choisir une communication native pour rack pour les modules des E/S TOR. Cette option est utilisée avec des modules des E/S distribuées. Le choix de la connexion native pour rack est réalisé lors de la configuration de l'adaptateur décentralisé. Par exemple, si vous souhaitez utiliser une connexion native pour rack avec des modules des E/S TOR appartenant à un système POINT I/O 1734 décentralisé, vous devez configurer le module 1734-AENT(R) de façon à ce qu'il utilise ce type de connexion. Une connexion native pour rack regroupe les composants de connexion entre l'automate et l'ensemble des modules des E/S TOR dans un châssis externe ou sur un même rail DIN. Plutôt que d'utiliser des connexions individuelles directes pour chaque module d'E/S, on n'utilise plus alors qu'une seule connexion pour l'ensemble du rack (ou rail DIN).

Configuration des modules des E/S distribuées standard en réseau EtherNet/IP

Votre système de commande Compact GuardLogix 5370 peut utiliser des modules des E/S distribuées en réseau EtherNet/IP.

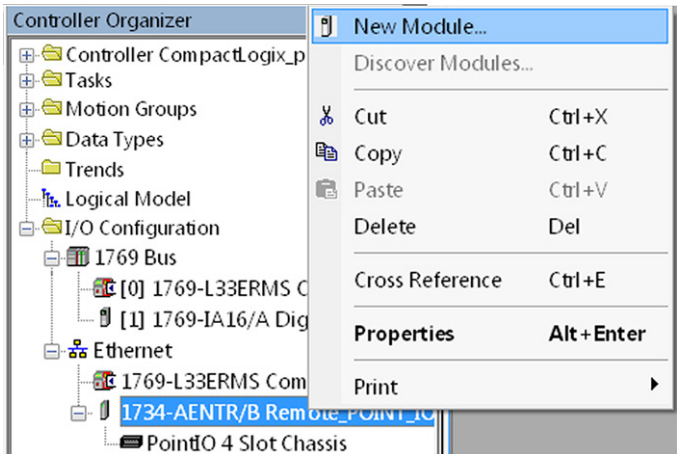
IMPORTANT Lors de l'ajout de modules des E/S distribuées, n'oubliez pas que c'est l'adaptateur Ethernet décentralisé qui doit être pris en compte pour le calcul du nombre maximum de stations EtherNet/IP admises pour votre automate.

Les modules des E/S décentralisées raccordés à l'automate par l'intermédiaire de cet adaptateur Ethernet décentralisé ne doivent pas être comptés.

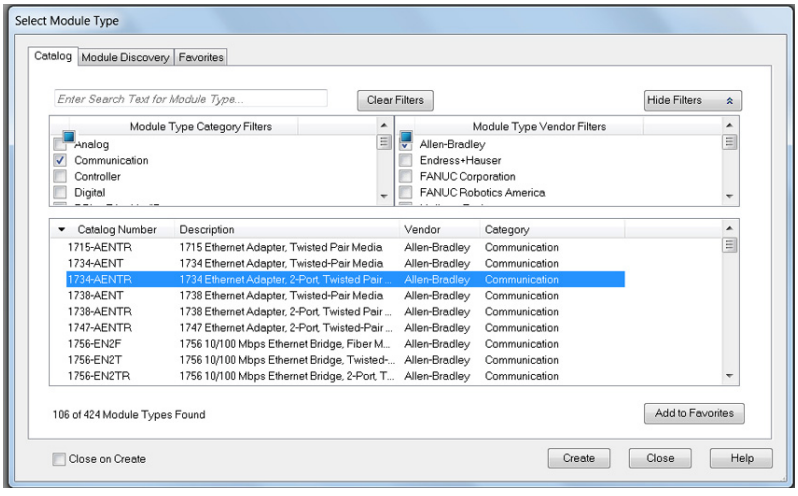
Pour de plus amples informations sur le nombre maximum de stations admissible, voir Stations d'un réseau EtherNet/IP, page 71.

Suivez les étapes ci-dessous pour configurer des modules des E/S distribuées en réseau EtherNet/IP.

1. Dans la fenêtre d'organisation de l'automate, sélectionnez 1734-AENT sous Ethernet, et faites un clic droit ; choisissez New Module (Nouveau module).

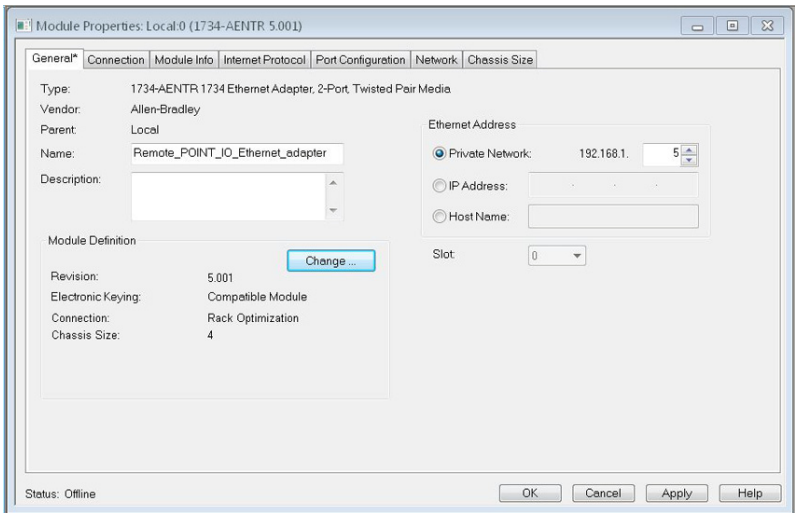


2. Sélectionnez l'adaptateur Ethernet désiré et cliquez sur Create (Créer).

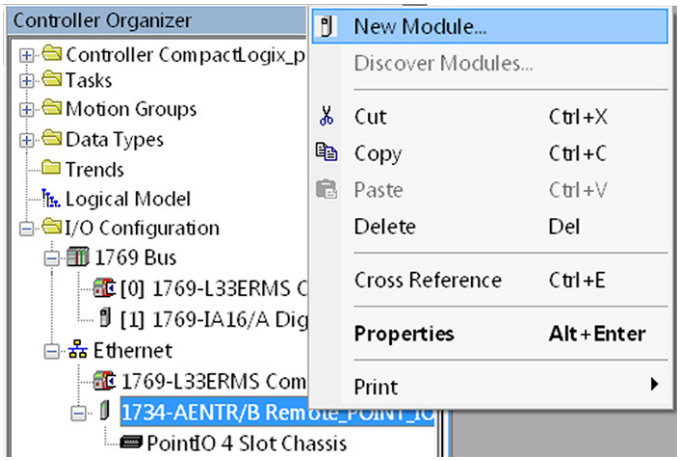


La boîte de dialogue New Module (Nouveau module) apparaît.

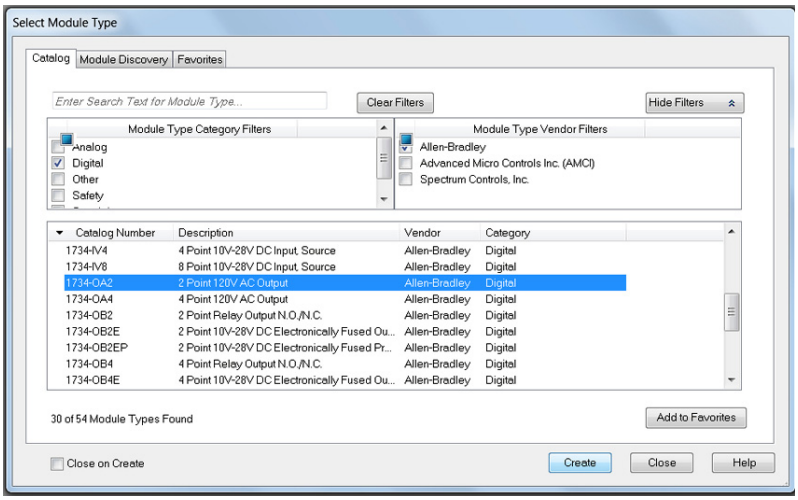
3. Configurez le nouvel adaptateur Ethernet comme souhaité et cliquez sur OK.



4. Dans la fenêtre d'organisation de l'automate, sélectionnez le nouvel adaptateur et faites un clic droit puis choisissez New Module (Nouveau module).

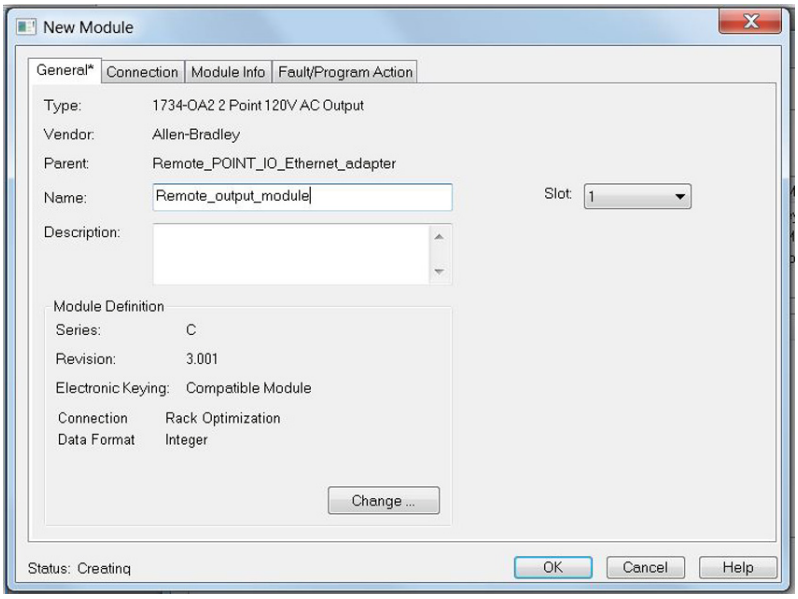


5. Sélectionnez le module d'E/S désiré et cliquez sur Create (Créer).



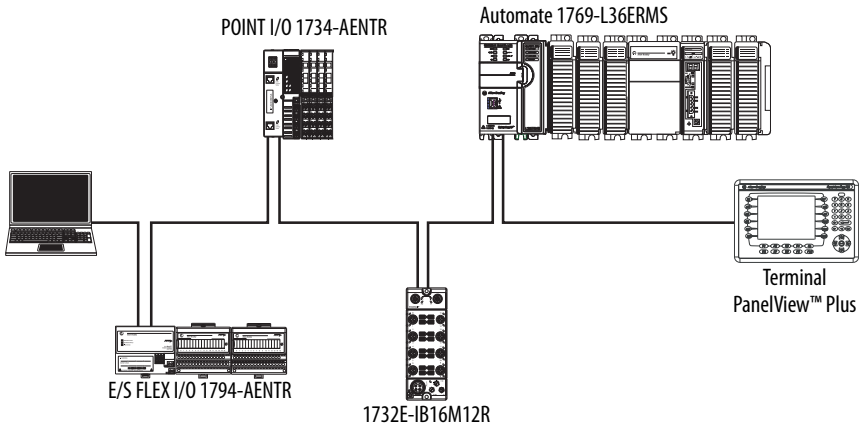
La boîte de dialogue New Module (Nouveau module) apparaît.

6. Configurez le nouveau module d'E/S comme souhaité et cliquez sur OK.



7. Répétez ces étapes pour ajouter les modules des E/S distribuées nécessaires au projet.

La figure suivante présente un exemple de système de commande 1769-L36ERMS utilisant des modules des E/S distribuées en réseau EtherNet/IP.



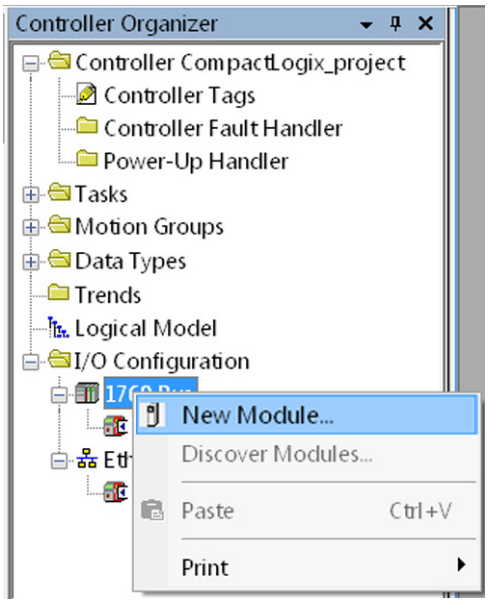
Configuration de modules des E/S distribuées standard en réseau DeviceNet

Votre système de commande Compact GuardLogix 5370 peut utiliser des modules des E/S distribuées standard en réseau DeviceNet.

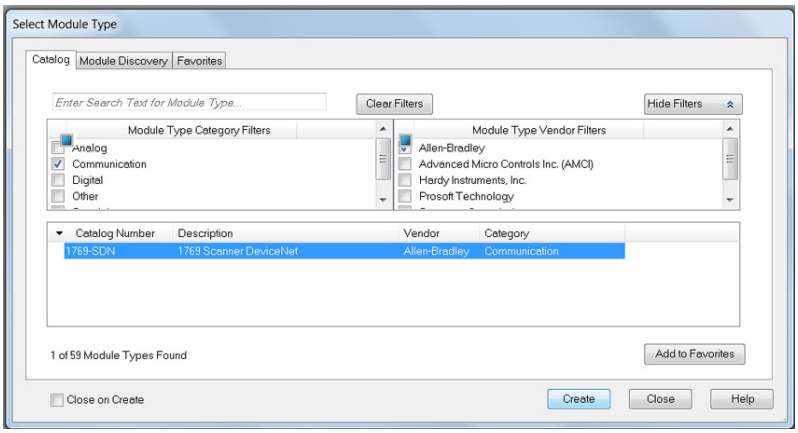
Suivez les étapes ci-dessous pour configurer des modules des E/S distribuées standard en réseau DeviceNet.

1. Si cela n'est pas déjà fait, installez un module scrutateur DeviceNet Compact I/O 1769-SDN dans la rangée locale de votre système de commande Compact GuardLogix 5370.

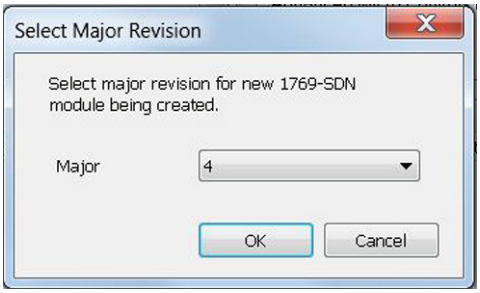
2. Dans la fenêtre d'organisation de l'automate, sélectionnez 1769 Bus sous la configuration des E/S (I/O Configuration) et faites un clic droit ; choisissez New Module (Nouveau module).



3. Sélectionnez le module scrutateur 1769-SDN et cliquez sur Create (Créer).

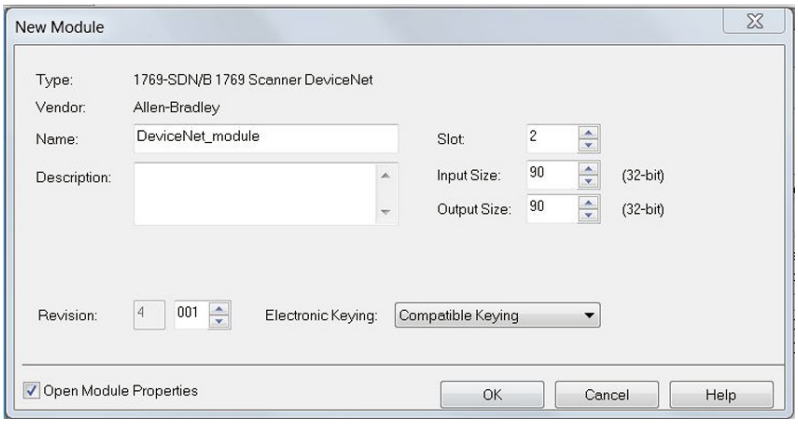


4. Choisissez un numéro de version majeure (Major Revision) et cliquez sur OK.



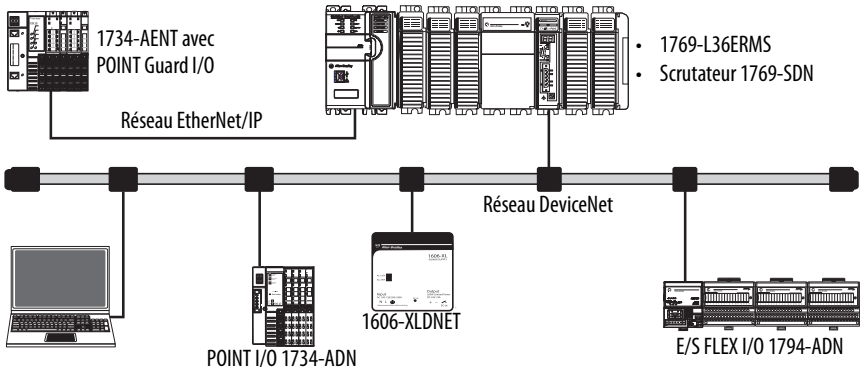
La boîte de dialogue New Module (Nouveau module) apparaît.

5. Configurez le nouveau module scrutateur 1769-SDN comme souhaité et cliquez sur OK.



6. Utilisez le logiciel RSNetWorx ™for DeviceNet pour définir la liste de scrutation du scrutateur 1769-SDN. Cette liste sera utilisée pour la transmission des données entre les dispositifs et l'automate par l'intermédiaire du scrutateur.

La figure suivante présente un exemple de système de commande 1769-L36ERMS utilisant des modules des E/S distribuées standard en réseau DeviceNet.

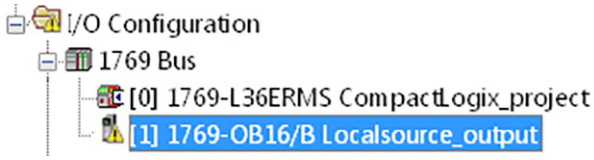


Surveillance des modules des E/S

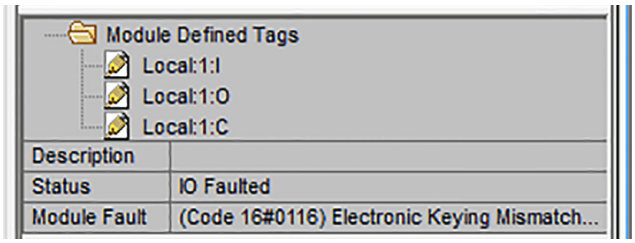
Les automates Compact GuardLogix 5370 permettent de surveiller les modules des E/S par les moyens suivants :

- Volet d'aperçu QuickView™ au-dessous de la fenêtre d'organisation de l'automate
- Onglet Connection (connexion) de la boîte de dialogue Module Properties (propriétés du module)
- Programmation de la logique pour surveiller les données de défaut afin de prendre les mesures appropriées.

Lorsqu'un défaut survient sur un module d'E/S, un triangle jaune s'affichant sur la représentation du module dans la fenêtre d'organisation de l'automate vous avertit à propos de ce défaut.

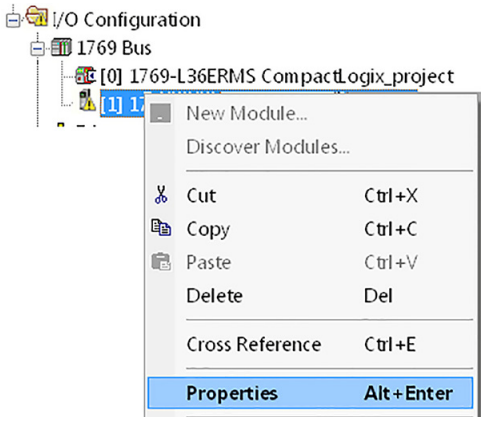


La figure ci-dessous illustre le volet d'aperçu Quick View, qui indique le type de défaut.



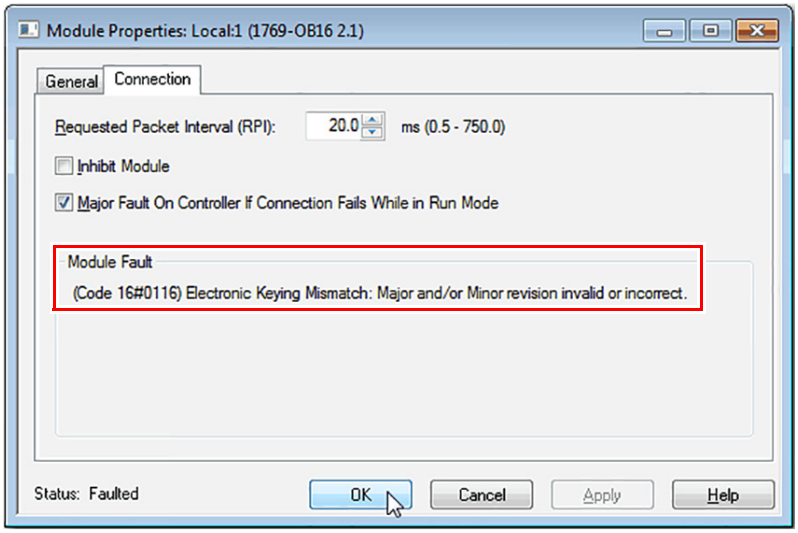
Pour voir la description du défaut dans l'onglet Connection (Connexion) de la boîte de dialogue Module Properties (Propriétés du module), suivez les étapes ci-dessous.

1. Dans la fenêtre d'organisation de l'automate, sélectionnez le module d'E/S en défaut sous la configuration des E/S (I/O Configuration) et faites un clic droit ; choisissez Properties (Propriétés).



2. Dans la boîte de dialogue Module Properties (Propriétés du module), cliquez sur l'onglet Connection (Connexion).

   Dans la section Module Fault (Défaut du module), utilisez la description du défaut pour diagnostiquer le problème.



3. Cliquez sur OK pour refermer la boîte de dialogue et remédier au problème.

Détection du cache de terminaison et défauts du module

La détection du cache de terminaison se fait par l'intermédiaire du dernier module raccordé au bus 1769. Si ce module présente un défaut qui l'empêche de communiquer sur le bus 1769, les événements suivants vont se produire :

- la détection du cache de terminaison échouera ;
- défauts de l'automate

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

Ajout de dispositifs d'E/S de sécurité

Pour tout ajout de dispositif d'E/S de sécurité au système, vous devez définir une configuration pour ce dispositif, notamment ce qui suit :

- L'adresse IP dans le cas d'un réseau EtherNet/IP

  Pour définir l'adresse IP, vous pouvez utiliser les sélecteurs rotatifs du dispositif, le logiciel DHCP (disponible auprès de Rockwell Automation), l'application Logix Designer ou récupérer l'adresse par défaut enregistrée en mémoire non volatile.
- Le numéro de réseau de sécurité (SNN) ; voir page 106 pour de plus amples informations sur le réglage du numéro SNN
- La signature de configuration, voir page 110 pour vérifier dans quels cas la signature de configuration est définie automatiquement ou doit l'être manuellement.
- La limite du temps de réponse, voir page 107 pour de plus amples informations sur la configuration de la limite de temps de réponse.
- Les paramètres d'entrée, de sortie et de test de sécurité terminent la configuration du module

Vous pouvez configurer les dispositifs d'E/S de sécurité via l'automate Compact GuardLogix®, à l'aide de l'application Logix Designer.

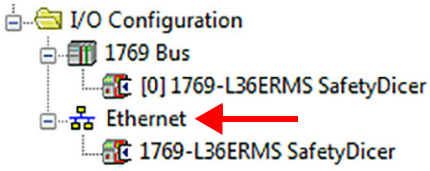
CONSEIL Les dispositifs d'E/S de sécurité prennent en charge les données standard et de sécurité. La configuration du dispositif définit les types de données disponibles.

Configuration des dispositifs d'E/S de sécurité

Ajoutez le dispositif d'E/S de sécurité au module de communication dans le dossier I/O Configuration du projet automate.

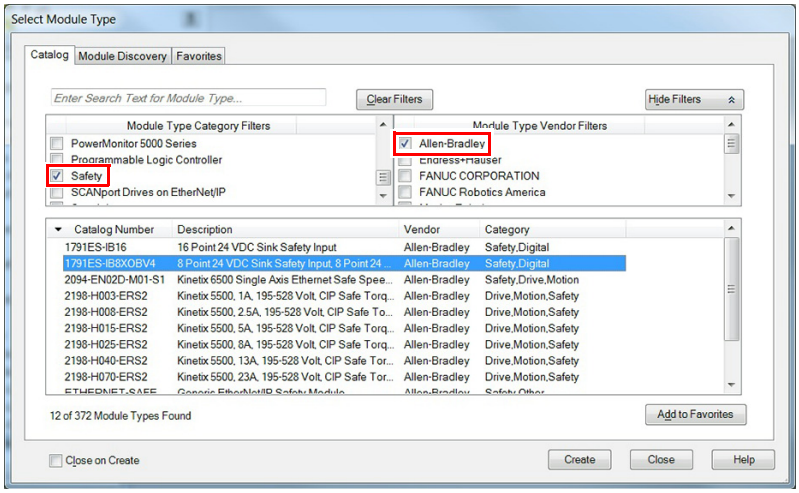
CONSEIL Vous ne pouvez ni ajouter, ni supprimer, un dispositif d'E/S de sécurité lorsque vous êtes en ligne.

1. Cliquez avec le bouton droit de la souris sur le réseau Ethernet et sélectionnez New Module (Nouveau module).

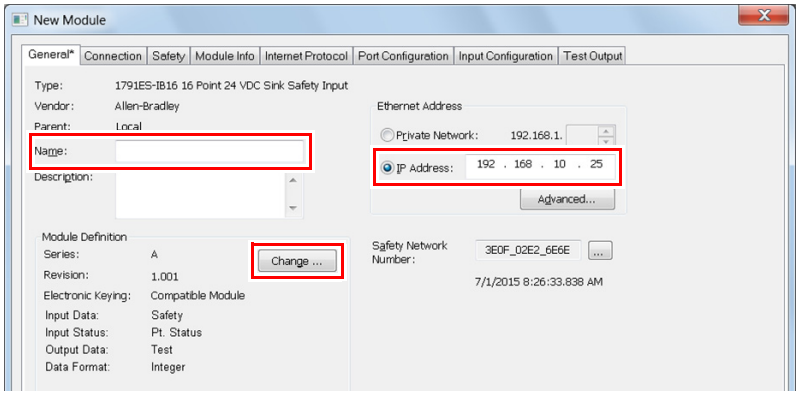


2. Sous l'onglet Catalog, sélectionnez le dispositif d'E/S de sécurité.

CONSEIL Utilisez les filtres pour réduire la liste de choix de modules.



3. Cliquez sur Create (Créer).
4. Saisissez un nom pour le nouveau dispositif.
5. S'il y a lieu, modifiez les paramètres de définition du module en cliquant sur le bouton Change (Modification).
6. L'adresse IP dans le cas d'un réseau EtherNet/IP.



Si votre réseau utilise la traduction d'adresse réseau (NAT), voir Définition de l'adresse IP par la traduction d'adresses réseau (NAT), page 105.

7. Pour modifier le numéro de réseau de sécurité, cliquez sur le bouton ... (si nécessaire).

   Voir page 106 pour plus de détails.

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

   Voir page 107 pour plus de détails.

9. Pour terminer la configuration du dispositif d'E/S de sécurité, reportez-vous à sa documentation d'utilisation et à l'aide en ligne de l'application Logix Designer.

Définition de l'adresse IP par la traduction d'adresses réseau (NAT)

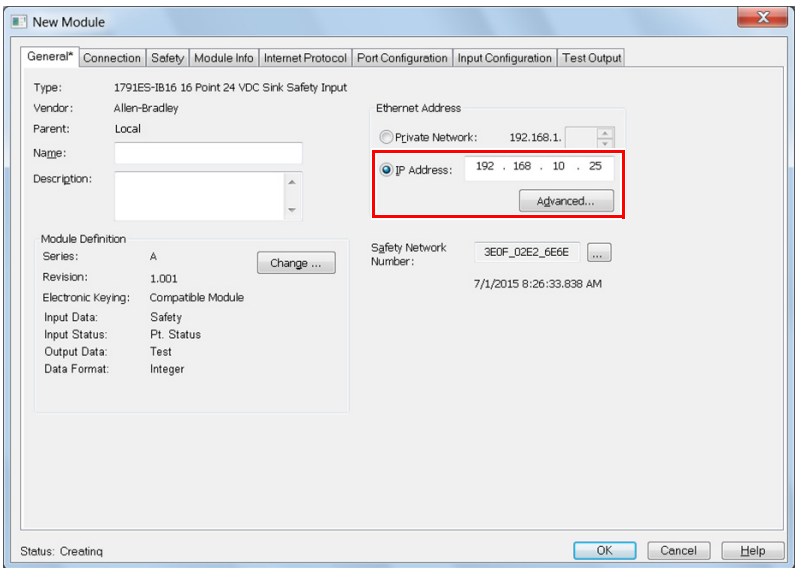
La fonction NAT traduit une adresse IP en une autre adresse IP par le biais d'un routeur ou d'un switch configuré pour la fonction NAT. Le routeur ou le switch traduit les adresses sources et les adresses de destination au sein des paquets de données à mesure que le trafic circule entre les sous-réseaux.

Ce service est utile si vous devez réutiliser des adresses IP sur l'ensemble d'un réseau. Par exemple, la fonction NAT permet de segmenter des dispositifs en plusieurs sous-réseaux privés identiques tout en conservant des identités uniques sur le sous-réseau public.

Si vous utilisez la fonction NAT, suivez la procédure ci-après pour configurer l'adresse IP.

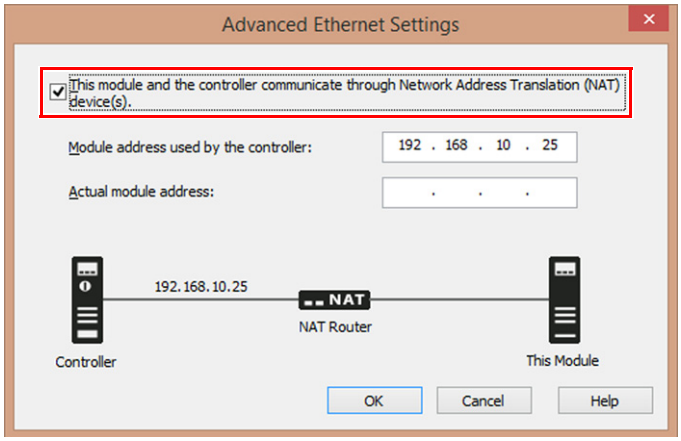
1. Dans le champ IP Address, saisissez l'adresse IP qui sera utilisée par l'automate.

   Il s'agit généralement de l'adresse IP sur le réseau public lors de l'utilisation de la fonction NAT.



2. Cliquez sur Advanced (Avancé) pour ouvrir la boîte de dialogue Advanced Ethernet Settings (Réglages Ethernet avancés).

3. Cochez la case pour indiquer que ce module et l'automate communiquent par le biais de dispositifs NAT.



4. Saisissez l'adresse effective du module.

   CONSEIL Si vous avez configuré l'adresse IP à l'aide des sélecteurs rotatifs, utilisez cette adresse sur le dispositif. L'adresse effective du module correspond également à l'adresse indiquée dans l'onglet Internet Protocol du dispositif.

5. Cliquez sur OK.

L'automate utilise l'adresse traduite, mais le protocole de sécurité CIP nécessite l'adresse réelle du dispositif.

Définition du numéro de réseau de sécurité (SNN)

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

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

Voir Attribution du numéro de réseau de sécurité (SNN), page 65.

Utilisation des connexions unicast sur les réseaux EtherNet/IP

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 la case Use Unicast Connection over EtherNet/IP (Utiliser la connexion d'envoi individuel sur EtherNet/IP).

Définition de la limite de temps de réponse de la connexion

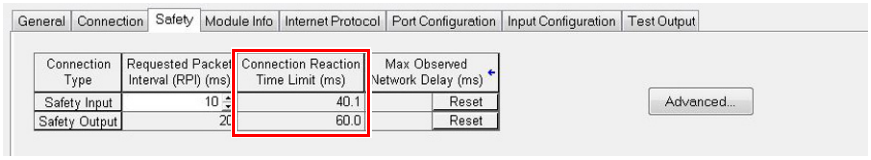
La valeur Connection Reaction Time Limit (Limite de temps de réponse de la connexion) correspond à l'âge maximal des trames de sécurité sur la connexion associée. Si l'âge des données utilisées par l'équipement consommateur dépasse la limite de temps de réponse de la connexion, un défaut de connexion 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 =
Valeur RPI des entrées x [Multiplicateur de timeout + Multiplicateur de délai réseau]

Limite de temps de réponse de la connexion en sortie =
Période de la tâche de sécurité x [Multiplicateur de timeout + Multiplicateur de délai 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 16 – Limite de temps de réponse de la connexion



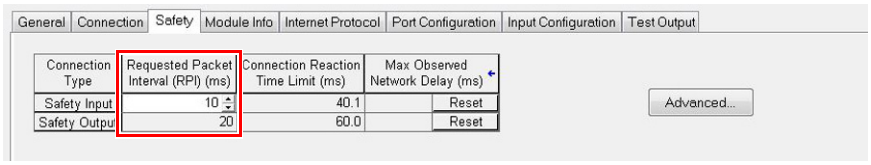
Définition de l'intervalle entre trames requis (RPI)

Le RPI spécifie la période de mise à jour 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 par défaut est de 10 ms.

La limite de temps de réponse de la connexion est immédiatement ajustée en cas de modification du RPI via l'application Logix Designer.

Figure 17 – intervalle entre trames requis



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

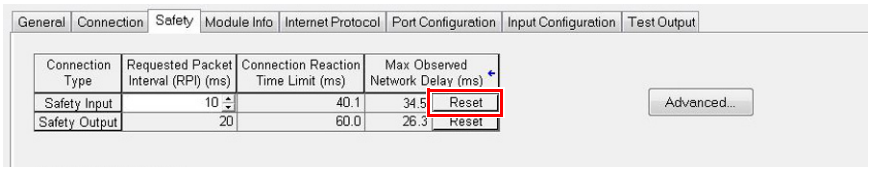
Pour de plus amples informations sur la période de la tâche de sécurité, voir Spécification de la période de la tâche de sécurité, page 140.

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 à la page 108.

Affichage du délai réseau maximum observé

Lorsque l'automate reçoit une trame de sécurité, le logiciel enregistre le délai de transmission maximum observé sur le réseau. Pour les entrées de sécurité, Maximum Observed Network Delay (Délai réseau maximum observé) indique le temps total nécessaire pour la transmission d'un paquet de données depuis le 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 réinitialiser Maximum Observed Network Delay (Délai réseau maximum observé) en cliquant sur Reset (Réinitialisation).

Figure 18 – Réinitialisation du délai réseau maximum observé

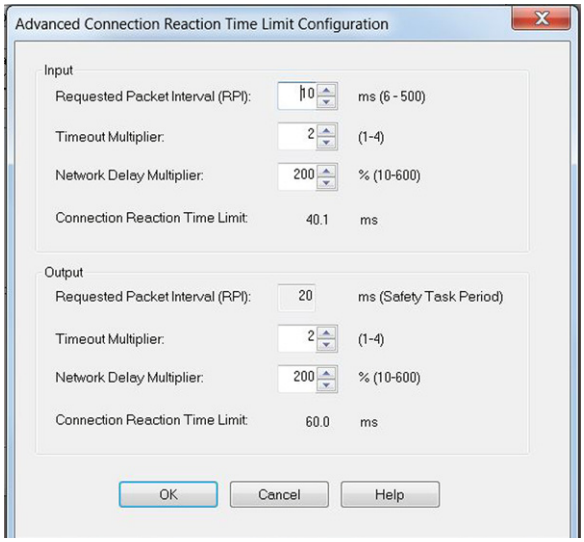


IMPORTANT La valeur réelle de Maximum Network Delay (Délai réseau maximum) du producteur au consommateur est inférieure à la valeur affichée dans le champ Maximum Network Delay (Délai réseau maximum) de l'onglet Safety (Sécurité). En général, le délai maximum réel de transmission d'un message est égal à environ la moitié de la valeur de Maximum Network Delay (Délai réseau maximum).

Configuration des paramètres de limite de temps de réponse avancé de la connexion

Configurez les paramètres de connexion, tels que le multiplicateur de timeout et le multiplicateur de délai du réseau dans la boîte de dialogue Advanced Connection Reaction Time Limit (Limite de temps de réponse avancée de la connexion).

Figure 19 – Configuration avancée



Multiplicateur de timeout

Le multiplicateur de timeout définit le nombre de RPI pendant lesquels il est possible d'attendre une trame avant qu'un timeout de connexion ne soit déclaré. 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'au moins un message est reçu dans un intervalle équivalent à 2 fois la valeur RPI (2 x RPI).

Multiplicateur de délai réseau

Le multiplicateur de délai réseau définit le temps d'acheminement d'un message imposé par le 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 le cas où le temps imposé pour l'acheminement des messages est notablement inférieur ou supérieur au 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.

Méthode 1 : utilisez le 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 %

Méthode 2 : utilisez le 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] ÷ 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 multiplicateur de délai réseau sera alors égal à :
[20 + 10] ÷ 50 = 60 %

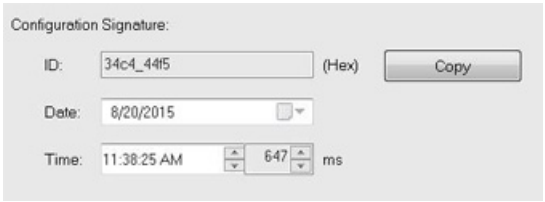
Utilité de la signature de configuration

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 l'application Logix Designer

Quand un dispositif d'E/S est configuré à l'aide de l'application Logix Designer, sa signature de configuration est créée automatiquement. Vous pouvez visualiser et copier cette signature de configuration à l'aide de l'onglet Safety (Sécurité) de la boîte de dialogue Module Properties (Propriétés du module).

Figure 20 – Affichage et copie de la signature de configuration



Propriétaire de configuration différent (connexion en écoute seule)

Lorsque la configuration d'un dispositif d'E/S appartient à un automate différent, vous devez copier la signature de configuration de ce module à partir du 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 dispositif est uniquement configuré pour des entrées, vous pouvez copier et coller la signature de configuration. Si le dispositif 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 est indisponible.

Réinitialisation de la propriété des dispositifs d'E/S de sécurité

Lorsque le projet automate 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 » apparaît. Lorsqu'un second dispositif est propriétaire de la configuration, « Remote » s'affiche, ainsi que le numéro de réseau de sécurité (SNN) et l'adresse de station ou le numéro d'emplacement du propriétaire de la configuration. Le message « Communication error » s'affiche en cas d'échec de la lecture du dispositif.

En ligne, cliquez sur Reset Ownership (Réinitialiser la propriété) pour rétablir la configuration d'origine du dispositif.

CONSEIL Vous ne pouvez pas réinitialiser le droit de propriété lorsqu'il y a des modifications des propriétés du module en attente, lorsqu'une signature de tâche de sécurité existe ou lorsque la sécurité est verrouillée.

Adressage des données E/S de sécurité

Lorsque vous ajoutez un dispositif au dossier de configuration des E/S, l'application Logix Designer crée automatiquement des points d'accès automate pour le dispositif.

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

Format d'adresse des modules des E/S de sécurité

L'adresse d'un module d'E/S de sécurité est similaire à l'exemple suivant.

EXEMPLE Nomdumodule:Type.Membre

Tableau 15 – Format d'adresse d'un dispositif d'E/S de sécurité

Adresse	Signification	
Nomdumodule	Le nom du dispositif d'E/S de sécurité	
Type	Type de donnée	Entrée : I Sortie : O
Membre	Données spécifiques au dispositif d'E/S	
	Module d'entrée uniquement	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

Format d'adresse d'un variateur Kinetix 5500, Kinetix 5700 et PowerFlex 527

L'adresse d'un variateur Kinetix® 5500, Kinetix 5700 et PowerFlex® 527 suit l'exemple ci-après.

EXEMPLE Nomduvariateur:Type.Membre

Tableau 16 – Format d'adresse d'un dispositif d'E/S de sécurité de variateur

Adresse	Signification	
Nomduvariateur	Le nom du variateur Kinetix ou PowerFlex	
Type	Type de donnée	Entrée : SI Sortie : SO
Membre	Données spécifiques au dispositif d'E/S	
	Module d'entrée uniquement	Nomduvariateur:SI.ConnectionStatus Nomduvariateur:SI.RunMode Nomduvariateur:SI.ConnectionFaulted Nomduvariateur:SI.Status Nomduvariateur:SI.TorqueDisabled Nomduvariateur:SI.SafetyFault Nomduvariateur:SI.ResetRequired
	Module de sortie uniquement	Nomduvariateur:SO.Command Nomduvariateur:SO.SafeTorqueOff Nomduvariateur:SO.Reset

Tableau 17 – Autres ressources

Documentation	Description
Chapitre 9, Développement d'applications de sécurité	Contient des informations sur le contrôle des points de données de sécurité
Logix5000 Controllers I/O and Tag Data Programming Manual », publication 1756-PM004	Fournit des informations sur l'adressage des dispositifs d'E/S standard

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

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

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

- Guard I/O™ EtherNet/IP Modules User Manual », publication 1791ES-UM001
- POINT Guard I/O™ Safety Modules Installation and User Manual », publication 1734-UM013
- Kinetix 5500 Servo Drives User Manual », publication 2198-UM001
- Kinetix 5700 Servo Drives User Manual », publication 2198-UM002
- PowerFlex 527 Adjustable Frequency AC Drive User Manual », publication 520-UM002

Réinitialisation d'un dispositif d'E/S de sécurité en condition d'origine

Si un module d'E/S de sécurité 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 projet automate 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 » apparaît. Lorsqu'un second dispositif est propriétaire de la configuration, « Remote » s'affiche, ainsi que le numéro de réseau de sécurité (SNN) et l'adresse de station ou le numéro d'emplacement du propriétaire de la configuration. Communication error » 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. Dans la fenêtre d'organisation de l'automate, cliquez sur le dispositif concerné avec le bouton droit de la souris et sélectionnez Properties (Propriétés).
2. Cliquez sur l'onglet Connection.
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. Dans la fenêtre d'organisation de l'automate, cliquez sur le dispositif concerné avec le bouton droit de la souris et sélectionnez Properties (Propriétés).
2. Cliquez sur l'onglet Safety (Sécurité).
3. Cliquez sur Reset Ownership (Réinitialiser la propriété).

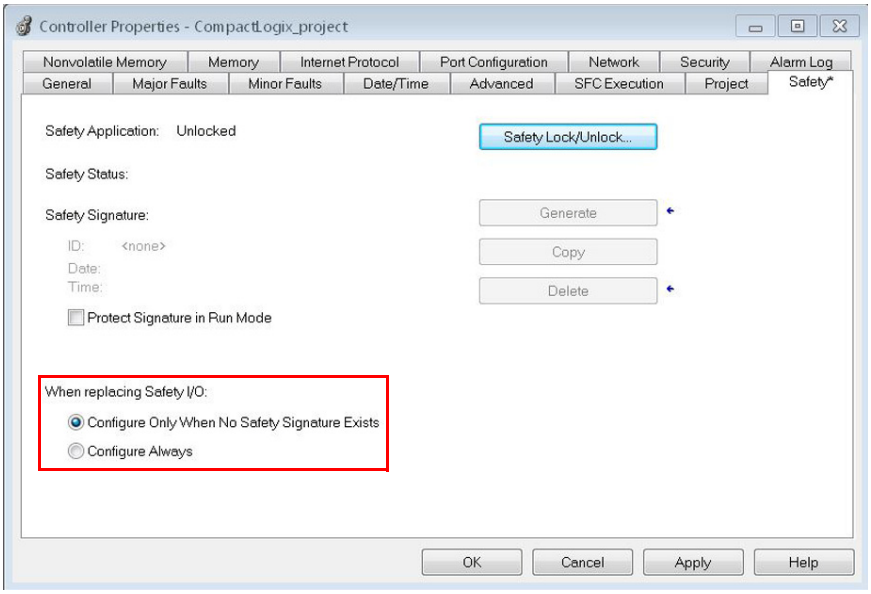
Remplacement d'un dispositif d'E/S de sécurité

Vous pouvez utiliser l'application Logix Designer pour remplacer un dispositif d'E/S de sécurité sur un réseau Ethernet. Si vous avez besoin de maintenir le niveau de sécurité SIL 3 dans tout ou partie du système CIP Safety pendant le remplacement et le test fonctionnel d'un dispositif, il est impossible d'utiliser la fonction Configure Always (Toujours configurer). Allez à Remplacement avec la fonctionnalité « Configure Only When No Safety Signature Exists » activée, page 114.

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 dispositif, la fonctionnalité Configure Always (Toujours configurer) peut être utilisée. Allez à Remplacement avec « Configure Always » activé, page 118.

Le remplacement du dispositif d'E/S de sécurité est configuré sous l'onglet Safety (Sécurité) de l'automate Compact GuardLogix.

Figure 21 – Remplacement de dispositif d'E/S de sécurité



Remplacement avec la fonctionnalité « Configure Only When No Safety Signature Exists » activée

Lors du remplacement d'un dispositif d'E/S de sécurité, la configuration est téléchargée à partir de l'automate de sécurité si le DeviceID du nouveau dispositif correspond à l'original. 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.

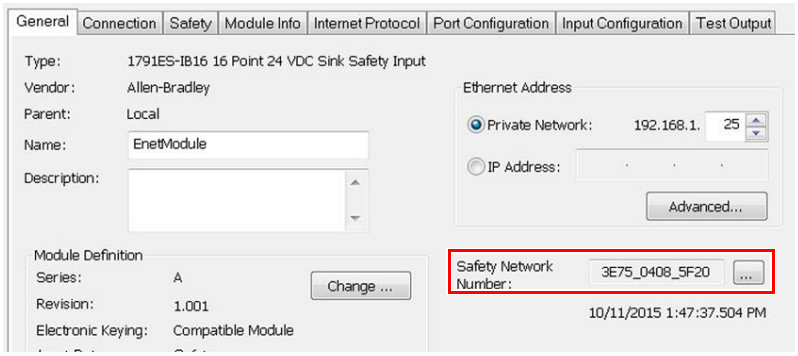
Si le projet est configuré selon « Configure Only When No Safety Signature Exists », suivez les étapes appropriées du Tableau 18 pour remplacer un dispositif d'E/S de sécurité en fonction de votre scénario. Après avoir effectué les étapes correctement, le DeviceID correspond à l'original, ce qui permet à l'automate de sécurité de télécharger la configuration de dispositif correcte et de rétablir la connexion de sécurité.

Tableau 18 – Remplacement d'un module

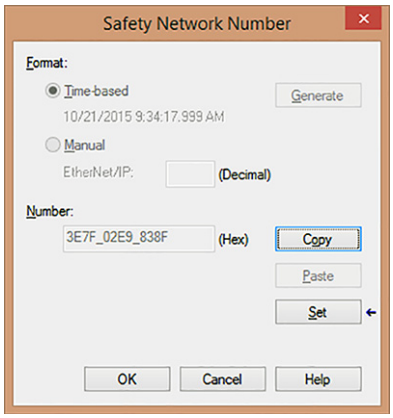
La signature de sécurité Compact GuardLogix existe	Condition du module de remplacement	Action requise
Non	Pas de SNN (matériel neuf)	Aucune Le dispositif est prêt à l'emploi.
Oui ou Non	Même SNN que dans la configuration de la tâche de sécurité originale	Aucune Le dispositif est prêt à l'emploi.
Oui	Pas de SNN (matériel neuf)	Voir Scénario 1 – Le dispositif de remplacement est dans sa condition d'origine et la signature de sécurité existe, page 115.
Oui	SNN différent de la configuration de la tâche de sécurité originale	Voir Scénario 2 – Le SNN du dispositif de remplacement est différent de l'original et une signature de sécurité existe, page 116.
Non		Voir Scénario 3 – Le SNN du dispositif de remplacement est différent de l'original et aucune signature de sécurité n'existe, page 118.

Scénario 1 – Le dispositif de remplacement est dans sa condition d'origine et la signature de sécurité existe

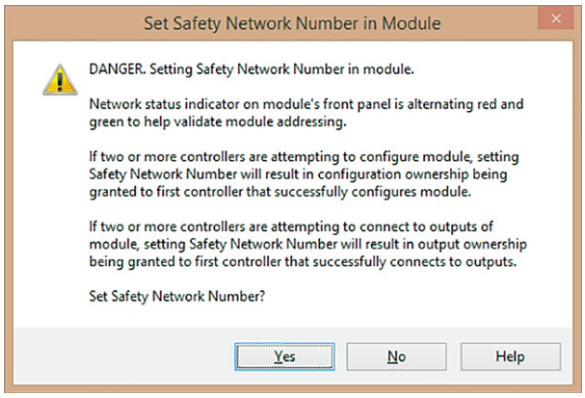
1. Démontez l'ancien dispositif d'E/S et installez le nouveau.
2. Cliquez avec le bouton droit de la souris sur le dispositif d'E/S de sécurité de remplacement et choisissez Properties (Propriétés).
3. Cliquez sur le bouton ... situé à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue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



4. Cliquez sur Set (Définir).



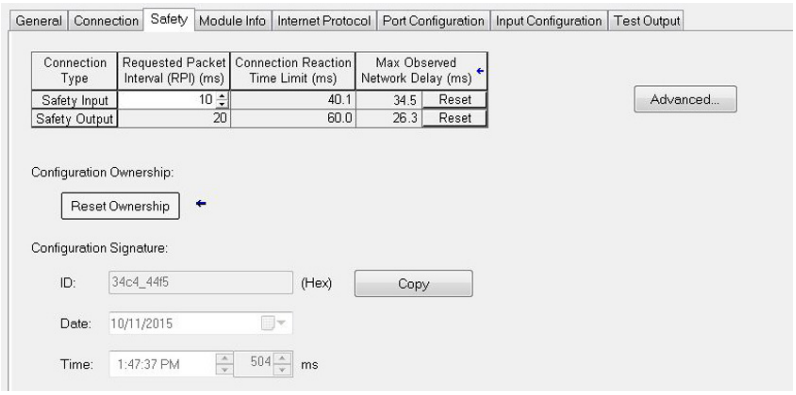
5. Vérifiez que le voyant d'état du réseau (NS) clignote alternativement en vert/rouge sur le dispositif correct avant de cliquer sur Yes (Oui) dans la boîte de dialogue de confirmation pour définir le SNN et accepter le dispositif de remplacement.



6. Suivez les procédures prescrites par votre entreprise pour réaliser les tests fonctionnels du nouveau dispositif d'E/S et du système et revalider le système.

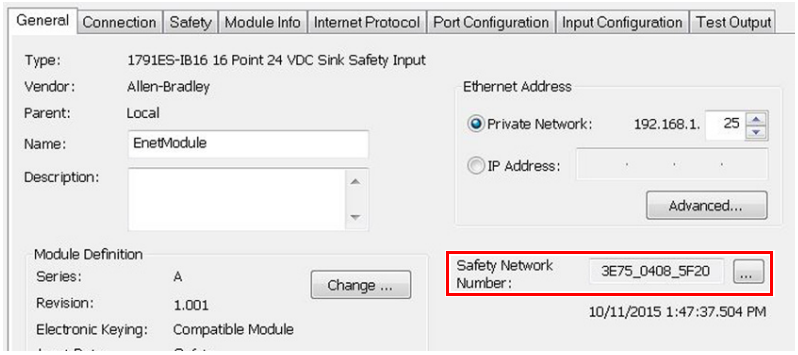
Scénario 2 – Le SNN du dispositif de remplacement est différent de l'original et une signature de sécurité existe

1. Démontez l'ancien dispositif d'E/S et installez le nouveau.
2. Cliquez avec le bouton droit de la souris sur le dispositif d'E/S de sécurité et choisissez Properties (Propriétés).
3. Cliquez sur l'onglet Safety (Sécurité).

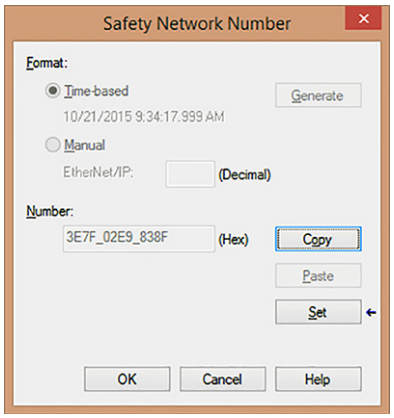


4. Cliquez sur Reset Ownership (Réinitialiser la propriété).
5. Cliquez sur OK.
6. Cliquez avec le bouton droit de la souris sur le dispositif et choisissez Properties (Propriétés).

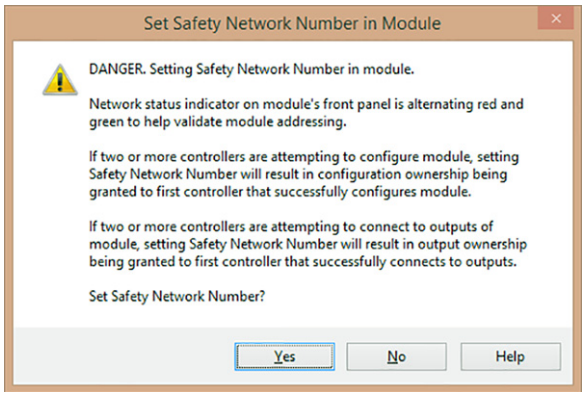
7. Cliquez sur le bouton [...] situé à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro de réseau de sécurité).



8. Cliquez sur Set (Définir).



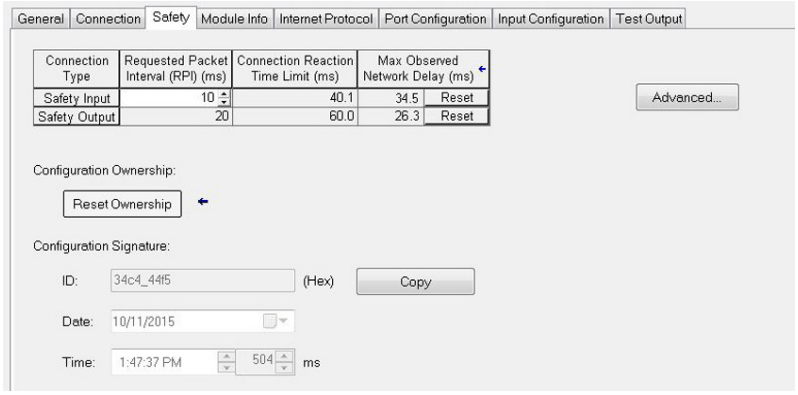
9. Vérifiez que le voyant d'état du réseau (NS) clignote alternativement en vert/rouge sur le dispositif correct avant de cliquer sur Yes (Oui) dans la boîte de dialogue de confirmation pour définir le SNN et accepter le dispositif de remplacement.



10. Suivez les procédures prescrites par votre entreprise pour réaliser les tests fonctionnels du nouveau dispositif d'E/S et du système et revalider le système.

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

1. Démontez l'ancien dispositif d'E/S et installez le nouveau.
2. Cliquez avec le bouton droit de la souris sur le dispositif d'E/S de sécurité 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 dispositif d'E/S et du système et revalider le système.

Remplacement avec « Configure Always » activé

ATTENTION : Activez la fonctionnalité « Configure Always » (Toujours configurer) uniquement si le système de commande CIP Safety complet n'est **pas** nécessaire pour maintenir le comportement SIL 3 pendant le remplacement et le test fonctionnel d'un dispositif.

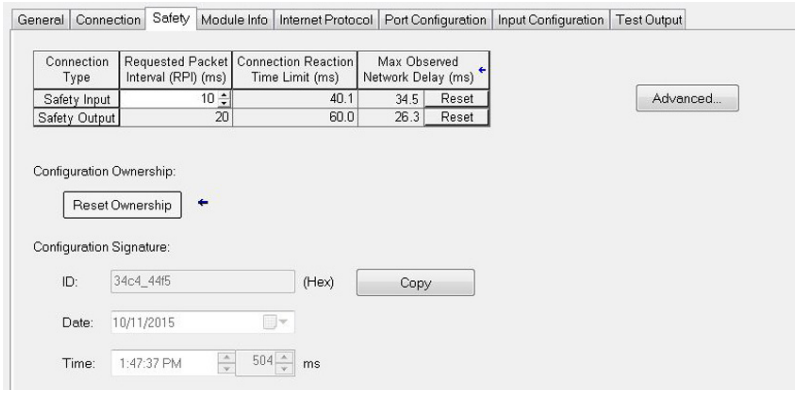
N'introduisez pas sur un réseau de sécurité CIP des dispositifs dans leur configuration d'origine lorsque la fonctionnalité Configure Always est activée, sauf en suivant cette procédure de remplacement.

Lorsque la fonctionnalité « Configure Always » est activée dans le projet automate, celui-ci recherche et se connecte automatiquement à un dispositif de remplacement qui répond à toutes les exigences suivantes :

- L'automate contient déjà des informations de configuration pour un dispositif de même type à cette adresse réseau.
- Le dispositif 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 dispositif d'E/S de sécurité.

1. Démontez l'ancien dispositif d'E/S et installez le nouveau.
   a. Si le dispositif est en condition d'origine, allez à l'étape 6. Aucune action n'est nécessaire pour l'acquisition de la propriété du dispositif par l'automate Compact GuardLogix.
   b. Si une erreur de discordance de SNN se produit, passez à l'étape suivante pour réinitialiser le dispositif en condition d'origine.
2. Cliquez avec le bouton droit de la souris sur le dispositif d'E/S de sécurité 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 dispositif d'E/S et du système et revalider le système.

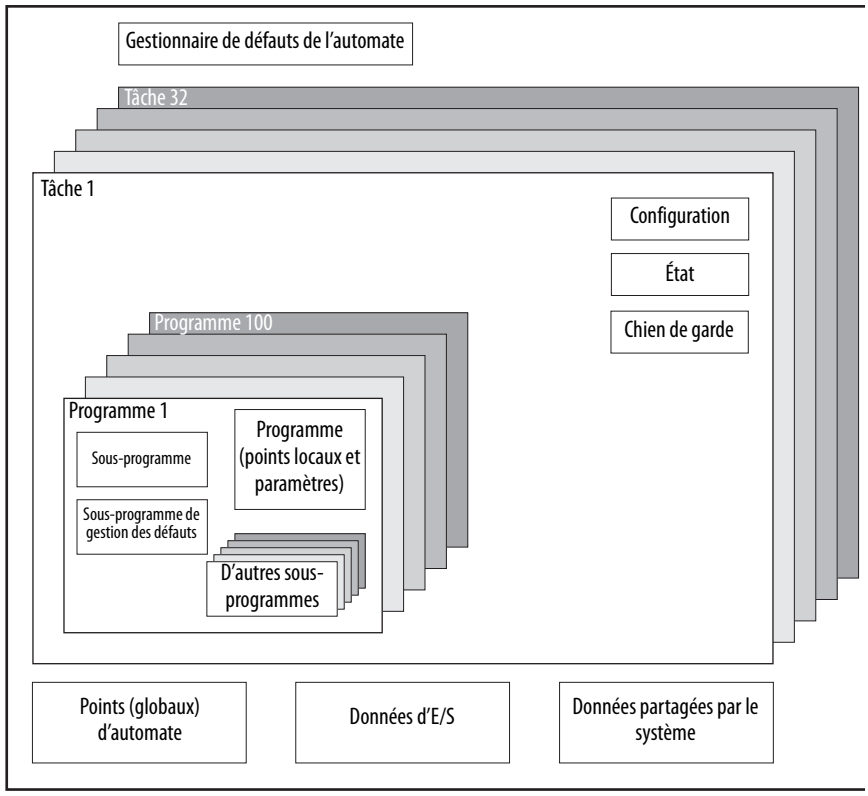
Notes :

Éléments d'une application de commande

Une application de commande est constituée de plusieurs éléments qui exigent une planification pour s'assurer de l'exécution efficace de l'application. Parmi les éléments d'application on peut citer les suivants :

- Tâches
- Programmes
- Sous-programmes
- Paramètres et points locaux

Figure 22 – Application de commande



Tâches

Un automate Logix5000™ vous permet d'utiliser un certain nombre de tâches pour planifier l'exécution et définir les priorités de vos programmes sur la base de critères particuliers. Ce fonctionnement multitâche permet de répartir le temps de traitement de l'automate entre les différentes opérations réalisées dans votre application :

- L'automate n'exécute qu'une tâche à la fois.
- Une tâche peut interrompre l'exécution d'une autre tâche et prendre le contrôle.
- Dans n'importe quelle tâche, plusieurs programmes peuvent être utilisés. Cependant, un seul programme est exécuté à la fois.
- Vous pouvez afficher les tâches dans la fenêtre d'organisation de l'automate ou la fenêtre d'organisation logique, selon le cas.

Figure 23 – Tâche d'une application de commande

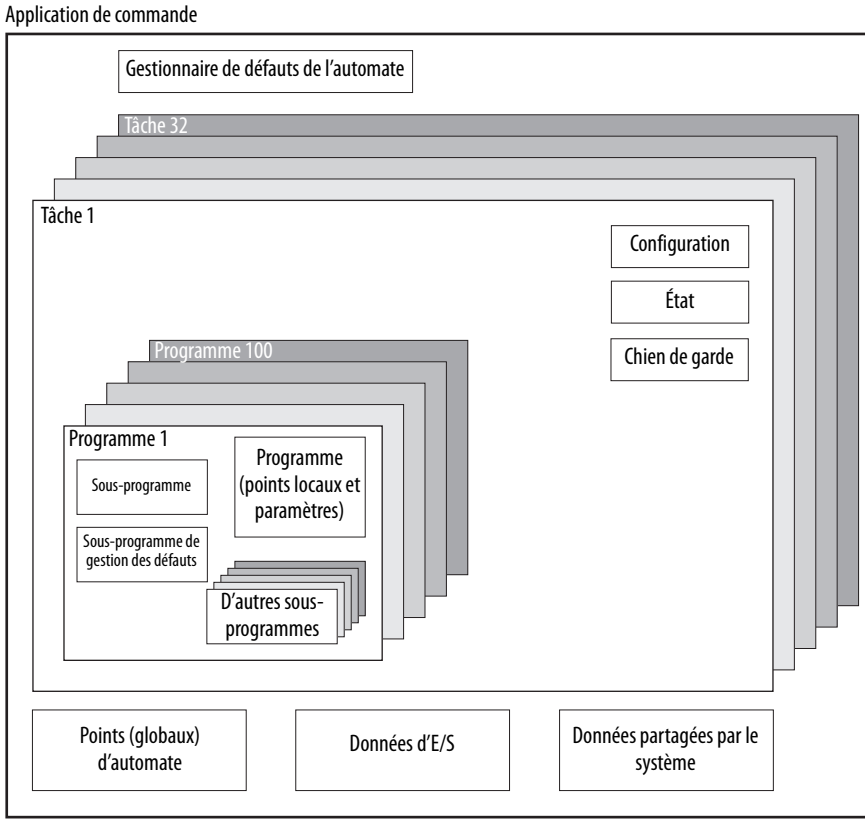
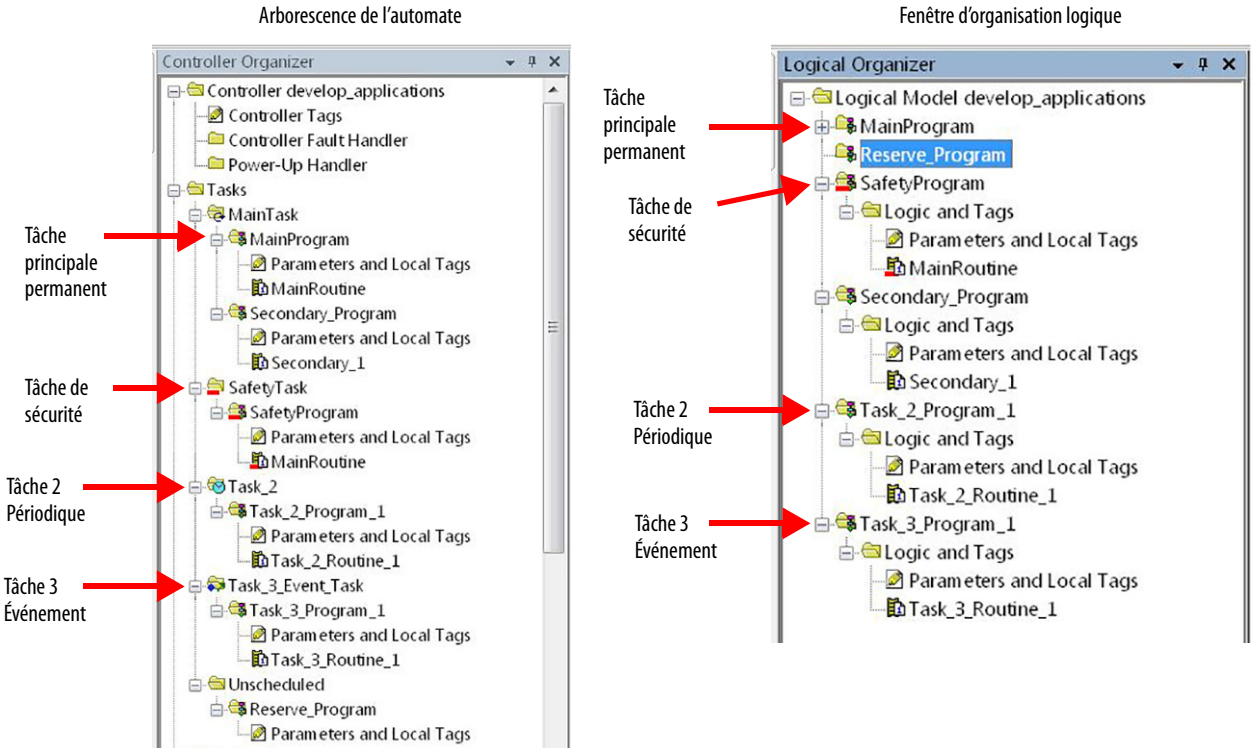
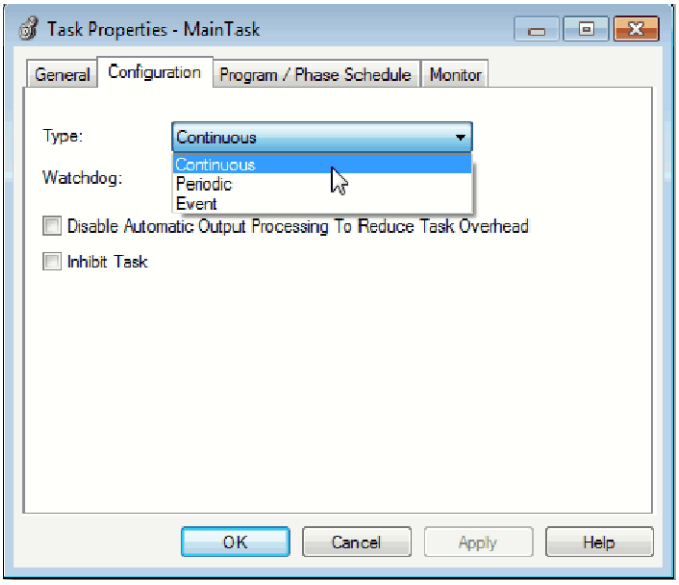


Figure 24 – Tâches d'une application



Une tâche fournit des informations de planification et de priorité pour un ou plusieurs programmes. La boîte de dialogue Task Properties (Propriétés de la tâche) permet de définir la tâche comme étant continue, périodique ou événementielle.

Figure 25 – Configuration du type de tâche



Ce tableau explique les types de tâches que vous pouvez configurer.

Tableau 19 – Types de tâche et fréquence d'exécution

Type de tâche	Exécution de la tâche	Description
Continu	En permanence	La tâche continue est exécutée en arrière-plan. Tout temps de traitement du processeur non alloué à d'autres opérations (telles que des commandes de mouvement, des communications et autres tâches) est utilisé pour l'exécution des programmes de la tâche continue : • La tâche continue est continuellement exécutée. Lorsqu'elle a terminé une scrutation complète, elle recommence immédiatement. • Un projet ne requiert pas de tâche continue. Le cas échéant, il ne peut y en avoir qu'une seule.
Périodique	• À un intervalle précis, tel que toutes les 100 ms • Plusieurs fois pendant la scrutation de votre autre programme logique	Une tâche périodique exécute une fonction à un intervalle donné : • Dès que le temps prévu pour la tâche périodique s'est écoulé, la tâche interrompt toute autre tâche de priorité inférieure, s'exécute une fois et revient à la ligne de commande à laquelle la tâche précédente avait été interrompue. • Vous pouvez définir l'intervalle de temps entre 0,1 et 2 000 000 ms. La valeur par défaut est de 10 ms. Cette valeur dépend également de l'automate et de la configuration. • La performance d'une tâche périodique dépend du type d'automate Logix5000 et du programme logique dans la tâche. • La tâche périodique traite les données d'E/S pour les automates CompactLogix™, FlexLogix™, DriveLogix™, et SoftLogix™ en tenant compte des points suivants : – Pour les automates CompactLogix, FlexLogix et DriveLogix, le niveau de priorité est de 6 – Pour les automates SoftLogix, la priorité est la priorité Windows, soit 16 (inactive) – Les tâches de priorité plus élevée sont prioritaires par rapport à la tâche d'E/S et peuvent influer sur le traitement – L'exécution se fait à l'intervalle RPI le plus rapide que vous avez programmé dans votre système – L'exécution se fait aussi longtemps qu'il faut pour scruter les modules des E/S configurés
Événement	Dès qu'un événement se produit	Une tâche événementielle exécute une fonction uniquement lorsqu'un événement (déclencheur) se produit. Le déclencheur d'une tâche événementielle peut être l'un des événements suivants : • Un point consommé • Une instruction EVENT • Un déclenchement d'axe • Un événement de mouvement • Changement d'état des données d'entrée du module

L'automate Compact GuardLogix 5370 prend en charge jusqu'à 32 tâches, dont une seule peut être continue.

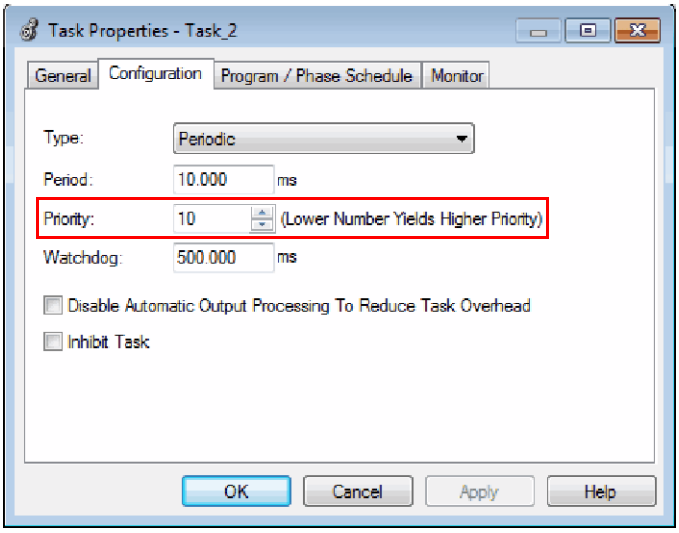
Une tâche peut comporter jusqu'à 100 Programmes distincts, chacun d'eux ayant ses propres sous-programmes exécutables et points d'accès programme. Une fois qu'une tâche est déclenchée (activée), tous les programmes affectés à cette tâche s'exécutent dans l'ordre dans lequel ils sont organisés. Plusieurs tâches ne peuvent pas partager des programmes et ces derniers n'apparaissent qu'une seule fois dans la fenêtre d'organisation de l'automate.

Priorité d'une tâche

Chaque tâche de l'automate possède un niveau de priorité. Le système d'exploitation utilise le niveau de priorité pour décider de la tâche à exécuter lorsque plusieurs tâches sont déclenchées. Une tâche de priorité élevée interrompra toute tâche de priorité plus faible. Une tâche périodique ou événementielle interrompt la tâche continue, qui a la priorité la plus faible.

Vous pouvez configurer les tâches périodiques avec un niveau de priorité allant du plus bas, 15, au plus haut, 1. Configurez la priorité de la tâche dans la boîte de dialogue Task Properties (Propriétés de la tâche).

Figure 26 – Configuration de la priorité d'une tâche



Programmes

Le système d'exploitation de l'automate est un système préemptif multitâche conforme à la norme CEI 1131-3. Il fournit :

- des programmes regroupant des données et de la logique ;
- des sous-programmes permettant d'encapsuler un code exécutable, écrit dans un seul langage de programmation.

Chaque programme comporte les éléments suivants :

- points locaux
- paramètres
- un sous-programme principal exécutable
- d'autres sous-programmes
- un sous-programme de gestion des défauts en option

Figure 27 – Programme d'une application de commande

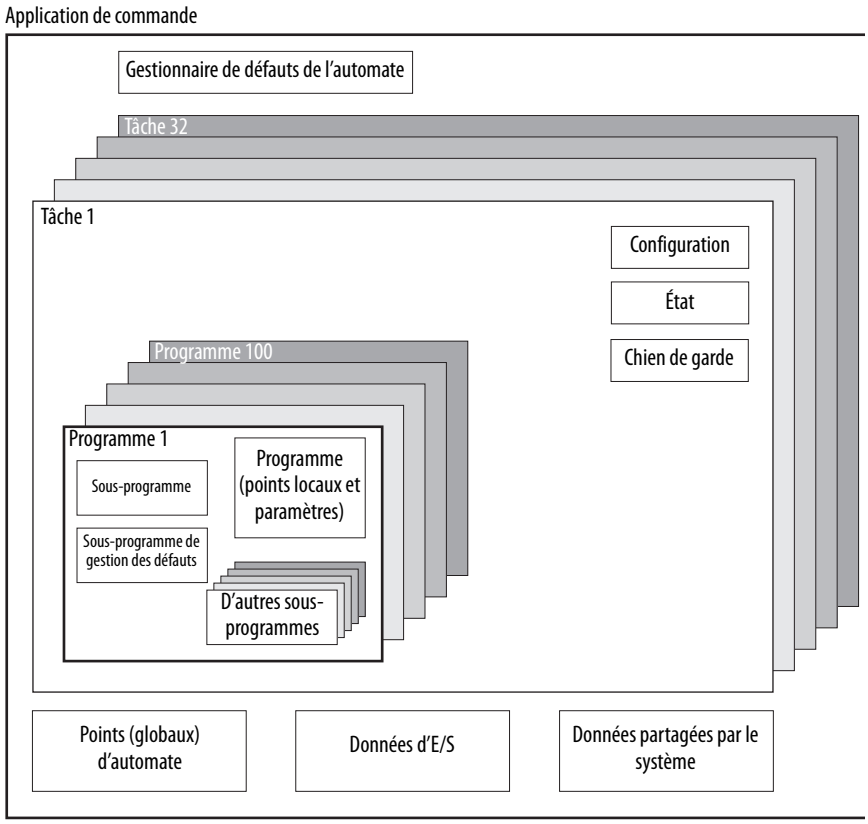
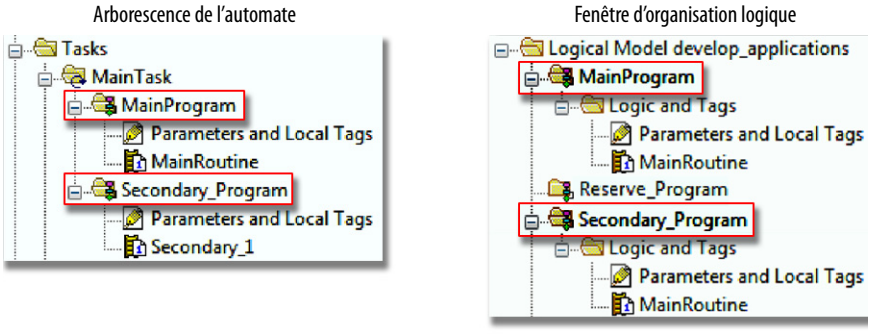


Figure 28 – Programmes de l'application



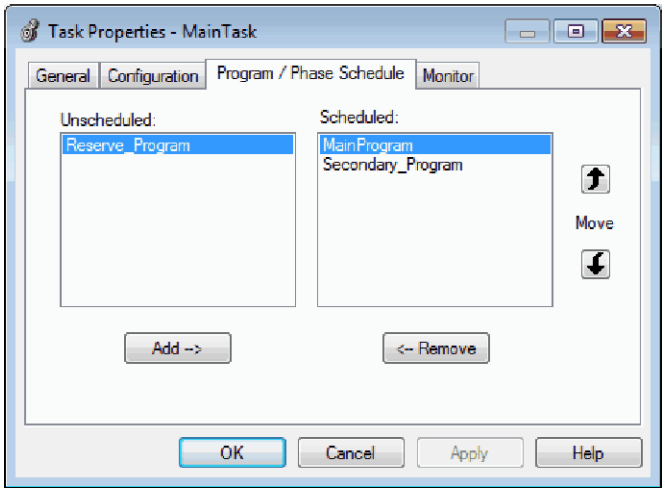
Programmes planifiés et non planifiés

Les programmes planifiés d'une tâche sont exécutés jusqu'à leur achèvement du premier au dernier. Les programmes qui ne sont pas rattachés à une quelconque tâche sont considérés comme des programmes non planifiés.

Les programmes non planifiés d'une tâche sont téléchargés vers l'automate avec l'ensemble du projet. L'automate vérifie les programmes non planifiés mais ne les exécute pas.

Vous devez planifier un programme dans une tâche avant que l'automate ne puisse scruter le programme. Pour planifier un programme non planifié, utilisez l'onglet Program/Phase Schedule (planification de programme/phase) dans la boîte de dialogue Task Properties (propriétés de la tâche).

Figure 29 – Planification d'un programme non planifié



Sous-programmes

Un sous-programme est un jeu d'instructions logiques rédigées dans un même langage de programmation, tel que la logique à relais. Dans un automate, les sous-programmes fournissent le code exécutable pour le projet.

Chaque programme possède un sous-programme principal. C'est le premier sous-programme exécuté lorsque l'automate déclenche la tâche associée et appelle le programme associé. Utilisez la logique, comme l'instruction JSR de saut vers sous-programme, pour appeler les autres sous-programmes.

Vous pouvez également appeler un sous-programme de gestion des défauts en option. L'automate exécute ce sous-programme s'il rencontre un défaut d'exécution d'instruction dans n'importe quel sous-programme du programme associé.

Figure 30 – Sous-programmes d'une application de commande

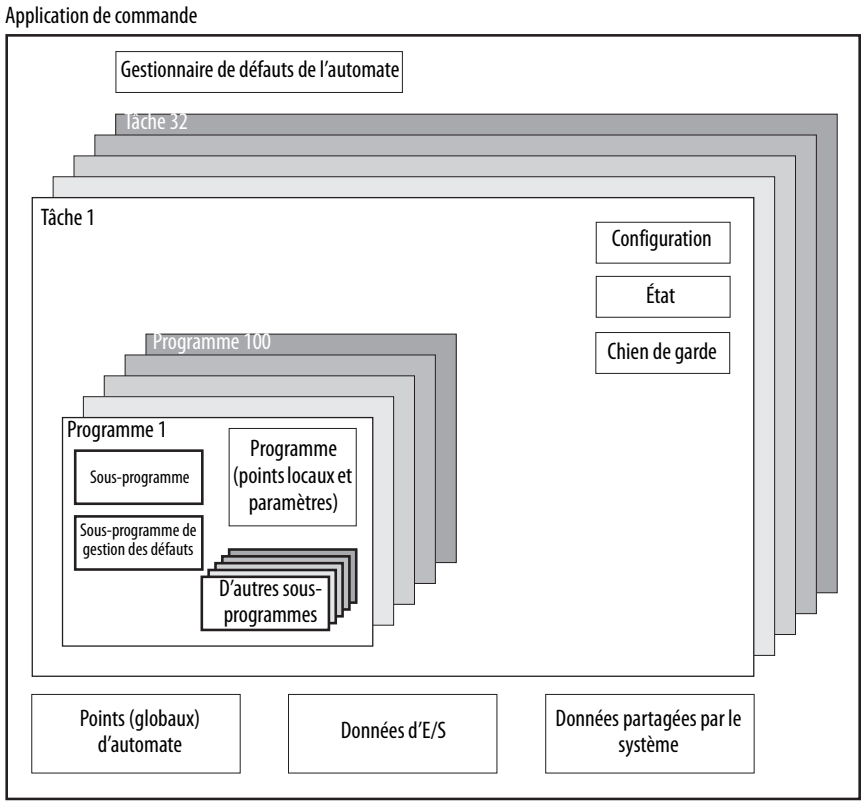
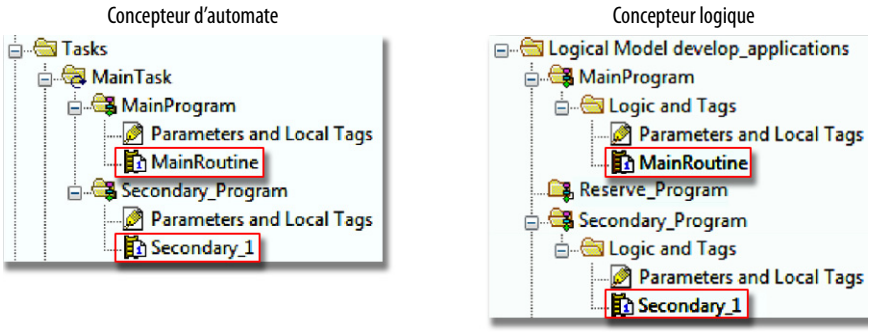


Figure 31 – Sous-programmes d'une application



Points

Avec un automate Logix5000, vous utilisez un point (nom alphanumérique) pour adresser les données (variables). Dans les automates Logix5000, il n'existe pas de format numérique fixe. Par exemple (voir ci-dessous), vous pouvez utiliser le nom de point **north_tank_mix** au lieu d'un format numérique tel que N7:0.0.

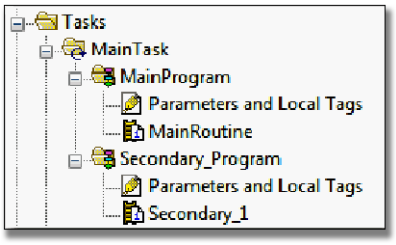
Le nom du point proprement dit identifie les données. Cela vous permet :

- d'organiser vos données pour refléter vos machines ;
- de documenter votre application au fur et à mesure que vous la développez.

La Figure 32 montre des points de données créés au sein du programme principal de l'automate.

Figure 32 – Exemple de points

Fenêtre d'organisation de l'automate – Paramètres et points locaux du programme principal



Fenêtre des points du programme – Points du programme principal

Scope: MainProgram Show: All Tags Enter Name Filter...

Name	Usage	Alias For	Base Tag	Data Type	Description	External Access	Constant	Style
north_tank_mix	Local			BOOL		Read/Write		Decimal
north_tank_pr...	Local			REAL		Read/Write		Float
north_tank_temp	Local			REAL		Read/Write		Float
one_shots	Local			DINT		Read/Write		Decimal
recipe	Local			TANK		Read/Write		
recipe_number	Local			DINT		Read/Write		Decimal
replace_bit	Local			BOOL		Read/Write		Decimal
running_hours	Local			COUNTER		Read/Write		
running_secon...	Local			TIMER		Read/Write		
start	Local			BOOL		Read/Write		Decimal
stop	Local			BOOL		Read/Write		Decimal

Dispositif d'E/S analogique
Valeur entière
Bit de stockage
Compteur
Temporisateur
Dispositif d'E/S TOR

Il existe plusieurs recommandations à connaître pour créer et configurer des paramètres et points locaux, de façon à obtenir une exécution optimale de la tâche et du programme. Pour de plus amples informations, consultez la publication 1756-PM004, « Logix5000 Controllers and I/O Tag Data Programming Manual ».

Propriétés étendues

La fonctionnalité de propriétés étendues (Extended Properties) vous permet de définir des informations complémentaires, comme des limites, des unités techniques ou des identifiants d'état pour un certain nombre de composants à l'intérieur de votre projet automate.

Composant	Propriétés étendues
Point	Dans l'éditeur de points, ajoutez des propriétés étendues à un point.
Type de données utilisateur	Dans l'éditeur de type de données, ajoutez des propriétés étendues aux types de données.
Instructions complémentaires	Dans les propriétés associées à la définition d'une instruction complémentaire, ajoutez des propriétés étendues aux instructions complémentaires.

La « propagation » est la capacité d'attribuer des propriétés étendues à un haut niveau d'une structure ou d'une instruction complémentaire et de répercuter automatiquement les propriétés étendues à tous les membres. Le comportement passant est applicable aux descriptions, aux identifiants d'état et aux unités techniques. Il est configurable par l'utilisateur. Configurez la propagation dans l'onglet Project (projet) de la boîte de dialogue Controller Properties (propriétés de l'automate). Si vous choisissez de ne pas afficher les propriétés passantes, seules les propriétés étendues qui ont été configurées spécifiquement pour un composant seront affichées.

Le comportement passant **ne s'applique pas** aux limites. Lorsqu'une instance d'un point est créée, si des limites sont associées au type de données, l'instance est copiée.

Vous avez besoin de connaître les points dotés de limites, car il n'existe aucune indication dans l'explorateur de points montrant que des propriétés étendues ont été définies pour un point donné. Par contre, si vous tentez d'utiliser des propriétés étendues qui n'ont pas été définies pour un point, les éditeurs en donne une indication visuelle et la vérification du sous-programme échoue.

Accès aux propriétés étendues dans la logique

Vous pouvez accéder aux limites définies dans les points au moyen de la syntaxe .@Min ou .@Max :

- Vous ne pouvez pas écrire sur les valeurs des propriétés étendues dans la logique.
- Pour utiliser les propriétés étendues de point dans une instruction complémentaire, vous devez les transmettre à cette instruction sous la forme d'opérandes d'entrée.
- Les alias de points dotés de propriétés étendues ne peuvent pas accéder à ces propriétés dans le programme.
- Les paramètres d'entrée et de sortie d'instructions complémentaires peuvent avoir des limites configurées. Cependant, les limites ne peuvent pas être définies sur un paramètre InOut d'une instruction complémentaire.

- L'accès aux limites est impossible par la logique d'une instruction complémentaire. Les limites sont exclusivement réservées aux applications IHM.

Si un point de tableau utilise un adressage indirect pour accéder aux limites dans la logique, les conditions suivantes s'appliquent :

- Si le point de tableau possède des limites configurées, ses propriétés étendues seront appliquées à tous les éléments du tableau qui ne possèdent pas de propriétés étendues particulières formellement configurées. Par exemple, si le point de tableau « MyArray » a une valeur Max configurée de 100, tous les éléments du tableau qui n'ont pas de valeur Max configurée hériteront de cette valeur 100 lorsqu'ils seront utilisés par le programme. Néanmoins, les valeurs héritées de « MyArray » n'apparaîtront pas aux yeux de l'utilisateur dans la configuration des propriétés du point.
- Au moins un élément du tableau doit posséder une limite configurée pour qu'un programme faisant indirectement référence à ce tableau puisse le vérifier. Par exemple, si l'expression « MyArray[x].@Max » est utilisée dans le programme, au moins un élément du tableau de MyArray[] devra avoir une valeur Max configurée dans ses propriétés étendues, si cette valeur n'est pas déjà configurée au niveau de « MyArray ».
- Dans les circonstances suivantes, une valeur par défaut de type de données est utilisée :
  - L'accès au tableau s'effectue via le programme avec une référence indirecte.
  - Le point de tableau n'a pas de propriété étendue configurée.
  - Un membre d'un tableau n'a pas la propriété étendue configurée.

  Par exemple, dans le cas d'un tableau de type SINT, lorsque la limite max. est appelée par le programme pour un membre, utilisez la valeur 127.

Si l'accès à un élément du tableau n'est pas direct, l'élément doit avoir la propriété étendue configurée. Dans le cas contraire, la vérification échoue.

Langages de programmation

L'automate Compact GuardLogix 5370 accepte les langages de programmation suivants, en ligne ou hors ligne :

Tableau 20 – Langages de programmation de l'automate Compact GuardLogix

Langage	Utilisation optimale avec
Logique à relais	Exécution continue ou parallèle de plusieurs opérations (non séquencées)
	Opérations booléennes ou binaires
	Opérations logiques complexes
	Traitement des messages et des communications
	Interverrouillage des machines
	Opérations que le personnel d'intervention ou de maintenance peut avoir besoin d'interpréter pour dépanner la machine ou le procédé
Diagramme de blocs fonctionnels(1)	Processus continu et commande de variateur
	Contrôle de boucle
	Calculs dans le flux des circuits
Graphe de fonctionnement séquentiel (SFC)(1)	Gestion de haut niveau de plusieurs opérations
	Séquence répétitive d'opérations
	Traitement par lots
	Commande d'axe à l'aide de texte structuré
	Opérations par état de machine
Texte structuré(1)	Opérations mathématiques complexes
	Traitement de boucle de tableau ou de table spécialisé
	Gestion de chaîne ASCII ou traitement de protocole

(1) Uniquement avec programmes standard.

Pour de plus amples informations sur la programmation dans ces langages, reportez-vous à la publication 1756-PM001, « Logix5000 Controllers Common Procedures Programming Manual ».

Instructions complémentaires

Pour accroître la cohérence du projet, vous pouvez concevoir et configurer des jeux d'instructions fréquemment utilisées. Semblables aux instructions intégrées dans les automates Logix5000, ces instructions que vous créez s'appellent des instructions complémentaires. Ces instructions complémentaires permettent de réutiliser des algorithmes de commande communs à d'autres applications. Elles vous permettent :

- Simplification de la maintenance grâce à l'animation du programme pour une seule instance.
- Protection de la propriété intellectuelle avec protection de la source.
- Réduction la durée d'élaboration de la documentation.

Vous pouvez utiliser vos instructions complémentaires dans plusieurs projets. Vous pouvez définir vos instructions, les obtenir de quelqu'un d'autre ou les copier à partir d'un autre projet.

Le Tableau 21 présente les principales fonctionnalités et avantages offerts par les instructions complémentaires.

Tableau 21 – Avantages des instructions complémentaires

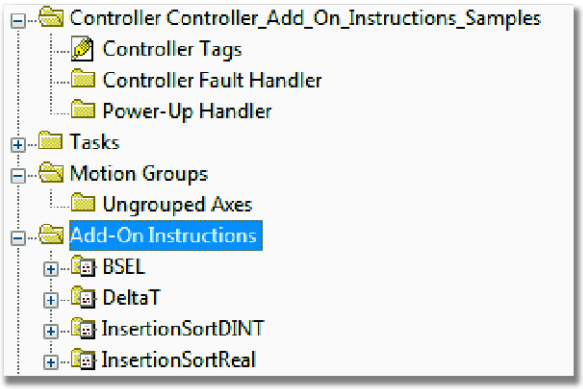
Avantage	Description
Économies de temps	Avec les instructions complémentaires, vous pouvez regrouper la logique que vous utilisez le plus souvent dans des jeux d'instructions réutilisables. Vous gagnerez ainsi du temps lorsque vous créerez des instructions pour vos projets et vous pourrez les partager avec d'autres utilisateurs. Les instructions complémentaires renforcent la cohérence du projet parce que les algorithmes couramment utilisés fonctionnent tous de la même manière, quel que soit la personne qui met en œuvre le projet.
Utilisation d'éditeurs standard	La création des instructions complémentaires s'effectue à l'aide de l'un des trois éditeurs suivants : • Logique à relais • Diagramme de blocs fonctionnels(1) • Texte structuré(1) Une fois que vous avez créé les instructions, vous pouvez les utiliser dans n'importe quel éditeur.
Exportation des instructions complémentaires	Vous pouvez exporter des instructions complémentaires vers d'autres projets, ou encore les copier/coller d'un projet à un autre. Donnez à chaque instruction un nom unique de manière à ne pas écraser accidentellement une autre instruction de même nom.
Utilisation de vues contextuelles	L'affichage contextuel vous permet de visualiser le programme d'une instruction à tout moment particulier de son exécution. Ceci simplifie le dépannage en ligne de vos instructions complémentaires. Chaque instruction comporte un indice de version, un historique des modifications, ainsi qu'une page d'aide générée automatiquement.
Création d'une aide personnalisée	Lorsque vous créez une instruction, renseignez les champs de description des boîtes de dialogue ; les informations saisies constituent l'aide personnalisée. L'aide personnalisée vous permet d'obtenir aisément l'aide nécessaire lorsque vous mettez les instructions en œuvre.
Protection de la source	En tant que créateur d'instructions complémentaires, vous pouvez limiter l'accès des utilisateurs de vos instructions à leur lecture seule. Vous pouvez encore interdire l'accès au programme interne ou aux paramètres locaux utilisés par ces instructions. Cette protection de la source évite toute modification indésirable de vos instructions et protège la propriété intellectuelle.

(1) Uniquement avec programmes standard.

Une fois qu'elles sont définies dans un projet, les instructions complémentaires se comportent de la même manière que les instructions intégrées dans les automates Logix5000. Pour en faciliter l'accès, elles apparaissent dans la barre d'outils des instructions, tout comme les instructions internes.

Figure 33 – Instructions complémentaires

Arborescence de l'automate



Barre d'outils des instructions

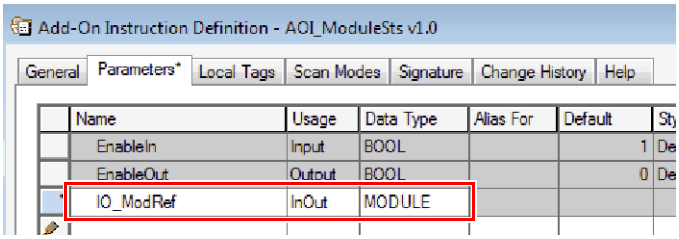
Accès à l'objet module

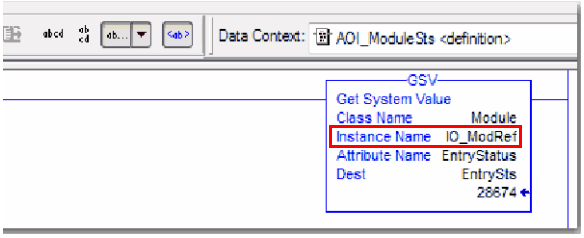
L'objet MODULE fournit des informations sur l'état du module. Pour sélectionner un objet module spécifique, paramétrez l'opérande Object Name (Nom d'objet) de l'instruction GSV/SSV avec le nom du module. Le module défini doit être présent dans la section I/O Configuration (configuration d'E/S) de la fenêtre d'organisation de l'automate et doit avoir un nom de dispositif.

Création de l'instruction complémentaire

Avec l'application Logix Designer, vous pouvez accéder à un objet MODULE directement depuis une instruction complémentaire. Auparavant, il était possible d'accéder aux données de l'objet MODULE, mais pas depuis une instruction complémentaire.

Vous devez créer un paramètre Module Reference (Référence module) lorsque vous définissez l'instruction complémentaire pour accéder aux données de l'objet MODULE. Un paramètre Module Reference est un paramètre InOut (entrée-sortie) de type MODULE qui pointe vers l'objet MODULE du module physique. Vous pouvez utiliser les paramètres de référence du module à la fois dans la logique de l'instruction complémentaire et dans la logique du programme.





Pour plus d'informations sur le paramètre Module Reference, reportez-vous à la publication 1756-PM010, « Logix5000 Controllers Add On Instructions Programming Manual », et l'aide en ligne de l'application Logix Designer.

L'objet MODULE utilise les attributs suivants pour fournir les informations d'état :

- EntryStatus
- FaultCode
- FaultInfo
- FWSupervisorStatus
- ForceStatus
- Instance
- LEDStatus
- Mode
- Path

L'attribut Path, disponible dans l'application Logix Designer, fournit un chemin d'accès au module.

Pour plus d'informations sur les attributs disponibles pour l'objet MODULE, reportez-vous à la publication 1756-RM009, « Automates Logix Instructions – Manuel de référence ».

Lorsque vous ajoutez une instruction GSV/SSV au programme, les classes d'objet, les noms d'objet et les noms d'attribut pour chaque instruction sont affichés. Avec une instruction GSV, vous pouvez obtenir les valeurs de tous les attributs disponibles. Pour l'instruction SSV, seuls les attributs que vous êtes autorisé à définir sont affichés.

Certains types d'objet apparaissent à plusieurs reprises. Vous devez en conséquence spécifier le nom de l'objet. Par exemple, votre application peut comporter plusieurs tâches. Chaque tâche a son propre objet Tâche auquel vous pouvez accéder au moyen de son nom.

Il existe plusieurs objets et attributs que vous pouvez utiliser avec les instructions GSV et SSV pour surveiller et configurer le système. Pour de plus amples informations sur les instructions GSV, les instructions SSV, les objets et les attributs, reportez-vous à la publication 1756-RM009, « Logix5000 Controllers General Instructions Reference Manual », et à la section Utilisation des instructions GSV et SSV, page 182.

Tranche de temps de traitement système

L'automate Compact GuardLogix 5370communique avec les autres dispositifs à une fréquence spécifiée (planifiée) ou lorsqu'il y a du temps disponible pour exécuter les communications.

La tranche de temps de traitement système correspond au pourcentage de temps qu'un automate consacre au traitement des communications de service. Si vous avez une tâche continue, la tranche de temps de traitement système (System Overhead Time Slice) saisie dans l'onglet Advanced (Avancé) de la boîte de dialogue Controller Properties (Propriétés de l'automate) spécifie le rapport tâche continue/communications de service. Cependant, s'il n'y a pas de tâche continue, cette valeur de tranche de temps de traitement système n'aura aucune incidence.

Le tableau suivant indique la répartition entre la tâche continue et les communications de service pour différentes valeur de tranche de temps de traitement système.

Tableau 22 – Rapport entre temps d'exécution de la tâche continue et temps d'exécution des communications de service

À cette tranche de temps	Durée d'exécution de la tâche continue	Les communications de service ont lieu pendant une durée maximum de
10 %	9 ms	1 ms
20 %	4 ms	1 ms
25 %	3 ms	1 ms
33 %	2 ms	1 ms
50 %	1 ms	1 ms
66 %	1 ms	2 ms
75 %	1 ms	3 ms
80 %	1 ms	4 ms
90 %	1 ms	9 ms

Comme le montre le Tableau 22, si la valeur de la tranche de temps de traitement système est inférieure ou égale à 50 % la durée restera figée à 1 ms. C'est le cas à 66 % et au-delà, sauf qu'à partir de cette valeur il y a plusieurs intervalles d'1 ms. Par exemple, à 66 % on aura deux intervalles de temps consécutifs de 1 ms et neuf à 90 %.

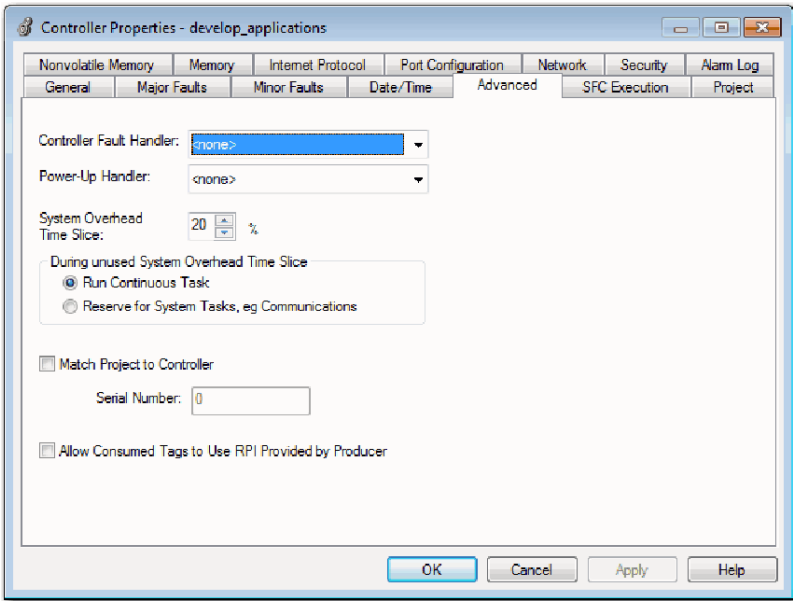
Configuration de la tranche de temps de traitement du système

Pour configurer la tranche de temps de traitement système, procédez comme suit.

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

   La boîte de dialogue Controller Properties (propriétés de l'automate) s'affiche.

2. Cliquez sur l'onglet Advanced (avancé).
3. Entrez une valeur numérique dans la case System Overhead Time Slice (tranche de temps de traitement système).
4. Choisissez soit « Run Continuous Task » (Exécuter la tâche continue – valeur par défaut) soit « Reserve for System Tasks » (Réserver pour les tâches système).
   - Cliquez sur Run Continue Task (exécuter la tâche continue) lorsqu'il n'existe pas de tâches de communication ou d'arrière-plan à traiter ; l'automate revient immédiatement à la tâche continue.
   - Cliquez sur Reserve for System Task (réserver pour tâches système) pour attribuer toute la durée de 1 ms de la tranche de temps de traitement système que l'automate ait des tâches de communication ou d'arrière-plan à exécuter ou non, avant de revenir à la tâche continue. Ceci vous permet de simuler une charge de communication sur l'automate pendant la phase de conception et de programmation, tant que les IHM, la messagerie de l'automate, etc., ne sont pas configurées.
5. Cliquez sur OK.



Notes :

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-RM099, « GuardLogix® 5570 and Compact GuardLogix® 5370 Controller Systems Safety Reference Manual ».

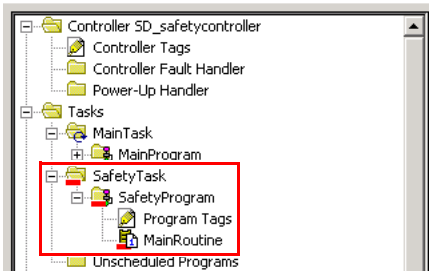
Ce manuel de référence sur la sécurité traite des sujets suivants :

- création d'une spécification détaillée pour un projet ;
- écriture, documentation, et test de l'application ;
- génération de la signature de la tâche de sécurité pour permettre l'identification et la protection du projet ;
- validation du projet par impression ou affichage du projet transféré et comparaison manuelle des configurations, des données de sécurité et de 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, examen de conformité de la sécurité par un organisme indépendant ;
- verrouillage de l'application de sécurité ;
- calcul du temps de réponse du système.

Tâche de sécurité

Lorsque vous créez un projet pour un automate de sécurité, l'application Logix Designer crée automatiquement une tâche de sécurité avec un programme de sécurité et un sous-programme principal (de sécurité).

Figure 34 – Tâche de sécurité dans la fenêtre d'organisation de l'automate



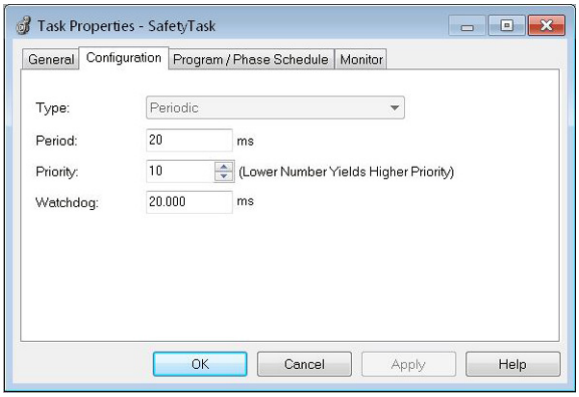
A l'intérieur de la tâche de sécurité, vous pouvez utiliser plusieurs programmes de sécurité, constitués de plusieurs sous-programmes de sécurité. L'automate GuardLogix prend en charge une tâche de sécurité. La tâche de sécurité ne peut pas être supprimée.

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 définir la priorité de la tâche et un temps de chien de garde via la boîte de dialogue Task Properties – Safety Task (Propriétés de la tâche – Tâche de sécurité). Pour ouvrir cette boîte de dialogue, cliquez avec le bouton droit sur la tâche de sécurité et choisir Properties (Propriétés).

Figure 35 – Configuration de la période de la tâche de sécurité



La tâche de sécurité est à haute priorité. 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 la tâche de sécurité 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 réponse du système.

Vous trouverez des informations détaillées sur le calcul du temps de réponse du système dans la publication 1756-RM099, « GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual ».

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 points suivants :

- La tâche de sécurité ne commence pas à s'exécuter 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.
- 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 154.
- Les valeurs des points 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

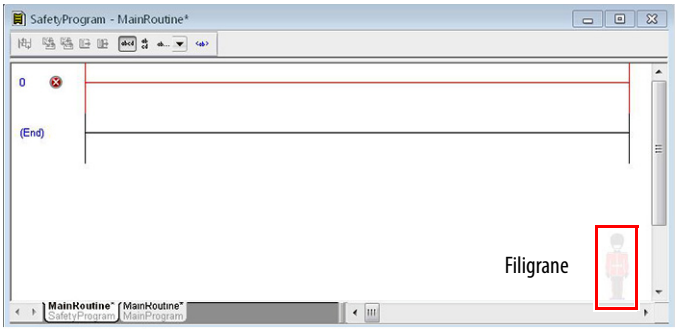
Les programmes de sécurité possèdent toutes les caractéristiques des programmes standard, excepté qu'ils ne peuvent être planifiés qu'à l'intérieur d'une tâche de sécurité et ne peuvent contenir que des composants de sécurité. Les programmes de sécurité peuvent seulement contenir des sous-programmes de sécurité. Un sous-programme de sécurité doit être désigné 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 Un filigrane permet 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, avec en plus des mécanismes certifiés pour permettre l'intégrité des données SIL 3.

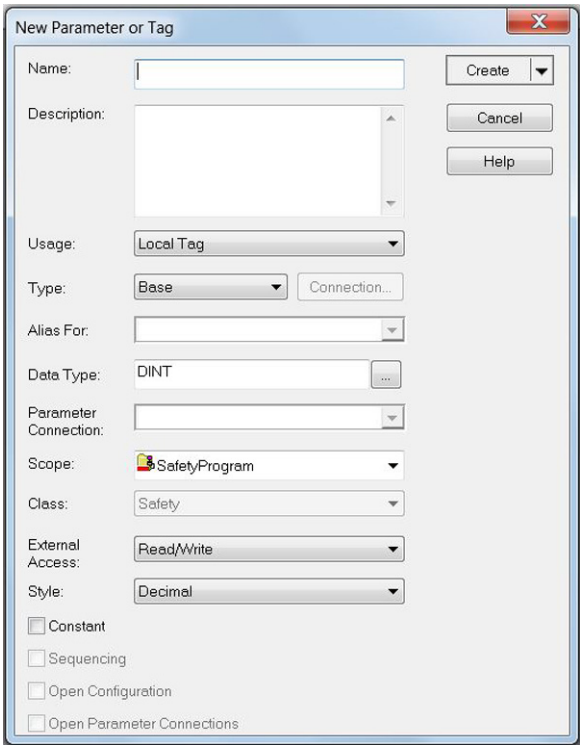
Lorsque vous créez un point, vous lui attribuez les propriétés suivantes :

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

Vous pouvez également indiquer si la valeur du point est une constante.

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

Figure 36 – Création d'un nouveau point



Type de point

Le Tableau 23 définit les quatre types de points.

Tableau 23 – Quatre types de point

Type de point	Description
Point de base	Ces points stockent des valeurs qui seront utilisées par le programme au sein du projet.
Alias de point	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 :** N'utilisez pas d'alias de points entre les points standard et les points de sécurité 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 des points de sécurité, page 154.
Point 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.
Point 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 période de mise à jour des données.

Type de données

Le type de données 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. Dans 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.

Ces types de données sont autorisés pour les points de sécurité.

Tableau 24 – 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

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 des manières suivantes :

- par plusieurs programmes du projet ;
- pour produire ou consommer des données ;
- pour communiquer avec un terminal PanelView™ ;
- pour le mappage d'un point de sécurité.

  Reportez-vous à Mappage des points de sécurité, page 154, 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 25 – Documentation connexe

Documentation	Description
Logix5000 Controllers I/O and Tag Data Programming Manual », publication 1756-PM004	Fournit des indications sur 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 lire ces points 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, l'application Logix Designer 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 comme une IHM, pour afficher ou modifier des valeurs de point. Ce réglage n'a pas d'impact sur l'accès via l'application Logix Designer. La valeur par défaut est lecture/écriture.

Tableau 26 – Niveaux de l'accès externe

Réglage de l'accès externe	Description
Aucune	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 et consommés

Pour transférer des données de sécurité entre des automates Compact GuardLogix de tous types, vous devez utiliser des points de sécurité produits et consommés. Les points produits et consommés nécessitent des connexions. Le type de connexion par défaut pour les points produits et consommés est l'envoi individuel (unicast).

Tableau 27 – Connexions produites et consommées

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

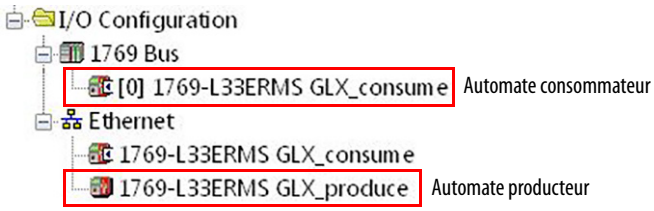
Configuration des numéros de réseau de sécurité des automates de sécurité homologues

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.

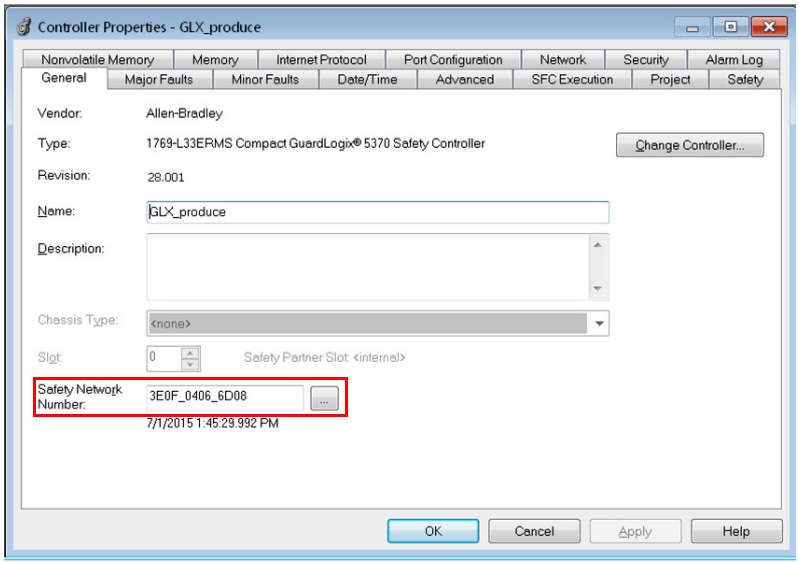
Suivez ces étapes pour copier et coller le SNN.

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

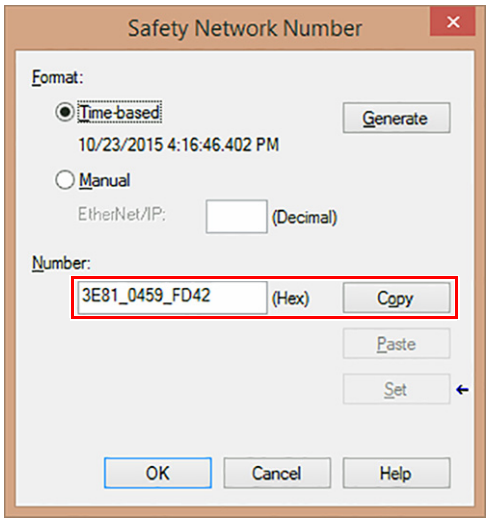
   CONSEIL Le même automate producteur ne doit pas apparaître plus d'une fois dans l'arborescence des E/S de votre automate pour éviter qu'une erreur de vérification se produise.



2. Dans le projet de l'automate producteur, cliquez sur l'automate producteur avec le bouton droit de la souris et sélectionnez Controller Properties (Propriétés de l'automate).
3. Cliquez sur ... pour ouvrir la boîte de dialogue Safety Network Number (Numéro de réseau de sécurité).

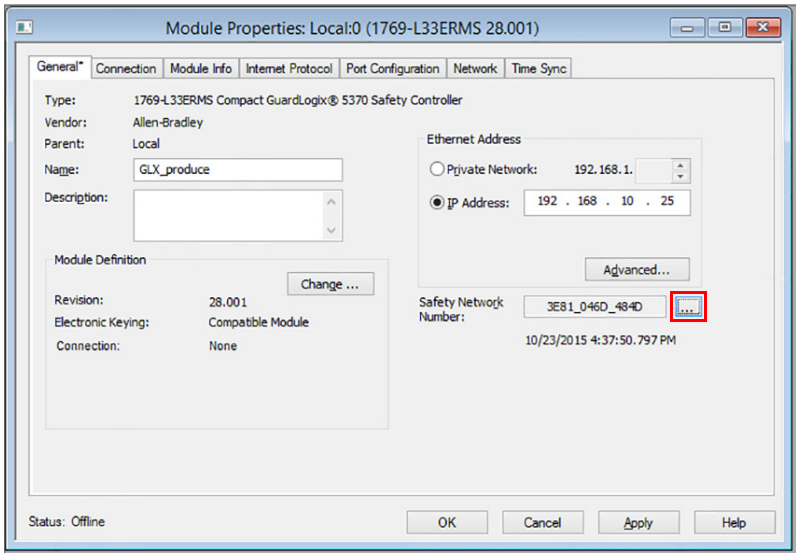


4. Cliquez sur Copy pour copier le numéro SNN de l'automate producteur.

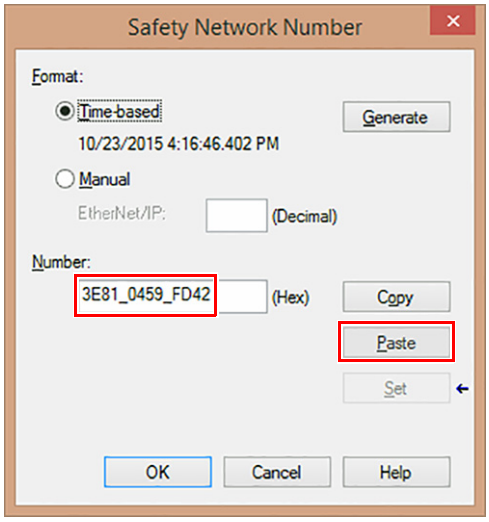


5. Dans le projet de l'automate consommateur, cliquez sur l'automate producteur avec le bouton droit de la souris et sélectionnez Module Properties (Propriétés du module).

6. Cliquez sur [...] pour ouvrir la boîte de dialogue Safety Network Number (Numéro de réseau de sécurité).

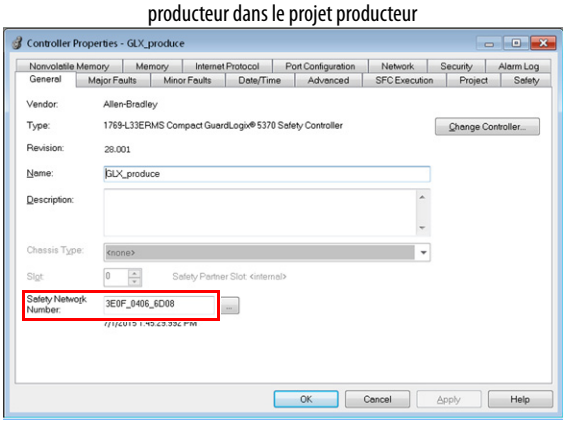


7. Collez le numéro SNN de l'automate producteur dans le champ du SNN de l'automate consommateur et cliquez sur OK.

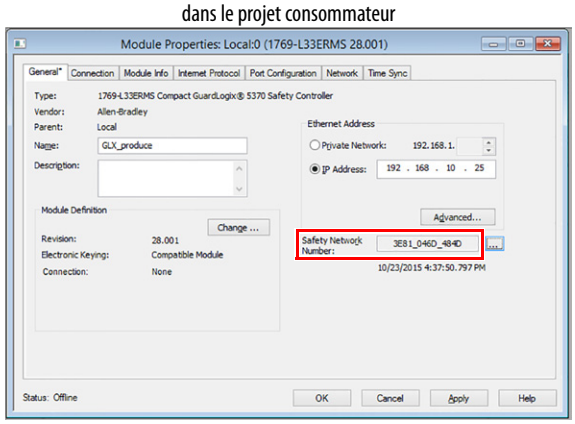


Les numéros de réseau de sécurité correspondent.

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



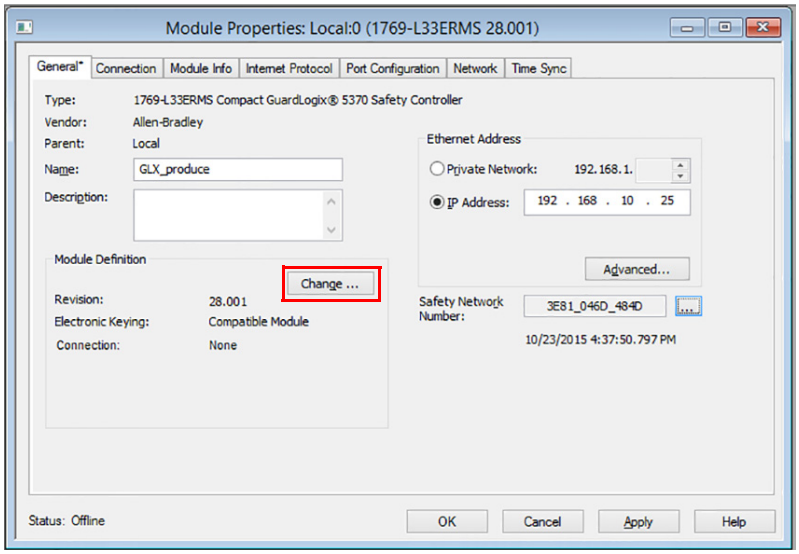
Boîte de dialogue des propriétés du module dans le projet consommateur



Modification du détrompage électronique

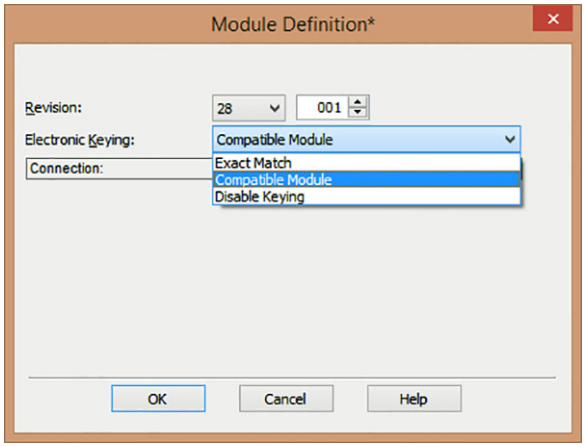
Pour modifier le détrompage électronique, procédez comme ci-après.

1. Dans le projet de l'automate consommateur, cliquez sur l'automate producteur avec le bouton droit de la souris et sélectionnez Module Properties (Propriétés du module).
2. Dans le champ Module Definition (Définition du module), cliquez sur Change.



La boîte de dialogue Module Properties (Propriétés du module) apparaît.

3. Dans le menu déroulant Electronic Keying (Détrompage électronique), choisissez l'option convenant à votre application.



IMPORTANT Si vous consommez des points de sécurité, vous devez choisir Exact Match (Correspondance exacte) ou Compatible Module (Module compatible) dans le menu déroulant.

Choisissez Disable Keying (Désactiver détrompage) uniquement lorsque des points standard sont consommés.

4. Cliquez sur OK pour enregistrer vos modifications et fermer la boîte de dialogue Module Definition (Définition du module).
5. Cliquez sur OK pour refermer la boîte de dialogue Module Properties (Propriétés du module).

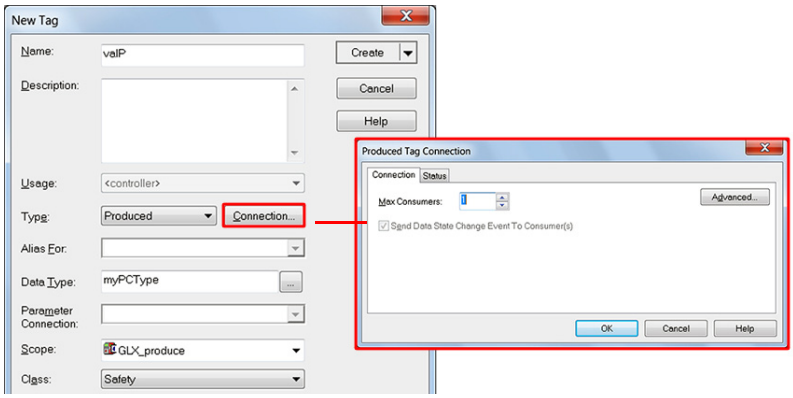
Production d'un point de sécurité

Pour permettre la production d'un point de sécurité, procédez comme suit :

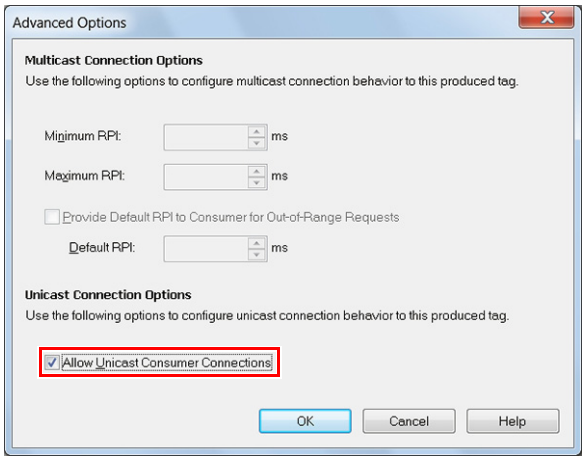
1. Dans le projet des automates producteurs, créez un type de données utilisateur pour définir la structure des données à produire.

   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 Produced (Produit) comme Type, Safety (Sécurité) comme Classe et le type de données utilisateur que vous avez créé à l'étape 1 comme Data Type (Type de données).
4. Cliquez sur Connection (Connexion) et entrez le nombre de consommateurs.



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



6. Cliquez sur OK.

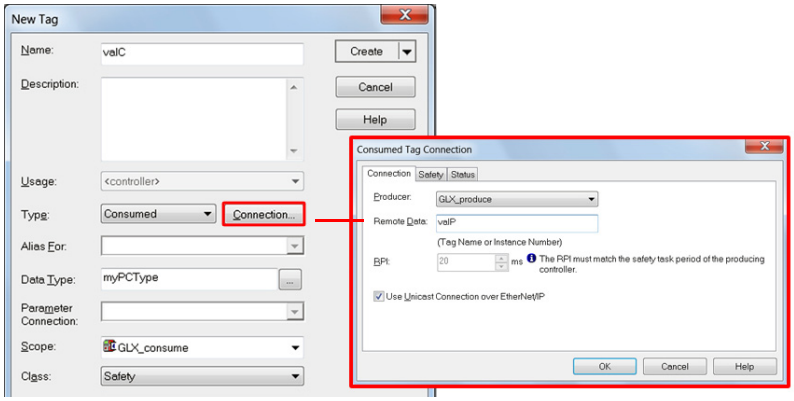
Consommation de points de données de sécurité

Pour autoriser la consommation de données produites par un autre automate, procédez comme suit :

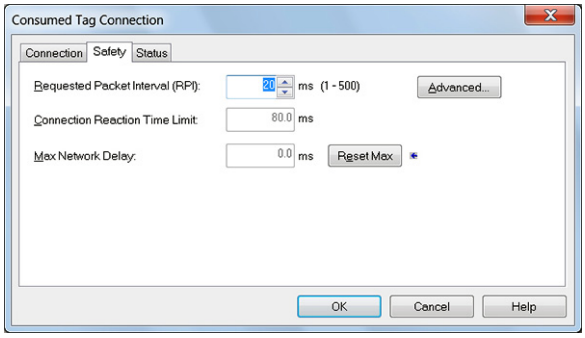
1. Dans le projet d'automate consommateur, créez un type de données utilisateur identique à celui créé dans le projet producteur.

   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 Consumed (Consommé) comme Type, Safety (Sécurité) comme Classe et le type de données utilisateur que vous avez créé à l'étape 1 comme Data Type (Type de données).
4. Cliquez sur Connection (Connexion) pour ouvrir la boîte de dialogue Consumed Tag Connection (Connexion de point consommé).



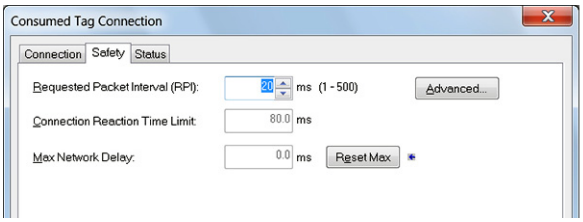
5. Dans les menus déroulants Producer (Producteur), sélectionnez l'automate qui produit les données.
6. Dans le champ Remote Data (Données décentralisées), entrez le nom du point produit.
7. Cliquez sur l'onglet Safety (Sécurité).



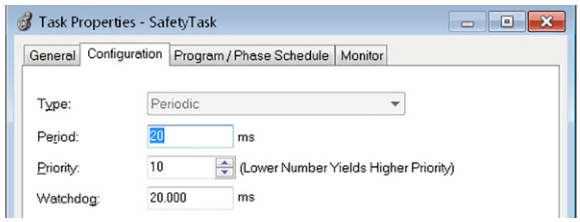
8. Dans le champ Requested Packet Interval (RPI), entrez le RPI pour la connexion par incréments de 1 ms. La valeur par défaut est de 20 ms.

   Le RPI spécifie la période de mise à jour des données via une connexion. Le RPI du point de sécurité consommé doit correspondre à la période de la tâche de sécurité du projet de sécurité producteur.

Projet consommateur



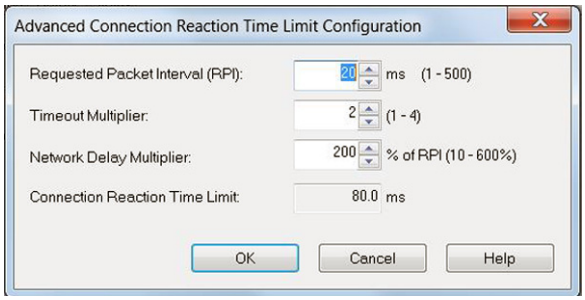
Projet producteur



La valeur limite du temps de réponse de la connexion correspond à l'âge maximal des trames de sécurité sur la connexion associée. 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 réinitialiser Max Network Delay en cliquant sur Reset Max.

9. Si la limite de temps de réponse de la connexion est acceptable, cliquez sur OK. Dans le cas de critères plus complexes, utilisez le bouton Advanced (Avancé) pour ajuster les paramètres Advanced Connection Reaction Time Limit (Limite de temps de réponse avancée de la connexion).



Le multiplicateur de timeout définit le nombre de RPI pendant lesquels il est possible d'attendre une trame avant qu'un timeout de connexion ne soit déclaré.

Le multiplicateur de délai réseau définit le temps d'acheminement d'un message imposé par le 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 28 – documentation connexe

Documentation	Description
Estimate Requested Packet Interval, page 85 et Module Fault Related to RPI Estimates, page 86	Fournit des informations complémentaires sur le réglage du RPI et sur la manière dont le délai réseau max., le multiplicateur de timeout, et les multiplicateurs de délai réseau influent sur le temps de réponse de la connexion
Logix5000™ Controllers Produced and Consumed Tags Programming Manual, publication 1756-PM011	Informations détaillées sur l'utilisation des points produits et consommés

Mappage des 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 :

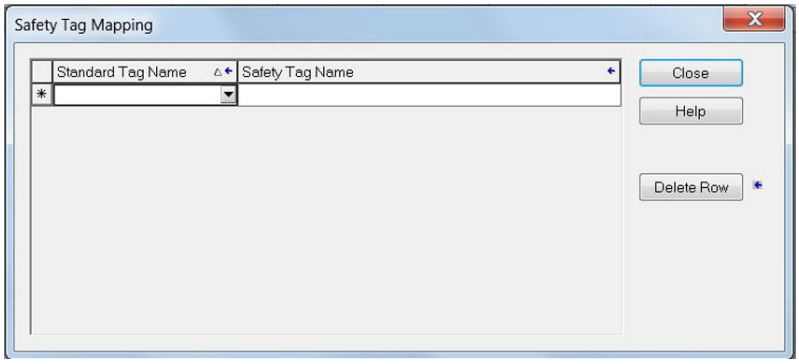
- la paire point de sécurité/point standard doit être en accès automate ;
- les types de données de la paire point de sécurité/point standard doivent correspondre ;
- les alias de points ne sont pas autorisés ;
- le mappage doit être applicable à l'ensemble du point. Par exemple, « myTimer.pre » ne sera 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 ;
  - 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 vérifier que leur utilisation est 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.

Consultez la publication 1756-RM099, « GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual », pour de plus amples informations.

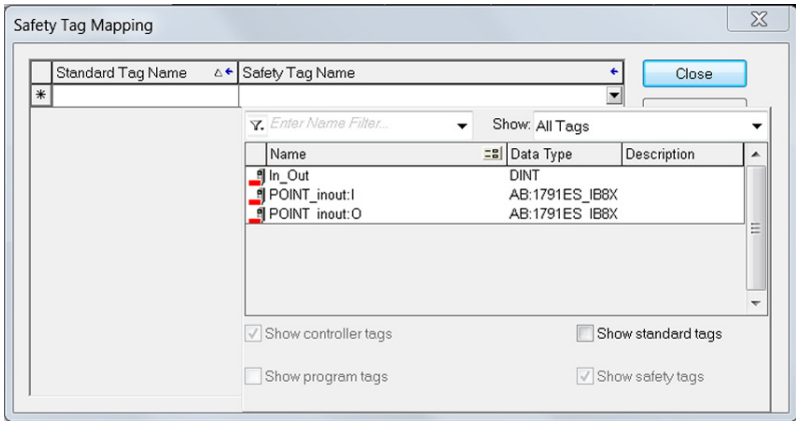
Création de paires de points mappées

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



2. Ajoutez un point existant à 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 une boîte de dialogue d'explorateur de points avec filtre. Si vous êtes dans la colonne Standard Tag Name (Nom de point standard), l'explorateur affiche uniquement les points standard d'accès automate. Si vous êtes dans la colonne Safety Tag Name (Nom de point de sécurité), l'explorateur affiche les points de sécurité d'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 nomdupoint), dans lequel « tagname » correspondra au nom que vous venez de saisir.

Contrôle de l'état du mappage des points

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

Tableau 29 – 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 rangée ou fermer la boîte de dialogue Safety Tag Mapping (Mappage de point de sécurité).(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 (Mappage de point de sécurité) tant que subsiste cette erreur de mappage.
	Indique la rangée actuellement sélectionnée.
	Indique la rangée 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 de points, page 154.

Protection de l'application de sécurité

Vous pouvez protéger votre programme d'application vis-à-vis 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 Compact GuardLogix de façon à empêcher toute modification des composants 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 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 (y compris les 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 la logique d'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.

Bouton d'état de la sécurité

La barre d'application affiche également les icônes suivantes pour indiquer si la sécurité de l'automate de sécurité est verrouillée ou non.

- = Sécurité de l'automate verrouillée
- = Automate déverrouillé

Vous pouvez sécuriser le projet 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 en attente ne doivent cependant pas être présentes.

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 de plus amples informations sur l'accès au journal de l'automate, reportez-vous à la publication 1756-PM015, « Logix5000™ Controllers Controller Information and Status Programming Manual ».

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

Figure 37 – 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 Définition des mots de passe pour le verrouillage et le déverrouillage de la sécurité, page 58.

La fonction de verrouillage de sécurité décrite dans la présente section, ainsi que les fonctions de sécurité standard de l'application Logix Designer sont applicables aux projets d'automate GuardLogix.

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

Génération d'une signature de tâche de sécurité

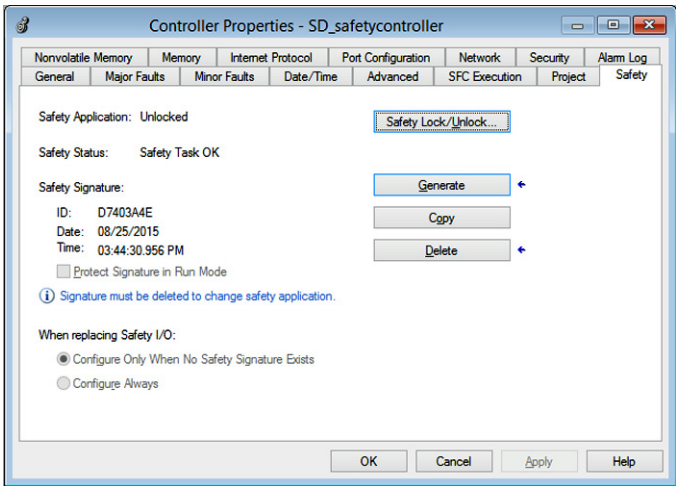
Avant d'entreprendre les tests de vérification, vous devez générer la signature de tâche de sécurité. Vous ne pouvez générer cette signature de sécurité que si l'automate GuardLogix est en ligne, en mode programmation, sécurité déverrouillée, sans forçage de sécurité, sans modifications de sécurité en 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 Run et la protection en mode d'exécution activée.

CONSEIL Vous pouvez visualiser l'état de la sécurité via le bouton situé sur la barre en ligne (voir page 157 Figure 38) ou dans l'onglet Safety (Sécurité) de la boîte de dialogue Controller Properties (Propriétés de l'automate), comme indiqué page.

Vous pouvez créer 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 choisir Tools>Safety>Generate Signature (Outils > Sécurité > Générer la signature).

Figure 38 – 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 l'accès au journal de l'automate, reportez-vous à la publication 1756-PM015, « Logix5000 Controllers Controller Information and Status Programming Manual ».

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

- programmation ou modifications en ligne et hors ligne (y compris les 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 la logique d'un sous-programme de sécurité) ;

Copie de 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 pour copier les composants d'identification, de date et d'heure dans le presse-papiers de Windows.

Suppression de la signature de tâche de sécurité

Cliquez sur Delete pour effacer la signature de la 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 Exécution avec le commutateur à clé dans la position RUN ;
- l'automate est en mode Exécution ou en mode Exécution à distance et la protection en mode d'exécution est activée.

ATTENTION : Si vous supprimez la signature de tâche de sécurité, vous devrez retester et revalider la conformité SIL 3/PLe de votre système.

Pour de plus amples informations sur les exigences SIL 3/PLe, reportez-vous à la publication 1756-RM099, « GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual ».

Restrictions de programmation

Des restrictions limitant l'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 lorsque :

- 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 absent
  - 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 des 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, la description, le type de châssis, le logement et le numéro de réseau de sécurité ;
- modifier ou supprimer la signature de la tâche de sécurité lorsque la sécurité est verrouillée.

Développement d'applications de commande d'axe intégrée en réseau EtherNet/IP

Les automates Compact GuardLogix® 5370 suivants sont capables de gérer la commande d'axe intégrée en réseau EtherNet/IP.

Les applications de commande d'axe intégrée sur EtherNet/IP utilisent les éléments suivants :

- un réseau EtherNet/IP standard
- des variateurs hautes performances, notamment ceux des familles :
  - Kinetix® 350
  - Kinetix® 5500 et Kinetix® 5700
  - Kinetix® 6500
  - PowerFlex® 527
  - PowerFlex® 755
- des composants d'infrastructure standard
- logiciel de programmation

De plus, les variateurs Kinetix 5500(1), Kinetix 5700 et PowerFlex 527 prennent en charge l'arrêt sécurisé du couple (STO) via une connexion unique de sécurité et de mouvement à un automate de sécurité Compact GuardLogix 5370. L'automate Compact GuardLogix émet la commande STO sur le réseau EtherNet/IP via CIP Safety et le variateur de sécurité exécute la commande.

Pour des informations complémentaires sur la configuration des variateurs qui utilisent la commande d'axe intégrée en réseau EtherNet/IP, consultez les manuels utilisateur propres aux différents variateurs, répertoriés à la section Documentation connexe, page 12 et la publication MOTION-UM003, « Configuration et mise en service de la commande d'axe intégrée en réseau EtherNet/IP – Manuel utilisateur ».

(1) Concerne uniquement les variateurs Kinetix 5500 de référence -ERS2.

Types d'axes pris en charge

Les automates 1769-L30ERMS, 1769-L33ERMS, 1769-L33ERMOS, 1769-L36ERMS, 1769-L36ERMOS et 1769-L37ERMOS prennent en charge ces axes :

- AXIS_VIRTUAL
- AXIS_CIP_DRIVE

Axes de type AXIS_VIRTUAL

Les axes de type AXIS_VIRTUAL sont des images d'axe à usage interne, non associées matériellement à un variateur. C'est-à-dire que vous pouvez configurer ces axes mais qu'ils ne génèrent aucun mouvement physique dans votre système.

Axes de type AXIS_CIP_DRIVE

Les axes de type AXIS_CIP_DRIVE sont des axes associés matériellement à des variateurs qui génèrent dans votre système un mouvement physique selon les paramètres de votre application.

Types de configuration

Lorsque vous ajoutez un axe à votre projet, vous devez l'associer à un variateur. Entre autres paramètres de configuration, vous devez définir un type de configuration. Ce type de configuration d'axe sera également considéré comme celui utilisé par le variateur.

Par exemple, un axe AXIS_CIP_DRIVE pourra utiliser une configuration en boucle de position (Position Loop) et être associé à un variateur Kinetix 350. Cet axe sera considéré comme configuré en boucle de position et le variateur associé sera également réputé configuré en boucle de position.

Les variateurs ci-dessous peuvent gérer les types de configuration indiqués :

- Variateurs Kinetix 350, Kinetix 5500, Kinetix 5700 et Kinetix 6500
  - Boucle de position
  - Boucle de vitesse
  - Boucle de couple
- Variateurs PowerFlex 527 et PowerFlex 755
  - Boucle de position
  - Boucle de vitesse
  - Boucle de couple
  - Commande en fréquence

Nombre maximum de variateurs configurables en boucle de position

Tout dispositif rattaché à une station Ethernet locale dans la configuration des E/S est pris en compte dans le total des stations de l'automate. Pour de plus amples informations, voir Stations d'un réseau EtherNet/IP, page 71.

Les variateurs sont comptabilisés dans le total des stations à la section de configuration des E/S de l'application Logix Designer. Si vous utilisez le nombre maximum de variateurs qu'un automate Compact GuardLogix 5370 peut accepter dans un même système, vous ne pourrez pas ajouter d'autres dispositifs EtherNet/IP à ce projet.

Nombre maximum de variateurs configurables en boucle de position

Dans le nombre total des variateurs gérables par les automates énumérés, un certain nombre seulement peut être configuré en boucle de position dans le projet de l'automate.

Par exemple, un automate 1769-L30ERMS n'accepte qu'un maximum de quatre variateurs configurés en boucle de position.

Le Tableau 30 regroupe les caractéristiques de capacité des automates dédiés à la commande d'axe intégrée en réseau EtherNet/IP.

Tableau 30 – Automates Compact GuardLogix 5370 prenant en charge la commande d'axe intégrée en réseau EtherNet/IP

Type d'automate	Nombre max. de variateurs gérés	Nombre max. de variateurs gérés configurables en boucle de position
1769-L30ERMS	16	4
1769-L33ERMS 1769-L33ERMOS	32	8
1769-L36ERMS 1769-L36ERMOS 1769-L37ERMOS(1)	48	16

(1) Accessible en tant que révision du firmware 30.

Si votre solution de commande nécessite plus de 16 variateurs configurés en boucle de position, envisagez plutôt d'utiliser une plate-forme ControlLogix®. La plate-forme ControlLogix permet en effet d'utiliser jusqu'à 100 variateurs configurés en boucle de position.

Synchronisation temporelle

La commande d'axe intégrée en réseau EtherNet/IP nécessite une synchronisation temporelle, également dénommée CIP Sync. CIP Sync permet la synchronisation en temps réel (heure locale effective) ou en temps universel coordonné (UTC) des automates Compact GuardLogix 5370 et des dispositifs connectés à un réseau EtherNet/IP.

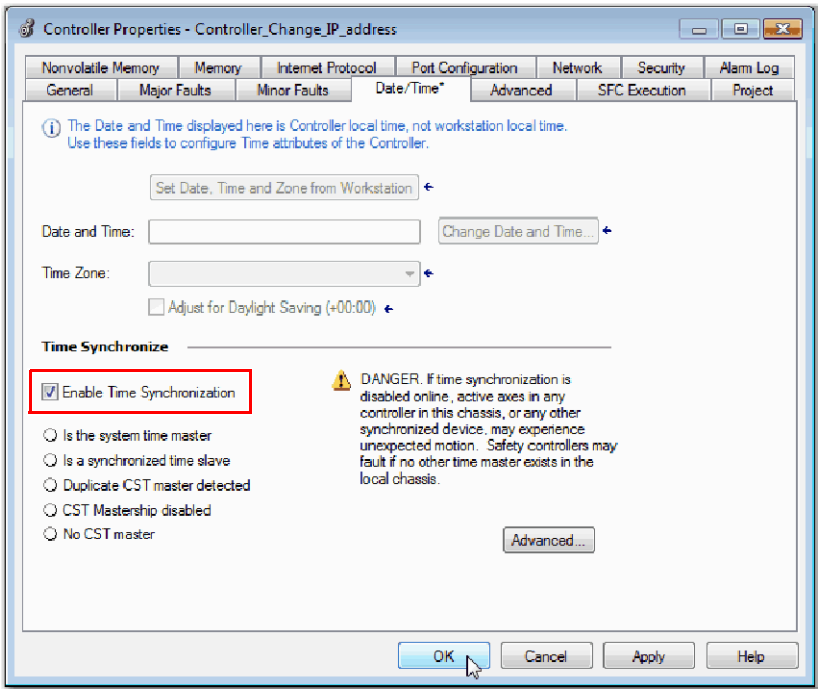
CIP Sync est un protocole de synchronisation temporelle qui peut être utilisé dans diverses applications. Ce chapitre traite spécifiquement de l'utilisation de ce protocole dans les applications de commande d'axe intégrée en réseau EtherNet/IP.

Tous les automates et modules de communication doivent avoir leur synchronisation temporelle activée pour pouvoir fonctionner en mode CIP Sync.

CIP Sync définit la hiérarchie suivante pour les dispositifs présent dans le système :

- Dispositif maître principal (Grandmaster), également appelé maître du temps système coordonné (CST) : définit la base de temps utilisée par l'ensemble du système et transmet cette base de temps à un maître.
- Maître (Master) : définit la base de temps utilisée par son bus intermodules.
- Esclave (Slave) : utilise la base de temps définie par le dispositif maître.

Vous pouvez activer la synchronisation temporelle à l'onglet Date/Time (Date/Heure) de la boîte de dialogue Controller Properties (Propriétés de l'automate).



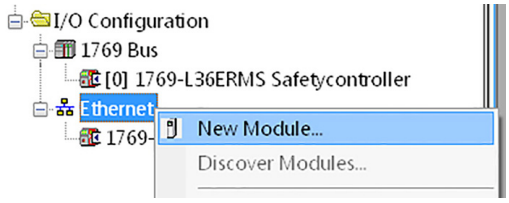
Configuration d'un système de commande d'axe intégrée en réseau EtherNet/IP

Pour ajouter un variateur à votre projet pour la commande d'axe intégrée en réseau EtherNet/IP, procédez comme suit.

IMPORTANT	Ces étapes font référence à un automate 1769-L36ERMS et un variateur Kinetix 350. La même procédure s'applique aux autres automates de la famille Compact GuardLogix 5370 et aux autres variateurs qui prennent en charge la commande d'axe intégrée en réseau EtherNet/IP.

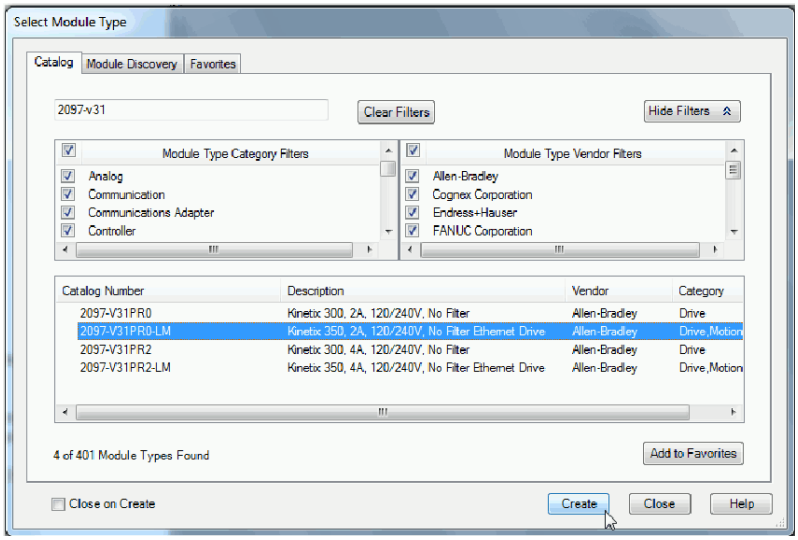
IMPORTANT	Cette section suppose que vous avez préalablement créé un projet pour votre automate 1769-L36ERMS et validé la synchronisation temporelle sur l'automate. Si ce n'est pas le cas, faites-le avant de poursuivre.

1. Dans la configuration des E/S, cliquez avec le bouton droit sur le réseau Ethernet et choisissez New Module (Nouveau module).



   La boîte de dialogue Select Module Type (Choix du type de module) apparaît.

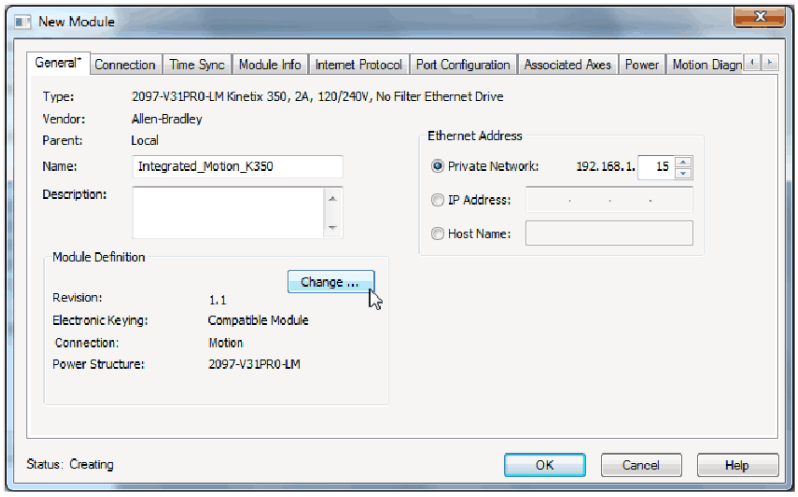
2. Choisissez le variateur souhaité et cliquez sur Create (Créer).



La boîte de dialogue New Module (Nouveau module) apparaît.

3. Entrez un nom pour ce module.
4. Tapez une description, si vous le désirez.
5. Attribuez lui une adresse EtherNet/IP.

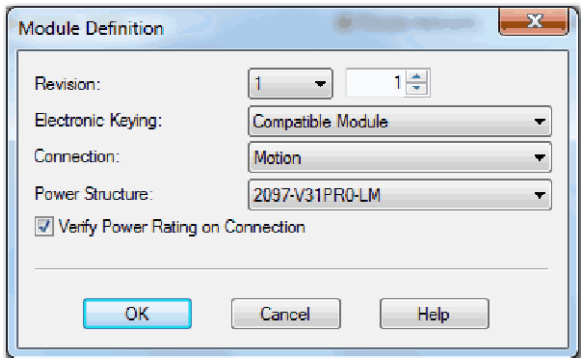
   Pour plus d'informations sur la définition des adresses IP, consultez les documentations propres aux différents types de variateurs, listées à la section Documentation connexe, page 12.



6. Si vous avez besoin de modifier la configuration d'un des paramètres suivants, cliquez sur Change (Modifier) dans le cadre Module Definition (définition du module) :
   - Version
   - Détrompage électronique
   - Connexion

     Pour les variateurs qui acceptent la sécurité et la commande de mouvement sur une seule connexion, vous pouvez choisir Motion Only (Mouvement uniquement), Motion and Safety (Mouvement et sécurité) ou Safety Only (Sécurité uniquement).
   - Power Structure (structure de puissance)
   - Verify Power Rating on Connection (vérifier la puissance nominale lors de la connexion)

   La boîte de dialogue du module apparaît.



7. Effectuez les modifications nécessaires et cliquez sur OK.
8. Cliquez sur OK pour créer le variateur dans votre projet.
9. Ajoutez les autres composants que votre projet exige.

Mise en ligne de l'automate

Points à prendre en compte

Le logiciel de programmation 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 Project to Controller Match (Correspondance Projet/Automate) affecte les processus de téléchargement, de transfert et de connexion 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 de programmation 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 des versions de firmware

La correspondance des versions de firmware a une incidence sur le processus de téléchargement. Si la version 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. L'application Logix Designer vous permet de mettre à jour le firmware lors de la séquence de téléchargement si l'automate est verrouillé par sécurité.

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 qui accompagne l'application Logix Designer.

CONSEIL Vous pouvez également mettre à niveau le firmware à l'aide de la fonction ControlFLASH™ du menu Tools (Outils) dans l'application Logix Designer.

État/défauts de 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 d'un transfert, la signature de la tâche de sécurité du projet hors ligne correspond 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 31 – Effets du verrouillage de la sécurité et de la signature de tâche de sécurité sur l'opération de téléchargement

État du verrouillage de la sécurité	État de la signature de tâche de sécurité	Fonctionnalité du chargement
Automate déverrouillé	La signature de la 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 la tâche de sécurité. La tâche de sécurité n'est pas chargée. L'état du verrouillage de la sécurité correspond à l'état dans le 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 correspond à l'état dans le projet hors ligne.
Sécurité de l'automate verrouillée	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 au chargement de se poursuivre.
	Les signatures de tâche de sécurité ne correspondent pas.	Vous devez d'abord déverrouiller la sécurité de 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 correspond à l'état dans le projet hors ligne.

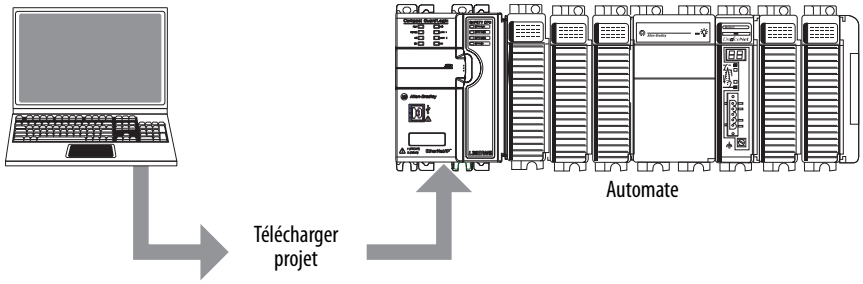
IMPORTANT Lors d'un téléchargement vers un automate dont la sécurité est déverrouillée, si le firmware de l'automate est différent de celui enregistré dans le projet hors ligne, vous pouvez soit :

- mettre à jour l'automate afin qu'il corresponde au 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

Suivez la procédure ci-dessous 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 automate que vous souhaitez télécharger.
3. Spécifiez le chemin vers l'automate.
   a. Cliquez sur Who Active .
   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 l'automate :
   - le numéro de série de l'automate (si la fonction Project to Controller Match est sélectionnée) ;
   - les versions majeures et mineures du firmware ;
   - l'état de la sécurité ;
   - la signature de la 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 renvoyé par le logiciel pour effectuer le téléchargement.

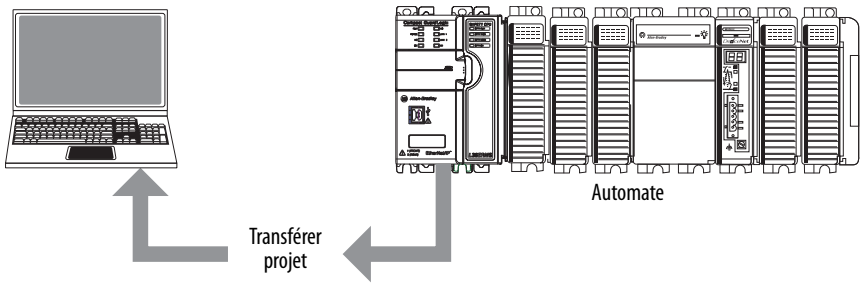
Si le logiciel indique	Alors
Download to the controller.	Cliquez sur Download (Télécharger). Le projet est téléchargé dans l'automate et l'application Logix Designer se met en ligne.
Unable to download to the controller. Discordance entre le numéro de série du projet hors ligne et le numéro de série de l'automate. Selected controller may be the wrong controller.	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 pour correspondre à celui de l'automate.
Unable to download to the controller. The major revision of the offline project and the controller's firmware are not compatible.	Choisissez Update Firmware (Mise à jour du firmware)(1). Choisissez la version requise, puis cliquez sur Update (Mise à jour). Cliquez sur Yes (Oui) pour confirmer votre choix.
Unable to download to controller. (Impossible de télécharger vers l'automate. Le matériel interne du partenaire de sécurité est défectueux).	Remplacez l'automate.
Unable to download to the controller. (Impossible de télécharger vers l'automate. La mise à jour du firmware n'est pas terminée).	Choisissez Update Firmware (Mise à jour du firmware) (1). Choisissez la version requise, puis cliquez sur Update (Mise à jour). Cliquez sur Yes (Oui) pour confirmer votre choix.
Unable to download to controller. Safety partnership has not been established.	Annulez le processus de chargement en cours, puis relancez-le.
Unable to download to controller. Incompatible safety task signature cannot be deleted while the project is safety-locked.	Annulez le téléchargement. Pour pouvoir télécharger le projet, vous devez préalablement déverrouiller la sécurité du projet hors ligne et effacer la signature de la tâche de sécurité. **IMPORTANT :** Le système de sécurité doit être revalidé.
Cannot download in a manner that preserves the safety task signature. La version mineure du firmware de l'automate n'est pas compatible avec la signature de tâche de sécurité dans le projet hors ligne	• En cas d'incompatibilité d'une version mineure du firmware, mettez-le à jour dans l'automate afin qu'il corresponde exactement à la version 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 chargement malgré l'incompatibilité de signature de tâche de sécurité, cliquez sur Download. La signature de la tâche de sécurité sera effacée. **IMPORTANT :** Le système de sécurité doit être revalidé.
Unable to download to controller. Controller is locked. Controller and offline project safety task signatures do not match.	Choisissez Unlock (Déverrouiller). La boîte de dialogue Safety Unlock for Download (Déverrouillage sécurité pour 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. Existence d'un temps système coordonné temps (CST) Existence d'un temps système coordonné temps (CST) maître non alloué.	Cochez Enable Time Synchronization (Activer la synchronisation temporelle) et cliquez sur Download (Télécharger) pour poursuivre l'opération.

(1) L'automate doit être déverrouillé.

Une fois le projet téléchargé avec succès, l'état du verrouillage de sécurité et la signature de la 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 la 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 Who Active .
   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 (Transfert).
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 de programmation 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 :
   - Annulez le transfert et connectez-vous à un automate qui correspond. La procédure de transfert pourra alors être relancée.
   - Sélectionnez un nouveau projet à transférer ou choisissez un autre projet avec Select File (Sélection fichier).
   - Mettez à jour le numéro de série du projet afin qu'il corresponde à celui de l'automate en cochant la case Update Project Serial Number (Mettre à jour le n° de série du projet) avant de sélectionner Upload (Transfert).
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).

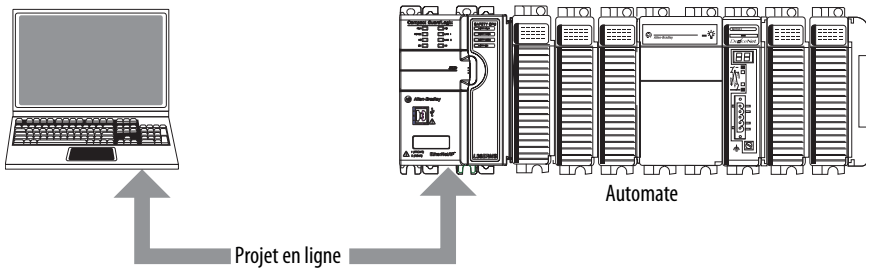
6. Le logiciel recherche les éventuelles modifications du projet hors ligne.
   a. En l'absence de modifications apportées au projet hors ligne, vous pourrez passer en ligne sans effectuer de transfert. Cliquez sur Go Online (Mise en ligne).
   b. Si le projet ouvert comporte des modifications non retranscrites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

   Si vous choisissez Upload (Transfert), 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 reflétera l'état d'origine du projet en ligne (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.

Mise 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 Who Active  .
   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 (Mise en ligne).

   Le logiciel vérifie si :
   - Le numéro de série du projet hors ligne correspond-il à celui de l'automate (si la fonction Project to Controller Match [Concordance Projet/Automate] est sélectionnée) ?
   - Le projet hors ligne comporte-t-il des modifications qui ne figurent pas dans celui de l'automate ?
   - Les versions du firmware indiquées dans le projet hors ligne correspondent-elles à celles de l'automate ?

- La sécurité dans le projet hors ligne ou l'automate est-elle verrouillée ?
- Le projet hors ligne et l'automate ont-ils une signature de tâche de sécurité compatible ?

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

Tableau 32 – Connexion à l'automate

Si le logiciel indique	Alors
Unable to connect to controller. Discordance entre le numéro de série du projet hors ligne et le numéro de série de l'automate. Selected controller may be the wrong controller.	Connectez-vous au bon automate, sélectionnez un autre fichier projet ou cochez la case Update project serial number (Mise à jour du n° de série du projet), puis sélectionnez Go Online (Mise 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. The revision of the offline project and the controller's firmware are not compatible.	Choisissez l'une des options suivantes : • Choisissez Update Firmware (Mise à jour du firmware). Choisissez la version requise, puis cliquez sur Update (Mise 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 de l'application Logix Designer compatible avec la version du firmware de votre automate.
You need to upload or download to go online by using the open project.	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 automate. • Sélectionnez File (Fichier) pour sélectionner un autre projet hors ligne.
Impossible de se connecter d'une manière qui préserve la signature de tâche de sécurité. La version mineure du firmware de l'automate n'est pas compatible avec la signature de tâche de sécurité dans le projet hors ligne.	• Pour préserver la signature de la tâche de sécurité quand la version mineure du firmware est incompatible, mettez à jour la version du firmware de l'automate pour correspondre exactement au projet hors ligne. Passez ensuite en ligne avec l'automate. • Pour procéder au chargement malgré l'incompatibilité de signature de tâche de sécurité, cliquez sur Download. La signature de la tâche de sécurité sera effacée. **IMPORTANT :** Le système de sécurité doit être revalidé.
Unable to connect to controller. Incompatible safety task signature cannot be deleted while project is safety-locked.	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 de programmation 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 la 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.

Surveillance de l'état et gestion des défauts

Voir l'Annexe A, Voyants d'état pour plus d'informations sur l'interprétation des voyants d'état de l'automate.

Visualisation de l'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 39 – 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). L'indicateur 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 de l'indicateur d'état.

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

Figure 40 – Affichage 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 33 – Icône d'état de la sécurité

Si la sécurité est dans l'état suivant	L'icône suivante est affichée
Tâche de sécurité OK	
Tâche de sécurité inexploitable	
Sécurité indisponible	
Hors ligne	

Ces icônes sont à fond vert lorsque la sécurité de l'automate est verrouillée, jaune lorsqu'elle est déverrouillée et 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 de 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 :

- un code d'état de défaut d'E/S est indiqué sur l'afficheur d'état de l'automate Compact GuardLogix® 5370 ;
- le voyant I/O en face avant de l'automate clignote en vert ;
- un symbole d'avertissement ⚠ apparaît sur le dossier de configuration des E/S et sur le dispositif qui est en timeout ;
- 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 pour mettre automatiquement l'automate en défaut en cas de perte de connexion. Vous devrez donc surveiller le déclenchement des défauts de connexion pour vous assurer que le système de sécurité maintient toujours son intégrité SIL 3/PLe.

Voir Connexions de sécurité, page 177.

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'entrée et de sortie, les points d'E/S de sécurité comportent un membre d'état de connexion appelé SafetyStatus. Pour chacun des deux types de données, deux bits sont utilisés : RunMode (Mode Exécution) et ConnectionFaulted (Connexion en défaut).

La valeur RunMode indique si les données consommées sont activement mises à jour par un dispositif en mode Exécution (1) ou en état d'inactivité (0). L'état d'inactivité est indiqué si la connexion est fermée, si la tâche de sécurité est en défaut ou si l'automate ou le dispositif distant est en mode de programmation ou de test.

La valeur ConnectionFaulted 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 RunMode et ConnectionFaulted.

Tableau 34 – État de la connexion de sécurité

État RunMode	État 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.
0 = Inactif	0 = Valable	La connexion est active et le producteur est en état d'inactivité. 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 valable.

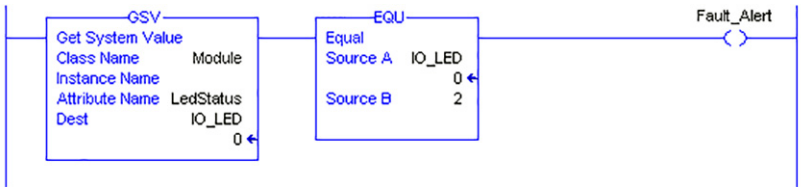
Si un module est inhibé, le bit ConnectionFaulted est mis en défaut (1) et le bit RunMode à l'état inactif (0) pour chaque connexion associée au module. En conséquence, les données de sécurité consommées sont remises à zéro.

Savoir si les communications d'E/S ont dépassé le timeout

L'exemple suivant peut être utilisé avec les automates Compact GuardLogix 5370 :

- L'instruction GSV obtient l'état du voyant d'état des E/S (via l'attribut LEDStatus de l'objet Module) et l'enregistre dans le point IO_LED.
- IO_LED est un point DINT qui enregistre l'état du voyant d'état des E/S ou de l'afficheur d'état en face avant de l'automate.
- Si la valeur d'IO_LED est égale à 2, cela signifie qu'au moins une connexion d'E/S a été perdue et Fault_Alert est alors activé.

Figure 41 – GSV utilisé pour identifier le timeout des E/S



Pour de plus amples informations sur les attributs disponibles avec l'objet Module, reportez-vous à la publication 1756-RM009, « Logix5000 Controllers General Instructions Reference Manual ».

Savoir si les communications d'E/S avec un module d'E/S spécifique ont dépassé le timeout

Si les communications avec un dispositif (module) présent dans la configuration des E/S de l'automate ont dépassé le timeout, l'automate génère un code de défaut et des informations de défaut pour le module en question. Vous pouvez utiliser les instructions GSV pour obtenir le code et les informations de défaut via les attributs FaultCode et FaultInfo de l'objet Module.

Pour de plus amples informations sur les attributs disponibles avec l'objet Module, reportez-vous à la publication 1756-RM009, « Logix5000 Controllers General Instructions Reference Manual ».

Indicateurs de surveillance d'état

Les automates Logix, y compris les automates Compact GuardLogix, prennent en charge des mots-clés d'état que vous pouvez utiliser dans votre logique pour surveiller des événements particuliers.

Pour de plus amples informations sur l'utilisation de ces mots-clés, reportez-vous à la publication 1756-PM015, « Logix5000™ Controllers Controller Information and Status Programming Manual ».

Affichage de l'état de sécurité

Vous pouvez afficher 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 42 – État de la tâche de sécurité

Les états possibles de la sécurité sont les suivants :

- Partenaire de sécurité est indisponible.
- Firmware du partenaire de sécurité incompatible.
- Tâche de sécurité inexploitable.
- Tâche de sécurité OK.

A l'exception du dernier état, 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 181.

Défauts de l'automate

Les défauts dans le système Compact 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 des 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 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 défauts de l'automate, l'exécution de l'application standard se poursuit.

ATTENTION : Le fait de contourner le défaut de sécurité ne l'efface 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.

Lorsqu'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 de les réinitialiser. Les sorties de sécurité sont placées en condition 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.

Codes de défaut

Le Tableau 35 montre les codes de défaut spécifiques aux automates Compact GuardLogix. Le type et le code indiqués correspondent à ceux affichés dans l'onglet Major Faults (Défauts majeurs) de la boîte de dialogue Controller Properties (Propriétés de l'automate) ainsi que dans les attributs MAJORFAULTRECORD (ou MINORFAULTRECORD) de l'objet PROGRAM.

Tableau 35 – 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.	Irrécupérable	Acquittez le défaut. 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.
02	Une erreur est présente dans un sous-programme de la tâche de sécurité.	Récupérable	Rectifiez l'erreur dans la logique du programme utilisateur.
07	La tâche de sécurité est inexploitable. Ce défaut se produit lorsque le programme de sécurité est incorrect. Par exemple, un timeout du chien de garde s'est produit ou la mémoire est corrompue.	Irrécupérable	Acquittez le défaut. Si une signature de tâche de sécurité existe, celle-ci réinitialisera 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	Acquittez le défaut. Configurez un dispositif pour être l'horloge maître CST.

La publication 1756-PM014, « Logix5000 Controllers Major and Minor Faults – Programming Manual », contient la description des codes de défaut communs aux automates Logix.

Développement d'un sous-programme de gestion des défauts

Si une condition de défaut se produit et qu'elle est 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 :

- sous-programme de gestion des défauts de programme
- gestionnaire de défauts de l'automate

Ces deux sous-programmes peuvent utiliser les instructions GSV et SSV, comme décrit à la page 182.

Sous-programme de gestion des défauts 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, « Logix5000 Controllers Major and Minor Faults Programming Manual », fournit des informations détaillées sur la création et le test d'un sous-programme de gestion de défauts.

Utilisation des instructions GSV et SSV

Les automates Logix stockent les données système dans des objets, plutôt que dans des fichiers d'état. Vous pouvez utiliser les instructions GSV (Get System Value/Récupérer une valeur système) et SSV (Set System Value/Définir une valeur système) pour lire et définir 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 36 montre les attributs dont vous pouvez lire les valeurs à l'aide de l'instruction GSV et ceux que vous êtes autorisé(e) 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 36 – Accessibilité des instructions GSV et SSV

Objet de sécurité	Nom de l'attribut	Type de données	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.	X		X	
	MaximumInterval	DINT[2]	Intervalle de temps maximum entre les exécutions successives de cette tâche.			X	X
	MaximumScanTime	DINT	Temps d'exécution maximal enregistré (en ms) pour cette tâche.			X	X
	MinimumInterval	DINT[2]	Intervalle de temps minimum entre les exécutions successives de cette tâche.			X	X
	Priority	INT	Priorité relative de cette tâche par rapport aux autres tâches. Les valeurs valables sont comprises entre 0 et 15.	X		X	
	Rate	DINT	Période de la tâche (en ms) ou timeout de la tâche (en ms).	X		X	
	Chien de garde	DINT	Limite de temps (en ms) assignée à l'exécution de tous les programmes associés à cette tâche.	X		X	
Programme de sécurité	Instance	DINT	Fournit le numéro d'instance de cet objet programme.	X		X	
	MajorFaultRecord[1]	DINT[11]	Enregistre les défauts majeurs survenus dans ce programme.	X	X	X	
	MaximumScanTime	DINT	Temps d'exécution maximal enregistré (en ms) pour ce programme.			X	X
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.	X			
Automate de sécurité	SafetyLocked	SINT	Indique si la sécurité de l'automate est verrouillée ou déverrouillée.	X		X	
	SafetyStatus[2]	INT	Définit l'état de la sécurité comme suit : • Tâche de sécurité OK. (1000000000000000) • Tâche de sécurité inexploitable. (1000000000000001) • Firmware incompatible. (0000000000000011)			X	
	SafetySignatureExists	SINT	Indique si une signature de tâche de sécurité est présente ou non.	X		X	
	SafetySignatureID	DINT	Numéro d'identification à 32 bits.			X	
	SafetySignature	String[3]	Numéro d'identification à 32 bits.			X	
	SafetyTaskFaultRecord[1][2]	DINT[11]	Enregistre les défauts de la tâche de sécurité.			X	
Instruction complémentaire (de sécurité)	LastEditDate	LINT	Horodatage de la dernière modification de la définition d'instruction complémentaire.			X	
	SignatureID	DINT	Numéro d'identification.			X	
	SafetySignatureID	DINT	Numéro d'identification à 32 bits.			X	

(1) Pour plus d'informations sur la façon d'accéder à cet attribut, voir Accès aux attributs FaultRecord, page 184.

(2) Pour plus d'informations sur la façon d'accéder à cet attribut, voir Saisie des informations de défaut, page 184.

(3) Longueur = 37.

(4) À partir de la tâche standard, l'accessibilité de 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 37 – Paramètres d'accès aux attributs FaultRecord

Nom	Type de données	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 de plus amples 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-RM009, « Logix Controllers Instructions Reference Manual ».

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-programme de gestion de défaut de l'automate qui efface le défaut et permet aux tâches standard de poursuivre leur exécution.

Enregistrement et chargement de programmes avec la carte Secure Digital

IMPORTANT La durée de vie prévisible de la mémoire non volatile dépend du nombre de cycles d'écriture réalisés. Le support non volatile utilise une technique de répartition de l'usure afin de prolonger la durée de service, mais il convient d'éviter les écritures trop fréquentes.

Évitez des écritures fréquentes lors de l'enregistrement de données. Il est recommandé d'enregistrer les données dans une mémoire tampon de l'automate et de limiter le nombre des écritures de ces données sur le support mémoire amovible.

Utilisation des cartes mémoire comme mémoire non volatile

Les automates Compact GuardLogix® 5370 prennent en charge une carte Secure Digital comme mémoire non volatile :

- Carte 1784-SD1 – Livrée avec l'automate Compact GuardLogix 5370 et fournissant 1 Go de mémoire. Vous pouvez commander des cartes 1784-SD1 supplémentaires si besoin.
- Carte 1784-SD2 – Livrable séparément et fournissant 2 Go de mémoire.

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 charger le projet enregistré depuis la mémoire non volatile dans la mémoire utilisateur de l'automate :

- 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 tout moment par l'intermédiaire du logiciel de programmation.

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

- Les modifications que vous faites après l'enregistrement du projet ne sont pas reflétées dans la mémoire non volatile.
- Si vous apportez des modifications au projet mais que vous ne les enregistrez pas, elles seront écrasées lorsque vous rechargerez le projet à partir de la mémoire non volatile. Dans ce cas, vous devrez passer en ligne pour transférer ou recharger le projet.
- Si vous voulez que les modifications telles que celles apportées en ligne, ou celles relatives aux valeurs des points soient prises en compte, sauvegardez à nouveau le projet après ces modifications.

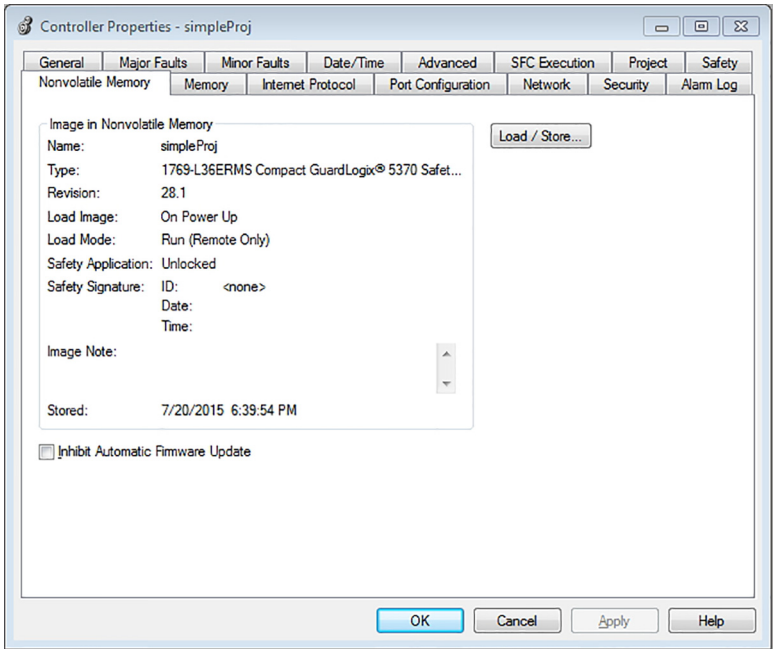
ATTENTION : Ne retirez pas la carte SD pendant que l'automate lit ou écrit sur cette carte, comme indiqué par le clignotement vert du voyant d'état SD. Cela peut entraîner une corruption des données sur la carte ou dans l'automate, ainsi que du firmware le plus récent de l'automate. Laissez la carte dans l'automate jusqu'à ce que le voyant d'état SD passe au vert fixe.

AVERTISSEMENT : Quand vous insérez ou retirez la carte SD alors que l'automate est sous tension un arc électrique peut se produire, susceptible de provoquer une explosion dans des installations en environnement dangereux.

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

Si une carte SD 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 la tâche de sécurité sont affichés.

Figure 43 – Onglet Nonvolatile Memory



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 est sauvegardé sur la carte SD.

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.

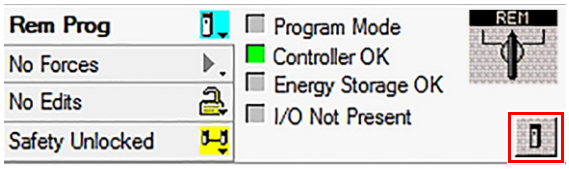
Si une signature de tâche de sécurité existe lorsque vous enregistrez un projet, les opérations suivantes se produisent :

- 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.

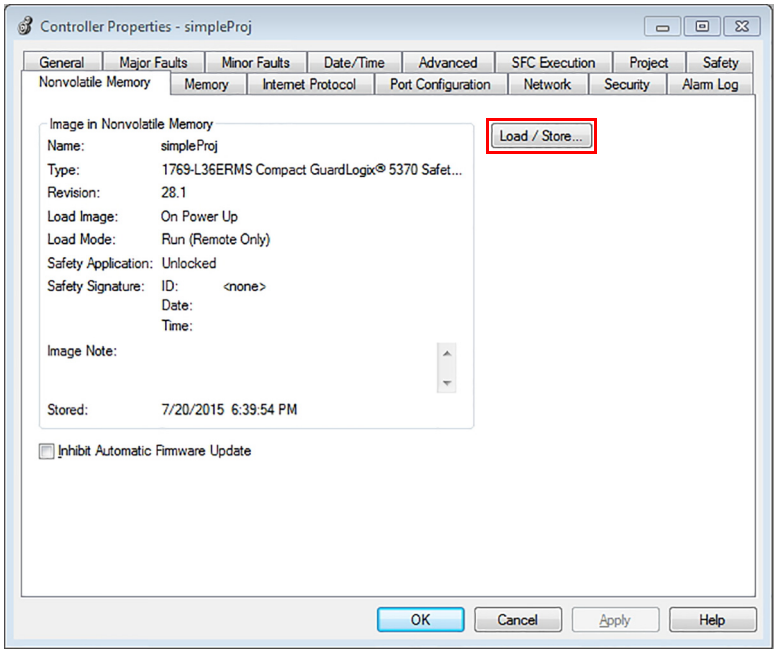
Lorsque vous enregistrez le projet d'une application de sécurité sur une carte SD, il est recommandé de sélectionner Program (Remote Only) (Programmation – à distance seulement) pour le mode de chargement (Load mode), c'est-à-dire le mode de fonctionnement dans lequel repassera l'automate au terme du chargement. Pour de plus amples informations, voir Chargement d'un projet de sécurité, page 190.

Suivez ces étapes pour sauvegarder un projet.

1. Mettez en ligne l'automate.
2. Placez l'automate en mode de programmation, c'est-à-dire sur Remote Program (programmation à distance) ou Program (programmation).
3. Dans la barre d'outils Online (En ligne), cliquez sur l'icône des propriétés de l'automate.



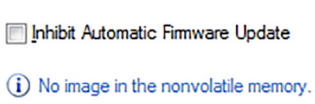
4. Cliquez sur l'onglet Nonvolatile Memory (Mémoire non volatile).
5. Cliquez sur Load/Store (Charger/Enregistrer).



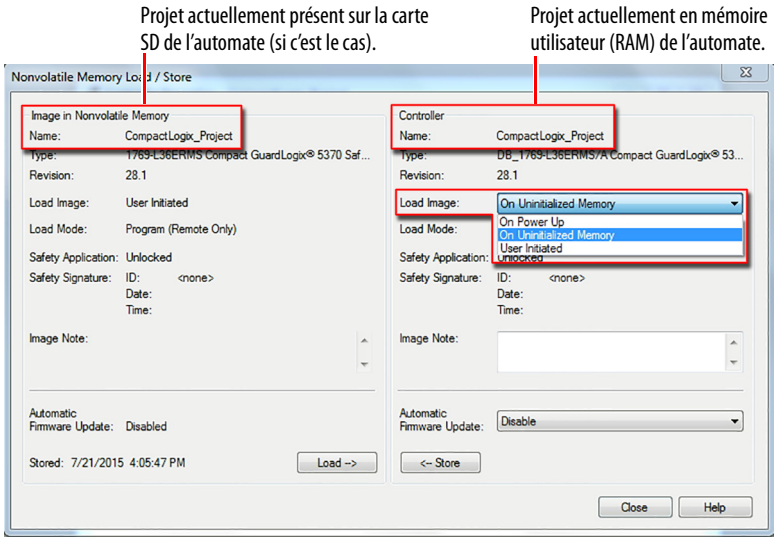
CONSEIL Si Load/Store (Charger/Enregistrer) apparaît en grisé (indisponible), vérifiez si :

- vous avez spécifié le bon chemin de communication et si l'automate est en ligne ;
- la carte SD est installée.

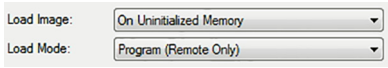
Si la carte SD n'est pas installée, cela est indiqué par un message apparaissant dans le coin inférieur gauche de l'onglet Nonvolatile Memory (Mémoire non volatile).



6. Choisissez le cas dans lequel le projet doit être chargé dans la mémoire utilisateur (RAM) de l'automate.



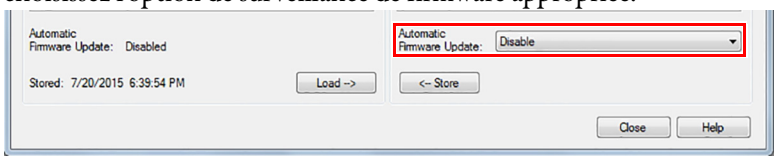
Si vous choisissez l'option On Power Up (à la mise sous tension) ou On Corrupt Memory (sur corruption de la mémoire), vous devez également choisir le mode dans lequel l'automate doit se placer après le chargement :



- Programmation (à distance uniquement)
- Exécution (à distance uniquement)

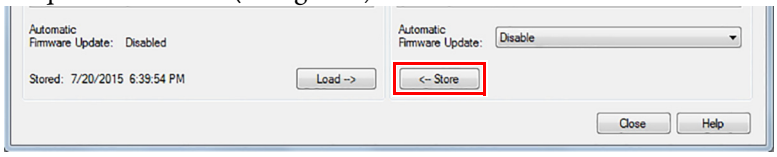
CONSEIL Lorsque vous enregistrez le projet d'une application de sécurité sur une carte SD, il est recommandé de sélectionner Program (Remote Only) (Programmation – à distance seulement) pour le mode de chargement (Load mode), c'est-à-dire le mode de fonctionnement dans lequel repassera l'automate au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

7. Dans le champ Automatic Firmware Update (Mise à jour automatique du firmware), utilisez le réglage par défaut (Disable – Désactiver) ou choisissez l'option de surveillance de firmware appropriée.



IMPORTANT L'option de surveillance de firmware n'est pas utilisée pour mettre à jour le firmware de l'automate.

8. Cliquez sur <- Store (Enregistrer).



IMPORTANT Ce bouton de sauvegarde n'est pas actif si la carte SD est verrouillée.

Une boîte de dialogue vous demande de confirmer l'enregistrement.

9. Pour sauvegarder définitivement le projet, cliquez sur Yes (oui).

Après que vous avez cliqué sur Store (sauvegarder), le projet va être enregistré sur la carte SD, comme l'indiquent les voyants d'état de l'automate. Les situations suivantes peuvent se produire :

- Lorsque la sauvegarde est en cours :
  - le voyant OK clignote en vert ;
  - le voyant SD clignote en vert ;
  - une boîte de dialogue indique que la sauvegarde est en cours.
- Lorsque l'enregistrement est terminé :
  - L'automate est réinitialisé automatiquement.

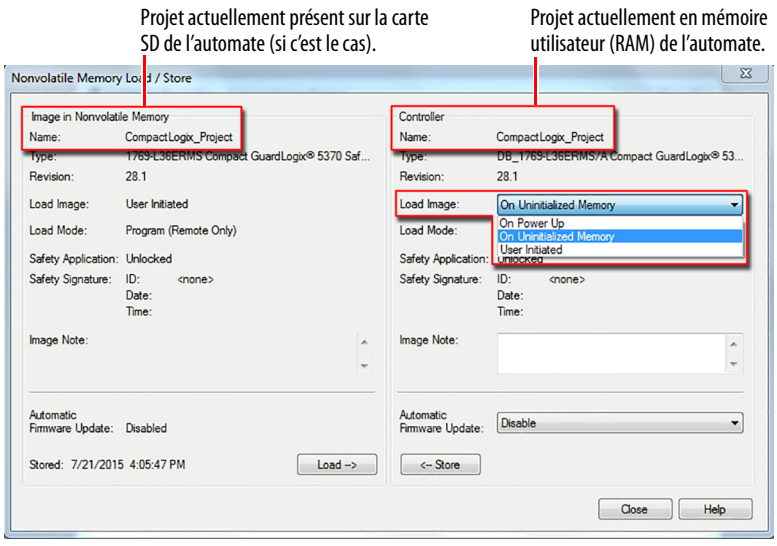
    Lorsque l'automate est en cours de réinitialisation, les voyants d'état passent par une série d'états différents ; par exemple, pendant un court laps de temps le voyant d'état OK est allumé en rouge fixe. Attendez que l'automate ait terminé la séquence.
  - Lorsque l'automate est entièrement réinitialisé, le voyant OK s'allume en vert fixe.
  - Et le voyant SD s'éteint.

IMPORTANT Laissez la sauvegarde se dérouler sans l'interrompre. Si vous interrompez un enregistrement, des données peuvent se trouver corrompues ou perdues.

Chargement d'un projet de sécurité

Vous pouvez lancer le chargement depuis la mémoire non volatile uniquement 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).



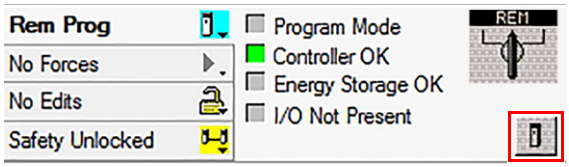
Vous disposez de plusieurs options (en fonction des circonstances) pour charger un projet dans la mémoire utilisateur de l'automate.

Tableau 38 – Options pour le chargement d'un projet

Si vous souhaitez charger le projet	Sélectionnez cette option de chargement d'image	Notes
Chaque fois que vous mettez ou remettez sous tension	On Power Up	• 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 enregistrées 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. Le 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 de programmation 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 Uninitialized Memory	• L'automate met à jour son firmware, si nécessaire. 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 de programmation pour charger le projet.
Uniquement avec le logiciel RSLogix 5000	User Initiated	• 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 d'un projet vers un automate dont la sécurité est verrouillée est autorisé uniquement lorsque la signature de la tâche de sécurité du projet sauvegardé dans la mémoire non volatile correspond au projet présent dans l'automate. • Si les signatures ne 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 la mémoire non volatile au terme de l'opération. • Si le firmware de l'automate principal correspond à la version enregistrée en mémoire non volatile, seul le firmware du partenaire de sécurité sera mis à jour si nécessaire. L'application se trouvant dans la mémoire non volatile sera chargée de façon à ce que l'état de la tâche de sécurité passe en Safety Task Operable (Tâche de sécurité exploitable). L'automate passera alors dans le mode sélectionné, Programme ou Exécution.

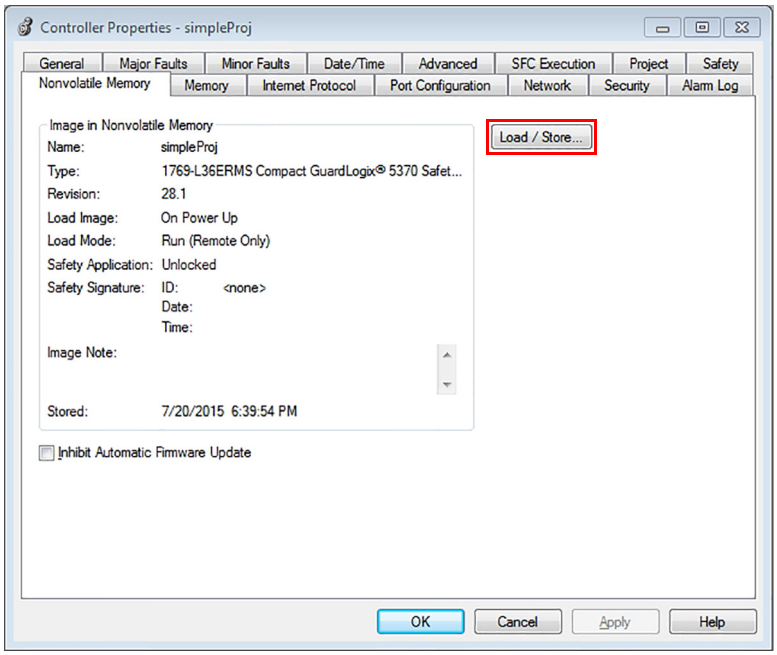
Suivez les étapes ci-dessous pour utiliser l'application pour charger le projet depuis une carte SD.

1. Mettez en ligne l'automate.
2. Placez l'automate en mode de programmation, c'est-à-dire sur Remote Program (programmation à distance) ou Program (programmation).
3. Dans la barre d'outils Online (En ligne), cliquez sur l'icône des propriétés de l'automate.

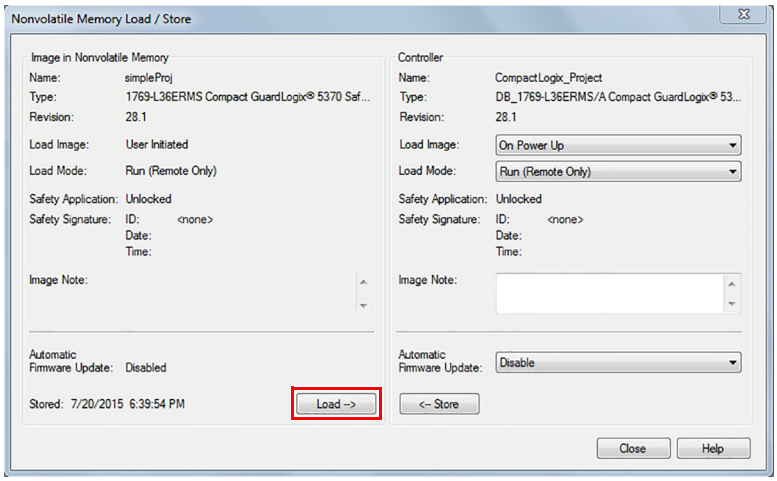


4. Cliquez sur l'onglet Nonvolatile Memory (Mémoire non volatile).

5. Cliquez sur Load/Store (Charger/Enregistrer).



6. Dans la boîte de dialogue Nonvolatile memory load/store (Chargement/Enregistrement depuis mémoire non volatile), cliquez sur Load (Charger).



   Une boîte de dialogue vous demande de confirmer le chargement.

7. Pour charger le projet, cliquez sur Yes (oui).

Une fois que vous avez cliqué sur Load (charger), le projet est chargé dans l'automate, comme l'indiquent les voyants d'état de cet automate. Les situations suivantes peuvent se produire :

- Lorsque le chargement est en cours :
  - L'automate est réinitialisé automatiquement.

    Lorsque l'automate est en cours de réinitialisation, les voyants d'état passent par une série d'états différents ; par exemple, pendant un court laps de temps le voyant d'état OK est allumé en rouge fixe. Attendez que l'automate ait terminé la séquence.
  - Lorsque l'automate est entièrement réinitialisé, le voyant OK s'allume en vert fixe
  - et le voyant SD s'éteint.

Gestion du firmware avec Firmware Supervisor

Vous pouvez utiliser la fonctionnalité Firmware Supervisor de l'application Logix Designer pour gérer le firmware sur les automates Compact GuardLogix 5370. 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 la carte SD de l'automate ;
- le dispositif doit accepter les mises à jour de firmware au moyen du logiciel 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 des E/S CIP Safety en réseau EtherNet/IP.

Suivez ces étapes 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/Enregistrer).
3. Dans le menu déroulant Automatic Firmware Updates (Mises à jour automatique de firmware), sélectionnez Enable and Store Files to Image (Activer et enregistrer les fichiers dans l'image).

L'application Logix Designer transfère les kits de firmware depuis votre ordinateur vers la carte SD de l'automate pour 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 du firmware de l'automate qui se produisent quand l'image de l'automate est rechargée à partir de la carte SD.

Notes :

Voyants d'état

Cette annexe explique comment interpréter les voyants d'état des automates CompactGuardLogix® 5370.

Figure 44 – Voyants d'état

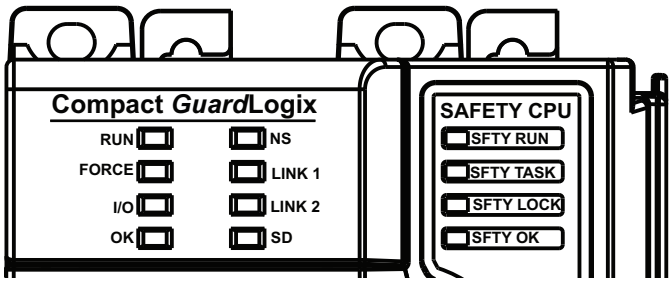


Tableau 39 – Voyant d'état du mode de fonctionnement de l'automate (RUN)

État	Description
Éteint	L'automate est en mode de programmation ou de test.
Vert	L'automate est en mode d'exécution.

Tableau 40 – Voyant d'état du forçage (FORCE)

État	Description
Éteint	Aucun point ne contient de valeurs de forçage des E/S. Pas de forçage d'E/S en cours (désactivé).
Jaune	Forçage d'E/S en cours (activé). Des valeurs de forçage d'E/S peuvent exister.
Jaune clignotant	Une ou plusieurs adresses d'entrée ou de sortie ont été forcées en position ON ou OFF, mais leur forçage n'est pas activé.

Tableau 41 – Voyant d'état I/O (E/S)

État	Description
Éteint	L'une des situations suivantes se produit : • Aucun dispositif n'est présent dans la configuration d'E/S de l'automate. • L'automate ne contient pas de projet.
Vert	L'automate communique normalement avec tous les dispositifs définis dans sa configuration d'E/S.
Vert clignotant	Un ou plusieurs dispositifs défini(s) dans la configuration d'E/S de l'automate ne répond(ent) pas.
Rouge clignotant	L'une des situations suivantes se produit : • L'automate ne communique avec aucun dispositif. • Un défaut s'est produit dans l'automate.

Tableau 42 – Voyant d'état général de l'automate (OK)

État	Description
Éteint	Absence d'alimentation.
Vert	L'automate est opérationnel.
Vert clignotant	L'automate est en train de sauvegarder un projet sur la carte SD ou de charger un projet à partir de la carte SD.
Rouge	L'automate a détecté un défaut majeur irrécupérable et a effacé le projet de sa mémoire.
Rouge clignotant	L'un des cas suivants : • L'automate a besoin d'une mise à jour de son firmware. • Un défaut majeur récupérable s'est produit dans l'automate. • L'automate a détecté un défaut majeur sur l'automate et a effacé le projet de sa mémoire.

Tableau 43 – Voyant d'état du réseau Ethernet (NS)

État	Description
Éteint	Le port n'est pas initialisé ; il ne possède pas d'adresse IP et fonctionne en mode BOOTP ou DHCP.
Vert	Le port possède une adresse IP et des connexions CIP sont établies.
Vert clignotant	Le port possède une adresse IP, mais aucune connexion CIP n'est établie.
Rouge	Le port a détecté que l'adresse IP assignée est déjà utilisée.
Rouge/vert clignotant	Le port exécute son auto-test à la mise sous tension.

Tableau 44 – Voyant d'état de la liaison Ethernet (LINK 1/LINK 2)

État	Description
Éteint	L'une des situations suivantes se produit : • Pas de liaison. • Le port a été désactivé par l'administrateur. • Le port a été désactivé parce qu'un défaut fugitif a été détecté sur l'anneau (LINK2).
Vert	L'une des situations suivantes se produit : • Une liaison à 100 Mbits/s (half ou full duplex) est présente et sans activité. • Une liaison à 10 Mbits/s (half ou full duplex) est présente et sans activité. • Le réseau annulaire fonctionne normalement et l'automate est en position de superviseur actif. • Le réseau annulaire a rencontré un défaut réseau partiel rare et l'automate est en position de superviseur actif.
Vert clignotant	Une liaison à 100 Mbits/s est présente et active.

Tableau 45 – Voyant d'état de l'activité de la carte SD (SD)

État	Description
Éteint	Aucune activité sur la carte SD.
Vert clignotant	L'automate lit le contenu de la carte SD ou y enregistre des données.
Rouge clignotant	La carte SD n'a pas de système de fichiers.

Tableau 46 – Voyant d'état SFTY RUN

État	Description
Éteint	La tâche de sécurité utilisateur ou les sorties de sécurité sont désactivées. L'automate est en mode Programmation ou Test, ou la tâche de sécurité est en défaut.
Vert	La tâche de sécurité utilisateur et les sorties de sécurité sont actives. La tâche 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. La tâche de sécurité est en cours d'exécution. La signature de tâche de sécurité est absente.

Tableau 47 – Voyant d'état SFTY TASK

État	Description
Éteint	Pas de partenariat établi.
Vert	L'état de l'automate de sécurité est satisfaisant. 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 satisfaisant. Le temps système coordonné (CST) n'est pas synchronisé.
Rouge	Le partenariat de sécurité a été perdu.
Rouge clignotant	La tâche de sécurité est inexploitable.

Tableau 48 – Voyant d'état SFTY LOCK

État	Description
Éteint	La tâche de sécurité est déverrouillée.
Vert	La tâche de sécurité est verrouillée.

Tableau 49 – Voyant d'état SFTY OK

État	Description
Éteint	Absence d'alimentation.
Vert	Le partenaire de sécurité est OK.
Vert clignotant	L'automate enregistre ou charge un projet dans ou à partir de la mémoire non volatile.
Rouge	L'automate a détecté un défaut majeur irrécupérable. Il a donc effacé le projet de sa mémoire.
Rouge clignotant	Le partenaire de sécurité interne nécessite une mise à jour de son firmware, ou une mise à jour de firmware est en cours.

Notes :

Changement de type d'automate

Les automates de sécurité ont des caractéristiques spécifiques et ne prennent pas en charge certaines fonctions standard. Il est par conséquent 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 votre projet. Changer le type de l'automate affecte en effet :

- fonctions prises en charge
- la configuration physique du projet, c'est-à-dire l'affectation du partenaire et des E/S de sécurité ;
- propriétés de l'automate
- les éléments du projet, comme les tâches, les programmes, les sous-programmes et les points ;
- les instructions complémentaires de sécurité.

Passage d'un automate standard à un automate de sécurité

Lors de la confirmation du passage d'un projet 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 :

- les composants de sécurité sont créés (c'est-à-dire la tâche de sécurité, le programme de sécurité, etc.) ;

  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 ;
- 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, le cas échéant.

Passage d'un automate de sécurité à un automate standard

Lors de la confirmation du passage d'un projet automate de sécurité à un automate standard, certains composants sont modifiés et d'autres supprimés, comme indiqué ci-dessous :

- les modules des 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 prend en charge des fonctions qui n'étaient pas disponibles dans l'automate de sécurité, ces nouvelles caractéristiques apparaissent dans la boîte de dialogue Controller Properties ;

  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 d'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.

Changement des types d'automate de sécurité

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 des E/S qui ne sont pas compatibles avec le nouvel automate sont supprimés.

EXEMPLE Les modules Compact I/O™ 1768 ne sont pas compatibles dans un système de commande Compact GuardLogix® 5370 (1769).

La représentation du partenaire de sécurité est mise à jour de façon à apparaître convenablement pour l'automate cible :

- Lors du changement à partir d'un automate Compact GuardLogix 5370 vers un automate GuardLogix 5570, le partenaire de sécurité est créé dans le logement *x* (logement principal + 1).
- Lors du changement vers un automate Compact GuardLogix 5370 depuis un automate GuardLogix 5570, le partenaire de sécurité est supprimé, car il est interne à l'automate Compact GuardLogix.

Numériques

A

B

C

D

E

F

G

I

K

L

M

N

V

Assistance Rockwell Automation

Les ressources suivantes sont à votre disposition pour vous assister.

Centre d'assistance technique	Articles de la base de connaissances, vidéos explicatives, foires aux questions, chats, forums utilisateur, et notification sur les mises à jour de produit.	https://rockwellautomation.custhelp.com/
Numéros de téléphone d'assistance technique locale	Trouvez le numéro de téléphone correspondant à votre pays.	http://www.rockwellautomation.com/global/support/get-support-now.page
Indicatifs de lignes directes	Trouvez l'indicatif de la ligne directe correspondant à votre produit. Utilisez l'indicatif pour être mis directement en contact avec un ingénieur d'assistance technique.	http://www.rockwellautomation.com/global/support/direct-dial.page
Bibliothèque documentaire	Notices d'installation, manuels, brochures et fiches techniques.	http://www.rockwellautomation.com/global/literature-library/overview.page
Centre de compatibilité et de téléchargement des produits (PCDC)	Trouvez comment vos produits interagissent, vérifiez les fonctionnalités et caractéristiques et recherchez le firmware associé.	http://www.rockwellautomation.com/global/support/pcdc.page

Commentaires

Vos commentaires nous aident à mieux vous servir. Si vous avez des suggestions sur la façon d'améliorer ce document, remplissez le formulaire « How Are We Doing? » à l'adresse http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.

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

www.rockwellautomation.com

Siège des activités « Power, Control and Information Solutions »

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

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

Publication 1769-UM022B-FR-P – Décembre 2016