



Ce manuel renvoie à l'article de la base de connaissances [Logix 5000 Controller Fault Codes](#) pour les codes de défaut ; téléchargez les feuilles de calcul maintenant pour un accès hors ligne.



# Automates ControlLogix 5580 et GuardLogix 5580

Série 1756



**Allen-Bradley**

by ROCKWELL AUTOMATION

## Informations importantes destinées à l'utilisateur

Lire ce document et les documents répertoriés dans la section Documentations connexes relatives 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 ELECTRIQUE** : L'étiquette ci-contre, placée sur l'équipement ou à l'intérieur (un centre de commande de moteurs, par ex.) indique qu'un arc électrique peut 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).

	<b>Préface</b>		
	Références.....	9	
	Sommaire des modifications .....	9	
	Présentation .....	9	
	Documentations connexes.....	10	
	<b>Chapitre 1</b>		
<b>Systèmes ControlLogix et GuardLogix</b>	Exigences minimales.....	13	
	Automates ControlLogix .....	14	
	Automates ControlLogix sans énergie stockée (NSE) .....	14	
	Automates ControlLogix-XT .....	14	
	Automates de process .....	15	
	Produits avec revêtement enrobant.....	15	
	Automates ControlLogix redondants .....	15	
	Système ControlLogix.....	16	
	Automate autonome avec E/S .....	16	
	Automates multiples dans un châssis .....	17	
	Dispositifs multiples connectés par l'intermédiaire de plusieurs réseaux.....	18	
	Système GuardLogix .....	19	
	Conception du système.....	22	
	Sécurité CIP.....	22	
	Systèmes d'automate sûr.....	23	
	Fonctionnalités de l'automate ControlLogix 5580 .....	23	
	Fonctionnalités de l'automate GuardLogix 5580.....	24	
	Fonctionnalités prises en charge par les automates GuardLogix 5380 via la tâche de sécurité.....	25	
		<b>Chapitre 2</b>	
	<b>Concept de sécurité des automates GuardLogix</b>	Capacité de sécurité fonctionnelle .....	27
Numéro de réseau de sécurité .....		28	
Signature de sécurité .....		28	
Distinction entre composants standard et de sécurité.....		29	
Capacités de flux de données de l'automate.....		30	
Terminologie de sécurité.....		31	
	<b>Chapitre 3</b>		
<b>Réseaux de communication</b>	Réseaux disponibles .....	33	
	Réseau de communication EtherNet/IP.....	34	
	Vitesses de liaison EtherNet/IP .....	34	
	Modules de communication EtherNet/IP .....	38	
	Communication de bus intermodules à Débit de données double (DDR) pour les automates ControlLogix.....	38	
	Réseau de communication ControlNet .....	39	
	Exemple de ControlNet GuardLogix.....	40	
	Modules ControlNet .....	41	
	Réseau de communication DeviceNet.....	42	
	Module passerelle et interfaces de connexion DeviceNet .....	43	
	Connexions sur les réseaux DeviceNet.....	43	
	Communication réseau Data Highway Plus (DH+) .....	43	
Communiquer sur un réseau DH+.....	44		

Communication avec les E/S décentralisées universelles (RIO).....	45
Communication sur un réseau d'E/S décentralisées universelles.....	47
Communication par Foundation Fieldbus .....	48
Communication HART.....	49

## Chapitre 4

### Connexion à un automate

Définir de l'adresse IP .....	51
Exigences .....	52
Autres méthodes pour définir l'adresse IP.....	52
Détection d'adresse IP dupliquée .....	52
Résolution d'adresse IP dupliquée.....	53
Adressage DNS .....	53
Mise à jour du firmware de l'automate .....	54
Directives de mise à niveau du firmware pour les automates de sécurité.....	54
Détermination du firmware d'automate requis .....	56
Obtention du firmware de l'automate .....	57
Utilisation du logiciel ControlFLASH Plus ou ControlFLASH pour mettre à jour le firmware .....	57
Utilisation d'AutoFlash pour mettre à jour le firmware .....	58

## Chapitre 5

### Commencer à utiliser l'automate

Création d'un projet d'application Logix Designer .....	61
Configuration supplémentaire pour un automate GuardLogix .....	62
Définir le niveau de sécurité pour un automate GuardLogix .....	62
Mots de passe pour verrouiller et déverrouiller la sécurité.....	64
Protection de la signature de sécurité en mode d'exécution .....	65
Attribuer le numéro de réseau de sécurité (SNN).....	66
Copier-coller un numéro de réseau de sécurité d'automate de sécurité.....	70
Passer en ligne avec l'automate .....	73
Utilisation de RSWho .....	73
Utilisation d'un chemin de communication récent .....	74
Considérations supplémentaires sur le passage en ligne avec un automate GuardLogix .....	75
Fonctionnalité Match Project to Controller .....	76
Correspondance des versions de firmware.....	76
État/défauts de sécurité .....	77
Signature de sécurité et état du verrouillage et du déverrouillage de la sécurité .....	77
Contrôles en vue du passage en ligne avec un automate GuardLogix.....	78
Téléchargement dans l'automate .....	79
Utilisation de Who Active .....	79
Utilisation du menu Controller Status (État de l'automate) .....	80
Considérations supplémentaires relatives au téléchargement dans un automate GuardLogix .....	80
Transfert depuis l'automate.....	82
Utilisation de Who Active .....	82
Utilisation du menu Controller Status .....	83
Considérations supplémentaire relatives au transfert depuis un automate GuardLogix .....	84
Choix du mode de fonctionnement de l'automate .....	85
Utilisation du sélecteur à clé pour changer le mode de fonctionnement.....	86
Utilisation de Logix Designer pour changer le mode de fonctionnement....	88
Bouton réinitialisation .....	89



	Réinitialisation de type 1 .....	90
	Réinitialisation de type 2 .....	91
	Réinitialisation du partenaire de sécurité .....	93
	<b>Chapitre 6</b>	
<b>Utilisation de la carte Secure Digital</b>	Considérations relatives au stockage et au transfert d'un projet de sécurité .....	97
	Stockage sur la carte SD .....	98
	Chargement depuis la carte SD .....	103
	Mise sous tension de l'automate .....	103
	Action initiée par l'utilisateur .....	104
	Autres tâches de la carte Secure Digital .....	106
	<b>Chapitre 7</b>	
<b>Gestion de la communication de l'automate</b>	Aperçu de la connexion .....	107
	Stations sur un réseau EtherNet/IP .....	108
	Dispositifs inclus dans le décompte des stations .....	108
	Dispositifs exclus du décompte des stations .....	109
	Interaction de la communication automate avec les données de commande .....	110
	Données produites et consommées (Verrouillage) .....	112
	Intervalle entre trames requises (RPI) de points multi-diffusés .....	113
	Envoi et réception de messages .....	114
	Déterminer s'il faut mettre en cache les connexions de message .....	115
	Interface de connexion .....	115
	Simple Network Management Protocol (SNMP) .....	116
	Utilisation d'un MSG CIP générique pour activer SNMP sur l'automate ..	116
	Utilisation d'un MSG CIP générique pour désactiver SNMP sur l'automate .....	118
	<b>Chapitre 8</b>	
<b>Modules d'E/S standard</b>	Choix des modules d'E/S ControlLogix .....	121
	Détrompage électronique .....	122
	Modules d'E/S locaux .....	123
	Ajout d'E/S locales à la configuration des E/S .....	123
	Modules d'E/S décentralisés .....	128
	Ajout d'E/S décentralisées sur le port Ethernet de l'automate .....	129
	Ajout d'E/S décentralisées à un module de communication local .....	131
	Ajout à la configuration d'E/S en étant en ligne .....	135
	Modules et dispositifs qui peuvent être ajoutés en ligne .....	136
	Détermination du moment où les données sont actualisées .....	136
	Organigramme de la mise à jour des données d'entrée .....	136
	Organigramme de la mise à jour des données de sortie .....	138
	<b>Chapitre 9</b>	
<b>Dispositifs d'E/S de sécurité</b>	Ajout de dispositifs d'E/S de sécurité .....	139
	Configuration des dispositifs d'E/S de sécurité .....	140
	Utilisation de la traduction d'adresses réseau (NAT) avec des dispositifs CIP Safety .....	142
	Définition du SNN d'un dispositif d'E/S de sécurité .....	143
	Changer le SNN d'un dispositif d'E/S de sécurité .....	144
	Copier et coller le SNN d'un dispositif d'E/S de sécurité .....	146
	Limite de temps de réponse de la connexion .....	148
	Signature de dispositif d'E/S de sécurité .....	149

Configuration via l'application Logix Designer .....	149
Propriétaire de configuration différent (connexion de données seules).....	150
Réinitialisation d'un dispositif d'E/S de sécurité en condition d'origine. ....	151
Format d'adresse d'un dispositif d'E/S de sécurité.....	152
Surveillance de l'état des dispositifs d'E/S de sécurité.....	152
Remplacement d'un dispositif d'E/S de sécurité.....	153
Propriété de configuration.....	153
Configuration de remplacement .....	154
Remplacement avec « Configure Only When No Safety Signature Exists » activé.....	155
Remplacement avec « Configure Always » activé .....	160

## Chapitre 10

### Développement d'applications standard

Éléments d'une application de commande.....	164
Tâches .....	165
Priorité des tâches .....	168
Programmes .....	168
Programmes planifiés et non planifiés .....	170
Sous-programmes .....	171
Paramètres et points locaux .....	172
Paramètres de programme.....	173
Langages de programmation .....	173
Instructions complémentaires.....	174
Propriétés étendues .....	175
Accès à l'objet Module à partir d'une instruction complémentaire .....	176
Surveillance de l'état de l'automate .....	177
Surveillance des connexions d'E/S .....	178
Déterminer si le délai d'attente de la communication d'E/S a expiré.....	178
Déterminer si une communication avec un module d'E/S particulier est en dépassement du temps d'attente.....	179
Gestion automatique des défauts de connexion de module d'E/S.....	179
Exemples de projets d'automate.....	180

## Chapitre 11

### Développement d'applications de sécurité

Tâche de sécurité.....	182
Période de la tâche de sécurité .....	183
Exécution de la tâche de sécurité .....	184
Programmes de sécurité.....	184
Sous-programmes de sécurité.....	185
Instructions complémentaires de sécurité .....	185
Points de sécurité .....	186
Types de données valides .....	186
Accès .....	187
Paramètres de programme .....	188
Points de sécurité produits/consommés .....	188
Configuration du SNN pour une connexion à un automate de sécurité homologue .....	189
Production d'un point de sécurité.....	193
Consommation de points de données de sécurité.....	194
Mappage de point de sécurité .....	197
Restrictions .....	197
Création de paires de points mappées.....	198
Contrôle de l'état du mappage des points .....	199

Protection de l'application de sécurité . . . . .	200
Verrouillage de sécurité de l'automate . . . . .	200
Définition des mots de passe pour verrouiller ou déverrouiller la sécurité . .	202
Générer une signature de sécurité . . . . .	203
Restrictions de programmation. . . . .	205
Surveillance de l'état de la sécurité . . . . .	206
Visualisation de l'état via la barre en ligne . . . . .	206
Visualisation de l'état via l'onglet Safety . . . . .	208
Surveillance des connexions de sécurité . . . . .	209
Utilisation de l'état . . . . .	210
Défauts de sécurité . . . . .	212
Défauts d'automate irrécupérables . . . . .	212
Défauts de sécurité irrécupérables dans l'application de sécurité. . . . .	212
Défauts récupérables dans l'application de sécurité. . . . .	213
Affichage des défauts. . . . .	214
Codes de défaut . . . . .	214
Développement d'un sous-programme de défaut pour les applications de sécurité . . . . .	215
Utilisation des instructions GSV/SSV dans une application de sécurité . . . . .	216

## Chapitre 12

### Développement d'applications sécurisées

Fonctionnalité de sécurité d'automate . . . . .	218
Fonctionnalités de sécurité au niveau système . . . . .	219
Fonctionnalités de sécurité spécifiques à l'automate. . . . .	221
Vérification de la mise en œuvre de la sécurité . . . . .	223
Configuration du logement sécurisé . . . . .	224
Configuration des défauts majeurs définissables par l'utilisateur . . . . .	225
Création d'un sous-programme de défaut . . . . .	225
Configuration du programme pour utiliser le sous-programme de défaut . .	226
Saut au sous-programme de défaut . . . . .	226
Protection de la source et de l'exécution basée sur licence . . . . .	227
Activation de protection sous licence . . . . .	228
Configurer Modifier la détection . . . . .	230
Journal d'audit de l'automate. . . . .	231
Désactivation du port Ethernet . . . . .	232
Désactivation du port Ethernet sous l'onglet Port Configuration . . . . .	233
Désactivation du port Ethernet avec une instruction MSG . . . . .	234
Désactivation des ports CIP Security . . . . .	236
Désactivation du port USB . . . . .	239
Désactivation de la carte SD . . . . .	241
Désactivation de l'afficheur d'état à 4 caractères. . . . .	243
Désactivation de toutes les catégories de messages . . . . .	243
Désactivation de catégories individuelles de messages . . . . .	245
Désactivation des pages Internet de l'automate . . . . .	247
Application Studio 5000 Logix Designer, version 33.00.00 ou ultérieure . .	247
Application Studio 5000 Logix Designer version 32.00.00 ou antérieure . .	247
Réglages par défaut des pages Internet de l'automate . . . . .	248
Utilisation d'un MSG CIP Generic pour désactiver les pages Internet de l'automate. . . . .	249
Utilisation d'un MSG CIP Generic pour activer les pages Internet de l'automate. . . . .	251

	<b>Chapitre 13</b>	
<b>Développement d'applications de mouvement</b>	Présentation de la commande de mouvement.....	254
	Programmation de la commande d'axe.....	255
	Obtenir les informations d'axe.....	257
	<b>Chapitre 14</b>	
<b>Dépannage de l'automate</b>	Diagnostics automatiques.....	259
	Considérations relatives aux diagnostics de perte de communication.....	260
	Diagnostics de l'automate avec Logix Designer.....	261
	Onglet Propriétés du module d'E/S.....	262
	Notification dans l'éditeur de point.....	263
	Activation du défaut majeur sur l'automate.....	264
	Diagnostics de port.....	265
	Synchronisation temporelle évoluée.....	267
	Diagnostics de l'automate avec le logiciel de type Linx.....	270
	Pages Internet de l'automate.....	271
	Page d'accueil Internet.....	273
	Page Internet des défauts.....	274
	Page Internet des tâches.....	275
	Page Internet Parcourir le châssis.....	276
	<b>Annexe A</b>	
<b>Voyants d'état</b>	Afficheur et voyants d'état.....	278
	Messages d'état général.....	279
	Messages d'état de GuardLogix.....	281
	Messages d'état du partenaire de sécurité.....	281
	Messages de défaut.....	282
	Messages de défaut majeur.....	283
	Codes de défaut d'E/S.....	283
	Voyants d'état d'automate.....	284
	Voyant RUN.....	284
	Voyant FORCE.....	284
	Voyant SD.....	285
	Voyant OK.....	285
	Voyant OK du partenaire de sécurité.....	286
	Voyants EtherNet/IP.....	286
	Surveillance thermique et comportement en défaut thermique.....	287
	<b>Annexe B</b>	
<b>Changement de type d'automate</b>	Passage d'un automate standard à un automate de sécurité.....	289
	Passage d'un automate de sécurité à un automate standard.....	290
	Changement du type d'automate de sécurité.....	290
	<b>Index</b> .....	291

## Références

Cette publication concerne les PC pour panneau 6300P

Références standard:	1756-L81E, 1756-L81EK, 1756-L82E, 1756-L82EK, 1756-L83E, 1756-L83EK, 1756-L84E, 1756-L84EK, 1756-L85E, 1756-L85EK
Références sans stockage d'énergie (NSE) :	1756-L81E-NSE, 1756-L82E-NSE, 1756-L83E-NSE, 1756-L84E-NSE, 1756-L85E-NSE
Références ControlLogix-XT :	1756-L81EXT, 1756-L82EXT, 1756-L83EXT, 1756-L84EXT, 1756-L85EXT
Références de process :	1756-L81EP, 1756-L83EP, 1756-L85EP
Références GuardLogix	1756-L81ES, 1756-L81ESK, 1756-L82ES, 1756-L82ESK, 1756-L83ES, 1756-L83ESK, 1756-L84ES, 1756-L84ESK, 1756-L8SP, 1756-L8SPK

## Sommaire des modifications

Ce manuel contient des informations nouvelles et mises à jour telles qu'indiquées dans le tableau suivant.

Rubrique	Page
Ajout des automates ControlLogix NSE, ControlLogix-XT et ControlLogix Process.	Tout au long du manuel
Actualisation de la définition de signature de sécurité.	28
Actualisation du comportement des voyants d'état de l'automate lors du chargement d'un projet à partir de la carte SD.	100
Ajout Interface de connexion	115
Ajout Diagnostics automatiques.	259
Ajout Considérations relatives aux diagnostics de perte de communication.	260

## Présentation

Ce manuel explique comment concevoir un système, exploiter un système basé sur les automates ControlLogix® ou GuardLogix® et développer des applications.

Vous devez être formé et expérimenté dans la création, l'exploitation et la maintenance des systèmes de sécurité.

Pour toute information sur les exigences du niveau d'intégrité de sécurité (SIL) et du niveau de performance (PL) ainsi que celles d'une application de sécurité, consultez la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».



## Documentations connexes

Ces documents contiennent des informations complémentaires relatives aux produits connexes de Rockwell Automation.

**Tableau 1 - Documentations connexes**

Documentation	Description	
Installation matérielle	Automates ControlLogix 5580, Notice d'installation, publication <a href="#">1756-IN043</a>	Fournit des instructions d'installation des automates ControlLogix 5580.
	Automates GuardLogix 5580 Notice d'installation, publication <a href="#">1756-IN048</a>	Fournit des instructions d'installation des automates GuardLogix 5580.
	Alimentation ControlLogix Notice d'installation, publication <a href="#">1756-ING19</a>	Décrit comment installer des alimentations standard.
	ControlLogix Redundant Power Supply Installation Instructions, publication <a href="#">1756-ING20</a>	Décrit comment installer des alimentations redondantes.
	Châssis ControlLogix Notice d'installation, publication <a href="#">1756-ING21</a>	Décrit comment installer des châssis ControlLogix.
	Replacement door labels for the 1756 I/O modules, publication <a href="#">IASIMP-SP021</a>	Contient des étiquettes de porte pour les modules d'E/S 1756 disponibles à l'impression.
Données techniques	1756 ControlLogix Controllers Technical Data, publication <a href="#">1756-TD001</a>	Caractéristiques techniques des automates ControlLogix.
	1756 ControlLogix I/O Specifications Technical Data, publication <a href="#">1756-TD002</a>	Présente les caractéristiques des modules d'E/S ControlLogix.
	1756 ControlLogix Communications Modules Specifications Technical Data, publication <a href="#">1756-TD003</a>	Fournit les caractéristiques des modules de communication ControlLogix.
	1756 ControlLogix Integrated Motion Modules Specifications Technical Data, publication <a href="#">1756-TD004</a>	Fournit les caractéristiques des modules de commande d'axe intégrée ControlLogix.
	1756 ControlLogix Power Supplies Specifications Technical Data, publication <a href="#">1756-TD005</a>	Fournit les caractéristiques des alimentations ControlLogix.
	1756 ControlLogix Chassis Specifications Technical Data, publication <a href="#">1756-TD006</a>	Fournit les caractéristiques des châssis ControlLogix.
Réseaux (ControlNet, DeviceNet, EtherNet/IP)	EtherNet/IP Network Devices User Manual, publication <a href="#">ENET-UM006</a>	Décrit comment configurer et utiliser des dispositifs EtherNet/IP™ avec un automate Logix 5000™ et communiquer avec divers dispositifs sur le réseau Ethernet.
	ControlNet Network Configuration User Manual, publication <a href="#">CNET-UM001</a>	Fournit des informations à propos des réseaux ControlNet®.
	DeviceNet Media Design Installation Guide, publication <a href="#">DNET-UM072</a>	Fournit des informations à propos des réseaux DeviceNet®.
Impératifs d'application de sécurité	Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité, publication <a href="#">1756-RM012</a>	Contient des exigences précises pour atteindre et maintenir le niveau SIL 2/PLd et SIL 3/PLe avec le système automate GuardLogix 5580, en utilisant l'application Studio 5000 Logix Designer®.
Mouvement	Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, publication <a href="#">MOTION-UM003</a>	Indique comment concevoir votre système ControlLogix pour les applications de commande d'axe intégrée sur réseau EtherNet/IP.
	Mouvement intégré sur le réseau EtherNet/IP Manuel de référence, publication <a href="#">MOTION-RM003</a>	Informations détaillées sur les modes et attributs de commande d'axe pour la commande de mouvement intégrée sur les réseaux EtherNet/IP.
	Système de coordonnées des mouvements Manuel utilisateur, publication <a href="#">MOTION-UM002</a>	Détaille comment créer et configurer l'application d'un système de mouvements coordonnés.
	SERCOS and Analog Motion Configuration and Startup User Manual, publication <a href="#">MOTION-UM001</a>	Fournit des détails sur la configuration d'un système pour une application de mouvement Sercos.

Tableau 1 - Documentations connexes (suite)

Documentation		Description
Considérations relatives à la conception	Logix 5000 Controllers Design Considerations Reference Manual, publication <a href="#">1756-RM094</a>	Fournit des informations pour aider à concevoir et planifier les systèmes Logix 5000.
	High Availability System Reference Manual, publication <a href="#">HIGHAV-RM002</a>	Fournit des informations pour aider à concevoir et planifier les systèmes à haute disponibilité.
	Ethernet Design Considerations Reference Manual, publication <a href="#">ENET-RM002</a>	Fournit des informations supplémentaires à propos de la conception du réseau pour votre système.
	FOUNDATION Fieldbus Design Considerations Reference Manual, <a href="#">PROCES-RM005</a>	Ce document fournit des choix de conception et les meilleures pratiques pour la mise en œuvre d'un réseau FOUNDATION Fieldbus avec les dispositifs de liaison 1788-EN2FFR ou 1788-CN2FFR.
	Using Logix 5000 Controllers as Masters or Slaves on Modbus Application Solution, publication <a href="#">CIG-AP129</a>	Informations complémentaires sur l'utilisation des exemples programmes Modbus.
Tâches et procédures de programmation	Logix 5000 Controllers Common Procedures Programming Manual, publication <a href="#">1756-PM001</a>	Fournit l'accès à l'ensemble des manuels de programmation des automates Logix 5000. Les manuels traitent de sujets tels que la gestion des fichiers de projet, l'organisation des points, le programme logique, les sous-programmes de test, la gestion des défauts, et ainsi de suite.
	Logix 5000 Controllers General Instructions Reference Manual, publication <a href="#">1756-RM003</a>	Décrit les instructions de programmation disponibles pour les projets d'application Logix Designer.
	Jeu des instructions d'application de la sécurité GuardLogix Manuel de référence, publication <a href="#">1756-RM095</a>	Fournit des informations sur le jeu d'instructions pour applications de sécurité GuardLogix.
Homologation des produits	Site Internet sur les certifications de produit, <a href="https://www.rockwellautomation.com/global/certification/overview.page">https://www.rockwellautomation.com/global/certification/overview.page</a> .	Fournit des déclarations de conformité, des certificats et d'autres détails relatifs à l'homologation.

Vous pouvez visualiser ou télécharger les publications sur le site [rok.auto/literature](http://rok.auto/literature).

**Notes :**

## Systèmes ControlLogix et GuardLogix

Ce chapitre décrit les fonctions et fonctionnalités qui sont associées aux automates CompactLogix® 5580 et Compact GuardLogix® 5580.

Rubrique	Page
Exigences minimales	13
Système ControlLogix	16
Système GuardLogix	19
Conception du système	22
Sécurité CIP	22
Systèmes d'automate sûr	23
Fonctionnalités de l'automate ControlLogix 5580	23

### Exigences minimales

#### S'applique à ces automates :

ControlLogix 5580

GuardLogix 5580

Les automates ont ces exigences minimales.

- Châssis ControlLogix Série C (le châssis série B fonctionne avec une plage de température déclassée)
- Alimentation de châssis ControlLogix
- logiciel de programmation

Système	Référence	Studio 5000 Logix Designer® <sup>(2)</sup>
ControlLogix	1756-L83E, 1756-L83EK <sup>(1)</sup> , 1756-L85E, 1756-L85EK	Version 28.00.00 ou ultérieure
	1756-L81E, 1756-L81EK, 1756-L82E, 1756-L82EK, 1756-L84E, 1756-L84EK	Version 29.00.00 ou ultérieure
	1756-L81E-NSE, 1756-L82E-NSE, 1756-L83E-NSE, 1756-L84E-NSE, 1756-L85E-NSE, 1756-L81EXT, 1756-L82EXT, 1756-L83EXT, 1756-L84EXT, 1756-L85EXT, 1756-L81EP, 1756-L83EP, 1756-L85EP	Version 31.00.00 ou ultérieure
GuardLogix	1756-L81ES, 1756-L81ESK, 1756-L82ES, 1756-L82ESK, 1756-L83ES, 1756-L83ESK, 1756-L84ES, 1756-L84ESK, 1756-L8SP, 1756-L8SPK	Version 31.00.00 ou ultérieure <sup>(3)</sup>

(1) Les références suivies de la lettre « K » indiquent une option de revêtement enrobant.

(2) Pour le logiciel de communication compatible basé sur Linx, et le logiciel ControlFLASH Plus™ et ControlFLASH™, voir le [Centre de compatibilité des produits et de téléchargement \(PCDC\)](#).

(3) Studio 5000 Logix Designer Professional, Full Edition, ou un éditeur de sécurité GuardLogix sous licence distincte doit être présent sur le poste de travail afin de modifier un projet GuardLogix.

**IMPORTANT** Si votre application exige des connexions de sécurité ou une logique de sécurité, vous devez utiliser un automate GuardLogix 5580.

## Automates ControlLogix

Les automates sont disponibles avec différentes fonctionnalités en fonction de votre application.

### Automates ControlLogix sans énergie stockée (NSE)

L'automate NSE est destiné à être utilisé dans des applications nécessitant que l'automate installé épuise son énergie résiduelle stockée à des niveaux spécifiques avant de le transporter dans ou hors de votre application.

L'énergie résiduelle stockée de l'automate NSE s'épuise à 400  $\mu$ J ou moins en 40 secondes.



**AVERTISSEMENT** : Si votre application nécessite que l'automate NSE épuise son énergie résiduelle stockée jusqu'à un niveau de 400  $\mu$ J ou moins avant de le retirer ou l'insérer dans l'application, suivez les étapes ci-dessous avant de procéder à la dépose de l'automate.

1. Coupez l'alimentation du châssis.

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

2. Attendre au moins **40 secondes** pour que l'énergie résiduelle diminue jusqu'à un niveau de 400  $\mu$ J ou moins avant de retirer l'automate.

Aucune indication visuelle n'indique que ce délai de 40 secondes est écoulé.

**Vous devez donc contrôler cette durée vous-même.**

---

**IMPORTANT** L'horloge temps réel (RTC) ne conserve pas son heure et sa date lorsque l'alimentation est coupée.

---

Certaines applications exigent que l'automate installé épuise son énergie résiduelle stockée à des niveaux spécifiques avant de le transporter dans ou hors de votre application. Cette exigence peut inclure d'autres dispositifs qui nécessitent également un temps d'attente avant de les retirer. Consultez la documentation de ces produits pour plus d'informations.

### Automates ControlLogix-XT

Les automates ControlLogix-XT™ fonctionnent de la même façon que les automates ControlLogix traditionnels, avec une plage de températures étendue, et sont dotés des mêmes fonctionnalités que les automates ControlLogix standard.

Les automates ControlLogix-XT sont dotés d'un revêtement enrobant pour ajouter une couche de protection lorsqu'ils sont exposés à des environnements difficiles et corrosifs. Si le système ControlLogix standard peut résister à des températures de 0 à 60 °C (33 à 140 °F), le système ControlLogix-XT peut, quant à lui, résister à des températures de -25 à +70 °C (-13 à 158 °F).



## Automates de process

L'automate de process est une extension de la famille d'automates Logix 5000 qui se concentre sur le contrôle de process à l'échelle de l'usine. L'automate de process est configuré avec un modèle de tâches de process par défaut et des instructions de process PlantPAx dédiées optimisées pour les applications de process et qui améliorent les efforts de conception et de déploiement.

Le matériel de l'automate de process ControlLogix est également recouvert d'un revêtement enrobant pour ajouter une couche de protection lorsqu'il est exposé à des environnements difficiles et corrosifs, et peut être utilisé dans des températures extrêmes de -25 à +70 °C (-13 à +158 °F) lorsqu'il est déployé comme partie d'un système Logix-XT.

## Produits avec revêtement enrobant



**ATTENTION** : Les produits avec revêtement enrobant sont livrés avec des caches de protection pour port installés afin de fournir une protection contre les environnements corrosifs. Afin de respecter la certification pour atmosphère corrosive du produit, des caches de port doivent être installés dans les ports inutilisés à tout moment pendant le stockage et le fonctionnement. Si un accès temporaire est nécessaire, les caches peuvent être retirés, mais doivent être replacés dès que celui-ci est terminé.

## Automates ControlLogix redondants

Vous pouvez utiliser les automates ControlLogix 5580 dans des applications redondantes avec l'application Studio 5000 Logix Designer, version 33.00.00 ou ultérieure.

Pour plus d'informations, reportez-vous aux publications suivantes :

- High Availability System Reference Manual, publication [HIGHAV-RM002](#)
- ControlLogix 5580 Redundant Controller User Manual, publication [1756-UM015](#)

## Système ControlLogix

S'applique à ces automates :

ControlLogix 5580

---

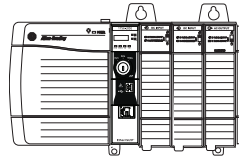
Le système ControlLogix est basé sur un châssis, ce qui offre des options pour configurer une variété de capacités de communications et d'E/S. Les automates ControlLogix prennent en charge plusieurs langages de programmation qui permettent le contrôle séquentiel, de process, de mouvement et de variateur.

Diverses options de configuration du système sont décrites dans les sections suivantes.

### Automate autonome avec E/S

L'une des configurations ControlLogix les plus simples consiste en un automate autonome avec des E/S, montés dans un châssis.

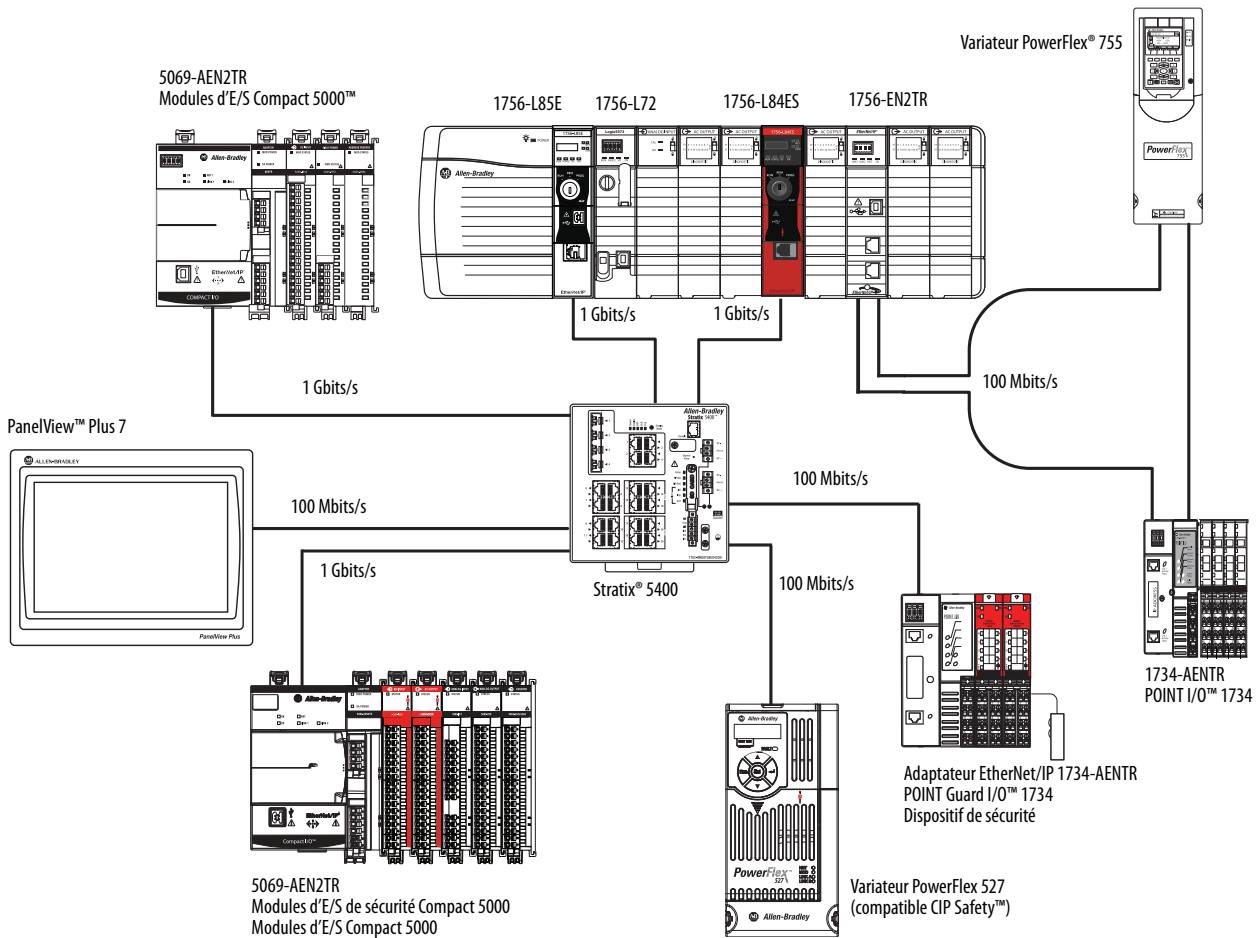
Figure 1 - Automate autonome avec E/S



## Automates multiples dans un châssis

Vous pouvez utiliser plusieurs automates dans un châssis ControlLogix. Cet exemple montre un automate ControlLogix 5580 (logement 0) connecté directement au réseau EtherNet/IP™, un automate ControlLogix 5570 (logement 1) connecté au réseau via un module 1756-EN2TR (logement 7) et un automate GuardLogix 5580 dans une configuration SIL 2/PLD (logement 5) connectée directement au réseau EtherNet/IP.

**Figure 2 - Automates multiples dans un châssis**



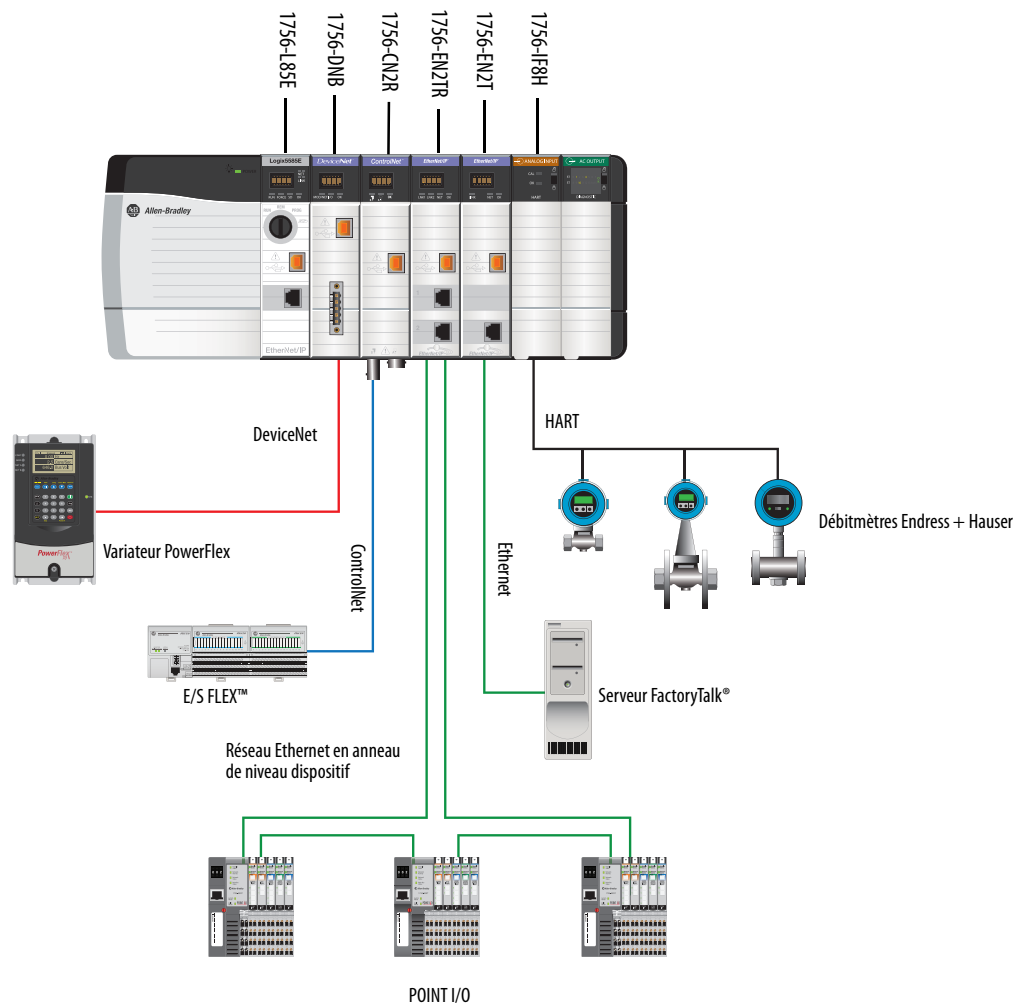
**IMPORTANT** Vous ne pouvez pas passer par le port Ethernet (avant) d'un autre automate pour ajouter des E/S décentralisées.

## Dispositifs multiples connectés par l'intermédiaire de plusieurs réseaux

Dans certaines applications, des périphériques divers peuvent être connectés au châssis ControlLogix par l'intermédiaire de plusieurs réseaux. Par exemple, un système peut être connecté à :

- des E/S distribuées par l'intermédiaire d'un réseau Ethernet ;
- un variateur PowerFlex au moyen d'un réseau DeviceNet® ;
- des E/S distribuées via un réseau ControlNet® ;
- des débitmètres en utilisant une connexion HART.

Figure 3 - Dispositifs multiples connectés par l'intermédiaire de plusieurs réseaux



## Système GuardLogix

---

### S'applique à ces automates :

---

GuardLogix 5580

---

Le système GuardLogix peut communiquer avec des dispositifs d'E/S de sécurité via CIP Safety sur un réseau EtherNet/IP (modules Guard I/O™, variateurs de sécurité intégrés, composants de sécurité intégrés).

Pour un automate GuardLogix, vous pouvez vous connecter aux E/S standard locales sur le bus intermodules via des tâches standard tout en vous connectant aux E/S de sécurité décentralisées via le port EtherNet/IP.

Le système GuardLogix prend en charge les applications de sécurité jusqu'à SIL 3 et PLe.

- Sans partenaire de sécurité installé, vous pouvez atteindre les performances SIL 2/PLd (Catégorie 3) avec l'utilisation de la tâche de sécurité et des E/S de sécurité.
- Avec l'utilisation de la tâche de sécurité et l'installation d'un partenaire de sécurité, vous pouvez atteindre la protection SIL 3/PLe (Catégorie 4).

---

**IMPORTANT** Pour la tâche de sécurité, les automates GuardLogix n'acceptent que le diagramme à relais.

Pour les tâches standard, les automates GuardLogix prennent en charge :

- Diagramme à relais (LD)
  - Texte structuré (ST)
  - Diagramme de bloc fonctionnel (FBD)
  - Graphe de fonctionnement séquentiel (SFC)
- 

Pour les applications de sécurité SIL 3, le système GuardLogix est composé d'un automate GuardLogix principal et d'un partenaire de sécurité qui fonctionnent ensemble dans une architecture 1oo2.

- L'automate principal est le processeur qui exécute les fonctions standard et de sécurité. Il communique avec le partenaire de sécurité pour les fonctions liées à la sécurité dans le système de commande GuardLogix.
- Le partenaire de sécurité est un coprocesseur qui fournit un deuxième canal isolé pour les fonctions liées à la sécurité dans le système. Le partenaire de sécurité ne comporte pas de sélecteur à clé, ni de port de communication. L'automate principal contrôle le mode de fonctionnement du partenaire de sécurité.
- Le partenaire de sécurité doit être installé dans le logement immédiatement à droite de l'automate principal. Les révisions majeures et mineures du firmware de l'automate principal et du partenaire de sécurité doivent correspondre parfaitement pour établir le partenariat de commande nécessaire aux applications de sécurité.

Pour toute information sur les exigences du niveau d'intégration de sécurité (SIL) et du niveau de performance (PL) ainsi que celles d'une application de sécurité, consultez la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

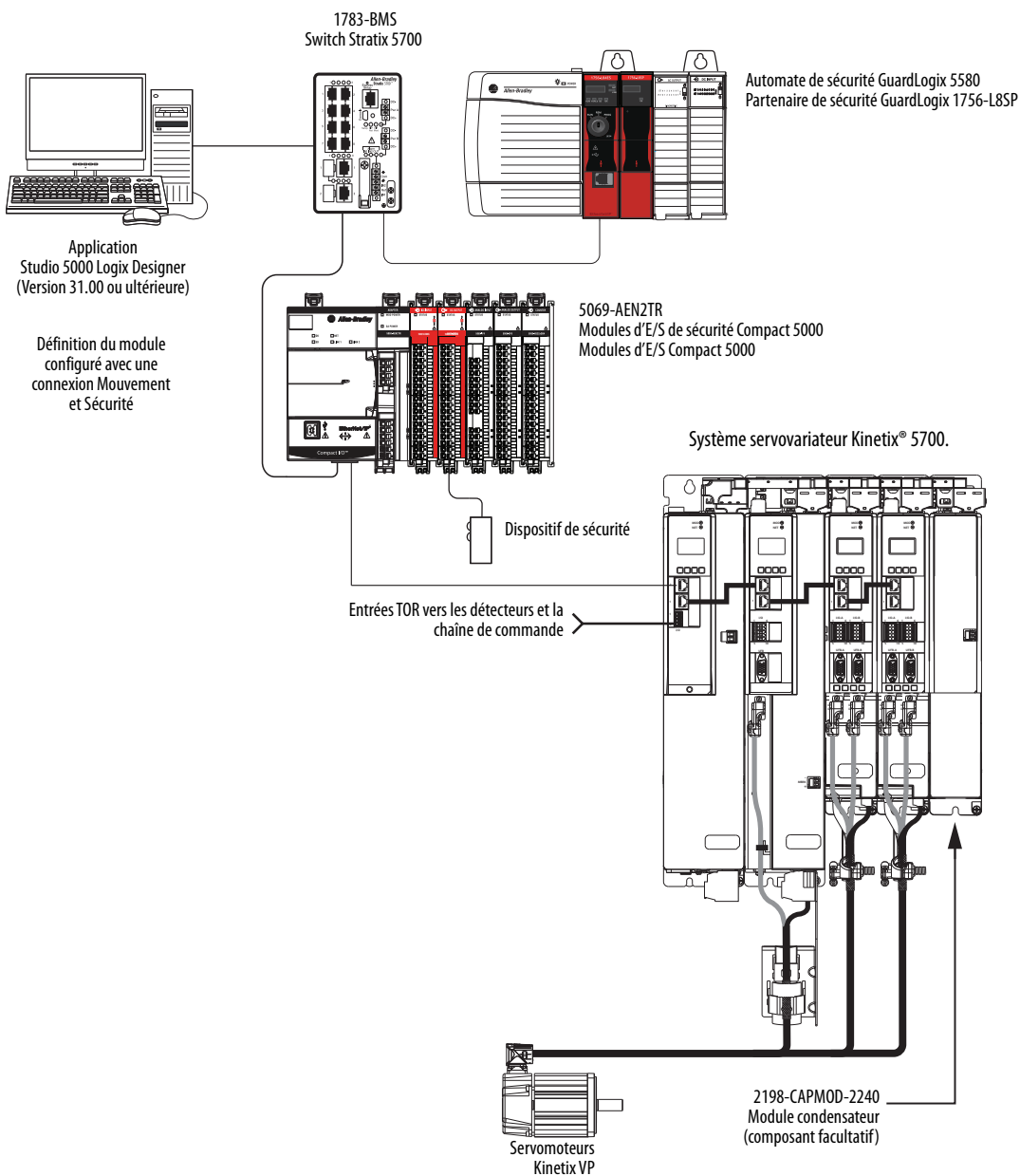


### GuardLogix avec E/S de sécurité et des variateurs de sécurité intégrés

Dans cet exemple, un seul automate de sécurité GuardLogix établit les connexions de mouvement et de sécurité.

**IMPORTANT** Si un seul automate est utilisé dans une application avec des connexions de commande d'axe et de sécurité, ce doit être un automate de sécurité tel que l'automate GuardLogix 5580.

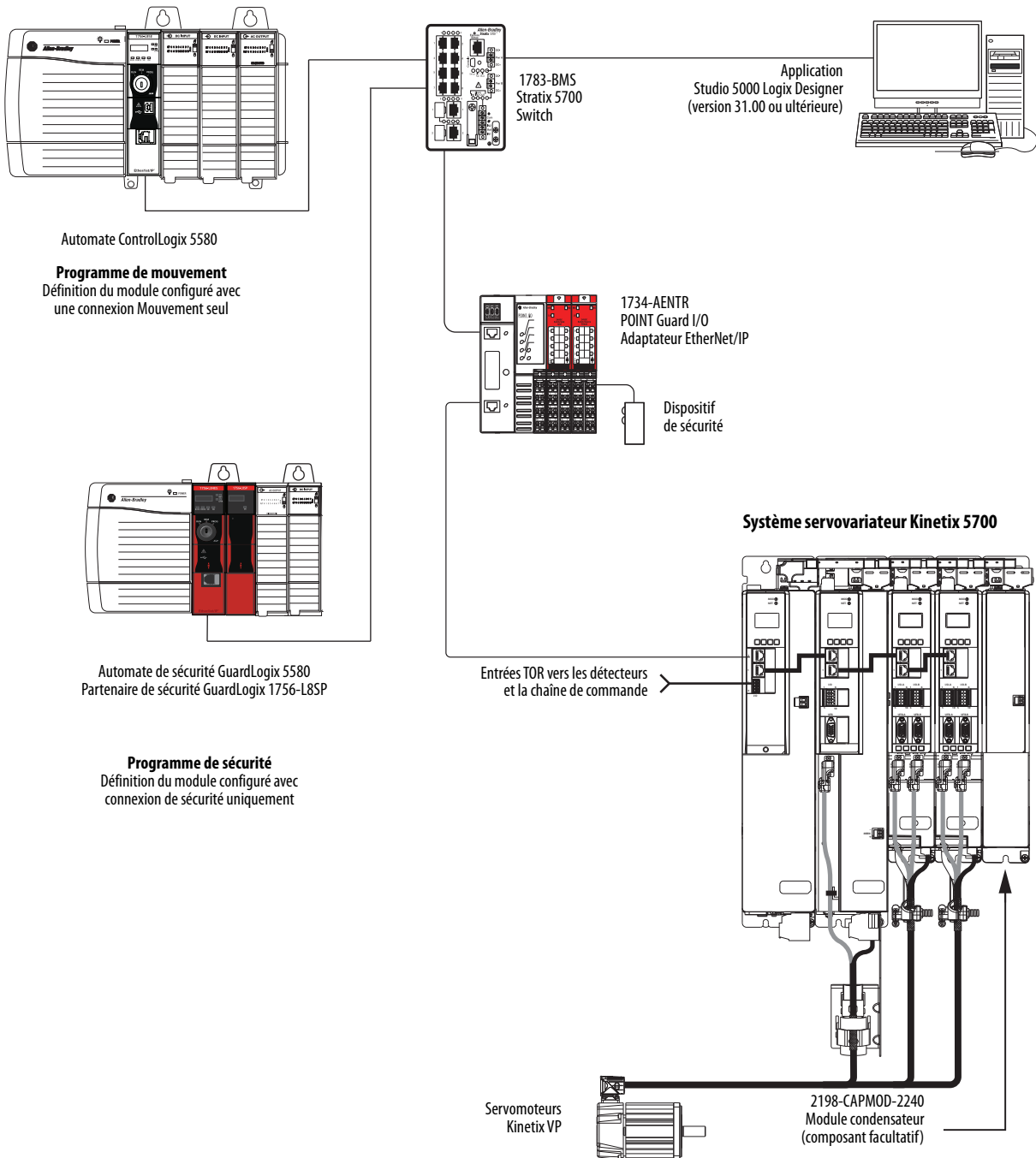
Figure 4 - Configuration du mouvement et de la sécurité (un seul automate)



Dans cet exemple, un automate standard établit la connexion exclusive de mouvement et un automate de sécurité GuardLogix 5580 distinct établit la connexion exclusive de sécurité.

**IMPORTANT** Si deux automates sont utilisés dans une application avec des connexions Motion-only et Safety-only, la connexion Safety-only doit être un automate GuardLogix tandis que la connexion Motion-only doit être un automate standard ou de sécurité.

**Figure 5 - Configuration du mouvement et de la sécurité (multi-automates)**



## Conception du système

---

### S'applique à ces automates :

---

ControlLogix 5580

---

GuardLogix 5580

---

Lorsque vous concevez un système, plusieurs types de composants système doivent être pris en compte pour votre application.

- Dispositifs d'E/S
- Axes et variateurs de commande de mouvement
- Modules de communication
- Automates
- Châssis
- Alimentations
- Application Studio 5000 Logix Designer

De plus, les systèmes de sécurité ont également des composants à prendre en compte :

- Automate de sécurité
- Partenaire de sécurité (pour les applications SIL 3/PLe)
- E/S de sécurité
- Dispositifs de sécurité

Pour plus d'informations sur la conception et la sélection des composants de votre système, consultez :

- 1756 ControlLogix Controllers Technical Data, publication [1756-TD001](#)
- 1756 ControlLogix I/O Specifications Technical Data, publication [1756-TD002](#)
- Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité, publication [1756-RM012](#)

## Sécurité CIP

CIP Security™ est une méthode de communication standard libre de source qui permet une transmission de données sécurisée sur un réseau EtherNet/IP.

Le transport de données sécurisé est utilisé entre certains dispositifs connectés pour aider à protéger les dispositifs contre les menaces posées par des utilisateurs non autorisés avec une intention malveillante.

Rockwell Automation utilise les produits suivants pour mettre en œuvre CIP Security :

- FactoryTalk Policy Manager
- FactoryTalk Linx
- Studio 5000® Design Environment
- Les produits Rockwell Automation compatibles CIP Security, par exemple les produits décrits dans cette publication.

Pour plus d'informations sur CIP Security, y compris les produits prenant en charge CIP Security, consultez la publication [SECURE-AT001](#), « CIP Security Application Technique ».

## Systèmes d'automate sûr

L'automate ControlLogix 5580, firmware révision 32, prend en charge les exigences de CEI-62443-4-2 SL 1. Pour les fonctionnalités de sécurité et la configuration système requise, voir [Développement d'applications sécurisées, page 217](#).

## Fonctionnalités de l'automate ControlLogix 5580

Ce tableau répertorie les fonctionnalités système, de communication et de programmation disponibles avec les automates ControlLogix 5580.

S'applique à ces automates :

ControlLogix 5580

**Tableau 1 - Fonctionnalités de l'automate ControlLogix 5580**

Fonctionnalité	1756-L81E, 1756-L81EK, 1756-L81E-NSE, 1756-L81EXT, 1756-L81EP	1756-L82E, 1756-L82EK, 1756-L82E-NSE, 1756-L82EXT	1756-L83E, 1756-L83EK, 1756-L83E-NSE, 1756-L83EXT, 1756-L83EP	1756-L84E, 1756-L84EK, 1756-L84E-NSE, 1756-L84EXT	1756-L85E, 1756-L85EK, 1756-L85E-NSE, 1756-L85EXT, 1756-L85EP
Mémoire utilisateur	3 Mo	5 Mo	10 Mo	20 Mo	40 Mo
Stations EtherNet/IP prises en charge, max. <sup>(1)</sup>	60 stations <sup>(4)</sup> 100 stations <sup>(5)</sup>	80 stations <sup>(4)</sup> 175 stations <sup>(5)</sup>	100 stations <sup>(3)</sup> 250 stations <sup>(5)</sup>	150 stations <sup>(4)</sup> 250 stations <sup>(5)</sup>	300 stations <sup>(6)</sup>
Ports de communication	1 - Port USB, 2.0 pleine vitesse, Type B 1 - Port EtherNet/IP, 10 Mbits/s, 100 Mbits/s, 1 Gbits/s				
Options de communication	<ul style="list-style-type: none"> <li>• EtherNet/IP</li> <li>• ControlNet</li> <li>• DeviceNet</li> <li>• Data Highway Plus™</li> <li>• E/S décentralisées</li> <li>• SynchLink™</li> <li>• Réseaux de procédé et de dispositif tiers</li> </ul>				
Tâches automate	<ul style="list-style-type: none"> <li>• 32 tâches</li> <li>• 1 000 programmes/tâche</li> <li>• Tâches d'événement : tous déclencheurs d'événement</li> </ul>				
Commande d'axe intégrée	<ul style="list-style-type: none"> <li>• Commande d'axe intégrée en réseau EtherNet/IP</li> <li>• Interface Sercos<sup>(2)</sup></li> <li>• Options analogiques<sup>(2)</sup>: <ul style="list-style-type: none"> <li>– Entrée codeur</li> <li>– Entrée capteur de déplacement linéaire (LDT)</li> <li>– Entrée interface série synchrone (SSI)</li> </ul> </li> </ul>				
Langages de programmation	<ul style="list-style-type: none"> <li>• Diagramme à relais (LD)</li> <li>• Texte structuré (ST)</li> <li>• Diagramme de bloc fonctionnel (FBD)</li> <li>• Graphe de fonctionnement séquentiel (SFC)</li> </ul>				

(1) Une station est un périphérique EtherNet/IP que vous ajoutez directement à la configuration des E/S, et qui est prise en compte dans le nombre limite de stations de l'automate. Pour plus d'informations sur les stations EtherNet/IP, consultez la publication [1756-UM543](#), « ControlLogix 5580 Controllers User Manual ».

(2) Avec l'application Studio 5000 Logix Designer, version 31 ou ultérieure.

(3) Avec Studio 5000 Logix Designer Application Versions 28 et 29.

(4) Avec l'application Studio 5000 Logix Designer, version 29.

(5) Avec l'application Studio 5000 Logix Designer, version 30 ou ultérieure.

(6) Avec l'application Studio 5000 Logix Designer, version 28 ou ultérieure.

## Fonctionnalités de l'automate GuardLogix 5580

S'applique à ces automates :

GuardLogix 5580

Ce tableau répertorie les fonctionnalités système, de communication et de programmation disponibles avec les automates GuardLogix 5580.

**Tableau 2 - Fonctionnalités de l'automate GuardLogix 5580**

Fonctionnalité	1756-L81ES	1756-L82ES	1756-L83ES	1756-L84ES
Mémoire utilisateur	3 Mo	5 Mo	10 Mo	20 Mo
Mémoire de sécurité	1,5 Mo	2,5 Mo	5 Mo	6 Mo
Stations EtherNet/IP prises en charge, max.	100	175	250	250
Ports de communication	1 - Port USB, 2.0 pleine vitesse, Type B 1 - Port EtherNet/IP : vitesses de liaison 10 Mbps/s, 100 Mbps/s, 1 Gbits/s			
Options de communication	<ul style="list-style-type: none"> <li>EtherNet/IP (1756-EWEB ne peut pas être utilisé pour les connexions de sécurité)</li> <li>Prise en charge de la traduction d'adresses réseau (NAT)</li> <li>ControlNet</li> <li>DeviceNet</li> <li>Data Highway Plus</li> <li>E/S décentralisées</li> <li>SynchLink</li> <li>Réseaux de procédé et de dispositif tiers</li> </ul>			
Tâches automate	<ul style="list-style-type: none"> <li>31 tâches standard, 1 tâche de sécurité</li> <li>1 000 programmes/tâche</li> <li>Tâches d'événement : tous déclencheurs d'événement</li> </ul>			
Commande d'axe intégrée	La commande d'axe intégrée est prise en charge uniquement dans une tâche standard. <ul style="list-style-type: none"> <li>Commande d'axe intégrée en réseau EtherNet/IP</li> <li>Interface Sercos</li> <li>Options analogiques :                             <ul style="list-style-type: none"> <li>Entrée codeur</li> <li>Entrée capteur de déplacement linéaire (LDT)</li> <li>Entrée série synchrone (SSI)</li> </ul> </li> </ul>			
Langages de programmation	<ul style="list-style-type: none"> <li>Pour la tâche de sécurité, les automates GuardLogix n'acceptent que le diagramme à relais.</li> <li>Pour les tâches standard, les automates GuardLogix prennent en charge :                             <ul style="list-style-type: none"> <li>Diagramme à relais (LD)</li> <li>Texte structuré (ST)</li> <li>Diagramme de bloc fonctionnel (FBD)</li> <li>Graphe de fonctionnement séquentiel (SFC)</li> </ul> </li> </ul>			
Sécurité intégrée	<ul style="list-style-type: none"> <li>Sécurité intégrée sur le réseau EtherNet/IP (variateurs Kinetix, variateurs PowerFlex, composants de sécurité)</li> <li>E/S de sécurité décentralisées et de commande (sur les réseaux EtherNet/IP et DeviceNet uniquement)</li> <li>Données de point de sécurité produites et consommées</li> </ul>			
Fonctionnalités de l'automate	<ul style="list-style-type: none"> <li>Contrôle d'accès aux données</li> <li>Firmware Supervisor</li> <li>Carte Secure Digital (SD)</li> <li>Connexions de sécurité</li> <li>Connexions standard</li> </ul>			



## Fonctionnalités prises en charge par les automates GuardLogix 5380 via la tâche de sécurité

Dans l'application Logix Designer, de version 31 ou ultérieure, la tâche de sécurité prend en charge un sous-ensemble de fonctionnalités qui sont elles-mêmes prises en charge dans la tâche standard, comme indiqué dans le tableau ci-après.

Fonctionnalité	Application Studio 5000 Logix Designer Version 31 ou ultérieure	
	Tâche de sécurité	Tâche standard
Instructions complémentaires	X	X
Alarmes et événements basés sur des instructions	—	X
Alarmes basées sur des points	—	X
Journal automate	X	X
Tâches événementielles <sup>(1)</sup>	—	X
Diagrammes de blocs fonctionnels (FBD)	—	X
Commande d'axe intégrée	X <sup>(2)</sup>	X
Mouvement analogique	—	X
Mouvement Sercos	—	X
Instructions de sécurité de variateur	X	—
Diagramme à relais (LD)	X	X
Commutation de langues	X	X
Protection de la source basée sur licence	—	X
Importation et exportation en ligne d'éléments de programme	—	X
Exportation en ligne d'éléments de programme	X	X
Sous-programmes en graphe de fonctionnement séquentiel (SFC)	—	X
Texte structuré (ST)	—	X

(1) Bien que la tâche de sécurité ne puisse pas être une tâche événementielle, les tâches événementielles classiques peuvent être déclenchées par l'utilisation d'une instruction événementielle dans la tâche de sécurité.

(2) Limitée à l'utilisation des instructions de sécurité de variateur avec les variateurs Kinetix 5700 ERS4.

---

**IMPORTANT** **Considérations relatives à la sécurité**

Les automates GuardLogix 5380 peuvent produire des points standard en envoi individuel (Unicast) ou multi-diffusion (Multicast), mais ils ne peuvent produire des points de sécurité qu'en envoi individuel.

Les automates peuvent consommer les points de sécurité en envoi individuel ou multi-diffusion.

Lorsque vous configurez un point de sécurité produit, vous ne pouvez que configurer des options de connexion en envoi individuel. Logix Designer ne vous permet pas de configurer des options de connexion en multi-diffusion.

Lorsque vous configurez un point consommé, il vous faut tenir compte des capacités du producteur :

- Si le producteur dans l'arborescence des E/S de cet automate est un automate GuardLogix 5580 ou Compact GuardLogix 5380, le point de sécurité consommé doit être configuré en envoi individuel.
  - Si le producteur dans l'arborescence des E/S de cet automate est un automate GuardLogix 5570 ou GuardLogix 5560 ou Compact GuardLogix 5370, le point de sécurité consommé peut être configuré en envoi individuel ou en multi-diffusion.
  - Les automates GuardLogix 5580 ne produisent pas de points de sécurité pour les automates GuardLogix 5570 (firmware révision 30 et versions antérieures) dans le même châssis, car les automates GuardLogix 5580 peuvent uniquement produire des points de sécurité en envoi individuel et les automates GuardLogix 5570 (firmware révision 30 et versions antérieures) ne peuvent pas configurer les points consommés en envoi individuel. Cette restriction ne s'applique pas sur EtherNet/IP, car les points consommés peuvent être configurés pour l'envoi individuel.
-

# Concept de sécurité des automates GuardLogix

Rubrique	Page
Capacité de sécurité fonctionnelle	27
Numéro de réseau de sécurité	28
Signature de sécurité	28
Distinction entre composants standard et de sécurité	29
Capacités de flux de données de l'automate	30
Terminologie de sécurité	31

## Capacité de sécurité fonctionnelle

### Concerné ces automates :

GuardLogix 5580

Le système automate GuardLogix® 5580 est certifié pour une utilisation dans des applications de sécurité jusqu'à SIL 2/PLd et SIL 3/PLe inclus, lorsque l'état hors tension est l'état sûr.

Pour les applications de sécurité SIL 3/PLe, le système GuardLogix est composé d'un automate principal et d'un partenaire de sécurité, qui fonctionnent ensemble dans une architecture 1oo2.

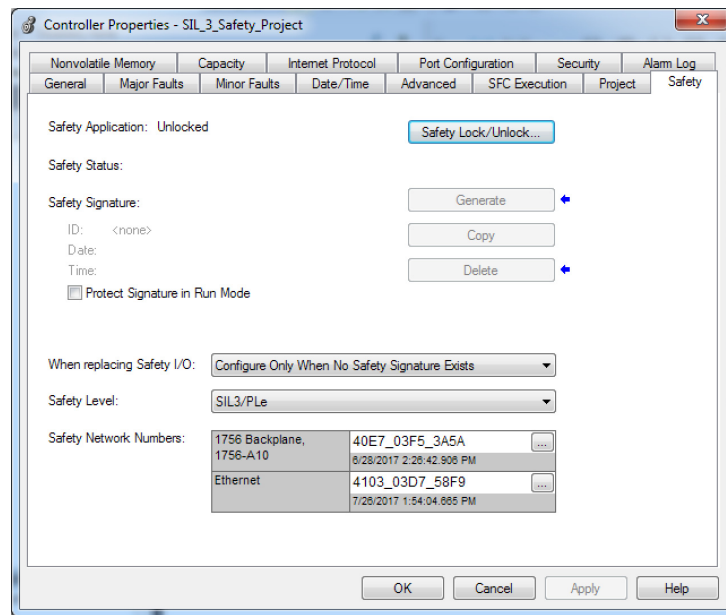
Pour les exigences relatives aux systèmes de sécurité SIL 2/PLd et SIL 3/PLe, y compris les intervalles de test de validation fonctionnelle, les temps de réponse du système et les calculs de PFD/PFH, reportez-vous à la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

Vous devez lire, comprendre et respecter pleinement ces exigences avant d'exploiter un système de sécurité GuardLogix SIL 2/PLd ou SIL 3/PLe.

## Numéro de réseau de sécurité

Le numéro de réseau de sécurité (SNN) identifie de manière unique les sous-réseaux CIP Safety™ au sein d'un réseau de sécurité routable. La combinaison SNN + Adresse de station identifie de manière unique chaque port CIP Safety de chaque dispositif du réseau de sécurité routable.

Les automates GuardLogix 5580 nécessitent deux numéros de réseau de sécurité : un pour le port Ethernet et un pour le fond de panier.



Pour une explication du numéro de réseau de sécurité, consultez la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

Pour savoir comment attribuer le SNN, reportez-vous à [Attribuer le numéro de réseau de sécurité \(SNN\), page 66](#).

## Signature de sécurité

La signature de sécurité se compose d'un numéro d'identification (ID) et d'un horodatage (date et heure). L'ID de signature de sécurité s'applique à l'ensemble de la partie sécurité de l'automate et identifie de manière unique chaque projet, y compris son programme, ses données et sa configuration.

Le système GuardLogix utilise la signature de sécurité pour authentifier l'intégrité du projet et vous permettre de vérifier que le bon projet est téléchargé dans l'automate cible. La possibilité de créer, d'enregistrer et de vérifier la signature de sécurité est une partie obligatoire du processus de développement de l'application de sécurité.

La signature de sécurité doit être présente pour fonctionner en tant qu'automate de sécurité SIL 2/PLd ou SIL 3/PLe.

Pour plus d'informations, reportez-vous à [Générer une signature de sécurité, page 203](#).

## **Distinction entre composants standard et de sécurité**

Les logements de châssis d'un système GuardLogix qui ne sont pas utilisés par la fonction de sécurité peuvent être occupés par d'autres modules ControlLogix® répondant aux Directives Basse Tension et CEM. Consultez la page Homologation des produits Rockwell Automation (<http://www.rockwellautomation.com/global/certification/overview.page?>) pour trouver le certificat CE de la gamme de produits ControlLogix et déterminer les modules qui sont homologués.

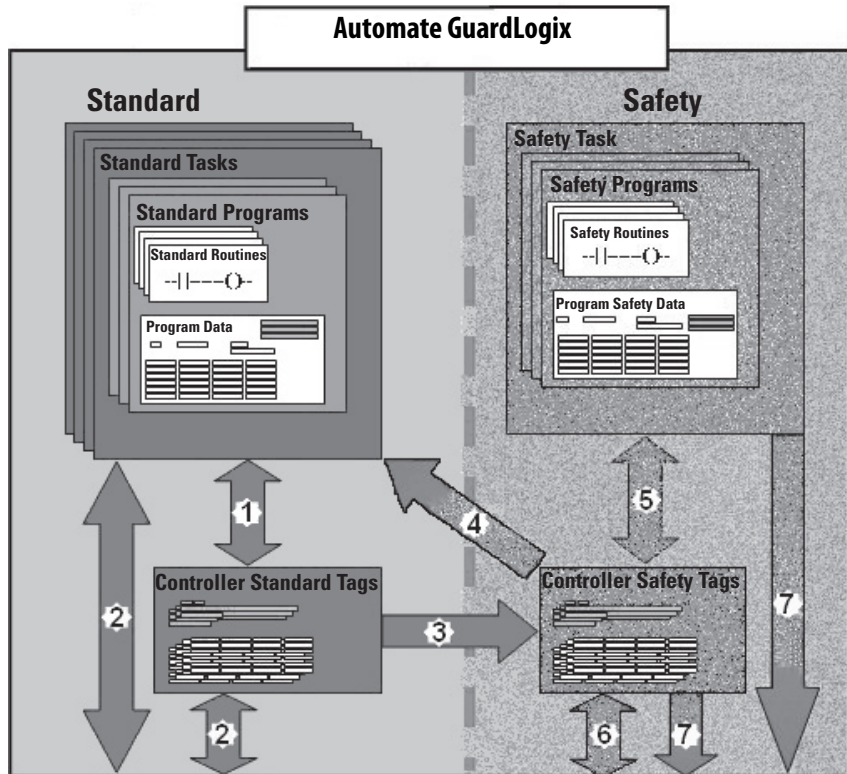
Vous devez créer et documenter les parties standard et de sécurité de l'application en les distinguant de façon claire, logique et visible. Pour favoriser cette distinction, l'application Studio 5000 Logix Designer® comporte des icônes d'identification de la sécurité permettant de reconnaître la tâche 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.

## Capacités de flux de données de l'automate

Cette illustration explique les capacités de flux de données standard et de sécurité de l'automate GuardLogix.

Figure 6 - Capacités de flux de données



N°	Description
1	Les points et le programme standard se comportent comme ils le font dans un automate ControlLogix standard.
2	Les données de points standard, qu'ils soient en accès programme ou automate, peuvent être échangées avec des IHM externes, des PC et d'autres automates.
3	Les automates GuardLogix 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. C'est la seule manière d'obtenir des données de points standard dans la tâche de sécurité. Le programme de sécurité dans la tâche de sécurité ne peut ni lire ni écrire le point standard qui est la source du transfert de données de mappage des points ; il peut uniquement renvoyer à la destination du point de sécurité du mappage. Par contre, il peut lire et écrire ce point de sécurité.  <div style="display: flex; align-items: center;">  <p><b>ATTENTION :</b> Les données de point mappé ne doivent pas être utilisées pour commander directement une sortie SIL 2/PLd ou SIL 3/PLe.</p> </div>
4	Les points de sécurité en accès automate peuvent être lus directement par un programme standard.
5	Les points de sécurité peuvent être lus ou écrits par un programme de sécurité.
6	Les points de sécurité peuvent être échangés par l'intermédiaire de réseaux Ethernet ou ControlNet® entre des automates de sécurité, notamment les automates GuardLogix 1756 et 5069.
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. Les dispositifs externes ne peuvent pas écrire dans des points de sécurité (que l'automate soit protégé ou non). Une fois lues, ces données sont considérées comme standard et non plus comme données de type SIL 3/PLe.

## Terminologie de sécurité

Vous trouverez dans ce tableau les termes de sécurité utilisés dans ce manuel.

**Tableau 3 - Termes et définitions de sécurité**

Abréviation	Signification	Définition
1oo1	Un sur Un	Identifie l'architecture d'automate électronique programmable. 1oo1 correspond à un système monovoie.
1oo2	One Out of Two (un sur deux)	Identifie l'architecture d'automate électronique programmable. 1oo2 correspond à un système bivoie.
CIP Safety	Common Industrial Protocol – Safety Certified	Version certifiée SIL 3/PLe du protocole CIP™.
DC	Couverture des diagnostics	Rapport entre le taux de défaillances détectées et le taux de défaillances totales.
PF	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	Classification de sécurité ISO 13849-1.
SIL	Niveau d'intégrité de sécurité	Niveau relatif de réduction des risques fourni par une fonction de sécurité ou spécifiant un niveau cible de réduction des risques.
SIL CL	SIL Claim Limit (limite SIL revendiquée)	Le niveau d'intégrité de sécurité (SIL) maximum réalisable.
SNN	Numéro de réseau de sécurité	Numéro unique qui identifie une section d'un réseau de sécurité.
UNID	Unique Node ID (identifiant, ou référence, unique de station)	La référence de station unique regroupe un numéro de réseau de sécurité (SNN) et l'adresse de station de l'équipement sur le réseau.

**Notes :**



## Réseaux de communication

Plusieurs réseaux de communication sont disponibles.

Rubrique	Page
Réseaux disponibles	33
Réseau de communication EtherNet/IP	34
Communication de bus intermodules à Débit de données double (DDR) pour les automates ControlLogix	38
Réseau de communication ControlNet	39
Réseau de communication DeviceNet	42
Communication réseau Data Highway Plus (DH+)	43
Communication avec les E/S décentralisées universelles (RIO)	45
Communication par Foundation Fieldbus	48
Communication HART	49

### Réseaux disponibles

Le [tableau 4](#) décrit les fonctionnalités d'application typiques utilisées avec les systèmes ControlLogix® et GuardLogix®, et répertorie les réseaux disponibles pour prendre en charge de telles fonctionnalités d'application.

**Tableau 4 - Applications et réseaux pris en charge**

Fonctionnalités d'application	Réseaux pris en charge par ControlLogix et GuardLogix pour les communications standard	Réseaux pris en charge par GuardLogix pour les communications CIP Safety™
Commande d'axe intégrée <sup>(1)</sup>	EtherNet/IP™	EtherNet/IP
Synchronisation temporelle;	EtherNet/IP	EtherNet/IP
Commande d'E/S distribuées	<ul style="list-style-type: none"> <li>• EtherNet/IP</li> <li>• DeviceNet®</li> <li>• ControlNet®</li> <li>• Foundation Fieldbus</li> <li>• HART</li> <li>• RIO universel</li> </ul>	La synchronisation temporelle n'utilise pas le protocole de sécurité.
Production/consommation de données entre automates	<ul style="list-style-type: none"> <li>• EtherNet/IP</li> <li>• ControlNet</li> </ul>	<ul style="list-style-type: none"> <li>• EtherNet/IP</li> <li>• ControlNet</li> </ul>
Messagerie vers/depuis d'autres périphériques, y compris accès à l'automate via l'application Studio 5000 Logix Designer®	<ul style="list-style-type: none"> <li>• EtherNet/IP</li> <li>• ControlNet</li> <li>• DeviceNet (seulement vers les périphériques)</li> <li>• Data Highway Plus™ (DH+™)</li> <li>• DH-485</li> </ul>	La messagerie n'utilise pas le protocole de sécurité.

(1) Les automates prennent également en charge les interfaces de commande d'axe analogique et Sercos. Pour plus d'informations, Consultez [Développement d'applications de mouvement, page 253](#)

Pour plus d'informations sur l'utilisation des messages, reportez-vous aux publications suivantes :

- Configuration du réseau EtherNet/IP Manuel utilisateur, publication [ENET-UM001](#)
- Modules de communication EtherNet/IP dans les systèmes de commande Logix5000 Manuel utilisateur, publication [ENET-UM004](#)

Pour plus d'informations sur la conception des réseaux, reportez-vous aux publications suivantes :

- Ethernet Design Considerations Reference Manual, publication [ENET-RM002](#).
- ControlNet Network Configuration User Manual, publication [CNET-UM001](#)
- DeviceNet Media Design Installation Guide, publication [DNET-UM072](#)
- FOUNDATION Fieldbus Design Considerations Reference Manual, publication [PROCES-RM005](#)

## Réseau de communication EtherNet/IP

---

### S'applique à ces automates :

---

ControlLogix 5580

---

GuardLogix 5580

---

Le réseau EtherNet/IP offre un ensemble complet de services de commande, de configuration et de collecte des données. Pour cela, il utilise le protocole CIP™ (Common Industrial Protocol) en surcouche sur les protocoles Internet standard tels que TCP/IP et UDP. Cette combinaison de normes très répandues apporte les capacités nécessaires pour pouvoir gérer à la fois l'échange de données à caractère informatique et les applications de commande.

---

**IMPORTANT** Vous ne pouvez pas passer par le port Ethernet (avant) d'un autre automate pour ajouter des E/S décentralisées.

---

## Vitesses de liaison EtherNet/IP

L'automate prend en charge les vitesses de liaison 10 Mbits/s, 100 Mbits/s et 1 Gbits/s.

Les performances du réseau dans un système d'automate sont optimales si la vitesse de liaison de 1 Gbits/s est utilisée. Cependant, les anciens dispositifs Ethernet ne prennent pas en charge la vitesse de liaison de 1 Gbits/s. Ils prennent plutôt en charge une vitesse maximale de 100 Mbits/s.

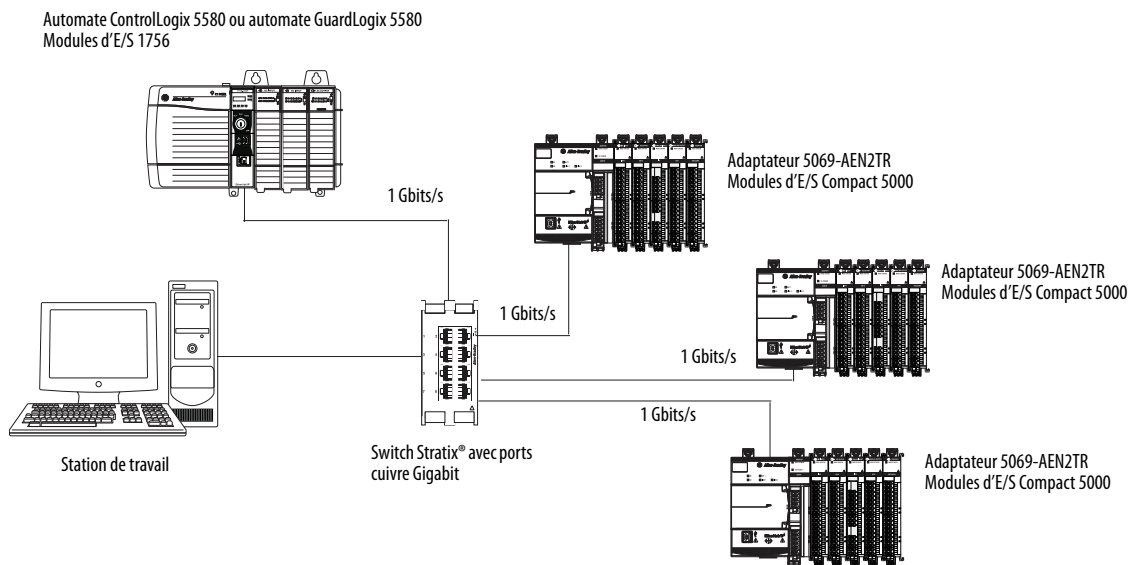
La différence de vitesses de liaison maximales a un impact sur votre système d'automate et, dans certaines applications, vous empêche d'utiliser les vitesses de liaison de 1 Gbits/s sur un automate.

Lorsque vous concevez un système d'automate et envisagez d'utiliser la vitesse de transmission de 1 Gbits/s sur l'automate, n'oubliez pas ce qui suit :

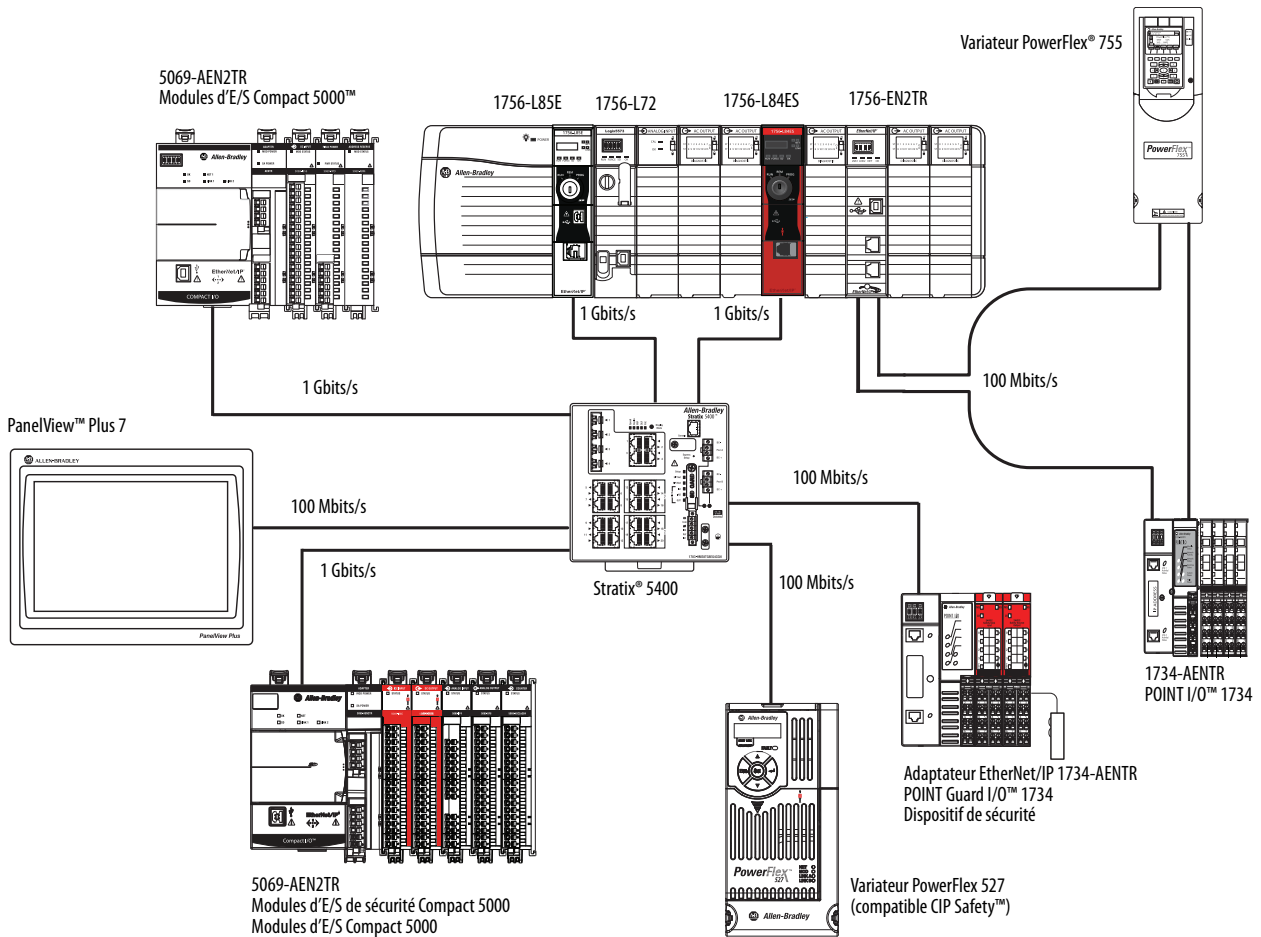
- Vous pouvez utiliser la vitesse de liaison de 1 Gbits/s sur le port de l'automate lorsque tous les dispositifs du réseau prennent en charge 1 Gbits/s, par exemple, des adaptateurs 5069-AEN2TR avec des modules d'E/S Compact 5000™.

Lorsque des switchs sont utilisés dans une topologie en étoile, configurez les ports de l'automate pour utiliser l'auto négociation.

**Figure 7 - Exemple de réseau EtherNet/IP 1 Gbits/s**



- Vous pouvez utiliser la vitesse de liaison de 1 Gbits/s sur le port de l'automate lorsque certains dispositifs du réseau prennent en charge une vitesse de liaison maximale de 100 Mbit/s. Toutefois, dans ce cas, l'automate doit être connecté à ces dispositifs au moyen d'un switch administrable.



- Ne mélangez pas des vitesses de liaison de 1 Gbits/s et 100 Mbits/s au sein d'un même réseau DLR en anneau ou linéaire.

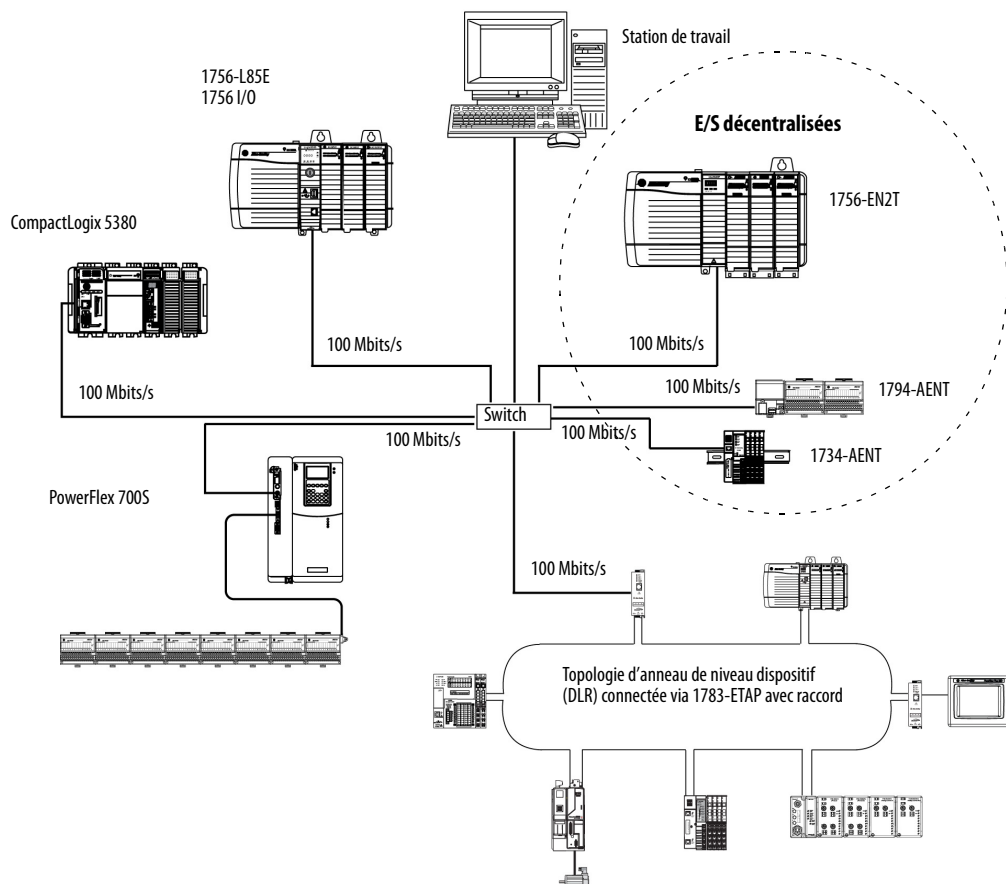
**IMPORTANT** Autrement dit, n'utilisez pas de vitesses de liaison réseau différentes sur les ports de dispositifs d'un même réseau EtherNet/IP sans un switch administrable.

Si vous utilisez au moins deux de ces composants **avec un ancien dispositif Ethernet dans une topologie en anneau ou linéaire**, réglez tous les dispositifs sur une vitesse fixe de 100 Mbit/s et en duplex intégral :

- Automates ControlLogix 5580/GuardLogix 5580
- Automates CompactLogix™ 5380
- Adaptateurs de communications 5069
- Adaptateurs de communication 5094

Cela peut aider à empêcher les rafales de trafic et l'inversion du trafic du DLR en raison d'une rupture d'anneau de causer des problèmes.

**Figure 8 - Exemple de réseau EtherNet/IP à 100 Mbits/s avec un switch non administrable**



## Modules de communication EtherNet/IP

Pour les communications réseau EtherNet/IP, vous avez le choix entre plusieurs modules. Le [tableau 5](#) répertorie les modules et leurs fonctionnalités principales.

Pour plus d'informations, consultez la publication [1756-TD003](#), « 1756 ControlLogix Communication Modules Specifications Technical Data ».

**Tableau 5 - Modules de communication EtherNet/IP**

Module	est utilisé pour
1756-L81E, 1756-L81EK <sup>(1)</sup> , 1756-L81E-NSE, 1756-L81EP, 1756-L81ES, 1756-L81ESK, 1756-L81EXT, 1756-L82E, 1756-L82EK, 1756-L82E-NSE, 1756-L82ES, 1756-L82ESK, 1756-L82EXT, 1756-L83E, 1756-L83EK, 1756-L83E-NSE, 1756-L83EP, 1756-L83ES, 1756-L83ESK, 1756-L83EXT, 1756-L84E, 1756-L84EK, 1756-L84E-NSE, 1756-L84ES, 1756-L84ESK, 1756-L84EXT, 1756-L85E, 1756-L85EK, 1756-L85E-NSE, 1756-L85EP, 1756-L85EXT	<ul style="list-style-type: none"> <li>Connecte directement l'automate à un réseau EtherNet/IP sans nécessiter de module passerelle.</li> <li>Communique avec des modules d'E/S décentralisés et d'autres dispositifs EtherNet/IP.</li> <li>Relie les messages sur un réseau EtherNet/IP.</li> <li>Prend en charge les vitesses de liaison 10 Mbits/s, 100 Mbits/s et 1 Gbits/s.</li> </ul>
1756-EN2T, 1756-EN2TK, 1756-EN2TXT	<ul style="list-style-type: none"> <li>Connecte directement l'automate à un réseau EtherNet/IP sans nécessiter de module passerelle.</li> <li>Communique avec des modules d'E/S décentralisés et d'autres dispositifs EtherNet/IP.</li> <li>Transmet les messages sur un réseau EtherNet/IP.</li> <li>Le 1756-EN2TXT fonctionne dans des environnements extrêmes avec des températures de -25 à 70 °C.</li> </ul>
1756-EN2TR, 1756-EN2TRK, 1756-EN2TRXT	<ul style="list-style-type: none"> <li>Exécute les mêmes fonctions que les modules 1756-EN2TR.</li> <li>Prend en charge la communication sur une topologie d'anneau pour un anneau de niveau dispositif (DLR) réseau en anneau à tolérance de défaut unique.</li> <li>Prend également en charge une topologie linéaire.</li> <li>Le 1756EN2TRXT fonctionne dans des environnements extrêmes avec des températures de -25 à 70 °C.</li> </ul>
1756-EN2F, 1756-EN2FK	<ul style="list-style-type: none"> <li>Exécute les mêmes fonctions que les modules 1756-EN2TR.</li> <li>Raccordement d'une liaison fibre au module au moyen d'un connecteur LC pour fibre optique.</li> </ul>
1756-EN2TP, 1756-EN2TPK	<ul style="list-style-type: none"> <li>Exécute les mêmes fonctions que les modules 1756-EN2TR.</li> <li>Prend en charge le protocole de redondance en parallèle</li> </ul>
1756-EN3TR, 1756-EN3TRK	<ul style="list-style-type: none"> <li>Exécute les mêmes fonctions que les modules 1756-EN2TR.</li> <li>Commande de mouvement intégrée de grande capacité en réseau EtherNet/IP</li> <li>Prise en charge de 128 axes de mouvement au maximum.</li> </ul>
1756-ENBT, 1756-ENBTK	<ul style="list-style-type: none"> <li>Connecte directement l'automate à un réseau EtherNet/IP sans nécessiter de module passerelle.</li> <li>Communique avec des modules d'E/S décentralisés et d'autres dispositifs EtherNet/IP.</li> <li>Transmet les messages sur un réseau EtherNet/IP.</li> </ul>
1756-EN2TSC	<ul style="list-style-type: none"> <li>Exécute les mêmes fonctions qu'un module 1756-ENBT, mais avec deux fois plus de capacité pour des applications plus exigeantes.</li> <li>Sécurise l'accès à un système de commande depuis le réseau de l'usine</li> </ul>
1756-EWEB, 1756-EWEBK	<ul style="list-style-type: none"> <li>Exécute les mêmes fonctions que les modules 1756-EN2TR.</li> <li>Fournit un accès à distance aux points d'un automate ControlLogix local par l'intermédiaire d'un navigateur Internet.</li> </ul> <p>Ce module ne permet pas la gestion des E/S ni des points produits/consommés. Ce module ne prend pas en charge CIP Safety</p>

(1) Les références suivies de la lettre « K » indiquent une option de revêtement enrobant.

## Communication de bus intermodules à Débit de données double (DDR) pour les automates ControlLogix

Les automates offrent des capacités de débit de données double sur le bus intermodules ControlLogix.

## Réseau de communication ControlNet

### S'applique à ces automates :

ControlLogix 5580

GuardLogix 5580

Le réseau ControlNet est un réseau de commande en temps réel, permettant le transport à grande vitesse d'E/S à temps critique, ainsi que des données de verrouillage et de messagerie. Ceci s'applique notamment au transfert et au chargement des programmes et des informations de configuration sur un même support physique de liaison.

Les réseaux ControlNet offrent un déterminisme et une répétabilité élevée. Ils ne sont pas affectés par les connexions ou les déconnexions des périphériques du réseau. Cette qualité se traduit par un fonctionnement fiable, synchronisé et coordonné en temps réel.

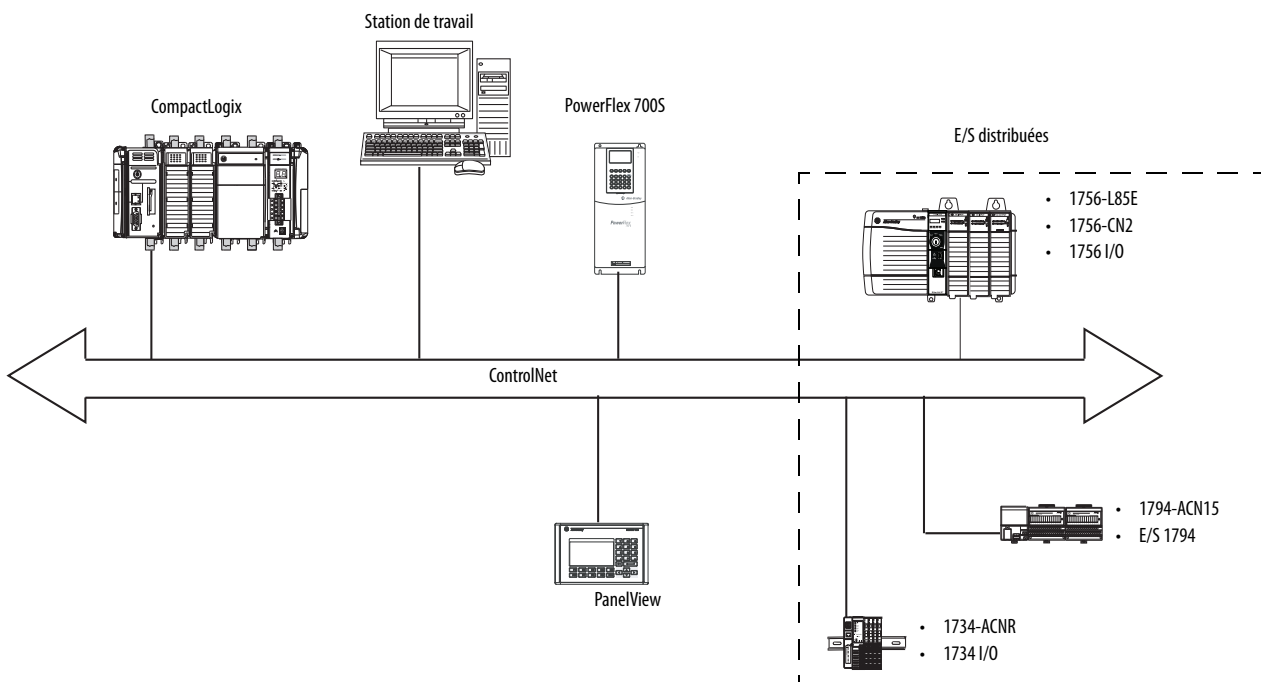
Un réseau ControlNet est souvent utilisé dans les conditions suivantes :

- comme substitut/remplacement d'un réseau d'E/S décentralisées (RIO) en raison de sa capacité à gérer efficacement un grand nombre de points d'E/S ;
- comme réseau de base pour plusieurs réseaux distribués DeviceNet ;
- comme réseau de verrouillage d'éléments appariés.

Dans l'exemple de la [figure 9](#), les actions suivantes sont réalisées par l'intermédiaire du réseau ControlNet :

- Les automates produisent et consomment des points.
- Les automates émettent des instructions MSG pour :
  - L'émission et la réception de données.
  - La configuration des dispositifs.
- La station de travail sert à :
  - Configurer à la fois les périphériques et le réseau ControlNet.
  - Télécharger et transférer des projets vers/depuis les automates.

**Figure 9 - Aperçu du réseau ControlNet**



## Exemple de ControlNet GuardLogix

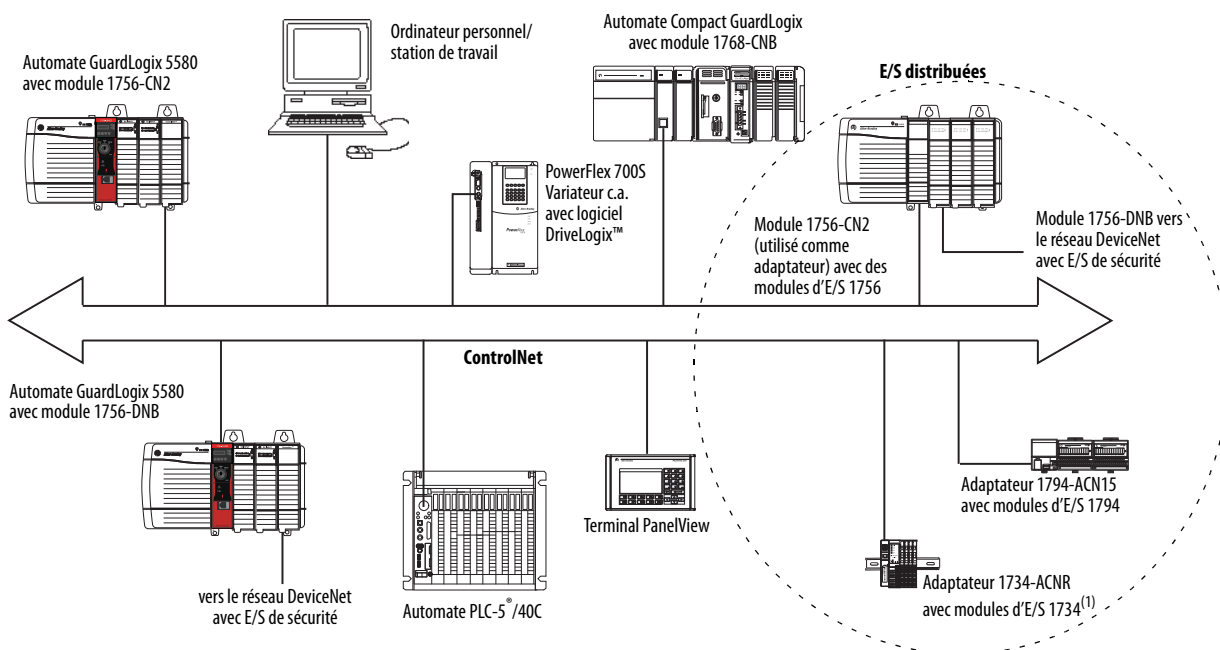
Les modules de communication ControlNet procurent ce qui suit :

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

Cet exemple démontre ce qui suit :

- Les automates GuardLogix peuvent produire et consommer des points standard ou de sécurité entre eux.
- Les automates GuardLogix peuvent lancer des instructions MSG qui envoient/reçoivent des données standard ou configurent des dispositifs. Les automates GuardLogix ne prennent pas en charge les instructions MSG pour les données de sécurité.
- Le module 1756-CN2 peut être utilisé comme passerelle, pour permettre à l'automate GuardLogix de produire et de consommer des données standard et de sécurité vers et depuis des dispositifs d'E/S.

Figure 10 - Exemple de communication ControlNet



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



## Modules ControlNet

Le [tableau 6](#) répertorie les modules ControlNet disponibles, ainsi que leurs principales fonctionnalités.

**Tableau 6 - Modules ControlNet ControlLogix**

Module	Système	Utilisation
1756-CN2, 1756-CN2K	ControlLogix GuardLogix	<ul style="list-style-type: none"> <li>Exécute les mêmes fonctions qu'un module 1756-CNB.</li> <li>Capacité de transfert double pour les applications les plus exigeantes.</li> </ul>
1756-CN2R, 1756-CN2RK, 1756-CN2RXT	ControlLogix GuardLogix	<ul style="list-style-type: none"> <li>Exécute les mêmes fonctions qu'un module 1756-CN2.</li> <li>Prend en charge les supports ControlNet redondants.</li> <li>Le 1756-CN2RXT fonctionne dans des environnements extrêmes avec des températures de -25 à 70 °C.</li> </ul>
1756-CNB,1756-CNBK	ControlLogix	<ul style="list-style-type: none"> <li>Modules de commande d'E/S.</li> <li>Communique avec d'autres dispositifs ControlNet (messagerie).</li> <li>Partage de données avec d'autres automates Logix 5000™ (production/consommation).</li> <li>Passerelle pour les liaisons ControlNet pour le routage de messages aux périphériques d'autres réseaux.</li> <li>Connexions standard uniquement.</li> </ul>
1756-CNBR, 1756-CNBRK	ControlLogix	<ul style="list-style-type: none"> <li>Exécute les mêmes fonctions qu'un module 1756-CNB.</li> <li>Prend en charge les supports ControlNet redondants.</li> <li>Connexions standard uniquement.</li> </ul>

Pour plus d'informations sur l'utilisation des modules ControlNet, reportez-vous à la publication [CNET-UM001](#), « ControlNet Modules in Logix5000 Control Systems User Manual ».

## Réseau de communication DeviceNet

**S'applique à ces automates :**

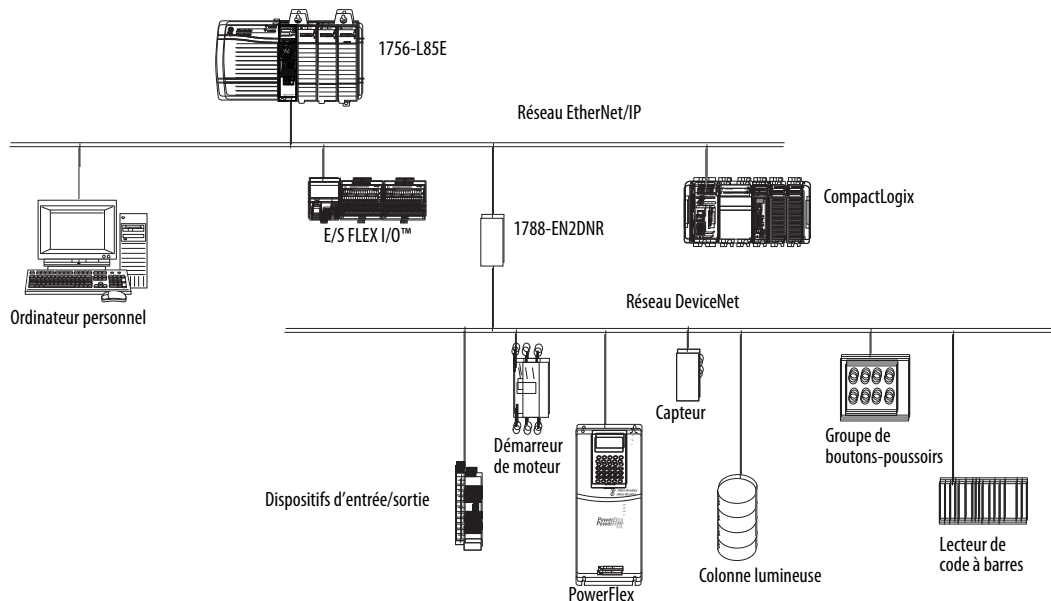
ControlLogix 5580

GuardLogix 5580

Le réseau DeviceNet utilise le protocole CIP pour fournir des capacités de commande, de configuration et de collecte de données des équipements industriels. Les réseaux DeviceNet utilisent la technologie éprouvée CAN (Controller Area Network). Celle-ci limite les coûts d'installation ainsi que les temps de montage et réduit les arrêts de production coûteux.

Un réseau DeviceNet permet d'accéder à l'intelligence présente dans les périphériques en facilitant la connexion directe de ces périphériques aux automates de l'unité de production, sans qu'il soit nécessaire de les raccorder individuellement par câblage à un module d'E/S.

**Figure 11 - Aperçu d'un réseau DeviceNet ControlLogix**



Dans cet exemple, l'automate ControlLogix est raccordé au réseau et aux périphériques DeviceNet par l'intermédiaire de l'interface de connexion 1788-EN2DNR.

Pour plus d'informations sur l'utilisation des modules et accessoires DeviceNet, reportez-vous à la publication [DNET-UM004](#), « DeviceNet Modules in Logix5000 Control Systems User Manual ».

## Module passerelle et interfaces de connexion DeviceNet

Le [tableau 7](#) répertorie les modules passerelle et les interfaces de connexion DeviceNet disponibles, utilisables avec le réseau DeviceNet.

**Tableau 7 - Modules de communication DeviceNet et capacités**

Module/Dispositif	Système	Utilisation
1756-DNB, 1756-DNBK	ControlLogix GuardLogix	<ul style="list-style-type: none"> <li>• Modules de commande d'E/S.</li> <li>• Communique avec d'autres dispositifs DeviceNet (par messages).</li> </ul>
1788-EN2DNR	ControlLogix	Interconnexion d'un réseau EtherNet/IP et d'un réseau DeviceNet.
1788-CN2DN	ControlLogix	Interconnexion d'un réseau ControlNet et d'un réseau DeviceNet.

## Connexions sur les réseaux DeviceNet

L'automate ControlLogix requiert deux connexions pour chaque module 1756-DNB. Une connexion sera réservée à la configuration et aux informations d'état du module. L'autre connexion est une connexion native pour rack, destinée aux données du dispositif.

## Communication réseau Data Highway Plus (DH+)

S'applique à ces automates :

ControlLogix 5580

Pour les communications en réseau DH+, vous avez deux options de module utilisables dans le châssis ControlLogix. Le [tableau 8](#) liste les modules DH+ et leurs capacités.

**Tableau 8 - Modules DH+ et capacités**

Module RIO	Utilisation
1756-DHRIO, 1756-DHRIOK	<ul style="list-style-type: none"> <li>• Fonctionne comme scrutateur d'E/S décentralisées (RIO).</li> <li>• Accepte soit 32 connexions logiques avec des châssis, soit 16 connexions de transfert par bloc par voie.</li> <li>• Permet l'établissement de connexions entre des automates et des adaptateurs d'E/S.</li> <li>• Assure la distribution des commandes de façon à ce que chaque automate ait ses propres E/S.</li> <li>• Utiliser pour les communications standard uniquement.</li> </ul>
1756-DHRIOXT	<ul style="list-style-type: none"> <li>• Exécute les mêmes fonctions qu'un module 1756-DHRIO</li> <li>• Fonctionne dans des environnements extrêmes avec des températures de -25 à 70 °C.</li> <li>• Utiliser pour les communications standard uniquement.</li> </ul>

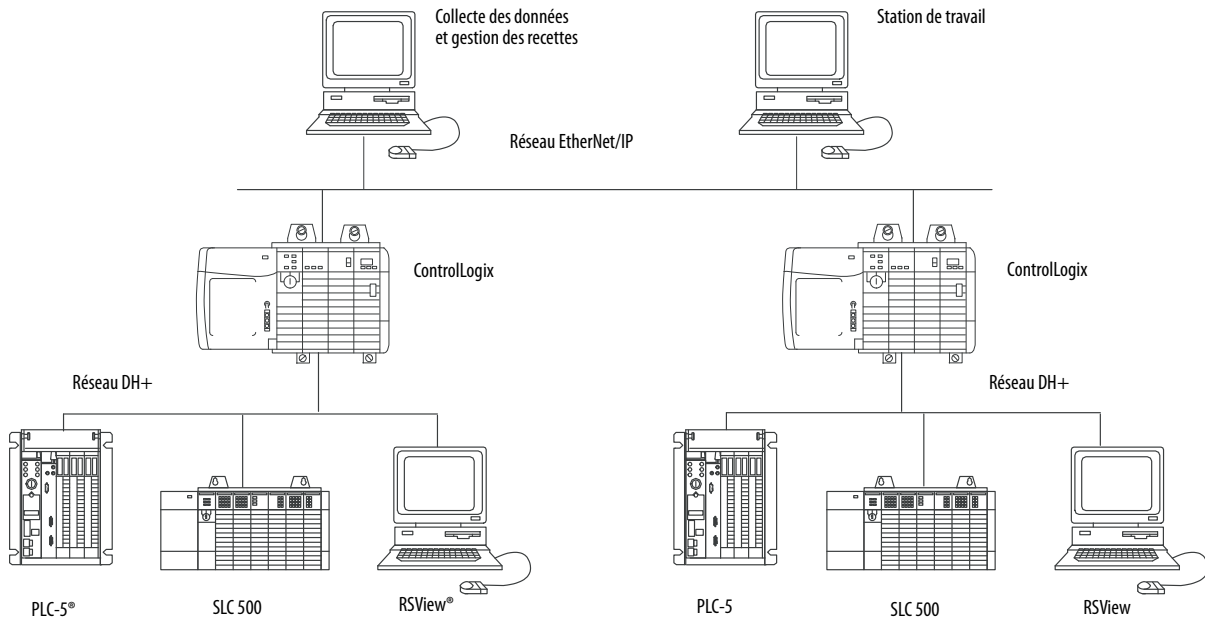
Pour les communication en réseau DH+, utiliser un module 1756-DHRIO ou 1756-DHRIOXT dans le châssis ControlLogix pour l'échange d'informations entre les automates suivants :

- automates PLC et SLC™ ;
- automates ControlLogix et automates PLC ou SLC ;
- automates ControlLogix.

Vous pouvez raccorder jusqu'à 32 stations sur une liaison DH+ :

- La voie A accepte des débits de 57,6 kbits/s, 115,2 kbits/s et 230,4 kbits/s.
- La voie B accepte des débits de 57,6 kbits/s et 115,2 kbits/s.

Figure 12 - Exemple de réseau de communication DH+ ControlLogix



### Communiquer sur un réseau DH+

Pour que l'automate puisse communiquer avec une station de travail ou d'autres dispositifs en réseau DH+, utilisez un logiciel basé sur Linx pour effectuer les opérations suivantes :

- spécifier un identifiant de liaison unique pour chaque bus intermodules ControlLogix et pour tout autre réseau figurant dans le chemin de communication ;
- configurer la table de routage pour le module 1756-DHRIO ou 1756-DHRIOXT.

Le module 1756-DHRIO ou 1756-DHRIOXT peut acheminer un message à travers quatre réseaux de communication et trois châssis au maximum. Cette limite ne s'applique qu'à l'acheminement des messages et non à la totalité des réseaux ou châssis d'un système.

Pour plus d'informations sur la configuration et l'utilisation d'un réseau DH+ par l'intermédiaire d'un module 1756DHRIO ou 1756-DHRIOXT, reportez-vous à la publication [1756-UM514](#), « Module d'interface de communication Data Highway Plus/RIO ControlLogix Manuel utilisateur ».

## Communication avec les E/S décentralisées universelles (RIO)

### S'applique à ces automates :

ControlLogix 5580

Pour les communications RIO, vous avez trois options de module utilisables dans le châssis ControlLogix. Le [tableau 9](#) répertorie les modules RIO et leurs capacités.

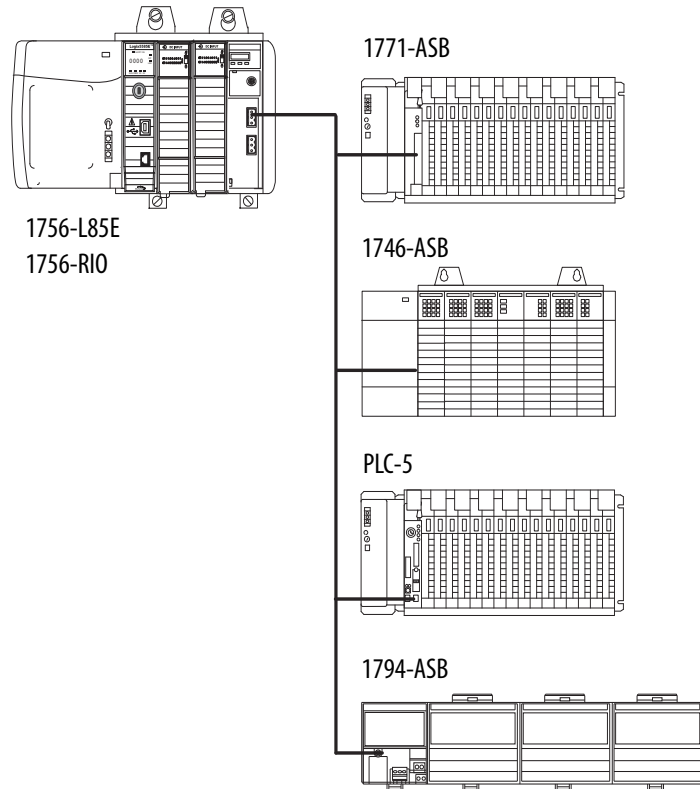
**Tableau 9 - Modules RIO et capacités**

Module RIO	Utilisation
1756-RIO, 1756-RIOK	<ul style="list-style-type: none"> <li>Fonctionne comme scrutateur et adaptateur RIO.</li> <li>Accepte des connexions à 32 châssis dans n'importe quelle combinaison de taille de châssis et de transfert par bloc.</li> <li>Actualise les données avec l'automate ControlLogix au moyen de connexions prioritaires.</li> <li>Utiliser pour les communications standard uniquement.</li> </ul>
1756-DHRIO, 1756-DHRIOK	<ul style="list-style-type: none"> <li>Fonctionne comme scrutateur RIO.</li> <li>Accepte soit 32 connexions logiques avec des châssis, soit 16 connexions de transfert par bloc par voie.</li> <li>Permet l'établissement de connexions entre des automates et des adaptateurs d'E/S.</li> <li>Assure la distribution des commandes de façon à ce que chaque automate ait ses propres E/S.</li> <li>Utiliser pour les communications standard uniquement.</li> </ul>
1756-DHRIOXT	<ul style="list-style-type: none"> <li>Exécute les mêmes fonctions qu'un module 1756-DHRIO</li> <li>Fonctionne dans des environnements extrêmes avec des températures de -25 à +70 °C.</li> <li>Utiliser pour les communications standard uniquement.</li> </ul>

Lorsqu'une des voies du module 1756-DHRIO ou 1756-DHRIOXT est configurée pour des E/S décentralisées, ce module fonctionne comme un scrutateur pour un réseau d'E/S décentralisées universelles. L'automate communique avec le module pour l'émission et la réception des données d'E/S sur le réseau d'E/S décentralisées universelles.

Le module 1756-RIO peut fonctionner soit comme scrutateur ou comme adaptateur sur le réseau d'E/S décentralisées. Le module 1756-RIO transfère les données numériques, de bloc-transfert, analogiques et spécialisées sans instructions de message.

Figure 13 - Exemple de communication avec des E/S décentralisées universelles ControlLogix



## Communication sur un réseau d'E/S décentralisées universelles

Pour que l'automate puisse commander des E/S décentralisées universelles en réseau, vous devez accomplir les opérations suivantes.

1. Configurer l'adaptateur d'E/S décentralisées.
2. Acheminer le câble réseau pour E/S décentralisées.
3. Raccorder le câble réseau pour E/S décentralisées.
4. Configurer la voie du scrutateur.

Pour plus d'informations sur la configuration d'un réseau d'E/S décentralisées avec des modules 1756RIO, 1756-DHRIO, ou 1756-DHRIOXT, reportez-vous aux publications suivantes :

- Module d'interface de communication Data Highway Plus/RIO ControlLogix Manuel utilisateur, publication [1756-UM514](#)
- ControlLogix Remote I/O Communication Module User Manual, publication [1756-UM534](#)

Lors de la conception de votre réseau d'E/S décentralisées, ayez à l'esprit les règles suivantes :

- Tous les périphériques connectés à un réseau d'E/S décentralisées doivent communiquer entre eux à la même vitesse de transmission. Vitesses de transmission possibles pour des E/S décentralisées :
  - 57,6 kbits/s
  - 115,2 kbits/s
  - 230,4 kbits/s
- Vous ne devez affecter qu'un seul châssis physique, qu'il soit partiellement ou totalement rempli, à chacune des voies utilisées en mode de scrutation d'E/S décentralisées.

Les deux voies d'un module 1756-DHRIO ou 1756-DHRIOXT ne peuvent pas scruter une même adresse de châssis (partiellement ou totalement rempli). Les deux voies du module peuvent communiquer dans les plages octales 00 à 37 ou 40 à 77, mais chacune de ces voies ne peut communiquer qu'avec une seule adresse à la fois, quelle que soit la plage à laquelle elle appartient.

## Communication par Foundation Fieldbus

S'applique à ces automates :

ControlLogix 5580

Foundation Fieldbus est un bus de terrain ouvert et interactif, conçu pour l'instrumentation de contrôle de procédé. Les dispositifs de bus terrain décrits dans le [tableau 10](#) peuvent être connectés à l'automate ControlLogix par l'intermédiaire d'un autre réseau, comme indiqué dans l'exemple ci-dessous.

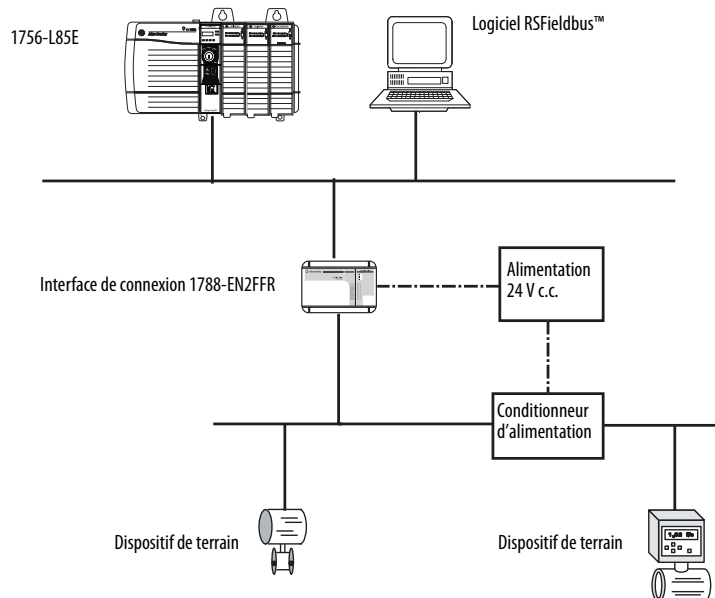
**Tableau 10 - Dispositifs Foundation Fieldbus et capacités**

Dispositif Fieldbus	Utilisation
1788-EN2FFR	<ul style="list-style-type: none"> <li>• Passerelle entre un réseau EtherNet/IP et Foundation Fieldbus.</li> <li>• Connexions réseau en modes série basse vitesse (H1) et Ethernet haute vitesse (HSE – High Speed Ethernet).</li> <li>• Accès direct aux périphériques via un serveur OPC.</li> <li>• Utiliser pour les communications standard uniquement.</li> </ul>
1788-CN2FFR	<ul style="list-style-type: none"> <li>• Connexions en mode série basse vitesse (H1).</li> <li>• Passerelle entre un réseau ControlNet et un Foundation Fieldbus.</li> <li>• Gestion des supports ControlNet redondants.</li> <li>• Utiliser pour les communications standard uniquement.</li> </ul>

Foundation Fieldbus distribue et exécute des commandes dans le dispositif. L'interface de connexion du bus terrain Foundation assure les fonctions suivantes :

- établissement d'une passerelle entre un réseau EtherNet/IP et une connexion H1 ;
- gestion des messages HSE ou EtherNet/IP et conversion de ces messages dans le protocole H1.

**Figure 14 - Exemple avec Foundation Fieldbus**



Pour plus d'informations sur l'utilisation des dispositifs Foundation Fieldbus proposés par Rockwell Automation, reportez-vous aux publications suivantes :

- EtherNet/IP and ControlNet to FOUNDATION Fieldbus Linking Device User Manual, publication [1788-UM057](#)
- FOUNDATION Fieldbus Design Considerations Reference Manual, publication [PROCES-RM005](#)



## Communication HART

### S'applique à ces automates :

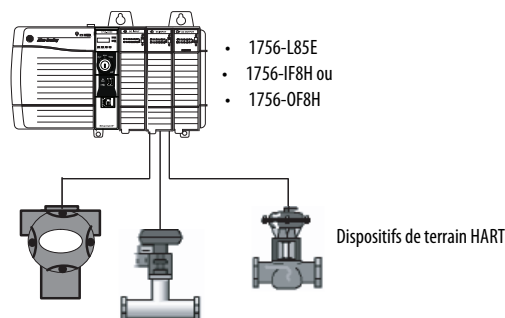
ControlLogix 5580

HART (Highway Addressable Remote Transducer) est un protocole ouvert conçu pour l'instrumentation de contrôle-commande de procédé.

Dispositif	Utilisation
Modules d'E/S analogiques HART 1756 : 1756-IF8H, 1756-IF8HK 1756-IF8IH 1756-IF16H, 1756-IF16HK 1756-IF16IH 1756-OF8H, 1756-OF8HK 1756-OF8IH	<ul style="list-style-type: none"> <li>• Fonctionnement en maître sur un réseau HART pour autoriser les communications avec les dispositifs de terrain HART.</li> <li>• Interface directe avec les dispositifs de terrain (par l'intermédiaire de modems HART intégrés), éliminant le besoin d'équipements externes et de câblages supplémentaires.</li> <li>• Accès élargi à encore plus de données en provenance des dispositifs de terrain, y compris les mesures de tension et d'intensité.</li> <li>• Connexion directe d'un logiciel de gestion d'actifs aux dispositifs HART.</li> <li>• Prise en charge des câblages différentiels dans les environnements requérant une immunité au bruit accrue (modules d'entrées).</li> <li>• Utiliser pour les communications standard uniquement.</li> </ul>
Interface ProSoft MVI56-HART	<ul style="list-style-type: none"> <li>• Acquisition de données ou applications de régulation présentant des caractéristiques de mise à jour lentes, comme pour un parc de stockage.</li> <li>• Ne nécessite aucun équipement externe pour accéder aux signaux HART.</li> <li>• Ne permet pas de connexion directe à un logiciel de gestion des actifs.</li> <li>• Utiliser pour les communications standard uniquement.</li> </ul>

Le protocole HART combine des signaux numériques avec des signaux analogiques pour conditionner le signal numérique destiné à la variable de procédé (VP). Le protocole HART fournit également des informations de diagnostic à partir des transmetteurs.

**Figure 15 - Exemple de protocole HART**



Pour plus d'informations sur l'utilisation des modules d'E/S HART, reportez-vous à la publication [1756-UM533](#), « Modules d'E/S analogiques HART ControlLogix Manuel utilisateur ».

Pour plus d'informations sur l'interface HART ProSoft, reportez-vous au site Internet de ProSoft Technologies à l'adresse <http://www.prosoft-technology.com>.

**Notes :**

## Connexion à un automate

Rubrique	Page
Définir de l'adresse IP	51
Détection d'adresse IP dupliquée	52
Adressage DNS	53
Mise à jour du firmware de l'automate	54

### S'applique à ces automates :

ControlLogix 5580

GuardLogix 5580

Avant de vous connecter à l'automate via le port Ethernet ou USB, vous devez configurer le driver EtherNet/IP™ ou USB dans le logiciel basé sur Linux sur votre poste de travail.

- L'automate à un port Ethernet qui prend en charge 10 Mbits/s, 100 Mbits/s, ou 1 Gbits/s
- L'automate possède un port USB pour connecteur type B. Le port est compatible USB 2.0 et fonctionne à 12 Mbits/s.
- Installer et configurer un module de communication dans le châssis de l'automate, comme décrit dans la notice d'installation du module de communication.

Pour plus d'informations sur l'installation des drivers de communication, reportez-vous à la publication [ENET-UM006](#), « EtherNet/IP Network Devices User Manual ».

## Définir de l'adresse IP

Lorsque l'automate est en état d'origine, ce qui suit s'applique aux adresses IP :

- Les automates sont livrés sans adresse IP.
- DHCP est activé sur l'automate. Autrement dit, l'automate est configuré pour obtenir une adresse IP via un serveur DHCP.

En l'absence de serveur DHCP ou si celui-ci n'est pas configuré pour définir l'adresse IP, vous devez la définir manuellement.

## Exigences

Pour définir l'adresse IP, vous avez besoin des éléments suivants :

- Drivers EtherNet/IP ou USB installés sur la station de travail de programmation
- L'identifiant MAC ID du dispositif qui figure sur l'étiquette apposée sur le côté du dispositif.
- Adresse IP recommandée pour le dispositif

## Autres méthodes pour définir l'adresse IP

L'automate prend en charge les méthodes suivantes pour modifier l'adresse IP :

- Utilitaire BOOTP/DHCP
- Le logiciel RSLinx® Classic
- Application Studio 5000 Logix Designer®

Pour plus d'informations sur l'utilisation de ces méthodes, reportez-vous à la publication [ENET-UM006](#), « EtherNet/IP Network Device User Manual ».

## Détection d'adresse IP dupliquée

L'automate vérifie que son adresse IP ne correspond à aucune autre adresse IP de dispositif du réseau lorsque vous effectuez l'une de ces tâches :

- Connecter le module à un réseau EtherNet/IP.
- Modifier l'adresse IP de l'automate.

Si l'adresse IP de l'automate correspond à celle d'un autre dispositif sur le réseau, le port EtherNet/IP de l'automate passe au mode Conflit (Conflit). En mode Conflit, ces conditions existent :

- L'indicateur d'état du réseau (NET) est rouge fixe.
- L'afficheur à 4 caractères indique le conflit.

L'afficheur fait défiler : <IP\_address\_of\_this\_module> Duplicate IP  
<Mac\_address\_of\_duplicate\_node\_detected>

Par exemple : 192.168.1.1 Duplicate IP - 00:00:BC:02:34:B4

## Résolution d'adresse IP dupliquée

Lorsque deux dispositifs sur un réseau ont des adresses IP conflictuelles, la résolution dépend des conditions dans lesquelles la duplication est détectée. Ce tableau décrit comment les adresses IP en double sont résolues.

Conditions de détection d'adresse IP dupliquée	Processus de résolution
<ul style="list-style-type: none"> <li>Les deux dispositifs prennent en charge la détection des adresses IP en double.</li> <li>Le deuxième dispositif est ajouté au réseau après que le premier dispositif fonctionne sur le réseau.</li> </ul>	<ol style="list-style-type: none"> <li>Le dispositif qui a commencé à fonctionner en premier utilise l'adresse IP et continue à fonctionner sans interruption.</li> <li>Le dispositif qui commence à fonctionner en deuxième détecte la duplication et entre en mode Conflit (Conflit). Pour attribuer une nouvelle adresse IP à l'automate et quitter le mode Conflit, définissez l'adresse IP du réseau avec l'outil de mise en service EtherNet/IP DHCP BootP. Consultez la publication <a href="#">ENET-UM006</a>, « EtherNet/IP Network Device User Manual ».</li> </ol>
<ul style="list-style-type: none"> <li>Les deux dispositifs prennent en charge la détection des adresses IP dupliquées.</li> <li>Les deux dispositifs ont été mis sous tension approximativement au même moment.</li> </ul>	<p>Les deux dispositifs EtherNet/IP passent en mode Conflit. Pour résoudre ce conflit, suivez ces étapes :</p> <ol style="list-style-type: none"> <li>Attribuez une nouvelle adresse IP à l'automate. Définissez l'adresse IP avec l'outil de mise en service BootP DHCP EtherNet/IP. Consultez la publication <a href="#">ENET-UM006</a>, « EtherNet/IP Network Devices User Manual ».</li> <li>Mettez l'autre dispositif sous tension.</li> </ol>
Un dispositif prend en charge la détection d'adresse IP dupliquée, mais pas un deuxième dispositif.	<ol style="list-style-type: none"> <li>Quel que soit le dispositif qui a obtenu l'adresse IP en premier, le dispositif qui ne prend pas en charge la détection d'adresse IP utilise l'adresse IP et continue à fonctionner sans interruption.</li> <li>Le dispositif qui prend en charge la détection d'adresse IP en double détecte la duplication et entre en mode Conflit. Pour attribuer une nouvelle adresse IP à l'automate et quitter le mode Conflit, définissez l'adresse IP du réseau avec l'outil de mise en service EtherNet/IP DHCP BootP. Consultez la publication <a href="#">ENET-UM006</a>, « EtherNet/IP Network Devices User Manual ».</li> </ol>

## Adressage DNS

Vous pouvez également utiliser l'adressage DNS pour spécifier un nom d'hôte pour un automate, un nom de domaine et des serveurs DNS. L'adressage DNS permet de configurer des structures de réseau et des séquences d'adresse IP similaires sous différents domaines.

L'adressage DNS n'est nécessaire que si vous vous référez à l'automate par le nom d'hôte, par exemple dans les descriptions de chemin des instructions MSG.

Procédez comme suit pour utiliser l'adressage DNS.

- Attribuez un nom d'hôte à l'automate.

Un administrateur réseau peut affecter un nom d'hôte. Les noms d'hôte corrects doivent être conformes à la norme CEI-1131-3.

- Configurez les paramètres de l'automate.
- Configurez l'adresse IP, le masque de sous-réseau, l'adresse de passerelle, un nom d'hôte pour l'automate, le nom de domaine et les adresses de serveur DNS principal/secondaire.

Dans le serveur DNS, le nom d'hôte doit correspondre à l'adresse IP de l'automate.

- Dans l'application Logix Designer, ajoutez l'automate à l'arborescence de configuration d'E/S.

---

**IMPORTANT** Si un sous-module réside dans le même domaine que son module parent, entrez le nom d'hôte. Si le domaine du module enfant diffère du domaine de son module parent, tapez le nom d'hôte et le nom de domaine (nomhôte.nomdomaine)

---

---

**IMPORTANT** Vous pouvez également utiliser l'adressage DNS dans un profil de module dans l'arborescence d'E/S de l'automate ou dans un chemin de message. Si le nom de domaine du module de destination diffère du nom de domaine du module source, utilisez un nom DNS pleinement qualifié (nomhôte.nomdomaine). Par exemple, pour envoyer un message de EN2T1.emplacement1.entrepriseA à EN2T1.emplacement2.entrepriseA, les noms d'hôte correspondent mais les domaines diffèrent. Sans la saisie d'un nom DNS pleinement qualifié, le module ajoute le nom de domaine par défaut au nom d'hôte spécifique.

---

## Mise à jour du firmware de l'automate

---

### S'applique à ces automates :

---

ControlLogix 5580

---

GuardLogix 5580

---

Pour mettre à jour le firmware de l'automate, procédez comme suit :

- Détermination du firmware d'automate requis
- Obtention du firmware de l'automate
- Pour mettre à jour le firmware utilisez soit [Utilisation du logiciel ControlFLASH Plus ou ControlFLASH pour mettre à jour le firmware](#), soit [Utilisation d'AutoFlash pour mettre à jour le firmware](#)

## Directives de mise à niveau du firmware pour les automates de sécurité

---

### **IMPORTANT** Considérations relatives à la sécurité

Vous ne pouvez pas mettre à jour un automate dont la sécurité est verrouillée.

---

La norme de sécurité fonctionnelle CEI 61508 exige une analyse d'impact avant de mettre à niveau ou de modifier des composants dans un système de sécurité fonctionnelle certifié. Cette section fournit des conseils de haut niveau sur la façon dont vous pouvez effectuer l'analyse d'impact pour les mises à niveau du matériel/firmware de l'automate de sécurité. Référez-vous à la norme pour vous assurer que vous remplissez toutes les exigences relatives à votre application.

Lorsque vous mettez à niveau le firmware de l'automate vers une version plus récente, tenez compte des éléments suivants :

- Toutes les versions majeures et mineures du firmware des systèmes d'automate GuardLogix sont certifiées pour une utilisation dans les applications de sécurité. Dans le cadre du processus de certification, Rockwell Automation teste les fonctions du firmware liées à la sécurité (par exemple les sous-systèmes de communication CIP Safety™, l'exécution des instructions de sécurité embarquées et les fonctions de diagnostic liées à la sécurité). Les notes de version du firmware identifient les modifications apportées aux fonctions liées à la sécurité.
- Effectuez une analyse d'impact de la mise à niveau prévue du firmware.
  - Examinez les notes de version du firmware pour les modifications apportées aux fonctionnalités liées à la sécurité.
  - Examinez la compatibilité du matériel et du firmware sur le site de compatibilité et de téléchargement des produits pour identifier les conflits de compatibilité potentiels.
  - Toute modification, amélioration ou adaptation de votre logiciel validé doit être planifiée et analysée pour tout impact sur le système de sécurité fonctionnelle, comme décrit dans la section « Modifier votre application de sécurité » dans le manuel de référence de sécurité de votre automate.
- Vous devez supprimer et régénérer la signature de sécurité dans le cadre du processus de mise à niveau du firmware. Utilisez le processus d'édition en ligne et hors ligne décrit dans le manuel de référence de sécurité de votre automate.

Pour de plus amples informations, reportez-vous à la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

---

**IMPORTANT** Les automates GuardLogix 5580 ont un compilateur différent de celui des automates précédents. Vous devez revalider que les applications des automates antérieurs se compilent correctement sur les automates GuardLogix 5580.

---

Pour les directives de gestion des changements de produit et les définitions sur la façon dont Rockwell Automation gère les versions des produits, consultez la publication [SECURE-RM001](#), « System Security Design Guidelines Reference Manual ».

Par exemple :

1. Depuis le centre de compatibilité et de téléchargement des produits :
  - a. Passez en revue toutes les notes de mise à jour du firmware, en commençant par la révision du firmware d'origine jusqu'à la nouvelle révision du firmware, pour identifier tout changement ayant un impact sur la mise en œuvre de l'application liée à la sécurité.
  - b. Examinez la compatibilité du matériel et du firmware pour identifier les restrictions entre les composants du système d'origine et les nouveaux composants du système.
2. Effectuez une évaluation des dangers et des risques pour tout changement identifié lors de l'analyse d'impact et déterminez quels tests supplémentaires sont nécessaires.
3. Effectuez le processus d'édition en ligne et hors ligne décrit dans le manuel de référence de sécurité de votre automate. Vous pouvez restreindre le bloc « Tester l'application » aux tests identifiés par l'évaluation des dangers et des risques.

### Détermination du firmware d'automate requis

---

**IMPORTANT** L'automate doit être en mode Programmation à distance ou Programmation et tous les défauts majeurs récupérables doivent être effacés pour pouvoir accepter les mises à jour.

---

Le niveau de révision majeur du firmware doit correspondre au niveau de version majeure du logiciel. Par exemple, si la révision du firmware de l'automate est 31.xxx, vous devez utiliser l'application Logix Designer, version 31.

---

**IMPORTANT** **Considérations relatives à la sécurité**

Pour un système GuardLogix® qui inclut un partenaire de sécurité (SIL 3/PLe uniquement), le firmware de l'automate principal et du partenaire de sécurité doit correspondre. Le partenaire de sécurité se met à jour automatiquement quand l'automate principal est mis à jour.

---



## Obtention du firmware de l'automate

Vous pouvez obtenir le firmware de l'automate de la manière suivante :

- Le firmware est fourni dans le cadre de l'installation de l'application Studio 5000 Logix Designer.

---

**IMPORTANT** Le firmware fourni avec l'installation du logiciel est la version initiale du firmware de l'automate. Des révisions ultérieures du firmware pour corriger des anomalies peuvent être publiées pendant la durée de vie d'un produit. Nous vous recommandons de consulter le Centre de compatibilité et de téléchargement des produits (PCDC) pour déterminer si des révisions ultérieures du firmware de l'automate sont disponibles. Pour plus d'informations, lisez la puce suivante.

---

- Depuis le centre de compatibilité et de téléchargement des produits de Rockwell Automation (PCDC). Vous pouvez rechercher les révisions disponibles du firmware de l'automate et télécharger le firmware, les fichiers associés et les notes de version du produit.

Le logiciel ControlFLASH Plus™ version 2.00.00 et ultérieure offre une intégration avec le PCDC pour une expérience améliorée pendant que vous recherchez les révisions du firmware, les téléchargements, les notes de version et l'accès aux avis importants.

Pour visiter le PCDC, accédez à l'adresse

<http://compatibility.rockwellautomation.com/Pages/home.aspx>.

## Utilisation du logiciel ControlFLASH Plus ou ControlFLASH pour mettre à jour le firmware

Pour des informations sur le téléchargement, l'installation et l'utilisation du logiciel ControlFLASH Plus ou ControlFLASH™, voir :

- la publication [CFP-QS001](#), « ControlFLASH Plus Quick Start Guide »
- ControlFLASH Firmware Upgrade Kit User Manual, publication [1756-UM105](#)

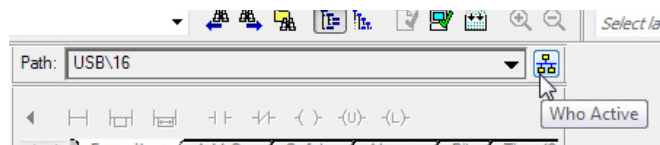
## Utilisation d'AutoFlash pour mettre à jour le firmware

Pour mettre à jour le firmware de votre automate à l'aide de la fonctionnalité AutoFlash, suivez ces étapes :

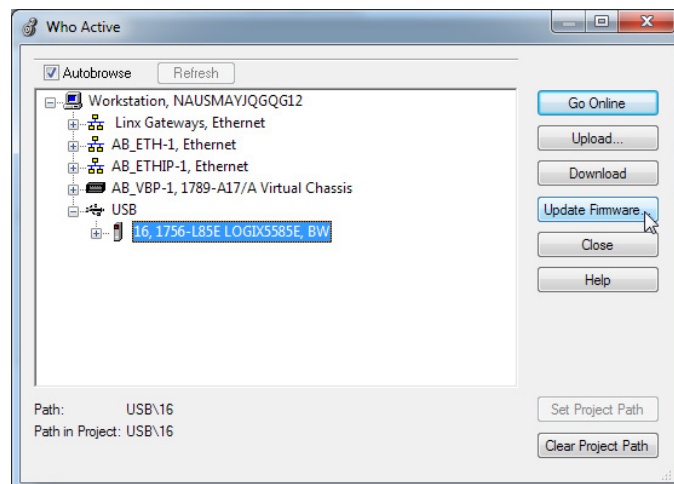


**ATTENTION :** Si la carte Secure Digital est verrouillée et configurée pour charger lors de la mise sous tension, cette mise à jour peut être écrasée par le firmware sur la carte SD.

1. Vérifiez si la connexion réseau est établie et que votre driver réseau est configuré dans un logiciel de communication basé sur Linx.
2. Utilisez l'application Logix Designer pour créer un projet d'automate.
3. Sur la barre Path, cliquez sur Who Active.

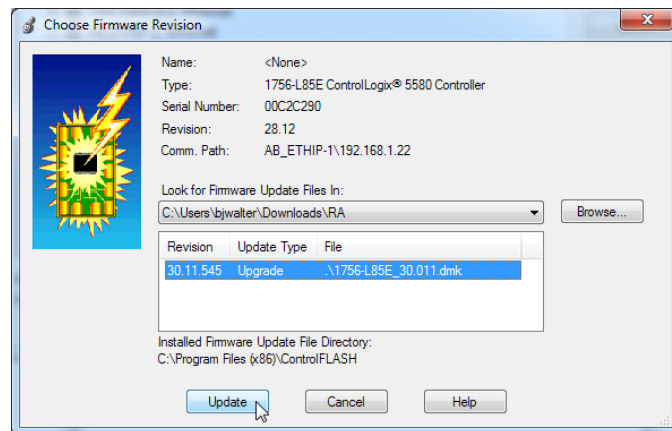


4. Dans la boîte de dialogue Who Active, sélectionnez l'automate sous le driver de communication que vous souhaitez utiliser, puis cliquez sur Update Firmware (Mise à jour firmware).

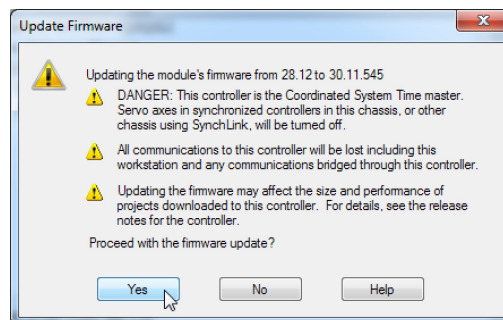


5. Dans la boîte de dialogue Choose Firmware Revision (Choisir la révision de firmware), accédez à l'emplacement des fichiers du firmware (C:\Program Files (x86)\ControlFLASH).

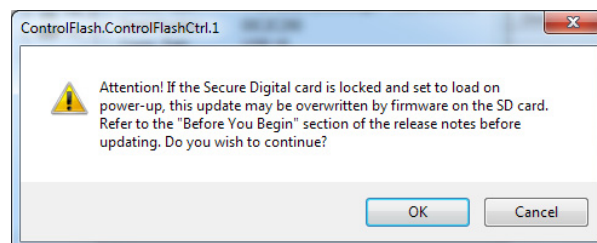
6. Sélectionnez la révision de firmware puis cliquez sur Update (Actualiser).



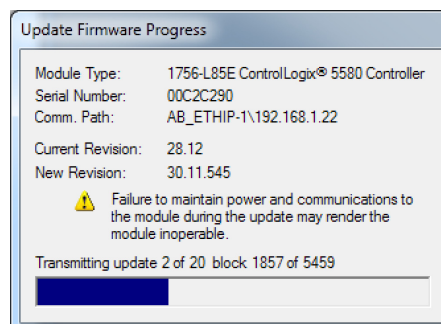
7. Dans la boîte de dialogue Confirmation, cliquez sur Yes (Oui).



8. Dans la boîte de dialogue ControlFlash Attention, cliquez sur OK.



La mise à jour du firmware commence.



Laissez la mise à jour du firmware se dérouler sans l'interrompre. Lorsque la mise à jour de firmware est terminée, la boîte de dialogue de progression se ferme.

**Notes :**

## Commencer à utiliser l'automate

Rubrique	Page
Création d'un projet d'application Logix Designer	61
Configuration supplémentaire pour un automate GuardLogix	62
Passer en ligne avec l'automate	73
Téléchargement dans l'automate	79
Transfert depuis l'automate	82
Choix du mode de fonctionnement de l'automate	85
Bouton réinitialisation	89

### Création d'un projet d'application Logix Designer

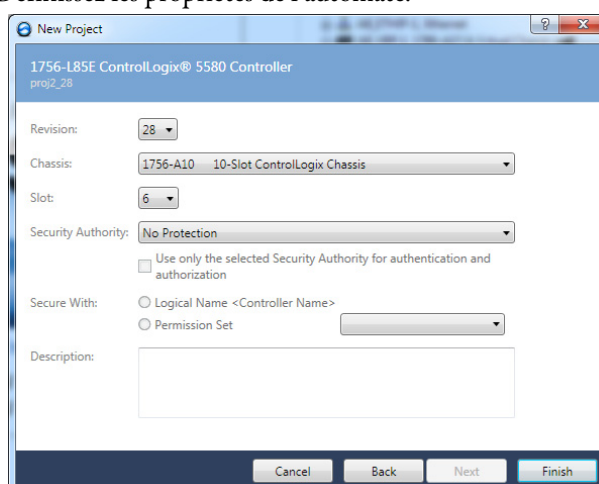
#### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Création d'un projet d'automate en utilisant l'application Studio 5000 Logix Designer®.

1. Créez un nouveau projet puis choisissez l'automate.
2. Définissez les propriétés de l'automate.



- Choisissez la révision majeure du firmware de l'automate.
- Choisissez la taille du châssis.
- Choisissez le logement de l'automate.
- Choisissez l'option d'autorité de la sécurité.  
Pour des informations détaillées sur la sécurité, reportez-vous à la publication [1756-PM016](#), « Sécurité des automates Logix5000 Manuel de programmation ».
- Saisissez une description du projet.

## Configuration supplémentaire pour un automate GuardLogix

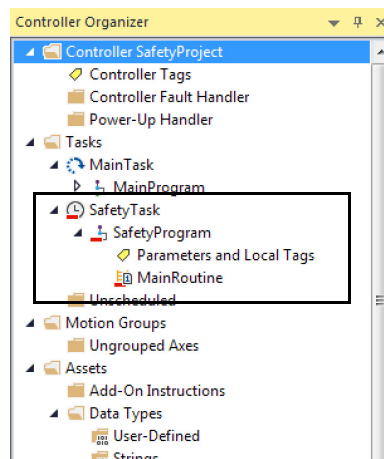
Concerne ces automates :

GuardLogix 5580

Les automates GuardLogix® requièrent une configuration supplémentaire après avoir créé le projet. Ces rubriques décrivent comment configurer votre automate.

Pour un automate GuardLogix, 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.

Un trait rouge sous l'icône permet de différencier les programmes et sous-programmes de sécurité des composants de projet standard dans l'organisateur de l'automate.



## Définir le niveau de sécurité pour un automate GuardLogix

Le niveau de sécurité déclare à l'application Logix Designer l'intention de l'application de sécurité. Le niveau de sécurité indique si le projet est au niveau de sécurité SIL 2/PLD ou SIL 3/PLE.

- Le niveau de sécurité requis pour une application est basé sur une évaluation des risques requise effectuée par le client.
- Le niveau de sécurité atteint est déterminé par la conformité aux exigences de niveau d'intégrité de sécurité (SIL) et de niveau de performance (PL) et aux exigences de l'application de sécurité. Consultez la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

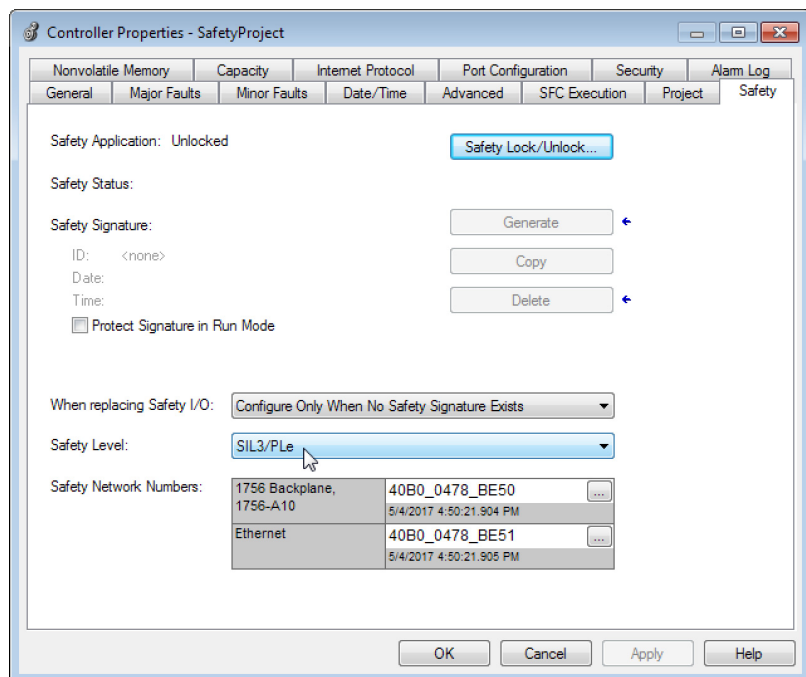
Vous devez spécifier le niveau de sécurité :

- Le réglage de niveau par défaut est SIL 2/PLD.
- Vous ne pouvez modifier le réglage hors ligne que si l'application de sécurité est à l'état Déverrouillé et qu'aucune signature de sécurité n'existe.
- Pour SIL 3/PLE, vous devez avoir un partenaire de sécurité 1756-L8SP installé à la droite de l'automate principal.

- Si vous choisissez SIL 3/PLe, un partenaire de sécurité apparaît dans l'arborescence des E/S de l'organisateur de l'automate. Si vous changez la valeur pour revenir à SIL 2/PLd, le partenaire de sécurité disparaît de l'arborescence des E/S.

Exécutez ces étapes pour définir le niveau de sécurité.

1. Dans la barre d'outils Online (En ligne), cliquez sur l'icône des propriétés de l'automate.
2. Dans le dialogue Controller Properties (Propriétés de l'automate), cliquez sur l'onglet Safety (Sécurité).
3. Sous l'onglet Safety (Sûreté), choisissez le niveau de sécurité.



4. Cliquez sur Apply (Appliquer).
5. Cliquez sur OK.

## Mots de passe pour verrouiller et déverrouiller la sécurité

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

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

---

**IMPORTANT** Rockwell Automation n'offre pas de service de dérogation au mot de passe ou à la sécurité. Lorsque les produits et les mots de passe sont configurés, Rockwell Automation invite les clients à adopter de bonnes pratiques de sécurité et de planifier en conséquence la gestion des mots de passe.

---

Pour savoir comment définir les mots de passe, consultez [Définition des mots de passe pour verrouiller ou déverrouiller la sécurité, page 202](#).



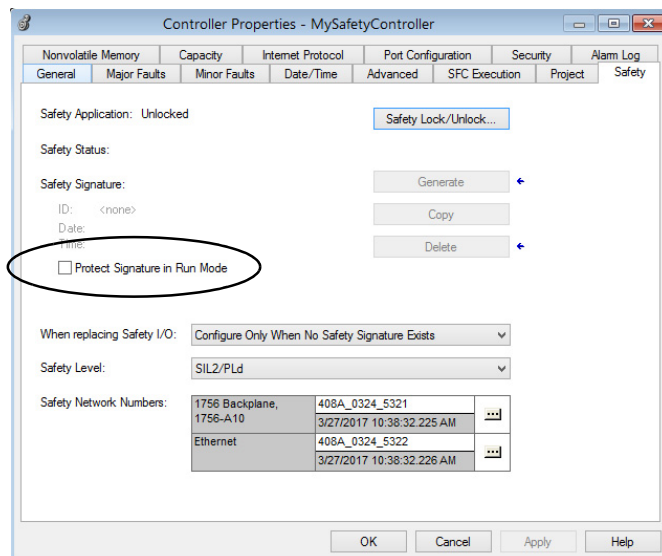
## Protection de la signature de sécurité en mode d'exécution

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

**IMPORTANT** Procédez comme suit avant de créer une signature de sécurité ou de verrouiller la sécurité de l'automate. Une fois qu'une signature de sécurité existe, ou que la sécurité de l'application est verrouillée, la case à cocher Protect Signature in Run Mode (Protéger signature en mode Exécution) n'est plus modifiable.

Procédez comme suit pour protéger la signature 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.



## Attribuer le numéro de réseau de sécurité (SNN)

Lorsque vous créez des projets d'automate, l'application Studio 5000 Logix Designer génère automatiquement une valeur SNN à chaque fois qu'elle reconnaît un nouveau sous-réseau qui contient des dispositifs CIP Safety™ :

- Un SNN est attribué à chaque port compatible CIP Safety de l'automate. Les automates GuardLogix 5580 ont deux numéros de réseau de sécurité : un pour le port EtherNet/IP™ et un pour le bus intermodules.
- Si une passerelle ou un dispositif adaptateur figure dans l'arborescence des E/S et qu'un dispositif CIP Safety enfant est ajouté, le sous-réseau qui est créé par la passerelle ou l'adaptateur se voit attribuer un numéro SNN.

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

- Un ou plusieurs ports d'automate sont sur un réseau CIP safety qui a déjà un numéro SNN établi.
- vous copiez un projet de sécurité dans une installation matérielle différente au sein du même système CIP Safety routable.

Rockwell Automation conseille de changer le SNN et de lui donner la valeur du SNN déjà défini pour le sous-réseau en question, le cas échéant. Ainsi, les dispositifs créés ultérieurement dans le projet recevront automatiquement le SNN correct.

Pour plus d'informations concernant l'ajout éventuel de ports d'automate ou Ethernet à des sous-réseaux existants, reportez-vous à la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

Chaque réseau de sécurité doit avoir un numéro de réseau de sécurité 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. Toutefois, pour plus de simplicité, nous recommandons de doter chaque sous-réseau CIP Safety d'un seul numéro SNN.

Pour une explication du numéro de réseau de sécurité, consultez la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la 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.

- [Attribution automatique du SNN temporel, page 67](#)
- [Attribution manuelle de SNN, page 68](#)

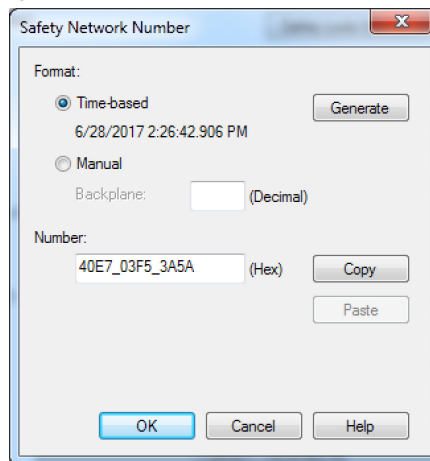
### *Attribution automatique du SNN temporel*

Lorsqu'un nouvel automate ou un nouveau dispositif est créé, un numéro SNN temporel est automatiquement attribué.

- Les dispositifs créés directement sous le port de l'automate ont par défaut le même SNN que ce port sur l'automate.
- Pour les dispositifs qui ne sont pas créés directement sous un port de l'automate, les dispositifs de sécurité ajoutés ultérieurement au même réseau CIP Safety reçoivent le même numéro SNN défini avec l'adresse la plus basse sur ce réseau CIP Safety.

Le format temporel définit la valeur SNN avec la date et l'heure auxquelles le numéro a été généré, conformément à l'horloge de l'ordinateur qui exploite le logiciel de configuration.

**Figure 16 - Format temporel**



### *Attribution manuelle de SNN*

L'attribution manuelle est utile si vous organisez le plan de votre réseau et placez des numéros SNN sur votre schéma de réseau. Il peut être plus facile de lire des SNN à partir d'un schéma que de les copier et coller à partir de multiples projets.

Toutefois, une définition manuelle du SNN est nécessaire si :

- Un ou plusieurs ports d'automate sont sur un réseau CIP Safety qui a déjà un numéro SNN établi.
- vous copiez un projet de sécurité dans une installation matérielle différente au sein du même système CIP Safety routable.

---

**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 SNN et référence de station unique. Vous pouvez toujours vérifier le projet mais Rockwell Automation vous recommande de résoudre les combinaisons en double.


Cependant, il peut y avoir des dispositifs de sécurité sur le réseau de sécurité routable qui ont les mêmes SNN et adresse de station, et ne sont pas dans le projet. Dans ce cas, ces dispositifs de sécurité sont inconnus de l'application Logix Designer, et aucun avertissement ne s'affichera.

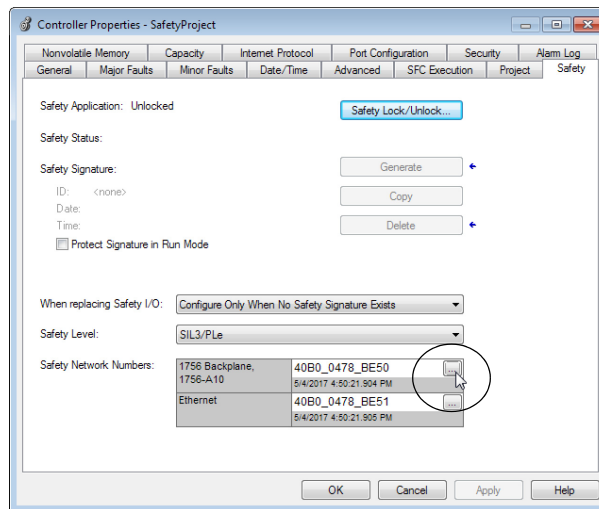
Si deux dispositifs différents ont les mêmes références de station, le système de sécurité ne peut pas détecter un paquet destiné à un dispositif mais reçu par l'autre.

S'il existe des références de station unique en double, en tant qu'utilisateur du système, vous devez prouver qu'une condition peu sûre ne peut pas en résulter.

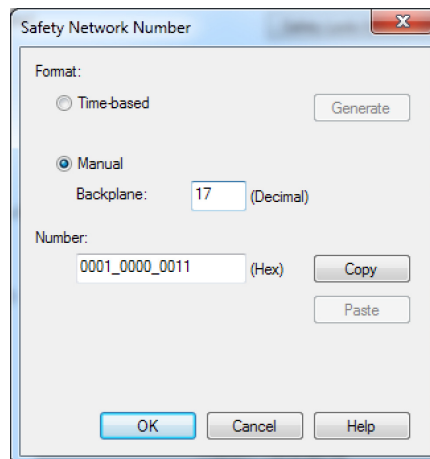
---

Procédez comme suit pour passer à une attribution manuelle des SNN d'automate :

1. Dans la barre d'outils Online (En ligne), cliquez sur l'icône des propriétés de l'automate.
2. Dans le dialogue Controller Properties (Propriétés de l'automate), cliquez sur l'onglet Safety (Sécurité).
3. Sous l'onglet Safety, cliquez  à droite du numéro de réseau de sécurité pour le port que vous souhaitez modifier.



4. Dans la boîte de dialogue Safety Network Number (Numéro de réseau de sécurité), sélectionnez Manual (Manuel).
5. Saisissez le numéro SNN comme une valeur décimale de 1 à 9999.



6. Cliquez sur OK.

Vous pouvez laisser l'application Logix Designer attribuer automatiquement un numéro SNN ou l'attribuer vous-même manuellement.

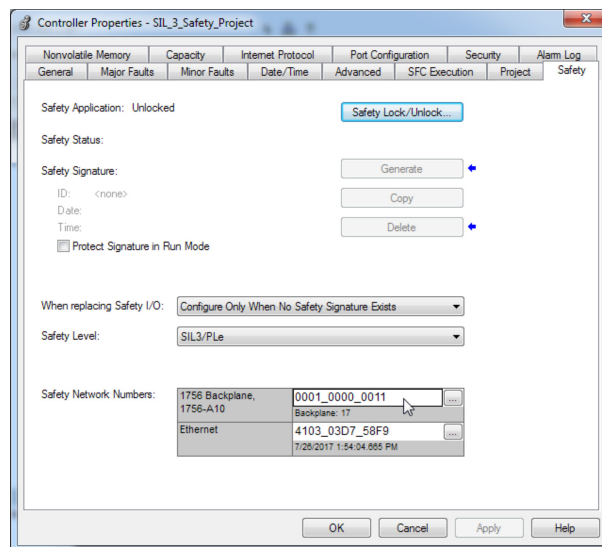
## Copier-coller un numéro de réseau de sécurité d'automate de sécurité

Si vous devez appliquer un numéro de réseau de sécurité (SNN) à d'autres automates de sécurité, vous pouvez copier et coller le SNN. Il existe plusieurs façons de copier et coller les SNN des automates de sécurité.


### *Copier un SNN d'automate de sécurité*

À partir de l'onglet Controller Properties Safety :

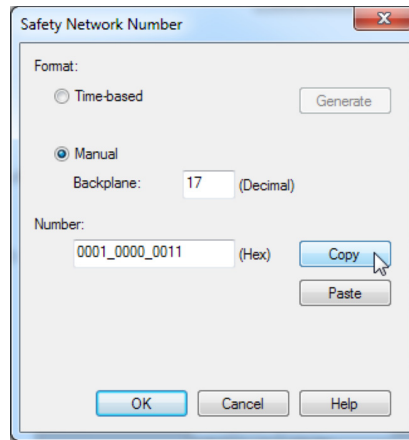
1. À l'onglet safety (Sécurité), cliquez sur le champ SNN que vous souhaitez copier.
2. Appuyez sur Ctrl-C pour copier le SNN.



À partir du dialogue Safety Network Number :

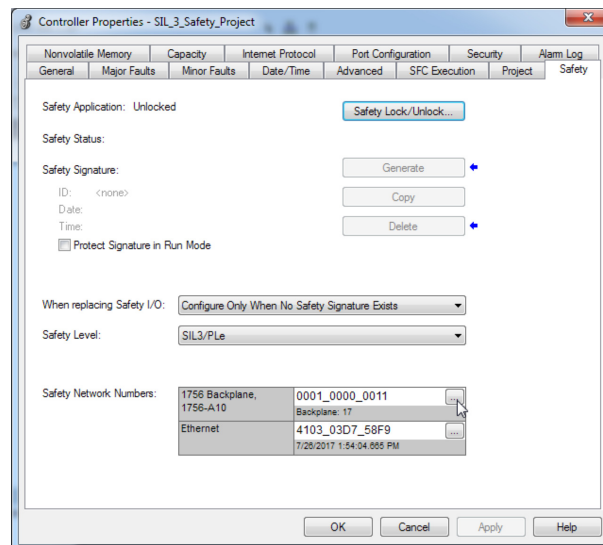
1. Dans le dialogue Controller Properties (Propriétés de l'automate), cliquez sur l'onglet Safety (Sécurité).
2. Cliquez  à droite du numéro de réseau de sécurité pour ouvrir le dialogue Safety Network Number (Numéro de réseau de sécurité).

3. Dans le dialogue Safety Network Number, cliquez sur Copy (Copier), ou cliquez sur le champ SNN et appuyez sur Ctrl-C.



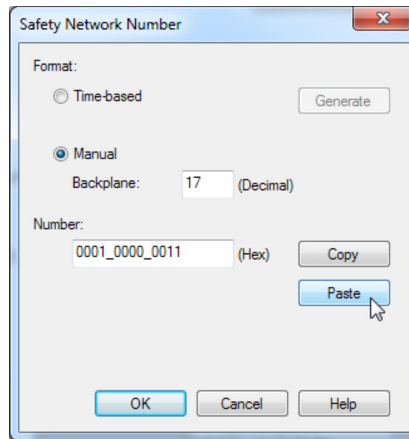
### *Coller un SNN d'automate de sécurité*

1. Dans le dialogue Controller Properties (Propriétés de l'automate), cliquez sur l'onglet Safety (Sécurité).



2. Cliquez [...] à droite du numéro de réseau de sécurité pour ouvrir le dialogue Safety Network Number (Numéro de réseau de sécurité).

3. Dans le dialogue Safety Network Number, cliquez sur Paste (Coller), ou cliquez sur le champ SNN et appuyez sur Ctrl-V.



4. Cliquez sur OK.
5. Dans le dialogue Controller Properties (Propriétés de l'automate), cliquez sur OK.



## Passer en ligne avec l'automate

### Concernes ces automates :

ControlLogix 5580

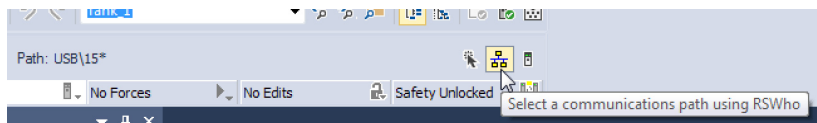
GuardLogix 5580

Pour passer en ligne avec l'automate, vous devez d'abord spécifier un chemin de communication dans l'application Logix Designer.

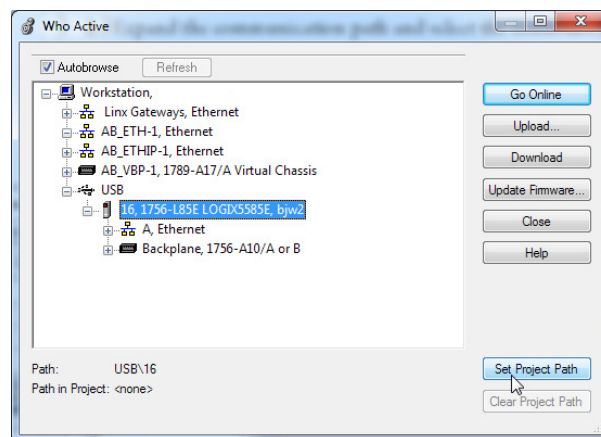
**CONSEIL** Pour cette section, le port USB a été choisi comme chemin de communication. D'autres chemins via le port Ethernet embarqué ou via le bus intermodules sont également possibles.

## Utilisation de RSWho

1. Ouvrez ou créez un projet d'application Logix Designer.
2. Dans l'application, cliquez sur RSWho.



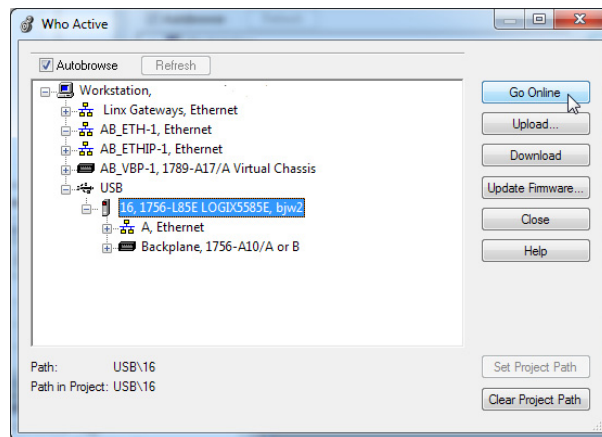
3. Développez le chemin de communication et sélectionnez l'automate.



4. Si vous souhaitez stocker le chemin d'accès dans le fichier de projet, cliquez sur Set Project Path (Définir le chemin du projet).

Si vous stockez le chemin du projet dans le projet, vous n'avez pas à choisir le chemin à chaque fois que vous passez en ligne.

- Après avoir choisi le chemin de communication, cliquez sur Go Online (Passer en ligne) dans la boîte de dialogue Who Active (Qui est actif).



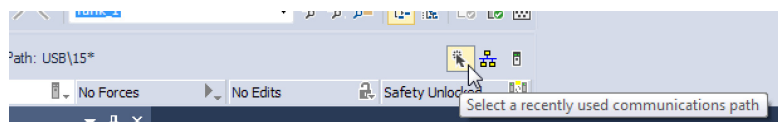
Passer en ligne utilise la station mise en surbrillance dans l'arborescence Who Active, quel que soit le réglage du chemin dans le projet. Pour plus d'informations sur la boîte de dialogue Who Active, consultez l'aide en ligne de Logix Designer.

Consultez [Considérations supplémentaires sur le passage en ligne avec un automate GuardLogix, page 75](#).

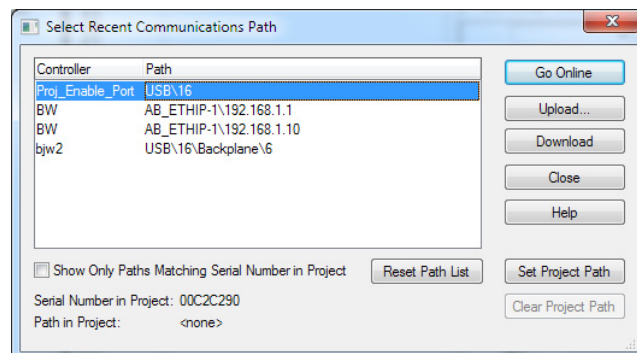
## Utilisation d'un chemin de communication récent

Vous pouvez également sélectionner un chemin de communication récent et passer en ligne ou l'appliquer à votre projet.

- Dans l'application, cliquez sur la flèche se trouvant sur la barre Path.



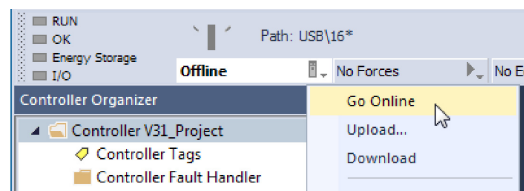
- Dans la boîte de dialogue Select Recent Communications Path (Sélectionner récent chemin de communication), choisissez le chemin.



3. Pour mémoriser le chemin dans votre projet, cliquez sur Set Project Path (Définir chemin du projet).
4. Cliquez sur Go Online (Mise en ligne).

Pour plus d'informations sur la boîte de dialogue Select Recent Communications Path, consultez l'aide en ligne de Logix Designer.

Une fois que vous avez établi un chemin de communication, vous pouvez choisir de passer en ligne à partir du menu Controller Status (État d'automate) lorsque vous travaillez dans le projet.



Consultez [Considérations supplémentaires sur le passage en ligne avec un automate GuardLogix, page 75.](#)

## Considérations supplémentaires sur le passage en ligne avec un automate GuardLogix

### Concerne ces automates :

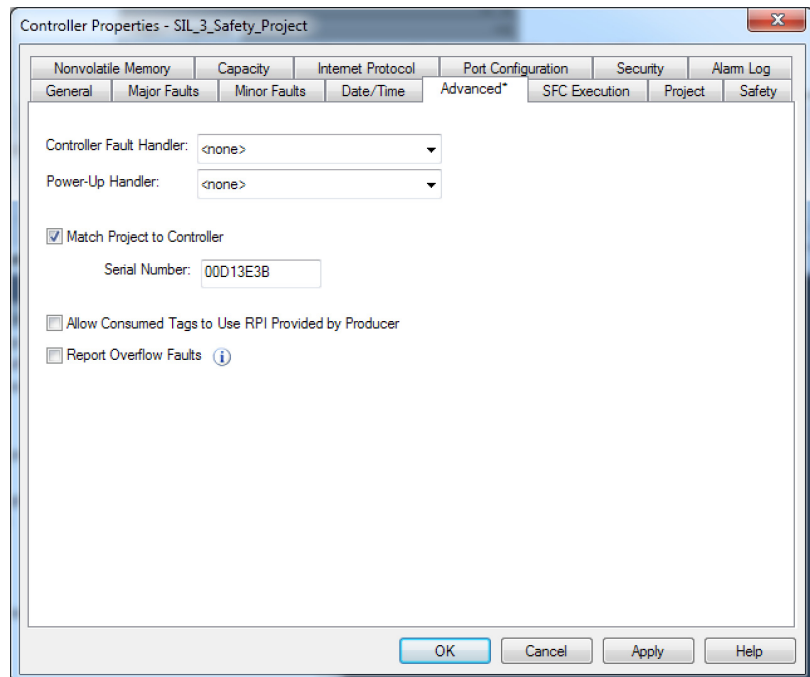
GuardLogix 5580

L'application Logix Designer détermine si vous pouvez passer en ligne avec un automate cible selon 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 affectent ces processus, notamment la fonctionnalité Project to Controller Match (Correspondance Projet/Automate), l'état de sécurité et les défauts, l'existence d'une signature de sécurité, l'état de verrouillage/déverrouillage de sécurité du projet et de l'automate, et le niveau de sécurité configuré en désaccord avec la présence ou l'absence d'un partenaire dans le châssis.

## Fonctionnalité Match Project to Controller

La fonctionnalité Match Project to Controller (Correspondance projet/ automate) affecte les processus de téléchargement, de transfert et de passage en ligne des projets standard et de sécurité. Cette fonctionnalité se trouve sous l'onglet Controller Properties Advanced (Propriétés avancées de l'automate).



Si la fonctionnalité Match Project to Controller (Correspondance projet/ automate) est activée dans le projet hors ligne, l'application Logix Designer compare le numéro de série de l'automate dans le projet hors ligne à celui de l'automate connecté. S'ils ne correspondent pas, vous devez annuler le téléchargement/transfert, vous connecter à l'automate correct ou confirmer que vous êtes connecté à l'automate correct qui met à jour le numéro de série dans le projet pour qu'il corresponde à 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 comme élément de la séquence de téléchargement.

---

**IMPORTANT** Pour mettre à jour le firmware de l'automate, commencez par installer un kit de mise à niveau du firmware. Un kit de mise à niveau est livré sur un DVD supplémentaire avec l'environnement Studio 5000®.

---

**CONSEIL** Vous pouvez également mettre à niveau le firmware en choisissant ControlFLASH Plus™ ou ControlFLASH™ dans le 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 sous l'onglet Safety (Sécurité) de la boîte de dialogue Controller Properties (Propriétés de l'automate).

## Signature de sécurité et état du verrouillage et du déverrouillage de la sécurité

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

La signature de sécurité et l'état du verrouillage de la 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.

Aux termes d'un transfert, la signature de sécurité du projet hors ligne correspond à celle de l'automate.

L'état du verrouillage de la sécurité est toujours transféré avec le projet, même en l'absence de signature de sécurité.

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

**Tableau 11 - Effets du verrouillage de sécurité et de la signature de sécurité sur l'opération de téléchargement**

État du verrouillage de sécurité	État de la signature de sécurité	Fonctionnalité de téléchargement
Automate déverrouillé	La signature de sécurité dans le projet hors ligne correspond à celle de l'automate.	Tous les composants de projet standard sont téléchargés. Les points de sécurité sont réinitialisés sur les valeurs qu'ils avaient à la création de la signature de sécurité. L'état du verrouillage de la sécurité correspond à l'état dans le projet hors ligne.
	Les signatures de sécurité ne correspondent pas.	Si l'automate avait une signature de sécurité, celle-ci est automatiquement supprimée et le projet est entièrement téléchargé. L'état du verrouillage de la sécurité correspond à l'état dans le projet hors ligne.
Sécurité de l'automate verrouillée	Les signatures de sécurité correspondent.	Si la sécurité est verrouillée dans le projet hors ligne et dans l'automate, tous les composants de projet standard sont téléchargés et les points de sécurité sont réinitialisés aux valeurs qu'ils avaient à la création de la signature de sécurité. Si la sécurité est déverrouillée dans le projet hors ligne mais qu'elle est verrouillée dans l'automate, le téléchargement est bloqué. Vous devrez d'abord déverrouiller l'automate pour permettre au téléchargement de se poursuivre.
	Les signatures de sécurité ne correspondent pas.	Vous devez d'abord déverrouiller la sécurité de l'automate pour permettre le téléchargement. Si l'automate avait une signature de sécurité, celle-ci est automatiquement supprimée et le projet est entièrement téléchargé. L'état du verrouillage de la sécurité correspond à l'état dans le projet hors ligne.

## Contrôles en vue du passage en ligne avec un automate GuardLogix

Pour un projet de sécurité, l'application Logix Designer contrôle les points suivants :

- Les numéros de série du projet hors ligne et de l'automate correspondent-ils (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 sécurité compatible ?

**Tableau 12 - Connexion à l'automate avec un projet de sécurité**

Si le logiciel indique	Alors
Unable to connect to controller (impossible de se connecter à l'automate) Mismatch between the offline project and the controller serial number (Discordance entre le projet hors ligne et le numéro de série de l'automate). Selected controller may be the wrong controller (L'automate choisi n'est peut-être pas le bon).	Connectez-vous au bon automate, sélectionnez un autre fichier projet ou cochez la case Update project serial number (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 : <ul style="list-style-type: none"> <li>• 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.</li> <li><b>IMPORTANT</b> : le projet en ligne sera supprimé.</li> <li>• Pour préserver le projet en ligne, annulez le processus de mise en ligne et installez une version de l'environnement du Studio 5000 compatible avec la révision du firmware de votre automate.</li> </ul>
You need to upload or download to go online by using the open project.	Choisissez l'une des options suivantes : <ul style="list-style-type: none"> <li>• Effectuez un transfert pour mettre à jour le projet hors ligne.</li> <li>• Effectuez un téléchargement pour mettre à jour le projet automate.</li> <li>• Sélectionnez File (Fichier) pour sélectionner un autre projet hors ligne.</li> </ul>
Unable to connect in a manner that preserves safety task signature. (impossible de se connecter en préservant la signature de la tâche de sécurité). The firmware minor revision on the controller is not compatible with safety signature in offline project (La révision mineure du firmware de l'automate est incompatible avec la signature de sécurité du projet hors ligne).	<ul style="list-style-type: none"> <li>• Pour préserver la signature de sécurité quand la révision 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.</li> <li>• Pour procéder au chargement malgré l'incompatibilité de signature de sécurité, cliquez sur Download. La signature de sécurité sera effacée.</li> <li><b>IMPORTANT</b> : le système de sécurité doit être revalidé.</li> </ul>
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 l'application Logix Designer sont en ligne, l'état du verrouillage de la sécurité et la signature de sécurité de l'automate correspondent à ceux du projet de l'automate. L'état du verrouillage de la sécurité et la signature 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.

## Téléchargement dans l'automate

### Concerne ces automates :

ControlLogix 5580

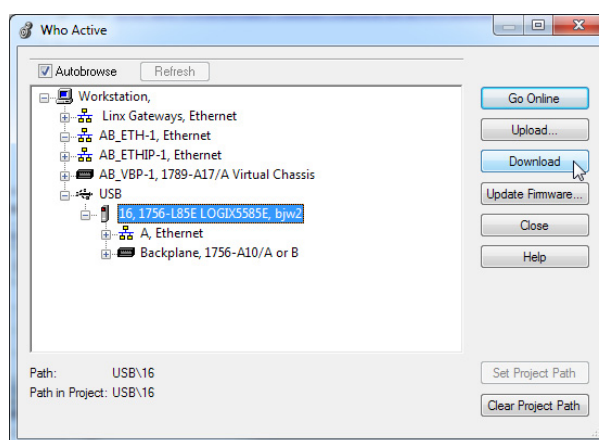
GuardLogix 5580

Lorsque vous téléchargez un projet vers l'automate, le projet de l'application Logix Designer est copié dans l'automate.

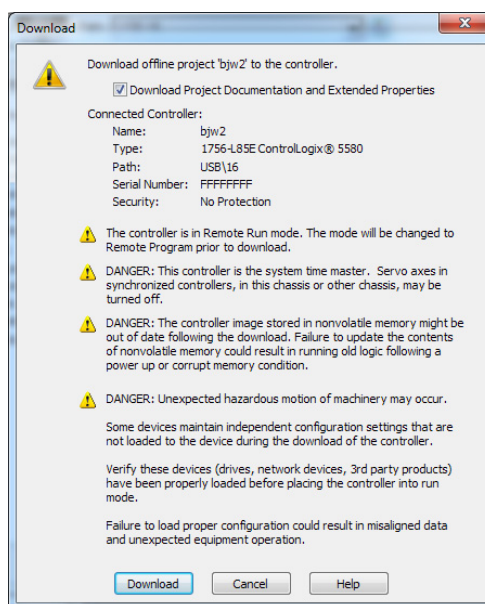
### Utilisation de Who Active

Vous pouvez utiliser les fonctionnalités de la boîte de dialogue Who Active (qui est actif) pour effectuer des téléchargements sur votre automate une fois que vous avez défini le chemin de communication. Exécutez ces étapes pour télécharger dans l'automate.

1. Après avoir choisi le chemin de communication, cliquez sur Download (Télécharger) dans la boîte de dialogue Who Active (Qui est actif).



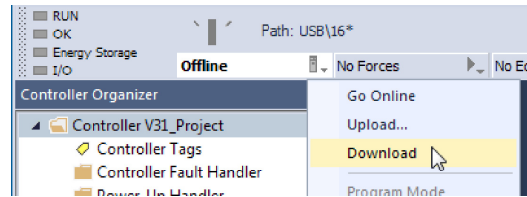
2. Après avoir lu les avertissements dans la boîte de dialogue Download, cliquez sur Download.



## Utilisation du menu Controller Status (État de l'automate)

Après avoir établi un chemin de communication dans l'application Logix Designer, vous pouvez utiliser le menu Controller Status (État de l'automate) pour procéder au téléchargement dans l'automate. Pour effectuer un téléchargement, choisissez Download (télécharger) dans le menu Controller Status.

Figure 17 - Téléchargement via le menu Controller Status



**CONSEIL** Après la fin du chargement, le nom du projet apparaît sur l'afficheur d'état défilant.

## Considérations supplémentaires relatives au téléchargement dans un automate GuardLogix

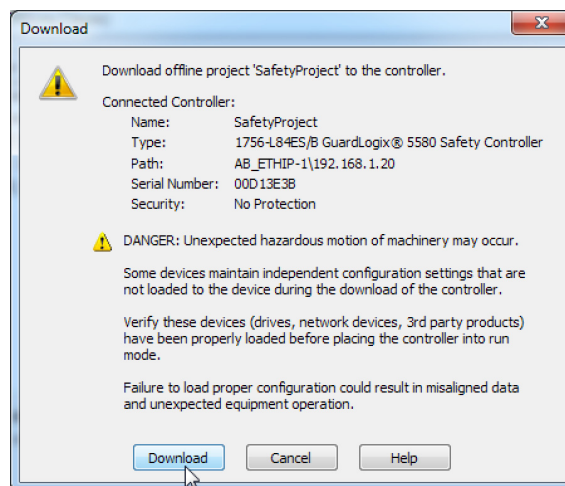
Concerne ces automates :

GuardLogix 5580

Pour un projet de sécurité, l'application Logix Designer compare les informations ci-après dans le projet hors ligne et dans 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 ;
- État de sécurité ;
- la signature de sécurité (s'il y en a une) ;
- l'état du verrouillage de la sécurité ;
- le partenaire de sécurité (s'il y en a un). L'application Logix Designer ne permet pas le téléchargement d'un projet configuré pour SIL 2 si un partenaire de sécurité se trouve à droite de l'automate principal.

Une fois les contrôles réussis, une boîte de dialogue de confirmation du téléchargement s'affiche. Cliquez sur Download.





L'application Logix Designer affiche les messages d'état dans le dialogue de téléchargement, l'écran d'avancement et la fenêtre des erreurs.

<b>Si le logiciel indique :</b>	<b>Alors :</b>
Unable to download to the controller. Mismatch between the offline project and the controller serial number. 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 n° 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). Choisissez la version requise, puis cliquez sur Update (Mise à jour). Cliquez sur Yes (Oui) pour confirmer votre choix.
Incapable de télécharger une application SIL 2, un partenaire de sécurité est présent.	Retirez le partenaire de sécurité.
Unable to download to controller. The safety partner is missing or unavailable.	Annulez le processus de téléchargement. Installez un partenaire de sécurité compatible avant de tenter à nouveau l'opération.
Unable to download to controller. The firmware revision of the safety partner is not compatible with the primary controller.	Mettez à jour la version du firmware du partenaire de sécurité. 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.
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 sécurité. <b>IMPORTANT</b> : le système de sécurité doit être revalidé.
Cannot download in a manner that preserves the safety task signature. La révision mineure de firmware de l'automate est incompatible avec la signature de la tâche de sécurité du projet hors ligne.	<ul style="list-style-type: none"> <li>En cas d'incompatibilité d'une révision mineure du firmware, mettez celui-ci 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 sécurité existante. Téléchargez ensuite le projet hors ligne.</li> <li>Pour procéder au chargement malgré l'incompatibilité de signature de sécurité, cliquez sur Download. La signature de sécurité sera effacée.</li> </ul> <b>IMPORTANT</b> : 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 à cocher Delete Signature (Effacer la signature) est sélectionnée et si vous choisissez Unlock (Déverrouiller), cliquez sur Yes (Oui) pour confirmer la suppression.
Téléchargement de la signature de sécurité	La signature de sécurité est présente dans le projet hors ligne et elle est en cours de chargement.
Retransférer la signature de sécurité...	La signature de sécurité est présente dans le projet hors ligne et n'est pas téléchargée, car une signature correspondante existe dans l'automate et est rechargée à partir de là.

Une fois le projet téléchargé avec succès, l'état du verrouillage de sécurité et la signature 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 sécurité.

## Transfert depuis l'automate

### Concerne ces automates :

ControlLogix 5580

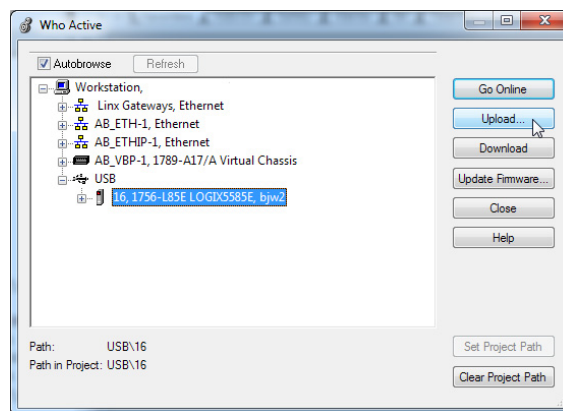
GuardLogix 5580

Lorsque vous transférez un projet à partir de l'automate, le projet est copié depuis l'automate vers l'application Logix Designer.

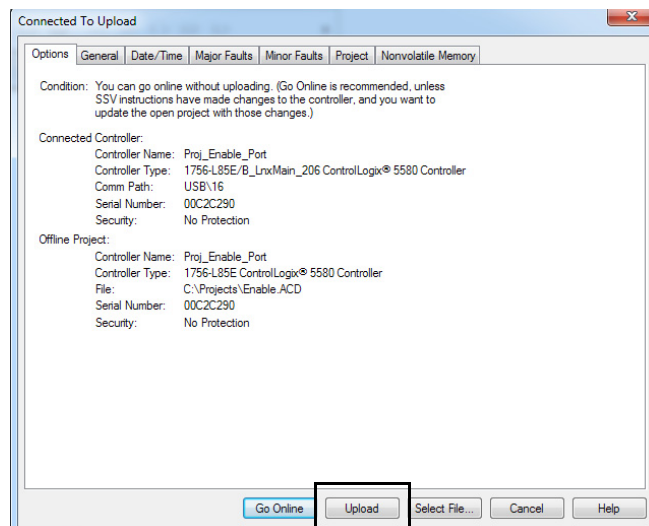
## Utilisation de Who Active

Vous pouvez utiliser les fonctionnalités de la boîte de dialogue Who Active (qui est actif) pour effectuer le transfert depuis votre automate une fois que vous avez défini le chemin de communication. Suivez les étapes ci-dessous pour transférer à partir de l'automate.

1. Après avoir choisi le chemin de communication, cliquez sur Upload (Transférer) dans la boîte de dialogue Who Active (Qui est actif).



2. Dans la boîte de dialogue Connected to Upload (Connecté pour transférer), vérifiez que le projet correspond bien à celui que vous souhaitez transférer.
3. Cliquez sur Upload (transférer).



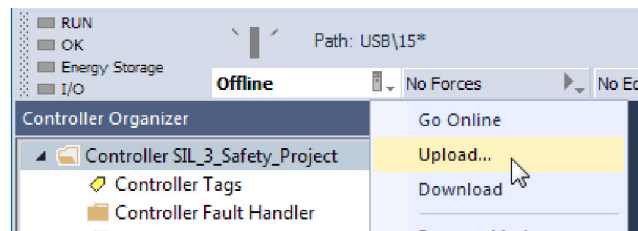
Pour plus d'informations sur la boîte de dialogue Connected to upload, consultez l'aide en ligne de Logix Designer.

## Utilisation du menu Controller Status

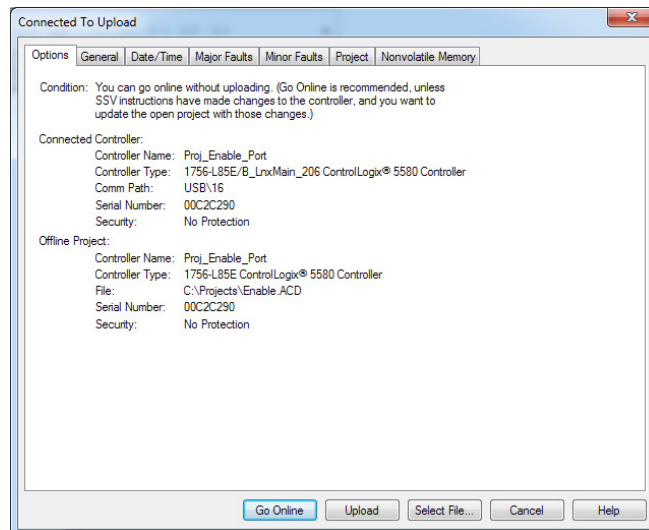
Après avoir établi un chemin de communication dans l'application Logix Designer, vous pouvez utiliser le menu Controller Status (État de l'automate) pour procéder au transfert depuis l'automate.

1. Depuis le menu Controller Status (État de l'automate), choisissez Upload (Transférer).

**Figure 18 - Transfert via le menu État de l'automate**



2. Dans la boîte de dialogue Connected to Upload (Connecté pour transférer), vérifiez que le projet correspond bien à celui que vous souhaitez transférer.
3. Cliquez sur Upload (transférer).



## Considérations supplémentaires relatives au transfert depuis un automate GuardLogix

### Concerne ces automates :

GuardLogix 5580

Pour un projet de sécurité, l'application Logix Designer compare les informations ci-après dans le projet et dans l'automate :

- le numéro de série de l'automate (si la fonction Project to Controller Match est sélectionnée) ;
- le projet ouvert et le projet de l'automate ;
- les versions majeures et mineures du firmware ;
- la signature de sécurité (s'il y en a une) ;

**IMPORTANT** Un transfert est autorisé quel que soit l'état de sécurité et l'état de verrouillage de la sécurité du projet hors ligne et de l'automate. L'état du verrouillage suit l'état du projet transféré.

Comportement au transfert :	Réponse :
Si la fonction Project to Controller Match (Concordance Projet/Automate) est sélectionnée, l'application Logix Designer vérifie si le numéro de série du projet ouvert correspond à celui de l'automate.	<ul style="list-style-type: none"> <li>• Connectez-vous au bon automate ou vérifiez qu'il s'agit bien de l'automate approprié.</li> <li>• Sélectionnez un nouveau projet à transférer ou choisissez un autre projet avec Select File (Sélection fichier).</li> <li>• 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.</li> </ul>
L'application Logix Designer vérifie si le projet ouvert correspond bien à celui de l'automate.	<ul style="list-style-type: none"> <li>• Si ces projets ne correspondent pas, vous devrez sélectionner un fichier approprié ou annuler le transfert.</li> <li>• Si les projets correspondent, le logiciel recherchera les éventuelles variations existant dans le projet hors ligne (ouvert).</li> </ul>
L'application Logix Designer recherche les éventuelles modifications du projet hors ligne.	<ul style="list-style-type: none"> <li>• 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).</li> <li>• 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.</li> </ul>
Uploading safety signature...	Ce message n'apparaît lors du téléchargement que si une signature de sécurité correspondant à celle de l'automate n'existe pas dans le projet hors ligne.

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

**CONSEIL** Avant le téléchargement, si une signature de sécurité hors ligne existe ou si la sécurité du projet hors ligne est verrouillée mais que la sécurité de l'automate est déverrouillée ou n'a pas de signature de sécurité, la signature de sécurité et l'état verrouillé hors ligne sont remplacées par les valeurs en ligne (sécurité déverrouillée sans signature de sécurité). Si vous ne souhaitez pas que ces modifications deviennent définitives, n'enregistrez pas le projet hors ligne après le transfert.


## Choix du mode de fonctionnement de l'automate

Référez-vous au tableau ci-après lorsque vous déterminez le mode de fonctionnement de votre automate.

### Concernes ces automates :

ControlLogix 5580

GuardLogix 5580

Position du sélecteur à clé <sup>(1)</sup>	Modes automate disponibles	Dans ce mode, vous pouvez :	Dans ce mode, vous ne pouvez pas :	 <b>ATTENTION :</b>
RUN	<b>Mode Run (Exécution)</b> – L'automate commande activement le procédé/la machine. Les projets ne peuvent pas être modifiés par l'application Logix Designer lorsqu'on se trouve dans ce mode.	<ul style="list-style-type: none"> <li>Mettre les sorties dans l'état commandé par la logique du projet</li> <li>Exécuter (scruter) les tâches</li> <li>Envoyer des messages</li> <li>Envoyer et recevoir des données en réponse à un message d'un autre automate</li> <li>Produire et consommer des points</li> </ul>	<ul style="list-style-type: none"> <li>Mettre les sorties à leur état configuré pour le mode Programmation</li> <li>Change le mode de l'automate via l'application Logix Designer</li> <li>Télécharger un projet</li> <li>Planifier un réseau ControlNet®</li> <li>Étant en ligne, modifier le projet</li> </ul>	Le mode Exécution est utilisé uniquement lorsque toutes les conditions sont sûres.
REM	<b>Mode Remote Run</b> (Exécution à distance) – Ce mode est identique au mode Exécution, sauf que vous pouvez modifier le projet en ligne et modifier le mode de l'automate via l'application Logix Designer.	<ul style="list-style-type: none"> <li>Mettre les sorties dans l'état commandé par la logique du projet</li> <li>Exécuter (scruter) les tâches</li> <li>Change le mode de l'automate via l'application Logix Designer</li> <li>Étant en ligne, modifier le projet</li> <li>Envoyer des messages</li> <li>Envoyer et recevoir des données en réponse à un message d'un autre automate</li> <li>Produire et consommer des points</li> </ul>	<ul style="list-style-type: none"> <li>Mettre les sorties à leur état configuré pour le mode Programmation</li> <li>Télécharger un projet</li> <li>Planifier un réseau ControlNet</li> </ul>	En mode Exécution à distance, vous pouvez modifier un fichier de projet en ligne. Assurez-vous de commander les sorties avec précaution pour éviter de blesser le personnel et d'endommager l'équipement.
	<b>Mode Remote Program</b> (Programmation à distance) – Ce mode fonctionne comme le mode Programmation, sauf que vous pouvez changer le mode de l'automate via l'application Logix Designer.	<ul style="list-style-type: none"> <li>Mettre les sorties à leur état configuré pour le mode Programmation</li> <li>Change le mode de l'automate via l'application Logix Designer</li> <li>Télécharger un projet</li> <li>Planifier un réseau ControlNet</li> <li>Étant en ligne, modifier le projet</li> <li>Envoyer et recevoir des données en réponse à un message d'un autre automate</li> <li>Produire et consommer des points</li> </ul>	<ul style="list-style-type: none"> <li>Mettre les sorties dans l'état commandé par la logique du projet</li> <li>Exécuter (scruter) les tâches</li> </ul>	Les sorties sont commandées dans leur état de mode Programmation, ce qui peut provoquer une situation dangereuse.
	<b>Mode Remote Test</b> (Test à distance) – Ce mode automate exécute le code, mais les E/S ne sont pas contrôlées. Vous pouvez modifier le projet en ligne et modifier le mode de l'automate via l'application Logix Designer. Les modules de sortie sont commandés dans leur état de mode Programmation (On, Off ou Maintien).	<ul style="list-style-type: none"> <li>Mettre les sorties à leur état configuré pour le mode Programmation</li> <li>Exécuter (scruter) les tâches</li> <li>Change le mode de l'automate via l'application Logix Designer</li> <li>Étant en ligne, modifier le projet</li> <li>Envoyer des messages</li> <li>Envoyer et recevoir des données en réponse à un message d'un autre automate</li> <li>Produire et consommer des points</li> </ul>	<ul style="list-style-type: none"> <li>Mettre les sorties dans l'état commandé par la logique du projet</li> <li>Télécharger un projet</li> <li>Planifier un réseau ControlNet</li> <li>Envoyer des messages</li> </ul>	
<b>Mode Program</b> (Programmation) – Ce mode automate n'exécute pas de code ni ne commande les E/S, mais des opérations de modification sont disponibles. Les modules de sortie sont commandés dans leur état de mode Programmation (On, Off ou Maintien). Dans cette position, les modes de l'automate ne peuvent pas être modifiés via l'application Logix Designer.	<ul style="list-style-type: none"> <li>Mettre les sorties à leur état configuré pour le mode Programmation</li> <li>Télécharger un projet</li> <li>Planifier un réseau ControlNet</li> <li>Étant en ligne, modifier le projet</li> <li>Envoyer et recevoir des données en réponse à un message d'un autre automate</li> <li>Produire et consommer des points</li> </ul>	<ul style="list-style-type: none"> <li>Mettre les sorties dans l'état commandé par la logique du projet</li> <li>Exécuter (scruter) les tâches</li> <li>Change le mode de l'automate via l'application Logix Designer</li> <li>Envoyer des messages</li> </ul>		
PROG	<b>Mode Program</b> (Programmation) – Ce mode automate n'exécute pas de code ni ne commande les E/S, mais des opérations de modification sont disponibles. Les modules de sortie sont commandés dans leur état de mode Programmation (On, Off ou Maintien). Dans cette position, les modes de l'automate ne peuvent pas être modifiés via l'application Logix Designer.	<ul style="list-style-type: none"> <li>Mettre les sorties à leur état configuré pour le mode Programmation</li> <li>Télécharger un projet</li> <li>Planifier un réseau ControlNet</li> <li>Étant en ligne, modifier le projet</li> <li>Envoyer et recevoir des données en réponse à un message d'un autre automate</li> <li>Produire et consommer des points</li> </ul>	<ul style="list-style-type: none"> <li>Mettre les sorties dans l'état commandé par la logique du projet</li> <li>Exécuter (scruter) les tâches</li> <li>Change le mode de l'automate via l'application Logix Designer</li> <li>Envoyer des messages</li> </ul>	N'utilisez pas le mode Programmation comme arrêt d'urgence (E-stop). Le mode programmation n'est pas un dispositif de sécurité. Les sorties sont commandées dans leur état de mode Programmation, ce qui peut provoquer une situation dangereuse.

(1) Le déplacement du sélecteur à clé de Run (Exécution) à Remote (Distance) laisse l'automate en mode Remote Run, (Exécution à distance) tandis que le déplacement du sélecteur de Program à Remote laisse l'automate en mode Remote Program (Programmation à distance). Vous ne pouvez pas choisir le mode Test à distance par le seul sélecteur de mode ; ce choix est uniquement disponible par l'application Logix Designer.

## Utilisation du sélecteur à clé pour changer le mode de fonctionnement

Pour changer le mode de fonctionnement, utilisez le sélecteur à clé. Le sélecteur à clé de l'automate fournit un moyen mécanique d'améliorer la sécurité de l'automate et du système de commande. Vous devez déplacer physiquement le sélecteur de mode sur l'automate pour changer son mode de fonctionnement de RUN, à REM ou à PROG.

Lorsque le sélecteur de mode de l'automate est réglé sur le mode RUN (Exécution), des fonctionnalités telles que la modification en ligne, les téléchargements de programmes et les mises à jour de firmware sont interdites. Consultez [Choix du mode de fonctionnement de l'automate, page 85](#) pour la liste complète des fonctionnalités prohibées.

Le sélecteur à clé physique peut compléter d'autres méthodes d'autorisation et d'authentification qui contrôlent de la même manière l'accès des utilisateurs à l'automate, comme le service FactoryTalk® Security.

---

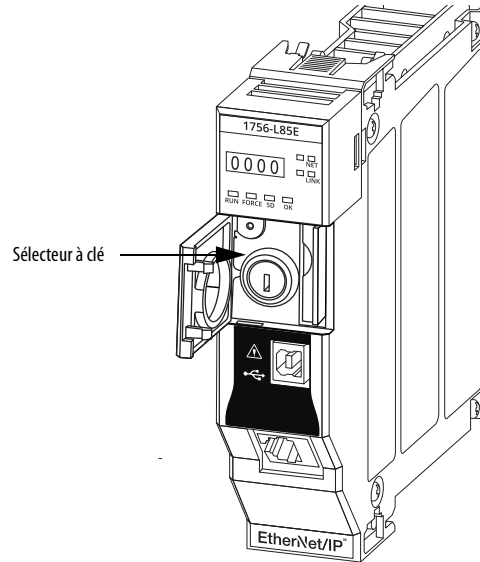
**IMPORTANT** Pendant le temps d'exécution, nous vous recommandons de placer le sélecteur à clé de l'automate sur la position RUN et de retirer la clé (le cas échéant) du sélecteur. Ceci contribuera à décourager les accès non autorisés à l'automate ou à éviter tout risque de modification intempestive de son programme, de sa configuration ou d'un firmware de périphérique.

Placez le sélecteur à clé de mode sur REM ou PROG pendant la mise en service et la maintenance de l'automate et chaque fois qu'un accès temporaire est nécessaire pour modifier le programme, la configuration ou le firmware du produit.

---

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

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



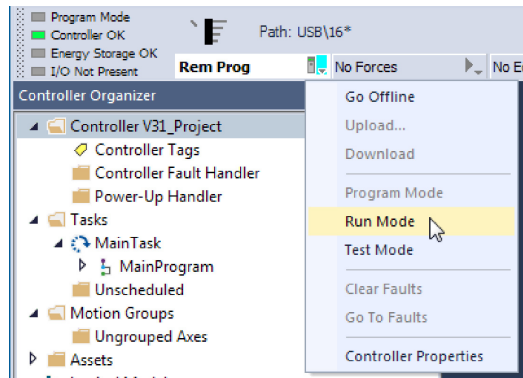
## Utilisation de Logix Designer pour changer le mode de fonctionnement

Lorsque vous êtes en ligne avec l'automate, et que le sélecteur à clé de l'automate est réglé sur REM (À distance, position centrale), vous pouvez utiliser Logix Designer pour changer le mode de fonctionnement.

Le menu d'état de l'automate vous permet de spécifier ces modes de fonctionnement :

- Programmation à distance
- Exécution à distance
- Test à distance

Figure 19 - Mode de fonctionnement



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



## Bouton réinitialisation

---

### Concerne ces automates :

---

ControlLogix 5580

---

GuardLogix 5580

---

Vous pouvez réinitialiser les automates ControlLogix® et GuardLogix, ainsi que le partenaire de sécurité 1756-L8SP avec le bouton de réinitialisation. Le bouton de réinitialisation est lu uniquement pendant une mise sous tension ou un redémarrage. Si vous appuyez sur le bouton de réinitialisation à un autre moment, l'enfoncement n'a aucun effet.

Pour un automate GuardLogix, l'état du verrouillage de sécurité ou la signature de sécurité ne vous empêche pas d'effectuer une réinitialisation de l'automate. Du fait que l'application est effacée de l'automate pendant la réinitialisation, le niveau de sécurité de l'automate est également effacé. Lorsque vous téléchargez un projet de sécurité dans l'automate, le niveau de sécurité est fixé au niveau spécifié dans le projet.

L'automate a deux types de réinitialisation :

- Une réinitialisation de type 1 efface le programme d'application et la mémoire, mais conserve l'adresse IP, tous les réglages réseau et la révision du firmware. Une réinitialisation de type 1 ne se produit que si l'automate contient une application utilisateur. Consultez [Réinitialisation de type 1, page 90](#).
- Une réinitialisation de type 2 rétablit les paramètres d'origine de l'automate (y compris le firmware), et efface tous les réglages réseau. Une réinitialisation de type 2 se produit uniquement si l'automate ne contient pas d'application utilisateur et que le firmware actuel de l'automate n'est pas une révision 1.x. Consultez [Réinitialisation de type 2, page 91](#).

La réinitialisation du partenaire de sécurité remet ses réglages en condition d'origine (y compris le firmware). Consultez [Réinitialisation du partenaire de sécurité, page 93](#).

---

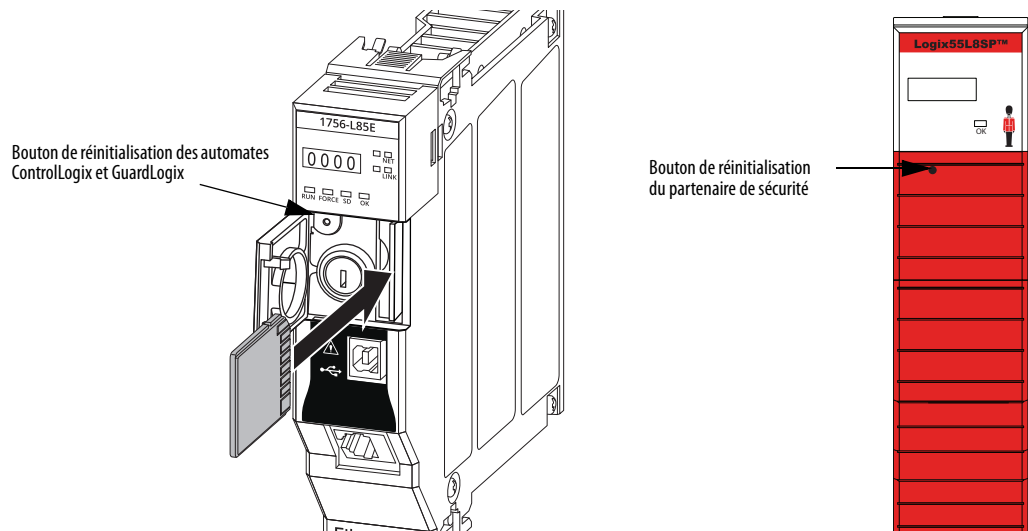
**IMPORTANT** Étant donné que l'état de validation/désactivation de port est associé au programme d'application, le port Ethernet de l'automate devient activé après une réinitialisation de type 1 ou de type 2.

---



**AVERTISSEMENT** : Lorsque vous appuyez sur le bouton de réinitialisation alors que l'alimentation est appliquée, 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 la zone n'est pas dangereuse avant de poursuivre.

---



## Réinitialisation de type 1

La réinitialisation de type 1 :

- efface le programme d'application ;
- conserve les paramètres réseau du port Ethernet embarqué ;
- conserve les informations APR (info position de mouvement) ;
- conserve tous les paramètres de configuration PTP (Synchronisation temporelle) ;
- conserve Wall Clock Time dans les capacités de rétention énergétique du module ;
- crée un enregistrement horodaté dans le journal de l'automate lorsqu'un événement de réinitialisation de type 1 se produit ;
- réinitialise l'automate pour commencer le processus de démarrage de l'automate ;
- évite que l'automate ne charge le firmware ou le logiciel à partir d'une carte SD au démarrage initial après la réinitialisation, quels que soient les paramètres de la carte SD, et sans modifier le contenu de la carte SD (le paramètre de protection en écriture n'est pas concerné) ; la carte SD sera rechargée (si elle est configurée pour le faire) lors des mises sous tension ultérieures ;
- active le port Ethernet, s'il avait été préalablement désactivé.

Pour réaliser une réinitialisation de type 1, procédez comme suit. Ce processus présume qu'une carte SD est installée dans l'automate.

1. Mettez l'automate hors tension.
2. Retirez la clé du sélecteur à clé.
3. Ouvrez la porte frontale de l'automate.

4. Utilisez un petit outil ayant le diamètre d'un trombone, pour appuyer et maintenir le bouton de réinitialisation. Le bouton est en retrait du panneau.
5. Tout en maintenant le bouton de réinitialisation enfoncé, mettez l'automate sous tension.
6. Continuez à maintenir le bouton de réinitialisation pendant que l'afficheur à 4 caractères fait défiler CLR, 4, 3, 2, 1, Project Cleared.
7. Après l'apparition de Project Cleared, relâchez le bouton de réinitialisation.

---

**IMPORTANT** Si vous relâchez le bouton de réinitialisation avant que Project Cleared (Projet effacé) ne défile sur l'afficheur, l'automate poursuit la mise sous tension et ne se réinitialise pas.

---

Après l'exécution d'une réinitialisation de type 1, chargez un projet d'application Logix Designer dans l'automate d'une des façons suivantes :

- Téléchargez le projet à partir de l'application Logix Designer - Pour plus d'informations, reportez-vous à [Téléchargement dans l'automate, page 79](#)
- Coupez et remettez l'automate sous tension pour charger un projet depuis la carte SD.

Cette option ne fonctionne que si le projet stocké sur la carte SD est configuré pour charger le projet à la mise sous tension.

## Réinitialisation de type 2

La réinitialisation de type 2 :

- remet le firmware du module à la révision 1.x, (c'est-à-dire la révision de firmware d'origine) ;
- efface tous les réglages utilisateur en condition d'origine, y compris les réglages de réseau et de synchronisation temporelle ;
- réinitialise l'automate pour commencer le processus de démarrage de l'automate ;
- il n'y aura aucune saisies dans le journal de l'automate après une réinitialisation de type 2, mais les enregistrements sauvegardés sur la carte SD sont conservés.

Pour réaliser une réinitialisation de type 2, procédez comme suit :

1. mettez l'automate hors tension ;
2. retirez la clé du sélecteur à clé ;
3. ouvrez la porte frontale de l'automate ;
4. retirez la carte SD.

5. Utilisez un petit outil ayant le diamètre d'un trombone, pour appuyer et maintenir le bouton de réinitialisation. Le bouton est en retrait du panneau.
6. Tout en maintenant le bouton de réinitialisation enfoncé, mettez l'automate sous tension.
7. Continuez à maintenir le bouton de réinitialisation pendant que l'afficheur à 4 caractères fait défiler DFLT, 4, 3, 2, 1, Factory Default
8. Après l'apparition de Factory Default, relâchez le bouton de réinitialisation.
9. Sur votre station de travail, supprimez tous les fichiers de la carte SD.
10. Mettez l'automate hors tension.
11. Réinstallez la carte SD.
12. Mettez l'automate sous tension.
13. Vérifiez que l'automate est à la révision de firmware 1.x, et que l'automate est réglé pour DHCP.

Après une réinitialisation de type 2 vous devez effectuer les tâches suivantes pour utiliser à nouveau l'automate :

- Configurer les ports Ethernet, régler le mode EtherNet/IP souhaité, et ensuite régler la configuration d'adresse IP de l'automate. Pour plus d'informations, reportez-vous à [Connexion à un automate, page 51](#).
- Mettez à jour la révision du firmware – Pour plus d'informations, reportez-vous à [Mise à jour du firmware de l'automate, page 54](#).
- Téléchargez un projet d'application Logix Designer dans l'automate de l'une des façons suivantes :
  - téléchargez le projet à partir de l'application Logix Designer - Pour plus d'informations, reportez-vous à [Téléchargement dans l'automate, page 79](#).
  - Coupez et remettez l'automate sous tension pour charger un projet depuis la carte SD. Cette option ne fonctionne que si le projet stocké sur la carte SD est configuré pour charger le projet à la mise sous tension.

## Réinitialisation du partenaire de sécurité

Exécutez ces étapes pour réinitialiser un partenaire de sécurité :

1. mettez le partenaire de sécurité hors tension.
2. utilisez un petit outil ayant le diamètre d'un trombone, pour appuyer et maintenir le bouton de réinitialisation. Ce bouton est en retrait de 5 mm (0,19 po) derrière le panneau.
3. tout en maintenant le bouton de réarmement enfoncé, remettez le partenaire de sécurité sous tension.
4. continuez à maintenir le bouton de réinitialisation pendant que l'afficheur à 4 caractères fait défiler DFLT, 4, 3, 2, 1, Factory Default.
5. Après l'apparition de Factory Default, relâchez le bouton de réinitialisation.

**Notes :**

## Utilisation de la carte Secure Digital

Rubrique	Page
Considérations relatives au stockage et au transfert d'un projet de sécurité	97
Stockage sur la carte SD	98
Chargement depuis la carte SD	103
Autres tâches de la carte Secure Digital	106

### Concerné ces automates :

ControlLogix 5580

GuardLogix 5580

Les automates sont fournis avec une carte Secure Digital (SD) installée. Nous vous conseillons de laisser la carte SD installée de sorte que si un défaut se produit, les données de diagnostic sont automatiquement écrites sur la carte. Rockwell Automation peut alors utiliser les données pour faciliter le diagnostic de la défaillance.

Nous vous conseillons d'utiliser les cartes SD disponibles auprès de Rockwell Automation:

- Carte SD 2 Go, référence 1784-SD2.
- Carte SD CodeMeter CmCard, 4 Go, référence 9509-CMSDCD4 (lorsque les fonctionnalités de protection de la source et de protection de l'exécution basées sur licence sont activées).

Bien que d'autres cartes SD puissent être utilisées avec l'automate, Rockwell Automation n'a pas testé l'utilisation de ces cartes avec l'automate et il se peut qu'il se produise une corruption ou des pertes de données.

Les cartes SD non fournies par Rockwell Automation peuvent avoir des valeurs nominales industrielles, environnementales et d'homologation différentes de celles des cartes disponibles auprès de Rockwell Automation. Ces cartes peuvent avoir des problèmes de durée de vie dans les environnements industriels pour lesquels les versions de qualité industrielle de Rockwell Automation sont conçues.

La carte mémoire compatible avec votre automate ControlLogix® est utilisée pour transférer ou stocker le contenu de la mémoire utilisateur de l'automate.

Lorsque vous utilisez la fonction Store, le projet qui est stocké sur la carte SD correspond au projet dans la mémoire de l'automate à ce moment-là. Les modifications que vous effectuez après avoir stocké le projet ne sont pas traduites dans le projet sur la carte SD.

Si vous apportez des modifications au projet dans la mémoire de l'automate mais que vous ne stockez pas ces modifications, au prochain chargement du projet dans l'automate à partir de la carte SD, ces modifications sont écrasées.

---

**IMPORTANT** Ne retirez pas la carte SD lorsque l'automate est en train de lire la carte ou d'écrire sur celle-ci. Si vous retirez la carte pendant l'une ou l'autre des opérations, les données sur la carte ou l'automate risquent de devenir corrompues.

Au moment où la carte est retirée, le firmware de l'automate peut aussi devenir corrompu. Laissez la carte dans l'automate jusqu'à ce que le voyant d'état OK passe au vert fixe.

---

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 la carte, l'état du verrouillage de la sécurité et la signature de sécurité sont affichés.

Le projet doit être en ligne pour pouvoir visualiser le contenu de la carte SD.

Pour des informations détaillées sur l'utilisation de la mémoire non volatile, reportez-vous à la publication [1756-PM017](#), « Logix 5000 Controllers Nonvolatile Memory Programming Manual ».



## Considérations relatives au stockage et au transfert d'un projet de sécurité

---

### Concerne ces automates :

---

GuardLogix 5580

---

Seuls les automates GuardLogix® 5380 prennent en charge des projets de sécurité. Les automates ControlLogix 5580 ne prennent pas en charge des projets 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 aussi enregistré sur la carte SD.

S'il n'y a pas de projet d'application dans l'automate, vous ne pourrez enregistrer 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) préexistante.

Si une signature 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 enregistrés avec leurs valeurs actuelles ;
- la signature de sécurité actuelle est sauvegardée.

Lorsque vous stockez un projet d'application de sécurité sur une carte SD, Rockwell Automation vous recommande de sélectionner Programme (à distance uniquement) comme mode de chargement, c'est-à-dire le mode dans lequel l'automate entre après le chargement d'un projet à partir de la carte SD.

---

**IMPORTANT** Pour éviter que le firmware stocké sur la carte SD n'écrase le firmware qui vient d'être mis à jour :

- Le processus de mise à jour vérifie d'abord l'option de chargement sur la carte SD, et transforme cette option en User Initiated (Initié par l'utilisateur), si nécessaire.
- La mise à jour du firmware a lieu.
- L'automate se réinitialise.
- L'option de chargement reste définie à User Initiated.

Si la carte SD est verrouillée, l'option de transfert ne change pas et le firmware qui est stocké sur la carte SD peut écraser le firmware qui vient d'être mis à jour.

---

## Stockage sur la carte SD

### Concernes ces automates :

ControlLogix 5580

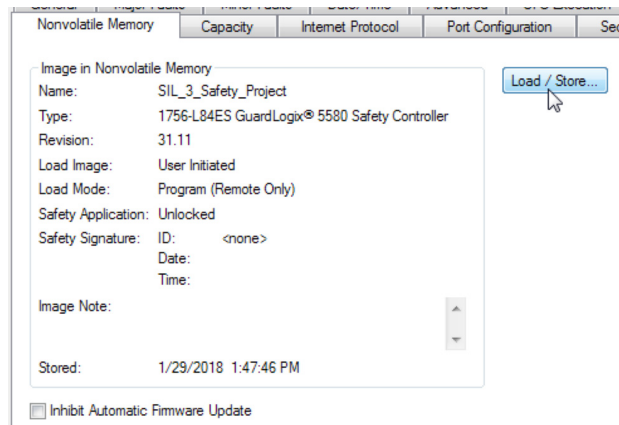
GuardLogix 5580

Nous vous recommandons de sauvegarder régulièrement votre projet Logix Designer sur une carte SD.

Si un défaut majeur irrécupérable se produit, qui supprime le programme de la mémoire de l'automate, la copie de sauvegarde sur la carte SD peut être restaurée automatiquement dans l'automate pour reprendre rapidement le fonctionnement normal.

Pour enregistrer un projet sur la carte SD, procédez comme suit.


1. Assurez-vous que l'automate est en ligne et en mode Programmation ou Programmation à distance.
2. Cliquez avec le bouton droit de la souris sur le nom de l'automate puis choisissez Properties (Propriétés).
3. À l'onglet Nonvolatile Memory (Mémoire non volatile), cliquez sur Load/Store (Charger/Enregistrer).



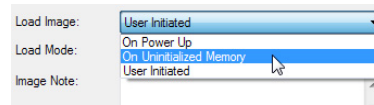
**CONSEIL** Si Load/Store (Charger/Stocker) est en grisé (indisponible), vérifiez les points suivants :

- l'automate est en mode Programmation ou Programmation à distance ;
- vous avez spécifié le chemin de communication correct ;
- la carte SD est installée ;
- la carte SD est déverrouillée. L'état verrouillé apparaît dans le coin inférieur gauche de la boîte de dialogue Nonvolatile memory/Load Store (Mémoire non volatile/Charger Stocker).

Si la carte SD n'est pas installée, un message dans le coin inférieur gauche de l'onglet Nonvolatile Memory (Mémoire non volatile) indique la carte manquante.

 Nonvolatile memory not present.

#### 4. Changez les propriétés du chargement de l'image en fonction des exigences de votre application.



Ce tableau décrit les options de chargement de l'image.

**Tableau 13 - Options de chargement d'image**

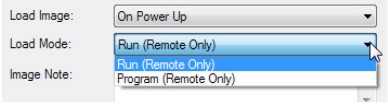
Si vous souhaitez charger le projet	Sélectionnez cette option de chargement d'image	Remarques	Consignes de sécurité
Chaque fois que vous mettez ou remettez sous tension	À la mise sous tension	<ul style="list-style-type: none"> <li>Lors d'une remise sous tension, vous perdrez toutes les modifications effectuées en ligne ainsi que les valeurs de point et les planifications réseau qui n'auront pas été enregistrées dans la mémoire non volatile.</li> <li>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.</li> <li>Vous pouvez toujours utiliser l'application Studio 5000 Logix Designer® pour charger le projet.</li> </ul>	<ul style="list-style-type: none"> <li>Pour une application de sécurité, le chargement à la mise sous tension a lieu que la sécurité de l'automate soit verrouillée ou non ou qu'il y ait une signature de sécurité ou pas.</li> </ul>
Lorsqu'il n'y a pas de projet dans l'automate et que vous mettez ou remettez le châssis sous tension.	Sur mémoire non initialisée	<ul style="list-style-type: none"> <li>Si le projet a été effacé de la mémoire, cette option recharge le projet dans l'automate à la mise sous tension.</li> <li>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, Programme ou Exécution.</li> <li>Vous pouvez toujours utiliser l'application Logix Designer pour charger le projet.</li> </ul>	<ul style="list-style-type: none"> <li>L'automate met aussi à jour le firmware du partenaire de sécurité, si nécessaire.</li> </ul>
Uniquement au moyen de l'application Logix Designer	Lancement par l'utilisateur	<ul style="list-style-type: none"> <li>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.</li> </ul>	<ul style="list-style-type: none"> <li>Vous pouvez lancer le chargement, quel que soit l'état de sécurité.</li> <li>Le chargement d'un projet sur un automate dont la sécurité est verrouillée n'est autorisé que si la signature de sécurité du projet enregistré dans la mémoire non volatile correspond au projet dans l'automate.</li> <li>Si les signatures ne correspondent pas ou si la sécurité de l'automate est verrouillée sans signature de sécurité, vous êtes invité à déverrouiller préalablement l'automate.</li> <li><b>IMPORTANT :</b> lorsque vous déverrouillez l'automate et que vous lancez le chargement du projet depuis la mémoire non volatile, l'état du verrouillage de la sécurité, les mots de passe et la signature de sécurité sont définis sur les valeurs enregistrées dans la mémoire non volatile aux termes de l'opération.</li> <li>Si le firmware de l'automate principal correspond à la révision dans la mémoire non volatile, le firmware du partenaire de sécurité est mis à jour, si nécessaire, l'application stockée dans la mémoire non volatile est chargée de sorte que l'état de la tâche de sécurité devienne la tâche de sécurité opérationnelle et que l'automate passe en mode programme.</li> </ul>

**IMPORTANT** Pour éviter que le firmware qui est stocké sur la carte SD n'écrase le firmware qui vient d'être mis à jour :

- Le processus de mise à jour vérifie d'abord l'option de chargement sur la carte SD, et transforme cette option en User Initiated (Initié par l'utilisateur), si nécessaire.
- La mise à jour du firmware a lieu.
- L'automate se réinitialise.
- L'option de chargement reste définie à User Initiated.

Si la carte SD est verrouillée, l'option de chargement ne change pas et le firmware qui est stocké sur la carte SD peut écraser le firmware qui vient d'être mis à jour.

5. Définissez les propriétés du mode de chargement en fonction des exigences de votre application.

Si vous souhaitez que l'automate passe dans ce mode après le chargement	Choisissez	Éléments du menu
Programme	Programmation (à distance uniquement)	
Marche	Exécution (à distance uniquement)	

**IMPORTANT Considérations relatives à la sécurité**

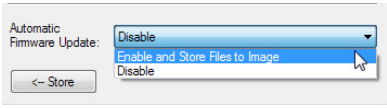
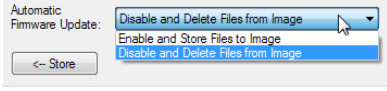

Rockwell Automation vous conseille d'utiliser Program (Remote Only) [Programmation à distance uniquement] lorsque vous définissez le mode de chargement pour un projet d'application de sécurité.

6. Selon les exigences de votre application, définissez les propriétés de mise à jour automatique du firmware des dispositifs d'E/S dans l'arborescence de configuration de l'automate. La propriété Mise à jour automatique du firmware est également appelée fonction de supervision du firmware.

**IMPORTANT Considérations relatives à la sécurité**

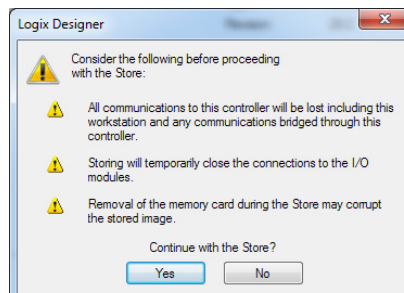
Certains dispositifs d'E/S de sécurité ne prennent pas en charge la fonction de supervision du firmware, Firmware Supervisor. Par exemple, les dispositifs d'E/S de sécurité sur les réseaux DeviceNet® et les modules POINT Guard I/O™ ne prennent pas en charge la fonctionnalité Firmware Supervisor.

Ce tableau décrit les options Automatic Firmware Update pour les dispositifs d'E/S.

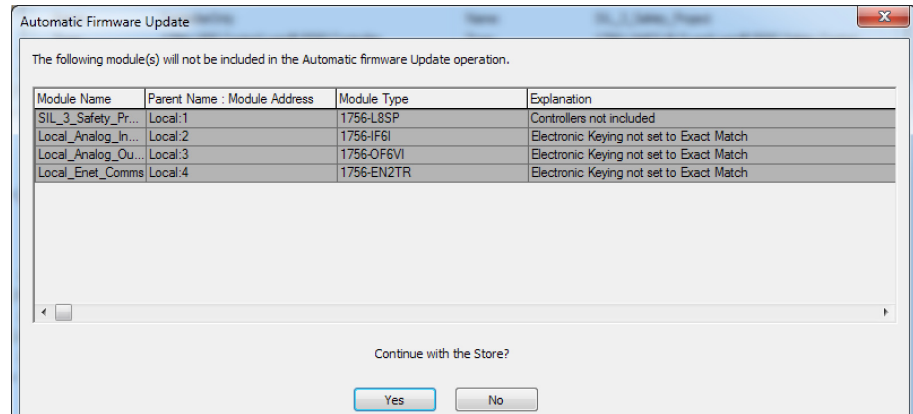
Réglage	Description	Éléments du menu
Disable	Désactive toute mise à jour automatique du firmware. Cet élément n'apparaît dans le menu qu'à l'enregistrement initial de l'image.	
Valider et stocker les fichiers dans l'image	Permet les mises à jour automatiques du firmware pour les dispositifs d'E/S figurant dans l'arborescence de configuration de l'automate. Sauvegarde le firmware du dispositif d'E/S et le firmware de l'automate dans l'image. Seuls les dispositifs d'E/S qui sont configurés en détrompage par correspondance exacte participent au processus de mise à jour automatique du firmware. <sup>(1)</sup>	
Disable and Delete Files from Image (désactiver et supprimer les fichiers de l'image)	Désactive les mises à jour automatiques de firmware pour les dispositifs d'E/S figurant dans l'arborescence de configuration de l'automate. Supprime le firmware du dispositif d'E/S de l'image, mais ne supprime pas le firmware de l'automate de l'image. Cet élément apparaît uniquement dans le menu lors des sauvegardes subséquentes de l'image.	

(1) Les dispositifs d'E/S utilisés avec cette option doivent être compatibles avec la version de firmware à laquelle on souhaite les actualiser.

7. Cliquez sur Store (Stockage).
8. Cliquez sur Yes (Oui) dans la boîte de dialogue de confirmation qui apparaît.



Si vous avez activé la mise à jour automatique du firmware, une boîte de dialogue vous indique quels modules ne sont pas inclus dans l'opération de mise à jour automatique du firmware.



**IMPORTANT** Ne retirez pas la carte SD lorsque l'automate est en train de lire la carte ou d'écrire sur celle-ci. Si vous retirez la carte pendant l'une ou l'autre des opérations, les données sur la carte ou l'automate risquent de devenir corrompues. Au moment où la carte est retirée, le firmware de l'automate peut aussi devenir corrompu. Laissez la carte dans l'automate jusqu'à ce que le voyant d'état OK passe au vert fixe.

9. Dans la boîte de dialogue Automatic Firmware Update, cliquez sur Yes (Oui).

Le projet est sauvegardé sur la carte SD comme indiqué par les voyants d'état de l'automate.

#### Ces indications montrent l'état du stockage

Pendant que l'enregistrement est **en cours**, il se produit ce qui suit :

- Le voyant OK clignote en vert.
- Le voyant SD clignote en vert.
- Saving... Do Not Remove SD Card est visualisé sur l'afficheur d'état.
- Une boîte de dialogue dans l'application Logix Designer indique que l'enregistrement est en cours.
- L'automate se réinitialise.
- SAVE est affiché sur l'écran d'état.

Lorsque l'enregistrement est **terminé**, les événements suivants se produisent :

- L'automate se réinitialise.

**IMPORTANT** Laissez la sauvegarde se dérouler sans l'interrompre. Si vous interrompez le stockage, une corruption ou une perte de données peut se produire.

## Chargement depuis la carte SD

### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Après avoir défini le chemin de communication, être passé en ligne avec l'automate, et mis l'automate en mode Programming, vous pouvez charger un projet dans l'automate depuis la carte mémoire.

**IMPORTANT** Avec la carte SD et des automates neufs en condition d'origine :

- Si vous insérez une carte SD avec une image dans un automate neuf en condition d'origine (firmware 1.x), à la mise sous tension l'automate met automatiquement à jour le firmware à la révision de firmware qui est stockée sur la carte SD. La mise à jour se produit quel que soit le réglage de chargement d'image sur la carte SD (User Initiated, On Power Up ou On Uninitialized Memory).
- Si l'image a été créée avec les réglages On Power Up ou On Uninitialized Memory, l'automate met à jour le firmware et charge le projet dans l'application d'automate.

Vous pouvez charger depuis une carte SD vers un automate de l'une des façons suivantes :

- [Mise sous tension de l'automate](#)
- [Action initiée par l'utilisateur](#)

**CONSEIL** Vous pouvez toujours utiliser l'application Logix Designer pour charger le projet.

## Mise sous tension de l'automate

Ce tableau indique ce qui se passe à la mise sous tension lorsque la carte SD installée dans l'automate contient une image.

Réglage de l'image	L'automate est en condition d'origine (firmware v1.x)	Firmware > 1.x et la mémoire interne non volatile n'est pas valide <sup>(2)</sup>	Firmware > 1.x et la mémoire interne non volatile est valide <sup>(2)</sup>
Initié par l'utilisateur	Charge le firmware uniquement <sup>(1)</sup>	Ne fait rien	Ne fait rien
À la mise sous tension	Charge à la fois le firmware et l'application	<ul style="list-style-type: none"> <li>• Charge le firmware s'il y a une discordance de révision</li> <li>• Charge l'application</li> </ul>	<ul style="list-style-type: none"> <li>• Charge le firmware s'il y a une discordance de révision</li> <li>• Charge l'application</li> </ul>
Sur mémoire non initialisée	Charge à la fois le firmware et l'application <sup>(1)</sup>	<ul style="list-style-type: none"> <li>• Charge le firmware s'il y a une discordance de révision</li> <li>• Charge l'application</li> </ul>	Ne fait rien

(1) Indique un changement de comportement du ControlLogix 5570 et des automates plus anciens.

(2) « Valide » inclut la condition No Projet (Sans projet).

## Action initiée par l'utilisateur

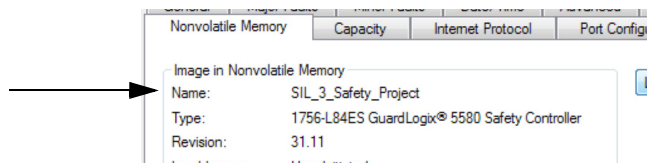
**IMPORTANT** Pour un automate en condition d'origine qui utilise la révision de firmware 1.xx, vous devez mettre à jour manuellement l'automate à la révision de firmware requise avant de pouvoir charger un projet sur l'automate.

Vous devez effectuer les étapes suivantes avant de pouvoir transférer un projet dans l'automate à partir de la carte SD lorsque l'automate est déjà sous tension :

- vérifier que l'automate a une révision du firmware opérationnelle ;
- établir le chemin de communication ;
- passer en ligne avec l'automate ;
- assurer que l'automate est en mode Programmation.

Pour charger un projet dans l'automate depuis la carte mémoire, procédez comme suit.

1. Ouvrez la boîte de dialogue Controller Properties (propriétés de l'automate) et cliquez sur l'onglet Nonvolatile Memory (mémoire non volatile).
2. Sur l'onglet Mémoire non volatile, vérifiez que le projet listé à coté de Name : est le projet que vous voulez charger.

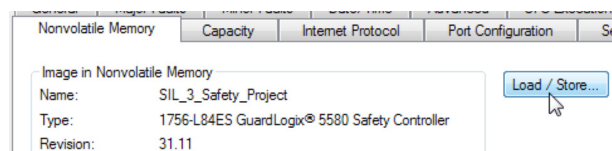


**CONSEIL** S'il n'y a pas de projet enregistré sur la carte SD, un message affiché dans le coin inférieur gauche de l'onglet Nonvolatile Memory (mémoire non volatile) indique qu'il n'existe pas d'image (ou de projet) disponible comme indiqué ici.

 No image in the nonvolatile memory.

**CONSEIL** Pour plus d'informations sur la façon de modifier le projet qui est disponible pour chargement à partir de mémoire non volatile, consultez la publication [1756-PM017](#), « Logix 5000 Controllers Nonvolatile Memory Programming Manual ».

3. Cliquez sur Load/Store (Chargement/Enregistrement).

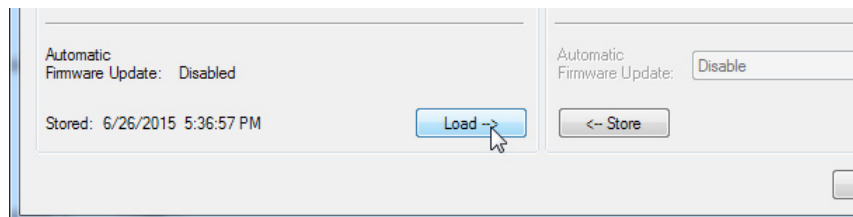




**CONSEIL** Si Load/Store (Charger/Stocker) est en grisé (indisponible), vérifiez les points suivants :

- vous avez spécifié le chemin de communication correct et êtes en ligne avec l'automate ;
- la carte SD est installée ;
- vérifiez que l'automate n'est pas en mode Exécution.

#### 4. Cliquez sur Load (Charger).



Une fois que vous avez cliqué sur Load (charger), le projet est chargé dans l'automate, comme l'indiquent les voyants d'état de l'automate. Une boîte de dialogue dans l'application Logix Designer indique que l'enregistrement est en cours.

**Tableau 14 - Ces indications affichent l'état de chargement**

Automate	Voyant SD	DEL OK sur l'automate	Message sur l'afficheur à quatre caractères
L'automate ControlLogix 5580 pendant le stockage du firmware ou projet	Vert clignotant	Rouge fixe	« LOAD » puis suivi par « UPDT »
Automate GuardLogix 5580 lorsqu'il restaure le firmware ou un projet SIL 2	Vert clignotant	Rouge fixe	« LOAD » puis suivi par « UPDT »
Automate GuardLogix 5580 SIL 3 pendant la mise à jour du firmware de l'automate principal	Vert clignotant	Vert fixe	« Updating Firmware... Do Not Remove SD Card »
Automate GuardLogix 5580 SIL 3 pendant la mise à jour du firmware du partenaire de sécurité	Vert clignotant	Vert fixe	« Updating Firmware... Do Not Remove SD Card »
Automate GuardLogix 5580 SIL 3 pendant le chargement du projet	Vert clignotant	Vert fixe	« Loading... Do Not Remove SD Card »

**IMPORTANT** Laissez le chargement se terminer sans interruption. Si vous interrompez le chargement, une corruption ou une perte de données peut se produire.

#### 5. Quand le chargement est terminé, l'automate redémarre.

## Autres tâches de la carte Secure Digital

---

### Concerne ces automates :

---

ControllLogix 5580

---

GuardLogix 5580

---

Vous pouvez utiliser la carte SD pour effectuer les tâches suivantes :

- changer l'image qui est chargée depuis la carte ;
- vérifiez un chargement qui a été terminé ;
- effacer une image de la carte SD ;
- enregistrer une image vide ;
- modifier les paramètres de chargement ;
- lire/écrire des données d'application sur la carte ;
- visualiser l'état du verrouillage de la sécurité et les signatures de sécurité à l'onglet Non-volatile Memory – automates GuardLogix 5580 uniquement.

Pour plus d'informations pour accomplir l'une de ces tâches, consultez la publication [1756-PM017](#), « Logix 5000 Controllers Nonvolatile Memory Card Programming Manual ».

## Gestion de la communication de l'automate

Rubrique	Page
Aperçu de la connexion	107
Stations sur un réseau EtherNet/IP	108
Interaction de la communication automate avec les données de commande	110
Données produites et consommées (Verrouillage)	112
Envoi et réception de messages	114
Interface de connexion	115
Simple Network Management Protocol (SNMP)	116

### Aperçu de la connexion

#### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

L'automate fournit des ressources de connexion quand des communications sont établies entre deux dispositifs.

Les connexions sont utilisées lorsque le système dispose des conditions ou activités suivantes :

- des modules d'E/S, des modules et adaptateurs de communication sont présents dans la configuration des E/S du projet de l'utilisateur ;
- des points produits ou consommés sont configurés dans le projet de l'utilisateur ;
- des messages connectés sont exécutés dans l'application de l'utilisateur ;
- des dispositifs externes, des terminaux de programmation ou d'IHM communiquent avec l'automate.

## Stations sur un réseau EtherNet/IP

<b>Concernes ces automates :</b>
ControlLogix 5580
GuardLogix 5580

Lorsque vous configurez votre système de commande, vous devez tenir compte du nombre de stations EtherNet/IP™ à inclure dans l'arborescence de configuration des E/S de votre projet. Le [tableau 15](#) montre le nombre maximum de stations EtherNet/IP pris en charge par chaque automate.

Avec la révision 29 du firmware et les versions ultérieures, le champ Ethernet Nodes (Stations Ethernet) de l'onglet Controllers Properties Capacity (Capacité des propriétés des automates) conserve un compte courant lorsque vous ajoutez des stations EtherNet/IP à l'arborescence de configuration des E/S. Consultez la [figure 20, page 109](#).

**Tableau 15 - Nombre maximum de stations EtherNet/IP prises en charge**

Système	Référence <sup>(1) (2)</sup>	Version 28	Version 29	Version 30	Version 31 ou ultérieure
ControlLogix®	1756-L81E, 1756-L81EK, 1756-L81E-NSE, 1756-L81EXT, 1756-L81EP	—	60	100	100
	1756-L82E, 1756-L82EK, 1756-L82E-NSE, 1756-L82EXT	—	80	175	175
	1756-L83E, 1756-L83EK, 1756-L83E-NSE, 1756-L83EXT, 1756-L83EP	100	100	250	250
	1756-L84E, 1756-L84EK, 1756-L84E-NSE, 1756-L84EXT	—	150	250	250
	1756-L85E, 1756-L85EK, 1756-L85E-NSE, 1756-L85EXT, 1756-L85EP	300	300	300	300
GuardLogix®	1756-L81ES, 1756-L81ESK	—	—	—	100
	1756-L82ES, 1756-L82ESK	—	—	—	175
	1756-L83ES, 1756-L83ESK	—	—	—	250
	1756-L84ES, 1756-L84ES, 1756-L84ESK	—	—	—	250

(1) Ce tableau s'applique également aux références à revêtement enrobant. Les références d'automate suivies d'un « K » indiquent un modèle à revêtement enrobant.

(2) Les automates ControlLogix NSE, les automates ControlLogix-XT et les automates de process ControlLogix sont disponibles avec la version 33 ou ultérieure.

**IMPORTANT** Les modules de communication EtherNet/IP dans le châssis local avec l'automate ne comptent pas comme des stations, mais les dispositifs EtherNet/IP connectés aux modules de communication comptent comme des stations. Consultez la [figure 20, page 109](#).

### Dispositifs inclus dans le décompte des stations

Tous les dispositifs EtherNet/IP que vous ajoutez à la section Configuration des E/S sont comptabilisés pour la limite de stations de l'automate. Voici des exemples de dispositifs qui doivent être comptabilisés :

- adaptateurs de communication décentralisés ;
- automates décentralisés ;
- dispositifs avec port EtherNet/IP embarqué, tels que les variateurs, les modules d'E/S et les dispositifs de liaison ;
- les dispositifs EtherNet/IP connectés à un module de communication dans le châssis local, même si le module de communication dans le châssis local ne compte pas comme une station ; Consultez la [figure 20, page 109](#).

- les terminaux d'IHM entrant dans la rubrique de configuration des E/S, comme les terminaux PanelView Plus ;
- les dispositifs tiers qui ne sont pas directement connectés au réseau EtherNet/IP.

## Dispositifs exclus du décompte des stations

Pour calculer le nombre total de stations Ethernet gérables par un automate ControlLogix 5580, vous n'avez pas besoin de compter les dispositifs 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 ajoutés** dans la section de configuration des E/S de votre projet et **ne sont pas comptés** dans le nombre total de stations :

- Ordinateur
- Modules de communication dans le châssis local.
- IHM qui ne sont pas ajoutées à la section Configuration des E/S.
- Dispositifs qui sont la cible des instructions MSG
- Dispositifs Ethernet standard avec lesquels l'automate communique via une interface de connexion

Cet exemple montre quatre stations dans l'arborescence des E/S

**Figure 20 - Exemple de stations EtherNet/IP**

The screenshot displays the 'Controller Organizer' window with the 'I/O Configuration' tree expanded. The tree structure is as follows:

- 1756 Backplane, 1756-A10
  - [0] 1756-L85E V31\_Test
  - [1] 1756-IB16 Local\_Input\_1
  - [2] 1756-EN2T Local\_Comm\_1
    - Ethernet
      - 1756-EN2T Local\_Comm\_1
      - 1734-AENT/B Remote\_Comm\_1
        - PointIO 1 Slot Chassis
  - [3] 1756-EN2T Local\_Comm\_2
    - Ethernet
      - 1756-EN2T Local\_Comm\_2
      - 2097-V32PR0/A Drive\_2
  - Ethernet
    - 1756-L85E V31\_Test
    - 5069-AEN2TR Remote\_Comm\_2
      - 5069 Backplane
        - [0] 5069-AEN2TR Remote\_Comm\_2
        - [1] 5069-IF8/A Remote\_Input
        - [2] 5069-OF8/A Remote\_Output
    - 2097-V33PR5-LM Main

Annotations on the left side of the tree:

- Arrow pointing to [2] 1756-EN2T Local\_Comm\_1: "N'est pas une station. Le module est dans le châssis local"
- Arrow pointing to [3] 1756-EN2T Local\_Comm\_2: "N'est pas une station. Le module est dans le châssis local"
- Arrow pointing to 1756-L85E V31\_Test: "Station"
- Arrow pointing to 5069-AEN2TR Remote\_Comm\_2: "Station"
- Arrow pointing to 2097-V33PR5-LM Main: "Station"

The 'Controller Properties - V31\_Test' dialog box is open, showing the 'Capacity' tab with the following data:

Capacity	
Total:	41,943,040 blocks
Available:	41,891,406 blocks
Used:	51,634 blocks

The 'Ethernet Nodes' section of the dialog shows:

Ethernet Nodes	
Recommended Maximum:	300 nodes
Used:	4 nodes

## Interaction de la communication automate avec les données de commande

<b>Concerner ces automates :</b>
ControlLogix 5580
GuardLogix 5580

L'automate exécute la tâche de communication indépendamment du code d'application. L'automate exécute les communications asynchroniquement par rapport à l'application. Par conséquent, il est important de s'assurer que les communications qui sont livrées à l'automate sont terminées avant l'exécution de l'application sur les nouvelles données livrées. Cela s'applique aux données qui entrent dans l'automate et aux données qui en sortent.

Par exemple, si un dispositif IHM écrit un bloc important de données de recette dans l'automate, le code d'application peut commencer à s'exécuter sur ces données avant que toutes les données soient écrites. Cette action aboutit à ce que la moitié de la recette actuelle et la moitié de la dernière recette se retrouvent dans l'espace d'application.

Traditionnellement, les programmeurs ont utilisé ce qui suit pour contrôler les effets des communications asynchrones :

- paires UID/UIE ;
- tâches périodiques ;
- déplacement des données avec des instructions CPS.

Ces options reposent sur la possibilité de contrôler quand le noyau principal peut commuter les tâches. Par conséquent, la tâche de communication ne peut pas modifier les données lorsque la tâche de commande les utilise. Comme l'automate traite les communications sur un cœur CPU indépendant, ces méthodes ne sont plus efficaces dans tous les cas.

Le [tableau 16](#) met en évidence le comportement des automates.

**Tableau 16 - Comportement des automates ControlLogix 5580 et GuardLogix 5580**

Éléments de l'application	Accès au point					
	IHM	MSG	Mise à jour E/S	Produit/Consomme	Autres tâches utilisateur	Générateur de trajectoire
UID/UIE	Permet	Permet	Permet	Permet	Bloque	Permet
CPS	Bloque	Bloque	Bloque	Bloque	Bloque	Bloque
Tâches périodiques	Permet	Permet	Permet	Permet	Permet	Permet

Bloque - Empêche le changement des valeurs de données source par les communications pendant l'exécution de l'application.

Permet - Les communications peuvent modifier les valeurs des données source pendant l'exécution de l'application.

Les automates ayant une intégrité de données sur 32 bits, cela ne s'applique qu'aux structures de données de plus de 32 bits. Si l'intégrité des données au niveau du mot est votre préoccupation principale, l'intégrité des données sur 32 bits n'affecte pas votre utilisation des données.

Une bonne pratique de programmation dicte l'utilisation de deux mots uniques au début et à la fin des données. L'automate valide les mots pour s'assurer que la structure entière a l'intégrité des données. Nous recommandons que les données d'établissement de liaison soient modifiées et que le code de l'application les valide à chaque transaction avant que le code d'application de l'automate ou le système de niveau supérieur ne lise les données de l'automate et n'agisse dessus.

Le [tableau 17](#) montre deux éléments de données ajoutés à une structure pour la vérification de l'intégrité des données : données de début et données de fin. Nous recommandons que l'automate valide les valeurs de données de début et de fin pour qu'il agisse sur My\_Recipe1.

Si les valeurs des données de départ et de fin ne correspondent pas, il est probable que les communications sont en train de remplir la structure. Il en va de même pour les systèmes de niveau supérieur qui reçoivent des données de l'automate.

**Tableau 17 - Éléments de données**

Structure	My_Recipe1	My_Recipe2	My_Recipe3
Données de début	101	102	103
Sucre	3	4	8
Farine	4	3	9
Chocolat	2	2	4
Huile	6	7	2
Données de fin	101	102	103

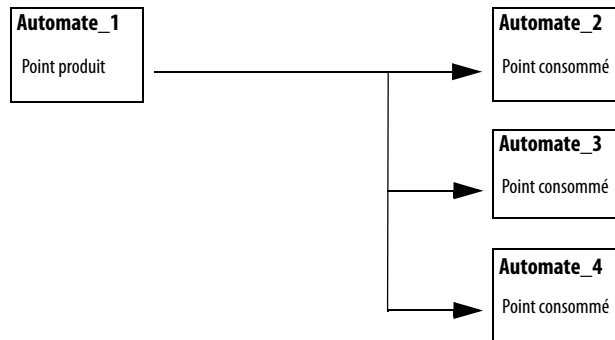
**CONSEIL** Nous vous recommandons d'effectuer ce test sur une copie des données mises en mémoire tampon et non sur l'élément de données réel qui est écrit par le noyau des communications. Si vous utilisez des données en mémoire tampon, vous empêchez le noyau de communication de modifier les données après avoir passé le test de validation des données.

## Données produites et consommées (Verrouillage)

<b>Concerne ces automates :</b>
ControlLogix 5580
GuardLogix 5580

Les automates vous permettent de produire (transmettre) et de consommer (recevoir) des points d'accès automate. Les automates ControlLogix 5580 et GuardLogix 5580 produisent le même point standard via les ports Ethernet et le bus intermodules, et le nombre de consommateurs concerne tous les consommateurs provenant de tous les ports.

Figure 21 - Représentation de la production et de la consommation de points



Le [tableau 18](#) décrit les points système partagés.

Tableau 18 - Définitions des points produits et consommés

Point	Définition
Point produit	Point qu'un automate met à la disposition d'autres automates pour l'utiliser. Plusieurs automates peuvent simultanément consommer (recevoir) les données. Un point produit envoie ses données à un ou plusieurs points consommés (consommateurs) sans utiliser de logique.
Point consommé	Un point qui reçoit les données d'un point produit. Le type de données du point consommé doit correspondre au type de données (y compris les dimensions du tableau) du point produit. Le RPI de l'étiquette consommée détermine la période de mise à jour des données.

Pour que deux automates puissent partager des points produits ou consommés, ils doivent être connectés au même réseau. Vous ne pouvez pas transmettre des points produits et consommés entre deux réseaux.

Les points produits et consommés utilisent des connexions de l'automate et des modules de communication utilisés. Pour plus d'informations sur les points de sécurité produits/consommés pour les automates GuardLogix 5580, consultez [Points de sécurité produits/consommés, page 188](#).

Dans le cas d'un réseau ControlNet™, les points produits et consommés utilisent les connexions prioritaires.



**Tableau 19 - Connexions ControlNet**

Connexion	Définition
Prioritaire (propre aux réseaux ControlNet)	<p>Une connexion prioritaire est propre aux communications ControlNet. Ce type de connexion permet d'envoyer et de recevoir des données de façon répétée selon un intervalle prédéfini correspondant à la valeur du RPI. Par exemple, une connexion à un module d'E/S est une connexion prioritaire parce que vous recevez des données d'un module de façon répétée à intervalle défini.</p> <p>Autres connexions prioritaires :</p> <ul style="list-style-type: none"> <li>• Dispositifs de communication</li> <li>• Points produits/consommés</li> </ul> <p>Avec un réseau ControlNet, on utilisera le logiciel RSNetWorx™ for ControlNet pour activer toutes les connexions prioritaires et définir le temps de rafraîchissement du réseau (Network Update Time – NUT). Une connexion prioritaire réserve de la bande passante réseau pour la gestion spécifique de cette connexion.</p>
non prioritaire	<p>Une connexion non prioritaire consiste en un transfert de message entre dispositifs, déclenché par l'intervalle entre trames requises (RPI) ou par le programme, par exemple par une instruction MSG. La messagerie non prioritaire vous permet d'envoyer et de recevoir des données lorsque vous en avez besoin.</p> <p>Les connexions non prioritaires utilisent le restant de la bande passante du réseau, lorsque la partie réservée aux connexions prioritaires a été allouée.</p>

### Intervalle entre trames requises (RPI) de points multi-diffusés

Le premier consommateur d'un point produit en multidiffusion sur un port de communication donné établit la valeur RPI pour ce port. Tous les consommateurs suivants qui utilisent le même port doivent demander la même valeur de RPI que le premier consommateur, sinon ils ne parviennent pas à se connecter. Les automates avec bus intermodules et ports EtherNet/IP peuvent produire des données à une valeur RPI indépendante sur chaque port.

Pour plus d'informations sur les points produits/consommés, consultez la publication [1756-PM011](#), « Étiquettes produites et consommées des Automates Logix 5000 Manuel de programmation ».

## Envoi et réception de messages

### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Les messages transfèrent des données vers d'autres dispositifs, tels que d'autres automates ou interfaces opérateur. L'instruction MSG est une instruction de sortie en diagramme logique à relais qui lit ou écrit asynchroniquement un bloc de données vers ou à partir d'un autre module sur le bus intermodules ou un réseau. La taille de l'instruction dépend des types de données et de la commande de message que vous programmez.

Les messages utilisent des ressources de connexion pour envoyer et recevoir des données. Les messages peuvent laisser la connexion ouverte (en cache) ou la fermer quand le message a terminé de transmettre.

Les messages peuvent être connectés ou non. Les messages non connectés dépendent de la disponibilité de mémoires tampons non connectées dans tous les dispositifs par lesquels le message transite. Les messages connectés commencent par une demande d'allocation des mémoires tampons de connexion dans tous ces dispositifs, avant d'envoyer le message réel. Choisir de mettre en cache un message connecté indique à l'automate de garder la connexion ouverte une fois le message terminé – cela améliore l'efficacité si le message est destiné à être envoyé de manière répétée.

Les messages connectés utilisent les ressources de connexion. Si le message connecté n'est pas mis en cache, les ressources sont utilisées temporairement chaque fois que le message est déclenché. Tant qu'un message connecté mis en cache reste dans le cache, les ressources restent allouées et ne sont pas disponibles pour les autres messages. Les messages mis en cache peuvent être extraits du cache si l'application dépasse la capacité de cache de l'automate.

Chaque message utilise une des connexions de l'automate, quel que soit le nombre de dispositifs dans le chemin du message.

**Tableau 20 - Types de message**

Type de message	Méthode de communication	Message connecté	Le message peut être mis en cache
Lecture ou écriture de tableau de données CIP™	—	Configurable	Oui <sup>(2)</sup>
PLC-2®, PLC-3®, PLC-5®, ou SLC™ (tous types)	CIP	Non	Non
	CIP avec ID source	Non	Non
	DH+™	Oui	Oui <sup>(2)</sup>
Générique CIP	—	Facultatif <sup>(1)</sup>	Oui <sup>(2)</sup>
Lecture ou écriture de transfert par bloc	—	Oui	Oui <sup>(2)</sup>

(1) Vous pouvez connecter des messages génériques CIP. Toutefois, pour la plupart des applications, nous vous recommandons de laisser les messages génériques CIP non connectés.

(2) Si possible, nous vous recommandons de mettre en cache les messages avec connexion qui surviennent plus d'une fois toutes les 60 secondes.

Pour plus d'informations sur l'utilisation des messages, consultez la publication [1756-PM012](#), « Logix 5000 Controllers Messages Programming Manual ».

## Déterminer s'il faut mettre en cache les connexions de message

Lorsque vous configurez une instruction MSG, vous pouvez choisir de mettre la connexion en cache. Utilisez le [tableau 21](#) pour déterminer les options de mise en cache des connexions.

**Tableau 21 - Options de mise en cache des connexions**

Si le message s'exécute	Alors
Fréquemment	Mettez la connexion en cache. Ceci gardera cette connexion ouverte et optimisera le temps d'exécution. L'ouverture d'une connexion chaque fois que le message est exécuté augmente le temps d'exécution.
Peu fréquemment	Ne mettez pas la connexion en cache. Ceci refermera cette connexion à la fin du message et la libérera ainsi pour d'autres utilisations.

**CONSEIL** Les connexions mises en cache transfèrent les données plus rapidement que les connexions non mises en cache. Les automates peuvent mettre en cache 256 messages et déclencher 256 messages simultanément.

## Interface de connexion

### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

L'automate peut utiliser des interfaces de connexion pour communiquer avec des dispositifs Ethernet qui ne prennent pas en charge le protocole d'application EtherNet/IP. L'interface de connexion est mise en œuvre via l'objet Socket. L'automate communique avec l'objet Socket via des instructions MSG. Vous devez utiliser des instructions MSG non connectées pour configurer et exploiter l'interface de connexion, et utiliser le Message to Self path. Pour communiquer avec un autre dispositif, vous devez comprendre le protocole de l'application de l'autre dispositif.

Les automates prennent en charge jusqu'à 32 instances d'interface de connexion par module ; 32 interfaces de connexion pour le port Ethernet embarqué, plus 32 autres pour chaque module de passerelle Ethernet dans le châssis local.

Pour plus d'informations sur l'interface de connexion, consultez la publication [ENET-AT002](#), « EtherNet/IP Socket Interface Application Technique ».

## Simple Network Management Protocol (SNMP)

SNMP permet que l'automate soit géré à distance via d'autres logiciels de gestion de réseau. SNMP définit la méthode de communication entre les dispositifs et désigne également un gestionnaire pour la surveillance et la supervision des dispositifs. Par défaut, SNMP est désactivé dans l'automate.

Pour de plus amples informations, consultez la publication [ENET-RM002](#), « Ethernet Design Considerations Reference Manual ».

### Utilisation d'un MSG CIP générique pour activer SNMP sur l'automate

1. Ajouter une instruction MSG à votre programme.

**IMPORTANT** Vous ne pouvez pas ajouter une instruction MSG à votre programme si le sélecteur à clé de l'automate est en mode Exécution ou si les réglages de FactoryTalk Security nient cette option de modification.

2. Configurez l'onglet Configuration de la boîte de dialogue Message Configuration comme suit :

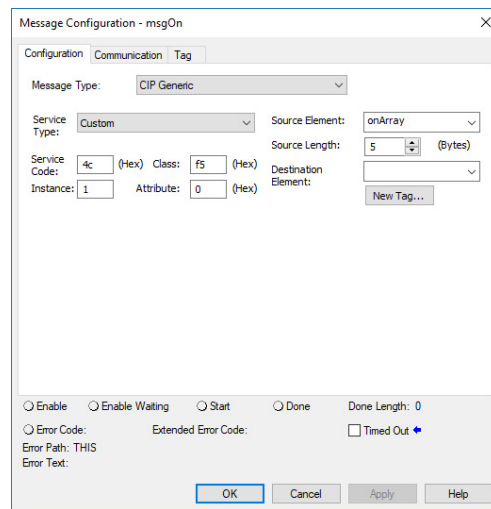
- Type de message - CIP Generic
- Type de service - Custom
- Code de service - 4c
- Instance - 1
- Classe - f5
- Attribut - 0
- Élément source - Point d'automate de type de données SINT[5].

Dans cet exemple, le point de l'automate est dénommé onArray et doit correspondre à l'illustration suivante.

**IMPORTANT** Le point d'élément source dans votre projet d'application Logix Designer doit correspondre aux valeurs affichées dans l'illustration. Si vous utilisez des valeurs différentes de celles illustrées, SNMP ne sera pas activé.

Name	Value	Style	Data Type
onArray	(...)	Decimal	USINT[5]
onArray[0]	1	Decimal	USINT
onArray[1]	161	Decimal	USINT
onArray[2]	0	Decimal	USINT
onArray[3]	17	Decimal	USINT
onArray[4]	1	Decimal	USINT

## – Longueur source - 5

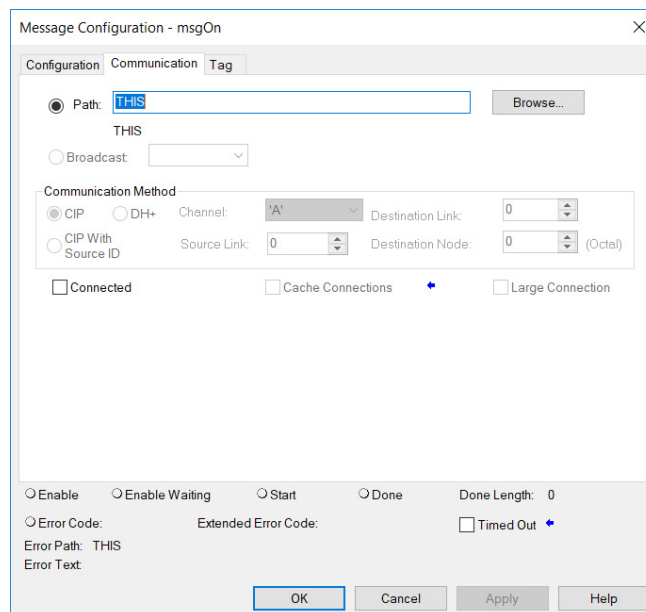


## 3. Configurez l'onglet Communication pour utiliser un « Path of THIS ».

---

**IMPORTANT** Les messages à THIS doivent être des messages non connectés.

---



## Utilisation d'un MSG CIP générique pour désactiver SNMP sur l'automate

1. Ajouter une instruction MSG à votre programme.

---

**IMPORTANT** Vous ne pouvez pas ajouter une instruction MSG à votre programme si le sélecteur à clé de l'automate est en mode Exécution ou si les réglages de FactoryTalk Security nient cette option de modification.

---

2. Configurez l'onglet Configuration de la boîte de dialogue Message Configuration comme suit :
  - Type de message - CIP Generic
  - Type de service - Custom
  - Code de service - 4c
  - Instance - 1
  - Classe - f5
  - Attribut - 0
  - Élément source – Point d'automate de type de données SINT[5].

Dans cet exemple, le point de l'automate est dénommé offArray et doit correspondre à l'illustration suivante.

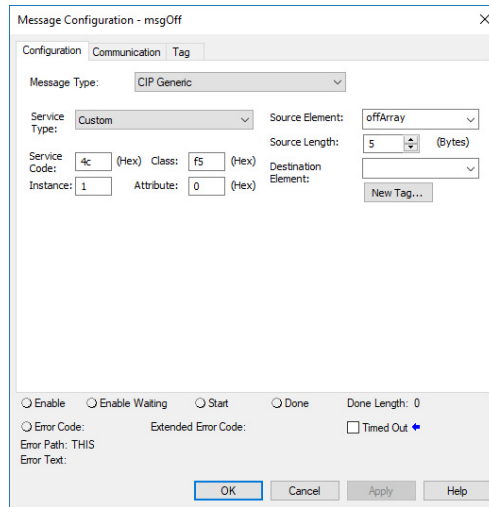
---

**IMPORTANT** Le point d'élément source dans votre projet d'application Logix Designer doit correspondre aux valeurs affichées dans l'illustration. Si vous utilisez des valeurs différentes de celles affichées, les pages Internet de l'automate ne sont pas désactivées.

offArray	(...) Decimal	USINT[5]
▸ offArray[0]	1 Decimal	USINT
▸ offArray[1]	161 Decimal	USINT
▸ offArray[2]	0 Decimal	USINT
▸ offArray[3]	17 Decimal	USINT
▸ offArray[4]	0 Decimal	USINT

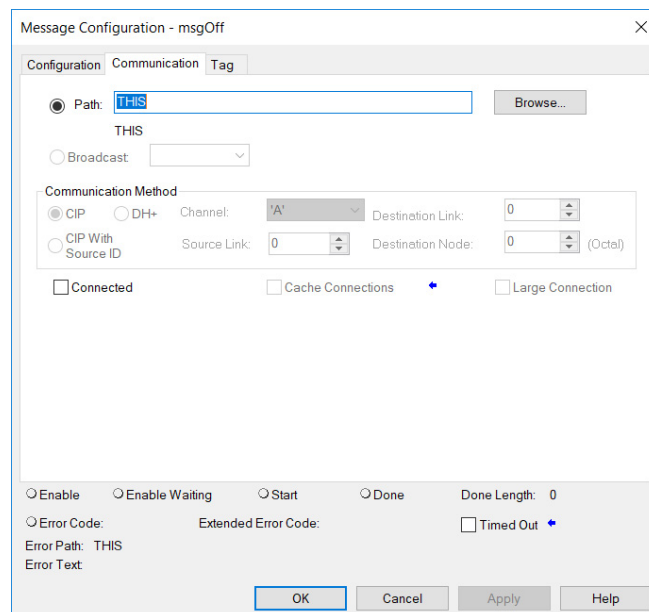
---

## – Longueur source - 5



3. Configurez l'onglet Communication pour utiliser un « Path of THIS ».

**IMPORTANT** Les messages à THIS doivent être des messages non connectés.



**Notes :**



## Modules d'E/S standard

Rubrique	Page
Choix des modules d'E/S ControlLogix	121
Modules d'E/S locaux	123
Modules d'E/S décentralisés	128
Ajout à la configuration d'E/S en étant en ligne	135
Détermination du moment où les données sont actualisées	136

### Choix des modules d'E/S ControlLogix

#### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Rockwell Automation propose un certain nombre de modules d'E/S utilisables dans les systèmes d'automate ControlLogix®. Pour obtenir une liste de toutes les gammes de produits d'E/S compatibles avec les automates ControlLogix, consultez la publication [1756-TD001](#), « 1756 ControlLogix Controllers Technical Data ».

Lorsque vous choisissez des modules d'E/S, n'oubliez pas ce qui suit :

- Rockwell Automation propose un grand choix de modules d'E/S TOR, analogiques et spécialisées. Un certain nombre de ces modules d'E/S prennent en charge les fonctionnalités suivantes :
  - diagnostics de terrain ;
  - fusibles électroniques ;
  - entrées/sorties isolées individuellement ;
  - horodatage des entrées ;
  - ordonnancement des sorties ;
  - détection d'événements de modèles d'entrée spécifiques.
- Des borniers amovibles (RTB) ou des systèmes de câblage 1492 sont requis pour une utilisation avec les modules d'E/S, et vous devrez peut-être les commander séparément.
- Possibilité d'utilisation de modules et de câbles PanelConnect™ 1492 pour le raccordement des modules d'entrées aux capteurs

## 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.

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

Les options de détrompage électronique suivantes sont disponibles.

Option de détrompage	Description
Compatible Module (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 : <ul style="list-style-type: none"> <li>• Même référence</li> <li>• Révision majeure de même niveau ou de niveau plus élevé</li> <li>• Révision mineure comme suit : <ul style="list-style-type: none"> <li>– si Révision majeure est du même niveau, Révision mineure doit être identique ou de niveau plus élevé ;</li> <li>– si Révision majeure est de niveau plus élevé, Révision mineure peut prendre toute valeur.</li> </ul> </li> </ul>
Disable Keying (Désactivation du détrompage)	Indique qu'aucun attribut de détrompage n'est pris en compte lors d'une tentative de communication avec un dispositif. Avec la désactivation du détrompage, la communication peut s'établir avec un dispositif autre que le type défini dans le projet. <b>ATTENTION</b> : soyez prudent si vous choisissez de désactiver le détrompage. Une utilisation incorrecte de cette option peut aboutir à des blessures graves voire mortelles, des dégâts matériels ou des pertes financières. Il est <b>fortement recommandé de ne pas utiliser</b> Disable Keying. Si vous désactivez le détrompage, vous devez vous assurer que le dispositif utilisé est capable de répondre aux exigences fonctionnelles de l'application.
Correspondance 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.

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

**IMPORTANT** Si vous modifiez les paramètres de détrompage électronique en ligne, les connexions à l'équipement sont interrompues de même que celles aux autres équipements connectés par le biais de l'équipement. 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.

*Autres informations*

Pour plus d'informations sur le détournement électronique, reportez-vous à la publication [LOGIX-AT001](#), « Electronic Keying in Logix 5000 Control Systems Application Technique ».

**Modules d'E/S locaux****Concerne ces automates :**

ControlLogix 5580

GuardLogix 5580

Le châssis ControlLogix que vous choisissez a une incidence sur le nombre de modules d'E/S locaux que vous pouvez utiliser. Plusieurs tailles de châssis ControlLogix sont proposées pour répondre à vos critères de configuration. Vous pouvez garnir les logements de montage avec n'importe quelle combinaison d'automates, de modules de communication et de modules d'E/S.

Le [tableau 22](#) répertorie les différents châssis ControlLogix disponibles et le nombre de logements de modules qu'ils proposent.

**Tableau 22 - Châssis ControlLogix et ControlLogix-XT™ et logements**

Châssis	Logements
1756-A4	4
1756-A7	7
1756-A7XT	
1756-A10	10
1756-A10XT	
1756-A13	13
1756-A17	17

Si vous avez des logements vides dans votre châssis, utilisez un module cache de logement 1756-N2 ou 1756-N2XT.

**Ajout d'E/S locales à la configuration des E/S**

Si vous ajoutez des E/S locales, vous devez ajouter le module d'E/S au fond de panier contenant l'automate. Pour ajouter un module d'E/S au châssis local, suivez ces étapes.

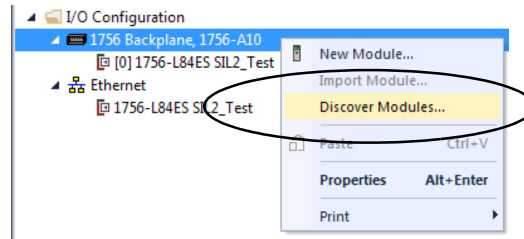
Il y a deux méthodes pour ajouter des modules d'E/S à un projet :

- [Découverte des modules, page 124](#)
- [Nouveau module, page 126](#)

### Découverte des modules

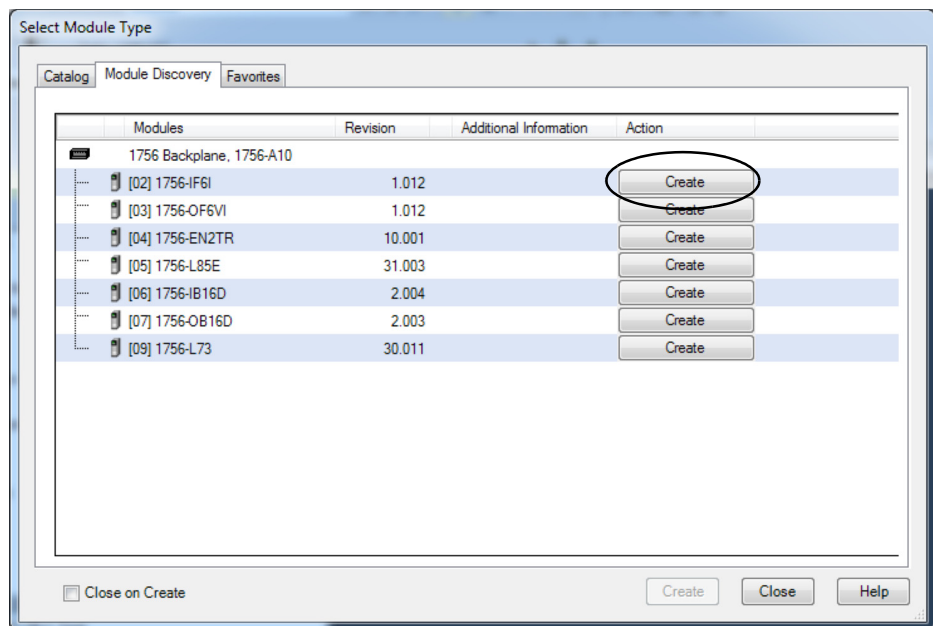
Pour utiliser Discover Modules (Découverte des modules) pour ajouter un module d'E/S local, procédez comme suit.

1. Passez en ligne avec votre application Studio 5000 Logix Designer®.
2. Faites un clic droit sur 1756 Backplane (Bus intermodules 1756) puis choisissez Discover Modules (Découvrir les modules).

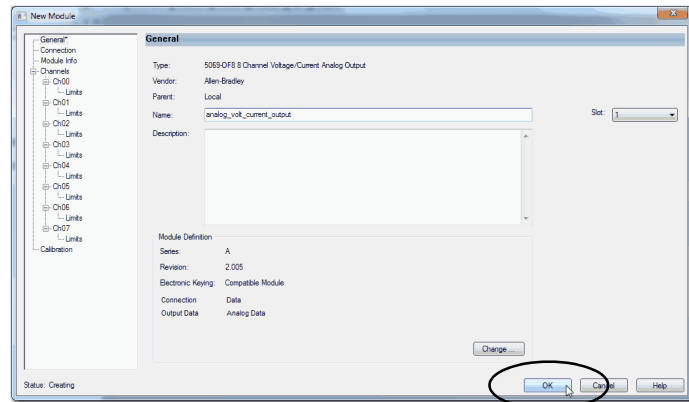


L'application Logix Designer détecte automatiquement les modules disponibles qui sont installés dans le système.

3. Dans la fenêtre Select Module Type (Sélectionner type de module), cliquez sur Create (Créer) pour ajouter un module découvert à votre projet.

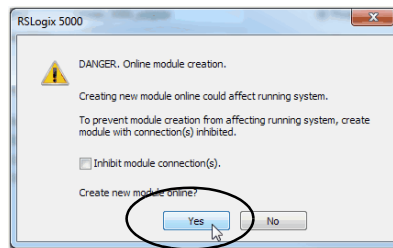


4. Dans la fenêtre New Module (Nouveau module), configurez les propriétés du module puis cliquez sur OK.



5. Dans la boîte de dialogue d'avertissement, cliquez sur Yes (Oui).

**CONSEIL** Si vous inhibez la connexion du module, vous devez vous souvenir de la désinhiber plus tard.



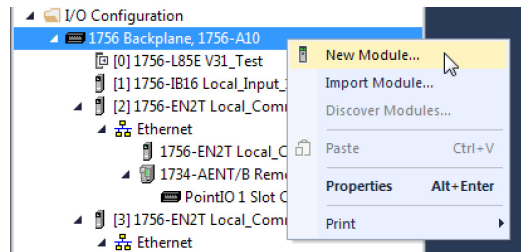
6. Fermez la boîte de dialogue Select Module Type (Sélectionner le type de module).

Pour ajouter d'autres modules d'E/S locaux, effectuez l'une des opérations suivantes :

- Si vous avez décoché la case Close on Create (Fermer à la création) au moment de la création du premier module d'E/S, renouvelez les étapes [3](#) à [6](#).
- Si vous n'avez pas désactivé la case à cocher Close on Create (Fermer à la création) lors de la création du premier module d'E/S, renouvelez les étapes [2](#) à [6](#).

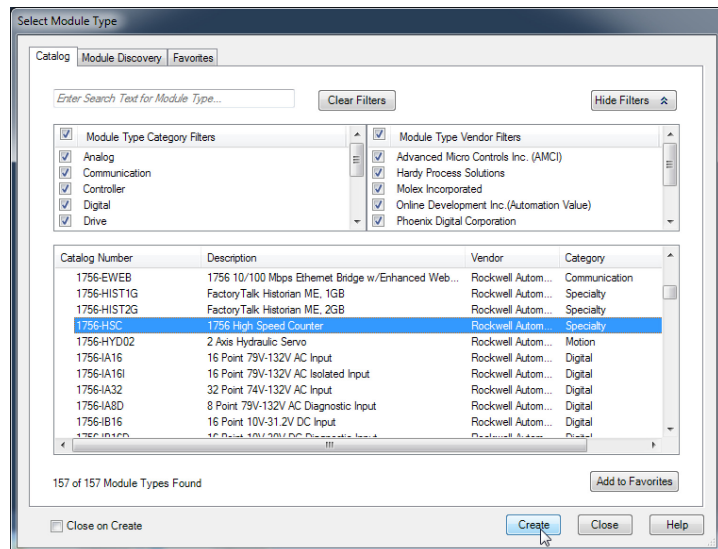
### Nouveau module

1. Cliquez avec le bouton droit de la souris sur le fond de panier et sélectionnez New Module (nouveau module).



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

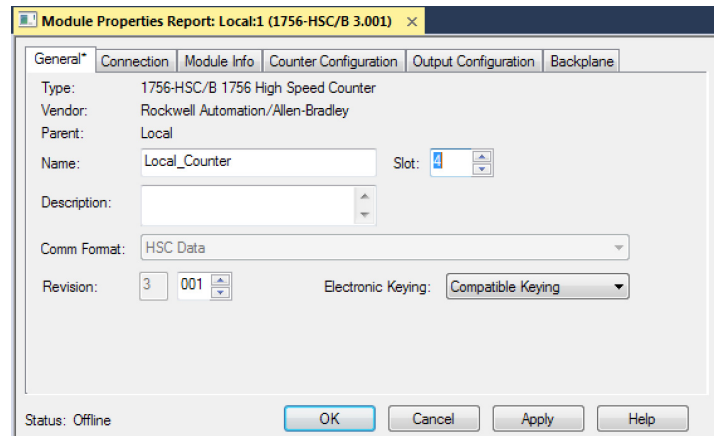
**CONSEIL** Utilisez les filtres pour réduire la liste de choix de modules.



La boîte de dialogue New Module (Nouveau module) s'affiche.

3. Configurez le module puis cliquez sur OK.

**CONSEIL** N'oubliez pas que si les valeurs des paramètres Série et Révision ne correspondent pas à celles du module auquel cette configuration est destinée, votre projet peut rencontrer des défauts de module.



Pour ajouter d'autres modules d'E/S locaux, effectuez l'une des opérations suivantes :

- Si vous avez décoché la case Close on Create (Fermer à la création) au moment de la création du premier module d'E/S, renouvelez les étapes [2](#) à [3](#).
- Si vous n'avez pas désactivé la case à cocher Close on Create (Fermer à la création) lors de la création du premier module d'E/S, renouvelez les étapes [1](#) à [3](#).

Reportez-vous à la rubrique [Documentations connexes](#) dans la préface pour de plus amples informations si vous concevez votre système ControlLogix pour l'un des modules suivants :

- E/S analogique
- Débitmètre configurable
- E/S TOR
- E/S analogiques HART
- E/S analogiques à grande vitesse
- Compteur rapide
- Compteur basse vitesse
- Interrupteur de fin de course programmable

## Modules d'E/S décentralisés

### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

E/S décentralisées réfère à des E/S qui ne sont pas situées dans le châssis local, mais qui sont connectées à l'automate par l'intermédiaire d'un réseau de communication. Il y a plusieurs gammes d'E/S qui sont décentralisées par à l'automate :

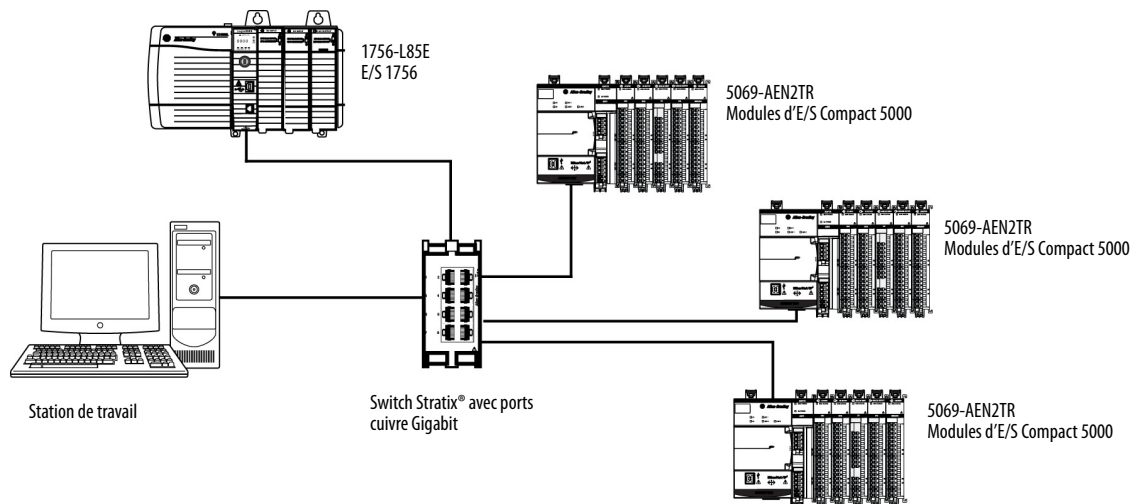
- Modules d'E/S Compact 5000™ dans une rangée décentralisée utilisant un Adaptateur 5069-AEN2TR ou similaire.
- E/S 1756 dans un châssis décentralisé via un module passerelle de réseau.
- Gammes d'E/S décentralisées telles que POINT I/O™ ou Block I/O™
- Gammes d'E/S On-Machine™, telles que ArmorPOINT® ou ArmorBlock® I/O

L'automate ControlLogix prend en charge l'utilisation d'E/S décentralisées par l'intermédiaire de ces réseaux :

- EtherNet/IP™
- ControlNet®
- DeviceNet®
- RIO universel

Pour plus d'informations sur les configurations réseau pouvant être utilisées pour connecter des E/S décentralisées, reportez-vous à [Réseaux de communication, page 33](#).

**Figure 22 - Automate ControlLogix 5580 et E/S décentralisées sur un réseau EtherNet/IP à 1 Gbits/s**



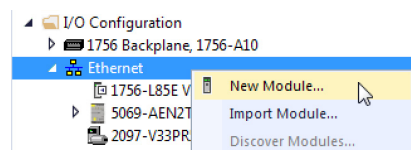


## Ajout d'E/S décentralisées sur le port Ethernet de l'automate

Si vous ajoutez des E/S décentralisées, vous pouvez ajouter les modules d'E/S au port Ethernet de l'automate. Pour ajouter des E/S décentralisées au dossier de configuration des E/S dans l'application Logix Designer, suivez ces étapes :

**IMPORTANT** Vous ne pouvez pas passer par le port Ethernet (avant) d'un autre automate pour ajouter des E/S décentralisées.

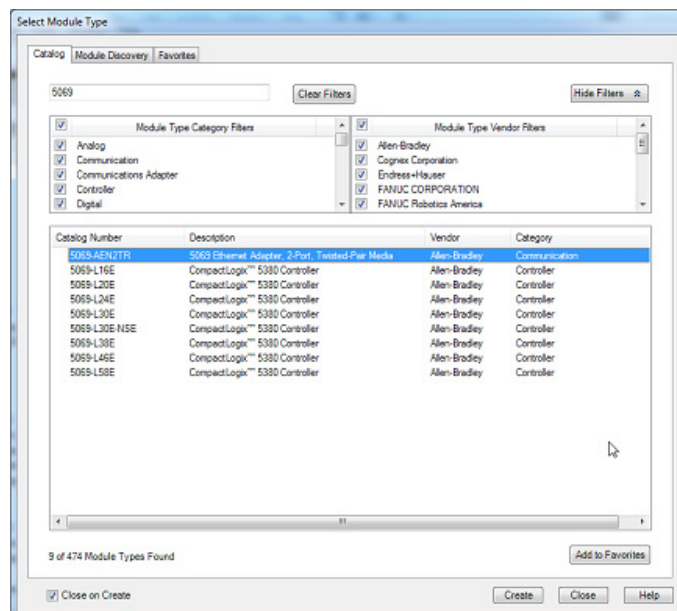
1. Dans l'arborescence de configuration des E/S, cliquez avec le bouton droit sur le réseau Ethernet et choisissez New Module.



2. Choisissez le module de communication décentralisé ou le dispositif EtherNet/IP.

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

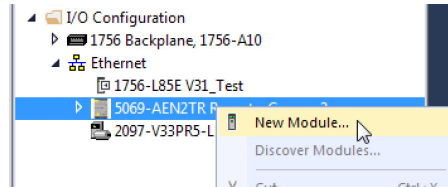
Pour certains modules, la boîte de dialogue Select Major Revision (Sélectionner la révision majeure) apparaît. Si cette boîte de dialogue apparaît, choisissez la révision majeure du module et cliquez sur OK.



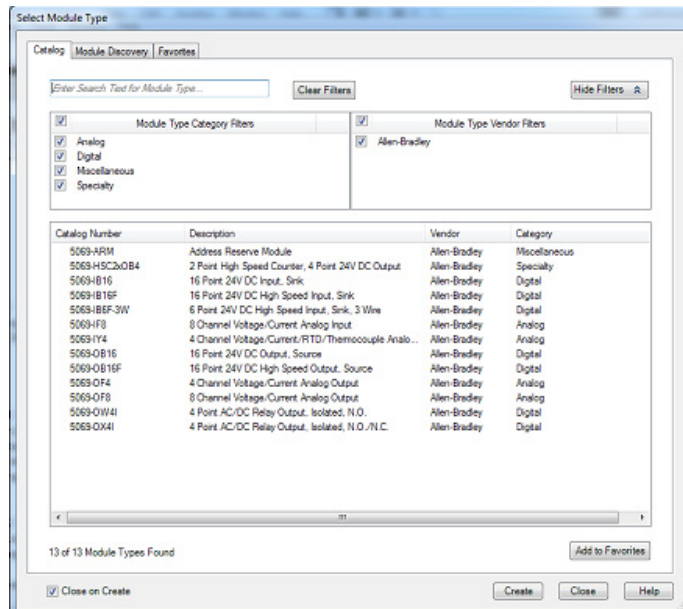
3. Assurez-vous que case Close on Create est cochée.
4. Cliquez sur Create (Créer).
5. Spécifiez les propriétés du module de communication en fonction de votre configuration réseau.

Pour plus d'informations sur les propriétés du module et du réseau de communication, consultez la rubrique [Documentations connexes](#) dans la préface.

6. Cliquez avec le bouton droit de la souris sur le fond de panier du module de communication que vous venez d'ajouter et sélectionnez New Module (nouveau module).



7. Sélectionnez le module d'E/S que vous voulez ajouter et cliquez sur OK.

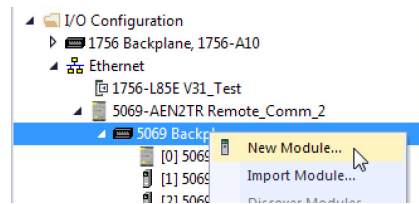


8. Assurez-vous que la case Close de Create est cochée.
9. Cliquez sur Create (Créer).
10. Spécifiez les propriétés du module (Module Properties) en fonction de votre module et de votre application.

Pour plus d'informations sur la configuration d'un des modules suivants, voir la rubrique [Documentations connexes](#) dans la préface :

- E/S analogique
- Débitmètre configurable
- E/S TOR
- E/S analogiques HART
- E/S analogiques à grande vitesse
- Compteur rapide
- Compteur basse vitesse
- Interrupteur de fin de course programmable

11. Ajoutez tous les autres modules d'E/S que vous utilisez dans le châssis décentralisé.

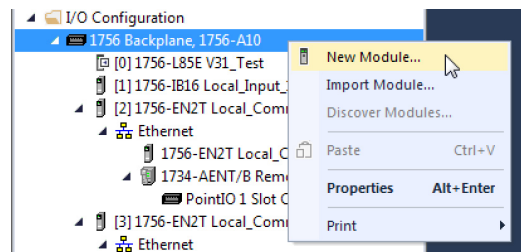


12. Répétez les étapes 1 à 11 jusqu'à ce que tout votre réseau d'E/S décentralisées et l'ensemble de vos modules d'E/S soient configurés.

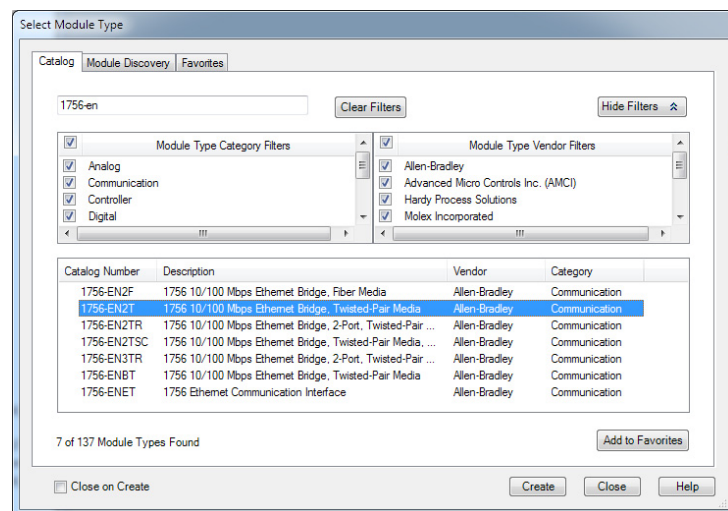
### Ajout d'E/S décentralisées à un module de communication local

Si vous utilisez des modules de communication locaux connectés à l'automate, ajoutez les modules d'E/S au fond de panier du module de communication. Pour ajouter des E/S décentralisées à l'arborescence de configuration des E/S dans l'application Logix Designer, exécutez ces étapes :

1. Cliquez avec le bouton droit de la souris sur le fond de panier et sélectionnez New Module (nouveau module).



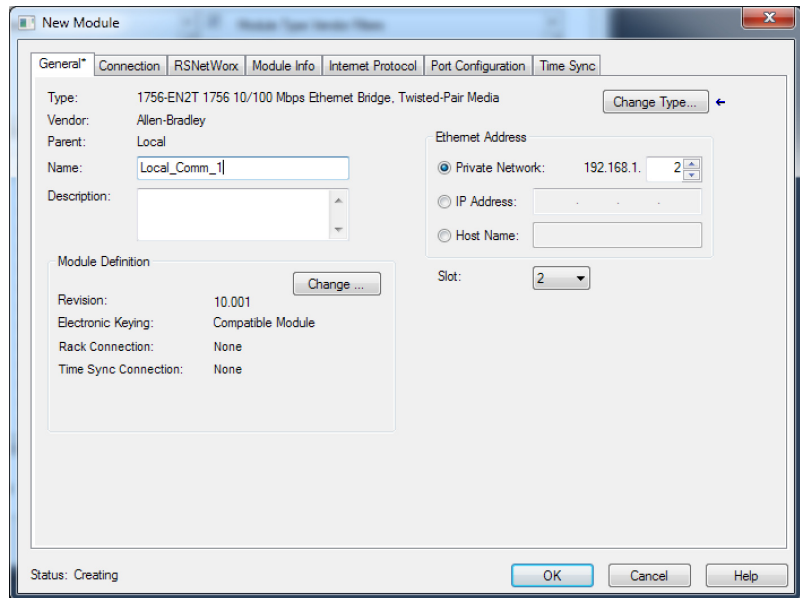
2. Sélectionnez un module de communication.



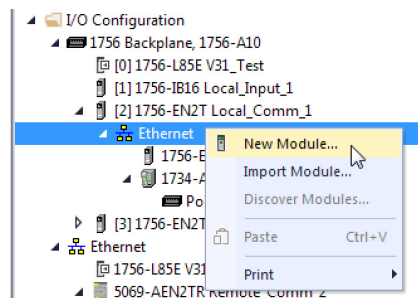
3. Cliquez sur Create (Créer).

- Spécifiez les propriétés du module de communication en fonction de votre configuration réseau.

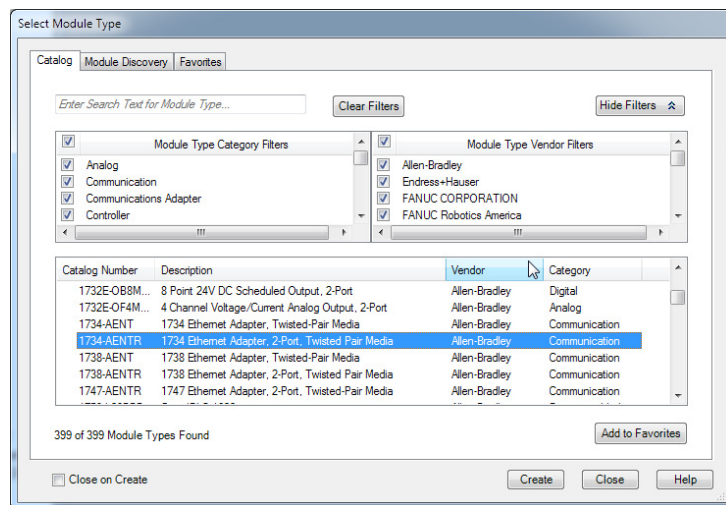
Pour plus d'informations sur les propriétés du module et du réseau de communication, consultez la rubrique [Documentations connexes](#) dans la préface.



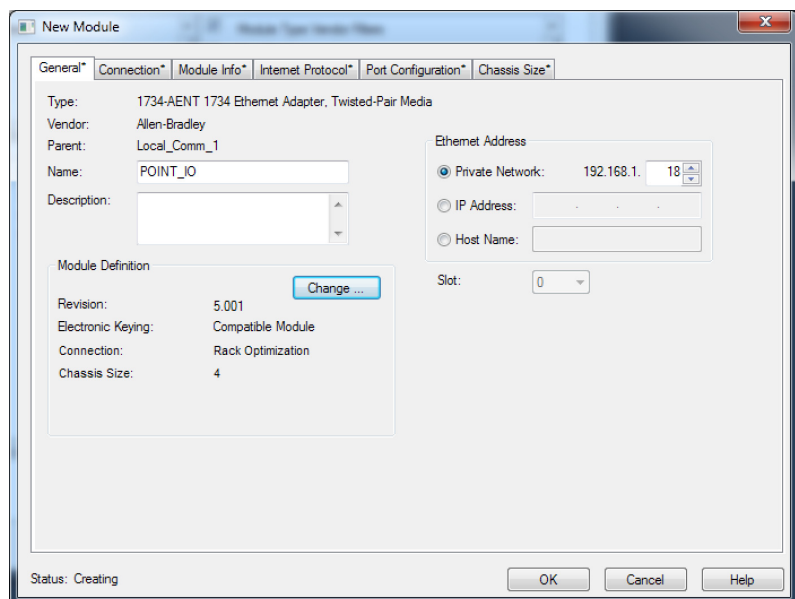
- Cliquez sur OK.
- Cliquez Close (Fermer) dans la boîte de dialogue Select Module Type (Choix du type de module).
- Faites un clic droit sur le réseau de communication sous le module de communication, et choisissez New Module (Nouveau module).



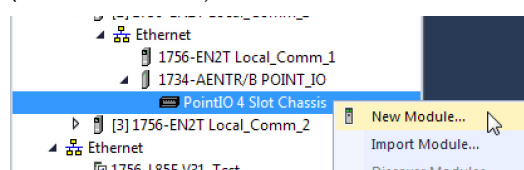
- Sélectionnez l'adaptateur de communications pour la plate-forme d'E/S distribuées que vous utilisez.



- Cliquez sur Create (Créer).
- Spécifiez les propriétés du module et de la connexion en fonction de votre configuration réseau.

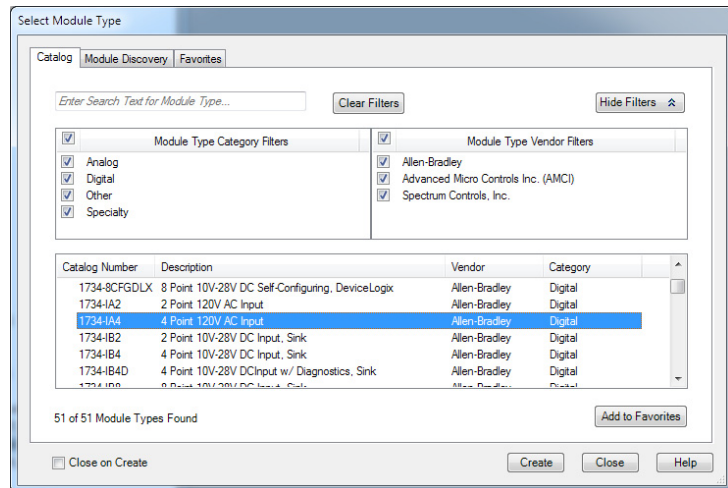


- Cliquez sur OK.
- Cliquez sur Close pour fermer la boîte de dialogue Select Module Type.
- Cliquez avec le bouton droit sur le fond de panier de l'adaptateur de communication que vous venez d'ajouter puis choisissez New Module (Nouveau module).

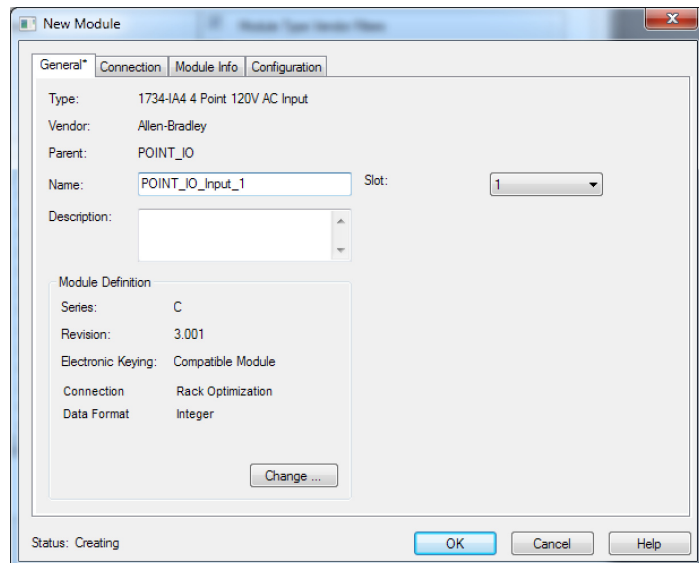


- Sélectionnez le module d'E/S que vous souhaitez ajouter puis cliquez sur Create (Créer).

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



- Spécifiez les propriétés du module (Module Properties) en fonction de votre module et de votre application. Pour plus d'informations sur les propriétés de configuration de module, reportez-vous au manuel utilisateur correspondant au module d'E/S que vous ajoutez.



- Ajoutez tous les autres modules d'E/S que vous utilisez sur ce bus.
- Répétez les étapes 1 à 16 jusqu'à ce que tout votre réseau d'E/S décentralisées et l'ensemble de vos modules d'E/S soient configurés.

## Ajout à la configuration d'E/S en étant en ligne

---

### Concerne ces automates :

---

ControlLogix 5580

---

GuardLogix 5580

---

Vous pouvez ajouter des E/S et d'autres dispositifs à la configuration de l'automate pendant que vous êtes en ligne et que le sélecteur à clé est en position REM ou PROG.

---

**IMPORTANT** Pour ajouter des modules d'E/S lorsque l'automate est en ligne, son sélecteur à clé doit être en position REM ou PROG.

Les modules d'E/S doivent déjà être installés dans le système. Vous ne pouvez pas installer des modules d'E/S quand le système est sous tension.

---

Les modules et composants que vous pouvez ajouter en ligne dépendent de la version du logiciel que vous utilisez. Les versions les plus récentes contiennent plus de modules et de dispositifs qui peuvent être ajoutés en ligne.

Des profils complémentaires (AOP) de modules sont disponibles entre les parutions de différentes versions de l'application Logix Designer. Il y a des cas où, après avoir téléchargé et installé le fichier AOP pour un module, vous pouvez ajouter le module à un projet en ligne.

Pour voir une liste des fichiers d'AOP disponibles, rendez-vous sur le site ;

<https://download.rockwellautomation.com/esd/download.aspx?downloadid=addonprofiles>

Vous pouvez ajouter des modules et dispositifs à la configuration du châssis local ou décentralisé via la portion non prioritaire d'un réseau ControlNet.

Pour plus d'informations sur le nombre de stations que vous pouvez avoir sur un réseau EtherNet/IP, consultez [Stations sur un réseau EtherNet/IP, page 108](#).

Pour plus d'informations sur l'ajout à la configuration d'E/S en ligne, consultez la publication [1756-RM094](#), « Logix 5000 Controllers Design Considerations Reference Manual ».

## Modules et dispositifs qui peuvent être ajoutés en ligne

Vous pouvez ajouter ces modules et dispositifs à la configuration des E/S en étant en ligne avec Logix Designer, version 28.00.00 ou ultérieure.

- Automates 1756
- Modules ControlNet 1756
- Passerelles DeviceNet 1756
- Modules EtherNet/IP 1756
- Adaptateurs EtherNet/IP et modules d'E/S Compact 5000
- Adaptateurs EtherNet/IP et modules d'E/S FLEX 5000™
- Modules d'E/S et spécialisés 1756
- 1756-DHRIO
- 1756-DHRIOXT

---

**IMPORTANT** Les modules ControlLogix suivants **ne peuvent pas** être ajoutés en ligne :

- modules d'axe (1756-M02AE, 1756-HYD02, 1756-M02AS, 1756-M03SE, 1756-M08SE, 1756-M08SEG, 1756-M16SE)
  - 1756-RIO
  - 1756-SYNCH
  - Safety I/O (E/S de sécurité)
- 

## Détermination du moment où les données sont actualisées

---

Concerne ces automates :

---

ControlLogix 5580

---

GuardLogix 5580

---

Les automates ControlLogix procèdent à la mise à jour des données de façon asynchrone à l'exécution du programme. Consultez les organigrammes suivants pour déterminer quand un automate, un module d'entrée ou une passerelle envoie des données :

- [Organigramme de la mise à jour des données d'entrée](#) sur cette page
- [Organigramme de la mise à jour des données de sortie, page 138](#)

## Organigramme de la mise à jour des données d'entrée

---

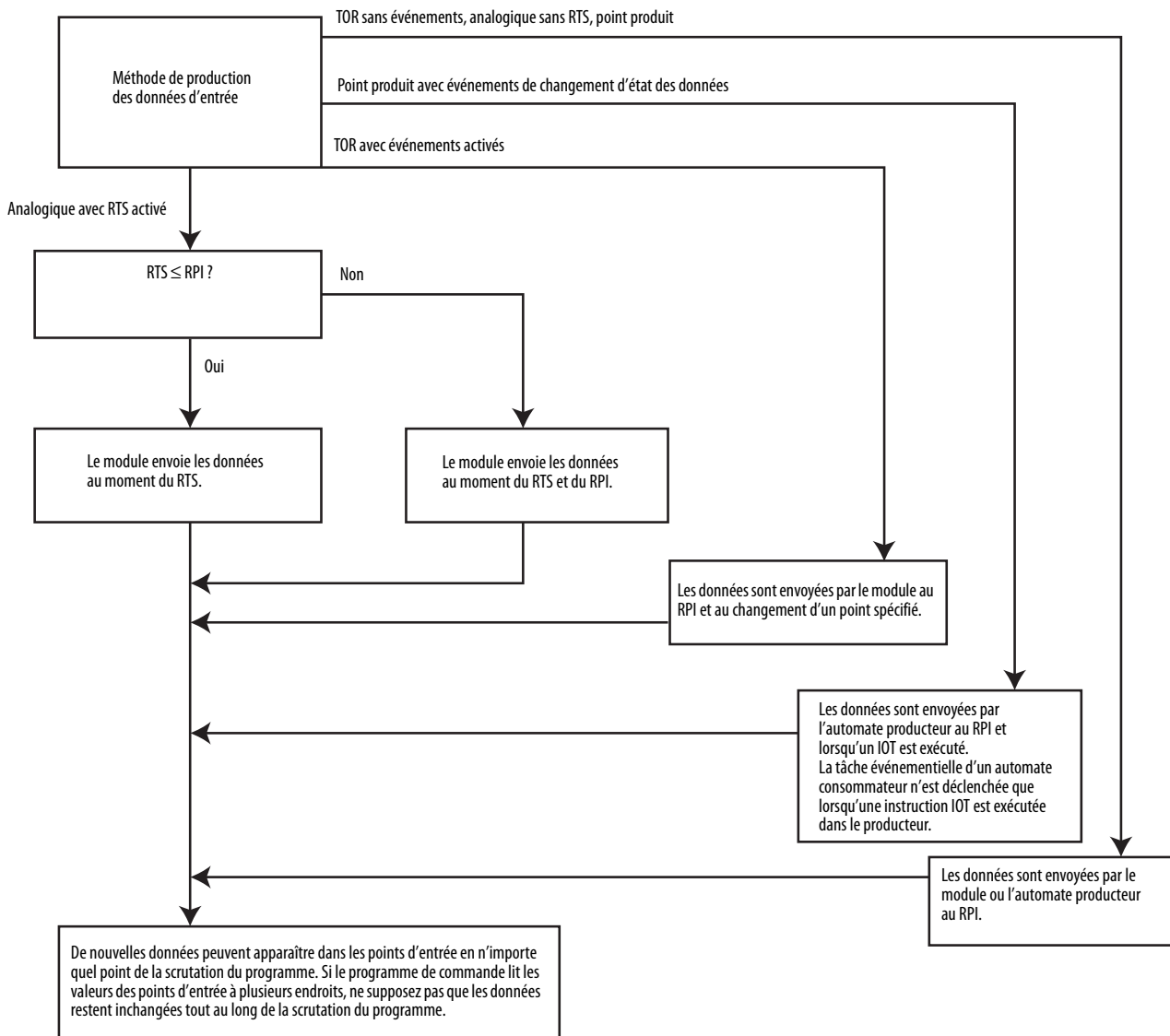
**IMPORTANT** **Considérations relatives à la sécurité**

Les entrées standard GuardLogix® sont mises à jour tout comme les entrées standard CompactLogix, mais les points d'entrée de sécurité GuardLogix (entrées consommées et adressées) sont mis à jour et gelés au début de l'exécution de la tâche de sécurité.

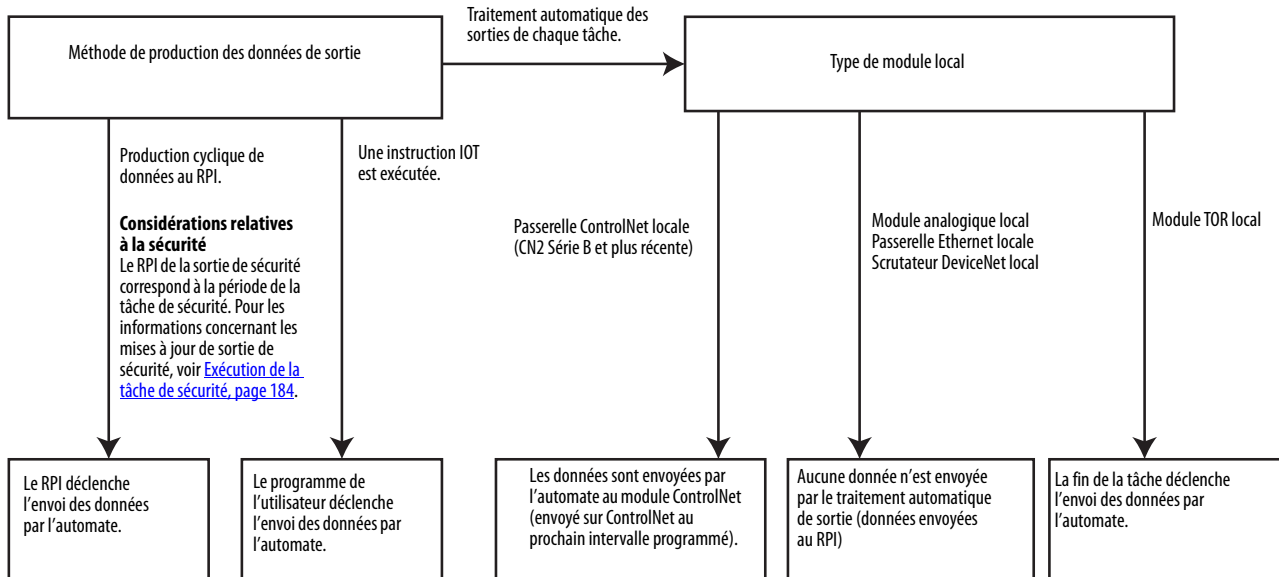
Consultez [Exécution de la tâche de sécurité, page 184](#).

---





## Organigramme de la mise à jour des données de sortie



## Dispositifs d'E/S de sécurité

Rubrique	Page
Ajout de dispositifs d'E/S de sécurité	139
Configuration des dispositifs d'E/S de sécurité	140
Utilisation de la traduction d'adresses réseau (NAT) avec des dispositifs CIP Safety	142
Définition du SNN d'un dispositif d'E/S de sécurité	143
Limite de temps de réponse de la connexion	148
Signature de dispositif d'E/S de sécurité	149
Format d'adresse d'un dispositif d'E/S de sécurité	152
Surveillance de l'état des dispositifs d'E/S de sécurité	152
Remplacement d'un dispositif d'E/S de sécurité	153
Réinitialisation d'un dispositif d'E/S de sécurité en condition d'origine	151

### Ajout de dispositifs d'E/S de sécurité

#### Concerne ces automates :

GuardLogix 5580

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

- Adresse de station pour les réseaux DeviceNet®
- Adresse IP pour les réseaux EtherNet/IP™
- Numéro de réseau de sécurité (SNN) Pour définir le SNN, voir page [143](#).
- Signature de configuration. Reportez-vous à la page [149](#) pour vérifier dans quels cas la signature de configuration est définie automatiquement ou doit l'être manuellement.
- Limite de temps de réponse. Pour définir la limite de temps de réponse, consultez la page [148](#).
- Les paramètres d'entrée, de sortie et de test de sécurité terminent la configuration du module.

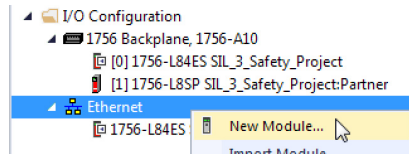
**IMPORTANT** Vous ne pouvez pas ajouter de dispositifs d'E/S de sécurité en étant en ligne avec l'automate.

## 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.

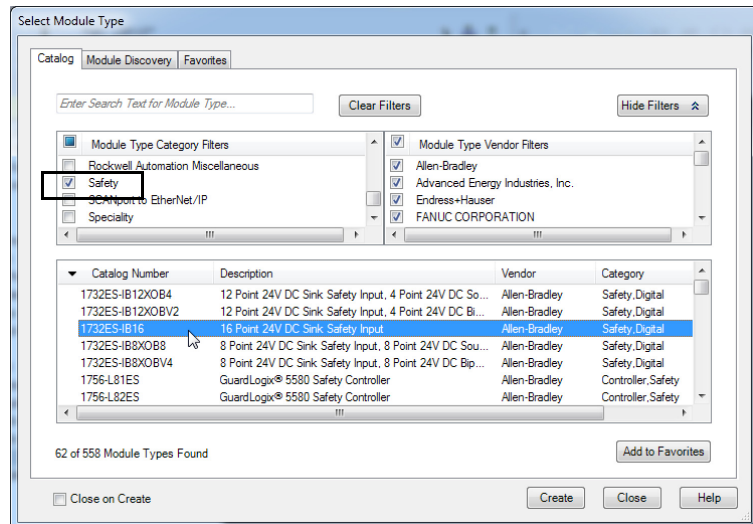
**CONSEIL** Certains dispositifs d'E/S de sécurité prennent en charge les données standard et de sécurité. La fonction de définition de module (Module Definition) définit les données disponibles.

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



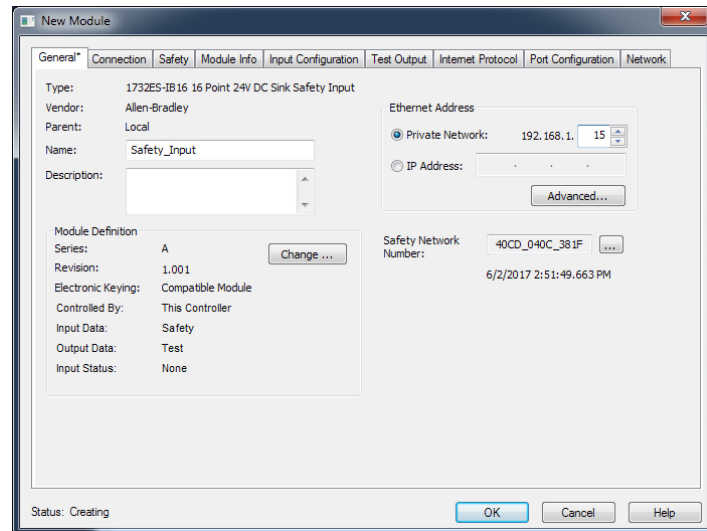
2. Sous l'onglet Catalog, sélectionnez le dispositif d'E/S de sécurité.

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



3. Cliquez sur Create (Créer).

- Saisissez un nom pour le nouveau dispositif.



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

---


**IMPORTANT** Pour les dispositifs d'E/S de sécurité, n'utilisez pas la désactivation du détrompage. Consultez [Détrompage électronique, page 122](#).

---

- Saisissez l'adresse de station pour les réseaux DeviceNet ou l'adresse IP pour les réseaux EtherNet/IP.

Seuls les numéros de station inutilisés apparaissent dans le menu déroulant.

Si votre réseau utilise la traduction d'adresse de réseau (NAT), reportez-vous à [Utilisation de la traduction d'adresses réseau \(NAT\) avec des dispositifs CIP Safety, page 142](#).

- Pour modifier le numéro de réseau de sécurité, cliquez sur le  bouton.

Pour plus de détails, reportez-vous à la page [143](#).

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

Pour plus de détails, reportez-vous à la page [148](#).

- Pour terminer la configuration du dispositif d'E/S de sécurité, reportez-vous à la documentation utilisateur et à l'aide en ligne de l'application Studio 5000 Logix Designer®.

## Utilisation de la traduction d'adresses réseau (NAT) avec des dispositifs CIP Safety

Concerne ces automates :

GuardLogix 5580

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. 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, comme par exemple pour de multiples machines ou lignes identiques.

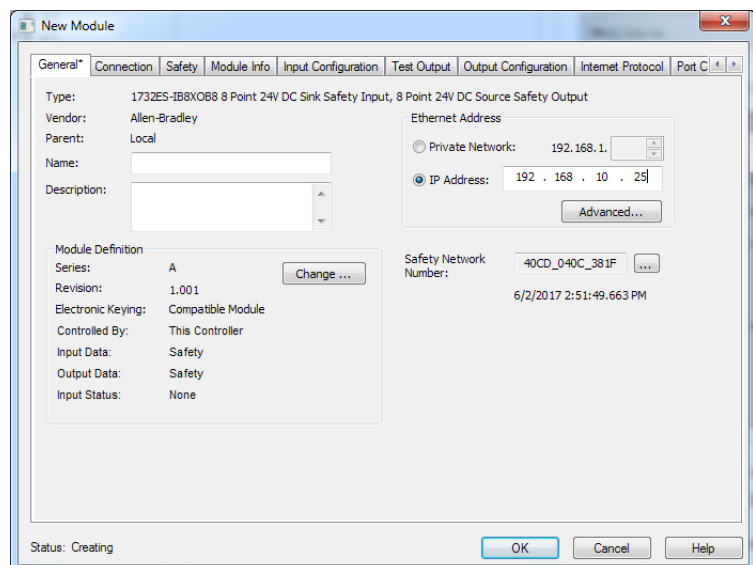
Cette section s'applique uniquement aux utilisateurs de sécurité où l'automate et les dispositifs avec lesquels il communique se trouvent sur des côtés distincts du routeur ou du switch configuré NAT.

Avec CIP Safety™, l'adresse IP du dispositif fait partie de la référence de station unique intégrée au protocole. Le dispositif compare la partie adresse IP de la référence de station unique dans les paquets CIP Safety à sa propre adresse IP et rejette tous les paquets qui ne correspondent pas. L'adresse IP dans la référence de station unique doit être l'adresse IP traduite par NAT. L'automate utilise l'adresse traduite, mais le protocole CIP Safety nécessite l'adresse réelle du dispositif.

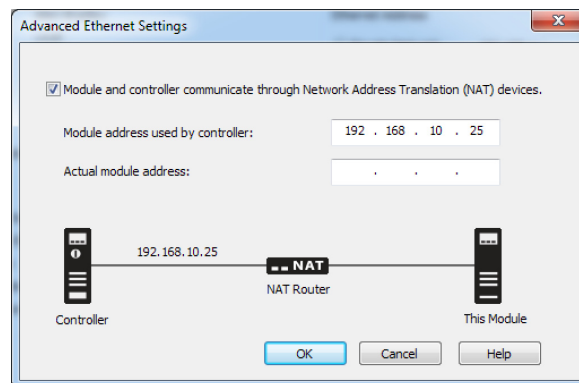
Si vous utilisez la fonction NAT pour communiquer avec un dispositif CIP Safety, procédez comme suit pour définir l'adresse IP.

1. Dans le champ IP Address, tapez l'adresse IP que l'automate utilisera.

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.

## Définition du SNN d'un dispositif d'E/S de sécurité

L'attribution d'un numéro SNN temporel est automatique lorsque vous ajoutez le premier dispositif d'E/S de sécurité au réseau. Cela ne s'applique pas au bus intermodules ou aux ports Ethernet de l'automate car ce dernier compte comme un dispositif sur le réseau.

Lorsque des dispositifs de sécurité sont ajoutés par la suite au même réseau, ils recevront le même numéro SNN que celui défini à l'adresse la plus basse de ce réseau CIP Safety, ou de l'automate lui-même dans le cas de ports rattachés à l'automate.


Un numéro SNN temporel créé automatiquement est suffisant dans la plupart des applications.

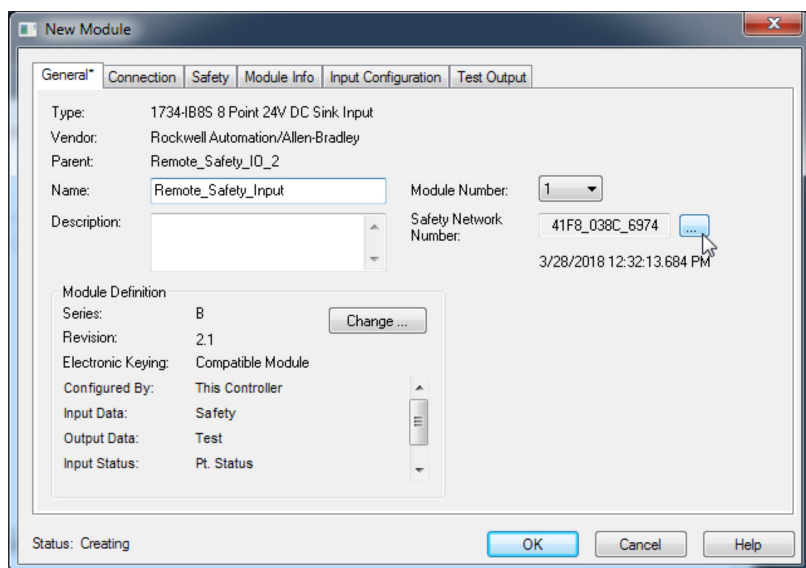
Si votre application exige que vous attribuiez manuellement le SNN des dispositifs d'E/S de sécurité, vous avez uniquement besoin d'affecter le SNN du premier dispositif d'E/S de sécurité que vous ajoutez au réseau distant ou au bus intermodules. Logix Designer attribue ensuite automatiquement le SNN du premier dispositif à tous les dispositifs supplémentaires que vous ajoutez au même réseau distant ou bus intermodules.

Pour une explication du numéro de réseau de sécurité, consultez la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

## Changer le SNN d'un dispositif d'E/S de sécurité

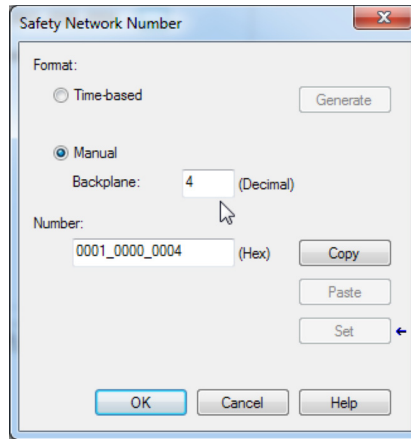
Procédez comme suit pour passer à une attribution manuelle du numéro SNN des dispositifs d'E/S de sécurité :

1. Faites un clic droit sur le module de communication EtherNet/IP distant dans l'arborescence de configuration d'E/S, et sélectionnez New Module (Nouveau module).
2. Sélectionnez votre dispositif d'E/S de sécurité, et cliquez sur Create (Créer).
3. Dans le dialogue de configuration New Module, cliquez sur  à droite du numéro de réseau de sécurité.

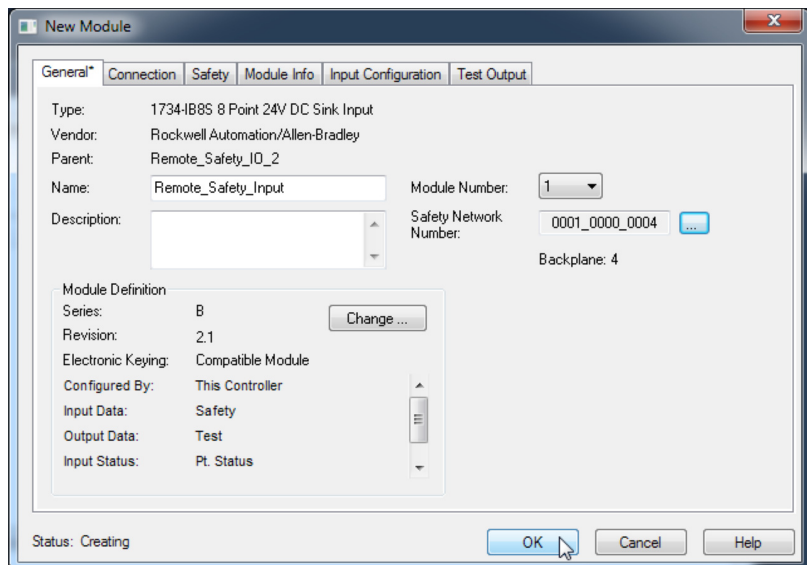




4. Dans la boîte de dialogue Safety Network Number (Numéro de réseau de sécurité), sélectionnez Manual (Manuel).
5. Saisissez le numéro SNN comme une valeur décimale de 1 à 9999.



6. Cliquez sur OK.
7. Dans le dialogue de configuration New Module, cliquez sur OK.



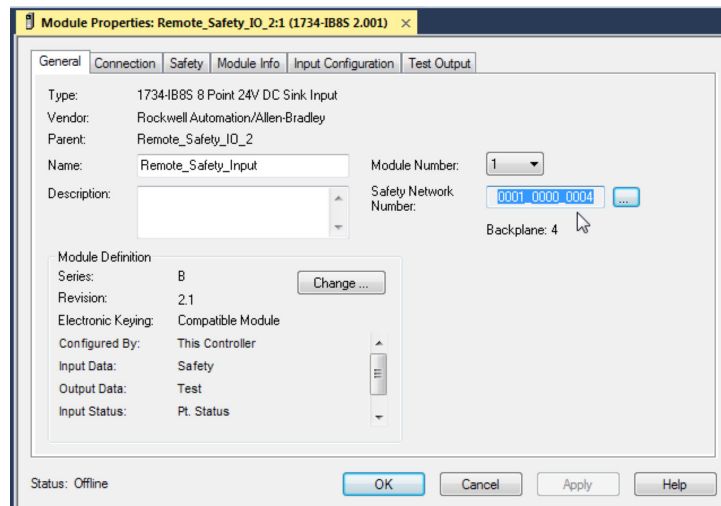
## Copier et coller le SNN d'un dispositif d'E/S de sécurité

Si vous devez appliquer un SNN à d'autres dispositifs d'E/S de sécurité, vous pouvez copier et coller le SNN. Il existe plusieurs façons de copier et coller les SNN de dispositif d'E/S de sécurité.


### Copier le SNN d'un dispositif d'E/S de sécurité

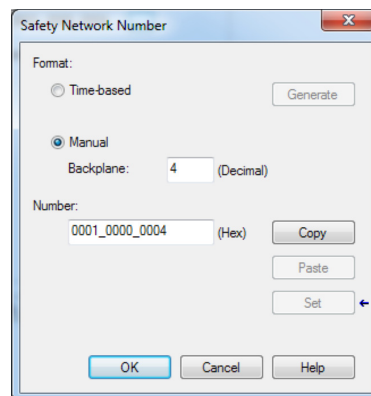
Dans l'onglet General de Module Properties (Propriétés du module), procédez comme suit :

1. Sélectionnez et mettez en surbrillance le numéro SNN.
2. Appuyez sur Ctrl-C pour copier le SNN.




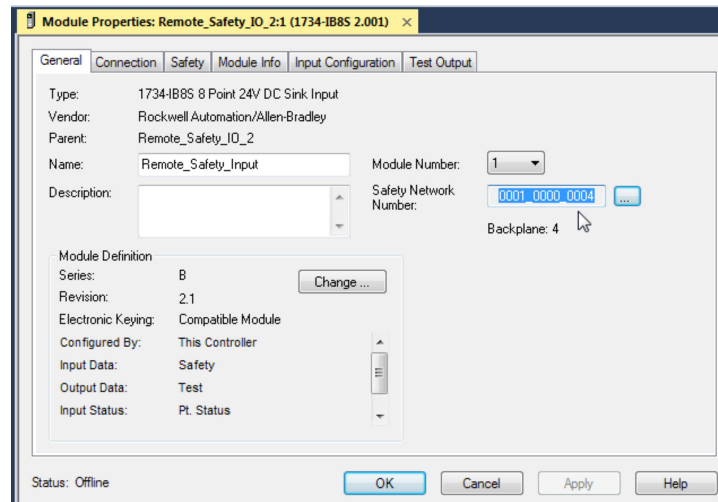
À partir du dialogue Safety Network Number :

1. Sous l'onglet General de Module Properties, cliquez sur  à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro de réseau de sécurité).
2. Dans le dialogue Safety Network Number, cliquez sur Copy (Copier), ou cliquez sur le champ SNN et appuyez sur Ctrl-C.

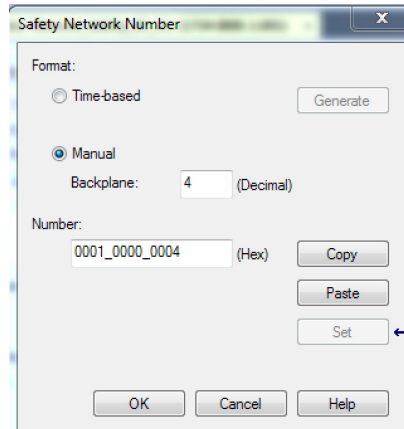


*Coller le SNN d'un dispositif d'E/S de sécurité*

1. Sous l'onglet General de Module Properties, cliquez sur  à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro de réseau de sécurité).



2. Dans le dialogue Safety Network Number, cliquez sur Paste (Coller), ou cliquez sur le champ SNN puis appuyez sur Ctrl-V.



Pour une explication du numéro de réseau de sécurité, consultez la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

## Limite de temps de réponse de la connexion

La limite de temps de réponse de la connexion (CRTL) est définie par les trois valeurs suivantes.

Valeur	Valeur par défaut	Description
Intervalle entre trames requis (RPI)	10 ms (RPI en entrée)	Fréquence à laquelle les paquets d'entrée et de sortie sont envoyés sur le circuit (réseau).
Multiplicateur de timeout	2	Le multiplicateur de timeout représente essentiellement le nombre d'essais de reconnexion avant le timeout.
Multiplicateur de délai réseau	200	Le multiplicateur de délai réseau prend en compte toutes les sources de retards identifiées sur le réseau. Lorsque ces retards se produisent, des timeouts peuvent être évités grâce à ce paramètre.

Si vous réglez ces valeurs, vous pouvez régler la limite du temps de réponse de la connexion. Si un paquet valide n'est pas reçu dans le temps CRTL défini, la connexion de sécurité prend fin, et les données en entrée et en sortie sont mises à l'état de sécurité (OFF).

---

**IMPORTANT** Les valeurs par défaut génèrent une limite de temps de réponse de la connexion d'entrée de 40 ms. Si aucune modification n'est apportée aux valeurs par défaut, vérifiez que cette limite de temps de réponse de la connexion est utilisée dans les calculs de temps de réponse de la sécurité.

---



---

**IMPORTANT** Pour des applications comportant de nombreuses rangées d'E/S de sécurité POINT Guard Safety I/O™, le temps limite de réponse de la connexion par défaut peut induire des pertes de la connexion avec les modules d'E/S de sécurité. Dans ces cas, il peut être nécessaire d'augmenter la valeur RPI par rapport à la valeur par défaut. Vérifiez que la nouvelle limite temps de réponse de la connexion est utilisée dans les calculs du temps de réponse de la sécurité.

---

Pour une explication sur les temps de réponse, consultez la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

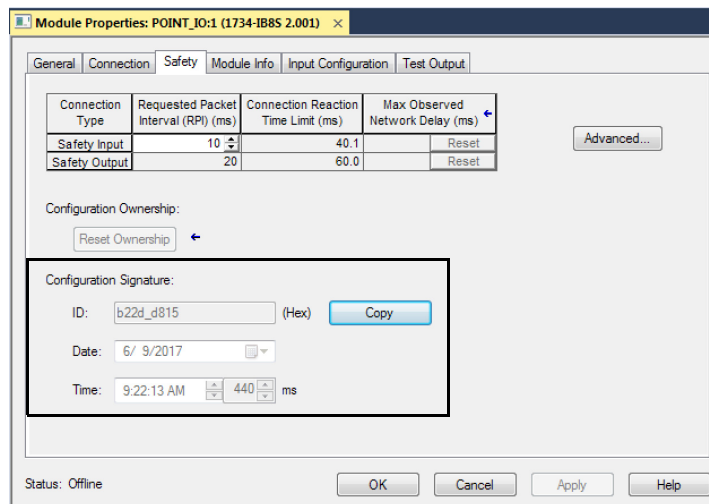
## Signature de dispositif d'E/S de sécurité

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).

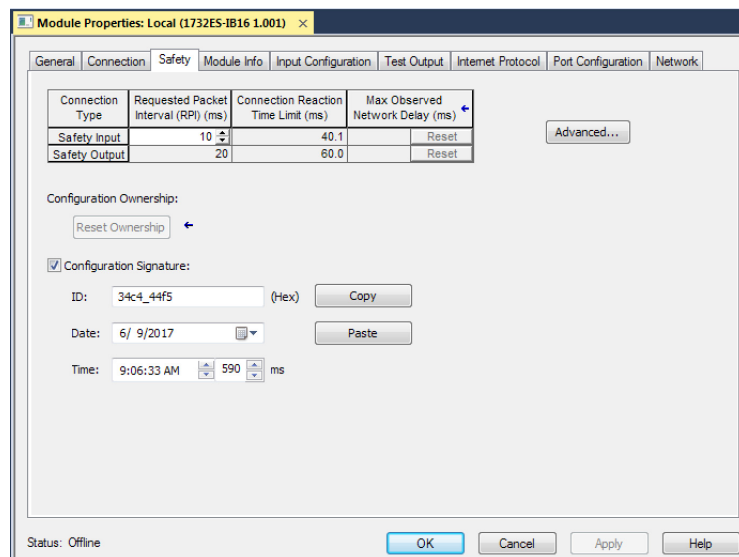
**Figure 23 - Afficher et copier la signature de configuration**



## Propriétaire de configuration différent (connexion de données seules)

Lorsque la configuration du dispositif d'E/S appartient à un autre automate, vous devez copier la signature de configuration du 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 d'un dispositif d'E/S de sécurité en condition d'origine

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

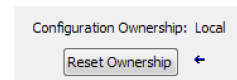
Lorsque le projet automate est en ligne, l'onglet Safety (Sûreté) de la boîte de dialogue Module Properties (Propriétés du module) affiche la propriété de configuration actuelle. Lorsque le projet ouvert possède la configuration, Local est affiché. Lorsqu'un second dispositif est propriétaire de la configuration, « Remote » s'affiche, ainsi que le numéro de réseau de sécurité (SNN) et l'adresse de station ou le numéro de logement 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. Faites un clic droit sur le module et choisissez 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. Faites un clic droit sur le module et choisissez Properties (Propriétés).
2. Cliquez sur l'onglet Safety (Sécurité).
3. Cliquez sur Reset Ownership (Réinitialiser la propriété).



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

## Format d'adresse d'un dispositif d'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.

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

**EXEMPLE** Modulename:Type.Membre

**Tableau 23 - Format d'adresse d'un dispositif d'E/S de sécurité**

Où	Est	
Modulename	Le nom du dispositif d'E/S de sécurité	
Type	Type de données	Entrée : I Sortie : O
Membre	Données spécifiques au dispositif d'E/S	
	Module d'entrée uniquement	Modulename:I.RunMode <sup>(1)</sup> Modulename:I.ConnectionFaulted <sup>(1)</sup> Modulename:I.Input Members
	Module de sortie uniquement	Modulename:I.RunMode <sup>(1)</sup> Modulename:I.ConnectionFaulted <sup>(1)</sup> Modulename:O.Output Members
	Module d'E/S mixte	Modulename:I.RunMode <sup>(1)</sup> Modulename:I.ConnectionFaulted <sup>(1)</sup> Modulename:I.Input Members Modulename:O.Output Members

(1) Ce membre est obligatoire.

**Tableau 24 - Autres documentations**

Documentation	Description
Données d'E/S et de point des automates Logix5000 Manuel de programmation, publication <a href="#">1756-PM004</a>	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 le dispositif. Pour plus d'informations, consultez la documentation produit du dispositif.



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

Ce chapitre fournit des informations sur le remplacement de dispositifs d'E/S de sécurité lorsque ces derniers sont connectés à des automates GuardLogix®.

### Propriété de configuration

Lorsque le projet automate est en ligne, l'onglet Safety (Sûreté) de la boîte de dialogue Module Properties (Propriétés du module) affiche la propriété de configuration actuelle.

- Lorsque le projet ouvert possède la configuration, Local est affiché.
- 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 du logement du propriétaire de la configuration.
- Le message « 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. Faites un clic droit sur le module et choisissez Properties (Propriétés).
2. Cliquez sur l'onglet Connection.
3. Cliquez sur Inhibit Connection (inhiber la connexion).
4. Cliquez sur Apply (Appliquer), puis sur OK.

## Configuration de remplacement

Vous pouvez utiliser l'application Logix Designer pour remplacer un dispositif d'E/S de sécurité sur un réseau Ethernet.

Pour remplacer un module Guard I/O sur un réseau DeviceNet, la méthode dépend du type de module.

**Tableau 25 - Logiciel**

Si vous utilisez un	Utiliser	Voir
dispositif d'E/S de sécurité sur réseau EtherNet/IP.	l'application Logix Designer	ci-dessous
Module Guard I/O 1791DS avec un adaptateur 1756-DNB	l'application Logix Designer	ci-dessous

- Si vous avez besoin de maintenir le niveau de sécurité SIL 2/PLd ou SIL 3/PLe dans tout ou partie du système CIP Safety pendant le remplacement et le test fonctionnel d'un dispositif, il est impossible d'utiliser la fonctionnalité Configure Always (Toujours configurer).

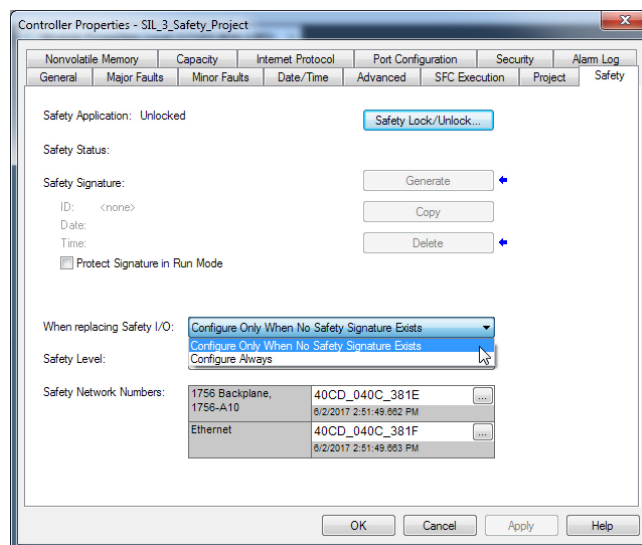
Accédez à [Remplacement avec « Configure Only When No Safety Signature Exists » activé, page 155](#)

- Si vous ne comptez pas sur la totalité du système de commande CIP Safety routable pour maintenir le niveau SIL 2/PLd ou SIL 3/PLe pendant le remplacement et le test fonctionnel du dispositif, la fonctionnalité Configure Always (Toujours configurer) peut être utilisée.

Accédez à [Remplacement avec « Configure Always » activé, page 160.](#)

Le remplacement du dispositif d'E/S de sécurité est configuré sous l'onglet Safety (Sécurité) de l'automate GuardLogix 5380.

**Figure 24 - Remplacement de dispositif d'E/S de sécurité**



## Remplacement avec « Configure Only When No Safety Signature Exists » activé

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 26](#) pour remplacer un dispositif d'E/S de sécurité en fonction de votre scénario. Après avoir exécuté toutes les étapes, 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.

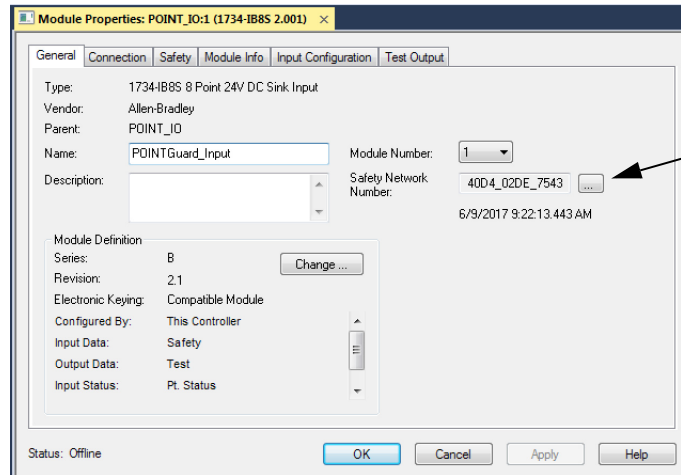
**Tableau 26 - Remplacement d'un module**

Une signature de sécurité GuardLogix® existe	Condition du module de remplacement	Action requise
Non	Pas de SNN (matériel neuf)	Aucune. Le module est prêt à être utilisé.
Oui ou non	Même SNN que dans la configuration de la tâche de sécurité originale	Aucune. Le module est prêt à être utilisé.
Oui	Pas de SNN (matériel neuf)	<a href="#">Consultez Scénario 1 – Le dispositif de remplacement est en condition d'origine et la signature de sécurité existe, page 155.</a>
Oui	SNN différent de la configuration de la tâche de sécurité originale	<a href="#">Consultez Scénario 2 – Le SNN du dispositif de remplacement est différent de l'original et une signature de sécurité existe, page 157.</a>
Non		<a href="#">Consultez Scénario 3 – Le SNN du dispositif de remplacement est différent de l'original et il n'existe pas de signature de sécurité, page 159.</a>

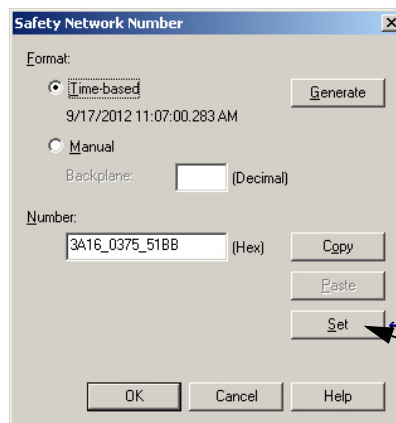
### *Scénario 1 – Le dispositif de remplacement est en condition d'origine et la signature de sécurité existe*

1. Démontez l'ancien dispositif d'E/S et installez le nouveau.
2. Faites un clic droit sur le dispositif d'E/S de sécurité de remplacement et choisissez Propriétés (Propriétés).

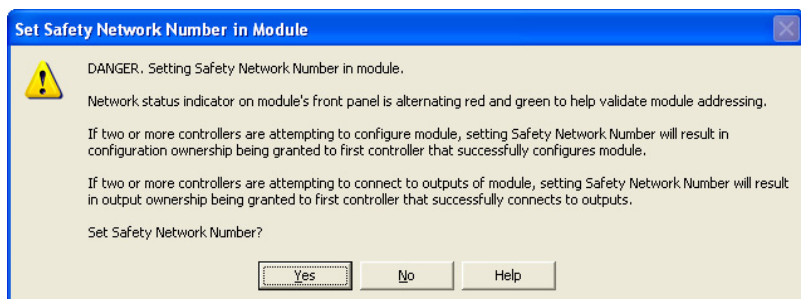
3. Cliquez sur le bouton  à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro de réseau de sécurité).



4. Cliquez sur Set (Définir).



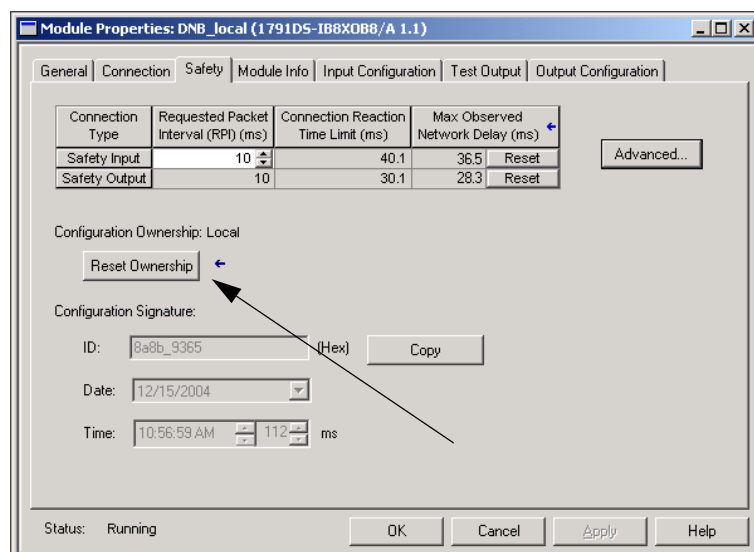
5. Vérifiez que le voyant d'état du réseau (NS) clignote alternativement en rouge/vert sur le dispositif correct avant de cliquer sur Yes (Oui) dans la boîte de dialogue de confirmation pour définir le SNN et accepter le dispositif de remplacement.




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

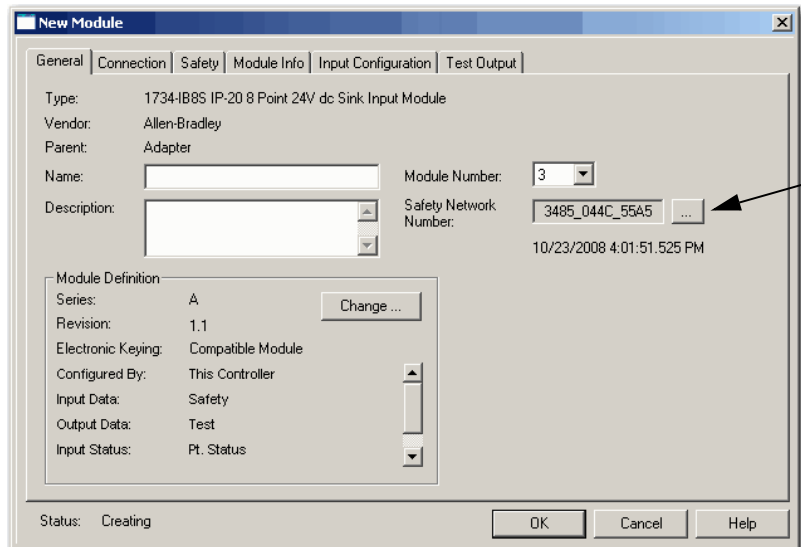
*Scénario 2 – Le SNN du dispositif de remplacement est différent de l'original et une signature de sécurité existe*

1. Démontez l'ancien dispositif d'E/S et installez le nouveau.
2. Faites un clic droit sur le dispositif d'E/S de sécurité et choisissez Propriétés (Propriétés).
3. Cliquez sur l'onglet Safety (Sûreté).
4. Cliquez sur Reset Ownership (Réinitialiser la propriété).

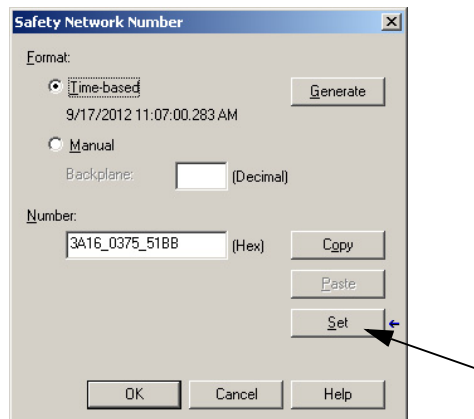


5. Cliquez sur OK.
6. Cliquez avec le bouton droit de la souris sur le dispositif puis choisissez Propriétés (Propriétés).

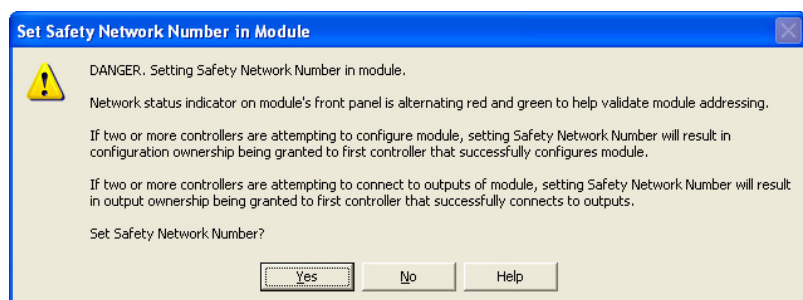
7. Cliquez sur  à droite du numéro de réseau de sécurité pour ouvrir la boîte de dialogue Safety Network Number (Numéro de réseau de sécurité).



8. Cliquez sur Set (Définir).



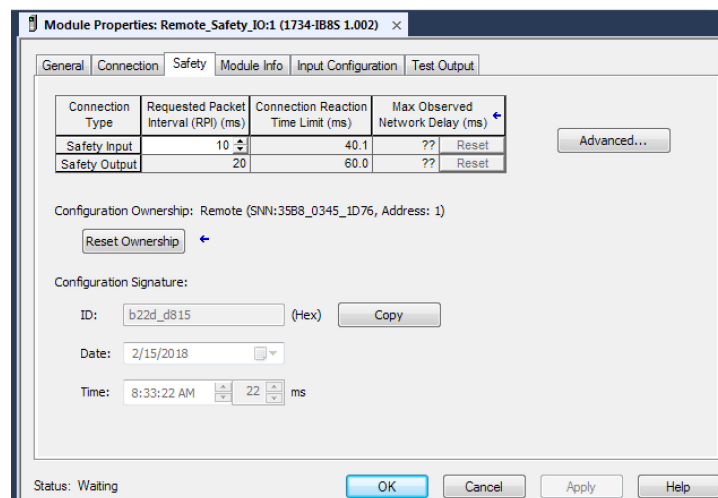
9. Vérifiez que le voyant d'état du réseau (NS) clignote alternativement en rouge/vert sur le dispositif correct avant de cliquer sur Yes (Oui) dans la boîte de dialogue de confirmation pour définir le SNN et accepter le dispositif de remplacement.



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

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

1. Démontez l'ancien dispositif d'E/S et installez le nouveau.
2. Faites un clic droit sur le dispositif d'E/S de sécurité et choisissez Properties (Propriétés).
3. Cliquez sur l'onglet Safety (Sûreté).



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 valider l'utilisation du 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** invoqué pour maintenir le comportement SIL 2/PLd ou SIL 3/PLe pendant le remplacement et le test fonctionnel d'un dispositif.

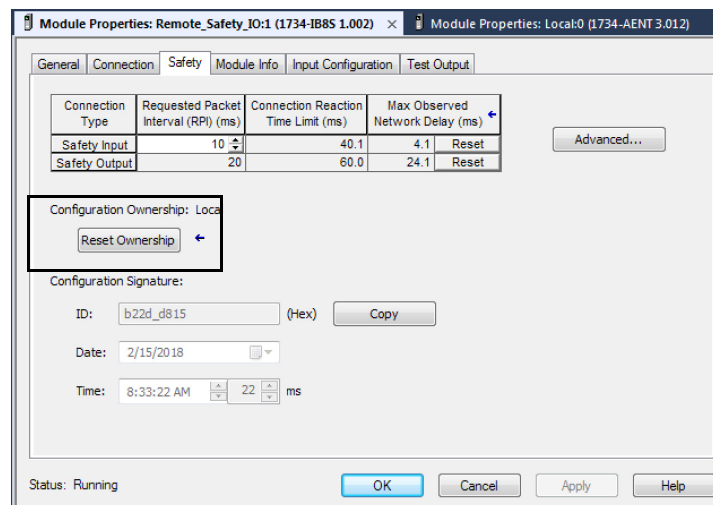
N'introduisez pas sur un réseau de sécurité CIP des dispositifs dans leur condition d'origine lorsque la fonctionnalité Configure Always est activée, sauf en suivant cette procédure de remplacement.

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 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. Faites un clic droit sur le dispositif d'E/S de sécurité et choisissez Properties (Propriétés).
3. Cliquez sur l'onglet Safety (Sûreté).
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 valider l'utilisation du système.

**Notes :**

## Développement d'applications standard

<b>Rubrique</b>	<b>Page</b>
Éléments d'une application de commande	164
Tâches	165
Programmes	168
Sous-programmes	171
Paramètres et points locaux	172
Langages de programmation	173
Instructions complémentaires	174
Propriétés étendues	175
Accès à l'objet Module à partir d'une instruction complémentaire	176
Surveillance de l'état de l'automate	177
Surveillance des connexions d'E/S	178

## Éléments d'une application de commande

**Concerne ces automates :**

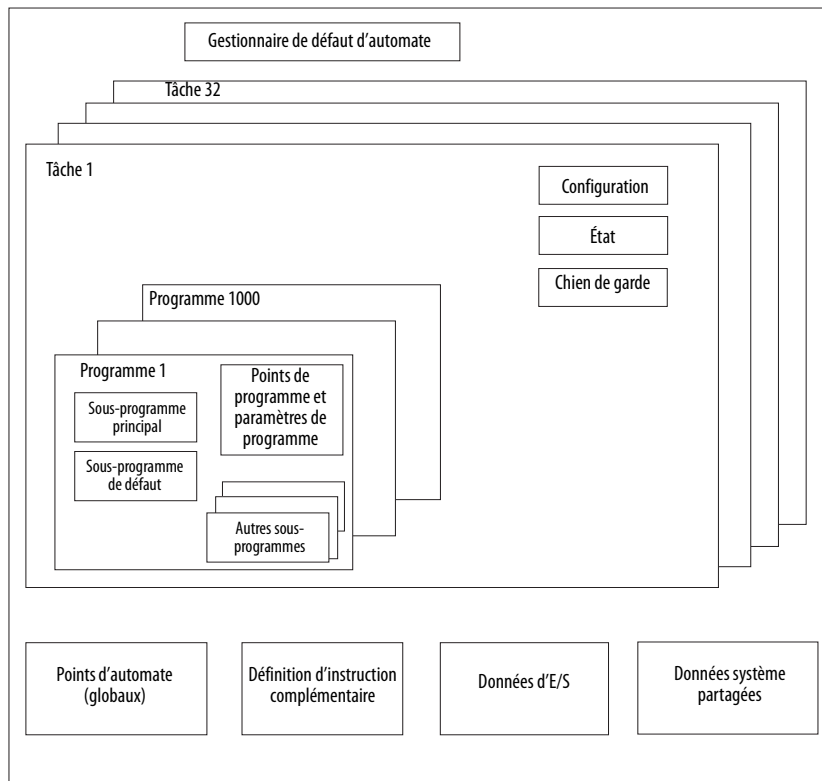
ControlLogix 5580

GuardLogix 5580

Une application de commande se compose de plusieurs éléments qui nécessitent une planification pour une exécution efficace de l'application. L'application comprend les éléments suivants :

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

**Figure 25 - Éléments d'une application de commande**



## Tâches

L'automate vous permet d'utiliser plusieurs tâches pour planifier et prioriser l'exécution de vos programmes en fonction de critères. Ce fonctionnement multitâche alloue le temps de traitement de l'automate parmi les opérations de votre application :

- L'automate n'exécute qu'une tâche à la fois.
- Selon sa priorité, une tâche peut interrompre l'exécution d'une autre 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 les vues de l'organisateur de l'automate ou logique, si nécessaire.

**Figure 26 - Tâche au sein d'une application de commande**

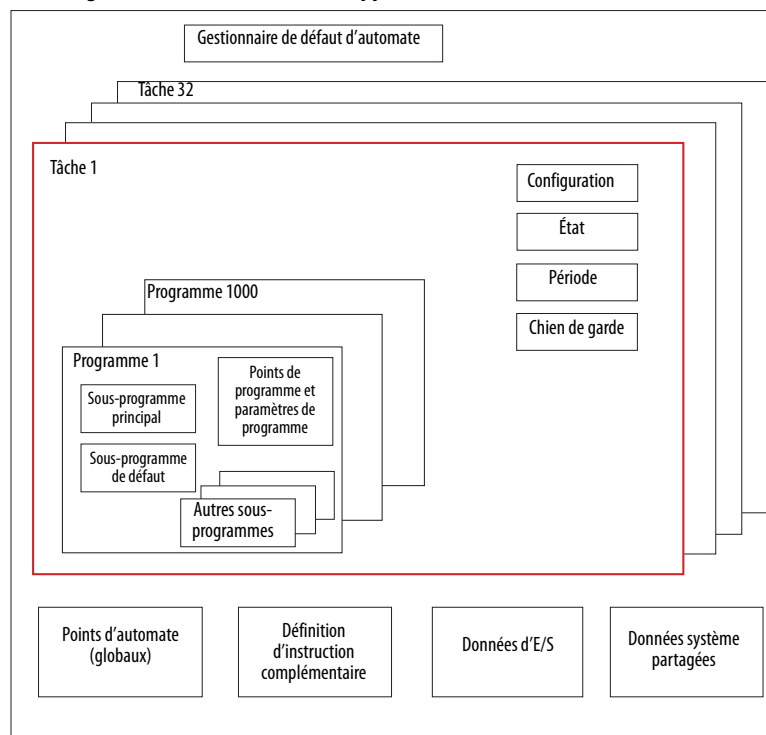
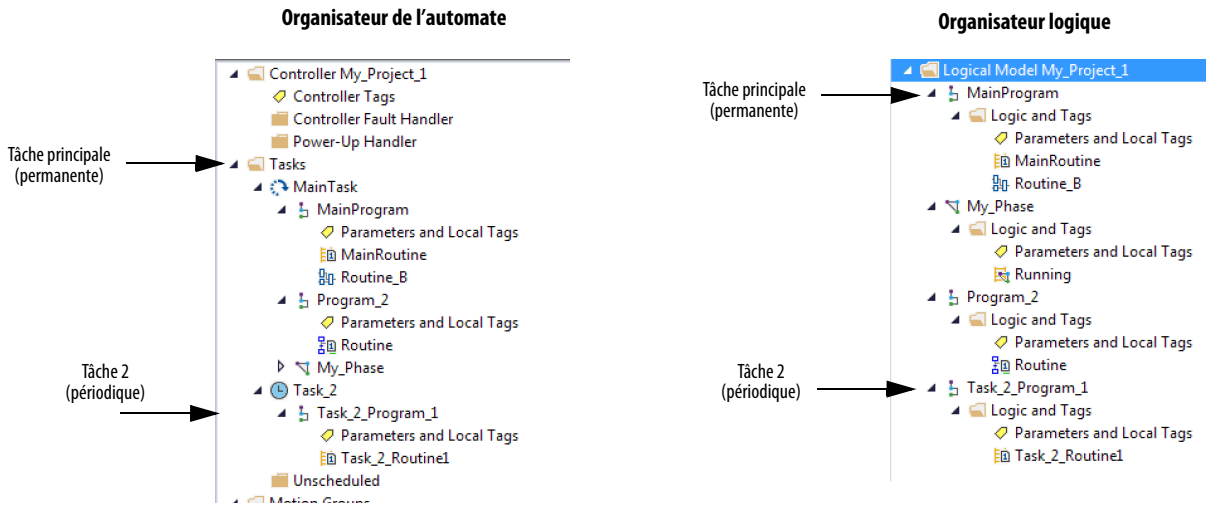
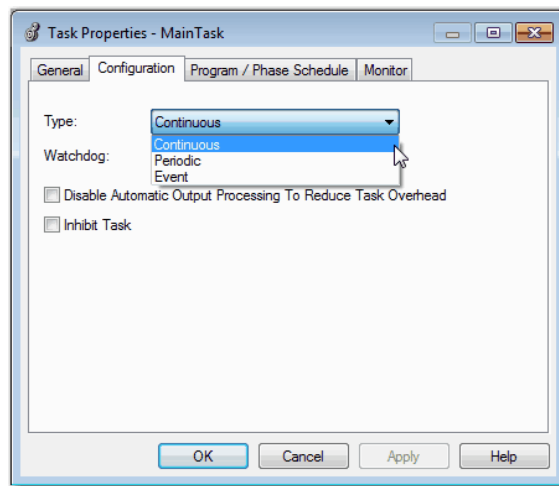


Figure 27 - Tâches



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

Figure 28 - Configuration du type de tâche



Le [tableau 27](#) explique les types de tâches que vous pouvez configurer.

**Tableau 27 - Types de tâche et fréquence d'exécution**

Type de tâche	Exécution de la tâche	Description
Permanente	Constante	La tâche permanente est exécutée en arrière plan. Tout temps processeur qui n'est pas affecté à d'autres opérations (telles que le mouvement et d'autres tâches) est utilisé pour exécuter les programmes dans la tâche permanente. <ul style="list-style-type: none"> <li>La tâche permanente fonctionne constamment. Lorsque la tâche permanente termine une scrutation complète, elle redémarre immédiatement.</li> <li>Un projet ne nécessite pas une tâche permanente. Le cas échéant, il ne peut y avoir qu'une seule tâche permanente.</li> </ul>
Périodique	À intervalle défini (par exemple, toutes les 100 ms)	Une tâche périodique exécute une fonction à chaque intervalle. <ul style="list-style-type: none"> <li>Chaque fois que le temps de la tâche périodique expire, la tâche interrompt les tâches de priorité inférieure, s'exécute une fois et retourne le contrôle à l'endroit où la tâche précédente s'est arrêtée.</li> <li>Vous pouvez configurer la durée de la période de 0,1 à 2 000 000,00 ms. La valeur par défaut est 10 ms. Elle est aussi dépendante de l'automate et de la configuration.</li> </ul>
événement	Immédiatement quand un événement se produit	Une tâche événementielle exécute une fonction quand un événement (déclencheur) se produit. Le déclencheur pour une tâche événementielle peut être le suivant : <ul style="list-style-type: none"> <li>des données d'entrée d'un module qui changent d'état ;</li> <li>le déclenchement par un point consommé ;</li> <li>une instruction EVENT ;</li> <li>le déclenchement par un axe ;</li> <li>le déclenchement par un événement de mouvement.</li> </ul> <p>Vous pouvez configurer un intervalle de timeout facultatif pour les déclencheurs d'événement manqués, ce qui entraîne l'exécution des tâches d'événement même en l'absence du déclencheur. Cochez la case à cocher « Check the Execute Task If No Event Occurs Within &lt;timeout period&gt; » pour la tâche.</p>

Les automates ControlLogix™ 5580 et GuardLogix® 5580 prennent en charge jusqu'à 32 tâches. Seulement une de ces tâche peut être permanente.

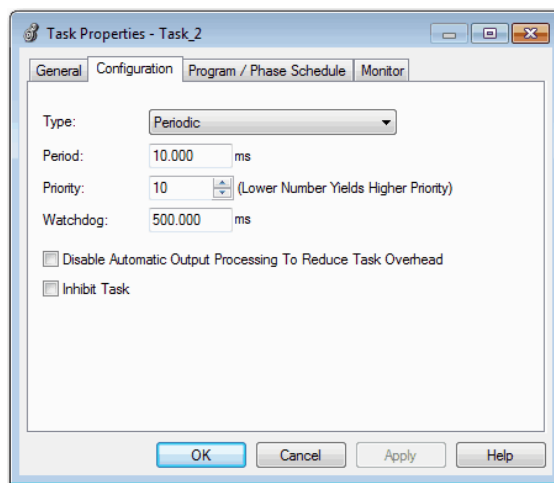
Une tâche peut avoir jusqu'à 1000 programmes, chacun avec ses sous-programmes exécutables et ses points d'accès programme. Une fois qu'une tâche est déclenchée (activée), les programmes affectés à la tâche s'exécutent dans l'ordre dans lequel ils sont groupés. Les programmes ne peuvent apparaître qu'une seule fois dans l'organisateur de l'automate et plusieurs tâches ne peuvent pas les partager.

## Priorité des tâches

Chaque tâche de l'automate possède un niveau de priorité. Le système d'exploitation utilise le niveau de priorité pour déterminer la tâche à exécuter lorsque plusieurs tâches sont déclenchées. Une tâche de priorité supérieure interrompt toute tâche de priorité inférieure. La tâche permanente a la priorité la plus faible et une tâche périodique ou événementielle peut l'interrompre.

Vous pouvez configurer les tâches périodiques et événementielles à exécuter à partir de la priorité 15, la plus faible, jusqu'à la priorité 1, la plus élevée. Utilisez la boîte de dialogue Task Properties (Propriétés de la tâche) pour configurer la priorité de la tâche

Figure 29 - Configuration de la priorité de la tâche



## Programmes

Le système d'exploitation de l'automate est un système multitâche préemptif conforme à la norme CEI 61131-3. Ce système fournit les éléments suivants :

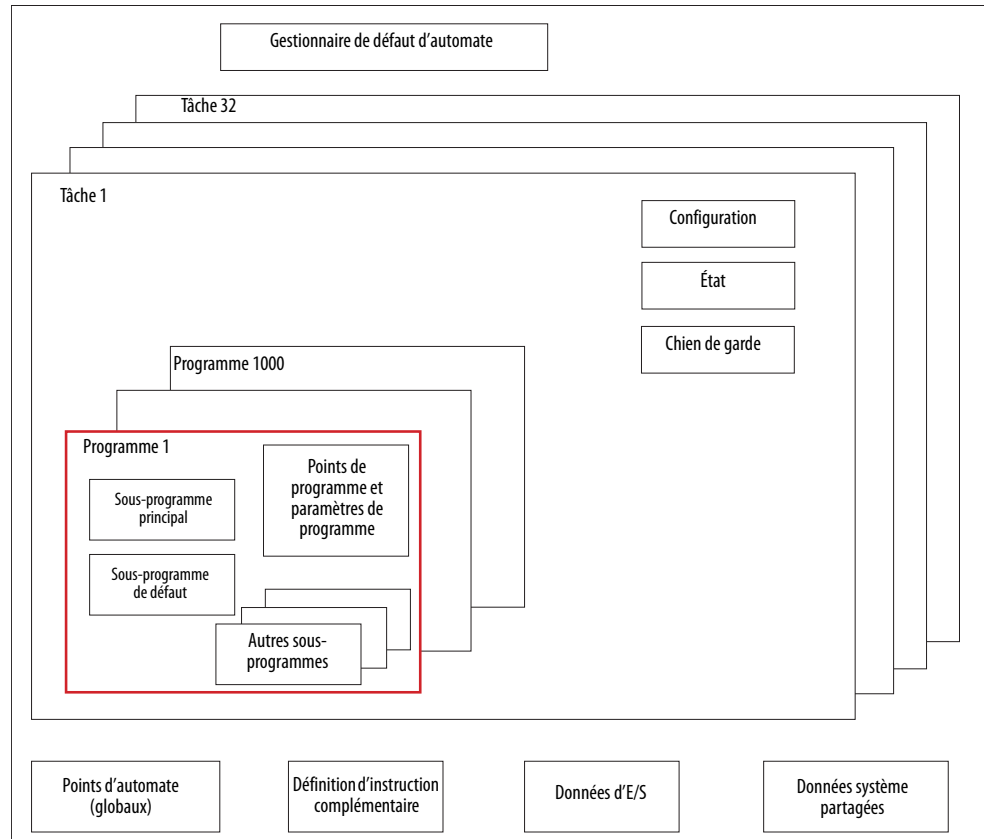
- Des programmes pour grouper les données et la logique
- Des sous-programmes pour encapsuler le code exécutable qui est écrit dans un langage de programmation.

Chaque programme contient les éléments suivants :

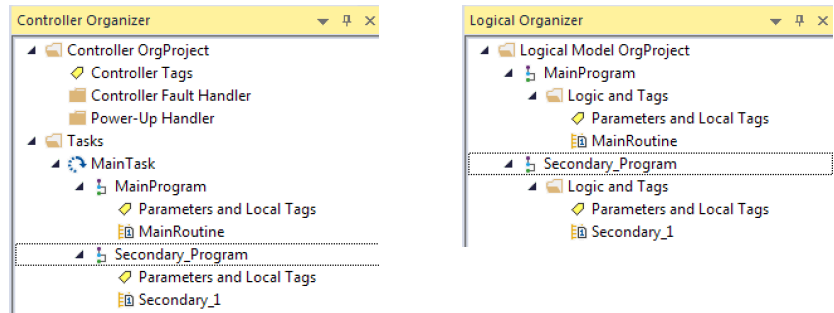
- des points locaux ;
- des paramètres ;
- un sous-programme principal exécutable ;
- d'autres sous-programmes ;
- un sous-programme de défaut facultatif.



**Figure 30 - Programme dans une application de commande**



**Figure 31 - Programmes**



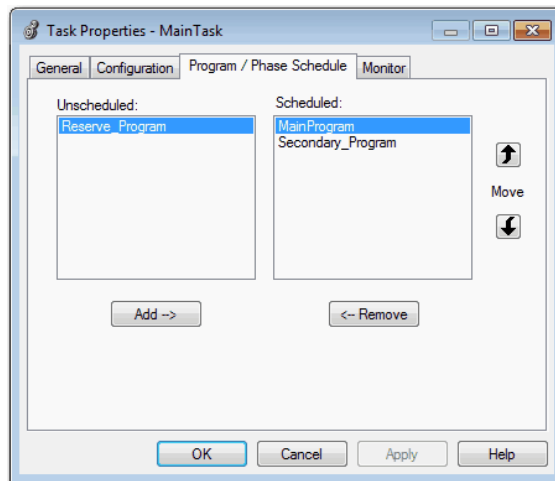
## Programmes planifiés et non planifiés

Les programmes planifiés dans une tâche s'exécutent entièrement du premier au dernier. Les programmes qui ne sont attachés à aucune tâche apparaissent comme des programmes non planifiés.

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

Vous devez planifier un programme au sein d'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 32 - Planification d'un programme non planifié



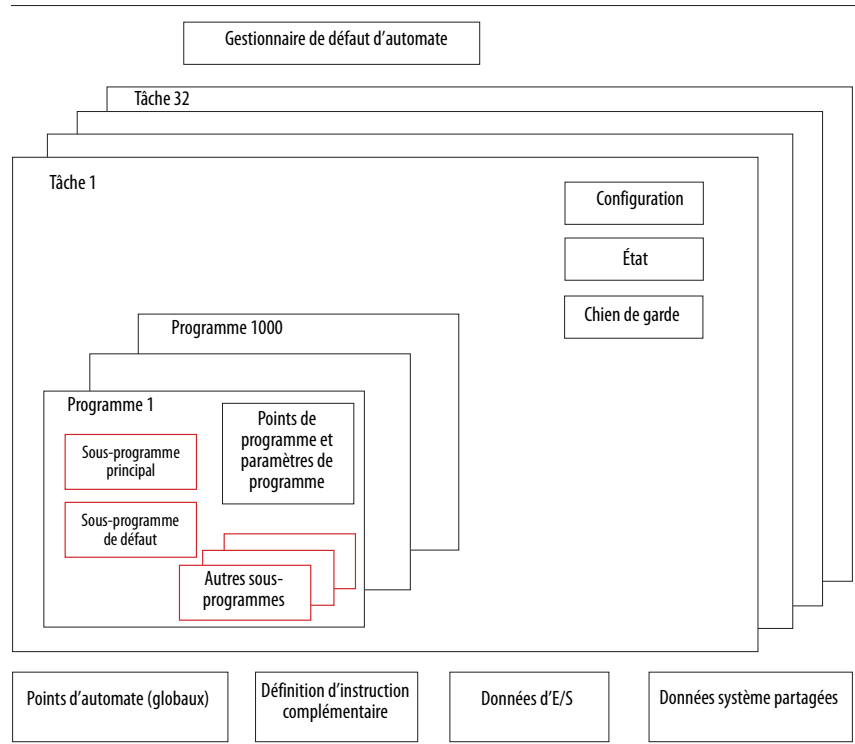
## Sous-programmes

Un sous-programme est un ensemble d'instructions logiques dans un seul langage de programmation, tel que le diagramme à relais (logique à relais). Les sous-programmes fournissent le code exécutable pour le projet dans un automate.

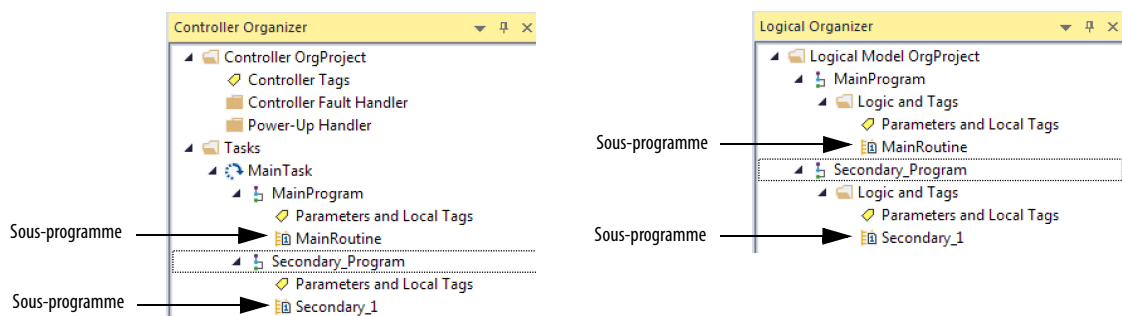
Chaque programme possède un sous-programme principal. C'est le premier sous-programme qui s'exécute quand l'automate déclenche la tâche associée et appelle le programme associé. Utilisez des commandes logiques telles que l'instruction JSR (Jump to Subroutine/saut vers le sous-programme), pour appeler les autres sous-programmes.

Vous pouvez également spécifier un sous-programme de gestion de défauts facultatif. L'automate exécutera ce sous-programme s'il rencontre une erreur d'exécution d'une instruction dans n'importe quel sous-programme associé au programme.

**Figure 33 - Sous-programmes dans une application de commande**



**Figure 34 - Sous-programmes**



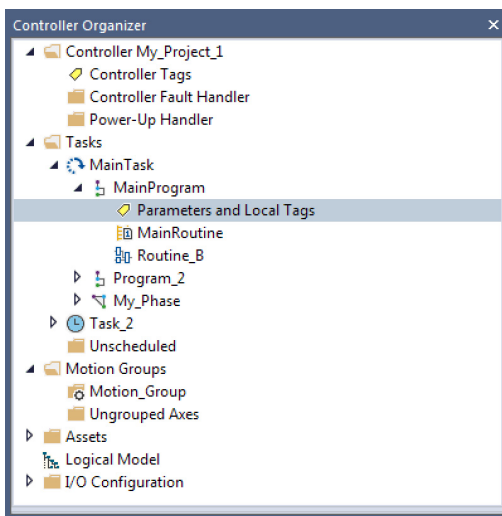
## Paramètres et points locaux

Avec un automate Logix 5000™, vous utilisez un point (nom alphanumérique) pour identifier les données (variables). Dans les automates Logix 5000 il n'y a pas de format numérique fixe. Un nom de point identifie les données et vous permet de faire ce qui suit :

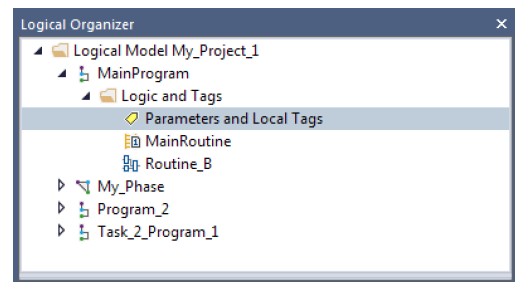
- Organiser vos données pour refléter vos machines.
- Documenter votre application pendant que vous la développez.

Cet exemple montre les points de données créés dans le cadre du programme principal de l'automate.

**Organisateur de l'automate – Paramètres et points locaux du programme principal**



**Organisateur logique – Paramètres et points locaux du programme principal**



**Fenêtre paramètres du programme et points locaux**

Name	Usage	Value	Style	Data Type	Description	Constant	Alias For
ADD_01	Local	{...}		FBD_MATH		<input type="checkbox"/>	
ADD_02	Local	{...}		FBD_MATH		<input type="checkbox"/>	
Disabled	Local	0	Decimal	BOOL		<input type="checkbox"/>	
Motor_Starter_01	Local	{...}		Motor_Starter	Starts the motor.	<input type="checkbox"/>	

Plusieurs directives permettent de créer et de configurer des paramètres et des points locaux pour une exécution optimale des tâches et des programmes. Pour plus d'informations, consultez la publication [1756-PM004](#), « Données d'E/S et de point des automates Logix5000 Manuel de programmation ».

## Paramètres de programme

Les paramètres de programme définissent une interface de données qui facilite le partage des données. Le partage de données entre les programmes peut être réalisé soit par des connexions prédéfinies entre les paramètres, soit directement par une notation spéciale.

Contrairement aux points locaux, tous les paramètres de programme sont publiquement accessibles en dehors du programme. De plus, l'accès externe via IHM peut être spécifié pour chaque paramètre.

Il existe plusieurs directives pour créer et configurer des paramètres et des points locaux pour une exécution optimale des tâches et des programmes :

- La publication [1756-PM004](#), « Données d'E/S et de point des automates Logix5000 Manuel de programmation »
- La publication [1756-PM021](#), « Logix 5000 Controllers Program Parameters Programming Manual »
- La publication [1756-RM094](#), « Logix 5000 Controllers Design Considerations Reference Manual »

## Langages de programmation

L'application Studio 5000 Logix Designer® prend en charge ces langages de programmation.

Langage	Convient le mieux aux programmes avec
Diagramme à relais (LD)	Exécution continue ou parallèle de multiples opérations (non séquencées)
	Opérations booléennes ou basées sur bits
	Opérations logiques complexes
	Traitement des messages et des communications
	Interverrouillage de machine
	Opérations que le personnel d'entretien ou de maintenance doit interpréter pour dépanner la machine ou le procédé
	<b>IMPORTANT</b> : le diagramme à relais est le seul langage de programmation qui peut être utilisé avec la tâche de sécurité sur les automates GuardLogix 5580.
Diagramme de bloc fonctionnel (FBD)	Commande continue de procédé et de variateur
	Contrôle de boucle
	Calculs en flux de circuit
Graphe de fonctionnement séquentiel (SFC)	Gestion de haut niveau de multiples opérations
	Séquence répétitive d'opérations
	Traitement par lots
	Commande de mouvement qui utilise du texte structuré
	Opérations par état de machine
Texte structuré (ST)	Opérations mathématiques complexes
	Traitement spécialisé de boucle de matrice ou de tableau
	Manipulation de chaînes ASCII ou traitement de protocoles

Pour plus d'informations, consultez la [1756-PM001](#), « Logix 5000 Controllers Common Procedures Programming Manual ».

## Instructions complémentaires

Avec l'application Logix Designer, vous pouvez concevoir et configurer des ensembles d'instructions couramment utilisées pour augmenter la cohérence du projet. Semblables aux instructions intégrées qui sont contenues dans les automates, ces instructions que vous créez sont appelées Instructions complémentaires.

Les instructions complémentaires réutilisent des algorithmes de commande communs. Avec elles, vous pouvez :

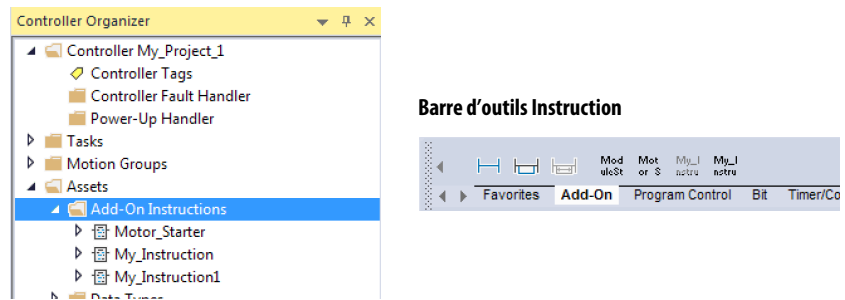
- faciliter la maintenance en créant la logique pour une instance ;
- appliquer la protection des sources pour protéger la propriété intellectuelle ;
- réduire le temps de développement de la documentation.

Vous pouvez utiliser les instructions complémentaires sur de nombreux projets. Vous pouvez définir vos instructions, les obtenir de quelqu'un d'autre ou les copier d'un autre projet. Le [tableau 28](#) explique quelques-uns des avantages et capacités offerts par l'utilisation d'instructions complémentaires.

**Tableau 28 - Capacités de l'instruction complémentaire**

Capacité	Description
Économiser du temps	Avec les instructions complémentaires, vous pouvez combiner votre logique la plus couramment utilisée en ensembles d'instructions réutilisables. Vous gagnez du temps lorsque vous créez des instructions pour vos projets et les partagez avec d'autres. Les instructions complémentaires augmentent la cohérence des projets car les algorithmes couramment utilisés fonctionnent de la même manière, quelle que soit la personne qui implémente du projet.
Utilisation d'éditeurs standard	La création des instructions complémentaires s'effectue à l'aide de l'un des trois éditeurs suivants : <ul style="list-style-type: none"> <li>• Diagramme à relais</li> <li>• Diagramme de bloc fonctionnel</li> <li>• Texte structuré</li> </ul>
Exportation/Importation d'instructions complémentaires	Vous pouvez exporter/importer des instructions complémentaires vers d'autres projets et les copier-coller d'un projet à un autre. Donnez à chaque instruction un nom unique et descriptif pour faciliter la gestion et la réutilisation de votre collection d'instructions complémentaires.
Utilisation des 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.
Documenter l'instruction	Lorsque vous créez une instruction, vous entrez des informations dans les champs de description. Chaque définition d'instruction inclut des informations de révision, d'historique de modification et de description. Le texte de la description devient également la rubrique d'aide pour l'instruction. Vous pouvez également générer une signature pour l'instruction complémentaire et l'inclure dans un groupe de suivi.
Application de la protection de la source	Lorsque vous créez des instructions complémentaires, vous pouvez limiter les utilisateurs de vos instructions à un accès en lecture seule, ou vous pouvez interdire l'accès à la logique interne ou aux paramètres locaux utilisés par les instructions. Cette protection de la source vous permet d'empêcher les modifications indésirables dans vos instructions et de protéger votre propriété intellectuelle. Vous pouvez pré-compiler et crypter votre instruction complémentaire pour une meilleure protection de la propriété intellectuelle. L'utilisation de cette fonctionnalité a moins d'impact sur les performances que la protection de source Logix-designer

Une fois définie dans un projet, les instructions complémentaires se comportent comme les instructions intégrées dans les automates. Avec l'application Studio 5000 Logix Designer version 31 et ultérieure, les instructions complémentaires apparaissent dans le dossier Assets (Actifs) de l'organisateur. Elles apparaissent également sur la barre d'outil des instructions pour un accès facile similaire aux instructions internes.

**Figure 35 - Instructions complémentaires (exemple d'application Studio 5000 Logix Designer version 31)**

## 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
Tag	Dans l'éditeur de point, ajoutez des propriétés étendues à un point.
Type de données défini par l'utilisateur	Dans l'éditeur de type de données, ajoutez des propriétés étendues aux types de données.
Instructions complémentaires	Dans les propriétés qui sont associées à la définition de l'instruction complémentaire, ajoutez des propriétés étendues aux instructions complémentaires.

Le comportement de Pass-through (intercommunication) est la capacité d'attribuer des propriétés étendues à un niveau supérieur d'une structure ou d'une instruction complémentaire et de disposer de cette propriété étendue automatiquement pour tous les membres. Le comportement de Pass-through est disponible pour les descriptions, les identificateurs d'état et les unités d'ingénierie et vous pouvez le configurer.

Configurez le comportement du Pass-through sous 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 Pass-through **n'est pas** disponible pour les limites. Lorsqu'une instance d'un point est créée, si des limites sont associées au type de données, l'instance est copiée.

Utilisez la syntaxe `.@Min` et `.@Max` pour définir des points qui ont des limites, car rien n'indique dans le navigateur de points que des propriétés étendues de limite sont définies pour un point. Si vous essayez d'utiliser des propriétés étendues qui n'ont pas été définies pour un point, les éditeurs affichent une indication visuelle et le sous-programme ne se vérifie pas. Les indicateurs visuels comprennent :

- une erreur de ligne en diagramme à relais ;
- une erreur de vérification X en diagrammes de bloc fonctionnel ;
- l'erreur soulignée en texte structuré.

Vous pouvez accéder aux propriétés étendues de limite définies par la syntaxe `.@ Min` et `.@ Max`. Toutefois, vous ne pouvez pas écrire de valeurs de propriétés étendues à l'aide de la logique du programme.

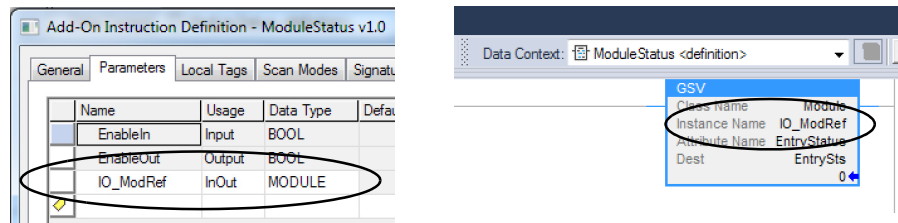
Pour plus d'informations sur les propriétés étendues, consultez la publication [1756-PM004](#), « Données d'E/S et de point des automates Logix5000 Manuel de programmation ».

## Accès à l'objet Module à partir d'une instruction complémentaire

L'objet MODULE fournit des informations d'état à propos d'un module. Pour sélectionner un objet module particulier, définissez l'opérande Object Name (Nom d'objet) de l'instruction GSV/SSV avec le nom du module. Le module spécifié doit être présent dans la section Configuration des E/S de la fenêtre d'organisation de l'automate et doit avoir un nom de dispositif.

Vous pouvez accéder à un objet MODULE directement depuis une instruction complémentaire. Auparavant, vous pouviez accéder aux données de l'objet MODULE, mais pas à partir d'une instruction complémentaire.

Pour accéder aux données de l'objet MODULE, vous devez créer un paramètre de référence de module lorsque vous définissez l'instruction complémentaire. Un paramètre de référence de module est un paramètre InOut du type de données MODULE qui pointe vers l'objet MODULE d'un module matériel. Vous pouvez utiliser les paramètres de référence du module dans la logique de l'instruction complémentaire et la logique du programme.



Pour plus d'informations sur le paramètre Module Reference, consultez l'aide en ligne de l'application Logix Designer et la publication [1756-PM010](#), « Logix 5000 Controllers Add-On Instructions Programming Manual ».

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

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

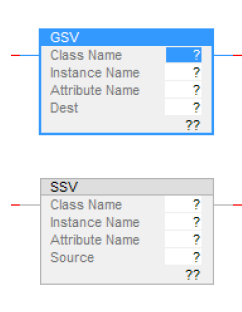


## Surveillance de l'état de l'automate

L'automate ControlLogix utilise des instructions GSV (Get System Value/obtenir une valeur système) et SSV (Set System Value/définir une valeur système) pour obtenir et définir (modifier) les données de l'automate. L'automate stocke les données système dans des objets.

L'instruction GSV récupère les informations spécifiées et les place dans la destination. L'instruction SSV définit l'attribut spécifié avec des données provenant de la source. Les deux instructions sont disponibles à partir de l'onglet Entrée/Sortie de la barre d'outils Instruction.

**Figure 36 - Instructions GSV et SSV pour surveiller et régler des attributs**



Lorsque vous ajoutez une instruction GSV/SSV au programme, les classes d'objets, les noms d'objets et les noms d'attributs de l'instruction sont affichés. Pour l'instruction GSV, vous pouvez obtenir les valeurs des attributs disponibles. Avec une instruction SSV, seuls les attributs modifiables sont affichés.

Certains types d'objet apparaissent à plusieurs reprises, vous devez donc spécifier le nom de l'objet. Par exemple, il peut y avoir plusieurs tâches dans votre application. Chaque tâche possède son propre objet Tâche auquel vous accédez par le nom de la tâche.

Les instructions GSV et SSV surveillent et définissent de nombreux objets et attributs. Consultez l'aide en ligne pour les instructions GSV et SSV.


## Surveillance des connexions d'E/S

Si la communication avec un dispositif dans la configuration d'E/S de l'automate ne se produit pas dans une période spécifique à l'application, la communication s'interrompt et l'automate produit des avertissements.

La période de temps d'attente minimale qui, une fois expirée sans communication, entraîne un timeout est de 100 ms. La période de temps d'attente peut être plus grande, selon le RPI de l'application. Par exemple, si votre application utilise le RPI par défaut = 20 ms, la période de temps d'attente est de 160 ms.

Pour plus d'informations sur la façon de déterminer la durée de votre demande, voir l'article de la base de connaissance [EtherNet/IP Reduced Heartbeats as of RSLogix5000 version 16](#).

Lorsqu'un timeout se produit, l'automate émet les alarmes suivantes :

- Une information d'état de défaut d'E/S défile sur l'afficheur d'état à 4 caractères de l'automate.
- Un  s'affiche sur le dossier de configuration des E/S et sur les dispositifs dont le délai d'attente est atteint.
- Un code de défaut de module est généré. Vous pouvez y accéder par les moyens suivants :
  - la boîte de dialogue Module Properties (Propriétés du module) ;
  - une instruction GSV.

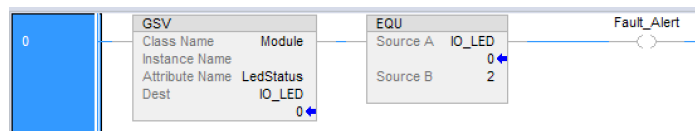
Pour plus d'informations à propos des défauts d'E/S, consultez la publication [1756-PM014](#), « Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual ».

### Déterminer si le délai d'attente de la communication d'E/S a expiré

Cet exemple peut être utilisé avec les automates ControlLogix 5580 ou GuardLogix 5580, et permet de savoir si la communication avec l'automate a expiré :

- 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 mémorise l'état de l'indicateur 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 37 - GSV utilisé pour identifier un délai d'attente d'E/S



#### IMPORTANT Considérations relatives à la sécurité

Les automates de sécurité ont un état de connexion individuel sur chaque module d'E/S de sécurité dans le cadre du point d'entrée.

## Déterminer si une communication avec un module d'E/S particulier est en dépassement du temps d'attente

Si la communication s'interrompt avec un dispositif (module) dans la configuration d'E/S de l'automate, celui-ci produit un code de défaut et des informations de défaut pour le module. Vous pouvez utiliser les instructions GSV pour obtenir le code d'erreur et les informations via les attributs FaultCode et FaultInfo de l'objet Module.

Pour les modules d'E/s de sécurité, consultez [Surveillance des connexions de sécurité, page 209](#).

## Gestion automatique des défauts de connexion de module d'E/S

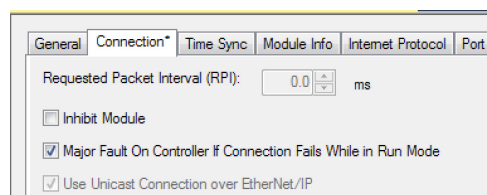
Selon votre application, vous souhaitez peut-être qu'une erreur de connexion d'E/S entraîne l'exécution du gestionnaire de défaut de l'automate. Pour ce faire, définissez la propriété du module pour qu'une erreur de connexion d'E/S provoque un défaut majeur. Le défaut majeur provoque l'exécution du gestionnaire de défaut de l'automate.



**ATTENTION :** Vous ne pouvez pas programmer les connexions du module d'E/S de sécurité ou les connexions de production/consommation de sécurité de façon à entraîner automatiquement un défaut majeur sur l'automate. Consultez [Développement d'applications de sécurité, page 181](#).

S'il est important d'interrompre votre scrutation de programme normale pour gérer un défaut de connexion d'E/S, définissez « Major Fault On Controller If Connection Fails While In Run Mode » (Défaut majeur sur l'automate en cas d'échec de la connexion en mode exécution) et placez la logique dans le gestionnaire de défauts de l'automate.

**Figure 38 - Défaut majeur provoqué par un défaut de connexion d'E/S**



Si la réponse à l'échec d'une connexion de module d'E/S peut attendre la prochaine scrutation du programme, placez la logique dans un sous-programme normal et utilisez la technique GSV décrite page [178](#) pour appeler la logique.

Tout d'abord, développez un sous-programme dans le gestionnaire de défaut de l'automate qui peut répondre aux défauts de connexion d'E/S. Ensuite, dans la boîte de dialogue Module Properties (Propriétés du module) du module d'E/S ou du module de communication parent, cochez « Major Fault On Controller If Connection Fails While in Run Mode ».

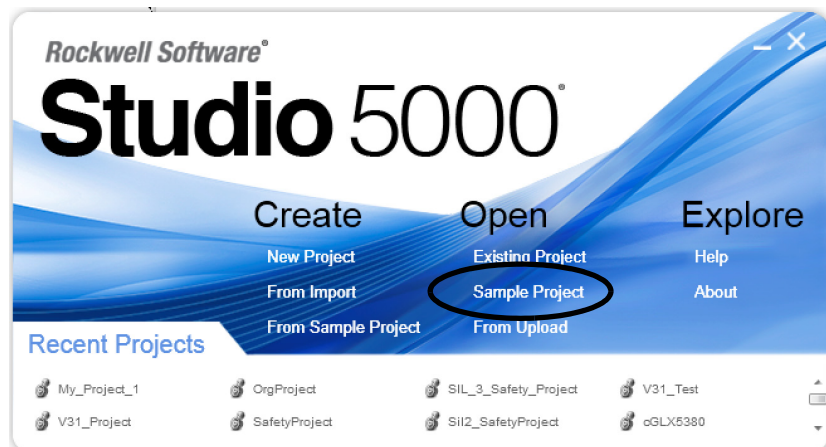
**CONSEIL** Il faut au moins 100 millisecondes pour détecter une perte de connexion d'E/S, même si le gestionnaire de défaut de l'automate est utilisé.

Pour plus d'informations sur la programmation du gestionnaire de défauts de l'automate, reportez-vous à la publication [1756-PM014](#), « Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual ».

## Exemples de projets d'automate

Logix Designer comprend des exemples de projets que vous pouvez copier et modifier pour convenir à votre application. Pour accéder aux exemples de projets, cliquez sur Sample Project (Exemple de projet) dans l'interface Studio 5000®.

Figure 39 - Ouvrir des exemples de projets



## Développement d'applications de sécurité

Rubrique	Page
Tâche de sécurité	182
Programmes de sécurité	184
Sous-programmes de sécurité	185
Instructions complémentaires de sécurité	185
Points de sécurité produits/consommés	188
Mappage de point de sécurité	197
Protection de l'application de sécurité	200
Restrictions de programmation	205
Surveillance de l'état de la sécurité	206
Défauts de sécurité	212
Développement d'un sous-programme de défaut pour les applications de sécurité	215
Utilisation des instructions GSV/SSV dans une application de sécurité	216

### S'applique à ces automates :

GuardLogix 5580

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.

La publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité », traite des sujets suivants :

- Directives et exigences à respecter pour le développement et la mise en service d'applications de sécurité SIL 2/PLd et SIL 3/PLe, y compris l'utilisation de profils complémentaires ;
- écriture, documentation et test de l'application ;
- création d'une spécification détaillée pour un projet ;
- génération de la signature de sécurité pour identifier et protéger le projet ;
- validation du projet transféré à partir de son impression ou de son affichage en comparant manuellement les configurations, les données de sécurité et la logique du programme de sécurité ;
- vérification du projet à l'aide de tests types, de simulations, de tests de vérification fonctionnelle ; et s'il y a lieu, un examen de conformité des fonctions de sécurité par un organisme indépendant ;

- verrouillage de l'application de sécurité ;
- calcul du temps de réaction du système.

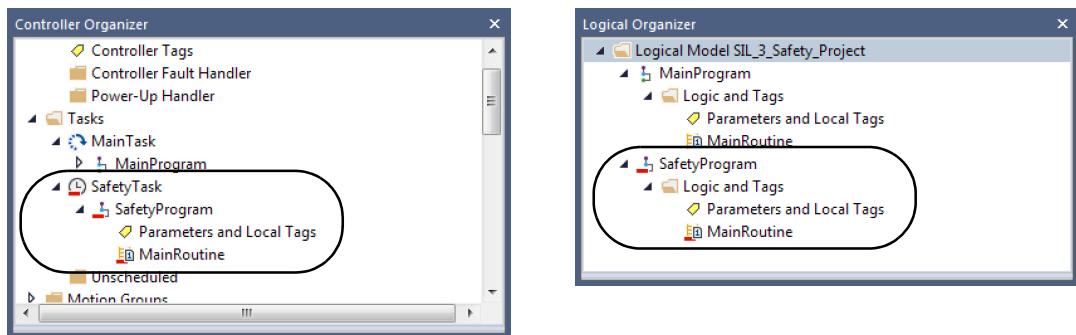


**ATTENTION** : L'exécution d'une modification en ligne (du programme logique, de données ou de la configuration) peut influencer sur la ou les fonctions de sécurité du système si la modification est apportée pendant l'exécution de l'application. Une modification doit uniquement être tentée en cas d'absolue nécessité. De plus, si la modification n'est pas exécutée correctement, elle peut arrêter l'application. Par conséquent, lorsqu'une signature de sécurité est supprimée pour modifier en ligne la tâche de sécurité, avant l'exécution de la modification en ligne vous devez mettre en œuvre des mesures de sécurité de remplacement, qui doivent être présentes pendant la durée de la mise à jour.

## Tâche de sécurité

Lorsque vous créez un projet pour un automate de sécurité, l'application Studio 5000 Logix Designer® crée automatiquement une tâche de sécurité avec un programme de sécurité et un sous-programme principal (de sécurité).

Figure 40 - Tâche de sécurité dans l'organisateur de l'automate et dans l'organisateur logique



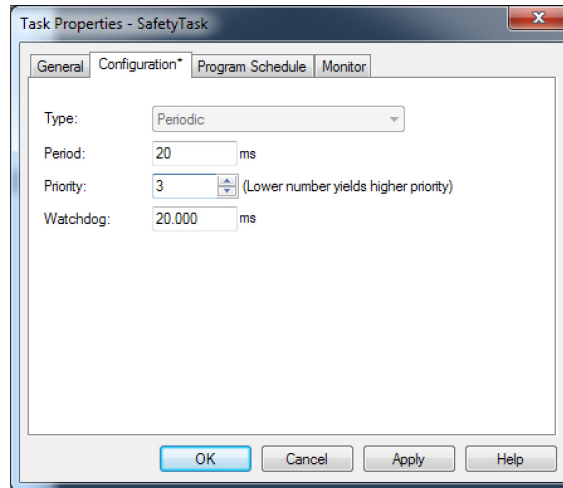
Dans la tâche de sécurité, vous pouvez utiliser plusieurs programmes de sécurité, constitués de plusieurs sous-programmes de sécurité. Les automates GuardLogix® 5580 prennent en charge une tâche de sécurité. La tâche de sécurité ne peut pas être supprimée.

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

## Période de la tâche de sécurité

La tâche de sécurité est une tâche périodique. Vous définissez 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 41 - Configuration de la période de la tâche de sécurité**



Pour avoir le temps d'exécution de la tâche de sécurité le plus cohérent, et pour minimiser les défauts de chien de garde de la tâche de sécurité, nous vous conseillons d'exécuter la tâche de sécurité comme la tâche utilisateur de la plus 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 l'intervalle de temps qui s'écoule entre les temps de démarrages successifs de la tâche de sécurité. 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.

Pour de plus amples informations sur le calcul du temps de réponse du système, reportez-vous à la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

## Exécution de la tâche de sécurité

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

- Pour une application SIL 3/PL, 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. Les tâches standard commencent 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, reportez-vous à la page [197](#).
- Les paquets de sortie de sécurité (points produits et modules de sortie) sont générés à la fin de l'exécution de la tâche de sécurité.
- Lorsque l'automate n'a pas de signature de sécurité et que sa sécurité n'est pas verrouillée, la tâche de sécurité peut être suspendue jusqu'à ce qu'une mise à jour des communications soit terminée.

## Programmes de sécurité

Les programmes de sécurité possèdent tous les attributs des programmes standard, hormis le fait qu'ils ne peuvent être planifiés qu'à l'intérieur de la 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.

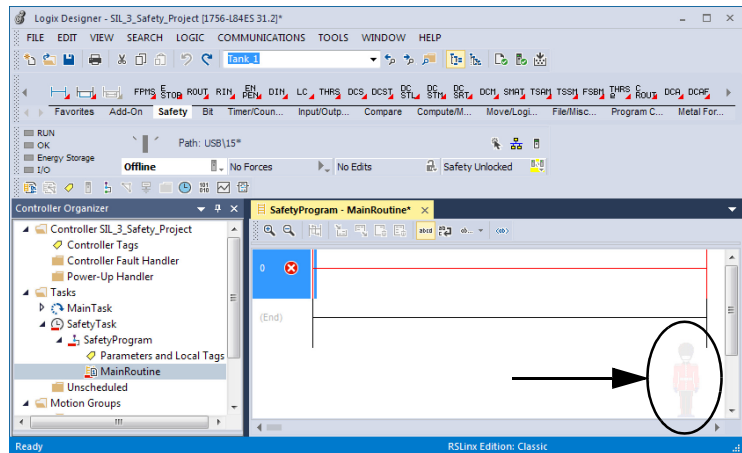
Les programmes de sécurité ne peuvent pas contenir de sous-programmes standard ou de points standard.



## 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. La programmation des sous-programmes de sécurité ne peut s'effectuer qu'avec la logique à relais.

**CONSEIL** Un filigrane permet de distinguer visuellement un sous-programme de sécurité d'un sous-programme standard.



## Instructions complémentaires de sécurité

Vous pouvez créer des instructions complémentaires de sécurité à utiliser dans des applications de sécurité. Les instructions complémentaires de sécurité sont caractérisées par une signature d'instruction de sécurité à utiliser dans les applications de sécurité jusqu'au niveau SIL 2 inclus.

Pour de plus amples informations, consultez la publication [1756-PM010](#), « Logix 5000 Controllers Add On Instructions Programming Manual ».

## Points de sécurité

Les points de sécurité possèdent tous les attributs des points standard, avec en plus des mécanismes certifiés pour permettre l'intégrité des données SIL 2/PLd et SIL 3/PLe.

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
- Si la valeur du point est une constante

---

**IMPORTANT** Vous ne pouvez pas créer un alias de point d'un point de sécurité. Les points standard peuvent plutôt être mappés sur les points de sécurité en utilisant le mappage de points de sécurité. Reportez-vous à [Mappage de point de sécurité, page 197](#).

---

L'application Logix Designer peut écrire directement sur des points de sécurité via l'éditeur de point lorsque l'automate GuardLogix 5580 est verrouillé en sécurité, ne possède pas de signature de sécurité et fonctionne sans défauts 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. Les dispositifs IHM peuvent avoir un accès en lecture seule aux points de sécurité (en fonction du réglage External Access [Accès externe]).

## Types de données valides

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 tableaux ou de types de données utilisateur.

Les automates Logix contiennent des types de données prédéfinis utilisables avec des instructions spécifiques. Les points de sécurité peuvent être composés des éléments suivants :

- Tous les types de données primitifs (par exemple, BOOL, SINT, INT, DINT, LINT, REAL)
- Types prédéfinis utilisés pour les instructions d'application de sécurité
- Types utilisateur ou tableaux qui sont constitués des deux types ci-dessus.

## Accès

L'accès d'un point détermine l'endroit d'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.

Les points de sécurité en accès automate peuvent être lus par un programme logique standard ou de sécurité ou tout autre dispositif de communication externe, mais ils peuvent uniquement être écrits par le programme logique de sécurité ou un autre automate de sécurité GuardLogix. Les points de sécurité d'accès programme peuvent être lus par des dispositifs de communication externes, mais seuls les sous-programmes de sécurité locaux peuvent y écrire. Il s'agit de sous-programmes qui résident dans le programme de sécurité.

Lorsque vous créez des points en accès programme, leur classe est automatiquement spécifiée en fonction du type de 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.

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 le mappage d'un point de sécurité.

Pour de plus amples informations, consultez [Mappage de point de sécurité, page 197](#)

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

## Paramètres de programme

Pour les paramètres de programme, un paramètre de sécurité ne peut pas être connecté ou lié à un paramètre standard ou à un point en accès automate.

Pour plus d'informations sur les paramètres de programme, consultez [Paramètres de programme, page 173](#).

## Points de sécurité produits/consommés

Pour transférer des données de sécurité entre des automates GuardLogix, vous devez utiliser des points de sécurité produits et consommés.

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/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. Ce membre est d'un type de données prédéfini dénommé CONNECTION\_STATUS.

**Tableau 29 - Connexions produites et consommées**

Point	Description de la connexion
Produit	<p>Les automates GuardLogix 5580 peuvent produire (envoyer) des points de sécurité vers d'autres automates GuardLogix.</p> <ul style="list-style-type: none"> <li>Les automates GuardLogix 5580 ne prennent en charge que des points produits en envoi individuel.</li> <li>Les automates GuardLogix 5580 prennent en charge la production d'un point à un maximum de 15 consommateurs si tous les consommateurs sont configurés pour consommer le point en envoi individuel.</li> <li>L'automate producteur utilise une connexion unique avec chaque consommateur.</li> <li>L'automate consommateur doit être à la révision de firmware 19 ou ultérieure. L'envoi individuel n'a pas été ajouté aux points produits/consommés de sécurité avant la révision 19 du firmware.</li> </ul>
Consommé	<p>Les automates GuardLogix 5580 peuvent consommer (recevoir) des points de sécurité d'autres automates GuardLogix dans les configurations suivantes :</p> <ul style="list-style-type: none"> <li>Si vous avez un automate GuardLogix 5580 (le producteur) dans l'arborescence d'E/S d'un autre automate GuardLogix 5580 (le consommateur), le consommateur ne peut consommer qu'un point en provenance du producteur si le point est en envoi individuel.</li> <li>Si l'automate producteur est un automate GuardLogix 5570, un automate consommateur GuardLogix 5580 peut consommer des points en multi-diffusion ou envoi individuel.</li> <li>Chaque point consommé utilise une connexion.</li> </ul>

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 de données 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 données 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, comme décrit ci-dessous.

## Configuration du SNN pour une connexion à un automate de sécurité homologue

L'automate de sécurité homologue est assujéti aux mêmes exigences de configuration que l'automate de sécurité local. L'automate de sécurité homologue doit également avoir un numéro SNN.

L'application de sécurité qui est téléchargée dans l'automate de sécurité homologue configure les valeurs SNN pour chaque port CIP Safety™ de l'automate.

**Tableau 30 - SNN et position de l'automate**

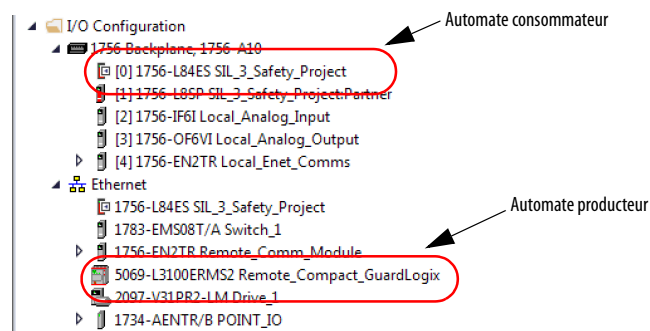
Position de l'automate de sécurité homologue	SNN
Placé dans le châssis local	L'application utilisateur sur l'automate homologue génère une valeur SNN pour le port du bus intermodules local de l'automate.
Dans un autre châssis	L'automate doit avoir un SNN unique.

Pour une explication du numéro de réseau de sécurité, consultez la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

Si le SNN attribué automatiquement de l'automate producteur ne correspond pas au SNN que l'automate utilise effectivement, vous pouvez procéder comme suit pour copier et coller le SNN.

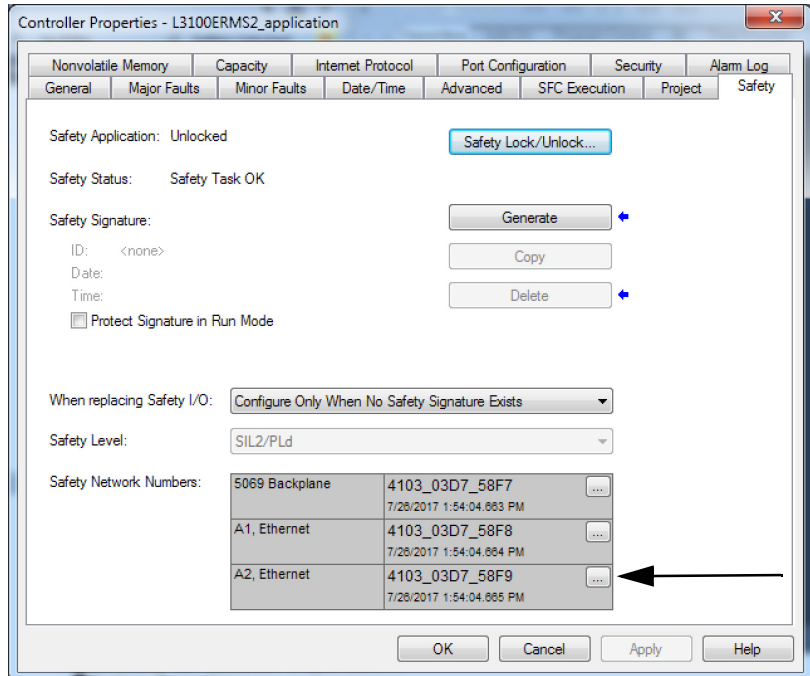
**CONSEIL** Régler les SNN corrects de l'automate comme décrit dans [Attribuer le numéro de réseau de sécurité \(SNN\), page 66](#) entraîne généralement l'attribution du SNN correct à l'automate producteur. Dans ces cas, vous n'avez pas besoin d'effectuer cette procédure.

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

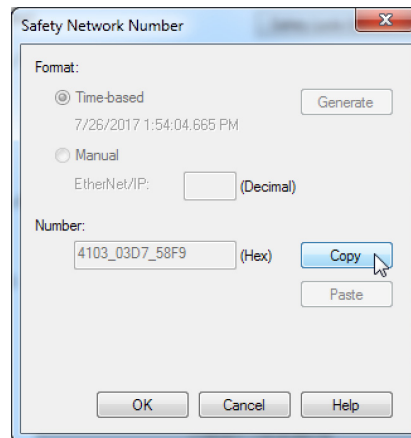


2. Dans le projet de l'automate producteur, cliquez sur l'automate producteur avec le bouton droit de la souris puis sélectionnez Contrôler Propriétés (Propriétés de l'automate).

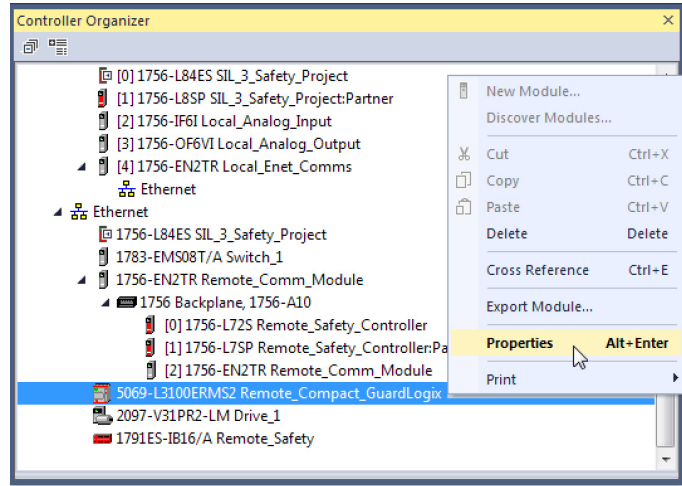
- À l'onglet Safety (Sécurité), cliquez sur [...] à côté du port (Ethernet ou bus intermodules) qui communique avec l'automate consommateur. La boîte de dialogue Safety Network Number (Numéro de réseau de sécurité) s'ouvre.




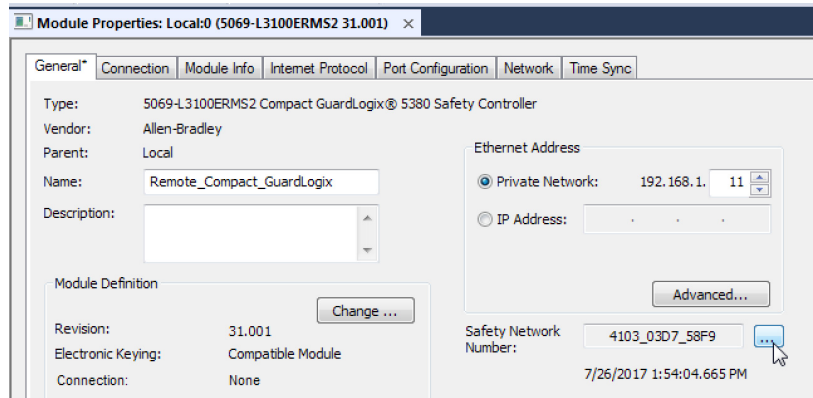
- Copiez le SNN de l'automate producteur.



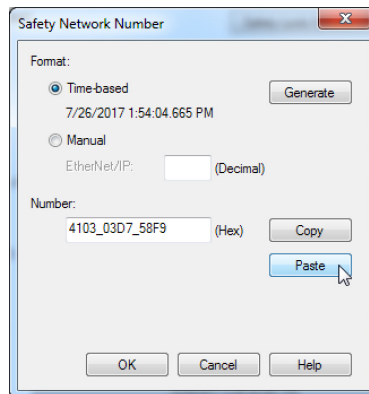
- Dans l'arborescence des E/S du projet d'automate consommateur, faites un clic droit sur le module qui représente l'automate producteur, et choisissez Properties (Propriétés).



- Sous l'onglet General de Module Properties (Propriétés du module) cliquez sur  pour ouvrir la boîte de dialogue Safety Network Number.

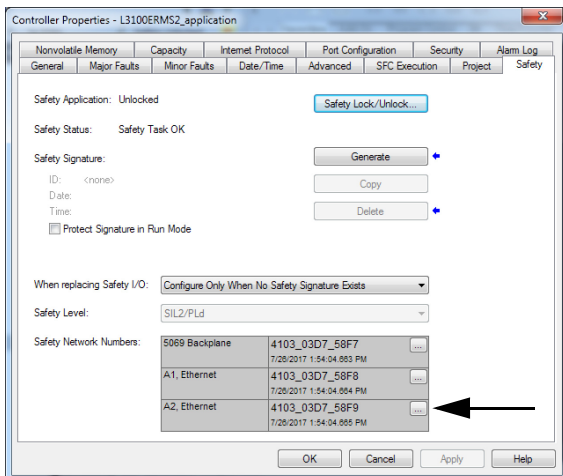


- Collez le SNN de l'automate producteur dans le champ du SNN et cliquez sur OK.

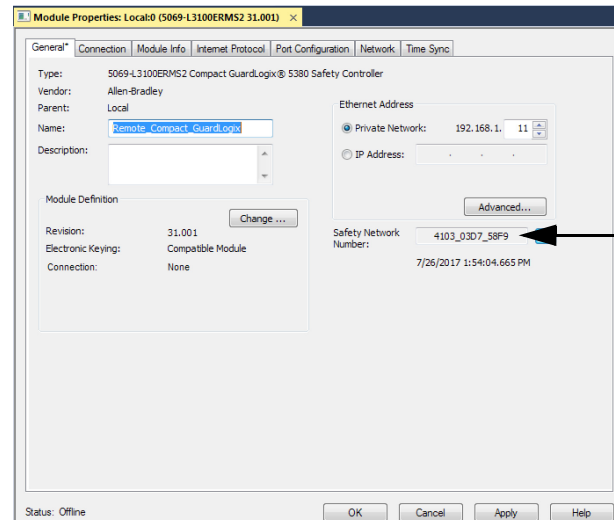


Les numéros de réseau de sécurité correspondent.

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



**Boîte de dialogue des propriétés du module dans le projet consommateur**

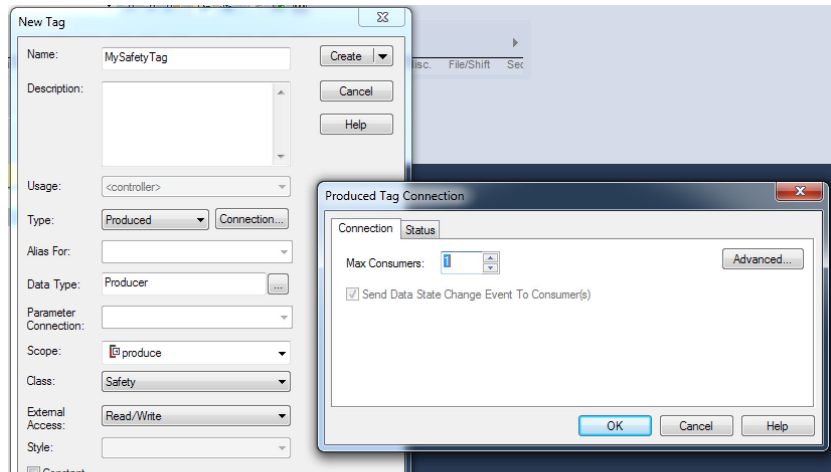




## Production d'un point de sécurité

Pour produire un point de sécurité, procédez comme suit.

1. Dans le projet des automates producteurs, créez un type de données utilisateur définissant 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 maximum de consommateurs (entre 1 et 15).



5. Cliquez sur OK.
6. Cliquez sur Create (Créer).

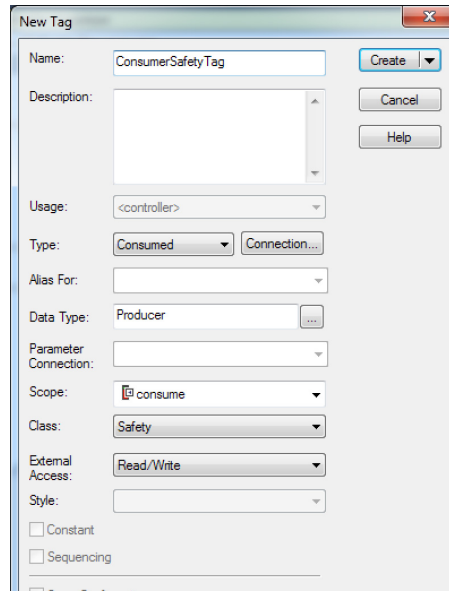
## Consommation de points de données de sécurité

Pour consommer des données produites par un autre automate, procédez comme suit :

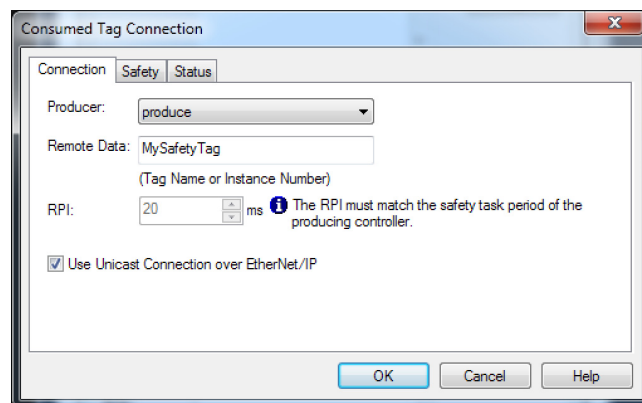
1. Dans le projet d'automate consommateur, créez un type de données utilisateur identique à celui créé dans le projet producteur (les noms des types de données utilisateur doivent correspondre).

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

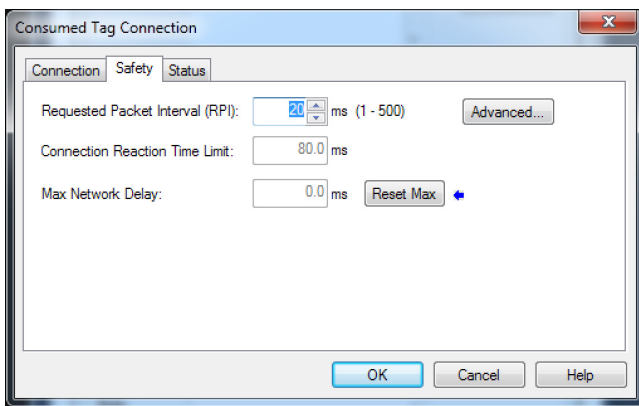
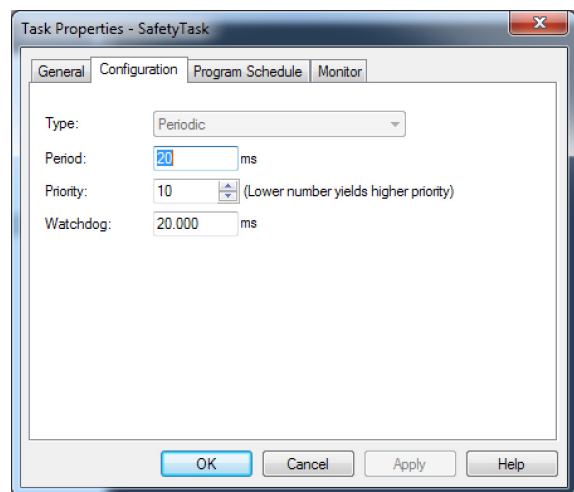
2. Cliquez avec le bouton droit sur Controller Tags (Points automate) et sélectionnez New Tag (Nouveau point).
3. Définissez Consumed (Consommé) comme Type, Safety (Sécurité) comme Classe et le type de données utilisateur que vous avez créé à l'étape 1 comme Data Type (Type de données).



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



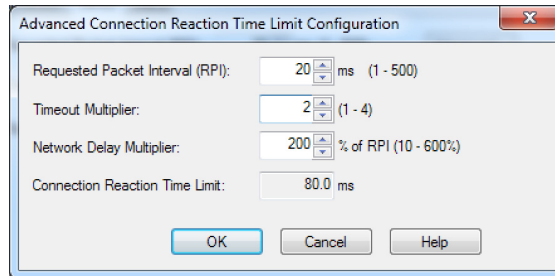
5. Dans les menus déroulants Producteur (Producteur), sélectionnez l'automate qui produit les données.
6. Dans le champ Remote Data (Données décentralisées), entrez le nom du point produit.
7. Cliquez sur l'onglet Safety (Sécurité).
8. Dans le champ Requested Packet Interval (RPI), entrez le RPI pour 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 du consommateur****Projet du 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 période de la tâche de sécurité de l'automate producteur, qui ajuste la valeur RPI, pour obtenir un temps limite acceptable pour la 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 le temps limite de réponse de la connexion est acceptable, cliquez sur OK.

**CONSEIL** Si un point de sécurité consommé a un code d'erreur : « 16#0111 Requested Packet Interval (RPI) out of range », vérifiez que le RPI du point consommé correspond à la période de la tâche de sécurité producteur.

- Dans le cas de critères plus complexes, cliquez sur Advanced de l'onglet Safety pour accéder aux paramètres Advanced Connection Reaction Time Limit (Temps limite avancé de réponse 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 le temps limite de réponse de la connexion.



**ATTENTION :** Si vous diminuez le multiplicateur de timeout ou le multiplicateur de délai réseau pour les passer au-dessous des valeurs par défaut, cela pourrait générer des pertes de connexion de sécurité préjudiciables. Si vous utilisez des réseaux sans fil, vous pourriez avoir besoin d'augmenter les valeurs au-dessous des valeurs par défaut.

Tableau 31 - Autres ressources

Documentation	Description
<a href="#">Limite de temps de réponse de la connexion, page 148</a>	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
<a href="#">Surveillance des connexions de sécurité, page 209</a>	Contient des informations sur le type de données prédéfini CONNECTION_STATUS.
Étiquettes produites et consommées des Automates Logix 5000 Manuel de programmation, publication <a href="#">1756-PM011</a>	Informations détaillées sur l'utilisation des points produits et consommés.

## Mappage de point de sécurité

Un sous-programme de sécurité ne peut pas accéder directement à des points standard. 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.

Les points mappés sont copiés depuis les points standard vers les points de sécurité correspondants au début de la tâche de sécurité. Cela risque d'accroître le temps de scrutation de la tâche de sécurité.

**CONSEIL** Les sous-programmes de tâche standard peuvent lire directement les points 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 une constante ;
- vous ne pouvez pas modifier le mappage de points lorsque l'une des conditions suivantes est vraie :
  - la sécurité du projet est verrouillée ;
  - il existe une signature de sécurité ;
  - le sélecteur à clé de l'automate est en position RUN ;
  - un défaut de sécurité irrécupérable existe ;
  - le partenariat entre l'automate principal et son partenaire de sécurité est incorrect.

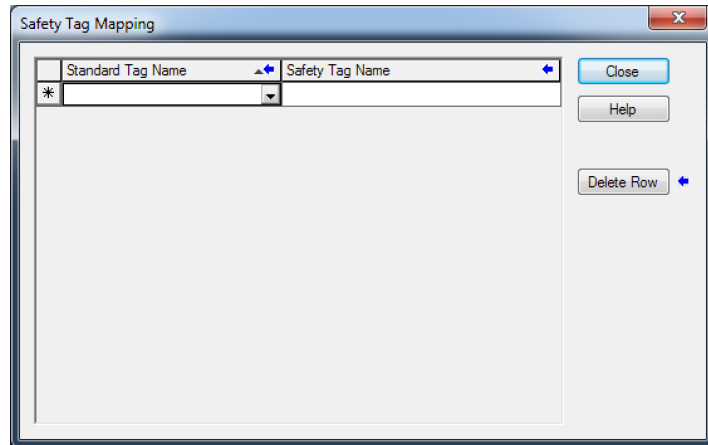


**ATTENTION :** Lorsque vous utilisez des données standard dans un sous-programme de sécurité, vous devez vérifier que leur utilisation est conforme. L'utilisation de données standard dans un point de sécurité n'en fait pas des données de sécurité. Vous ne devez pas commander directement une sortie de sécurité SIL 2/PLd ou SIL 3/PLe avec des données provenant d'un point standard.

Pour de plus amples informations, reportez-vous à la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

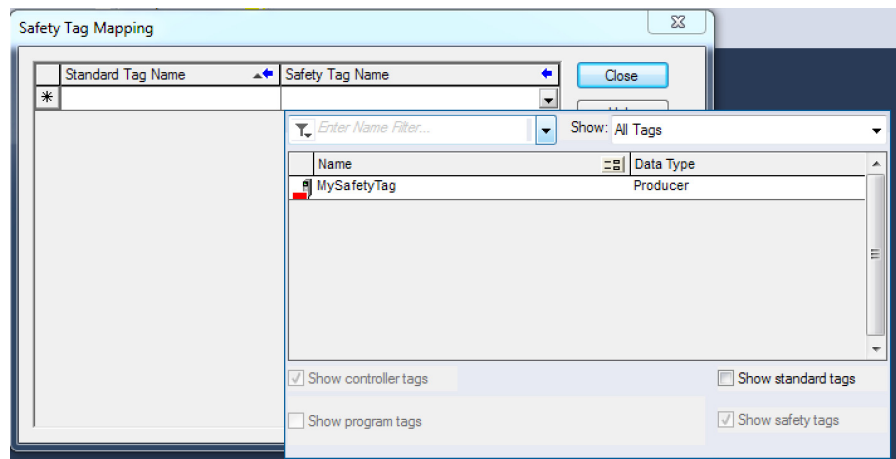
## Création de paires de points mappées

1. Sélectionnez Map Safety Tags (Mapper des points de sécurité) dans le menu Logic 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 et 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 32 - Icônes d'état du mappage des points**

Contenu de la cellule	Description
Vide	Le mappage de points est correct.
	Lorsque vous êtes hors ligne, l'icône X indique que le mappage des points est incorrect. Vous pouvez passer à une autre ligne ou fermer la boîte de dialogue Safety Tag Mapping (Mappage de point de sécurité). <sup>(1)</sup> 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 [197](#).

## Protection de l'application de sécurité

Vous pouvez protéger votre programme d'application vis-à-vis de toute modification illicite en générant une signature de sécurité, en définissant des mots de passe et en verrouillant la sécurité de l'automate.

### Verrouillage de sécurité de l'automate



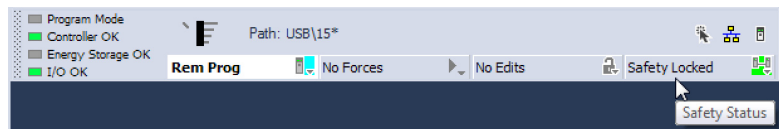
**ATTENTION** : Le verrouillage de la sécurité en tant que tel ne satisfait pas aux exigences SIL 2/PLd ou SIL 3/PLe.

Vous pouvez verrouiller l'automate GuardLogix 5580 pour protéger les composants de contrôle liés à la sécurité contre toute modification et empêcher la suppression accidentelle de la signature de 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 sécurité.

**CONSEIL** Il existe de plusieurs façons de voir l'état du verrouillage de la sécurité de l'automate :

- L'afficheur à 4 caractères sur l'automate indique l'état du verrouillage.
- Dans l'application Logix Designer, le texte du bouton Safety Status (État de sécurité) sur la barre en ligne indique l'état du verrouillage de la sécurité.



- La barre d'application Logix Designer affiche également les icônes ci-après 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 l'état de la sécurité lorsque le sélecteur à clé de mode de l'automate est en position RUN (Exécution).

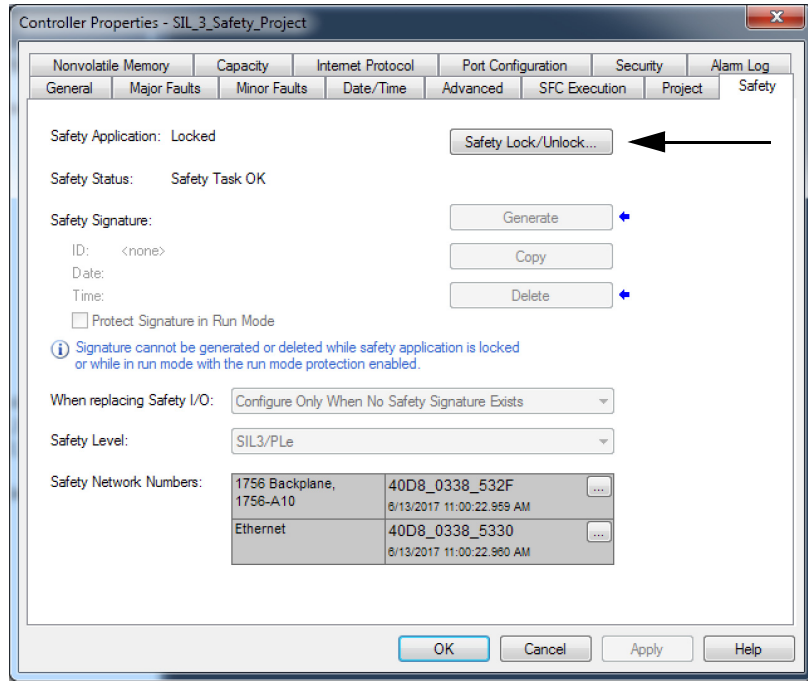
**CONSEIL** Les actions de verrouillage ou de déverrouillage de la sécurité sont enregistrées dans le journal de l'automate.

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).

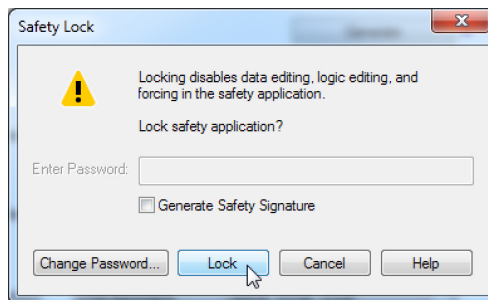
**Figure 42 - Verrouillage de sécurité de l'automate**



**CONSEIL** Dans l'application Logix Designer, vous pouvez aussi choisir **Tools > Safety > Safety Lock/Unlock** (Outils > Sécurité > Verrouiller/Déverrouiller sécurité).

Si vous avez défini un mot de passe pour la fonctionnalité 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).

**Figure 43 - Verrouillage de la sécurité de l'automate**



Vous pouvez également définir ou modifier le mot de passe à partir de la boîte de dialogue Safety Lock (Verrouillage de la sécurité) : Reportez-vous à [Définition des mots de passe pour verrouiller ou déverrouiller la sécurité, page 202.](#)

La fonctionnalité de verrouillage de sécurité décrite dans cette section, ainsi que les mesures de sécurité standard de l'application Logix Designer sont applicables aux projets d'automate GuardLogix.

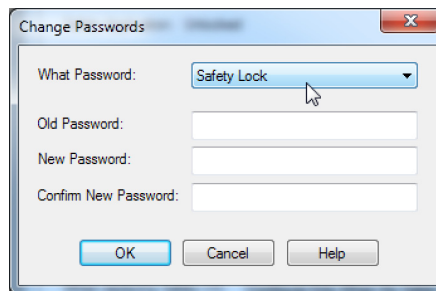
Pour des informations complémentaires sur les fonctionnalités de sécurité de Logix Designer, reportez-vous à la publication [1756-PM016](#), « Sécurité des automates Logix5000 Manuel de programmation ».

## Définition des mots de passe pour verrouiller ou déverrouiller la sécurité

La fonctionnalité 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. Dans la barre de menus Logix Designer, cliquez sur Tools > Safety > Change Passwords (Outils > Sécurité > Changer 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.

**CONSEIL** 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 : ' ~ ! @ # \$ % ^ & \* ( ) \_ + , - = { } | [ ] \ ; ? / .  
Pour effacer un mot de passe existant, saisissez un nouveau mot de passe de longueur nulle.

---

**IMPORTANT** Rockwell Automation n'offre pas de service de dérogation au mot de passe ou à la sécurité. Lorsque les produits et les mots de passe sont configurés, Rockwell Automation invite les clients à adopter de bonnes pratiques de sécurité et de planifier en conséquence la gestion des mots de passe.

---

## Générer une signature de sécurité

**IMPORTANT** Pour générer une signature, l'automate doit être en mode Programmation.

Avant d'entreprendre les tests de vérification, vous devez générer la signature de sécurité. Vous ne pouvez générer la signature de sécurité que si les conditions suivantes sont remplies :

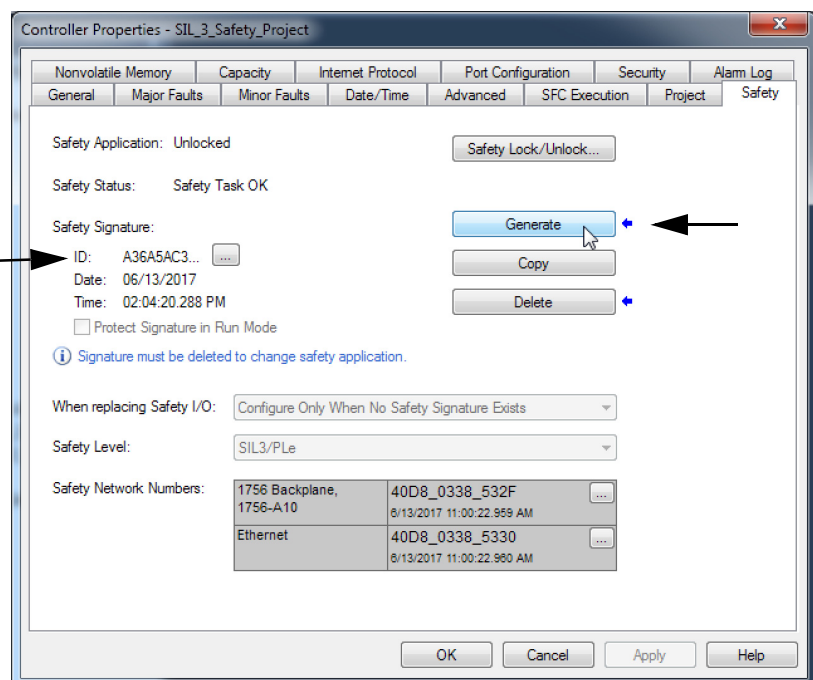
- Le projet de l'automate GuardLogix 5580 déverrouillé en sécurité est en ligne ;
- il n'y a pas de forçages de sécurité, de modifications de sécurité en ligne en attente, ni de défauts de sécurité ;
- L'état de la sécurité doit être « Safety Task OK » (Tâche de sécurité OK).

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

Pour générer la signature de sécurité depuis l'onglet Safety (Sécurité) de la boîte de dialogue Controller Properties (Propriétés de l'automate), cliquez sur Generate (Générer).

**Figure 44 - Génération d'une signature de sécurité**

Pour la signature de sécurité, les automates GuardLogix 5580 ont un ID de 32 octets. Seuls les 4 premiers octets de l'ID sont affichés sous l'onglet. Pour voir et copier l'identifiant complet à 32 octets, cliquez sur [...] pour ouvrir la boîte de dialogue Safety Signature ID (ID de signature de sécurité).



**CONSEIL** Dans l'application Logix Designer, vous pouvez aussi choisir Tools > Safety > Generate Signature (Outils > Sécurité > Générer signature).

Si une signature précédente existe, vous êtes invité à l'écraser.

**CONSEIL** La création et la suppression d'une signature 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 modification en ligne et hors ligne (y compris les instructions complémentaires de sécurité) ;
- forcer les E/S de sécurité ;
- modifier l'état d'inhibition des E/S de sécurité ou des automates producteur ;
- manipulation des données de sécurité (sauf par la logique d'un sous-programme de sécurité) ;
- télécharger une nouvelle application de sécurité.

#### *Copier la signature de sécurité*

Vous pouvez utiliser le bouton Copy (Copier) pour créer un enregistrement de la signature de sécurité, 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.

#### *Supprimer la signature de sécurité*

Cliquez sur Delete (Supprimer) pour effacer la signature de sécurité.

La signature de sécurité ne peut pas être supprimée lorsque :

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



**ATTENTION** : Si vous supprimez la signature de tâche de sécurité, vous devrez retester et revalider la conformité SIL 2/PLD ou SIL 3/PLE de votre système.

Pour de plus amples informations sur les exigences du niveau d'intégration de sécurité (SIL) et du niveau de performance (PL), consultez la publication [1756-RM012](#), « Systèmes de commande GuardLogix 5580 et Compact GuardLogix 5380 Manuel de référence sur la sécurité ».

---

## Restrictions de programmation

Des restrictions limitant la disponibilité de certains éléments de menu et fonctionnalités (c'est-à-dire couper, coller, supprimer et remplacer) sont imposées par l'application Logix Designer pour protéger les composants de sécurité contre toute modification chaque fois que l'une de ces conditions est vraie :

- la sécurité de l'automate est verrouillée ;
- une signature de sécurité existe ;
- des défauts de sécurité sont présents ;
- l'état de la sécurité est dans l'un de ces états lorsqu'il est en ligne :
  - Partenaire absent
  - Partenaire indisponible
  - Matériel incompatible
  - Firmware incompatible

---

**IMPORTANT** Les temps maximum et récents de scrutation de la tâche de sécurité et des programmes de sécurité peuvent être réinitialisés en ligne.

---

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

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

Lorsque la sécurité de l'automate est verrouillée, vous ne pouvez pas modifier ou supprimer la signature de sécurité.

## Surveillance de l'état de la sécurité

Vous pouvez surveiller l'état de la sécurité d'une des façons suivantes :

- la barre en ligne dans l'application Logix Designer ;
- l'onglet Safety (Sécurité) dans la boîte de dialogue Controller Properties (Propriétés 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 45 - Boutons d'état



#### État de l'automate

Lorsque le bouton d'état de l'automate **Rem Prog** est sélectionné, comme dans la figure ci-dessus, la barre en ligne affiche le mode de fonctionnement de l'automate (Remote Program) et l'état (OK). L'indicateur Energy Storage OK (Stockage d'énergie OK) représente l'état combiné de l'automate principal et du partenaire de sécurité.

Si l'un ou l'autre présente un défaut de stockage d'énergie, l'indicateur d'état s'allume. L'indicateur I/O (E/S) représente l'état combiné des E/S standard et de sécurité. L'E/S ayant l'état d'erreur le plus important s'affiche à côté de l'indicateur d'état.

#### État des forçages


Le bouton Forces Status (État des forçages) **No Forces** indique Forces (Forçages) ou No Forces (Pas de forçages). Lorsque le bouton est sélectionné, la barre en ligne indique si les forçages d'E/S ou SFC sont activés ou désactivés et installés ou non. Le menu ForcesStatus (État des forçages) contient des commandes de suppression, d'activation et de désactivation de tous les forçages.

#### État des modifications en ligne

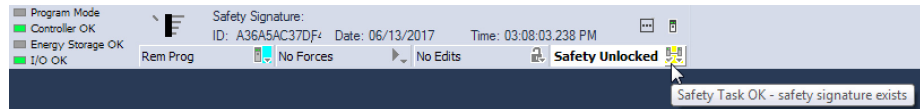
Le bouton Online Edit Status (État des modifications en ligne)


**No Edits** indique s'il existe ou non des modifications dans le sous-programme en logique à relais ou le diagramme de blocs fonctionnels en ligne. Lorsque le bouton est sélectionné, la barre en ligne indique l'état des modifications de l'automate. Si des modifications sont apportées par un autre utilisateur, cette zone affiche une description textuelle des modifications.

### État de sécurité












Lorsque vous cliquez sur le bouton Safety Status (État de la sécurité) , la barre en ligne indique la signature de sécurité.

**Figure 46 - 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. En présence d'une signature de sécurité, l'icône comporte une petite coche. 

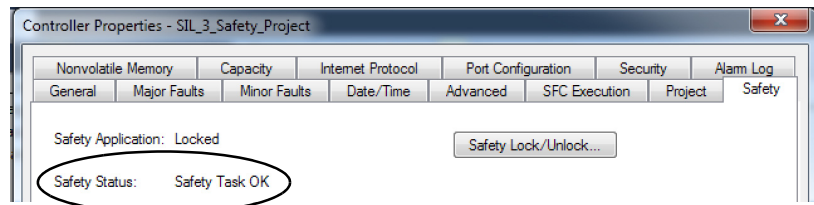
**Tableau 33 - Icône d'état de la sécurité**

Si l'état de la sécurité est	Cette icône apparaît	
	Application SIL 2/PLD, à la fois en ligne et hors ligne	Application SIL 3/PLE
Sécurité déverrouillée		 La sécurité de l'automate n'est pas verrouillée et en ligne.  La sécurité de l'automate n'est pas verrouillée et hors ligne.
Sécurité verrouillée		 La sécurité de l'automate est verrouillée et en ligne.  La sécurité de l'automate est verrouillée et hors ligne.
Défaut de sécurité		
Tâche de sécurité inexploitable.	 La sécurité de l'automate n'est pas verrouillée et la tâche de sécurité est inexploitable.  La sécurité de l'automate est verrouillée et la tâche de sécurité est inexploitable.  Il y a un défaut de sécurité et la tâche de sécurité est inexploitable.	

## Visualisation de l'état via l'onglet Safety

Vous pouvez afficher l'information d'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 47 - État de la tâche de sécurité**



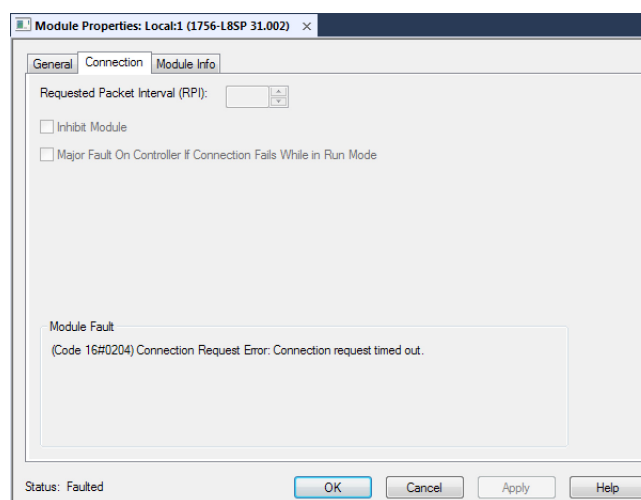
- Le partenaire de sécurité est absent ou indisponible (SIL 3).
- Le matériel du partenaire de sécurité est incompatible avec l'automate principal.
- Le firmware du partenaire de sécurité est incompatible avec l'automate principal.
- Tâche de sécurité inexploitable.
- Tâche de sécurité OK.

A l'exception de la tâche de sécurité OK, les descriptions indiquent qu'il existe des défauts de sécurité irrécupérables.

Reportez-vous à [Défauts de sécurité majeurs \(Type 14\), page 214](#), pour connaître les codes de défaut et les actions correctives.

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

**Figure 48 - État du partenaire de sécurité**





## Surveillance des connexions de sécurité

Pour les points associés à des données de sécurité 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 : `ConnectionFaulted` (Connexion en défaut) et `RunMode` (Mode Exécution).

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, pour une raison quelconque, `ConnectionFaulted` est mis en défaut (1), les données de sécurité sont réinitialisées et la valeur `RunMode` est réglée à l'état inactif (0).

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. Pour les connexions d'E/S de sécurité, l'état `RunMode` est toujours l'inverse de l'état `ConnectionFaulted`. Il ne fournit pas des données uniques.

Le tableau suivant décrit les combinaisons des états `ConnectionFaulted` et `RunMode`.

**Tableau 34 - État de la connexion de sécurité**

État <code>ConnectionFaulted</code>	État <code>RunMode</code>	Fonctionnement de la connexion de sécurité
0 = Valable	1 = Exécution	Les données sont activement commandées par le dispositif producteur. Le producteur est en mode Exécution.
0 = Valable	0 = Inactif	La connexion est active et le producteur est en état d'inactivité. La donnée de sécurité est remise à zéro. Cela concerne uniquement les connexions consommées.
1 = en défaut	0 = Inactif	La connexion de sécurité est en défaut. L'état du dispositif producteur est inconnu. Les données de sécurité sont réinitialisées et la valeur <code>RunMode</code> est réglée à l'état inactif (0).
1 = en défaut	1 = Exécution	État non valable.

Si un dispositif est inhibé, le bit `ConnectionFaulted` est mis en condition Faulted (1) et le bit `RunMode` est mis en condition Idle (0) pour chaque connexion associée au dispositif. En conséquence, les données de sécurité consommées sont remises à zéro.

## Utilisation de l'état

L'état de connexion (.ConnectionFaulted) est l'état de la connexion de sécurité entre l'automate de sécurité et le module d'E/S de sécurité. Lorsque la connexion fonctionne correctement, ce bit est à l'état bas (0). Lorsque la connexion NE fonctionne PAS correctement, ce bit est à l'état haut (1). Lorsque l'état de la connexion est haut (connexion ne fonctionnant pas correctement), tous les autres points définis du module sont bas et doivent être considérés comme des données « non valides ».

L'état du point est disponible à la fois pour les entrées de sécurité (.PtxxInputStatus) et les sorties de sécurité (.PtxxOutputStatus). Lorsque le point d'état du point est haut (1), il indique que la voie individuelle fonctionne et est correctement câblée, et que la connexion de sécurité entre l'automate de sécurité et le module d'E/S de sécurité sur lequel réside la voie fonctionne correctement.

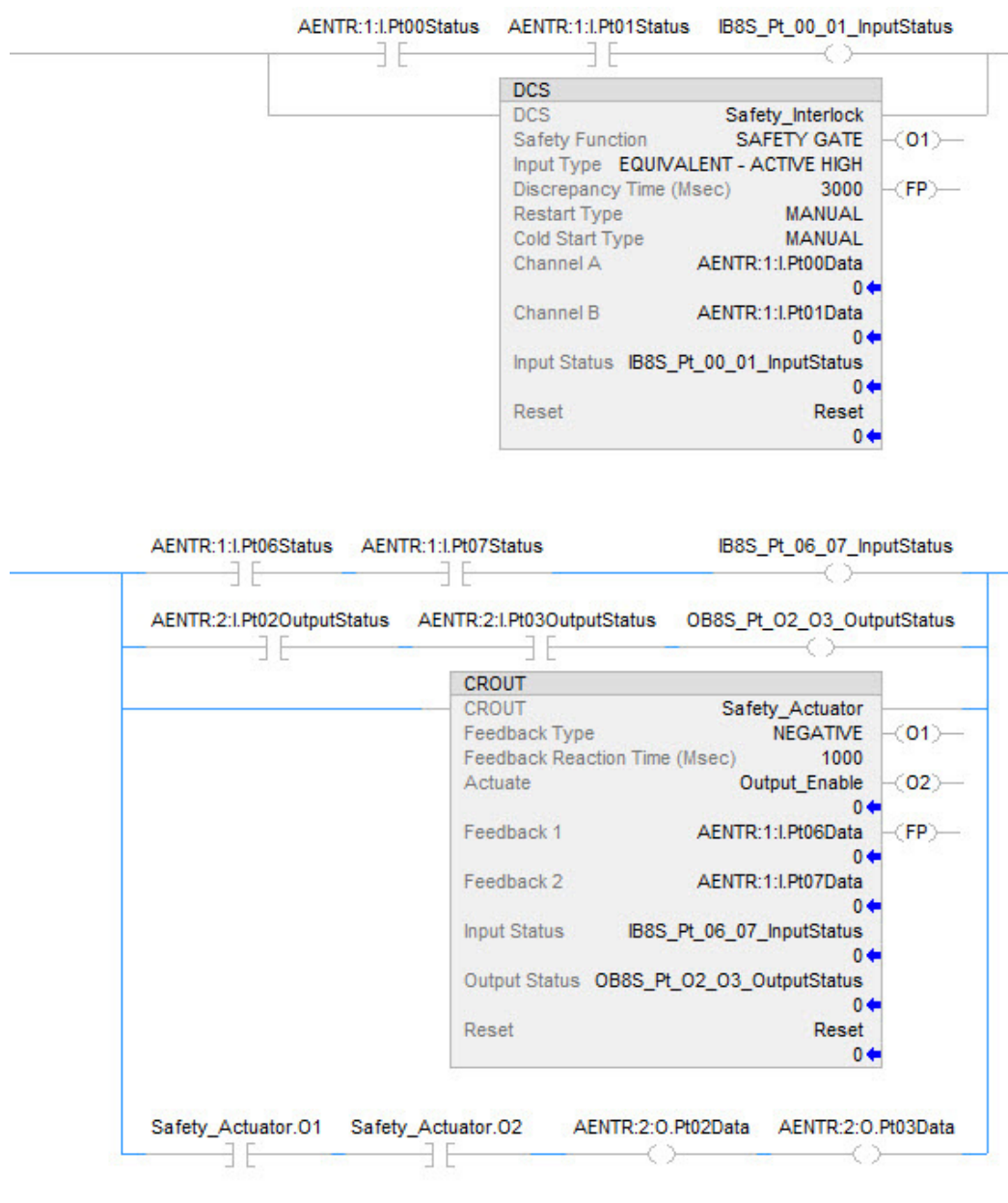
L'état combiné est aussi disponible à la fois pour les entrées de sécurité (.CombinedInputStatus) et les sorties de sécurité (.CombinedOutputStatus). Lorsque le point de l'état combiné est haut (1), il indique que toutes les voies d'entrée ou de sortie du module fonctionnent et sont correctement câblées, et que la connexion de sécurité entre l'automate de sécurité et le module d'E/S de sécurité sur lequel résident les voies fonctionne correctement.

L'utilisation de l'état combiné ou de l'état du point dépend de l'application. L'état du point fournit simplement des informations plus granulaires.

Les instructions de sécurité à double voie intègrent une surveillance de l'état des E/S de sécurité. L'état d'entrée et l'état de sortie sont des paramètres pour les instructions d'entrée et de sortie de sécurité. L'instruction DCS (et autres instructions de sécurité à double voie) possède un état d'entrée pour les voies d'entrée A et B. L'instruction CROUT possède un état d'entrée pour les retours 1 et 2, et un état de sortie pour les voies de sortie qui sont pilotées par les sorties CROUT O1 et O2. Les indicateurs d'état utilisés dans ces instructions doivent être hauts (1) pour le ou les points de sortie des instructions de sécurité (O1 pour les instructions d'entrée et O1/O2 pour CROUT) à activer.

Pour le bon fonctionnement des instructions de sécurité, il est important de piloter les points d'état d'entrée et d'état de sortie AVANT/AU-DESSUS DE l'instruction de sécurité, comme indiqué [figure 49](#).

**Figure 49 - Exemples d'instruction**



L'état des E/S de sécurité doit être interrogé lors d'utilisation d'instructions telles que XIC et OTE. C'est l'utilisateur qui en assume la responsabilité. L'utilisateur doit vérifier que l'état de la voie d'entrée de sécurité est haut (1) avant d'utiliser une voie d'entrée de sécurité comme verrouillage. L'utilisateur doit vérifier que l'état de la voie de sortie de sécurité est haut (1) avant d'alimenter une voie de sortie de sécurité.

## Défauts de sécurité

Les défauts majeurs dans le système GuardLogix peuvent être :

- Des défauts d'automate récupérables
- Des défauts d'automate irrécupérables
- Des défauts de sécurité irrécupérables dans l'application de sécurité
- Des défauts de sécurité récupérables dans l'application de sécurité

### Défauts d'automate irrécupérables

Ces défauts se produisent en cas d'échec des diagnostics internes de l'automate. Si un défaut d'automate irrécupérable se produit, l'exécution des tâches standard et de sécurité s'arrête et les connexions sortantes s'arrêtent. Les dispositifs d'E/S de sécurité réagissent à la perte des données de sortie en passant à l'état sûr. La récupération nécessite que vous rechargiez le programme d'application.

Si un défaut se produit, les données de diagnostic sont automatiquement écrites sur la carte SD. Rockwell Automation peut alors utiliser les données pour faciliter le diagnostic de la défaillance. Contactez l'assistance technique.

### Défauts de sécurité irrécupérables dans l'application de sécurité

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

Lorsque la tâche de sécurité rencontre un défaut de sécurité irrécupérable, un défaut majeur récupérable standard est également enregistré et l'automate procède à l'exécution du gestionnaire de défaut de l'automate s'il en existe un. Si le gestionnaire de défaut de l'automate gère ce défaut, les tâches standard continuent de s'exécuter, même si la tâche de sécurité reste en défaut.



**ATTENTION** : la neutralisation d'un défaut de sécurité n'efface pas le défaut. Si vous neutralisez le défaut de sécurité, il est de votre responsabilité de prouver que le fonctionnement de votre système reste sûr.

Il vous appartient de démontrer à votre organisme de certification que votre système peut continuer à fonctionner en toute sécurité après avoir ignoré un défaut de sécurité.

---

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

- Si vous utilisez le bouton Clear Majors (Effacer défauts majeurs) ou l'option de menu Clear Faults (Effacer défaut) dans Logix Designer pour effacer le défaut, l'application standard doit continuer à s'exécuter pendant que l'application de sécurité est récupérée depuis l'image instantanée.
- Si vous utilisez la méthode du sélecteur à clé (tournez le sélecteur à clé sur Programme, puis de nouveau sur Exécution), l'application de sécurité est récupérée à partir de l'instantané, mais l'application standard sort brièvement du mode Exécution.

### Défauts récupérables dans l'application de sécurité

Si un défaut récupérable se produit dans l'application de sécurité, le système peut interrompre l'exécution de la tâche de sécurité, selon que le défaut est traité ou non par les sous-programmes de gestion des défauts dans l'application de sécurité.

Lorsqu'un défaut récupérable est acquitté par programmation, la tâche de sécurité se poursuit sans interruption.

Quand un défaut récupérable dans l'application de sécurité n'est pas effacé par programmation, 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.

Si le défaut de sécurité récupérable n'est pas traité, un défaut majeur récupérable standard est également enregistrée et l'automate procède à l'exécution du gestionnaire de défaut de l'automate, s'il en existe un. Si le gestionnaire de défaut de l'automate gère ce défaut, les tâches standard continuent de s'exécuter, même si la tâche de sécurité reste en défaut.

L'apparition de défauts récupérables indique que le code de l'application ne se protège pas des valeurs ou des conditions de données non valides. Pour éliminer ces défauts, envisagez de modifier l'application plutôt que de les gérer à l'exécution.



**ATTENTION** : la neutralisation d'un défaut de sécurité n'efface pas le défaut. Si vous neutralisez le défaut de sécurité, il est de votre responsabilité de prouver que le fonctionnement de votre système reste sûr.

Il vous appartient de démontrer à votre organisme de certification que votre système peut continuer à fonctionner en toute sécurité après avoir ignoré un défaut de sécurité.

## Affichage des défauts

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

L'affichage de l'état de l'automate montre également des codes de défaut avec un bref message d'état, comme indiqué à partir de la page [216](#).

## Codes de défaut

Le [tableau 35](#) montre les codes de défaut spécifiques aux GuardLogixautomates. 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 ou le partenaire de sécurité a été retiré.	Nonrecoverable (irrépérable)	Effacez le défaut. Si une signature de sécurité est présente, la mémoire de sécurité est réinitialisée et la tâche de sécurité recommence son exécution. En l'absence de signature de sécurité, vous devrez recharger le programme pour permettre à nouveau l'exécution de la tâche de sécurité. Réinsérez le partenaire de sécurité (s'il a été démonté).
02	Une erreur est présente dans un sous-programme de la tâche de sécurité.	Recoverable (Répérable)	Rectifiez l'erreur dans la logique du programme utilisateur.
03	Le partenaire de sécurité est manquant.	Nonrecoverable (irrépérable)	Installez un partenaire de sécurité compatible.
04	Le partenaire de sécurité est indisponible.	Nonrecoverable (irrépérable)	Installez un partenaire de sécurité compatible.
05	Matériel du partenaire de sécurité incompatible.	Nonrecoverable (irrépérable)	Installez un partenaire de sécurité compatible.
06	Firmware du partenaire de sécurité incompatible.	Nonrecoverable (irrépérable)	Mettez à jour le partenaire de sécurité de sorte que les révisions majeure et mineure de son firmware correspondent à celles de l'automate principal.
07	La tâche de sécurité est inexploitable. Ce défaut se produit lorsque le programme de sécurité est incorrect. Par exemple, lorsqu'une incompatibilité existe entre le programme de l'automate principal et celui du partenaire de sécurité, un timeout du chien de garde s'est produit ou lorsque la mémoire est corrompue.	Nonrecoverable (irrépérable)	Effacez le défaut. Si une signature de sécurité existe, celle-ci réinitialise la mémoire de sécurité et la tâche de sécurité recommence son exécution. S'il n'y a pas de signature de sécurité, vous devez recharger le programme pour permettre l'exécution de la tâche de sécurité.
09	Défaut irrépérable de l'automate au niveau du partenaire de sécurité.	Nonrecoverable (irrépérable)	Effacez le défaut et rechargez le programme dans l'automate. Si le problème persiste, remplacez le partenaire de sécurité.

La publication [1756-PM014](#), « Logix 5000 Controllers Major and Minor Faults Programming Manual », contient la description des codes de défaut communs aux automates Logix.

## Développement d'un sous-programme de défaut pour les applications de sécurité

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.

Certaines applications refusent que tous les défauts de sécurité provoquent l'arrêt de l'ensemble de votre système. Dans ce cas, utilisez 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** : Il vous appartient de démontrer à votre organisme de certification que votre système peut continuer à fonctionner en toute sécurité après avoir ignoré un défaut de sécurité.

L'apparition de défauts récupérables indique que le code de l'application ne se protège pas des valeurs ou des conditions de données non valides. Pour éliminer ces défauts, envisagez de modifier l'application plutôt que de les gérer à l'exécution.

L'automate prend en charge deux niveaux de gestion des défauts majeurs dans une application de sécurité :

- sous-programme de gestion des défauts de programme
- Gestionnaire de défaut de l'automate

Ces deux sous-programmes peuvent utiliser les instructions GSV et SSV, comme décrit page [216](#).

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 défaut du programme n'efface pas le défaut, ou s'il n'existe pas de sous-programme de défaut de programme, la tâche de sécurité se met en défaut et s'arrête.

Lorsque la tâche de sécurité se met en défaut, un défaut récupérable majeur standard est également consigné, et l'automate passe à l'exécution du gestionnaire de défauts de l'automate, s'il existe. Si le gestionnaire de défaut de l'automate gère ce défaut, les tâches standard continuent de s'exécuter, même si la tâche de sécurité reste en défaut.

Le gestionnaire de défauts de l'automate est un composant facultatif qui s'exécute lorsque le sous-programme de défaut du programme ne peut pas effacer le défaut ou n'existe pas.

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

La publication [1756-PM014](#), « Logix 5000 Controllers Major and Minor Faults Programming Manual », fournit des informations détaillées sur la création et le test d'un sous-programme de défauts.

## Utilisation des instructions GSV/SSV dans une application de sécurité

Pour les tâches standard, vous pouvez utiliser l'instruction GSV pour obtenir les valeurs des attributs disponibles. Lorsque vous utilisez l'instruction SSV, le logiciel affiche uniquement les attributs que vous pouvez 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 dispositif d'E/S de sécurité.



**ATTENTION :** Utilisez l'instruction SSV avec précaution. La modification des objets peut entraîner un fonctionnement imprévu de l'automate, voire des blessures corporelles.

### Accès aux attributs FaultRecord

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

**Tableau 36 - 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)

### 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.

Pour de plus amples informations sur l'utilisation des instructions GSV et SSV dans les applications de sécurité, reportez-vous au chapitre Input/Output Instructions de la publication [1756-RM003](#), « Manuel de référence des Automates Logix 5000 – Instructions Manuel de référence ».



## Développement d'applications sécurisées

Rubrique	Page
Fonctionnalité de sécurité d'automate	218
Configuration du logement sécurisé	224
Configuration des défauts majeurs définissables par l'utilisateur	225
Protection de la source et de l'exécution basée sur licence	227
Configurer Modifier la détection	230
Journal d'audit de l'automate	231
Désactivation du port Ethernet	232
Désactivation des ports CIP Security	236
Désactivation du port USB	239
Désactivation de la carte SD	241
Désactivation de l'afficheur d'état à 4 caractères	243
Désactivation des pages Internet de l'automate	247

### Concerne ces automates :

ControlLogix 5580

Ces automates ControlLogix® 5580 prennent en charge les exigences de sécurité de CEI-62443-4-2 SL 1 :

- automates standard ControlLogix 5580, révision de firmware 32 ou ultérieure ;
- automates ControlLogix 5580 NSE, XT et de process, révision de firmware 33 ou ultérieure.

Ces automates **ne prennent pas** en charge les exigences de sécurité de CEI-62443-4-2 SL 1 :

- automates ControlLogix 5580 compatibles redondance ;
- automates de sécurité GuardLogix 5580®.

Pour satisfaire à ces exigences, vous devez utiliser cette publication et la publication [SECURE-UM001](#), « Security Configuration User Manual ». Le manuel utilisateur de configuration de la sécurité décrit comment configurer et utiliser les produits Rockwell Automation pour améliorer la sécurité de votre système d'automatisation industrielle.

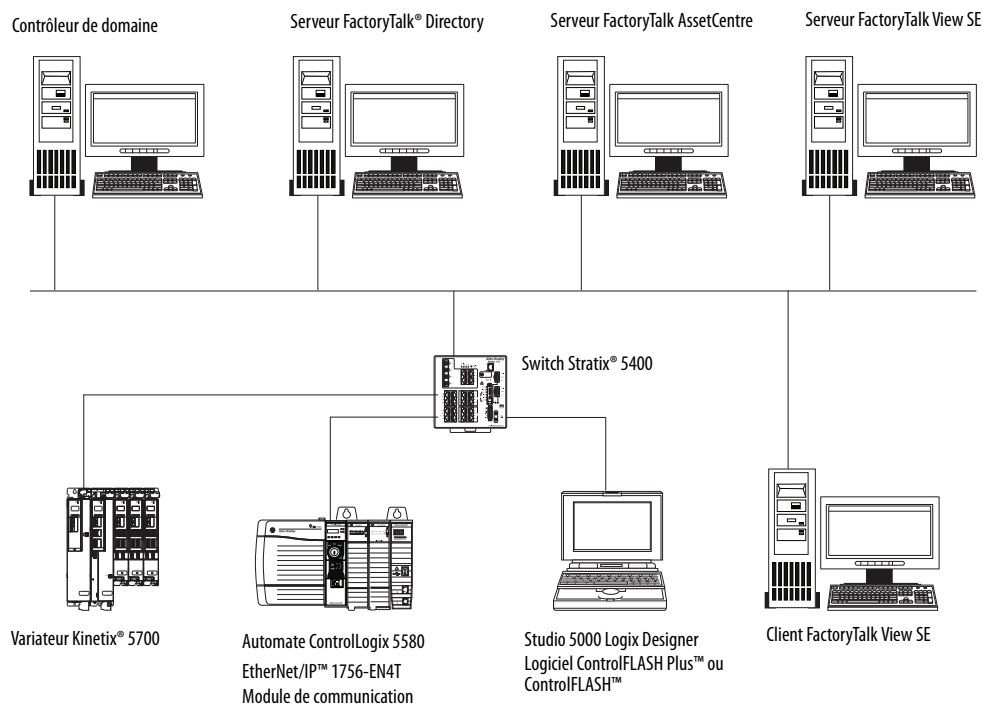
L'automate accepte toutes les valeurs appropriées pour un type de données de point, et il incombe au programme utilisateur de spécifier des plages valides et d'effectuer un contrôle de validité pour ces plages. L'automate vérifie la syntaxe, la longueur et le format de tous les messages entrant.

Vous pouvez appliquer ces mêmes mesures à d'autres automates ControlLogix et GuardLogix, mais sans la certification.

Documentation	Description
« Security Design Guide Reference Manual », publication <a href="#">SECURE-RM001</a>	Fournit des conseils sur la façon d'effectuer des évaluations de sécurité, de mettre en œuvre les produits Rockwell Automation dans un système sécurisé, de durcir le système de commande, de gérer l'accès des utilisateurs et de mettre au rebut l'équipement.
« Sécurité des automates Logix5000 Manuel de programmation », publication <a href="#">1756-PM016</a>	Décrit comment configurer la sécurité pour l'application Studio 5000 Logix Designer® et explique comment configurer la protection des sources pour votre programme et vos projets.
« CIP Security Application Technique », publication <a href="#">SECURE-AT001</a>	Décrit comment planifier et mettre en œuvre un système Rockwell Automation qui prend en charge le protocole CIP Security™.
« Converged Plantwide Ethernet (CPwE) Design and Implementation Guide », publication <a href="#">ENET-TD001</a>	Définit des architectures de référence axées sur la fabrication pour aider à accélérer le déploiement réussi des technologies de mise en réseau standard et la convergence des réseaux de fabrication et d'entreprise/de commercialisation.

## Fonctionnalité de sécurité d'automate

Pour que l'automate ControlLogix soit conforme aux exigences de certification, implémentez le système de commande avec ces autres produits axés sur la sécurité.



## Fonctionnalités de sécurité au niveau système

Rockwell Automation propose plusieurs produits dotés de fonctionnalités qui augmentent la sécurité au niveau système. Utilisez la liste de contrôle suivante pour sécuriser votre système d'automate.

Pour durcir le système de commande :

✓	Produit	Requis pour répondre à CEI-62443-4-2 SL 1	Détails
	logiciel ControlFLASH Plus™ ou ControlFLASH™ ;	Oui	Utilisation du logiciel ControlFLASH Plus ou ControlFLASH pour mettre à jour le firmware de l'automate Les fichiers de firmware signés numériquement ont une extension .DMK (Device Management Kit). Le logiciel ControlFLASH authentifie l'origine d'un fichier DMK et valide le fichier avant de le télécharger dans le dispositif.
	Application Studio 5000 Logix Designer :	Oui	Vous pouvez générer une signature sur une instruction complémentaire. Cette signature scelle (crypte) l'instruction complémentaire pour empêcher toute modification.
	logiciel FactoryTalk AssetCentre	Oui	Le serveur FactoryTalk AssetCentre facilite la sauvegarde et la restauration. Les sauvegardes n'interfèrent pas avec le fonctionnement de l'automate. Configurez l'opération de sauvegarde appropriée en fonction de la conception de votre système, du modèle de menace et de l'évaluation des risques. Pour plus d'informations, consultez la publication <a href="#">SECURE-UM001</a> , « Configure System Security Features User Manual »,

Pour surveiller le système de commande :

✓	Produit	Requis pour répondre à CEI-62443-4-2 SL 1	Détails
	logiciel FactoryTalk AssetCentre	Oui	Le serveur FactoryTalk AssetCentre suit et gère de manière centralisée les modifications de configuration et restreint les personnes autorisées à apporter des modifications. Cette fonctionnalité de serveur facilite les diagnostics et le dépannage et réduit le temps de maintenance des actifs de production. Configuration de la surveillance de dispositif – Modifier le fonctionnement de détection de l'automate Pour plus d'informations, consultez la publication <a href="#">SECURE-UM001</a> , « Configure System Security Features User Manual »,

Pour gérer l'accès utilisateur par programme :

✓	Produit	Requis pour répondre à CEI-62443-4-2 SL 1	Détails
	Application Studio 5000 Logix Designer :	Oui	<p>Configurer le projet de l'automate dans Logix Designer pour utiliser ces méthodes d'accès utilisateur.</p> <ul style="list-style-type: none"> <li>• La protection des sources basée sur licence limite l'accès aux projets aux seuls utilisateurs disposant de la licence requise. Les utilisateurs ne disposant pas de la licence requise ne peuvent pas ouvrir le projet ou importer des composants protégés par la licence.</li> <li>• La protection de fonctionnement basée sur la licence permet le fonctionnement du composant uniquement sur une gamme d'automates spécifique, ou uniquement sur les automates d'une gamme spécifique qui contiennent la licence d'exécution.</li> <li>• La protection par mot de passe utilise une clé source (mot de passe) pour aider à protéger le programme source. Toutes les clés sources sont stockées dans le fichier sk.dat.</li> <li>• L'application Logix Designer possède deux attributs de point qui contrôlent l'accès aux données de point. L'attribut External Access (accès externe) gère la façon dont les applications externes peuvent accéder aux points. L'attribut Constant détermine si un point peut être modifié par le programme logique de l'automate.</li> </ul> <p>Pour plus d'informations, consultez la publication <a href="#">1756-PM016</a>, « Sécurité des automates Logix5000 Manuel de programmation »,</p>
	Logiciel FactoryTalk Security Application Studio 5000 Logix Designer :	Oui	<p>Configurez FactoryTalk Security pour définir les stratégies, les groupes d'utilisateur et autres ensembles d'autorisation.</p> <ul style="list-style-type: none"> <li>• L'application Logix Designer applique la stratégie en fonction des stratégies d'accès qui lui sont fournies par FT Security pour l'utilisateur authentifié par le logiciel. Une fois authentifiée, l'application Logix Designer agit comme votre interface avec l'automate. Cela s'applique à toutes les communications CIP™ protégées vers l'automate, qu'elles proviennent d'Ethernet, du bus intermodules ou de l'USB.</li> <li>• La plate-forme FactoryTalk Services offre un contrôle d'accès aux fonctionnalités pour gérer l'accès des utilisateurs aux fonctionnalités du produit telles que le téléchargement de l'automate, l'importation de projets, la création de projets et la mise à jour du firmware.</li> <li>• Dans FactoryTalk Security, définissez quels utilisateurs peuvent modifier les modes de l'automate et télécharger des projets dans l'automate.</li> <li>• L'obligation d'autorité de sécurité restreint l'automate à une instance spécifique de FactoryTalk Security. Cette obligation réduit la surface d'attaque pour l'usurpation de serveur de sécurité car le logiciel client et le logiciel de sécurité déterminent l'identité de l'autorité de sécurité chargée de contrôler l'accès.</li> </ul> <p>Pour plus d'informations, consultez la publication <a href="#">SECURE-UM001</a>, « Configure System Security Features User Manual ».</p>
	Logiciel FactoryTalk Policy Manager	Oui	<p>Utilisez le logiciel FactoryTalk Policy Manager pour définir un transport de données sécurisé sur un réseau EtherNet/IP vers l'automate.</p> <p>Pour plus d'informations, consultez la publication <a href="#">SECURE-UM001</a>, « Configure System Security Features User Manual ».</p>

## Fonctionnalités de sécurité spécifiques à l'automate

L'automate prend en charge ces fonctionnalités spécifiques au produit que vous utilisez avec les fonctionnalités au niveau système. Utilisez la liste de contrôle suivante pour sécuriser physiquement votre automate.

Pour durcir l'automate :

✓	Fonctionnalité de l'automate	Requis pour répondre à CEI-62443-4-2 SL 1	Détails
	Mise à jour de firmware	Oui	<p>Pour répondre aux exigences de sécurité de CEI-62443-4-2 SL 1, vous devez utiliser la dernière révision disponible du firmware de l'automate.</p> <p>L'automate est conçu afin que :</p> <ul style="list-style-type: none"> <li>vous ne puissiez pas mettre à jour le firmware si le sélecteur est sur la position RUN (Exécution) ;</li> <li>vous ne puissiez pas passer en ligne avec l'automate pendant le processus de mise à jour du firmware.</li> </ul> <p>Pour plus d'informations, reportez-vous à la page <a href="#">55</a>.</p>
	Cryptage de la carte SD	Peut être requis en fonction de la conception du système, du modèle de menace et de l'évaluation des risques.	<p>Si votre système autorise l'utilisation de la carte SD, le processus de chargement sur la carte SD crypte et signe numériquement le projet à l'aide de la clé de l'automate. La carte SD n'est pas cryptée elle-même.</p> <p>Lorsque vous enregistrez (chargez) le firmware sur la carte SD, le processus stocke le firmware et les certificats cryptés sur la carte SD.</p> <p>N'utilisez pas un Message to Self (MSG avec un Path of THIS) pour écrire automatiquement les journaux de l'automate ou pour forcer manuellement l'écriture journaux de l'automate sur la carte SD. Cela peut aider à prévenir la perte potentielle des journaux de l'automate avant que FactoryTalk AssetCentre ne puisse les lire.</p> <p>Pour plus d'informations, consultez la page <a href="#">91</a>.</p>
	Logement sécurisé	Pour contrôler la segmentation du réseau, configurez un logement sécurisé (Trusted slot).	<p>La fonctionnalité de logement sécurisé restreint les chemins de communication par lesquels certaines opérations sont effectuées sur les automates Logix 5000™. Un logement sécurisé n'est pas configuré par défaut.</p> <p>Pour plus d'informations, consultez la page <a href="#">224</a>.</p>
	Défauts majeurs définis par l'utilisateur	Peuvent être requis en fonction de la conception du système, du modèle de menace et de l'évaluation des risques.	<p>Si votre application nécessite un défaut majeur, en plus de ceux déjà surveillés par l'automate, définissez un état prédéterminé avec un défaut majeur afin que les sorties soient désactivées.</p> <p>Pour plus d'informations, consultez la page <a href="#">232</a>.</p>

Pour surveiller l'automate :

✓	Fonctionnalité de l'automate	Requis pour répondre à CEI-62443-4-2 SL 1	Détails
	Protection et exécution de la source basée sur la licence	Peut être requis en fonction de la conception du système, du modèle de menace et de l'évaluation des risques.	<p>Configurez les licences pour gérer l'accès au programme source de l'automate et l'exécution de ce programme. Ces licences ne sont pas activées par défaut.</p> <ul style="list-style-type: none"> <li>• La protection des sources basée sur les licences limite l'accès aux projets aux seuls utilisateurs disposant de la licence requise. Les utilisateurs sans la licence requise ne peuvent pas ouvrir le projet ou importer des composants protégés par la licence.</li> <li>• La protection de l'exécution basée sur la licence permet l'exécution du composant uniquement sur une gamme d'automates spécifique, ou uniquement sur les automates d'une gamme d'automates spécifique qui contiennent la licence d'exécution.</li> <li>• La protection par mot de passe utilise une clé source (mot de passe) pour aider à protéger le programme source. Toutes les clés sources sont stockées dans le fichier sk.dat.</li> <li>• L'application Logix Designer possède deux attributs de point qui contrôlent l'accès aux données de point. L'attribut External Access (accès externe) gère la façon dont les applications externes peuvent accéder aux points. La valeur de l'attribut Constant détermine si un point peut être modifié par le programme logique de l'automate.</li> </ul> <p>Pour plus d'informations, consultez la page <a href="#">227</a>.</p>
	Détection des modifications	Oui	<p>Active la fonctionnalité de détection des modifications pour surveiller les composants du programme afin de déterminer s'ils changent. La fonctionnalité de détection des modifications n'est pas activée par défaut.</p> <p>Pour plus d'informations, consultez la page <a href="#">230</a>.</p>
	Journal d'audit de l'automate	Oui	<p>Le journal d'audit de l'automate stocke automatiquement les événements liés à la sécurité auxquels il est possible d'accéder en écriture via le logiciel FactoryTalk AssetCentre.</p> <p>Pour plus d'informations, consultez la page <a href="#">231</a>.</p>

Pour gérer l'accès physique à l'automate par l'utilisateur :

✓	Fonctionnalités de l'automate	Requis pour répondre à CEI-62443-4-2 SL 1	Détails
	Position du commutateur à clé	Peut être requis en fonction de la conception du système, du modèle de menace et de l'évaluation des risques.	Placez le sélecteur à clé en position RUN pour empêcher les modifications de configuration à distance non autorisées de l'automate et restreindre certains services de communication. Retirez la clé du sélecteur d'un automate en fonctionnement pour éviter toute modification de la configuration ou du programme. <b>IMPORTANT</b> : n'appliquez pas de nouvelle stratégie de sécurité lorsque l'automate est en mode RUN. Le mode RUN n'aide pas à empêcher les mises à jour de la stratégie de sécurité, et un changement de stratégie a le potentiel de perturber un système de commande en cours d'exécution.
	Désactivation du port Ethernet	Peut être requis en fonction de la conception du système, du modèle de menace et de l'évaluation des risques.	Le port Ethernet est activé par défaut. Désactivez le port Ethernet si la conception du système, le modèle de menace ou l'évaluation des risques l'exigent. Pour plus d'informations, consultez la page <a href="#">232</a> .
	Désactivation du Simple Network Management Protocol (SNMP)	Peut être requis en fonction de la conception du système, du modèle de menace et de l'évaluation des risques.	SNMP est désactivé par défaut. Si SNMP a été activé, désactivez-le si la conception du système, le modèle de menace ou l'évaluation des risques l'exigent. Pour plus d'informations, consultez la page <a href="#">119</a> .
	Désactivation des ports CIP Security	Peut être requis en fonction de la conception du système, du modèle de menace et de l'évaluation des risques.	Les ports CIP Security sur l'automate sont activés par défaut. Désactivez les ports CIP Security si la conception du système, le modèle de menace ou l'évaluation des risques l'exigent. Pour plus d'informations, consultez la page <a href="#">236</a> .
	Désactivation des ports USB	Peut être requis en fonction de la conception du système, du modèle de menace et de l'évaluation des risques.	Le port USB de l'automate est activé par défaut. Désactivez le port USB si requis par la conception du système, le modèle de menace et l'évaluation des risques. Pour plus d'informations, consultez la page <a href="#">239</a> .
	Désactivation de la carte SD	Peut être requis en fonction de la conception du système, du modèle de menace et de l'évaluation des risques.	La carte SD est activée par défaut. Désactivez la carte SD si requis par la conception du système, le modèle de menace et l'évaluation des risques. Pour plus d'informations, consultez la page <a href="#">241</a> .
	Désactivation des pages Internet de l'automate	Peut être requis en fonction de la conception du système, du modèle de menace et de l'évaluation des risques.	Les pages Internet de diagnostics de l'automate sont en lecture seule. Avec l'application Studio 5000 Logix Designer, version 33.00.00 ou ultérieure, les pages Internet de l'automate sont désactivées par défaut. Si les pages Internet de l'automate sont actuellement activées, alors désactivez-les si nécessaire en fonction de la conception du système, du modèle de menace et de l'évaluation des risques. Pour plus d'informations, consultez la page <a href="#">247</a> .

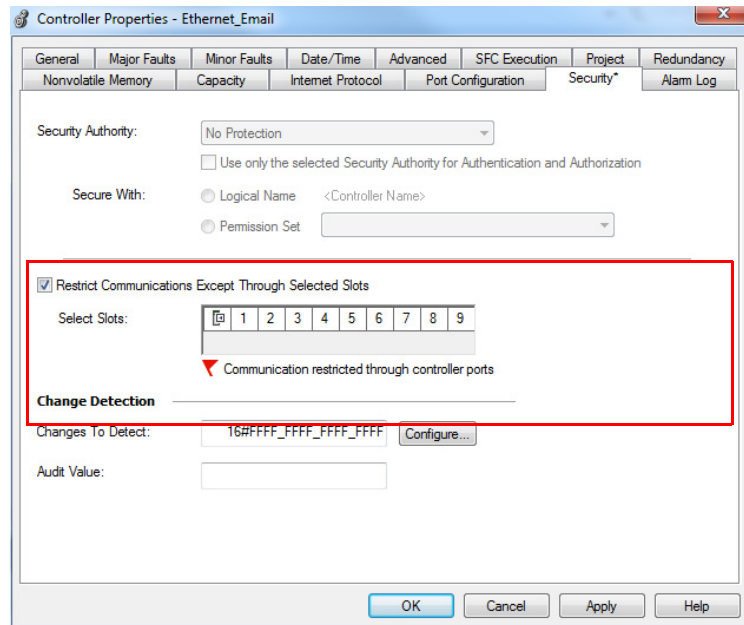
## Vérification de la mise en œuvre de la sécurité

Suivez les listes de contrôle ci-dessus pour sécuriser le système et l'automate. Il est de votre responsabilité de surveiller périodiquement le système pour vous assurer que les réglages de sécurité fonctionnent comme vous les avez configurés. Par exemple :

- Essai de connexion avec un nom d'utilisateur ou un mot de passe invalide.
- Essai d'accéder à un port USB désactivé.

## Configuration du logement sécurisé

Pour maintenir la segmentation du réseau, configurez le logement sécurisé. Dans l'onglet Sécurité des propriétés de l'automate, la fonctionnalité de logement sécurisé restreint les chemins de communication par lesquels certaines opérations sont effectuées sur les automates Logix.



### *Communication restreinte sauf via les logements sélectionnés*

Cochez cette case pour restreindre la communication à travers tout logement de châssis qui n'est pas sécurisé. Décochez la case pour permettre à l'automate de communiquer sans restrictions de communication.

---

**IMPORTANT** Lorsque cette case est cochée, la communication est limitée via les ports USB ou série et les mises à jour du firmware sont limitées aux logements sécurisés lors de l'utilisation d'AutoFlash ou des logiciels ControlFLASH Plus et ControlFLASH. La prise en charge est limitée pour les outils qui nécessitent un accès à des données restreintes via des connexions de classe 3.

---

### *Logements sélectionnés*

Seuls les logements sélectionnés sous Select Slots (Choix des logements) sont des chemins de communication sécurisés pour l'automate. La grille Select Slots configure les logements sécurisés pour l'automate. Lorsque vous cochez la case Restreindre les communications à l'exception des logements sélectionnés, vous devez cliquer sur au moins un logement qui n'est pas occupé par l'automate.

Si la taille du châssis du projet est connue, le nombre de logements égal à la taille du châssis s'affiche dans la boîte de dialogue. Sinon, 17 logements (0 à 16) sont affichés dans la boîte de dialogue.



## Configuration des défauts majeurs définissables par l'utilisateur

Pour interrompre (arrêter) l'automate en fonction des conditions de l'application, créez un défaut majeur défini par l'utilisateur. Avec un défaut majeur défini par l'utilisateur :

- le type de défaut = 4.
- Définissez une valeur pour le code de défaut. Choisissez une valeur comprise entre 990 et 999. Ces codes sont réservés pour les défauts définis par l'utilisateur.
- L'automate traite le défaut comme les autres défauts majeurs.
- L'automate passe en mode programmation et cesse de faire fonctionner le programme logique. Les sorties passent à leur état configuré ou à la valeur de mode défaut.

Pour créer un défaut majeur défini par l'utilisateur, procédez ainsi :

1. créez un sous-programme de défaut pour le programme ;
2. configurez le programme pour qu'il utilise le sous-programme de défaut ;
3. sautez dans le sous-programme de défaut.

### Création d'un sous-programme de défaut

Pour créer un sous-programme de défaut, procédez ainsi ;

1. dans l'organisateur de l'automate, faites un clic droit sur le programme et cliquez sur Add > New Routine (Ajout > Nouveau sous-programme)
2. Dans la boîte de dialogue New Routine, dans le champ Name, tapez un nom pour le sous-programme de défaut.
3. Dans le champ Type, utilisez le réglage par défaut, Ladder Diagram (Diagramme à relais).
4. Dans le champ In Program ou Phase, choisissez le programme ou la phase où le sous-programme résidera.
5. Dans le champ Assignment (Attribution), sélectionnez Fault (Défaut).
6. (facultatif) cochez la case Open Routine (Ouvrir le sous-programme), pour ouvrir immédiatement le programme en logique à relais.
7. Cliquez sur OK.

## Configuration du programme pour utiliser le sous-programme de défaut

Pour configurer le programme afin qu'il utilise le sous-programme de défaut, procédez comme suit :

1. Dans l'organisateur de l'automate, cliquez avec le bouton droit sur le programme puis cliquez sur Propriétés (Propriétés).
2. Dans la boîte de dialogue Propriétés (Propriétés), cliquez sur l'onglet Configuration.
3. Dans le champ Fault, choisissez Fault Routine.
4. Cliquez sur OK.

## Saut au sous-programme de défaut

Dans le sous-programme principal du programme, entrez la ligne suivante, dans laquelle :

- Fault\_Routine\_1 est le nom du sous-programme de défaut du programme ;
- 999 est la valeur du code de défaut ;



Lorsque Tag\_1.0 = 1, l'exécution saute au nom\_du\_sous-programme\_de\_défaut, un défaut majeur se produit et l'automate passe en mode défaut. Les sorties passent à leur état en défaut. La boîte de dialogue Controller Properties, onglet Major Faults, affiche le code 999.

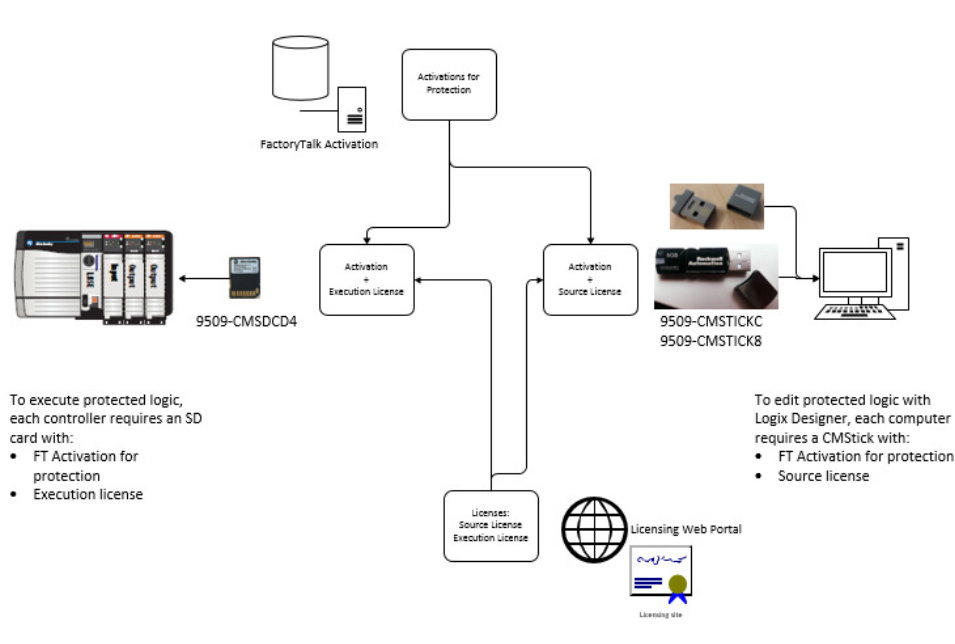


## Protection de la source et de l'exécution basée sur licence

La protection de la source aide à empêcher la modification des composants logiques en fonction d'une licence.

La protection d'exécution ajoute une protection supplémentaire à la logique du programme de l'automate. La protection d'exécution garantit que le bon automate a accès pour exécuter le programme protégé. Utilisez ceci avec la protection de la source pour vous assurer que le bon programmeur a accès pour modifier la logique du programme.

Chaque dispositif (automate ou ordinateur) nécessite une activation pour accéder aux fonctionnalités de protection. Chaque composant ou programme logique nécessite une licence pour être accessible ou exécuté.

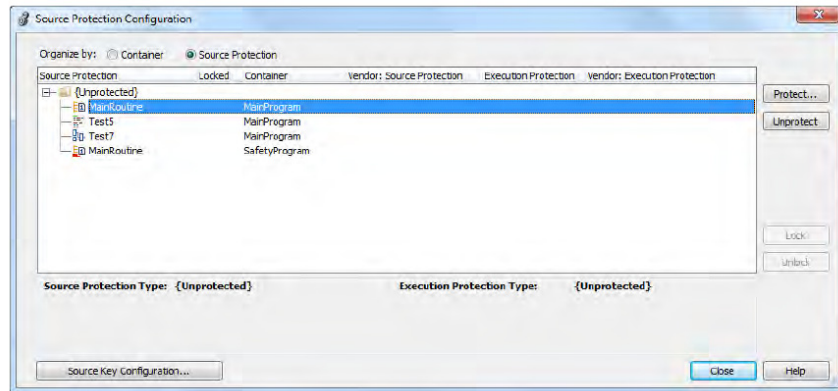


Pour appliquer une protection basée sur une licence, vous avez besoin de l'élément suivant :

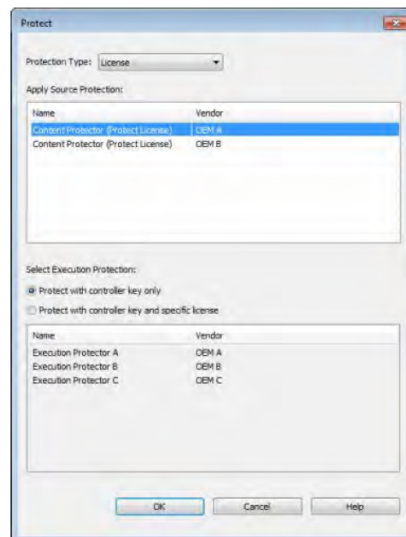
- un CmStick qui contient une licence avec l'autorisation d'utilisation doit être présent localement sur n'importe quel port USB de l'ordinateur. L'autorisation d'utilisation ne peut pas être obtenue à partir d'un serveur de licence réseau. Tous les autres privilèges de licence peuvent être contenus sur le CmStick local ou fournis par un serveur de licences sur le réseau.
- Une licence qui contient l'autorisation de protection, soit sur un CmStick local, soit fournie par un serveur de licences sur le réseau. Lorsque les composants sont verrouillés, les utilisateurs non autorisés ne peuvent pas afficher ou modifier le composant, mais les utilisateurs autorisés peuvent exécuter le projet sans CmStick.

## Activation de protection sous licence

1. Cliquez sur Tools > Security > Configure Source Protection pour ouvrir la boîte de dialogue de configuration de la protection de la source.



2. Insérez le CmStick qui contient la licence que vous souhaitez utiliser pour protéger le composant dans le port USB de l'ordinateur. Les licences doivent contenir l'autorisation de protection à utiliser pour protéger les composants. Si une licence ne contient pas l'autorisation de protection, elle n'apparaît pas dans la liste des licences.
3. Dans la boîte de dialogue Configuration de la protection de la source, sélectionnez le composant à protéger puis cliquez sur Protect (Protéger).
4. Dans la boîte de dialogue Protect, sélectionnez la licence à appliquer.



5. Sur les automates ControlLogix 5580 et GuardLogix 5580, sélectionnez le type de protection d'exécution :
  - Protéger avec la clé de l'automate uniquement. Cette option est sélectionnée par défaut. Avec cette option sélectionnée, le composant, lorsqu'il est verrouillé, s'exécute uniquement sur un automate de la même gamme que celui spécifié pour le projet. Par exemple, si vous verrouillez un composant protégé par licence pour un projet sur un automate ControlLogix 5580, le composant ne peut être exécuté que sur un autre automate ControlLogix 5580.
  - Protection avec la clé de l'automate et une licence spécifique. Lorsque vous sélectionnez cette option, le composant s'exécute uniquement sur un automate de la même gamme que celui spécifié pour le projet et qui contient une CmCard avec la licence d'exécution que vous sélectionnez. Si vous sélectionnez Protéger avec une clé d'automate et une licence spécifique, sélectionnez la licence d'exécution dans la liste des licences disponibles.

Sur les automates ControlLogix 5580 et GuardLogix 5580, une fois les composants protégés, ils peuvent également être verrouillés. Lorsque vous verrouillez un composant, cela empêche les utilisateurs d'afficher ou de modifier le composant, mais permet aux utilisateurs autorisés de l'exécuter.

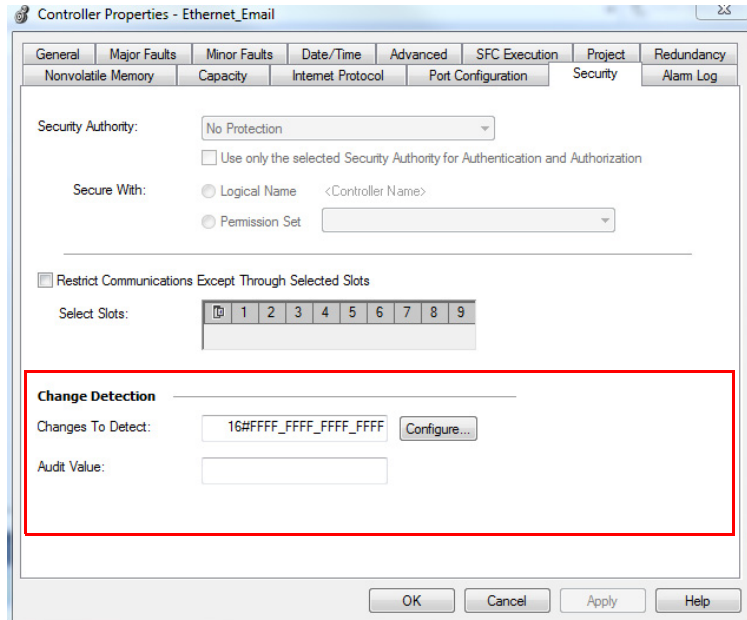
6. Pour revenir à la boîte de dialogue Configuration de la protection de la source, cliquez sur OK.

**CONSEIL** Pour enregistrer les modifications apportées à un composant protégé par une protection de source basée sur une licence, un CmStick contenant la licence requise doit être connecté à l'ordinateur qui exécute l'application Logix Designer.

Assurez-vous d'enregistrer vos modifications dans le projet ou de verrouiller les composants protégés avant de supprimer le CmStick qui contient la licence requise. Si la licence n'est pas présente, vous pourriez perdre vos modifications du projet.

## Configurer Modifier la détection

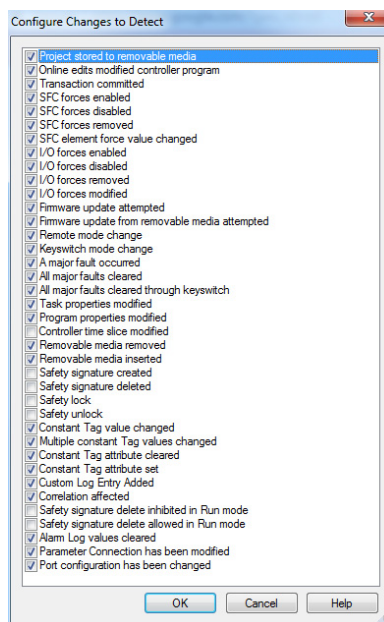
Sous l'onglet Sécurité des propriétés de l'automate, la Fonctionnalité de détection des modifications suit un ensemble de composants du programme et vérifie si ces composants ont changé.



### Modifications de la détection

Identifie les types d'événements qui peuvent provoquer la modification de la boîte Valeur d'audit. Par défaut, tous les types d'événements peuvent entraîner la modification de la valeur d'audit, ce qui donne une valeur par défaut de : 0xFFFFFFFFFFFFFFFF.

Cliquez sur Configurer pour ouvrir la boîte de dialogue Configurer les modifications à détecter. Nous vous recommandons de suivre ces modifications pour un automate ControlLogix 5580 standard :



### *Valeur d'audit*

Valeur de vérification unique générée lorsqu'un projet est téléchargé dans l'automate ou chargé à partir d'un support de stockage amovible. Cette valeur est mise à jour quand un événement se produit. Certains événements entraînent toujours une modification de la valeur d'audit, tandis que d'autres peuvent être sélectionnés dans la boîte de dialogue Configure Changes to Detect (Configurer les modifications à détecter). Lorsque l'automate est hors ligne, la boîte Valeur d'audit est vide.

## **Journal d'audit de l'automate**

Le journal d'audit de l'automate stocke divers événements liés à la sécurité qui peuvent être écrits sur une carte SD ou accessibles via FactoryTalk Asset Center. Certains de ces événements sont des erreurs de demande d'application Logix Designer, des événements de système de contrôle, des événements de sauvegarde/restauration et des changements de configuration.

- Avec l'application Studio 5000 Logix Designer version 32 ou antérieure, le journal contient 100 événements, puis se renouvelle et écrase les données qui s'y trouvent.
- Avec l'application Studio 5000 Logix Designer version 33 ou ultérieure, le journal contient 500 événements, puis se renouvelle et écrase les données qui s'y trouvent.

Pour une journalisation plus robuste et pour aider à empêcher le retournement, utilisez FactoryTalk AssetCentre.

## Désactivation du port Ethernet

Vous pouvez désactiver le port Ethernet de l'automate avec l'application Studio 5000 Logix Designer, version 28.00.00 ou ultérieure.

---

**IMPORTANT** N'oubliez pas les points suivants :

- Une fois qu'un port Ethernet est désactivé, vous perdez toute connexion établie via le port Ethernet de l'automate.
  - Vous ne pouvez pas désactiver les ports Ethernet si l'automate est en mode Exécution ou si les réglages de FactoryTalk Security nient cette option de modification.
- 

Les ports Ethernet retournent au réglage par défaut lorsque l'un de ces événements se produit sur l'automate :

- réinitialisation de type 1 ;
- réinitialisation de type 2 ;
- un nouveau projet est téléchargé - Dans ce cas, les réglages du nouveau projet prennent effet ;
- le programme est effacé dans l'automate - Les exemples suivants illustrent ce qui efface le programme d'un automate :
  - un défaut majeur irrécupérable se produit
  - une mise à jour de firmware se produit

Vous devez reconfigurer les réglages pour désactiver un port Ethernet après que le port soit revenu à ses réglages par défaut.

Il existe deux façons de désactiver le port Ethernet :

- [Désactivation du port Ethernet sous l'onglet Port Configuration, page 233](#)
- [Désactivation du port Ethernet avec une instruction MSG, page 234](#)



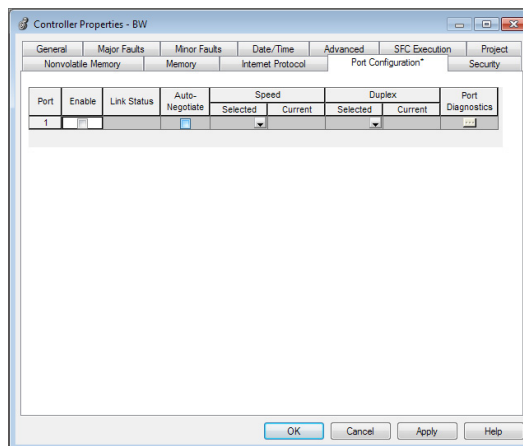
## Désactivation du port Ethernet sous l'onglet Port Configuration

Vous pouvez désactiver le port Ethernet embarqué sur l'automate. Cette méthode conserve les réglages du projet, si bien qu'à chaque téléchargement du projet vers l'automate, le port Ethernet est désactivé.

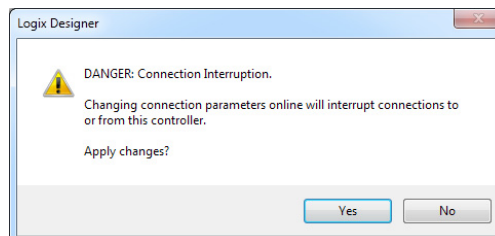
1. Dans la barre d'outils Online (En ligne), cliquez sur l'icône des propriétés de l'automate.



2. Dans la boîte de dialogue Controller Properties (Propriétés de l'automate), cliquez sur l'onglet Port Configuration (Configuration du port).
3. Sous l'onglet Configuration du port, décochez la case Enable.



4. Sous l'onglet Port Configuration, cliquez sur Apply (Appliquer).
  - Si vous êtes en ligne lorsque vous effectuez cette modification, cliquez sur Yes (Oui) dans la boîte de dialogue Alerte. Dans la boîte de dialogue, cliquez sur Yes (Oui). La modification prend effet immédiatement.



- Si vous êtes hors ligne, alors le changement prend effet lorsque vous téléchargez le programme dans l'automate.
5. Sous l'onglet Port Configuration, cliquez sur OK.

## Désactivation du port Ethernet avec une instruction MSG

Pour exécuter cette option, utilisez une instruction MSG CIP Generic avec « Path of THIS ». Vous ne pouvez pas utiliser cette instruction MSG pour désactiver le port Ethernet sur un autre automate.

1. Ajouter une instruction MSG à votre programme.

Ce message doit être exécuté une seule fois, et non pas à chaque scrutation de programme.

---

**IMPORTANT** Vous ne pouvez pas ajouter une instruction MSG à votre programme si le sélecteur à clé de l'automate est en mode Exécution ou si les réglages de FactoryTalk Security nient cette option de modification.

---

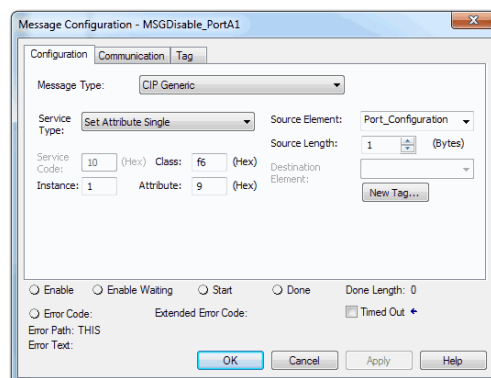
2. Configurez l'onglet Configuration de la boîte de dialogue Message Configuration comme suit :

---

**IMPORTANT** Ces valeurs sont mémorisées dans la mémoire NVS de telle sorte que l'instruction MSG ne doit pas être exécutée à chaque mise sous tension de l'automate.

---

- Type de message - CIP Generic
  - Type de service - Set Attribute Single
  - Instance - 1
  - Classe - f6
  - Attribut - 9
  - Élément source - Point d'automate de type de données SINT
- Dans cet exemple, le point d'automate est dénommé Port\_Configuration.
- Longueur de la source - 1

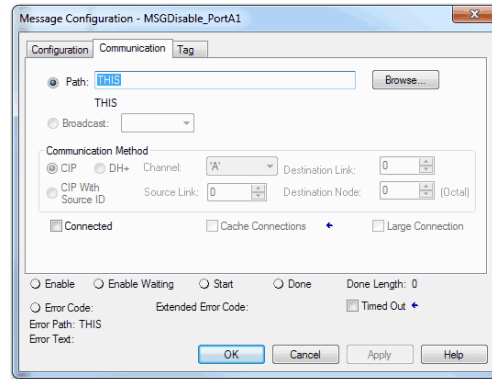


3. Configurez l'onglet Communication pour utiliser un « Path of THIS ».

---

**IMPORTANT** Les messages à THIS doivent être des messages non connectés.

---



4. Avant d'activer l'instruction MSG, assurez-vous que la valeur de l'élément source est 2.

---

**IMPORTANT** Vous pouvez réactiver un port Ethernet après sa désactivation. Pour réactiver le port, exécutez les étapes décrites dans cette section. Toutefois, avant d'activer les instructions MSG, assurez-vous que la valeur du point source est 1.

---

## Désactivation des ports CIP Security

Avec l'application Studio 5000 Logix Designer, version 32.00.00 ou ultérieure, vous utilisez un MSG générique CIP avec un Path of THIS pour exécuter cette option.

**IMPORTANT** Cette procédure désactive les ports CIP Security. Pour réactiver les ports, vous devez utiliser le bouton de réinitialisation de l'automate pour effectuer une réinitialisation de type 2 (remettre l'automate à l'état d'origine par défaut). Consultez [Réinitialisation de type 2, page 91](#).

Vous ne pouvez pas utiliser cette instruction MSG pour désactiver les ports CIP Security sur un automate différent.

Ce message doit être exécuté une seule fois, et non pas à chaque scrutation de programme.

1. Création d'un point automate de type de données SINT[9].

Dans cet exemple, le point de l'automate est dénommé CIPSEC\_DISABLE et doit correspondre aux caractéristiques suivantes.

Name	Value	Style	Data Type
▲ CIPSEC_DISABLE	{...}	Hex	SINT[9]
▶ CIPSEC_DISABLE[0]	16#02	Hex	SINT
▶ CIPSEC_DISABLE[1]	16#ad	Hex	SINT
▶ CIPSEC_DISABLE[2]	16#08	Hex	SINT
▶ CIPSEC_DISABLE[3]	16#11	Hex	SINT
▶ CIPSEC_DISABLE[4]	16#00	Hex	SINT
▶ CIPSEC_DISABLE[5]	16#ad	Hex	SINT
▶ CIPSEC_DISABLE[6]	16#08	Hex	SINT
▶ CIPSEC_DISABLE[7]	16#06	Hex	SINT
▶ CIPSEC_DISABLE[8]	16#00	Hex	SINT

Avant d'activer l'instruction MSG, tenez compte des éléments suivants :

- l'élément CIPSEC\_DISABLE[4] est responsable de la désactivation du port UDP 2221 et d'EtherNet/IP par DTLS, classe de transport 0/1.
- l'élément CIPSEC\_DISABLE[8] est responsable de la désactivation du port TCP 2221 et d'EtherNet/IP par TLS, UCMM, et classe de transport 3.
- pour désactiver les ports CIP Security de l'automate, les éléments CIPSEC\_DISABLE[4] et CIPSEC\_DISABLE[8] dans le tableau SINT pour l'élément source CIPSEC\_DISABLE doivent être à 0.

2. Ajouter une instruction MSG à votre programme.

**IMPORTANT** Vous ne pouvez pas ajouter une instruction MSG à votre programme si l'automate est en mode Exécution ou si les réglages de FactoryTalk Security nient cette option de modification.

3. Configurez l'onglet Configuration de la boîte de dialogue Message Configuration comme suit :
  - Type de message - CIP Generic
  - Type de service - Custom
  - Code de service - 4c
  - Instance - 1
  - Classe - f5
  - Attribut - 0
  - Élément source - Point d'automate de type de données SINT[9].  
C'est le point d'automate que vous avez créé à l'étape 1.
  - Longueur de la source - 9

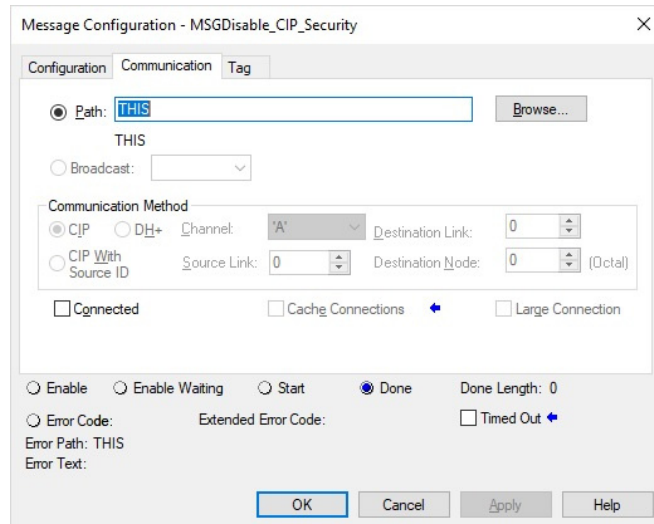
The screenshot shows the 'Message Configuration - MSGDisable\_CIP\_Security' dialog box. It has three tabs: 'Configuration', 'Communication', and 'Tag'. The 'Configuration' tab is selected. The settings are as follows:

- Message Type: CIP Generic (dropdown)
- Service Type: Custom (dropdown)
- Service Code: 4c (Hex) (text box)
- Instance: 1 (text box)
- Class: f5 (Hex) (text box)
- Attribute: 0 (Hex) (text box)
- Source Element: CIPSEC\_DISABLE (dropdown)
- Source Length: 9 (text box) (Bytes)
- Destination Element: (empty dropdown)
- New Tag... (button)

At the bottom, there are radio buttons for 'Enable', 'Enable Waiting', 'Start', and 'Done' (which is selected). There is also a 'Done Length: 0' field. Below that are 'Error Code:', 'Error Path: THIS', and 'Error Text:' labels. At the very bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

- Configurez l'onglet Communication pour utiliser un « Path of THIS ».

**IMPORTANT** Les messages à THIS doivent être des messages non connectés.



- Coupez et remettez l'automate sous tension pour que la configuration prenne effet.

## Désactivation du port USB

Avec l'application Studio 5000 Logix Designer, version 32.00.00 ou ultérieure, vous pouvez utiliser un MSG générique CIP avec un Path of THIS pour exécuter cette option.

1. Ajouter une instruction MSG à votre programme.

Ce message doit être exécuté une seule fois, et non pas à chaque scrutation de programme.

---

**IMPORTANT** Vous ne pouvez pas ajouter une instruction MSG à votre programme si l'automate est en mode Exécution ou si les réglages de FactoryTalk Security nient cette option de modification.

---

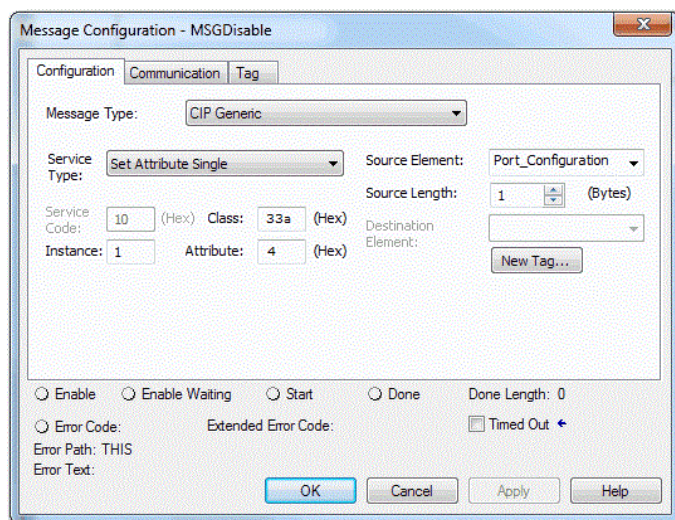
2. Configurez l'onglet Configuration de la boîte de dialogue Message Configuration comme suit :

---

**IMPORTANT** Ces valeurs sont mémorisées dans la mémoire NVS de telle sorte que l'instruction MSG ne doit pas être exécutée à chaque mise sous tension de l'automate.

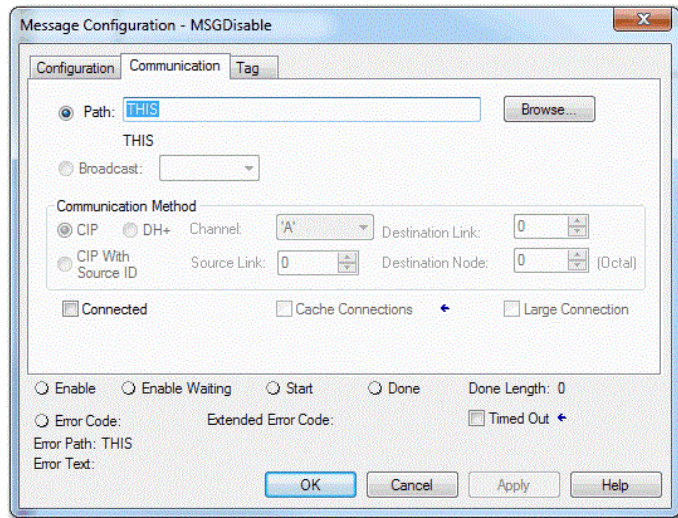
---

- Type de message - CIP Generic
- Type de service - Set Attribute Single
- Instance - 1
- Classe - 33a
- Attribut - 4
- Élément source - Point d'automate de type de données SINT  
Dans cet exemple, l'élément source est dénommé Port\_Configuration.
- Longueur de la source - 1



3. Configurez l'onglet Communication pour utiliser un « Path of THIS ».

**IMPORTANT** Les messages à THIS doivent être des messages non connectés.





## Désactivation de la carte SD

Avec l'application Studio 5000 Logix Designer, version 32.00.00 ou ultérieure, vous pouvez utiliser un MSG générique CIP avec un Path of THIS pour exécuter cette option.

---

**IMPORTANT** N'oubliez pas les points suivants :

- Une carte SD ne peut être désactivée qu'avec un message à elle-même.
- Une fois qu'un logement SD est désactivé, vous perdez toute possibilité de communiquer avec une carte SD insérée dans le logement. Ceci inclut toute information de diagnostic.
- Vous pouvez réactiver la carte SD :
  - avec une réinitialisation de type 2
  - et avec un firmware V33 ou ultérieur, un message à elle-même

- 
1. Ajouter une instruction MSG à votre programme.

Ce message doit être exécuté une seule fois, et non pas à chaque scrutation de programme.

---

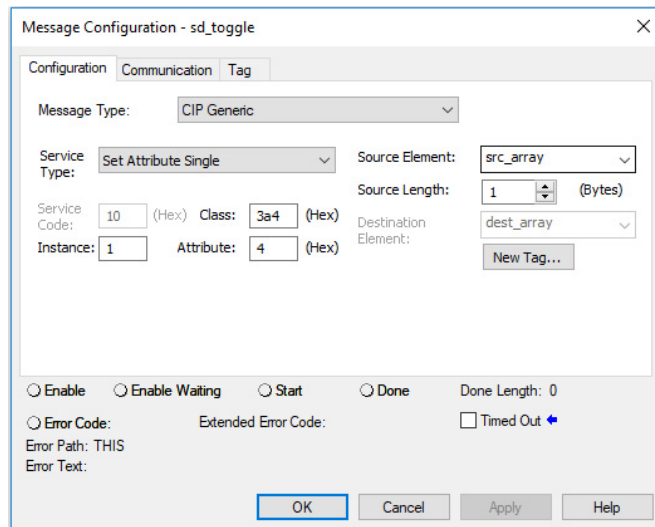
**IMPORTANT** Vous ne pouvez pas ajouter une instruction MSG à votre programme si l'automate est en mode Exécution ou si les réglages de FactoryTalk Security nient cette option de modification.

- 
2. Configurez l'onglet Configuration de la boîte de dialogue Message Configuration comme suit :

---

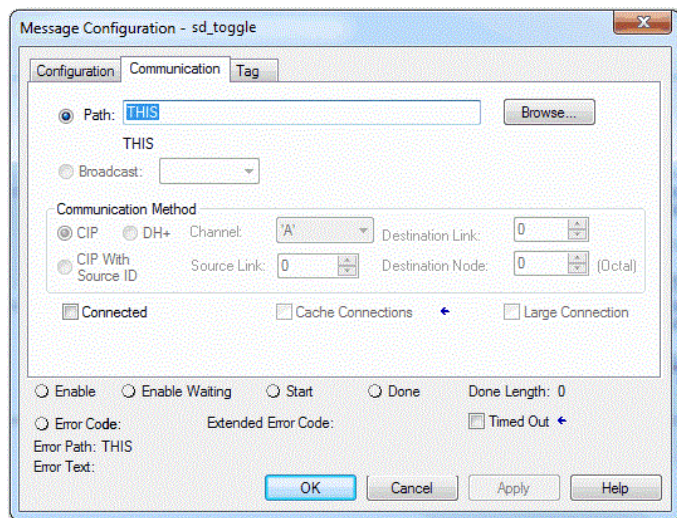
**IMPORTANT** Ces valeurs sont mémorisées dans la mémoire NVS de telle sorte que l'instruction MSG ne doit pas être exécutée à chaque mise sous tension de l'automate.

- 
- Type de message - CIP Generic
  - Type de service - Set Attribute Single
  - Instance - 1
  - Classe - 3a4
  - Attribut - 4
  - Élément source - Point d'automate de type de données Tableau SINT  
Dans cet exemple, l'élément source est dénommé src\_array
  - Longueur de la source - 1



3. Configurez l'onglet Communication pour utiliser un « Path of THIS ».

**IMPORTANT** Les messages à THIS doivent être des messages non connectés.



## Désactivation de l'afficheur d'état à 4 caractères

Avec l'application Studio 5000 Logix Designer, version 29.00.00 ou ultérieure, vous pouvez désactiver certaines catégories de messages sur l'afficheur d'état à 4 caractères :

- [Désactivation de toutes les catégories de messages, page 243](#)
- [Désactivation de catégories individuelles de messages, page 245](#)

Utilisez une instruction MSG CIP Generic pour exécuter chaque option.

---

**IMPORTANT** Les messages système ci-après sont toujours affichés et ne peuvent pas être désactivés :

- Messages à la mise sous tension (tels que TEST, PASS, CHRG)
  - Message concernant les références
  - Message de révision du firmware
  - Messages de défaillance majeure/critique
- 

L'afficheur d'état à 4 caractères revient au réglage par défaut lorsque l'une des actions ci-après est exécutée sur l'automate :

- réinitialisation de type 1 ;
- réinitialisation de type 2 ;
- un nouveau projet est téléchargé - Dans ce cas, les réglages du nouveau projet prennent effet ;
- le programme est effacé dans l'automate - Les exemples suivants illustrent ce qui efface le programme d'un automate :
  - un défaut majeur irrécupérable se produit
  - une mise à jour de firmware se produit.

Vous devez reconfigurer les réglages pour désactiver l'afficheur d'état à 4 caractères après qu'il ait retrouvé ses réglages par défaut.

## Désactivation de toutes les catégories de messages

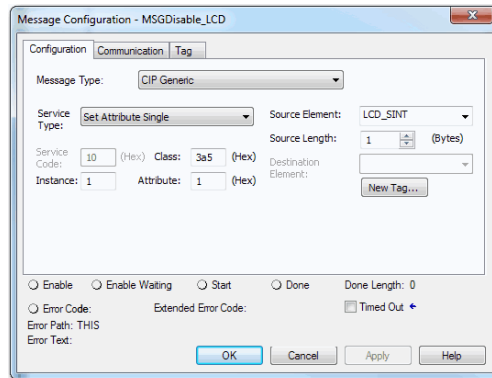
Lorsque vous désactivez toutes les catégories de messages, ces informations ne s'affichent plus :

- le nom du projet ;
- l'état de la liaison ;
- l'état du port ;
- Adresse IP.

Procédez comme suit.

1. Ajouter une instruction MSG à votre programme.
2. Configurez l'onglet Configuration de la boîte de dialogue Message Configuration comme suit :
  - Type de message - CIP Generic
  - Type de service - Set Attribute Single

- Instance - 1
- Classe - 3a5
- Attribut - 1
- Élément source - Point d'automate de type de données SINT  
Dans cet exemple, le point d'automate est dénommé LCD\_SINT.
- Longueur de la source - 1

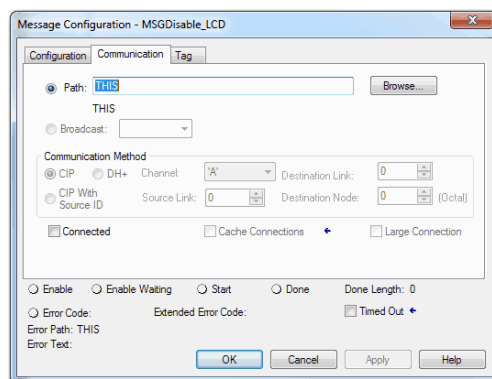


3. Configurez l'onglet Communication pour utiliser un « Path of THIS ».

---

**IMPORTANT** Les messages à THIS doivent être des messages non connectés.

---



4. Avant d'activer l'instruction MSG, assurez-vous que la valeur de l'élément source est 1.

---

**IMPORTANT** Vous pouvez réactiver l'afficheur à 4 caractères après sa désactivation.  
Pour réactiver l'afficheur à 4 caractères, exécutez les étapes décrites dans cette section. Toutefois, avant d'activer les instructions MSG, assurez-vous que la valeur de l'élément source est 0.

---

## Désactivation de catégories individuelles de messages

Vous pouvez désactiver un sous-ensemble d'informations qui défilent sur l'afficheur à 4 caractères de l'automate. Vous pouvez désactiver les sous-ensembles suivants :

- nom du projet et état de la liaison ;
- état du port et adresse IP.

Procédez comme suit.

1. Ajouter une instruction MSG à votre programme.

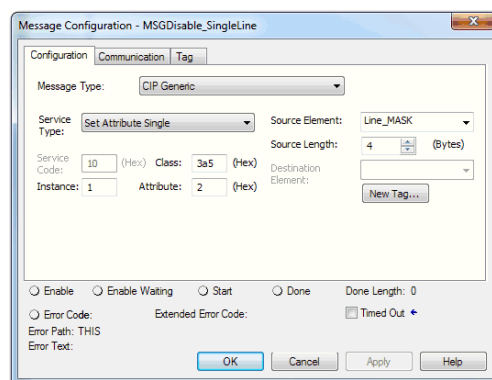
Ce message doit être exécuté une seule fois, et non pas à chaque scrutation de programme.

---

**IMPORTANT** Vous ne pouvez pas ajouter une instruction MSG à votre programme si le sélecteur à clé de l'automate est en mode Exécution ou si les réglages de FactoryTalk Security nient cette option de modification.

---

2. Configurez l'onglet Configuration de la boîte de dialogue Message Configuration comme suit :
  - Type de message - CIP Generic
  - Type de service - Set Attribute Single
  - Instance - 1
  - Classe - 3a5
  - Attribut - 2
  - Élément source - Point d'automate de type de données DINT  
Dans cet exemple, le point d'automate est dénommé Line\_MASK.
  - Longueur source - 4

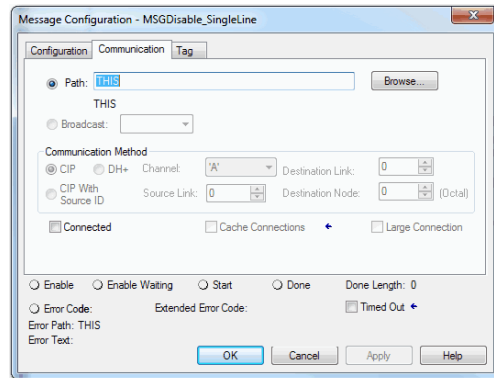


3. Configurez l'onglet Communication pour utiliser un « Path of THIS ».

---

**IMPORTANT** Les messages à THIS doivent être des messages non connectés.

---



4. Avant d'activer l'instruction MSG, assurez-vous que l'élément source utilise l'une des valeurs de point suivantes en fonction des informations que vous souhaitez désactiver :

- Nom de projet et état de la liaison - Bit 0 de l'élément source = 1
- État du port et adresse IP - Bit 1 de l'élément source = 1

---

**IMPORTANT** Vous pouvez réactiver les sous-ensembles d'informations sur l'afficheur à 4 caractères après leur désactivation.

Pour réactiver les sous-ensembles, exécutez les étapes décrites dans cette section. Toutefois, avant d'activer les instructions MSG, assurez-vous que le bit approprié dans la valeur du point de l'élément source est à 0.

---

## Désactivation des pages Internet de l'automate

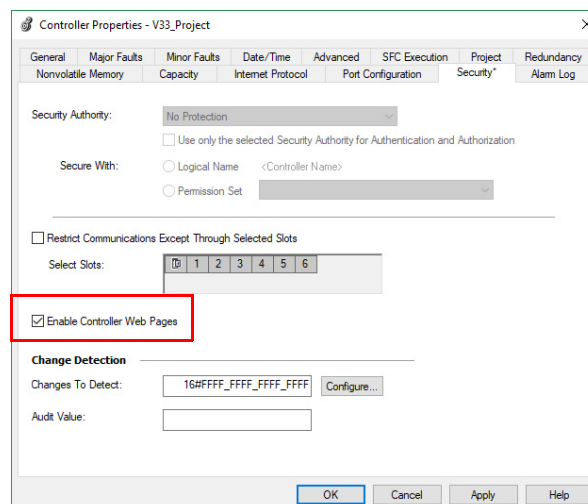
Vous pouvez désactiver les pages Internet de l'automate avec l'application Studio 5000 Logix Designer, version 28.00.00 ou ultérieure.

### Application Studio 5000 Logix Designer, version 33.00.00 ou ultérieure

Avec l'application Studio 5000 Logix Designer version 33.00.00 et ultérieure, les pages Internet de l'automate sont désactivées par défaut.

Bien que l'utilisation d'un MSG CIP Generic pour désactiver les pages Internet de l'automate soit prise en charge dans les versions 33.00.00 et ultérieures, Rockwell Automation recommande ces méthodes pour désactiver les pages Internet de l'automate :

- Si les pages Internet de l'automate sont activées, décochez la case dans l'onglet Logix Designer Controller Properties (Propriétés de sécurité de l'automate Logix Designer) pour désactiver les pages Internet.



- Pour les applications CIP Security vous pouvez également utiliser FactoryTalk Policy Manager pour désactiver les pages Internet (cela remplace la case à cocher Propriétés de l'automate).

### Application Studio 5000 Logix Designer version 32.00.00 ou antérieure

Pour l'application Studio 5000 Logix Designer, version 32.00.00 ou antérieure, vous utilisez un MSG CIP Generic pour exécuter cette option.

Consultez :

- [Utilisation d'un MSG CIP Generic pour désactiver les pages Internet de l'automate, page 249.](#)
- [Utilisation d'un MSG CIP Generic pour activer les pages Internet de l'automate, page 251.](#)

## Réglages par défaut des pages Internet de l'automate

Les réglages par défaut pour les pages Internet de l'automate sont :

- pages Internet activées pour le firmware automate révision 32 et antérieure ;
- pages Internet désactivées pour le firmware automate révision 33 et ultérieure.

Les pages Internet de l'automate reprennent leur réglage par défaut dans ces situations :

- une réinitialisation de type 1 pour toutes les versions de l'application Logix Designer ;
- une réinitialisation de type 2 pour toutes les versions de l'application Logix Designer.

---

**IMPORTANT** Lorsque vous mettez à jour le firmware de l'automate vers la révision 33 ou une version ultérieure sans réinitialisation, l'automate conserve la configuration précédente de la page Internet de l'automate (pages Internet activées) et ne passe pas automatiquement au réglage par défaut pour V33 (désactive les pages Internet).

---

- Vous devez reconfigurer les réglages pour désactiver la page Internet de l'automate après qu'il ait retrouvé ses réglages par défaut.

Les pages Internet de l'automate retournent au réglage par défaut lorsque les événements suivants se produisent sur l'automate :

- un nouveau projet est téléchargé - Dans ce cas, les réglages du nouveau projet prennent effet ;
- lorsque l'automate reçoit un message de configuration, il prend le réglage du message de configuration.



## Utilisation d'un MSG CIP Generic pour désactiver les pages Internet de l'automate

**IMPORTANT** Si vous utilisez FactoryTalk Policy Manager pour désactiver les pages Internet dans une application CIP Security, le message-to-self CIP générique remplace le réglage FactoryTalk Policy Manager.

1. Ajouter une instruction MSG à votre programme.

**IMPORTANT** Vous ne pouvez pas ajouter une instruction MSG à votre programme si le sélecteur à clé de l'automate est en mode Exécution ou si les réglages de FactoryTalk Security nient cette option de modification.

2. Configurez l'onglet Configuration de la boîte de dialogue Message Configuration comme suit :

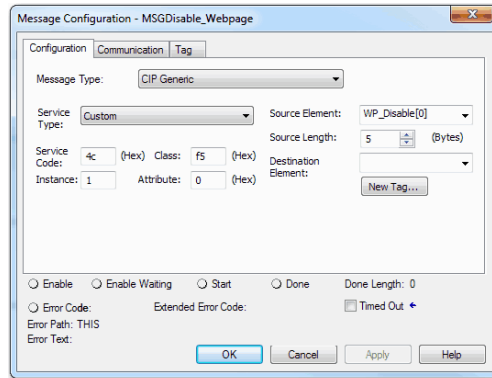
- Type de message - CIP Generic
- Type de service - Custom
- Code de service - 4c
- Instance - 1
- Classe - f5
- Attribut - 0
- Élément source - Point d'automate de type de données SINT[5].

Dans cet exemple, le point de l'automate est dénommé WP\_Disable et doit correspondre aux caractéristiques suivantes.

**IMPORTANT** Le point d'élément source dans votre projet d'application Logix Designer doit correspondre aux valeurs affichées dans l'illustration. Si vous utilisez des valeurs différentes de celles affichées, les pages Internet de l'automate ne sont pas désactivées.

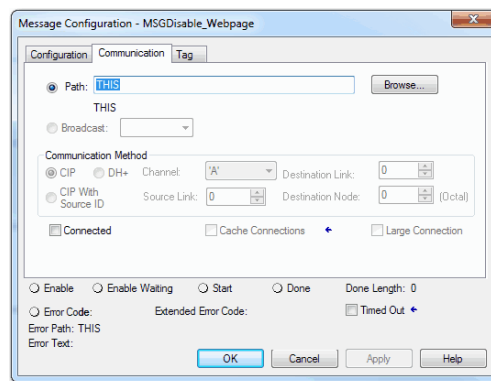
WP_Disable	{...}	Decimal	SINT[5]
WP_Disable[0]	1	Decimal	SINT
WP_Disable[1]	80	Decimal	SINT
WP_Disable[2]	0	Decimal	SINT
WP_Disable[3]	6	Decimal	SINT
WP_Disable[4]	0	Decimal	SINT

– Longueur source - 5



3. Configurez l'onglet Communication pour utiliser un « Path of THIS ».

**IMPORTANT** Les messages à THIS doivent être des messages non connectés.



## Utilisation d'un MSG CIP Generic pour activer les pages Internet de l'automate

1. Ajouter une instruction MSG à votre programme.

---

**IMPORTANT** Vous ne pouvez pas ajouter une instruction MSG à votre programme si le sélecteur à clé de l'automate est en mode Exécution ou si les réglages de FactoryTalk Security nient cette option de modification.

---

2. Configurez l'onglet Configuration de la boîte de dialogue Message Configuration comme suit :

- Type de message - CIP Generic
- Type de service - Custom
- Code de service - 4c
- Instance - 1
- Classe - f5
- Attribut - 0
- Élément source - Point d'automate de type de données SINT[5].

Dans cet exemple, le point de l'automate est dénommé WP\_Enable et doit correspondre aux caractéristiques suivantes.

---

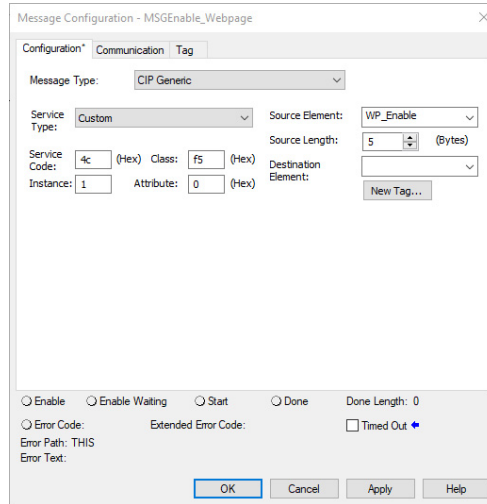
**IMPORTANT** Le point d'élément source dans votre projet d'application Logix Designer doit correspondre aux valeurs affichées dans l'illustration.

Si vous utilisez des valeurs différentes de celles affichées, les pages Internet de l'automate ne sont pas activées.

---

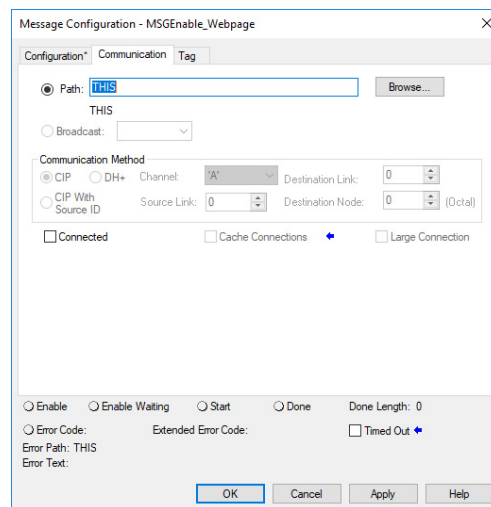
▲ WP_Enable	{...}	Decimal	SINT[5]
▶ WP_Enable[0]	1	Decimal	SINT
▶ WP_Enable[1]	80	Decimal	SINT
▶ WP_Enable[2]	0	Decimal	SINT
▶ WP_Enable[3]	6	Decimal	SINT
▶ WP_Enable[4]	1	Decimal	SINT

– Longueur source - 5



3. Configurez l'onglet Communication pour utiliser un « Path of THIS ».

**IMPORTANT** Les messages à THIS doivent être des messages non connectés.



## Développement d'applications de mouvement

Rubrique	Page
Présentation de la commande de mouvement	254
Obtenir les informations d'axe	257
Programmation de la commande d'axe	255

### S'applique à ces automates :

ControlLogix 5580

GuardLogix 5580

Les automates prennent en charge ces interfaces de commande d'axe :

- Commande d'axe intégrée en réseau EtherNet/IP™.
- Les interfaces variateur numériques incluent les variateurs connectés sur EtherNet/IP, ainsi que par l'intermédiaire d'une interface Sercos.
- Les variateurs à commande analogique acceptent des sorties analogiques de  $\pm 10$  V. Ils peuvent s'interfacer avec une grande variété de types de capteur de retour ; notamment des codeurs en quadrature, ainsi que des capteurs SSI et LVDT.

Pour plus d'informations, consultez les publications suivantes :

- Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, publication [MOTION-UM003](#).
- Mouvement intégré sur le réseau EtherNet/IP Manuel de référence, publication [MOTION-RM003](#).
- SERCOS and Analog Motion Configuration and Startup User Manual, publication [MOTION-UM001](#).

## Présentation de la commande de mouvement

Les automates prennent en charge jusqu'à 256 axes de mouvement intégré. Les 256 axes peuvent constituer n'importe quelle combinaison d'axes CIP™, virtuels et consommés. Vous pouvez ajouter tous les axes à un groupe d'axes, et vous pouvez affecter n'importe quelle combinaison d'axes à différents plannings de mise à jour d'axe.

**CONSEIL** Rockwell Automation recommande d'utiliser le port EtherNet/IP intégré pour les applications de mouvement hautes performances.

Vous pouvez associer les commandes d'axes intégrées à n'importe quel variateur approprié, que le chemin de communication vers le variateur se fasse via le port Ethernet embarqué ou via le bus intermodules 1756 (via un pont Ethernet tel qu'un 1756-EN2T)

Le processus de configuration varie selon votre application et votre choix de variateur. Les étapes suivantes permettent de configurer une application de mouvement.

1. Créez un projet d'automate.
2. Sélectionnez le type du variateur.

Type de variateur	Exigences
CIP Motion™	<ul style="list-style-type: none"> <li>• Module de communication EtherNet/IP</li> <li>• Variateur numérique avec une connexion EtherNet/IP</li> </ul>
Interface Sercos	Sélectionnez un module d'interface Sercos : <ul style="list-style-type: none"> <li>• 1756-M03SE</li> <li>• 1756-M08SE</li> <li>• 1756-M16SE</li> </ul>
Interface analogique	Sélectionnez un module d'interface analogique : <ul style="list-style-type: none"> <li>• 1756-HYD02</li> <li>• 1756-M02AE</li> <li>• 1756-M02AS</li> </ul>

3. Définissez les points d'axe selon les besoins.
4. Configurez le variateur.
5. Créez des axes selon les besoins.

## Programmation de la commande d'axe

L'automate fournit un ensemble d'instructions de commande d'axe pour vos axes :

- L'automate utilise ces instructions exactement comme le reste des instructions Logix 5000™.
- Chaque instruction de mouvement fonctionne sur un ou plusieurs axes.
- Vous pouvez effectuer la programmation d'instructions de commande de mouvement au moyen de ces langages de programmation :
  - Diagramme à relais (LD)
  - Texte structuré (ST)
  - Graphe de fonctionnement séquentiel (SFC)
- Chaque instruction de mouvement nécessite un point de commande d'axe. Le point utilise un type de données MOTION\_INSTRUCTION et enregistre les informations d'état de l'instruction.

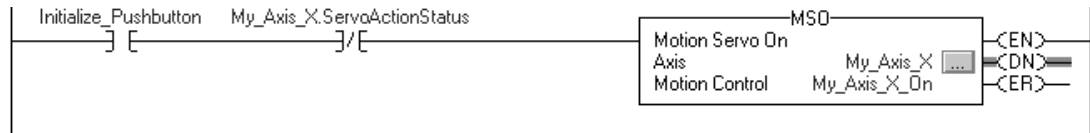
Pour plus d'informations, consultez la publication [MOTION-RM002](#), « Logix 5000 Controller Motion Instructions Reference Manual ».



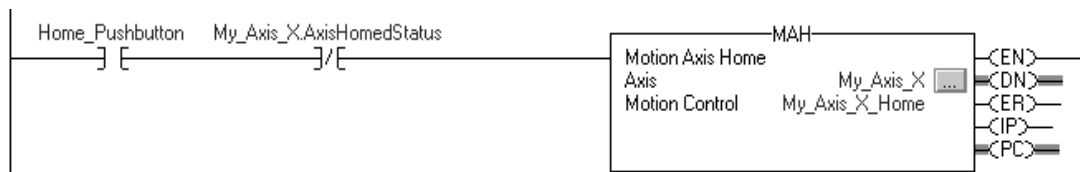
**ATTENTION :** Utilisez chaque point de commande d'axe uniquement dans une seule instruction de mouvement. Un fonctionnement involontaire peut se produire si vous réutilisez le même point de commande d'axe dans d'autres instructions de mouvement ou si vous écrivez sur l'un des éléments de point de commande d'axe.

Dans cet exemple, un simple diagramme à relais prend l'origine, déplace par à-coups et positionne un axe.

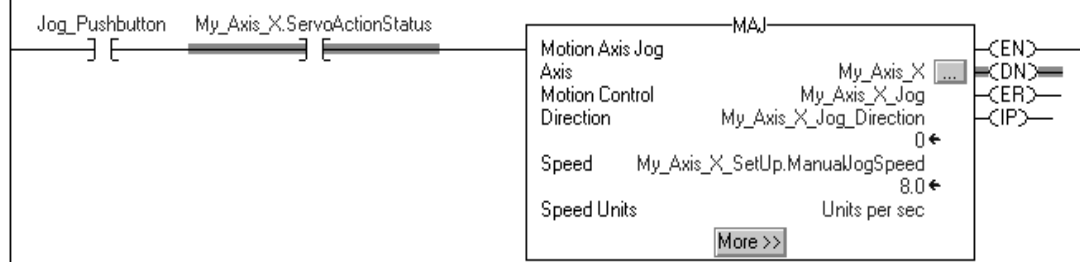
Si Initialize\_Pushbutton = on et que l'axe est à l'arrêt (My\_Axis\_X.ServoActionStatus = off), l'instruction MSO active l'axe.



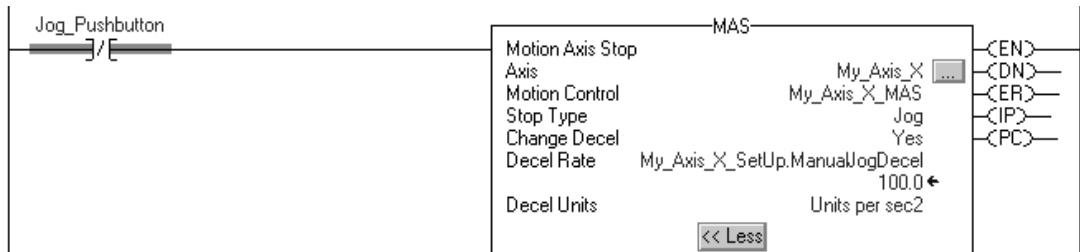
Si Home\_Pushbutton = on et que l'origine de l'axe n'a pas été prise (My\_Axis\_X.AxisHomedStatus = off), l'instruction MAH envoie l'axe à l'origine.



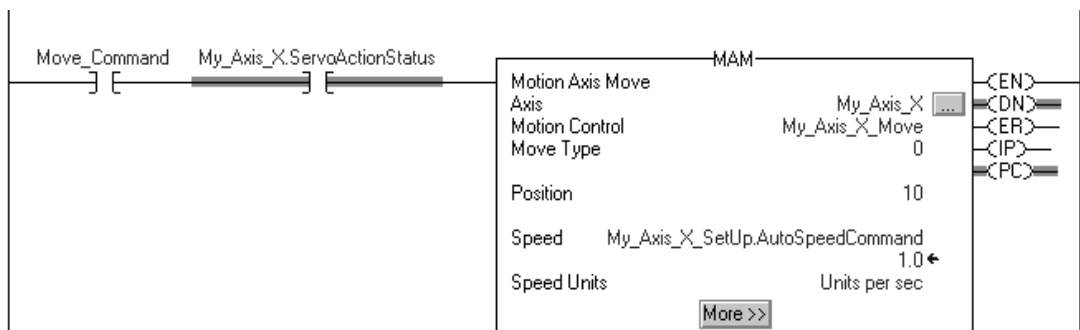
Si Jog\_Pushbutton = on et que l'axe est activé (My\_Axis\_X.ServoActionStatus = on), l'instruction MAJ avance l'axe par à-coups à 8 unités/seconde.



Si Jog\_Pushbutton = off, l'instruction MAS arrête l'axe à 100 unités/.seconde<sup>2</sup>. Assurez-vous que Change Decel est sur Yes. Sinon, l'axe décélère à sa vitesse maximum.



Si Move\_Command = on et que l'axe est activé (My\_Axis\_X.ServoActionStatus = on), l'instruction MAM met l'axe en mouvement. L'axe se déplace jusqu'à la position 10 unités à 1 unité/seconde.



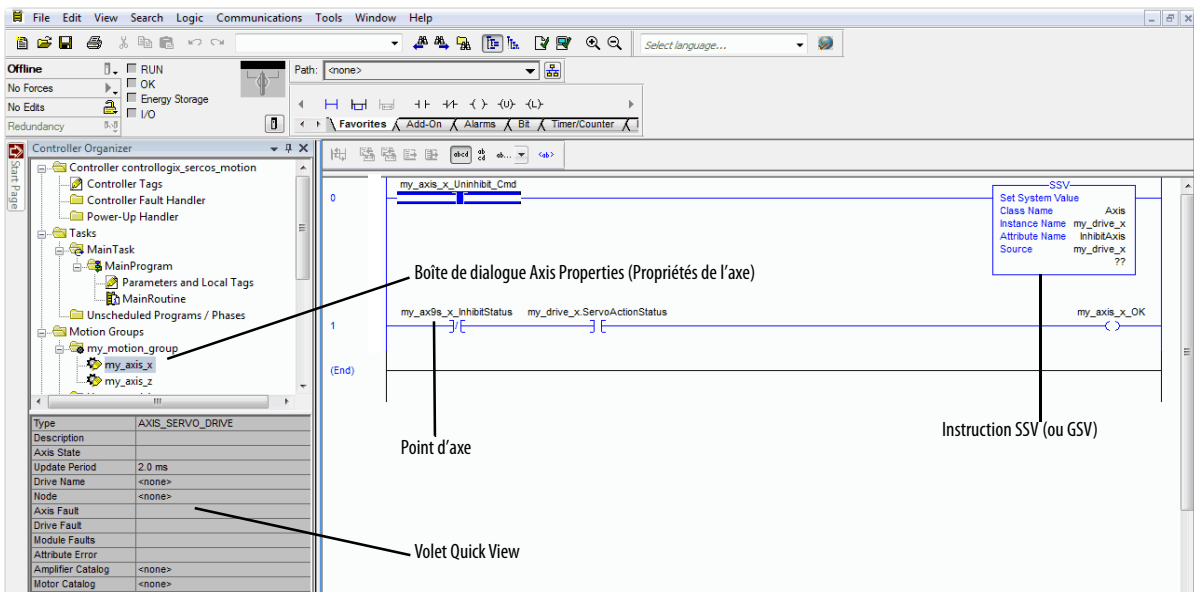


## Obtenir les informations d'axe

Vous pouvez obtenir des informations sur un axe au moyen de l'une de ces méthodes :

- Double cliquez sur l'axe pour ouvrir la boîte de dialogue Axis Properties (Propriétés de l'axe).
- Utilisez une instruction Get System Value (GSV) ou Set System Value (SSV) pour lire ou modifier la configuration pendant la durée d'exécution.
- Affichez le volet QuickView™ pour voir l'état et les défauts d'un axe.
- Utilisez un point d'axe pour connaître l'état et les défauts.

**Figure 50 - Obtenir les informations d'axe**



**Notes :**

## Dépannage de l'automate

Rubrique	Page
Diagnostics automatiques	259
Considérations relatives aux diagnostics de perte de communication	260
Diagnostics de l'automate avec Logix Designer	261
Diagnostics de l'automate avec le logiciel de type Linx	270
Pages Internet de l'automate	271

Ce chapitre décrit comment dépanner l'automate si des problèmes se produisent pendant le fonctionnement normal. En plus des méthodes décrites dans ce chapitre, vous pouvez utiliser des messages sur l'afficheur à 4 caractères pour dépanner l'automate. Pour plus d'informations, consultez [Voyants d'état, page 277](#).

### Diagnostics automatiques

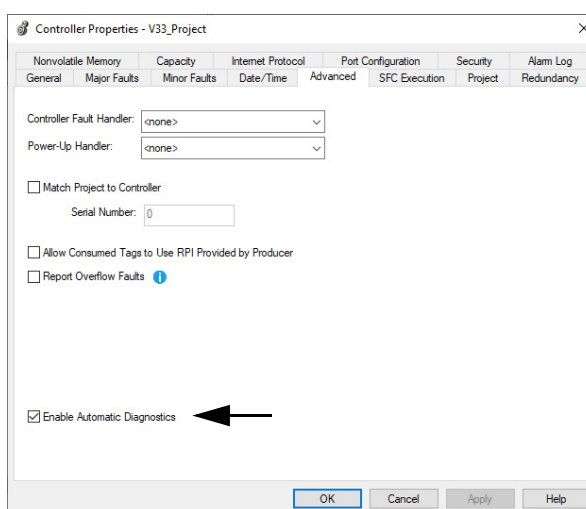
#### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Les diagnostics automatiques sont une fonctionnalité de niveau système des automates Logix 5000 qui fournissent des diagnostics de dispositif aux IHM et à d'autres clients, sans aucune programmation. Les diagnostics incluent la description des conditions du dispositif et les événements d'état.

Les diagnostics automatiques sont activés par défaut dans les automates Logix 5000 avec la révision de firmware 33 ou ultérieure. Vous pouvez désactiver et activer l'ensemble de la fonctionnalité en ligne ou hors ligne à partir de l'onglet Advanced (Avancé) de la boîte de dialogue Controller Properties (Propriétés de l'automate). Vous pouvez également désactiver les diagnostics automatiques pour un dispositif spécifique dans sa configuration.



## Considérations relatives aux diagnostics de perte de communication

### Concerné ces automates :

ControlLogix 5580

GuardLogix 5580

Le temps de réponse et les informations de diagnostic en cas de perte de communication dépendent du dispositif et des réglages de configuration.

Type de connexion	Comportement du dispositif
Connexion directe à un automate Logix 5000	Le dispositif signale une perte de communication. La perte de communication du dispositif peut être remplacée par le diagnostic d'un adaptateur de communication
Pas de connexion avec un automate Logix 5000	Les adaptateurs de communication qui n'ont pas de connexion avec l'automate ne signalent pas de diagnostic de perte de communication. Il est recommandé de configurer vos adaptateurs de communication pour une connexion d'état afin de s'assurer qu'ils signalent tout diagnostic de perte de communication en temps opportun.
Connexions de données	Le dispositif signale une perte de communication. La perte de communication du dispositif peut être remplacée par le diagnostic d'un adaptateur de communication
Connexion native pour rack	Le dispositif ne signale pas de diagnostic de perte de communication. L'adaptateur de communication signale des diagnostics de perte de communication. Un dispositif avec une connexion native pour rack a un ensemble de diagnostics réduit par rapport à une connexion directe.

Lorsqu'elle est activée, la fonctionnalité de diagnostic automatique permet :

- de diagnostiquer la perte de communication pour tous les dispositifs de la configuration des E/S de l'automate ;
- d'évaluer les diagnostics automatiques au niveau dispositif pour tous les dispositifs non inhibés et activés.

Vous pouvez désactiver les diagnostics automatiques pour un dispositif spécifique dans sa configuration. Le diagnostic de perte de communication reste actif même si le dispositif désactive les diagnostics automatiques. Pour désactiver le diagnostic de perte de communication, inhibez le dispositif ou désactivez les diagnostics automatiques de l'automate.

## Diagnostics de l'automate avec Logix Designer

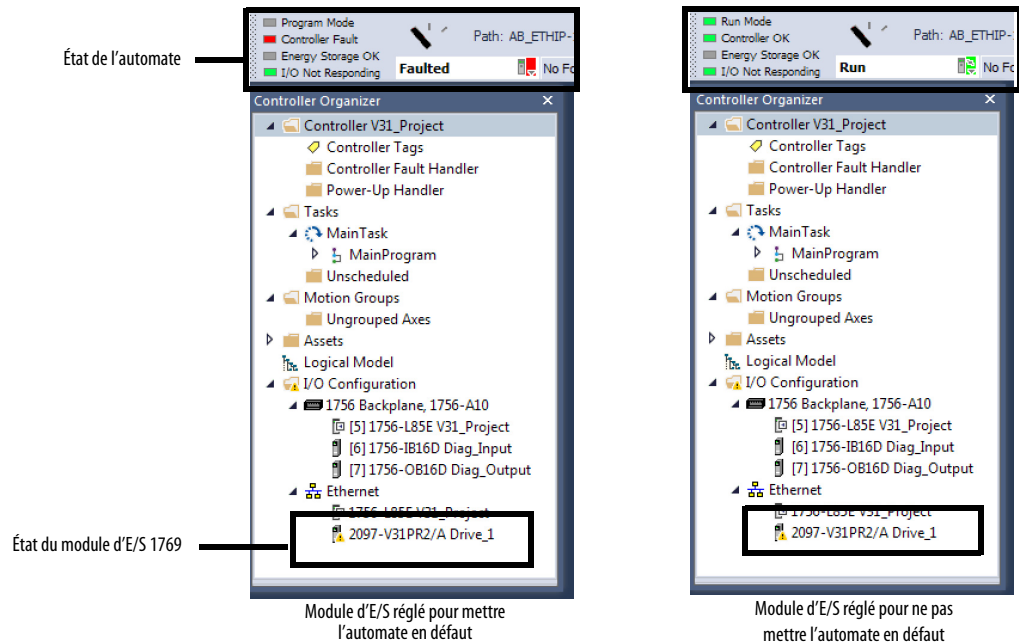
### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Un symbole d'avertissement apparaît dans l'organisateur de l'automate, près du module d'E/S. Cela se produit en présence de défauts ou d'autres conditions dans le module d'E/S, ou si la connexion au module d'E/S échoue en mode d'exécution.

- Si vous avez configuré un module d'E/S standard pour mettre l'automate en défaut lorsque la connexion échoue, l'état de l'automate indique Faulted (En défaut) et l'afficheur d'état de l'automate affiche Controller Fault (Défaut d'automate) et s'allume en rouge fixe. Le voyant I/O Not Responding clignote en vert.
- Si vous avez configuré un module d'E/S standard pour qu'il ne provoque pas de défaillance de l'automate lorsque la connexion échoue ou qu'il y a un défaut de connexion de sécurité, l'afficheur d'état de l'automate affiche Controller OK et s'allume en vert fixe. Le voyant I/O Not Responding clignote en vert.



### IMPORTANT Considérations relatives à la sécurité

Vous ne pouvez pas configurer des connexions de sécurité de façon à entraîner automatiquement un défaut de l'automate.

## Onglet Propriétés du module d'E/S

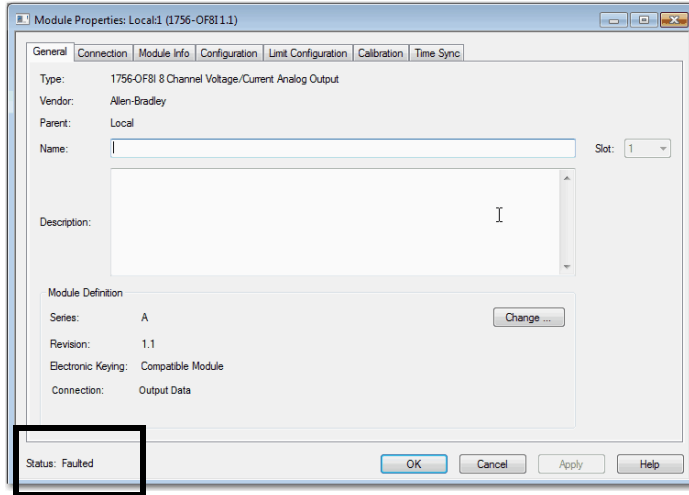
**Concernes ces automates :**

ControlLogix 5580

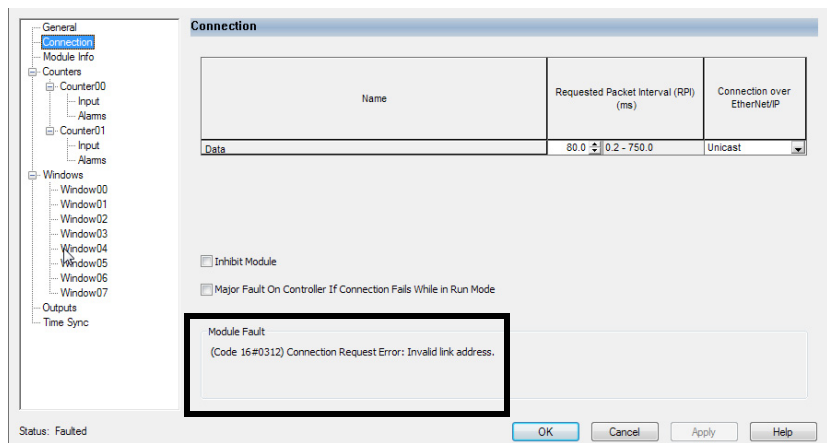
GuardLogix 5580

Les onglets General, Connection et Module Info montrent les informations de défaut.

- Message dans la ligne d'état de l'onglet General des propriétés d'un module d'E/S.



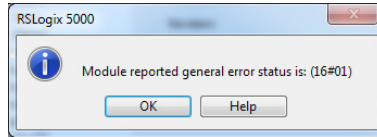
- L'onglet Connection montre le défaut du module. Cet exemple montre un défaut de communication.



- La section Status (État) de l'onglet Module Info (Infos du module) indique les défauts majeurs et mineurs (options Major Fault et Minor Fault), ainsi que l'état interne (option Internal State) du module.

L'onglet Module Info requiert des communications réussies. Si la communication avec le module d'E/S est OK, mais que le module lui-même est en défaut, nous vous recommandons d'utiliser la catégorie Module Info (Info du module) pour dépanner le défaut. S'il y a un défaut de communication, alors l'onglet Connection serait plus utile.

Si les communications sont en défaut et que vous essayez d'afficher l'onglet Module Info, une boîte de dialogue s'affiche et montre l'état d'erreur général du module et le code d'erreur.



## Notification dans l'éditeur de point

Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Les défauts généraux du module sont également signalés dans l'éditeur de point. Les défauts de diagnostic sont signalés uniquement dans l'éditeur de points. Lorsque le champ Value (Valeur) est mis à 1, un défaut existe.

**Figure 51 - Défaut module d'E/S**

Name	Value	Force Mask	Style	Data Type
Local:1:C	{...}	{...}		AB:1756_OF8I:C:0
Local:1:I	{...}	{...}		AB:1756_OF8I:I:0
Local:1:I.Fault	2#1111_11...		Binary	DINT
Local:1:I.Fault.0	1		Decimal	BOOL
Local:1:I.Fault.1	1		Decimal	BOOL
Local:1:I.Fault.2	1		Decimal	BOOL
Local:1:I.Fault.3	1		Decimal	BOOL
Local:1:I.Fault.4	1		Decimal	BOOL

**Figure 52 - Défaut de connexion d'E/S de sécurité**

Name	Value	Force Mas	Style	Data Type
Remote_Safety_Input_2:I	{...}	{...}		AB:1732ES_IB12XOB4_Safe
Remote_Safety_Input_2:I.ConnectionFaulted	1		Decimal	BOOL
Remote_Safety_Input_2:I.Pt00Data	0		Decimal	BOOL
Remote_Safety_Input_2:I.Pt01Data	0		Decimal	BOOL
Remote_Safety_Input_2:I.Pt02Data	0		Decimal	BOOL
Remote_Safety_Input_2:I.Pt03Data	0		Decimal	BOOL

## Activation du défaut majeur sur l'automate

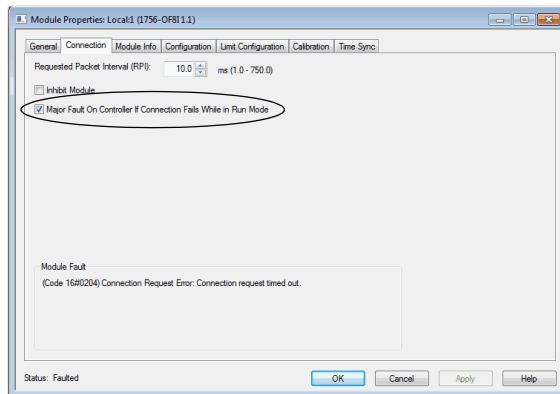
Concerne ces automates :

ControlLogix 5580

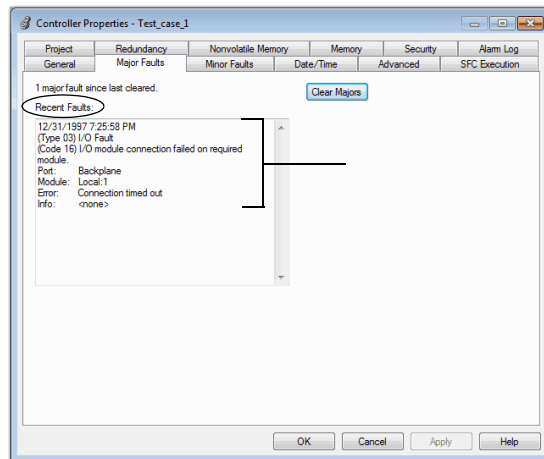
Pour afficher les informations récentes sur les défauts d'E/S dans l'onglet Défauts majeurs de l'écran Propriétés de l'automate, vous devez d'abord cocher l'option Défaut majeur de l'automate dans l'onglet Connexion des propriétés d'E/S.



**AVERTISSEMENT :** Si vous sélectionnez cette option, un défaut de connexion sur le module d'E/S peut provoquer un défaut majeur sur l'automate. Un défaut majeur sur l'automate fait passer les sorties à leur état de défaut configuré.



Lorsque vous surveillez les propriétés de configuration d'un module dans l'application Studio 5000 Logix Designer® et que vous recevez un message de défaut de communication, l'onglet Major Faults indique le type de défaut sous Recent Faults (défauts récents).





## Diagnostics de port

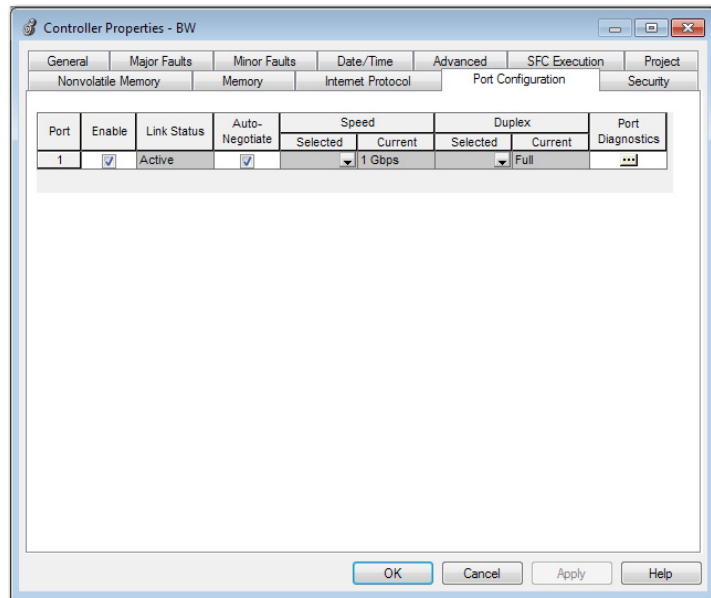
### Concerne ces automates :

ControlLogix 5580

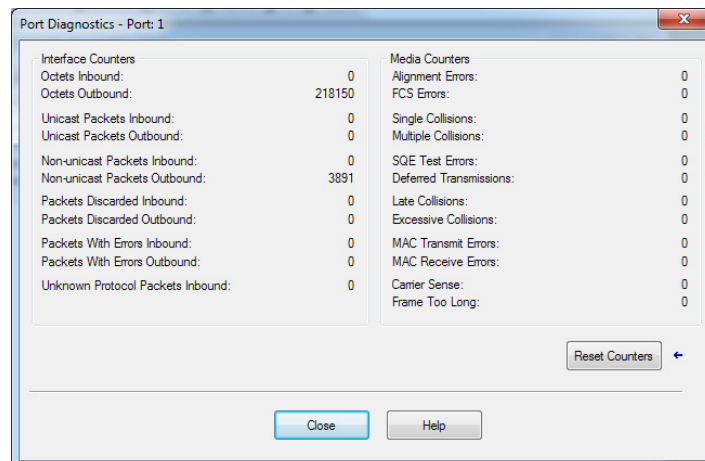
GuardLogix 5580

Lorsque votre projet est en ligne, vous pouvez afficher l'état du port Ethernet embarqué dans l'automate.

1. Dans la configuration des E/S, double-cliquez sur l'automate pour afficher ses propriétés.
2. Cliquez sur l'onglet Port Configuration.
3. Dans l'onglet Port Configuration, cliquez sur le bouton Port Diagnostics.



La page Port Diagnostics affiche les informations concernant le port. Voir le [tableau 37, page 266](#), pour la description des paramètres.



**Tableau 37 - Paramètres de diagnostics de port – Application Logix Designer**

Paramètre	Description
<b>Interface Counters</b>	Les valeurs des compteurs d'interface n'ont aucune signification lorsque vous êtes hors ligne ou en ligne et qu'il y a une erreur de communication.
Octets Inbound	Affiche le nombre d'octets qui sont reçus sur l'interface.
Octets Outbound	Affiche le nombre d'octets qui sont transmis à l'interface.
Unicast Packets Inbound	Affiche le nombre de paquets en envoi individuel qui sont reçus sur l'interface.
Unicast Packets Outbound	Affiche le nombre de paquets en envoi individuel qui sont transmis à l'interface.
Non-unicast Packets Inbound	Affiche le nombre de paquets pas en envoi individuel qui sont reçus sur l'interface.
Non-unicast Packets Outbound	Affiche le nombre de paquets pas en envoi individuel qui sont transmis à l'interface.
Packets Discarded Inbound	Affiche le nombre de paquets en amont qui sont reçus sur l'interface mais écartés.
Packets Discarded Outbound	Affiche le nombre de paquets en aval qui sont transmis à l'interface mais écartés.
Packets With Errors Inbound	Affiche le nombre de paquets en amont qui contiennent des erreurs (à l'exclusion des paquets en amont écartés).
Packets With Errors Outbound	Affiche le nombre de paquets en aval qui contiennent des erreurs (à l'exclusion des paquets en aval écartés).
Unknown Protocol Packets Inbound	Affiche le nombre de paquets en amont dont le protocole est inconnu.
<b>Media Counters</b>	Les valeurs Media Counters (Compteurs de média) n'ont pas de valeur si vous êtes hors ligne ou en ligne et qu'il y a une erreur de communication.
Alignment Errors	Affiche le nombre de trames reçues dont la longueur n'est pas un nombre entier d'octets.
FCS Errors	Affiche le nombre de trames reçues qui ne passent pas la vérification FCS.
Single Collisions	Affiche le nombre de trames transmises avec succès qui ont eu exactement une collision.
Multiple Collisions	Affiche le nombre de trames transmises avec succès qui ont eu des collisions multiples.
SQE Test Errors	Affiche le nombre de fois qu'un message d'erreur de test SQE a été généré.
Deferred Transmissions	Affiche le nombre de trames pour lesquelles la tentative de transmission a été retardée parce que le média est occupé.
Late Collisions	Affiche le nombre de fois qu'une collision est détectée plus tard que 512 octets de temps lors de la transmission d'un paquet.
Excessive Collisions	Affiche le nombre de trames pour lesquelles la transmission échoue en raison de collisions excessives.
MAC Transmit Errors	Affiche le nombre de trames pour lesquelles la transmission échoue en raison d'une erreur de transmission de sous-couche MAC interne.
MAC Receive Errors	Affiche le nombre de trames pour lesquelles la réception d'une interface échoue en raison d'une erreur de réception de sous-couche MAC interne.
Carrier Sense (détection de la porteuse)	Affiche le nombre de fois où la condition de détection de la porteuse a été perdue ou n'a jamais été affirmée lors d'une tentative de transmission de trame.
Frame Too Long	Affiche le nombre de trames reçues dépassant la taille maximum autorisée.
Reset Counters	<p>Cliquez sur Reset Counter (RAZ compteur) pour mettre à zéro les valeurs de l'interface et du compteur de support sur le module et actualiser les valeurs dans la boîte de dialogue.</p> <p>Reset Counter apparaît en grisé lorsque :</p> <ul style="list-style-type: none"> <li>• hors ligne</li> <li>• en ligne et une erreur de communication s'est produite</li> </ul>

## Synchronisation temporelle évoluée

### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Le dialogue Advanced Time Sync affiche des informations relative à la synchronisation temporelle CIP Sync™. Les informations apparaissent uniquement si le projet est en ligne et que la synchronisation temporelle est activée sous l'onglet Date/Heure.

### IMPORTANT Logiciel Precision Time Protocol (PTP)

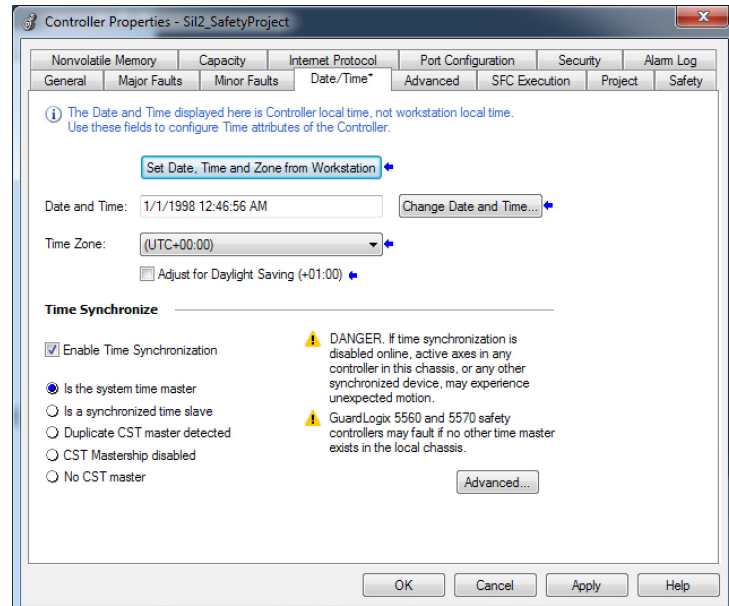
- L'accès au logiciel qui gère/met à jour le Precision Time Protocol sur un réseau de système de commande doit être limité aux utilisateurs formés à l'administration du temps du système de commande industriel, y compris PTP.

Cela inclut l'outil de mise à jour PTP fourni par Rockwell Automation ou un autre logiciel de gestion PTP accessible au public.

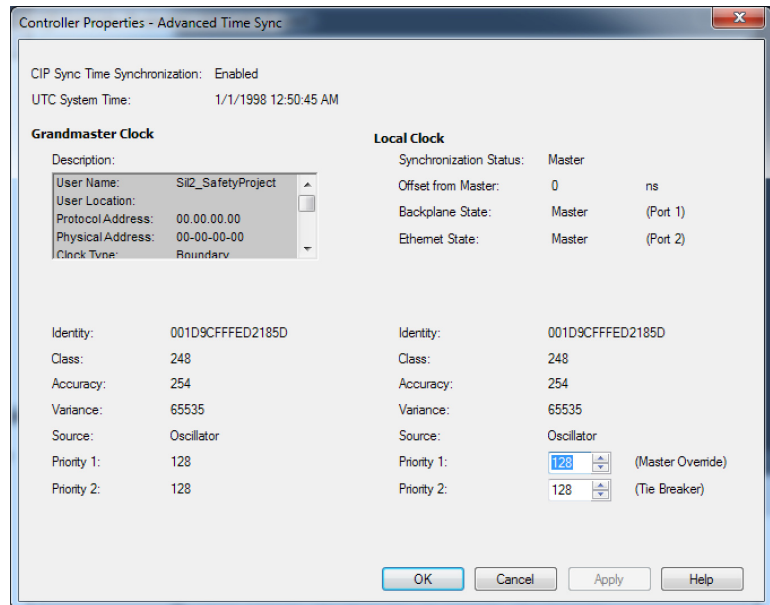
Des mises à jour incorrectes pendant le fonctionnement d'un système de commande peuvent perturber le fonctionnement du système de commande (y compris des défauts majeurs et certains dispositifs mis hors ligne).

- Lors de la désactivation de PTP sur un automate, pour donner à l'automate le temps de traiter la désactivation, utilisez un délai de deux secondes avant de régler le WallClockTime (WCT) dans l'automate. Sinon, il y a un risque que l'horloge maître (Grandmaster) écrase le WCT.

1. Sous l'onglet Date/Time cliquez sur le bouton Advanced (Évolué).



La boîte de dialogue Advanced Time Sync s'ouvre. Voir le [tableau 38](#), [page 268](#), pour la description des paramètres.



**Tableau 38 - Paramètres Time Sync**

Grandmaster Clock	
Description	<p>Affiche des informations sur l'horloge maître. Le fournisseur des dispositifs d'horloge maître contrôle ces informations. Les informations suivantes sont spécifiées :</p> <ul style="list-style-type: none"> <li>• User Name (nom d'utilisateur)</li> <li>• User Location (Localisation de l'utilisateur)</li> <li>• Protocol Address (Adresse du protocole)</li> <li>• Physical Address (Adresse physique)</li> <li>• Clock Type (Type d'horloge)</li> <li>• Manufacturer Name (Nom du fabricant)</li> <li>• Model (Modèle)</li> <li>• Serial Number (Numéro de série)</li> <li>• Hardware Revision (Révision matérielle)</li> <li>• révision de firmware</li> <li>• Software Revision</li> <li>• Profile Identity (Identité du profil)</li> <li>• Physical Protocol (Protocole physique)</li> <li>• Network Protocol (Protocole réseau)</li> <li>• Port Number (Numéro de port)</li> </ul> <p>Utilisez la barre de défilement verticale pour visualiser les données.</p>
Identity	Indique l'identifiant unique de l'horloge maître. Le format dépend du protocole réseau. Le réseau Ethernet code l'adresse MAC dans l'identificateur.
Classe	Indique l'appréciation de la qualité de l'horloge maître. Les valeurs sont définies entre 0 et 255 avec 0 comme la meilleure horloge.
Accuracy	Indique la précision absolue attendue de l'horloge maître par rapport à l'époque de la synchronisation PTP. La précision est définie comme une échelle graduée qui commence à 25 ns et se termine au-dessus de 10 secondes ou inconnu. Plus la valeur de précision est faible, meilleure est l'horloge.
Variance	Indique la mesure des propriétés de stabilité inhérente de l'horloge maître. La valeur est en unités de décalage mises à l'échelle. Plus la variance est faible, meilleure est l'horloge.

**Tableau 38 - Paramètres Time Sync (suite)**

Source	Affiche la source de temps de l'horloge maîtresse. Les valeurs disponibles sont : <ul style="list-style-type: none"> <li>• Horloge atomique</li> <li>• GPS</li> <li>• Radio</li> <li>• PTP</li> <li>• NTP</li> <li>• Réglage manuel</li> <li>• Autres</li> <li>• Oscillator</li> </ul>
Priority 1 / Priority 2	Indique la priorité relative de l'horloge maîtresse par rapport aux autres horloges du système. Les valeurs de priorité vont de 0 à 255. La priorité la plus élevée est 0. La valeur par défaut est 128 pour les deux réglages.
<b>Local Clock</b>	
Synchronization Status	Indique si l'horloge locale est synchrone ou asynchrone avec l'horloge maîtresse. Une horloge est synchrone si elle a un port à l'état esclave et qu'elle reçoit des mises à jour du maître temps.
Offset to Master	Affiche le nombre de déviations entre l'horloge locale et l'horloge maîtresse en nanosecondes.
Backplane State (état du fond de panier)	Affiche l'état actuel du fond de panier. Les valeurs suivantes sont disponibles : Initializing, Faulty, Disabled, Listening, PreMaster, Master, Passive, Uncalibration, Slave ou None.
Ethernet State (état Ethernet)	Affiche l'état du port Ethernet. Les valeurs suivantes sont disponibles : Initializing, Faulty, Disabled, Listening, PreMaster, Master, Passive, Uncalibration, Slave ou None.
Identity	Indique l'identifiant unique de l'horloge locale. Le format dépend du protocole réseau. Le réseau Ethernet code l'adresse MAC dans l'identificateur.
Classe	Indique la mesure de la qualité de l'horloge locale. Les valeurs sont définies entre 0 et 255 avec 0 comme la meilleure horloge.
Accuracy	Indique la précision absolue attendue de l'horloge locale par rapport à l'époque de la synchronisation PTP. La précision est définie comme une échelle graduée qui commence à 25 ns et se termine au-dessus de 10 secondes ou inconnu. Plus la valeur de précision est faible, meilleure est l'horloge.
Variance	Indique la mesure des propriétés de stabilité inhérente de l'horloge locale. La valeur est en unités de décalage mises à l'échelle. Plus la variance est faible, meilleure est l'horloge.
Source	Affiche la source de temps de l'horloge locale. Les valeurs disponibles sont : <ul style="list-style-type: none"> <li>• Horloge atomique</li> <li>• GPS</li> <li>• Radio terrestre</li> <li>• PTP</li> <li>• NTP</li> <li>• Réglage manuel</li> <li>• Autres</li> <li>• Oscillator</li> </ul>

## Diagnostique de l'automate avec le logiciel de type Linx

### Concerne ces automates :

ControlLogix 5580

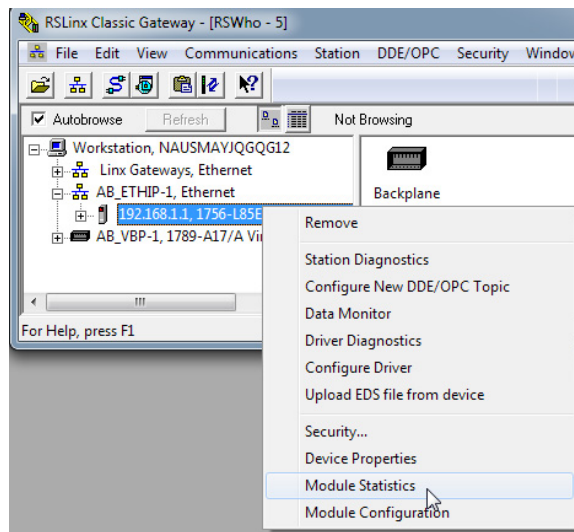
GuardLogix 5580

Vous pouvez également voir les informations de diagnostic dans le logiciel de type Linx.

1. Dans le menu Communications, choisissez RSWWho.

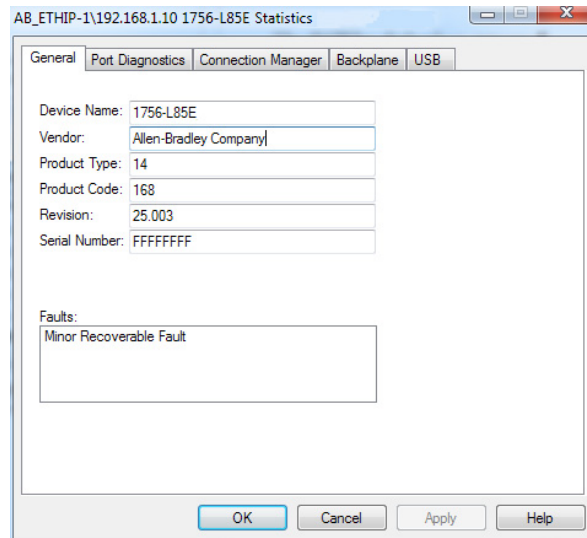
La boîte de dialogue RSWWho apparaît.

2. Naviguez jusqu'au réseau Ethernet.
3. Cliquez avec le bouton droit de la souris sur l'automate et choisissez Module Statistics.



La boîte de dialogue Module Statistics (Statistiques du module) affiche les informations suivantes :

- L'onglet Général montre des informations dispositif et n'importe quel défaut de l'automate.
- L'onglet Port Diagnostics (Diagnostics du port) montre les informations concernant le port EtherNet/IP™.
- L'onglet Connection Manager (Gestionnaire de connexion) affiche les informations sur les demandes de connexion.
- L'onglet Backplane (Fond de panier) affiche l'état général et des informations de diagnostic sur le bus intermodules ControlLogix®.
- L'onglet USB fournit des informations sur le port USB.



## Pages Internet de l'automate

Concerne ces automates :

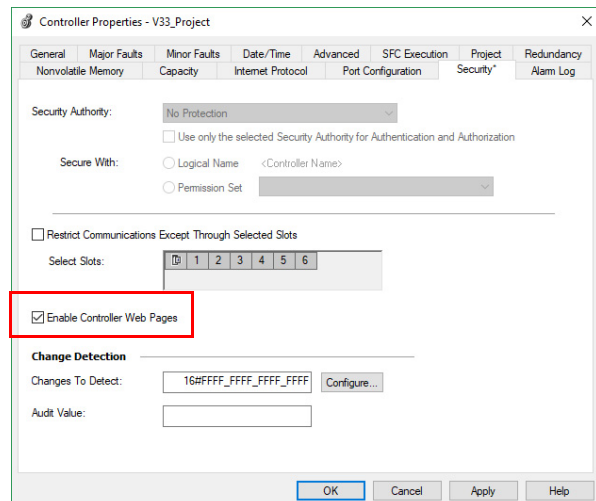
ControlLogix 5580

GuardLogix 5580

L'automate fournit des pages Internet de diagnostic pour suivre les performances de l'automate, du réseau et du bus intermodules. Les pages Internet de l'automate sont en lecture seule.

**IMPORTANT** Vous pouvez désactiver les pages Internet de l'automate avec l'application Studio 5000 Logix Designer, version 33.00.00 ou ultérieure.

- Pour activer les pages Internet de l'automate, cochez la case dans l'onglet Logix Designer Controller Properties Security (Sécurité Logix Designer des propriétés de l'automate).



- Pour les applications CIP Security, vous pouvez également utiliser FactoryTalk Policy Manager pour activer les pages Internet (cela remplace la case à cocher Propriétés de l'automate).

Pour accéder aux pages Internet de diagnostic, suivez les étapes ci-après.

1. Ouvrez votre navigateur Internet.
2. Dans le champs Address, tapez l'adresse IP de l'automate et appuyez sur Enter.

Pour accéder aux pages Internet de diagnostic, ouvrez le dossier correspondant dans la barre de navigation la plus à gauche et cliquez sur le lien de chaque page Internet que vous devez surveiller.

- La page d'accueil fournit des informations sur les dispositifs et sur l'état de l'automate.
- La page Internet Faults montre les défauts majeurs et mineurs de l'automate.
- Les pages Internet de diagnostics fournissent les données de communication et de messagerie de l'automate.
- Les pages Internet de diagnostics évolués fournissent les données concernant le réseau TCP/IP et le Precision Time Protocole.

Voir aussi :

- [Page d'accueil Internet, page 273](#)
- [Page Internet des défauts, page 274](#)
- [Page Internet des tâches, page 275](#)
- [Page Internet Parcourir le châssis, page 276](#)



## Page d'accueil Internet

Avec l'application Studio 5000 Logix Designer, version 32 ou ultérieure, la page d'accueil Internet est également montrée.

- Messages actuels de l'afficheur à 4 caractères
- État des indicateurs d'état de l'automate
- État des indicateurs d'état d'EtherNet/IP
- Signature de sécurité, état de verrouillage de sécurité, état de sécurité (pour les automates GuardLogix® 5580 et Compact GuardLogix 5380)

Pour définir le taux d'actualisation des pages Internet, saisissez le nombre de secondes dans le champ Refresh (Actualiser) en bas de la page Internet.

### Page d'accueil Internet de ControlLogix 5580

**V32\_Project** Home Allen-Bradley Rockwell Automation

Expand Minimize Home Faults (0/0) Tasks Diagnostics Browse Chassis

General Information		Resources
Device Name	1756-L85E/B_Rel_Ice2_R32_54	<a href="#">Visit AB.com for additional information</a>
Project Name	V32_Project	<a href="#">Contacts</a>
Device Description		
Device Location		
Ethernet Address (MAC)	00:1D:9C:D6:0D:65	
IP Address	192.168.1.3	
Product Revision	32.008	
Firmware Version Date	Oct 10 2018, 17:03:01	
Serial Number	00D0535	
Uptime	00h:52m:34s	

Controller Diagnostics	
Keyswitch Position	Remote
Controller Mode	Run
Change Detection Audit Value	16#D704_CEOC_8CF9_9F29
I/O Forces	Disabled - None Installed
SFC Forces	Disabled - None Installed

Status Indicators	
Controller Status	<input checked="" type="checkbox"/> Run <input type="checkbox"/> Force <input type="checkbox"/> SD <input checked="" type="checkbox"/> OK
EtherNet/IP Status	<input checked="" type="checkbox"/> Net <input checked="" type="checkbox"/> Link

4-Character Display Messages

V32\_Project  
Link 1 - 1Gb/FULL  
Port A - 192.168.1.3

Seconds Between Refresh:  Disable Refresh with 0.

Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved.

### Page d'accueil Internet de GuardLogix 5580

**V32\_Safety\_Project** Home Allen-Bradley Rockwell Automation

Expand Minimize Home Faults (0/0) Tasks Diagnostics Browse Chassis

General Information		Resources
Device Name	1756-L84E5/B_Rel_Ice2_R32_77	<a href="#">Visit AB.com for additional information</a>
Project Name	V32_Safety_Project	<a href="#">Contacts</a>
Device Description		
Device Location		
Ethernet Address (MAC)	00:1D:9C:DC:15:0D	
IP Address	192.168.1.10	
Product Revision	32.008	
Firmware Version Date	Oct 19 2018, 12:56:54	
Serial Number	0DEEFC98	
Uptime	00h:31m:18s	

Controller Diagnostics	
Keyswitch Position	Remote
Controller Mode	Run
Change Detection Audit Value	16#EECB_2753_E9A1_0882
I/O Forces	Disabled - None Installed
SFC Forces	Disabled - None Installed

Safety Controller Diagnostics	
Safety Signature	0FDEEAF0 - B680BF4 - 98A4CDE2 - SECDDA24 - 3B75E9E9 - 8E63F96F - AD12CF85 - D083CA77
Safety Locked Status	Locked
Safety Status	SIL-3 Safety Task OK

Status Indicators	
Controller Status	<input checked="" type="checkbox"/> Run <input type="checkbox"/> Force <input type="checkbox"/> SD <input checked="" type="checkbox"/> OK
EtherNet/IP Status	<input checked="" type="checkbox"/> Net <input checked="" type="checkbox"/> Link

4-Character Display Messages

V32\_Safety\_Project  
Link 1 - 1Gb/FULL  
Port A - 192.168.1.10

Seconds Between Refresh:  Disable Refresh with 0.

Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved.

## Page Internet des défauts

Avec l'application Studio 5000 Logix Designer version 32 ou ultérieure, la page Internet Défauts affiche les défauts majeurs et mineurs de l'automate.

### Page Internet Défauts de ControlLogix 5580

V32\_Project Allen-Bradley Rockwell Automation

Expand Minimize Home Faults (2/8)

Home  
Faults  
Tasks  
Diagnostics  
Browse Chassis

**Major faults (2)**

2018-10-24 12:55:30	Type 04	Program Fault (can be trapped by a fault routine)	Code 20	Array subscript too large, or CONTROL data type POS or LEN invalid.
2018-10-24 12:55:30	Type 04	Program Fault (can be trapped by a fault routine)	Code 20	Array subscript too large, or CONTROL data type POS or LEN invalid.

**Minor faults (8)**

2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.

Seconds Between Refresh:  Disable Refresh with 0.

Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved.

### Page Internet Défauts de GuardLogix 5580

V32\_Safety\_Project Allen-Bradley Rockwell Automation

Expand Minimize Home Faults (1/0)

Home  
Faults  
Tasks  
Diagnostics  
Browse Chassis

**Major Faults (1)**

1998-01-01 05:30:40	Type 14	Safety Task Fault	Code 01	Task watchdog expired. May have been caused by infinite loop, complex program, higher priority task, or removal of Safety partner.
---------------------	---------	-------------------	---------	--

**Minor faults (0)**

No faults found.

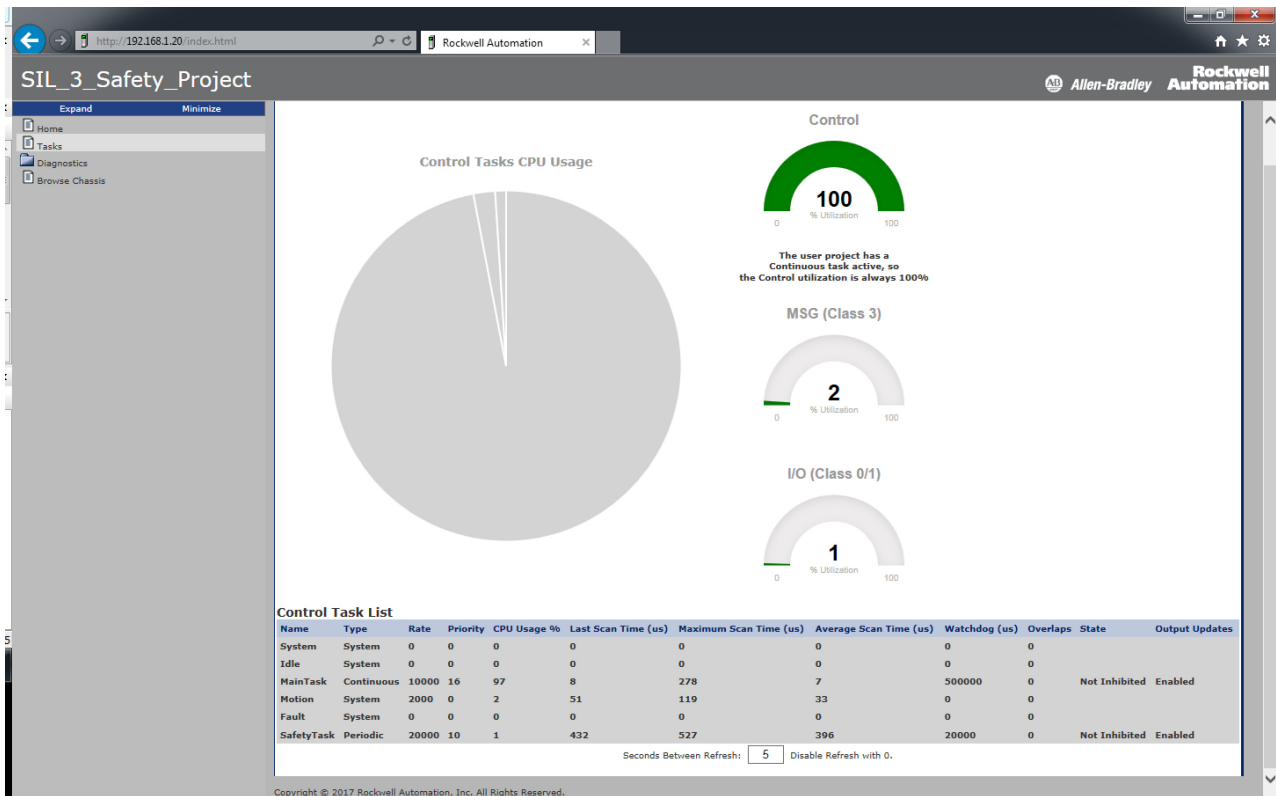
Seconds Between Refresh:  Disable Refresh with 0.

Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved.

## Page Internet des tâches

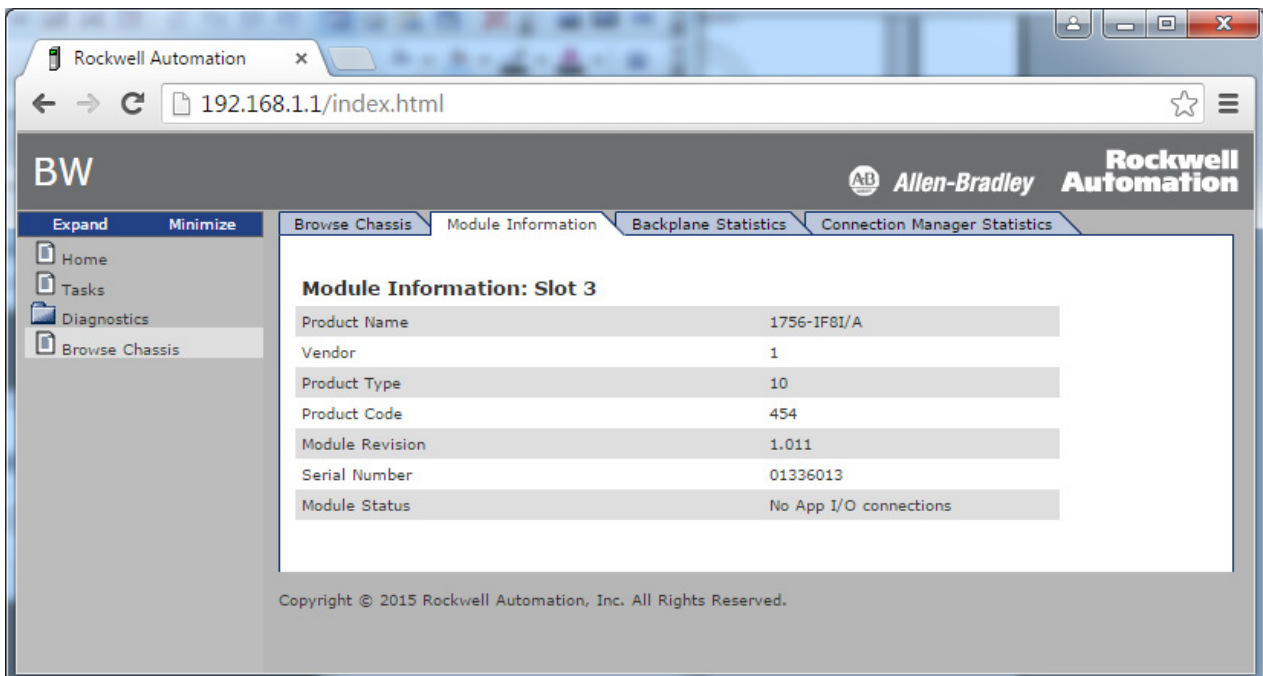
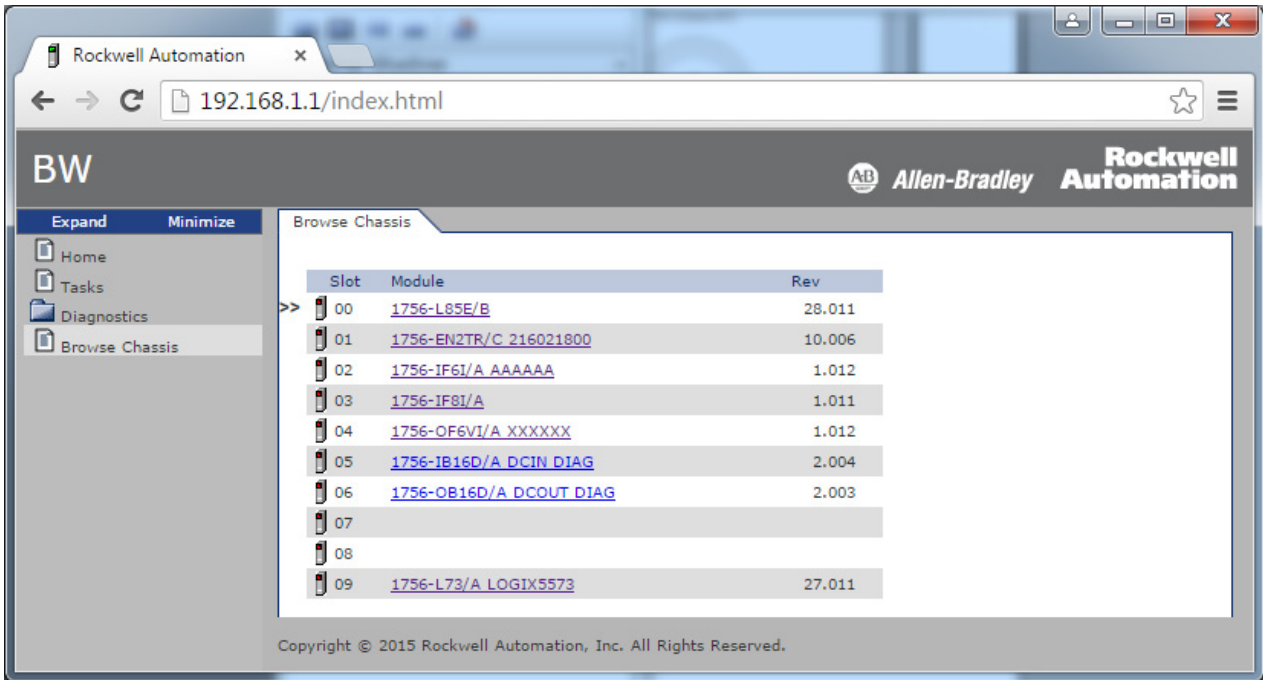
Sur la page Internet Tâches, le graphique à secteurs indique le pourcentage de l'UC du noyau de commande consommé par les tâches qui sont sur ce noyau. Les jauges montrent l'utilisation de l'UC par les noyaux de commande et de communication. Le tableau montre les tâches qui sont exécutées sur le noyau de commande (toutes les tâches système sont résumées en une seule tâche).

Cet exemple montre la page Internet Tâches d'un automate GuardLogix 5580 :



## Page Internet Parcourir le châssis

Parcourir le châssis vous permet d'afficher les informations sur les modules, les statistiques du fond de panier et les statistiques de connexion pour les modules du châssis local.

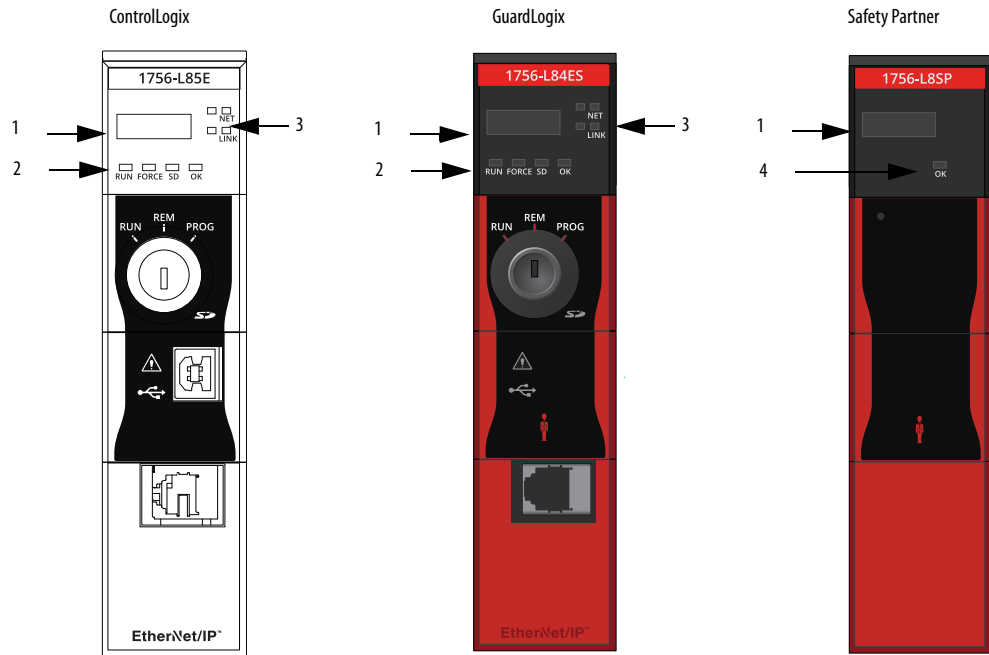


## Voyants d'état

L'automate possède six voyants d'état et un afficheur d'état défilant à quatre caractères. Le partenaire de sécurité 1756-L8SP possède un afficheur d'état défilant à 4 caractères et un voyant d'état OK.

<b>Rubrique</b>	<b>Page</b>
Afficheur et voyants d'état	278
Messages d'état général	279
Messages d'état de GuardLogix	281
Messages d'état du partenaire de sécurité	281
Messages de défaut	282
Messages de défaut majeur	283
Codes de défaut d'E/S	283
Voyants d'état d'automate	284
Voyant OK du partenaire de sécurité	286
Voyants EtherNet/IP	286
Surveillance thermique et comportement en défaut thermique	287

## Afficheur et voyants d'état



Élément	Description
1	Afficheur d'état défilant à 4 caractères Vous pouvez désactiver certains de ces messages, voir <a href="#">Désactivation de l'afficheur d'état à 4 caractères, page 243</a> .
2	Voyants d'état de l'automate, voir <a href="#">page 284</a> .
3	Voyants d'état EtherNet/IP™, voir <a href="#">page 286</a> .
4	Voyant d'état OK du partenaire de sécurité, voir <a href="#">page 286</a> .

## Messages d'état général

### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Les messages défilants qui sont décrits dans le [tableau 39](#) sont habituellement affichés à la mise sous tension et à la mise hors tension et pendant le fonctionnement de l'automate pour montrer son état.

**Tableau 39 - Messages d'état général de l'automate**

Message	Interprétation
Aucun message n'est indiqué	L'automate est hors tension Contrôler le voyant OK pour vérifier si l'automate est sous tension et déterminer l'état de l'automate.
Discordance d'identité – Contactez l'assistance technique	L'identité de ce produit a été modifiée par rapport à son état de production d'origine et l'intégrité du produit a été compromise. Cela peut être le résultat de modifications non autorisées apportées au produit ou le produit peut ne pas être un produit authentique de Rockwell Automation. Ce produit ne doit pas être mis en service.
TEST	L'automate exécute les tests à la mise sous tension.
CHRG	Le circuit de stockage d'énergie embarqué se recharge.
PASS	Les tests à la mise sous tension ont été accomplis avec succès.
Saving... Do Not Remove SD Card	L'automate est sur le point d'enregistrer une image sur la carte SD.
SAVE	Un projet est en cours d'enregistrement sur la carte SD. Vous pouvez également examiner le <a href="#">Voyant SD</a> (voir <a href="#">page 285</a> ) pour obtenir des informations d'état supplémentaires. Laissez la sauvegarde se terminer avant de : <ul style="list-style-type: none"> <li>retirer la carte SD ;</li> <li>débranchez l'alimentation.</li> </ul> <b>IMPORTANT</b> : ne retirez pas la carte SD pendant que l'automate enregistre sur la carte SD. Laissez le chargement se terminer sans l'interrompre. Si vous interrompez l'enregistrement, une corruption ou une perte de données peut se produire.
LOAD	Un projet est en cours de chargement depuis la carte SD. Vous pouvez également examiner le <a href="#">Voyant SD</a> (voir <a href="#">page 285</a> ) pour obtenir des informations d'état supplémentaires. Laissez le chargement se terminer avant de : <ul style="list-style-type: none"> <li>retirer la carte SD ;</li> <li>débranchez l'alimentation.</li> </ul> <b>IMPORTANT</b> : ne retirez pas la carte SD pendant que l'automate se charge depuis la carte SD. Laissez le chargement se dérouler sans l'interrompre. Si vous interrompez le chargement, une corruption ou une perte de données peut se produire.
UPDT	Une mise à jour du firmware est effectuée à partir de la carte SD lors de la mise sous tension. Vous pouvez également examiner le <a href="#">Voyant SD</a> (voir <a href="#">page 285</a> ) pour obtenir des informations d'état supplémentaires. Si vous ne souhaitez pas que le firmware soit mis à jour lors de la mise sous tension, modifiez la propriété Load Image (Chargement de l'image) de l'automate.
Rev. <i>XX.xxx</i>	Numéros de révision majeure et mineure du firmware de l'automate.
1756-L8XX	La référence et la série de l'automate.
Link Down	Ce message apparaît lorsqu'un port EtherNet/IP n'a pas de connexion. Le message défile continuellement pendant le fonctionnement.
Liaison désactivée	Ce message apparaît lorsque vous avez désactivé le port EtherNet/IP. Le message défile continuellement pendant le fonctionnement.
DHCP- 00:00:XX:XX:XX:XX	Le message s'affiche lorsque l'automate est réglé pour DHCP, mais n'est pas configuré sur un réseau. Le message affiche l'adresse MAC de l'automate. Le message défile continuellement en cours de fonctionnement si aucune adresse IP n'est définie.
Ethernet Port Rate/Duplex State	La vitesse de transmission du port et l'état duplex actuels lorsque le port EtherNet/IP a une connexion. Le message défile continuellement pendant le fonctionnement.
Adresse IP	L'adresse IP de l'automate. Apparaît à la mise sous tension et défile continuellement pendant le fonctionnement. Si l'adresse IP n'est pas encore définie, l'adresse MAC s'affiche.

Tableau 39 - Messages d'état général de l'automate (suite)

Message	Interprétation
Duplicate IP - 00:00:XX:XX:XX:XX	Un message apparaît lorsque l'automate détecte un dispositif sur le réseau qui a la même adresse IP que le port Ethernet de l'automate. Le message indique l'adresse MAC du dispositif avec l'adresse IP dupliquée. Le message défile continuellement pendant le fonctionnement.
No Project	Aucun projet n'est chargé dans l'automate Pour charger un projet, utilisez une des méthodes suivantes : <ul style="list-style-type: none"> <li>• utilisez l'application Studio 5000 Logix Designer<sup>®</sup> pour télécharger le projet dans l'automate ;</li> <li>• utilisez une carte SD pour charger un projet dans l'automate.</li> </ul>
Project Name	Le nom du projet chargé dans l'automate.
BUSY	Les modules d'E/S qui sont associés à l'automate ne sont pas encore entièrement alimentés. Laissez le temps à ces modules d'E/S de se mettre sous tension et d'effectuer leur auto-test.
Corrupt Certificate Received	Le certificat de sécurité associé au firmware est corrompu. Accédez à <a href="http://www.rockwellautomation.com/support/">http://www.rockwellautomation.com/support/</a> et téléchargez la révision du firmware vers laquelle vous essayez de mettre à jour. Remplacez la révision du firmware que vous avez précédemment installée par celle placée sur le site Internet de l'Assistance technique.
Corrupt Image Received	Le fichier de firmware est corrompu. Accédez à <a href="http://www.rockwellautomation.com/support/">http://www.rockwellautomation.com/support/</a> puis téléchargez la révision du firmware que vous essayez de mettre à jour. Remplacez la révision du firmware que vous avez précédemment installée par celle placée sur le site Internet de l'Assistance technique.
Backup Energy HW Failure - Save Project	Une défaillance du circuit de stockage d'énergie embarqué s'est produite et l'automate est incapable de sauvegarder le programme en cas de panne de courant. Si vous voyez ce message, enregistrez votre programme sur la carte SD avant de couper l'alimentation et de remplacer l'automate.
Backup Energy Low - (Énergie de sauvegarde basse) Enregistrez le projet	Le circuit de stockage embarqué n'a pas suffisamment d'énergie pour permettre à l'automate de sauvegarder le programme en cas de panne de courant. Si vous voyez ce message, enregistrez votre programme sur la carte SD avant de couper l'alimentation et de remplacer l'automate.
Flash in Progress	Une mise à niveau de firmware initié via les utilitaires ControlFLASH Plus <sup>™</sup> , ControlFLASH <sup>™</sup> ou AutoFlash, est en cours. Laissez la mise à jour du firmware se dérouler sans l'interrompre.
Firmware Installation Required	L'automate utilise le firmware d'amorçage, c'est-à-dire, la révision 1.xxx, et nécessite une mise à jour de firmware.
SD Card Locked	Une carte SD verrouillée est installée.
Download in Progress	Un téléchargement actif est en cours.
Aborting Download	Un téléchargement actif est en train d'être abandonné. Il peut s'agir d'une annulation exécutée par un utilisateur, d'un échec du téléchargement ou d'une perte de connexion. Une fois terminé, le message d'état No Project (Aucun projet) s'affiche.



## Messages d'état de GuardLogix

### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

En plus des messages d'état général du [tableau 39](#), un afficheur d'automate GuardLogix® 5580 peut afficher ces messages défilants.

**Tableau 40 - Messages d'état d'automate de sécurité**

Message	Interprétation
No Safety Signature	La tâche de sécurité est en mode Exécution sans signature de sécurité. Générez une signature de sécurité.
Safety Unlocked	L'automate est en mode Exécution avec une signature de sécurité, mais la sécurité n'est pas verrouillée. Verrouillez la sécurité de l'automate.
Safety Partner Missing	Le partenaire de sécurité est manquant ou indisponible. Assurez-vous que le partenaire de sécurité est correctement installé dans le logement qui se trouve immédiatement à droite de l'automate de sécurité. L'automate affiche ce message uniquement dans une configuration SIL 3/PLe.
Hardware Incompatible	Le matériel du partenaire de sécurité est incompatible avec l'automate principal. Avec les automates GuardLogix 5580, vous devez utiliser le partenaire de sécurité 1756-L8SP. L'automate affiche ce message uniquement dans une configuration SIL 3/PLe.
Firmware incompatible.	Les niveaux de révision de firmware du partenaire de sécurité et de l'automate principal sont incompatibles. Mettez les modules à jour avec la révision de firmware correcte. L'automate affiche ce message uniquement dans une configuration SIL 3/PLe.
Tâche de sécurité inexploitable.	Le programme logique de sécurité est incorrect. Par exemple, une discordance s'est produite entre l'automate principal et le partenaire de sécurité, un timeout du chien de garde s'est produit ou la mémoire est corrompue.

## Messages d'état du partenaire de sécurité

### Concerne ces automates :

GuardLogix 5580

L'afficheur du partenaire de sécurité peut afficher ces messages défilants.

**Tableau 41 - Messages d'état du partenaire de sécurité**

Message	Interprétation
L8SP	Texte affiché standard S'il y a un défaut majeur irrécupérable, le code de défaut défile sur l'afficheur.
Flash in Progress	Une mise à niveau de firmware initié via les utilitaires ControlFLASH Plus, ControlFLASH ou AutoFlash, est en cours. Laissez la mise à jour du firmware se dérouler sans l'interrompre.

## Messages de défaut

### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Si l'automate affiche un défaut, ces messages défilant peuvent apparaître sur l'afficheur d'état.

**Tableau 42 - Messages de défaut**

Message	Interprétation
Message de défaut majeur T:XX:CY	<p>Un défaut majeur de Type <i>XX</i> et Code <i>XX</i> a été détecté.</p> <p>Par exemple, si l'afficheur d'état indique MajorFault T04:C42 Invalid JMP Target, une instruction JMP est programmée pour sauter à une instruction LBL incorrecte.</p> <p>Pour les détails concernant les défauts majeurs récupérables, consultez la publication <a href="#">1756-PM014</a>, « Logix 5000™ Major, Minor, and I/O Fault Codes Programming Manual ».</p>
Message de défaut d'E/S local: X#XXXX	<p>Un défaut d'E/S s'est produit sur un module du châssis local. Le numéro de logement et le code de défaut sont indiqués avec une brève description.</p> <p>Par exemple, I/O Fault Local:3 #0107 Connection Not Found indique qu'une connexion vers le module d'E/S local dans le logement trois n'est pas ouverte.</p> <p>Prenez une action corrective spécifique au type de défaut indiqué.</p> <p>Pour les détails concernant chaque défaut d'E/S, consultez la publication <a href="#">1756-PM014</a>, « Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual ».</p>
Message de défaut d'E/S <i>ModuleName</i> #XXXX	<p>Un défaut d'E/S s'est produit sur un module dans un châssis décentralisé. Le nom du module en défaut est indiqué avec le code de défaut et une brève description du défaut.</p> <p>Par exemple, I/O Fault My_Module #0107 Connection Not Found indique qu'une connexion à un module dénommé My_Module n'est pas ouverte.</p> <p>Prenez une action corrective spécifique au type de défaut indiqué.</p> <p>Pour les détails concernant chaque défaut d'E/S, consultez la publication <a href="#">1756-PM014</a>, « Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual ».</p>
Message de défaut d'E/S <i>ModuleParent.X</i> #XXXX	<p>Un défaut d'E/S s'est produit sur un module dans un châssis décentralisé. Le nom de parent du module est indiqué car aucun nom de module n'est configuré dans l'arborescence de configuration des E/S de l'application Logix Designer. De plus, le code de défaut est indiqué par une brève description du défaut.</p> <p>Par exemple, « I/O Fault My_CNet:3 #0107 Connection Not Found » indique que la connexion avec un module situé dans le logement numéro 3 du châssis et associé au module de communication nommé « My_CNet » n'est pas établie.</p> <p>Prenez une action corrective spécifique au type de défaut indiqué.</p> <p>Pour les détails concernant chaque défaut d'E/S, consultez la publication <a href="#">1756-PM014</a>, « Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual ».</p>
XDéfauts d'E/S	<p>Des défauts d'E/S sont présents et <i>X</i> = le nombre de défauts d'E/S présents.</p> <p>S'il y a de multiples défauts d'E/S, l'automate indique le premier défaut signalé. À mesure que chaque défaut d'E/S est résolu, le nombre de défauts indiqués diminue et le message d'erreur d'E/S indique le prochain défaut déclaré.</p> <p>Prenez une action corrective spécifique au type de défaut indiqué.</p> <p>Pour les détails concernant chaque défaut d'E/S, consultez la publication <a href="#">1756-PM014</a>, « Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual ».</p>

## Messages de défaut majeur

### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Le message de défaut majeur *T.XX:C.XX* sur l'afficheur défilant de l'automate indique les défauts majeurs.



Ce manuel renvoie à l'article de la base de connaissance [Logix 5000 Controller Fault Codes](#) pour les codes de défaut. Vous pouvez télécharger la feuille de calcul de cet article public.

Il vous sera demandé de vous connecter à votre compte Internet Rockwell Automation ou de créer un compte si vous n'en avez pas. Vous n'avez pas besoin d'un contrat d'assistance pour accéder à cet article.

Pour les méthodes de récupération préconisées des défauts majeurs, consultez la publication [1756-PM014](#), « Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual ».

## Codes de défaut d'E/S

### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

L'automate indique les défauts d'E/S sur l'afficheur d'état dans l'un des formats suivants :

- Défaut d'E/S local : message *X#XXXX*
- Défaut d'E/S : message *ModuleName#XXXX*
- Défaut d'E/S : message *ModuleParent.X#XXXX*

La première partie du format est utilisée pour indiquer l'emplacement du module en défaut. Comment l'emplacement est indiqué dépend de votre configuration d'E/S et des propriétés du module qui sont spécifiées dans l'application Logix Designer.

La dernière partie du format, *#XXXX* message, peut être utilisée pour diagnostiquer le type de défaut d'E/S et les actions correctives potentielles.



Pour les codes de défaut, ce manuel renvoie à l'article de la base de connaissance [Logix 5000 Controller Fault Codes](#). Vous pouvez télécharger la feuille de calcul de cet article public.

Il vous sera demandé de vous connecter à votre compte Internet Rockwell Automation ou de créer un compte si vous n'en avez pas. Vous n'avez pas besoin d'un contrat d'assistance pour accéder à cet article.

Pour les descriptions détaillées et les méthodes de récupération préconisées pour les défauts d'E/S, consultez la publication [1756-PM014](#), « Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual ».

## Voyants d'état d'automate

### Concerne ces automates :

ControlLogix 5580

GuardLogix 5580

Les voyants d'état sont situés en dessous de l'afficheur d'état de l'automate. Ils indiquent l'état de l'automate décrit dans ces tableaux.

### IMPORTANT Considérations relatives à la sécurité

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

## Voyant RUN

Le voyant RUN montre le mode actuel de l'automate.

Pour changer le mode de l'automate, vous pouvez utiliser le sélecteur à clé en face avant de l'automate ou le menu Controller Status (État de l'automate) dans l'application Logix Designer.

**Tableau 43 - Voyant RUN (Exécution)**

État	Description
Éteint	L'automate est en mode Programmation ou Test.
Vert fixe	Le module est en mode Exécution.

## Voyant FORCE

Le voyant Force indique si des forçages d'E/S sont activés sur l'automate.

**Tableau 44 - Voyant FORCE**

État	Description
Éteint	Aucuns points ne contient de valeurs de forçage d'E/S, et les valeurs de forçage d'E/S ne sont pas activées.
Orange fixe	Des forçages d'E/S sont activés. Si des valeurs de forçage d'E/S existent, elles sont actives. <b>IMPORTANT</b> : soyez prudent si vous modifiez des valeurs de forçage. Dans cet état, les changements prennent effet immédiatement.
Ambre clignotant	Des forçages d'E/S existent dans l'application, mais ne sont pas actifs parce que les forçages d'E/S ne sont pas activés. <b>IMPORTANT</b> : soyez prudent si vous activez des forçages d'E/S. Toutes les valeurs de forçage d'E/S existantes prennent effet immédiatement.

## Voyant SD

Le voyant SD montre si la carte SD est utilisée.

**Tableau 45 - Voyant SD**

État	Description
Éteint	Aucune activité ne se produit avec la carte SD.
Vert clignotant	L'automate lit ou écrit sur la carte SD.
Vert fixe	<b>IMPORTANT</b> : ne retirez pas la carte SD lorsque l'automate est en train de lire ou écrire. Laissez la lecture/écriture se terminer sans interruption. Si vous interrompez la lecture/écriture, une corruption ou une perte de données peut se produire.
Rouge clignotant	Le système de fichier de la carte SD est incorrect.
Rouge fixe	L'automate ne reconnaît pas la carte SD.

## Voyant OK

Le voyant OK montre l'état de l'automate.

**Tableau 46 - Voyant OK des automates ControlLogix® et GuardLogix**

État	Description
Éteint	Aucune tension n'est appliquée à l'automate.
Rouge clignotant	L'une ou l'autre de ces explications est possible : <ul style="list-style-type: none"> <li>Il s'agit d'un nouvel automate, tout juste déballé, qui requiert une mise à jour du firmware. Si une mise à jour du firmware est nécessaire, l'afficheur d'état indique Firmware Installation Required (installation du firmware nécessaire). Pour mettre à jour le firmware, consultez <a href="#">Mise à jour du firmware de l'automate, page 54</a>.</li> <li>Il s'agit d'un automate déjà été utilisé précédemment ou encore en cours d'utilisation et un défaut majeur s'est produit. Toutes les tâches utilisateur standard et de sécurité sont arrêtées.</li> <li>Pour plus de détails sur les défauts majeurs récupérables et irrécupérables, reportez-vous à la publication <a href="#">1756-PM014</a>, « Logix5000 Major, Minor, and I/O Fault Codes Programming Manual ».</li> </ul>
Rouge fixe	L'une ou l'autre de ces explications est possible : <ul style="list-style-type: none"> <li>L'automate exécute les diagnostics à la mise sous tension.</li> <li>La charge du condensateur du module ESM est en cours d'épuisement suite à une coupure d'alimentation.</li> <li>L'automate est alimenté, mais il est inutilisable.</li> <li>L'automate est en train de charger un projet dans la mémoire non volatile.</li> <li>L'automate subit un défaut de préservation du matériel en raison d'une température interne élevée du module. Dans cette condition, seul le voyant d'état est alimenté. Une fois que l'automate est refroidi à une température acceptable, la pleine puissance est appliquée.</li> </ul>
Vert fixe	L'automate fonctionne normalement.

## Voyant OK du partenaire de sécurité

<b>Concerne ces automates :</b>
GuardLogix 5580

Le partenaire de sécurité possède un voyant d'état OK.

**Tableau 47 - Voyant OK du partenaire de sécurité 1756-L8SP**

État	Description
Éteint	L'alimentation n'est pas appliquée.
Vert	Le partenaire de sécurité fonctionne sans défauts.
Rouge	L'une ou l'autre de ces explications est possible : <ul style="list-style-type: none"> <li>Le partenaire de sécurité termine ses diagnostics à la mise sous tension.</li> <li>La charge du condensateur du module ESM est en cours d'épuisement suite à une coupure d'alimentation.</li> <li>Le partenaire de sécurité est sous tension, mais inexploitable.</li> <li>Le partenaire de sécurité est en train de charger un projet en mémoire non volatile.</li> <li>Le partenaire de sécurité subit un défaut de préservation du matériel en raison d'une température interne élevée du module. Dans cette condition, seul le voyant d'état est alimenté. Une fois que le partenaire de sécurité a refroidi à une température acceptable, la pleine puissance est appliquée.</li> </ul>
Rouge clignotant	L'automate est configuré pour un fonctionnement SIL 2 mais un partenaire de sécurité est installé.

## Voyants EtherNet/IP

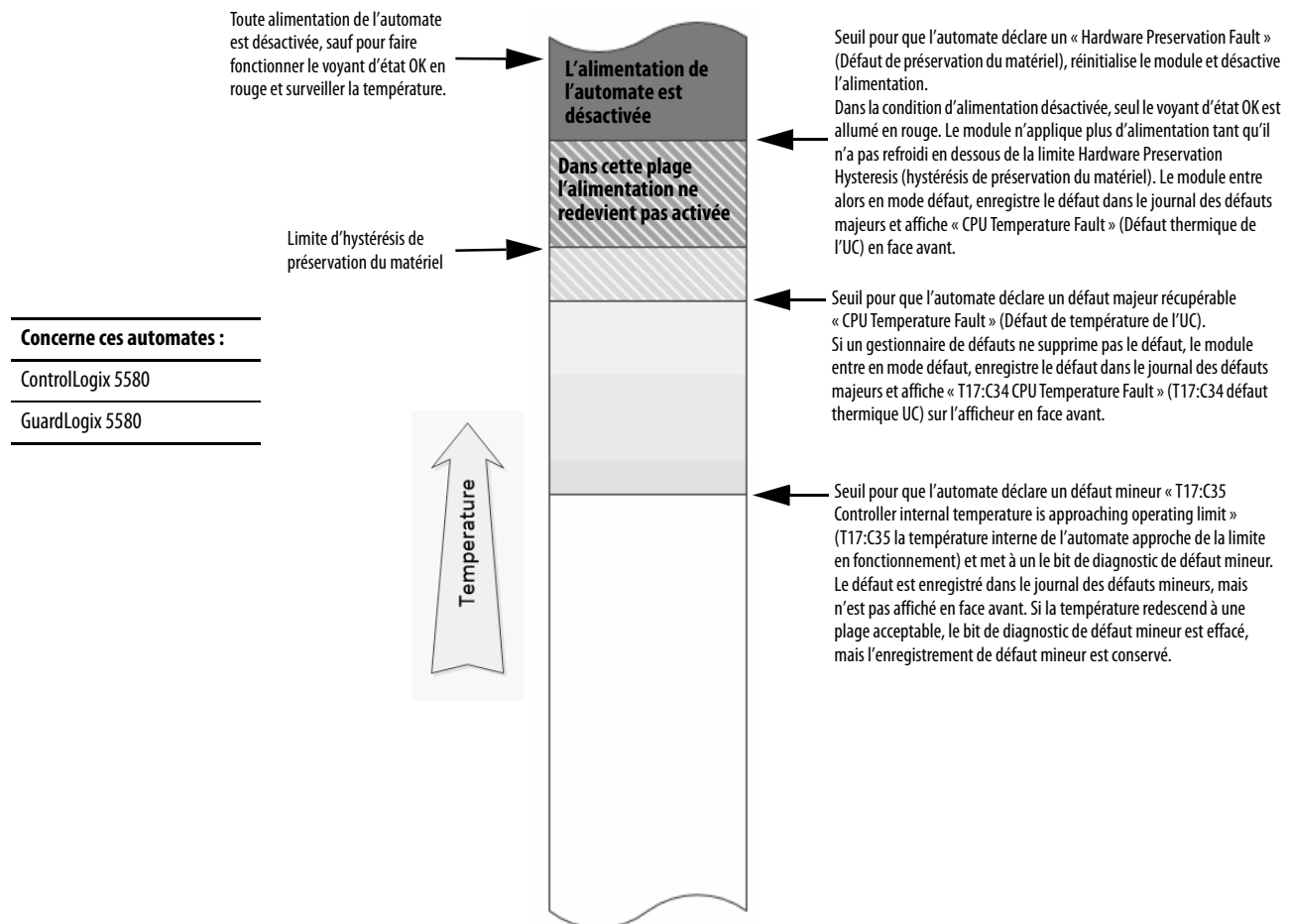
<b>Concerne ces automates :</b>
ControlLogix 5580
GuardLogix 5580

Les voyants EtherNet/IP montrent l'état du port EtherNet/IP et l'activité de communications.

Voyant	État	Description
NET	Éteint	<ul style="list-style-type: none"> <li>L'automate n'est pas configuré ou n'a pas d'adresse IP.</li> <li>Le port est administrativement désactivé.</li> </ul>
	Vert clignotant	L'automate possède une adresse IP, mais aucune connexions actives ne sont établies.
	Vert fixe	L'automate possède une adresse IP et au moins une connexion active est établie.
	Rouge fixe	Adresse IP dupliquée ou configuration incorrecte.
LINK	Éteint	Pas d'activité. L'une des conditions suivantes existe : <ul style="list-style-type: none"> <li>Aucune liaison n'existe sur le port.</li> <li>Vérifiez que les câbles RJ45 sont correctement installés dans l'adaptateur et les équipements connectés.</li> <li>Le port est administrativement désactivé.</li> </ul>
	Vert clignotant	Activité présente sur le port.

## Surveillance thermique et comportement en défaut thermique

Les automates peuvent surveiller les températures internes du module et prendre des mesures lorsque la température augmente, comme dans cette illustration.



**IMPORTANT** Si vous suivez les limites recommandées pour la température ambiante (entrante) et appliquez les distances requises autour du système, il est peu probable que l'automate atteigne la température d'avertissement initial (défaut mineur). Consultez la publication [1756-TD001](#), « 1756 ControlLogix Controllers Technical Data ».

**IMPORTANT** La présence d'un avertissement de température quelconque indique que des mesures doivent être prises pour réduire la température ambiante du module.

Les instructions pour l'utilisation d'un programme en logique à relais pour rechercher un défaut mineur peuvent être trouvées dans la publication [1756-TD001](#), « Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual ».

Vous pouvez utiliser une instruction GSV pour lire l'attribut MinorFaultBits du nom de classe FaultLog. Si le bit de diagnostics de défaut mineur (Bit 17) est à un, un défaut mineur de température peut être présent. Vérifiez l'onglet Minor Faults (Défauts mineurs) de la boîte de dialogue Controller Properties (Propriétés de l'automate) dans l'application Logix Designer pour voir si le défaut mineur est un avertissement de température.

**Notes :**



## Changement de type d'automate

Rubrique	Page
Passage d'un automate standard à un automate de sécurité	289
Passage d'un automate de sécurité à un automate standard	290
Changement du type d'automate de sécurité	290

Les automates de sécurité ont des exigences spécifiques et ne prennent pas en charge certaines fonctions standard. Il est donc important de bien comprendre les incidences sur le comportement du système d'une modification du type de l'automate de standard à sécurité (ou de sécurité à standard) dans un projet automate.

Changer le type de l'automate affecte en effet :

- les fonctionnalités prises en charge ;
- la configuration physique du projet (partenaire de sécurité et E/S de sécurité) ;
- les propriétés de l'automate ;
- les éléments du projet, comme les tâches, les programmes, les sous-programmes et les points ;
- les instructions complémentaires de sécurité.

### Passage d'un automate standard à un automate de sécurité

S'applique à ces automates :

ControlLogix 5580

GuardLogix 5580

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 :

- La tâche de sécurité n'est créée que si le nombre maximal de tâches téléchargeables n'est pas atteint. La tâche de sécurité est initialisée avec ses valeurs par défaut.

**CONSEIL** Si votre projet contient déjà 32 tâches, et que vous tentez de passer d'un automate standard à un automate de sécurité, le projet n'est pas converti et reste rattaché à l'automate standard.

- Les composants de sécurité sont créés (c'est-à-dire la tâche de sécurité, le programme de sécurité, etc.).
- Le projet de sécurité prend par défaut le niveau de sécurité SIL 2/PLd.
- Un numéro de réseau de sécurité (SNN) temporel est généré pour le châssis local.
- Un numéro de réseau de sécurité temporel (SNN) est également généré pour le port EtherNet/IP™ embarqué.

- Toutes les fonctionnalités 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

### S'applique à ces automates :

ControlLogix 5580

GuardLogix 5580

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 :

- Le partenaire de sécurité est supprimé du châssis des E/S, le cas échéant.
- Les dispositifs d'E/S de sécurité et leurs points sont supprimés.
- La tâche, les programmes et les sous-programmes de sécurité sont modifiés en tâche, programmes et sous-programmes standard.
- Tous les points de sécurité, à l'exception de ceux consommés, sont transformés en points standard. Les points de sécurité consommés sont supprimés.
- Les mappages de points de sécurité sont supprimés.
- Les numéros de réseau de sécurité (SNN) sont supprimés.
- Les mots de passe de verrouillage et de déverrouillage de la sécurité sont supprimés.
- Si l'automate standard prend en charge des fonctionnalités qui n'étaient pas disponibles dans l'automate de sécurité, ces nouvelles fonctionnalités 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 produire des erreurs de vérification.
- Les points consommés sont supprimés lorsque le module producteur est supprimé.
- Suite aux modifications ci-dessus 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 du type 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 d'E/S qui ne sont plus compatibles avec l'automate cible sont supprimés.

La représentation du partenaire de sécurité est mise à jour de façon à apparaître convenablement pour l'automate cible :

## Nombres

- 10/100/1000** 51
- 1756-CN2**
  - utilisations 41
- 1756-CN2R**
  - utilisations 41
- 1756-CN2RXT**
  - utilisations 41
- 1756-CNB**
  - utilisations 41
- 1756-CNBR**
  - utilisations 41
- 1756-DHRIO** 43
  - communication via 44
  - utilisations
    - E/S décentralisées 45
- 1756-DHRIOXT**
  - utilisation 45
  - utilisations 43
- 1756-DNB**
  - utilisations 43
- 1756-EN2F**
  - utilisations 38
- 1756-EN2T**
  - utilisations 38
- 1756-EN2TR**
  - utilisations 38
- 1756-EN2TRXT**
  - utilisations 38
- 1756-EN2TSC**
  - utilisations 38
- 1756-EN2TXT**
  - utilisations 38
- 1756-EN3TR**
  - utilisations 38
- 1756-ENBT**
  - utilisations 38
- 1756-EWEB**
  - utilisations 38
- 1756-IF8H**
  - utilisations 49
- 1756-N2** 123
- 1756-N2XT** 123
- 1756-RIO**
  - utilisations 45
- 1784-SD1**
  - chargement depuis 103
- 1784-SD2**
  - chargement depuis 103
- 1788-CN2DN**
  - utilisations 43
- 1788-CN2FFR**
  - utilisations 48
- 1788-EN2DNR**
  - utilisations 43
- 1788-EN2FFR**
  - utilisations 48

## A

- accès externe** 186
- activation de la protection sous licence** 228
- adresses IP**
  - détection d'adresse dupliquée 52
- adressage DNS** 53
- adresse de station** 139
- adresse IP dupliquée**
  - détection 52
  - résolution 53
- adresse réseau**
  - adressage DNS 53
- adresses IP**
  - résolution d'adresse dupliquée 53
- affichage**
  - état de la sécurité 77
- ajout**
  - E/S décentralisées 129, 131
  - E/S locale 123
- application**
  - éléments 164
  - réseaux et 33
- application Logix Designer**
  - instructions complémentaires 174
  - points 172
  - programme 168
  - sous-programme 171
  - tâches 165
- applications sécurisées** 217
  - configuration du logement sécurisé 224
  - configurer changer la détection
    - valeur d'audit 231
  - configurer modifier la détection 230
    - modifications de la détection 230
  - défauts majeurs définissables par
    - l'utilisateur 225
  - désactivation de l'afficheur d'état à 4
    - caractères 243
  - désactivation des pages Internet de
    - l'automate 247
  - désactivation du port Ethernet 232
    - sous l'onglet configuration
      - du port 233
  - désactiver la carte SD 241
  - désactiver le port Ethernet
    - avec une instruction MSG 234
  - désactiver le port USB 239
  - désactiver les ports CIP Security 236
  - journal d'audit de l'automate 231
  - protection de la source et de l'exécution
    - basée sur licence 227
  - protection sous licence de la source et de
    - l'exécution
      - activation de la protection
        - sous licence 228
  - sécurité au niveau système 219
  - sécurité de l'automate 218
  - sécurité niveau système
    - durcir le système de commande 219
    - gérer l'accès utilisateur par programmation 220

- surveiller le système
    - de commande 219
  - sécurité spécifique à l'automate 221
    - durcir le système de commande 221
    - gérer l'accès physique de l'utilisateur à l'automate 223
    - surveillance du système de commande 222
  - vérification de la mise en œuvre de la sécurité 223
  - arrêt sécurisé du couple**
    - configurations
      - intégré 20, 21
  - AutoFlash**
    - mise à jour 58
  - automate**
    - changement de type 289
    - chemin de communication
      - définir 73
    - comportement 110
    - conception système avec 22
    - ControlLogix 5580
      - options communication 23
      - options de communication 24
    - correspondance 76
    - discordance des numéros de série 81
    - discordance du numéro de série 78
    - enregistrement
      - signature de sécurité 204
      - verrouillage, déverrouillage de la sécurité 200
    - firmware 54
      - obtention 57
    - gestionnaire de défaut 215
    - mode de fonctionnement
      - changer avec le sélecteur à clé 86
      - changer avec Logix Designer 88
    - modes disponibles 85
    - numéro de série 76
    - passer en ligne 73
    - points 172
    - programme 168
    - références
      - automates à revêtement enrobant 13
      - automates de sécurité 13
      - automates standard 13
    - sous-programme 171
    - surveillance
      - connexions 178
    - tâches 165
    - transfert d'un projet 82
    - voyants d'état 284
  - Automate de process ControlLogix 5580 15**
  - automate de sécurité homologue**
    - emplacement 189
    - partage de données 188
    - SNN 189
  - automate principal**
    - description 19
  - automates à revêtement enrobant 13**
  - Automates ControlLogix redondants 15**
  - Automates ControlLogix sans énergie stockée (NSE) 14**
  - Automates ControlLogix-XT 14**
  - automates de process 15**
  - Automates NSE 14**
  - axe**
    - obtenir les informations 257
  - axes**
    - consommés 254
    - virtuels 254
- ## B
- barre en ligne 206**
  - bit ConnectionFaulted 209**
  - bit RunMode 209**
  - bloque la communication 110**
  - bouton de réinitialisation 89**
    - réinitialisation de type 1 90
    - réinitialisation de type 2 91
    - réinitialisation du partenaire de sécurité 93
- ## C
- cache**
    - messages
      - à propos 114
      - options message 115
  - cache de logement**
    - logement, cache 123
  - caractéristiques 10, 22, 287**
  - carte mémoire 98**
    - autres tâches 106
    - chargement depuis 103
  - carte SD 26**
    - désactiver 241
  - Carte Secure Digital (SD) 26, 98**
  - carte Secure Digital (SD)**
    - autres tâches 106
    - chargement depuis 103
    - désactiver 241
  - changement des automates 290**
  - chargement**
    - depuis la carte mémoire 103
  - chargement d'un projet**
    - à la mise sous tension 99
    - lancement par l'utilisateur 99
    - sur corruption de la mémoire 99
  - châssis**
    - ControlLogix
      - liste 123
  - chemin**
    - définir
      - communication 73
  - choix**
    - E/S 121
  - CIP Safety 31, 161**
  - code de défaut**
    - afficheur d'état 214
    - utiliser GSV pour obtenir 179
  - codes de défaut**
    - défauts de sécurité majeurs 214

- commande d'axe intégrée**
    - en réseau EtherNet/IP 23, 24
  - commande de mouvement**
    - à propos 254
    - application 253
  - communication**
    - bloque 110
    - chemin
      - définir 73
    - Data Highway Plus 43, 44
    - E/S décentralisées universelles 45
    - Foundation Fieldbus 48
    - HART 49
    - options réseau 23, 24
    - permet 110
  - communication restreinte**
    - configurer le logement sécurisé 224
  - comportement**
    - défaut thermique 287
  - conception**
    - système 22
  - condition d'origine** 155
  - condition d'origine**
    - réinitialisation de module 151
  - configuration**
    - commande de mouvement 254
  - configuration d'E/S**
    - ajout
      - E/S décentralisées 129
      - E/S locale 123
  - configuration de logement sécurisé**
    - logements sélectionnés 224
  - configuration des E/S**
    - ajout
      - E/S décentralisées 131
      - étant en ligne 135
  - configuration du logement sécurisé** 224
  - configurer changer la détection**
    - valeur d'audit 231
  - configurer modifier la détection** 230
    - modifications de la détection 230
  - configurer un logement sécurisé**
    - communication restreinte 224
  - CONNECTION\_STATUS** 188, 209
  - connexion**
    - DeviceNet
      - réseau 43
    - état 209
    - EtherNet/IP 108
    - message, requis 114
    - non prioritaire
      - ControlNet 113
    - prioritaire
      - ControlNet 113
  - connexion de données seules** 150
  - consommation de données de point** 194
  - consommer**
    - des données 112
  - ControlLogix**
    - cache de logement 123
    - châssis
      - liste 123
    - conception système 22
    - E/S
      - choix 121
      - décentralisées 128
    - E/S décentralisées
      - local 123
  - ControlLogix-XT**
    - châssis
      - liste 123
  - ControlNet**
    - connexion non prioritaire
      - connexion non prioritaire 113
    - connexion prioritaire
      - connexion prioritaire 113
    - exemple 40
    - module 40
    - réseau 39
  - copier**
    - signature de sécurité 204
  - correspondance projet/automate** 76
  - créer un sous-programme de défaut** 225
- D**
- Data Highway Plus** 43
  - DDR (débit de données double)** 38
  - décentralisées**
    - E/S 128
  - défaut**
    - d'automate irrécupérable 212
    - effacer 213
    - préservation du matériel 287
    - recupérable 213, 287
    - sécurité irrécupérable 208, 212
    - sous-programmes 215
    - température de l'UC 287
  - défaut d'automate irrécupérable** 212
  - défaut de sécurité irrécupérable** 208, 212
  - défaut de sécurité irrécupérable**
    - démarrage de la tâche de sécurité 213
  - défaut récupérable** 213
    - effacer 213
  - défauts de sécurité majeurs** 214
  - défauts majeurs définissables par l'utilisateur** 225
    - créer un sous-programme de défaut 225
    - saut au sous-programme de défaut 226
    - utilisation d'un sous-programme de défaut 226
  - délai réseau maximum observé**
    - réinitialisation 195
  - désactivation de l'afficheur d'état à 4 caractères** 243
  - désactivation des pages Internet de l'automate** 247
  - désactivation des ports CIP Security** 236
  - Désactivation du port Ethernet** 92
    - avec une instruction MSG 234
  - désactivation du port Ethernet** 232
    - sous l'onglet configuration du port 233

**désactivation du port USB** 239  
**désactiver la carte SD** 241  
**détecter les modifications de l'automate** 230  
**détrompage électronique**  
à propos 122  
**développement**  
applications 163  
applications de commande  
de mouvement 253  
**déverrouillage de l'automate** 201  
**DeviceNet**  
réseau 42  
utilisation de la connexion 43  
**DH+** 43  
**diagnostics**  
avec le logiciel RSLinx 270  
avec Logix Designer 261  
catégorie configuration de port 265  
catégorie synchro temporelle 267  
**diagnostics automatiques** 259  
**diagnostics de port** 265  
**données de commande** 110  
**données standard dans un sous-programme  
de sécurité** 197  
**durcir le système de commande** 219, 221

## E

**E/S**  
codes 283  
ControlLogix  
choix 121  
décentralisées 128  
décentralisées 128  
déterminer la mise à jour des données 136  
**E/S CIP Safet**  
ajout 139  
**E/S CIP Safety**  
adresse de station 139  
**E/S décentralisées** 43  
ajout 129, 131  
ControlLogix  
local 123  
universelles 45  
**E/S décentralisées universelles** 45  
communication via 47  
**effacer**  
défauts 213  
**éléments**  
application de commande 164  
**en ligne**  
ajout  
à la configuration des E/S 135  
passer 73  
**enregistrement d'un projet** 97  
**envoi**  
messages 114  
**établissement de liaison** 110  
**état**  
messages 281

affichage 279  
messages de défaut 282  
partenaire de sécurité 208  
surveillance  
connexions 178  
voyants 284  
**état de la sécurité**  
affichage 77, 206, 208  
bouton 203, 207  
effet sur le téléchargement 77  
restrictions de programmation 205  
signature de sécurité 203

## état du réseau

voyant 156, 158

## Ethernet 51

vitesses de liaison 34

## EtherNet/IP

connexions 108  
réseau 34  
stations 108

## exigences minimales 13

## F

### firmware

automate 54  
mise à jour avec AutoFlash, usage 58  
obtention 57  
requis 56

### fonctionnalités 23

automate  
communication 23  
programmation 23

### forçage 204

### Foundation Fieldbus 48

## G

### gérer l'accès physique de l'utilisateur à l'automate 223

### gérer l'accès utilisateur par programmation 220

### GSV

code de défaut 179  
surveillance  
connexion 178

## H

### HART. Voir Highway Addressable Remote Transducer.

### Highway Addressable Remote Transducer 49

## I

### indicateur 284

### instruction

mouvement 255

### Instructions complémentaires 25, 290

**instructions complémentaires**

dans un projet 174

**intervalle entre trames requis** 188

point consommé 195

**J****journal d'audit de l'automate** 231**K****kit de mise à niveau du firmware** 76**L****langages de programmation** 173**Limite de temps de réponse****de la connexion** 195**local**

E/S

ajout 123

E/S décentralisées 123

**logiciel**

restrictions 205

**logiciel ControlFLASH** 57, 76**Logiciel ControlFLASH Plus** 57**logiciel ControlFLASH Plus** 57, 76**logiciel RSLinx**

diagnostics automate 270

**logiciel RSLogix 5000**

restrictions 205

**Logix Designer**changer le mode de fonctionnement de  
l'automate 88**M****MajorFaultRecord** 216**mémoire non volatile**

onglet 96

**message**

à propos 114

affichage d'état 279

cache 115

déterminer si 115

défaut 282

**messages**

état de sécurité 281

**messages d'état général** 279**messages de défaut** 282

E/S 283

**mise à jour**

déterminer la fréquence 136

**mise à jour firmware**

AutoFlash, usage 58

**Mode STO intégré** 20**mode STO intégré** 21**modification** 204**mot de passe**

définir 64, 202

**mouvement**

instructions 255

programme 255

**multiplicateur de délai réseau** 196**multiplicateur de timeout** 196**MVI56-HART**

utilisations 49

**N****Niveau de performance** 31**non planifié**

programme 170

**numéro de réseau de sécurité**

attribution automatique 67

attribution manuelle 68

coller 70

copier 70

définition 31, 143

description 28, 66

gestion 66

**numéro de série** 76**O****obtenir**

informations d'axe 257

**obtention**

firmware 57

**onglet défauts majeurs** 214**onglet défauts mineurs** 214**onglet Safety** 201, 203, 208**onglet safety**

remplacement d'un module 154

signature de configuration 149

visualiser l'état de la sécurité 77, 208

**onglet sécurité**

déverrouillé 201

générer la signature de sécurité 203

sécurité de l'automate verrouillée 201

sécurité verrouillée 201

**optimiser les performances de réseau****EtherNet/IP** 34**P****pages Internet** 271

désactivation 247

**pages Internet de l'automate** 271

désactivation 247

**partenaire de sécurité**

état 208

**période de la tâche de sécurité** 183, 188**permet la communication** 110**planifié**

programme 170

- point**
    - consommer 112
    - dans un projet 172
    - produire 112
  - point consommé** 188
  - point produit** 188
  - points**
    - accès 187
    - accès automate 187
    - accès externe 186
    - dénomination 152
    - données de sécurité produites/consommées 188
    - E/S de sécurité 188
    - type de données 186
  - points de sécurité**
    - accès automate 187
    - description 186
    - mappage 197 - 199
  - port Ethernet**
    - désactivation 92, 232
    - diagnostics Logix Designer 265
  - port USB**
    - désactivation 239
  - ports CIP Security**
    - désactivation 236
  - priorité**
    - tâche 168
  - probabilité de défaillance par heure (PFH)**
    - définition 31
  - probabilité de défaillance sur sollicitation (PFD)**
    - définition 31
  - production d'un point** 193
  - produire**
    - des données 112
  - produire/consommer**
    - des données 112
  - programmation** 204
  - programme**
    - dans le projet 168
    - non planifié 170
    - planifié 170
  - Programmes de sécurité** 184
  - projet**
    - éléments 164
    - instructions complémentaires 174
    - passer en ligne 73
    - points 172
    - programme 168
    - sous-programme 171
    - tâches 165
    - transfert 82
  - propriétaire de la configuration** 150
    - réinitialisation 151
  - propriétaire de la configuration owner**
    - réinitialiser 153
  - protection de l'application de sécurité** 200 - 204
    - sécurité 202
    - signature de sécurité 203
    - verrouillage de sécurité 200
  - protection de la signature en mode exécution** 65
  - protection de la source et de l'exécution basée sur licence** 227
  - protection sous licence de la source et de l'exécution**
    - activation de la protection sous licence 228
  - Protocole simple de gestion de réseau** 116
- R**
- réception**
    - messages 114
  - références automate de sécurité** 13
  - références automate standard** 13
  - réinitialisation**
    - module 151
  - réinitialisation de module** 151, 153
  - réinitialiser**
    - propriété 151
  - remplacer**
    - configurer uniquement... activé 155
    - module Guard I/O 154
    - toujours configurer activé 160
  - requis**
    - connexions messages 114
  - réseau**
    - application et 33
    - ControlNet 39
    - Data Highway Plus 44
    - DeviceNet 42
    - DH+. Consultez Data Highway Plus.
    - E/S décentralisées universelles 45
    - EtherNet/IP 34
    - Foundation Fieldbus 48
    - HART 49
    - options automate 23, 24
  - réseau EtherNet/IP**
    - commande d'axe intégrée 23, 24
    - nombre de stations prises en charge 24
    - optimiser les performances réseau 34
    - vitesse de communication réseau 34
  - restrictions**
    - en présence d'une signature de sécurité 204
    - logiciel 205
    - mappage de points de sécurité 197
    - programmation 205
  - restrictions de programmation** 205
  - révision de firmware**
    - correspondance 76
  - RIO. Voir E/S décentralisées universelles**
  - RSWho**
    - définir chemin 73



## S

**SafetyTaskFaultRecord** 216  
**sans énergie stockée** 14  
**saut au sous-programme de défaut** 226  
**sécurité au niveau système** 219  
**sécurité de l'automate** 218  
**sécurité déverrouillée**  
 automate 201  
 icône 200  
**sécurité niveau système**  
 durcir le système de commande 219  
 gérer l'accès utilisateur  
 par programmation 220  
 surveiller le système de commande 219  
**sécurité spécifique à l'automate** 221  
 durcir le système de commande 221  
 gérer l'accès physique de l'utilisateur à  
 l'automate 223  
 surveillance du système de commande 222  
**sécurité verrouillée**  
 automate 201  
 icône 200  
**sélecteur à clé**  
 changer le mode de fonctionnement de  
 l'automate 86  
 position 85  
**signature de configuration**  
 composants 149  
 copier 149  
**signature de sécurité**  
 actions interdites 204  
 afficher 207  
 copier 204  
 effet sur le téléchargement 77  
 effet sur le transfert 77  
 enregistrement d'un projet 97  
 générer 203  
 restrictions 205  
 supprimer 204  
**snmp** 116  
**sous-programme**  
 dans un projet 171  
**sous-programme de gestion des défauts de  
 programme** 215  
**sous-programme de sécurité** 185  
 utilisant des données standard 197  
**stations sur un réseau EtherNet/IP** 108  
**supprimer**  
 signature de sécurité 204  
**Surveillance de l'état des dispositifs d'E/S de  
 sécurité** 152  
**surveillance du système de commande** 222  
**surveiller le système de commande** 219  
**système** 23  
**Système ControlLogix**  
 exigences minimales 13

## T

**tâche**  
 dans un projet 165  
 événement 167  
 périodique 167  
 permanente 167  
 priorité 168  
**tâche de sécurité** 182  
 exécution 184  
 priorité 183  
 temps de chien de garde 183  
**tâche événementielle** 167  
**tâche périodique** 167  
**tâche permanente** 167  
**taux de couverture des tests de diagnostic** 31  
**téléchargement**  
 effet de l'état de la sécurité 77  
 effet de la correspondance de l'automate 76  
 effet de la correspondance de révision du  
 firmware 76  
**température**  
 avertissement 287  
 limite 287  
**temps de chien de garde** 183  
**temps de réponse** 183  
**temps de scrutation**  
 réinitialisation 205  
**terminologie** 31  
**toujours configurer** 160  
**traduction d'adresses réseau (NAT)**  
 définir l'adresse IP 142  
**tranfert**  
 effet de la signature de sécurité 77  
**transfert**  
 effet de la correspondance de l'automate 76  
 effet du verrouillage de sécurité 77  
 projet 82  
**types de données**  
 CONNECTION\_STATUS 188

**U**

**utilisation d'un sous-programme  
 de défaut** 226

**V**

**valeur d'audit** 231  
**vérification de la mise en œuvre de la  
 sécurité** 223  
**verrouillage de la sécurité**  
 mot de passe 201  
**verrouillage de sécurité** 200  
 effet sur le téléchargement 77  
 effet sur le transfert 77  
**verrouiller**  
 voir verrouillage de sécurité  
**version de firmware**  
 discordance 78, 81

**vitesse de communication réseau**

sur un réseau EtherNet/IP 34

**vitesse de liaison**

EtherNet/IP 34

**voyant**

FORCE 284

OK 285

SD 285

**voyant FORCE 284**

**voyant OK 285**

**voyant SD 285**



## Assistance Rockwell Automation

Utilisez ces ressources pour accéder aux informations d'assistance.

<b>Centre d'assistance technique</b>	Aide proposée via des vidéos pratiques, foires aux questions, discussions, forums utilisateurs et notifications des mises à jour de produits.	<a href="http://rok.auto/support">rok.auto/support</a>
<b>Base de connaissances</b>	Accès aux articles de la base de connaissances.	<a href="http://rok.auto/knowledgebase">rok.auto/knowledgebase</a>
<b>Numéros de l'assistance technique locale</b>	Trouvez le numéro de téléphone pour votre pays.	<a href="http://rok.auto/phonesupport">rok.auto/phonesupport</a>
<b>Bibliothèque documentaire</b>	Trouvez les notices d'installation, les manuels, les brochures et les publications de données techniques.	<a href="http://rok.auto/literature">rok.auto/literature</a>
<b>Centre de compatibilité des produits et de téléchargement (PCDC)</b>	Téléchargez le firmware, les fichiers associés, tels que les fichiers AOP, EDS et DTM, et accédez aux notes de mise à jour de produit.	<a href="http://rok.auto/pcdc">rok.auto/pcdc</a>

## Commentaires sur la documentation

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? », disponible sur le site [rok.auto/docfeedback](http://rok.auto/docfeedback).

## Déchets d'équipements électriques et électroniques (DEEE)



En fin de vie, cet équipement doit être collecté séparément des déchets non triés.

Rockwell Automation tient à jour les données environnementales relatives à ses produits sur son site Internet, à l'adresse [rok.auto/pec](http://rok.auto/pec).

Allen-Bradley, ArmorBlock, ArmorPOINT, Block I/O, Compact 5000, CompactLogix, ControlBus, ControlFLASH, ControlFLASH Plus, ControlLogix, ControlLogix-XT, Data Highway Plus, DH+, DriveLogix, FactoryTalk, FLEX I/O, FLEX 5000, Guard I/O, GuardLogix, Kinetix, Logix 5000, On-Machine, PanelConnect, PanelView, PLC-2, PLC-3, PLC-5, POINT I/O, POINT Guard I/O, PowerFlex, QuickView, Rockwell Automation, Rockwell Software, RSFieldbus, RSLinx, RSNetWorx, RSVIEW, SLC, Stratix, Studio 5000, Studio 5000 Logix Designer et SynchLink sont des marques commerciales de Rockwell Automation.

CIP, CIP Motion, CIP Safety, CIP Security, CIP Sync, ControlNet, DeviceNet et EtherNet/IP sont des marques commerciales d'ODVA, Inc.

Les marques commerciales n'appartenant pas à Rockwell Automation sont la propriété de leurs sociétés respectives.

Suivez-nous.



[rockwellautomation.com](http://rockwellautomation.com)

expanding human possibility®

AMÉRIQUES : Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 États-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](http://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