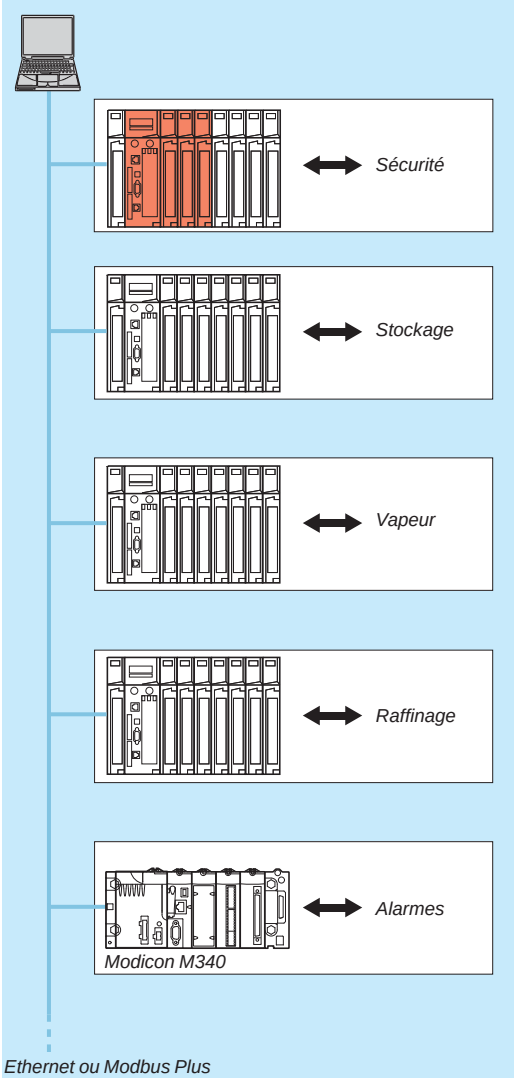
Plate-forme d'automatisme Modicon Quantum
Automates de sécurité

Pour toute information détaillée concernant l'installation, l'utilisation et la maintenance d'un système selon les prescriptions du standard CEI 61508, se référer au document "*Quantum Safety PLC, Safety Reference Manual*", 02/2015, n° 33003879.06 en anglais, approuvé par TÜV Rheinland *et* disponible sur le site **www.schneider-electric.com**.

Unity Pro



Le même logiciel de programmation et les mêmes composants matériels système et communication pour les fonctions de sécurité et d'automatisme.

Présentation

Du fait des conséquences importantes que peut avoir un accident industriel sur le plan humain, financier et environnemental, la sécurité est un élément de plus en plus déterminant pour les entreprises. Il s'agit non seulement de protéger les employés et les riverains des sites mais aussi de protéger les outils de production et l'environnement tout en respectant la législation en vigueur. De nouveaux défis liés à la sécurité s'ajoutent aux habituels défis industriels tels que la réduction des coûts de fonctionnement et l'optimisation des coûts de fabrication.
Pour répondre à de telles demandes, Schneider Electric a développé une offre d'automates de sécurité basée sur la gamme Modicon Quantum. Cette offre d'automates de sécurité Quantum a été certifiée par le TÜV (Rheinland Group) conformément à la norme CEI 61508 applicable à des applications nécessitant un niveau de sécurité jusqu'à SIL3.

L'intégration de fonctionnalités de sécurité certifiées et de mode Hot Standby dans une même plateforme d'automates configurables, le tout, programmable avec un outil commun à la plateforme et aux automates standard font des automates de sécurité Quantum une offre à ce jour unique sur le marché des automatismes.
Cette nouvelle offre permet la réalisation d'architectures de sécurité simples et standard :
- Diagnostic interne approfondi au niveau de la gestion des E/S.
- Architecture interne processeur de type 1oo2.
- Pas de fonction d'élection externe ni de composants matériels additionnel pour assurer le niveau de sécurité.

La partie sécurité étant intégrée dans l'automate lui-même, le câblage des E/S est identique à celui des automates standard.
Les architectures de sécurité sont identiques à celles des Modicon Quantum standard. Elles utilisent :
- Le système d'E/S décentralisées standard.
- Les modules CRP/CRA de déport d'E/S assurant une redondance de câblage entre les racks distants et le rack principal.
- Un système de câblage standard.
- Les bacs fond de panier Quantum standard.
- Une alimentation redondante standard.
- Une architecture Hot Standby similaire au Hot Standby standard Quantum, très simple à câbler et ne nécessitant pas de développement logiciel spécifique.

Applications cibles

Les processeurs Quantum Safety Unity certifiés SIL3 répondent parfaitement aux process de contrôles industriels.
Ils sont en particulier certifiés pour être utilisés dans les applications suivantes :
- Systèmes d'arrêt d'urgence (ESD – *Emergency Shut Down*).
- Systèmes de contrôle de brûleur.
- Applications "*Fire and Gas*", système d'alarme et de détection de feu.
- Machines de sécurité.

Sécurité des procédés : généralités

Système de sécurité

Un système est considéré comme fonctionnellement "de sécurité" si des causes de défaillances aléatoires ou systématiques n'entraînent pas un dysfonctionnement du système, ne provoquent pas de blessures ou de décès de personnes, de perte de matériel ni de pollution de l'environnement.

Safety Instrumented System (SIS)

Un "Safety Instrumented System" est un système indépendant composé de capteurs, de contrôleurs logiques (les automates Quantum certifiés SIL3 par exemple) et d'actionneurs prévus pour placer le process dans un état sécuritif lorsque les conditions prédéterminées de bon fonctionnement sont violées.

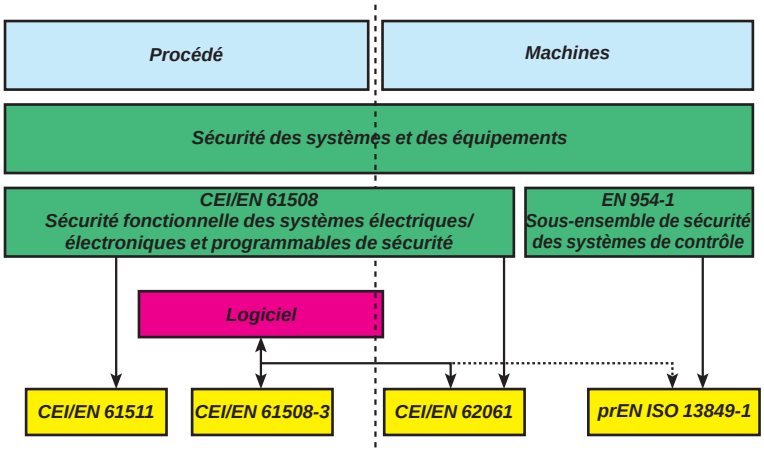
Plate-forme d'automatisme Modicon Quantum
Automates de sécurité

Sécurité des procédés : généralités (suite)

Safety Integrity Level (SIL)

"Safety Integrity Level" (SIL) est devenu un synonyme de sécurité fonctionnelle. SIL définit sur un plan sécurité le niveau de performance ou de fiabilité d'un système électrique ou électronique. De ce fait, le niveau SIL est l'indicateur de la capacité d'un système à effectuer des tâches de sécurité.

Normes de sécurité (CEI 61508 et CEI 61511)



La norme CEI 61508 "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems" a été publiée en 1998 et validée en 2002.
Ce nouveau standard de sécurité définit pour la première fois les besoins de sécurité en automatisme d'une manière indépendante de l'application. La norme CEI 61508 est une norme technique concernant la sécurité fonctionnelle d'équipements électriques ou électronique. Un système est dit de sécurité s'il réalise une ou plusieurs fonctions spécifiques de manière à ce que les risques encourus restent à un niveau acceptable. De telles fonctions sont définies comme étant des fonctions de sécurité.

La norme CEI 61508 contient des exigences générales permettant de minimiser les risques suivants :
- Mauvaises spécifications du système (sur un plan matériel ou logiciel).
- Oublis dans les spécifications.
- Défaillances aléatoires du matériel.
- Défaillances systématiques du matériel ou du logiciel.
- Défaillances en général.
- Influences environnementales (CEM, température …).
- Perturbations d'alimentation.

Alors que la norme CEI 61508 vise principalement les fabricants de composants pour la protection des équipements et des produits, la norme CEI 61511 : Functional Safety – Technical Safety Systems for the Process Industry, vise les utilisateurs et concepteurs d'équipements de sécurité.
La norme CEI 61511 propose des recommandations et cible l'estimation des risques de dommages aux installations. Elle fournit également une assistance dans la sélection de composants de sécurité.
La norme CEI 61511 est un standard spécifique aux process industriels :
- Largement appliqué aux systèmes de sécurité instrumentés.
- Principalement défini pour les concepteurs de systèmes, les intégrateurs et les utilisateurs d'équipements ou systèmes de sécurité.

TÜV Rheinland

TÜV est un groupe de compagnies habilitées à délivrer les certifications CEI 61508. L'une d'entre-elles, TÜV Rheinland (Allemagne) a une réputation mondiale de leader dans les systèmes de sécurité.
Reconnue comme l'une des meilleures agences de certification au monde, TÜV Rheinland a reçu l'aval à la fois des assurances et des gouvernements.

TÜVRheinland®

Plate-forme d'automatisme Modicon Quantum
Automates de sécurité

Certifications et normes

L'offre d'automates Safety Modicon Quantum est certifiée par TÜV Rheinland pour une utilisation dans des applications nécessitant un niveau de sécurité jusqu'à SIL3 compris.

Cette certification assure que les automates de sécurité Modicon Quantum sont conformes aux normes suivantes :
- CEI 61508 second edition: sécurité fonctionnelle de systèmes électriques, électroniques, systèmes de sécurité programmables, section 1-7, deuxième édition, septembre 2012.
- CEI 61131 : automates programmables : section 2 : exigences des équipements et tests : deuxième édition, février 2003.
- Protection des chaudières :
  - normes européennes : EN 50156,
  - normes USA : NFPA 85 et NFPA 86.
- EN 54-2 : détection d'incendie et système d'alarme incendie.
- EN 298 : système de contrôle automatique de brûleur de gaz (avec ou sans ventilation).
- Sécurité des mécanismes : CEI 62061 et EN ISO 13849.

Les automates Safety Modicon Quantum sont également conformes aux exigences des certifications :
- UL.
- CSA.
- CE.
- Hazardous Locations.
- ATEX, selon modèle, voir pages 48286/2 à 48286/9.

Formation

Fort d'une expérience de plus de 30 ans dans le contrôle et la conduite de process critiques, Schneider Electric met à votre disposition ses meilleurs experts en sécurité à travers des prestations d'assistance et de conseil.

En collaboration avec vos équipes, ils estiment le risque, en déterminant les paramètres raisonnablement prévisibles et, si la mise en place d'un système de sécurité est nécessaire, ils déterminent le niveau SIL requis. Ils peuvent également prendre en charge la conception de l'architecture et la spécification des fonctions de sécurité associées. Enfin, ils sauront vous accompagner dans l'obtention de la certification du système et de l'application.

- Formation à la sécurité fonctionnelle.
- Analyse de danger et de risque.
- Définition des fonctions de sécurité et du niveau de SIL requis.
- Conception de l'architecture du système de sécurité et spécification des fonctions de sécurité.
- Evaluation du niveau de sécurité intrinsèque.
- Assistance technique au développement.
- Pilotage de la recette du système de sécurité.
- Assistance au démarrage de l'application.
- Assistance à la maintenance préventive.

Plate-forme d'automatisme Modicon Quantum
Automates de sécurité

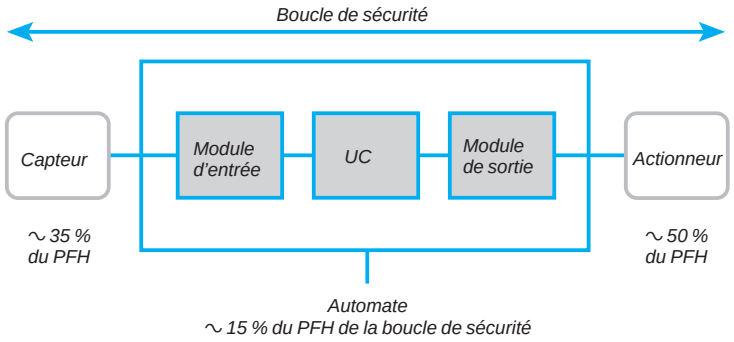
Processeurs et modules de sécurité

L'offre d'automates Safety Modicon Quantum comprend cinq références : deux processeurs et trois modules d'E/S et utilise également le module d'alimentation **140CPS12420**.
Ces produits sont certifiés pour être utilisés dans des applications de sécurité nécessitant un niveau inférieur ou égal à SIL3 :

Processeur de sécurité	**140CPU65160S**
Processeur de sécurité Hot Standby	**140CPU67160S**
Entrées TOR de sécurité	**140SDI95300S**
Sorties TOR de sécurité	**140SDO95300S**
Entrées analogiques de sécurité	**140SAI94000S**
Alimentation	**140CPS12420** *(1)*

Description de la boucle de sécurité

La boucle de sécurité dans laquelle est inséré l'automate de sécurité Quantum est constituée des 3 parties suivantes :
- Les capteurs.
- L'automate de sécurité Quantum.
- Les actionneurs.



Probabilités de défaillance PFD, PFH

Pour les applications SIL3, le standard CEI 61508 définit la probabilité de défaillance sur demande de puissance (sollicitation) (PFD), la probabilité de défaillance par heure (PFH), selon le mode d'opération du système :
- $10^{-4} \leq PFD < 10^{-3}$ en mode d'opération de faible sollicitation,
- $10^{-8} \leq PFH < 10^{-7}$ en mode de fortes sollicitations.

L'automate de sécurité Quantum est certifié pour l'utilisation dans les systèmes à faibles ou fortes sollicitations.
Pour le calcul des valeurs PFD/PFH d'un système typique, un maximum de 15 % est généralement admis pour l'automate. Les valeurs PFD/PFH des modules de sécurité Quantum, pour les valeurs de PTI *(3)* de 5 ans et 10 ans, sont données dans le tableau ci-dessous :

	Référence	PTI = 5 ans		PTI = 10 ans	
		PFD ($x10^{-5}$)	PFH ($x10^{-9}$)	PFD ($x10^{-5}$)	PFH ($x10^{-9}$)
Processeur de sécurité	**140CPU65160S**	4,9	5,1	9,9	5,6
Processeur de sécurité Hot Standby	**140CPU67160S**	4,9	5,1	9,9	5,6
Entrées TOR de sécurité	**140SDI95300S**	0,3	1,9	0,6	1,9
Sorties TOR de sécurité	**140SDO95300S**	0,4	1,2	0,7	1,2
Entrées analogiques de sécurité	**140SAI94000S**	0,4	1,4	0,9	1,4
Alimentation	**140CPS12420** *(2)*	–	–	–	–
Alimentation	**140CPS22400** *(2)*	–	–	–	–

(1) Module non interférent certifié par TÜV Rheinland, consulter notre site internet www.schneider-electric.com.
(2) La version "Conformal Coating" comportant la lettre "C" en fin de référence a une valeur identique.
(3) Proof Test Interval, voir page 43480/6.

Plate-forme d'automatisme Modicon Quantum
Automates de sécurité

PTI

Le test de qualification est un processus périodique d'essais destinés à déterminer si le système doit être rénové complètement ou partiellement. PTI (*Proof Test Interval*) est l'intervalle de temps entre deux qualifications.

Exemple 1 : boucle de sécurité

Avec :
- 1 module d'entrées TOR :
- 1 module de sorties TOR,
- 1 UC autonome.

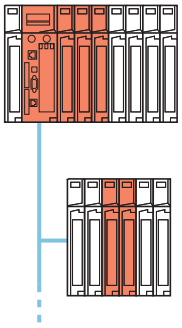
L'automate de sécurité Quantum contribue à la boucle de sécurité pour :
0,2 + 1,1 + 0,2 = 1,5 %.
Les capteurs et actionneurs disposent de = 98,5 %.

Exemple 2 : boucle de sécurité redondante

Avec 2 capteurs :
- 2 modules d'entrées analogiques redondants,
- 2 modules de sorties TOR redondants,
- 2 UC à haute disponibilité (Hot Standby).

L'automate de sécurité Quantum contribue à la boucle de sécurité pour :
0,2 + 1,1 + 0,2 = 1,5 %.
Les capteurs et actionneurs disposent de = 98,5 %.

***Note** : Tout module doublé contribue seulement 1 fois car la redondance n'est en place que pour l'augmentation de la disponibilité.*
Par suite, seulement 1 module est actif dans la boucle de sécurité.



Unity Pro XLS favorise la mixité des E/S de sécurité et des E/S non interférentes.

Modules non interférents

Certains modules d'E/S du catalogue Quantum peuvent être utilisés dans une architecture de sécurité et sont considérés comme n'interférant pas avec le process de sécurité.
En opposition avec les modules de sécurité, ces modules dits "non interférents" ne sont pas utilisés pour exécuter des fonctions de sécurité.
Liste des modules Quantum non interférents pleinement compatibles avec une configuration Quantum de sécurité *(1)* :

Type	Référence
Coupleur tête de réseau d'E/S décentralisées	**140CRP93200**
Coupleur de station d'E/S décentralisées	**140CRA93200**
Répéteur fibre optique de station RIO	**140NRP95400**
	140NRP95401C
Module Ethernet	**140NOE77111**
Rack 16 slots	**140XBP01600**
Rack 10 slots	**140XBP01000**
Rack 6 slots	**140XBP00600**
Entrées TOR	**140DDI35300**
Sorties TOR	**140DDO35300**
Entrées analogiques	**140ACI04000**
Sorties analogiques	**140ACO02000**
Bornier 40 points	**140XTS00200**
	140XTS00100
Module d'entrées multifonctions	**140ERT85420**
Répéteur optique	**140NRP95400**

Traitement pour environnements sévères

Les processeurs de sécurité **140CPU6●160S** et les modules d'entrées/sorties de sécurité **140SD●95300S**, **140SAI94000S** bénéficient d'un vernis "Humiseal 1A33" qui les rend apte à fonctionner en environnement sévère (voir page 48286/2).
Les modules non-interférents et les racks compatibles avec les automates de sécurité sont également disponibles en version "Conformal Coating" avec le même traitement (voir pages 48286/2 à 48286/9).

Les références de ces modules et racks vernis se construisent en ajoutant la lettre "**C**" en fin de la référence du module standard.

(1) Modules non interférents certifiés par TÜV Rheinland, consulter notre site internet www.schneider-electric.com.

Processeurs : page 0497Q/2 | Architectures d'E/S : page 0520Q/2 | Entrées/sorties : page 0482Q/2 | Communication : page 0439Q/2 | Logiciels : page 0516Q/2

Logiciel de programmation Unity Pro XL Safety

Un automate de sécurité Quantum est programmé avec Unity Pro XL Safety.
Cet outil de programmation est commun à de nombreuses gammes d'automates Schneider Electric (Modicon M340, Modicon Premium, Standard Modicon Quantum, Safety Modicon Quantum). Ethernet et Modbus Plus permettent la connexion à d'autres automates, de sécurité ou non, ainsi qu'à la supervision.
Afin de satisfaire les exigences de la norme CEI 61508, seul un logiciel de programmation certifié est autorisé pour programmer des applications de sécurité. Schneider Electric a développé la version sécurité Unity Pro XLS (XL Safety) de son logiciel de programmation.
Cette version de Unity Pro est capable d'effectuer à la fois les diagnostics d'erreurs et d'assurer la protection de projet jusqu'au niveau requis pour la programmation d'une application de sécurité.
Unity Pro XLS peut être utilisé pour générer aussi bien des applications de sécurité que des applications standard.
Il n'est donc pas nécessaire d'avoir un autre logiciel de programmation, une seule version peut être installée sur le PC.
Pour plus d'informations, voir page 48388/2.

Instructions à virgule flottante

Unity Pro XLS version 4.1 ou supérieure permet l'utilisation des instructions numériques au format à virgule flottante *(floating point)* pour la programmation des applications de sécurité.

Différences entre automate de sécurité Quantum et automate standard Quantum

L'automate de sécurité Quantum diffère de l'automate Quantum standard dans ses fonctions et comportements afin de satisfaire aux exigences du standard CEI 61508.

Caractéristique	Automate Quantum standard	Automate de sécurité Quantum
Configuration	■ Fond de panier ■ Rack local ■ E/S distantes ■ Toutes les alimentations ■ Extensions de fond de panier ■ E/S distribuées ■ E/S sur bus de terrain	■ Fond de panier ■ Rack local ■ E/S distantes ■ Alimentation dédiée
Firmware	Standard	De sécurité
Logiciels	■ Unity Pro XLS ■ Unity Pro XL ■ Unity Pro L	Unity Pro XLS
Logique utilisateur	■ FBD ■ LD ■ IL ■ ST ■ SFC	■ FBD ■ LD
Types de données	■ EDT ■ DDT	■ EDT ■ Uniquement tableaux simples
Mode	–	■ Mode maintenance ■ Mode sécurité
Comportement en redémarrage	■ Démarrage en stop ■ Reprise à froid ■ Reprise à chaud	■ Démarrage en stop ■ Reprise à froid
Mode sécurité	Non	Oui
Durée minimale d'exécution de MAST en mode cyclique	3 ms	20 ms
Forçage en mode sécurité par clé de verrouillage	Non	Oui
Vérification mémoire	Non	Oui
Mot de passe	Non	Oui
Blocs MSTR	Oui	Non
Abonnement Global Data (Ethernet)	Partout	Uniquement en zone sans restriction
Lecture I/O scanner (Ethernet)	Partout	Uniquement en zone sans restriction
Cartes PCMCIA	Slot A et B	Slot A

***Nota** : L'automate de sécurité Quantum peut seulement effectuer un démarrage à froid : l'application est réinitialisée à chaque démarrage.*
L'automate de sécurité Quantum peut fonctionner en mode cyclique ou périodique.

Communication Ethernet et Modbus Plus

Principe général

Quel que soit le réseau Ethernet ou Modbus Plus utilisé et quel que soit le protocole mis en œuvre, l'envoi d'informations vers un automate ou un terminal IHM extérieur est possible sans restriction. En revanche la réception (écriture d'information dans l'automate de sécurité) ne peut se faire que dans la zone mémoire "sans restriction" *(1)*.

Communication d'automate à automate

L'automate de sécurité Quantum est en mesure de communiquer avec d'autres automates à travers :
- Modbus TCP. Connexion CPU ou module **140NOE77111/140NOE77111C**.
- Modbus Plus (port série de l'UC), serveur uniquement.
- Modbus RS232/RS485 (port série de l'UC).

Cette communication est certifiée pour être utilisée dans des boucles de sécurité. Ces communications sont catégorisées comme non interférentes.

Communication Ethernet

Le réseau Ethernet se connecte :
- Par le port Ethernet de l'UC.
- Par un module Ethernet **140NOE77111/140NOE77111C**.

Nota : Dans le cas d'une UC de sécurité Hot Standby, le port Ethernet est réservé à l'échange de données entre automate primaire et redondant.

Le module Ethernet **140NOE77111/140NOE77111C** est un produit certifié non interférent pour l'utilisation dans un automate de sécurité Quantum.
La communication peut être Peer-to-Peer ou Global Data. Pour le câblage, tous les constituants Ethernet standard peuvent être utilisés.

Communication Ethernet Peer-to-Peer

Cette communication se définit via Unity Pro XLS dans la configuration réseau Ethernet, indépendamment pour la lecture et l'écriture. Unity Pro XLS vérifie que la lecture utilise (écrit dans) la zone mémoire "sans restriction" *(1)* seulement.

Communication Ethernet Global Data

La communication Global Data est configurée dans Unity Pro XLS dans la configuration réseau Ethernet pour publier des données en écriture et pour s'abonner à des données en lecture.
La lecture est autorisée uniquement à destination de la zone mémoire "sans restriction" *(1)*.

Communication Modbus Plus

Sur un réseau Modbus Plus, la communication Peer-to-Peer et les échanges Global Data sont autorisés par le port Modbus Plus du processeur.

Communication Peer-to-Peer sur Modbus Plus

Cette communication se définit via Unity Pro XLS dans la configuration réseau Modbus Plus, indépendamment pour la lecture et l'écriture. Unity Pro XLS vérifie que la lecture utilise (écrit dans) la zone mémoire "sans restriction" *(1)* seulement.

Communication Global Data sur Modbus Plus

La communication Global Data est définit dans Unity Pro XLS dans la configuration réseau Modbus Plus pour publier des données en écriture et pour s'abonner à des données en lecture.
La lecture est autorisée uniquement à destination de la zone mémoire "sans restriction" *(1)*.

(1) Mémoire de sécurité et mémoire sans restriction, voir page 43481/3.

Communication avec des terminaux IHM

Un terminal IHM est autorisé à lire des données de l'automate de sécurité Quantum mais il ne peut écrire que dans la zone mémoire "sans restriction" *(1)* à travers :
- Modbus TCP : soit par la prise UC, soit par module **140NOE77111/ 140NOE77111C**.
- Modbus Plus.
- Modbus RS232/RS485.

Cette communication n'étant pas définie avec Unity Pro XLS, c'est l'automate de sécurité Quantum qui se protège lui-même contre les tentatives d'écriture du terminal IHM : une éventuelle commande d'écriture en mémoire de sécurité *(1)* est ignorée.

Ecriture en mode Maintenance

Même en mode maintenance, il y a une protection en écriture dans la mémoire de sécurité, par d'autres automates ou par des terminaux IHM.

Il n'est possible de passer en mode maintenance qu'avec Unity Pro XLS et après présentation d'un mot de passe. En mode maintenance, Unity Pro XLS ou un serveur de données OPC peuvent modifier et régler les données de cette zone :
- Modification de la logique du programme.
- Affectation de valeurs.
- Forçage de valeurs.
- Débogage.

Communication PC-automate

La communication entre Unity Pro XLS et l'automate de sécurité Quantum se fait à travers :
- Modbus TCP. Prise CPU ou module NOE.
- Modbus Plus.
- Modbus RS232/RS485.
- USB.

Même si la communication entre Unity Pro XLS et l'automate de sécurité Quantum ne fait pas partie de la boucle de sécurité, elle est néanmoins soumise à des vérifications, par exemple de CRC pour s'assurer que les données sont transférées correctement et qu'il n'y a pas d'erreur de communication.

(1) Mémoire de sécurité et mémoire sans restriction, voir page 43481/4.

Plate-forme d'automatisme Modicon Quantum
Architectures de sécurité

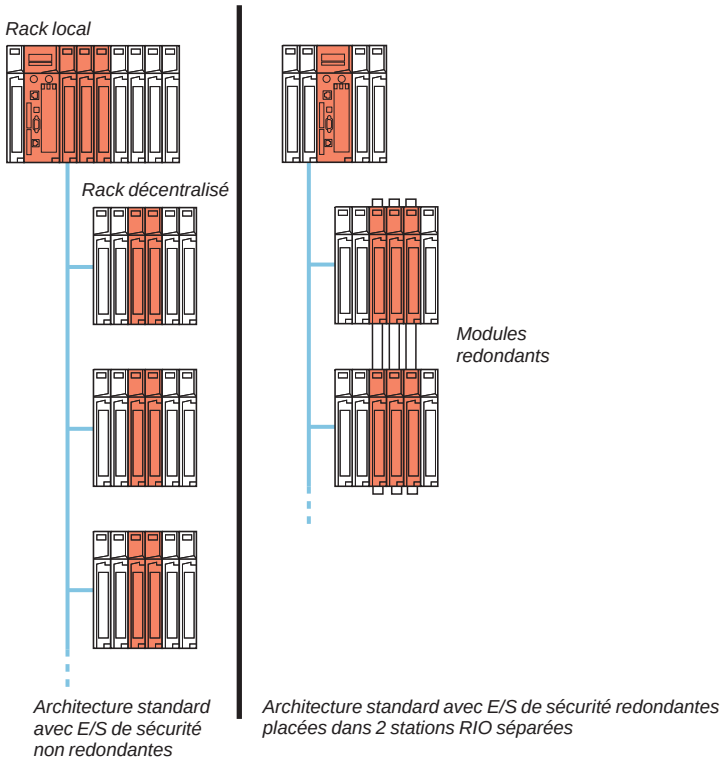
Introduction

Les architectures d'automates de sécurité Quantum bénéficient de la même flexibilité et des mêmes capacités de haute disponibilité que les architectures d'automates Quantum standard.

Flexibilité des architectures

Architectures processeurs "1oo2"

Exemple d'architecture avec des E/S de sécurité redondantes ou non *(1)*



Ces architectures mettent en œuvre l'unité centrale **140CPU65160S**.

(1) Détail des topologies avec câble unique, voir page 43488/3

Plate-forme d'automatisme Modicon Quantum
Architectures de sécurité

Flexibilité des architectures (suite)

Architectures Hot Standby de sécurité : architectures processeurs "1oo2 Hot Repair"

Les architectures Hot Standby de sécurité permettent :
- D'accroître de façon significative la disponibilité du système.
- D'éliminer les phases d'arrêt du process grâce aux processeurs redondants.
- La redondance est possible à tous les niveaux de l'architecture : processeurs, câblage, alimentation, E/S, …

Le système Hot Standby, compatible avec le logiciel Unity Pro XL Safety, confère aux processeurs Quantum de sécurité le niveau requis par les applications les plus exigeantes, quant à la disponibilité de leur système de contrôle/commande.

Au centre du système se trouvent deux racks automates Quantum de sécurité, communément appelés automate "Primaire" et automate "Redondant".
Leurs configurations matérielles doivent être identiques (même modules dans chaque rack local). L'élément clé, sur chacun d'entre eux, est le processeur **140CPU67160S**, spécialement étudié pour les architectures Hot Standby avec le logiciel Unity Pro XL Safety. Ce processeur est un module double emplacement, qui conjugue, dans le même boîtier, la fonction Unité Centrale et celle de coprocesseur de redondance.

L'automate "Primaire" exécute le programme application et assure le contrôle des entrées/sorties. L'automate "Redondant" reste lui en retrait, prêt à prendre la main si nécessaire. L'automate "Redondant" est relié à l'automate "Primaire" par l'intermédiaire d'une liaison fibre optique à haut débit (100 Mbit/s) intégrée au processeur.
Cette liaison fibre optique (multimode 62,5/125 µm) peut être étendue à 2 km, sans dispositif supplémentaire particulier. C'est par son intermédiaire que s'opère la mise à jour cyclique des données de l'application utilisateur sur l'automate "Redondant".

En cas de défaillance inopinée survenant sur l'automate "Primaire", le système de redondance opère une commutation automatique basculant l'exécution du programme application et le contrôle des entrées/sorties sur l'automate "Redondant", avec un contexte de données à jour. A l'issue du basculement, l'automate "Redondant" devient l'automate "Primaire". Une fois l'automate défaillant remis en état de marche et reconnecté au système de redondance, il intervient en tant qu'automate "Redondant".

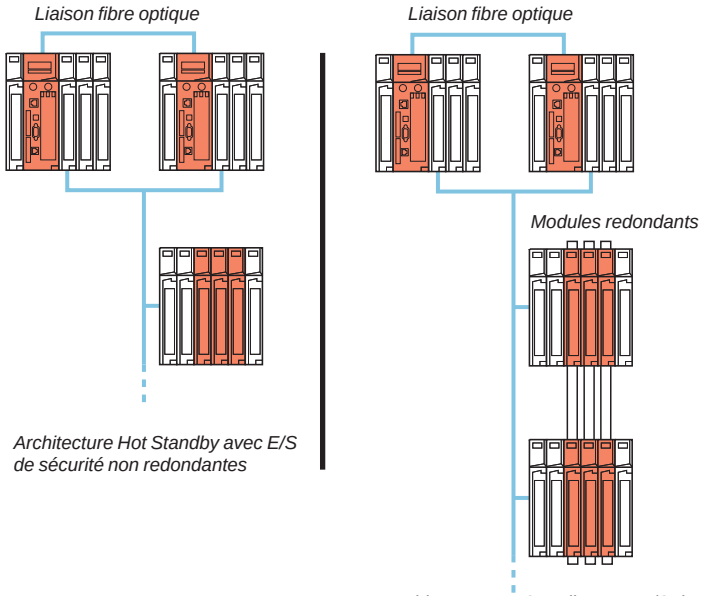
L'utilisation du système de redondance Hot Standby avec le logiciel Unity Pro XL Safety autorise un basculement de la redondance qui s'effectue sans à-coup sur les sorties, et intervient de façon transparente pour le procédé, dont la gestion ne sera en définitive pas altérée par l'occurrence d'une défaillance matérielle.
Le système Hot Standby avec le logiciel Unity Pro XL Safety est le gage d'une productivité accrue, du fait de sa contribution à la réduction des temps d'arrêt.

Processeurs : page 0497Q/2 | Architectures d'E/S : page 0520Q/2 | Entrées/sorties : page 0482Q/2 | Communication : page 0439Q/2 | Logiciels : page 0516Q/2

Plate-forme d'automatisme Modicon Quantum
Architectures de sécurité

Flexibilité des architectures (suite)

Exemple d'architecture Hot Standby avec des E/S de sécurité redondantes ou non



Architecture Hot Standby avec E/S de sécurité non redondantes

Architecture Hot Standby avec E/S de sécurité redondantes placées dans 2 stations RIO séparées

Architecture "1oo2 Hot Repair"

Une architecture Hot Standby permet d'associer sécurité et haute disponibilité dans un même automate. Elle garantit que même si l'un des processeurs est arrêté, le système est toujours un système de sécurité de niveau SIL3. Comme les automates Quantum de sécurité sont basés sur la même architecture Hot Standby que les automates Quantum standard, la solution est indiscutablement robuste et éprouvée sur le terrain.

Grâce au design "1oo2" des processeurs de sécurité (voir page 43481/2), l'ensemble reste simple et efficace en terme de coûts, comparée aux solutions multiprocesseurs à 3 UC et vote d'inter-contrôle avec matériel externe. La redondance complète des fonctions, des E/S jusqu'à la supervision, offre l'avantage de pouvoir supporter plus d'une erreur tout en garantissant le niveau de sécurité fonctionnel exigé.

Particulièrement adaptée pour la conception de systèmes de production sûrs, disponibles et économiquement efficaces, la solution est à la base du concept d'architecture **"1oo2 Hot Repair"** de TÜV Rheinland.

Détails

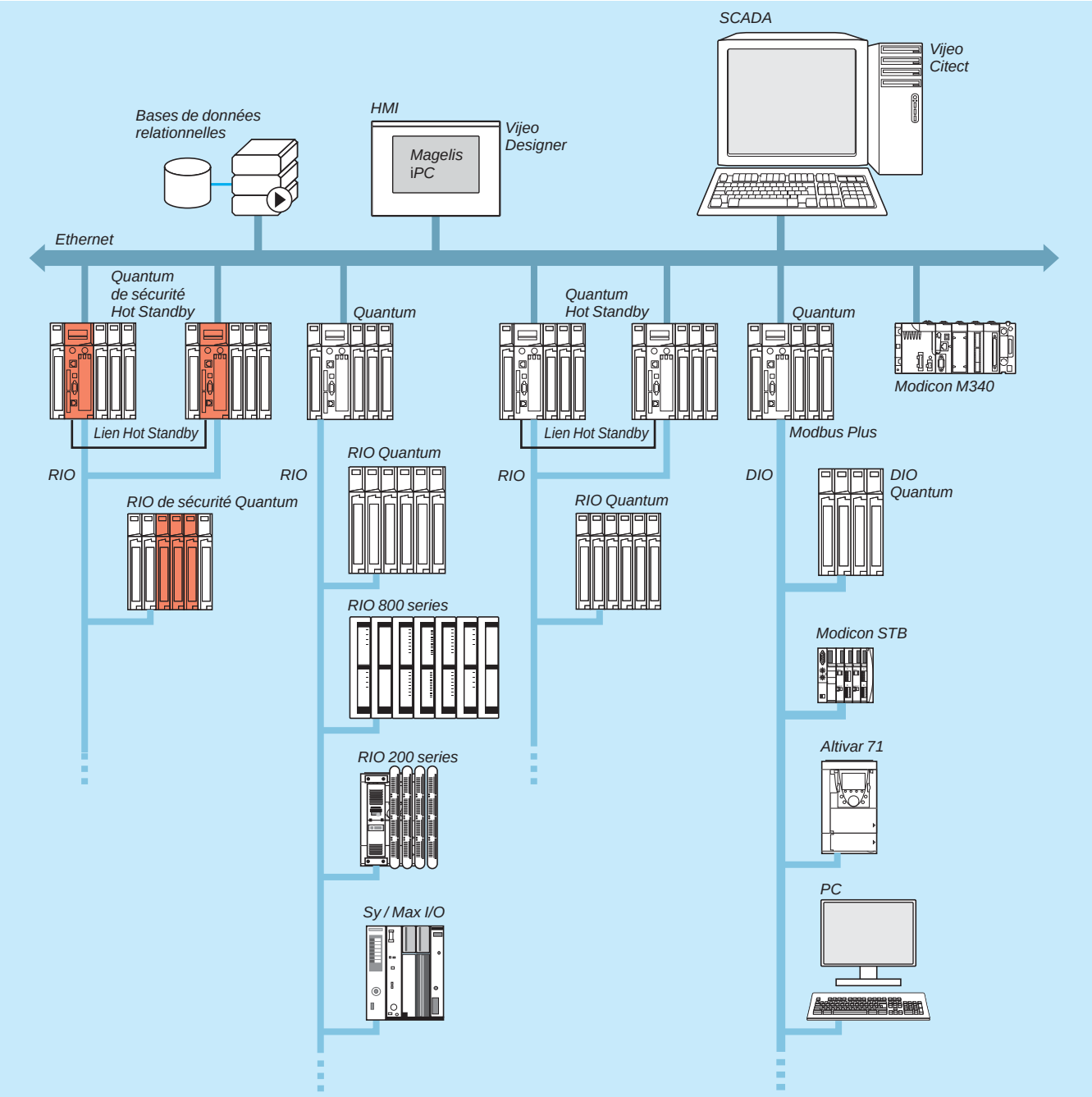
Ces architectures sont conçues avec deux **140CPU67160S** reliés par liaison optique. Les modules d'E/S de sécurité sont placés dans des stations RIO décentralisées pour que leur contrôle soit possible par les deux UC *(1)*.

L'UC à haute disponibilité de sécurité Quantum diffère de l'UC autonome **140CPU65160S** par l'usage du port Ethernet. Dans une configuration autonome, celui-ci est utilisé pour communiquer avec d'autres équipements par des câbles Ethernet standard. Dans une configuration à haute disponibilité de sécurité, le port Ethernet est utilisé pour échanger des données entre contrôleur primaire et redondant par lien à fibre optique. Comme ce lien à fibre optique ne fait pas partie de la boucle de sécurité, les valeurs PFD et PFH de l'UC à haute disponibilité sont les mêmes que celles de l'UC autonome.

(1) Détail des raccordements, voir page 43489/7.

Plate-forme d'automatisme Modicon Quantum
Architectures de sécurité

Architecture collaborative



L'automate de sécurité Quantum est d'un usage simple en architecture collaborative :

- Le même outil logiciel est utilisé pour les automates de sécurité et les automates de contrôle.
- L'automate de sécurité bénéficie de toutes les protections nécessaires contre les écritures en provenance des autres équipements de l'architecture.

Processeurs : page 0497Q/2 | Architectures d'E/S : page 0520Q/2 | Entrées/sorties : page 0482Q/2 | Communication : page 0439Q/2 | Logiciels : page 0516Q/2

Plate-forme d'automatisme Modicon Quantum
Architectures de sécurité

Fonctions de haute disponibilité

Les fonctions disponibles pour la haute disponibilité, en fonction du mode maintenance/sécurité de l'automatisme, sont les suivantes :

Fonction	Mode maintenance	Mode sécurité
Haute disponibilité	Oui	Oui
Echange de rôle	Oui	Oui
Echange de rôle par EFB	–	Oui
Commutateur à clé	Oui	Oui
Différence de logique	Oui	–
Chargement d'OS	Oui, si automate secondaire en stop et déconnecté	–
Transfert d'application	Oui	Oui, par clavier UC

Modules d'E/S de sécurité dans les configurations à haute disponibilité

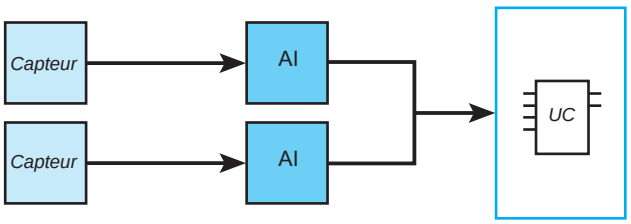
Les modules d'E/S de sécurité peuvent être utilisés en redondance pour accroître la disponibilité de l'automatisme.
Schneider Electric offre des blocs fonctions pour superviser l'état d'une configuration à modules redondants.
L'état des modules est disponible dans des mots système, à la disposition des opérateurs et personnels de maintenance pour les informer qu'un module est défectueux et doit être changé.

Pour augmenter le niveau de disponibilité du système, Schneider Electric recommande de mettre en œuvre des racks d'E/S décentralisés différents pour des modules d'E/S en redondance.

Modules d'entrées analogiques

2 capteurs distincts sont utilisés pour une entrée analogique de sécurité à haute disponibilité, et chacun est connecté à une voie d'acquisition propre.
Il est conseillé de placer ces deux voies d'acquisition sur des modules d'entrées analogiques différents.

Schéma fonctionnel :



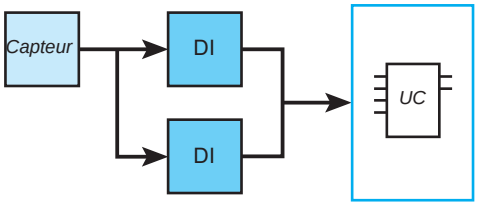
Le bloc fonction S_AISIL2 est utile pour la sélection des données des deux entrées analogiques redondantes et pour la supervision des états des entrées.

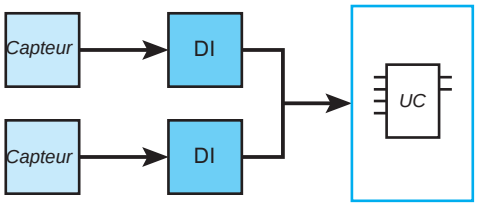
Plate-forme d'automatisme Modicon Quantum
Architectures de sécurité

Modules d'entrées TOR

Les entrées TOR de sécurité redondantes peuvent être connectées à 1 ou 2 capteurs. Il est préférable que les 2 voies d'entrées soient localisées sur des modules d'entrées différents.
Dans le cas d'utilisation d'un capteur unique, les modules partagent la même alimentation process. Il convient de définir le câblage adapté pour respecter les conditions d'utilisations des modules (caractéristiques des entrées en court-circuit, circuit ouvert, niveaux logiques 0 et 1, tensions et courants) spécifiés dans le document Guide de Référence Matériel Quantum.

Schémas fonctionnels :



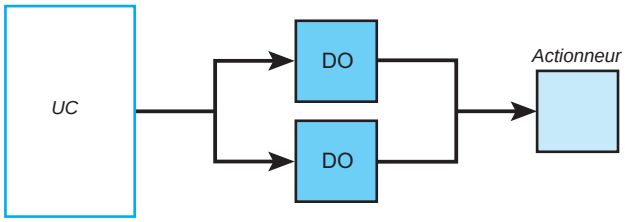


Le bloc fonction S_DISIL2 est utile pour la sélection des données de 2 entrées TOR redondantes et pour superviser les états des entrées.

Modules de sorties TOR

Pour des sorties TOR à haute disponibilité, les 2 sorties sont localisées sur des modules séparés, câblées en parallèle pour la connexion à 1 actionneur.

Schéma fonctionnel :



Un bloc fonction n'est pas nécessaire car un signal unique en provenance de l'UC est connecté aux 2 sorties.

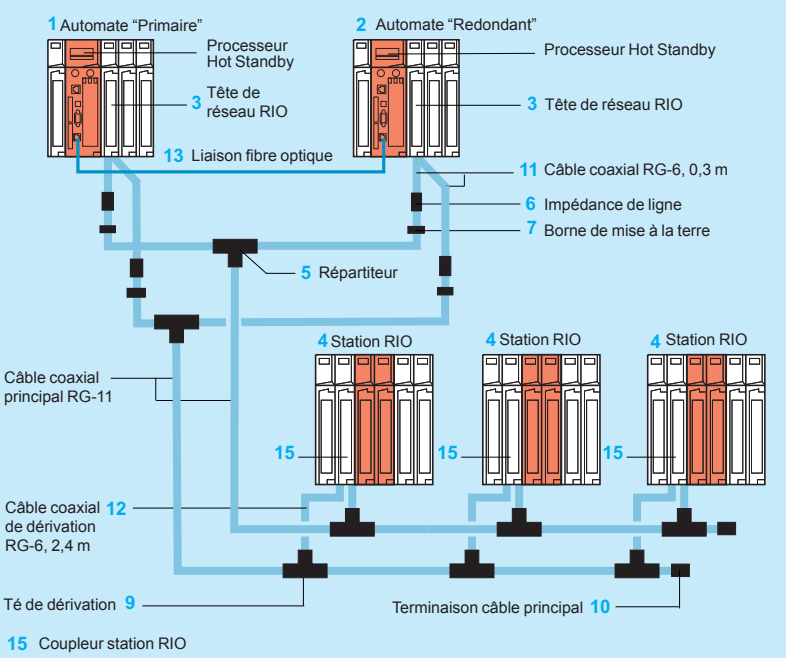
Plate-forme d'automatisme Modicon Quantum
Architectures de sécurité Hot Standby

Architecture de sécurité Hot Standby
Architecture entrées/sorties décentralisées (RIO)

Ces stations d'entrées/sorties, constituées de modules Quantum, sont reconnues et configurées depuis l'environnement de programmation du logiciel Unity Pro XL Safety.
Elles bénéficient d'une scrutation synchrone par rapport au temps de cycle.

Un répartiteur 5 **MA0186100** est utilisé pour permettre l'échange des E/S des stations RIO 4 avec les automates "Primaire" 1 et "Redondant" 2.
Les impédances de ligne 6 **520411000** permettent de conserver une ligne adaptée lorsque la déconnexion de l'un des processeurs E/S est nécessaire. Les bornes de mise à la terre 7 **600545000**, facultatives, permettent de maintenir, dans ces conditions, la mise à la terre du câble coaxial.

La disponibilité de ce système d'entrées/sorties est renforcée par l'utilisation d'un système de câblage des E/S en double médium.



***Nota** : repères 1 à 15, voir page 43480/17.*

Les constituants sont proposés en ensembles.
Par exemple, la configuration ci-dessous peut être réalisée avec :
- 1 ensemble de répartition **140CHS32000**,
- 4 ensembles de connexion de tête de réseau **RPXKITCRP**,
- 6 ensembles de dérivation vers station **RPXKIT6F**,
- 1 câble coaxial principal RG-11 : par exemple en rouleau de 320 m, **975951000**, voir page 43488/7.

Plate-forme d'automatisme Modicon Quantum
Architectures de sécurité Hot Standby

140CPU67160S

Références

Processeur Hot Standby de sécurité avec Unity Pro XL Safety

Processeur Hot Standby		Capacité mémoire application maxi		Fibre optique	Ports de communication	Sécurité	Référence	Masse
Fréquence horloge	Coprocesseur	RAM interne disponible (avec variables référencées)	Avec carte PCMCIA	Type et distance maxi				
MHz		Ko	Ko					kg/lb
266 MHz	Oui, Ethernet TCP/IP intégré, usage réservé Hot Standby	1024	7168	multimode 2 km	1 Modbus *(1)* 1 Modbus Plus 1 USB 1 port Ethernet 100 Mbit/s, dédié Hot Standby	Oui	**140CPU67160S**	–

140NOE77111

Coupleurs associés

Désignation	Type d'architecture	Topologie	Transparent Ready	Rep. *(2)*	Sécurité	Référence	Masse kg/lb
Coupleur tête de réseau RIO	E/S décentralisées (RIO) et mixte	Câble redondant	–	3	Non interférent	**140CRP93200** **140CRP93200C**	–
Coupleur de station RIO				15	Non interférent	**140CRA93200** **140CRA93200C**	–
Répéteur fibre optique de station RIO *(3)*	E/S décentralisées (RIO)	Fibre optique multimode (unique ou redondant)	–	–	Non interférent	**140NRP95400** **140NRP95400C**	–
		Fibre optique monomode (unique ou redondant)	–	–	Non interférent	**140NRP95401C**	–
Coupleur réseau Ethernet Modbus/TCP	Mixte	Bus ou anneau (cuivre ou fibre optique)	Classe C30	–	Non interférent	**140NOE77111** **140NOE77111C**	–

(1) Port Modbus RS 232/RS 485.
(2) Repères, voir page 43480/16.
(3) Module déclarable et configurable dans Unity Pro XLSafety version 7.0 et ultérieures. Ce module peut cependant être utilisé sans être déclaré avec les versions antérieures de Unity Pro XLS.

***Nota** : Pour tout accessoire et raccord, voir page 43489/3.*