

Modicon M580

Manuel de sécurité

Traduction de la notice originale

QGH46983.10
06/2024

Mentions légales

Les informations fournies dans ce document contiennent des descriptions générales, des caractéristiques techniques et/ou des recommandations concernant des produits/solutions.

Ce document n'est pas destiné à remplacer une étude détaillée ou un plan de développement ou de représentation opérationnel et propre au site. Il ne doit pas être utilisé pour déterminer l'adéquation ou la fiabilité des produits/solutions pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur individuel d'effectuer, ou de faire effectuer par un professionnel de son choix (intégrateur, spécificateur ou équivalent), l'analyse de risques exhaustive appropriée ainsi que l'évaluation et les tests des produits/solutions par rapport à l'application ou l'utilisation particulière envisagée.

La marque Schneider Electric et toutes les marques de commerce de Schneider Electric SE et de ses filiales mentionnées dans ce document sont la propriété de Schneider Electric SE ou de ses filiales. Toutes les autres marques peuvent être des marques de commerce de leurs propriétaires respectifs.

Ce document et son contenu sont protégés par les lois sur la propriété intellectuelle applicables et sont fournis à titre d'information uniquement. Aucune partie de ce document ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), à quelque fin que ce soit, sans l'autorisation écrite préalable de Schneider Electric.

Schneider Electric n'accorde aucun droit ni aucune licence d'utilisation commerciale de ce document ou de son contenu, sauf dans le cadre d'une licence non exclusive et personnelle, pour le consulter tel quel.

Schneider Electric se réserve le droit d'apporter à tout moment des modifications ou des mises à jour relatives au contenu de ce document ou à son format, sans préavis.

Dans la mesure permise par la loi applicable, Schneider Electric et ses filiales déclinent toute responsabilité en cas d'erreurs ou d'omissions dans le contenu informatif du présent document ou pour toute conséquence résultant de l'utilisation des informations qu'il contient.

Table des matières

Consignes de sécurité	9
Avant de commencer	10
Démarrage et test.....	11
Fonctionnement et réglages	12
À propos de ce manuel	13
Fonction de sécurité M580	20
Fonction de sécurité du M580.....	21
Normes et certifications	25
Certifications	26
Normes et certifications.....	30
Modules pris en charge par le système de sécurité M580	31
Modules certifiés pour le système de sécurité M580	32
Modules non perturbateurs.....	34
Cybersécurité du système de sécurité M580	39
Cybersécurité pour le système de sécurité M580	39
Cycle de vie des applications	40
Cycle de vie des applications.....	40
Modules d'E/S de sécurité M580	50
Caractéristiques communes des modules d'E/S de sécurité M580	51
Présentation des modules d'E/S de sécurité M580	51
Présentation des diagnostics pour le M580 Modules d'E/S de sécurité.....	53
Module d'entrée analogique du BMXSAI0410	56
Module d'entrée analogique de sécurité BMXSAI0410.....	56
Connecteur de câblage du BMXSAI0410	58
Exemples de câblage d'application du module d'entrée BMXSAI0410.....	60
Structure des données du BMXSAI0410.....	66
Module d'entrée numérique du BMXSDI1602	70
Module d'entrée numérique de sécurité BMXSDI1602	70
Connecteur de câblage du BMXSDI1602.....	72
Exemples de câblage pour les applications du du BMXSDI1602.....	78
Structure des données du BMXSDI1602.....	98
Module de sortie numérique du BMXSDO0802.....	103
Module de sortie numérique de sécurité BMXSDO0802.....	103

Connecteur de câblage du BMXSDO0802	105
Exemples de câblage d'application du module de sortie	
BMXSDO0802.....	107
Structure des données du BMXSDO0802	113
Module de sortie relais numérique du BMXSRA0405.....	118
Module de sortie relais numérique de sécurité BMXSRA0405	118
Connecteur de câblage du BMXSRA0405	119
Exemples de câblage d'application du module de sortie	
BMXSRA0405	121
Structure des données du BMXSRA0405	130
Alimentations de sécurité M580.....	135
Alimentations de sécurité du M580	136
Diagnostics des modules d'alimentation de sécurité du M580	139
Type de données dérivé (DDT, Derived Data Type)M580.....	141
Validation d'un système de sécurité M580	143
Architectures de modules de sécurité M580.....	144
Architecture de sécurité des CPU et du coprocesseur de sécurité	
M580	144
Architecture de sécurité du module d'entrée analogique	
BMXSAI0410.....	148
Architecture de sécurité du module d'entrée numérique	
BMXSDI1602	149
Architecture de sécurité du module de sortie numérique	
BMXSDO0802.....	150
Architecture de sécurité du module de sortie relais numérique	
BMXSRA0405	152
Valeurs SIL et MTTR des modules de sécurité M580.....	153
Calculs du niveau d'intégrité de la sécurité (SIL).....	153
Calculs de performance et de chronologie d'un système de sécurité	
M580	161
Délai de sécurité du processus	161
Incidence des communications CIP Safety sur le temps de réaction du	
système de sécurité	170
Bibliothèque de sécurité.....	174
Bibliothèque de sécurité	174

Séparation des données dans un système de sécurité M580	178
Séparation des données dans un projet de sécurité M580	179
Procédure de transfert de données entre zones d'espace de nom	182
Communications du système de sécurité M580	184
Synchronisation horaire	185
Configuration de la synchronisation horaire avec le micrologiciel de contrôleur de version 3.10 ou antérieure	185
Synchronisation horaire pour micrologiciel de CPU de version 3.20 ou ultérieure	190
Communication d'égal à égal	192
Communication d'égal à égal	192
Architecture d'égal à égal avec micrologiciel d'UC de version 3.10 ou antérieure	193
Configuration du bloc de fonction dérivé (DFB, Derived Function Block) S_ WR_ETH_MX dans la logique de programme du contrôleur récepteur	200
Configuration du bloc DFB S_RD_ETH_MX dans la logique de programme du contrôleur récepteur	202
Architecture d'égal à égal avec micrologiciel d'UC de version 3.20 ou ultérieure	206
Configuration du bloc DFB S_WR_ETH_MX2 dans la logique de programme du contrôleur récepteur	214
Configuration du bloc de fonction dérivé (DFB, Derived Function Block) S_ RD_ETH_MX2 dans la logique de programme du contrôleur d'automatisation programmable (PAC) récepteur	216
Communications par canal noir M580	221
Communication de l'UC M580 vers les E/S de sécurité	223
M580 Communications entre PAC de sécurité et E/S	223
Diagnostics d'un système de sécurité M580	225
Diagnostics de l'UC et du coprocesseur de sécurité M580	226
Diagnostic de la condition bloquante	226
Diagnostics de condition non bloquante	229
Diagnostics par voyant LED de la CPU de sécurité du M580	231
Diagnostics par LED du coprocesseur de sécurité M580	234
Voyant d'accès de la carte mémoire	236
Diagnostics des alimentations de sécurité M580	239

Diagnostics fournis par les voyants LED de l'alimentation	239
Diagnostics du module d'entrée analogique BMXSAI0410	241
Diagnostics DDDT du BMXSAI0410	241
Diagnostics par voyant LED du module d'entrée analogique BMXSAI0410	242
Diagnostics du module d'entrée numérique BMXSDI1602	246
Diagnostics DDDT du BMXSDI1602	246
Diagnostics par voyant LED du module d'entrée numérique BMXSDI1602	248
Diagnostics du module de sortie numérique BMXSDO0802	252
Diagnostics DDDT du BMXSDO0802	252
Diagnostics par voyant LED du module de sortie numérique BMXSDO0802	254
Diagnostics du module de sortie relais numérique BMXSRA0405	258
Diagnostics DDDT du BMXSRA0405	258
Diagnostics par voyant LED du module de sortie relais numérique BMXSRA0405	259
Utilisation d'un système de sécurité M580	262
Zones de données de processus, sécurité et globale dans Control Expert	263
Séparation des données dans Control Expert	264
Modes de fonctionnement, états de fonctionnement et tâches	268
Modes de fonctionnement du contrôleur de sécurité M580	268
États de fonctionnement du contrôleur de sécurité M580	273
Séquences de démarrage	279
Tâches du contrôleur de sécurité M580	283
Création d'un projet de sécurité M580	287
Génération d'un projet de sécurité M580	287
Signature SAFE	287
Verrouillage de la configuration des modules d'E/S de sécurité M580	295
Verrouillage de la configuration des modules d'E/S de sécurité M580	295
Initialisation des données dans Control Expert	298
Initialisation des données dans Control Expert pour le PAC de sécurité M580	298
Utilisation des tables d'animation dans Control Expert	299

Tables d'animations et écrans des opérateurs	299
Ajout de sections de code	304
Ajout d'un code à un projet de sécurité M580	304
Requête de diagnostic.....	308
Commandes de permutation et d'effacement	311
Gestion de la sécurité de l'application.....	314
Application Protection	314
Safety-Related Area Password Protection	321
Program Unit, Section and Subroutine Password and Protection	325
Protection du micrologiciel.....	328
Data Storage/Web Protection	330
Perte du mot de passe	332
Gestion de la sécurité des stations de travail	339
Gestion de l'accès au EcoStruxure Control Expert.....	339
Droits d'accès.....	342
Modifications apportées à Control Expert pour le système de sécurité M580	355
Transfert et importation de projets et de code de sécurité M580 dans Control Expert	355
Enregistrement et restauration de données entre un fichier et le PAC.....	356
Fonction CCOTF pour un PAC de sécurité M580.....	356
Modifications apportées aux outils du PAC de sécurité M580	358
CIP Safety	360
Présentation du protocole CIP Safety pour les PAC de sécurité M580.....	361
Communication CIP Safety.....	361
Configuration de la CPU CIP Safety M580.....	365
Configuration de l'identifiant OUNID de la CPU	365
Configuration de l'équipement CIP Safety cible.....	367
Présentation de la configuration de l'équipement CIP Safety	367
Configuration de l'équipement CIP Safety à l'aide d'un outil fourni par le fabricant.....	369
Configuration des DTM des équipements de sécurité	371
Utilisation des DTM.....	371
DTM d'équipements de sécurité - Informations sur le fichier et le fabricant.....	374

DTM d'équipements de sécurité - Numéro du réseau de sécurité.....	375
DTM d'équipements de sécurité - Vérification et validation de la configuration	377
DTM d'équipements de sécurité - Connexions d'E/S.....	378
Vérification de l'identité de l'équipement distant.....	381
DTM d'équipements de sécurité - Paramètres des connexions d'E/S	382
Paramètres d'adresse IP de l'équipement de sécurité	383
Opérations CIP Safety	385
Transfert d'une application CIP Safety depuis Control Expert vers le PAC	385
Structure d'une requête SafetyOpen de type 2	386
Opérations de l'équipement CIP Safety	387
Interactions entre les opérations du contrôleur de sécurité et la connexion cible.....	389
Commandes du DTM CIP Safety	393
Diagnostic CIP Safety	395
DDDT de l'équipement CIP Safety	395
Codes d'erreur de l'équipement CIP Safety.....	398
DDDT de la CPU CIP Safety autonome	402
Diagnostics du DTM du régulateur	402
Diagnostics de connexion de l'équipement CIP Safety	403
Annexes	407
CEI 61508	408
Informations générales relatives à la norme IEC 61508	409
Stratégie SIL	411
Objets système	416
M580 - Bits système de sécurité	417
Mots système de sécurité du système M580.....	419
Références SRAC.....	423
Glossaire.....	429
Index.....	434

Consignes de sécurité

Informations importantes

Lisez attentivement ces instructions et examinez le matériel pour vous familiariser avec l'appareil avant de tenter de l'installer, de le faire fonctionner, de le réparer ou d'assurer sa maintenance. Les messages spéciaux suivants que vous trouverez dans cette documentation ou sur l'appareil ont pour but de vous mettre en garde contre des risques potentiels ou d'attirer votre attention sur des informations qui clarifient ou simplifient une procédure.



La présence de ce symbole sur une étiquette “Danger” ou “Avertissement” signale un risque d'électrocution qui provoquera des blessures physiques en cas de non-respect des consignes de sécurité.



Ce symbole est le symbole d'alerte de sécurité. Il vous avertit d'un risque de blessures corporelles. Respectez scrupuleusement les consignes de sécurité associées à ce symbole pour éviter de vous blesser ou de mettre votre vie en danger.

DANGER

DANGER signale un risque qui, en cas de non-respect des consignes de sécurité, **provoque** la mort ou des blessures graves.

AVERTISSEMENT

AVERTISSEMENT signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** la mort ou des blessures graves.

ATTENTION

ATTENTION signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** des blessures légères ou moyennement graves.

AVIS

AVIS indique des pratiques n'entraînant pas de risques corporels.

Remarque Importante

L'installation, l'utilisation, la réparation et la maintenance des équipements électriques doivent être assurées par du personnel qualifié uniquement. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de ce matériel.

Une personne qualifiée est une personne disposant de compétences et de connaissances dans le domaine de la construction, du fonctionnement et de l'installation des équipements électriques, et ayant suivi une formation en sécurité leur permettant d'identifier et d'éviter les risques encourus.

Avant de commencer

N'utilisez pas ce produit sur les machines non pourvues de protection efficace du point de fonctionnement. L'absence de ce type de protection sur une machine présente un risque de blessures graves pour l'opérateur.

 **AVERTISSEMENT**

EQUIPEMENT NON PROTEGE

- N'utilisez pas ce logiciel ni les automatismes associés sur des appareils non équipés de protection du point de fonctionnement.
- N'accédez pas aux machines pendant leur fonctionnement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Cet automate et le logiciel associé permettent de commander des processus industriels divers. Le type ou le modèle d'automatisme approprié pour chaque application dépendra de facteurs tels que la fonction de commande requise, le degré de protection exigé, les méthodes de production, des conditions inhabituelles, la législation, etc. Dans certaines applications, plusieurs processeurs seront nécessaires, notamment lorsque la redondance de sauvegarde est requise.

Vous seul, en tant que constructeur de machine ou intégrateur de système, pouvez connaître toutes les conditions et facteurs présents lors de la configuration, de l'exploitation et de la maintenance de la machine, et êtes donc en mesure de déterminer les équipements automatisés, ainsi que les sécurités et verrouillages associés qui peuvent être utilisés correctement. Lors du choix de l'automatisme et du système de commande, ainsi que du logiciel associé pour une application particulière, vous devez respecter les normes et réglementations locales et nationales en vigueur. Le document National Safety Council's Accident Prevention Manual (reconnu aux Etats-Unis) fournit également de nombreuses informations utiles.

Dans certaines applications, telles que les machines d'emballage, une protection supplémentaire, comme celle du point de fonctionnement, doit être fournie pour l'opérateur. Elle est nécessaire si les mains ou d'autres parties du corps de l'opérateur peuvent entrer dans la zone de point de pincement ou d'autres zones dangereuses, risquant ainsi de provoquer des blessures graves. Les produits logiciels seuls, ne peuvent en aucun cas protéger les opérateurs contre d'éventuelles blessures. C'est pourquoi le logiciel ne doit pas remplacer la protection de point de fonctionnement ou s'y substituer.

Avant de mettre l'équipement en service, assurez-vous que les dispositifs de sécurité et de verrouillage mécaniques et/ou électriques appropriés liés à la protection du point de fonctionnement ont été installés et sont opérationnels. Tous les dispositifs de sécurité et de verrouillage liés à la protection du point de fonctionnement doivent être coordonnés avec la programmation des équipements et logiciels d'automatisation associés.

NOTE: La coordination des dispositifs de sécurité et de verrouillage mécaniques/électriques du point de fonctionnement n'entre pas dans le cadre de cette bibliothèque de blocs fonction, du Guide utilisateur système ou de toute autre mise en œuvre référencée dans la documentation.

Démarrage et test

Avant toute utilisation de l'équipement de commande électrique et des automatismes en vue d'un fonctionnement normal après installation, un technicien qualifié doit procéder à un test de démarrage afin de vérifier que l'équipement fonctionne correctement. Il est essentiel de planifier une telle vérification et d'accorder suffisamment de temps pour la réalisation de ce test dans sa totalité.

▲ AVERTISSEMENT

RISQUES INHERENTS AU FONCTIONNEMENT DE L'EQUIPEMENT

- Assurez-vous que toutes les procédures d'installation et de configuration ont été respectées.
- Avant de réaliser les tests de fonctionnement, retirez tous les blocs ou autres cales temporaires utilisés pour le transport de tous les dispositifs composant le système.
- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Effectuez tous les tests de démarrage recommandés dans la documentation de l'équipement. Conservez toute la documentation de l'équipement pour référence ultérieure.

Les tests logiciels doivent être réalisés à la fois en environnement simulé et réel

Vérifiez que le système entier est exempt de tout court-circuit et mise à la terre temporaire non installée conformément aux réglementations locales (conformément au National Electrical Code des Etats-Unis, par exemple). Si des tests diélectriques sont nécessaires, suivez les recommandations figurant dans la documentation de l'équipement afin d'éviter de l'endommager accidentellement.

Avant de mettre l'équipement sous tension :

- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.
- Fermez le capot du boîtier de l'équipement.
- Retirez toutes les mises à la terre temporaires des câbles d'alimentation entrants.
- Effectuez tous les tests de démarrage recommandés par le fabricant.

Fonctionnement et réglages

Les précautions suivantes sont extraites du document NEMA Standards Publication ICS 7.1-1995 :

(En cas de divergence ou de contradiction entre une traduction et l'original anglais, le texte original en anglais prévaudra.)

- Malgré le soin apporté à la conception et à la fabrication de l'équipement ou au choix et à l'évaluation des composants, des risques subsistent en cas d'utilisation inappropriée de l'équipement.
- Il arrive parfois que l'équipement soit dérégulé accidentellement, entraînant ainsi un fonctionnement non satisfaisant ou non sécurisé. Respectez toujours les instructions du fabricant pour effectuer les réglages fonctionnels. Les personnes ayant accès à ces réglages doivent connaître les instructions du fabricant de l'équipement et les machines utilisées avec l'équipement électrique.
- L'opérateur ne doit avoir accès qu'aux réglages fonctionnels dont il a besoin. L'accès aux autres commandes doit être limité afin d'empêcher les changements non autorisés des caractéristiques de fonctionnement.

À propos de ce manuel

Objectif du document

Cette documentation s'adresse au personnel qualifié connaissant bien la sécurité fonctionnelle et le logiciel Control Expert Safety. La mise en service et l'utilisation du système de sécurité M580 doivent être effectuées uniquement par des personnes autorisées en accord avec les normes de sécurité fonctionnelle établies.

NOTE:

- La version originale de ce manuel est le texte anglais.
- En cas de demande de modification ou de problème de qualité en rapport avec l'offre de sécurité M580, veuillez contacter votre service clientèle local pour obtenir une assistance technique. Vous trouverez des informations complémentaires dans la section *Assistance / Nous contacter* du site Web de Schneider Electric à l'adresse :

www.se.com/b2b/en/support/

Champ d'application

Ce document s'applique à EcoStruxure™ Control Expert 16.0 avec ControlExpert_V160_HF001 M580 Safety ou les versions ultérieures.

Documents à consulter

Titre de documentation	Référence
M580, Conditions d'application liées à la sécurité — Plan de vérification	EIO0000004540 (ENG) EIO0000004741 (FRE) EIO0000004742 (GER) EIO0000004744 (ITA) EIO0000004743 (SPA) EIO0000004745 (CHS)
Modicon M580 - Guide de planification du système de sécurité	QGH60283 (Anglais), QGH60284 (Français), QGH60285 (Allemand), QGH60286 (Espagnol), QGH60287 (Italien), QGH60288 (Chinois)
EcoStruxure™ Control Expert, Safety Block Library	QGH60275 (Anglais), QGH60278 (Français), QGH60279 (Allemand), QGH60280 (Italien), QGH60281 (Espagnol), QGH60282 (Chinois)

Titre de documentation	Référence
Plates-formes automate Modicon - Cybersécurité, Manuel de référence	EIO0000001999 (Anglais), EIO0000002001 (Français), EIO0000002000 (Allemand), EIO0000002002 (Italien), EIO0000002003 (Espagnol), EIO0000002004 (Chinois)
Modicon M580 - Redondance d'UC, Guide de planification du système pour architectures courantes	NHA58880 (Anglais), NHA58881 (Français), NHA58882 (Allemand), NHA58883 (Italien), NHA58884 (Espagnol), NHA58885 (Chinois)
Modicon M580 - Matériel, Manuel de référence	EIO0000001578 (Anglais), EIO0000001579 (Français), EIO0000001580 (Allemand), EIO0000001582 (Italien), EIO0000001581 (Espagnol), EIO0000001583 (Chinois)
Modicon M580 Autonome, Guide de planification du système pour architectures courantes	HRB62666 (Anglais), HRB65318 (Français), HRB65319 (Allemand), HRB65320 (Italien), HRB65321 (Espagnol), HRB65322 (Chinois)
Modicon M580 - Guide de planification du système pour topologies complexes	NHA58892 (Anglais), NHA58893 (Français), NHA58894 (Allemand), NHA58895 (Italien), NHA58896 (Espagnol), NHA58897 (Chinois)
EcoStruxure™ Automation Device Maintenance - Guide utilisateur	EIO0000004033 (Anglais), EIO0000004048 (Français), EIO0000004046 (Allemand), EIO0000004049 (Italien), EIO0000004047 (Espagnol), EIO0000004050 (Chinois)
Unity Loader - Manuel de l'utilisateur	33003805 (Anglais), 33003806 (Français), 33003807 (Allemand), 33003809 (Italien), 33003808 (Espagnol), 33003810 (Chinois)
EcoStruxure™ Control Expert, Modes de fonctionnement	33003101 (Anglais), 33003102 (Français), 33003103 (Allemand), 33003104 (Espagnol), 33003696 (Italien), 33003697 (Chinois)
EcoStruxure™ Control Expert - Bits et mots système, Manuel de référence	EIO0000002135 (Anglais), EIO0000002136 (Français), EIO0000002137 (Allemand), EIO0000002138 (Italien), EIO0000002139 (Espagnol), EIO0000002140 (Chinois)

Pour rechercher des documents en ligne, visitez le centre de téléchargement Schneider Electric (www.se.com/ww/en/download/).

Information spécifique au produit

DANGER

RISQUE DE CHOC ÉLECTRIQUE, D'EXPLOSION OU D'ARC ÉLECTRIQUE

- Coupez l'alimentation de tous les équipements, y compris les appareils connectés, avant de retirer des caches ou des portes d'accès ou avant d'installer ou de retirer des accessoires, matériels, câbles ou fils, sauf dans les cas de figure spécifiquement indiqués dans le guide de référence du matériel correspondant à cet équipement.
- Utilisez toujours un appareil de mesure de tension réglé correctement pour vous assurer que l'alimentation est coupée lorsque cette précaution est mentionnée.
- Remettez en place et fixez tous les caches, accessoires, matériels, câbles et fils, puis vérifiez que l'équipement est correctement relié à la terre avant de le mettre sous tension.
- Utilisez uniquement la tension indiquée pour faire fonctionner l'équipement et les produits associés.

Le non-respect de ces instructions provoquera la mort ou des blessures graves.

▲ AVERTISSEMENT

PERTE DE CONTRÔLE

- Réalisez une analyse des modes de défaillance et de leurs effets (FMEA) ou une analyse de risques équivalente sur l'application et appliquez les contrôles de prévention et de détection appropriés avant la mise en œuvre.
- Prévoyez un état de repli pour les événements ou séquences de commande indésirables.
- Le cas échéant, prévoyez des chemins de commande séparés et redondants.
- Définissez les paramètres appropriés, notamment pour les limites.
- Examinez les conséquences des retards de transmission et prenez les mesures correctives nécessaires.
- Examinez les conséquences des interruptions de la liaison de communication et prenez des mesures correctives nécessaires.
- Prévoyez des chemins indépendants pour les fonctions de commande critiques (arrêt d'urgence, dépassement de limites, conditions d'erreur, etc.) en fonction de votre évaluation des risques ainsi que des réglementations et consignes applicables.
- Appliquez les réglementations et les consignes locales de sécurité et de prévention des accidents.¹
- Testez chaque mise en œuvre d'un système pour vérifier son bon fonctionnement avant de l'utiliser en environnement de production.

Le non-respect de ces consignes peut entraîner la mort, des blessures graves ou des dommages matériels.

¹ Pour plus d'informations, consultez le document NEMA ICS 1.1 (dernière édition), « Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control » (Directives de sécurité pour l'application, l'installation et la maintenance de commande statique) et le document NEMA ICS 7.1 (dernière édition), « Safety Standards for Construction and Guide for Selection, Installation, and Operation of Adjustable-Speed Drive Systems » (Normes de sécurité relatives à la construction et manuel de sélection, installation et opération de variateurs de vitesse) ou son équivalent en vigueur dans votre pays.

⚠ AVERTISSEMENT

FONCTIONNEMENT INATTENDU DE L'ÉQUIPEMENT

- N'utilisez que le logiciel approuvé par Schneider Electric pour faire fonctionner cet équipement.
- Mettez à jour votre programme d'application chaque fois que vous modifiez la configuration matérielle physique.

Le non-respect de ces consignes peut entraîner la mort, des blessures graves ou des dommages matériels.

Informations concernant la terminologie inclusive/sensible

Schneider Electric s'efforce de mettre constamment à jour ses communications et ses produits pour respecter ses engagements en matière de terminologie inclusive/sensible. Il se peut malgré tout que nos contenus présentent encore des termes jugés inappropriés par certains clients.

Terminologie utilisée dans les normes

Les termes techniques, la terminologie, les symboles et les descriptions correspondantes employés dans ce manuel ou figurant sur les produits eux-mêmes proviennent généralement des normes internationales.

Dans le domaine des systèmes de sécurité fonctionnelle, des variateurs et de l'automatisme en général, il s'agit par exemple de termes tels que *sécurité*, *fonction de sécurité*, *état sécurisé*, *défaut*, *réinitialisation de défaut*, *dysfonctionnement*, *panne*, *erreur*, *message d'erreur*, *dangereux*, etc.

Ces normes incluent entre autres les éléments suivants :

Norme	Description
IEC 61131-2:2007	Automates programmables, partie 2 : Spécifications et essais des équipements.
ISO 13849-1:2023	Sécurité des machines : Composants liés à la sécurité dans les systèmes de commande. Principes généraux de conception

Norme	Description
EN 61496-1:2020	Sécurité des machines : Equipement de protection électrosensible. Partie 1 : Exigences générales et tests.
ISO 12100:2010	Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque
EN 60204-1:2006	Sécurité des machines - Equipement électrique des machines - Partie 1 : exigences générales
ISO 14119:2013	Sécurité des machines - Dispositifs de verrouillage associés à des protecteurs - Principes de conception et de choix
ISO 13850:2015	Sécurité des machines - Fonction d'arrêt d'urgence - Principes de conception
IEC 62061:2021	Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électrique, électronique et électronique programmables relatifs à la sécurité
IEC 61508-1:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Exigences générales.
IEC 61508-2:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Exigences concernant la sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité.
IEC 61508-3:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Configuration logicielle requise.
IEC 61784-3:2021	Réseaux de communication industriels - Profils - Partie 3 : Bus de terrain liés à la sécurité fonctionnelle - Règles générales et définitions de profil.
2006/42/EC	Directive Machines
2014/30/EU	Directive sur la compatibilité électromagnétique
2014/35/EU	Directive sur les basses tensions

De plus, des termes utilisés dans le présent document peuvent provenir d'autres normes telles que :

Norme	Description
Série IEC 60034	Machines électriques rotatives
Série IEC 61800	Entraînements électriques de puissance à vitesse variable
Série IEC 61158	Communications numériques pour les systèmes de mesure et de commande – Bus de terrain utilisés dans les systèmes de commande industriels

Enfin, le terme *zone de fonctionnement* peut être utilisé dans le contexte de la description de dangers spécifiques et a la même signification que *zone à risque* ou *zone dangereuse* dans la directive *Machines (2006/42/EC)* et *ISO 12100:2010*.

NOTE: Les normes susmentionnées peuvent s'appliquer ou pas aux produits cités dans la présente documentation. Pour plus d'informations sur chacune des normes applicables aux produits décrits dans le présent document, consultez les tableaux de caractéristiques de ces références de produit.

Fonction de sécurité M580

Introduction

Ce chapitre présente la fonction de sécurité M580 pour le système de sécurité M580 et pour chaque module de sécurité.

Fonction de sécurité du M580

Présentation de la fonction de sécurité du M580

En utilisant Control Expert avec la sécurité, vous pouvez programmer, configurer et maintenir une application de sécurité. Lors de la conception et de la programmation de cette application, vous appliquez des fonctions de sécurité aux seuls composants d'une boucle de sécurité.

NOTE: N'incluez dans une boucle de sécurité que des modules de sécurité, leurs paramètres de configuration et leurs données.

Après la mise en service, tandis qu'il fonctionne en mode de sécurité, votre système de sécurité M580 lit périodiquement les entrées de sécurité, traite la logique de sécurité du programme de l'application, effectue des diagnostics et applique les résultats de la logique aux sorties de sécurité.

Si les diagnostics du contrôleur ou des E/S détectent une erreur, le système de sécurité place la partie concernée du système dans un état sécurisé défini. En fonction de la nature de l'erreur détectée, la réponse de sécurité peut affecter un seul canal d'E/S, un module d'E/S ou le système tout entier dans l'état sécurisé défini.

L'état sécurisé défini est l'état non alimenté. Par exemple :

- Si le module d'entrée analogique du BMXSAI0410 ou le module d'entrée numérique du BMXSDI1602 détecte une erreur non récupérable, il définit la valeur de ses entrées dans le contrôleur sur 0 (état non alimenté) et cet état est maintenu jusqu'à ce que la cause sous-jacente soit résolue.
- Si le module de sortie numérique BMXSDO0802 ou le module de sortie relais numérique BMXSRA0405 détecte une erreur non récupérable, il place ses sorties dans l'état non alimenté et elles y restent jusqu'à ce que la cause sous-jacente ait été résolue et le module redémarré.
- Si le module de sortie numérique BMXSDO0802 ou le module de sortie relais numérique BMXSRA0405 détecte une erreur de communication sur une liaison de canal noir au contrôleur, il place ses sorties dans leur état de repli.

NOTE: Vous pouvez utiliser Control Expert Safety pour configurer l'état de repli (alimenté, non alimenté ou dernière valeur conservée) en cas de perte de la communication de canal noir entre le contrôleur et le module de sortie.

- Si un contrôleur BMEP58•040S autonome ou un contrôleur BMEH58•040S redondante détecte une erreur de communication sur une liaison de canal noir à un module d'entrée de sécurité, elle règle les entrées concernées sur 0 (non alimenté) jusqu'à ce que le canal noir redevienne opérationnel et que le contrôleur puisse à nouveau lire les valeurs d'entrée réelles.

Boucle de sécurité

Une boucle de sécurité est l'ensemble des équipements et des logiques qui exécutent un processus de sécurité. Un projet de sécurité peut comprendre plusieurs boucles de sécurité. Pour chaque boucle de sécurité, vous devez vérifier que les conditions suivantes sont satisfaites :

- Le temps de sécurité du processus, page 161 est supérieur au temps de réaction du système, page 161.
- La somme des valeurs PFD ou PFH, page 153 de tous les composants de la boucle de sécurité ne dépasse pas le maximum admissible pour les valeurs ciblées suivantes :
 - niveau d'intégrité de la sécurité (1, 2, 3 ou 4)
 - mode de fonctionnement (faible demande ou forte demande)
 - intervalle entre tests périodiques

Incluez exclusivement des équipements de sécurité dans une boucle de sécurité. Certes, vous pouvez ajouter des modules non perturbateurs, page 34 à un projet de sécurité, mais vous ne devez les utiliser que pour des tâches non sécurisées (MAST, FAST, AUX0 ou AUX1).

⚠ AVERTISSEMENT

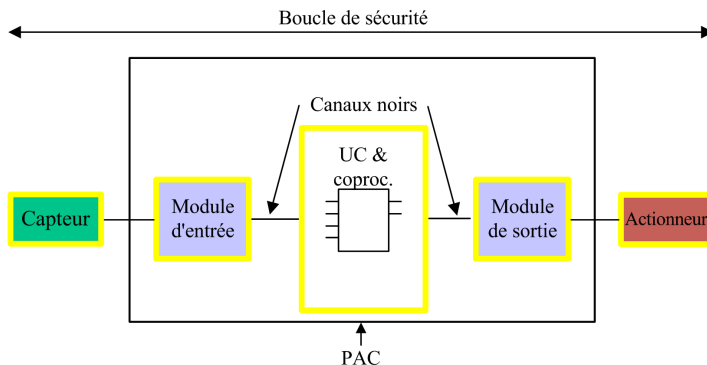
PERTE DE LA CAPACITE A EXECUTER LES FONCTIONS DE SECURITE

- Utilisez uniquement des modules de sécurité pour assurer des fonctions de sécurité.
- N'utilisez pas les entrées ou les sorties de modules non perturbateurs pour les fonctions liées à la sécurité.
- N'utilisez pas de variables de la zone globale pour les fonctions liées à la sécurité.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Vous trouverez une description des variables de la zone globale dans la section *Séparation des données dans un projet de sécurité M580*, page 179.

Boucle de sécurité :



Les équipements de sécurité comprennent les modules de sécurité Schneider Electric M580 suivants :

- contrôleur BME•58•040S et coprocesseur BMEP58CPROS3 :

Le contrôleur et le coprocesseur assurent conjointement les tâches de lecture des entrées de sécurité, de traitement de la logique de sécurité, d'exécution des diagnostics et d'application des résultats aux sorties. Toutes ces tâches font partie de la boucle de sécurité. Les ports utilisés pour les communications par canal noir participent également à la boucle de sécurité. En revanche, d'autres composants du contrôleur tels que le port USB, la carte mémoire SD et la zone de mémoire RAM statique non volatile (nvSRAM) sont en dehors de la boucle de sécurité.

NOTE: Lors d'un démarrage système à froid ou à chaud, le contrôleur et le coprocesseur ne chargent pas les données stockées en mémoire nvSRAM dans la tâche de sécurité (ces données sont utilisées uniquement dans les tâches non liées à la sécurité comme MAST, FAST et AUX). Au lieu de cela, le contrôleur et le coprocesseur appliquent initialement les paramètres de configuration par défaut provenant de la carte mémoire SD, puis ils appliquent les valeurs reçues directement des entrées au cours du fonctionnement.

- Modules d'E/S de sécurité (BMXSAI0410, BMXSDI1602, BMXSDO0802 et BMXSRA0405) :

Les fonctions qui consistent à envoyer les signaux d'entrée, à recevoir les signaux de sortie et à effectuer les diagnostics font partie de la boucle de sécurité.

- Alimentations BMXCPS4002S, BMXCPS4022S et BMXCPS3522S :

Ces alimentations de sécurité assurent la détection des surtensions et cela fait partie de la boucle de sécurité. Comme la fiabilité de chaque alimentation (c'est-à-dire son taux de défaillances dangereuses) est plus de 100 fois supérieure au seuil défini pour la norme SIL3, ces alimentations de sécurité ne sont pas incluses dans les calculs du niveau d'intégrité de la sécurité d'une boucle de sécurité.

La boucle de sécurité comprend également des équipements qui ne sont pas propres à la sécurité :

- Capteurs, actionneurs et leur câblage aux modules d'E/S de sécurité. Ces derniers effectuent des diagnostics de câblage pour les capteurs et les actionneurs pour mieux gérer la boucle de sécurité.

NOTE: Lors de la conception de votre application de sécurité, vous devez identifier les caractéristiques des capteurs et des actionneurs (notamment leurs valeurs de PFD/PFH).

Normes et certifications

Introduction

Ce chapitre décrit les normes et certifications qui s'appliquent au système de sécurité M580 et aux modules qui le composent.

Certifications

Normes de certification du contrôleur d'automatisation programmable (PAC) de sécurité M580

Le contrôleur d'automatisation programmable (PAC) de sécurité M580 est certifié par TÜV Rheinland Group pour une utilisation dans des applications allant jusqu'à :

- SIL3 / CEI 61508 / CEI 61511
- SIL4/EN 50126 (CEI 62278), EN 50128 (CEI 62279), EN 50129 (CEI 62245)
- SIL CL3 / CEI 62061
- PLe, Cat. 4 / ISO 13849-1

Pour plus d'informations sur le calibrage SIL, reportez-vous à la section [Description du calibrage SIL](#), page 412.

Spécifications des contrôleurs programmables

- IEC 61131-2 : contrôleurs programmables - Partie 2 : Spécifications et essais des équipements.
- CEI/EN 61010-2-201, UL 61010-2-201, CSA -C22.2 No. 61010-2-201 : Exigences de sécurité pour les équipements électriques - Partie 2-201 : Exigences particulières pour les équipements de contrôle.

Caractéristiques environnementales

Reportez-vous aux [Normes et certifications M580](#), page 30 pour connaître les niveaux des tests d'environnement.

Exemples de spécifications de zones

Pour États-Unis et Canada : Zone dangereuse classe I, division 2, groupes A, B, C et D

- CSA 22.2 No213, ANSI/ISA12.12.01 et FM3611

Pour les autres pays : CE ATEX (directive 2014/34/EU) ou IECEx dans une zone à atmosphère définie de zone 2 (gaz) et/ou de zone 22 (poussière)

- IEC/EN 60079-0 ; IEC/EN 60079-7; IEC/EN 60079-15

Spécifications des systèmes d'automatisation de distribution électrique

- IEC/EN 61000-6-5 Compatibilité électromagnétique - Partie 6-5 : Normes génériques - Immunité pour les environnements de station d'alimentation et de sous-station.
- IEC/EN 61850-3 Réseaux et systèmes de communication pour l'automatisation des services de distribution d'énergie - Partie 3 : règles générales

Pour plus d'informations sur les limites d'installation, consultez le document M580 Normes et certifications, page 30.

Spécifications ferroviaires

- EN 45545–2 / IEC 60332–3–24: Applications ferroviaires - Essai de résistance au feu des câbles pour trains.
- EN 50126 / CEI 62278 : Applications ferroviaires - Spécification et démonstration de fiabilité, de disponibilité, de maintenabilité et de sécurité (RAMS).
- EN 50128 / CEI 62279 : Applications ferroviaires - Systèmes de communication, de signalisation et de traitement - Logiciel pour les systèmes de contrôle et de protection ferroviaires.
- EN 50129 / CEI 62245 : Applications ferroviaires - Systèmes de communication, de signalisation et de traitement - Systèmes électroniques liés à la sécurité pour la signalisation.
- EN 50155 / CEI 60571 : Applications ferroviaires - Matériel roulant - Équipement électronique.
- EN 50121-3-2 / CEI 62236-3-2 : Applications ferroviaires - Compatibilité électromagnétique - Partie 3-2 : Matériel roulant - Appareil.
- EN 50121-4 / CEI 62236-4 : Applications ferroviaires - Compatibilité électromagnétique - Partie 4 : Émission et immunité de l'appareil de signalisation et de télécommunication.
- EN 50121-5 / CEI 62236-5 : Applications ferroviaires - Compatibilité électromagnétique - Partie 5 : Émission et immunité des installations et appareils d'alimentation fixes.
- EN 50125-1 : Chemin de fer - Conditions environnementales pour l'équipement - Partie 1 : Matériel roulant et matériel embarqué.
- EN 50125-3 : Chemin de fer - Conditions environnementales pour l'équipement - Partie 3 : Équipement de signalisation et de télécommunication.

- EN 50124-1 : Chemin de fer - Coordination de l'isolation - Partie 1 : Exigences de base - Dégagements et distances de fuite pour tous les équipements électriques et électroniques.

Pour plus d'informations sur les limites d'installation, consultez le document M580 Normes et certifications, page 30.

Spécifications de sécurité fonctionnelle

- IEC/EN 61000-6-7 Compatibilité électromagnétique - Partie 6-7 : Normes génériques - Exigences d'immunité pour les équipements destinés à exécuter des fonctions dans un système lié à la sécurité (sécurité fonctionnelle) sur des sites industriels.
- IEC 61326-3-1 : Équipement électrique pour la mesure, le contrôle et l'utilisation en laboratoire - Partie 3-1 : Exigences d'immunité pour les systèmes liés à la sécurité et les équipements destinés à exécuter des fonctions liées à la sécurité - Application industrielle générale.
- CEI 61508 : Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Partie 1-7, édition 2.0.
- la norme IEC 61511-1 : Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur de l'industrie des processus - Partie 1 : Configuration, définitions, exigences système, matériel et logiciel.
- la norme IEC 61511-2 : Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur de l'industrie des processus - Partie 2 : Directives pour l'application de la norme CEI 61511-1.
- la norme IEC 61511-3 : Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur de l'industrie des processus - Partie 3 : Conseils pour déterminer les niveaux d'intégrité de sécurité requis.

Spécifications de sécurité des machines

- IEC/EN 62061 Sécurité des machines - Sécurité fonctionnelle des systèmes de contrôle électriques, électroniques et électroniques programmables liés à la sécurité
- ISO EN 13849-1 : Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1 : Principes généraux de conception

Sécurité fonctionnelle dans les spécifications des systèmes

- EN 54-2 : Systèmes de détection et d'alarme incendie Partie 2 : Contrôle et signalisation des équipements.
- EN 50156-1 : Équipement électrique pour fours et équipements auxiliaires - Partie 1 : Exigences pour la conception et l'installation de l'application.
- EN 50130-4 : Systèmes d'alarme - Partie 4 : Compatibilité électromagnétique - Norme de la famille de produits : Exigences d'immunité pour les composants des systèmes d'alarme incendie, d'intrusion, de maintien, de vidéosurveillance, de contrôle d'accès et d'alarme sociale.
- EN 298 : Systèmes de contrôle automatique du brûleur pour brûleurs et appareils brûlant des combustibles gazeux ou liquides.
- NFPA 85 : Code des dangers liés aux systèmes de chaudière et de combustion.
- NFPA 86 : Standard pour fours et fourneaux.
- NFPA 72 : Code d'alarme et de signalisation incendie national.

Remarques

Vous trouverez la liste complète des normes (avec leurs révisions et leurs dates) qui sont certifiées par TÜV sur le site Web :

www.certipedia.com ou <https://fs-products.tuvasi.com/certificates>.

Normes et certifications

Télécharger

Cliquez sur le lien correspondant à votre langue favorite pour télécharger les normes et les certifications (format PDF) qui s'appliquent aux modules de cette gamme de produits :

Titre	Langues
Plates-formes Modicon M580, M340 et X80 I/O, Normes et certifications	• Anglais : EIO0000002726 • Français : EIO0000002727 • Allemand : EIO0000002728 • Italien : EIO0000002730 • Espagnol : EIO0000002729 • Chinois : EIO0000002731

Modules pris en charge par le système de sécurité M580

Introduction

Un projet de sécurité M580 peut inclure à la fois des modules de sécurité et d'autres types de modules (non liés à la sécurité). Vous pouvez utiliser :

- Des modules de sécurité dans la tâche SAFE.
- Des modules non liés à la sécurité uniquement pour les tâches non liées à la sécurité (MAST, FAST, AUX0 et AUX1)

NOTE: Vous pouvez ajouter des modules non liés à la sécurité à un projet de sécurité s'ils ne perturbent pas la fonction de sécurité.

Utilisez exclusivement le logiciel de programmation Control Expert de Schneider Electric pour la programmation, la mise en service et l'exploitation de votre application de sécurité M580.

- Control Expert L Safety fournit toutes les fonctionnalités de Control Expert L et peut être utilisé avec les contrôleurs de sécurité BMEP582040S et BMEH582040S .
- Control Expert XL Safety fournit toutes les fonctionnalités de Control Expert XL et peut s'utiliser avec tous les contrôleurs de sécurité BMEP58•040S et BMEH58•040S .

Cette section répertorie les modules de sécurité et non liés à la sécurité pris en charge par le système de sécurité M580.

Modules certifiés pour le système de sécurité M580

Modules certifiés

Le contrôleur d'automatisation programmable (PAC) de sécurité du M580 est un système de sécurité certifié par TÜV Rheinland Group, selon :

- SIL3 / IEC 61508 / IEC 61511
- SIL4 / EN 50126 (IEC 62278), EN 50128 (IEC 62279), EN 50129 (IEC 62245)
- SIL CL3 / IEC 62061
- PLe, Cat. 4 / ISO 13849-1
- CIP Safety IEC 61784-3

Seules les versions du produit de sécurité et du logiciel Control Expert mentionnées dans la liste de révision du certificat TÜV sont conformes pour une utilisation de sécurité.

Les informations les plus récentes sur les versions de produit certifiées sont disponibles sur le site Web de TÜV Rheinland Group : <https://www.certipedia.com/> or <https://fs-products.tuvasi.com/>.

Elles sont basées sur la famille M580 de contrôleurs d'automatisation programmables (ou PAC, Programmable Automation Controllers) Les modules de sécurité M580 Schneider Electric suivants sont certifiés :

- Contrôleur autonome BMEP582040S
- Contrôleur autonome BMEP584040S
- Contrôleur autonome BMEP586040S
- Contrôleur redondant BMEH582040S
- Contrôleur redondant BMEH584040S
- Contrôleur redondant BMEH586040S
- Coprocesseur BMEP58CPROS3
- Module d'entrée analogique BMXSAI0410
- Module d'entrée numérique BMXSDI1602
- Module de sortie numérique BMXSDO0802
- Module de sortie relais numérique BMXSRA0405
- Alimentation BMXCPS4002S
- Alimentation BMXCPS4022S
- Alimentation BMXCPS3522S

NOTE: Outre les modules de sécurité répertoriés ci-dessus, vous pouvez également inclure les modules non liés à la sécurité non perturbateurs, page 34 à un projet de sécurité.

NOTE: L'offre de sécurité Modicon cible au maximum le niveau 3 d'intégrité de la sécurité (SIL3) (reg. IEC 61508) et PLe (reg. ISO 13849), ce qui signifie qu'elle est également compatible avec les niveaux SIL1/SIL2 et PL a, b, c, d.

NOTE:

- Chaque fois que SIL2 ou SIL3 est mentionné dans le document sans référence standard, cela concerne IEC 61508 / IEC 61511.
- Chaque fois que SIL2 est mentionné, il s'agit également du niveau SIL3 selon EN 50126 / EN 50128 / EN 50129.
- Chaque fois que SIL3 est mentionné, il s'agit également du niveau SIL4 selon EN 50126 / EN 50128 / EN 50129.

Remplacement d'un contrôleur

Il est possible de remplacer un contrôleur BME•58•040S par un autre BME•58•040S. Toutefois, ce remplacement ne fonctionne pas si les limites suivantes sont dépassées :

- nombre d'E/S
- nombre de stations d'E/S
- nombre de variables
- taille de la mémoire de l'application

Consultez les rubriques :

- *Compatibilité de la configuration* dans le *Guide de planification du système de redondance de CPU Modicon M580 pour architectures courantes* pour une description des applications Control Expert compatibles avec les contrôleurs de sécurité et de redondance.
- *Caractéristiques des performances des contrôleurs et coprocesseurs M580* dans le *Guide de planification du système de sécurité Modicon M580* pour une description des limitations des contrôleurs.

Modules non perturbateurs

Introduction

Un projet de sécurité M580 peut inclure à la fois des modules de sécurité et d'autres types de modules (non liés à la sécurité). Vous ne pouvez utiliser des modules non liés à la sécurité, que pour des tâches non liées à la sécurité. Vous pouvez ajouter des modules non liés à la sécurité à un projet de sécurité s'ils ne perturbent pas la fonction de sécurité.

Qu'est-ce qu'un module non interférent ?

NOTE: Vérifiez que les données d'entrée et les données de sortie des modules non perturbateurs ne sont pas utilisées pour le contrôle des sorties liées à la sécurité. Les modules sans fonction de sécurité peuvent traiter uniquement des données non sécurisées.

Un module non interférent est un module qui ne risque pas de perturber la fonction de sécurité. Pour les modules M580 dans embase (BMEx, BMXx, PMXx et PMEx), il existe deux types de modules non perturbateurs :

- **Type 1** : un module de type 1 peut être installé dans la même embase que des modules de sécurité (lorsque le module de sécurité est placé dans l'embase rack principale ou dans une embase étendue).
- **Type 2** : un module non interférent de type 2 ne peut pas être installé dans la même embase principale que des modules de sécurité (lorsque le module de sécurité est placé dans l'embase principale ou dans une embase étendue).

NOTE: Les modules de type 1 et de type 2 sont répertoriés sur les sites web de TÜV Rheinland aux adresses www.certipedia.com/certificates et <https://fs-products.tuvasi.com/certificates>.

Pour les modules Mx80 qui ne sont pas dans une embase, tous les équipements Ethernet (DIO ou DRS) peuvent être considérés comme non perturbateurs et donc utilisés dans un système de sécurité M580.

Modules non perturbateurs de type 1 pour les applications SIL3

Les modules ci-dessous non liés à la sécurité peuvent être considérés comme non perturbateurs de type 1 dans un système de sécurité M580.

NOTE: La liste des modules non liés à la sécurité non perturbateurs de type 1 peut être modifiée de temps en temps. La liste actuelle est disponible sur le site Web de TÜV Rheinland à l'adresse <https://fs-products.tuvasi.com/certificates>.

Type de module	Référence du module
Embase 4 emplacements	BMEXBP0400
Embase 8 emplacements	BMEXBP0800
Embase 12 emplacements	BMEXBP1200
Embase 16 emplacements	BMEXBP1600
Embase 4 emplacements	BMXXBP0400
Embase 6 emplacements	BMXXBP0600
Embase 8 emplacements	BMXXBP0800
Embase 12 emplacements	BMXXBP1200
Embase 16 emplacements	BMXXBP1600
Embase 6 emplacements avec emplacements doubles pour alimentations redondantes	BMEXBP0602
Embase 10 emplacements avec emplacements doubles pour alimentations redondantes	BMEXBP1002
Embase 14 emplacements avec emplacements doubles pour alimentations redondantes	BMEXBP1402
Communication : adaptateur de station Ethernet X80 Performance 1 canal	BMXCRA31210
Communication : adaptateur de station Ethernet X80 Performance 1 canal	BMECRA31210
Communication : module Ethernet avec services Web standard	BMENOC0301
Communication : module Ethernet avec transfert IP	BMENOC0321
Communication : module Ethernet avec services Web FactoryCast	BMENOC0311
Communication : module d'extension d'embase	BMXXBE1000
Communication : AS-Interface	BMXEIA0100
Communication : données globales	BMXNGD0100
Communication : convertisseur fibre MM/LC 2 canaux 100 Mb	BMXNRP0200
Communication : convertisseur fibre SM/LC 2 canaux 100 Mb	BMXNRP0201
Communication : module de communication IEC 61850 M580	BMENOP0300

Type de module	Référence du module
Communication : serveur OPC UA intégré	BMENUA0100
Compteur : module SSI 3 canaux	BMXEAE0300
Compteur : compteur rapide 2 canaux	BMXEHC0200
Compteur : compteur rapide 8 canaux	BMXEHC0800
Mouvement : PTO (sortie à train d'impulsions) 2 canaux indépendants	BMXMSP0200
Analogique : HART à courant isolé 8 entrées analogiques	BMEAH10812
Analogique : HART à courant isolé 4 sorties analogiques	BMEAH00412
Analogique : 4 entrées analogiques rapides isolées tension/courant	BMXAMI0410
Analogique : 4 entrées analogiques rapides non isolées tension/courant	BMXAMI0800
Analogique : 8 entrées analogiques rapides isolées tension/courant	BMXAMI0810
Analogique : 4 entrées et 4 sorties analogiques tension/courant	BMXAMM0600
Analogique : 2 sorties analogiques isolées tension/courant	BMXAMO0210
Analogique : 4 sorties analogiques isolées tension/courant	BMXAMO0410
Analogique : 8 sorties analogiques non isolées courant	BMXAMO0802
Analogique : 4 entrées analogiques isolées TC/RTD	BMXART0414.2
Analogique : 8 entrées analogiques isolées TC/RTD	BMXART0814.2
TOR : 8 entrées numériques 220 VCA	BMXDAI0805
TOR : 8 entrées numériques isolées 100 à 120 VCA	BMXDAI0814
TOR : 16 entrées numériques 24 VCA/24 VCC logique négative	BMXDAI1602
TOR : 16 entrées numériques 48 VCA	BMXDAI1603
TOR : 16 entrées numériques 100 à 120 VCA 20 broches	BMXDAI1604
TOR : 16 entrées numériques supervisées canaux 100 à 120 VCA 40 broches	BMXDAI1614
TOR : 16 entrées numériques supervisées canaux 200 à 240 VCA 40 broches	BMXDAI1615
TOR : 16 sorties numériques triacs 100 à 240 VCA 20 broches	BMXDAO1605
TOR : 16 sorties numériques triacs 24 à 240 VCA 40 broches	BMXDAO1615
TOR : 16 entrées numériques 24 VCC logique positive	BMXDDI1602
TOR : 16 entrées numériques 48 VCC logique positive	BMXDDI1603
TOR : 16 entrées numériques 125 VCC logique positive	BMXDDI1604T
TOR : 32 entrées numériques 24 VCC logique positive	BMXDDI3202K

Type de module	Référence du module
TOR : 64 entrées numériques 24 VCC logique positive	BMXDDI6402K
TOR : 8 entrées numériques 24 VCC 8 S logique négative Tr	BMXDDM16022
TOR : 8 entrées numériques 24 VCC 8 S relais	BMXDDM16025
TOR : 16 entrées numériques 24 VCC 16 S logique négative Tr	BMXDDM3202K
TOR : 16 sorties numériques trans logique positive 0,5 A	BMXDDO1602
TOR : 16 sorties numériques trans logique négative	BMXDDO1612
TOR : 32 sorties numériques trans logique positive 0,5 A	BMXDDO3202
	BMXDDO3202H
TOR : 32 sorties numériques trans logique positive 0,1 A	BMXDDO3202K
TOR : 64 sorties numériques trans logique positive 0,1 A	BMXDDO6402K
TOR : 8 sorties numériques 125 VCC	BMXDRA0804T
TOR : 8 sorties numériques isolées 24 VCC ou 24 à 240 VCA relais	BMXDRA0805
TOR : 16 sorties numériques relais non isolées canaux 5 à 125 VCC ou 25 à 240 VCA	BMXDRA0815
TOR : 16 sorties numériques relais	BMXDRA1605
TOR : sortie relais numérique NC 5 à 125 VCC ou 24 à 240 VCA	BMXDRC0805
TOR : 16 entrées numériques 24/125 VCC horodatage	BMXERT1604
Commutateur d'option réseau Mx80	BMENOS0300
Entrée fréquence turbomachines 2 canaux	BMXETM0200
Module Profibus DP/DPV1 maître	PMEPXM0100
Module RTU avancé MX80	BMENOR2200H

Modules non perturbateurs de type 2 pour applications SIL2/3

Les modules ci-dessous dans une embase et non liés à la sécurité peuvent être considérés comme non perturbateurs de type 2 dans un système de sécurité M580.

NOTE: La liste des modules non liés à la sécurité non perturbateurs de type 2 peut être modifiée de temps en temps. La liste actuelle est disponible sur le site Web de TÜV Rheinland à l'adresse <https://fs-products.tuvsi.com/certificates>.

Type de module	Référence du module
Communication : adaptateur de station Ethernet X80 Standard 1 canal	BMXCRA31200
Alimentation CA standard	BMXCPS2000
Alimentation CC isolée standard	BMXCPS2010
Alimentation haute puissance isolée 24 à 48 VCC	BMXCPS3020
Alimentation 125 VCC redondante standard	BMXCPS3522
Alimentation 24/48 VCC redondante standard	BMXCPS4022
Alimentation CA redondante standard	BMXCPS4002
Alimentation CA haute puissance	BMXCPS3500
Alimentation CC haute puissance	BMXCPS3540T
Communication : module de bus 2 ports RS485/232	BMXNOM0200
TOR : 32 entrées numériques 12/24 VCC logique positive ou négative	BMX DDI 3232
TOR : 32 entrées numériques 48 VCC logique positive	BMXDDI3203
Maître CANopen X80	BMECXM0100
Module de pesage	PMESWT0100
Module de diagnostic partenaire	PMXCDA0400
Module de communication universel Ethernet TCP Open	PMEUCM0302

NOTE: Tous les équipements d'un système M580 reliés à des modules de sécurité via Ethernet sont considérés comme non perturbateurs. Par conséquent, tous les modules des gammes Quantum et STB Advantys (non enfichables dans la même embase que les modules de sécurité M580) sont des modules non perturbateurs de type 2.

Cybersécurité du système de sécurité M580

Introduction

Ce chapitre évoque les informations disponibles pour développer une approche de la cybersécurité pour le PAC de sécurité M580.

Cybersécurité pour le système de sécurité M580

Référence de cybersécurité

Le but d'une stratégie de cybersécurité est de réduire, autant que possible, la vulnérabilité d'un système de sécurité aux cyberattaques. Pour plus d'informations sur le développement d'une stratégie de cybersécurité pour votre système de sécurité M580, consultez le manuel *Modicon Controllers Platform Cybersecurity Reference Manual* (Référence EIO0000001999 (EN)).

Cycle de vie des applications

Introduction

Cycle de vie des applications

Introduction

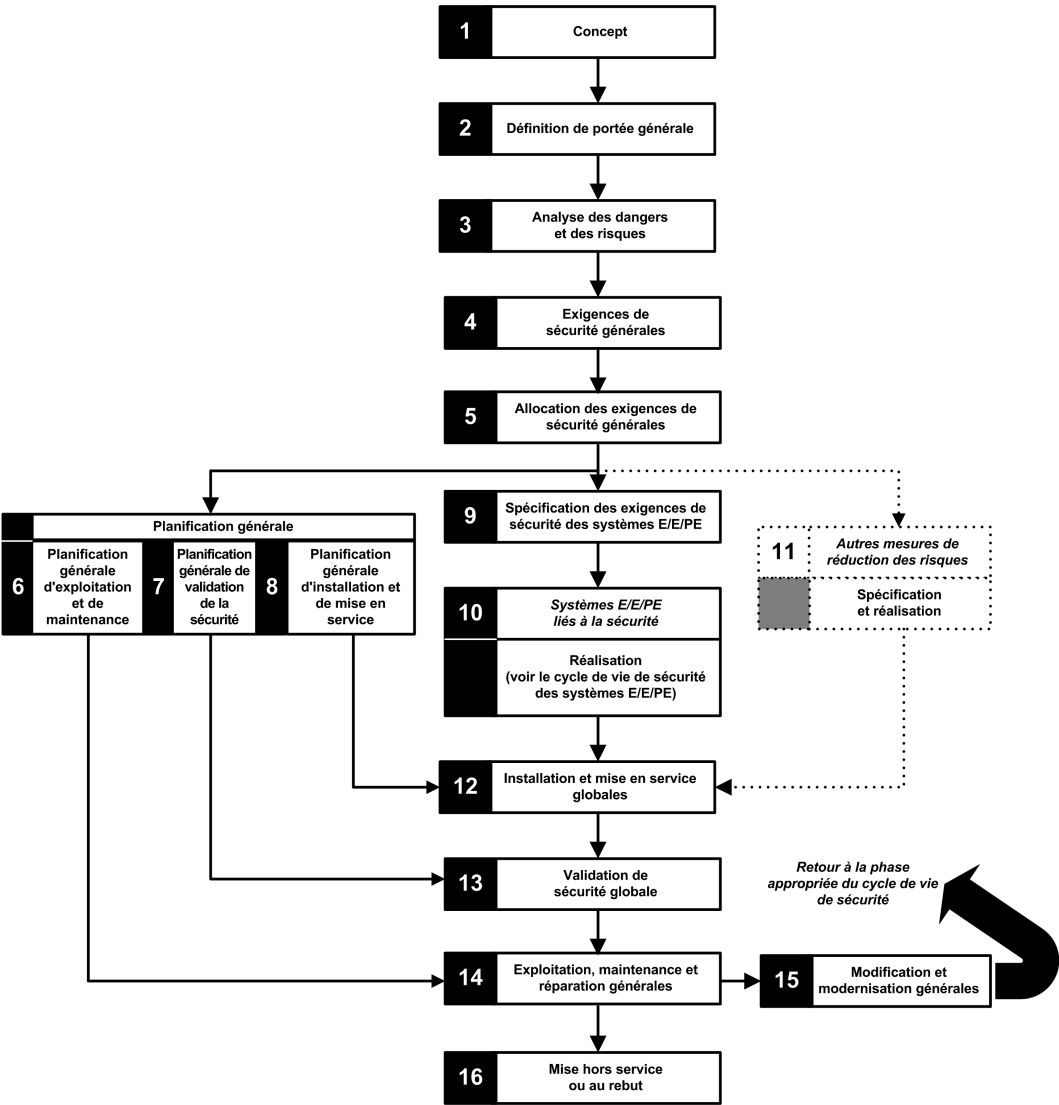
Lors de la conception d'une application de sécurité, suivez les recommandations de l'une des normes de sécurité qui s'appliquent à votre domaine d'application. La plupart des normes d'application dérivent de la norme générique CEI 61508 ou sont liées à celle-ci, notamment la norme sur l'industrie des procédés (CEI 61511), les normes sur l'industrie des machines (CEI 62061 et ISO 13489), la norme sur l'industrie nucléaire (CEI 61513), les normes sur les chemins de fer (EN 5012x), etc.

La norme IEC 61508 définit le cycle de vie d'une application sous la forme d'une séquence d'étapes. Chaque étape remplit un rôle défini, nécessite des documents d'entrée obligatoires et produit des documents de sortie. La décision d'utiliser un système intégré de sécurité (SIS) est prise à la fin de l'étape d'allocation des besoins en matière de sécurité (étape 5).

Cette section définit les vérifications nécessaires liées à l'utilisation d'un système de sécurité M580 que vous devez effectuer lors des étapes suivantes :

9.	Spécification des exigences de sécurité des systèmes E/E/PE
10.	Réalisation de systèmes liés à la sécurité E/E/PE
12.	Installation et mise en service globales
13.	Validation de sécurité globale
14.	Exploitation, maintenance et réparation générales
15.	Modification et modernisation générales

Le diagramme suivant présente une vue d'ensemble du cycle de vie d'une application de sécurité :



Étape 9 : Spécification des exigences de sécurité des systèmes E/E/PE

Cette étape a lieu lorsque l'analyse des risques est terminée et a fourni (entre autres) les informations suivantes :

- Définition des fonctions intégrées de sécurité
- Performances exigées desdites fonctions (temps, réduction des risques, niveau SIL, etc.)
- Modes de défaillance de ces fonctions

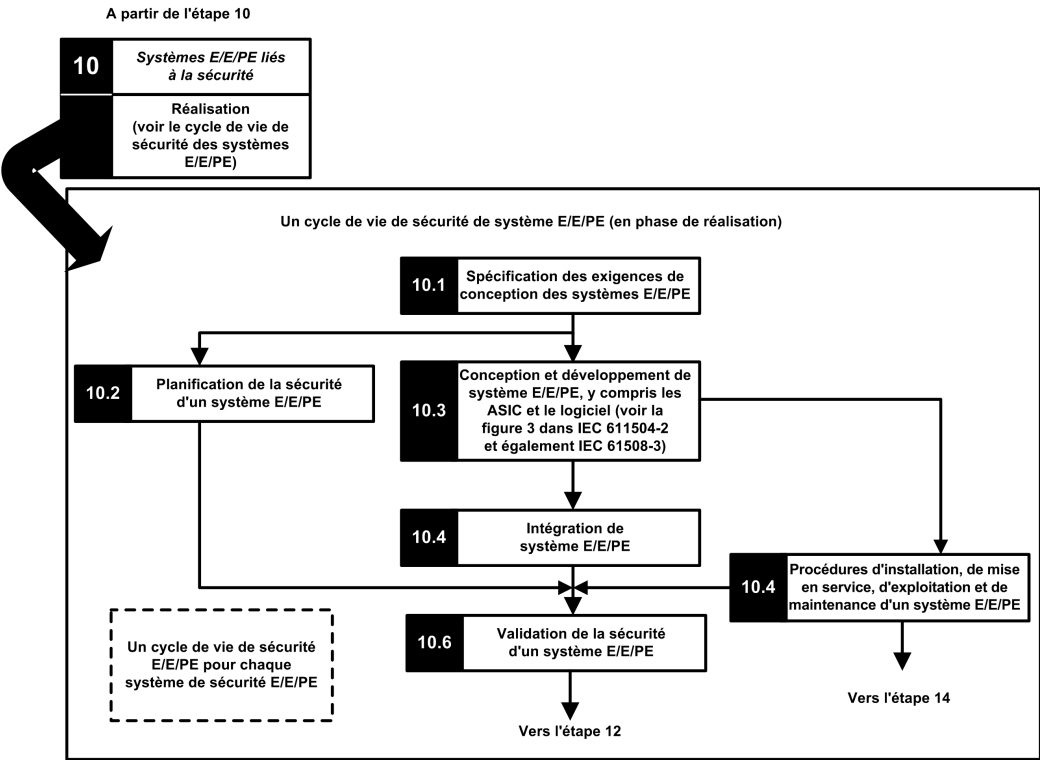
Elle doit produire les spécifications du besoin en matière de sécurité, lesquelles comprendront au minimum les informations suivantes nécessaires à la conception d'une application sécurisée à l'aide de n'importe quel type de contrôleur d'automatisation programmable (PAC) de sécurité :

- État sécurisé défini des fonctions de sécurité intégrées
- Analyse du mode de fonctionnement du SIS (y compris le comportement en mode de marche, d'arrêt, de mise sous tension, de maintenance, de réparation, etc.)
- Intervalle de test de la fonction de sécurité (SIF)
- MTTR du SIS
- Choix d'avoir la SIF alimentée ou non alimentée
- Performance du solveur de logique (temps de réaction, précision, etc.)
- Besoins en matière de performance
 - Tolérance aux défaillances
 - Intégrité
 - Taux maximum de déclenchements infondés
 - Taux maximum de défaillances dangereuses
- Spécifications environnementales (CEM, conditions mécaniques, chimiques, climatiques, etc.)

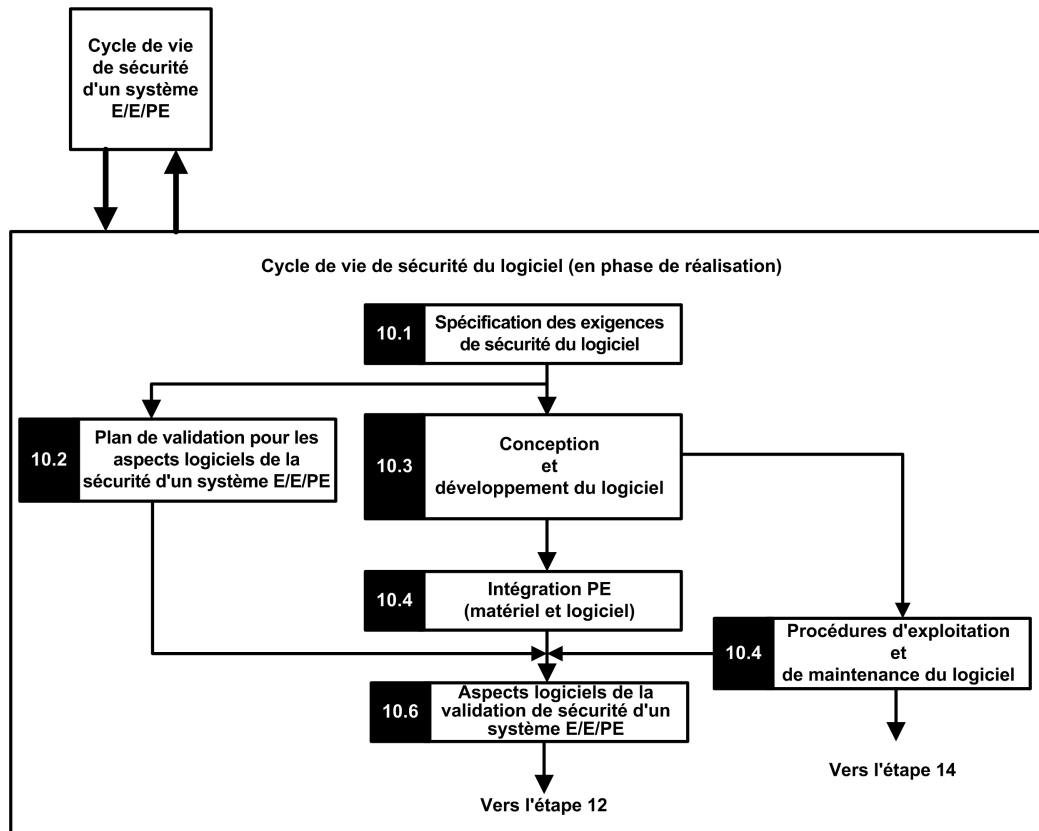
Étape 10 : Réalisation de systèmes liés à la sécurité E/E/PE

La norme IEC 61508 divise cette étape en 2 sous-cycles : un pour la réalisation du système et un pour la réalisation du logiciel.

Réalisation du système :



Réalisation du logiciel :



La première sous-étape (10.1) a pour but de convertir les exigences de sécurité du SIS en spécifications de la conception matérielle, des tests du matériel, de la conception logicielle, des tests du logiciel et des tests d'intégration. Elle doit fournir au minimum les informations suivantes, nécessaires pour concevoir une application sécurisée utilisant le système de sécurité M580 :

- Architecture matérielle, en tenant compte des points suivants :
 - Le respect des règles M580 concernant le mélange des modules de sécurité et non sécurisés : tous les modules de sécurité (modules d'E/S de sécurité et contrôleurs/copresseurs de sécurité) sont placés dans des embases où l'embase principal et l'embase étendu sont alimentés par des blocs d'alimentation dédiés et ne contiennent que des modules de sécurité ou des modules non interférents de type 1.
 - consommation électrique par embase
 - règles de déclassement

- Architecture de l'alimentation :
 - Alimentation TBTS/TBTP uniquement
- Architecture logicielle :
 - y compris l'utilisation de variables globales M580 ; une variable globale ne doit pas empêcher le déclenchement d'une action de sécurité à moins qu'un *protocole d'application sécurisé* soit utilisé.
- Intégration du matériel (câblage, armoire, etc.) :
 - Protection par fusibles.
 - Accessoires pour diagnostic du câblage.
- Interfaces homme-machine :
 - Y compris l'utilisation de variables globales M580 ; une variable globale ne doit pas empêcher le déclenchement d'une action de sécurité à moins qu'un « protocole d'application sécurisé » soit utilisé.
- Interfaces électriques/numériques :
 - état sécurisé défini
 - capteur et actionneur
- Algorithme
- Performances (y compris la définition de la période, du chien de garde et du timeout de la tâche) et prédiction d'un bon comportement à l'aide de la formule :

$$\sum_{\text{toutes tâches}} \frac{Exec_{\text{tâche}}}{Période_{\text{tâche}}} < 80 \%$$

NOTE: Cette formule s'applique uniquement lorsque la tâche MAST n'est pas en mode cyclique.

- Comportement dans les cas suivants :
 - configuration déverrouillée
 - mode de maintenance
 - entrée de maintenance
 - canal non valide
 - interruption de câblage
 - intégrité du canal
 - intégrité du module
- Gestion des identifiants uniques (UID) des modules d'E/S de sécurité (définir quand un UID doit être modifié).

- Serveur NTP :
 - Choix du contrôleur d'automatisation programmable (PAC) en tant que serveur NTP ou serveur NTP externe (en fonction de l'utilisation de l'horodatage des E/S dans l'application de processus)
 - redondance de serveurs
 - perte de serveur

Les sous-étapes suivantes affinent les spécifications en spécifications techniques détaillées, effectuent la conception elle-même, exécutent tous les plans de test et produisent les rapports associés.

Étape 12 : Installation et mise en service globales

Cette étape a pour but de définir les besoins pour les procédures d'installation, de planification des tâches, d'instrumentation et de mise en service, puis de générer le système et de vérifier qu'il est correct.

- Pour les applications redondantes, vérifiez que le timeout de repli, page 164 des modules de sortie de sécurité remplit les conditions définies pour les opérations de permutation, page 166 et de basculement, page 167, puis vérifiez le temps de maintien du CRA.
- Vérifiez que le timeout de sécurité de repli (S_TO) pour les modules de sorties de sécurité est, au moins supérieur à 40 ms ou à $(2,5 * T_{SAFE})$, où T_{SAFE} est égal à la période de la tâche SAFE configurée.
- Effacez toute application préexistante dans l'automate ou utilisez une application configurée sans équipement de sécurité CIP avant d'installer l'équipement de sécurité sur un réseau de sécurité Ethernet (avec équipements de sécurité CIP).

Dans un système de sécurité M580, la procédure de mise en service doit comprendre les points suivants :

- Vérifier l'intégrité de Control Expert : exécution de la fonction d'autotest.
- Vérifier que la version de Control Expert est notifiée dans la liste de révision du certificat TÜV.
- Vérification des versions de micrologiciel du contrôleur et du coprocesseur via la surveillance des mots système %SW14 (version de micrologiciel du processeur de l'automate) et %SW142 (version de micrologiciel du coprocesseur).
- Vérification des adresses de tous les modules (position dans l'embase, commutateurs CRA).

- Vérification du câblage :
 - Vérification point à point : de la variable interne au module d'E/S et à l'actionneur ou au capteur
 - Fusibles
 - équipement de diagnostic du câblage
- À la fin de la procédure, les modules de sécurité sont en mode verrouillage. Incluez la vérification de l'application de sécurité.
- Vérification de la configuration de chaque module (y compris les timeouts)
 - Lisez la configuration à l'aide de l'écran Control Expert et comparez-la à la spécification.
- Toutes les applications de sécurité ont été régénérées à l'aide de l'option **Régénérer tout le projet**, puis téléchargées vers chaque automate, et leur identifiant (SAId) a été enregistré ainsi que leur archive.
- La période et le chien de garde des tâches sont corrects.
- Références et versions des modules.
- Utilisation d'alimentations SELV/PELV uniquement.
- Si l'application de sécurité contient des équipements CIP Safety :
 - L'identifiant de configuration de sécurité (SCID) peut être considéré comme validé (option activée dans le DTM CIP Safety dans Control Expert) et la configuration cible est verrouillée après le test par l'utilisateur.
 - Pour vérifier que la configuration source créée par l'utilisateur à l'aide du logiciel Control Expert a bien été envoyée et enregistrée dans le module source CIP Safety M580, comparez visuellement les paramètres de la configuration cible CIP Safety affichés dans les DDDT cibles (en mode connecté avec le contrôleur d'automatisation programmable (PAC), dans une table d'animation) à ceux affichés et configurés dans l'onglet *Vérification de la configuration*, page 377 du DTM cible. Les valeurs doivent toutes être identiques.
 - Une fois que les configurations de connexion de sécurité ont été appliquées dans le module source CIP Safety M580, testez chacune de ces connexions cibles pour vérifier qu'elles fonctionnent comme prévu.
 - Avant d'installer des équipements CIP Safety dans le réseau de sécurité, attribuez-leur les adresses MAC et les débits appropriés.
- Les téléchargements d'application sont validés au moyen d'un test utilisateur.

Étape 13 : Validation de sécurité globale

Cette étape a pour but de confirmer que le système intégré de sécurité satisfait aux exigences définies. Elle exécute tous les tests et produit les rapports définis à l'étape 7 du « cycle de vie de la sécurité ». Elle doit notamment :

- Vérifier qu'il n'y a pas de condition de dépassement (overrun) au cours d'aucun des états du système (vérification du bit système %S19 dans les tâches MAST, FAST, AUX0) et que le temps d'exécution maximum et actuel de la tâche SAFE (%SW42 et %SW43) sont inférieurs à la période de la tâche SAFE.

$$\sum_{\text{toutes tâches}} \frac{\text{Exec}_{\text{tâche}}}{\text{Période}_{\text{tâche}}} < 80 \%$$

- Vérifiez la formule de charge du contrôleur :
NOTE: Vous pouvez utiliser les mots systèmes %SW110 à %SW115, page 419 pour effectuer une évaluation en temps réel de la charge moyenne pour les tâches du contrôleur (si toutes les tâches sont périodiques, %SW116 doit être inférieur à 80).
- Vérifiez que le temps d'exécution de la tâche FAST (si elle est configurée) est le plus court possible. Il ne doit pas être supérieur à la moitié de la période configurée pour la tâche SAFE.
- Vérifiez les modes de fonctionnement spéciaux (déverrouillage de module, entrée de maintenance, canal non valide, interruption de câblage).
- Pour les applications redondantes, vérifiez que toutes les tâches sont correctement synchronisées à l'aide de la liaison redondante et des bits MAST_SYNCHRONIZED, FAST_SYNCHRONIZED et SAFE_SYNCHRONIZED du DDT T_M_ECPU_HSBY. Reportez-vous au *Modicon M580 - Redondance d'UC, Guide de planification du système pour architectures courantes* pour une description du DDTT_M_ECPU_HSBY.

Étape 14 : Exploitation, maintenance et réparation générales

- Exécuter les tests périodiques à intervalles corrects.
- Surveiller l'identifiant SAId remarque.

NOTE: Tant que le SAId n'a pas changé, la portion de sécurité de l'application n'a pas été modifiée. Voir le bloc fonction S_SYST_STAT_MX pour plus de détails sur le comportement du SAId.

- Surveiller l'état de verrouillage de la configuration de chaque module de sécurité.
- Enregistrer les opérations de réparation.

- Si un module est remplacé, l'équipement de remplacement doit être correctement configuré et vous (l'utilisateur) devez vérifier son bon fonctionnement. Effectuez (au minimum) les opérations de mise en service applicables à ce module.
- Enregistrer les écarts.

Étape 15 : Modification et modernisation générales

Toute modification doit être traitée comme une nouvelle conception. Une analyse d'impact peut permettre de définir quelle partie de l'ancien système de sécurité peut être conservée et quelle partie doit être reconçue.

NOTE: Lorsqu'une modification ne concerne pas l'application sécurisée, utilisez la signature du source SAFE pour vous assurer qu'aucun changement n'a été apporté involontairement au code SAFE. Cette signature permet de vérifier *théoriquement* que l'application n'a pas changé. Elle ne remplace pas le SAId, qui représente l'unique moyen de s'assurer qu'un contrôleur d'automatisation programmable (PAC) exécute bien l'application sécurisée qui a été validée.

Modules d'E/S de sécurité M580

Présentation

Cette section décrit les modules d'E/S de sécurité M580.

Caractéristiques communes des modules d'E/S de sécurité M580

Introduction

Cette section décrit les fonctionnalités partagées ou communes des modules d'E/S de sécurité M580.

Présentation des modules d'E/S de sécurité M580

Introduction

Les quatre modules d'E/S de sécurité M580 suivants sont certifiés pour les applications de sécurité :

- BMXSAI0410 (entrée analogique)
- BMXSDI1602 (entrée numérique)
- BMXSDO0802 (sortie numérique)
- BMXSRA0405 (sortie relais numérique)

Utilisez ces quatre modules d'E/S de sécurité pour connecter le contrôleur d'automatisation programmable (PAC) de sécurité aux capteurs et actionneurs qui composent la boucle de sécurité. Chaque module d'E/S de sécurité inclut un processeur de sécurité dédié. Vous pouvez installer ces modules d'E/S sur l'embase locale ou sur les stations d'E/S distantes (RIO).

Contraintes relatives au lieu d'installation

Installez votre équipement de M580sécurité conformément aux normes suivantes :

- Norme de pollution de degré 2 de l'IEC 60950 concernant la sécurité des équipements informatiques
- Norme de protection IP54 contre la pénétration de corps étrangers de l'IEC 60529, qui stipule à la fois que :
 - La présence de poussière ne perturbe pas le fonctionnement des équipements.
 - La projection d'eau n'a pas d'effet nocif sur les équipements ou leur fonctionnement.

Pour respecter ces normes, il suffit généralement de placer les équipements de sécurité dans une enceinte protégée telle qu'une armoire.

Altitude maximale d'exploitation

L'altitude de fonctionnement maximale pour les modules d'E/S de sécurité M580 est de 2 000 m au-dessus du niveau de la mer.

Communication entre contrôleur d'automatisation programmable (PAC) et E/S

Le contrôleur de sécurité M580 et le coprocesseur contrôlent ensemble tous les échanges de l'embase, tandis que les E/S de sécurité répondent aux commandes du contrôleur et du coprocesseur. Les modules d'E/S de sécurité peuvent être installés dans une embase X Bus BMXXBP**** ou dans une embase Ethernet BMEXBP****.

Les communications entre le contrôleur d'automatisation programmable (PAC) de sécurité et les modules d'E/S de sécurité de l'embase principale locale passent par l'embase.

Les communications entre le contrôleur d'automatisation programmable (PAC) de sécurité et les modules d'E/S de sécurité installés dans une station distante (RIO) passent par un module adaptateur installé sur la station d'E/S distante (RIO), à savoir :

- adaptateur BMXCRA31210 pour une embase Ethernet, ou
- adaptateur BMXCRA31210 , pour une embase X Bus.

NOTE: Avec le micrologiciel de contrôleur de version 3.20 ou ultérieure, la communication entre le contrôleur d'automatisation programmable (PAC) et les E/S de sécurité nécessite un BM•CRA31210 équipé d'un micrologiciel de version 2.60 au minimum.

NOTE: Un adaptateur BMXCRA31200 ne peut pas être utilisé pour connecter des modules d'E/S de sécurité au contrôleur d'automatisation programmable (PAC) de sécurité M580.

Vous pouvez éventuellement utiliser des modules répéteurs à fibre optique BMXNRP0200 ou BMXNRP0201 pour étendre la liaison physique entre le contrôleur et le coprocesseur de l'embase locale et l'adaptateur installé dans la station d'E/S distante (RIO). Ces modules améliorent l'immunité au bruit du réseau d'E/S distantes (RIO) et permettent d'augmenter la distance de câblage tout en conservant l'intégralité de la plage dynamique du réseau et le niveau d'intégrité de la sécurité.

Le protocole de communication assure les échanges entre E/S et contrôleur d'automatisation programmable (PAC) de sécurité. Il permet aux deux équipements de vérifier l'exactitude des données reçues, de détecter les données corrompues et de déterminer si le module émetteur cesse d'être opérationnel. Une boucle de sécurité peut ainsi inclure toute embase et tout adaptateur RIO non parasite, page 34.

Alimentation externe utilisée avec les modules d'E/S de sécurité numériques

Les modules numériques BMXSDI1602 et BMXSDO0802 nécessitent une alimentation externe très basse tension (SELV/PELV) protégée 24 VCC pour alimenter les capteurs et les actionneurs. Les modules d'E/S de sécurité supervisent l'alimentation des processus hors sécurité pour détecter les conditions de tension excessive ou insuffisante.

DANGER

ALIMENTATION SELV/PELV DE CATÉGORIE DE SURTENSION II REQUISE

Utilisez obligatoirement une alimentation de type SELV/PELV de catégorie de surtension II, avec une sortie maximum de 60 VCC, pour alimenter les capteurs et les actionneurs.

Le non-respect de ces instructions provoquera la mort ou des blessures graves.

AVIS

NON-CONFORMITÉ DES CIRCUITS ÉLECTRIQUES

Ne raccordez pas le 0V d'une alimentation SELV à la terre.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Présentation des diagnostics pour le M580 Modules d'E/S de sécurité

Introduction

Chaque module d'E/S de sécurité du M580 présente les fonctions de diagnostic suivantes :

- Autotest au démarrage du module
- Autotest intégré continu en temps réel pendant l'exécution
- Voyants de diagnostic de module et de canal

En outre, les modules d'E/S de sécurité numériques effectuent également des diagnostics de câblage.

Autotest à la mise sous tension

Au moment de la mise sous tension, les modules d'E/S exécutent une série étendue d'autotests. Si ces tests ont pour résultat :

- Succès : les modules sont jugés intègres et sont opérationnels.
- Insuccès : Les modules ne sont pas jugés intègres et ne sont pas opérationnels. Le cas échéant, les entrées sont définies sur 0 et les sorties ne sont plus alimentées.

NOTE: Si l'alimentation externe 24 VCC n'est pas reliée à un module d'entrée numérique ou à un module de sortie numérique, les autotests de mise sous tension ne sont pas effectués et le module ne démarre pas.

Tests intégrés continus

Pendant l'exécution, les modules d'E/S effectuent continuellement des autotests. Les modules d'entrée vérifient qu'ils sont en mesure de lire les données provenant des capteurs sur l'intégralité de la plage. Les modules de sortie vérifient que l'état réel de la sortie est le même que l'état commandé.

Voyants

Chaque module d'E/S de sécurité comporte en face avant des voyants LED de diagnostic du module et des canaux :

- Les quatre voyants LED situés en haut (**Run**, **Err**, **I/O** et **Lck**) décrivent ensemble l'état du module.
- Les deux ou quatre (selon le module) rangées de voyants LED situées en bas se combinent aux quatre voyants LED du haut et indiquent l'état et l'intégrité de chaque canal d'entrée ou de sortie.

Pour chacun des modules d'E/S de sécurité suivants, la section traitant des diagnostics par voyant LED explique comment lire les voyants LED du module concerné :

- Module d'entrée analogique de sécurité du BMXSAI0410 [Diagnostics par voyant LED du module d'entrée analogique BMXSAI0410, page 242](#)
- Module d'entrée numérique de sécurité du BMXSDI1602 [Diagnostics par voyant LED du module d'entrée numérique BMXSDI1602, page 248](#)
- Module de sortie numérique de sécurité du BMXSDO0802 [Diagnostics par voyant LED du module de sortie numérique BMXSDO0802, page 254](#)
- Module de sortie relais numérique de sécurité du BMXSRA0405 [Diagnostics par voyant LED du module de sortie relais numérique BMXSRA0405, page 259](#)

Diagnostique de câblage des modules numériques

Le module d'entrée numérique de sécurité comme le module de sortie numérique de sécurité peuvent détecter les conditions suivantes concernant le câblage des canaux :

- Fil ouvert (ou rompu)
- Court-circuit à la terre 0 V
- Court-circuit sur le 24 VCC
- Circuits croisés entre deux canaux.

NOTE: La disponibilité de ces fonctions de diagnostic dépend de la conception du câblage du module à ses appareils de terrain. Pour plus d'informations, reportez-vous aux exemples de câblage fournis pour les modules d'E/S numériques de sécurité suivants :

- Module d'entrée numérique de sécurité du BMXSDI1602 Exemples de câblage pour les applications du du BMXSDI1602, page 78
- Module de sortie numérique de sécurité du BMXSDO0802 Exemples de câblage d'application du module de sortie BMXSDO0802, page 107

Module d'entrée analogique du BMXSAI0410

Introduction

Cette section décrit les modules d'entrée analogiques de sécurité du BMXSAI0410 .

Module d'entrée analogique de sécurité BMXSAI0410

Introduction

Les caractéristiques du module d'entrée analogique de sécurité BMXSAI0410 sont les suivantes :

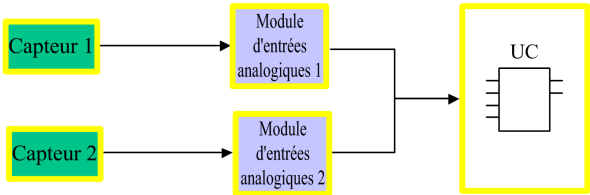
- 4 canaux isolés d'entrée analogique de courant de 4 à 20 mA.
- 12 500 comptages de résolution, couvrant la plage de données de 0 à 25 mA.
- Détection des intensités de courant hors plage pour les valeurs inférieures à 3,75 mA ou supérieures à 20,75 mA.
- Prise en charge des normes SIL3 (IEC61508) suivantes :
 - Le module peut atteindre jusqu'à la catégorie 2 (Cat2) / le niveau de performance d (PLd) à l'aide de 1 voie d'entrée (évaluation un-sur-un (1oo1)). Ainsi, Cat1 et Cat2 / PL a, b, c, d peuvent être atteints à l'aide de 1 voie d'entrée.
 - Le module peut atteindre jusqu'à la catégorie 4 (Cat4) / le niveau de performance e (PLe) à l'aide de 2 voies d'entrée (évaluation un sur deux (1oo2)). Ainsi, Cat3 et Cat4 / PL d, il est possible d'atteindre l'e à l'aide de 2 voies d'entrée.
- Affichage de diagnostics par LED, page 242 pour le module et pour chaque canal d'entrée.
- Permutation de module à chaud pendant le fonctionnement.
- CCOTF (modification de configuration à la volée) pendant le fonctionnement en mode de maintenance, page 269. (La fonction CCOTF n'est pas prise en charge en mode de sécurité, page 268.)

Haute disponibilité

Vous pouvez concevoir votre application de sécurité pour différents niveaux de performance et de disponibilité en utilisant des canaux d'entrée et des modules uniques ou redondants, de la manière suivante :

Conception :	Niveaux de la fonction de sécurité :			
Canaux d'entrée => Modules	SIL	Cat	PL	Haute disponibilité ?
Un seul canal d'entrée sur un seul module d'entrée, page 62	SIL3	Cat 2	PLd	–
Un seul canal d'entrée sur modules d'entrée redondants, page 63	SIL3	Cat 2	PLd	✓
Canaux d'entrée redondants sur un seul module d'entrée, page 64	SIL3	Cat 4	PLe	–
Canaux d'entrée redondants sur modules d'entrée redondants, page 65	SIL3	Cat 4	PLe	✓
✓ : Fourni				
– : Non fourni				

La figure suivante illustre la configuration de modules d'entrée analogique redondants :



Les valeurs analogiques de courant d'entrée fournies par les capteurs 1 et 2 sont envoyées respectivement par les modules d'entrée 1 et 2 à une CPU de sécurité via un contrôleur de sécurité. Le contrôleur exécute un bloc fonction dédié (S_AIHA), (S_AIHA, dans deux programmes logiques compilés distincts pour gérer et sélectionner les données en provenance des deux modules d'entrée. Ce bloc fonction se comporte comme suit :

- Si l'état d'intégrité des données d'entrée en provenance du module 1 est correct, ces données sont utilisées dans la fonction de sécurité.
- Si l'état d'intégrité des données d'entrée en provenance du module 1 n'est pas correct mais que celui des données en provenance du module 2 est correct, les données du module 2 sont utilisées.
- Si l'état d'intégrité des données d'entrée en provenance des deux modules 1 et 2 est incorrect, le système active la fonction de sécurité.

Connecteur de câblage du BMXSAI0410

Introduction

Le module d'entrée analogique du BMXSAI0410 comprend 4 entrées analogiques. Il présente deux paires de broches pour chaque entrée : deux broches de canal (Ch) positives et deux broches communes (Com) négatives.

Pour chaque entrée :

- Les deux broches de canal (Ch n) sont connectées en interne.
- Les deux broches communes (Com n) sont également connectées en interne.

Pour câbler un capteur analogique à une entrée, vous pouvez utiliser l'une ou l'autre broche de canal et l'une ou l'autre broche commune de cette entrée.

Borniers

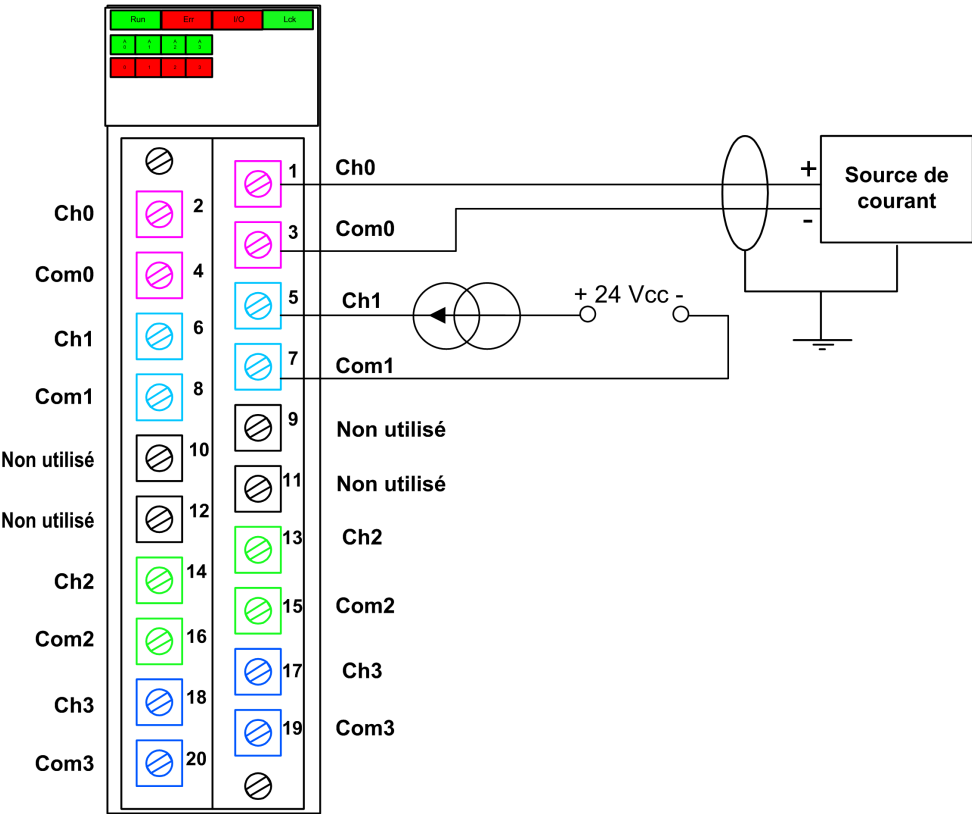
Vous pouvez utiliser les borniers Schneider Electric à 20 points suivants pour le connecteur à 20 broches en face avant du module :

- bornier à vis étriers BMXFTB2010
- bornier à vis à cage BMXFTB2000
- bornier à ressorts BMXFTB2020

NOTE: Il n'est possible de retirer les borniers que lorsque le module est hors tension.

Connecteur de câblage

L'exemple suivant présente un modèle de câblage générique pour les entrées du module :



NOTE: Le module détecte une condition de câble rompu et la signale en tant que condition de courant hors plage (moins de 3,75 mA) en définissant l'élément `OOR` de la structure `T_U_ANA_SIS_CH_IN`, page 69 sur la valeur "1".

Mappage des entrées aux broches du connecteur

Les broches du module d'entrée analogique du BMXSAI0410 sont décrites ci-après :

Description de la broche	Numéro de broche sur le bornier		Description de la broche
Entrée (+) du canal 0	2	1	Entrée (+) du canal 0
Entrée (–) du canal 0	4	3	Entrée (–) du canal 0
Entrée (+) du canal 1	6	5	Entrée (+) du canal 1

Description de la broche	Numéro de broche sur le bornier		Description de la broche
Entrée (–) du canal 1	8	7	Entrée (–) du canal 1
Inutilisée	10	9	Inutilisée
Inutilisée	12	11	Inutilisée
Entrée (+) du canal 2	14	13	Entrée (+) du canal 2
Entrée (–) du canal 2	16	15	Entrée (–) du canal 2
Entrée (+) du canal 3	18	17	Entrée (+) du canal 3
Entrée (–) du canal 3	20	19	Entrée (–) du canal 3

NOTE: Comme les deux broches positives associées à chaque entrée sont connectées en interne, vous n'avez besoin d'utiliser qu'une seule broche positive d'un canal d'entrée. De la même manière, les deux broches négatives associées à chaque entrée sont connectées en interne et vous n'avez besoin d'en utiliser qu'une seule.

Par exemple, pour câbler un capteur analogique au canal d'entrée 0, vous pouvez connecter :

- le fil positif du capteur à la broche 1 ou à la broche 2
- le fil négatif du capteur à la broche 3 ou à la broche 4

Exemples de câblage d'application du module d'entrée BMXSAI0410

Introduction

Vous pouvez câbler le module d'entrée analogique de sécurité BMXSAI0410 à des capteurs analogiques pour obtenir la conformité SIL3, et cela de plusieurs manières en fonction des éléments suivants :

- la catégorie (Cat2 ou Cat4) et le niveau de performance (PLd ou PLe) requis
- les exigences de l'application en matière de haute disponibilité

Le niveau d'intégrité de sécurité (SIL) maximum est déterminé par la fiabilité du capteur et la longueur de l'intervalle entre tests périodiques conformément à la norme IEC 61508.

▲ AVERTISSEMENT

PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ

Raccordez les capteurs, qui ne répondent pas à la fiabilité des normes SIL visées, en redondance sur deux canaux.

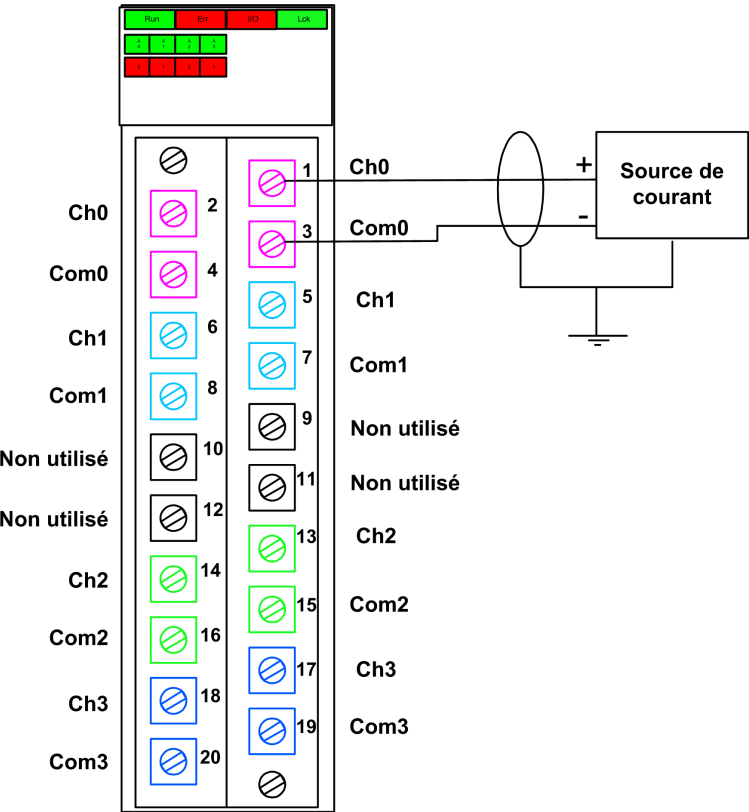
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Les exemples suivants de câblage d'application d'entrée numérique SIL3 sont décrits ci-après :

- Cat2/PLd :
 - capteur unique câblé à une seule entrée
- Cat2/PLd avec haute disponibilité :
 - deux capteurs câblés à deux points d'entrée sur différents modules d'entrée
- Cat4/PLe :
 - deux capteurs câblés à deux points d'entrée distincts du même module d'entrée
- Cat4/PLe avec haute disponibilité :
 - deux paires de capteurs (soit quatre capteurs au total) : les capteurs de la première paire sont câblés chacun à un point d'entrée distinct d'un module et les capteurs de la seconde paire sont câblés chacun à un point d'entrée distinct de l'autre module

SIL3 Cat2/PLd

L'exemple suivant présente un unique capteur câblé à un seul point d'entrée d'un module d'entrée. Le contrôleur effectue l'évaluation 1oo1D sur l'unique valeur surveillée :



⚠ AVERTISSEMENT

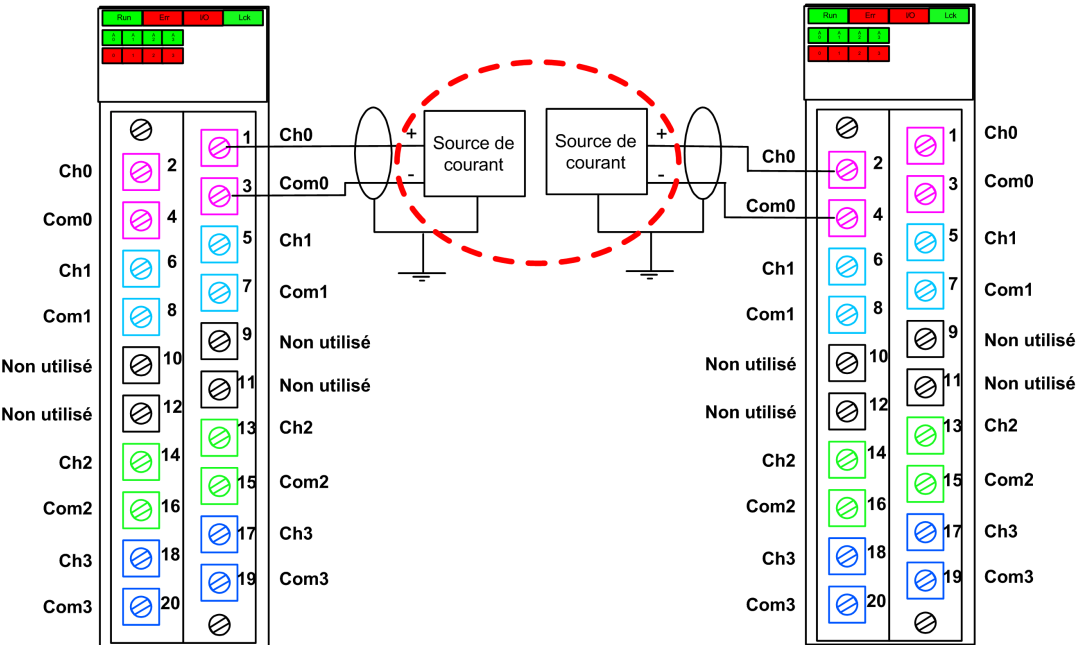
PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ

Utilisez le capteur homologué approprié pour obtenir le niveau SIL3 conformément à la norme IEC61508 et Category 2/Performance Level e conformément à la norme ISO13849 en utilisant ce mode de câblage.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

SIL3 Cat2/PLd avec haute disponibilité

L'exemple suivant présente deux capteurs qui surveillent la même variable de processus. Chaque capteur est connecté à un seul point d'entrée de différents modules d'entrée. Le contrôleur effectue l'évaluation 1oo1D de l'unique valeur surveillée :



NOTE: Dans cette conception, utilisez le bloc fonction `S_AIHA` de la tâche `SAFE` pour gérer les deux valeurs de la variable de processus fournies par les deux capteurs.

⚠ Avertissement

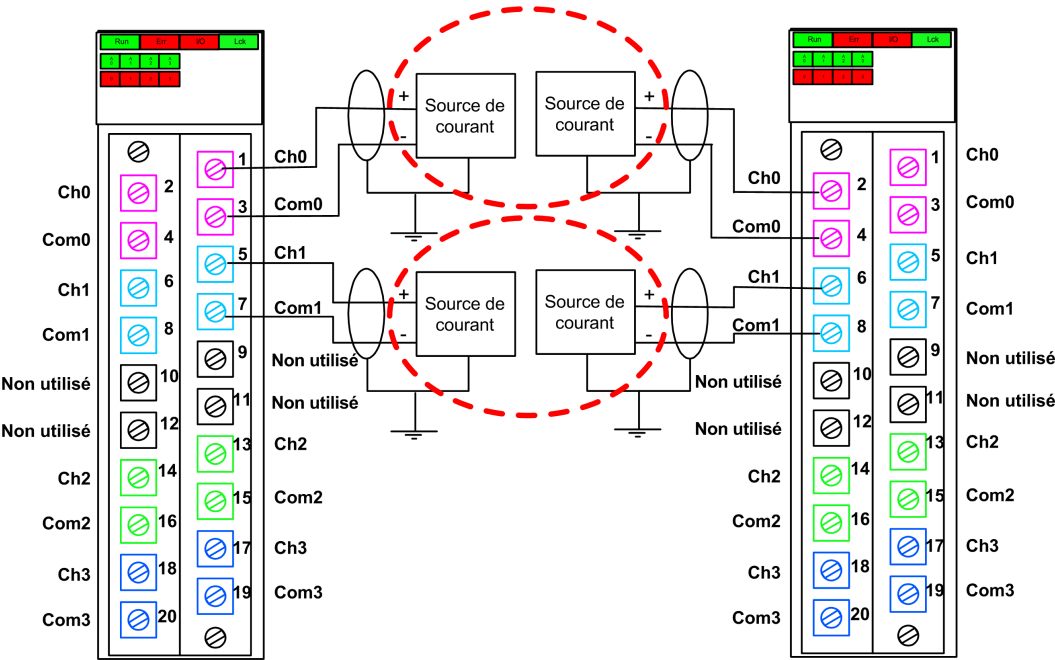
PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ

Utilisez le capteur homologué approprié pour obtenir le niveau SIL3 conformément à la norme IEC61508 et Category 2/Performance Level e conformément à la norme ISO13849 en utilisant ce mode de câblage.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

SIL3 Cat4/PLe avec haute disponibilité

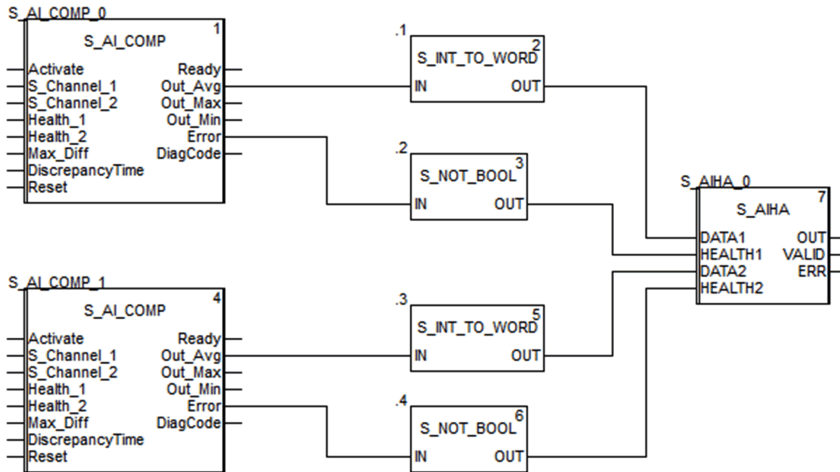
L'exemple suivant présente deux paires de capteurs redondants surveillant la même variable de processus. Chaque capteur est connecté à un seul point d'entrée de deux modules d'entrée distincts (deux entrées sur chaque module). Cette configuration permet au contrôleur d'effectuer une évaluation 1oo2D :



NOTE: Dans cette conception, vous devez utiliser les blocs fonction S_AI_COMP et S_AIHA dans la tâche SAFE afin de gérer les quatre signaux d'entrée :

- S_AI_COMP pour l'évaluation 1oo2 de deux paires de valeurs provenant des deux capteurs connectés au même module.
- S_AIHA pour la gestion de la haute disponibilité.

Le schéma FBD suivant décrit la conception des segments de code référencée ci-avant :



⚠ AVERTISSEMENT

PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ

Utilisez le capteur homologué approprié pour obtenir le niveau SIL3 conformément à la norme IEC 61508 et Category 4/Performance Level e conformément à la norme ISO13849 en utilisant ce mode de câblage.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Structure des données du BMXSAI0410

Introduction

Le DDDT (Device Derived Data Type) T_U_ANA_SIS_IN_4 est l'interface entre le module d'entrée analogique BMXSAI0410 et l'application qui s'exécute dans le contrôleur. Le DDDT

T_U_ANA_SIS_IN_4 intègre les types de données T_SAFE_COM_DBG_IN et T_U_ANA_SIS_CH_IN.

Toutes ces structures sont décrites ci-après.

Structure du DDDT T_U_ANA_SIS_IN_4

La structure du DDDT T_U_ANA_SIS_IN_4 comprend les éléments suivants :

Elément	Type de données	Description	Accès
MOD_HEALTH ¹	BOOL	1 : Le module fonctionne normalement. 0 : le module ne fonctionne pas correctement.	L
SAFE_COM_STS ¹	BOOL	1 : la communication du module est valide. 0 : la communication du module n'est pas valide.	L
S_COM_DBG	T_SAFE_COM_DBG_IN	Structure de débogage de communication sécurisée	L
CONF_LOCKED	BOOL	1 : la configuration du module est verrouillée. 0 : la configuration du module n'est pas verrouillée.	L
CH_IN	ARRAY[0...3] of T_U_ANA_SIS_CH_IN	Tableau de la structure des canaux.	–
MUID ²	ARRAY[0...3] of DWORD	ID unique du module (affecté automatiquement par Control Expert)	L
RESERVE	ARRAY[0...9] of INT	–	–
1. 1. Lorsque la tâche SAFE n'est pas en mode d'exécution dans le contrôleur, les données échangées entre le contrôleur et le module ne sont pas mises à jour et MOD_HEALTH comme SAFE_COM_STS ont pour valeur 0. 2. Cette valeur générée automatiquement peut être modifiée à l'aide de la commande Générer > Renouveler les ID et Régénérer tout dans le menu principal de Control Expert.			

Structure T_SAFE_COM_DBG_IN

La structure T_SAFE_COM_DBG_IN comprend les éléments suivants :

Elément	Type de données	Description	Accès ¹
S_COM_EST	BOOL	1 : la communication avec le module est établie. 0 : la communication avec le module n'est pas établie ou est corrompue.	L
M_NTP_SYNC	BOOL	Avec un micrologiciel de contrôleur de version 3.10 ou antérieure : 1 : le module est synchronisé avec le serveur NTP. 0 : le module n'est pas synchronisé avec le serveur NTP. NOTE: Avec un micrologiciel de contrôleur de version 3.20 ou ultérieure, la valeur est toujours 1.	L
CPU_NTP_SYNC	BOOL	Avec un micrologiciel de contrôleur de version 3.10 ou antérieure : 1 : le contrôleur est synchronisé avec le serveur NTP. 0 : le contrôleur n'est pas synchronisé avec le serveur NTP. NOTE: Avec un micrologiciel de contrôleur de version 3.20 ou ultérieure, la valeur est toujours 1.	L
CHECKSUM	BYTE	Somme de contrôle de trame de communication.	L
COM_DELAY	UINT	Délai de communication entre deux valeurs reçues par le module : 1...65534 : temps écoulé (en ms) depuis la réception par le contrôleur de la dernière communication émise par le module. 65535 : le contrôleur n'a pas reçu de communication du module.	L
COM_TO	UINT	Valeur du délai d'expiration pour les communications en provenance du module. NOTE: Vous avez la possibilité de modifier cette valeur accessible en lecture/écriture pour qu'elle soit égale ou supérieure au temps de communication réel du module (dans une station R/O distante, par exemple).	R/W
STS_MS_IN	UINT	Valeur de l'horodatage sécurisé des données reçues du module, à la milliseconde la plus proche.	L
S_NTP_MS	UINT	Valeur horaire sécurisée du cycle en cours, à la milliseconde la plus proche.	L

Elément	Type de données	Description	Accès ¹
STS_S_IN	UDINT	Valeur de l'horodatage sécurisé des données reçues du module, en secondes.	L
S_NTP_S	UDINT	Valeur horaire sécurisée du cycle en cours, en secondes.	L
CRC_IN	UDINT	Valeur CRC pour les données reçues du module.	L

Structure T_U_ANA_SIS_CH_IN

La structure T_U_ANA_SIS_CH_IN comprend les éléments suivants :

Elément	Type de données	Description	Accès
FCT_TYPE	WORD	1 : le canal est activé. 0 : le canal n'est pas activé.	L
CH_HEALTH ¹	BOOL	1 : La voie est opérationnelle. 0 : une erreur a été détectée sur le canal, lequel n'est pas opérationnel. Formule : CH_HEALTH = non (OOR ou IC) et SAFE_COM_STS	L
VALUE	INT	Valeur de l'entrée analogique. Formule : VALUE = si (SAFE_COM_STS et non (IC)) alors READ_VALUE sinon 0	L
OOR	BOOL	1 : la valeur du courant d'entrée du canal est hors plage, à savoir : < 3,75 mA > 20,75 mA 0 : la valeur du courant d'entrée du canal est comprise dans la plage.	L
IC	BOOL	1 : canal non valide détecté par le module. 0 : le canal est déclaré opérationnel en interne par le module.	L

1. Lorsque la tâche SAFE n'est pas en mode d'exécution dans le contrôleur, les données échangées entre le contrôleur et le module ne sont pas mises à jour et CH_HEALTH a pour valeur 0.

Module d'entrée numérique du BMXSDI1602

Introduction

Cette section décrit le module d'entrée numérique de sécurité du BMXSDI1602 .

Module d'entrée numérique de sécurité BMXSDI1602

Introduction

Les caractéristiques du module d'entrée numérique de sécurité BMXSDI1602 sont les suivantes :

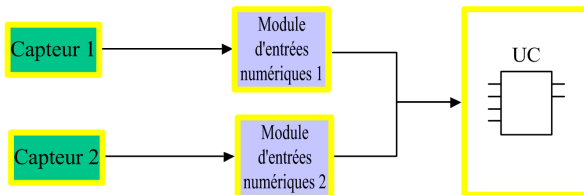
- 16 entrées de type 3 (IEC61131-2), en deux groupes non isolés électriquement de 8 entrées.
- Tension d'entrée nominale de 24 VCC.
- Avec pour résultat :
 - SIL3 IEC61508, SILCL3 IEC62061.
 - SIL4 EN5012x.
 - Catégorie 2 (Cat13849) / Niveau de performance d (PLd) ISO13849 en utilisant 1 canal d'entrée (évaluation 1oo1 (un sur un)).
 - Catégorie 4 (Cat4) / Niveau de performance e (PLe) ISO13849 en utilisant 2 canaux d'entrée (évaluation 1oo2D (deux sur deux avec diagnostic)).
- Compatibilité avec les détecteurs de proximité 2 ou 3 fils.
- Deux sorties 24 VCC en option (VS1 et VS2) pour la surveillance des conditions de court-circuit sur le 24 VCC :
 - VS1 surveille les entrées 0 à 3 (rangs A et B).
 - VS2 surveille les entrées 4 à 7 (rangs A et B).
- Surveillance de la tension d'alimentation de capteur externe 24 VCC.
- Affichage de diagnostics par LED, page 248 pour le module et pour chaque canal d'entrée.

- **Diagnostics configurables (activés/désactivés) du câblage des canaux, page 79** pouvant détecter les conditions suivantes :
 - Fil ouvert (ou rompu)
 - Court-circuit à la terre 0 V
 - Court-circuit sur le 24 VCC (si l'alimentation des capteurs est fournie en interne)
 - Circuits croisés entre deux canaux (si l'alimentation des capteurs est fournie en interne)
- Permutation de module à chaud pendant le fonctionnement.
- CCOTF (modification de configuration à la volée) pendant le fonctionnement en mode de maintenance, page 269. (La fonction CCOTF n'est pas prise en charge en mode de sécurité, page 268.)

Haute disponibilité

Vous pouvez utiliser deux capteurs connectés à deux canaux d'entrée différents sur des modules d'entrée distincts pour surveiller la même valeur physique, ce qui permet d'augmenter la disponibilité du système.

La figure suivante illustre la configuration de modules d'entrée numérique redondants :



Les valeurs d'état de l'entrée fournies par les capteurs 1 et 2 sont envoyées respectivement par les modules d'entrée 1 et 2 à un contrôleur de sécurité via un canal noir. Le contrôleur exécute un bloc fonction dédié, S_DIHA, pour gérer et sélectionner les données en provenance des deux modules d'entrée. Ce bloc fonction se comporte comme suit :

- Si l'état d'intégrité des données d'entrée en provenance du module 1 est correct, ces données sont utilisées dans la fonction de sécurité.
- Si l'état d'intégrité des données d'entrée en provenance du module 1 n'est pas correct mais que celui des données en provenance du module 2 est correct, les données du module 2 sont utilisées.
- Si l'état d'intégrité des données d'entrée en provenance des deux modules 1 et 2 est incorrect, l'état de l'entrée est défini sur 0 (état sécurisé défini) afin d'activer la fonction de sécurité.

Reportez-vous aux **exemples de câblage d'application d'entrée, page 78** pour plus d'informations sur la manière de câbler le module aux fins de haute disponibilité.

Connecteur de câblage du BMXSDI1602

Introduction

Le module d'entrées numériques BMXSDI1602 présente 16 entrées en deux groupes de 8 entrées. Le premier groupe comprend les entrées 0 à 3 (de rangs A et B) ; le second groupe comprend les entrées 4 à 7 (de rangs A et B). Il n'existe aucun isolement entre ces deux groupes.

L'alimentation peut être fournie aux capteurs directement depuis la source externe ou en mode interne via les alimentations VS1 et VS2. Chaque conception est présentée ci-après.

Borniers

Vous pouvez utiliser les borniers Schneider Electric à 20 points suivants pour le connecteur à 20 broches en face avant du module :

- bornier à vis étriers BMXFTB2010
- bornier à vis à cage BMXFTB2000
- bornier à ressorts BMXFTB2020

NOTE: Il n'est possible de retirer les borniers que lorsque le module est hors tension.

Alimentation process

Une alimentation process de catégorie II très basse tension (TBTS/TBTP) protégée 24 VCC est requise. Utilisez une alimentation qui ne rétablit pas automatiquement le courant après une coupure.

Le niveau d'intégrité de sécurité (SIL) maximum est déterminé par la fiabilité du capteur et la longueur de l'intervalle entre tests périodiques conformément à la norme IEC 61508.

DANGER

PERTE DE LA CAPACITE A EXECUTER LES FONCTIONS DE SECURITE

Utilisez obligatoirement un module d'alimentation process de type SELV/PELV avec sortie maximale de 60 V.

Le non-respect de ces instructions provoquera la mort ou des blessures graves.

AVIS

NON-CONFORMITÉ DES CIRCUITS ÉLECTRIQUES

Ne raccordez pas le 0V d'une alimentation SELV à la terre.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Fusible

Un fusible à fusion rapide est nécessaire pour protéger l'alimentation externe contre les situations de court-circuit et de surtension.

AVIS

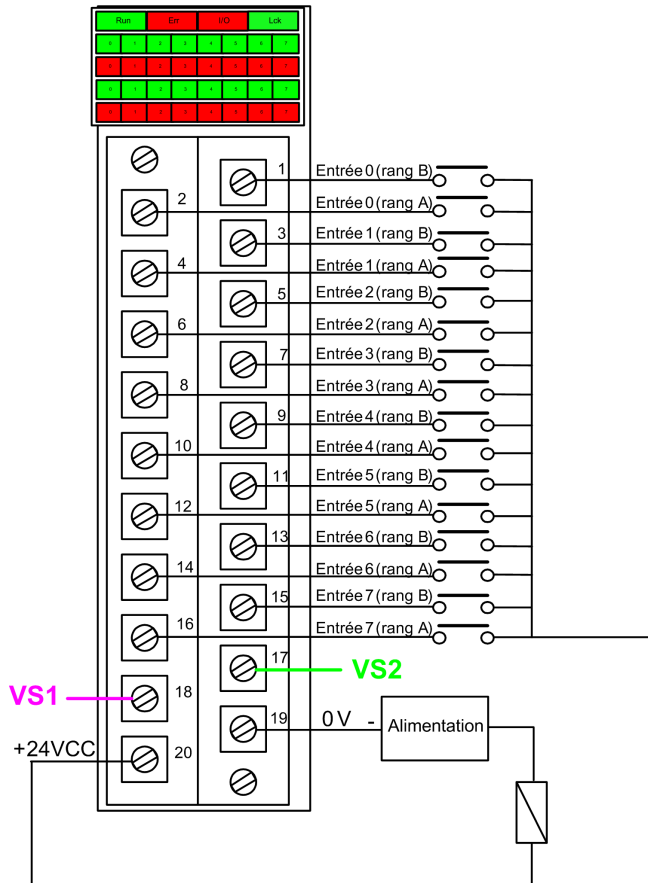
SELECTION DE FUSIBLE INCORRECTE

Utilisez des fusibles à fusion rapide pour protéger les composants électroniques du module d'entrée numérique contre les excès d'intensité électrique.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Connecteur de câblage : Capteurs alimentés par une alimentation externe

Dans la conception suivante, les capteurs sont alimentés directement par une source externe :



alimentation électrique : 24Vdc

Fusible : fusible à fusion rapide de 0,5 A

NOTE: L'alimentation des capteurs par une source externe limite les diagnostics de canal que le module peut effectuer. Selon le schéma de câblage ci-après, le module peut détecter les conditions suivantes :

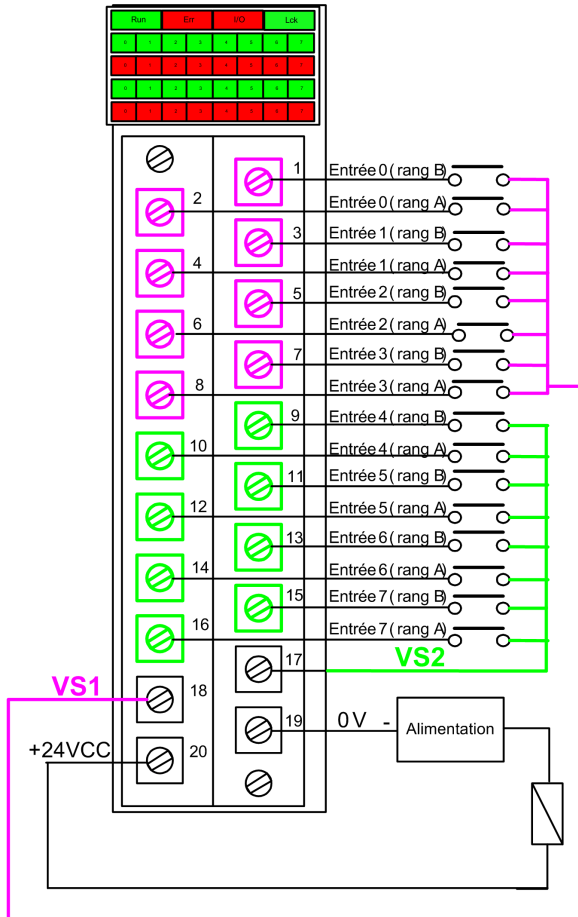
- Rupture (ou ouverture) du câblage (si l'option est activée pour ce canal dans Control Expert).
- Court-circuit à la terre.

En revanche, dans cette configuration, le module ne détecte pas les conditions suivantes :

- Court-circuit de 24 VCC.
- Circuit transversal avec autre entrée de câblage.

Connecteur de câblage : Capteurs alimentés par l'alimentation VS interne

Dans la conception suivante, les capteurs correspondant aux canaux 0 à 3 sont alimentés par la source surveillée VS1 et les capteurs correspondant aux canaux 4 à 7 sont alimentés par la source surveillée VS2 :



Si vous utilisez cette configuration, appliquez l'alimentation interne aux groupes de canaux de la manière suivante :

- Utilisez VS1 pour les canaux 0 à 3 (rangs A et B).
- Utilisez VS2 pour les canaux 4 à 7 (rangs A et B).

NOTE: Selon cette conception, le module peut détecter les conditions suivantes :

- Court-circuit sur 24 VCC (si l'option est activée pour le canal dans Control Expert).
- Circuit transversal avec autre entrée de câblage.
- Rupture (ou ouverture) du câblage (si l'option est activée pour ce canal dans Control Expert).
- Court-circuit à la terre.

Mappage des entrées aux broches de connecteur et aux canaux Control Expert

Le tableau suivant décrit chaque broche du module d'entrée BMXSDI1602 et indique le canal correspondant tel qu'il apparaît dans l'onglet **Configuration** du module dans Control Expert Safety :

Canal Control Expert	Description de la broche	Numéro de broche sur le bornier		Description de la broche	Voie Control Expert
0	Entrée 0 (rang A)	2	1	Entrée 0 (rang B)	8
1	Entrée 1 (rang A)	4	3	Entrée 1 (rang B)	9
2	Entrée 2 (rang A)	6	5	Entrée 2 (rang B)	10
3	Entrée 3 (rang A)	8	7	Entrée 3 (rang B)	11
4	Entrée 4 (rang A)	10	9	Entrée 4 (rang B)	12
5	Entrée 5 (rang A)	12	11	Entrée 5 (rang B)	13
6	Entrée 6 (rang A)	14	13	Entrée 6 (rang B)	14
7	Entrée 7 (rang A)	16	15	Entrée 7 (rang B)	15
–	Alimentation VS1	18	17	Alimentation VS2	–
–	Alimentation process 24 VCC	20	19	Alimentation process 24 VCC	–

Exemples de câblage pour les applications du du BMXSDI1602

Introduction

Vous pouvez câbler le module d'entrée numérique de sécurité BMXSDI1602 avec des capteurs pour obtenir la conformité SIL3, et cela de plusieurs manières en fonction des éléments suivants :

- la catégorie (Cat2 ou Cat4) et le niveau de performance (PLd ou PLe) requis
- les exigences de l'application en matière de haute disponibilité

Le niveau d'intégrité de sécurité (SIL) maximum est déterminé par la fiabilité du capteur et la longueur de l'intervalle entre tests périodiques conformément à la norme IEC 61508.

▲ AVERTISSEMENT

PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ

Câblez les capteurs, qui ne répondent pas à la fiabilité des normes SIL visées, en redondance sur deux canaux.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Les exemples suivants de câblage d'application d'entrée numérique SIL3 sont décrits ci-après :

- Cat2/PLd :
 - capteur unique câblé à une seule entrée
- Cat2/PLd avec haute disponibilité :
 - capteur unique câblé à deux points d'entrée sur différents modules d'entrée
 - deux capteurs câblés à deux points d'entrée sur différents modules d'entrée
- Cat4/PLe :
 - capteur unique câblé à deux points d'entrée sur le même module d'entrée
 - deux capteurs câblés à deux points d'entrée distincts du même module d'entrée
- Cat4/PLe avec haute disponibilité :
 - deux capteurs câblés à deux points d'entrée distincts sur différents modules d'entrée

Diagnostics de câblage configurables dans Control Expert

Sur le module d'entrée numérique de sécurité BMXSDI1602, utilisez la page **Configuration** dans Control Expert pour effectuer les actions suivantes :

- Activer l'option **Détection de court-circuit à 24 V** pour chaque canal alimenté. Ce test effectue les diagnostics de câblage d'actionneur suivants pour un canal :
 - Détection de court circuit à 24 VCC.
 - Détection de circuit croisé entre deux canaux de sortie.

Le principe consiste à fournir l'alimentation aux capteurs, par groupes de 8 canaux, avec VS1 pour les canaux 0 à 3 (rangs A et B) et VS2 pour les canaux 4 à 7 (rangs A et B). Une impulsion vers l'état OFF est appliquée périodiquement à ces sorties d'énergie, avec une période inférieure à 1 seconde et une durée inférieure à 1 milliseconde. Pendant cette impulsion, si l'intensité de courant lue au niveau de l'entrée est nulle, le module considère que cette entrée est en court-circuit.

- Activer l'option **Détection de fil ouvert** pour chacun des huit canaux afin d'obtenir les diagnostics de câblage suivants pour le canal concerné :
 - Détection de fil ouvert (ou rompu) (canal d'entrée non connecté au capteur).
 - Détection de court-circuit vers la terre 0 VCC.

Le principe consiste à générer artificiellement un courant de fuite (Ileakage) sur la ligne (avec une résistance en parallèle du capteur) lorsque le capteur est ouvert, puis à mesurer ce courant. Si le module ne parvient pas à mesurer ce courant de fuite ($0,4 \text{ mA} < I_{\text{leakage}} < 1,3 \text{ mA}$) sur la ligne d'entrée, la ligne externe est considérée comme coupée (ou en court-circuit à la terre). Le diagnostic est effectué selon une période inférieure à 10 ms.

- Pour un capteur à contacts secs, configurez en parallèle une résistance de 33 k Ω .
- En cas d'utilisation de 2 ou 3 fils DDP, le courant de fuite doit descendre dans les limites définies ci-avant. Vous devez définir la valeur de la résistance à configurer parallèlement au capteur en tenant compte du courant de fuite naturel du capteur et de la résistance interne de l'entrée (7,5 K Ω).

AVERTISSEMENT

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

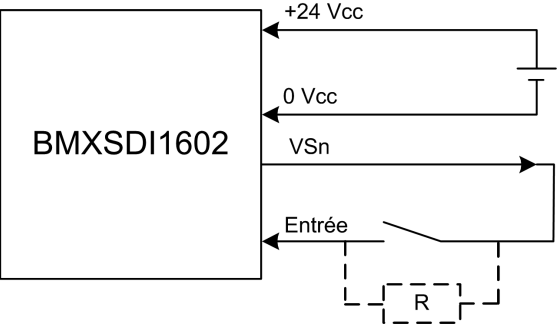
Activez les diagnostics disponibles fournis dans Control Expert pour détecter ou exclure les conditions énumérées ci-dessus.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Si aucun test de diagnostic n'est activé ou n'est disponible dans Control Expert, appliquez d'autres mesures de sécurité pour détecter ou exclure ces conditions.

SIL3 Cat2/PLd

Capteur unique connecté avec une seule entrée, avec alimentation VS interne :



Dans cet exemple, selon que la puissance interne est fournie via :

- VS1 - utilisez les canaux 0 à 3, rangs A et B.
- VS2 - utilisez les canaux 4 à 7, rangs A et B.

Comme le capteur est alimenté en interne via une broche VS, les diagnostics de câblage de canaux suivants s'appliquent :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC ¹	Oui	< 1 s
Circuits croisés entre deux canaux ¹	Oui	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Dans le cas d'un **capteur unique connecté avec une seule entrée, avec alimentation VS**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité de circuits croisés entre les canaux du même groupe.

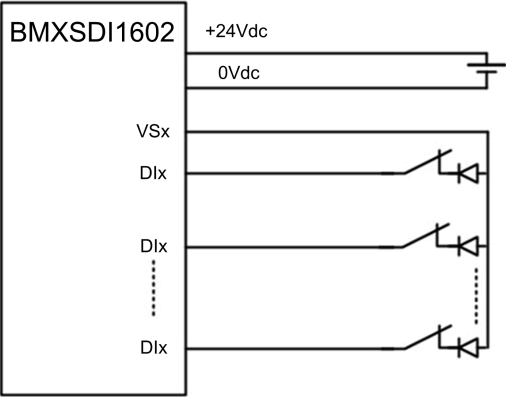
⚠ AVERTISSEMENT

CIRCUITS CROISÉS ENTRE CANAUX DU MÊME GROUPE

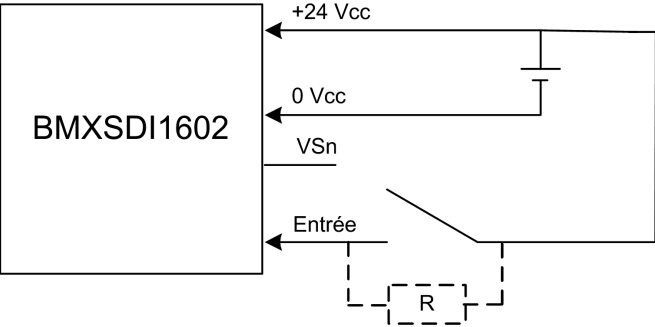
Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux du même groupe VS.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

NOTE: Prévoyez l'ajout d'une diode Shottky à la boucle d'entrée, entre le capteur et le point d'entrée, pour réduire la probabilité qu'une condition de court-circuit sur le 24 VCC sur un canal puisse créer la même condition sur un canal adjacent.



Capteur unique connecté avec une seule entrée avec source d'alimentation externe :



Le capteur étant alimenté par une source externe, les diagnostics de câblage de canal suivants s'appliquent :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC	Non	–
Circuits croisés entre deux canaux	Non	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

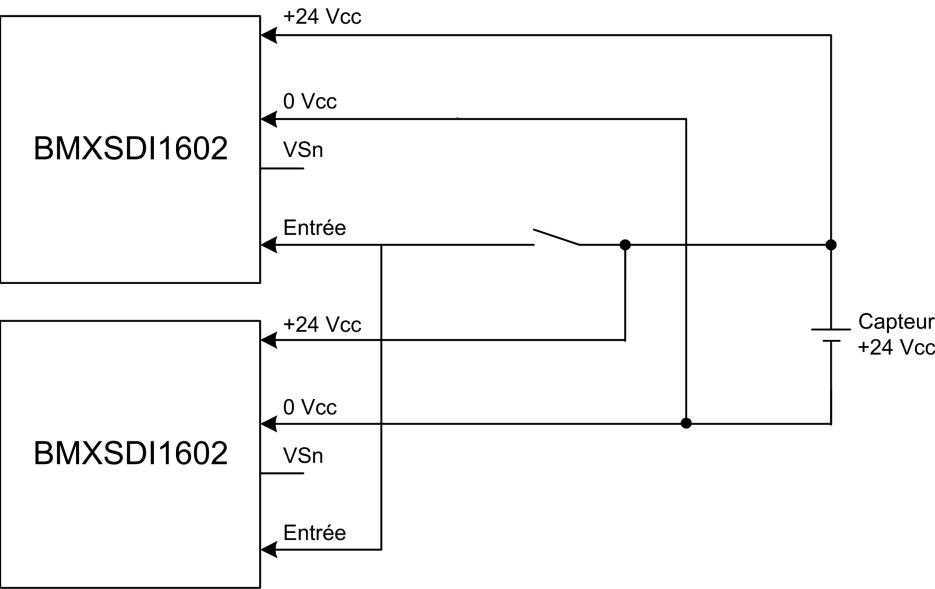
Dans le cas d'un **capteur unique connecté avec une seule entrée, alimenté par une source externe**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité d'un court-circuit vers le 24 VC et/ou de circuits croisés entre deux canaux.

⚠ AVERTISSEMENT

CIRCUITS CROISÉS ENTRE LES CANAUX OU COURT-CIRCUIT VERS LE 24 VCC
Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux ou un court-circuit vers le 24 VC.
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

SIL3 Cat2/PLd avec haute disponibilité

Capteur unique connecté sur deux entrées avec source d'alimentation externe :



Le capteur unique étant alimenté par une source externe, les diagnostics de câblage de canal suivants s'appliquent :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Non	—
Court-circuit vers la terre 0 V	Non	

Condition	Délectable ?	Temps de détection typique
Court-circuit vers le 24 VCC ¹	Non	
Circuits croisés entre deux canaux	Non	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Dans le cas d'un **capteur unique connecté sur deux entrées avec source d'alimentation externe**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité d'un court-circuit vers le 24 VC et/ou de circuits croisés entre deux canaux.

 **AVERTISSEMENT**

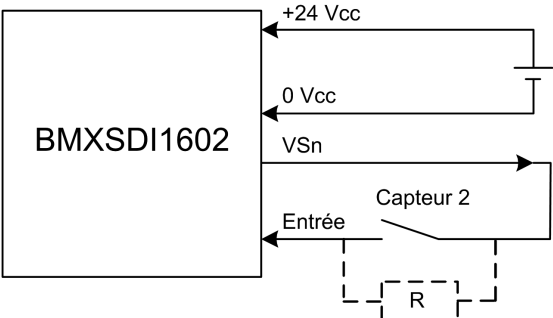
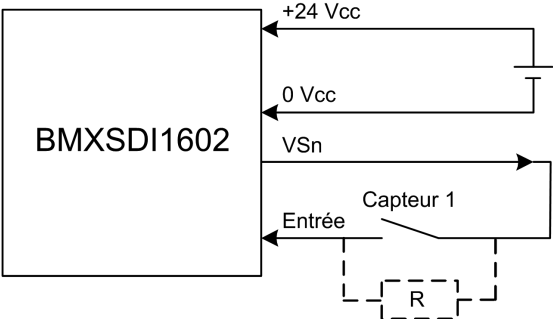
CIRCUITS CROISÉS ENTRE CANAUX OU COURT-CIRCUIT VERS LE 24 VCC

Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux ou un court-circuit vers le 24 VC.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Deux capteurs redondants connectés sur des entrées distinctes de deux modules via VS :

L'exemple suivant présente deux capteurs redondants (qui peuvent éventuellement être liés mécaniquement) utilisés pour acquérir la même variable de processus. Chaque capteur est câblé à un seul point d'entrée sur un module d'entrée distinct, l'énergie étant fournie par l'alimentation VS surveillée :



Dans cet exemple, si la puissance interne est fournie via :

- VS1 - utilisez les canaux 0 à 3, rangs A et B.
- VS2 - utilisez les canaux 4 à 7, rangs A et B.

NOTE:

- Dans cette conception, vous pourriez utiliser le bloc fonction `S_DIHA` pour gérer les deux signaux d'entrée.
- Prévoyez l'ajout d'une diode Shottky à la boucle d'entrée, entre le capteur et le point d'entrée, pour réduire la probabilité qu'une condition de court-circuit sur 24 VCC sur un canal puisse créer la même condition sur un canal adjacent.

Comme le capteur est alimenté en interne via une broche VS, les diagnostics de câblage de canaux suivants s'appliquent :

Condition	Détectable ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms

Condition	DéTECTABLE ?	Temps de détection typique
Court-circuit vers la terre 0 V	Oui	< 1 s
Court-circuit vers le 24 VCC ¹	Oui	
Circuits croisés entre deux canaux	Oui	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Dans le cas de **deux capteurs redondants connectés sur des entrées distinctes de deux modules via VS**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité de circuits croisés entre les canaux du même groupe.

 **AVERTISSEMENT**

CIRCUITS CROISÉS ENTRE CANAUX DU MÊME GROUPE
Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux du même groupe VS.
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Deux capteurs redondants connectés sur des entrées distinctes de deux modules avec alimentation externe :

NOTE: L'alimentation peut également être fournie aux capteurs par une source externe. Dans ce cas, une condition de court-circuit vers le 24 VCC et de circuits croisés entre deux canaux ne sont pas détectables.

Comme le capteur est alimenté en interne via une broche VS, les diagnostics de câblage de canaux suivants s'appliquent :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC	Non	–
Circuits croisés entre deux canaux	Non	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Dans le cas de **deux capteurs redondants connectés sur des entrées distinctes de deux modules avec alimentation externe**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité d'un court-circuit vers le 24 VC et/ou de circuits croisés entre deux canaux.

⚠ AVERTISSEMENT

CIRCUITS CROISÉS ENTRE CANAUX OU COURT-CIRCUIT VERS LE 24 VCC

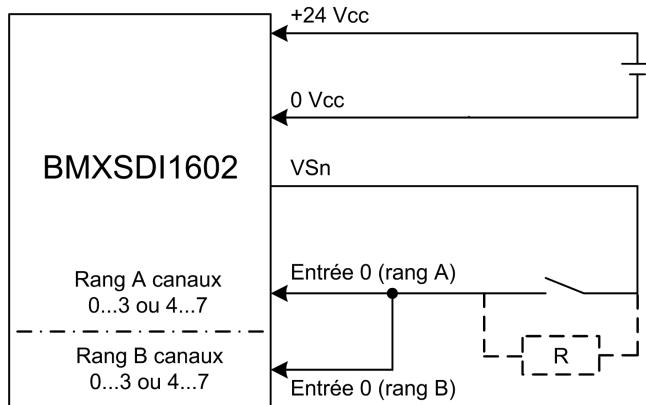
Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux ou un court-circuit vers le 24 VC.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Cat4/PLe

Capteur unique connecté à deux entrées du même module avec alimentation VS :

L'exemple suivant présente un seul capteur câblé à deux points d'entrée du même module d'entrée, l'énergie étant fournie par l'alimentation VS surveillée :



Dans cet exemple, si la puissance interne est fournie via :

- VS1 - utilisez les canaux 0 à 3, rangs A et B.
- VS2 - utilisez les canaux 4 à 7, rangs A et B.

NOTE:

- Dans cette conception, vous pourriez utiliser le bloc fonction `S_EQUIVALENT` pour gérer les deux signaux d'entrée.
- Prévoyez l'ajout d'une diode Shottky à la boucle d'entrée, entre le capteur et le point d'entrée, pour réduire la probabilité qu'une condition de court-circuit sur le 24 VCC sur un canal puisse créer la même condition sur un canal adjacent.

Diagnostic de câblage pour un capteur unique connecté à deux entrées, avec alimentation fournie par la broche VS :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC ¹	Oui	< 1 s
Circuits croisés entre deux canaux	Oui	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Dans le cas d'un **capteur unique connecté à deux entrées du même module avec alimentation VS**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité de circuits croisés entre les canaux du même groupe.

⚠ AVERTISSEMENT

CIRCUITS CROISÉS ENTRE CANAUX DU MÊME GROUPE
Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux du même groupe VS.
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Capteur unique connecté à deux entrées du même module avec alimentation externe :

NOTE: L'alimentation peut également être fournie aux capteurs par une source externe. Dans ce cas, les conditions de court-circuit vers le 24 VCC et de circuits croisés entre deux canaux ne sont pas détectables.

Diagnostic de câblage pour un capteur unique connecté à deux entrées avec alimentation externe :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC ¹	Non	–
Circuits croisés entre deux canaux	Non	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Dans le cas d'un **capteur unique connecté à deux entrées du même module avec alimentation externe**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité d'un court-circuit vers le 24 VC et/ou de circuits croisés entre deux canaux.

⚠ AVERTISSEMENT

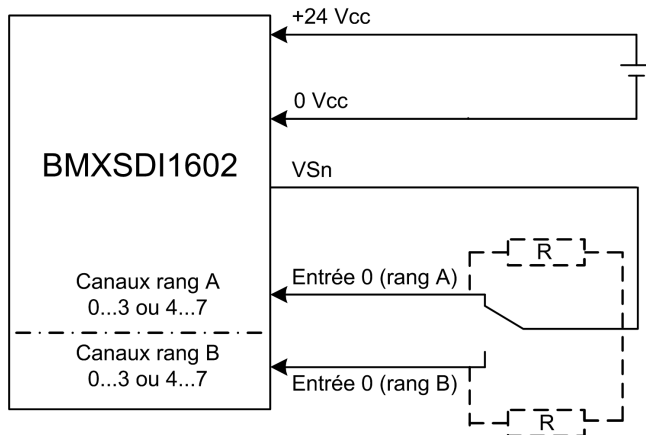
CIRCUITS CROISÉS ENTRE CANAUX OU COURT-CIRCUIT VERS LE 24 VCC

Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux ou un court-circuit vers le 24 VC.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Capteur non équivalent connecté à deux entrées non équivalentes du même module avec alimentation par VS :

L'exemple suivant présente un seul capteur non équivalent câblé à deux points d'entrée du même module d'entrée, l'énergie étant fournie par l'alimentation VS surveillée : Le module effectue une évaluation 1oo2D :



Dans cet exemple, si la puissance interne est fournie via :

- VS1 - utilisez les canaux 0 à 3, rangs A et B.
- VS2 - utilisez les canaux 4 à 7, rangs A et B.

NOTE:

- Dans cette conception, vous pourriez utiliser le bloc fonction `S_ANTIIVALENT` pour gérer les deux signaux d'entrée.
- Prévoyez l'ajout d'une diode Shottky à la boucle d'entrée, entre le capteur et le point d'entrée, pour réduire la probabilité qu'une condition de court-circuit sur le 24 VCC sur un canal puisse créer la même condition sur un canal adjacent.

Diagnostic de câblage pour un seul capteur non équivalent connecté à deux entrées, avec alimentation fournie par la broche VS :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC ¹	Oui	< 1 s
Circuits croisés entre deux canaux	Oui	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Capteur non équivalent connecté sur deux entrées non équivalentes du même module avec alimentation externe :

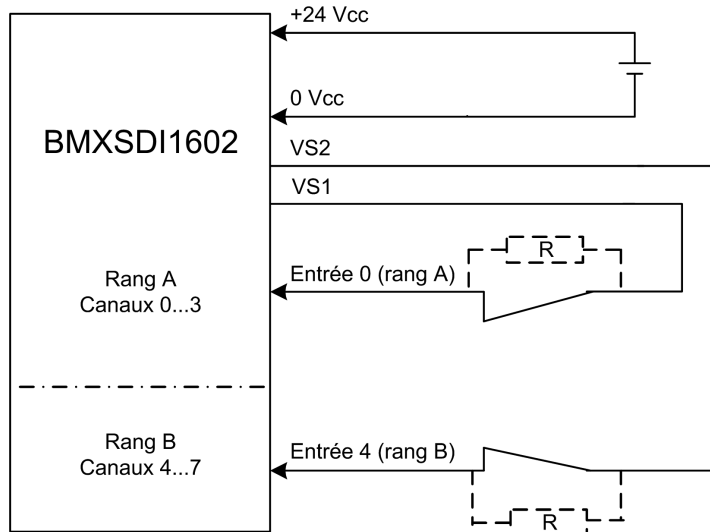
NOTE: L'alimentation peut également être fournie aux capteurs par une source externe. Dans ce cas, une condition de court-circuit vers le 24 VCC et de circuits croisés entre deux canaux ne sont pas détectables.

Diagnostic de câblage pour un seul capteur non équivalent connecté à deux entrées avec alimentation externe :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC ¹	Non	–
Circuits croisés entre deux canaux	Non	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Acquisition de la même variable de processus à l'aide de deux capteurs distincts (liés mécaniquement ou pas) avec alimentation par VS :

L'exemple suivant présente deux capteurs redondants (qui peuvent éventuellement être liés mécaniquement) utilisés pour acquérir la même variable de processus. Chaque capteur est câblé à un point d'entrée distinct du même module d'entrée, l'énergie étant fournie par l'alimentation VS surveillée :



NOTE:

- Les entrées 0 à 3 du rang A sont utilisées avec les entrées 4 à 7 du rang B.
- Les entrées 0 à 3 du rang B sont utilisées avec les entrées 4 à 7 du rang A.

⚠ AVERTISSEMENT

PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ

Utilisez les capteurs homologués appropriés pour obtenir le niveau SIL3 conformément à la norme IEC 61508 et Category 4/Performance Level e conformément à la norme ISO13849 en utilisant ce mode de câblage.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Dans cet exemple, si la puissance interne est fournie via :

- VS1 - utilisez les canaux 0 à 3, rangs A et B.
- VS2 - utilisez les canaux 4 à 7, rangs A et B.

NOTE:

- Dans cette conception, vous pourriez utiliser le bloc fonction S_EQUIVALENT pour gérer les deux signaux d'entrée.
- Prévoyez l'ajout d'une diode Shottky à la boucle d'entrée, entre le capteur et le point d'entrée, pour réduire la probabilité qu'une condition de court-circuit sur le 24 VCC sur un canal puisse créer la même condition sur un canal adjacent.

Diagnostic de câblage pour un capteur unique connecté à deux entrées, avec alimentation fournie par la broche VS :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC ¹	Oui	< 1 s
Circuits croisés entre deux canaux	Oui	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Dans le cas de l'**acquisition de la même variable de processus à l'aide de deux capteurs distincts (liés mécaniquement ou pas) avec alimentation par VS**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité de circuits croisés entre les canaux du même groupe.

⚠ AVERTISSEMENT

CIRCUITS CROISÉS ENTRE CANAUX DU MÊME GROUPE

Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux du même groupe VS.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Acquisition de la même variable de processus à l'aide de deux capteurs distincts (liés mécaniquement ou pas) avec alimentation externe :

NOTE: L'alimentation peut également être fournie aux capteurs par une source externe. Dans ce cas, une condition de court-circuit vers le 24 VCC et de circuits croisés entre deux canaux ne sont pas détectables.

Diagnostic de câblage pour un capteur unique connecté à deux entrées avec alimentation externe :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms

Condition	DéTECTABLE ?	Temps de détection typique
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC ¹	Non	–
Circuits croisés entre deux canaux	Non	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Dans le cas de l'**acquisition de la même variable de processus à l'aide de deux capteurs distincts (liés mécaniquement ou pas) avec alimentation externe**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité d'un court-circuit vers le 24 VC et/ou de circuits croisés entre deux canaux.

⚠ AVERTISSEMENT

CIRCUITS CROISÉS ENTRE CANAUX OU COURT-CIRCUIT VERS LE 24 VCC
Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux ou un court-circuit vers le 24 VC.
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

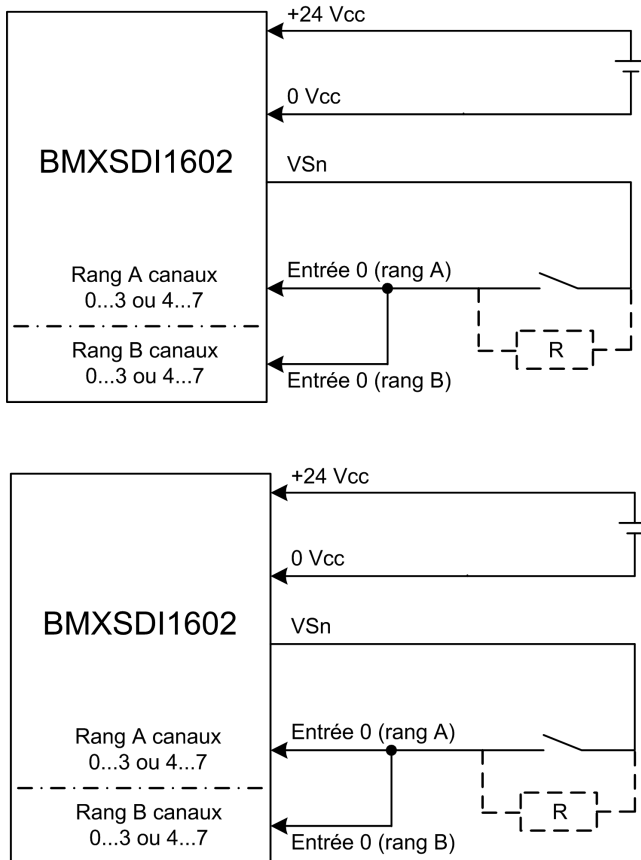
⚠ AVERTISSEMENT

PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ
Utilisez un capteur homologué appropriés pour obtenir les niveaux SIL3/Cat4/PLe à l'aide de ce câblage.
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Cat4/PLe avec haute disponibilité

Schéma de câblage avec connexion monocanal de deux capteurs monocanaux redondants avec alimentation par VS :

L'exemple suivant présente deux capteurs monocanaux redondants (qui peuvent éventuellement être liés mécaniquement) câblés chacun à deux points d'entrées sur deux modules d'entrée distincts, l'énergie étant fournie par l'alimentation VS surveillée :



Dans cet exemple, si la puissance interne est fournie via :

- VS1 - utilisez les canaux 0 à 3, rangs A et B.
- VS2 - utilisez les canaux 4 à 7, rangs A et B.

NOTE:

- Dans cette conception, vous pourriez utiliser les blocs fonctions `S_EQUIVALENT` et `S_DIHA` pour gérer les quatre signaux d'entrée.
- Prévoyez l'ajout d'une diode Shottky à la boucle d'entrée, entre le capteur et le point d'entrée, pour réduire la probabilité qu'une condition de court-circuit sur le 24 VCC sur un canal puisse créer la même condition sur un canal adjacent.

Diagnostic de câblage pour un capteur unique connecté à deux entrées, avec alimentation fournie par la broche VS :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC ¹	Oui	< 1 s
Circuits croisés entre deux canaux	Oui	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Dans le cas d'une **connexion monocal de deux capteurs monocanaux redondants avec alimentation par VS**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité de circuits croisés entre les canaux du même groupe.

⚠ AVERTISSEMENT

CIRCUITS CROISÉS ENTRE CANAUX DU MÊME GROUPE
Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux du même groupe VS.
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Schéma de câblage avec connexion monocanal de deux capteurs monocanaux redondants avec alimentation externe :

NOTE: L'alimentation peut également être fournie aux capteurs par une source externe. Dans ce cas, une condition de court-circuit vers le 24 VCC et de circuits croisés entre deux canaux ne sont pas détectables.

Diagnostic de câblage pour un capteur unique connecté à deux entrées avec alimentation externe :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC ¹	Non	–
Circuits croisés entre deux canaux	Non	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Dans le cas d'une **connexion monocanal de deux capteurs monocanaux redondants avec alimentation**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité d'un court-circuit vers le 24 VC et/ou de circuits croisés entre deux canaux.

▲ AVERTISSEMENT

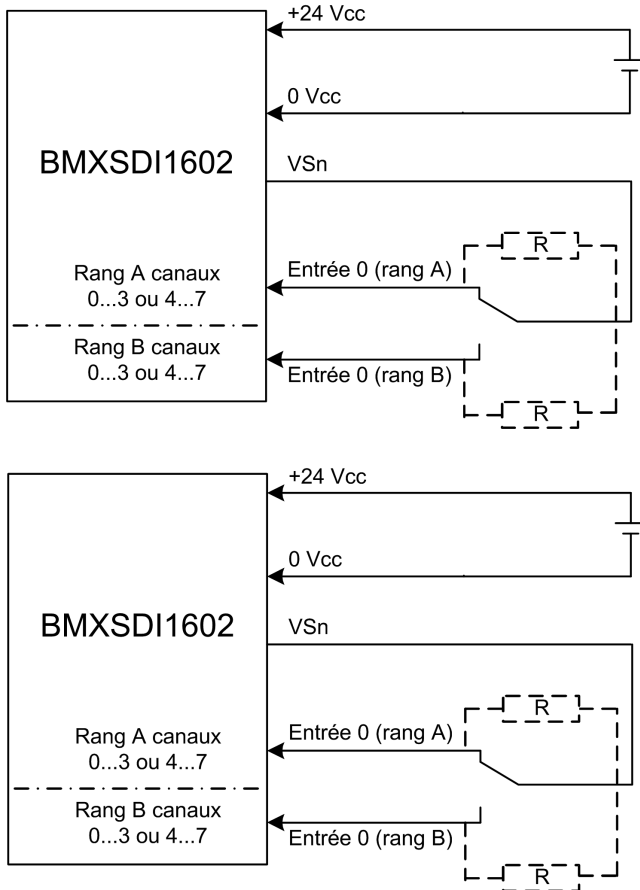
CIRCUITS CROISÉS ENTRE CANAUX OU COURT-CIRCUIT VERS LE 24 VCC

Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux ou un court-circuit vers le 24 VC.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Capteurs non équivalents (liés mécaniquement ou pas) connectés sur deux entrées non équivalentes de deux modules distincts avec alimentation par VS :

L'exemple suivant présente deux paires de capteurs non équivalents redondants (qui peuvent éventuellement être liés mécaniquement) câblées chacune à un seul point d'entrée sur deux modules d'entrée distincts (deux sur chaque module), l'énergie étant fournie par l'alimentation VS surveillée :



Dans cet exemple, si la puissance interne est fournie via :

- VS1 - utilisez les canaux 0 à 3, rangs A et B.
- VS2 - utilisez les canaux 4 à 7, rangs A et B.

NOTE:

- Dans cette conception, vous devez utiliser les blocs fonctions S_ANTIVALENT et S_DIHA pour gérer les quatre signaux d'entrée.
 - S_ANTIVALENT pour l'évaluation 1oo2 de deux paires de valeurs provenant des deux capteurs connectés au même module.
 - S_DIHA pour la gestion de la haute disponibilité.
- Prévoyez l'ajout d'une diode Shottky à la boucle d'entrée, entre le capteur et le point d'entrée, pour réduire la probabilité qu'une condition de court-circuit sur le 24 VCC sur un canal puisse créer la même condition sur un canal adjacent.

Comme le capteur est alimenté en interne via une broche VS, les diagnostics de câblage de canaux suivants s'appliquent :

Condition	DéTECTABLE ?	Temps de détection typique
Fil ouvert (ou rompu) ¹	Oui	< 10 ms
Court-circuit vers la terre 0 V	Oui	
Court-circuit vers le 24 VCC ¹	Oui	< 1 s
Circuits croisés entre deux canaux	Oui	
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert.		

Dans le cas de **capteurs non équivalents (liés mécaniquement ou pas) connectés sur deux entrées non équivalentes de deux modules distincts avec alimentation par VS**, appliquez d'autres mesures de sécurité pour détecter ou exclure la possibilité de circuits croisés entre les canaux du même groupe.

⚠ AVERTISSEMENT

CIRCUITS CROISÉS ENTRE CANAUX DU MÊME GROUPE

Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux du même groupe VS.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Capteur non équivalent (lié mécaniquement ou pas) connecté sur deux entrées non équivalentes de deux modules distincts avec alimentation externe :

NOTE: L'alimentation des capteurs peut également être fournie par une source externe (dans le cas d'un capteur non équivalent connecté sur deux entrées non équivalentes de deux modules distincts avec une alimentation externe). Dans ce cas, une condition de circuits croisés entre deux canaux n'est pas détectable.

⚠️ AVERTISSEMENT

CIRCUITS CROISÉS ENTRE DEUX CANAUX

Appliquez d'autres mesures de sécurité au module pour détecter les circuits croisés entre deux canaux.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠️ AVERTISSEMENT

PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ

Utilisez les capteurs homologués appropriés pour obtenir le niveau SIL3 conformément à la norme IEC 61508 et Category 4/Performance Level e conformément à la norme ISO13849 en utilisant ce mode de câblage.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Structure des données du BMXSDI1602

Introduction

Le DDDT (Device Derived Data Type) `T_U_DIS_SIS_IN_16` est l'interface entre le module d'entrée numérique BMXSDI1602 et l'application qui s'exécute dans le contrôleur. Le DDDT `T_U_DIS_SIS_IN_16` intègre les types de données `T_SAFE_COM_DBG_IN` et `T_U_DIS_SIS_CH_IN`.

Toutes ces structures sont décrites ci-après.

Structure du DDDT `T_U_DIS_SIS_IN_16`

La structure du DDDT `T_U_DIS_SIS_IN_16` comprend les éléments suivants :

Elément	Type de données	Description	Accès
MOD_HEALTH ¹	BOOL	1 : Le module fonctionne normalement. 0 : le module ne fonctionne pas correctement.	L
SAFE_COM_STS ¹	BOOL	1 : la communication du module est valide. 0 : la communication du module n'est pas valide.	L
PP_STS	BOOL	1 : l'alimentation process est opérationnelle. 0 : l'alimentation process n'est pas opérationnelle.	L
CONF_LOCKED	BOOL	1 : la configuration du module est verrouillée. 0 : la configuration du module n'est pas verrouillée.	L
S_COM_DBG	T_SAFE_COM_DBG_IN	Structure de débogage de communication sécurisée	L
CH_IN_A	ARRAY[0...7] of T_U_DIS_SIS_CH_IN	Tableau de la structure de canal du rang A.	–
CH_IN_B	ARRAY[0...7] of T_U_DIS_SIS_CH_IN	Tableau de la structure de canal du rang B.	–
MUID ²	ARRAY[0...3] of DWORD	ID unique du module (affecté automatiquement par Control Expert)	L
RESERVE	ARRAY[0...9] of INT	–	–
1. 1. Lorsque la tâche SAFE n'est pas en mode d'exécution dans le contrôleur, les données échangées entre le contrôleur et le module ne sont pas mises à jour et MOD_HEALTH comme SAFE_COM_STS ont pour valeur 0. 2. Cette valeur générée automatiquement peut être modifiée à l'aide de la commande Générer > Renouveler les ID et Régénérer tout dans le menu principal de Control Expert.			

Structure T_SAFE_COM_DBG_IN

La structure T_SAFE_COM_DBG_IN comprend les éléments suivants :

Elément	Type de données	Description	Accès
S_COM_EST	BOOL	1 : la communication avec le module est établie. 0 : la communication avec le module n'est pas établie ou est corrompue.	L
M_NTP_SYNC	BOOL	Avec un micrologiciel de contrôleur de version 3.10 ou antérieure : 1 : le module est synchronisé avec le serveur NTP. 0 : le module n'est pas synchronisé avec le serveur NTP. NOTE: Avec un micrologiciel de contrôleur de version 3.20 ou ultérieure, la valeur est toujours 1.	L
CPU_NTP_SYNC	BOOL	Avec un micrologiciel de contrôleur de version 3.10 ou antérieure : 1 : le contrôleur est synchronisé avec le serveur NTP. 0 : le contrôleur n'est pas synchronisé avec le serveur NTP. NOTE: Avec un micrologiciel de contrôleur de version 3.20 ou ultérieure, la valeur est toujours 1.	L
CHECKSUM	BYTE	Somme de contrôle de trame de communication.	L
COM_DELAY	UINT	Délai de communication entre deux valeurs reçues par le module : 1...65534 : temps écoulé (en ms) depuis la réception par le contrôleur de la dernière communication émise par le module. 65535 : le contrôleur UC n'a pas reçu de communication du module.	L
COM_TO	UINT	Valeur du délai d'expiration pour les communications en provenance du module.	R/W
STS_MS_IN	UINT	Valeur de l'horodatage sécurisé des données reçues du module, à la milliseconde la plus proche.	L
S_NTP_MS	UINT	Valeur horaire sécurisée du cycle en cours, à la milliseconde la plus proche.	L
STS_S_IN	UDINT	Valeur de l'horodatage sécurisé des données reçues du module, en secondes.	L

Élément	Type de données	Description	Accès
S_NTP_S	UDINT	Valeur horaire sécurisée du cycle en cours, en secondes.	L
CRC_IN	UDINT	Valeur CRC pour les données reçues du module.	L

Structure T_U_DIS_SIS_CH_IN

La structure T_U_DIS_SIS_CH_IN comprend les éléments suivants :

Élément	Type de données	Description	Accès
CH_HEALTH ¹	BOOL	1 : La voie est opérationnelle. 0 : une erreur a été détectée sur le canal, lequel n'est pas opérationnel. Formule : CH_HEALTH = non (OC ou IC ou SC) et SAFE_COM_STS	L
VALUE ²	EBOOL	1 : l'entrée est alimentée. 0 : l'entrée n'est pas alimentée. Formule : VALUE = si (SAFE_COM_STS et non (IC)) alors READ_VALUE sinon 0	L
OC	BOOL	1 : le canal est ouvert ou court-circuité à la terre. 0 : le canal est connecté et n'est pas court-circuité à la terre.	L
SC	BOOL	1 : le canal est court-circuité vers une source 24 V ou inter-circuité entre deux canaux. 0 : le canal n'est pas court-circuité sur une source 24 V ni inter-circuité entre deux canaux.	L
IC	BOOL	1 : canal non valide détecté par le module. 0 : le canal est déclaré opérationnel en interne par le module.	L
V_OC	BOOL	État de configuration du test d'ouverture ou de court-circuit à la terre : 1 : Activé. 0 : Désactivé.	L

Elément	Type de données	Description	Accès
V_SC	BOOL	État de configuration du test de court-circuit vers une source 24 V : • 1 : Activé. • 0 : Désactivé.	L
1. Lorsque la tâche SAFE n'est pas en mode d'exécution dans le contrôleur, les données échangées entre le contrôleur et le module ne sont pas mises à jour et CH_HEALTH a pour valeur 0. 2. L'élément VALUE peut être horodaté par le BMX CRA ou le BME CRA.			

Module de sortie numérique du BMXSDO0802

Introduction

Cette section décrit le module de sortie numérique de sécurité du BMXSDO0802 .

Module de sortie numérique de sécurité BMXSDO0802

Introduction

Les caractéristiques du module de sortie numérique de sécurité BMXSDO0802 sont les suivantes :

- 8 sorties 0,5 A non isolées électriquement.
- Tension de sortie nominale de 24 VCC.
- Avec pour résultat :
 - SIL3 IEC61508, SILCL3 IEC62061.
 - SIL4 EN5012x.
 - Catégorie 4 (Cat4) / Niveau de performance e (PLe) ISO13849.
- Surveillance de l'alimentation pré-actionneur externe.
- Affichage de diagnostics par LED, page 254 pour le module et pour chaque canal de sortie.
- Diagnostics de câblage des canaux fournis automatiquement pouvant détecter les conditions suivantes lorsque la sortie est *alimentée* :
 - Courant de surcharge
 - Court-circuit à la terre 0 VCC
- Diagnostics configurables (activés/désactivés) du câblage des canaux, page 108 pouvant détecter les conditions suivantes :
 - Fil ouvert (ou rompu)
- Diagnostics configurables (activés/désactivés) du câblage des canaux pouvant détecter les conditions suivantes lorsque la sortie est *non alimentée* :
 - Court-circuit à la terre 0 V

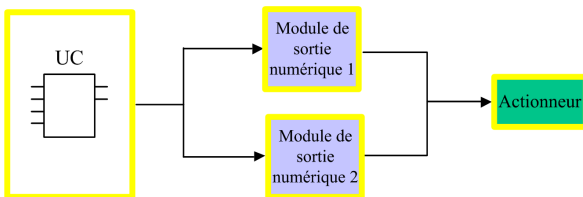
- Diagnostics configurables (activés/désactivés) du câblage des canaux pouvant détecter les conditions suivantes lorsque la sortie est *alimentée* ou *non alimentée* :
 - Court-circuit sur le 24 VCC
 - Circuits croisés entre deux canaux (si l'alimentation des capteurs est fournie en interne)
- Paramètres de repli configurables pour chaque canal, appliqués en cas de perte de la communication entre le contrôleur et le module de sortie.
- Permutation de module à chaud pendant le fonctionnement.
- CCOTF (modification de configuration à la volée) pendant le fonctionnement en mode de maintenance, page 269. (La fonction CCOTF n'est pas prise en charge mode de sécurité, page 268.)

NOTE: un auto-test est réalisé sur chaque sortie pour vérifier si elle peut être non alimentée et atteindre son état sécurisé défini sans impacter la charge (impulsion désactivée < 1 ms). Cette opération s'applique alternativement à chaque sortie alimentée selon une période inférieure à 1 seconde. Lorsque la sortie est connectée à une entrée statique d'un produit, cette entrée peut détecter l'impulsion. L'installation d'un filtre peut s'avérer nécessaire pour éviter que l'impulsion n'affecte l'entrée.

Haute disponibilité

Vous pouvez connecter le contrôleur à deux modules de sortie via un canal noir, puis connecter chaque module de sortie à un seul actionneur. Aucun bloc fonction n'est nécessaire puisque le signal en provenance du contrôleur est connecté aux deux canaux de sortie.

La figure suivante illustre la configuration de sorties numériques redondantes aux fins de haute disponibilité :



L'état d'intégrité de chaque module de sortie peut être lu à partir des éléments de sa structure `T_U_DIS_SIS_OUT_8`, page 114. Vous pouvez utiliser ces données pour déterminer si un module a besoin d'être remplacé. Si un module cesse d'être opérationnel et doit être remplacé, le système continue de fonctionner dans une configuration conforme au niveau SIL3 pendant l'opération d'échange de module.

Pour plus de détails sur cette conception, reportez-vous à l'exemple de câblage des sorties aux fins de haute disponibilité, page 111.

Connecteur de câblage du BMXSDO0802

Introduction

Le module de sortie numérique BMXSDO0802 présente un groupe unique de 8 sorties.

- Les deux broches d'alimentation +24 VCC communes (18 et 20) sont connectées en interne.
- Toutes les broches 0 V communes (1, 3, 5, 7, 9, 11, 13, 15, 17 et 19) sont connectées en interne.

Borniers

Vous pouvez utiliser les borniers Schneider Electric à 20 points suivants pour le connecteur à 20 broches en face avant du module :

- bornier à vis étriers BMXFTB2010
- bornier à vis à cage BMXFTB2000
- bornier à ressorts BMXFTB2020

NOTE: Il n'est possible de retirer les borniers que lorsque le module est hors tension.

Alimentation process

Une alimentation process de catégorie II très basse tension (TBTS/TBTP) protégée 24 VCC est requise. Utilisez une alimentation qui ne rétablit pas automatiquement le courant après une coupure.

AVIS	
NON-CONFORMITÉ DES CIRCUITS ÉLECTRIQUES	
Ne raccordez pas le 0V d'une alimentation SELV à la terre.	
Le non-respect de ces instructions peut provoquer des dommages matériels.	

Fusible

Un fusible à fusion rapide de 6 A maximum est nécessaire pour protéger l'alimentation externe contre les situations de court-circuit et de surtension.

AVIS

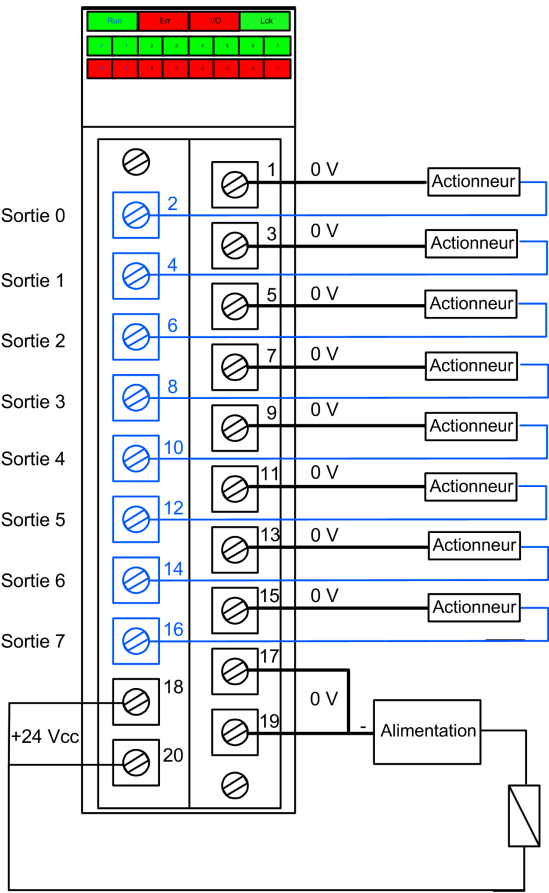
SÉLECTION DE FUSIBLE INCORRECTE

Utilisez des fusibles à fusion rapide pour protéger les composants électroniques du module de sortie numérique contre les excès d'intensité électrique.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Broches du connecteur de câblage

Le schéma de câblage suivant présente un module de sortie connecté à lui seul à 8 actionneurs :



Mappage des sorties et des broches du connecteur

Les broches du module de sortie BMXSDO0802 sont décrites ci-après :

Description de la broche	Numéro de broche sur le bornier		Description de la broche
Sortie 0	2	1	0 V commun
Sortie 1	4	3	0 V commun
Sortie 2	6	5	0 V commun
Sortie 3	8	7	0 V commun
Sortie 4	10	9	0 V commun
Sortie 5	12	11	0 V commun
Sortie 6	14	13	0 V commun
Sortie 7	16	15	0 V commun
Alimentation process 24 VCC	18	17	0 V commun
Alimentation process 24 VCC	20	19	0 V commun

Exemples de câblage d'application du module de sortie BMXSDO0802

Introduction

Vous pouvez câbler le module de sortie numérique de sécurité BMXSDO0802 à des actionneurs pour assurer la conformité SIL3 Cat4/PLe de différentes manières en fonction des exigences en matière de haute disponibilité.

Le niveau d'intégrité de sécurité (SIL) maximum est déterminé par la fiabilité de l'actionneur et la longueur de l'intervalle entre tests périodiques conformément à la norme IEC 61508.

⚠ Avertissement

PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ

Raccordez les actionneurs, qui ne répondent pas à la fiabilité des normes SIL visées, en redondance sur deux canaux.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Les exemples suivants de câblage d'application de sortie numérique SIL3 Cat4/PLe sont décrits ci-après :

- Cat4/PLe :
 - un seul canal du module de sortie commande une seule variable de processus. Un seul actionneur est utilisé dans cette conception.
- Cat4/PLe avec haute disponibilité :
 - deux modules de sortie redondants, avec sur chacun un canal connecté à un actionneur distinct, mais commandant la même variable de processus.

Lorsque l'équipement est utilisé dans une application impliquant des risques d'incendie et d'émanation de gaz, ou encore lorsque l'état de demande de la sortie est alimenté, suivez les instructions suivantes :

▲ AVERTISSEMENT

FONCTIONNEMENT INATTENDU DE L'ÉQUIPEMENT

- Incluez un test périodique de la détection de fil rompu qui consiste à retirer le bornier et à vérifier que les bits d'erreur correspondants sont définis.
- Vérifiez l'efficacité de la détection de court-circuit à la terre, soit en activant la fonction de diagnostic **Test d'impulsion pour l'état alimenté** dans l'onglet **Configuration** du module, soit en implémentant une autre procédure (par exemple, en définissant la sortie sur 1 et en vérifiant les diagnostics, et ainsi de suite).

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

N'utilisez pas des actionneurs de type lampe car leur impédance est très faible à l'état alimenté, ce qui peut créer le risque de détecter une condition erronée de court-circuit ou de surcharge.

Diagnostics de câblage configurables dans Control Expert

Sur le module de sortie numérique de sécurité BMXSDO0802, utilisez la page **Configuration** dans Control Expert pour effectuer les actions suivantes :

- Activer l'option **Détection de court-circuit à 24 V** pour chaque canal alimenté. Ce test effectue les diagnostics de câblage d'actionneur suivants pour un canal :
 - Détection de court-circuit sur 24 VCC.
 - Détection de circuit croisé entre deux canaux de sortie.

- Activer l'option **Détection de fil ouvert** pour chacun des huit canaux afin d'obtenir les diagnostics de câblage suivants pour le canal concerné :
 - Détection de fil ouvert (ou rompu) (le canal de sortie n'est pas connecté à l'actionneur)
 - Détection de court-circuit à la terre 0 VCC
- Activer le **Test d'impulsion pour l'état alimenté** pour chaque canal de sortie. Ce test est exécuté périodiquement lorsque la sortie est dans l'état non alimenté ; il applique une impulsion (de moins de 1 ms) à la sortie pour déterminer si celle-ci peut passer à l'état alimenté. Si le courant dépasse le seuil de 0,7 A, la sortie est signalée comme condition de court-circuit avec la terre 0 VCC. La période de test est inférieure à 1 s.

AVERTISSEMENT

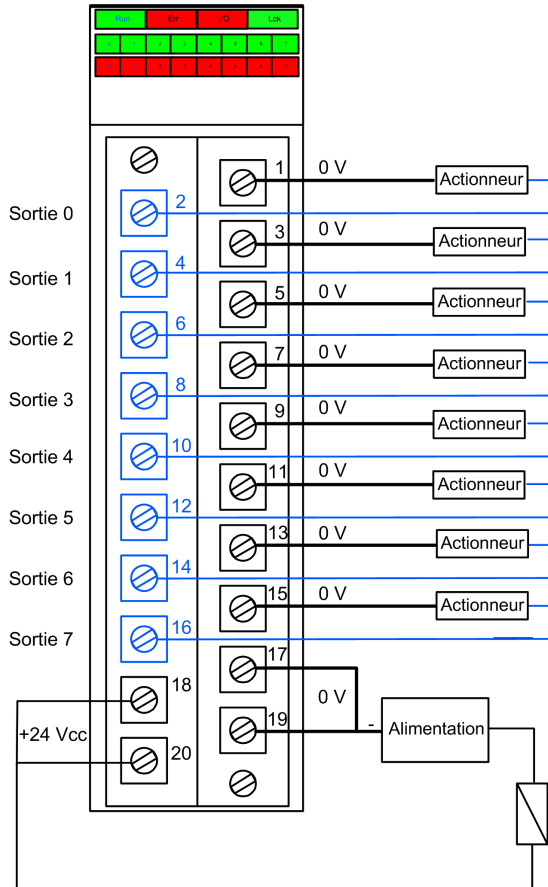
FONCTIONNEMENT INATTENDU DE L'ÉQUIPEMENT

- Activez les diagnostics disponibles fournis dans Control Expert pour détecter et réagir aux conditions énumérées ci-dessus.
- Appliquez d'autres mesures de sécurité pour détecter ou exclure ces conditions lorsqu'un test de diagnostic n'est pas activé ou n'est pas disponible dans Control Expert.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

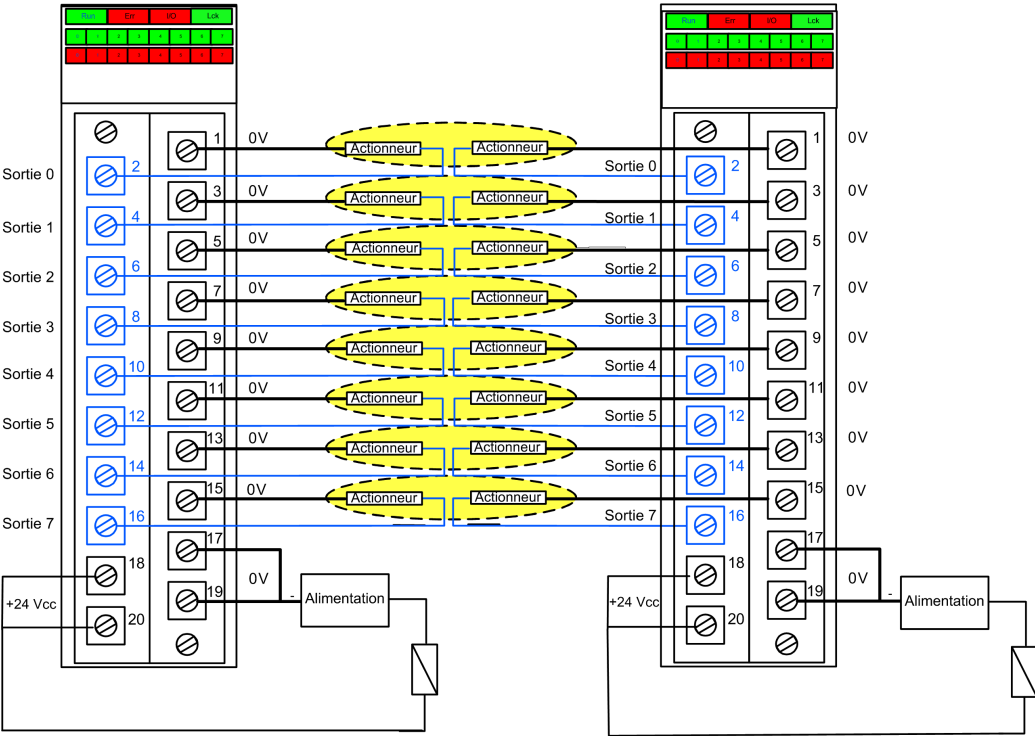
SIL 3 Cat4/PLe - Exemple pour un seul module de sortie numérique

L'exemple suivant présente un actionneur exclusif câblé à chaque sortie d'un module de sortie. Chaque boucle respecte les normes SIL3 Cat4/PLe :



Exemple pour SIL 3 Cat4/PLe haute disponibilité :

Dans le schéma de câblage suivant, deux sorties redondantes commandent la même variable de processus. Comme le montre la représentation suivante, chaque sortie est connectée à un actionneur distinct, puis chaque actionneur exécute la même commande envoyée sur différents canaux. Une autre solution consiste à câbler les deux sorties redondantes ensemble pour commander le même actionneur.



Récapitulatif des diagnostics de câblage des sorties

Les deux solutions fournissent les diagnostics de câblage suivants :

Condition	Diagnostic fourni comme état de la sortie ?	
	Alimenté	Non alimenté
Fil ouvert (ou rompu) ¹	Oui. Diagnostic à chaque cycle.	Oui. Diagnostic à chaque cycle.
Sortie en surcharge ²	Oui. Diagnostic à chaque cycle.	Non.
Court-circuit à la terre 0 V	Oui. Diagnostic à chaque cycle.	Oui. Période de diagnostic < 1 s.

Condition	Diagnostic fourni comme état de la sortie ?	
	Alimenté	Non alimenté
Court-circuit vers le 24 VCC ¹	Oui. Période de diagnostic < 1 s.	Oui. Diagnostic à chaque cycle.
Circuits croisés entre deux canaux	Oui. Période de diagnostic < 1 s.	Oui. Diagnostic à chaque cycle.
1. Cette fonction de diagnostic est exécutée si elle est activée dans l'onglet Configuration du module dans Control Expert. 2. Une fois la condition résolue, réarmez la sortie en la mettant hors tension.		

⚠ AVERTISSEMENT

DETECTION DE COURT-CIRCUIT A LA TERRE 0 VCC.

- Activez l'option **Détection de fil ouvert** dans le module **Configuration** pour la condition de court-circuit à la terre 0 V avec l'état de sortie non alimenté.
- Sinon, appliquez une autre mesure de sécurité pour détecter ou exclure cette condition.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠ AVERTISSEMENT

COURT-CIRCUIT VERS LE 24 VCC

- Activez l'option **Détection de court-circuit vers le 24 VCC** dans le module **Configuration** pour la condition de court-circuit 24 VCC avec l'état de sortie alimenté ou non alimenté.
- Sinon, appliquez une autre mesure de sécurité pour détecter ou exclure cette condition.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠ AVERTISSEMENT

CIRCUITS CROISÉS

Appliquez d'autres mesures de sécurité lorsque le module ne peut pas détecter la condition de circuits croisés entre deux canaux avec l'état de sortie non alimenté et l'autre canal non alimenté. Cette mesure de sécurité supplémentaire détecte ou exclut cette condition si elle se produit lorsque l'état de sortie passe à alimenté.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠ AVERTISSEMENT

CIRCUITS CROISÉS

- Activez l'option **Détection de court-circuit vers le 24 VCC** dans le module **Configuration** pour la condition de circuits croisés entre deux canaux avec l'état de sortie non alimenté et l'autre canal alimenté.
- Sinon, appliquez d'autres mesures de sécurité pour détecter ou exclure cette condition lorsque la sortie passe à l'état alimenté.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠ AVERTISSEMENT

CIRCUITS CROISÉS

Appliquez d'autres mesures de sécurité lorsque le module ne peut pas détecter la condition de circuits croisés entre deux canaux avec l'état de sortie alimenté et l'autre canal non alimenté. Cette mesure de sécurité supplémentaire détecte ou exclut cette condition.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠ AVERTISSEMENT

CIRCUITS CROISÉS

- Activez l'option **Détection de court-circuit vers le 24 VCC** dans le module **Configuration** pour la condition de circuits croisés entre deux canaux avec l'état de sortie alimenté et l'autre canal non alimenté.
- Sinon, appliquez une autre mesure de sécurité pour détecter ou exclure cette condition.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Structure des données du BMXSDO0802

Introduction

Le DDDT (Device Derived Data Type) `T_U_DIS_SIS_OUT_8` est l'interface entre le module de sortie numérique BMXSDO0802 et l'application qui s'exécute dans le contrôleur. Le

DDDT T_U_DIS_SIS_OUT_8 intègre les types de données T_SAFE_COM_DBG_OUT et T_U_DIS_SIS_CH_OUT.

Toutes ces structures sont décrites ci-après.

Structure du DDDT T_U_DIS_SIS_OUT_8

La structure du DDDT T_U_DIS_SIS_OUT_8 comprend les éléments suivants :

Élément	Type de données	Description	Accès
MOD_HEALTH ¹	BOOL	1 : Le module fonctionne normalement. 0 : le module ne fonctionne pas correctement.	L
SAFE_COM_STS ¹	BOOL	1 : la communication du module est valide. 0 : la communication du module n'est pas valide.	L
PP_STS	BOOL	1 : l'alimentation process est opérationnelle. 0 : l'alimentation process n'est pas opérationnelle.	L
CONF_LOCKED	BOOL	1 : la configuration du module est verrouillée. 0 : la configuration du module n'est pas verrouillée.	L
S_COM_DBG	T_SAFE_COM_DBG_OUT	Structure de débogage de communication sécurisée	L
CH_OUT	ARRAY[0...7] of T_U_DIS_SIS_CH_OUT	Tableau de la structure des canaux.	L
S_TO	UINT	Délai de sécurité à l'issue duquel le module passe en état de repli.	L
MUID ²	ARRAY[0...3] of DWORD	ID unique du module (affecté automatiquement par Control Expert)	L
RESERVED_1	ARRAY[0...8] of INT	–	–
RESERVED_2	ARRAY[0...6] of INT	–	–
1. 1. Lorsque la tâche SAFE n'est pas en mode d'exécution dans le contrôleur, les données échangées entre le contrôleur et le module ne sont pas mises à jour et MOD_HEALTH comme SAFE_COM_STS ont pour valeur 0. 2. Cette valeur générée automatiquement peut être modifiée à l'aide de la commande Générer > Renouveler les ID et Régénérer tout dans le menu principal de Control Expert.			

Structure T_SAFE_COM_DBG_OUT

La structure T_SAFE_COM_DBG_OUT comprend les éléments suivants :

Elément	Type de données	Description	Accès
S_COM_EST	BOOL	1 : la communication avec le module est établie. 0 : la communication avec le module n'est pas établie ou est corrompue.	L
M_NTP_SYNC	BOOL	Avec un micrologiciel de contrôleur de version 3.10 ou antérieure : 1 : le module est synchronisé avec le serveur NTP. 0 : le module n'est pas synchronisé avec le serveur NTP. NOTE: Avec un micrologiciel de contrôleur de version 3.20 ou ultérieure, la valeur est toujours 1.	L
CPU_NTP_SYNC	BOOL	Avec un micrologiciel de contrôleur de version 3.10 ou antérieure : 1 : le contrôleur est synchronisé avec le serveur NTP. 0 : le contrôleur n'est pas synchronisé avec le serveur NTP. NOTE: Avec un micrologiciel de contrôleur de version 3.20 ou ultérieure, la valeur est toujours 1.	L
CHECKSUM	BYTE	Somme de contrôle de trame de communication.	L
COM_DELAY	UINT	Délai de communication entre deux valeurs reçues par le module : 1...65534 : temps écoulé (en ms) depuis la réception par le contrôleur de la dernière communication émise par le module. 65535 : le contrôleur UC n'a pas reçu de communication du module.	L
COM_TO	UINT	Valeur du délai d'expiration pour les communications en provenance du module.	R/W
STS_MS_IN	UINT	Valeur de l'horodatage sécurisé des données reçues du module, à la milliseconde la plus proche.	L
S_NTP_MS	UINT	Valeur horaire sécurisée du cycle en cours, à la milliseconde la plus proche.	L

Elément	Type de données	Description	Accès
STS_S_IN	UDINT	Valeur de l'horodatage sécurisé des données reçues du module, en secondes.	L
S_NTP_S	UDINT	Valeur horaire sécurisée du cycle en cours, en secondes.	L
CRC_IN	UDINT	Valeur CRC pour les données reçues du module.	L
STS_MS_OUT	UINT	Valeur de l'horodatage sécurisé des données à envoyer au module, à la milliseconde la plus proche.	L
STS_S_OUT	UDINT	Valeur de l'horodatage sécurisé des données à envoyer au module, en secondes.	L
CRC_OUT	UDINT	Valeur de CRC pour les données à envoyer au module.	L

Structure T_U_DIS_SIS_CH_OUT

La structure T_U_DIS_SIS_CH_OUT comprend les éléments suivants :

Elément	Type de données	Description	Accès
CH_HEALTH ¹	BOOL	1 : La voie est opérationnelle. 0 : une erreur a été détectée sur le canal, lequel n'est pas opérationnel. Formule : CH_HEALTH = not (SC ou OL ou IC ou OC) et SAFE_COM_STS et non (module à l'état Repli)	L
VALUE	EBOOL	Commande de canal de sortie : 1 : commande de sortie fermée (alimentée) 0 : commande de sortie ouverte (non alimentée)	R/W
TRUE_VALUE ²	BOOL	Valeur de lecture du canal de relais de sortie : 1 : la sortie est fermée (alimentée) 0 : la sortie est ouverte (non alimentée)	L
OC	BOOL	1 : le canal est ouvert ou court-circuité à la terre. 0 : le canal est connecté et n'est pas court-circuité à la terre.	L

Elément	Type de données	Description	Accès
SC	BOOL	1 : le canal est court-circuité sur une source 24 V ou inter-circuité avec un autre canal. 0 : 0 : le canal n'est pas court-circuité sur une source 24 V ni inter-circuité.	L
OL	BOOL	1 : le canal est surchargé ou court-circuité sur le 0 V. 0 : le canal n'est pas surchargé ni court-circuité sur le 0 V.	L
IC	BOOL	1 : canal non valide détecté par le module. 0 : le canal est déclaré opérationnel en interne par le module.	L
V_OC	BOOL	Etat de configuration du test de circuit ouvert : 1 : Activé. 0 : Désactivé.	L
V_SC	BOOL	État de configuration du test de court-circuit vers une source 24 V : 1 : Activé. 0 : Désactivé.	L
V_PULSE_ON	BOOL	État de configuration du test d'impulsion de mise sous tension : 1 : Activé. 0 : Désactivé.	L
CH_FBC	BOOL	Configuration du réglage de repli du canal : 1 : Valeur définie par l'utilisateur. 0 : Maintien dernière valeur	L
CH_FBST	BOOL	Configuration de l'état de repli du canal lorsque l'utilisateur défini est sélectionné : 1 : Alimenté. 0 : Non alimenté.	RO
1. Lorsque la tâche SAFE n'est pas en mode d'exécution dans le contrôleur, les données échangées entre le contrôleur et le module ne sont pas mises à jour et CH_HEALTH a pour valeur 0. 2. L'élément TRUE_VALUE peut être horodaté par le BMX CRA ou le BME CRA.			

Module de sortie relais numérique du BMXSRA0405

Introduction

Cette section décrit le module de sortie relais numérique de sécurité du BMXSRA0405 .

Module de sortie relais numérique de sécurité BMXSRA0405

Introduction

Les caractéristiques du module de sortie relais numérique de sécurité BMXSRA0405 sont les suivantes :

- 4 sorties relais de courant 5 A.
- Tension de sortie nominale de 24 VCC et 24 à 230 VCA (surtension de catégorie II).
- Atteint jusqu'à l'évaluation SIL4 (EN5012x) / SIL3 (IEC61508) Catégorie 4 (Cat4) / Niveau de performance e (PLe).
- Prise en charge de 8 choix prédéfinis de configuration de câblage de l'application.
- Surveillance automatique par autotest configurable de la capacité du relais à exécuter l'état de sortie commandé (en fonction de la configuration de câblage d'application sélectionnée).
- Paramètres configurables de mode de repli et de délai de repli (en ms) du module.
- Affichage de diagnostics par LED, page 259 pour le module et pour chaque canal de sortie.
- Permutation de module à chaud pendant le fonctionnement.
- CCOTF (modification de configuration à la volée) pendant le fonctionnement en mode de maintenance, page 269. (La fonction CCOTF n'est pas prise en charge en mode de sécurité, page 268.)

Connecteur de câblage du BMXSRA0405

Introduction

Le module de sortie relais numérique du BMXSRA0405 comprend 4 relais et prend en charge jusqu'à 4 sorties. Il présente une paire de broches *a* et *b* pour chaque relais. Pour chaque relais :

- Les deux broches *a* sont connectées en interne.
- Les deux broches *b* sont également connectées en interne.

Borniers

Vous pouvez utiliser les borniers Schneider Electric à 20 points suivants pour le connecteur à 20 broches en face avant du module :

- bornier à vis étriers BMXFTB2010
- bornier à vis à cage BMXFTB2000
- bornier à ressorts BMXFTB2020

NOTE: Il n'est possible de retirer les borniers que lorsque le module est hors tension.

Alimentation process

Vous devez installer l'alimentation process 24 VCC ou 24 VCA à 230 VCA appropriée.

Fusible

Il est obligatoire d'installer un fusible à action rapide de 6 A maximum, approprié à l'application sélectionnée et à la conception des relais.

AVIS
SÉLECTION DE FUSIBLE INCORRECTE Utilisez des fusibles à fusion rapide pour protéger les composants électroniques du module de sortie numérique contre les excès d'intensité électrique. Le non-respect de ces instructions peut provoquer des dommages matériels.

Installez un fusible externe en série avec l'alimentation externe, le relais et la charge.

⚠️ AVERTISSEMENT

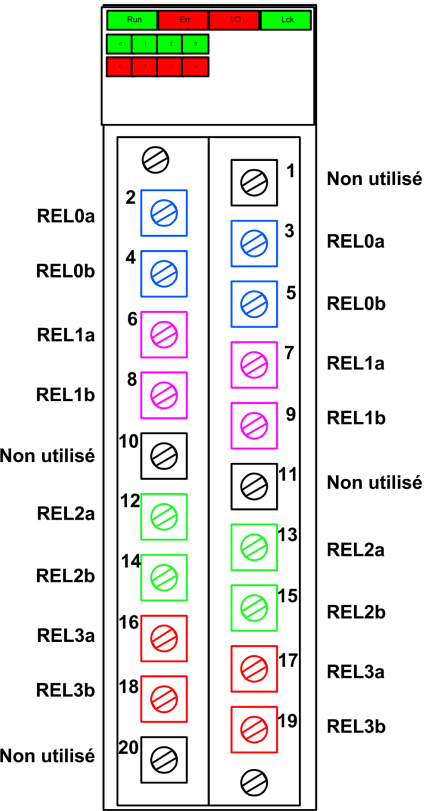
FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT

Mettez en oeuvre les diagnostics de câblage appropriés pour détecter et éviter les erreurs sur le câblage externe.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Connecteur de câblage

L'illustration suivante présente les broches situées sur le module relais :



Mappage des entrées aux des broches du connecteur

Les broches du module de sortie relais numérique du BMXSRA0405 sont décrites ci-après :

Description de la broche	Numéro de broche sur le bornier		Description de la broche
Contact NO, relais 0a	2	1	Inutilisée
Contact NO, relais 0b	4	3	Contact NO, relais 0a
Contact NO, relais 1a	6	5	Contact NO, relais 0b
Contact NO, relais 1b	8	7	Contact NO, relais 1a
Inutilisée	10	9	Contact NO, relais 1b
Contact NO, relais 2a	12	11	Inutilisée
Contact NO, relais 2b	14	13	Contact NO, relais 2a
Contact NO, relais 3a	16	15	Contact NO, relais 2b
Contact NO, relais 3b	18	17	Contact NO, relais 3a
Inutilisée	20	19	Contact NO, relais 3b

NOTE: Les deux broches *a* associées à chaque relais étant connectées en interne, vous n'avez besoin d'utiliser qu'une seule broche *a* pour chaque relais. De même, les deux broches *b* associées à chaque relais étant connectées en interne, vous n'avez besoin d'utiliser qu'une seule broche *b* pour chaque relais.

Exemples de câblage d'application du module de sortie BMXSRA0405

Introduction

Vous pouvez configurer le module de sortie relais numérique de sécurité BMXSRA0405 pour les standards SIL2 / Cat2/PLc ou SIL3 / Cat4/PLe de différentes manières, en fonction des conditions suivantes :

- Nombre de sorties que le module devra prendre en charge
- Façon dont vous souhaitez tester la capacité du module à placer l'actionneur dans l'état de demande voulu, à savoir :
 - test automatique par le module (auquel cas il n'y a pas de transition d'état pour l'actionneur)
 - procédure qui exécute et vérifie une transition journalière du signal communiqué par le module à l'actionneur (auquel cas la transition impacte l'état de l'actionneur)

Effectuez cette configuration en sélectionnant un numéro d'application (voir les tableaux ci-après) dans la liste **Fonction** figurant sous l'onglet **Configuration** dans Control Expert.

Applications de câblage pour SIL2 Cat2/PLc :

Fonction	État de demande	Relais	Sorties	Test de signal ?		Schéma de câblage (voir plus bas)
				Test de signal automatique ?	Transition de signal quotidienne ?	
Application_1	Non alimenté	1	4	Non	Oui	A
Application_2	Non alimenté	2	2	Oui	Non	B
Application_3	Alimenté	1	4	Non	Oui	A
Application_4	Alimenté	2	2	Oui	Non	C
1. Le test de signal automatique n'impacte pas l'état de l'actionneur.						

Applications de câblage pour SIL3 Cat4/PLe :

Fonction	État de demande	Relais	Sorties	Test de signal ?		Schéma de câblage (voir plus bas)
				Test de signal automatique ? ¹	Transition de signal quotidienne ?	
Application_5	Non alimenté	2	2	Non	Oui	C
Application_6	Non alimenté	4	1	Oui	Non	D
Application_7	Alimenté	2	2	Non	Oui	C
Application_8	Alimenté	2	2	Oui	Non	C
1. Le test de signal automatique n'impacte pas l'état de l'actionneur.						

Chacun de ces huit choix d'application est décrit dans les exemples qui suivent.

Application_1 : 4 sorties, SIL2 / Cat2 / PLc, état non alimenté, pas de test de signal automatique

L'état de la demande pour cette conception d'application est "non alimenté". Si le module détecte une erreur interne pour une sortie, il met celle-ci en état non alimenté.

⚠ AVERTISSEMENT

PERTE DE LA CAPACITE A EXECUTER LES FONCTIONS DE SECURITE

Pour réaliser le niveau SIL2 de la norme IEC61508 et le niveau Cat2/PLc de la norme ISO 13849 avec cette conception de câblage, effectuez au moins une transition de signal quotidienne de l'état alimenté vers l'état non alimenté.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

La conception du câblage pour Application_1 est décrite dans le schéma de câblage A, page 127 ci-après.

Application_2 : 2 sorties, SIL2 / Cat2 / PLc, état non alimenté, test de signal automatique

L'état de la demande pour cette conception d'application est "non alimenté". Si le module détecte une erreur de sortie interne sur un des relais utilisés pour une sortie, il met les deux relais associés à cette sortie (relais 0 et relais 1 ou relais 2 et relais 3) en état non alimenté.

Votre programme d'application doit commander le même état de sortie à tous les relais qui activent le même actionneur.

Le module effectue séquentiellement un test d'impulsion périodique automatique sur chaque relais. La durée de ce test est inférieure à 50 ms. En raison de la configuration des deux relais utilisés (en parallèle), le test n'a pas d'impact sur la charge de sortie (normalement *alimentée*). Vous pouvez configurer la fréquence de ce test en définissant le paramètre **Période de surveillance** dans l'onglet **Configuration** du module. Les valeurs valides de périodicité pour ce test vont de 1 à 1440 minutes.

La conception du câblage pour Application_2 est décrite dans le schéma de câblage B, page 128 ci-après.

Application_3 : 4 sorties, conformité SIL2 et Cat2/PLc, état alimenté, pas de test de signal automatique

L'état de la demande pour cette conception d'application est alimenté. Si le module détecte une erreur interne pour une sortie, il met celle-ci en état non alimenté (état de sécurité défini).

▲ AVERTISSEMENT

PERTE DE LA CAPACITÉ A EXÉCUTER LES FONCTIONS DE SÉCURITÉ

Pour réaliser le niveau SIL2 de la norme IEC61508 et le niveau Cat2/PLc de la norme ISO 13849 avec cette conception de câblage, effectuez au moins une transition de signal quotidienne de l'état non alimenté vers l'état alimenté.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

La conception du câblage pour Application_3 est décrite dans le schéma de câblage A, page 127 ci-après.

Application_4 : 2 sorties, SIL2 / Cat2 / PLc, état alimenté, test de signal automatique

L'état de la demande pour cette conception d'application est "alimenté". Si le module détecte une erreur de sortie interne sur un des relais utilisés pour une sortie, il met les deux relais associés à cette sortie (relais 0 et relais 1 ou relais 2 et relais 3) en état non alimenté.

Votre programme d'application doit commander le même état de sortie à tous les relais qui activent le même actionneur.

Le module effectue séquentiellement un test d'impulsion périodique sur chaque relais. La durée de ce test est inférieure à 50 ms. En raison de la configuration des deux relais utilisés (en parallèle), le test n'a pas d'impact sur la charge de sortie (normalement *alimentée*). Vous pouvez configurer la fréquence de ce test en définissant le paramètre **Période de surveillance** dans l'onglet **Configuration** du module. Les valeurs valides de périodicité pour ce test vont de 1 à 1440 minutes.

La conception du câblage pour Application_4 est décrite dans le schéma de câblage C, page 129 ci-après.

Application_5 : 2 sorties, conformité SIL3 et Cat4/PLe, état non alimenté, pas de test de signal automatique

L'état de la demande pour cette conception d'application est "non alimenté". Si le module détecte une erreur de sortie interne sur un des relais utilisés pour une sortie, il met les deux relais associés à cette sortie (relais 0 et relais 1 ou relais 2 et relais 3) en état non alimenté.

Votre programme d'application doit commander le même état de sortie à tous les relais qui activent le même actionneur.

▲ AVERTISSEMENT

PERTE DE LA CAPACITÉ À EXÉCUTER LES FONCTIONS DE SÉCURITÉ

Pour réaliser le niveau SIL3 de la norme IEC61508 et le niveau Cat4/PLe de la norme ISO 13849 avec cette conception de câblage, effectuez au moins une transition de signal quotidienne de l'état alimenté vers l'état non alimenté.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

La conception du câblage pour Application_5 est décrite dans le schéma de câblage C, page 129 ci-après.

Application_6 : 1 sortie, conformité SIL3 et Cat4/PLe, état non alimenté, test de signal automatique

L'état de la demande pour cette conception d'application est "non alimenté". Si le module détecte une erreur de sortie interne sur un des relais utilisés pour une sortie, il met tous les relais du module (relais 0, relais 1, relais 2 et relais 3) en état non alimenté.

Votre programme d'application doit commander le même état de sortie à tous les relais qui activent le même actionneur.

Le module effectue séquentiellement un test d'impulsion périodique sur chaque relais. La durée de ce test est inférieure à 50 ms. En raison de la configuration des quatre relais utilisés (2 paires de 2 relais série configurés en parallèle), le test n'a pas d'impact sur la charge de sortie (normalement *alimentée*). Vous pouvez configurer la fréquence de ce test en définissant le paramètre **Période de surveillance** dans l'onglet **Configuration** du module. Les valeurs valides de périodicité pour ce test vont de 1 à 1440 minutes.

La conception du câblage pour Application_6 est décrite dans le schéma de câblage D, page 130 ci-après.

Application_7 : 2 sorties, conformité SIL3 et Cat4/PLe, état alimenté, pas de test de signal automatique

L'état de la demande pour cette conception d'application est "alimenté". Si le module détecte une erreur de sortie interne sur un des relais utilisés pour une sortie, il met les deux relais associés à cette sortie (relais 0 et relais 1 ou relais 2 et relais 3) en état non alimenté.

Votre programme d'application doit commander le même état de sortie à tous les relais qui activent le même actionneur.

⚠ AVERTISSEMENT

PERTE DE LA CAPACITÉ A EXÉCUTER LES FONCTIONS DE SÉCURITÉ

Pour réaliser le niveau SIL3 de la norme IEC61508 et le niveau Cat4/PLe de la norme ISO 13849 avec cette conception de câblage, effectuez au moins une transition de signal quotidienne de l'état non alimenté vers l'état alimenté.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

La conception du câblage pour Application_7 est décrite dans le schéma de câblage C, page 129 ci-après.

Application_8 : 2 sorties, SIL3 Cat4 / PLe, état alimenté, test de signal automatique

L'état de la demande pour cette conception d'application est "alimenté". Si le module détecte une erreur de sortie interne sur un des relais utilisés pour une sortie, il met les deux relais associés à cette sortie (relais 0 et relais 1 ou relais 2 et relais 3) en état non alimenté.

Votre programme d'application doit commander le même état de sortie à tous les relais qui activent le même actionneur.

Le module effectue séquentiellement un test d'impulsion périodique sur chaque relais. La durée de ce test est inférieure à 50 ms. En raison de la configuration des deux relais utilisés (en série), le test n'a pas d'impact sur la charge de sortie (normalement *non alimentée*). Vous pouvez configurer la fréquence de ce test en définissant le paramètre **Période de surveillance** dans l'onglet **Configuration** du module. Les valeurs valides de périodicité pour ce test vont de 1 à 1440 minutes.

La conception du câblage pour Application_8 est décrite dans le schéma de câblage C, page 129 ci-après.

Schéma de câblage A

Ce schéma de câblage concerne Application_1 et Application_3 :

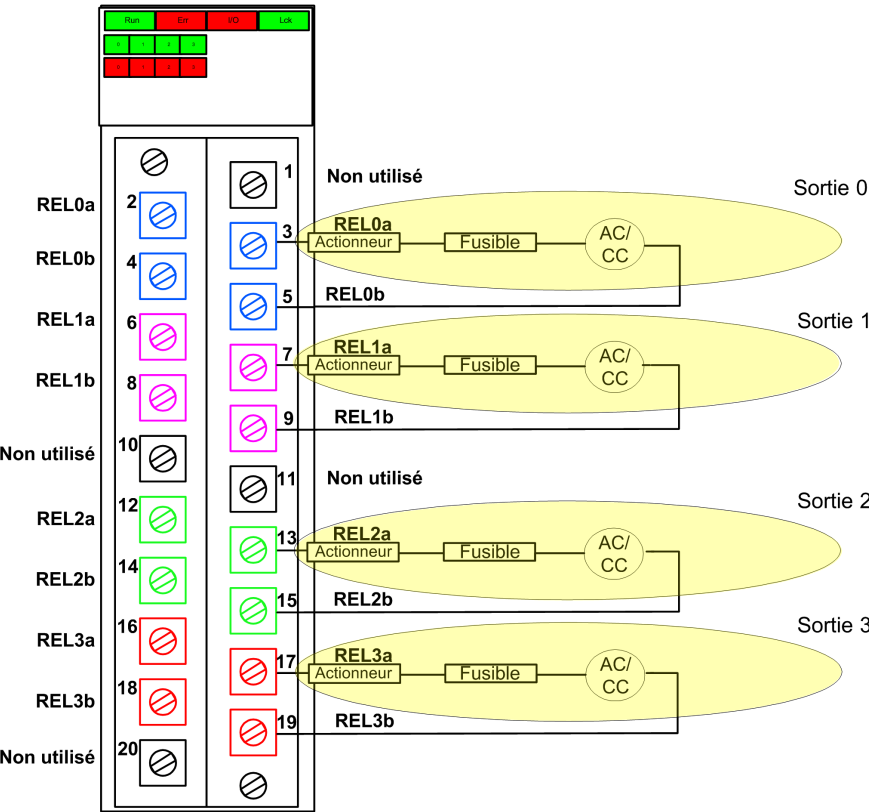


Schéma de câblage B

Ce schéma de câblage concerne Application_2 :

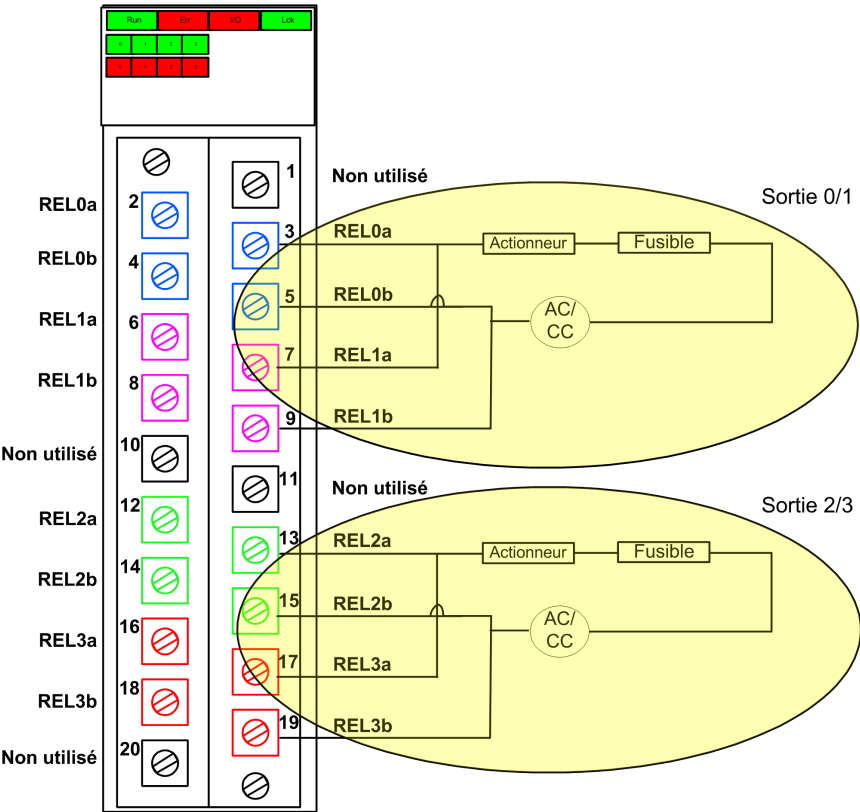


Schéma de câblage C

Ce schéma de câblage concerne Application_4, Application_5, Application_7 et Application_8 :

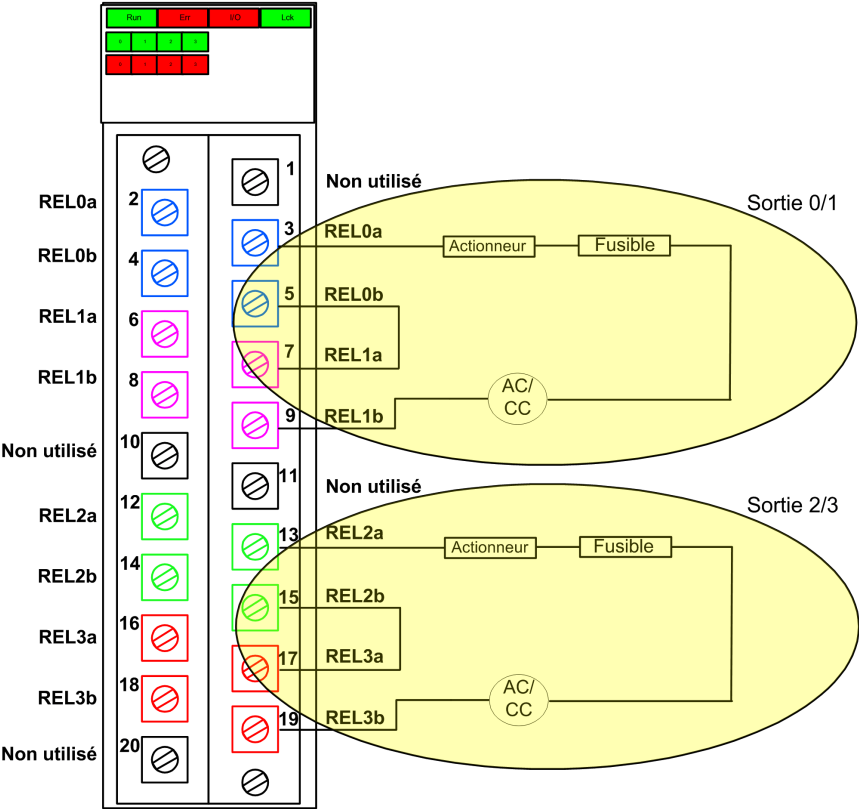
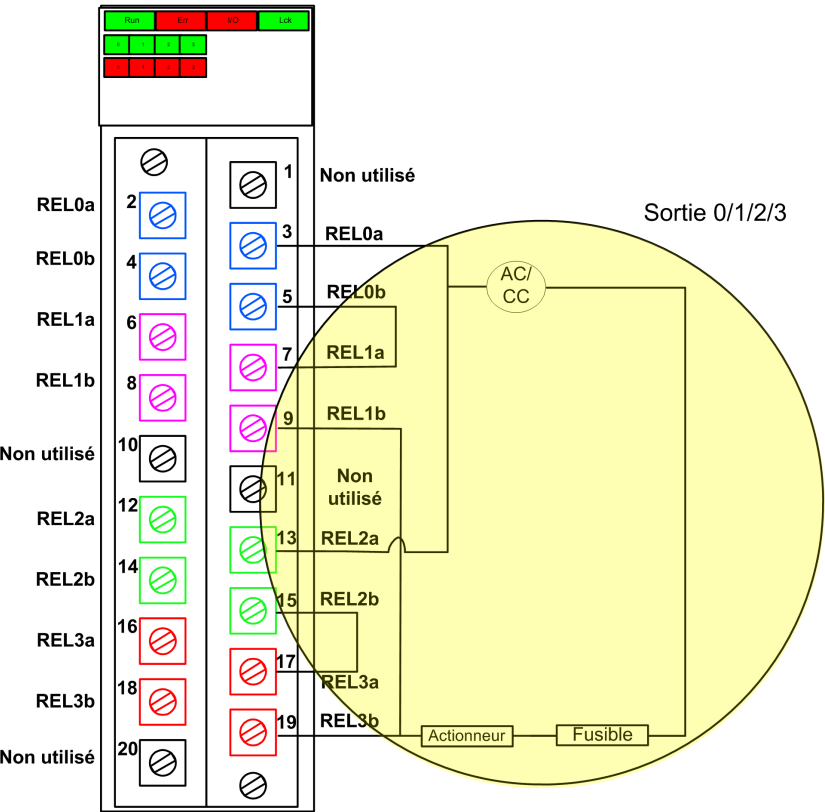


Schéma de câblage D

Ce schéma de câblage concerne Application_6 :



Structure des données du BMXSRA0405

Introduction

Le DDDT (Device Derived Data Type) `T_U_DIS_SIS_OUT_4` est l'interface entre le module de sortie relais BMXSRA0405 et l'application qui s'exécute dans le contrôleur. Le DDDT `T_U_DIS_SIS_OUT_4` intègre les types de données `T_SAFE_COM_DBG_OUT` et `T_U_DIS_SIS_CH_ROUT`.

Toutes ces structures sont décrites ci-après.

Structure du DDDT T_U_DIS_SIS_OUT_4

La structure du DDDT T_U_DIS_SIS_OUT_4 comprend les éléments suivants :

Elément	Type de données	Description	Accès
MOD_HEALTH ¹	BOOL	1 : Le module fonctionne normalement. 0 : le module ne fonctionne pas correctement.	L
SAFE_COM_STS ¹	BOOL	1 : la communication du module est valide. 0 : la communication du module n'est pas valide.	L
CONF_LOCKED	BOOL	1 : la configuration du module est verrouillée. 0 : la configuration du module n'est pas verrouillée.	L
APPLI	UINT	Configuration d'application relais : 1, 2, 3, 4, 5, 6 ou 7.	L
TIME_PERIOD	UINT	Périodicité de la surveillance automatique de relais (en minutes).	L
S_COM_DBG	T_SAFE_COM_DBG_OUT	Structure de débogage de communication sécurisée	L
CH_OUT	ARRAY[0...3] of T_U_DIS_SIS_CH_ROUT	Tableau de la structure des canaux.	–
S_TO	UINT	Délai de sécurité à l'issue duquel le module passe en état de repli.	L
MUID ²	ARRAY[0...3] of DWORD	ID unique du module (affecté automatiquement par Control Expert)	L
RESERVED_1	ARRAY[0...7] of INT	–	–
RESERVED_2	ARRAY[0...6] of INT	–	–
1. Lorsque la tâche SAFE n'est pas en mode d'exécution dans la CPU, les données échangées entre la CPU et le module ne sont pas mises à jour et MOD_HEALTH comme SAFE_COM_STS ont pour valeur 0. 2. Cette valeur générée automatiquement peut être modifiée à l'aide de la commande Générer > Renouveler les ID et Régénérer tout dans le menu principal de Control Expert.			

Structure T_SAFE_COM_DBG_OUT

La structure T_SAFE_COM_DBG_OUT comprend les éléments suivants :

Elément	Type de données	Description	Accès
S_COM_EST	BOOL	1 : la communication avec le module est établie. 0 : la communication avec le module n'est pas établie ou est corrompue.	L
M_NTP_SYNC	BOOL	Avec un micrologiciel de CPU de version 3.10 ou antérieure : 1 : le module est synchronisé avec le serveur NTP. 0 : le module n'est pas synchronisé avec le serveur NTP. NOTE: Avec un micrologiciel de CPU de version 3.20 ou ultérieure, la valeur est toujours 1.	L
CPU_NTP_SYNC	BOOL	Avec un micrologiciel de CPU de version 3.10 ou antérieure : 1 : la CPU est synchronisée avec le serveur NTP. 0 : la CPU n'est pas synchronisée avec le serveur NTP. NOTE: Avec un micrologiciel de CPU de version 3.20 ou ultérieure, la valeur est toujours 1.	L
CHECKSUM	BYTE	Somme de contrôle de trame de communication.	L
COM_DELAY	UINT	Délai de communication entre deux valeurs reçues par le module : 1...65534 : temps écoulé (en ms) depuis la réception par le contrôleur de la dernière communication émise par le module. 65535 : La CPU n'a pas reçu de communication du module.	L
COM_TO	UINT	Valeur du délai d'expiration pour les communications en provenance du module.	R/W
STS_MS_IN	UINT	Valeur de l'horodatage sécurisé des données reçues du module, à la milliseconde la plus proche.	L
S_NTP_MS	UINT	Valeur horaire sécurisée du cycle en cours, à la milliseconde la plus proche.	L
STS_S_IN	UDINT	Valeur de l'horodatage sécurisé des données reçues du module, en secondes.	L
S_NTP_S	UDINT	Valeur horaire sécurisée du cycle en cours, en secondes.	L

Elément	Type de données	Description	Accès
CRC_IN	UDINT	Valeur CRC pour les données reçues du module.	L
STS_MS_OUT	UINT	Valeur de l'horodatage sécurisé des données à envoyer au module, à la milliseconde la plus proche.	L
STS_S_OUT	UDINT	Valeur de l'horodatage sécurisé des données à envoyer au module, en secondes.	L
CRC_OUT	UDINT	Valeur de CRC pour les données à envoyer au module.	L

Structure T_U_DIS_SIS_CH_ROUT

La structure T_U_DIS_SIS_CH_ROUT comprend les éléments suivants :

Elément	Type de données	Description	Accès
CH_HEALTH ¹	BOOL	1 : La voie est opérationnelle. 0 : une erreur a été détectée sur le canal, lequel n'est pas opérationnel. Formule : CH_HEALTH = not (IC) and SAFE_COM_STS and not (module à l'état Repli)	L
VALUE	EBOOL	Commande de canal de sortie : 1 : commande de sortie fermée (alimentée) 0 : commande de sortie ouverte (non alimentée)	R/W
TRUE_VALUE ²	BOOL	Valeur de lecture du canal de sortie relais : 1 : la sortie est fermée (alimentée) 0 : la sortie est ouverte (non alimentée)	L
IC	BOOL	1 : canal non valide détecté par le module. 0 : le canal est déclaré opérationnel en interne par le module.	L
CH_FBC	BOOL	Configuration du réglage de repli du canal : 1 : Valeur définie par l'utilisateur. 0 : Maintien dernière valeur	L

Elément	Type de données	Description	Accès
CH_FBST	BOOL	Configuration de l'état de repli du canal lorsque l'utilisateur défini est sélectionné : • 1 : Alimenté. • 0 : Non alimenté.	L
1. Lorsque la tâche SAFE n'est pas en mode d'exécution dans la CPU, les données échangées entre la CPU et le module ne sont pas mises à jour et CH_HEALTH a pour valeur 0. 2. L'élément TRUE_VALUE peut être horodaté par le BMX CRA ou le BME CRA.			

Alimentations de sécurité M580

Introduction

Ce chapitre décrit les modules d'alimentation de sécurité M580.

Alimentations de sécurité du M580

Introduction

Les alimentations suivantes peuvent être utilisées avec le contrôleur d'automatisation programmable (PAC) de sécurité M580 :

- BMXCPS4002S - alimentation de sécurité redondante 100 à 240 VCA
- BMXCPS4022S - alimentation de sécurité haute puissance redondante 24/48 VCC
- BMXCPS3522S - alimentation de sécurité haute puissance redondante 125 VCC

 **AVERTISSEMENT**

PERTE DE LA CAPACITE A EXECUTER LES FONCTIONS DE SECURITE

Utilisez uniquement un module d'alimentation BMXCPS4002S, BMXCPS4022S ou BMXCPS3522S dans une embase comprenant un module de sécurité M580.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Vérifiez à la fois votre installation physique et votre projet dans Control Expert pour confirmer que seuls des modules d'alimentation de sécurité M580 sont utilisés.

Fonctionnalité des alimentations

Chaque module d'alimentation de sécurité M580 convertit l'alimentation VCC ou VCA en deux tensions de sortie, 24 VCC et 3,3 VCC, comme indiqué ci-après :

Caractéristiques	Alimentation		
	BMXCPS4002S	BMXCPS4022S	BMXCPS3522S
Réseau d'alimentation d'entrée principal	100 à 240 VCA 50 à 60 Hz	24...48 VCC	100...150 VCC
Sortie d'alimentation limite vers l'embase	40 VCC	40 Vcc	40 Vcc

Caractéristiques	Alimentation		
	BMXCPS4002S	BMXCPS4022S	BMXCPS3522S
Température ambiante pour l'alimentation limite	-25° C...+60° C	-25° C...+60° C	-25° C...+60° C
Câblage vers	• Réseau CA avec neutre câblé à la terre OU • Réseau CA avec neutre isolé et impédant par rapport à la terre, neutre CA équipé d'un fusible par l'utilisateur.	Réseau CC 24 à 48 VCC	Réseau CC 125 VCC

Chaque alimentation détecte les conditions de surtension, de surcharge et de court-circuit sur les lignes d'embase 3,3 VCC et 24 VCC.

Si le seuil maximum de 40 VCC est détecté, le module réagit en effectuant les actions suivantes :

- Une réinitialisation qui relance les modules alimentés par le module d'alimentation.
- Si le seuil maximum de tension a été détecté :
 - sur la ligne d'embase 24 VCC : le contrôleur d'automatisation programmable (PAC) est mis hors tension.
 - sur la ligne d'embase 3,3 VCC : l'opération du contrôleur d'automatisation programmable (PAC) s'arrête, mais le contrôleur d'automatisation programmable (PAC) continue d'être alimenté.

Pour plus d'informations sur la manière de réagir à ces conditions, reportez-vous à la section *Diagnostics des tensions d'embase 24 VCC et 3,3 VCC*, page 139.

Modules d'alimentation redondante

Les modules BMXCPS4002S, BMXCPS4022S et BMXCPS3522S fournissent une alimentation redondante. Deux de ces modules d'alimentation peuvent être installés dans une embase Ethernet redondante : un en tant que module principal et l'autre en tant que module secondaire. Les configurations suivantes sont possibles :

Configuration	Caractéristiques		
	Gestion de la redondance (commande de l'alimentation et signaux des voyants LED)	Envoi des données à l'application	Surveillance et enregistrement des données d'alimentation
deux alimentations dans l'embase principale	✓	✓	✓
deux alimentations dans l'embase étendue	✓	X	✓
deux alimentations dans une embase existante	X	X	✓
✓ = Pris en charge. X = Non pris en charge.			

Pour plus d'informations sur les alimentations redondantes, consultez le document *Description des modules d'alimentation Modicon X80* (voir *Modicon X80, Embases et alimentations, Manuel de référence du matériel*).

Diagnostics des modules d'alimentation de sécurité du M580

Diagnostics du module d'alimentation

Les alimentations de sécurité BMXCPS4002S, BMXCPS4022S et BMXCPS3522S fournissent automatiquement la détection d'une condition de surtension, de surcharge ou de court-circuit susceptible de se produire, à la fois pour les tensions d'embase 24 VCC et 3,3 VCC.

Si l'alimentation détecte l'une de ces conditions sur la tension 24 VCC, les événements suivants ont lieu :

- La fonction de conversion de puissance est arrêtée pour l'ensemble de l'embase.
- Une commande RESET est émise pour tous les modules de l'embase.
- Le voyant LED d'alimentation **OK** s'éteint.
- L'ensemble du contrôleur d'automatisation programmable (PAC) est mis hors tension.

Si l'alimentation détecte l'une de ces conditions sur la tension 3,3 VCC, les événements suivants ont lieu :

- La fonction de conversion de puissance est arrêtée pour la tension d'embase 3,3 VCC.
- Une commande RESET est émise pour tous les modules de l'embase.
- Le voyant d'alimentation **OK** s'éteint.
- Le programme du contrôleur d'automatisation programmable (PAC) s'arrête en totalité, même si certains circuits PAC peuvent continuer de recevoir de l'alimentation.

Dans les deux cas, procédez de la manière suivante pour résoudre ces conditions :

1. Mettez hors tension la ligne d'alimentation principale.
2. Vérifiez la compatibilité entre la consommation d'énergie estimée du contrôleur d'automatisation programmable (PAC) par rapport à la capacité du module d'alimentation de sécurité sur les lignes d'embase 24 VCC et 3,3 VCC.
3. Éliminez la cause profonde de la condition détectée.
4. Attendez 1 minute après la mise hors tension.
5. Appliquez l'alimentation à la ligne principale pour redémarrer le module d'alimentation de sécurité .

Diagnostics du contact de relais d'alarme

Les alimentations de sécurité BMXCPS4002S, BMXCPS4022S et BMXCPS3522S présentent un contact de relais d'alarme à deux broches que vous pouvez utiliser pour obtenir les informations suivantes :

- Si le relais est activé (fermé) :
 - Les tensions d'embase 24 VCC et 3,3 VCC sont toutes les deux OK
 - RESET n'est pas actif
 - Si l'alimentation est placée dans l'embase locale principale :
 - Le contrôleur est opérationnel.
 - Le contrôleur est en mode RUN.
- Si le relais est désactivé (c'est-à-dire ouvert), l'un des événements suivants peut se produire :
 - L'une au moins des deux tensions d'embase 24 VCC et 3,3 VCC n'est pas OK
 - RESET est actif.
 - Si l'alimentation est placée dans l'embase locale principale :
 - Le contrôleur n'est pas opérationnel.
 - Le contrôleur est en mode STOP.

Type de données dérivé (DDT, Derived Data Type) M580

Introduction

Les modules d'alimentation de sécurité M580 présentent deux ensembles de types de données dérivé (DDT, Derived Data Type) :

- PWS_DIAG_DDT_V2 pour les diagnostics
- PWS_CMD_DDT pour les commandes

PWS_DIAG_DDT_V2

Décalage d'octet	Nom	Type	Commentaire
0	Réservé	BYTE	–
1	Réservé	BYTE	–
2	PwsMajorVersion	BYTE	Version majeure du micrologiciel d'alimentation
3	PwsMinorVersion	BYTE	Version mineure du micrologiciel d'alimentation
4	Model	BYTE	Identifiant de modèle Identifiant de modèle : • BMXCPS4002S = 01 • BMXCPS4022S = 02 • BMXCPS3522S = 03
5	State	BYTE	État de l'alimentation
6	I33BacPos	UINT	Mesure le courant sur la ligne d'embase 3,3 V dans le rôle nominal (producteur)
8	V33Buck	UINT	Mesure la tension 3,3 V abaissée
10	I24Bac	UINT	Mesure le courant sur la ligne d'embase 24 V
12	V24Int	UINT	Mesure la tension 24 V interne
14	Temperature	INT	Mesure la température ambiante
16	OperTimeMasterSincePO	UDINT	Temps de fonctionnement en tant que maître depuis la dernière mise sous tension
20	OperTimeSlaveSincePO	UDINT	Temps de fonctionnement en tant qu'esclave depuis la dernière mise sous tension

Décalage d'octet	Nom	Type	Commentaire
24	OperTimeMaster	UDINT	Temps de fonctionnement en tant que maître depuis la fabrication
28	OperTimeSlave	UDINT	Temps de fonctionnement en tant qu'esclave depuis la fabrication
32	Work	UDINT	Travail fourni depuis la fabrication
36	RemainingLTPC	UINT	Durée de vie restante en pourcentage
38	NbPowerOn	UINT	Nombre de mises sous tension depuis la fabrication
40	NbVoltageLowFail	UINT	Nombre d'erreurs détectées par le seuil inférieur de la tension principale
42	NbVoltageHighFail	UINT	Nombre d'erreurs détectées par le seuil supérieur de la tension principale
44	Réservé	UDINT	–
48	Réservé	UDINT	–
52	RemainingLTMO	UINT	Durée de vie restante en mois
54	Réservé	BYTE	–
63	Réservé	BYTE	–

PWS_CMD_DDT

Décalage d'octet	Nom	Type	Commentaire
0	Réservé	BYTE	–
1	Code	BYTE	Code de commande : 1 = permutation 3 = effacement
2	PwsTarget	BYTE	Cible alimentation : 1 pour gauche, 2 pour droite, 3 pour les deux Cible d'alimentation : 1 = gauche 2 = droite
3	Réservé	BYTE	–
15	Réservé	BYTE	–

Validation d'un système de sécurité M580

Introduction

Ce chapitre explique comment effectuer les calculs permettant de valider un système de sécurité M580.

Architectures de modules de sécurité M580

Introduction

Cette section présente les architectures internes des modules de sécurité.

Architecture de sécurité des CPU et du coprocesseur de sécurité M580

Introduction

Les CPU BME•58•040S et le coprocesseur BMEP58CPROS3, qui agissent comme une paire de processeurs, sont certifiés par TÜV Rheinland Group pour l'utilisation dans des solutions de sécurité M580 de niveau SIL3 (Safety Integrity Level).

Le CPU et le coprocesseur assurent conjointement les fonctions de sécurité de niveau SIL3 suivantes :

- Double exécution indépendante du code des tâches de sécurité.
- Comparaison des résultats de la double exécution du code.
- Autotests périodiques.
- Prise en charge d'une architecture a 1oo2D ("un sur deux") avec diagnostic.

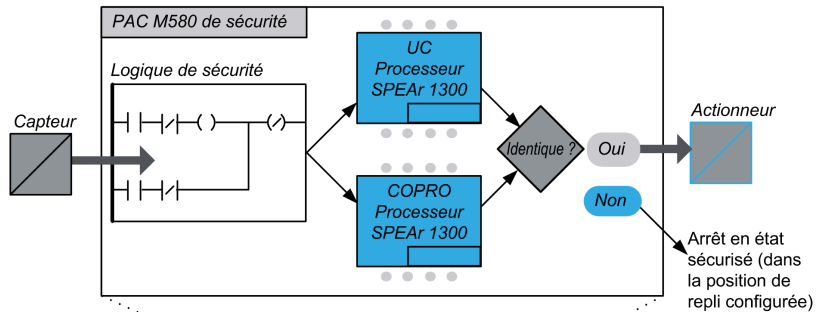
NOTE: Outre la fonctionnalité de sécurité, les CPU BMEP58•040S offrent des fonctionnalités comparables à celles des CPU M580 autonomes non liées à la sécurité équivalentes, et les CPU BMEH58•040S offrent des fonctionnalités comparables à celles des CPU M580 redondantes non liées à la sécurité équivalentes. Reportez-vous aux documents *Modicon M580 - Matériel*, *Manuel de référence* et *Modicon M580 - Redondance d"UC*, *Guide de planification du système pour architectures courantes* pour plus d'informations sur les fonctionnalités non liées à la sécurité de ces CPU de sécurité.

Description de l'architecture interne de la CPU et du coprocesseur

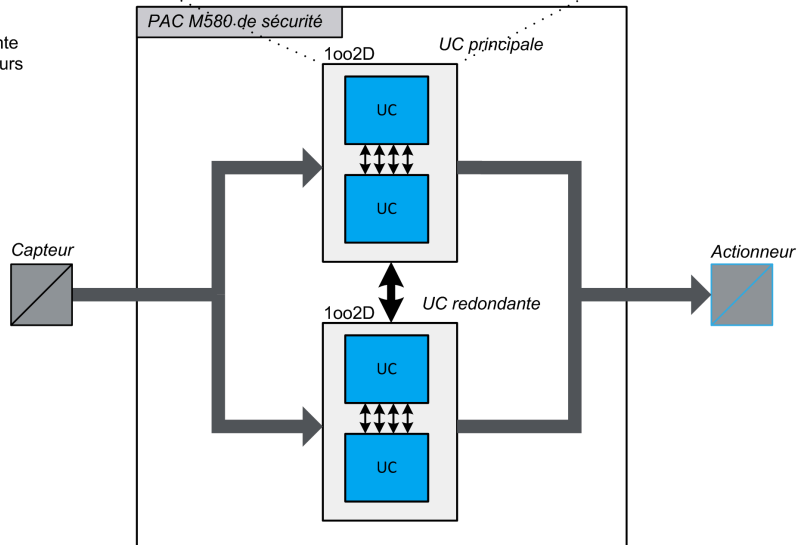
Le CPU et coprocesseur de sécurité M580 contiennent chacun un processeur SPEAr 1300. Chaque processeur exécute la logique de sécurité dans sa propre zone mémoire et compare les résultats de cette exécution à la fin de la tâche de sécurité.

Les figures suivantes illustrent l'architecture interne de la CPU M580 Safety dans des configurations simple et redondante :

Architecture simple
basée sur 2 processeurs



Architecture redondante
basée sur 4 processeurs



Génération et exécution de code en double

Les deux processeurs du contrôleur d'automatisation programmable (PAC) de sécurité M580 assurent la génération et l'exécution de code en double. Cette diversité offre les avantages suivants en matière de détection des erreurs :

- Deux programmes exécutables sont générés indépendamment. L'utilisation de deux compilateurs de code distincts favorise la détection des erreurs systémiques dans la génération du code.

- Les deux programmes générés sont exécutés par deux processeurs distincts. Ainsi, la CPU peut détecter à la fois les erreurs systématiques lors de l'exécution du code et les erreurs aléatoires du contrôleur d'automatisation programmable (PAC).
- Chacun des deux processeurs utilise sa propre zone de mémoire indépendante. Le contrôleur d'automatisation programmable (PAC) peut ainsi détecter les erreurs aléatoires de la RAM et il n'est pas nécessaire de tester entièrement la RAM à chaque scrutation.

Architecture 1oo2D

L'architecture 1oo2D ("un sur deux avec diagnostic") veut dire que deux canaux indépendants exécutent la logique de sécurité et que, si une erreur est détectée sur l'un ou l'autre canal, le système passe dans son état de sécurité défini.

Architecture simple

L'architecture de contrôleur d'automatisation programmable (PAC) M580 Safety simple repose sur un système 1oo2D constitué de processeurs doubles qui assurent le niveau de sécurité SIL3 même dans une architecture non redondante.

Architecture redondante

L'architecture de contrôleur d'automatisation programmable (PAC) M580 Safety redondante offre un maximum de disponibilité du système et de temps de traitement en apportant une redondance totale (quadruple structure, soit quatre CPU) du contrôle, de l'alimentation et de la communication.

Une des CPU (paire de processeurs) agit en tant que CPU principale et fait tourner l'application en exécutant la logique de programme et en contrôlant les E/S. La CPU (paire de processeurs) principale met à jour la CPU secondaire pour qu'elle soit prête à prendre le contrôle des E/S.

Le système se surveille lui-même continuellement. En cas d'erreur irrécupérable sur le contrôleur principal, le système bascule le contrôle vers le contrôleur secondaire. Dans ce mode dégradé, le système reste au niveau SIL3. Lorsque des erreurs irrécupérables se produisent sur le contrôleur principal et le contrôleur secondaire, le système passe à l'état sécurisé défini.

Le contrôleur d'automatisation programmable (PAC) M580 Safety redondant, grâce à son architecture quadruple (4 processeurs), permet d'augmenter la disponibilité du système et assure la conformité au niveau SIL3.

Horloge de surveillance

Un matériel et un micrologiciel de chien de garde vérifient l'activité du contrôleur d'automatisation programmable (PAC) et le temps requis pour exécuter la logique du programme de sécurité.

NOTE: Configurez le chien de garde logiciel (dans la boîte de dialogue **Propriétés** de la tâche SAFE) pour définir les aspects suivants :

- temps d'exécution de l'application
- filtrage des erreurs de communication des E/S
- délai de sécurité du processus.

Pour plus d'informations, reportez-vous à la section *Délai de sécurité du processus*, page 161.

Vérification de la mémoire

L'intégrité du contenu de la mémoire statique est testée via un contrôle de redondance cyclique (CRC) et via la double exécution de code. L'intégrité du contenu de la mémoire dynamique est testée par la double exécution de code, par un test de mémoire périodique et par un mécanisme de correction d'erreur (ECC) qui détecte et corrige les exemples les plus courants de corruption de données internes. Lors du démarrage à froid, ces tests sont réinitialisés et intégralement exécutés avant le passage de la CPU en mode STOP ou RUN.

Surveillance des surtensions

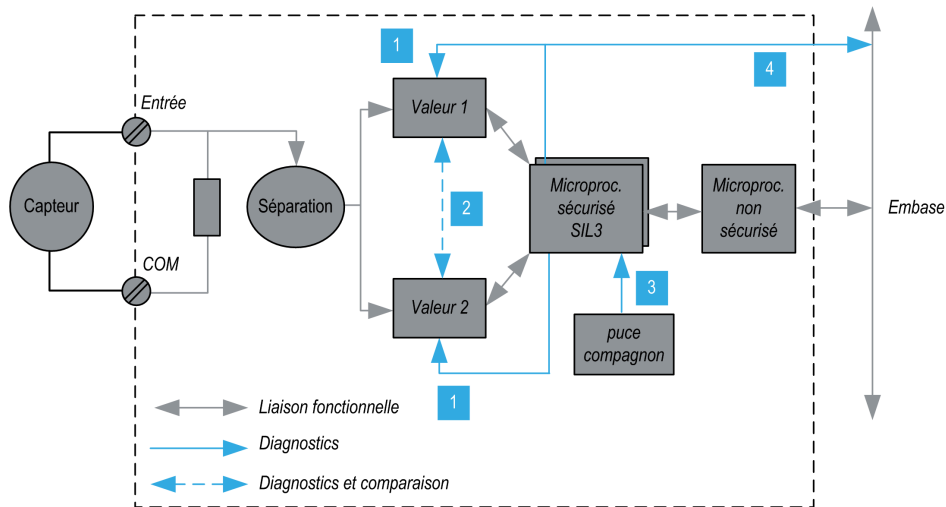
La CPU reçoit son alimentation du module de sécurité M580 dédié via l'embase. Ce module d'alimentation fournit une tension régulée de 24 V avec une tension maximum absolue comprise entre 0 et 36 V.

La CPU comprend une fonction intégrée qui vérifie les alimentations internes. Si une condition de tension insuffisante ou excessive est détectée, le contrôleur d'automatisation programmable (PAC) s'arrête.

Architecture de sécurité du module d'entrée analogique BMXSAI0410

Architecture de la fonction de sécurité

L'architecture interne du module BMXSAI0410 exécute sa fonction de sécurité de la manière suivante :



1 Les équipements de mesure sont surveillés régulièrement pour vérifier leur capacité à mesurer sans erreur détectée 10 valeurs analogiques entre 4 et 20 mA. La linéarité des phases de mesure est vérifiée en même temps.

2 Chaque valeur d'entrée est acquise par 2 circuits identiques. Les valeurs mesurées sont comparées par le processeur de sécurité. Si elles sont différentes, le canal concerné est jugé non valide. Un écart maximum de 0,35 % de la plage de pleine échelle 20 mA entre les deux valeurs est toléré.

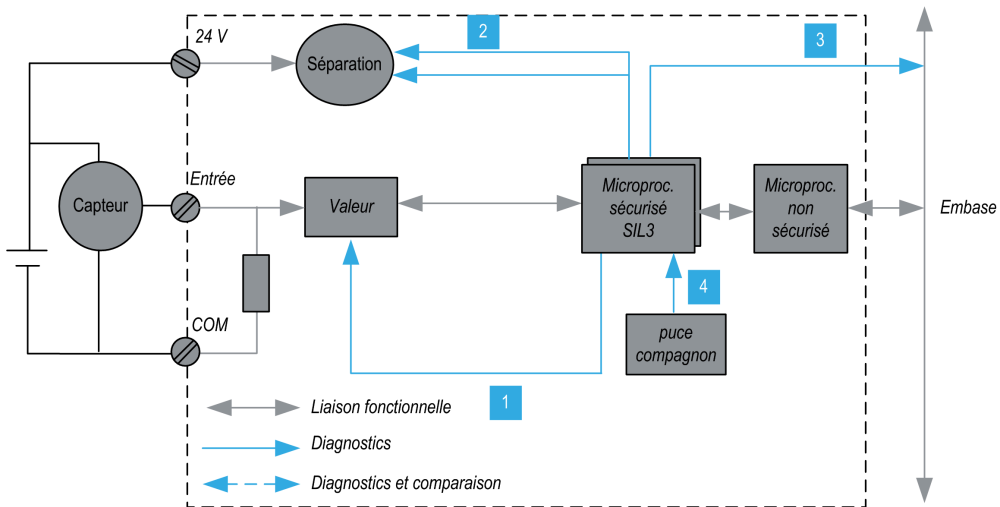
3 La puce compagnon alimente le processeur de sécurité, assure continuellement le diagnostic de celui-ci et surveille la tension de l'embase.

4 La tension en provenance de l'embase est surveillée pour détecter les conditions de tension excessive ou insuffisante.

Architecture de sécurité du module d'entrée numérique BMXSDI1602

Architecture de la fonction de sécurité

L'architecture interne du module BMXSDI1602 exécute la fonction de sécurité de la manière suivante :



1 Les équipements de mesure sont surveillés continuellement pour évaluer leur capacité à mesurer un "1" et un "0".

2 L'alimentation 24 VCC externe est surveillée continuellement par le processeur de sécurité. Chaque valeur d'entrée est acquise par deux circuits identiques. Les valeurs acquises sont comparées par le processeur de sécurité. Si elles sont différentes, le canal correspondant est déclaré non valide.

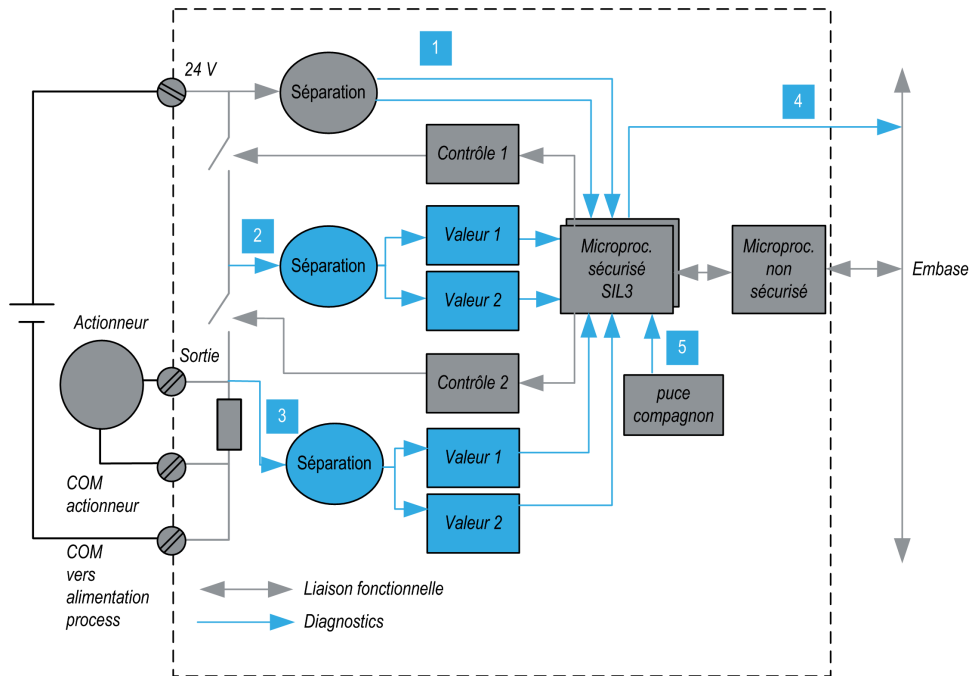
3 La tension en provenance de l'embase est surveillée pour détecter les conditions de tension excessive ou insuffisante.

4 La puce compagnon alimente le processeur de sécurité, assure continuellement le diagnostic de celui-ci et surveille la tension de l'embase.

Architecture de sécurité du module de sortie numérique BMXSDO0802

Architecture de la fonction de sécurité

L'architecture interne du module BMXSDO0802 exécute la fonction de sécurité de la manière suivante :



1 L'alimentation 24 VCC externe est surveillée continuellement par le processeur de sécurité.

2 Chaque sortie se compose de 2 commutateurs en série entre l'alimentation +24 VCC externe et la terre. La valeur de point médian (2) est lue de manière redondante et envoyée au processeur de sécurité. Les valeurs médianes mesurées sont comparées par le processeur de sécurité. Si ces valeurs ne sont pas celles escomptées, le canal est déclaré non valide.

3 La valeur de point bas (3) est également supervisée en vue d'effectuer un diagnostic de câblage externe.

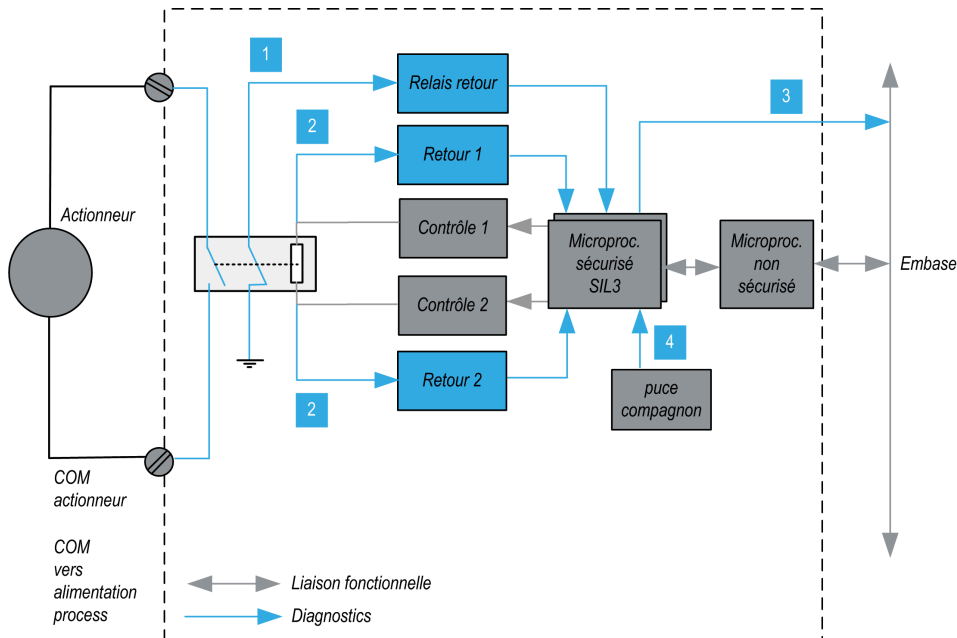
4 La tension en provenance de l'embase est surveillée pour détecter les conditions de tension excessive ou insuffisante.

5 La puce compagnon alimente le processeur de sécurité, assure continuellement le diagnostic de celui-ci et surveille la tension de l'embase.

Architecture de sécurité du module de sortie relais numérique BMXSRA0405

Architecture de la fonction de sécurité

L'architecture interne du module BMXSRA0405 exécute la fonction de sécurité de la manière suivante :



1 L'état du relais est surveillé continuellement par le processeur de sécurité, lequel lit l'état d'un contact normalement fermé lié mécaniquement au contact normalement ouvert et se relie à son tour à l'actionneur.

2 L'état de la commande de relais est surveillé continuellement. Chaque valeur d'entrée est reçue par 2 circuits identiques. Les valeurs mesurées sont comparées par le processeur de sécurité. Si elles sont différentes, le canal correspondant est déclaré non valide.

3 La tension en provenance de l'embase est surveillée pour détecter les conditions de tension excessive ou insuffisante.

4 La puce compagne alimente le processeur de sécurité, assure continuellement le diagnostic de celui-ci et surveille la tension de l'embase.

Valeurs SIL et MTTR des modules de sécurité M580

Introduction

Cette section présente les valeurs SIL et MTTF que vous pouvez utiliser dans les calculs de vos modules de sécurité M580.

Calculs du niveau d'intégrité de la sécurité (SIL)

Classification des produits Schneider Electric

Le contrôleur d'automatisation programmable (PAC) de sécurité M580 peut se composer des éléments suivants :

- Modules de sécurité pouvant assurer des fonctions de sécurité, à savoir :
 - CPU et coprocesseur
 - Modules d'E/S
 - alimentation
- Modules non perturbateurs, page 34 n'assurant aucune fonction de sécurité mais permettant d'ajouter des éléments hors sécurité au projet de sécurité.

NOTE:

- Les modules non perturbateurs ne faisant pas partie de la boucle de sécurité, ils n'entrent pas en compte dans les calculs du niveau d'intégrité de la sécurité.
- Une erreur détectée dans un module non interférent n'a pas d'impact négatif sur l'exécution des fonctions de sécurité.
- Les alimentations BMXCPS4002S, BMXCPS4022S et BMXCPS3522S sont certifiées. Comme elles présentent un taux de défaillance dangereuse négligeable (moins de 1 % de la cible SIL3), l'alimentation n'est pas incluse dans les calculs du niveau d'intégrité de la sécurité effectués pour la boucle de sécurité. Par conséquent, aucune valeur PFH ou PFD n'est fournie pour les modules d'alimentation.

Valeurs PFD/PFH des modules de sécurité M580

Schneider Electric propose les modules de sécurité suivants certifiés pour une utilisation dans des applications de sécurité. Ces modules de sécurité sont répertoriés avec leurs

probabilités de défaillance, page 157 (PFD/PFH) respectives pour différents intervalles de test périodique, page 160 (PTI). Les probabilités PFD/PFH sont exprimées en tant que valeurs contribuant aux probabilités PFD/PFH globales de l'ensemble de la boucle de sécurité, page 22.

Les tableaux ci-après répertorient les modules de sécurité et leurs valeurs PFD/PFH pour les applications SIL2 et SIL3 (le cas échéant) :

Type de produit	Référence du produit	SIL	PTI = 1 an	
			PFD _G	PFH _G
CPU avec coprocesseur avec coprocesseur	BME•58•040S & BMEP58CPROS3	SIL3 ¹	4.41E-07	1.01E-10
Entrée analogique	BMXSAI0410	SIL3 ²	5.76E-06	1.31E-09
Entrée numérique	BMXSDI1602	SIL3 ²	6.81E-06	1.56E-09
Sortie numérique	BMXSDO0802	SIL3 ¹	5.75E-06	1.31E-09
Sortie relais numérique	BMXSRA0405	SIL2 ³	5.85E-06	1.68E-09
		SIL3 ⁴	5.84E-06	1.34E-09
		SIL3 ⁵	–	1.35E-09
Alimentation	BMXCPS4002S, BMXCPS4022S et BMXCPS3522S	SIL3	–	–
1. 1 sortie à 80 °C 2. 1 entrée à 80 °C 3. 1 relais par sortie à 80 °C 4. 2 relais par sortie à 80 °C 5. 4 relais par sortie à 80 °C				

Type de produit	Référence du produit	SIL	PTI = 5 ans	
			PFD _G	PFH _G
CPU & coprocesseur	BME•58•040S & BMEP58CPROS3	SIL3 ¹	2.22E-06	1.02E-10
Entrée analogique	BMXSAI0410	SIL3 ²	2.88E-05	1.31E-09
Entrée numérique	BMXSDI1602	SIL3 ²	3.41E-05	1.56E-09
Sortie numérique	BMXSDO0802	SIL3 ¹	2.88E-05	1.31E-09
Sortie relais numérique	BMXSRA0405	SIL2 ³	2.92E-05	1.68E-09
		SIL3 ⁴	2.92E-05	1.34E-09
		SIL3 ⁵	–	1.35E-09

Type de produit	Référence du produit	SIL	PTI = 5 ans	
			PFD _G	PFH _G
Alimentation	BMXCPS4002S, BMXCPS4022S et BMXCPS3522S	SIL3	–	–
1. 1 sortie à 80 °C 2. 1 entrée à 80 °C 3. 1 relais par sortie à 80 °C 4. 2 relais par sortie à 80 °C 5. 4 relais par sortie à 80 °C				

Type de produit	Référence du produit	SIL	PTI = 10 ans	
			PFD _G	PFH _G
CPU & coprocesseur	BME•58•040S & BMEP58CPROS3	SIL3 ¹	4.47E-06	1.03E-10
Entrée analogique	BMXSAI0410	SIL3 ²	5.76E-05	1.31E-09
Entrée numérique	BMXSDI1602	SIL3 ²	6.81E-05	1.56E-09
Sortie numérique	BMXSDO0802	SIL3 ¹	5.75E-05	1.31E-09
Sortie relais numérique	BMXSRA0405	SIL2 ³	5.84E-05	1.68E-09
		SIL3 ⁴	5.84E-05	1.34E-09
		SIL3 ⁵	–	1.35E-09
Alimentation	BMXCPS4002S, BMXCPS4022S et BMXCPS3522S	SIL3	–	–
1. 1 sortie à 80 °C 2. 1 entrée à 80 °C 3. 1 relais par sortie à 80 °C 4. 2 relais par sortie à 80 °C 5. 4 relais par sortie à 80 °C				

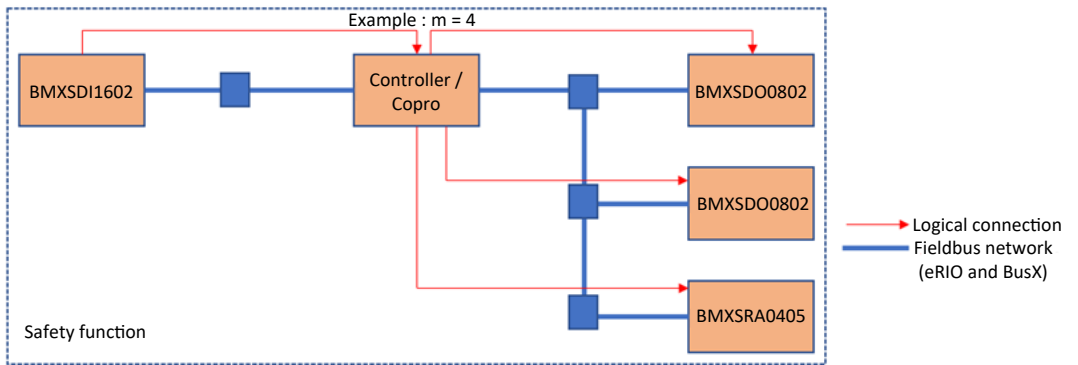
Type de produit	Référence du produit	SIL	PTI = 20 ans	
			PFD _G	PFH _G
CPU & coprocesseur	BME•58•040S & BMEP58CPROS3	SIL3 ¹	9.06E-06	1.05E-10
Entrée analogique	BMXSAI0410	SIL3 ²	1.15E-04	1.31E-09
Entrée numérique	BMXSDI1602	SIL3 ²	1.36E-04	1.56E-09

Type de produit	Référence du produit	SIL	PTI = 20 ans	
			PFD _G	PFH _G
Sortie numérique	BMXSDO0802	SIL3 ¹	1.15E-04	1.31E-09
Sortie relais numérique	BMXSRA0405	SIL2 ³	1.17E-04	1.68E-09
		SIL3 ⁴	1.17E-04	1.34E-09
		SIL3 ⁵	–	1.35E-09
Alimentation	BMXCPS4002S, BMXCPS4022S et BMXCPS3522S	SIL3	–	–
1. 1 sortie à 80 °C 2. 1 entrée à 80 °C 3. 1 relais par sortie à 80 °C 4. 2 relais par sortie à 80 °C 5. 4 relais par sortie à 80 °C				

Valeurs PFH pour la communication de sécurité entre le contrôleur et les modules d'E/S de sécurité Mx80

Pour les applications à forte demande, vous devez tenir compte de l'erreur résiduelle liée à la communication de sécurité (canal noir) entre le contrôleur et les modules d'E/S de sécurité BMX. Pour chaque communication logique entre le contrôleur et un module d'E/S de sécurité BMX impliqué dans la fonction de sécurité, un taux d'erreur résiduel de 1.5E-10 doit être compté dans le calcul du PFH.

Si « m » est le nombre de modules d'E/S de sécurité (SDI, SDO, SAI ou SRA) utilisés dans la fonction de sécurité, le PFH lié aux communications de sécurité égal à « m * 1,5E-10 » doit être ajouté à la valeur PFH globale :



Probabilités de défaillance pour les applications SIL3

Pour les applications SIL3, la norme IEC 61508 définit les probabilités de défaillance sur demande (PFD) et les probabilités de défaillance par heure (PFH) suivantes pour chaque boucle de sécurité, en fonction du mode de fonctionnement :

- $PFD \geq 10^{-4}$ à $< 10^{-3}$ pour une faible demande
- $PFH \geq 10^{-8}$ à $< 10^{-7}$ pour une forte demande

Le contrôleur d'automatisation programmable (PAC) de sécurité M580 est certifié pour une utilisation dans les systèmes à faible et forte demande.

Exemple de calcul du niveau d'intégrité de la sécurité (SIL)

Cet exemple explique comment déterminer :

- la contribution de risque présentée par les modules de sécurité Schneider Electric dans votre application de sécurité.
- Pour les applications à forte demande, la contribution des communications de sécurité entre le contrôleur et les modules E/S de sécurité Mx80.
- la quantité restante de risque due à d'autres appareils de la boucle de sécurité (capteurs et actionneurs, par exemple) pour un niveau SIL et un mode de fonctionnement donnés

NOTE: Pour le calcul de la contribution de risque des capteurs et des actionneurs dans votre application de sécurité, demandez aux constructeurs de ces appareils les valeurs de PFD/PFH correspondant à l'intervalle de test périodique (PTI) approprié.

Cet exemple inclut les modules de sécurité Schneider Electric suivants :

- 1 : BMEP584040S CPU
- 1 : BMEP58CPROS3 Coprocesseur
- 1 : BMXSAI0410 Entrée analogique
- 1 : BMXSDO0802 Sortie numérique
- 1 : BMXCPS4002S Alimentation

Le calcul suivant utilise les valeurs de PFH_G correspondant à un mode de fonctionnement à forte demande pour une boucle de sécurité SIL3 avec un intervalle de test périodique (PTI) de 20 ans. La valeur de PFH maximum admissible pour cette application de sécurité est 10^{-7} (ou $1.0E-7$) :

Modules de sécurité	Contribution (notation scientifique)	Contribution résiduelle des capteurs et actionneurs
CPU avec coprocesseur	7.01E-10	—
Entrée analogique	1.31E-09	

Modules de sécurité		Contribution (notation scientifique)	Contribution résiduelle des capteurs et actionneurs
Sortie numérique		1.31E-09	
Alimentation		–	
Communications d'E/S de sécurité (m=2)		2 * 1.5E-10	
Total	numérique	3.62E-09	96.38E-09
	% max	3,62 %	96,38 %
remarque n°1 : La sortie de relais utilise quatre relais pour prendre en charge une sortie.			

Valeurs pour les modules de sécurité M580 destinés aux machines industrielles

Schneider Electric propose les modules de sécurité certifiés suivants pour une utilisation dans des applications de sécurité de machines industrielles, conformément à la norme ISO13849-1. Le tableau suivant répertorie les modules de sécurité ainsi que leurs valeurs, catégorie et niveau (selon le cas) :

Type de produit	Référence du produit	Configuration	Catégorie	Niveau de performance	MTTFd (années)	DCav
CPU avec coprocesseur	BME•58•040S & BMEP58CPROS3	NA	4	e	235	Élevé (> 99 %)
Entrée analogique	BMXSAI0410	avec 1 canal	2	d	255	99,66 %
		avec 2 canaux	4	e	255	99,66 %
Entrée numérique	BMXSDI1602	avec 1 canal	2	d	231	99,69 %
		avec 2 canaux	4	e	231	99,69 %
Sortie numérique	BMXSDO0802	NA	4	e	253	99,63 %
Sortie relais numérique	BMXSRA0405	avec 1 canal	2	c	156	99,77 %
		avec 2 canaux	4	e	156	99,77 %

Valeurs des modules de sécurité M580 pour les chemins de fer

Schneider Electric propose les modules de sécurité suivants certifiés pour le secteur ferroviaire conformément aux normes Cenelec EN50126, EN50128, EN50129. Le tableau ci-dessous répertorie les modules de sécurité et leurs valeurs de fiabilité :

Type de produit	Référence du produit	SIL	TFFR (PTI = 20 ans)
CPU & coprocesseur	BME•58•040S & BMEP58CPROS3	SIL4	1.04E-10
Entrée analogique	BMXSAI0410	SIL4	1.31E-09
Entrée numérique	BMXS DI1602	SIL4	1.56E-09
Sortie numérique	BMXS DO0802	SIL4	1.31E-09
Sortie relais numérique	BMXSRA0405	SIL3 ¹	1.68E-09
		SIL4 ²	1.34E-09
		SIL4 ³	1.35E-09
Alimentation	BMXCPS4002S, BMXCPS4022S et BMXCPS3522S	SIL4	–
NOTE: Les valeurs SIL sont à 80 °C			
1. 1 relais par sortie à 80 °C			
2. 2 relais par sortie à 80 °C			
3. 4 relais par sortie à 80 °C			

La somme du TFFR d'un module d'entrée, de la CPU et du coprocesseur, de l'alimentation et d'un module de sortie est toujours inférieure à 3,5E-09/h, ce qui est inférieur au budget alloué maximal de 40 % ciblé comme taux de défaillance résiduelle maximum pour une fonction de sécurité SIL4 permettant d'intégrer d'autres produits dans la boucle de sécurité.

TFFR par heure et fonction	Attribut SIL
$10^{-9} \leq \text{TFFR} \leq 10^{-8}$	4
$10^{-8} \leq \text{TFFR} \leq 10^{-7}$	3
$10^{-7} \leq \text{TFFR} \leq 10^{-6}$	2
$10^{-60} \leq \text{TFFR} \leq 10^{-5}$	1

Description des temps de sécurité

Le contrôleur d'automatisation programmable (PAC) de sécurité M580 présente un temps de cycle PAC minimum de 10 ms, ce qui est nécessaire pour traiter les signaux des modules

d'E/S, exécuter la logique de programme et définir les sorties. Pour calculer le temps de réaction maximum du contrôleur d'automatisation programmable (PAC), vous devez connaître le temps de réaction maximum des capteurs et des actionneurs en cours d'utilisation. De plus, le temps de réaction maximum du contrôleur d'automatisation programmable (PAC) dépend du temps de sécurité (PST), page 161 requis par votre processus.

Intervalle entre tests périodiques

Le test de la preuve est un test périodique que vous devez effectuer pour détecter les erreurs dans un système lié à la sécurité, de sorte que, si nécessaire, le système puisse être restauré dans une nouvelle condition ou aussi proche que possible de cette condition. La périodicité de ces tests est défini par l'intervalle PTL.

L'intervalle entre tests périodiques dépend du niveau d'intégrité de la sécurité ciblé, des capteurs, des actionneurs et de l'application de contrôleur. Le système de sécurité M580 est adapté à une utilisation dans une application SIL3 selon la norme CEI 61508 et à un intervalle de test périodique de 20 ans.

NOTE: Un test de périodique peut être effectué et considéré comme réussi si le contrôleur fonctionne correctement après le redémarrage (OFF puis ON) de la configuration de sécurité complète comprenant la CPU et les E/S. Dans ce cas, il n'est pas nécessaire de régénérer l'application.

Calculs de performance et de chronologie d'un système de sécurité M580

Introduction

Cette section explique comment calculer le temps de réaction du PAC, le temps de réaction du système et les délais de sécurité de processus pour un système de sécurité M580.

Délai de sécurité du processus

Description du délai de sécurité de processus

Le délai de sécurité de processus (PST) est une mesure importante pour un processus exécuté par une boucle de sécurité. Il est défini comme étant la période entre l'occurrence d'une erreur sur un équipement sous contrôle (EUC) et l'occurrence d'un événement dangereux si la fonction de sécurité n'est pas exécutée (autrement dit, si l'état de sécurité défini n'est pas appliqué).

NOTE: Le délai de sécurité de processus (PST) est déterminé par le processus de sécurité spécifique. Vous devez vérifier que votre système de sécurité peut assurer ses fonctions de sécurité dans le délai de sécurité du processus.

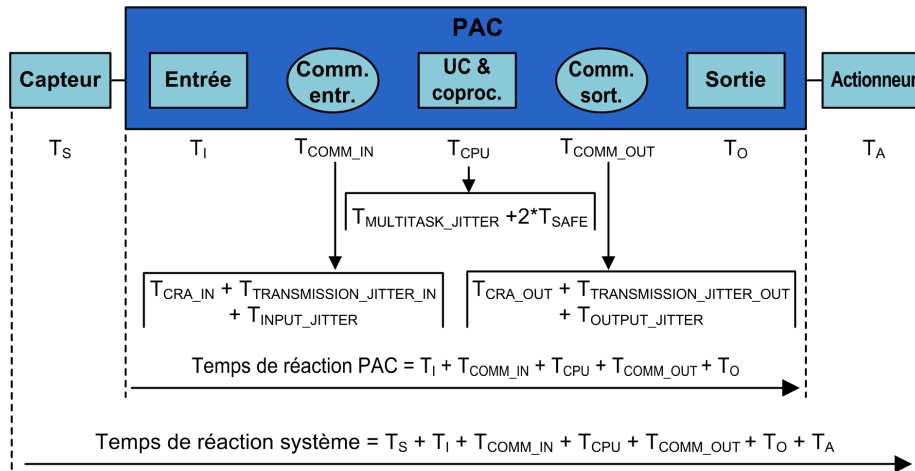
Description du temps de réaction du système

Le temps de réaction du système est la somme du temps de réaction du contrôleur d'automatisation programmable (PAC) et des temps de réaction du capteur sélectionné (T_S) et de l'actionneur sélectionné (T_A).

NOTE: T_S et T_A sont spécifiques à l'équipement.

Pour chaque boucle de sécurité, vérifiez que le temps de réaction du système est inférieur au délai de sécurité du processus.

Le temps de réaction du système est illustré ci-après :



Le temps de réaction du système peut inclure les composants suivants :

Composant	Description	Valeur estimée du pire cas
T_S	Temps nécessaire au capteur sélectionné pour réagir à un événement de processus.	Spécifique à l'équipement.
T_I	Temps nécessaire au module d'entrée pour échantillonner et vérifier un événement de capteur. Il comprend : - une période d'échantillonnage de module d'entrée ; - plusieurs périodes d'échantillonnage de module d'entrée pour le filtrage.	6 ms
T_{COMM_IN}	Délai de communication d'entrée. Ses composants sont décrits dans la rubrique <i>Temps de réponse de l'application</i> dans le document <i>Modicon M580 Autonome - Guide de planification du système pour architectures courantes</i> , et sont les suivants (numéros correspondant au calcul de l'ART dans la rubrique référencée) : T_{CRA_IN} : CRA_Drop_Process (2) + RPI Entrée CRA (3) T_{JITTER_IN} : Network_In_Time (4) + Network_In_Jitter (5) + CPU_In_Jitter (6)	—
T_{CPU}	Le temps de réaction de la CPU et du coprocesseur, qui est égal à la somme du retard dû à des tâches prioritaires en attente (la tâche FAST) plus deux temps de scrutation de la tâche SAFE (dont le premier est une scrutation manquée et le second, une scrutation réussie) : $T_{MULTITASK_JITTER} + 2 \cdot T_{SAFE}$.	
$T_{MULTITASK_JITTER}$	Retard maximum dû à l'exécution des tâches prioritaires en attente. En l'occurrence, la tâche FAST.	—

Composant	Description	Valeur estimée du pire cas
	$T_{MULTITASK_JITTER} = T_{FAST}$.	
T_{SAFE}	Période de la tâche SAFE configurée.	—
T_{FAST}	Cette valeur est incluse car l'exécution de la tâche FAST est prioritaire sur la tâche SAFE. NOTE: Pour simplifier la formule, l'hypothèse est qu'aucune tâche système n'est en condition de dépassement (overrun). Cette valeur est donc égale à la période de la tâche FAST configurée ou à 0 si la tâche FAST n'est pas configurée.	—
T_{COMM_OUT}	Délai de communication des sorties. Ses composants sont décrits dans la rubrique <i>Temps de réponse de l'application</i> dans le document <i>Modicon M580 Autonome - Guide de planification du système pour architectures courantes</i> , et sont les suivants (numéros correspondant au calcul de l'ART dans la rubrique référencée) : • T_{CRA_OUT} : CRA_Drop_Process (12) • T_{JITTER_IN} : CPU_Out_Jitter (9) + Network_Out_Time (10) + Network_Out_Jitter (11)	—
T_O	Égal à la somme des temps suivants : • Délai entre la lecture et l'application de la valeur de sortie de la CPU (0 à 3 ms). • Temps nécessaire au module de sortie de sécurité pour modifier la sortie physique, c'est-à-dire pour propager la modification de la RAM X à la sortie physique (entre 0 et 3 ms).	6 ms
T_A	Temps de réaction de l'actionneur sélectionné.	Spécifique à l'équipement.

Description du temps de réaction du contrôleur d'automatisation programmable (PAC)

Pour les E/S situées dans le rack principal local (avec la CPU), le temps de réaction du contrôleur d'automatisation programmable (PAC) est la somme des temps de réaction du module d'entrée sélectionné (T_I) et du module de sortie sélectionné (T_O), augmentée du temps de réaction de la CPU et du coprocesseur (T_{CPU}) :

Temps de réaction du contrôleur d'automatisation programmable (PAC) (local) = $T_{CPU} + T_I + T_O$

Si les E/S sont situées dans un rack distant, le temps de réaction du contrôleur d'automatisation programmable (PAC) inclut également le délai de communication d'entrée (T_{COMM_IN}) et le délai de communication de sortie (T_{COMM_OUT}) : (T_{COMM_OUT}) :

PAC reaction time (remote) = $T_{\text{CPU}} + T_{\text{COMM_IN}} + T_{\text{I}} + T_{\text{COMM_OUT}} + T_{\text{O}}$

Description du temps de réaction de la CPU et du coprocesseur

Le temps de réaction de la CPU et du coprocesseur est directement affecté par la période de la tâche SAFE et la période de la tâche FAST. Vérifiez que la logique de sécurité sera exécutée dans la période de la tâche SAFE.

Dans la mesure où un signal peut apparaître juste au début du cycle d'exécution alors que les signaux ont déjà été traités, deux cycles de la tâche SAFE sont parfois nécessaires pour réagir au signal.

La tâche FAST étant prioritaire sur la tâche SAFE, vous devez aussi tenir compte du temps nécessaire pour exécuter la tâche FAST dans votre estimation de la jigue.

D'où l'équation suivante pour le temps de réaction maximum (pire cas) :

Temps de réaction CPU & coproc. = $2 \times T_{\text{SAFE}} + T_{\text{FAST}}$

NOTE: Si vous utilisez la communication sécurisée d'égal à égal, page 192 pour exécuter la fonction de sécurité, l'estimation du temps de réaction de la CPU est différente.

Description du temps nécessaire aux modules d'entrée

Le temps maximum (pire cas) nécessaire au module d'entrée numérique de sécurité et au module d'entrée analogique de sécurité T_{I} est de 6 ms.

Description du temps nécessaire aux modules de sortie

Le temps maximum T_{O} nécessaire au module de sortie numérique de sécurité est estimé à 6 ms.

Un timeout de sécurité de repli S_TO doit être configuré pour le module de sorties numériques, page 114 et le module de sorties relais numériques, page 131. Selon la période de tâche SAFE configurée (T_{SAFE}), la valeur de S_TO doit être configurée comme suit :

- Si $(2,5 \times T_{\text{SAFE}}) \leq 40$ ms, réglez S_TO sur une valeur minimum de 40 ms.
- Si $(2,5 \times T_{\text{SAFE}}) > 40$ ms, réglez S_TO sur une valeur minimum de $(2,5 \times T_{\text{SAFE}})$ ms.

AVIS

DÉTÉRIORATION DE L'ÉQUIPEMENT

Réglez le timeout de sécurité de repli (S_TO) pour un module de sorties de sécurité sur une valeur au moins supérieure à 40 ms ou $(2.5 * T_{SAFE})$, où T_{SAFE} est égal à la période de la tâche SAFE configurée.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Pour les applications redondantes, considérez l'impact sur le paramètre S_TO du temps supplémentaire (T_{SWAP}) requis par une permutation, page 166, et du temps supplémentaire T_{SWITCH} requis par un basculement, page 167.

Calcul du temps de réaction du système

Connaissant le délai de sécurité du processus (PST) et le temps de réaction maximum des capteurs et actionneurs, vous pouvez calculer le temps de réaction du système (SRT) maximum tolérable dans votre processus.

Le temps de réaction maximum (pire cas) du système peut être calculé comme suit :

Pour les systèmes dont les E/S se trouvent dans des stations distantes :

$$SRT \text{ max.} = T_S + T_I + 2 \times T_{CRA} + T_{RPI} + 2 \times T_{SAFE} + T_{FAST} + T_O + T_A.$$

ou

$$SRT \text{ max.} = 16 \text{ ms} + T_S + 2,5 \times T_{SAFE} + T_{FAST} + T_A.$$

Pour les systèmes à E/S locales :

$$SRT \text{ max.} = T_S + T_I + 2,5 \times T_{SAFE} + T_{FAST} + T_O + T_A.$$

ou

$$SRT \text{ max.} = 15 \text{ ms} + T_S + 2,5 \times T_{SAFE} + T_{FAST} + T_A.$$

NOTE: Pour les contrôleurs d'automatisation programmables (PAC) redondants, les composants supplémentaires aux calculs ci-dessus sont à prendre en compte pour calculer le temps de réaction de sécurité maximum :

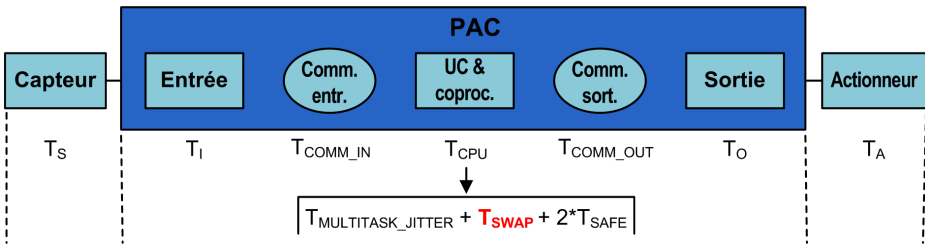
- En cas de basculement, le temps de réaction de sécurité maximum peut augmenter en ajoutant le composant , page 167 T_{SWITCH} aux calculs ci-dessus.
- Lorsque l'opérateur du système effectue une permutation, le temps de réaction de sécurité maximum peut augmenter en ajoutant un composant , page 166 T_{SWAP} aux calculs ci-dessus.

Temps de réaction du système pendant une permutation

Une permutation désigne l'action déclenchée par l'opérateur sur un système redondant et qui échange les rôles des contrôleurs principal et redondant. Une permutation consomme du temps supplémentaire, car aucune information ne peut être perdue et toutes les sorties du système doivent se voir appliquer un timeout de sécurité.

Le temps de permutation supplémentaire est ajouté au temps T_{CPU} après le composant T_{JITTER} normal, comme ci-dessous :

Le temps T_{SWAP} est ajouté au temps T_{CPU} après le composant T_{JITTER} normal. Cette séquence est affichée ci-dessous. Sauf en cas d'inclusion du composant de permutation, le temps de réaction du système est identique à celui décrit ci-dessus, page 161 :



Le temps T_{SWAP} est la somme des éléments suivants :

$$T_{ADDITIONAL_JITTER} + T_{TRANSFER}$$

Les composants propres à la permutation sont décrits ci-après :

Composant	Description	Valeur estimée du pire cas
$T_{ADDITIONAL_JITTER}$	Jigle introduite par le système multitâche pour redémarrer la tâche sur le nouveau contrôleur d'automatisation programmable (PAC). D'où, $T_{ADDITIONAL_JITTER} = T_{SAFE}$.	—
$T_{TRANSFER}$	Pendant le diagnostic de la tâche MAST, le contrôleur d'automatisation programmable (PAC) accepte la commande de permutation et débute le transfert de toutes les dernières données de chaque tâche.	Reportez-vous à la formule ci-dessous.

$T_{TRANSFER}$ peut se calculer comme suit :

$$K3 \times (MAST_{KB} + 2 \times SAFE_{KB} + FAST_{KB}) + K4 \times (MAST_{DFB} + 2 \times SAFE_{DFB} + FAST_{DFB}) / 1000$$

Où :

- $TASK_{KB}$ = Taille des données (en Ko) échangées pour la tâche entre le contrôleur d'automatisation programmable (PAC) principal et le contrôleur d'automatisation programmable (PAC) redondant.
- $MAST_{DFB}$ = Nombre de DFB (blocs dérivés) déclarés dans la tâche TASK.

- K3 et K4 sont des constantes, dont les valeurs sont déterminées par le module CPU spécifique utilisé dans l'application, comme suit :

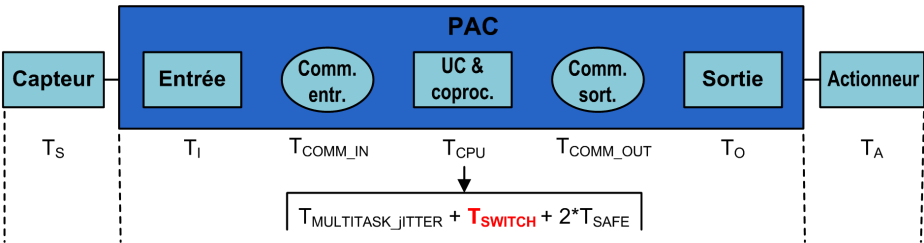
Coefficient	BMEH582040S	BMEH584040S ou BMEH586040S
K3	46,4 µs/ko	14,8 µs/ko
K4	34,5 µs/instance de DFB	11,0 µs/instance de DFB

Si l'opérateur du système souhaite effectuer une permutation sans que les sorties du module de sécurité ne prennent leur état de repli, réglez le paramètre Timeout de sécurité de repli des modules de sortie de sécurité (S_TO) sur, au minimum, une valeur supérieure à : $T_{MULTITASK_JITTER} + T_{SWAP} + T_{SAFE}$.

Temps de réaction du système pendant un basculement

Un basculement survient lorsque le contrôleur redondant d'un système redondant devient le contrôleur principal, par exemple lorsque le matériel du contrôleur principal devient subitement inopérant. L'objectif du basculement pour le nouveau contrôleur d'automatisation programmable (PAC) principal est de remplacer l'ancien de manière transparente, puis de lancer les opérations au point où l'ancien contrôleur d'automatisation programmable (PAC) principal a cessé de fonctionner. Pourtant, le dernier cycle peut être réexécuté. L'objectif du système est d'atteindre la reprise le plus rapidement possible.

Le temps T_{SWITCH} est ajouté au temps T_{CPU} après le composant T_{JITTER} normal. Cette séquence est affichée ci-dessous. Sauf en cas d'inclusion du composant de basculement, le temps de réaction du système est identique à celui décrit ci-dessus, page 161 :



Le temps T_{SWITCH} est la somme des éléments suivants :

$$T_{DETECT} + T_{ADDITIONAL_JITTER}$$

Les composants propres au basculement sont décrits ci-après :

Composant	Description	Valeur estimée du pire cas
T_{DETECT}	Temps utilisés par le contrôleur d'automatisation programmable (PAC) redondant pour détecter et vérifier que le contrôleur d'automatisation programmable (PAC) principal est devenu inopérant.	15 ms
$T_{\text{ADDITIONAL_JITTER}}$	Jigue introduite par le système multitâche pour redémarrer la tâche sur le nouveau contrôleur d'automatisation programmable (PAC). D'où, $T_{\text{ADDITIONAL_JITTER}} = T_{\text{SAFE}}$.	–

Contrairement à une permutation, aucun temps supplémentaire n'est nécessaire pour effectuer un transfert de données.

Pour autoriser le système à répondre à une erreur détectée et effectuer un basculement sans que les sorties du module de sécurité ne prennent leur état de repli, réglez le paramètre Timeout de sécurité de repli des modules de sortie de sécurité (S_TO) sur, au minimum, une valeur supérieure à : $T_{\text{JITTER}} + T_{\text{SWITCH}} + T_{\text{SAFE}}$.

Configuration des périodes maximum des tâches SAFE et FAST de la CPU

Le contrôleur d'automatisation programmable (PAC) de sécurité M580 ne peut effectuer qu'une exécution périodique des tâches SAFE et TAST (l'exécution cyclique n'est pas prise en charge pour ces tâches).

La **Période** de la tâche SAFE et le **Chien de garde** maximum de la CPU sont configurés dans l'onglet **Général** de la boîte de dialogue **Propriétés de la tâche SAFE**. La valeur **Timeout de repli** des modules de sortie numérique de sécurité est configurée dans l'onglet **Configuration** du module de sortie, page 108.

De la même manière, la **Période** de la tâche FAST et le **Chien de garde** maximum de la CPU sont configurés dans l'onglet **Général** de la boîte de dialogue **Propriétés de la tâche FAST**.

NOTE:

- La plage de valeurs de période admissibles pour la tâche SAFE va de 10 à 255 ms, avec une valeur par défaut de 20 ms.
- La plage de valeurs de période admissibles pour la tâche FAST va de 1 à 255 ms, avec une valeur par défaut de 5 ms.
- La plage de valeurs admissibles pour le chien de garde va de 10 à 500 ms, avec une valeur par défaut de 250 ms.
- La plage de valeurs admissibles pour le timeout de repli des modules de sortie numérique va de 0 à 65535 ms, avec une valeur par défaut de 500 ms.

Assurez-vous que la valeur du chien de garde est supérieure à la période de la tâche SAFE.

Vérifiez la période de la tâche SAFE de la CPU lors de la mise en service de votre projet. À ce moment, Control Expert Safety fournit les valeurs en temps réel émanant du contrôleur d'automatisation programmable (PAC).

Vous trouverez ces informations dans Control Expert Safety en ouvrant l'onglet **Tâche** et en utilisant le menu **Outils > Écran PLC**.

La période de la tâche SAFE du contrôleur doit être inférieure au délai de sécurité de processus de votre projet.

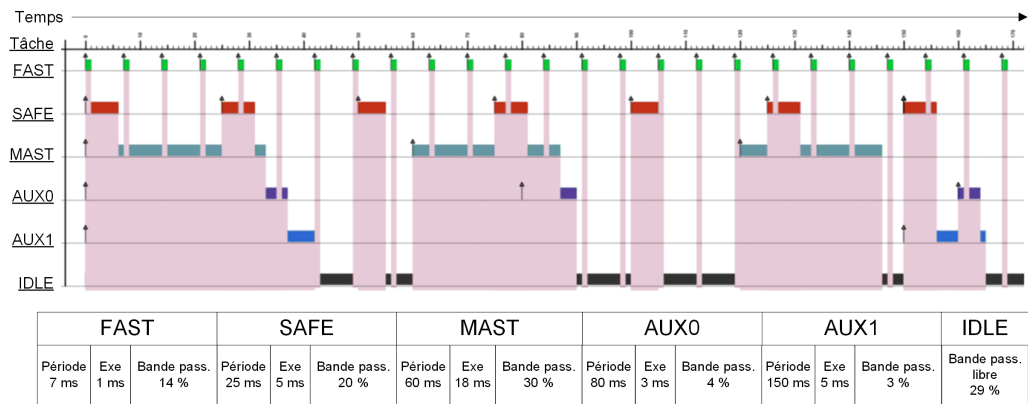
▲ **AVERTISSEMENT**

DÉPASSEMENT DU DÉLAI DE SÉCURITÉ DU PROCESSUS

Définissez la période maximum de la tâche SAFE du contrôleur en tenant compte du délai de sécurité de votre processus.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

La figure suivante illustre l'exécution de chaque tâche dans un système multitâche et décrit la préemption des ressources de la CPU en fonction de la priorité de la tâche :



NOTE: Lorsque la tâche MAST est en mode périodique et pour optimiser les performances de la CPU, le pourcentage total de la bande passante de la CPU consommé par une application ne doit pas dépasser 80 %.

Calcul de l'impact des périodes d'exécution des tâches sur la bande passante de la CPU

Chaque tâche configurée consomme une portion du temps de traitement (ou bande passante) de la CPU. Le pourcentage estimé de bande passante de la CPU qui est consommé par une tâche est le résultat (quotient) du temps d'exécution estimé de la tâche (E_{TASK}) divisé par la période d'exécution configurée pour cette tâche (T_{TASK}), d'où la formule suivante :

Bande passante de la tâche = E_{TASK} / T_{TASK} .

Par conséquent, le pourcentage total de bande passante de CPU consommé par une application est la somme des pourcentages de bande passante consommés par toutes les tâches.

NOTE: Lorsque la tâche MAST est en mode périodique et pour optimiser les performances de la CPU, le pourcentage total de la bande passante de la CPU consommé par une application ne doit pas dépasser 80 %.

Le tableau suivant présente deux applications et indique l'impact de tâches à haute priorité (FAST et SAFE) sur la consommation totale de la bande passante de la CPU :

#	FAST			SAFE			MAST			AUX0			To- tal
	Per.	Exe- c.	% BP	Per.	Exec.	% BP	Per.	Exec.	% BP	Per.	Exec.	% BP	
1	5 ms	1 ms	20 %	20 ms	5 ms	25 %	50 ms	18 ms	35 %	200 ms	30 ms	15 %	96 %
2	7 ms	1 ms	14 %	25 ms	5 ms	20 %	60 ms	18 ms	30 %	200 ms	30 ms	15 %	79 %
Per. = période de la tâche (T_{TASK})													
Exec. = temps d'exécution de la tâche (E_{TASK})													
% BP = bande passante consommée par la tâche													

Incidence des communications CIP Safety sur le temps de réaction du système de sécurité

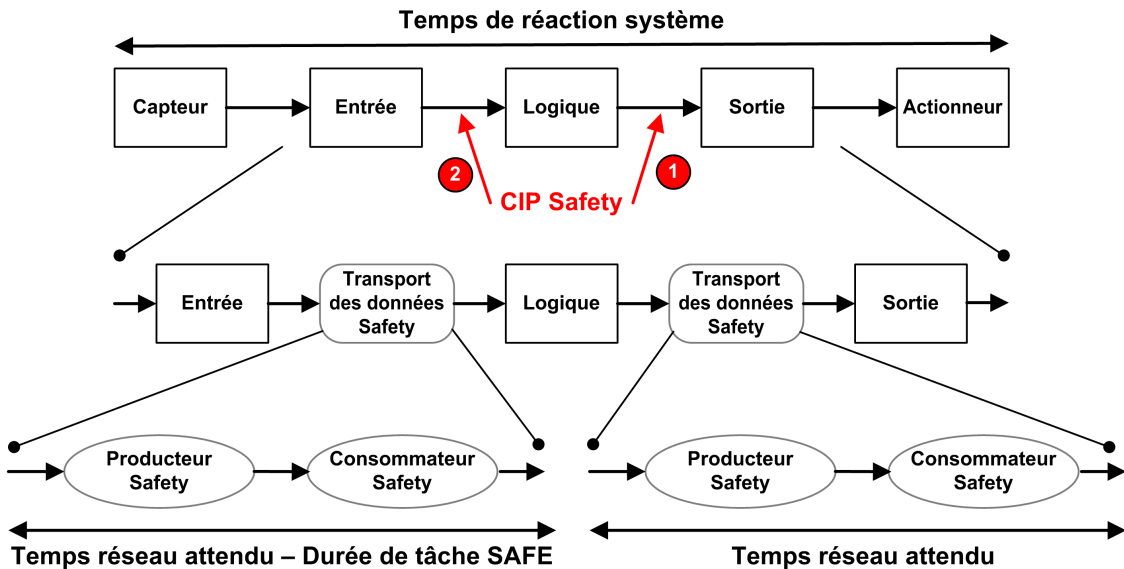
Introduction

Le temps consommé par la communication CIP Safety, soit le *temps réseau attendu*, est ajouté au *temps de réaction système*, page 161. Il représente la période maximale (scénario le plus pessimiste) entre la capture des données par le producteur de données de sécurité et la reconnaissance d'un état de sécurité par l'application consommatrice. Ce paramètre inclut également les erreurs en phases de production et consommation.

Lorsque la communication CIP Safety est établie entre une entrée et la logique, remplacez la variable de délai TCOMM_IN dans le calcul du délai de sécurité du processus, page 161 par *Temps réseau attendu - Durée_tâche_SAFE*. Lorsque la communication CIP Safety est établie entre la logique et une sortie, remplacez la variable TCOMM_OUT dans le calcul du délai de sécurité du processus par *Temps réseau attendu*.

Les mesures par défaut du temps réseau attendu varient selon que la CPU de sécurité M580 joue le rôle de producteur ou de consommateur.

Le schéma suivant définit les composantes du temps réseau attendu et leur organisation dans le contexte du temps de réaction système :



1 Module CPU CIP Safety producteur

2 Module CPU CIP Safety consommateur

Calcul du temps réseau attendu

Le temps réseau attendu est calculé selon la formule suivante :

Temps réseau attendu = Multiplicateur_temps_réseau_attendu * 128 µSec > (EPI * Multiplicateur_timeout + Durée_message_sécurité(max) + Délai_message_coordination_horaire(max) + Constante_correction_connexion * 128 µSec)

Où :

- **Durée_message_sécurité(max)** correspond à la durée réelle entre le moment où les données sont capturées par le producteur de données de sécurité et transmises à l'application consommatrice.
- **Délai_message_coordination_horaire(max)** correspond au délai maximal d'envoi des informations de coordination horaire du consommateur au producteur.
- **Multiplicateur_timeout** correspond à un paramètre utilisé lors du traitement CIP Safety, qui détermine le nombre de messages pouvant être perdus avant qu'une erreur de connexion soit déclarée. La valeur 1 indique qu'aucun message ne peut être perdu.
- **Constante_correction_connexion** correspond à une valeur par incréments de 128 µSec, soustraite de l'horodatage, qui représente la pire erreur causée par un écart de temps, la nature asynchrone des horloges producteur et consommateur, et le délai minimal pour la transmission du message de coordination horaire entre le consommateur et le producteur.
- **EPI** correspond à l'intervalle attendu entre paquets, en fonction de la période configurée pour la tâche SAFE.
- **Multiplicateur_temps_réseau_attendu** et **Multiplicateur_timeout** sont des paramètres de communication CIP configurés pour la trame de connexion SafetyOpen de type 2, page 386.

Valeurs de temps réseau attendu par défaut

La valeur de temps réseau attendu par défaut varie selon que la CPU CIP Safety joue le rôle de consommateur (cas 2 dans le schéma précédent) ou de producteur (cas 1).

Module CPU consommateur (cas 2) :

- $\text{Multiplicateur_timeout} = 2$
- $\text{EPI} = \text{Période_tâche_SAFE} / 2$
- $\text{Durée_message_sécurité(max)} = \text{Période_tâche_SAFE} + 20 \text{ ms}$ (pire scénario)
- $\text{Délai_message_coordination_horaire(max)} = \text{Période_tâche_SAFE} + 20 \text{ ms}$ (pire scénario)
- $\text{Constante_correction_connexion} = 0 \text{ ms}$

Temps réseau attendu = $1,5 * \text{Temps_réseau_attendu_minimal} = 1,5 * (3 * \text{Période_tâche_SAFE} + 40 \text{ ms}) = 4,5 * \text{Période_tâche_SAFE} + 60 \text{ ms}$

Module CPU producteur (cas 1) :

- $\text{Multiplicateur_timeout} = 2$
- $\text{EPI} = \text{Période_tâche_SAFE}$
- $\text{Durée_message_sécurité(max)} = \text{Période_tâche_SAFE} + 20 \text{ ms}$ (pire scénario)
- $\text{Délai_message_coordination_horaire(max)} = \text{Période_tâche_SAFE} + 20 \text{ ms}$ (pire scénario)

- $\text{Constante_correction_connexion} = 0 \text{ ms}$

Temps réseau attendu = $1,5 * \text{Temps_réseau_attendu_minimal} = 1,5 * (4 * \text{Période_tâche_SAFE} + 40 \text{ ms}) = 6 * \text{Période_tâche_SAFE} + 60 \text{ ms}$

Bibliothèque de sécurité

Bibliothèque de sécurité

Présentation de la bibliothèque de sécurité

Lorsque vous installez Control Expert Safetyy, une bibliothèque de sécurité composée de fonctions élémentaires (EF), de blocs fonction élémentaires (EFB) et de blocs de fonction dérivés (DFB, Derived Function Block) est automatiquement incluse. Ces EF, EFB et DFB sont identifiés par le préfixe "S_" et leur utilisation est réservée aux sections de code gérées par la tâche SAFE.

NOTE: Un ensemble supplémentaire d'EF, d'EFB et de DFB est également installé. Il contient les mêmes objets de données que ceux utilisés par les contrôleurs d'automatisation programmables (PAC) 580 standard (non dédiés à la sécurité). Ces EF, EFB et DFB ne peuvent être utilisés que dans des sections de code gérées par les tâches de l'espace de nom des processus (MAST, FAST, AUX0 et AUX1).

Pour une description des blocs inclus dans la bibliothèque de sécurité M580, consultez le document *Bibliothèque de blocs de sécurité Control Expert - Bibliothèque de blocs de sécurité*.

Fonctions et blocs fonction de sécurité certifiés

▲ AVERTISSEMENT

FONCTIONNEMENT INATTENDU DE L'ÉQUIPEMENT

- N'utilisez pas la V1.00 du bloc fonction dérivé S_GUARD_LOCKING dans votre application.
- Dans Unity Pro 13.0 XLS (ou version ultérieure), mettez à jour le bloc fonction S_GUARD_LOCKING dans votre application avec la version V1.01 (ou ultérieure) et régénérez l'application.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

NOTE:

Unity Pro est l'ancien nom de Control Expert pour les versions 13.1 et antérieures.

Le sous-ensemble de fonctions élémentaires et de blocs fonction pouvant être utilisés dans la logique de sécurité sont décrits ci-après. Ils se trouvent dans la bibliothèque de sécurité.

Famille	Groupe ou nom	Type	Description
Logique	S_AND_*, S_OR_*, S_XOR_*, S_NOT_*, S_SHL_*, S_SHR_*, S_ROR_*, S_ROL_*	EF	Spécifique au type, par ex. S_AND avec 2 à 32 entrées (code en ligne)
Logique	S_RS, S_SR, S_F_TRIG, S_R_TRIG	EFB	–
Mathématiques	S_ADD_*, S_MUL_*, S_SUB_*, S_DIV_*, S_ABS_*, S_SIGN_*, S_NEG_*, S_MOVE, S_SQRT_REAL	EF	Gestion des erreurs détectées spécifique au type (par ex. débordement) à considérer (code en ligne)
Comparaison	S_GT_*, S_GE_*, S_LT_*, S_LE_*, S_NE_*, S_EQ_*	EF	Spécifique au type (code en ligne)
Statistique	S_LIMIT_*, S_MAX_*, S_MIN_*, S_MUX_*, S_SEL	EF	Spécifique au type (code en ligne)
Type à type	S_BIT_TO*, S_BOOL_TO_*, S_BYTE_TO_*, S_DINT_TO_*, S_DWORD_TO_*, S_INT_TO_*, S_REAL_TO_*, S_TIME_TO_*, S_UDINT_TO_*, S_UINT_TO_*, S_WORD_TO_*	EF	Spécifique au type (code en ligne)
Temporisa- teurs et compteurs	S_CTU_*, S_CTD_*, S_CTUD_*	EFB	Spécifique au type
Temporisa- teurs et compteurs	S_TON, S_TOF, S_TP	EFB	–
Egal à égal	S_RD_ETH_MX, S_WR_ETH_MX, S_RD_ETH_MX2, S_WR_ETH_MX2	DFB	Fonctions permettant d'effectuer une communication de sécurité d'égal à égal
Connexion d'actionneur	S_EDM, S_ENABLE_SWITCH, S_ESPE, S_OUTCONTROL, S_GUARD_LOCKING, S_GUARD_MONITORING, S_MODE_SELECTOR	DFB	Blocs fonction de sécurité des machines liés aux actionneurs
Connexion de capteur	S_EQUIVALENT, S_ANTIValent, S_EMERGENCYSTOP, S_TWO_HAND_CONTROL_TYPE_II, S_TWO_HAND_CONTROL_TYPE_III, S_MUTING_SEQ, S_MUTING_PAR, S_AI_COMP	DFB	Blocs fonction de sécurité des machines liés aux capteurs
Système	S_SYST_STAT_MX, S_SYST_TIME_MX, S_SYST_CLOCK_MX, S_SYST_RESET_TASK_BIT_MX, S_SYST_READ_TASK_BIT_MX	EFB	Blocs fonction système

Fonctions et blocs fonction de sécurité non certifiés

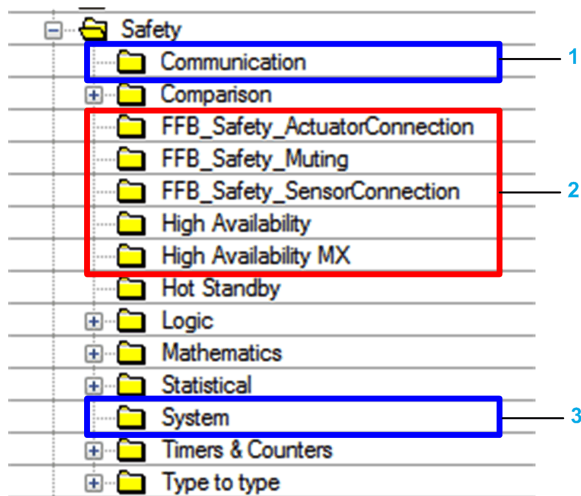
Le sous-ensemble de blocs de fonction dérivés (DFB, Derived Function Block) pouvant être utilisés dans la logique de sécurité sont décrits ci-après. Ces blocs fonction ne sont pas certifiés. Ils visent à fournir des blocs fonction de sécurité pouvant être réutilisés et adaptés.

Vous pouvez copier et coller ces blocs fonction dans votre application et les modifier selon vos besoins.

Famille	Groupe ou nom	Type	Description
MX haute disponibilité	S_DIHA, S_AIHA	DFB	Fonction modules d'entrées numériques SIL2 ou SIL3 à haute disponibilité (code en ligne)
Câblage des capteurs	AI_COMP	DFB	Blocs fonction de sécurité des machines liés aux capteurs

Affichage de la bibliothèque de sécurité dans Control Expert

Vous pouvez accéder à la bibliothèque de sécurité à partir de la tâche SAFE uniquement. Lorsque vous ouvrez la bibliothèque de sécurité dans l'**Éditeur FBD**, elle présente des groupes de types EF, EFB et DFB. Certains de ces groupes comprennent des versions de sécurité pour des fonctions et blocs utilisés dans les tâches non liées à la sécurité. D'autres groupes, indiqués ci-après, contiennent des fonctions et des blocs propres à la tâche SAFE.



1 Blocs pour lire et écrire des valeurs de données de sécurité.

2 Blocs pour effectuer des tâches spécifiques à la sécurité.

3 Blocs pour lire et écrire des valeurs du système de sécurité.

Vous trouverez un exemple d'implémentation des blocs de sécurité S_RD_ETH_MX et S_WR_ETH_MX. dans la section Exemple de configuration de la communication de contrôleur PAC à contrôleur PAC, page 194.

Consultez également la *Control ExpertBibliothèque de blocs de sécurité™* pour une description de chaque fonction et bloc de sécurité disponibles.

Séparation des données dans un système de sécurité M580

Introduction

Ce chapitre présente la division des données dans un système de sécurité M580.

Séparation des données dans un projet de sécurité M580

Séparation et portée des données

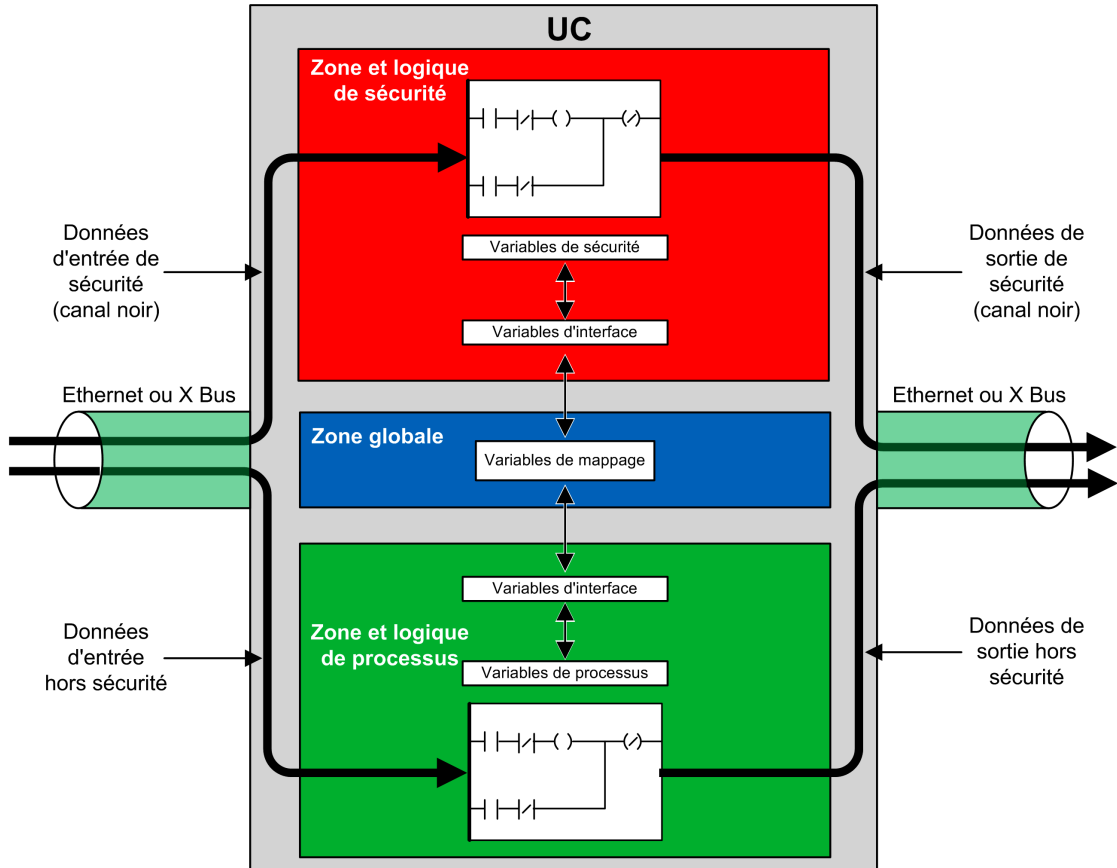
Un projet de sécurité M580 comprend un programme de sécurité et un programme de processus (non lié à la sécurité). Control Expert isole la logique et les données utilisées par le programme de sécurité de celles utilisées par le programme de processus. Pour cela, Control Expert place chaque partie du projet dans son propre espace de nom (également appelé zone), à savoir *sécurité* ou *processus*.

Grâce à cette conception, la portée d'une variable de sécurité est restreinte à la zone de sécurité et la portée d'une variable de processus est restreinte à la zone de processus. Cela apparaît lorsque vous ajoutez une logique de programme à l'application :

- Lorsque vous configurez une EF ou un EFB dans la tâche SAFE, seules les variables créées dans la zone de sécurité sont visibles. Les variables créées dans la zone de processus ne sont pas visibles.
- Lorsque vous configurez une EF ou un EFB dans une tâche non liée à la sécurité (MAST, FAST, AUX0 ou AUX1), seules les variables créées dans la zone de processus sont visibles. Les variables créées dans la zone de sécurité ne sont pas visibles.

Pour permettre la communication entre la zone de sécurité et la zone de processus, Control Expert fournit également une zone *globale*. La zone globale sert de zone de transit pour les transmissions de données entre la zone de sécurité et la zone de processus. Vous déclarez des variables d'interface dans les zones de sécurité et de processus, puis vous liez ces variables d'interface à des variables correspondantes déclarées dans la zone globale.

La séparation des données dans l'UC et le coprocesseur de sécurité M580 est illustrée graphiquement ci-après :



Propriétés des zones de sécurité, de processus et globale

Les trois zones de données d'un projet de sécurité M580 présentent les propriétés suivantes :

Zone	Types de variables pris en charge	Portée	Accès externe
Globale	Variables non localisées uniquement. NOTE: Il n'est pas possible d'utiliser des variables localisées pour la mise en correspondance avec une variable d'interface de sécurité ou de processus.	Peuvent accéder aux : - Variables de sécurité, via un adressage d'espace de nom. - Variables de processus, via un adressage d'espace de nom. - Autres variables globales.	Les variables des trois zones sont accessibles par les applications HMI, SCADA ou FactoryCast. (Voir la remarque ci-dessous.)
Sécurité	Variables non localisées uniquement.	Peuvent accéder uniquement à d'autres variables de sécurité.	
Proces-sus	Les deux : - Variables localisées - Variables non localisées	Peuvent accéder uniquement à d'autres variables de processus.	

Lorsqu'un consultant externe cherche à lire une variable de processus, le format d'adressage dépend de la configuration de l'option **Utilisation de l'espace de nom de processus** dans la zone **Portée > commune** de la fenêtre **Outils > Paramètres du projet...** Si l'option **Utilisation de l'espace de nom de processus** est

- sélectionnée : l'écran de l'opérateur permet de lire les variables de la zone de processus uniquement via le format "PROCESS.<nom de la variable>".
- Si non sélectionné : l'écran d'exploitation ne permet de lire les variables de la zone de processus qu'en utilisant le format <nom de la variable> sans le préfixe PROCESS. Dans ce cas, vérifiez que chaque nom de variable de processus est unique et qu'il n'est pas identique à un nom de variable globale.

NOTE: Si l'option **Utilisation de l'espace de nom de processus** est désélectionnée, vérifiez que chaque nom de variable de processus est unique et qu'il n'est pas identique à un nom de variable globale. Si un nom de variable existe à la fois dans la zone globale et dans la zone de processus, Control Expert détectera une erreur lors de la génération du projet.

Procédure de transfert de données entre zones d'espace de nom

Introduction

Le contrôleur d'automatisation programmable (PAC) de sécurité M580 comprend trois éditeurs de données différents :

- Un **Éditeur de données de sécurité** pour gérer les données utilisées dans l'espace de nom sécurisé.
- Un **Éditeur de données de processus** pour gérer les données utilisées dans l'espace de nom de processus.
- Un **Éditeur de données globales** pour gérer les variables et les types de données globaux utilisés dans l'ensemble de l'application.

L'**Éditeur de données de sécurité** et l'**Éditeur de données de processus** comprennent tous les deux un onglet **Interface**. Utilisez l'onglet **Interface** pour créer des variables non localisées dans l'espace de nom correspondant. L'onglet **Interface** présente deux groupes de variables non localisées :

- <entrées> : une variable créée dans ce groupe peut être liée à, et recevoir des données de, une variable de transit globale dans l'**Éditeur de données globales**.
- <sorties> : une variable de ce groupe peut être liée à, et envoyer des données à, une variable de transit globale dans l'**Éditeur de données globales**.

NOTE: Une variable créée dans l'un ou l'autre des onglets **Interface** doit être tout à la fois :

- une variable de catégorie EDT ou DDT
- du même type de données que la variable globale à laquelle elle est liée
- non liée à un bit extrait d'une variable localisée (par exemple, pas %MW10.1)

Les variables non localisées créées dans les groupes de l'onglet **Interface** de l'**Éditeur de données de sécurité** et de l'**Éditeur de données de processus** peuvent être reliées comme suit :

Une variable de processus de ce groupe de l'Éditeur de données de processus...	Peut être liée à une variable de sécurité de ce groupe de l'Éditeur de données de sécurité...
<entrées>	<sorties>
<sorties>	<entrées>

Ces trois éditeurs de données permettent de configurer le transfert de données entre l'espace de noms de sécurité et l'espace de noms de processus.

Transfert de données entre espaces de noms

Le transfert de données entre l'espace de nom sécurisé et l'espace de données de processus, et le transfert de données entre l'espace de nom sécurisé et l'espace de données de processus sont des images miroirs l'une de l'autre. L'exemple suivant vous montre comment transférer des données depuis la zone de processus vers la zone sécurisée :

Etape	Action
1	Ouvrez l' Éditeur de données de processus , cliquez sur l'onglet Interface du programme, puis créez une variable dans la partie <sorties> de l'éditeur de données.
2	Ouvrez l' Éditeur de données de sécurité , cliquez sur l'onglet Interface du programme, puis créez une variable du même type que celle créée à l'étape 1 dans la partie <entrées> de l'éditeur de données. Ensuite, double-cliquez sur le champ Paramètre effectif . La boîte de dialogue de l' Éditeur d'étendue des données : Sélection de variable s'ouvre.
3	Dans le menu déroulant en haut à droite de la boîte de dialogue, sélectionnez l'espace de noms cible PROCESSUS . Les variables dans l'espace de noms PROCESSUS sélectionné dans la partie <sorties> s'affichent.
4	Sélectionnez la variable de processus créée à l'étape 1, à lier à la variable SAFE que vous avez créée à l'étape 2, puis cliquez sur OK . La variable cible sélectionnée apparaît dans le champ Paramètre effectif .
5	Enregistrez vos modifications.

Après compilation, téléchargement et exécution du programme d'application modifié, la valeur est transférée comme suit :

- Les données de l'onglet **Interface** créées dans la partie **<sorties>** sont publiées à la fin de l'exécution de la tâche correspondante.
- Les données de l'onglet **Interface** **Interface** créées dans la partie **<entrées>** sont souscrites au début de l'exécution de la tâche correspondante.

Communications du système de sécurité M580

Introduction

Ce chapitre décrit les communications au sein du système de sécurité M580.

Synchronisation horaire

Introduction

Pour un contrôleur d'automatisation programmable (PAC) équipé du micrologiciel de CPU de version 3.10 ou antérieure :	La configuration du service NTP est nécessaire pour permettre une communication sécurisée. Les émetteurs et récepteurs doivent être synchronisés à l'aide de services NTP.
Pour un contrôleur d'automatisation programmable (PAC) équipé du micrologiciel de CPU de version 3.20 ou ultérieure :	La synchronisation horaire sécurisée s'appuie sur une horloge interne et "monotone". La communication sécurisée n'a pas besoin de synchronisation NTP : • Le contrôleur de sécurité partage son heure sécurisée avec toutes ses E/S locales et distantes. • Le module de communication avec les E/S distantes BM•CRA31210 nécessite un micrologiciel de version 2.60 ou ultérieure. • Pour les communications d'égal à égal, les contrôleurs partagent leur horaire sécurisé.

Configuration de la synchronisation horaire avec le micrologiciel de contrôleur de version 3.10 ou antérieure

Introduction

Si vous installez des modules d'E/S de sécurité dans une station d'E/S distante, configurez l'heure du contrôleur, qui peut être obtenue en utilisant trois conceptions avec le micrologiciel de contrôleur de version 3.10 ou antérieure :

1. **Conception de serveur NTP distant avec contrôleur comme client NTP :**
Configurez un équipement dans le réseau de contrôle en tant que serveur NTP, puis configurez le contrôleur de sécurité en tant que client NTP.
2. **Conception du serveur NTP local :** Configurez le contrôleur de sécurité en tant que serveur NTP pour les équipements du réseau RIO Ethernet.

3. **Conception de serveur NTP distant avec eNOC ou eNOP** : Dans le rack local principal, configurez un équipement dans le réseau de contrôle en tant que serveur NTP, puis un module (un module BMENOP0300, un module BMENOC0301 ou un module BMENOC0311) et activez la fonctionnalité facultative suivante dans le DTM correspondant :

Actualisation de l'heure du contrôleur > Mettre à jour l'heure du contrôleur avec ce module

Si des équipements de sécurité sont installés sur une station d'E/S distante (RIO), configurez le contrôleur de sécurité en tant que serveur NTP comme indiqué dans le cas 2 précédent.

Dans les deux conceptions :

- Activez le service NTP.
- Définissez la période d'interrogation NTP sur 20 s.

Si le contrôleur de sécurité n'est pas configurée en tant que serveur NTP ou client NTP, les paramètres temporels des modules d'E/S de sécurité distants et du contrôleur ne seront pas synchronisés, et la communication par canal ne fonctionnera pas correctement. Les entrées et sorties des modules d'E/S de sécurité dans les stations d'E/S distantes (RIO) passeront à l'état sécurisé (non alimenté) défini ou l'état de repli.

NOTE: Si vous installez des modules d'E/S de sécurité dans une station d'E/S distante, configurez l'heure du contrôleur avec le micrologiciel de version 3.10 ou antérieure. Activez le service NTP pour votre système M580 et configurez le contrôleur de sécurité en tant que serveur NTP ou client NTP.

Configurez deux sources NTP, qui peuvent fonctionner de manière redondante, l'une comme serveur primaire et la seconde comme serveur de temps redondant. Configurez les deux serveurs pour qu'ils soient synchronisés. Tout réglage supérieur ou égal à 2 s dans une période d'interrogation NTP entraîne la désynchronisation du contrôleur et des modules d'E/S de sécurité et une dérive par rapport au serveur de temps NTP.

Modification des paramètres temporels NTP durant les opérations

Si vous utilisez Control Expert V13.0 ou V13.1 ou un micrologiciel de contrôleur de version 2.70 ou antérieure, la modification de l'heure pendant le fonctionnement peut entraîner une perte de communication et un arrêt du système de sécurité.

AVIS

ÉQUIPEMENT INOPÉRANT

Ne modifiez pas le paramètre de temps pendant le fonctionnement (avec Control Expert V13.0 ou V13.1 ou avec un micrologiciel de contrôleur de version 2.70 ou antérieure).

Le non-respect de ces instructions peut provoquer des dommages matériels.

Un changement d'heure durant les opérations peut entraîner une désynchronisation avec l'horloge de référence. Il peut également entraîner une perte de communication de sécurité, ce qui ferait passer les E/S à l'état de repli ou l'état de sécurité défini. Surveillez le système pour détecter toute désynchronisation, et, si cela arrive, restaurer la synchronisation pour éviter une perte de communication. Si la désynchronisation se produit, suivez la procédure suivante, page 187 pour resynchroniser le système.

Si vous utilisez Control Expert version 14.0 ou ultérieure et le micrologiciel de contrôleur 2.80, 2.90 ou 3.10 : Vous pouvez modifier le réglage de l'heure dans le serveur NTP ou le contrôleur pendant le fonctionnement sans impact négatif. Effectuez cette opération en suivant la procédure définie ci-dessous immédiatement après une modification de l'heure.

Pour plus d'informations sur la configuration du service NTP pour un contrôleur *Onglet NTP* du document *Modicon M580 - Manuel de référence du matériel M580*.

Procédure de synchronisation des paramètres temporels NTP

En cas de redémarrage ou de réinitialisation du contrôleur, et si celui-ci reçoit d'abord une heure d'un serveur NTP externe, procédez comme suit pour synchroniser l'heure du contrôleur.

AVIS

ÉQUIPEMENT INOPÉRANT

Synchronisez l'heure SAFE avec le serveur NTP externe en utilisant %SW128 une fois que le serveur NTP externe est opérationnel (lorsque %SW152 passe de 0 à 1) tout en utilisant l'option **Mettre à jour le temps CPU avec ce module** sur un module BMENOP0300, un module BMENOC0301 ou un module BMENOC0311 pour mettre à jour l'heure du contrôleur.

Le non-respect de ces instructions peut provoquer des dommages matériels.

La procédure décrite ci-après est valide avec la tâche SAFE à l'état RUN, en utilisant Control Expert V14.0 ou une version supérieure et le micrologiciel de contrôleur de version 2.80, 2.90 ou 3.10.

Étape	Action
1	Vérifiez que l'horloge du serveur du contrôleur ou du serveur NTP externe est valide, intègre et stable.
2	Si la configuration inclut une ou plusieurs stations d'E/S distantes, attendez deux périodes d'interrogation NTP pour permettre l'envoi de la nouvelle valeur de temps de référence à tous les modules CRA. Effectuez cette opération après le rétablissement du service NTP ou après la modification de l'heure (qui a entraîné la désynchronisation).
3	Synchronisez le système sur l'horloge de référence en utilisant le mot système %SW128 : - Définissez %SW128 sur 16#1AE5 pendant au moins 500 ms. - Définissez %SW128 sur #E51A pendant au moins 500 ms.
4	Vérifiez que l'horloge est synchronisée en confirmant que la valeur des paramètres CPU_NTP_SYNC et M_NTP_SYNC dans DDDT IO de sécurité est vrai (1)

Si la séquence de synchronisation n'est pas correctement exécutée, exécutez-la à nouveau.

AVIS
ÉQUIPEMENT INOPÉRANT Effectuer une procédure de synchronisation pour éviter que les E/S de sécurité n'entrent dans leur état de sécurité défini ou leur état de repli après une dérive de l'horloge d'environ un délai d'expiration de la communication. Le non-respect de ces instructions peut provoquer des dommages matériels.

Si vous utilisez Control Expert V14.0 ou version ultérieure et le micrologiciel de contrôleur 2.80 ou version ultérieure pour effectuer une modification d'horloge de contrôleur, faites suivre cette modification de la procédure de synchronisation décrite précédemment.

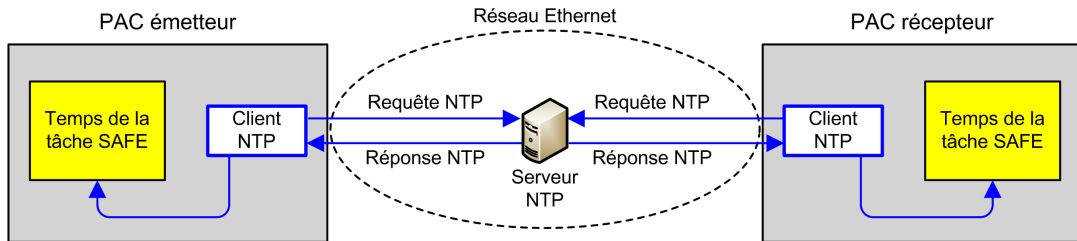
Au cours de l'étape 3 de la procédure de synchronisation horaire, les diagnostics de communication de sécurité sont désactivés pendant 500 ms. Effectuez au maximum une modification d'horloge et une synchronisation par jour.

Service NTP pour la communication d'égal à égal

La communication entre contrôleurs de sécurité Ethernet nécessite la synchronisation de la base de temps du contrôleur émetteur et du contrôleur récepteur.

NOTE: Configurez dans chaque contrôleur (soit le contrôleur de sécurité, soit un module BMENOP0300, un module BMENOC0301 ou un module BMENOC011) un client NTP et configurez un autre équipement du réseau en tant que serveur NTP.

La figure suivante illustre le principe de la synchronisation de la base de temps des contrôleurs émetteur et récepteur :



Dans Control Expert, configurez les paramètres du service NTP de chaque client de la manière suivante :

- Sélectionnez **Client NTP**.
- Dans **Adresse IP du serveur NTP principal**, indiquez l'adresse IP du serveur NTP distant..
- Définissez le paramètre **Période d'interrogation** sur 20 secondes.

Cohérence horaire du serveur NTP et bits système

Cohérence horaire du serveur NTP :

- Si l'heure du serveur NTP est cohérente avec l'heure interne du contrôleur affichée par la fonction élémentaire (EF) `S_SYST_CLOCK` à moins de 2 secondes près, la valeur de l'heure dans la fonction élémentaire (EF) `S_SYST_CLOCK` est mise à jour sur la dernière heure reçue du serveur NTP, filtrée avec une pente de 1 ms/s.

- Si l'heure reçue du serveur NTP diffère de plus de 2 secondes de l'heure interne du contrôleur affichée par l'EF S_SYST_CLOCK :
 - Le contrôleur ignore la dernière heure reçue du serveur NTP.
 - la valeur de l'heure affichée par l'EF S_SYST_CLOCK est actualisée en interne.
 - Le paramètre de État S_SYST_CLOCK est défini sur 0.
 - Le paramètre de sortie SYNCHRO_NTP du S_RD_ETH_MX et les blocs DFB S_WR_ETH_MX sont définis sur 0 pour indiquer cette condition.

Dans ce cas, réinitialisez l'heure interne du contrôleur de l'une des manières suivantes :

- Réinitialisez l'application par un démarrage à froid.
- Téléchargez l'application.
- Redémarrez le contrôleur.
- Suivez les étapes de la section pour modifier les paramètres temporels NTP, page 187.

NOTE: Si la synchronisation NTP est perdue sur l'un des deux contrôleurs (paramètre SYNCHRO_NTP défini sur 0), la base de temps des deux contrôleurs émetteur et récepteur peut être désynchronisée. Dans ce cas, la communication d'égal à égal sécurisée risque de cesser d'être opérationnelle (le paramètre de sortie health du bloc DFB S_RD_ETH_MX est défini sur 0).

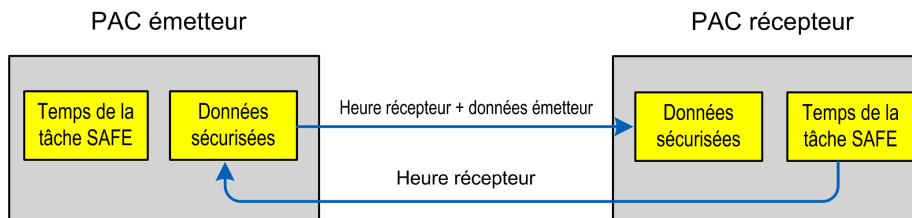
Synchronisation horaire pour micrologiciel de CPU de version 3.20 ou ultérieure

Synchronisation horaire pour la communication d'égal à égal

NOTE: Avec le micrologiciel de contrôleur de version 3.20 ou supérieure, le service NTP n'est pas utilisé pour synchroniser l'heure.

La communication de contrôleur à contrôleur de sécurité Ethernet nécessite que les contrôleurs émetteur et récepteur partagent une heure sécurisée commune.

La figure suivante illustre le principe de partage d'heure entre le contrôleur émetteur et récepteur :



Dans Control Expert, configurez :

- une communication de l'émetteur au récepteur pour la transmission des données
- une communication du récepteur à l'émetteur pour la transmission de l'heure sécurisée

Cohérence horaire

Une heure sécurisée interne (indépendante de NTP) est distribuée par le contrôleur à tous ses modules d'E/S de sécurité locaux et distants.

Communication d'égal à égal

Introduction

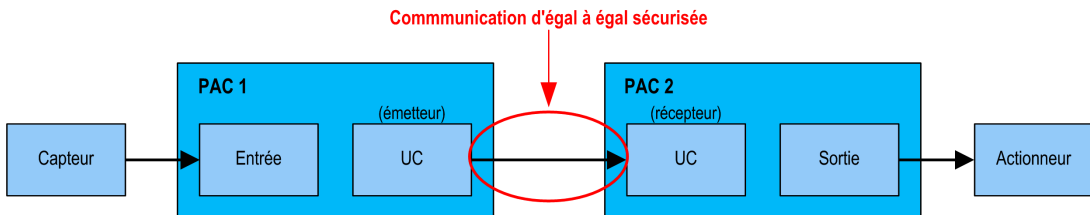
Cette section décrit les communications d'égal à égal entre les contrôleurs de sécurité du M580.

Communication d'égal à égal

Introduction

Vous pouvez en configurer deux contrôleurs de sécurité M580 pour effectuer une communication de sécurité d'égal à égal sur Ethernet. La configuration s'appuie sur la communication de scrutateur Modbus TCP incorporée dans un canal.

Présentation des caractéristiques fonctionnelles générales de la communication sécurisée d'égal :



La communication est effectuée par deux blocs fonction élémentaires issus de la bibliothèque de blocs fonction de sécurité M580 qui gèrent la boucle de sécurité au niveau SIL3. Le protocole détecte les erreurs de transmission (omissions, insertions, séquences mal ordonnées, retards, adressage incorrect, bits déguisés) et gère les retransmissions.

Cette communication d'égal à égal de sécurité est possible uniquement entre :

- deux contrôleurs de sécurité M580 avec micrologiciel de version 3.10 ou antérieure
- deux contrôleurs de sécurité M580 avec micrologiciel de version 3.20 ou postérieure

NOTE: La communication d'égal à égal de sécurité est également possible entre un contrôleur de sécurité Modicon Quantum et un contrôleur de sécurité M580 avec micrologiciel de version 3.10 ou antérieure.

NOTE: Avec un micrologiciel de contrôleur de version antérieure à 4.20, la communication d'égal à égal de sécurité ne fonctionne pas si le **Mode de liaison d'ingénierie** est réglé sur **Appliqué** sur le contrôleur récepteur.

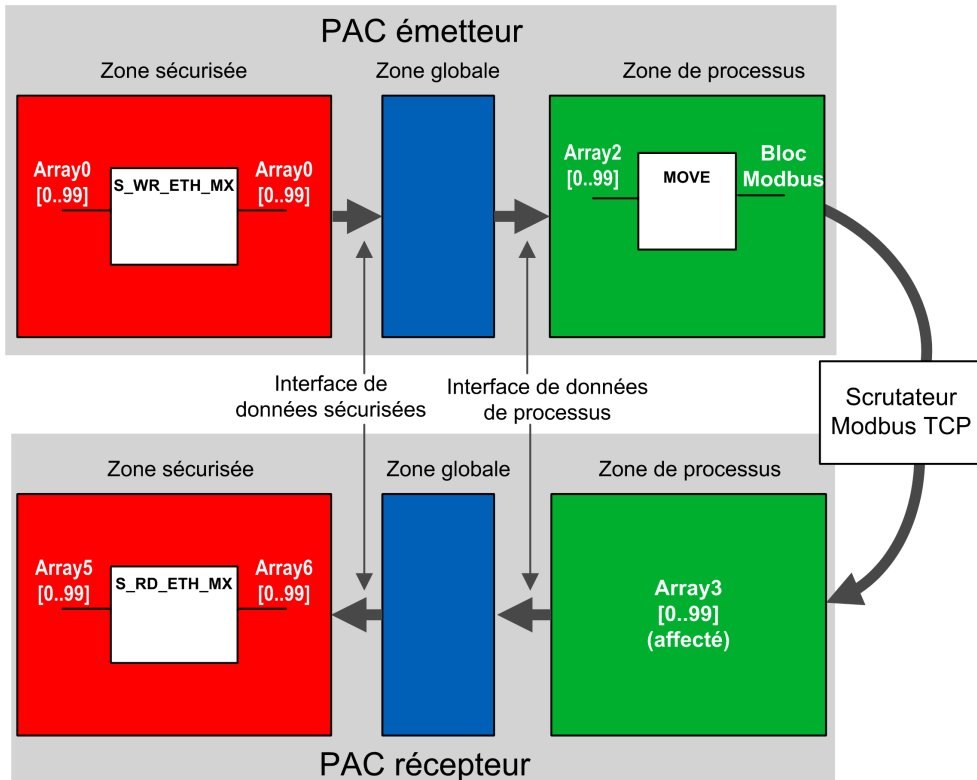
Architecture d'égal à égal avec micrologiciel d'UC de version 3.10 ou antérieure

Conception de l'architecture

Avec un micrologiciel d'UC de version 3.10 ou antérieure, l'architecture de la solution repose sur les éléments suivants :

- Service NTP pour la synchronisation temporelle.
- Exécution de 2 DFB (S_WR_ETH_MX et MOVE dans le PAC émetteur et de 1 DFB (S_RD_ETH_MX) dans le PAC récepteur.
- Scrutation via Modbus TCP pour le transport des données.

L'illustration suivante donne un aperçu du processus impliqué pour assurer la communication d'égal à égal de façon sécurisée :



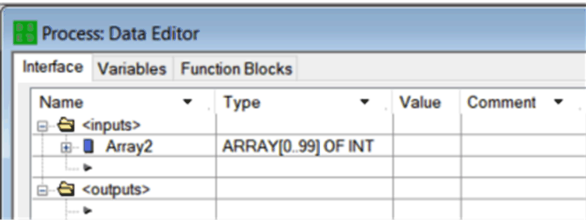
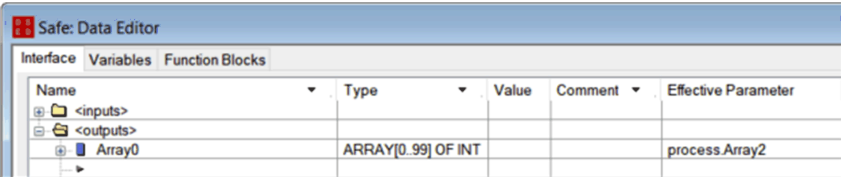
Dans la figure ci-dessus, Control Expert crée automatiquement – et masque dans la vue externe – les tableaux 1 et 4 dans les zones globales des PAC homologues. Du point de vue

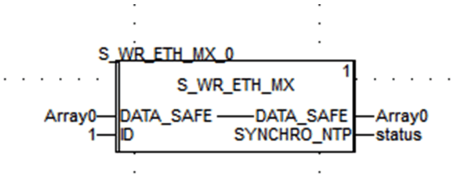
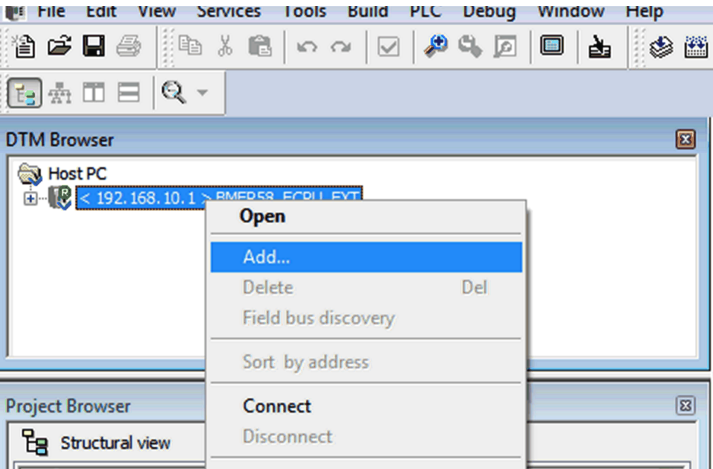
d'un utilisateur, les liaisons sont établies du tableau Array 0 à Array 2, et du tableau Array 3 à Array 5.

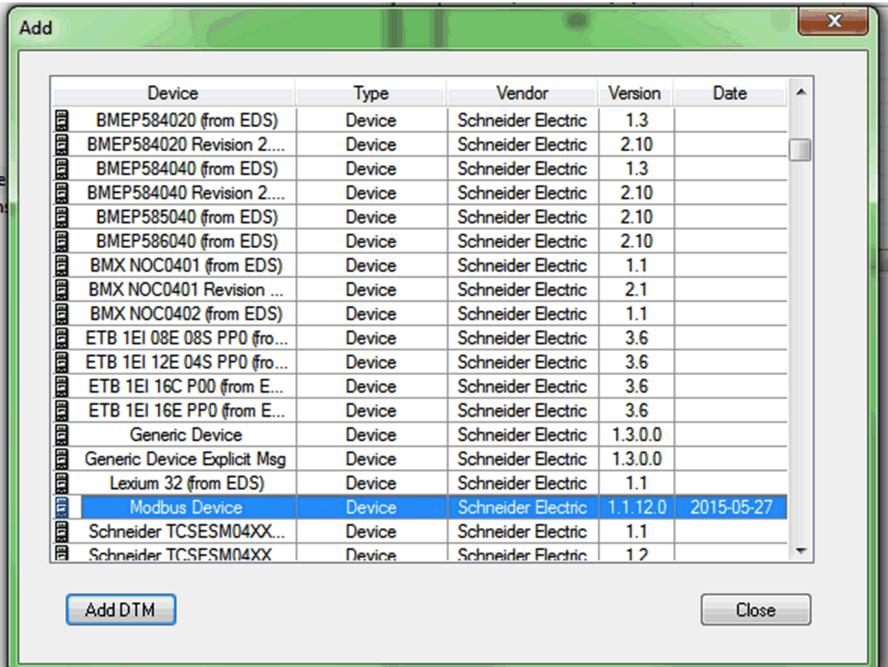
NOTE: Sur le réseau Ethernet, vous êtes autorisé à mélanger des données liées à la sécurité et des données hors sécurité sans impacter le niveau de sécurité des premières. Aucune restriction ne s'applique au réseau Ethernet lorsque la communication d'égal à égal sécurisée est utilisée.

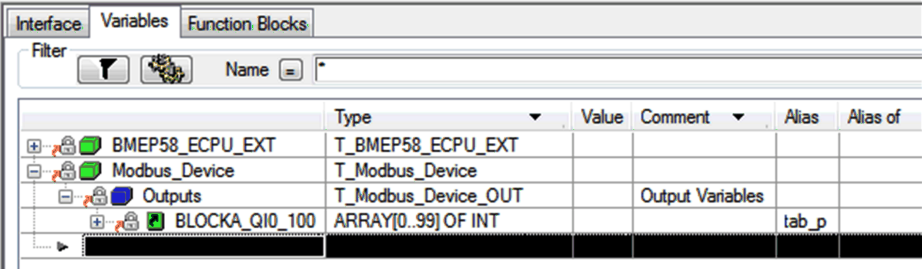
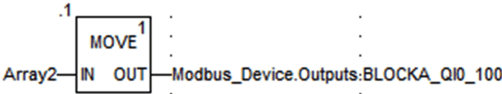
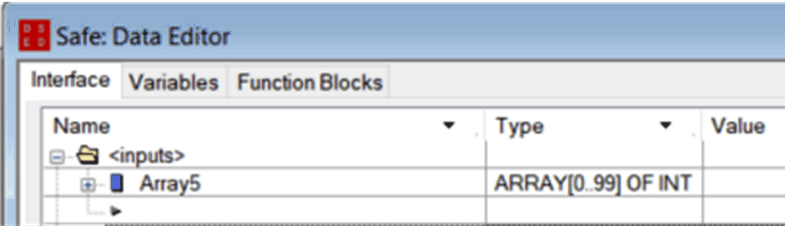
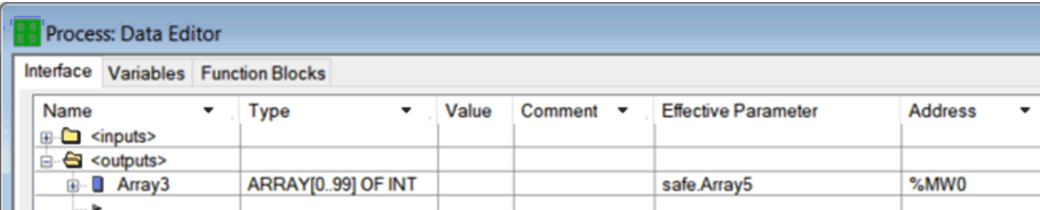
Détails de la configuration du transfert de données d'égal à égal

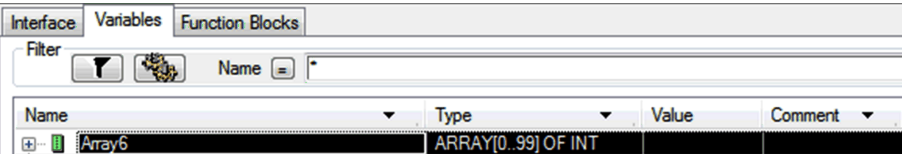
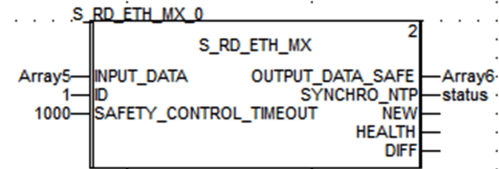
L'exemple suivant montre comment configurer un transfert de données d'égal à égal entre deux PAC de sécurité avec le micrologiciel d'UC de version 3.10 ou antérieure et Control Expert version 14.1 ou antérieure :

Eta-pe	Action
1	Sur le PAC émetteur, utilisez l'Editeur de données de processus pour créer un tableau (array) de 100 entiers comme entrée dans la zone Interface. Dans cet exemple, le nom du tableau est Array2 : 
2	Sur le PAC émetteur, créez un autre tableau de 100 entiers comme sortie dans l'onglet Interface de l'Editeur de données de sécurité et liez-le au tableau d'entrée créé à l'étape 1 dans la colonne Paramètre effectif. Dans cet exemple, le nom du tableau est Array0 :  NOTE: Les variables entières d'indices 0 à 90 de ce tableau contiennent les valeurs de variables de sécurité à échanger avec le PAC récepteur. La zone restante est réservée aux données de diagnostic générées automatiquement, dont la valeur CRC et l'horodatage. Ces données de diagnostic sont utilisées par le PAC récepteur pour déterminer si les données transférées sont sûres.

Eta-pe	Action
3	Sur le PAC émetteur, configurez le DFB S_WR_ETH_MX dans une section de la tâche SAFE. Liez ce DFB à Array0 : 
4	Dans le Navigateur de DTM du PAC émetteur, sélectionnez l'UC (pour cet exemple) ou un module de communications NOC (le cas échéant), puis cliquez sur Ajouter... pour créer un scrutateur Modbus qui puisse envoyer des données via Modbus TCP depuis le PAC émetteur vers le PAC récepteur : 

Eta- pe	Action																																																																																																				
5	Sélectionnez Equipement Modbus et cliquez sur Ajouter un DTM pour ajouter le scrutateur Modbus :  <table><thead><tr><th>Device</th><th>Type</th><th>Vendor</th><th>Version</th><th>Date</th></tr></thead><tbody><tr><td>BMEP584020 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.3</td><td></td></tr><tr><td>BMEP584020 Revision 2....</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr><tr><td>BMEP584040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.3</td><td></td></tr><tr><td>BMEP584040 Revision 2....</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr><tr><td>BMEP585040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr><tr><td>BMEP586040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr><tr><td>BMX NOC0401 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr><tr><td>BMX NOC0401 Revision ...</td><td>Device</td><td>Schneider Electric</td><td>2.1</td><td></td></tr><tr><td>BMX NOC0402 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr><tr><td>ETB 1EI 08E 08S PP0 (fro...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr><tr><td>ETB 1EI 12E 04S PP0 (fro...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr><tr><td>ETB 1EI 16C P00 (from E...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr><tr><td>ETB 1EI 16E PP0 (from E...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr><tr><td>Generic Device</td><td>Device</td><td>Schneider Electric</td><td>1.3.0.0</td><td></td></tr><tr><td>Generic Device Explicit Msg</td><td>Device</td><td>Schneider Electric</td><td>1.3.0.0</td><td></td></tr><tr><td>Lexium 32 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr><tr><td>Modbus Device</td><td>Device</td><td>Schneider Electric</td><td>1.1.12.0</td><td>2015-05-27</td></tr><tr><td>Schneider TCSESM04XX...</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr><tr><td>Schneider TCSESM04XX</td><td>Device</td><td>Schneider Electric</td><td>1.2</td><td></td></tr></tbody></table>	Device	Type	Vendor	Version	Date	BMEP584020 (from EDS)	Device	Schneider Electric	1.3		BMEP584020 Revision 2....	Device	Schneider Electric	2.10		BMEP584040 (from EDS)	Device	Schneider Electric	1.3		BMEP584040 Revision 2....	Device	Schneider Electric	2.10		BMEP585040 (from EDS)	Device	Schneider Electric	2.10		BMEP586040 (from EDS)	Device	Schneider Electric	2.10		BMX NOC0401 (from EDS)	Device	Schneider Electric	1.1		BMX NOC0401 Revision ...	Device	Schneider Electric	2.1		BMX NOC0402 (from EDS)	Device	Schneider Electric	1.1		ETB 1EI 08E 08S PP0 (fro...	Device	Schneider Electric	3.6		ETB 1EI 12E 04S PP0 (fro...	Device	Schneider Electric	3.6		ETB 1EI 16C P00 (from E...	Device	Schneider Electric	3.6		ETB 1EI 16E PP0 (from E...	Device	Schneider Electric	3.6		Generic Device	Device	Schneider Electric	1.3.0.0		Generic Device Explicit Msg	Device	Schneider Electric	1.3.0.0		Lexium 32 (from EDS)	Device	Schneider Electric	1.1		Modbus Device	Device	Schneider Electric	1.1.12.0	2015-05-27	Schneider TCSESM04XX...	Device	Schneider Electric	1.1		Schneider TCSESM04XX	Device	Schneider Electric	1.2	
Device	Type	Vendor	Version	Date																																																																																																	
BMEP584020 (from EDS)	Device	Schneider Electric	1.3																																																																																																		
BMEP584020 Revision 2....	Device	Schneider Electric	2.10																																																																																																		
BMEP584040 (from EDS)	Device	Schneider Electric	1.3																																																																																																		
BMEP584040 Revision 2....	Device	Schneider Electric	2.10																																																																																																		
BMEP585040 (from EDS)	Device	Schneider Electric	2.10																																																																																																		
BMEP586040 (from EDS)	Device	Schneider Electric	2.10																																																																																																		
BMX NOC0401 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
BMX NOC0401 Revision ...	Device	Schneider Electric	2.1																																																																																																		
BMX NOC0402 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
ETB 1EI 08E 08S PP0 (fro...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 12E 04S PP0 (fro...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 16C P00 (from E...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 16E PP0 (from E...	Device	Schneider Electric	3.6																																																																																																		
Generic Device	Device	Schneider Electric	1.3.0.0																																																																																																		
Generic Device Explicit Msg	Device	Schneider Electric	1.3.0.0																																																																																																		
Lexium 32 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
Modbus Device	Device	Schneider Electric	1.1.12.0	2015-05-27																																																																																																	
Schneider TCSESM04XX...	Device	Schneider Electric	1.1																																																																																																		
Schneider TCSESM04XX	Device	Schneider Electric	1.2																																																																																																		
6	Ouvrez l'équipement Modbus que vous venez d'ajouter, ajoutez une requête, puis effectuez les actions suivantes dans l'onglet Configuration de requête : - Affectez la valeur 100 à la colonne Longueur (écriture) (il s'agit de la longueur des données à écrire), puis - Renseignez la colonne Adresse (écriture). Il s'agit de l'adresse à laquelle la table du PAC récepteur va écrire les données reçues (dans cet exemple : 0, ce qui signifie que le PAC émetteur va écrire dans la table à partir de %MW0 sur le PAC récepteur).																																																																																																				

Eta-pe	Action
8	Une fois la configuration enregistrée et générée, le bloc (BLOCKA_QI0_100 dans l'exemple) est créé automatiquement en tant que variable de processus : 
9	Sur le PAC émetteur, dans une section de code de processus, utilisez un DFB MOVE pour copier le contenu de Array2 vers le tableau défini précédemment dans la structure d'équipement Modbus : 
10	Sur le PAC récepteur, utilisez l'Editeur de données de sécurité pour créer un tableau de 100 entiers (Array5) en tant qu'entrée dans la zone Interface : 
11	Sur le PAC récepteur, dans l'Editeur de données de processus, créez un tableau (Array3) de 100 INT dans la section <sorties> de l'onglet Interface. Liez ce tableau au tableau de la zone des données (Array5, créé à l'étape 10) dans la colonne Paramètre effectif. Les données envoyées par le PAC émetteur seront écrites dans ce tableau via le scrutateur Modbus, à condition que cette variable soit située à l'adresse définie dans le scrutateur du PAC émetteur (%MW0 dans cet exemple) : 

Eta-pe	Action
12	Sur le PAC récepteur, utilisez l'Editeur de données de sécurité pour créer un tableau de 100 entiers (Array6) : 
13	Sur le PAC récepteur, dans une section de code de la tâche SAFE, instanciez le DFB S_RD_ETH_MX avec le tableau créé à l'étape 10 (Array5) comme paramètre d'entrée et le tableau créé à l'étape 12 (Array6) comme paramètre de sortie : 

Communication d'égal à égal par canal noir

Chaque transmission de données d'égal à égal se compose à la fois de *données de sécurité utilisateur*, comprenant le contenu lié à l'application qui est transmis, et de *données réservées*. Les *données réservées* sont utilisées par le PAC de sécurité pour tester la fiabilité de la transmission par rapport aux exigences du niveau SIL3. Elles comprennent les éléments suivants :

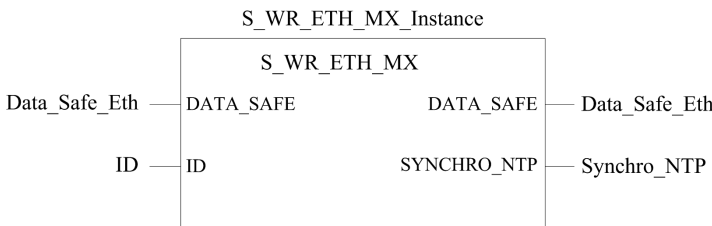
- CRC calculé par le PAC émetteur à partir des données à transmettre. Le PAC récepteur vérifie le CRC avant d'utiliser les données transmises.
- Identifiant de communication inclus dans le calcul de CRC, afin de favoriser la prévention des attaques par insertion et déguisement de bits lors de la transmission de données de sécurité.

- Horodatage de la transmission à la milliseconde près. Cette valeur s'appuie sur le service NTP et permet de synchroniser les PAC émetteur et récepteur. Le PAC émetteur de données ajoute une valeur d'horloge aux données envoyées au PAC récepteur. Le PAC récepteur compare l'horodatage reçu à sa propre valeur d'horloge, aux fins suivantes :
 - Vérifier l'ancienneté des données.
 - Rejeter les transmissions en double.
 - Déterminer l'ordre chronologique des transmissions reçues.
 - Déterminer le temps écoulé entre réceptions de données transmises.

Configuration du bloc de fonction dérivé (DFB, Derived Function Block) `S_WR_ETH_MX` dans la logique de programme du contrôleur récepteur

Représentation

Représentation du DFB :



Vous trouverez une description détaillée de ce DFB dans le document *EcoStruxure™ Control Expert - Sécurité, Bibliothèque de blocs*.

Description

Le DFB `S_WR_ETH_MX` est destiné aux contrôleurs utilisant le micrologiciel de version 3.10 ou antérieure. Il calcule les données (données réservées contenant un CRC et un horodatage) requises par le contrôleur récepteur pour vérifier et gérer les erreurs détectées pendant la communication d'égal à égal sécurisée.

Appelez le bloc fonction DFB `S_WR_ETH_MX` à chaque cycle dans le contrôleur expéditeur. Pendant le cycle, il est exécuté dans la logique une fois que toutes les modifications nécessaires ont été apportées aux données à envoyer. Cela signifie que les données à envoyer ne peuvent pas être modifiées pendant le cycle après l'exécution du DFB. Sinon,

les informations de CRC utilisées dans la zone des données réservées seront incorrectes et la communication d'égal à égal de sécurité échoue.

Affectez au paramètre ID une valeur unique qui identifie la communication d'égal à égal sécurisée entre un émetteur et un récepteur.



AVERTISSEMENT

PERTE DE LA CAPACITÉ À EXÉCUTER LES FONCTIONS DE SÉCURITÉ

La valeur du paramètre ID doit être unique et immuable dans le réseau pour une paire émetteur/récepteur.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Description du tableau DATA_SAFE

Utilisez les onglets **Interface** de l'**éditeur de données de sécurité** et de l'**éditeur de données de processus** dans Control Expert pour lier les variables de processus et les variables de sécurité.

Le processus de liaison et les variables de sécurité peuvent :

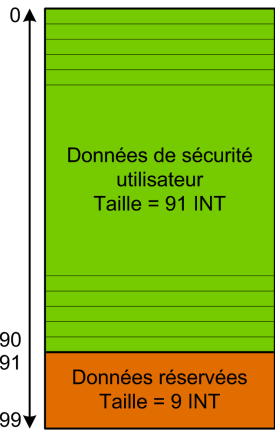
- transférer la valeur des variables de sécurité vers les variables de processus, via des variables globales associées ;
- envoyer des valeurs variables de la zone de processus du contrôleur émetteur vers la zone de processus du contrôleur récepteur, par messagerie explicite via Modbus TCP.

Le tableau DATA_SAFE est composé de deux zones :

- La zone **Données de sécurité utilisateur** contient les données de la zone de sécurité du contrôleur. Cette zone commence à l'indice 0 et se termine à l'indice 90.
- La zone **Données réservées** est réservée aux données de diagnostic générées automatiquement, dont la valeur CRC et l'horodatage. Le contrôleur récepteur utilise cette information d'horodatage pour déterminer si les données de la zone **Données de sécurité utilisateur** sont sûres ou non. Cette zone commence à l'indice 91 et se termine à l'indice 99.

NOTE: Aucune donnée ne doit être inscrite dans la zone **Données réservées**. L'écriture dans cette zone remplace les données de diagnostic générées automatiquement.

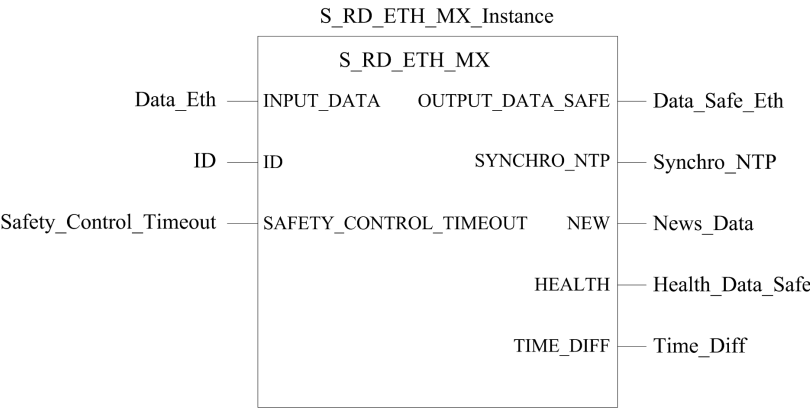
Représentation de la structure du tableau DATA_SAFE (array[0..99] of INT) :



Configuration du bloc DFB S_RD_ETH_MX dans la logique de programme du contrôleur récepteur

Représentation

Représentation du DFB :



Reportez-vous au *EcoStruxure™ Control Expert - Sécurité, Bibliothèque de blocs* pour une description détaillée de ce DFB.

Description

Le DFB `S_RD_ETH_MX` est destiné aux contrôleurs utilisant le micrologiciel de version 3.10 ou antérieure. Il copie les données reçues dans la zone de processus vers la zone de sécurité et valide l'exactitude des données reçues.

⚠️ AVERTISSEMENT

PERTE DE LA CAPACITÉ À EXÉCUTER LES FONCTIONS DE SÉCURITÉ

- Appelez le bloc fonction DFB `S_RD_ETH_MX` lors de chaque cycle dans la logique de programme du contrôleur récepteur avant que les données du cycle soient utilisées
- La valeur du paramètre `ID` doit être unique et immuable dans le réseau pour une paire émetteur/récepteur..
- Testez la valeur de bit `HEALTH` du code DFB `S_RD_ETH_MX` à chaque cycle avant d'utiliser toute donnée de sécurité pour gérer la fonction de sécurité.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Le bloc fonction `S_RD_ETH_MX` :

- copie les données du registre `INPUT_DATA` dans le registre `OUTPUT_DATA_SAFE` à condition que les tests suivants soient concluants :
 - Le bloc fonction vérifie le CRC du dernier paquet de données reçu, via le scrutateur d'E/S sur Ethernet (Modbus TCP). Si le CRC est incorrecte, les données sont considérées comme non sûres et ne sont pas inscrites dans le registre `OUTPUT_DATA_SAFE` de la zone de sécurité.
 - Le bloc fonction vérifie les dernières données reçues pour savoir si elles sont postérieures à celles inscrites dans le registre `OUTPUT_DATA_SAFE` de la zone de sécurité (en comparant les horodatages). Si les dernières données reçues ne sont pas plus récentes, elles ne sont pas copiées dans le registre `OUTPUT_DATA_SAFE` de la zone de sécurité.
- vérifie l'âge des données dans la zone de sécurité. Si l'âge est supérieur à la valeur maximale configurable définie dans le registre d'entrée `SAFETY_CONTROL_TIMEOUT`, les données sont déclarées non sûres et le bit `HEALTH` est défini sur 0.

NOTE: L'âge des données correspond à la différence entre l'heure à laquelle elles sont calculées dans le contrôleur émetteur et le moment où elles sont vérifiées dans le contrôleur récepteur. La référence horaire est mise à jour régulièrement en fonction de l'heure reçue d'un serveur NTP.

Si le bit `HEALTH` est réglé sur 0, les données disponibles dans le tableau `OUTPUT_DATA_SAFE` sont considérées non sûres. Vous devez alors réagir en conséquence.

Description des tableaux INPUT_DATA et OUTPUT_DATA_SAFE

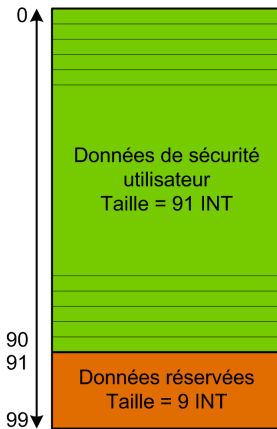
Les données du tableau INPUT_DATA proviennent de la zone mémoire des données de processus. Les tableaux OUTPUT_DATA_SAFE contiennent des variables de sécurité. Utilisez les onglets **Interface des données de sécurité** et **Interface des données de processus** de Control Expert pour établir le lien entre les variables de processus et les variables de sécurité.

Les tableaux INPUT_DATA et OUTPUT_DATA_SAFE comportent deux zones :

- La zone **Données de sécurité utilisateur** contient les données utilisateur. Cette zone commence à l'indice 0 et se termine à l'indice 90.
- La zone **Données réservées** est réservée aux données de diagnostic générées automatiquement, dont la valeur CRC et l'horodatage. Le contrôleur récepteur utilise cette information d'horodatage pour déterminer si les données de la zone **Données de sécurité utilisateur** sont sûres ou non. Cette zone commence à l'indice 91 et se termine à l'indice 99.

NOTE: Aucune donnée ne doit être inscrite dans la zone **Données réservées**. L'écriture dans cette zone remplace les données de diagnostic générées automatiquement.

Représentation de la structure des tableaux INPUT_DATA et OUTPUT_DATA_SAFE (array [0..99] of INT) :



Calcul d'une valeur SAFETY_CONTROL_TIMEOUT

Lors du calcul d'une valeur SAFETY_CONTROL_TIMEOUT, tenez compte des éléments suivants :

- valeur minimale: $\text{SAFETY_CONTROL_TIMEOUT} > T1$

- valeur type : $\text{SAFETY_CONTROL_TIMEOUT} > 2 * T1$

$T1 = \text{Temps de cycle MAST contrôleur}_{\text{émetteur}} + \text{Temps de cycle SAFE}_{\text{émetteur}} + \text{Période de répétition} + \text{Délai de transmission réseau} + \text{Temps de cycle MAST contrôleur}_{\text{récepteur}} + \text{Temps de cycle SAFE contrôleur}_{\text{récepteur}}$

Où :

- *Temps de cycle MAST contrôleur_{émetteur}* correspond au temps de cycle MAST du contrôleur émetteur.
- *Temps de cycle SAFE_{contrôleur émetteur}* correspond au temps de cycle SAFE du contrôleur émetteur.
- *Période de répétition* correspond à la période pendant laquelle le scrutateur d'E/S transmet la requête du contrôleur émetteur au contrôleur récepteur.
- *Délai de transmission réseau* correspond au délai nécessaire pour que les données soient transmises du contrôleur émetteur au contrôleur récepteur sur le réseau Ethernet.
- *Temps de cycle MAST contrôleur_{récepteur}* correspond au temps de cycle MAST du contrôleur récepteur.
- *Temps de cycle SAFE contrôleur_{récepteur}* correspond au temps de cycle SAFE du contrôleur récepteur.

La valeur attribuée au paramètre `SAFETY_CONTROL_TIMEOUT` a une incidence directe sur la fiabilité et la disponibilité de la communication poste à poste sécurisée. Lorsque la valeur `SAFETY_CONTROL_TIMEOUT` dépasse $T1$, la communication peut connaître des retards (à cause du réseau, par exemple) ou des données corrompues peuvent être transmises.

Configurez votre réseau Ethernet de manière que la charge n'entraîne pas un retard excessif sur le réseau lors de la transmission de données, sous peine de dépasser le délai imparti. Pour éviter que la communication poste à poste sécurisées ne subisse des retards excessifs dus à la transmission de données non sûres sur le même réseau, il est conseillé d'utiliser un réseau Ethernet dédié pour le protocole poste à poste sécurisé.

Lors de la mise en service du projet, estimez les performances des communications poste à poste de sécurité en vérifiant les valeurs du paramètre de sortie `TIME_DIFF` et en évaluant le temps restant en fonction du paramètre `SAFETY_CONTROL_TIMEOUT`.

Description du bit HEALTH

Lorsque le bit `HEALTH` est à :

- 1 : L'intégrité des données est correcte (CRC) et l'âge des données est inférieur à la valeur définie dans le registre d'entrée `SAFTETY_CONTROL_TIMEOUT`.

NOTE: L'âge des données correspond à l'écart entre :

- le début du cycle de calcul des données dans le contrôleur émetteur et
- le début du cycle de vérification des données dans le contrôleur récepteur.

- 0 : Aucune nouvelle donnée valide n'a été reçue dans l'intervalle indiqué (la temporisation est écoulée et le bit `HEALTH` est réglé sur 0).

NOTE: Lorsque le `HEALTH` est à 0, les données du tableau de sortie `OUTPUT_DATA_SAFE` sont considérées comme non sûres.

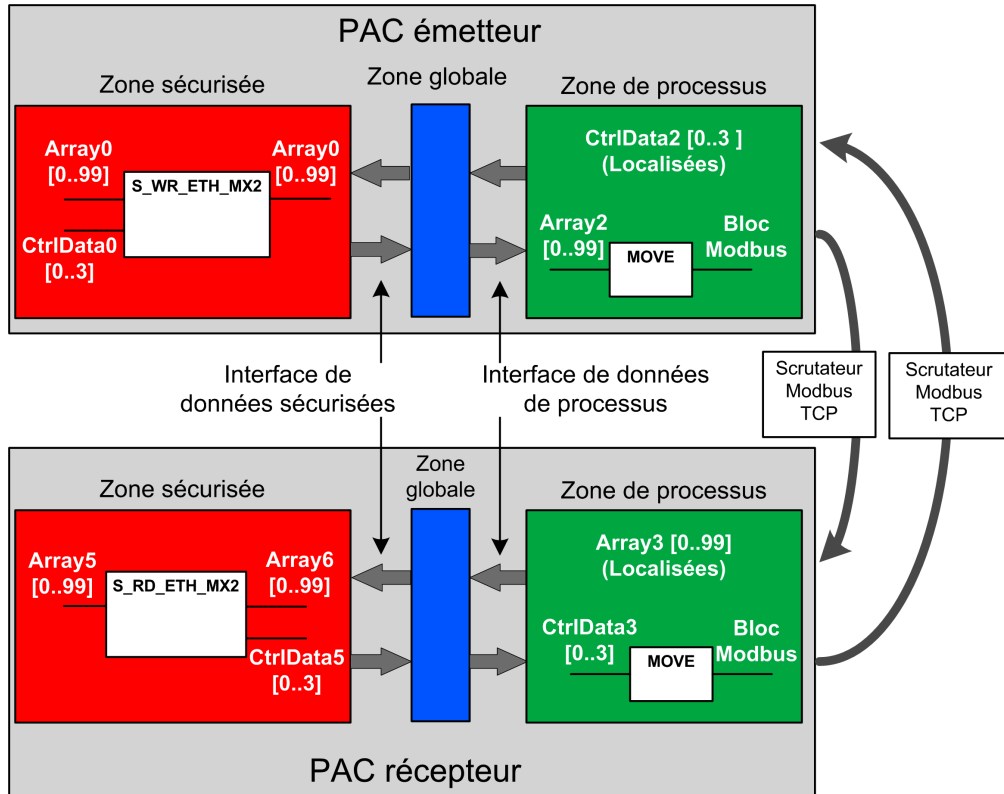
Architecture d'égal à égal avec micrologiciel d'UC de version 3.20 ou ultérieure

Conception de l'architecture

Avec un micrologiciel d'UC de version 3.20 ou ultérieure, l'architecture de la solution repose sur les éléments suivants :

- Exécution de 2 DFB (`S_WR_ETH_MX2` et `MOVE`) dans le PAC émetteur et de 2 DFB (`S_RD_ETH_MX2` et `MOVE`) dans le PAC récepteur.
- Scrutation via Modbus TCP pour le transport des données sécurisées de l'émetteur vers le récepteur.
- Scrutation via Modbus TCP pour le transport des données de contrôle du récepteur vers l'émetteur.

L'illustration suivante donne un aperçu du processus impliqué pour assurer la communication d'égal à égal de façon sécurisée :

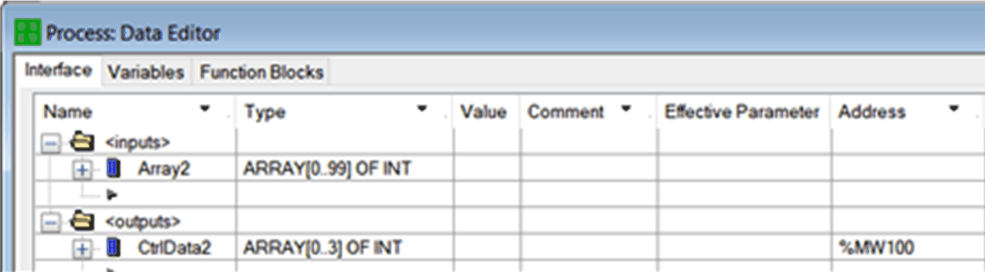
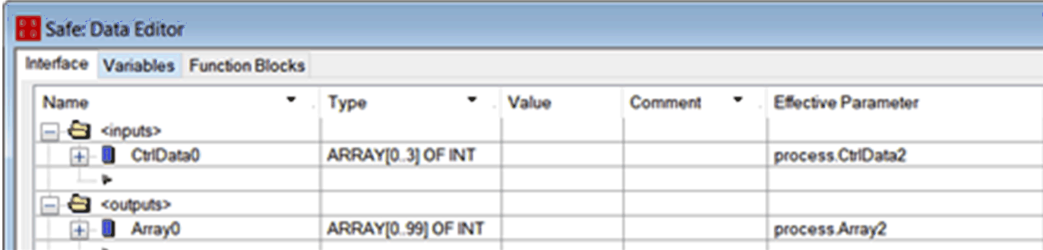
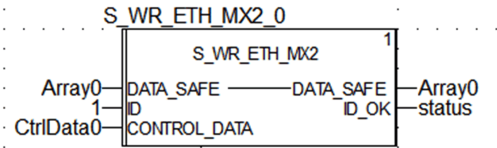


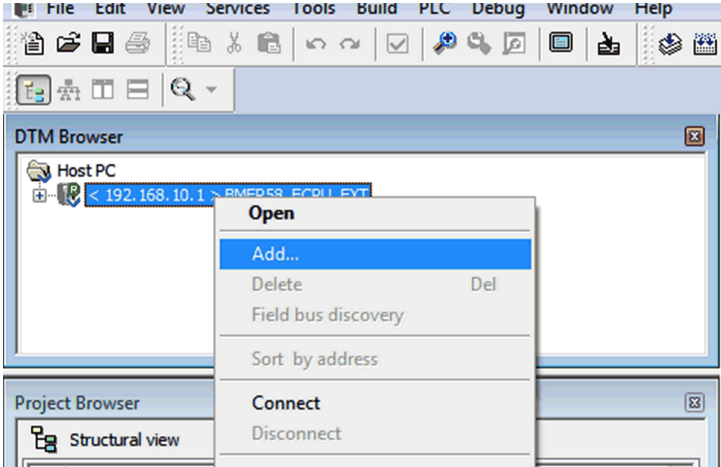
Dans la figure précédente, Control Expert crée automatiquement - et cache à toute vue externe – Array1 et Array4 dans les zones globales des PAC homologues. Du point de vue d'un utilisateur, les liaisons sont établies de Array0 à Array2 et de Array3 à Array5.

NOTE: Sur le réseau Ethernet, vous êtes autorisé à mélanger des données liées à la sécurité et des données hors sécurité sans impacter le niveau de sécurité des premières. Aucune restriction ne s'applique au réseau Ethernet lorsque la communication d'égal à égal sécurisée est utilisée.

Détails de la configuration du transfert de données d'égal à égal

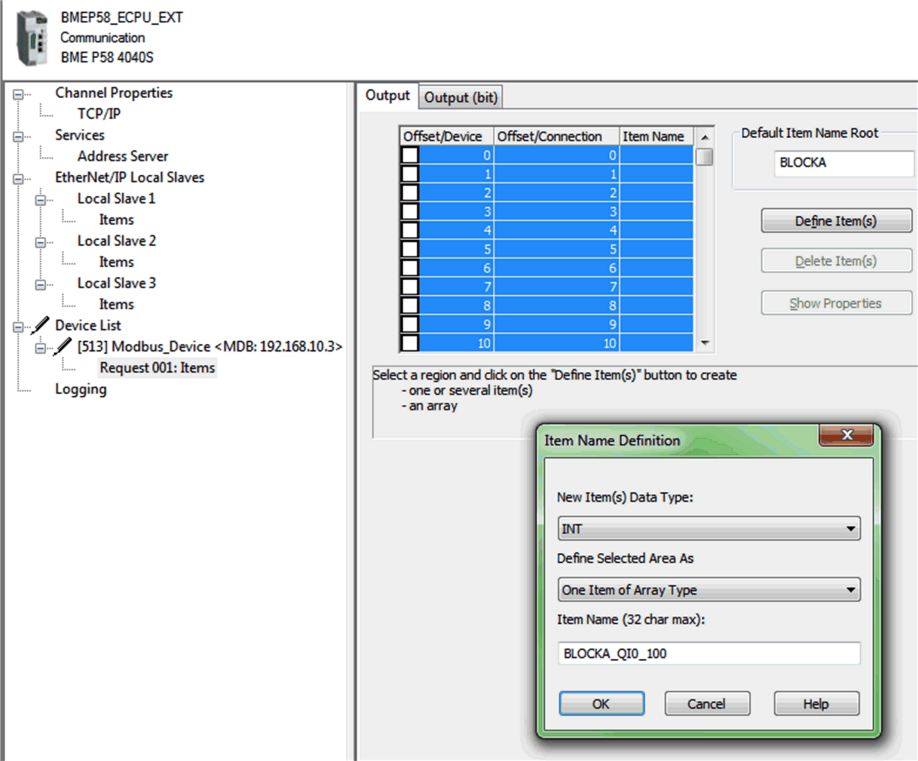
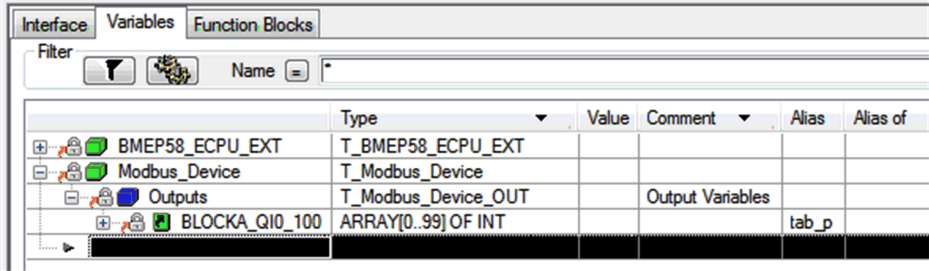
L'exemple suivant montre comment configurer un transfert de données d'égal à égal entre deux PAC de sécurité avec le micrologiciel d'UC de version 3.20 ou ultérieure et Control Expert 15.0 ou supérieur :

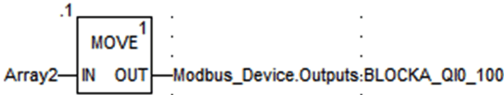
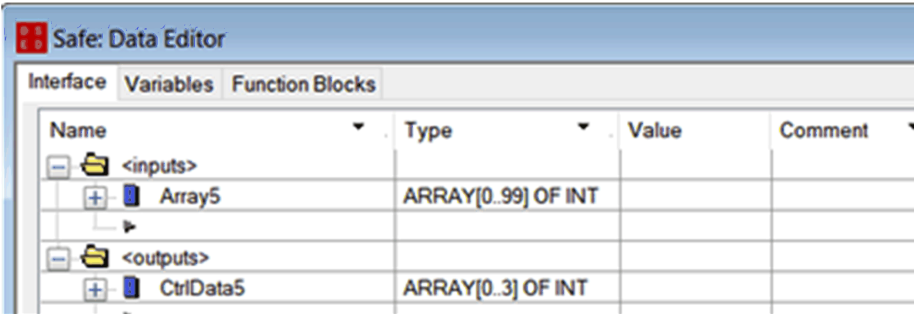
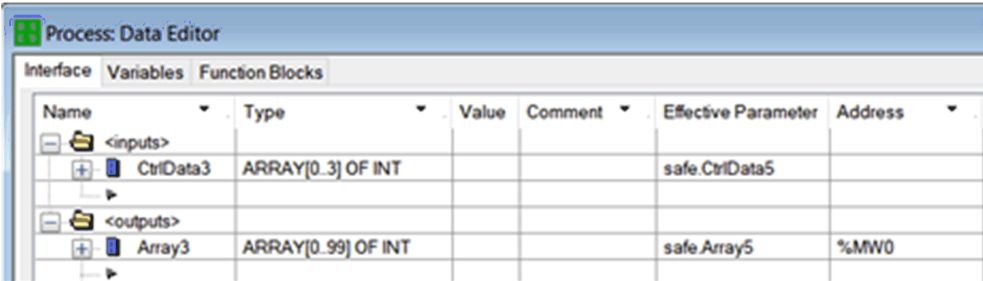
Eta-pe	Action
1	Sur le PAC émetteur, utilisez l'Editeur de données de processus pour créer un tableau de 100 entiers (Array2) en tant qu'entrée dans la zone Interface. Dans le même Editeur de données de processus, créez un tableau de 4 entiers (CtrlData2) en tant que sortie dans la zone Interface. Les données de contrôle envoyées par le PAC récepteur seront écrites dans le tableau CtrlData2 via le scrutateur Modbus, à condition que cette variable CtrlData2 soit située à l'adresse définie dans le scrutateur du PAC émetteur (%MW100 dans cet exemple - voir l'étape 4) : 
2	Sur le PAC émetteur, utilisez l'Editeur de données de sécurité pour créer un autre tableau de 100 entiers (Array0) en tant que sortie dans la zone Interface et liez ce tableau au tableau process.Array2 (créé à l'étape 1) dans la colonne Paramètre effectif. Dans le même Editeur de données de sécurité, créez un tableau de 4 entiers (CtrlData0) en tant qu'entrée dans la zone de sécurité Interface et liez ce tableau au tableau process.CtrlData2 (créé à l'étape 1) dans la colonne Paramètre effectif.  NOTE: Les variables de type entier indexées de 0 à 90 dans le tableau contiennent les valeurs des variables de sécurité que vous souhaitez échanger avec le PAC récepteur. La zone restante est réservée aux données de diagnostic générées automatiquement, dont la valeur CRC et l'horodatage. Ces données de diagnostic sont utilisées par le PAC récepteur pour déterminer si les données transférées sont sûres.
3	Sur le PAC émetteur, configurez le DFB S_WR_ETH_MX2 dans une section de la tâche SAFE. Liez ce DFB à Array0 et CtrlData0 : 

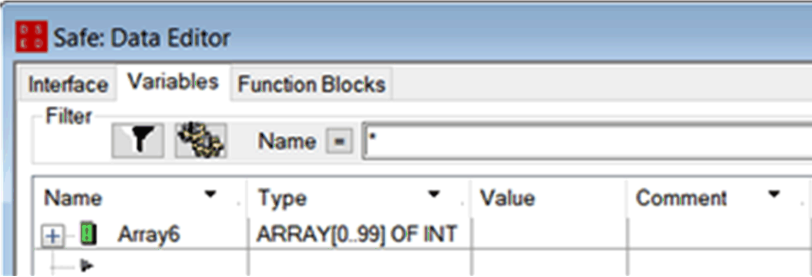
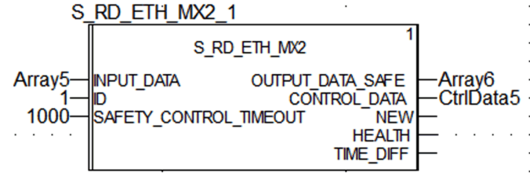
Eta-pe	Action
4	Dans le Navigateur de DTM du PAC émetteur, sélectionnez l'UC (pour cet exemple) ou un module de communications NOC (le cas échéant), puis cliquez sur Ajouter... pour créer un scrutateur Modbus qui puisse envoyer des données via Modbus TCP depuis le PAC émetteur vers le PAC récepteur : 
5	Sélectionnez Equipement Modbus et cliquez sur Ajouter un DTM pour ajouter le scrutateur Modbus :

6 Ouvrez l'équipement Modbus que vous venez d'ajouter puis effectuez les actions suivantes dans l'onglet **Configuration de requête** :

- Affectez la valeur 100 à la colonne **Longueur (écriture)** (il s'agit de la longueur des données à écrire), puis
- Renseignez la colonne **Adresse (écriture)**. Il s'agit de l'adresse à laquelle la table du PAC récepteur va écrire les données reçues (dans cet exemple : 0, ce qui signifie que le PAC émetteur va écrire dans la table à partir de %MW0 sur le PAC récepteur).

Eta-pe	Action
7	Sélectionnez le noeud Requête 001 : Eléments puis, dans l'onglet Sortie, définissez le type de tableau INT (soit ≥ 100 entiers). Il s'agit de la table du PAC émetteur qui sera écrite sur le PAC récepteur : 
8	Une fois la configuration enregistrée et générée, le bloc (BLOCKA_QI0_100 dans cet exemple) est automatiquement créé en tant que variable de processus : 

Eta-pe	Action
9	Sur le PAC émetteur, dans une section de code de processus, utilisez un DFB MOVE pour copier le contenu du tableau "tab_p" vers le tableau défini plus haut dans la structure de l'équipement Modbus : 
10	Sur le PAC récepteur, utilisez l'Editeur de données de sécurité pour créer un tableau de 100 entiers (Array5) en tant qu'entrée dans la zone Interface. Dans le même Editeur de données de sécurité, créez un tableau de 4 entiers (CtrlData5) en tant que sortie dans la zone Interface. 
11	Sur le PAC récepteur, utilisez l'Editeur de données de sécurité pour créer un tableau de 100 entiers (Array3) en tant que sortie de la zone Interface. Liez le tableau Array3 au tableau Array5 (créé à l'étape 10) dans la colonne Paramètre effectif. Les données en provenance du PAC émetteur seront écrites dans le tableau Array3 via le scrutateur Modbus, à condition que Array3 soit situé à l'adresse définie dans le scrutateur du PAC émetteur (%MW0 dans cet exemple). Dans le même Editeur de données de processus, créez un tableau de 4 entiers (CtrlData3) en tant qu'entrée dans la zone Interface. Liez le tableau CtrlData3 au tableau CtrlData5 (créé à l'étape 10) dans la colonne Paramètre effectif. 

Eta-pe	Action
12	Sur le PAC récepteur, utilisez l'Editeur de données de sécurité pour créer un tableau de 100 entiers (Array6) : 
13	Sur le PAC récepteur, dans une section de code de la tâche SAFE, instanciez le DFB S_RD_ETH_MX2 avec le tableau créé à l'étape 10 (Array5) en tant que paramètre d'entrée et avec les tableaux créés à l'étape 10 (CtrlData5) et à l'étape 12 (Array6) en tant que paramètres de sortie : 
14	Sur le PAC récepteur, répétez les étapes 4 à 9 pour configurer une communication de 4 entiers en vue d'envoyer le tableau CtrlData2 du PAC récepteur vers le PAC émetteur. Dans cet exemple, les données CtrlData doivent être écrites sur le PAC émetteur à l'adresse %MW100.

Communication d'égal à égal par canal noir

Chaque transmission de données d'égal à égal se compose à la fois de *données de sécurité utilisateur*, comprenant le contenu lié à l'application qui est transmis, et de *données réservées*. Les *données réservées* sont utilisées par le PAC de sécurité pour tester la fiabilité de la transmission par rapport aux exigences du niveau SIL3. Elles comprennent les éléments suivants :

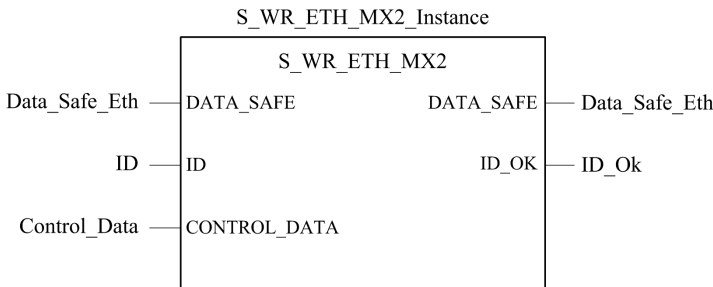
- CRC calculé par le PAC émetteur à partir des données à transmettre. Le PAC récepteur vérifie le CRC avant d'utiliser les données transmises.
- Identifiant de communication inclus dans le calcul de CRC, afin de favoriser la prévention des attaques par insertion et déguisement de bits lors de la transmission de données de sécurité.

- Horodatage de la transmission à la milliseconde près. Avec le micrologiciel d'UC de version 3.20 ou ultérieure, cet horodatage est la valeur horaire sécurisée fournie par l'UC du récepteur. Le PAC émetteur de données ajoute une valeur d'horloge aux données envoyées au PAC récepteur. Le PAC récepteur compare l'horodatage reçu à sa propre valeur d'horloge, aux fins suivantes :
 - Vérifier l'ancienneté des données.
 - Rejeter les transmissions en double.
 - Déterminer l'ordre chronologique des transmissions reçues.
 - Déterminer le temps écoulé entre réceptions de données transmises.

Configuration du bloc DFB S_WR_ETH_MX2 dans la logique de programme du contrôleur récepteur

Représentation

Représentation du bloc DFB :



Vous trouverez une description détaillée de ce bloc DFB dans le document *EcoStruxure™ Control Expert - Sécurité, Bibliothèque de blocs*.

Description

Le bloc DFB S_WR_ETH_MX2 s'applique aux contrôleurs utilisant le micrologiciel de version 3.20 ou ultérieure. Il calcule les données (données réservées contenant un contrôleur et un horodatage) requises par le récepteur pour vérifier et gérer les erreurs détectées pendant la communication d'égal à égal de sécurité.

NOTE: Lorsque vous configurez la communication de sécurité entre des contrôleurs de sécurité M580 et des contrôleurs de sécurité Quantum, utilisez les blocs fonction S_RD_ETH_MX, page 202 et S_WR_ETH_MX, page 200 au lieu des blocs fonction S_RD_ETH_MX2 et S_WR_ETH_MX2.

Appelez le bloc fonction DFB S_WR_ETH_MX2 à chaque cycle dans le contrôleur expéditeur. Pendant le cycle, il est exécuté dans la logique une fois que toutes les modifications nécessaires ont été apportées aux données à envoyer. Cela signifie que les données à envoyer ne peuvent pas être modifiées pendant le cycle après l'exécution du bloc DFB. Sinon, les informations de CRC utilisées dans la zone des données réservées sont incorrectes et la communication d'égal à égal de sécurité échoue.

Affectez au paramètre ID une valeur unique qui identifie la communication d'égal à égal sécurisée entre un émetteur et un récepteur.

⚠ AVERTISSEMENT

PERTE DE LA CAPACITÉ À EXÉCUTER LES FONCTIONS DE SÉCURITÉ

La valeur du paramètre ID doit être unique et immuable dans le réseau pour une paire émetteur/récepteur.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Description du tableau DATA_SAFE

Utilisez les onglets **Interface** de l'**éditeur de données de sécurité** et de l'**éditeur de données de processus** dans Control Expert pour lier les variables de processus et les variables de sécurité.

Le processus de liaison et les variables de sécurité peuvent :

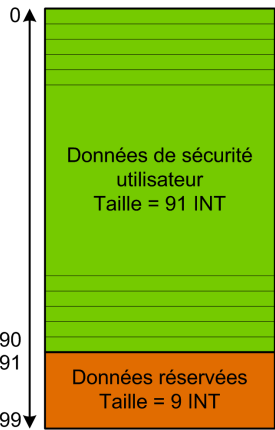
- transférer la valeur des variables de sécurité vers les variables de processus, via des variables globales associées ;
- envoyer des valeurs variables de la zone de processus du contrôleur émetteur vers la zone de processus du contrôleur récepteur, par messagerie explicite via Modbus TCP.

Le tableau DATA_SAFE est composé de deux zones :

- La zone **Données de sécurité utilisateur** contient les données de la zone de sécurité du contrôleur. Cette zone commence à l'indice 0 et se termine à l'indice 90.
- La zone **Données réservées** est réservée aux données de diagnostic générées automatiquement, dont la valeur CRC et l'horodatage. Le contrôleur récepteur utilise cette information d'horodatage pour déterminer si les données de la zone **Données de sécurité utilisateur** sont sûres ou non. Cette zone commence à l'indice 91 et se termine à l'indice 99.

NOTE: Aucune donnée ne doit être inscrite dans la zone **Données réservées**. L'écriture dans cette zone remplace les données de diagnostic générées automatiquement.

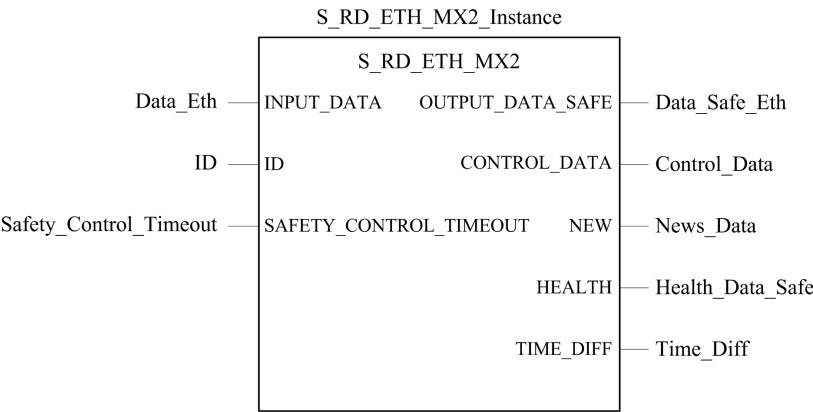
Représentation de la structure du tableau DATA_SAFE (array[0..99] of INT) :



Configuration du bloc de fonction dérivé (DFB, Derived Function Block) S_RD_ETH_MX2 dans la logique de programme du contrôleur d'automatisation programmable (PAC) récepteur

Représentation

Représentation du DFB :



Reportez-vous au *EcoStruxure™ Control Expert - Sécurité, Bibliothèque de blocs* pour une description détaillée de ce DFB.

Description

Le bloc DFB `S_RD_ETH_MX2` s'applique aux contrôleurs d'automatisation programmables (PAC) utilisant le micrologiciel de CPU de version 3.20 ou ultérieure. Il copie les données reçues dans la zone de processus vers la zone de sécurité et valide l'exactitude des données reçues.

NOTE: Lorsque vous configurez la communication de sécurité entre des CPU de sécurité M580 et des CPU de sécurité Quantum, utilisez les blocs fonction `S_RD_ETH_MX`, page 202 et `S_WR_ETH_MX`, page 200 au lieu des blocs fonction `S_RD_ETH_MX2` et `S_WR_ETH_MX2`.

AVERTISSEMENT

PERTE DE LA CAPACITÉ À EXÉCUTER LES FONCTIONS DE SÉCURITÉ

- Le bloc fonction DFB `S_RD_ETH_MX2` doit être appelé lors de chaque cycle dans la logique de programme du contrôleur d'automatisation programmable (PAC) récepteur et il doit être exécuté avant que les données du cycle soient utilisées
- La valeur du paramètre `ID` doit être unique et immuable dans le réseau pour une paire émetteur/récepteur..
- Testez la valeur de bit `HEALTH` du code DFBS `S_RD_ETH_MX2` à chaque cycle avant d'utiliser toute donnée sûre pour gérer la fonction de sécurité.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Le bloc fonction `S_RD_ETH_MX2` :

- copie les données du registre `INPUT_DATA` dans le registre `OUTPUT_DATA_SAFE` à condition que les tests suivants soient concluants :
 - Le bloc fonction vérifie la CRC du dernier paquet de données reçu, via le scrutateur d'E/S sur Ethernet (Modbus TCP). Si la CRC est incorrecte, les données sont considérées comme non sûres et ne sont pas inscrites dans le registre `OUTPUT_DATA_SAFE` de la zone de sécurité.
 - Le bloc fonction vérifie les dernières données reçues pour savoir si elles sont postérieures à celles inscrites dans le registre `OUTPUT_DATA_SAFE` de la zone de sécurité (en comparant les horodatages). Si les dernières données reçues ne sont pas plus récentes, elles ne sont pas copiées dans le registre `OUTPUT_DATA_SAFE` de la zone de sécurité.

- vérifie l'âge des données dans la zone de sécurité. Si l'âge est supérieur à la valeur maximale configurable définie dans le registre d'entrée `SAFETY_CONTROL_TIMEOUT`, les données sont déclarées non sûres et le bit `HEALTH` est défini sur 0.

NOTE: L'âge des données correspond à la différence entre l'heure à laquelle elles sont calculées dans le contrôleur d'automatisation programmable (PAC) émetteur et l'heure à laquelle elles sont vérifiées dans le contrôleur d'automatisation programmable (PAC) récepteur.

Si le bit `HEALTH` est réglé sur 0, les données disponibles dans le tableau `OUTPUT_DATA_SAFE` sont considérées comme non sûres. Vous devez alors réagir en conséquence.

Description des tableaux `INPUT_DATA` et `OUTPUT_DATA_SAFE`

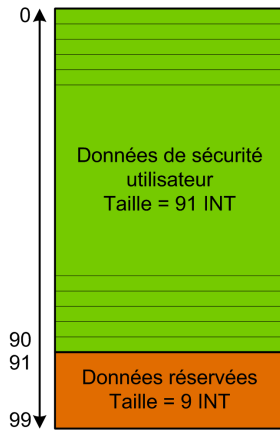
Les données du tableau `INPUT_DATA` proviennent de la zone mémoire des données de processus. Les tableaux `OUTPUT_DATA_SAFE` contiennent des variables de sécurité. Utilisez les onglets **Interface des données de sécurité** et **Interface des données de processus** de Control Expert pour établir le lien entre les variables de processus et les variables de sécurité.

Les tableaux `INPUT_DATA` et `OUTPUT_DATA_SAFE` comportent 2 zones :

- La zone **Données de sécurité utilisateur** contient les données utilisateur. Cette zone commence à l'indice 0 et se termine à l'indice 90.
- La zone **Données réservées** est réservée aux données de diagnostic générées automatiquement, dont la valeur CRC et l'horodatage. Le contrôleur d'automatisation programmable (PAC) récepteur utilise cette information d'horodatage pour déterminer si les données de la zone **Données de sécurité utilisateur** sont sûres ou non. Cette zone commence à l'indice 91 et se termine à l'indice 99.

NOTE: Aucune donnée ne doit être inscrite dans la zone **Données réservées**. L'écriture dans cette zone remplace les données de diagnostic générées automatiquement.

Représentation de la structure des tableaux `INPUT_DATA` et `OUTPUT_DATA_SAFE` (array [0..99] of INT) :



Description du tableau `CONTROL_DATA`

Le tableau `CONTROL_DATA` doit être lié à des variables de la zone "globale" (définies via l'interface de données de sécurité), puis les variables "globales" doivent être liées à des variables localisées de la zone "processus" (définies via l'interface de données de processus) pour que les données soient envoyées par le scrutateur d'E/S à l'expéditeur correspondant.

Calcul d'une valeur `SAFETY_CONTROL_TIMEOUT`

Lors du calcul d'une valeur `SAFETY_CONTROL_TIMEOUT`, tenez compte des éléments suivants :

- Valeur minimale : $\text{SAFETY_CONTROL_TIMEOUT} > 2 * T1$
- Valeur type : $\text{SAFETY_CONTROL_TIMEOUT} > 3 * T1$

$T1 = \text{Temps de cycle MAST UC}_{\text{émettrice}} + \text{Temps de cycle SAFE UC}_{\text{émettrice}} + \text{Période de répétition} + \text{Délai de transmission réseau} + \text{Temps de cycle MAST UC}_{\text{réceptrice}} + \text{Temps de cycle SAFE UC}_{\text{réceptrice}}$

Où :

- *Temps de cycle MAST UC_{émettrice}* correspond au temps de cycle MAST du contrôleur d'automatisation programmable (PAC) émetteur.
- *Temps de cycle SAFE UC_{émettrice}* correspond au temps de cycle SAFE du contrôleur d'automatisation programmable (PAC) émetteur.

- *Période de répétition* correspond à la période pendant laquelle le scrutateur d'E/S transmet la requête du contrôleur d'automatisation programmable (PAC) émetteur au contrôleur d'automatisation programmable (PAC) récepteur.
- *Délai de transmission réseau* correspond au délai nécessaire pour que les données soient transmises du contrôleur d'automatisation programmable (PAC) émetteur au contrôleur d'automatisation programmable (PAC) récepteur sur le réseau Ethernet.
- *Temps de cycle MAST UC_{réceptrice}* correspond au temps de cycle MAST du contrôleur d'automatisation programmable (PAC) récepteur.
- *Temps de cycle SAFE UC_{réceptrice}* correspond au temps de cycle SAFE du contrôleur d'automatisation programmable (PAC) récepteur.

La valeur attribuée au paramètre `SAFETY_CONTROL_TIMEOUT` a une incidence directe sur la fiabilité et la disponibilité de la communication poste à poste sécurisée. Lorsque la valeur `SAFETY_CONTROL_TIMEOUT` dépasse trop largement T1, la communication peut connaître des retards (à cause du réseau, par exemple) ou des données corrompues peuvent être transmises.

Configurez votre réseau Ethernet de manière que la charge n'entraîne pas un retard excessif sur le réseau lors de la transmission de données, sous peine de dépasser le délai imparti. Pour éviter que les communications poste à poste sécurisées ne subissent des retards excessifs dus à la transmission de données non sûres sur le même réseau, il est conseillé d'utiliser un réseau Ethernet dédié pour le protocole poste à poste sécurisé.

Lors de la mise en service du projet, estimez les performances des communications poste à poste sécurisées en vérifiant les valeurs du paramètre de sortie `TIME_DIFF` et en évaluant le temps restant en fonction du paramètre `SAFETY_CONTROL_TIMEOUT`.

Description du bit HEALTH

Lorsque le bit `HEALTH` est à :

- 1 : L'intégrité des données est correcte (CRC) et l'âge des données est inférieur à la valeur définie dans le registre d'entrée `SAFETY_CONTROL_TIMEOUT`.

NOTE: L'âge des données correspond à l'écart entre :

- le début du cycle de calcul des données dans le contrôleur d'automatisation programmable (PAC) émetteur et
 - le début du cycle de vérification des données dans le contrôleur d'automatisation programmable (PAC) récepteur.
- 0 : Aucune nouvelle donnée valide n'a été reçue dans l'intervalle indiqué (la temporisation est écoulée et le bit `HEALTH` est réglé sur 0).

NOTE: Lorsque le `HEALTH` est à 0, les données du tableau de sortie `OUTPUT_DATA_SAFE` sont considérées comme non sûres. Prenez alors les mesures qui s'imposent.

Communications par canal noir M580

Canal noir

Un canal noir est un mécanisme permettant de chiffrer et valider les données de sécurité transmises :

- Seuls les équipements de sécurité Schneider Electric peuvent chiffrer et déchiffrer les données envoyées via le canal noir dans un système de sécurité M580.
- L'intégrité de chaque transmission de données de sécurité est testée par les deux modules de sécurité d'envoi et de réception, pour chaque message transmis.

L'intérêt du canal noir est de permettre la transmission de données de sécurité via des équipements intermédiaires non liés à la sécurité, notamment des embases, des câbles Ethernet, des adaptateurs de communication, etc. Les transmissions par canal noir étant chiffrées, les équipements intermédiaires ne peuvent pas lire ni modifier les contenus de sécurité transmis sans être détectés.

Les transmissions par canal noir se font indépendamment du protocole de communication utilisé :

- X Bus est la porteuse utilisée pour les transmissions par embase entre les équipements de sécurité d'une même embase (par exemple du contrôleur la CPU vers les modules d'E/S locales ou d'un adaptateur distant de communication (CRA) vers les modules d'E/S locales).
- EtherNet/IP est la porteuse utilisée pour les transmissions de données entre les embases (par exemple, depuis le contrôleur vers un module adaptateur CRA).

Les modules d'E/S de sécurité et le contrôleur peuvent envoyer et recevoir des communications par canal noir. Pour chaque transmission, l'équipement émetteur (contrôleur ou module d'E/S) ajoute les informations suivantes au message :

- une balise CRC permettant de tester le contenu du message
- un horodatage permettant de tester la ponctualité du message
- d'autres informations (notamment la version de l'application et la configuration de modules d'E/S utilisés) qui identifient le module d'E/S dans la transmission.

Avec un micrologiciel de contrôleur de version 3.10 ou antérieure et des modules d'E/S de sécurité sur une embase distante, configurez le contrôleur en tant que client NTP ou serveur NTP.

Si aucune de ces configurations n'est mise en œuvre, les horloges des modules d'E/S de sécurité et du contrôleur ne sont pas synchronisées, et la communication par canal noir ne fonctionne pas correctement. Les entrées et sorties des modules d'E/S de sécurité dans les stations d'E/S distantes (RIO) passent à l'état sécurisé défini (non alimenté) ou l'état de repli.

NOTE: Si vous installez des modules d'E/S de sécurité dans une station d'E/S distante, configurez l'heure du contrôleur avec le micrologiciel de version 3.10 ou antérieure. Activez le service NTP pour votre système M580 et configurez le contrôleur de sécurité en tant que serveur NTP ou client NTP.

L'équipement récepteur (E/S ou contrôleur) déchiffre le message et teste l'exactitude de son contenu. Les conditions suivantes peuvent être détectées :

Condition	Description
Erreurs de transmission	Erreur détectée dans l'adresse ou le routage du message.
Répétitions	Message envoyé plusieurs fois.
Données supprimées	Il manque une partie du message ou le message est perdu.
Données insérées	Des données ont été ajoutées au message.
Séquence des données incorrecte	L'ordre du message a été modifié.
Données corrompues	Une erreur de bit au moins est détectée dans le message.
Retards	Le délai de livraison du message est excessivement long.
Déguisement	La source du message n'est pas autorisée à envoyer les données.

Lorsque ces erreurs sont détectées, le canal est déclaré non intègre et la fonction de sécurité appropriée est exécutée :

- Si le contrôleur détecte qu'une transmission en provenance d'un module d'entrée n'est pas intègre, il fait passer les valeurs d'entrée de ce module à l'état sécurisé défini (non alimenté) ou à l'état de repli.
- Si un module de sortie détecte qu'une transmission en provenance du contrôleur n'est pas intègre, il place ses sorties dans leur état de repli préconfiguré.

Les sorties prennent automatiquement l'état commandé par le contrôleur, dès que la communication entre le contrôleur et le module de sortie est correctement rétablie.

AVIS
CHANGEMENT INATTENDU D'ETAT DES SORTIES LORS DU RETABLISSEMENT DE LA COMMUNICATION Surveillez l'état des canaux de sortie et activer la fonction de sécurité en conséquence, en faisant passer les commandes de sorties à l'état sécurisé défini. Le non-respect de ces instructions peut provoquer des dommages matériels.

Communication de l'UC M580 vers les E/S de sécurité

Introduction

Cette section décrit les communications entre l'UC de sécurité M580 et les modules d'E/S de sécurité.

M580 Communications entre PAC de sécurité et E/S

Communication entre PAC et E/S

L'UC et le coprocesseur de sécurité M580 contrôlent ensemble tous les échanges de l'embase, tandis que les E/S de sécurité répondent aux commandes de l'UC et du coprocesseur. Les modules d'E/S de sécurité peuvent être installés dans un rack X Bus BMXXBP**** ou dans un rack Ethernet BMEXBP****.

Les communications entre le PAC de sécurité et les modules d'E/S de sécurité du rack principal local passent par l'embase.

Les communications entre le PAC de sécurité et les modules d'E/S de sécurité installés dans une station distante (RIO) passent par un module adaptateur installé sur la station d'E/S distante (RIO), à savoir :

- adaptateur BMEXBP**** pour un rack Ethernet
- adaptateur BMXXBP**** pour un rack X Bus

NOTE: Avec un micrologiciel d'UC de version 3.20 ou ultérieure, le module d'adaptation BM•CRA31210 a besoin d'un micrologiciel de version 2.60 ou supérieure.

NOTE: Un adaptateur BMXXBP**** ne peut pas être utilisé pour connecter des modules d'E/S de sécurité au PAC de sécurité M580.

Les communications en provenance du PAC de sécurité et des modules d'E/S de sécurité (dans le rack principal local ou dans une station RIO) passent par le [canal noir](#), [page 221](#).

La manière de synchroniser les réglages horaires de l'UC et des modules d'E/S de sécurité dépend de la version de micrologiciel de l'UC :

- Pour les PAC équipés d'un micrologiciel d'UC de version 3.10 ou antérieure, la configuration du service NTP est requise.

NOTE: Si vous installez des modules d'E/S de sécurité sur le rack local (ou une extension de celui-ci), il n'est pas nécessaire d'activer le service NTP.

- Pour les PAC équipés d'un micrologiciel d'UC de version 3.20 ou ultérieure, la synchronisation horaire sécurisée s'appuie sur une horloge interne et "monotone".

Pour plus d'informations, reportez-vous au chapitre *Synchronisation horaire*, page 185.

Vous pouvez éventuellement utiliser des modules répéteurs à fibre optique BMXNRP0200 ou BMXNRP0201 pour étendre la liaison physique entre l'UC et Copro du rack local et l'adaptateur installé dans la station d'E/S distante (RIO). Ces modules améliorent l'immunité au bruit du réseau d'E/S distantes (RIO) et permettent d'augmenter la distance de câblage tout en conservant l'intégralité de la plage dynamique du réseau et le niveau d'intégrité de la sécurité.

Le protocole de communication assure les échanges entre E/S et PAC de sécurité. Il permet aux deux équipements de vérifier l'exactitude des données reçues, de détecter les données corrompues et de déterminer si le module émetteur cesse d'être opérationnel. Une boucle de sécurité peut ainsi inclure toute embase et tout adaptateur RIO non parasite, page 34.

Alimentation des E/S de sécurité

Les E/S de sécurité sont alimentées en 24 VCC et 3,3 VCC via l'embase par le module d'alimentation de sécurité, page 135M580. Le module d'alimentation de sécurité surveille la tension qu'il fournit pour qu'elle ne dépasse pas 36 VCC.

Alimentation des fonctions non liées à la sécurité :

Chaque module d'E/S de sécurité applique à ses fonctions non liées à la sécurité la tension 5 VCC fournie par l'embase.

Alimentation externe des E/S de sécurité numériques :

Une alimentation externe, inférieure ou égale à 60 VCC, est requise pour les processus non liés à la sécurité (capteur, actionneur) et peut être une alimentation de type II de surtension de catégorie II très basse tension de protection (TBTS/TBTP). L'alimentation des processus non liés à la sécurité est supervisée par le module d'E/S de sécurité qui détecte les condition de tension excessive ou insuffisante.

Diagnostics d'un système de sécurité M580

Présentation

Ce chapitre fournit des informations sur les diagnostics qui peuvent être établis à l'aide d'indicateurs matériels (état des voyants) et de bits ou de mots système pour un système de sécurité M580.

Diagnostics de l'UC et du coprocesseur de sécurité M580

Introduction

Cette section décrit les diagnostics disponibles pour les UC de sécurité BME•58•040S et le coprocesseur de sécurité BMEP58CPROS3.

Diagnostic de la condition bloquante

Introduction

Les conditions bloquantes qui se produisent pendant l'exécution du programme de sécurité ou du programme de processus sont dues à la détection d'erreurs système ou à l'état HALT d'une tâche dans laquelle l'erreur a été détectée.

NOTE: Le contrôleur de sécurité M580 peut être dans deux états HALT indépendants :

- L'état HALT de processus s'applique aux tâches non liées à la sécurité (MAST, FAST, AUX0 et AUX1) Si une tâche de processus passe à l'état HALT, toutes les autres tâches de processus passent à l'état HALT.
- L'état SAFE HALT s'applique uniquement à la tâche SAFE.

Reportez-vous à la section *États de fonctionnement du contrôleur de sécurité M580*, page 273 pour obtenir la description des états HALT et STOP.

Diagnostics

Lorsque le contrôleur détecte une condition bloquante entraînant une erreur système, l'erreur détectée est décrite dans le mot système %SW124.

Lorsque le contrôleur détecte une condition bloquante entraînant un état HALT, l'erreur détectée est décrite dans le mot système %SW125.

Valeurs du mot système %SW124 et description de la condition bloquante détectée correspondante :

Valeur (hex) %SW124	Description de la condition bloquante
5AF2	Erreur RAM détectée dans la vérification de mémoire
5AFB	Erreur détectée dans le code du micrologiciel de sécurité
5AF6	Débordement de chien de garde de sécurité détecté sur le contrôleur

Valeur (hex) %SW124	Description de la condition bloquante
5AFF	Détection d'un dépassement du chien de garde de sécurité sur le coprocesseur
5B01	Coprocesseur non détecté au démarrage

Valeurs du mot système %SW125 et description de la condition bloquante détectée correspondante :

Valeur (hex) %SW125	Description de la condition bloquante
0...	exécution d'une fonction indéterminable
0002	Fonctionnalité de signature de la carte SD (utilisée avec les fonctions <i>SIG_CHECK</i> et <i>SIG_WRITE</i>)
2258	Exécution de l'instruction HALT
2259	Flux d'exécution différent du flux de référence
23..	Exécution d'une fonction CALL vers un sous-programme non défini
5AF3	erreur de comparaison détectée par le contrôleur
5AF9	Erreur d'instruction détectée au démarrage ou pendant l'exécution
5AFA	Erreur de comparaison détectée sur la valeur CRC
5AFC	Erreur de comparaison détectée par le coprocesseur
5AFD	Erreur interne détectée par le coprocesseur, sous-code dans %SW126 : 1 (résultat inconnu), 2 (application du CRC), 7 (compteur d'activités incorrect)
5AFE	Erreur de synchronisation du coprocesseur - contrôleur uniquement ; sous-code dans %SW126 : 3 (diagnostic), 4 (fin UL), 5 (comparaison), 6 (BC out), 8 (HALT pendant UL), 9 HALT pendant comparaison), 10 (HALT pendant BC out).
81F4	Nœud SFC incorrect
82F4	Code SFC inaccessible
83F4	Espace de travail SFC inaccessible
84F4	Trop d'étapes SFC initiales
85F4	Trop d'étapes SFC actives
86F4	Code de séquence SFC incorrect
87F4	Description de code SFC incorrecte
88F4	Table de référence SFC incorrecte
89F4	Erreur détectée de calcul de l'index interne SFC
8AF4	Etat d'une étape SFC non disponible
8BF4	Mémoire SFC trop petite après changement dû à un téléchargement

Valeur (hex) %SW125	Description de la condition bloquante
8CF4	Section transition/action inaccessible
8DF4	Espace de travail SFC trop petit
8EF4	Version du code SFC plus ancienne que l'interpréteur
8FF4	Version du code SFC plus récente que l'interpréteur
90F4	Mauvaise description d'un objet SFC : pointeur NULL
91F4	Identificateur d'action non autorisé
92F4	Mauvaise définition du temps pour un identificateur d'action
93F4	Etape macro introuvable dans la liste des étapes actives pour désactivation
94F4	Dépassement (overflow) dans la table des actions
95F4	Dépassement (overflow) dans la table d'activation/désactivation des étapes
9690	Erreur détectée dans le CRC de l'application (somme de contrôle)
DE87	Erreur de virgule flottante détectée dans le calcul
DEB0	Dépassement de watchdog de tâche (%S11 et %S19 sont définis)
DEF0	Division par 0
DEF1	Erreur détectée de transfert d'une chaîne de caractères
DEF2	Dépassement de capacité
DEF3	Débordement de l'index
DEF4	Périodes de tâche incohérentes
DEF7	Erreur détectée d'exécution SFC
DEFE	Étapes SFC non définies

Redémarrage de l'application

A la suite d'une condition bloquante, il est nécessaire d'initialiser les tâches en état HALT. Selon que l'état HALT concerne :

- une tâche de processus (MAST, FAST, AUX0, ou AUX1) : l'initialisation est effectuée soit par la commande Control Expert contrôleur **Init** soit en réglant le bit %S0 sur 1.
- Tâche SAFE, l'initialisation est effectuée par la commande contrôleur Control Expert **Init Safety**.

Lors de l'initialisation, l'application se comporte comme suit :

- les données reprennent leur valeur initiale.

- les tâches sont arrêtées en fin de cycle,
- l'image des entrées est actualisée,
- les sorties sont commandées en position de repli.

La commande RUN redémarre l'application ou les tâches.

Diagnostics de condition non bloquante

Introduction

Le système rencontre une condition non bloquante lorsqu'il détecte une erreur d'entrée/sortie sur le bus de l'embase (X Bus ou Ethernet) ou via l'exécution d'une instruction, qui peut être traitée par le programme utilisateur et ne modifie pas l'état fonctionnel du contrôleur.

Cette section décrit quelques-uns des bits et mots système que vous pouvez utiliser pour détecter l'état du système de sécurité et des modules qui le composent.

NOTE: Les bits et mots système disponibles ne comprennent pas toutes les informations relatives à l'état des modules de sécurité. Utilisez la structure DDDT du contrôleur de sécurité et des modules d'E/S de sécurité pour déterminer l'état du système de sécurité M580.

Pour plus d'informations sur le DDDT du contrôleur de sécurité M580, reportez-vous à la rubrique *Structure de type des données dérivé (DDT, Derived Data Type) autonome pour contrôleurs M580* dans le document *Modicon M580 - Matériel - Manuel de référence*.

Pour plus d'informations sur les DDDT des modules d'E/S de sécurité M580, reportez-vous aux sections suivantes :

- Structure des données du BMXSAI0410, page 66 pour le module d'entrée analogique de sécurité
- Structure des données du BMXSDI1602, page 98 pour le module d'entrée numérique de sécurité
- Structure des données du BMXSDO0802, page 113 pour le module de sortie numérique de sécurité
- Structure des données du BMXSRA0405, page 130 pour le module de sortie relais numérique de sécurité

NOTE: Vous pouvez établir des diagnostics avancés des dispositifs Ethernet au moyen de messages explicites. Pour cela, utilisez au choix :

- Le bloc fonction bloc fonction READ_VAR (voir EcoStruxure™ Control Expert, Communication, Block Library) pour les équipements Modbus TCP

- Le bloc fonction DATA_EXCH (voir Modicon M580, Matériel, Manuel de référence), indique le protocole CIP dans le bloc ADDM, pour les équipements EtherNet/IP

Conditions liées aux diagnostics d'E/S

Une condition non bloquante liée aux E/S est diagnostiquée avec les indications suivantes :

- combinaison du voyant LED I/O du contrôleur : allumé fixe
- combinaison du voyant LED I/O : allumé fixe
- bits système (type de l'erreur détectée) :
 - %S10 %S10 à 0 : erreur d'E/S globale détectée sur un des modules dans l'embase Ethernet ou X Bus locale ou distante
 - %S16 réglé sur 0 : erreur d'E/S détectée dans la tâche en cours sur une embase X Bus
 - %S40...%S47 réglé sur 0 : erreur d'E/S détectée sur une embase X Bus à l'adresse 0 à 7
 - %S117 réglé sur 0 : erreur RIO détectée sur une embase de bus X distante
 - %S119 réglé sur 0 : erreur I/O détectée sur une embase de bus X locale

NOTE: Ces bits (%S10, %S16, %S40...%S47, %S117, et %S119) signalent de nombreuses erreurs détectées liées aux modules d'E/S de sécurité.
- bits et mots système combinés avec le canal qui présente une erreur détectée (numéro de canal d'E/S et type d'erreur détectée) ou informations d'Device DDT du module I/O (pour les modules configurés en mode d'adressage l'Device DDT) :
 - %Ir.m.c.ERR bit à 1 : erreur de canal détectée (échanges implicites)
 - %MWr.m.c.2 : la valeur de ce mot précise le type de l'erreur détectée sur le canal indiqué et dépend du module d'E/S (échanges implicites)

Conditions liées à l'exécution du diagnostic du programme

Une condition non bloquante liée à l'exécution du programme est diagnostiquée par les bits et mots système suivants :

- Bits système – type de l'erreur détectée :
 - %S15 réglé sur 1 : Erreur de manipulation de chaîne de caractères détectée.
 - %S18 réglé sur 1 : Débordement de capacité, erreur détectée sur flottant ou division par 0
(Reportez-vous à la section *Bits système pour l'exécution de tâche SAFE*, page 417 pour plus d'informations.)
Lorsque %S18 est réglé à 1, %SW17 contient une description de l'événement en cause, page 419.
 - %S20 réglé à 1 : Débordement de l'index.
NOTE: Si le bit système configurable %S78 est défini dans le programme, la tâche SAFE passe à l'état HALT lorsque le bit système %S18 est réglé à 1.
- Mot système – nature de l'erreur détectée :
 - %SW125 (see Modicon M580, Hardware, Reference Manual) (toujours mis à jour)

Diagnostics par voyant LED de la CPU de sécurité du M580

Voyants LED de la CPU

Utilisez les voyants LED situés sur la face avant de la CPU (voir Modicon M580 - Guide de planification du système de sécurité), pour des diagnostics généraux sur l'état du contrôleur d'automatisation programmable (PAC) pendant la mise en service ou le dépannage.

 **AVERTISSEMENT**

RISQUE DE DIAGNOSTIC SYSTEME INEXACT
Ne pas utiliser les voyants LED comme des indicateurs de fonctionnement.
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Dans le *Modicon M580 - Redondance d"UC, Guide de planification du système pour architectures courantes*, consultez la rubrique *Diagnostics par voyant LED de la CPU redondante M580* pour savoir comment diagnostiquer les voyants LED en lien avec la redondance, dont [A], [B], [PRIM], [STBY] et [REMOTE RUN].

État du contrôleur d'automatisation programmable (PAC)	Noms et couleurs des voyants LED :							
	RUN	ERR	IO ¹	ETH MS	ETH NS	DL	SRUN	SMOD
	Vert	Rouge	Rouge	Vert/rouge	Vert/rouge	Vert	Vert	Vert
Hors tension								
Sous tension • Autotest								
Non configuré					 Aucun câble branché et raccordé à un autre dispositif alimenté			
					 Dans le cas contraire			
Configuré : • Aucune erreur externe détectée							—	—
• Erreur externe détectée				—	—		—	—
• Aucune liaison Ethernet, embase Ethernet comprise							—	—
• Adresse IP en double			—				—	—

État du contrôleur d'automatisation programmable (PAC)	Noms et couleurs des voyants LED :							
	RUN	ERR	IO ¹	ETH MS	ETH NS	DL	SRUN	SMOD
	Vert	Rouge	Rouge	Vert/rouge	Vert/rouge	Vert	Vert	Vert
État STOP			 Erreur détectée sur le module d'E/S, le canal ou la configuration  Aucune erreur détectée sur l'E/S configurée		 Non connecté  Connecté  Pas de câble		 Tâche SAFE en cours d'exécution  Tâche SAFE arrêtée	 Mode de sécurité  Mode de maintenance
État RUN			—		 Non connecté  Connecté  Pas de câble		 Tâche SAFE en cours d'exécution  Tâche SAFE arrêtée	 Mode de sécurité  Mode de maintenance
État HALT (erreur récupérable détectée)			—				 Tâche SAFE en cours d'exécution	 Mode de sécurité

État du contrôleur d'automatisation programmable (PAC)	Noms et couleurs des voyants LED :							
	RUN	ERR	IO ¹	ETH MS	ETH NS	DL	SRUN	SMOD
	Vert	Rouge	Rouge	Vert/rouge	Vert/rouge	Vert	Vert	Vert
							 Tâche SAFE arrêtée	 Mode de maintenance
État SAFE (erreur non récupérable détectée)								
Mise à jour du système d'exploitation								
1. Les erreurs détectées pour un module d'E/S de sécurité ne sont pas toutes signalées par les voyants LED. Consultez les DDDT associés à ces modules pour obtenir des informations plus complètes.								

Légende :

Symbole	Description	Symbole	Description	Symbole	Description
	Vert en continu		Rouge en continu		Éteint
	Vert clignotant (500 ms allumé, 500 ms éteint)		Rouge clignotant (500 ms allumé, 500 ms éteint)	–	Non applicable

Diagnostics par LED du coprocesseur de sécurité M580

Voyants LED du coprocesseur

Utilisez les voyants LED en face avant du coprocesseur (voir Modicon M580, Guide de planification du système de sécurité) pour établir un diagnostic de l'état du PAC, de la manière suivante :

Etat du coprocesseur	Noms et couleurs des voyants :			
	SRUN	ERR	SMOD	DL
	Vert	Rouge	Vert	Vert
Hors tension				
Etat WAIT (attendre le téléchargement du micrologiciel à partir de l'UC)				
Non configuré (pas d'application)				
Configuré et fonctionnant en mode de sécurité : Tâche SAFE arrêtée				
Tâche SAFE en cours d'exécution				
Configuré et fonctionnant en mode de maintenance : Tâche SAFE arrêtée				
Tâche SAFE en cours d'exécution				
Tâche SAFE en état HALT (erreur récupérable détectée)				
Etat SAFE (erreur non récupérable détectée)				

Légende :

Symbole	Description	Symbole	Description	Symbole	Description
	Vert en continu		Rouge en continu		Eteint

Symbole	Description		Symbole	Description		Symbole	Description
	Vert clignotant (500 ms allumé, 500 ms éteint)			Rouge clignotant (500 ms allumé, 500 ms éteint)			

Voyant d'accès de la carte mémoire

Introduction

Le LED vert d'accès à la carte mémoire situé sous la porte du logement de carte mémoire SD indique si la CPU accède à la carte mémoire (quand une carte est insérée). Ce LED est visible lorsque la porte est ouverte.

États des LED dédiés

À lui seul, l'**accès à la carte mémoire** (LEDs) indique ces états :

État du voyant LED	Description
Allumé	La carte mémoire est reconnue, mais la CPU n'y accède pas.
clignotant	La CPU est en train d'accéder à la carte mémoire.
scintillant	La carte mémoire n'est pas reconnue.
Éteint	La carte mémoire peut être extraite de l'emplacement de la CPU ou la CPU ne reconnaît pas la carte mémoire.

NOTE: Vérifiez que le LED est éteint avant de retirer la carte de son logement.

Signification des combinaisons de voyants LED

Le LED de la carte d'accès fonctionne avec le voyant LED **BKP** (voir Modicon M580, Matériel, Manuel de référence). Leurs états combinés indiquent les informations de diagnostic suivantes :

État de la carte mémoire	Conditions	État de la CPU	Voyant d'accès de la carte mémoire	Voyant BKP
absence de carte mémoire dans l'emplacement	—	absence de configuration		
carte mémoire non OK	—	absence de configuration		
carte mémoire sans projet	—	absence de configuration		
carte mémoire avec projet non compatible	—	absence de configuration		
carte mémoire avec projet compatible	Une erreur est détectée lorsque le projet est restauré à partir de la carte mémoire vers la RAM de la CPU.	absence de configuration	en cours de transfert :  fin de transfert : 	en cours de transfert :  fin de transfert : 
	Aucune erreur n'est détectée lorsque le projet est restauré à partir de la carte mémoire vers la RAM de la CPU	—	en cours de transfert :  fin de transfert : 	en cours de transfert :  fin de transfert : 
— pas de circonstances ni d'état particuliers de la CPU				

Cette légende indique les différentes combinaisons du LED :

Symbole	Signification	Symbole	Signification
	éteint		rouge fixe
	vert fixe		vert clignotant

Diagnostics des alimentations de sécurité M580

Introduction

Cette section décrit les diagnostics disponibles pour les alimentations de sécurité M580.

Diagnostics fournis par les voyants LED de l'alimentation

Voyants LED de l'alimentation

Les alimentations de sécurité BMXCPS4002S, BMXCPS4022S et BMXCPS3522S présentent en face avant les voyants LED de diagnostic suivants :

- **OK** : état de fonctionnement
- **ACT** : activité
- **RD** : redondance (pour les conceptions à alimentations redondantes)

Les voyants LED d'alimentation de sécurité M580 peuvent présenter les informations de diagnostic suivantes :

Voyant	Description
OK	• Allumé (vert) : Toutes les conditions suivantes sont satisfaites : ◦ La tension 24 VCC de l'embase est OK. ◦ La tension 3,3 VCC de l'embase est OK. ◦ Le bouton de réinitialisation n'a pas été activé. • Clignotant : L'une des conditions suivantes est vraie : ◦ Le courant 24 VCC de l'embase n'est pas OK. ◦ Le courant 3,3 VCC de l'embase n'est pas OK et le bouton de réinitialisation n'a pas été activé. • Eteint : Une au moins des conditions suivantes est vraie : ◦ La tension 24 VCC de l'embase n'est pas OK. ◦ La tension 3,3 VCC de l'embase n'est pas OK. ◦ Le bouton de réinitialisation a été activé.
ACT	• Allumé (vert) : La source d'alimentation fournit de l'énergie. Dans une conception à alimentations redondantes, le module a le rôle principal. • Eteint : L'alimentation ne fournit pas d'énergie. Dans une conception à alimentations redondantes, le module a le rôle de secours.
RD	• Allumé (vert) : La communication entre les deux modules d'alimentation est OK. • Clignotant : L'une des conditions suivantes est vraie : ◦ Le courant 24 VCC de l'embase n'est pas OK. ◦ Le courant 3,3 VCC de l'embase n'est pas OK. • Eteint : Une au moins des conditions suivantes est vraie : ◦ La communication entre les deux modules d'alimentation n'est pas OK. ◦ Des autotests sont en cours d'exécution.

Diagnostics du module d'entrée analogique BMXSAI0410

Introduction

Cette section décrit les outils de diagnostic disponibles pour le module d'entrée analogique de sécurité BMXSAI0410.

Diagnostics DDDT du BMXSAI0410

Introduction

Le module d'entrée analogique de sécurité BMXSAI0410 fournit les diagnostics suivants à l'aide des éléments de son DDT de dispositif `T_U_ANA_SIS_IN_4`, page 67 :

- diagnostics d'entrée
- détection d'erreur interne
- diagnostics de câblage des canaux

Diagnostics d'entrée

Les capteurs connectés à chaque canal sont surveillés pour déterminer leur capacité à mesurer précisément 10 valeurs d'entrée analogique entre 4 et 20 mA. Si les tests de mesure d'entrée ne sont pas satisfaisants, le bit `CH_HEALTH` de la structure DDDT `T_U_ANA_SIS_CH_IN`, page 69 est défini sur 0, ce qui indique qu'il n'est pas opérationnel.

Détection d'erreur interne

Le module traite la valeur d'entrée à l'aide de deux circuits parallèles distincts. Les deux valeurs sont comparées pour déterminer si une erreur interne est détectée dans le processus du module. Si les valeurs comparées sont différentes, le bit `IC` de la structure DDDT `T_U_ANA_SIS_CH_IN` est défini sur 1, ce qui indique qu'il n'est pas opérationnel.

Reportez-vous au diagramme d'architecture, page 148 du module d'entrée analogique de sécurité BMXSAI0410 pour examiner une présentation graphique de ce processus.

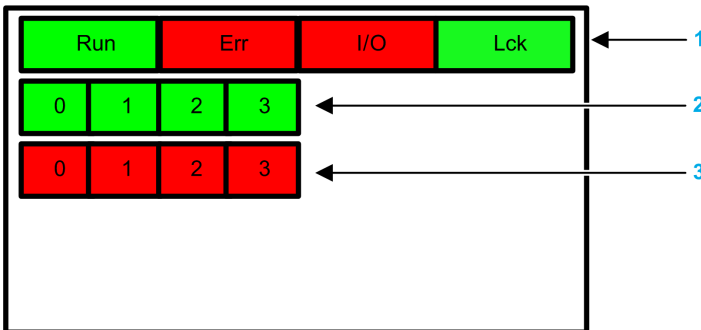
Diagnostics de câblage des canaux

Le câblage du capteur au canal d'entrée fait l'objet d'un diagnostic continu visant à détecter une condition de fil rompu où le courant mesuré est inférieur à 3,75 mA ou supérieur à 20,75 mA. Le cas échéant, le bit `OOR` de la structure `DDDT T_U_ANA_SIS_CH_IN` est défini sur 1.

Diagnostics par voyant LED du module d'entrée analogique BMXSAI0410

Panneau des voyants LED

Le module d'entrée analogique BMXSAI0410 présente le panneau de voyants LED suivant sur sa face avant :



1 Voyants d'état du module

2 Voyants d'état des canaux

3 Voyants d'erreur de canal

NOTE:

- Les voyants LED d'erreur de canal ne sont opérationnels qu'une fois que le module a été correctement configuré. Lorsqu'une erreur de canal est détectée, le voyant LED correspondant reste allumé jusqu'à ce que la condition sous-jacente soit résolue.
- Comme le module d'entrée comprend seulement quatre canaux, les voyants des positions 4 à 7 ne sont pas utilisés et ne s'allument jamais.

Diagnostics du module

Utilisez les quatre voyants LED de la partie supérieure du panneau pour établir le diagnostic de l'état du module d'entrée analogique BMXSAI0410 :

Voyants du module				Etat du module	Solution possible
Exécution	Err	I/O	LCK		
Clignote-ment ¹	Clignote-ment ¹	Clignote-ment ¹	Clignote-ment ¹	Autotest à la mise sous tension.	—
Clignote-ment ¹	Allumé	Éteint	Clignote-ment ¹	L'autotest à la mise sous tension a détecté une erreur interne sur les canaux d'entrée.	Remplacez le module.
Éteint	Allumé	Éteint	Éteint	Erreur interne détectée.	Remplacez le module si cette condition persiste.
Éteint	Clignote-ment ¹	Éteint	X	Module d'E/S non configuré.	Configurez le module via le contrôleur.
X	X	Allumé	X	Erreur externe détectée sur un canal d'entrée.	Voir la section <i>Diagnostics des canaux</i> , page 244 (ci-après).
Allumé	Clignote-ment ¹	X	X	Aucune communication entre contrôleur et module d'E/S.	Vérifiez que : • Le contrôleur est un contrôleur de sécurité M580 et il est opérationnel. • L'embase est opérationnelle (si le module d'E/S est sur le rack principal). • Le câble entre le contrôleur et le module d'E/S est opérationnel et correctement connecté (si le module d'E/S est sur un rack étendu ou distant).
Allumé	Clig. rapide ²	X	Éteint	Communication non sécurisée et configuration déverrouillée.	Recherchez la condition sous-jacente à l'aide des variables DDDT, page 66 de l'instance du module d'E/S.
Allumé	Clig. rapide ²	X	Allumé	Communication non sécurisée et configuration verrouillée.	Vérifiez que : • La configuration verrouillée dans le module est identique à la configuration du module stockée dans l'application sur le contrôleur et configurée à l'aide de Control Expert

Voyants du module				Etat du module	Solution possible
Exécution	Err	I/O	LCK		
					Recherchez la condition sous-jacente à l'aide des variables DDDT, page 66 de l'instance du module d'E/S.
Allumé	Allumé	Éteint	X	Erreur interne de canal d'entrée détectée	Remplacez le module si cette condition persiste.
Allumé	Éteint	Éteint	Éteint	La communication avec le contrôleur est OK et la configuration est déverrouillée.	–
Allumé	Éteint	Éteint	Allumé	La communication avec le contrôleur est OK et la configuration est verrouillée.	–
X indique que le voyant LED peut être soit allumé, soit éteint. 1. Clignotant : 500 ms allumé / 500 ms éteint 2. Clignotement rapide : 50 ms allumé / 50 ms éteint.					

Diagnosics des canaux

Utilisez tous les voyants LED du module d'entrée analogique BMXSAI0410 pour diagnostiquer l'état des canaux :

LED du module				Voyants des canaux		Etat voie	Solution possible
Exécution	Err	I/O	LCK	État du canal (Voyant 0 à 3)	Erreur détectée (Voyant 0 à 3)		
Allumé	Éteint	Éteint	X	Allumé	Éteint	Le courant d'entrée est dans la plage 4...20 mA sur le canal.	–
Allumé	Éteint	Allumé	X	OFF	Éteint	Le courant d'entrée est en dehors de la plage 4...20 mA sur le canal.	Vérifiez que l'alimentation externe, le câblage externe et le capteur sont opérationnels.
Allumé	Allumé	Éteint	X	OFF	Allumé	Le canal n'est pas opérationnel.	Remplacez le module si cette condition persiste.
X indique que le voyant peut être soit allumé, soit éteint.							

Diagnostics du module d'entrée numérique BMXSDI1602

Introduction

Cette section décrit les outils de diagnostic disponibles pour le module d'entrée numérique de sécurité BMXSDI1602.

Diagnostics DDDT du BMXSDI1602

Introduction

Le module d'entrée numérique de sécurité BMXSDI1602 fournit les diagnostics suivants à l'aide des éléments de son DDT de dispositif `T_U_DIS_SIS_IN_16`, page 98 :

- diagnostics d'entrée
- détection d'erreur interne
- diagnostics de câblage des canaux
- diagnostics de surtension et de sous-tension

Diagnostics d'entrée

Chaque canal d'entrée est testé pour évaluer son efficacité opérationnelle au début de chaque cycle (ou scrutation). Chaque canal est forcé à l'état alimenté et testé pour vérifier que cet état a été réalisé. Le canal est ensuite forcé à l'état non alimenté et testé à nouveau pour vérifier que cet état a été réalisé.

Si le canal ne bascule pas correctement entre les états alimenté et non alimenté, le bit `CH_HEALTH` de la structure DDDT `T_U_DIS_SIS_CH_IN`, page 101 est défini sur 0, ce qui indique qu'il n'est pas opérationnel.

Détection d'erreur interne

A chaque cycle, le module effectue une séquence de diagnostics d'entrée. Le module traite la valeur d'entrée à l'aide de deux circuits identiques distincts. Les deux valeurs sont comparées pour déterminer s'il y a une erreur interne dans le processus interne du module. Si les valeurs comparées sont différentes, le bit `IC` de la structure DDDT `T_U_DIS_SIS_CH_IN` est défini sur 1, ce qui indique qu'il n'est pas opérationnel.

Reportez-vous au [diagramme d'architecture](#), page 149 du module d'entrée numérique de sécurité BMXSDI1602 pour examiner une présentation graphique de ce processus.

Diagnostics de câblage des canaux

Le câblage du capteur au canal d'entrée peut être diagnostiqué en continu pour identifier les conditions suivantes :

- fil rompu (circuit ouvert)
- court-circuit sur 24 VCC
- court-circuit sur 0 VCC
- circuit transversal entre deux canaux parallèles

La disponibilité de ces diagnostics dépend de la source d'alimentation utilisée par la [conception spécifique du câblage](#), page 78 et de la fonction de diagnostic activée dans la page de configuration du module.

Si l'une de ces conditions est détectée, la structure DDDT `T_U_DIS_SIS_CH_IN` définit le bit associé sur 1, de la manière suivante :

- Le bit `OC` est défini sur 1 si une condition de fil rompu (ouvert) ou de court-circuit à la terre 0 VCC est détectée.
- Le bit `SC` est défini sur 1 si un court-circuit sur la source 24 VCC ou un circuit transversal entre deux canaux est détecté.

Diagnostics de surtension et de sous-tension

Le module teste continuellement les conditions de surtension et de sous-tension. Les valeurs de seuil suivantes s'appliquent :

- Seuil de sous-tension = 18,6 VCC
- Seuil de surtension = 33 VCC

Si l'une ou l'autre condition est détectée, le module définit le bit `PP_STS` du DDDT `T_U_DIS_SIS_IN_16` sur 0.

Diagnostics par voyant LED du module d'entrée numérique BMXSDI1602

Panneau des voyants

Le module d'entrée numérique BMXSDI1602 présente le panneau de voyants suivant sur sa face avant :



- 1 Voyants d'état du module
- 2 Voyants d'état des canaux (rang A)
- 3 Voyants d'erreur des canaux (rang A)
- 4 Voyants d'état des canaux (rang B)
- 5 Voyants d'erreur des canaux (rang B)

NOTE: Lorsqu'une erreur de canal est détectée, le voyant LED correspondant reste allumé jusqu'à ce que la condition sous-jacente soit résolue.

Diagnostics du module

Utilisez les quatre voyants LED de la partie supérieure du panneau pour établir le diagnostic de l'état du module d'entrée numérique BMXSDI1602 :

Voyants du module				Etat du module	Solution possible
Exécution	Err	I/O	LCK		
Clignotant	Clignotement ¹	Clignotement ¹	Clignotement ¹	Autotest à la mise sous tension.	—
Clignotant	Allumé	Éteint	Clignotement ¹	L'autotest à la mise sous tension a détecté une erreur	Remplacez le module.

Voyants du module				Etat du module	Solution possible
Exécution	Err	I/O	LCK		
				interne sur les canaux d'entrée.	
Clignotant	Allumé	Allumé	Clignotement ¹	- L'autotest à la mise sous tension a détecté une erreur interne sur les canaux d'entrée ou - L'alimentation 24 VCC externe n'est pas dans la plage	Vérifiez que l'alimentation 24 VCC du pré-actionneur externe est opérationnelle et connectez l'alimentation 24 VCC.
Éteint	Allumé	Éteint	Éteint	Erreur interne détectée.	Remplacez le module si cette condition persiste.
Éteint	Clignotement ¹	Éteint	X	Module d'E/S non configuré.	Configurez le module via la CPU.
X	XX	Allumé	X	- Alimentation 24 VCC externe hors plage ou - Erreur externe détectée sur un canal d'entrée.	- Vérifiez que l'alimentation 24 VCC du pré-actionneur externe est opérationnelle. - Reportez-vous à la section <i>Diagnostics des canaux</i>, page 250.
Allumé	Clignotement ¹	X	X	Aucune communication entre CPU et module.	Vérifiez que : - La CPU est une CPU de sécurité M580 safety CPU et elle est opérationnelle. - L'embase est opérationnelle (si le module d'E/S est sur le rack principal). - Le câble entre la CPU et le module d'E/S est opérationnel et correctement connecté (si le module d'E/S est sur un rack étendu ou distant).
Allumé	Clig. rapide ²	X	Éteint	Communication non sécurisée et configuration déverrouillée.	Recherchez la condition sous-jacente à l'aide des variables DDDT, page 98 de l'instance du module d'E/S.
Allumé	Clig. rapide ²	X	Allumé	Communication non sécurisée et configuration verrouillée.	Vérifiez que la configuration verrouillée dans le module est identique à la configuration du module stockée dans l'application sur la CPU et configurée à l'aide de Control Expert

Voyants du module				Etat du module	Solution possible
Exécution	Err	I/O	LCK		
					Recherchez la condition sous-jacente à l'aide des variables DDDT, page 98 de l'instance du module d'E/S.
Allumé	Allumé	Éteint	X	Erreur interne de canal d'entrée détectée	Remplacez le module si cette condition persiste.
Allumé	Éteint	Éteint	Éteint	La communication avec la CPU est OK et la configuration est déverrouillée.	–
Allumé	Éteint	Éteint	Allumé	La communication avec la CPU est OK et la configuration est verrouillée.	–
X indique que le voyant LED peut être soit allumé, soit éteint. 1. Clignotement : 500 ms allumé / 500 ms éteint. 2. Clignotement rapide : 50 ms allumé / 50 ms éteint.					

Diagnostics des canaux

Utilisez tous les voyants LED du module d'entrée numérique BMXSDI1602 pour diagnostiquer l'état des canaux :

Voyants du module				Voyants des canaux		État du canal	Solution possible
Exécution	Err	I/O	LCK	État du canal (LED 0 à 7, rang A/B)	Erreur détectée (LED 0 à 7, rang A/B)		
Allumé	Éteint	Éteint	X	Allumé	Éteint	Entrée en état activé.	–
Allumé	Éteint	Éteint	X	OFF	Éteint	Entrée en état désactivé.	–
Allumé	Allumé	Éteint	X	OFF	Allumé	Entrée en état désactivé. Une erreur interne est détectée sur le canal.	Changez le module si cette condition persiste.
Allumé	Allumé	Allumé	X	OFF	Allumé	L'alimentation 24 VCC externe n'est pas dans la plage.	Vérifiez que l'alimentation 24 VCC du pré-actionneur externe est opérationnelle.

Voyants du module				Voyants des canaux		État du canal	Solution possible
Exé- cu- tion	Err	I/O	LCK	État du canal (LED 0 à 7, rang A/B)	Erreur détectée (LED 0 à 7, rang A/ B)		
Allu- mé	Étei- nt	Allu- mé	X	X	Clignotement ¹	L'entrée est dans une des conditions suivantes : - condition de circuit ouvert ou - condition de court-circuit avec le 0 VCC.	Vérifiez que le câblage est opérationnel et correctement connecté.
Allu- mé	Étei- nt	Allu- mé	X	X	Clig. rapide ²	L'entrée est dans une des conditions suivantes : - condition de court-circuit avec le 24 VCC ou - condition de court-circuit avec le 0 VCC.	Vérifiez que le câblage est opérationnel et correctement connecté.
X indique que le voyant LED peut être soit allumé, soit éteint.							

Diagnostics du module de sortie numérique BMXSDO0802

Introduction

Cette section décrit les outils de diagnostic disponibles pour le module de sortie numérique de sécurité BMXSDO0802.

Diagnostics DDDT du BMXSDO0802

Introduction

Le module de sortie numérique de sécurité BMXSDO0802 fournit les diagnostics suivants à l'aide des éléments de son DDT de dispositif `T_U_DIS_SIS_OUT_8`, page 114 :

- diagnostics de sortie
- détection d'erreur interne
- diagnostics de câblage des canaux
- diagnostics de surtension et de sous-tension

Diagnostics de sortie

Chaque canal de sortie est testé pour évaluer son efficacité opérationnelle au début de chaque cycle (ou scrutation). Le test consiste à faire basculer les états des contacts de sortie (de l'état ON à l'état OFF ou de l'état OFF à l'état ON) pendant une durée trop courte pour provoquer une réaction d'actionneur (moins de 1 ms). Si le canal ne bascule pas correctement entre les états alimenté et non alimenté, le bit `CH_HEALTH` de la structure DDDT `T_U_DIS_SIS_CH_OUT`, page 116 est défini sur 0, ce qui indique qu'il n'est pas opérationnel.

Détection d'erreur interne

Le module traite la valeur de sortie à l'aide de deux circuits identiques distincts. Chaque circuit lit la tension médiane sur le canal. Les deux valeurs sont ensuite comparées et, si les valeurs ne sont pas celles escomptées, une erreur interne détectée est signalée en définissant le bit `IC` de la structure DDDT `T_U_DIS_SIS_CH_OUT` sur 1, ce qui indique que le canal n'est pas opérationnel.

Reportez-vous au [diagramme d'architecture](#), page 150 du module de sortie numérique de sécurité BMXSDO0802 pour examiner une présentation graphique de ce processus.

Diagnostics de câblage des canaux

Le câblage de l'actionneur au canal de sortie peut être diagnostiqué en continu pour identifier les conditions suivantes :

- fil rompu (circuit ouvert)
- court-circuit sur 24 VCC
- court-circuit sur 0 VCC
- circuit transversal entre deux canaux parallèles
- surcharge de canal

NOTE: La surcharge des canaux ne peut être détectée que si la sortie est alimentée.

La disponibilité de ces diagnostics dépend de la fonction de diagnostic activée dans la page de configuration du module.

Si l'une de ces conditions est détectée, la structure `DDDT T_U_DIS_SIS_CH_OUT` définit le bit associé sur 1, de la manière suivante :

- Le bit `OC` est défini sur 1 si une condition de fil rompu (ouvert) est détectée.
- Le bit `SC` est défini sur 1 si un court-circuit sur la source 24 VCC ou un circuit transversal entre deux canaux est détecté.
- Le bit `OL` est défini sur 1 si une condition de court-circuit sur le 0 V ou de surcharge de canal est détectée.

Diagnostics de surtension et de sous-tension

Le module teste continuellement les conditions de surtension et de sous-tension. Les valeurs de seuil suivantes s'appliquent :

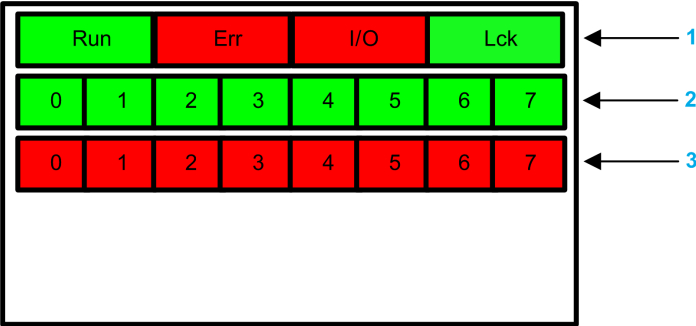
- Seuil de sous-tension = 18 VCC
- Seuil de surtension = 31,8 VCC

Si l'une ou l'autre condition est détectée, le module définit le bit `PP_STS` du `DDDT T_U_DIS_SIS_OUT_8` sur 0.

Diagnostics par voyant LED du module de sortie numérique BMXSDO0802

Panneau des voyants

Le module de sortie numérique BMXSDO0802 présente le panneau de voyants LED suivant sur sa face avant :



1 Voyants d'état du module

2 Voyants d'état des canaux

3 Voyants d'erreur de canal

NOTE: Lorsqu'une erreur de canal est détectée, le voyant LED correspondant reste allumé jusqu'à ce que la condition sous-jacente soit résolue.

Diagnostics du module

Utilisez les quatre voyants LED de la partie supérieure du panneau pour établir le diagnostic de l'état du module de sortie numérique BMXSDO0802 :

Voyants du module				Etat du module	Solution possible
Exécution	Err	I/O	LCK		
Clignote-ment ¹	Clignote-ment ¹	Clignote-ment ¹	Clignote-ment ¹	Autotest à la mise sous tension.	–
Clignote-ment ¹	Allumé	Éteint	Clignote-ment ¹	L'autotest à la mise sous tension a détecté une erreur interne sur les canaux de sortie.	Remplacez le module.

Voyants du module				Etat du module	Solution possible
Exécution	Err	I/O	LCK		
Clignote- ment ¹	Allumé	Allumé	Clignote- ment ¹	- L'autotest à la mise sous tension a détecté une erreur interne sur les canaux de sortie ou - L'alimentation 24 VCC externe n'est pas dans la plage	Vérifiez que l'alimentation 24 VCC du pré-actionneur externe est opérationnelle et connectez l'alimentation 24 VCC.
Éteint	Allumé	Éteint	Éteint	Erreur interne détectée.	Remplacez le module si cette condition persiste.
Éteint	Clignote- ment ¹	Éteint	X	Module d'E/S non configuré.	Configurez le module via la CPU.
X	X	Allumé	X	- Alimentation 24 VCC externe hors plage ou - Erreur externe détectée sur un canal de sortie.	- Vérifiez que l'alimentation 24 VCC du pré-actionneur externe est opérationnelle. - Reportez-vous à la section <i>Diagnostics des canaux</i>, page 256 (ci-après).
Allumé	Clignote- ment ¹	X	X	Aucune communication entre CPU et module. Le module est en état de repli (ou de réinitialisation s'il n'a jamais fonctionné normalement).	Vérifiez que : - La CPU est une CPU de sécurité M580 safety CPU et elle est opérationnelle. - L'embase est opérationnelle (si le module d'E/S est sur le rack principal). - Le câble entre la CPU et le module d'E/S est opérationnel et correctement connecté (si le module d'E/S est sur un rack étendu ou distant).
Allumé	Clig. rapide ²	X	Éteint	Communication non sécurisée et configuration déverrouillée. Le module est en état de repli (ou de réinitialisation s'il n'a jamais fonctionné normalement).	Vérifiez les variables disponibles dans le DDDT pour sécuriser la communication.

Voyants du module				Etat du module	Solution possible
Exécution	Err	I/O	LCK		
Allumé	Clig. rapide ²	X	Allumé	Communication non sécurisée et configuration verrouillée. Le module est en état de repli.	- Vérifiez que la configuration verrouillée dans le module est identique à la configuration du module stockée dans l'application sur la CPU et configurée à l'aide de Control Expert - Recherchez la condition sous-jacente à l'aide des variables DDDT, page 113 de l'instance du module d'E/S.
Allumé	Allumé	Éteint	X	Erreur interne détectée sur un canal de sortie.	Remplacez le module si cette condition persiste.
Allumé	Éteint	Éteint	Éteint	La communication avec la CPU est sécurisée et la configuration est déverrouillée.	–
Allumé	Éteint	Éteint	Allumé	La communication avec la CPU est sécurisée et la configuration est verrouillée.	–

X indique que le voyant LED peut être soit allumé, soit éteint.

1. Clignotement : 500 ms allumé / 500 ms éteint.

2. Clignotement rapide : 50 ms allumé / 50 ms éteint.

Diagnosics des canaux

Utilisez tous les voyants LED du module de sortie numérique BMXSDO0802 pour diagnostiquer l'état des canaux :

Voyants du module				Voyants des canaux		État du canal	Solution possible
Exé- cu- tion	Err	I/O	LCK	État du canal (Voyant 0 à 7)	Erreur détectée (LED 0 à 7)		
Allu- mé	Étei- nt	Étei- nt	X	Allumé	Éteint	Sortie en état activé.	–
Allu- mé	Étei- nt	Étei- nt	X	OFF	Éteint	Sortie en état désactivé.	–

Voyants du module				Voyants des canaux		État du canal	Solution possible
Exé- cu- tion	Err	I/O	LCK	État du canal (Voyant 0 à 7)	Erreur détectée (LED 0 à 7)		
Allu- mé	Allu- mé	Étei- nt	X	OFF	Allumé	Sortie en état désactivé. Erreur interne détectée sur un canal de sortie.	Remplacez le module si cette condition persiste.
Allu- mé	Allu- mé	Allu- mé	X	OFF	Allumé	L'alimentation 24 VCC du pré-actionneur externe n'est pas dans la plage	Vérifiez que l'alimentation 24 VCC est opérationnelle.
Allu- mé	Étei- nt	Allu- mé	X	Éteint	Clignotement ¹	La sortie présente l'une des conditions suivantes : • condition de circuit ouvert ou • condition de court- circuit avec le 0 VCC ou • surcharge de tension	Vérifiez que le câblage est opérationnel et correctement connecté.
Allu- mé	Étei- nt	Allu- mé	X	Allumé	Clig. rapide ²	La sortie présente l'une des conditions suivantes : • condition de court- circuit avec le 24 VCC ou • condition de court- circuit avec un autre canal de sortie actif	Vérifiez que le câblage est opérationnel et correctement connecté.
X indique que le voyant LED peut être soit allumé, soit éteint. 1. Clignotement : 500 ms allumé / 500 ms éteint. 2. Clignotement rapide : 50 ms allumé / 50 ms éteint.							

Diagnostics du module de sortie relais numérique BMXSRA0405

Introduction

Cette section décrit les outils de diagnostic disponibles pour le module de sortie relais numérique de sécurité BMXSRA0405.

Diagnostics DDDT du BMXSRA0405

Introduction

Le module de sortie relais numérique de sécurité BMXSRA0405 fournit les diagnostics suivants à l'aide des éléments de son DDT de dispositif `T_U_DIS_SIS_OUT_4`, page 131 :

- diagnostics de contact de sortie
- détection d'erreur interne

Diagnostics de contact de sortie

En fonction du numéro d'application configuré pour le module, ce dernier peut tester automatiquement sa capacité à faire basculer les états de contact de sortie (de l'état ON à l'état OFF ou de l'état OFF à l'état ON) pendant une durée trop courte pour provoquer une réponse d'actionneur. Si le canal ne bascule pas correctement entre les états alimenté et non alimenté, le bit `CH_HEALTH` de la structure DDDT `T_U_DIS_SIS_CH_ROUT`, page 133 est défini sur 0, ce qui indique qu'il n'est pas opérationnel.

NOTE: Les applications numéro 2, 4, 6 et 8 effectuent ce test de signal automatique. Ce n'est pas le cas des applications 1, 3, 5 et 7 qui nécessitent par conséquent une transition manuelle quotidienne de l'état du canal de sortie pour vérifier son état de fonctionnement.

Diagnostics de commande de sortie (détection d'erreur interne)

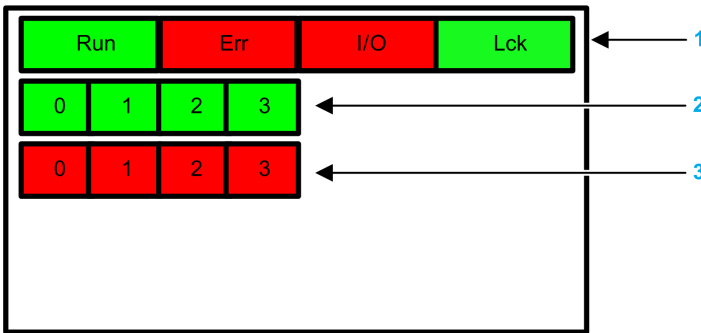
La commande de relais est traitée à l'aide de deux circuits parallèles distincts. Les valeurs de ces circuits sont comparées. Si les valeurs comparées sont différentes, le canal est jugé non opérationnel et le bit `IC` de la structure DDDT `T_U_DIS_SIS_CH_ROUT` est défini sur 1.

Reportez-vous au diagramme d'architecture, page 152 du module de sortie relais numérique de sécurité BMXSRA0405 pour examiner une présentation graphique de ce processus.

Diagnostics par voyant LED du module de sortie relais numérique BMXSRA0405

Panneau des voyants LED

Le module de sortie relais numérique BMXSRA0405 présente le panneau de voyants LED suivant sur sa face avant :



1 Voyants d'état du module

2 Voyants d'état des canaux

3 Voyants d'erreur de canal

NOTE:

- Lorsqu'une erreur de canal est détectée, le voyant LED correspondant reste allumé jusqu'à ce que la condition sous-jacente soit résolue.
- Comme le module de sortie relais comprend seulement quatre canaux, les voyants LED des positions 4 à 7 ne sont pas utilisés et ne s'allument jamais.

Diagnostics du module

Utilisez les quatre voyants LED de la partie supérieure du panneau pour établir le diagnostic de l'état du module de sortie relais numérique BMXSRA0405 :

Voyants du module				État du module	Solution possible
Run	Err	I/O	LCK		
Clignote-ment ¹	Clignote-ment ¹	Clignote-ment ¹	Clignote-ment ¹	Autotest à la mise sous tension.	–
Clignote-ment ¹	Allumé	Clignote-ment ¹	Clignote-ment ¹	L'autotest à la mise sous tension a détecté une erreur interne sur les canaux de sortie.	–
Éteint	Allumé	Éteint	Éteint	Erreur interne détectée.	Remplacez le module si cette condition persiste.
Éteint	Clignote-ment ¹	Éteint	X	Module d'E/S non configuré.	Configurez le module via la CPU.
Allumé	Clignote-ment ¹	Éteint	X	Aucune communication entre la CPU et le module. Ce dernier est en état de repli.	Vérifiez que : • La CPU est une CPU de sécurité M580 safety CPU et elle est opérationnelle. • L'embase est opérationnelle (si le module d'E/S est sur le rack principal). • Le câble entre la CPU et le module d'E/S est opérationnel et correctement connecté (si le module d'E/S est sur un rack étendu ou distant).
Allumé	Clignote-ment rapide ²	Éteint	Éteint	Aucune communication entre CPU et module. Le module est en état de repli (ou de réinitialisation s'il n'a jamais fonctionné normalement).	Recherchez la condition sous-jacente à l'aide des variables DDDT, page 130 de l'instance du module d'E/S.
Allumé	Clignote-ment rapide ²	Éteint	Allumé	Communication non sécurisée et configuration verrouillée. Le module est en état de repli (ou de réinitialisation s'il n'a jamais fonctionné normalement).	• Vérifiez que la configuration verrouillée dans le module est identique à la configuration du module stockée dans l'application sur la CPU et configurée à l'aide de Control Expert. • Recherchez la condition sous-jacente à l'aide des variables DDDT, page 130 de l'instance du module d'E/S.
Allumé	Allumé	Éteint	X	Erreur interne détectée sur le canal de sortie.	Remplacez le module si cette condition persiste.
Allumé	Éteint	Éteint	Éteint	La communication avec la CPU est sécurisée et la configuration est déverrouillée.	–

Voyants du module				État du module	Solution possible
Run	Err	I/O	LCK		
Allumé	Éteint	Éteint	Allumé	La communication avec la CPU est sécurisée et la configuration est verrouillée.	–
X indique que le voyant LED peut être soit allumé, soit éteint. 1. Clignotement : 500 ms allumé / 500 ms éteint. 2. Clignotement rapide : 50 ms allumé / 50 ms éteint.					

Diagnostics des canaux

Utilisez tous les voyants LED du module de sortie relais numérique BMXSRA0405 pour diagnostiquer l'état des canaux :

Voyants du module				Voyants des canaux		État du canal	Solution possible
Run	Err	I/O	LCK	État du canal (Voyant 0 à 3)	Erreur détectée (Voyant 0 à 3)		
Allumé	Éteint	Éteint	X	Allumé	Éteint	Le relais de sortie est fermé.	–
Allumé	Éteint	Éteint	X	Éteint	Éteint	Le relais de sortie est ouvert.	–
Allumé	Allumé	Éteint	X	Éteint	Allumé	Le relais de sortie n'est pas opérationnel.	Remplacez le module si cette condition persiste.
X indique que le voyant LED peut être soit allumé, soit éteint.							

Utilisation d'un système de sécurité M580

Présentation

Ce chapitre indique comment utiliser un système de sécurité M580.

Zones de données de processus, sécurité et globale dans Control Expert

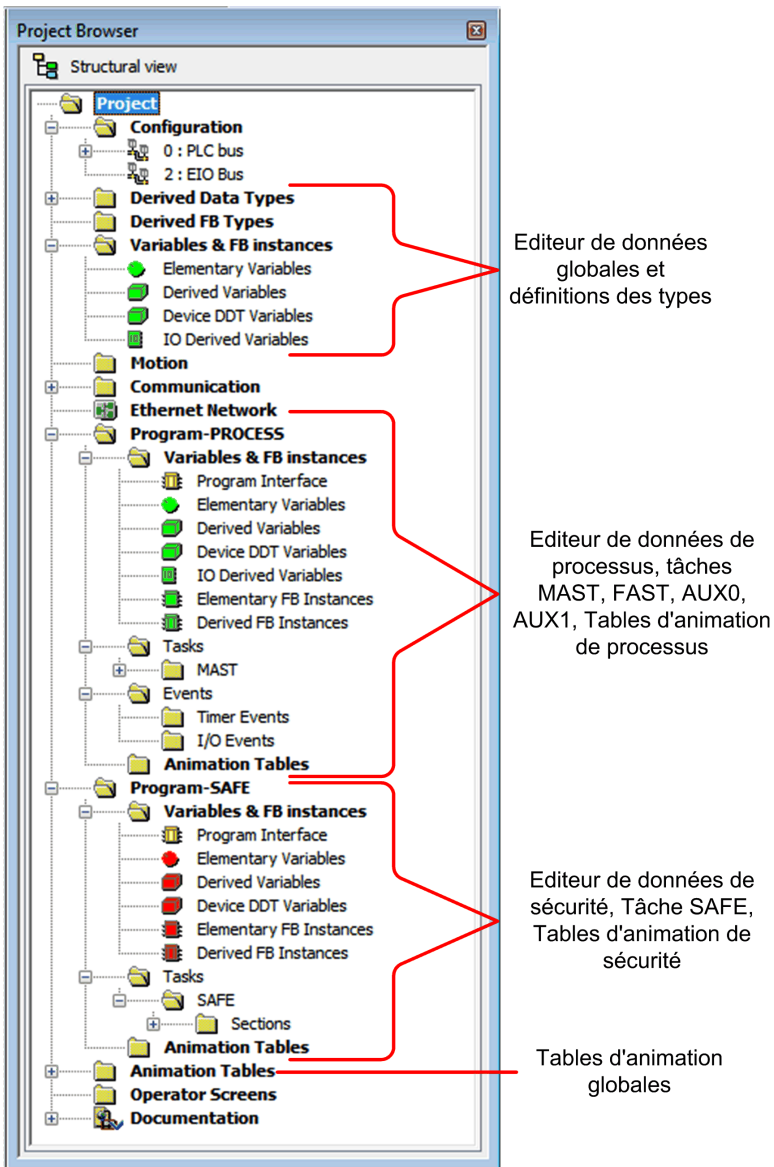
Introduction

Cette section décrit la séparation des zones de données dans un projet de sécurité M580 Control Expert.

Séparation des données dans Control Expert

Zones de données dans Control Expert

La **Vue structurelle** du **Navigateur de projet** affiche la séparation des données dans Control Expert.. Comme indiqué ci-dessous, chaque zone de données a son propre éditeur de données et ses propres tables d'animation :



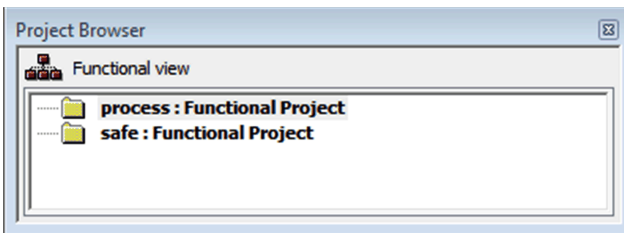
Lors d'une recherche dans le **Navigateur de projet** :

- La zone de sécurité contient l'éditeur des données de sécurité, la logique de sécurité et les instances des blocs fonction utilisés par la tâche SAFE. Remarques :
 - Les événements d'E/S, les événements de temporisation et les sous-routines ne sont pas pris en charge dans un programme de sécurité.
 - Les variables IODDT ne sont pas prises en charge par la tâche SAFE et ne sont pas incluses à la zone de sécurité.
 - Les icônes rouges indiquent les parties SAFE du programme.
- La zone de processus contient l'éditeur des données de processus, la logique de sécurité et les instances des blocs fonction utilisés par les tâches non liées à la sécurité (c'est-à-dire : MAST, FAST, AUX0 et AUX1).
- La zone globale contient l'éditeur des données globales, les données dérivées et les types de blocs fonction instantiés dans les programmes de processus et de sécurité.

NOTE: Le terme *données globales* dans cette rubrique désigne les objets de données de portée application ou globale dans un projet de sécurité. Il ne se rapporte pas au service Global Data pris en charge par les modules Ethernet de Schneider Electric.

Navigateur de projet dans la vue fonctionnelle

La **Vue fonctionnelle** du Control Expert **Navigateur de projet** d'un système de sécurité M580 présente deux projets fonctionnels : un pour l'espace de nom de processus, un pour l'espace de nom de sécurité :



La gestion d'un projet fonctionnel dans un système de sécurité M580 est similaire à la gestion d'un projet dans la vue fonctionnelle d'un système M580 non lié à la sécurité, excepté pour les tables d'animation et les sections de code.

Conséquences sur la vue structurelle :

Lorsque vous ajoutez une section de code ou une table d'animation à un projet fonctionnel, il est associé à l'espace de nom correspondant au projet fonctionnel. L'ajout d'une section de code ou d'une table d'animation à :

- **processus : projet fonctionnel** l'ajoute à l'espace de nom de processus du projet dans la vue structurelle.
- **sécurité : projet fonctionnel** l'ajoute à l'espace de nom de sécurité du projet dans la vue structurelle.

Langages et tâches disponibles :

Lorsque vous créez une nouvelle section de code pour un projet fonctionnel (en sélectionnant **Créer > Nouvelle section...**), les options de **Langage** et **Tâche** disponibles dépendent du projet fonctionnel :

Lorsque vous créez une nouvelle section de code pour un projet fonctionnel (en sélectionnant **Créer > Nouvelle section...**), les options de **Langage** et de **Tâche** disponibles dépendent du projet fonctionnel associé :

Projet fonctionnel	Langages et tâches disponibles	
	Langages ¹	Tâches ²
processus : projet fonctionnel	• IL • FBD • LD • Segment LL984 • SFC • ST	• MAST • FAST • AUX0 • AUX1
sécurité : projet fonctionnel	• FBD • LD	• SAFE
1. Sélectionné dans l'onglet Général de la boîte de dialogue de la nouvelle section. 2. Sélectionné dans l'onglet Localisation de la boîte de dialogue de la nouvelle section. La tâche MAST est disponible par défaut. D'autres sections sont disponibles uniquement après leur création dans le programme de processus.		

Code couleur des icônes

Pour vous aider à faire la distinction entre les parties processus et sécurité du projet, des icônes rouges sont utilisées pour identifier les parties sécurité de votre application.

Modes de fonctionnement, états de fonctionnement et tâches

Présentation

Cette section décrit les modes de fonctionnement, les états de fonctionnement et les tâches prises en charge par le PAC de sécurité M580.

Modes de fonctionnement du contrôleur de sécurité M580

Deux modes de fonctionnement

Le contrôleur de sécurité M580 présente deux modes de fonctionnement :

- Mode sécurité : mode de fonctionnement par défaut utilisé pour les opérations de sécurité.
- Mode maintenance : mode de fonctionnement facultatif qui peut être activé de façon temporaire pour effectuer le débogage, modifier le programme d'application ou modifier la configuration.

Le logiciel Control Expert Safety est le seul outil qui permet de gérer les transitions du mode de fonctionnement.

NOTE: La configuration du mode de fonctionnement d'un contrôleur redondant (mode sécurité ou maintenance) n'est pas incluse dans le transfert d'une application du contrôleur primaire vers le contrôleur redondant. Lors d'un basculement, lorsqu'un contrôleur de sécurité passe du rôle redondant au rôle de contrôleur primaire, le mode de fonctionnement est automatiquement défini sur le mode de sécurité.

Mode de sécurité et ses limitations

Le mode de sécurité est le mode par défaut du contrôleur de sécurité. Lorsque le contrôleur de sécurité est mis sous tension avec une application valide présente, il passe en mode sécurité. Le mode sécurité permet de contrôler l'exécution de la fonction de sécurité. Vous pouvez charger, télécharger, exécuter et arrêter le projet en mode sécurité.

Lorsque le contrôleur de sécurité M580 fonctionne en mode sécurité, les fonctions suivantes ne sont **pas** disponibles :

- Téléchargement d'une configuration modifiée entre Control Expert et le contrôleur.

- Modification et/ou forçage des valeurs des variables de sécurité et de l'état des E/S de sécurité.
- Débogage de la logique de l'application, via des points d'arrêt, points de visualisation et exécution de code pas à pas.
- Utilisation de tables d'animation ou requêtes UMAS (par exemple, via une HMI) pour écrire des variables de sécurité et des E/S de sécurité.
- Modification des paramètres de configuration des modules de sécurité via CCOTF. (L'utilisation de CCOTF pour les modules non perturbateurs est prise en charge.)
- Modification en ligne de l'application de sécurité.
- Utilisation de l'animation de liens.

NOTE: En mode sécurité, toutes les variables de sécurité et les états des E/S sont en lecture seule. Vous ne pouvez pas modifier directement la valeur d'une variable de sécurité.

Vous pouvez créer une variable globale, et l'utiliser pour transmettre une valeur entre une variable de processus associée (non liée à la sécurité) et une variable de sécurité associée en utilisant les onglets de l'interface de l'éditeur des données de processus et l'éditeur des données de sécurité. Une fois la liaison établie, le transfert est exécuté comme suit :

- Au début de chaque tâche SAFE, les valeurs de la variable non liée à la sécurité sont copiées avec les variables de sécurité.
- A la fin de chaque tâche SAFE, les valeurs des variables de sortie de sécurité sont copiées avec les variables non liées à la sécurité.

Fonctionnement du mode de maintenance

Le mode de maintenance est comparable au mode normal d'un contrôleur M580 non lié à la sécurité. Il permet d'effectuer le débogage et le réglage de la tâche SAFE de l'application. Le mode maintenance est temporaire car le contrôleur de sécurité passe automatiquement en mode sécurité en cas de perte de communication entre Control Expert et le contrôleur, ou en cas d'exécution d'une commande de déconnexion. En mode maintenance, les personnes ayant les droits appropriés peuvent lire et écrire des valeurs dans les variables de sécurité et les E/S de sécurité configurées pour accepter des modifications.

En mode maintenance, l'exécution double du code de la tâche SAFE est effectuée, mais les résultats ne sont pas comparés.

Lorsque le contrôleur de sécurité M580 est en mode maintenance, les fonctions suivantes ne sont pas disponibles :

- Téléchargement d'une configuration modifiée entre Control Expert et le contrôleur.
- Modification et/ou forçage des valeurs des variables de sécurité et de l'état des E/S de sécurité.

- Débogage de la logique de l'application, via des points d'arrêt, points de visualisation et exécution de code pas à pas.
- Utilisation de tables d'animation ou requêtes UMAS (par exemple, via une HMI) pour écrire des variables de sécurité et des E/S de sécurité.
- Modification de la configuration via CCOTF.
- Modification en ligne de l'application de sécurité.
- Utilisation de l'animation de liens.

En mode maintenance, le niveau SIL du contrôleur de sécurité n'est pas maintenu.

▲ AVERTISSEMENT
PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ Prenez les mesures appropriées pour garantir l'état sécurisé défini du système lorsque le contrôleur de sécurité est en mode maintenance. Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Autorisation de maintenance

L'entrée `%lr.m.c` peut être paramétrée pour autoriser le contrôleur de sécurité à passer en mode de **maintenance** comme suit :

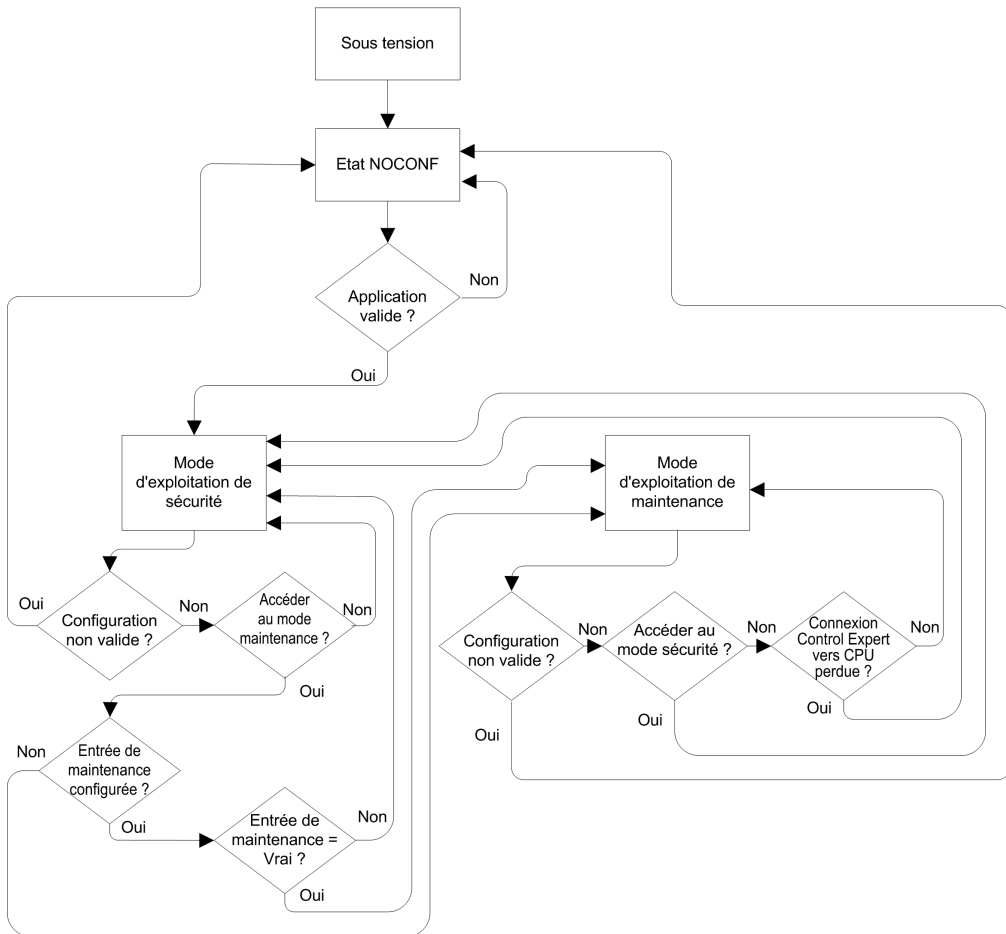
- `%lr.m.c` définie sur 1 : Le contrôleur de sécurité peut passer en mode de **maintenance**.
- `%lr.m.c` définie sur 0 : Le contrôleur de sécurité ne peut pas passer en mode de **maintenance**.

NOTE:

- Si l'entrée est détectée comme une erreur, l'entrée `%lr.m.c` est considérée comme étant définie sur à 1 (le passage en mode de **Maintenance** peut être activé). Pour supprimer cette autorisation dans l'écran de configuration, l'entrée ne doit pas être détectée en tant qu'erreur.
- Le format d'entrée est `%lr.m.c` ou *Type de données dérivé (DDT, Derived Data Type) d'équipement* à partir d'un module d'entrée non lié à la sécurité.

Transitions entre les modes de fonctionnement

Le schéma suivant montre comment le contrôleur de sécurité M580 effectue la transition entre le mode sécurité et le mode maintenance :



Lors du passage du mode sécurité au mode maintenance :

- Le passage du mode maintenance au mode sécurité est possible avec forçage sur ON. Dans ce cas, la valeur forcée de la variable ou l'état des E/S perdue après la transition jusqu'à la transition suivante entre le mode sécurité et le mode maintenance.

- La transition entre le mode maintenance et le mode sécurité peut être effectuée de plusieurs manières :
 - Manuellement dans, par une commande de menu ou de barre d'outils dans Control Expert.
 - Automatiquement, via le contrôleur de sécurité, si la communication entre Control Expert et le contrôleur est perdue durant environ 50 secondes..
- La fonction d'entrée de maintenance, si elle est configurée, fonctionne comme une vérification de la transition entre le mode sécurité et le mode maintenance. La fonction d'entrée de maintenance est configurée dans Control Expert dans l'onglet **Configuration** du contrôleur comme suit :
 - Sélectionnez le paramètre **Entée de maintenance**, et
 - Entrez l'adresse topologique d'un bit entrée (%I) pour un module d'entrée numérique non perturbateur sur le rack local.

Lorsque l'entrée de maintenance est configurée, la transition entre le mode sécurité et le mode maintenance prend en compte l'état du bit d'entrée désigné (%I). Si le bit est défini sur 0 (faux), le contrôleur est verrouillé en mode sécurité. Si le bit est défini sur 1 (true), la transition peut être effectuée entre le mode maintenance et le mode sécurité.

Passage du mode sécurité et du mode maintenance dans Control Expert

Le passage du mode maintenance au mode sécurité est possible pour le contrôleur de sécurité si :

- Le contrôleur est en mode Débogage.
- Un point d'arrêt est activé dans une section de la tâche SAFE.
- Un point de visualisation est activé dans une section de la tâche SAFE.

Si le mode débogage n'est pas actif, aucun point d'arrêt de tâche SAFE n'est activé, et aucun point de visualisation de tâche SAFE n'est défini. Vous pouvez activer manuellement une transition entre le mode sécurité et le mode maintenance, comme suit :

- Pour passer du mode sécurité au mode maintenance :
 - Sélectionnez **PLC > Maintenance**, ou
 - Cliquez sur le bouton  dans la barre d'outils.
- Pour passer du mode maintenance au mode sécurité :
 - Sélectionnez **PLC > Sécurité**, ou
 - Cliquez sur le bouton  dans la barre d'outils.

NOTE: Les événements d'activation et de désactivation du mode sécurité sont consignés par le serveur SYSLOG sur le contrôleur.

Identification du mode de fonctionnement

Vous pouvez déterminer le mode de fonctionnement actif d'un contrôleur de sécurité M580 en consultant les voyants LED **SMOD** du contrôleur et le coprocesseur, ou Control Expert.

Si les voyants, LED **SMOD** du contrôleur et du coprocesseur sont comme suit :

- *Clignotants*, le contrôleur est en mode maintenance.
- *Fixes*, le contrôleur est en mode sécurité.

Si Control Expert est connecté au contrôleur, il identifie le mode du contrôleur de sécurité M580 de différentes façons :

- Les mots système %SW12 (coprocesseur) et %SW13 (contrôleur), page 419 indiquent le mode de fonctionnement du contrôleur, comme suit :
 - si la valeur de %SW12 est 16#A501 (hex) et celle de %SW13 est 16#501A (hex), le contrôleur est en mode maintenance.
 - si la valeur de l'un de ces mots système ou des deux est 16##5AFE (hex), le contrôleur est en mode sécurité.
- Les sous-onglets **Tâche** et **Information** de l'onglet **Animation** du contrôleur indiquent le mode de fonctionnement du contrôleur.
- La barre des tâches située au bas de la fenêtre principale de Control Expert indique le mode de fonctionnement (MAINTENANCE ou SECURITE).

États de fonctionnement du contrôleur de sécurité M580

États de fonctionnement

Le contrôleur de sécurité M580 présente les états de fonctionnement suivants.

NOTE: Pour une description de la relation entre les états de fonctionnement du contrôleur de sécurité M580 et les états de fonctionnement du contrôleur redondant M580 , consultez le document *Modicon M580 - Redondance d"UC, Guide de planification du système pour architectures courantes* et les rubriques *États du contrôleur redondant* et *Affectations et transitions de l'état du contrôleur redondant*.

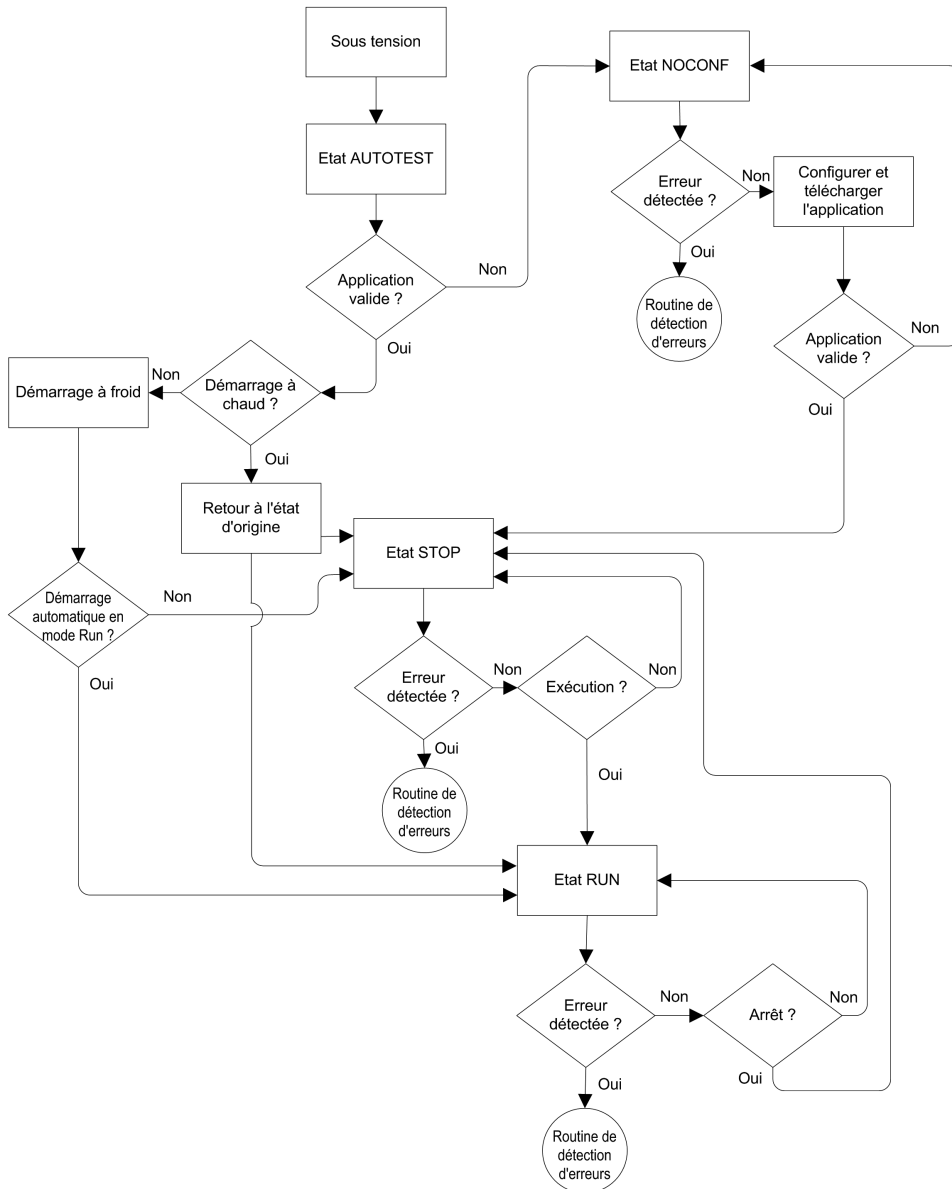
Etat de fonctionnement	Applicable à	Description
AUTOTEST	Contrôleur	La contrôleur exécute des autotests internes. NOTE: Si des embases d'extension sont connectées à l'embase locale principale et que les connecteurs inutilisés du module d'extension d'embase ne sont pas munis de terminaisons de ligne, le contrôleur reste à l'état AUTOTEST à l'issue des autotests.
NOCONF	Contrôleur	Le programme d'application n'est pas valide.
STOP	Contrôleur ou tâche	Le contrôleur contient une application valide et aucune erreur n'est détectée, mais le fonctionnement s'est arrêté car : • Au démarrage, Démarrage automatique en mode Run n'est pas défini (mode de sécurité, page 268). • Exécution arrêtée par l'exécution de la commande STOP (mode sécurité, page 268 ou maintenance, page 269) • Les points d'arrêt ont été définis en mode maintenance, puis la connexion entre Control Expert et le contrôleur a été perdue durant plus de 50 secondes. Le contrôleur lit les entrées associées à chaque tâche, mais n'actualise pas les sorties, qui passent à l'état de repli. Vous pouvez redémarrer le contrôleur lorsque vous êtes prêt. NOTE: L'envoi de la commande STOP dans Control Expert arrête toutes les tâches. L'événement STOP est enregistré sur le serveur SYSLOG du contrôleur.
HALT	Tâche	Le contrôleur de sécurité M580 peut être dans deux états HALT indépendants : • L'état HALT de processus s'applique aux tâches non liées à la sécurité (MAST, FAST, AUX0 et AUX1) Si une tâche de processus passe à l'état HALT, toutes les autres tâches passent à l'état HALT. La tâche SAFE n'est pas affectée par une condition HALT de processus. • L'état SAFE HALT s'applique uniquement à la tâche SAFE. Les tâches de processus ne sont pas affectées par une condition SAFE HALT. Dans chaque cas, les opérations de la tâche sont arrêtées car une condition bloquante a été détectée, entraînant une condition récupérable, page 229. Le contrôleur lit les entrées associées à chaque tâche arrêtée, mais n'actualise pas les sorties, qui sont à l'état de repli.
RUN	Contrôleur ou tâche	En présence d'une application valide et en l'absence d'erreur détectée, le contrôleur lit les entrées associées à chaque tâche, exécute le code associé à chaque tâche, puis actualise les sorties associées. • En mode sécurité, page 268 : la fonction de sécurité est effectuée, et toutes les restrictions sont appliquées. • En mode maintenance, page 269 : le contrôleur fonctionne comme un contrôleur non lié à la sécurité. L'exécution double du code de la tâche SAFE est effectuée, mais les résultats ne sont pas comparés.

Etat de fonctionnement	Applicable à	Description
		NOTE: L'envoi de la commande RUN dans Control Expert démarre toutes les tâches. L'événement RUN est enregistré sur le serveur SYSLOG du contrôleur.
WAIT	Contrôleur	Le contrôleur est dans un état transitoire pendant qu'il sauvegarde ses données quand une condition de mise hors tension est détectée. Le contrôleur démarre à nouveau lorsque l'alimentation est rétablie et que la réserve de courant est remplie. Comme l'état WAIT est transitoire, il se peut qu'il ne soit pas visible. Le contrôleur effectue une reprise à chaud, page 282 pour quitter l'état WAIT.
ERROR	Contrôleur	Le contrôleur, page 226 est arrêté suite à la détection d'une erreur matérielle ou système. L'état ERROR déclenche la fonction de sécurité, page 21. Lorsque le système est prêt à redémarrer, effectuez un Démarrage à froid, page 282 du contrôleur pour quitter l'état ERROR, soit par un redémarrage, soit par une réinitialisation (RESET).
OS DOWNLOAD	Contrôleur	Un téléchargement du micrologiciel du contrôleur ou du coprocesseur est en cours.

Consultez les rubriques *M580 - Voyants de diagnostic du contrôleur*, page 231 et *M580 - Voyants de diagnostic du coprocesseur de sécurité*, page 231 pour plus d'informations sur les états de fonctionnement du contrôleur.

Transitions entre états de fonctionnement

Les transitions entre les différents états d'un contrôleur de sécurité M580 sont décrites ci-dessous :



Consultez la rubrique *Traitement des erreurs détectées*, page 277 pour plus d'informations sur la façon dont système de sécurité gère les erreurs.

Traitement des erreurs détectées

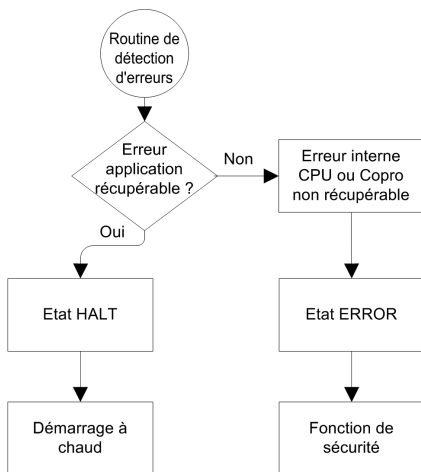
Le contrôleur de sécurité M580 gère les erreurs détectées par le contrôleur des types suivants :

- Erreurs récupérables détectées par l'application : Ces événements font passer la ou les tâches associées à l'état HALT.

NOTE: Comme les tâches MAST, FAST et AUX sont exécutées dans la même zone de mémoire, un événement qui fait passer l'une de ces tâches à l'état HALT, fait également passer les autres tâches (non liées à la sécurité) à l'état HALT. Comme la tâche SAFE est exécutée dans une zone de mémoire distincte, les tâches non liées à la sécurité ne sont pas affectées si la tâche SAFE passe à l'état HALT.

- Erreurs non récupérables détectées par l'application : Erreurs détectées sur le contrôleur ou le coprocesseur interne : Ces événements font passer le contrôleur à l'état ERROR. La fonction de sécurité est appliquée à la portion affectée de la boucle de sécurité.

La logique de traitement des erreurs détectées est décrite ci-dessous :



L'impact des erreurs détectées sur chacune des tâches est décrit ci-dessous :

Type de l'erreur détectée	Etat des tâches			
	FAST	SAFE	MAST	AUX
Dépassement du chien de garde de la tâche FAST	HALT	RUN ¹	HALT	HALT
Dépassement du chien de garde de la tâche SAFE	RUN	HALT ²	RUN	RUN
Dépassement du chien de garde de la tâche MAST	HALT	RUN	HALT	HALT
Dépassement du chien de garde de la tâche AUX	HALT	RUN	HALT	HALT
Erreur détectée dans l'exécution double de code sur le contrôleur	RUN	HALT ²	RUN	RUN
Dépassement du chien de garde de sécurité ³	ERROR	ERROR ²	ERROR	ERROR
erreur détectée interne au contrôleur	ERROR	ERROR ²	ERROR	ERROR
1. Comme la priorité de la tâche FAST est supérieure à la priorité de la tâche SAFE, le retard de la tâche FAST peut faire passer la tâche SAFE à l'état HALT ou ERROR au lieu de l'état RUN. 2. Les états ERROR et HALT de la tâche SAFE peut mettre les sorties de sécurité à l'état configurable par l'utilisateur (repli ou maintien). 3. La valeur du chien de garde de sécurité est définie sur 1,5 fois celle du chien de garde de la tâche SAFE.				

Visualiseur de l'état de sécurité sur la barre des tâches

Lorsque Control Expert est connecté au contrôleur de sécurité M580 , la barre des tâches inclut un champ décrivant les états de fonctionnement de la tâche SAFE et des tâches de processus (MAST, FAST, AUX0, AUX1) comme suit :

État des tâches de processus	Etat de la tâche SAFE	Message
STOP (toutes les tâches de processus à l'état STOP)	STOP	STOP
STOP (toutes les tâches de processus à l'état STOP)	RUN	RUN
STOP (toutes les tâches de processus à l'état STOP)	HALT	SAFE HALT
RUN (au moins une tâche de processus est à l'état RUN)	STOP	RUN
RUN (au moins une tâche de processus est à l'état RUN)	RUN	RUN
RUN (au moins une tâche de processus est à l'état RUN)	HALT	SAFE HALT
HALT	STOP	PROC HALT
HALT	RUN	PROC HALT
HALT	HALT	HALT

Séquences de démarrage

Introduction

Le contrôleur de sécurité M580 peut passer à la séquence de démarrage dans les cas suivants :

- Au démarrage initial.
- En réponse à l'interruption de l'alimentation.

Selon le type de tâche, et le contexte de l'interruption de l'alimentation, le contrôleur de sécurité M580 peut effectuer un nouveau **démarrage à froid** , page 282 ou un **démarrage à chaud**, page 282 lorsque l'alimentation est restaurée.

Démarrage initial

Lors du démarrage initial, le contrôleur de sécurité M580 effectue un démarrage à froid. Toutes les tâches, y compris la tâche SAFE et les tâches non liées à la sécurité (MAST, FAST, AUX0, AUX1), passent à l'état STOP sauf si **Démarrage automatique en mode Run** est activé, auquel cas les tâches passent à l'état RUN.

Démarrage après une coupure de courant

L'alimentation de sécurité M580 constitue une réserve d'alimentation qui continue à alimenter tous les modules du rack durant 10 ms en cas de coupure de courant. Si la réserve d'alimentation est vide, le contrôleur de sécurité M580 effectue un cycle d'alimentation complet.

Avant la mise hors tension du système, le contrôleur de sécurité stocke les données suivantes qui définissent le contexte du fonctionnement lors de l'arrêt :

- Date et heure de la mise hors tension (stocké dans %SW54 à %SW58)
- Etat de chaque tâche.
- Etat des temporisateurs d'événement.
- Valeurs des compteurs d'exécution.
- Signature de l'application.
- Données de l'application (valeurs en cours des variables de l'application)
- Somme de contrôle de l'application.

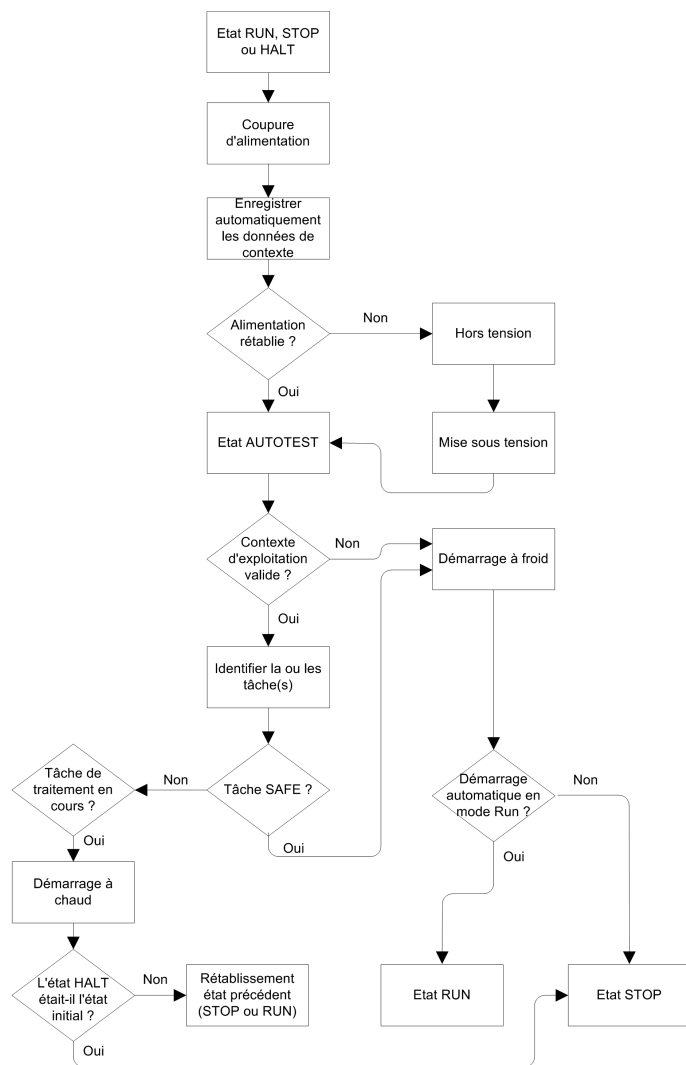
Après une mise hors tension, le démarrage peut être automatique (si l'alimentation a été restaurée avant la fin de la mise hors tension) ou manuel (dans le cas contraire).

Ensuite, le contrôleur de sécurité M580 effectue des auto-tests et vérifie la validité des données du contexte de fonctionnement qui ont été sauvegardées à la mise hors tension, comme suit :

- La somme de contrôle de l'application est vérifiée.
- La carte mémoire SD est lue pour vérifier qu'elle contient une application valide.
- Si l'application de la carte mémoire SD est valide, les signatures sont vérifiées pour déterminer si elles sont bien identiques.
- La signature de l'application enregistrée est vérifiée en la comparant à la signature stockée.

Si le contexte de fonctionnement est valide, les tâches non liées à la sécurité effectuent un démarrage à chaud. Si le contexte de fonctionnement n'est pas valide, les tâches non liées à la sécurité effectuent un démarrage à froid. Dans les deux cas, la tâche SAFE effectue un démarrage à froid.

Cette séquence de démarrage après une coupure d'alimentation est présentée ci-dessous :



Démarrage à froid

Lors d'un démarrage à froid, toutes les tâches, y compris la tâche SAFE et les tâches non liées à la sécurité (MAST, FAST, AUX0, AUX1), passent à l'état STOP sauf si **Démarrage automatique en mode Run** est activé, auquel cas les tâches passent à l'état RUN.

Lors d'un démarrage à froid, les opérations suivantes sont exécutées :

- Les valeurs initiales définies par l'application sont attribuées aux données de l'application (notamment : bits internes, données d'E/S, mots internes, etc.).
- Les fonctions élémentaires sont configurées sur leurs valeurs par défaut.
- Les blocs fonction élémentaires et leurs variables sont configurés sur leurs valeurs par défaut.
- Les bits et mots système sont configurés sur leurs valeurs par défaut.
- Initialisation de toutes les variables forcées en appliquant leurs valeurs par défaut (initialisées).

Vous pouvez exécuter un démarrage à froid pour les données, les variables et les fonctions dans l'espace de nom de processus en sélectionnant **PLC > Init** dans *Control Expert*, page 298, ou en configurant le bit système %S0 (COLDSTART) sur 1. Le bit système %S0 n'a aucun effet sur les données et les fonctions appartenant à l'espace de nom de sécurité.

NOTE: Après un démarrage à froid, la tâche SAFE ne peut pas démarrer tant que la tâche MAST n'a pas démarré.

Démarrage à chaud

Lors d'un démarrage à chaud, chaque tâche de processus (notamment les tâches MAST, FAST, AUX0 et AUX1) repasse à l'état de fonctionnement où elle se trouvait lors de la coupure de courant. Par contre, lors d'un démarrage à chaud, la tâche SAFE passe à l'état STOP, sauf si **Démarrage automatique en mode RUN** est sélectionné.

NOTE: Si une tâche était à l'état HALT ou à un point d'arrêt lors de la coupure de courant, elle passe à l'état STOP après le démarrage à chaud.

Lors d'un démarrage à chaud, les opérations suivantes sont exécutées :

- Restauration de la dernière valeur des variables de l'espace de nom de processus.
- Initialisation des variables de l'espace de nom de sécurité en appliquant leurs valeurs par défaut (initialisées).
- Initialisation de toutes les variables forcées en appliquant leurs valeurs par défaut (initialisées).
- Restauration de la dernière valeur des variables de l'application.
- Configuration de %S1 (WARMSTART) sur 1.
- Les connexions entre le contrôleur et le contrôleur sont réinitialisées.

- Les modules d'E/S sont re-configurés (si nécessaire) en utilisant les paramètres stockés.
- Les événements, la tâche FAST et les tâches AUX sont désactivées.
- La tâche MAST est redémarrée au début du cycle.
- %S1 est configuré sur 0 à la fin de la première exécution de la tâche MAST.
- Les événements, la tâche FAST et les tâches AUX sont activés.

Si une tâche était en cours d'exécution lors de la coupure de courant, elle est exécutée depuis le début après le démarrage à chaud.

▲ AVERTISSEMENT

FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT

Assurez-vous que la sélection de **Démarrage automatique en mode RUN** est conforme au comportement correct de votre système ; sinon, désactivez la fonction.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Tâches du contrôleur de sécurité M580

Introduction

Un contrôleur de sécurité M580 peut exécuter des applications monotâches et multitâches. A la différence d'une application monotâche qui exécute uniquement la tâche MAST, une application multitâche définit la priorité de chaque tâche.

Le contrôleur de sécurité M580 prend en charge les tâches suivantes :

- FAST
- SAFE
- MAST
- AUX0
- AUX1

Caractéristiques des tâches

Caractéristiques des tâches du contrôleur de sécurité M580

Nom de la tâche	Priorité	Modèle temporel	Plage de la période	Période par défaut	Plage de chien de garde	Chien de garde par défaut
FAST	1	Périodique	1 à 255 ms	5 ms	10 à 500 ms ²	100 ms ²
SAFE	2	Périodique	10 à 255 ms	20 ms	10 à 500 ms ²	250 ms ²
MAST ¹	3	Cyclique ⁴ ou périodique	1 à 255 ms	20 ms	10 à 1 500 ms ²	250 ms ²
AUX0 ³	4	Périodique	10 à 2550 ms	100 ms	100 à 5000 ms ²	2000 ms ²
AUX1 ³	5	Périodique	10 à 2550 ms	200 ms	100 à 5000 ms ²	2000 ms ²
1. La tâche MAST est requise, elle ne peut pas être désactivée. 2. Si CCOTF est activé (en sélectionnant Modification en ligne en mode RUN ou STOP dans l'onglet Configuration de la boîte de dialogue des propriétés du contrôleur, la valeur minimale du Chien de garde est 64 ms. 3. Pris en charge par le contrôleur de sécurité BMEP58•040S autonome. Non pris en charge par les contrôleur redondant de sécurité BMEH58•040S. 4. Les contrôleurs de sécurité BMEP58•040S autonomes prennent en charge les modèles temporels cycliques et périodiques. BMEH58•040S Les automates de sécurité à redondance de CPU prennent uniquement en charge le modèle de temps périodique.						

Priorité de la tâche

Les contrôleur de sécurité de priorité de tâche M580 exécutent les tâches en cours selon leur priorité. Lorsqu'une tâche est en cours d'exécution, elle peut être interrompue par une autre tâche de priorité supérieure. Par exemple, si une tâche périodique est planifiée pour exécuter du code, elle interrompt une tâche de priorité inférieure, mais elle attend la fin de l'exécution d'une tâche de priorité supérieure.

Remarques relatives à la configuration des tâches

Toutes les tâches non liées à la sécurité (MAST, FAST, AUX0 et AUX1) sont exécutées dans la même zone de mémoire, tandis que la tâche SAFE est exécutée dans une zone de mémoire distincte indépendante. Résultat :

- Si une tâche non liée à la sécurité dépasse son chien de garde, toutes les tâches non liées à la sécurité passent à l'état HALT, tandis que la tâche SAFE reste opérationnelle.
- Si la tâche SAFE dépasse son chien de garde, elle passe à l'état HALT, tandis que les tâches non liées à la sécurité restent opérationnelles.

Lors de la création et la configuration de tâches pour votre application, tenez compte des fonctionnalités suivantes :

Tâche SAFE :

Vous pouvez configurer cette tâche périodique uniquement pour exécuter des sections de code liées à la sécurité pour les modules d'E/S de sécurité. Comme la priorité de la tâche SAFE est inférieure à celle de la tâche FAST, l'exécution de la tâche SAFE peut être interrompue par la tâche FAST.

Définissez le temps d'exécution maximal de la tâche SAFE en configurant une valeur appropriée pour le chien de garde. Tenez compte du temps requis pour exécuter le code et lire et écrire les données liées à la sécurité. Si le temps d'exécution de la tâche SAFE dépasse la valeur du chien de garde, la tâche SAFE passe à l'état HALT, et le mot système %SW125 affiche le code d'erreur détecté 16#DEB0.

NOTE:

- Comme la priorité de la tâche FAST est supérieure à celle de la tâche SAFE, vous pouvez inclure le délai de la tâche FAST à la configuration du chien de garde de la tâche SAFE.
- Si le dépassement de l'exécution de la tâche SAFE est égal au chien de garde de sécurité (valeur égale à 1 fois et demie la valeur du chien de garde de la tâche SAFE), le contrôleur et le coprocesseur passent à l'état ERROR et la fonction de sécurité est appliquée.

Tâche MAST :

Cette tâche peut être configurée pour être cyclique ou périodique. En mode cyclique, définissez un temps d'exécution maximal en entrant une valeur appropriée pour le chien de garde MAST. Ajoutez un petit intervalle de temps à cette valeur à la fin de chaque cycle afin de permettre l'exécution des tâches système de priorité inférieure. Comme la priorité des tâches AUX est inférieure à celle de la tâche MAST, si cet intervalle n'est pas défini, cela peut empêcher l'exécution des tâches AUX. Vous pouvez ajouter un intervalle de temps de 10 % du temps d'exécution du cycle, de 1 ms minimum et 10 ms maximum.

Si le temps d'exécution d'une tâche MAST cyclique dépasse le chien de garde, la tâche MAST et toutes les autres tâches non liées à la sécurité passent à l'état HALT, et le mot système %SW125 affiche le code de l'erreur détectée 16#DEB0.

En mode périodique, la tâche MAST peut dépasser sa période. Dans ce cas, la tâche MAST est exécutée en mode cyclique et le bit système %S11 est défini.

Tâche FAST :

L'objectif de cette tâche périodique est d'exécuter une partie à haute priorité de l'application. Définissez le temps d'exécution maximal en configurant la valeur du chien de garde FAST. Comme la tâche FAST interrompt l'exécution de toutes les autres tâches, y compris de la tâche SAFE, configurez un temps d'exécution le plus court possible pour la tâche FAST. La valeur du chien de garde de la tâche FAST ne doit pas être supérieure à la période FAST.

Le temps d'exécution de la tâche FAST ne doit pas dépasser la moitié de la période configurée pour la tâche SAFE. Si cette limite est dépassée, le contrôleur peut s'arrêter.

Il est certain que le temps d'exécution de la tâche FAST ne doit pas être supérieur à la moitié de la période configurée pour la tâche SAFE, sinon le chien de garde de sécurité risque de se déclencher et de mettre le système à l'état ERROR.

Si le temps d'exécution de la tâche FAST dépasse le chien de garde, la tâche FAST et toutes les autres tâches non liées à la sécurité passent à l'état HALT, et le mot système %SW125 affiche le code de l'erreur détectée 16#DEB0.

Tâches AUX :

Les tâches AUX0 et AUX1 sont périodiques et facultatives. Leur objectif est d'exécuter une partie à faible priorité de l'application. Les tâches AUX sont exécutées uniquement après la fin de l'exécution des tâches MAST, SAFE et FAST.

Définissez le temps d'exécution maximal des tâches AUX en configurant une valeur appropriée pour le chien de garde. Si le temps d'exécution d'une tâche AUX dépasse le chien de garde, la tâche AUX et toutes les autres tâches non liées à la sécurité passent à l'état HALT, et le mot système %SW125 affiche le code de l'erreur détectée 16#DEB0.

Création d'un projet de sécurité M580

Génération d'un projet de sécurité M580

Génération d'un projet de sécurité M580

Le menu Control Expert for Safety - **Générer** propose trois commandes de génération différentes ainsi qu'une commande de signature Safe, comme suit :

Commande	Description
Générer des modifications	Permet de compiler uniquement les modifications qui ont été effectuées dans le programme d'application depuis la génération précédente, et de les ajouter au programme d'application précédemment généré.
Regénérer tout le projet	Permet de re-compiler l'ensemble du programme d'application, en remplaçant la génération précédente du programme d'application. NOTE: Pour les modules d'E/S de sécurité M580, cette commande ne génère pas un nouvel identifiant MUID (identifiant unique du module). La valeur MUID précédente est conservée.
Renouveler les ID et Regénérer tout	Permet de re-compiler l'ensemble du programme d'application, en remplaçant la génération précédente du programme d'application. NOTE: - Exécutez cette commande uniquement si les modules d'E/S de sécurité sont déverrouillés, page 295. - Pour les modules d'E/S de sécurité M580, cette commande génère un nouvel identifiant MUID (identifiant unique du module) et remplace l'identifiant existant par la nouvelle valeur.
Mettre à jour la signature SAFE	Permet de générer manuellement une signature de source SAFE, page 287 pour l'application sécurisée. NOTE: cette commande est activée uniquement si le paramètre Général > Options de génération > Gestion de la signature SAFE est défini sur A la demande de l'utilisateur .

Signature SAFE

Introduction

Les contrôleurs de sécurité M580 - à la fois autonomes et Hot Standby - incluent un mécanisme permettant de générer une empreinte SHA256 de l'application sécurisée sur la base d'un algorithme : la signature du source SAFE. Lors du transfert de l'application du PC vers le contrôleur, Control Expert compare la signature dans le PC à celle se trouvant dans

le contrôleur afin de déterminer si les applications sécurisées dans le PC et le contrôleur sont identiques ou différentes.r.

La fonction de signature SAFE est facultative. La génération d'une signature de source SAFE prend plus ou moins de temps selon la taille de l'application sécurisée. Les options de gestion de la signature SAFE vous offrent la possibilité de générer une signature de source SAFE sous la forme d'un algorithme pour votre application sécurisée :

- à chaque génération ou
- seulement si vous souhaitez générer manuellement cette signature et l'ajouter à la dernière génération ou
- dans aucun cas de figure.

Actions modifiant la signature de source SAFE

Les modifications apportées à la configuration et aux valeurs de variables peuvent entraîner la modification de la signature de source SAFE.

Changements de configuration : Les opérations de configuration suivantes modifient la signature :

Équipement	Action
Contrôleur de sécurité	Changement de référence de contrôleur à l'aide de l'option Remplacer le processeur...
	Changement de version de contrôleur à l'aide de l'option Remplacer le processeur...
	Modification d'un paramètre dans les onglets de configuration Configuration ou Redondance du contrôleur.
	Modification d'un paramètre dans un onglet du module de communication Ethernet du contrôleur (Sécurité, IP Config, RSTP, SNMP, NTP, ServicePort, Safety ..).
Coprocasseur de sécurité	Non applicable, car le coprocasseur n'est pas configurable.
Autre module de sécurité	Ajoutez/Supprimez/Déplacez un module, soit : • directement (via une commande), • indirectement (par exemple, en remplaçant une embase Ethernet à 8 emplacements avec un module de sécurité à l'emplacement 7 par une embase Ethernet à 4 emplacements, entraînant ainsi la suppression d'un module)
	Modification d'un paramètre du module de sécurité dans l'onglet Configuration Configuration (par exemple, Court-circuit pour détection 24 V, , Détection de fil ouvert) et dans le volet de gauche de l'éditeur (par exemple, Fonction, Repli).
	Modification de l'identifiant du module via la commande Renouveler les ID & Régénérer tout .

Équipement	Action
	Modification du nom de l'instance de type de données dérivé (DDT, Derived Data Type) d'équipement
Module CIP Safety	Ajout/suppression d'un module
	Modification d'un paramètre d'un module CIP Safety dans l'éditeur de DTM de l'équipement CIP Safety ou dans la liste d'équipements de l'éditeur de DTM du contrôleur maître
	Modification du nom de l'instance de type de données dérivé (DDT, Derived Data Type) d'équipement.
Alimentation de sécurité	Ajout/suppression d'une alimentation de sécurité.
Autre équipement lié à la sécurité	Modification de l'adresse topologique d'un équipement prenant en charge un équipement de sécurité, par exemple : • Déplacement d'un rack contenant un équipement de sécurité • Déplacement d'un bus ou d'une station contenant un équipement de sécurité

Changements de valeur : Sauf exception, les éléments suivants interviennent dans le calcul de la signature du source SAFE. La modification de leur valeur entraîne celle de la signature :

Type	Éléments
Programme	Tâche SAFE et sections de code associées
Variables	Variables de zone SAFE et attributs associés
type des données dérivés (DDTs, Derived Data Type)	Attributs de type de données dérivé (DDT, Derived Data Type) DDT SAFE, à l'exception des attributs de date et version
	Variables contenues dans chaque type de données dérivé (DDT, Derived Data Type), y compris les attributs associés
	DDT SAFE, même ceux non utilisés dans l'application sécurisée
DFB	Attributs de DFB SAFE, à l'exception des attributs de date et version
	Variables contenues dans chaque DFB, y compris les attributs associés
	DFB SAFE, même ceux non utilisés dans l'application sécurisée
Paramètres de portée SAFE	Tous les Paramètres du projet pour Portée = safe.
Paramètres de portée commune	Les éléments de Paramètres du projet suivants pour Portée = commun :
	Variables • Chiffres en début autorisés • Jeu de caractères • Autoriser l'utilisation du front sur EBOOL • Autoriser INT/DINT à la place de ANY_BIT

Type	Éléments
	- Autoriser l'extraction de bits pour BYTE, INT, UINT, DINT, UDINT, WORD et DWORD - Autoriser la représentation directe de tableaux - Activer la scrutation rapide de tendance - Forcer l'initialisation des références
	Programme > Langues > Commun - Autoriser les procédures - Autoriser les commentaires imbriqués - Autoriser les affectations en cascade [a:=b:=c] (ST/LD) - Autoriser les paramètres vides dans les appels informels (ST/IL) - Maintenir les liens de sortie sur les EF désactivées (EN=0) - Afficher les commentaires complets d'élément de structure
	Programme > Langues > LD Détection de front montant unique pour EBOOL
	Général > Heure¹ - Fuseau horaire personnalisé - Fuseau horaire - Décalage - Régler automatiquement l'horloge sur l'heure d'été - Tous les paramètres DEBUT et FIN sous Régler automatiquement l'horloge sur l'heure d'été
1. Ces variables ne sont pas exportées, mais la modification de leur valeur entraîne celle de la signature partielle de configuration.	

Gestion de la signature de source SAFE

La signature de source SAFE est gérée dans Control Expert dans la zone **Outils > Paramètres du projet**, en sélectionnant **Général > Paramètres de génération**, puis en sélectionnant l'un des paramètres **Gestion des signatures Safe** suivants :

- Automatique** (par défaut) : permet de générer une nouvelle signature de source SAFE à chaque exécution d'une commande **Générer**.
- A la demande de l'utilisateur** : permet de générer une nouvelle signature de source SAFE lorsque la commande **Générer > Mettre à jour la signature SAFE** est exécutée.

NOTE: avec l'option **A la demande de l'utilisateur**, Control Expert crée une signature de source SAFE égale à 0 à chaque génération. Si vous n'exécutez pas la commande **Générer > Mettre à jour la signature SAFE**, cela signifie que vous décidez de ne pas utiliser la fonction de signature SAFE.

Transférer une application de l'ordinateur vers le contrôleur

Lors du téléchargement d'une application du PC vers le contrôleur, Control Expert compare la signature de source SAFE de l'application téléchargée avec celle présente dans le contrôleur. Control Expert se comporte comme suit :

Nouvelle signature SAFE	Signature SAFE de contrôleur	Control Expert affiche :
Quelconque	Pas d'application	Confirmation du transfert
Toute valeur (sauf 0)	0	Confirmation du transfert
0	0	Confirmation du transfert
0	Toute valeur (sauf 0)	Confirmation du transfert, puis "Cette action réinitialisera la signature SAFE", puis nouvelle confirmation du transfert
XXXX = YYYY ²	YYYY	Confirmation du transfert
XXXX ≠ YYYY ³	YYYY	Confirmation du transfert, puis "Cette action modifiera l'application SAFE", puis nouvelle confirmation du transfert
1. La valeur "0" indique qu'aucune signature de source SAFE n'a été générée (automatiquement ou manuellement). 2. L'application sécurisée du PC (XXXX) et l'application sécurisée du contrôleur (YYYY) sont IDENTIQUES. 3. L'application sécurisée du PC (XXXX) et l'application sécurisée du contrôleur (YYYY) sont DIFFÉRENTES.		

Affichage de la signature de source SAFE

Chaque signature de source SAFE utilisée se compose d'une série de valeurs hexadécimales, qui peut être très longue. Il est donc difficile pour un utilisateur de lire et comparer directement ces valeurs. Pour réaliser facilement des comparaisons, il est possible de coller ces valeurs dans un éditeur de texte adéquat. Vous trouverez la signature de source SAFE à différents endroits dans Control Expert :

- **Propriétés du projet**, onglet > **Identification** (voir EcoStruxure™ Control Expert, Modes de fonctionnement) : Dans le **Navigateur du projet**, cliquez avec le bouton droit sur **Projet** et sélectionnez **Propriétés**.
- **PLCScreen**, onglet > **Information** (voir EcoStruxure™ Control Expert, Modes de fonctionnement) : Dans le **Navigateur du projet**, accédez à **Projet > Configuration > Bus PLC > <CPU>**, cliquez avec le bouton droit et sélectionnez **Ouvrir**, puis sélectionnez l'onglet **Animation**.
- Boîte de dialogue **PC < - - > Comparaison PLC** (voir EcoStruxure™ Control Expert, Modes de fonctionnement) : Sélectionnez cette commande dans le menu **PLC**.

- Boîte de dialogue **Transférer le projet vers PLC** (voir EcoStruxure™ Control Expert, Modes de fonctionnement) : Sélectionnez cette commande dans le menu **PLC** (ou dans la boîte de dialogue **PC < - - > Comparaison PLC**).

Différences entre la signature de source SAFE et le SAId

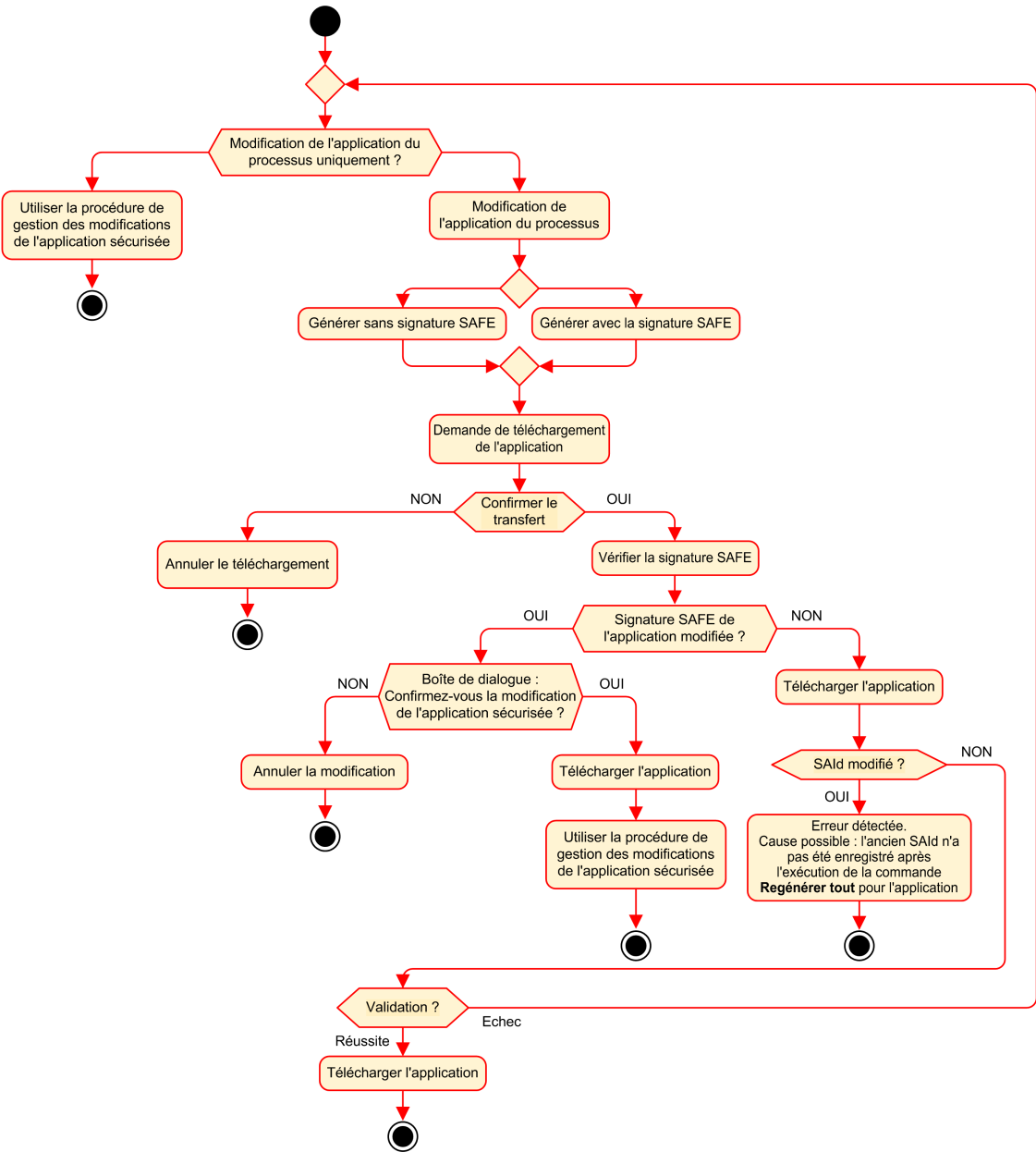
La signature de source SAFE a été introduite afin de vérifier *théoriquement* que l'application sécurisée n'a pas changé. Utilisez cette fonction chaque fois que l'application du processus est modifiée, page 293, pour éviter toute modification involontaire de l'application sécurisée.

Bien qu'elle soit fiable, la signature de source SAFE ne suffit pas pour les applications de sécurité. En effet, un même code source peut correspondre à différents codes binaires (exécutables), en fonction de l'option de génération utilisée après la dernière modification du code sécurisé.

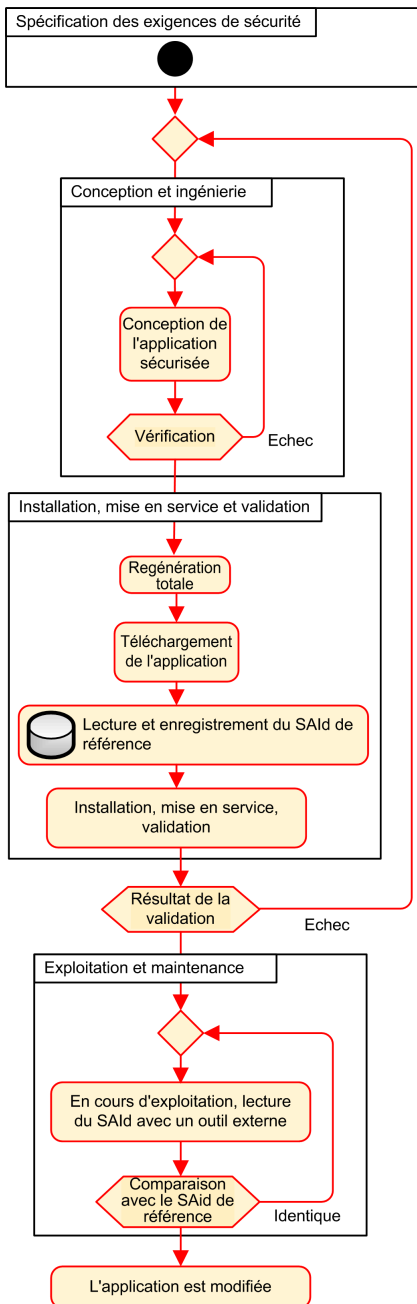
Le SAId, page 386 peut être évalué en cours d'exécution seulement. Il est calculé deux fois et comparé par le contrôleur et par le coprocesseur, sur la base du code binaire exécuté par l'application sécurisée. Le SAId étant sensible à toutes les modifications, y compris celles apportées par une commande **Regénérer tout** après la génération du projet, utilisez une commande **Regénérer tout** pour générer une version de référence de l'application sécurisée. Cette procédure, page 294 vous permet toute forme de génération (**Regénérer tout**, **Générer des modifications** en ligne ou hors ligne) pour les modifications de l'application de processus, sans aucune modification de l'identifiant SAId.

Utilisez le SAId pour vous assurer que l'application sécurisée est bien celle qui a été validée. Le SAId n'est pas automatiquement testé par l'application. Pour cette raison, vérifiez régulièrement (par exemple, via Control Expert ou une IHM) en lisant la sortie du bloc fonction S_SYST_STAT_MX ou le contenu du mot système %SW169, page 419.

Modification de l'application du processus - Procédure simplifiée



Gestion du SAId



Verrouillage de la configuration des modules d'E/S de sécurité M580

Verrouillage de la configuration des modules d'E/S de sécurité M580

Verrouillage de la configuration d'un module d'E/S de sécurité

Chaque module d'E/S de sécurité dispose d'un bouton de verrouillage de la configuration (voir Modicon M580 - Guide de planification du système de sécurité), que vous trouverez en haut à l'avant du module. Ce bouton de verrouillage permet d'éviter les modifications indésirables de la configuration du module d'E/S. Le verrouillage de la configuration d'un module d'E/S peut permettre d'éviter une tentative de configuration frauduleuse, ou simplement d'éviter les erreurs de configuration.

Pour atteindre un niveau d'intégrité de la sécurité (SIL), verrouillez chaque module d'E/S de sécurité après sa configuration, et avant de commencer ou continuer des opérations.

⚠ AVERTISSEMENT

PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ

Verrouillez chaque module d'E/S de sécurité, une fois configuré mais avant de lancer les opérations.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Les mécanismes de verrouillage et de déverrouillage fonctionnent comme suit :

- Pour verrouiller la configuration d'un module d'E/S, appuyez en continu sur le bouton de verrouillage durant plus de 3 secondes, puis relâchez-le.
- Pour déverrouiller la configuration d'un module d'E/S, appuyez en continu sur le bouton durant plus de 3 secondes, puis relâchez-le.

Scénarios de verrouillage de configuration de module d'E/S de sécurité

La procédure à suivre pour verrouiller la configuration d'un module d'E/S de sécurité de niveau SIL3 varie en fonction du contexte, par exemple :

- Première configuration de modules d'E/S

- Remplacement rapide de modules d'E/S
- Modification de configuration en temps réel (CCOTF) de modules d'E/S

La procédure à suivre pour chaque scénario est décrite ci-dessous.

Première configuration de modules d'E/S de niveau SIL3 :

Etape	Action
1	Connectez Control Expert au contrôleur de sécurité M580.
2	Utilisez la commande Transférer le projet à partir de PLC l'automate pour charger le projet du contrôleur dans Control Expert.
3	Dans la fenêtre Bus PLC de Control Expert, ouvrez chaque module d'E/S de sécurité SIL3 et vérifiez qu'il est correctement configuré.
4	Dans une table d'animation de Control Expert, affichez le DDDT de chaque module d'E/S de sécurité SIL3 et vérifiez que la configuration de chaque module est identique à celle de l'étape 3 ci-dessus.
5	Verrouillez la configuration de chaque module d'E/S SIL3, en appuyant en continu sur le bouton de verrouillage de la configuration (voir Modicon M580 - Guide de planification du système de sécurité) pendant plus de 3 secondes, puis relâchez-le.
6	Vérifiez dans la table d'animation la validité de l'état du bit de verrouillage (CONF_LOCKED) pour chaque module d'E/S SIL3.

Remplacement rapide d'un module d'E/S SIL3 :

Etape	Action
1	Remplacez le module d'E/S de sécurité SIL3 par un module neuf.
2	Connectez Control Expert au contrôleur de sécurité M580 en mode de fonctionnement de maintenance, page 269.
3	Dans la fenêtre Bus PLC de Control Expert, ouvrez chaque module d'E/S de sécurité SIL3 et vérifiez qu'il est correctement configuré.
4	Dans une table d'animation de Control Expert, affichez le DDDT de chaque module d'E/S de sécurité SIL3 et vérifiez que la configuration de chaque module n'a pas été modifiée et est identique à celle de l'étape 3 ci-dessus.
5	Verrouillez la configuration de chaque module d'E/S SIL3, en appuyant en continu sur le bouton de verrouillage de la configuration (voir Modicon M580 - Guide de planification du système de sécurité) pendant plus de 3 secondes, puis relâchez-le.
6	Vérifiez dans la table d'animation la validité de l'état du bit de verrouillage (CONF_LOCKED) pour chaque module d'E/S SIL3.

Changement de configuration en temps réel (CCOTF) pour ajouter un nouveau module d'E/S de sécurité SIL3 :

Etape	Action
1	Connectez Control Expert au contrôleur de sécurité M580 en mode de fonctionnement de maintenance, page 269.
2	Ajoutez un nouveau module d'E/S de sécurité SIL3 à la configuration, et modifiez ses réglages au besoin.
3	Exécutez la commande Générer > Générer le projet .
4	Dans la fenêtre Bus PLC de Control Expert, ouvrez chaque module d'E/S de sécurité SIL3 et vérifiez qu'il est correctement configuré.
5	Dans une table d'animation de Control Expert, affichez le DDDT de chaque module d'E/S de sécurité SIL3 et vérifiez que la configuration de chaque module n'a pas été modifiée et est identique à celle de l'étape 3 ci-dessus.
6	Verrouillez la configuration de chaque module d'E/S SIL3, en appuyant en continu sur le bouton de verrouillage de la configuration (voir Modicon M580 - Guide de planification du système de sécurité) pendant plus de 3 secondes, puis relâchez-le.
7	Vérifiez dans la table d'animation la validité de l'état du bit de verrouillage (CONF_LOCKED) pour chaque module d'E/S SIL3.
8	Dans le menu PLC de Control Expert, configurez le contrôleur en mode sécurité, page 268.

Initialisation des données dans Control Expert

Initialisation des données dans Control Expert pour le PAC de sécurité M580

Deux commandes d'initialisation

Le menu **Automate** de Control Expert contient deux commandes d'initialisation des données :

- La commande **Initialiser** initialise les données de l'espace de nom de processus (non liées à la sécurité), qui peuvent être utilisées par les tâches MAST, FAST, AUX0 et AUX1. Vous pouvez exécuter cette commande si le PAC est en mode sécurité ou en maintenance et à l'état STOP. Cette commande équivaut à la configuration du bit système %S0 (COLDSTART) sur 1.
NOTE: La configuration du bit %S0 sur 1 initialise les données uniquement dans l'espace de nom de processus. Il n'affecte pas les données de l'espace de nom de sécurité.
- La commande **Initialiser** initialise uniquement les données de l'espace de nom de sécurité, qui peuvent être utilisées exclusivement par la tâche SAFE. Vous pouvez exécuter cette commande uniquement si la tâche SAFE est en mode maintenance et à l'état STOP ou HALT. Si cette commande est exécutée lorsque la tâche SAFE est à l'état HALT, la tâche SAFE redémarre à l'état STOP.

Les commandes **Initialiser** et **Initialiser la sécurité** entraînent un démarrage à froid, page 282.

Utilisation des tables d'animation dans Control Expert

Tables d'animations et écrans des opérateurs

Introduction

Un contrôleur de sécurité M580 prend en charge trois types de tables d'animation, chacune associée à l'une des zones de données suivantes :

- Les tables d'animation de la zone de processus peuvent inclure uniquement des données de l'espace de nom de traitement.
- Les tables d'animation de la zone de sécurité peuvent inclure uniquement des données de l'espace de nom de sécurité.
- Les tables d'animation globales peuvent inclure des données de l'ensemble de l'application, notamment les données créées pour l'espace de nom de sécurité et de processus, et les variables globales.

NOTE: Dans une table d'animation globale, les noms des variables de données incluent un préfixe indiquant l'espace de nom source, comme suit :

- Une variable de données de l'espace de nom Safe s'affiche sous la forme "SAFE.<nom de la variable>".
- Une variable de données de l'espace de nom Process s'affiche sous la forme PROCESS.<nom de la variable>".
- Une variable de données située dans l'espace de nom Global (ou Application) n'affiche que le <nom de la variable>, sans le préfixe d'espace de nom.

Les données de processus et de sécurité d'un contrôleur de sécurité M580 sont également accessibles via des processus externes (par exemple SCADA ou HMI)

Les possibilités de création et de modification d'une table d'animation et d'exécution des fonctions de la table d'animation dépendent de l'espace de nom des variables attribuées et du mode de fonctionnement du projet de sécurité.

Conditions de création et de modifications des tables d'animation

La création et la modification des tables d'animation impliquent l'ajout ou la suppression de variables de données. La possibilité d'ajout ou de suppression de variables de données dans une table d'animation dépend des éléments suivants :

- Espace de nom (sécurité ou processus) où se trouvent les variables de données.

- Mode de fonctionnement (sécurité ou maintenance) du contrôleur de sécurité M580.

Lorsque Control Expert est connecté au contrôleur de sécurité M580 , vous pouvez créer et modifier des tables d'animation comme suit

- Vous pouvez ajouter ou supprimer des variables d'espace de nom de processus dans un processus ou une table d'animation globale si le contrôleur de sécurité M580 fonctionne en mode sécurité ou maintenance.
- Vous pouvez ajouter ou supprimer des variables d'espace de nom de sécurité dans une table d'animation de sécurité si le contrôleur de sécurité M580 fonctionne en mode maintenance.
- Vous pouvez ajouter ou supprimer des variables d'espace de nom de sécurité dans une table d'animation de sécurité si le contrôleur de sécurité M580 fonctionne en mode sécurité uniquement dans le cas où les paramètres du projet n'incluent pas de tables d'animation dans les informations transférées.

NOTE: Pour inclure ou inclure des tables d'animation des informations de chargement dans Control Expert, sélectionnez **Outils > Paramètres du projet...** pour ouvrir la fenêtre **Paramètres du projet...** , puis naviguez jusqu'à **Paramètres du projet > Général > Données intégrées PLC > Informations de chargement > Tables d'animation.**

Conditions d'utilisation des tables d'animation

Vous pouvez utiliser les tables d'animation pour forcer une valeur de variable, annuler le forçage d'une valeur de variable, modifier une valeur de variable ou modifier plusieurs valeurs de variables. La possibilité d'exécuter ces fonctions dépend de l'espace de nom dans lequel se trouve une variable et du mode de fonctionnement du contrôleur de sécurité M580 :

- La lecture et l'écriture des valeurs des variables de processus ou de données globales sont possibles en mode sécurité et maintenance.
- Le mode maintenant permet la lecture et l'écriture des valeurs des variables de sécurité.
- Le mode sécurité permet uniquement la lecture des valeurs des variables de sécurité.

Création de tables d'animation dans l'espace de nom de sécurité ou de processus dans Control Expert

Control Expert permet de créer des tables d'animation pour l'espace de nom de sécurité ou de processus :

- Dans une fenêtre de section de code de sécurité ou de processus, cliquez avec le bouton droit dans la fenêtre de code, puis sélectionnez :
 - **Initialiser la table d'animation** pour ajouter l'objet de données à une table d'animation existante dans un espace de nom de sécurité ou de processus, ou
 - **Initialiser une nouvelle table d'animation** pour ajouter l'objet de données à une nouvelle table d'animation dans un espace de nom de sécurité ou de processus.

Dans chaque cas, toutes les variables de la section de code sont ajoutées à la table d'animation (existante ou nouvelle).

- Dans le **Navigateur de projet**, dans la zone de données de processus ou de sécurité, cliquez avec le bouton droit sur le dossier **Tables d'animation**, puis sélectionnez **Nouvelle table d'animation..** Control Expert pour créer une nouvelle table d'animation vide. Vous pouvez ensuite ajouter des variables issues d'un espace de nom (de sécurité ou de processus) lié à la table.

Création de tables d'animation de portée globale

Créez une table d'animation dans le **Navigateur de projet** en cliquant avec le bouton droit sur le dossier **Tables d'animation** puis sélectionnez la **Nouvelle table d'animation**. Vous pouvez ajouter des variables à la nouvelle table d'animation de plusieurs manières :

- *Glisser-déposer* : Vous pouvez faire glisser une variable d'un éditeur de données pour la déposer dans la table d'animation globale. Comme la portée de la table d'animation inclut l'ensemble de l'application, vous pouvez faire glisser la variable de l'**Éditeur de données de sécurité**, l'**Éditeur de données de processus**, ou l'**Éditeur de données globales**.
- *Boîte de dialogue Sélection d'instance* : Vous pouvez double cliquer sur une ligne de la table d'animation, puis cliquez sur le bouton en forme d'ellipse pour ouvrir la boîte de dialogue **Sélection d'instance**. Utilisez la liste de filtrage en haut à droite de la boîte de dialogue pour sélectionner l'une des zones suivantes du projet :
 - **SECURITE** : afficher des objets de données associés à la zone de sécurité.
 - **PROCESSUS** : afficher des objets de données associés à la zone de processus.
 - **APPLICATION** : afficher les objets de données de portée application de niveau supérieur.

Sélectionnez un objet de données, puis cliquez sur **OK** pour ajouter l'élément à la table d'animation.

NOTE: Pour les objets de données ajoutés à une table d'animation globale depuis :

- la zone des processus, le préfixe **PROCESS** est ajouté au nom de la variable (par exemple **PROCESS.variable_01**)
- la zone de sécurité, le préfixe **SAFE** est ajouté au nom de la variable (par exemple **SAFE.variable_02**)
- la zone globale, aucun préfixe n'est ajouté au nom de la variable.

Affichage des données sur les écrans d'exploitation

Vous pouvez afficher des données sur un écran d'exploitation (application HMI, SCADA ou FactoryCast, par exemple) de la même façon que des données dans une table d'animation. Les variables de données disponibles sont les variables incluses dans le dictionnaire de données de Control Expert.

Pour activer le dictionnaire de données, ouvrez la fenêtre **Outils > Paramètres du projet...**, puis dans la fenêtre **Étendue > commune** de la fenêtre, sélectionnez **Général > Données intégrées PLC > Dictionnaire de données**.

Le dictionnaire de données permet à l'opérateur de visualiser les variables de données sur l'écran d'exploitation :

- Les variables du nom d'espace de sécurité incluent toujours le préfixe SAFE, et sont accessibles uniquement via le format "SAFE.<nom de la variable>".
- Les variables de l'espace de nom Global ou Application n'incluent pas de préfixe et ne sont accessibles qu'en utilisant le <nom de la variable> sans préfixe.
- Le paramètre **Utilisation de l'espace de nom de processus** détermine la façon dont l'écran d'exploitation permet d'accéder aux variables d'espace de nom de processus.
 - Si vous sélectionnez **Utilisation de l'espace de nom de processus**, l'écran d'exploitation peut lire les variables de la zone de processus uniquement via le format "PROCESS.<nom de la variable>".
 - Si vous sélectionnez **Utilisation de l'espace de nom de processus**, l'écran d'exploitation ne peut lire les variables de la zone de processus qu'en utilisant le format "<nom de la variable>" sans le préfixe PROCESS.

NOTE: Si deux variables sont déclarées avec le même nom (une dans l'espace de nom de processus et l'autre dans l'espace de nom global), seule la variable de l'espace de nom global est accessible par une IHM, un système SCADA ou une application Factory Cast.

Vous pouvez utiliser la boîte de dialogue **Sélection d'instance** pour accéder à des objets de données spécifiques.

AVIS
VALEUR DE VARIABLE INATTENDUE • Assurez-vous que les paramètres de projet de l'application sont corrects. • Vérifiez la syntaxe permettant d'accéder aux variables dans les différents espaces de nom. Le non-respect de ces instructions peut provoquer des dommages matériels.

Pour éviter d'accéder à la mauvaise variable :

- Utilisez des noms différents pour déclarer les variables dans l'espace de nom de processus et dans l'espace de nom global ou
- Sélectionnez **Utilisation de l'espace de nom de processus** et respectez la syntaxe suivante pour accéder aux variables portant un nom identique :
 - "PROCESS.<nom de la variable>" pour les variables déclarées dans l'espace de nom de processus.
 - <nom de la variable> sans préfixe pour les variables déclarées dans l'espace de nom global

Outil d'analyse des tendances

L'outil d'analyse des tendances de Control Expert n'est pas utilisable avec un projet de sécurité M580.

Ajout de sections de code

Ajout d'un code à un projet de sécurité M580

Utilisation des tâches dans Control Expert

Dans l'espace de nom de processus, Control Expert inclut la tâche MAST par défaut. La tâche MAST ne peut pas être supprimée. Cependant, vous pouvez ajouter les tâches FAST, AUX0 et AUX1. Notez que la création d'une tâche dans la partie processus d'un projet de sécurité est similaire à la création d'une tâche dans un projet non lié à la sécurité. Pour plus d'informations, consultez la rubrique *tâcheCréer et configurer une tâche* dans le manuel *EcoStruxure™ Control Expert - Modes de fonctionnement*.

Dans l'espace de nom de sécurité, Control Expert inclut la tâche SAFE par défaut. La tâche SAFE ne peut pas être supprimée et aucune autre tâche ne peut être ajoutée à la section **Sécurité du programme** du **Navigateur de projet** dans Control Expert. Vous pouvez ajouter plusieurs sections à la tâche SAFE.

Configuration des propriétés de la tâche SAFE

La tâche SAFE ne prend en charge que l'exécution périodique (l'exécution cyclique n'est pas prise en charge). Les paramètres **Période** et **Chien de garde** de la tâche SAFE sont des entrées de la boîte de dialogue **Propriétés** de la tâche SAFE et prennent en charge la plage de valeurs suivante :

- Période de la tâche SAFE : 10 à 255 ms avec une valeur par défaut de 20 ms.
- Chien de garde de la tâche SAFE : De 10 à 500 ms, par incréments de 10 ms, avec une valeur par défaut de 250 ms.

Réglez la **Période** de la tâche SAFE sur une valeur minimum en fonction de la taille des données liées à la sécurité et du modèle d'automate. La période minimum de la tâche SAFE peut être calculée avec les formules suivantes :

- Valeur absolue minimum pour une communication sécurisée des E/S :
 - 10 ms
- Durée (en ms) nécessaire pour transférer et comparer les données liées à la sécurité entre l'UC et le coprocesseur :
 - $(0,156 \times \text{Data_Safe_Size}) + 2$ ms (pour BMEP584040S, BMEP586040S, BMEH584040S et BMEH586040S)
 - $(0,273 \times \text{Taille_Données_Safe}) + 2$ ms (pour BMEP582040S et BMEH582040S)

Où Taille_Données_Safe est la taille en Ko des données liées à la sécurité.

- Temps supplémentaire (en ms) dont les PAC redondants ont besoin pour transférer les données liées à la sécurité entre le PAC principal et le PAC redondant :
 - $(K1 \times T\grave{a}che_{ko} + K2 \times T\grave{a}che_{DFB}) / 500$

Dans cette formule :

- $T\grave{a}che_{DFB}$ = nombre de DFB déclarés dans la partie sécurisée de l'application.
- $T\grave{a}che_{ko}$ = taille (en Ko) des données liées à la sécurité, échangées par la tâche SAFE entre les PAC principal et redondant.
- K1 et K2 sont des constantes, dont les valeurs sont déterminées par le module d'UD utilisé dans l'application :

Coefficient	BMEH582040S	BMEH584040S et BMEH586040S
K1	32,0	10,0
K2	23,6	7,4

NOTE:

- La valeur obtenue par ces formules est un minimum absolu pour la période de la tâche SAFE, valable uniquement pour une première estimation de la durée limite du cycle SAFE. Cela n'inclut pas le temps nécessaire pour exécuter le code utilisateur, ni la marge nécessaire pour l'opération prévue du système multitâche du PAC. Consultez la rubrique Considérations relatives au débit du système dans le document *Modicon M580 - Guide de planification du système autonome pour architectures courantes*.
- Par défaut, les valeurs Taille_Safe_Données et Taille_{ko} sont égales. Elles sont consultables respectivement dans le menu **Automate > Utilisation de la mémoire** et l'écran **Automate > Redondance d'UC**.

Exemples de calcul

Exemples de résultats de calcul de la période minimum de la tâche SAFE :

Période minimum de la tâche Safe (ms)					
Taille _{ko} ¹	Nb _{inst_DFB}	BMEP582040S	BMEP584040S ou BMEP586040S	BMEH582040S	BMEH584040S ou BMEH586040S
0	0	10	10	10	10
50	10	16	10	20	11
100	10	30	18	37	20
150	10	43	25	54	29
200	10	57	33	70	37

Période minimum de la tâche Safe (ms)					
Taille _{ko} ¹	Nb _{inst_DFB}	BMEP582040S	BMEP584040S ou BMEP586040S	BMEH582040S	BMEH584040S ou BMEH586040S
250	10	71	41	87	46
300	20	84	49	105	55
350	20	98	57	121	64
400	20	112	64	138	73
450	20	125	72	155	81
500	20	139	80	172	90
550	30	-	88	-	99
600	30	-	96	-	108
650	30	-	103	-	117
700	30	-	111	-	126
750	30	-	119	-	134
800	40	-	127	-	143
850	40	-	135	-	152
900	40	-	142	-	161
950	40	-	150	-	170
1000	40	-	158	-	179
1. Sizekbytes et Data_Safe_Size sont supposés être égaux.					

NOTE: Configurez le chien de garde de la tâche SAFE avec une valeur supérieure à la **Période** de la tâche SAFE.

Pour obtenir des informations sur la manière dont la configuration de la tâche SAFE affecte le délai de sécurité du processus, consultez la rubrique *Délai de sécurité de processus*, page 161.

Pour obtenir des informations sur la priorité d'exécution de la tâche SAFE, consultez la rubrique *Tâches du PAC de sécurité M580*, page 283.

Création de sections de code

Cliquez avec le bouton droit sur le dossier **Section** d'une tâche et sélectionnez **Nouvelle section...** pour ouvrir une boîte de configuration. Pour les tâches de sécurité et de processus, les langages de programmation suivants sont disponibles :

Langage	Tâches de sécurité	Tâches de processus			
	SAFE	MAST	FAST	AUX0	AUX1
IL	–	✓	✓	✓	✓
FBD	✓	✓	✓	✓	✓
LD	✓	✓	✓	✓	✓
Segment LL984	–	✓	✓	✓	✓
SFC	–	✓	✓	✓	✓
ST	–	✓	✓	✓	✓
✓ : disponible					
– : non disponible					

Excepté ces restrictions sur le langage de programmation disponibles pour la tâche SAFE, la configuration de la nouvelle section est similaire à celle d'un projet M580 non lié à la sécurité. Pour plus d'informations, consultez la rubrique *sections FBD, LD, IL ou ST*Boîte de dialogue des propriétés des sections FBD, LD, IL ou ST dans le manuel *EcoStruxure™ Control Expert - Modes de fonctionnement*.

Ajout de données aux sections de code

Comme la tâche SAFE est séparée des tâches de processus, seules les données accessibles dans l'**Editeur de données de sécurité** sont disponibles pour l'ajout à la section de code de la tâche SAFE. Ces données incluent :

- Variables de sécurité non localisées (c'est-à-dire sans adresse %M ou %MW) créées dans l'**Editeur de données de sécurité**.
- Objets de données inclus aux structures DDT des équipements de modules de sécurité M580.

Les données disponibles pour les sections de code non liées à la sécurité incluent toutes les données de la portée de l'espace de nom de processus. Cela inclut toutes les données de projet, sauf :

- Données exclusivement disponibles pour l'espace de nom SAFE (voir ci-dessus).
- Objets de données créés dans l'**Editeur de données globales**.

Analyse de code

Lorsque vous analysez ou créez un projet, Control Expert affiche un message de détection d'erreur si :

- les données appartenant à l'espace de nom de processus sont incluses à la tâche SAFE.
- les données appartenant à l'espace de nom de sécurité sont incluses à une tâche de processus (MAST, FAST, AUX0, AUX1).
- Les bits (%M) ou les mots (%MW) localisés sont inclus à la section de la tâche SAFE.

Requête de diagnostic

Introduction

La requête de diagnostic n'est disponible que pour les alimentations de sécurité M580 situées dans un rack principal, via le bloc fonction PWS_DIAG. Un rack principal est défini par une adresse égale à 0 et un module d'UC ou CRA (adaptateur de communication) à l'emplacement 0 ou 1. Un rack d'extension n'est pas un rack principal.

L'UC peut émettre une requête de diagnostic concernant les alimentations redondantes du rack local et, via un CRA, les alimentations redondantes situées sur un rack distant. Si les alimentations maître et esclave sont opérationnelles, l'alimentation maître passe en mode de diagnostic maître et l'alimentation esclave passe en mode de diagnostic esclave. Les voyants LED indiquent que le test est en cours d'exécution.

NOTE: Cette requête n'est pas implémentée lors de la mise sous tension.

Une fois le test de diagnostic terminé, l'alimentation maître retourne au mode de fonctionnement normal et l'esclave passe soit dans l'état normal, soit dans l'état d'erreur (en fonction des résultats des tests). Les résultats des tests sont stockés dans la mémoire de l'alimentation.

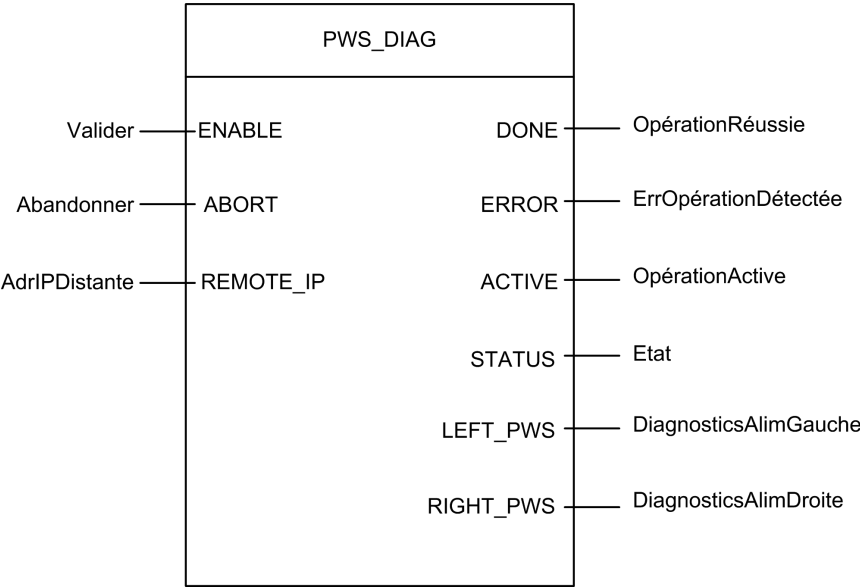
Données renvoyées par une requête de diagnostic

Les alimentations renvoient à l'UC les informations de diagnostic suivantes :

- Température ambiante de l'alimentation.
- Tension et intensité sur la ligne d'embase 3,3 V.
- Tension et intensité sur la ligne d'embase 24 V.
- Energie totale cumulée par l'alimentation, depuis sa fabrication, sur les lignes d'embase 3,3 V et 24 V.
- Temps de fonctionnement en tant que maître depuis la dernière mise sous tension et depuis la fabrication.
- Temps de fonctionnement total en tant qu'esclave depuis la dernière mise sous tension et depuis la fabrication.

- Durée de vie restante en pourcentage (LTPC) ou délai de maintenance préventive : de 100 % à 0 %.
NOTE: Pas de permutation si 0 %.
- Nombre de mises sous tension de l'alimentation.
NOTE: Le système SCADA permet de réinitialiser le nombre de mises sous tension depuis l'installation et tous les autres diagnostics.
- Nombre de fois où la tension principale du BMXCPS4002S a chuté au-dessous du niveau de sous-tension 1 (95 VCA).
- Nombre de fois où la tension principale du BMXCPS4002S a dépassé le niveau de surtension 2 (195 VCA).
- Nombre de fois où la tension principale du BMXCPS4022S a chuté au-dessous du niveau de sous-tension 1 (20 VCC).
- Nombre de fois où la tension principale du BMXCPS4022S a dépassé le niveau de sous-tension 2 (40 VCC).
- Nombre de fois où la tension principale du BMXCPS3522S a chuté au-dessous du niveau de sous-tension 1 (110 VCC).
- Nombre de fois où la tension principale du BMXCPS3522S a dépassé le niveau de sous-tension 2 (140 VCC).
- Statut actuel de l'alimentation (maître/esclave/inopérante)

Représentation en FBD



Paramètres

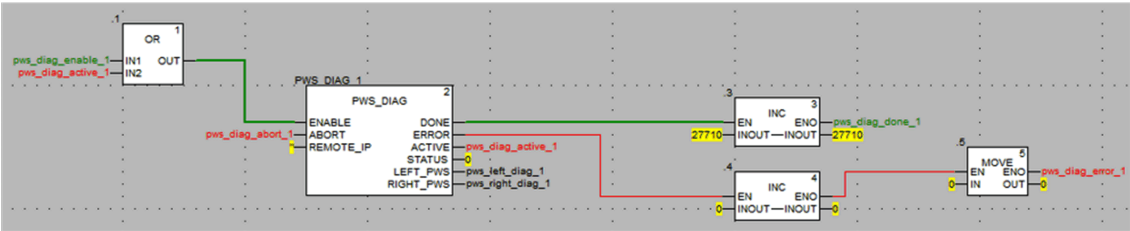
Paramètres d'entrée :

Nom du paramètre	Type de données	Description
ENABLE	BOOL	Si ce paramètre est activé, l'opération est activée.
ABORT	BOOL	Si ce paramètre est activé, l'opération active est abandonnée.
REMOTE_IP	STRING	Adresse IP ("ip1.ip2.ip3.ip4") de la station contenant le module d'alimentation. Laissez ce champ vide (chaîne "") ou n'attachez aucune variable à la broche de contact avec l'alimentation située dans le rack local.

Paramètres de sortie:

Nom du paramètre	Type de données	Description
DONE	BOOL	Activé lorsque l'opération s'est déroulée correctement.
ERROR	BOOL	Activé lorsque l'opération a été abandonnée suite à un échec.
ACTIVE	BOOL	Activé lorsque l'opération est active.
STATUS	WORD	Identifiant d'erreur détectée.
LEFT_PWS	ANY	Données de diagnostic pour l'alimentation de gauche. Utilisez une variable de type PWS_DIAG_DDT_V2, page 141 pour une interprétation correcte.
RIGHT_PWS	ANY	Données de diagnostic pour l'alimentation de droite. Utilisez une variable de type PWS_DIAG_DDT_V2 pour une interprétation correcte.

Exemple



pws_left_diag_1		PWS_DIAG_DDT	
pws_right_diag_1		PWS_DIAG_DDT	
PwsMajorVersion	153	BYTE	Power Supply major version
PwsMinorVersion	162	BYTE	Power Supply minor version
Model	0	BYTE	Power Supply Model identifier
State	12	BYTE	Power Supply state
I33BacPos	0	UINT	Measure current of 3V3 Bac in nominal role (producer)
V33Buck	0	UINT	Measure voltage of 3V3 Buck
I24Bac	0	UINT	Measure current of 24V Bac
V24Int	0	UINT	Measure voltage of 24V Int
Temperature	0	INT	Measure of Ambient Temperature
OperTimeMaster...	16935	DINT	Operating Time as Master since last Power ON
OperTimeSlaveSi...	2	DINT	Operating Time as Slave since last Power ON
OperTimeMaster	282128	DINT	Operating Time as Master since Manufacturing
OperTimeSlave	44	DINT	Operating Time as Slave Since Manufacturing
Work	0	DINT	Work supplied since Manufacturing
RemainingLTPC	0	UINT	Remaining Life Time in percent
NbPowerOn	0	UINT	Number of Power ON since Manufacturing
NbVoltageLowFail	0	UINT	Number of failure detected on Primary Voltage by Low Threshold
NbVoltageHighFail	0	UINT	Number of failure detected on Primary Voltage by High Threshold

Commandes de permutation et d'effacement

Introduction

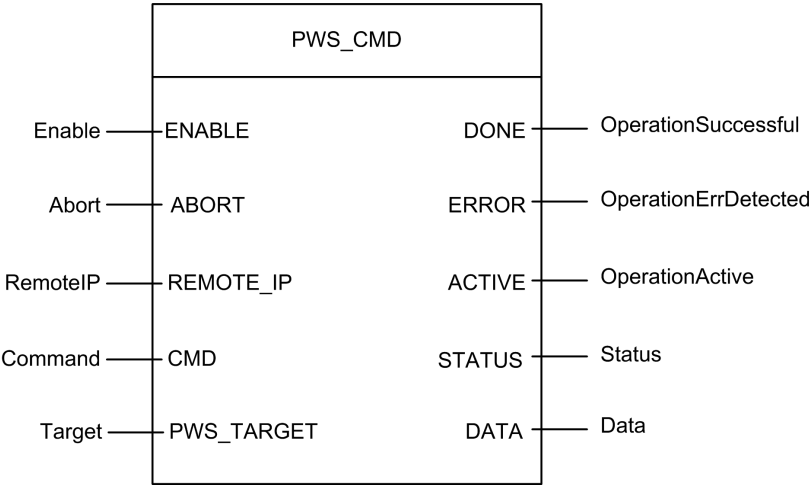
Le bloc fonction PWS_CMD peut être utilisé pour émettre deux commandes :

- Demande de permutation : cette commande indique l'alimentation à utiliser en tant que maître. Si les deux alimentations sont opérationnelles, l'alimentation spécifiée devient l'alimentation maître et l'autre devient l'esclave.
- Demande d'effacement : cette commande remet à zéro les compteurs suivants :
 - nombre de chutes de la tension principale au-dessous du seuil de sous-tension 1.
 - nombre de chutes de la tension principale au-dessous du seuil de sous-tension 2.
 - nombre de mises sous tension de l'alimentation.

Ces deux commandes ne sont disponibles que pour les alimentations installées sur le rack principal. Un rack principal est défini par une adresse égale à 0 et un module d'UC ou CRA (adaptateur de communication) à l'emplacement 0 ou 1. Un rack d'extension n'est pas un rack principal.

Les voyants LED indiquent l'état d'exécution en cours de la commande. Un enregistrement de l'événement est stocké dans la mémoire de l'alimentation.

Représentation en FBD



Paramètres

Paramètres d'entrée:

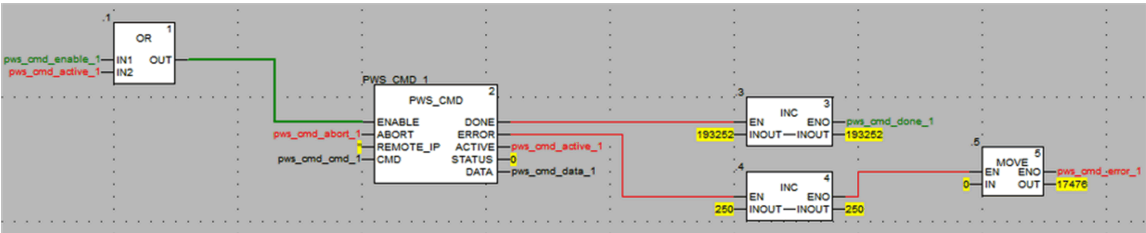
Nom du paramètre	Type de données	Description
ENABLE	BOOL	Si ce paramètre est activé, l'opération est activée.
ABORT	BOOL	Si ce paramètre est activé, l'opération active est abandonnée.
REMOTE_IP	STRING	Adresse IP ("ip1.ip2.ip3.ip4") de la station contenant le module d'alimentation. Laissez ce champ vide (chaîne "") ou n'attachez aucune variable à la broche de contact avec l'alimentation située dans le rack local.
CMD	ANY	Utilisez une variable de type PWS_CMD_DDT pour une interprétation correcte. Codes de commande disponibles : 1 = permutation 3 = effacement
PWS_TARGET	BYTE	Alimentation vers l'adresse : 1 = gauche 2 = droite 3 = les deux

Paramètres de sortie:

Nom du paramètre	Type de données	Description
DONE	BOOL	Activé lorsque l'opération s'est déroulée correctement.
ERROR	BOOL	Activé lorsque l'opération a été abandonnée suite à un échec.
ACTIVE	BOOL	Activé lorsque l'opération est active.
STATUS	WORD	Identifiant d'erreur détectée.
DATA	ANY	Données de réponse (en fonction du code de commande). Aucune donnée n'est rapportée pour les commandes de permutation et d'effacement.

Exemple

Le schéma suivant illustre l'utilisation d'un bloc PWS_CMD pour une demande de permutation :



La capture d'écran suivante de l'éditeur de données montre les valeurs variables d'une requête de permutation :

Name	Value	Type	Comment
pws_cmd_enable_1	1	BOOL	
pws_cmd_abort_1	0	BOOL	
pws_cmd_active_1	0	BOOL	
pws_cmd_done_1	1	BOOL	
pws_cmd_error_1	0	BOOL	
pws_cmd_status_1	16#0000	WORD	
pws_cmd_last_error_1	16#4444	WORD	
pws_cmd_OKCount_1	195842	DINT	
pws_cmd_KOCount_1	251	DINT	
pws_cmd_cmd_1		PWS_CMD_DDT	
Code	3	BYTE	Command code: 1 = swap, 3 = clear, etc.
PwsTarget	2	BYTE	Power supply target: 1 for left, 2 for right, 3 for both
pws_cmd_ip_str_1	"	string[64]	
pws_cmd_data_1		PWS_DATA_DDT	

Gestion de la sécurité de l'application

Présentation

Control Expert permet de restreindre l'accès des utilisateurs au PAC de sécurité M580 à l'aide de mots de passe. Cette section décrit l'attribution des mots de passe dans Control Expert.

Application Protection

Overview

EcoStruxure Control Expert has a password mechanism to help guard against unauthorized access to the application.

EcoStruxure Control Expert password protects these actions:

- Open the application in EcoStruxure Control Expert.
- Connect to the controller in EcoStruxure Control Expert.

Setting an application password helps prevent unwanted application modification, download, or opening of application files. The password is encrypted within the application.

In addition to setting the password, you can encrypt `.STU`, `.STA`, and `.ZEF` files. The file encryption feature in EcoStruxure Control Expert helps prevent modifications and reinforces the protection of intellectual property. The file encryption option is protected by a password mechanism.

NOTE: When a controller is managed as part of a system project, the application password and file encryption are disabled in EcoStruxure Control Expert editor and managed with Topology Manager.

Password Construction

The construction of the password conforms to the IEEE 1686–2013 standard.

A valid password contains at least 8 characters and includes at least one uppercase letter, one lowercase letter, one number, and one non-alphanumeric character (\$, %, &, etc.).

NOTE: The application password is cleared when you export a non-encrypted project to an `.XEF` or `.ZEF` file.

Create a New Project

By default, a new EcoStruxure Control Expert Classic application (project) has these characteristics:

- The project is not protected by a password.
- The project application files are not encrypted.

When you create a project, you can exercise these options in the **Security enforcement** dialog box:

- Set a password for the application.
- Apply encryption to your application files through a file-encryption password.

Access the **Security enforcement** dialog box in EcoStruxure Control Expert Classic:

Step	Action
1	Open the New Project window in EcoStruxure Control Expert (File > New).
2	Select a controller for the project.
3	Click the OK button to open the Security enforcement dialog box.
4	Choose to create a project with or without passwords and follow the directions in the appropriate table below.

No Passwords: Create a project without an application password:

Step	Action
1	Access the Security enforcement dialog box.
2	In the Security enforcement dialog box, select I do not want to set an application password for this project .
3	Click the OK button to continue.

With Passwords: Use the directions below to create a project with an application password and an (optional) file encryption password.

NOTE: You can configure an expiration date for these passwords on the **Policies** tab in the Security Editor.

Step	Action
1	Access the Security enforcement dialog box.
2	In the Application password group box, create a password to help protect the application and increase the security for access to the controller: - Enter a password in the Entry field. - Reenter the password in the Confirmation field.
3	In the File encryption password group box, create a password to help protect the intellectual property: - Enter a password in the Entry field. - Reenter the password in the Confirmation field. NOTE: - You can configure a file-encryption password only after you configure an application password. - Use different passwords for the application password and the file-encryption password.
4	Press the OK button to apply your password settings and close the Security enforcement dialog box.

NOTE:

- If no password is entered, the application files are not encrypted. In this case, the next time you open your EcoStruxure Control Expert project, the **Password** dialog box opens. To access your project, do not type a password and click **OK**. Then use the instructions below to set an application password and enable file encryption.
- You can create or change an application password at any time, but you cannot clear the application password when a file-encryption password is configured for the project.

Set an Application Password

Set the application password:

Step	Action
1	Right-click Project in the Project Browser .
2	Select Properties from the pop-up menu to open the Properties of Project window.
3	Select the Project & Controller Protection tab.

Step	Action
4	In the Application field, click Change password ... to open the Modify Password window.
5	Enter the new password in the Entry field.
6	Enter the confirmation of the new password in the Confirmation field.
7	Click OK to confirm.
8	Click OK or Apply in the Properties of Project window to confirm the changes.

Change the Application Password

Change the application protection password:

Step	Action
1	Right-click Project in the Project Browser .
2	Select Properties command from the pop-up menu to open the Properties of Project window.
3	Select Project & Controller Protection tab.
4	In the Application field, click Change password ... to open the Modify Password window.
5	Enter previous password in the Old password field.
6	Enter the new password in the Entry field.
7	Enter the confirmation of the new password in the Confirmation field.
8	Click OK to confirm.
9	Click OK or Apply in the Properties of Project window to confirm the changes.

Delete the Application Password

Use these steps to clear the application protection password.

NOTE: You cannot clear the application password while file encryption is enabled.

Step	Action
1	Right-click Project in the Project Browser .
2	Select the Properties command from the pop-up menu to open the Properties of Project window.
3	Select the Project & Controller Protection tab.
4	In the Application field, click Clear password... to open the Password window.

Step	Action
5	Enter the password in the Password field.
6	Click OK to confirm.
7	Click OK or Apply in the Properties of Project window to confirm the changes.

Auto-Lock Feature

To exercise the option to limit access to the EcoStruxure Control Expert tool after a configured time of inactivity, select (check) the **Auto-lock** check box and enter a value in the **Minutes before lock** field to set the timeout for the time of inactivity.

An optional auto-lock feature limits access to the EcoStruxure Control Expert software programming tool after a configured time of inactivity. You can activate the auto-lock feature with the **Auto-lock** check box and select the time-out for the time of inactivity with **Minutes before lock**.

If the auto-lock feature is enabled and the configured inactivity time elapses, a dialog box for the application password appears. Behind the dialog box, editors remain open in the same position. As a result, anyone can read the content of the EcoStruxure Control Expert windows but cannot continue to work with EcoStruxure Control Expert.

NOTE: If you have not assigned a password to the project, the dialog box is not displayed.

Password Request Condition

Opening an existing application (project):

When you open an application file, an **Application Password** dialog box opens.

Enter the password and click **OK**.

Result: If the password is correct, the application opens. If the password is incorrect, an on-screen message indicates that the password is not valid, and a new **Application Password** dialog box opens.

If you click **Cancel**, the application is not opened.

Accessing the application in EcoStruxure Control Expert after an auto-lock, when EcoStruxure Control Expert is not connected to the controller or when the project in EcoStruxure Control Expert is *equal* to the project in the controller:

When the auto-lock time is elapsed, an **Application Password** dialog box opens.

Enter the password and click **OK**.

Result: If the password is correct, EcoStruxure Control Expert becomes active again. If the password is incorrect, a message box indicates that the password is not valid, and a new **Application Password** dialog box opens.

Click **Close** to close the unsaved application.

Accessing the application in the controller after an auto-lock, when EcoStruxure Control Expert is connected to the controller and the application in EcoStruxure Control Expert is *different* from the application in the controller:

On connection, if the EcoStruxure Control Expert software application and the controller application are not equal, an **Application Password** dialog box opens.

Enter the password and click **OK**.

Result: If the password is correct, the connection is established. If the password is incorrect, a message box indicates that an incorrect password was entered, and a new **Application Password** dialog box opens.

If you click **Cancel**, the connection is not established.

NOTE: On connection, if the EcoStruxure Control Expert software application and the controller applications are equal, there is no password request. If no password has been initially entered (left empty on project creation), click **OK** to establish the connection on password prompt.

NOTE:

- After three attempts with an invalid password, wait an increasing amount of time between subsequent password attempts. The delay increases from 15 seconds to 1 hour, with the wait increment increasing by a factor of 2 after each attempt with an invalid password.
- For forgotten passwords, refer to the instructions for addressing *lost passwords*, page 332.

Enable the File Encryption Option

NOTE: Set an application password *before* you enable file encryption.

Enable the file encryption option:

Step	Action
1	Right-click Project in the Project Browser .
2	Select the Properties command from the pop-up menu to open the Properties of Project window.
3	Select the Project & Controller Protection tab.
4	Select the File encryption active check box to open the Create Password window.
5	Enter the password in the Entry field.

Step	Action
6	Enter the confirmation of the password in the Confirmation field.
7	Click OK to confirm.
8	Click OK or Apply in the Properties of Project window to confirm the changes.

Disable the File Encryption Option

Disable the file encryption option:

Step	Action
1	Right-click Project in the Project Browser .
2	Select the Properties command from the pop-up menu to open the Properties of Project window.
3	Select the Project & Controller Protection tab.
4	Clear (<i>uncheck</i>) the File encryption active check box to open the File Encryption Password window.
5	Enter the password and click OK to confirm that the application is not encrypted.
6	Click OK or Apply in the Properties of Project window to confirm all changes.

Change the File Encryption Password

Change the file encryption password:

Step	Action
1	Right-click Project in the Project Browser .
2	Select the Properties command from the pop-up menu to open the Properties of Project window.
3	Select the Project & Controller Protection tab.
4	In the File encryption field, click Change password ... to open the Modify Password window.
5	Enter the previous password in the Old password field.
6	Enter the new password in the Entry field.
7	Enter the confirmation of the new password in the Confirmation field.
8	Click OK to confirm.
9	Click OK or Apply in the Properties of Project window to confirm the changes.

Clear the File Encryption Password

Clear the file encryption password:

Step	Action
1	Right-click Project in the Project Browser .
2	Select the Properties command from the pop-up menu to open the Properties of Project window.
3	Select the Project & Controller Protection tab.
4	In the File encryption field, click Clear password... to open the Password window.
5	Enter the password in the Password field.
6	Click OK to confirm.
7	Click OK or Apply in the Properties of Project window to confirm the changes.

NOTE: For forgotten file-encryption passwords, refer to the instructions for addressing lost passwords, page 332.

Compatibility Rules

You cannot open encrypted `.STA` and `.ZEF` application files in EcoStruxure Control Expert 15.0 Classic or earlier versions.

You cannot import encrypted `.ZEF` application files to EcoStruxure Control Expert with Topology Manager.

The compatibility rules between the application version and the EcoStruxure Control Expert/Unity Pro version apply to `.ZEF` files that are exported without encryption.

NOTE: When file encryption is enabled for your project, you cannot save archived application files (`.STA`) without encryption.

Safety-Related Area Password Protection

At a Glance

Safety-related controllers include a safety-related area password protection function, which is accessible from the **Properties** dialog box of the project. This function helps protect project elements located within the safety-related area of the functional safety-related project.

NOTE: When the safety-related area password protection function is active, the safety-related parts of the application cannot be modified

Modifications to the following safety-related parts are not permitted when safety-related area password protection is enabled:

Safety-related Part	Forbidden action (offline AND online)
Configuration	Modify controller characteristics
	Add, Delete, Modify a safety-related module in the rack
	Modify safety-related Power supply
Types	Create, Delete, Modify a safety-related DDT
	Change a DDT attribute: from NOT SAFE->defined SAFE-STATE
	Change a DDT attribute: from defined SAFE-STATE->NOT SAFE
	Create, Delete, Modify a safety-related DFB
	Change a DFB attribute: from NOT SAFE->defined SAFE-STATE
	Change a DFB attribute: from defined SAFE-STATE->NOT SAFE
Program-SAFE	Any Change under the Variables an FB instances node
	Create Task
	Import Task
	Modify Task
	Create Section
	Delete Section
	Import Section
	Modify Section
Project Settings	Modify SAFE project settings
	Modify COMMON project settings

NOTE:

- To access maintenance mode, enter the password when prompted.
- If you are prompted to enter the password due to inactivity while EcoStruxure Control Expert Classic is connected to the safety-related controller in programming mode and the safety-related controller is in maintenance mode, the safety-related controller transitions to safety mode after five minutes if you do not enter the password.

Encryption

The safety-related area password uses the standard encryption SHA-256.

Safety-Related Area Password Function versus Functional Safety-Related Project User Rights

The activation of the safety-related area password and the implementation of user rights created in the **Security Editor** are mutually exclusive security functions, as follows:

- If the user launching EcoStruxure Control Expert has been assigned a user profile, that user can access the safety-related areas of the safety-related application if the user enters the safety-related area password and has been granted access rights in the **Security Editor**.
- If user profiles have not been assigned, a user can access the safety-related areas of the safety-related application by entering the safety-related area password.

Visual Indicators in EcoStruxure Control Expert

The state of the safety-related area protection function can be visibly detected by viewing the **Program-SAFE** node in the **Project Browser**:

- A locked padlock indicates a safety-related area password has been created and activated.
- An unlocked padlock indicates a safety-related area password has been created but not activated.
NOTE: If the safety-related application is closed then re-opened, the safety-related area password is automatically activated on reopening.
- No padlock indicates a safety-related area password has not been created.

Compatibility

As of EcoStruxure Control Expert version 14.0, the safety-related area password function exists for M580 safety-related controllers as of firmware version 2.80.

NOTE:

- Application program .STU, .STA, and .ZEF files (which are created as of EcoStruxure Control Expert version 14.0) cannot be opened in Unity Pro version 13.1 or earlier.
- Replacing an M580 safety-related controller in a EcoStruxure Control Expert version 14.0 application has the following effect:
 - Upgrading from firmware 2.70 to 2.80 (or any subsequent supporting version(s)) adds the safety-related area password functionality to the **Program & Safety Protection** tab of the **Project > Properties** window.
 - Downgrading from firmware 2.80 (and any subsequent comparable version(s)) to 2.70 removes the safety-related area password functionality.

Activating Protection and Creating Password

Activate the protection of sections and create the password:

Step	Action
1	Right-click Project in the Project Browser .
2	Select the Properties command from the popup menu to open the Properties of Project window.
3	Select the Program & Safety Protection tab.
4	In the Safety area, activate the protection by selecting the Protection active check box to open the Modify Password dialog box.
5	Enter a password in the Entry field.
6	Enter the confirmation of the password in the Confirmation field.
7	Follow the on-screen prompts to confirm and apply your modifications.

Changing the Password

Procedure for changing the project sections protection password:

Step	Action
1	Right-click Project in the Project Browser .
2	Select the Properties command from the popup menu to open the Properties of Project window.
3	Select the Program & Safety Protection tab.
4	In the Safety area, click Change password ... to open the Modify Password dialog box.

Step	Action
5	Enter previous password in the Old password field.
6	Enter the new password in the Entry field.
7	Enter the confirmation of the new password in the Confirmation field.
8	Follow the on-screen prompts to confirm and apply your modifications.

Deleting the Password

Procedure for deleting the project sections protection password:

Step	Action
1	In the project browser right-click Project .
2	Select Properties command from the popup menu. Result: The Properties of Project window appears.
3	Select the Program & Safety Protection tab.
4	In the Safety area, click Clear password... Result: The Access control dialog box appears:
5	Enter the previous password in the Password field.
6	Follow the on-screen prompts to confirm and apply your modifications.

Program Unit, Section and Subroutine Password and Protection

At a Glance

In offline mode, you can apply a password to your project and lock a section or program unit for editing.

It does not prevent you to:

- Connect to the controller
- Upload application from the controller
- Change the configuration
- Add new Program Units and/or sections

- Change the logic in a new section that is not password protected

NOTE: To lock a section or Program Unit for editing, you need to both:

- Activate **Protection active** on project level. Refer to the process *Activating Protection and Creating Password*, page 326.
- Select the type of protection in the **Protection** field of a section or Program Unit. Refer to the process *Locking a Section or Program Unit for Editing*, page 326.

Activating Protection and Creating Password

Follow these steps to activate a password at the project level:

Step	Action
1	In the project browser, right-click Project and select Properties .
2	Select the Program & Safety Protection tab.
3	Select the Protection active checkbox. Result: The Modify Password dialog box appears.
4	Enter a password in the Entry field.
5	Enter the confirmation of the password in the Confirmation field.
6	Select Crypted check box if an enhanced password protection is required. NOTE: A project with a crypted password cannot be edited with Unity Pro V4.0 or earlier version.
7	Click OK to confirm.
8	Click OK or Apply in the Properties window to confirm the changes. If you click Cancel in the Properties of Project window, the changes are discarded.

Locking a Section or Program Unit for Editing

Follow these steps to lock a section or Program Unit for editing:

Step	Action
1	Right-click on your section or program unit and select Properties .
2	In the General tab, select the type of protection in the Protection field.
3	Click OK to confirm.

NOTE: To lock a section or Program Unit for editing, you also need to active **Protection active** on project level. Refer to the process *Activating Protection and Creating Password*, page 326.

NOTE:

- A locked padlock next to a section or Program Unit indicates that you locked it for editing and that you activated **Protection active** on project level.
- An unlocked padlock next to a section or Program Unit indicates that you locked it for editing but that you did not activate **Protection active** on project level. Therefore, the protection of your section or Program Unit is disabled.

Changing the Password

Procedure for changing the project protection password for sections and Program Units:

Step	Action
1	In the project browser, right-click Project and select Properties . Result: The Properties of Project window appears.
2	Select Program & Safety Protection tab.
3	In the Sections & Program Units field, click Change password Result: The Modify Password dialog box appears:
4	Enter previous password in the Old password field.
5	Enter the new password in the Entry field.
6	Enter the confirmation of the new password in the Confirmation field.
7	Select Crypted check box if an enhanced password protection is required. NOTE: A project with a crypted password cannot be edited with Unity Pro V4.0 or earlier version.
8	Click OK to confirm.
9	Click OK or Apply in the Properties of Project window to confirm the changes. If you click Cancel in the Properties of Project window, the changes are discarded.

Deleting the Password

Procedure for deleting the project protection password for sections and Program Units:

Step	Action
1	In the project browser, right-click Project and select Properties . Result: The Properties of Project window appears.
2	Select Program & Safety Protection tab.
3	In the Sections & Program Units field, click Clear password.... Result: The Access control dialog box appears.
4	Enter the password in the Password field.
5	Click OK to confirm.
6	Click OK or Apply in the Properties of Project window to confirm the changes. If you click Cancel in the Properties of Project window, the changes are discarded.

Protection du micrologiciel

Présentation

La protection du micrologiciel par un mot de passe permet d'éviter tout accès indésirable au micrologiciel du module.

Mot de passe

Le mot de passe différencie les majuscules des minuscules. Il est composé de 8 à 16 caractères alphanumériques. Il est plus sécurisé s'il contient un mélange de majuscules, de minuscules, de caractères alphabétiques, numériques et spéciaux.

NOTE: Lors de l'importation d'un fichier ZEF, le mot de passe du micrologiciel est stocké dans le module uniquement si l'option **Cryptage de fichier** est sélectionnée.

Modification du mot de passe

Vous pouvez modifier ce mot de passe à tout moment.

NOTE: La valeur par défaut du mot de passe du micrologiciel dans l'application Control Expert est : **fwdownload**.

- Pour le micrologiciel V4.01 et les versions ultérieures, vous devez modifier la valeur par défaut du mot de passe du micrologiciel, faute de quoi vous ne pourrez pas générer l'application Control Expert.
- Pour les versions de micrologiciel antérieures à V4.01, il n'est pas obligatoire, mais néanmoins vivement recommandé, de modifier la valeur par défaut du mot de passe du micrologiciel.

Pour modifier le mot de passe de protection du firmware, procédez comme suit :

Étape	Action
1	Dans le navigateur de projet, cliquez avec le bouton droit sur Projet .
2	Dans le menu contextuel, choisissez la commande Propriétés . Résultat : La fenêtre Propriétés de projet apparaît.
3	Sélectionnez l'onglet Protection du projet et du contrôleur .
4	Dans le champ Firmware , cliquez sur Modifier le mot de passe.... Résultat : La fenêtre Modification du mot de passe apparaît.
5	Saisissez l'ancien mot de passe dans le champ Ancien mot de passe .
6	Saisissez le nouveau mot de passe dans le champ Saisie .
7	Confirmez votre nouveau mot de passe dans le champ Confirmation .
8	Cliquez sur OK pour confirmer.
9	Cliquez sur OK ou sur Appliquer dans la fenêtre Propriétés de Projet pour confirmer toutes les modifications. Si vous cliquez sur Annuler dans la fenêtre Propriétés de Projet , toutes les modifications sont annulées.

Réinitialisation du mot de passe

La réinitialisation du mot de passe affecte sa valeur par défaut au mot de passe du micrologiciel dans l'application Control Expert si le mot de passe actuel est confirmé.

Pour réinitialiser le mot de passe, procédez comme suit :

Étape	Action
1	Dans le navigateur de projet, cliquez avec le bouton droit sur Projet .
2	Dans le menu contextuel, choisissez la commande Propriétés .

Étape	Action
	Résultat : La fenêtre Propriétés de projet apparaît.
3	Sélectionnez l'onglet Protection du projet et du contrôleur .
4	Dans le champ Firmware , cliquez sur Réinitialiser le mot de passe... Résultat : La fenêtre Mot de passe apparaît.
5	Saisissez le mot de passe dans le champ Mot de passe .
6	Cliquez sur OK pour confirmer.
7	Cliquez sur OK ou sur Appliquer dans la fenêtre Propriétés de Projet pour confirmer toutes les modifications. Le nouveau mot de passe est le mot de passe par défaut : fwdownload . Si vous cliquez sur Annuler dans la fenêtre Propriétés de Projet , toutes les modifications sont annulées.

Data Storage/Web Protection

Overview

Protection by a password helps prevent unwanted access to the data storage zone of the SD memory card (if a valid card is inserted in the controller).

For Modicon M580 controllers in a project created by EcoStruxure Control Expert with version:

- Earlier than version 15.1, you can provide password protection for data storage access.
- As of version 15.1, you can provide password protection for both web diagnostics and data storage access.

NOTE: When a controller is managed as part of a system project, the **Web Diagnostic/Data Storage** password is disabled in EcoStruxure Control Expert editor and needs to be managed by using the Topology Manager.

Password

The password is case-sensitive and contains 8 to 16 alphanumeric characters. The password robustness is increased when it contains a mix of upper and lower case, alphabetical, numerical, and special characters.

NOTE: When importing a ZEF file, the Data Storage/Web password is stored inside the module only if the **File encryption** option is selected.

Changing the Password

It is possible to change a password at any time.

NOTE: Data Storage/Web password has a default value in the EcoStruxure Control Expert application. This default value depends on the version of EcoStruxure Control Expert:

- **datadownload**: EcoStruxure Control Expert versions earlier than 15.1
- **webuser**: EcoStruxure Control Expert versions as of 15.1

Changing the default password is mandatory, or not, depending on the module firmware version:

- As of firmware version 4.01, you need to change the Data Storage/Web password default value. Otherwise it is not possible to build the EcoStruxure Control Expert application.
- For firmware versions earlier than 4.01 it is not mandatory but strongly advised to change Data Storage/Web password default value.

Procedure for changing the Data Storage/Web password:

Step	Action
1	Right-click Project in the Project Browser .
2	Select the Properties command from the popup menu to open the Properties of Project window.
3	Select Project & Controller Protection tab.
4	In the Data Storage (or Web Diagnostics/Data Storage) field, click Change password ... to open the Modify Password window.
5	Enter previous password in the Old password field.
6	Enter the new password in the Entry field.
7	Enter the confirmation of the new password in the Confirmation field.
8	Follow the on-screen prompts to confirm and apply your modifications.

Resetting the Password

Resetting the password assigns its default value to the Data Storage/Web password in the EcoStruxure Control Expert application if the password is confirmed.

Program Unit, Section and Subroutine Password and Protection, page 325

Reset the password:

Step	Action
1	Right-click Project in the Project Browser .
2	Select the Properties command from the popup menu to open the Properties of Project window.
3	Select the Project & Controller Protection tab.
4	In the Data Storage (or Web Diagnostic/Data Storage) field, click Reset password... to open the Password window.
5	Enter your password in the Password field.
6	Follow the on-screen prompts to confirm and apply your modifications.

Perte du mot de passe

Présentation

Si vous avez oublié votre mot de passe, procédez comme suit et contactez le support Schneider Electric.

NOTE: La procédure de récupération du mot de passe de l'application varie selon que l'option de cryptage de fichier est activée ou désactivée.

Mot de passe d'application Control Expert sans option de cryptage de fichier

La procédure de réinitialisation de mot de passe d'application décrite ci-après est valide lorsque l'option de cryptage de fichier est désactivée ou pour un fichier d'application géré avec Control Expert 15.0 Classic ou des versions antérieures.

Le support Schneider Electric a besoin de la chaîne de caractères alphanumériques qui s'affiche dans la fenêtre contextuelle **Mot de passe oublié** dès que vous appuyez sur **SHIFT+F2** dans la boîte de dialogue **Mot de passe**

Les conditions suivantes doivent être remplies pour accéder à la boîte de dialogue **Mot de passe** :

- Lors de l'ouverture, sélectionnez l'application. La boîte de dialogue **Mot de passe** s'affiche.
- Lors du verrouillage automatique, la boîte de dialogue **Mot de passe** s'affiche. Si vous avez oublié le mot de passe, cliquez sur **Fermer**. Ouvrez à nouveau l'application. La boîte de dialogue **Mot de passe** s'affiche..

NOTE: si l'application est fermée sans qu'un mot de passe n'ait été saisi après un verrouillage automatique, toutes les modifications sont perdues.

Pour réinitialiser le mot de passe de l'application, procédez comme suit :

Étape	Action
1	Condition La boîte de dialogue Mot de passe s'affiche.
2	Appuyez sur <code>SHIFT+F2</code> . Résultat : La fenêtre contextuelle Mot de passe oublié s'ouvre et une chaîne de caractères alphanumériques s'affiche.
3	Copiez cette chaîne et transmettez-la au support Schneider Electric.
4	Le mot de passe généré est envoyé par le support Schneider Electric. REMARQUE : Ce mot de passe est temporaire. Il est disponible tant que vous ne modifiez pas l'application.
5	Entrez ce mot de passe.
6	Modifiez ce mot de passe (ancien mot de passe = celui fourni par le support Schneider Electric).
7	Cliquez sur Générer > Générer des modifications .
8	Enregistrez l'application à l'aide de la commande Enregistrer..

Mot de passe d'application Control Expert avec option de cryptage de fichier

Si vous oubliez le mot de passe de votre application alors que le cryptage de fichier est activé, vous devez envoyer le fichier d'application au support Schneider Electric. Vous recevez ensuite du support Schneider Electric le fichier d'application crypté avec un nouveau mot de passe de cryptage d'application de fichier.

NOTE: Modifiez le mot de passe de l'application lors de la première utilisation.

Mot de passe de l'application du contrôleur

Pour réinitialiser le mot de passe de l'application de controller si le fichier *.STU correspondant est disponible, procédez comme suit :

Étape	Action
1	Ouvrez le fichier *.STU correspondant.
2	Lorsque la boîte de dialogue Mot de passe s'affiche, appuyez sur <code>SHIFT+F2</code> . Résultat : La fenêtre contextuelle Mot de passe oublié s'ouvre et une chaîne de caractères alphanumériques s'affiche.

Étape	Action
3	Copiez cette chaîne et transmettez-la au support Schneider Electric.
4	Le mot de passe généré est envoyé par le support Schneider Electric. Remarque : Ce mot de passe est temporaire. Il est disponible tant que vous ne modifiez pas l'application.
5	Entrez ce mot de passe.
6	Modifiez ce mot de passe (ancien mot de passe = celui fourni par le support Schneider Electric).
7	Connectez-vous au contrôleur.
8	Cliquez sur Générer > Générer des modifications .
9	Enregistrez l'application à l'aide de la commande Enregistrer..

Pour réinitialiser le mot de passe de l'application du contrôleur si le fichier *.STU correspondant n'est pas disponible, procédez comme suit :

Étape	Action
1	Condition Lors de la connexion, la boîte de dialogue Mot de passe s'affiche.
2	Appuyez sur SHIFT+F2 . Résultat : La fenêtre contextuelle Mot de passe oublié s'ouvre et une chaîne de caractères alphanumériques s'affiche.
3	Copiez cette chaîne et transmettez-la au support Schneider Electric.
4	Le mot de passe généré est envoyé par le support Schneider Electric. Remarque : Le mot de passe fourni par le support Schneider Electric est temporaire. Il est disponible tant que vous ne modifiez pas l'application.
5	Entrez ce mot de passe.
6	Chargez l'application à partir du contrôleur.
7	Enregistrez l'application à l'aide de la commande Enregistrer..
8	Modifiez le mot de passe (ancien mot de passe = celui fourni par le support Schneider Electric).
9	Cliquez sur Générer > Générer des modifications .
10	Enregistrez l'application à l'aide de la commande Enregistrer..

Mot de passe de cryptage de fichier

Le support Schneider Electric a besoin de la chaîne de caractères alphanumériques qui s'affiche dans la fenêtre contextuelle **Mot de passe oublié** dès que vous appuyez sur **SHIFT+F2** dans la boîte de dialogue **Mot de passe**

Pour accéder à la boîte de dialogue **Mot de passe** :

- Accédez à **Projet > Propriétés de projet > Protection du projet et du contrôleur**
- Dans le champ **Cryptage de fichier**, cliquez sur **Effacer mot de passe....** La boîte de dialogue **Mot de passe** s'affiche.

Procédure de réinitialisation du mot de passe de cryptage de fichier :

Étape	Action
1	Condition La boîte de dialogue Mot de passe s'affiche.
2	Appuyez sur SHIFT+F2 . Résultat : La fenêtre contextuelle Mot de passe oublié s'ouvre et une chaîne de caractères alphanumériques s'affiche.
3	Copiez cette chaîne et transmettez-la au support Schneider Electric.
4	Le mot de passe généré est envoyé par le support Schneider Electric. Remarque : Ce mot de passe est temporaire. Il est disponible tant que vous ne modifiez pas l'application.
5	Entrez ce mot de passe et cliquez sur OK pour fermer la boîte de dialogue Mot de passe .
6	Cliquez sur Modifier le mot de passe et modifiez le mot de passe (ancien mot de passe = mot de passe fourni par le support Schneider Electric).
7	Cliquez sur OK pour fermer la boîte de dialogue Modifier le mot de passe , puis cliquez sur OK ou Appliquer dans la fenêtre Propriétés du projet pour confirmer toutes les modifications. Si vous cliquez sur Annuler dans la fenêtre Propriétés de Projet , toutes les modifications sont annulées.

Mot de passe de la zone de sécurité

Le support Schneider Electric a besoin de la chaîne de caractères alphanumériques qui s'affiche dans la fenêtre contextuelle **Mot de passe oublié** dès que vous appuyez sur **SHIFT+F2** dans la boîte de dialogue **Mot de passe**

Pour accéder à la boîte de dialogue **Mot de passe** :

- Accédez à **Projet > Propriétés de projet > Protection du programme et de la sécurité**

- Dans le champ **Sécurité**, cliquez sur **Modifier le mot de passe....** La boîte de dialogue **Mot de passe** s'affiche.

Pour réinitialiser le mot de passe de la zone de sécurité, procédez comme suit :

Étape	Action
1	Condition La boîte de dialogue Mot de passe s'affiche.
2	Appuyez sur SHIFT+F2 . Résultat : La fenêtre contextuelle Mot de passe oublié s'ouvre et une chaîne de caractères alphanumériques s'affiche.
3	Copiez cette chaîne et transmettez-la au support Schneider Electric.
4	Le mot de passe généré est envoyé par le support Schneider Electric. Remarque : Ce mot de passe est temporaire. Il est disponible tant que vous ne modifiez pas l'application.
5	Entrez ce mot de passe et cliquez sur OK pour fermer la boîte de dialogue Mot de passe .
6	Cliquez sur Modifier le mot de passe et modifiez le mot de passe (ancien mot de passe = mot de passe fourni par le support Schneider Electric).
7	Cliquez sur OK pour fermer la boîte de dialogue Modifier le mot de passe , puis cliquez sur OK ou Appliquer dans la fenêtre Propriétés du projet pour confirmer toutes les modifications. Si vous cliquez sur Annuler dans la fenêtre Propriétés de Projet , toutes les modifications sont annulées.

Mot de passe du micrologiciel

Le support Schneider Electric a besoin de la chaîne de caractères alphanumériques qui s'affiche dans la fenêtre contextuelle **Mot de passe oublié** dès que vous appuyez sur **SHIFT+F2** dans la boîte de dialogue **Mot de passe**

Pour accéder à la boîte de dialogue **Mot de passe** :

- Accédez à **Projet > Propriétés de projet > Protection du projet et du contrôleur**
- Dans le champ **Firmware**, cliquez sur **Réinitialiser le mot de passe....** La boîte de dialogue **Mot de passe** s'affiche.

Pour réinitialiser le mot de passe de micrologiciel, procédez comme suit :

Étape	Action
1	Condition La boîte de dialogue Mot de passe s'affiche.
2	Appuyez sur SHIFT+F2 . Résultat : La fenêtre contextuelle Mot de passe oublié s'ouvre et une chaîne de caractères alphanumériques s'affiche.

Étape	Action
3	Copiez cette chaîne et transmettez-la au support Schneider Electric.
4	Le mot de passe généré est envoyé par le support Schneider Electric. Remarque : Ce mot de passe est temporaire. Il est disponible tant que vous ne modifiez pas l'application.
5	Entrez ce mot de passe et cliquez sur OK pour fermer la boîte de dialogue Mot de passe .
6	Cliquez sur Modifier le mot de passe et modifiez le mot de passe (ancien mot de passe = mot de passe fourni par le support Schneider Electric).
7	Cliquez sur OK pour fermer la boîte de dialogue Modifier le mot de passe , puis cliquez sur OK ou Appliquer dans la fenêtre Propriétés du projet pour confirmer toutes les modifications. Si vous cliquez sur Annuler dans la fenêtre Propriétés de Projet , toutes les modifications sont annulées.

Mot de passe pour le stockage des données/Web

Le support Schneider Electric a besoin de la chaîne de caractères alphanumériques qui s'affiche dans la fenêtre contextuelle **Mot de passe oublié** dès que vous appuyez sur **SHIFT+F2** dans la boîte de dialogue **Mot de passe**

Pour accéder à la boîte de dialogue **Mot de passe** :

- Accédez à **Projet > Propriétés de projet > Protection du projet et du contrôleur**
- Dans le champ **Stockage des données**, cliquez sur **Réinitialiser le mot de passe...**
La boîte de dialogue **Mot de passe** s'affiche.

Pour modifier le mot de passe de stockage des données, procédez comme suit :

Étape	Action
1	Condition La boîte de dialogue Mot de passe s'affiche.
2	Appuyez sur SHIFT+F2 . Résultat : La fenêtre contextuelle Mot de passe oublié s'ouvre et une chaîne de caractères alphanumériques s'affiche.
3	Copiez cette chaîne et transmettez-la au support Schneider Electric.
4	Le mot de passe généré est envoyé par le support Schneider Electric. Remarque : Ce mot de passe est temporaire. Il est disponible tant que vous ne modifiez pas l'application.
5	Entrez ce mot de passe et cliquez sur OK pour fermer la boîte de dialogue Mot de passe .

Étape	Action
6	Cliquez sur Modifier le mot de passe et modifiez le mot de passe (ancien mot de passe = mot de passe fourni par le support Schneider Electric).
7	Cliquez sur OK pour fermer la boîte de dialogue Modifier le mot de passe, puis cliquez sur OK ou Appliquer dans la fenêtre Propriétés du projet pour confirmer toutes les modifications. Si vous cliquez sur Annuler dans la fenêtre Propriétés de Projet, toutes les modifications sont annulées.

Gestion de la sécurité des stations de travail

Introduction

Schneider Electric fournit l'outil de gestion de l'accès *Security Editor* qui permet de limiter et de contrôler l'accès à la station de travail ou aux stations de travail sur lesquelles est installé le logiciel Control Expert. Cette section décrit les fonctions de cet outil spécifiquement conçu pour les projets de sécurité M580.

Gestion de l'accès au EcoStruxure Control Expert

Introduction

Schneider Electric fournit un outil de configuration de l'*Éditeur de sécurité* qui vous permet de gérer l'accès au EcoStruxure Control Expert logiciel installé sur un ou plusieurs postes de travail. (L'utilisation de cet outil est facultative.)

NOTE: La gestion de l'accès concerne le matériel (généralement une ou plusieurs stations de travail) sur lequel le logiciel EcoStruxure Control Expert est installé. Le projet dispose de son propre système de protection.

Pour plus d'informations, reportez-vous à *EcoStruxure™ Control Expert, Security Editor, Operation Guide*.

NOTE: Les profils des utilisateurs de sécurité requièrent également des droits d'accès à la partie processus de l'application de sécurité. Lorsque vous créez ou modifiez des profils d'utilisateur, vérifiez que toutes les modifications applicables sont effectuées.

Catégories d'utilisateurs

L'outil *Security Editor* prend en charge les catégories d'utilisateurs suivantes :

- **SecurityAdmin** : Uniquement le *SecurityAdmin* peut gérer la sécurité d'accès du logiciel. Cet utilisateur administrateur détermine qui peut accéder au logiciel et définit leurs droits d'accès. Au cours de l'installation du logiciel EcoStruxure Control Expert sur la station d'E/S, seul *SecurityAdmin* peut accéder à la configuration de la sécurité sans limitation de droits (sans mot de passe).

NOTE: L'utilisateur *SecurityAdmin* joue le rôle administratif qui était pris en charge par le *Supervisor (superutilisateur)* dans les versions héritées de EcoStruxure Control Expert (antérieures à la version 15.3).

- **Utilisateurs** : Les utilisateurs du logiciel sont définis dans la liste des utilisateurs par *SecurityAdmin* lorsque la sécurité d'accès est active pour EcoStruxure Control Expert. Si votre nom figure dans la liste, vous pouvez accéder à une instance du logiciel en saisissant votre nom (tel qu'il apparaît dans la liste) et votre mot de passe.

Profil utilisateur

Les profils d'utilisateur incluent tous les droits d'accès des utilisateurs correspondants. *SecurityAdmin* peut personnaliser ces profils ou les créer en appliquant un profil préconfiguré inclus dans l'outil de l'*Éditeur de sécurité*.

Profils utilisateur préconfigurés

L'*Éditeur de sécurité* contient les profils d'utilisateurs préconfigurés suivants, qui s'appliquent au programme de sécurité ou au programme de processus :

Profil	Type de programme applicable		Description
	Processus	Sécurité	
Lecture seule	✓	✓	L'utilisateur peut accéder au projet uniquement en mode lecture, mais il peut modifier l'adresse du contrôleur d'automatisation programmable (PAC). L'utilisateur peut également copier ou charger le projet.
Exploitation	✓	—	L'utilisateur a les mêmes droits qu'avec le profil Lecture seule , et il peut également modifier les paramètres d'exécution (constantes, valeurs initiales, durée de cycle des tâches, etc.).
Sécurité_Exploitation	—	✓	L'utilisateur dispose de droits similaires au profil Operate par rapport au programme de sécurité, à ces différences près : • Le transfert des valeurs de données vers le contrôleur d'automatisation programmable (PAC) n'est pas autorisé. • La commande du programme de sécurité pour accéder au mode de maintenance est autorisée.
Réglage	✓	—	L'utilisateur a les mêmes droits qu'avec le profil Exploitation , et il peut également charger un projet (transfert vers l'automate) et modifier le mode de marche de l'automate (Run , Stop , etc.).
Sécurité_Réglage	—	✓	L'utilisateur dispose de droits similaires au profil Adjust par rapport au programme de sécurité, à ces différences près :

Profil	Type de programme applicable		Description
	Processus	Sécurité	
			- Le transfert des valeurs de données vers le contrôleur d'automatisation programmable (PAC) n'est pas autorisé. - La commande du programme de sécurité pour accéder au mode de maintenance est autorisée.
Débugage	✓	—	L'utilisateur a les mêmes droits qu'avec le profil Réglage , mais il peut également utiliser les outils de débogage.
Sécurité_ Débugage	—	✓	L'utilisateur dispose de droits similaires au profil Debug, mais par rapport au programme de sécurité, à ces différences près : - L'arrêt et le démarrage du programme ne sont pas autorisés. - La mise à jour des valeurs d'initialisation ne sont pas autorisées. - Le transfert des valeurs de données vers le contrôleur d'automatisation programmable (PAC) n'est pas autorisé. - Le forçage des entrées, sorties ou bits internes n'est pas autorisé. - La commande du programme de sécurité pour accéder au mode de maintenance est autorisée.
Programme	✓	—	L'utilisateur a les mêmes droits qu'avec le profil Débugage , mais il peut également modifier le programme.
Sécurité_ Programme	—	✓	L'utilisateur dispose de droits similaires au profil Program par rapport au programme de sécurité, à ces différences près : - L'arrêt et le démarrage du programme ne sont pas autorisés. - La mise à jour des valeurs d'initialisation ne sont pas autorisées. - Le transfert des valeurs de données vers le contrôleur d'automatisation programmable (PAC) n'est pas autorisé. - La restauration du projet sur le contrôleur d'automatisation programmable (PAC) à partir d'une sauvegarde n'est pas autorisée. - Le forçage des entrées, sorties ou bits internes n'est pas autorisé. - La commande du programme de sécurité pour accéder au mode de maintenance est autorisée.
Désactivé	✓	—	L'utilisateur ne peut pas accéder au projet.

Attribution d'un utilisateur préconfiguré

SecurityAdmin peut attribuer un utilisateur préconfiguré (dérivé du profil préconfiguré) à un utilisateur spécifique de l'onglet **Utilisateurs** de l'*Éditeur de sécurité*. Ces utilisateurs préconfigurés disponibles sont les suivants :

- Utilisateur_Sécurité_Réglage
- Utilisateur_Sécurité_Débogage
- Utilisateur_Sécurité_Exploitation
- Utilisateur_Sécurité_Programme
- Utilisateur_Réglage
- Utilisateur_Débogage
- Utilisateur_Exploitation
- Utilisateur_Programme

Reportez-vous à la description du *certificate whitelist* dans *EcoStruxure EcoStruxure Control Expert, Éditeur de sécurité, Guide d'exploitation*.

Droits d'accès

Introduction

Cette rubrique présente les droits d'accès disponibles pour chaque profil d'utilisateur préconfiguré.

Les droits d'accès EcoStruxure Control Expert sont regroupés dans les catégories suivantes :

- Topology Manager

Les droits d'accès EcoStruxure Control Expert Classic sont regroupés dans les catégories suivantes :

- Services projet
- Réglage/Débogage
- Bibliothèques
- Modification globale
- Modification élémentaire d'une variable
- Modification élémentaire d'une données composées de type de données dérivé (DDT, Derived Data Type)
- Modification élémentaire d'un type de bloc de fonction dérivé (DFB, Derived Function Block)

- Modification élémentaire d'une instance de bloc de fonction dérivé (DFB, Derived Function Block)
- Éditeur de configuration de bus
- Éditeur de configuration des entrées/sorties
- Écrans d'exploitation.
- Cybersécurité
- Sécurité

NOTE: Les droits d'accès EcoStruxure Control Expert Classic s'appliquent également à EcoStruxure Control Expert editor.

Topology Manager

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécurité_Déboga-ge	Exploita-tion	Sécu-rité_Exploita-tion	Program-me	Sécu-rité_Pro-gramme
Create projet système	–	–	–	–	–	–	✓	✓
Modify projet système	–	–	–	–	–	–	✓	✓
Import projet système	–	–	–	–	–	–	✓	✓
Delete projet système	–	–	–	–	–	–	✓	✓
Manage projet système settings	–	–	–	–	–	–	✓	✓
✓ : Inclus								
– : Non inclus								

Services de projet

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécurité_Déboga-ge	Exploita-tion	Sécu-rité_Exploita-tion	Program-me	Sécu-rité_Pro-gramme
Créer un nouveau projet	–	–	–	–	–	–	✓	✓
Ouvrir un projet existant	✓	✓	✓	✓	✓	✓	✓	✓
Enregistrer un projet	–	–	–	–	–	–	✓	✓
Enregistrer sous un projet	✓	✓	✓	✓	✓	✓	✓	✓
Importer un projet	–	–	–	–	–	–	✓	✓
Générer hors ligne	–	–	–	–	–	–	✓	✓
Générer un arrêt (STOP) en ligne	–	–	–	–	–	–	✓	✓
Générer un arrêt (RUN) en ligne	–	–	–	–	–	–	✓	✓
Démarrer, arrêter ou initialiser le contrôleur d'automatisation programmable (PAC)*	✓	–	✓	–	–	–	✓	✓
Mettre à jour les valeurs d'initialisation avec les valeurs courantes (uniquement données non liées à la sécurité)	–	–	✓	–	–	–	✓	✓
Transférer un projet depuis le contrôleur d'automatisation programmable (PAC)	✓	✓	✓	✓	✓	✓	✓	✓
Transférer un projet vers le contrôleur d'automatisation programmable (PAC)	✓	✓	✓	✓	–	–	✓	✓
Transférer des valeurs de données du fichier vers le contrôleur PAC (uniquement données non liées à la sécurité)	✓	–	✓	–	✓	–	✓	✓
Restaurer une sauvegarde de projet sur le contrôleur	–	–	–	–	–	–	✓	✓

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécu-rité_Déboga-ge	Exploita-tion	Sécu-rité_Exploita-tion	Program-me	Sécu-rité_Pro-gramme
d'automatisation programmable (PAC)								
Enregistrer vers sauvegarde de projet sur le contrôleur d'automatisation programmable (PAC)	–	–	–	–	–	–	✓	✓
Définir une adresse	✓	✓	✓	✓	✓	✓	✓	✓
Modifier des options	✓	✓	✓	✓	✓	✓	✓	✓
* Seules les tâches de processus sont démarrées ou arrêtées. Pour un contrôleur d'automatisation programmable (PAC) non lié à la sécurité, cela signifie que le contrôleur d'automatisation programmable (PAC) est démarré ou arrêté. Pour un contrôleur d'automatisation programmable (PAC) de sécurité M580, cela signifie que les tâches non liées à la sécurité (autres que SAFE) sont démarrées ou arrêtées. ✓ : Inclus – : Non inclus								

Réglage/Débogage

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécu-rité_Déboga-ge	Exploi-tation	Sécu-rité_Exploi-tation	Program-me	Sécu-rité_Pro-gramme
Modifier des valeurs de variable	✓	–	✓		✓		✓	✓
Modifier des valeurs des variables de sécurité	–	✓	–	✓	–	✓	–	✓
Forcer des bits internes	–	–	✓	–	–	–	✓	✓
Forcer des sorties	–	–	✓	–	–	–	✓	✓
Forcer des entrées	–	–	✓	–	–	–	✓	✓
Gestion des tâches	–	–	✓	–	–	–	✓	✓

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécurité_Débo-gage	Exploi-tation	Sécurité_Exploi-tation	Program-me	Sécurité_Pro-gramme
Gestion de la tâche SAFE	–	–	–	✓	–	–	–	✓
Modification de la durée de cycle de la tâche	✓	–	✓		✓	–	✓	✓
Modification de la durée du cycle de la tâche SAFE	–	✓	–	✓	–	✓	–	✓
Supprimer un message dans le visualiseur	✓	✓	✓	✓	✓	✓	✓	✓
Mettre au point un exécutable	–	–	✓	✓	–	–	✓	✓
Remplacer une variable du projet	–	–	–	–	–	–	✓	✓
Remplacer une variable du projet de sécurité	–	–	–	–	–	–	–	✓
✓ : Inclus – : non inclus								

Bibliothèques

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécurité_Débo-gage	Exploi-tation	Sécurité_Exploi-tation	Program-me	Sécurité_Pro-gramme
Créer des bibliothèques ou des familles	–	–	–	–	–	–	✓	✓
Créer des bibliothèques ou des familles de sécurité	–	–	–	–	–	–	–	✓
Supprimer des bibliothèques ou des familles	–	–	–	–	–	–	✓	✓

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécurité_Débo-gage	Exploi-tation	Sécurité_Exploi-tation	Program-me	Sécurité_Pro-gramme
Supprimer des bibliothèques ou des familles de sécurité	–	–	–	–	–	–	–	✓
Placer un objet dans une bibliothèque	–	–	–	–	–	–	✓	✓
Placer un objet dans une bibliothèque de sécurité	–	–	–	–	–	–	–	✓
Supprimer un objet d'une bibliothèque	–	–	–	–	–	–	✓	✓
Supprimer un objet d'une bibliothèque de sécurité	–	–	–	–	–	–	–	✓
Obtenir un objet d'une bibliothèque	–	–	–	–	–	–	✓	✓
Obtenir un objet de la bibliothèque de sécurité	–	–	–	–	–	–	–	✓
✓ : Inclus								
– : non inclus								

Modification globale

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécurité_Débo-gage	Exploita-tion	Sécurité_Exploi-tation	Program-me	Sécurité_Pro-gramme
Modifier la documentation	✓	✓	✓	✓	✓	✓	✓	✓
Modifier la vue fonctionnelle	–	–	–	–	–	–	✓	✓
Modifier les tables d'animation	✓	✓	✓	✓	✓	✓	✓	✓
Modifier une valeur de constante	✓	–	✓	–	✓	–	✓	✓

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécurité_Débo-gage	Exploitation	Sécurité_Exploitation	Program-me	Sécurité_Pro-gramme
Modifier une valeur de constante de sécurité	–	✓	–	✓	–	✓	–	✓
Modifier la structure du programme	–	–	–	–	–	–	✓	✓
Modifier la structure du programme de sécurité	–	–	–	–	–	–	–	✓
Modifier des sections du programme	–	–	–	–	–	–	✓	✓
Modifier des sections du programme de sécurité	–	–	–	–	–	–	–	✓
Modifier des paramètres de projet	–	–	–	–	–	–	✓	✓
✓ : Inclus – : non inclus								

Modification élémentaire d'une variable

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécurité_Débo-gage	Exploitation	Sécurité_Exploitation	Program-me	Sécurité_Pro-gramme
Ajout/Suppression de variable	–	–	–	–	–	–	✓	✓
Ajout/Suppression de variable de sécurité	–	–	–	–	–	–	–	✓
Modification des attributs principaux d'une variable	–	–	–	–	–	–	✓	✓
Modification des attributs principaux d'une variable de sécurité	–	–	–	–	–	–	–	✓

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécu-rité_Débo-gage	Exploi-tation	Sécu-rité_Exploi-tation	Program-me	Sécu-rité_Pro-gramme
Modification des attributs secondaires d'une variable	✓	–	✓	–	✓	–	✓	✓
Modification des attributs secondaires d'une variable de sécurité	–	✓	–	✓	–	✓	–	✓
✓ : Inclus								
– : non inclus								

Modification élémentaire de données composées d'un type de données dérivé (DDT, Derived Data Type)

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécu-rité_Réglage	Déboga-ge	Sécu-rité_Déboga-ge	Exploita-tion	Sécu-rité_Exploi-tation	Program-me	Sécu-rité_Pro-gramme
Ajout/Suppression de type de données dérivé (DDT, Derived Data Type)	–	–	–	–	–	–	✓	✓
Modifications de type de données dérivé (DDT, Derived Data Type)	–	–	–	–	–	–	✓	✓
✓ : Inclus								
– : non inclus								

Modification élémentaire d'un type de bloc de fonction dérivé (DFB, Derived Function Block)

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débugage	Sécurité_Débogage	Exploitation	Sécurité_Exploitation	Programme	Sécurité_Programme
Ajout/Suppression d'un type de bloc de fonction dérivé (DFB, Derived Function Block)	–	–	–	–	–	–	✓	✓
Ajout/Suppression d'un type de bloc de fonction dérivé (DFB, Derived Function Block) de sécurité	–	–	–	–	–	–	–	✓
Modification de la structure d'un type de bloc de fonction dérivé (DFB, Derived Function Block)	–	–	–	–	–	–	✓	✓
Modification de la structure d'un type de bloc de fonction dérivé (DFB, Derived Function Block) de sécurité	–	–	–	–	–	–	–	✓
Modification des sections d'un type de bloc de fonction dérivé (DFB, Derived Function Block)	–	–	–	–	–	–	✓	✓
Modification des sections d'un type de bloc de fonction dérivé (DFB, Derived Function Block) de sécurité	–	–	–	–	–	–	–	✓
✓ : Inclus								
– : non inclus								

Modification élémentaire d'une instance de bloc de fonction dérivé (DFB, Derived Function Block)

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débogage	Sécurité_Débogage	Exploitation	Sécurité_Exploitation	Programme	Sécurité_Programme
Modification d'une instance de bloc de fonction dérivé (DFB, Derived Function Block)	–	–	–	–	–	–	✓	✓
Modification d'une instance de bloc de fonction dérivé (DFB, Derived Function Block) de sécurité	–	–	–	–	–	–	–	✓
Modification des attributs secondaires d'une instance de bloc de fonction dérivé (DFB, Derived Function Block)	✓	–	✓	–	✓	–	✓	✓
Modification des attributs secondaires d'une instance de bloc de fonction dérivé (DFB, Derived Function Block) de sécurité	–	✓	–	✓	–	✓	–	✓
✓ : Inclus – : non inclus								

Éditeur de configuration de bus

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débogage	Sécurité_Débogage	Exploitation	Sécurité_Exploitation	Programme	Sécurité_Programme
Modifier la configuration	–	–	–	–	–	–	✓	✓
Modifier la configuration de sécurité	–	–	–	–	–	–	–	✓

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécu- rité_ Réglage	Déboga- ge	Sécu- rité_ Déboga- ge	Exploi- tation	Sécu- rité_ Exploi- tation	Pro- gramme	Sécu- rité_ Pro- gramme
Surveillance des communications d'E/S	–	–	–	–	–	–	✓	✓
✓ : Inclus – : non inclus								

Éditeur de configuration des entrées/sorties

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Régla- ge	Sécu- rité_ Réglage	Débo- gage	Sécu- rité_ Déboga- ge	Exploita- tion	Sécu- rité_ Exploi- tation	Pro- gramme	Sécu- rité_ Pro- gramme
Modifier la configuration des E/S	–	–	–	–	–	–	✓	✓
Modifier la configuration des E/S de sécurité	–	–	–	–	–	–	–	✓
Régler les E/S	✓	–	✓	–	✓	–	✓	✓
Régler les E/S de sécurité	–	✓	–	✓	–	✓	–	✓
Enregistrer param	–	–	✓	–	–	–	✓	✓
Restaurer_param	–	–	✓	–	–	–	✓	✓
✓ : Inclus – : non inclus								

Écrans d'exploitation

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécurité_Débo-gage	Exploitation	Sécurité_Exploitation	Program-me	Sécurité_Pro-gramme
Modifier les écrans	–	–	–	–	–	–	✓	✓
Modifier les messages	–	–	–	–	–	–	✓	✓
Ajouter/Supprimer des écrans ou des familles	–	–	–	–	–	–	✓	✓
✓ : Inclus								
– : non inclus								

Cybersécurité

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécurité_Débo-gage	Exploitation	Sécurité_Exploitation	Program-me	Sécurité_Pro-gramme
Créer ou modifier le mot de passe d'une application	–	–	–	–	–	–	✓	✓
Accéder au mode de maintenance	–	✓	–	✓	–	✓	–	✓
Adapter le délai de verrouillage automatique	✓	✓	✓	✓	✓	✓	✓	✓
✓ : Inclus								
– : non inclus								

Sécurité

Les droits d'accès de cette catégorie sont les suivants :

Droit d'accès	Profil d'utilisateur préconfiguré							
	Réglage	Sécurité_Réglage	Débo-gage	Sécurité_Débo-gage	Exploitation	Sécurité_Exploitation	Programme	Sécurité_Programme
Accéder au mode de maintenance	–	✓	–	✓	–	✓	–	✓
✓ : Inclus – : non inclus								

Modifications apportées à Control Expert pour le système de sécurité M580

Introduction

Cette section décrit les fonctionnalités de Control Expert qui ont été modifiées ou restreintes pour le système de sécurité M580.

Transfert et importation de projets et de code de sécurité M580 dans Control Expert

Transfert d'un projet de sécurité de Control Expert vers le PAC de sécurité

Vous pouvez utiliser la commande **Automate > Transférer le projet vers l'automate** pour envoyer le projet de Control Expert vers le PAC si les conditions suivantes sont remplies :

- Control Expert est connecté en mode programmation (voir EcoStruxure™ Control Expert, Modes de fonctionnement) au PAC de sécurité M580 ;
- un projet est ouvert dans Control Expert ;
- toutes les tâches du PAC sont en état STOP.

NOTE: Vous ne pouvez transférer une application de sécurité que vers un PAC de sécurité. Une application de sécurité ne peut pas être transférée vers un PAC non dédié à la sécurité.

Transfert d'un projet de sécurité du PAC de sécurité vers Control Expert

De la même façon, vous pouvez utiliser la commande **Automate > Transférer le projet depuis l'automate** pour transférer le projet du PAC vers Control Expert si les conditions suivantes sont remplies :

- Control Expert est connecté en mode programmation (voir EcoStruxure™ Control Expert, Modes de fonctionnement) au PAC de sécurité M580 ;
- aucun projet n'est ouvert dans Control Expert.

Vous pouvez transférer le contenu lié à une tâche (SAFE, MAST, FAST, AUX0 ou AUX1) en mode sécurité ou maintenance.

Importation de projets et de sections de code dans Control Expert

Control Expert Safety prend en charge l'importation de projets entiers (**Fichier > Ouvrir**) et de sections de code (**Tâches > Importer...** ou **Sections > Importer...**), sous réserve que les conditions suivantes soient remplies :

- Seuls les fonctions ou les types de bloc fonction, qui existent dans la bibliothèque de sécurité (**Editeur de données > <Libset> > Sécurité**) ou dans la bibliothèque personnalisée (**Editeur de données > <Libset> > Personnaliser Bibliothèque**), peuvent être inclus dans une section de code gérée par la tâche SAFE.
- Une section de code gérée par une tâche de processus (MAST, FAST, AUX0 ou AUX1) ne peut inclure que des fonctions ou des types de bloc fonction qui existent dans des bibliothèques autres que la bibliothèque de sécurité.

Enregistrement et restauration de données entre un fichier et le PAC

Fonctions Enregistrer et Restaurer pour les données non liées à la sécurité

Control Expert prend en charge les commandes **Automate > Enregistrer les données de l'automate dans un fichier** et **Automate > Restaurer les données du fichier sur l'automate** pour les données des zones de processus et globale. Les données enregistrées et restaurées ne comprennent pas les variables et les instances de blocs fonction créées dans l'espace de nom de sécurité.

Pour plus d'informations sur l'utilisation de ces commandes pour les données non liées à la sécurité, reportez-vous à la section *Enregistrement/restauration de données entre un fichier et l'automate* du document *EcoStruxure™ Control Expert - Modes de fonctionnement*.

Fonction CCOTF pour un PAC de sécurité M580

Modification de configuration à la volée

La fonction de modification de configuration à la volée CCOTF (change configuration on the fly) permet de modifier une configuration Control Expert lorsque le PAC est en cours d'exécution. Les modifications suivantes peuvent être prises en charge :

- Ajout d'une station
- Ajout d'un module d'E/S

- Suppression d'un module d'E/S
- Modification de la configuration d'un module d'E/S, par exemple :
 - Modification de la valeur d'un paramètre
 - Ajout d'une fonction de canal
 - Suppression d'une fonction de canal
 - Modification d'une fonction de canal

NOTE: les fonctions CCOTF ne s'appliquent pas aux équipements CIP Safety.

La fonctionnalité CCOTF est activée par la case à cocher **Modification en ligne en mode RUN ou STOP** dans l'onglet **Configuration** du module d'UC.

La fonctionnalité de base de CCOTF a été implémentée dans le PAC de sécurité M580 avec les limites décrites ci-après.

Vous trouverez une description complète de CCOTF dans le document *Modicon M580 - Change Configuration on the Fly - Guide utilisateur*.

Limites de CCOTF pour un PAC de sécurité M580

Les limites de l'implémentation de CCOTF dans le PAC de sécurité M580 se fondent sur la fonction et le type spécifiques du module d'E/S :

Fonction CCOTF	Type et mode de fonctionnement du module d'E/S			
	Module d'E/S non perturbateur		Module d'E/S de sécurité SIL3	
	Mode Maintenance	Mode Safety	Mode Maintenance	Mode Safety
Ajouter une station	✓	✓	✓ ¹	✓
Ajouter un module	✓	✓	✓ ¹	X
Supprimer un module	✓	✓	✓	X
Modifier la configuration d'un module d'E/S	✓	✓	X	X
✓ : Autorisé				
X : Non autorisé				
1. Pour ajouter à la fois une station et un module de sécurité, deux sessions CCOTF sont nécessaires : une session CCOTF pour ajouter la station et une seconde session CCOTF pour ajouter le module de sécurité. Ces actions ne peuvent pas être effectuées au sein d'une même session CCOTF.				

NOTE: Les modifications effectuées dans une même session CCOTF ne peuvent concerner qu'une seule tâche (SAFE, MAST, FAST, AUX0 ou AUX1).

Modifications apportées aux outils du PAC de sécurité M580

Introduction

Le PAC de sécurité M580 prend en charge plusieurs outils connexes. Certains de ces outils ont été modifiés pour être utilisés avec le PAC de sécurité M580. Cette section en évoque quelques-uns.

Bilan mémoire

L'écran **Bilan mémoire** présente les informations suivantes :

- la répartition physique de la mémoire du PAC (mémoire interne et carte mémoire)
- l'occupation mémoire d'un projet (données, programme, configuration, système)

Pour le PAC de sécurité M580, cet écran fournit deux nouveaux paramètre, **Données de sécurité déclarées** et **Code exécutable de sécurité**, qui sont décrits ci-après.

NOTE: Vous pouvez également utiliser la commande **Optimiser** dans cet écran pour réorganiser la mémoire lorsque cela est possible.

Pour plus d'informations, reportez-vous à la section *Bilan mémoire* du manuel utilisateur *EcoStruxure™ Control Expert - Modes de fonctionnement*.

Pour le PAC de sécurité M580, les paramètres suivants sont affichés :

Paramètre	Description
Données utilisateur	Ce champ indique l'espace mémoire (en mots) occupé par les données utilisateur (objets concernant la configuration) : • Données : données localisées associées au processeur (%M, %MW, %S, %SW, etc.) ou aux modules d'entrée/sortie. • Données déclarées : données non localisées (déclarées dans l'éditeur de données de processus) enregistrées après une coupure de courant. • Données déclarées non enregistrées : données non localisées (déclarées dans l'éditeur de données de processus) non enregistrées après une coupure de courant. • Données de sécurité déclarées : données non localisées (déclarées dans l'éditeur de données de sécurité) non enregistrées après une coupure de courant.
Programme utilisateur	Ce champ indique l'espace mémoire (en mots) occupé par le programme du projet : • Constantes : constantes statiques associées au processeur (%KW) et aux modules d'entrées/sorties, valeurs initiales des données. • Code exécutable : code exécutable de la zone de processus du programme du projet, types EF, EFB et DFB.

Paramètre	Description
	• Informations d'upload : informations concernant le chargement d'un projet (code graphique des langages, symboles, etc.). • Code exécutable de sécurité : code exécutable de la zone de sécurité du programme du projet, types EF, EFB et DFB.
Autre	Ce champ indique l'espace mémoire (en mots) occupé par les autres données liées à la configuration et à la structure du projet : • Configuration : autres données concernant la configuration (configurations matérielle et logicielle). • Système : données utilisées par le système d'exploitation (pile des tâches, catalogues, etc.). • Diagnostic : informations relatives aux diagnostics de processus ou système, tampon de diagnostic. • Dictionnaire de données : dictionnaire des symboles de variables avec leurs caractéristiques (adresse, type, etc.).
Mémoire interne	Ce champ montre l'organisation de la mémoire interne du PAC. Il indique également l'espace mémoire disponible (Total), l'espace mémoire contigu maximal (Maximum) et le niveau de fragmentation (due aux modifications en ligne).

Observateur d'événements

L'*Observateur d'événements* est un utilitaire MS-Windows qui capture les événements journalisés par Control Expert. Vous pouvez utiliser l'*Observateur d'événements* pour consulter un historique des événements journalisés.

Vous accédez à l'*Observateur d'événements* dans MS-Windows via le dossier *Outils d'administration* du *Panneau de configuration*. A l'ouverture de cet utilitaire, sélectionnez **Afficher le volet d'actions** puis cliquez sur **Créer une vue personnalisée** pour afficher cette boîte de dialogue. Vous pouvez alors créer une vue personnalisée pour les événements Control Expert.

NOTE: Dans la boîte de dialogue **Créer une vue personnalisée**, sélectionnez d'abord **Par source**, puis choisissez la source **TraceServer** pour afficher les événements Control Expert.

CIP Safety

Présentation

Ce chapitre décrit les communications CIP Safety IEC 61784-3 prises en charge par les CPU de sécurité M580 BMEP58•040S autonomes.

Présentation du protocole CIP Safety pour les PAC de sécurité M580

Communication CIP Safety

Introduction

Les contrôleurs de sécurité autonomes BMEP58•040S prennent en charge la communication CIP Safety (CEI 61784-3) et peuvent utiliser ce protocole pour établir une connexion avec un équipement CIP Safety sur EtherNet/IP.

Basé sur le mécanisme de consommateur/producteur, le protocole CIP Safety permet d'échanger des données entre des nœuds SAFE via EtherNet/IP. (Les communications DeviceNet et Sercos III ne sont pas compatibles.) Le contrôleur (la source) établit une connexion EtherNet/IP individuelle avec chaque équipement de sécurité cible. Il peut établir une connexion CIP Safety avec des équipements cibles compatibles CIP Safety et une connexion CIP (non sécurisée) avec des équipements cibles compatibles CIP.

A l'instar des autres contrôleurs de sécurité, le contrôleur CIP Safety et le coprocesseur exécutent deux fois la pile CIP Safety en parallèle et comparent les résultats obtenus.

Architectures prises en charge

Les contrôleurs de sécurité M580 autonomes prennent en charge les équipements CIP Safety appartenant à des nuages DIO.

NOTE: pour l'instant, il n'existe pas d'équipement CIP Safety compatible RSTP pouvant être installé dans un rack eX80. Cela signifie qu'il est actuellement impossible de connecter un équipement CIP Safety au port double de réseau d'équipements du contrôleur. Par contre, vous pouvez le connecter au port de service du contrôleur.

Les nuages DIO nécessitent uniquement une connexion cuivre (sans anneau) et peuvent être connectés :

- à un module de sélection d'options de réseau BMENOS0300,
- Au port de service du contrôleur.
- au port de service d'un module adaptateur d'E/S Ethernet eX80 BM•CRA312•0 dans une station d'E/S distantes,
- au port cuivre d'un commutateur double anneau Ethernet.

NOTE: lorsqu'un équipement CIP Safety est connecté au port de service d'un module adaptateur d'E/S Ethernet eX80 BM•CRA312•0 dans une station d'E/S distantes, il se peut que l'équipement CIP Safety cible ne démarre pas automatiquement tandis que le module CRA est en train de charger sa configuration. Pour que les connexions CIP Safety s'établissent comme prévu, vous aurez peut-être besoin de gérer le bit de contrôle de la connexion CIP Safety dans le DDDT cible (CTRL_IN ou CTRL_OUT) et de le faire passer de False à True une fois la configuration du BM•CRA312•0 chargée.

Comme les autres équipements présents dans des nuages DIO, les équipements CIP Safety ne sont pas scrutés dans l'anneau d'E/S distantes principal et les LED du contrôleur n'indiquent pas l'état de leur connexion.

Pour plus d'informations sur les nuages DIO, reportez-vous aux documents *Modicon M580 Autonome - Guide de planification du système pour architectures courantes* et *Modicon M580 - Guide de planification du système pour topologies complexes*.

Présentation de la configuration

La procédure de configuration des communications CIP Safety comprend trois étapes :

- Configurez le contrôleur autonome de sécurité M580 à l'aide de paramètres CIP Safety dans *Control Expert*, page 365. Cette étape inclut la création d'un identifiant unique de réseau source (OUNID) qui identifie le contrôleur de façon unique. L'identifiant OUNID est créé dans *Control Expert* et correspond à la concaténation de deux composants :
 - Numéro de réseau de sécurité (SNN) : Identifiant du contrôleur créé dans *Control Expert*.
 - Adresse IP principale du contrôleur, indiquée dans *Control Expert* sous les paramètres d'adresse IP du contrôleur.

Configurez le paramètre OUNID du contrôleur une seule fois, dans la configuration initiale. En cas de modification ultérieure, vous devrez reconfigurer l'ensemble des équipements CIP Safety connectés au contrôleur.

- Configurer l'équipement CIP Safety, page 369 à l'aide d'un outil de configuration de réseau de sécurité (SNCT) fourni par le fabricant de l'équipement. Cette étape inclut deux opérations :
 - Création d'un identifiant de configuration de sécurité (SCID) : Également appelé signature de configuration, le SCID est créé dans le SNCT et utilisé par *Control Expert* lors de la configuration de la connexion CIP Safety entre la source (contrôleur) et la cible (équipement CIP Safety).
 - Affectation d'un numéro de réseau de sécurité (SNN) : Le SNN est généralement créé pour l'équipement CIP Safety par *Control Expert* et est affecté à l'équipement par le SNCT.

- Configurez la connexion CIP Safety entre le contrôleur l'équipement CIP Safety, page 371. La connexion est associée à un identifiant TUNID créé avec le DTM de connexion d'équipement dans Control Expert qui utilise un DTM CIP Safety, lequel peut être basé sur un fichier EDS fourni par le fabricant ou utilisé de manière autonome si ce fichier n'est pas disponible.

Gestion des connexions d'équipement CIP Safety

Le contrôleur de sécurité CIP Safety établit une connexion avec un équipement CIP configuré et gère ensuite cet équipement. Control Expert prend en charge les protocoles CIP et CIP Safety, ce qui lui permet de gérer les connexions CIP avec :

- des équipements CIP, qui mettent en œuvre le protocole CIP sur EtherNet/IP, mais pas CIP Safety ;
- des équipements CIP Safety, qui mettent en œuvre le protocole CIP Safety sur EtherNet/IP, mais pas CIP ;
- des équipements CIP hybrides, qui mettent en œuvre les protocoles CIP et CIP Safety sur EtherNet/IP.

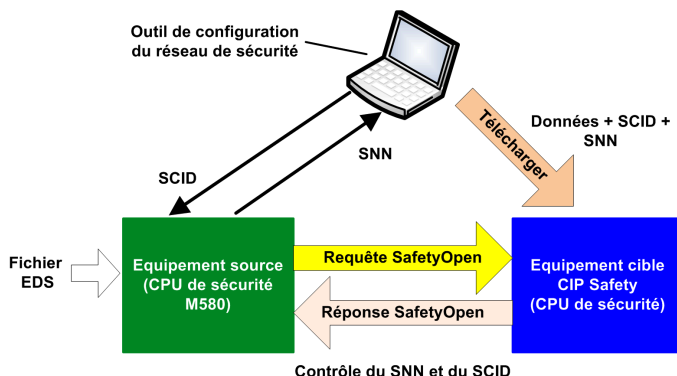
NOTE: en présence d'un équipement CIP et d'un équipement CIP Safety, chacun doit être configuré avec un DTM spécifique. Un équipement CIP hybride (mettant en œuvre les protocoles CIP et CIP Safety) nécessite deux DTM : un configuré comme équipement CIP et un autre comme équipement CIP Safety.

Etablissement d'une connexion Source -> Cible

Le contrôleur M580 autonome établit une connexion avec un équipement CIP Safety uniquement via une requête SafetyOpen de type 2. Pour qu'une telle connexion puisse être établie, l'équipement de sécurité doit avoir été configuré par un SNCT. Si l'équipement CIP Safety provient d'un fabricant tiers, Control Expert ne dispose pas du fichier de configuration adéquat. Cela signifie qu'il ne peut pas le télécharger sur l'équipement ni être utilisé comme SNCT.

NOTE: avec une requête SafetyOpen de type 1, les paramètres de configuration sont fournis à l'équipement de sécurité et la connexion est établie. Les contrôleurs CIP Safety M580 ne prennent pas en charge les requêtes de connexion SafetyOpen de type 1.

Le schéma suivant montre comment établir une connexion CIP Safety entre le contrôleur (source) et l'équipement CIP Safety (cible) :



Voici le déroulé des événements :

1. Control Expert crée un DTM de connexion entre le contrôleur et l'équipement CIP Safety d'après un fichier EDS envoyé par le fabricant.
2. Le SNN de l'équipement est généré dans Control Expert, puis indiqué dans le SNCT.
3. Le SNCT crée l'identifiant SCID de l'équipement, lequel est indiqué dans Control Expert dans la configuration de la connexion.
4. Le SNCT télécharge les éléments suivants sur l'équipement : les paramètres de configuration de l'équipement, l'identifiant SCID généré par le SNCT et le SNN généré par Control Expert pour la connexion.
5. Le contrôleur (la source) envoie une requête SafetyOpen de type 2 à l'équipement.
6. L'équipement CIP Safety envoie une réponse SafetyOpen au contrôleur.
7. Si les sommes de contrôle de la requête et de la réponse correspondent, la connexion est établie.

Configuration de la CPU CIP Safety M580

Présentation

Cette section décrit la procédure de configuration de la CPU CIP Safety autonome en tant que source des communications CIP Safety.

Configuration de l'identifiant OUNID de la CPU

CPU en tant que source

L'onglet (voir Modicon M580, Matériel, Manuel de référence) **Safety** de la CPU de sécurité M580 autonome permet de configurer cet équipement en tant que source CIP Safety, en lui affectant un identifiant de réseau source unique (OUNID).

Un identifiant OUNID est une valeur hexadécimale concaténée de 10 octets, composée :

- d'un numéro de réseau de sécurité (6 octets),
- d'une adresse IP (4 octets).

NOTE: il est possible de modifier l'identifiant OUNID en local. Une fois la configuration mise à jour générée, l'application peut être téléchargée sur le PAC.

Numéro du réseau de sécurité

Le numéro du réseau de sécurité de l'identifiant OUNID peut être généré automatiquement par Control Expert ou indiqué manuellement par l'utilisateur. Vous pouvez créer le SNN :

- automatiquement, en sélectionnant **Horaire**, puis en cliquant sur l'option **Générer** (la valeur générée automatiquement s'affiche dans le champ **Numéro**) ;
- manuellement, en sélectionnant **Manuel**, puis en saisissant une chaîne hexadécimale de 6 octets dans le champ **Numéro**.

NOTE: l'utilisateur doit affecter un SNN unique à chaque CPU M580 source connectée à un même réseau de sécurité.

Adresse IP

Ce paramètre en lecture seule est automatiquement renseigné en fonction du paramètre **Adresse IP principale** configuré pour la CPU dans l'onglet (voir Modicon M580, Matériel, Manuel de référence) **IPConfig**.

OUNID

Une fois créé, l'identifiant OUNID sert de paramètre dans la requête SafetyOpen de type 2, [page 386](#) et permet d'établir une connexion entre la CPU (source) et l'équipement CIP Safety (cible).

Configuration de l'équipement CIP Safety cible

Présentation

Cette section décrit la procédure de configuration de l'équipement CIP Safety cible, y compris à l'aide d'un outil de configuration fourni par le fabricant.

Présentation de la configuration de l'équipement CIP Safety

Introduction

La procédure de configuration de l'équipement CIP Safety comprend deux étapes :

- Configurer les paramètres de l'équipement CIP Safety, page 369 à l'aide d'un outil de configuration du réseau de sécurité (SNCT) fourni par le fabricant
- Configurer la connexion entre la CPU CIP Safety source et l'équipement CIP Safety cible, via un DTM dans Control Expert. Le DTM peut être :
 - basé sur un fichier EDS fourni par le fabricant ;
 - un DTM Control Expert générique, en l'absence de fichier EDS.

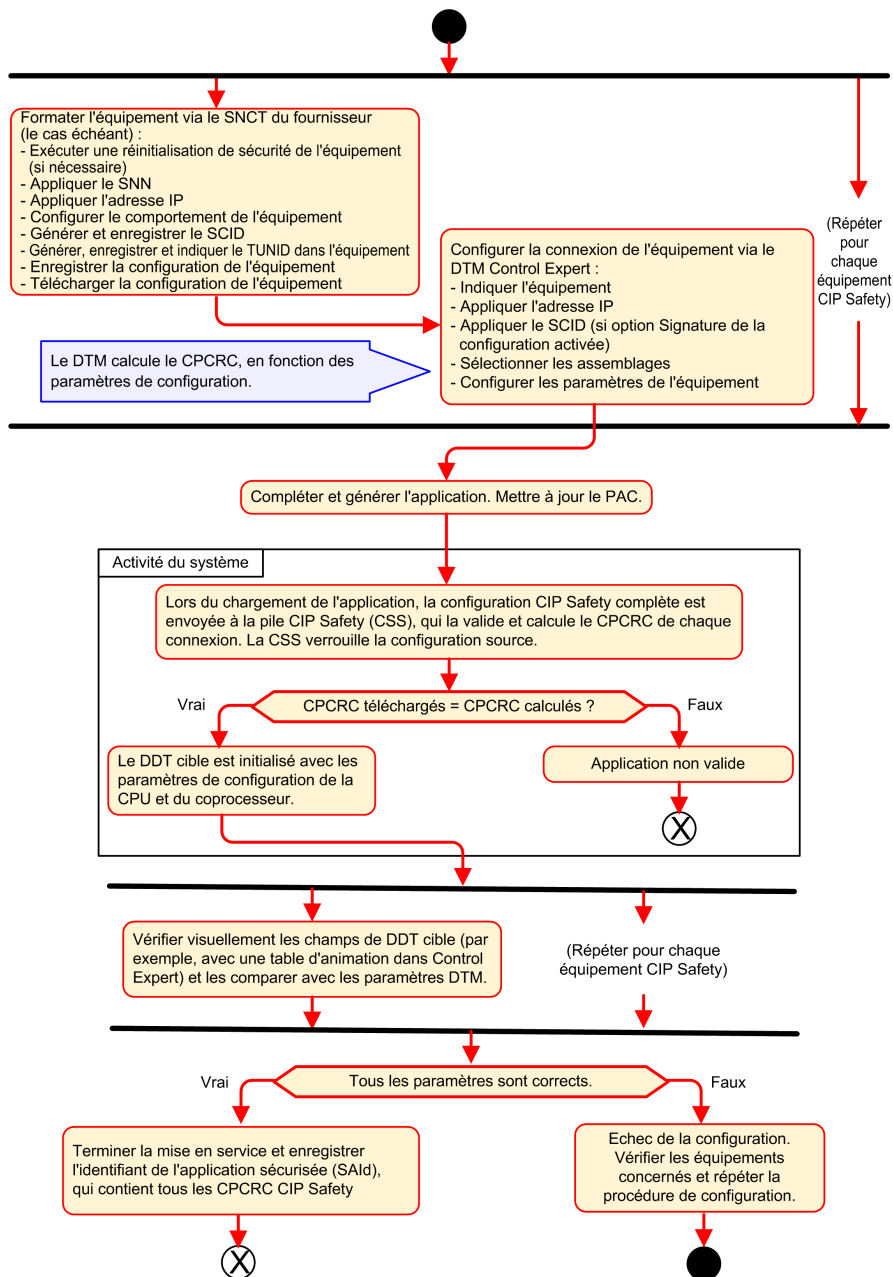
Double contrôle de la configuration

Combinés, les deux processus suivants permettent de confirmer avec un haut degré de certitude que la configuration générée via le logiciel Control Expert a bien été téléchargée et enregistrée sur la CPU CIP Safety M580 source :

- Comparaison visuelle par l'utilisateur (après téléchargement de l'application) des paramètres de configuration de la connexion CIP Safety apparaissant dans le DDDT cible avec ceux du DTM cible
- Comparaison automatique, par la CPU et le coprocesseur, du CRC des paramètres de connexion (CPCRC) calculé par le DTM avec celui calculé par la pile CIP Safety (CSS) exécutée dans la CPU et le coprocesseur

Présentation de la procédure de configuration

Procédure de configuration et de validation de l'équipement CIP Safety :



Configuration de l'équipement CIP Safety à l'aide d'un outil fourni par le fabricant

Introduction

L'équipement CIP Safety cible est configuré à l'aide d'un outil de configuration de réseau de sécurité (SNCT), et non via le logiciel Control Expert. Comme il est fourni par le fabricant de l'équipement CIP Safety, l'outil SNCT est propre à cet équipement.

Avec le SNCT, vous pouvez :

- configurer et télécharger sur l'équipement les paramètres nécessaires à son bon fonctionnement ;
- configurer un identifiant de configuration de sécurité (SCID) propre à l'équipement, puis le copier et le transférer vers le logiciel Control Expert. Egalement appelé "signature de la configuration" de l'équipement, le SCID est utilisé dans Control Expert lors de la configuration de la connexion Source -> Cible, page 376 ;
- affecter à l'équipement son identifiant TUNID unique, constitué :
 - d'un numéro de réseau de sécurité (SNN), page 375 et
 - d'une adresse IP unique.

NOTE: en général, le SNN est généré par le logiciel de configuration Control Expert (lors de la configuration de la connexion Source -> Cible), puis appliqué à l'équipement. L'adresse IP est indiquée à la fois dans le SNCT et dans le DTM de connexion de l'équipement dans Control Expert.

Configuration de l'identifiant SCID

Le SCID est défini dans le SNCT et sert d'identifiant de configuration hexadécimal unique pour l'équipement CIP Safety cible. Il correspond à la concaténation des éléments suivants :

- CRC de configuration de sécurité (SCCRC) : valeur de contrôle de redondance cyclique (CRC) des paramètres de configuration de l'équipement CIP Safety (4 octets).
- Horodatage de configuration de sécurité (SCTS) : valeur hexadécimale de date et heure de 6 octets.

NOTE: Si le contrôleur CPU M580 est configuré comme équipement CIP Safety source, testez et vérifiez le bon fonctionnement du système avant de contrôler la fonction de sécurité associée via une communication CIP Safety. Lorsque les tests et la vérification ont été correctement exécutés, activez la signature de la configuration CIP Safety cible (si elle existe) dans les DTM CIP Safety Control Expert.

Une fois l'identifiant SCID généré via le SNCT, vous pouvez indiquer ses différents éléments dans l'onglet **Safety** du DTM d'équipement dans Control Expert :

- **ID** : saisissez la valeur SCCRC.

- **Date** : saisissez la date à laquelle le SCID a été créé (mm/jj/aaaa).
- **Heure** : saisissez l'heure à laquelle le SCID a été créé (hh/mm/ss/ms).

Procédure de configuration de l'équipement CIP Safety

La procédure de configuration standard d'un équipement CIP Safety est décrite ci-dessous :

1. Récupérez le SNN de l'équipement (depuis Control Expert).
2. Appliquez le SNN dans le SNCT du fabricant.
3. Exécutez une réinitialisation de sécurité de l'équipement (facultatif, seulement si l'identifiant OUNID de la source a changé depuis la dernière connexion de l'équipement).
4. Appliquez l'identifiant TUNID dans l'équipement.
5. Configurez les paramètres qui contrôleront le comportement de l'équipement.
6. Configurez l'équipement à l'aide de l'outil de configuration du réseau de sécurité (SNCT) du fabricant.
7. Verrouillez la configuration et assurez-vous qu'elle est exacte.
8. Enregistrez les paramètres dans la configuration de la source (SCID, numéros d'assemblage, adresse IP, etc.).
9. Enregistrez une copie de la configuration de l'équipement pour un usage ultérieur (si celui-ci doit être remplacé, par exemple).

Configuration des DTM des équipements de sécurité

Présentation

Cette section décrit la procédure de configuration des équipements de sécurité cibles et de leur connexion à la CPU source à l'aide des DTM dans Control Expert.

Utilisation des DTM

Utilisation des DTM

La configuration de la connexion entre la CPU source et l'équipement CIP Safety cible s'effectue à l'aide d'un DTM. Control Expert prend en charge les DTM suivants, selon le profil d'équipement :

- DTM CIP Safety : permet de configurer une connexion à un équipement CIP Safety. Cela peut être effectué à l'aide d'un fichier EDS fourni par le fabricant ou du *fichier EDS de sécurité générique* inclus dans Control Expert.
- DTM générique : permet de configurer une connexion standard (non sécurisée) à un équipement, d'après le fichier EDS fourni par le fabricant.

Les paramètres indiqués via un DTM sont stockés dans Control Expert dans le DDDT, page 396 T_CIP_SAFETY_CONF et utilisés par la requête SafetyOpen de type 2, page 386 pour établir une connexion entre la CPU source et l'équipement cible.

Lorsqu'un fichier EDS est disponible

Lorsqu'un fichier EDS fourni par un fabricant est disponible pour un équipement, utilisez-le pour créer un nouveau DTM et ajoutez-le au **catalogue DTM de** Control Expert comme suit :

Étape	Action
1	Dans Control Expert, sélectionnez Outils > Navigateur DTM .
2	Dans le Navigateur de DTM , cliquez avec le bouton droit de la souris sur le DTM de la CPU (BMEP58_ECPU_EXT) pour ouvrir le menu contextuel.

Étape	Action
3	Sélectionnez le menu Équipement > Fonctions supplémentaires > Ajouter un fichier EDS à la bibliothèque . L'assistant Ajout EDS s'ouvre.
4	Reportez-vous à la Ajouter un fichier EDS au catalogue de matériels (voirEcoStruxure™ Control Expert, Modes de fonctionnement pour la procédure détaillée expliquant pas à pas comment Ajouter un fichier EDS au catalogue DTM.

Une fois le DTM ajouté au **Catalogue DTM**, vous pouvez l'ajouter dans votre projet Control Expert.

Fichier EDS non disponible

Control Expert inclut un DTM de sécurité générique dans le **Catalogue DTM**. que vous pouvez utiliser pour configurer un équipement CIP Safety si aucun fichier EDS n'est disponible pour cet équipement.

Equipements hybrides

Un équipement hybride prend en charge les connexions standard et les connexions de sécurité. Lors de l'ajout d'un équipement hybride au **catalogue DTM** via la commande **Ajouter l'EDS à la bibliothèque**, deux DTM sont créés dans le **Catalogue DTM** pour l'équipement DTM : un DTM standard et un DTM de sécurité.

Lorsque vous ajoutez un équipement hybride à votre projet, vous devez configurer à la fois le DTM standard et le DTM de sécurité.

Ajout d'un DTM à un projet Control Expert

Pour ajouter un DTM à un projet Control Expert :

Etape	Action
1	Dans le Navigateur de DTM , cliquez avec le bouton droit de la souris sur le DTM de la CPU (BMCP58_ECPU_EXT), puis sélectionnez Ajouter . La boîte de dialogue Ajouter s'ouvre.
2	Sélectionnez le DTM à ajouter. Il peut s'agir : - d'un DTM CIP Safety créé d'après le fichier EDS d'équipement CIP Safety fourni par le fabricant ou - d'un DTM CIP Safety sans fichier EDS.

Etape	Action
3	Cliquez sur Ajouter un DTM . Le DTM sélectionné apparaît dans le Navigateur de DTM , sous le DTM de la CPU.
4	Cliquez avec le bouton droit de la souris sous le nouveau DTM, puis sélectionnez l'option Ouvrir . La fenêtre de configuration du DTM s'affiche.

Configuration du DTM

Le DTM CIP Safety est associé aux mêmes écrans de configuration dans Control Expert, qu'il ait été créé avec ou sans le fichier EDS du fabricant :

Arborescence de navigation/Onglets de configuration		Type de DTM	
		Avec le fichier EDS du fabricant	Sans le fichier EDS du fabricant
<Nœud du haut>		✓	✓
	Nœud Général		
	Onglet Equipement	✓	X
	Onglet Safety	✓	✓
	<Connexions>		
	Onglet Connexion	✓	✓
	Onglet Vérification d'identité	✓	✓
	Onglet Paramètres de configuration	✓	X
	Onglet Vérification de la configuration	✓	✓
	< > = nom défini par l'utilisateur		
	✓ = inclus		
	X = non inclus		

Les onglets de configuration disponibles pour chaque type de DTM dans Control Expert sont décrits dans les sections suivantes.

DTM d'équipements de sécurité - Informations sur le fichier et le fabricant

Introduction

Peu importe qu'il ait été créé ou non à l'aide du fichier EDS fourni par le fabricant, le DTM CIP Safety contient une description du fichier EDS source et du fabricant de l'équipement. Deux scénarios sont possibles :

- DTM CIP Safety créé à partir du fichier EDS du fabricant : ces informations sont accessibles en lecture seule depuis le <Nœud du haut> de l'arborescence de navigation du DTM (volet de gauche).
- DTM CIP Safety créé sans le fichier EDS du fabricant : ces informations apparaissent à deux endroits distincts :
 - <Nœud du haut> : informations concernant le fichier EDS, en lecture seule.
NOTE: la référence de fichier EDS est un fichier EDS de sécurité générique interne (Schneider Electric est le fabricant), qui permet à Control Expert de créer le DTM CIP Safety.
 - Onglet **Général > Equipement** : informations sur le fabricant, modifiables.

Informations concernant le fichier EDS

Les informations suivantes concernant le fichier EDS sont accessibles en lecture seule :

- Description
- Date de création du fichier
- Heure de création du fichier
- Date de la dernière modification
- Heure de la dernière modification
- Révision du fichier EDS

Informations concernant le fabricant

Les informations suivantes concernant le fabricant sont accessibles en lecture seule pour un DTM CIP Safety créé à partir du fichier EDS du fabricant :

- Nom du fabricant
- Type d'équipement
- Révision majeure

- Révision mineure
- Nom du produit

Les informations suivantes concernant le fabricant sont accessibles en lecture/écriture pour un DTM CIP Safety créé sans le fichier EDS du fabricant :

- ID fabricant
- Type de produit
- Code du produit
- Révision majeure
- Révision mineure

NOTE: pour les DTM configurés sans fichier EDS, renseignez les informations fabricant à l'aide des données fournies par celui-ci. Par défaut, ces valeurs sont définies sur 0 et ne sont pas prises en charge.

DTM d'équipements de sécurité - Numéro du réseau de sécurité

Numéro du réseau de sécurité

L'onglet **Général > Safety** du DTM d'équipement CIP Safety permet de configurer un numéro de réseau de sécurité (SNN) pour l'équipement de sécurité. Ce SNN sert à définir l'identifiant de réseau cible unique (TUNID), un ID qui identifie l'équipement CIP Safety et constitue un élément essentiel de la requête `SafetyOpen` de type 2, page 386 émise par le contrôleur source pour établir une connexion CIP Safety.

Configuration du module SNN

Le SNN est une valeur hexadécimale configurée à la fois pour les connexions CIP Safety (avec Control Expert) et pour les équipements CIP Safety (avec un SNCT). En général, il est créé dans Control Expert et copié (ou saisi) dans le SNCT. Cet outil génère ensuite un identifiant TUNID sur la base du SNN et de l'adresse IP, qu'il transfère à l'équipement CIP Safety.

Control Expert permet aussi d'envoyer directement le SNN depuis le DTM de connexion CIP Safety vers l'équipement cible, page 394.

Configurer le SNN :

Eta-pe	Action
1	Dans l'onglet Général > Safety , cliquez sur le bouton représentant des points de suspension (...). La boîte de dialogue Numéro de réseau de sécurité s'affiche.
2	Dans la boîte de dialogue Numéro de réseau de sécurité, sélectionnez l'une des options suivantes : • Horaire : permet de générer une valeur hexadécimale basée sur le mois, le jour, l'année, l'heure, les minutes, les secondes et les millisecondes au moment de la génération. • Manuel : permet de générer une valeur basée sur une valeur décimale d'entrée comprise entre 1 et 9 999, concaténée avec deux valeurs hexadécimales comme suit : ◦ mot 1 : 0004 (fixe) ◦ mot 2 : 0000 (fixe) ◦ Mot 3 : 0001...270F (valeur hexadécimale de la valeur d'entrée comprise entre 1 et 9 999) • Spécifique au fournisseur : Identifiant spécifique au fournisseur basé sur 3 mots hexadécimaux d'entrée : ◦ Mot 1 : 05B5...2DA7 (du fournisseur) ◦ mot 2 : 0000 (fixe) ◦ Mot 3 : 0001...270F (du fournisseur) • Une valeur hexadécimale indiquée directement (saisie ou collée par l'utilisateur), composée des éléments suivants : ◦ Mot 1 : 2DA8...FFFE ◦ Mots 2 et 3 : 00000000...05265BFF
3	Avec l'option Horaire, Manuel ou Spécifique du fabricant, cliquez sur Générer.. Si vous saisissez directement une valeur hexadécimale, cliquez sur Définir.
4	Cliquez sur OK pour enregistrer le SNN et fermer la boîte de dialogue. Le SNN apparaît dans le champ Numéro de réseau de sécurité.

Configuration de l'identifiant SCID

Le SCID, ou signature de la configuration, est défini dans l'outil de configuration du réseau de sécurité (SNCT) fourni par le fabricant et correspond à l'identifiant de configuration hexadécimal unique de l'équipement CIP Safety. Il correspond à la concaténation des éléments suivants :

- CRC de configuration de sécurité (SCCRC) : Il s'agit de la valeur de contrôle de redondance cyclique (CRC) des paramètres de configuration d'un équipement de sécurité sous la forme d'une valeur hexadécimale de 4 octets.
- Horodatage de configuration de sécurité (SCTS) : Il s'agit de l'horodatage représentant une valeur hexadécimale de date et heure de 6 octets.

Indiquer le SCID :

Etape	Action
1	Récupérez les informations suivantes dans la configuration de l'équipement à l'aide du SNCT : • le SCCRC, • la date (mm/jj/aaaa) et l'heure (hh/mm/ss/ms) de configuration dans le SNCT.
2	Sélectionnez Signature de la configuration .
3	Saisissez le SCCRC dans le champ ID .
4	Saisissez les valeurs de date et heure dans les champs Date et Heure .

NOTE: si vous configurez des connexions de sécurité avec un SCID égal à 0 (configuration du SCID désactivée), vérifiez que l'équipement Safety source et les équipements Safety cibles du M580 sont correctement configurés.

DTM d'équipements de sécurité - Vérification et validation de la configuration

Vérification visuelle de la configuration du DTM

Dans l'onglet **Général > Vérification de la configuration** du DTM CIP Safety (créé avec ou sans le fichier EDS du fabricant), comparez les paramètres définis dans le DTM (et affichés dans cet onglet) avec ceux définis dans le DDDT de l'équipement cible. Pour ce faire, vous pouvez utiliser une table d'animation (à condition que Control Expert soit exécuté en mode connecté et connecté à la CPU).

NOTE: après le téléchargement d'une application, vérifiez visuellement pour chaque cible CIP Safety que les paramètres de configuration CIP Safety téléchargés sur la source M580 pour la cible en question correspondent à ceux configurés dans le DTM cible. Pour cela, vous pouvez comparer les paramètres de configuration figurant dans le DDDT cible CIP Safety (avec une table d'animation Control Expert en mode connecté) avec ceux configurés dans le DTM et affichés dans l'onglet Vérification de la configuration.

Validation de la configuration téléchargée

Une fois que toutes les configurations CIP Safety ont été téléchargées, elles peuvent être validées par l'utilisateur. L'un des tests consiste à vérifier les configurations de connexion de sécurité appliquées dans une source pour s'assurer que la connexion cible fonctionne comme prévu.

DTM d'équipements de sécurité - Connexions d'E/S

Introduction

Le DTM CIP Safety contient des nœuds de connexion de sécurité, qu'il ait été créé avec ou sans le fichier EDS du fabricant. Selon les fonctions de l'équipement, les nœuds d'entrée et de sortie de sécurité peuvent être pris en charge. L'onglet **Connexion** contient les paramètres de la connexion d'entrée ou de sortie sélectionnée.

Des connexions sont sélectionnées par défaut lorsque le DTM a été créé avec le fichier EDS du fabricant. Les commandes **Supprimer la connexion** et **Ajouter une connexion** permettent d'ajuster les paramètres de connexion en fonction des exigences de l'application.

Paramètres des connexions d'entrée de sécurité

Chaque connexion d'entrée de sécurité est associée aux paramètres suivants :

- **Taille de l'entrée** (lecture/criture) : taille des données d'entrée configurée dans l'équipement CIP Safety, en octets. Valeur définie sur 0 par défaut.
NOTE: remplacez la valeur par défaut par les paramètres indiqués par le fabricant, car la valeur 0 n'est pas prise en charge.
- **Intervalle demandé entre paquets** (lecture/écriture) : RPI représente la période d'actualisation de la connexion. Valeur définie par défaut sur (Durée de la tâche SAFE)/ 2.
NOTE: la durée de la tâche SAFE (Tsaf) est définie dans la boîte de dialogue **Propriétés de SAFE** (Navigateur du projet > Tâches > SAFE > Propriétés) dans Control Expert.
- **Temps_reseau_attendu** (lecture/écriture) : Temps, en millisecondes, consommé par la communications CIP Safety Incidence des communications CIP Safety sur le temps de réaction du système de sécurité, page 170. Lorsque cette valeur est inférieure à la valeur *Temps_reseau_attendu_minimal*, une notification de détection d'erreur s'affiche. Elle équivaut par défaut à $\text{Temps_reseau_attendu_minimal} * 1,5$.
- **Multiplicateur_timeout** (lecture/écriture) : élément de l'équation ayant pour résultat la valeur *Temps_reseau_attendu_minimal*. Cette valeur équivaut à $\text{Temps_reseau_attendu} / 128 \mu\text{Sec}$. Le $\text{Temps_reseau_attendu_minimal} = \text{RPI} * \text{Multiplicateur_timeout} + \text{Tsaf} + 40$.

- **Transmission_réseau_max** (lecture/écriture) : âge le plus élevé (en ms) des données au moment où le consommateur reçoit la trame. Ce paramètre sert uniquement à calculer la valeur minimale à indiquer pour Temps_réseau_attendu (voir description ci-dessous). Il peut être affiné en vérifiant la valeur *âge_max-données* au niveau de l'équipement consommateur longtemps après avoir exécuté une communication réseau CIP Safety.

Ce paramètre est utilisé pour calculer la valeur minimale du paramètre Temps_réseau_attendu, comme suit :

$$\text{Temps_réseau_attendu_minimal} = \text{RPI} * \text{Multiplicateur_timeout} + \text{Transmission_réseau_max}$$

La modification de la valeur Tsafe a une incidence sur ce paramètre et, par voie de conséquence, sur la valeur minimale de *Temps_réseau_attendu*.

Attributs de ce paramètre :

- Valeur minimale = 1- ms
- Valeur maximale = 5 800 ms
- Valeur par défaut = 40 + Tsafe

Le DTM d'équipement s'appuie sur ces paramètres d'entrée pour procéder aux calculs suivants :

Variable	Valeur		
	Par défaut	Minimale	Maximum
Durée de la tâche SAFE (ms)	20	10	255
Intervalle de trame demandé en entrée (ms)	$\text{RPI} = \text{Tsafe} / 2$	5	500
Multiplicateur de timeout	2	1	255
Transmission_réseau_max (ms)	$40 + 2 * \text{Tsafe}$	10	5800
Temps réseau attendu	$\text{Temps_réseau_attendu_minimal} * 1,5$	$\text{RPI} * \text{Multiplicateur_timeout} + \text{Transmission_réseau_max}$	5800

Paramètres des connexions de sortie de sécurité

Chaque connexion de sortie de sécurité est associée aux paramètres suivants :

- **Taille de la sortie** (lecture/écriture) : taille des données de sortie configurée dans l'équipement CIP Safety, en octets. Valeur définie sur 0 par défaut.

NOTE: remplacez la valeur par défaut par les paramètres indiqués par le fabricant, car la valeur 0 n'est pas prise en charge.

- **Intervalle demandé entre paquets** (lecture seulement) : RPI représente la période d'actualisation de la connexion. Cette valeur équivaut à la durée de la tâche SAFE (Tsafe).
- **Temps réseau attendu** (lecture/écriture) : Temps, en millisecondes, consommé par la communications CIP Safety Incidence des communications CIP Safety sur le temps de réaction du système de sécurité, page 170. Lorsque cette valeur est inférieure à la valeur *Temps_réseau_attendu_minimal*, une notification de détection d'erreur s'affiche. Elle équivaut par défaut à *Temps_réseau_attendu_minimal* * 1,5.
- **Multiplicateur de timeout** (lecture/écriture) : élément de l'équation ayant pour résultat la valeur *Temps_réseau_attendu_minimal*. Cette valeur équivaut à *Temps_réseau_attendu* / 128 µSec. Le *Temps_réseau_attendu_minimal* = RPI * Multiplicateur_timeout + Tsafe + 40.
- **Transmission_réseau_max** (lecture/écriture) : âge le plus élevé (en ms) des données au moment où le consommateur reçoit la trame. Ce paramètre sert uniquement à calculer la valeur minimale à indiquer pour *Temps_réseau_attendu* (voir description ci-dessous). Il peut être affiné en vérifiant la valeur *âge_max-données* au niveau de l'équipement consommateur longtemps après avoir exécuté une communication réseau CIP Safety.

Ce paramètre est utilisé pour calculer la valeur minimale du paramètre *Temps_réseau_attendu*, comme suit :

$$\text{Temps_réseau_attendu_minimal} = \text{RPI} * \text{Multiplicateur_timeout} + \text{Transmission_réseau_max}$$

La modification de la valeur Tsafe a une incidence sur ce paramètre et, par voie de conséquence, sur la valeur minimale de *Temps_réseau_attendu*.

Attributs de ce paramètre :

- Valeur minimale = 1- ms
- Valeur maximale = 5800 ms
- Valeur par défaut = 40 + 2*Tsafe

Le DTM d'équipement s'appuie sur ces paramètres de sortie pour procéder aux calculs suivants :

Variable	Valeur		
	Par défaut	Minimale	Maximum
Durée de la tâche SAFE (ms)	20	10	255
Intervalle de trame demandé en entrée (ms)	RPI = Tsafe	10	255
Multiplicateur de timeout	2	1	255
Transmission_réseau_max (ms)	40 + 2 * Tsafe	10	5800
Temps réseau attendu	Temps_réseau_attendu_minimal * 1,5	RPI * Multiplicateur_timeout + Transmission_réseau_max	5800

Vérification de l'identité de l'équipement distant

Utilisez cet onglet pour indiquer dans quelle mesure un équipement distant (détecté sur le réseau) est conforme aux paramètres de configuration du même équipement distant dans le projet d'application Control Expert. Control Expert ne conserve pas les connexions à un équipement distant qui ne réussit pas cette vérification d'identité.

NOTE: Cette page apparaît uniquement pour les types de DTM génériques qui prennent en charge les connexions, par exemple, un DTM d'équipement générique, un DTM générique avancé et un DTM de sécurité générique.

Le DTM de message explicite d'équipement générique ne prend pas en charge les connexions.

Pour ouvrir cette page, procédez comme suit :

Étape	Action
1	Double-cliquez sur l'équipement distant dans le Navigateur de DTM pour ouvrir son DTM dans l' Éditeur d'équipement .
2	Dans l'arborescence de navigation du volet gauche de l' Éditeur d'équipement , sélectionnez le nœud de connexion que vous souhaitez configurer.
3	Dans le volet droit de l' Éditeur de périphérique , cliquez sur l'onglet Vérification d'identité .

NOTE: Lorsque cette page est ouverte, vous pouvez utiliser la commande **Supprimer la connexion** pour supprimer la connexion sélectionnée.

Propriétés d'identité des équipements distants

Une connexion à un équipement Schneider Electric distant peut présenter les propriétés suivantes :

Propriété	Description
Vérifier l'identité	Cette propriété définit la règle que Control Expert utilise pour comparer l'équipement configuré à l'équipement distant réel. Voici les valeurs disponibles : • Correspondance exacte requise : le fichier DTM ou EDS correspond exactement à l'équipement distant. • Désactiver : aucune vérification n'a lieu. La partie identité de la connexion est remplie de valeurs égales à zéro (paramètre par défaut). • Doit être compatible : si l'équipement distant est différent de celui défini par le DTM/EDS, il émule les définitions DTM/EDS. • Aucune : aucune vérification n'a lieu. La partie identité de la connexion est omise. • Personnaliser : permet de définir individuellement les six paramètres suivants.
Si Vérification d'identité est défini sur Personnaliser , renseignez les champs suivants :	

Propriété	Description
Mode de compatibilité	• Vrai : pour chacun des tests sélectionnés ci-dessous, le DTM/EDS et l'équipement distant doivent être compatibles. • Faux : pour chacun des tests sélectionnés suivants, le DTM/EDS et l'équipement distant doivent correspondre exactement.
Version mineure	Pour chacun de ces éléments, sélectionnez un paramètre : • Compatible : inclure le paramètre dans le test. • Non vérifié : ne pas inclure le paramètre dans le test.
Version majeure	
Code du produit	
Type de produit	
Fournisseur du produit	

DTM d'équipements de sécurité - Paramètres des connexions d'E/S

Introduction

Lorsqu'il est créé sans le fichier EDS du fabricant, le DTM CIP Safety contient l'onglet **Paramètres de configuration** pour le nœud de connexion.

L'onglet **Paramètres de configuration** permet de configurer la connexion entre la CPU et l'équipement distant.

Paramètres

L'onglet **Paramètres de configuration** contient les paramètres suivants :

- **Instance d'entrée** : numéro d'assemblage propre à l'équipement associé aux transmissions d'entrée (T→O).
- **Instance de sortie** : numéro d'assemblage propre à l'équipement associé aux transmissions de sortie (O→T).
- **Instance de configuration** : numéro d'assemblage propre à l'équipement associé aux paramètres de configuration d'équipement.

Paramètres d'adresse IP de l'équipement de sécurité

Modification du DTM maître de la CPU M580

Les paramètres d'adresse IP et DHCP d'un équipement CIP Safety peuvent être configurés au niveau du DTM maître de la CPU M580.

NOTE: l'adresse IP n'est pas définie dans le DTM de connexion de l'équipement, contrairement aux autres paramètres de configuration de la connexion de l'équipement cible.

Accès aux paramètres d'adresse IP de l'équipement de sécurité

Pour modifier les paramètres d'adresse IP et DHCP d'un équipement CIP Safety, procédez comme suit :

Etape	Action
1	Déconnectez Control Expert de l'équipement cible et apportez les modifications suivantes en mode local.
2	Dans le Navigateur de DTM de Control Expert, double-cliquez sur le DTM maître de la CPU M580 (BMEP58_ECPU_EXT) pour afficher sa configuration.
3	Dans l'arborescence de navigation, développez la liste d'équipements afin d'afficher les instances d'esclave local associées.
4	Sélectionnez l'équipement CIP Safety.
5	Sélectionnez l'onglet Paramètres d'adresse .

Configuration des paramètres d'adresse IP de l'équipement de sécurité

Dans l'onglet **Paramètres d'adresse**, modifiez les paramètres suivants de l'équipement de sécurité sélectionné :

Champ	Paramètre	Description
Configuration IP	Adresse IP	Saisissez l'adresse IP de l'équipement sélectionné.
	Masque de sous-réseau	Masque de sous-réseau de l'équipement. NOTE: définissez le masque de sous-réseau de sorte que l'adresse IP de l'équipement appartienne au même sous-réseau que l'adresse IP principale de la CPU source.

Champ	Paramètre	Description
	Passerelle	Adresse de passerelle utilisée pour atteindre cet équipement. La valeur par défaut 0.0.0.0 indique que cet équipement se trouve sur le même sous-réseau que la CPU source.
Serveur d'adresses	DHCP de cet équipement	• Désactivé (par défaut) : désactive le client DHCP dans l'équipement. • Activé : active le client DHCP dans l'équipement.
	Identifié par	Si le service DHCP est activé, sélectionnez le type d'identifiant de l'équipement : • Adresse MAC • Nom de l'équipement
	Identificateur	Si le service DHCP est activé et l'option Nom de l'équipement sélectionnée, indiquez le nom de l'équipement.

Pour plus d'informations sur la configuration des paramètres d'équipement dans le DTM maître de la CPU M580, reportez-vous à la section Paramètres de la liste des équipements (voir Modicon M580, Matériel, Manuel de référence).

Opérations CIP Safety

Présentation

Cette section décrit les opérations CIP Safety.

Transfert d'une application CIP Safety depuis Control Expert vers le PAC

Début du téléchargement de l'application

Lancez le téléchargement à l'aide de la commande **Automate > Transférer le projet vers l'automate**.

Si l'automate contient déjà une application, le fait de télécharger une nouvelle application invalide l'ancienne. Si l'ancienne application inclut des équipements configurés, le PAC ferme les connexions vers ces équipements.

Fin du téléchargement de l'application

La configuration CIP Safety est écrite dans la pile CIP Safety (CSS) de la CPU, laquelle calcule le CRC des paramètres de connexion (CPCRC) pour chaque connexion. Chaque valeur CPCRC calculée par la CSS est alors comparée à la valeur CPCRC correspondante stockée dans la configuration et calculée par le DTM cible. Voici ce qui se produit :

- Si les CPCRC ne correspondent pas, la CSS rejette l'application et le PAC reste à l'état NOCONF.
- Si les CPCRC correspondent :
 - Le CPCRC et les paramètres de connexion sont copiés dans le DDDT cible, page 395 correspondant.
 - Le paramètre CSIO_HEALTH, page 402 du DDDT de la CPU (T_BMEP58_ECPU_EXT) est défini sur 0.
 - Les bits HEALTH du DDDT, page 395 de l'équipement CIP Safety cible sont définis sur 0.
 - Le PAC connecte les équipements configurés via des requêtes SafetyOpen de type 2, page 386.

Si les CPCRC ne correspondent pas, la CSS rejette l'application et le PAC reste à l'état NOCONF.

Nouveau calcul de l'ID de l'application de sécurité

L'ID de l'application de sécurité (SAId) correspond à la signature de la partie sécurisée de l'application Control Expert. Il est stocké dans le mot système %SW169, page 419. La CSS calcule un CRC sur toutes les instances du paramètre CPCRC. Ce CRC est ensuite ajouté au calcul de l'identifiant SAId. Par conséquent, une modification de la configuration cible CIP Safety modifie également la valeur SAId.

Structure d'une requête SafetyOpen de type 2

Structure de trame d'une connexion CIP SafetyOpen de type 2

Les CPU de sécurité M580 autonomes prennent en charge les connexions CIP Safety établies via des requêtes SafetyOpen de type 2. La structure de trame de ce type de requête est décrite ci-dessous :

Nom du paramètre		Description
Multiplicateur de timeout de la connexion		Permet au consommateur d'une connexion de déterminer si l'une des trois connexions standard doit expirer. Formule de calcul de la valeur de timeout d'une connexion : $\text{RPI de la connexion} * (\text{CTM}+1) * 4$
RPI O->T		Intervalle de trame demandé de la connexion O→T
RPI T->O		Intervalle de trame demandé de la connexion T→O
Electronic Key.Vendor ID		Identifiant du fabricant de l'équipement
Electronic Key.Prod Type		Type d'équipement
Electronic Key.Prod Code		Code produit de l'équipement
Electronic Key.Compatible/Major Rev		Révision majeure
Electronic Key.Minor Rev		Révision mineure
SCID	CRC de la configuration de sécurité	Identifiant de la configuration de sécurité : fourni par l'outil de configuration du réseau de sécurité (SNCT), cet identifiant est utilisé lors de la mise en service, de l'établissement de la connexion et du remplacement de l'équipement.
	Date de configuration	
	Heure de configuration	
TUNID	Date de génération du TUNID	Identifiant de réseau cible unique : identifie la cible dans la requête SafetyOpen.
	Heure de génération du TUNID	
	ID du nœud cible	

Nom du paramètre		Description
OUNID	Date de génération du OUNID	Identifiant de réseau source unique : identifie la source dans la requête SafetyOpen.
	Heure de génération du OUNID	
	ID du nœud source	
Ping_Interval_EPI_Multiplier		Intervalle de comptage de ping de la connexion
Time_Coord_Msg_Min_Multiplier		Nombre minimal d'incréments de 128 µS nécessaires pour transmettre un message de coordination horaire du consommateur au producteur
Network_Time_Expectation_Multiplier		Age maximal des données de sécurité autorisé par un consommateur, en incréments de 128 µS
Timeout_Multiplier		Nombre de tentatives de production des données à inclure dans l'équation pour une connexion non détectée
Max_Fault_Number		Nombre de trames en erreur pouvant être abandonnées avant que la connexion soit fermée
CRC des paramètres de connexion (CPCRC)		CRC des paramètres de connexion. Valeur CRC-S32 des paramètres de connexion cible contenus dans la requête SafetyOpen de type 2

Opérations de l'équipement CIP Safety

Introduction

Cette section décrit les opérations de l'équipement CIP Safety, y compris les mécanismes de détection des erreurs système et de réponse, ainsi que les états de fonctionnement de l'équipement :

- auto-contrôle de mise sous tension
- réponse à une erreur détectée non récupérable
- erreur détectée récupérable
- gestion de la validité de la connexion cible
- état Run/Repos de l'équipement CIP Safety

Auto-contrôle de mise sous tension de la source et de la cible

CIP Safety

Lors de la mise sous tension et à chaque chargement d'une nouvelle application, le système CIP Safety exécute les opérations suivantes :

- Le contrôleur transfère les paramètres de configuration vers la pile CIP Safety (CSS) du contrôleur et du coprocesseur.
- La CSS, du contrôleur et du coprocesseur, évalue le CPCRC pour chaque connexion.
- Pour chaque connexion, le système CIP Safety compare le CPCRC téléchargé (calculé par le DTM source) aux CPCRC calculés par le contrôleur et par le coprocesseur.
- La CSS verrouille la configuration source.
- L'application lance des requêtes SafetyOpen de type 2 pour connecter chaque équipement CIP Safety.
- Chaque équipement CIP Safety :
 - calcule son CPCRC et le compare à celui provenant de la source ;
 - compare l'identifiant SCID à celui stocké en interne (contrôle réservé aux équipements configurables).

Les échanges d'E/S entre les équipements source et cible démarrent seulement si tous ces tests sont concluants.

NOTE: en plus des auto-tests de mise sous tension ci-dessus, le système réalise les auto-tests d'exécution exigés par la norme CIP Safety IEC 61784-3.

Réponse à une erreur détectée non récupérable

Si les diagnostics du contrôleur ou des E/S détectent une erreur non récupérable, le système de sécurité place la partie concernée du système dans un état sécurisé défini. Cette partie est alors arrêtée et mise hors tension, et les entrées de sécurité sont réglées sur 0. Les sorties de sécurité concernées passent dans l'état de repli configuré.

Réponse à une erreur détectée récupérable

En général, les erreurs détectées récupérables concernent des événements, comme la perte de connexion d'un module. Elles sont signalées dans le bit de validité du DDDT de l'équipement (T_CIP_SAFETY_IO, page 395), lequel contient la valeur ET logique des bits de validité Status_IN et Status_OUT. En cas de détection d'une erreur récupérable sur une entrée, la valeur de l'entrée est forcée sur l'état sécurisé défini et réglée sur 0.

Gestion de la validité de la connexion cible

La validité de la connexion à la cible CIP Safety est signalée dans le bit de validité des paramètres Status_IN et Status_OUT, tel que décrit pour le type de données T_CIP_SAFETY_STATUS, page 396. La cible peut être ouverte et opérationnelle, ou une erreur peut être détectée.

Pour les entrées, l'état de connexion est fourni par le valideur de sécurité côté serveur. Pour les sorties, il provient du valideur de sécurité côté client.

Run/Repos

L'état de fonctionnement de l'équipement CIP Safety (Run ou Repos) est signalé dans le bit Run_Idle du paramètre Status_IN ou Status_OUT, tel que décrit pour le type de données T_CIP_SAFETY_STATUS, page 396.

Pour un équipement d'entrée :

Lors de la connexion d'un module d'entrée, le producteur (l'entrée) fait passer le bit Run_Idle à l'état Repos (0) jusqu'à ce que la coordination horaire initiale ait été exécutée. Ensuite, ce bit prend la valeur 1 (état Run) ou 0 (état Repos). Si le bit Run_Idle est à 0 (état Repos), les valeurs des données d'entrée sont forcées sur 0 (état sécurisé défini).

Pour un équipement de sortie :

La source (le contrôleur) règle le bit Run_Idle des sorties sur 1 lorsque le contrôleur passe à l'état Run et que la coordination horaire initiale a été exécutée. Elle règle ce même bit sur 0 lorsque le contrôleur passe à l'état Stop ou Repos, en cas d'échec de la coordination horaire initiale ou suite à la fermeture de la connexion. Si le bit Run_Idle est réglé sur 0 (état Repos), l'équipement de sortie doit appliquer l'état de repli approprié à ses sorties.

Interactions entre les opérations du contrôleur de sécurité et la connexion cible

Introduction

Cette section décrit les interactions entre les opérations/états du contrôleur de sécurité source et la connexion de l'équipement cible :

- temps de réaction système
- état RUN
- état Stop/Halt
- Réinitialisation / redémarrage

- commande Initialiser SAFE
- Mode Maintenance
- CCOTF
- Connexion/déconnexion/remplacement d'un équipement

System Reaction Time (temps de réaction système)

Le temps consommé par la communication CIP Safety (*temps réseau attendu*) est ajouté au *temps de réaction du système* de sécurité M580. Pour plus d'informations, reportez-vous à la rubrique *Incidence des communications CIP Safety sur le temps de réaction du système de sécurité*.

Etat Run

Lorsque le système CIP Safety est à l'état Run :

- Les bits de validité du DDDT, page 395 de communication de l'équipement CIP Safety sont mis à jour en début de cycle de la tâche SAFE.
- Les valeurs d'entrée sont mises à jour en début de cycle de la tâche SAFE, en fonction de la dernière valeur reçue.
- Les valeurs de sortie sont mises à jour et transmises une fois la tâche SAFE exécutée.
- Le bit Run_Idle des sorties est réglé sur 1 dans le DDDT de communication de l'équipement CIP Safety.
- Les bits de validité du DDDT de communication de l'équipement CIP Safety sont mis à jour.

Etat Stop

Lorsque la tâche SAFE passe à l'état Stop (tâche arrêtée ou point d'arrêt atteint) :

- La connexion Source->Cible reste ouverte.
- Les échanges de données entre le contrôleur et l'équipement CIP Safety démarrent.
- Les bits de validité du DDDT, page 395 de communication de l'équipement CIP Safety sont mis à jour.
- Le bit Run_Idle des sorties est réglé sur 0 dans le DDDT de communication de l'équipement CIP Safety et les équipements de sortie passent dans l'état de repli configuré.

Etat Halt

A l'état Halt, les valeurs de sortie ne sont pas envoyées du contrôleur vers l'équipement CIP Safety et les bits de validité de l'équipement sont réglés sur 0.

Redémarrage ou réinitialisation

En cas de redémarrage ou de réinitialisation :

- La partie sécurisée de l'application exécute un démarrage à froid, page 282.
- Le contrôleur exécute la même séquence d'opérations que pour un téléchargement d'application, page 385.

Commande Initialiser SAFE

La commande **Automate > Initialiser SAFE** de Control Expert permet d'initialiser les valeurs du DDDT, page 395 de communication de l'équipement CIP Safety, en rétablissant leurs valeurs d'usine par défaut.

Mode Maintenance

L'activation du mode Maintenance, page 269 du contrôleur de sécurité M580 n'a pas d'incidence sur les opérations de l'équipement CIP Safety. Le contrôleur continue de comparer les calculs qu'elle et le coprocesseur réalisent séparément. En revanche, aucune autre comparaison n'est faite avec les valeurs du DDDT cible. C'est pourquoi un contrôleur fonctionnant en mode Maintenance n'est pas considéré comme sécurisé.

CCOTF

Les équipements CIP Safety ne prennent pas en charge la fonction Modifier la configuration en temps réel (CCOTF). Comme leurs paramètres de configuration proviennent non pas du contrôleur source, mais d'un outil de configuration du réseau de sécurité (SNCT) fourni par le fabricant, il est impossible de modifier ces paramètres depuis le contrôleur.

Connexion/déconnexion/remplacement d'un équipement CIP Safety

Lors du démarrage d'une application ou de l'exécution d'une commande **Automate > Initialiser SAFE**, les bits CTRL_IN et CTRL_OUT du DDDT, page 395 sont activés (1) par

défaut. Si un équipement est connecté à un contrôleur en mode Stop ou Run et si son bit CTRL_IN ou CTRL_OUT est activé (1), les échanges de données démarrent automatiquement.

NOTE: Un redémarrage active les bits CTRL_IN et CTRL_OUT. Aussi, veuillez à prendre les mesures nécessaires dans l'application de tâche SAFE pour éviter toute opération involontaire lors d'un redémarrage.

▲ AVERTISSEMENT

FONCTIONNEMENT INATTENDU DE L'ÉQUIPEMENT

N'utilisez pas les bits CTRL_IN ou CTRL_OUT comme mesure de sécurité pour faire passer les données cibles à l'état sécurisé défini.

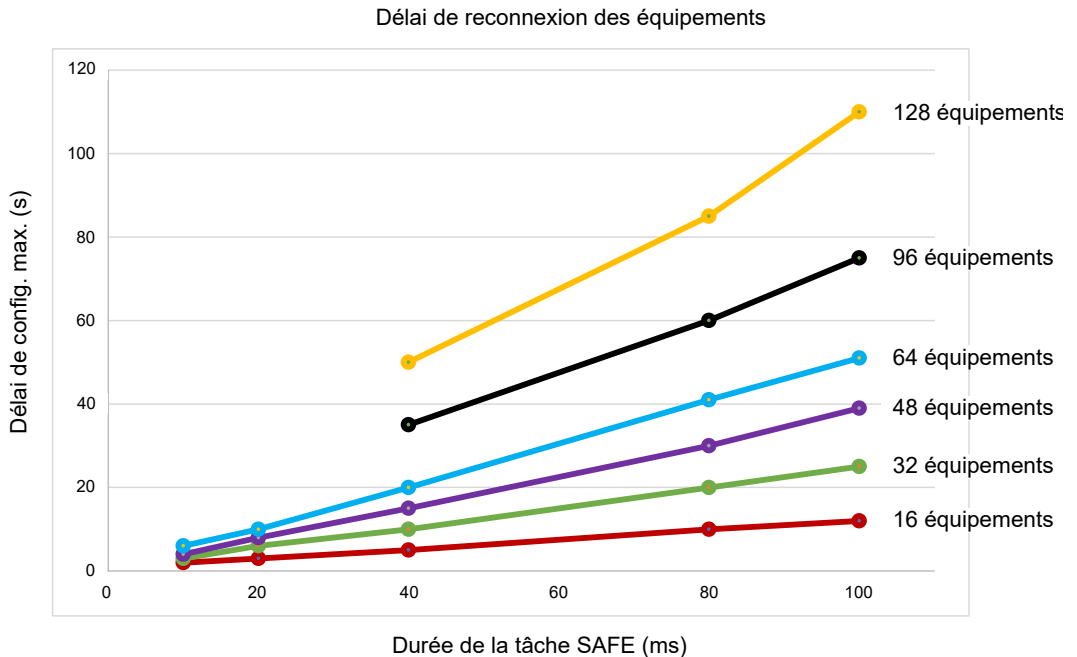
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Lorsque le contrôleur détecte une erreur nécessitant l'arrêt de la connexion d'un équipement, il désactive (met à 0) le bit CTRL_IN ou CTRL_OUT correspondant. L'équipement reste à l'état désactivé jusqu'à ce qu'il repasse à 1 (par exemple, lorsque l'erreur est résolue et qu'une requête de réouverture de connexion est exécutée).

Pour exécuter une requête de réouverture de connexion, réactivez le bit de contrôle correspondant (CTRL_IN ou CTRL_OUT) en le réglant à nouveau sur 1 dans le DDDT.

Lorsque vous reconnectez un équipement, le délai de connexion varie en fonction de la durée de la tâche SAFE et du nombre d'équipements connectés :

- Pour un équipement avec une durée de tâche SAFE inférieure à 100 ms, le délai de reconnexion estimé est inférieur à 2 secondes.
- Pour plusieurs équipements, reportez-vous au graphique des délais de reconnexion estimés.



Pour le contrôleur CIP Safety, un remplacement d'équipement équivaut à une opération de déconnexion/reconnexion. Le nouvel équipement est reconfiguré en local avec les mêmes paramètres que l'équipement d'origine (le contrôleur n'intervient pas dans cette procédure).

Commandes du DTM CIP Safety

Introduction

Le DTM CIP Safety est associé à l'onglet **Safety**, qui contient les commandes suivantes :

- **REINITIALISER la propriété**
- **placer TUNID**

Ces commandes sont accessibles après avoir sélectionné une connexion dans l'arborescence de navigation du DTM. Elles sont activées lorsque le DTM est connecté à l'équipement CIP Safety et fonctionnent en mode connecté.

REINITIALISER la propriété

La commande **REINITIALISER la propriété** permet de rétablir les valeurs par défaut (définies en usine) des paramètres de configuration de l'équipement CIP Safety. Les conditions suivantes doivent être remplies pour pouvoir réinitialiser ces paramètres :

- La commande émane de la CPU source identifiée par l'OUNID stocké dans l'équipement.
- Les paramètres de configuration du module ne sont pas verrouillés.

Une fois réinitialisé, le module n'a plus de propriétaire et peut donc être configuré par une autre source.

NOTE: la commande de réinitialisation ne s'applique pas si des connexions sont actives sur le module.

placer TUNID

La commande **placer TUNID** permet de définir le numéro du réseau de sécurité (SNN) dans l'équipement CIP Safety cible. Lors de son exécution, le numéro du réseau de sécurité, page 375 stocké dans la configuration du DTM de l'équipement CIP Safety est transféré à l'équipement cible et remplace la valeur SNN éventuellement présente dans l'équipement.

NOTE: avant d'exécuter cette commande, assurez-vous d'avoir identifié correctement l'équipement vers lequel vous souhaitez transférer le SNN.

Diagnostic CIP Safety

Présentation

Cette section présente les outils de diagnostic disponibles pour l'équipement CIP Safety et la connexion CIP Safety entre cet équipement et la CPU de sécurité M580 autonome.

DDDT de l'équipement CIP Safety

T_CIP_SAFETY_IO DDDT

Le DDDT T_CIP_SAFETY_IO décrit chaque instance d'équipement CIP Safety et contient les paramètres suivants :

Paramètre	Type de données	Description
Health	BOOL	Validité globale = ET logique entre : - Status_IN.Health - Status_OUT.Health Pour obtenir une description de ces bits de validité, reportez-vous au type de données T_CIP_SAFETY_STATUS, page 396.
Status_IN	T_CIP_SAFETY_STATUS	Etat de l'entrée
Status_OUT	T_CIP_SAFETY_STATUS	Etat de la sortie
CTRL_IN	BOOL	Activer/désactiver la connexion d'entrée
CTRL_OUT	BOOL	Activer/désactiver la connexion de sortie
Conf_In	T_CIP_SAFETY_CONF	Signatures et paramètres CIP de la connexion d'entrée
Conf_Out	T_CIP_SAFETY_CONF	Signatures et paramètres CIP de la connexion de sortie
Input	Array[0...n] of BYTE	Valeurs d'entrée (taille variable en fonction du type d'équipement). 4 octets du module alignés sur la taille configurée dans le DTM.
Output	Array[0...m] of BYTE	Valeurs de sortie (taille variable en fonction du type d'équipement). 4 octets du module alignés sur la taille configurée dans le DTM.

Les types de données CIP Safety mentionnés ci-dessus sont décrits ci-après.

T_CIP_SAFETY_STATUS

Paramètres du type de données T_CIP_SAFETY_STATUS :

Paramètre	Type de données	Description
Health	BOOL	Validité de l'entrée ou de la sortie : • Entrée : ◦ 1 : communication d'entrée ouverte et opérationnelle ◦ 0 : erreur de communication d'entrée détectée par le valideur de sécurité côté serveur • Sortie : ◦ 1 : communication de sortie ouverte et opérationnelle ◦ 0 : erreur de communication de sortie détectée par le valideur de sécurité côté client
Run_Idle	BOOL	Etat des entrées ou sorties de l'équipement CIP Safety : • Défini par le producteur (entrée) pour les entrées : ◦ 1 : entrée à l'état Run ◦ 0 : entrée au repos ou coordination horaire initiale pas encore exécutée • Défini par la source (CPU) pour les sorties : ◦ 1 : PAC à l'état Run ou coordination horaire initiale exécutée ◦ 0 : PAC à l'état Stop ou Halt, connexion fermée ou échec de la coordination horaire initiale
Error_Code	WORD	Reportez-vous à la liste des codes d'erreur détectée, page 398.
Error_Sub_Code	WORD	Reportez-vous à la liste des sous-codes d'erreur détectée, page 399.

T_CIP_SAFETY_CONF

Le type de données T_CIP_SAFETY_CONF contient les paramètres suivants, qui sont transmis dans la requête SafetyOpen de type 2, page 386 :

Paramètre	Type de données	Description
TO_MULTIPLIER	BYTE	Multiplicateur de timeout. Permet au consommateur d'une connexion de déterminer si l'une des trois connexions standard doit expirer. Formule de calcul de la valeur de timeout d'une connexion : RPI de la connexion * (CTM+1) * 4
Output_RPI	UDINT	Intervalle de trame demandé de la connexion O→T
Input_RPI	UDINT	Intervalle de trame demandé de la connexion T→O
Device_Vendor_ID	UINT	Identifiant du fabricant affecté par l'ODVA
Device_Type	UINT	Groupe ODVA auquel appartient l'équipement
Device_Product_Code	UINT	Code produit affecté par l'ODVA
Major_Revision	BYTE	Révision majeure du micrologiciel de l'équipement
Minor_Revision	BYTE	Révision mineure du micrologiciel de l'équipement
Configuration_Assembly_Nb	UINT	Numéro d'assemblage propre à l'équipement associé aux paramètres de configuration d'équipement
Output_Assembly_Nb	UINT	Numéro d'assemblage propre à l'équipement associé aux transmissions de sortie (O→T)
Input_Assembly_Nb	UINT	Numéro d'assemblage propre à l'équipement associé aux transmissions d'entrée (T→O)
SC_CRC	UDINT	CRC de la configuration de sécurité. Contrôle de redondance cyclique (CRC) de la configuration d'équipement CIP Safety.
Configuration_Date	UINT	Date à laquelle la configuration a été générée (mois, jour et année)
Configuration_Time	UDINT	Heure à laquelle la configuration a été générée (heure, minutes, secondes et millisecondes)
TUNID_Time	UDINT	Date à laquelle l'identifiant de réseau cible unique a été généré (mois, jour et année)
TUNID_Date	UINT	Heure à laquelle l'identifiant de réseau cible unique a été généré (heure, minutes, secondes et millisecondes)
TUNID_NodeID	UDINT	Identifiant de réseau unique de l'équipement cible
OUNID_Time	UDINT	Date à laquelle l'identifiant de réseau source unique a été généré (mois, jour et année)
OUNID_Date	UINT	Heure à laquelle l'identifiant de réseau source unique a été généré (heure, minutes, secondes et millisecondes)
OUNID_NodeID	UDINT	Identifiant de réseau unique de l'équipement source
Ping_Interval_EPI_Multiplier	UINT	Intervalle de comptage de ping de la connexion

Paramètre	Type de données	Description
Time_Coordination_Msg_Min_Mult	UINT	Nombre minimal d'incréments de 128 µS nécessaires pour transmettre un message de coordination horaire du consommateur au producteur
Network_Time_Expectation_Mult	UINT	Age maximal des données de sécurité autorisé par un consommateur, en incréments de 128 µS
Timeout_Multiplier	BYTE	Nombre de tentatives de production des données à inclure dans l'équation pour une connexion non détectée
Max_Fault_Number	UDINT	Nombre de trames en erreur pouvant être abandonnées avant que la connexion soit fermée
CPCRC	UDINT	CRC des paramètres de connexion. Valeur CRC-S32 des paramètres de connexion cible contenus dans la requête SafetyOpen de type 2

Codes d'erreur de l'équipement CIP Safety

Codes d'erreur détectée

Les codes et sous-codes d'erreur détectée suivants concernent le type de données T_CIP_SAFETY_STATUS et figurent dans les paramètres Status_IN et Status_OUT du DDDT de l'équipement CIP Safety.

Codes d'erreur détectée

Code d'erreur détectée	Signification
0001	Connexion ouverte : pas de réponse
0002	Connexion ouverte : réponse à l'erreur détectée de l'équipement
0003	Connexion ouverte : réponse non valide de l'équipement
0004	Serveur (consommateur) inopérant
0005	Client (producteur) inopérant

Sous-codes d'erreur détectée

NOTE: Les sous-codes d'erreur détectée autres que ceux indiqués ci-dessous sont réservés pour un usage interne Schneider Electric. Si vous rencontrez ces sous-codes, signalez-les au support Schneider Electric.

Sous-codes d'erreur détectée pour les connexions ouvertes :

Sous-code d'erreur détectée (hex)	Signification
0100	Connexion utilisée ou Forward_Open en double.
0103	Combinaison de classe de transport et de déclencheur non prise en charge.
0105	Configuration déjà détenue par une autre source.
0106	Sortie déjà détenue par une autre source.
0107	Connexion cible introuvable (Forward_Close).
0108	Paramètre de connexion réseau incorrect
0109	Taille de connexion non valide
0110	Équipement non configuré.
0111	RPI O->T, RPI T->O ou RPI de correction de l'heure non pris en charge.
0113	Aucune instance de valideur de sécurité disponible.
0114	Le paramètre Device_Vendor_ID ou Device_Product_Code indiqué dans la clé électronique ne correspond pas.
0115	Le paramètre Device_Type indiqué dans la clé électronique ne correspond pas.
0116	Le paramètre Major_Revision ou Minor_Revision indiqué dans la clé électronique ne correspond pas.
0117	Chemin d'application créé ou utilisé incorrect
0118	Chemin d'application de configuration incorrect ou incohérent
011 A	Objet cible hors connexion
011B	Intervalle de trame demandé (RPI) plus petit que la durée d'inhibition de production.
011C	Classe de transport non prise en charge.
011D	Déclencheur de production non pris en charge.
011E	Sens non pris en charge.
0123	Type de connexion du réseau cible non valide pour l'émetteur
0124	Type de connexion du réseau de l'émetteur vers le destinataire non valide

Sous-code d'erreur détectée (hex)	Signification
0126	Taille de configuration non valide
0127	Taille de l'émetteur vers le destinataire non valide
0128	Taille du destinataire vers l'émetteur non valide
0129	Chemin d'application de configuration non valide
012 A	Chemin d'application de consommation non valide
012B	Chemin d'application de production non valide
012C	Symbole de configuration inexistant.
012D	Symbole de consommation inexistant.
012E	Symbole de production inexistant.
012F	Combinaison de chemin d'application incohérente
0130	Format de données de consommation incohérent
0131	Format de données de production incohérent
0203	Connexion expirée.
0204	Absence de réponse de la cible suite à une requête non connectée.
0205	Erreur de paramètre détectée dans la requête SafetyOpen.
0207	Accusé de réception de requête non connectée sans réponse.
0315	Type de segment non valide dans le chemin de connexion.
031B	Connexion au module déjà établie.
031C	Aucun code d'état étendu supplémentaire applicable.
031F	Plus de ressources de liaison consommateur configurables par l'utilisateur disponibles dans le module producteur.
0801	Paramètre Ping_Interval_EIP_Multiplier ou Max_Consumer_Number non valide sur liaison multicast.
0802	Taille de connexion de sécurité non valide.
0803	Format de connexion de sécurité non valide.
0804	Paramètres de connexion de correction de l'heure non valides.
0805	Paramètre Ping_interval_EIP_Multiplier non valide
0806	Paramètre Time_Coordination_Msg_Min_Mult non valide
0807	Paramètre Attente_Temps_Réseau_Mult non valide
0808	Paramètre Multiplicateur_Timeout non valide

Sous-code d'erreur détectée (hex)	Signification
0809	Paramètre Nombre_Max_ Consommateurs non valide
080 A	CPCRC non valide
080B	ID de connexion de la correction de l'heure non valide
080C	Différence d'identifiant SCID
080D	Identifiant TUNID non défini
080E	Différence d'identifiant TUNID
080F	Opération de configuration non autorisée.

Sous-codes d'erreur détectée pour le serveur ou le client :

Sous-code d'erreur détectée (hex)	Signification
271D	Message de coordination horaire reçu avec bit Ping_Response non défini.
2730	Message de coordination horaire non reçu dans le délai imparti.
2732	Contrôle du message de coordination horaire : message avec horodatage identique déjà reçu de ce consommateur.
2733	Contrôle du message de coordination horaire erreur de contrôle de la parité détectée.
2734	Contrôle du message de coordination horaire erreur de contrôle Ack_Byte_2 détectée.
2735	Contrôle du message de coordination horaire : message non reçu dans la limite des 5 secondes.
2736	Contrôle du message de coordination horaire : message non reçu dans le même intervalle de ping ou dans l'intervalle suivant.
2738	Contrôle du message de coordination horaire différence de CRC.
2820	Différence de CRC d'horodatage.
2821	Écart d'horodatage égal à 0.
2822	Écart d'horodatage supérieur à la durée de réseau attendue.
2823	Age des données d'un message supérieur au temps réseau attendu.
2824	Age des données d'un message valide supérieur au temps réseau attendu.
2825	Différence de CRC des données réelles.
2826	Différence de CRC des données complémentaires.
282E	Différence de CRC des données réelles (sans fermeture de connexion).

Sous-code d'erreur détectée (hex)	Signification
282F	Différence de CRC des données complémentaires (sans fermeture de connexion).
2832	Expiration du moniteur d'activité du consommateur.

DDDT de la CPU CIP Safety autonome

Ajouts CIP Safety à T_BMEP58_ECPU_EXT

Le DDDT de la CPU de sécurité M580 autonome (T_BMEP58_ECPU_EXT) inclut deux variables CIP Safety :

- CSIO_SCANNER : état du bit de contrôle du scrutateur d'E/S CIP Safety. Ce champ booléen peut être défini sur :
 - 1 : Le service fonctionne normalement.
 - 0 : Le service ne fonctionne pas normalement.

Pour plus d'informations, consultez la liste des entrées du DDDT SERVER_STATUS2paramètres d'entrée (voir Modicon M580 - Manuel de référence du matériel).

- CSIO_HEALTH : validité des équipements CIP Safety connectés. Cette variable est un tableau de 128 valeurs booléennes, où chaque bit indique la validité d'un équipement connecté :
 - 1 : Le service fonctionne normalement.
 - 0 : Le service ne fonctionne pas normalement.

Pour plus d'informations, reportez-vous à la rubrique Modicon M580Modicon M580 .

Diagnostics du DTM du régulateur

Diagnostics via le DTM de contrôleur du M580

Le DTM de contrôleur du M580 propose les services de diagnostic suivants :

- Détection d'équipements
- Validité de la connexion des équipements d'E/S CIP Safety

Détection des équipements CIP Safety

Lorsque Control Expert fonctionne en mode connecté, vous pouvez utiliser le service de détection de bus de terrain pour détecter les équipements CIP Safety de premier niveau sur votre réseau, c'est-à-dire ceux qui sont directement reliés au contrôleur. Vous ne pouvez détecter que les équipements dont le DTM correspond à celui enregistré dans le **Catalogue de DTM** du PC hôte.

Pour détecter des équipements, cliquez avec le bouton droit de la souris sur le DTM du contrôleur (BMEP58_ECPU_EXT) dans le **Navigateur de DTM**, puis sélectionnez l'option **Découverte de bus de terrain**. Une boîte de dialogue du même nom s'affiche et présente les équipements détectés. Vous pouvez ajouter des DTM d'équipement à votre projet à l'aide des outils disponibles dans cette boîte de dialogue. Les équipements ajoutés apparaissent sous le contrôleur dans le **Navigateur de DTM** et dans l'arborescence de navigation du DTM du contrôleur.

Pour plus d'informations sur l'utilisation de ce service, reportez-vous à la rubrique Service de découverte de bus de terrain (voir la rubrique EcoStruxure™ Control Expert, Modes de fonctionnement)..

État de connexion de l'équipement CIP Safety

Lorsque Control Expert fonctionne en mode connecté, l'arborescence de navigation du DTM du contrôleur contient une icône indiquant la validité de chaque connexion pour les équipements d'E/S CIP Safety ajoutés au projet :

-  : connexion à l'état RUN.
-  : connexion à l'état STOP, non connecté ou indéterminable.

Pour plus d'informations sur l'utilisation de cette fonctionnalité, reportez-vous à la rubrique Présentation des diagnostics dans le DTM de Control Expert (voir Matériel Modicon M580, Manuel de référence).

Diagnostics de connexion de l'équipement CIP Safety

Introduction

Les nœuds de connexion d'un DTM CIP Safety sont associés à deux onglets qui permettent d'identifier et de diagnostiquer la connexion de l'équipement :

- infos du module
- infos d'état

Onglet Infos du module

L'onglet **Infos du module** du DTM CIP Safety contient les valeurs statiques des paramètres d'identification du module suivants :

- ID du fournisseur
- type de produit,
- code produit
- révision du logiciel
- numéro de série
- nom du produit
- adresse MAC

Onglet Infos d'état

L'onglet **Infos d'état** du DTM CIP Safety contient des valeurs dynamiques concernant la connexion de la CPU à l'équipement CIP Safety :

État	Description
État CIP Safety	État actuel de l'équipement, tel que défini à la section 5-4.2.1.5 de la norme CIP Safety : • 0 : non défini • 1 : auto-test • 2 : inactif • 3 : exception d'auto-test • 4 : exécution • 5 : abandon • 6 : erreur critique • 7 : configuration • 8 : en attente de l'identifiant TUNID • 9...50 : réservé • 51 : en attente de l'identifiant TUNID avec couple autorisé Voir REMARQUE • 52 : exécution avec couple autorisé Voir REMARQUE • 53...99 : propre à l'équipement • 100...255 : propre au fabricant NOTE: Autorisé et défini uniquement dans les profils d'équipement de mouvement de sécurité : 0x2E et 0x2F
État d'exception	Attribut d'un octet indiquant l'état des alarmes et erreurs pour l'équipement, fourni de façon standard ou étendue. Pour plus d'informations, reportez-vous à la section 5-4.2.1.6 relative à l'état d'exception de la norme CIP Safety.

État	Description
Défaut majeur	Condition propre à l'équipement. Pour plus d'informations, consultez le manuel de l'équipement.
Défaillance mineure.	Condition propre à l'équipement. Pour plus d'informations, consultez le manuel de l'équipement.
Adresse IP	Adresse IP de l'équipement CIP Safety, définie dans le champ M580 DTM du contrôleur, page 383.
TUNID	Identifiant de réseau cible unique.
OUNID	Identifiant de réseau source unique, page 365.
État de verrouillage	État de la configuration de l'équipement, tel que défini par un outil de configuration du réseau de sécurité (SNCT) : • Verrouillé : configuration en lecture seule • Déverrouillé : configuration en lecture/écriture
Signature de la configuration	Identifiant de configuration de sécurité de la connexion de l'équipement cible (SCID, page 376).

Annexes

Contenu de cette partie

CEI 61508	408
Objets système	416
Références SRAC	423

Présentation

Les annexes contiennent des informations sur la norme IEC 61508 et le modèle SIL. Ils fournissent également les données techniques des modules de sécurité et non perturbateurs ainsi que des exemples de calcul.

CEI 61508

Contenu de ce chapitre

Informations générales relatives à la norme IEC 61508..... 409
Stratégie SIL 411

Présentation

Cette section fournit des informations sur les concepts de sécurité de la norme IEC 61508 en général, et du modèle SIL en particulier.

Informations générales relatives à la norme IEC 61508

Présentation

Les systèmes liés à la sécurité sont conçus pour être utilisés dans des processus où il est nécessaire de protéger les personnes, l'environnement, l'équipement et la production en maintenant les risques à des niveaux acceptables. Les risques sont définis selon leur gravité et leur probabilité, ce qui permet de définir les mesures de protection nécessaires.

Concernant les processus de sécurité, 2 aspects sont à prendre en compte :

- réglementations et exigences définies par les organismes officiels afin de faciliter la protection des personnes, de l'environnement, de l'équipement et de la production
- mesures par lesquelles sont appliquées ces réglementations et ces exigences

Description de la norme IEC 61508

La norme technique qui définit les exigences des systèmes liés à la sécurité est

- the IEC 61508.

Elle concerne la sécurité fonctionnelle des systèmes électriques, électroniques ou programmables liés à la sécurité. Un système lié à la sécurité est un système qui doit exécuter une ou plusieurs fonctions spécifiques pour assurer le maintien des risques à un niveau acceptable. Ces fonctions sont appelées fonctions de sécurité. Un système est défini comme étant fonctionnellement sécurisé si des défaillances de causes communes, systématiques et aléatoires n'entraînent pas un dysfonctionnement, des blessures ou la mort de personnes, des émissions atmosphériques et la perte de matériel ou de production :

La norme définit une approche générique pour toutes les activités du cycle de vie pour les systèmes utilisés pour exécuter les fonctions de sécurité. Elle établit des procédures à appliquer à la conception, le développement et la validation du matériel et des logiciels dans le cadre des systèmes liés à la sécurité. Elle détermine également les règles relatives à la gestion de la sécurité fonctionnelle et la documentation.

Description de la norme IEC 61511

Les exigences de la sécurité fonctionnelle définies dans la norme IEC 61508 sont renforcées pour les processus industriels dans la norme technique suivante :

- IEC 61511 : Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le domaine de la production par processus

Cette norme guide l'utilisateur durant les activités liées à l'application du système de sécurité, dans chacune des phases (notamment : projet, démarrage, modifications et mise hors service). En résumé, elle couvre le cycle de vie de la sécurité de tous les composants d'un système lié à la sécurité utilisé dans le secteur de l'industrie des processus.

Description des risques

La norme IEC 61508 est fondée sur les concepts de l'analyse des risques et la fonction de sécurité. Les risques sont définis par un niveau de gravité et une probabilité. Ils peuvent être réduits à un niveau tolérable en appliquant une fonction de sécurité qui est constituée d'un système électrique, électronique ou programmable. Ils doivent également être réduits à un niveau qui est aussi faible que raisonnablement réalisable.

En résumé, les risques dans la norme IEC 61508 sont définis comme suit :

- Le risque zéro ne peut jamais pas être atteint.
- La sécurité doit être considérée dès le départ.
- Les risques intolérables doivent être réduits.

Stratégie SIL

Introduction

La valeur SIL permet d'évaluer la robustesse d'une application contre les défaillances, ce qui indique la capacité d'un système à réaliser une fonction de sécurité avec une probabilité définie. La norme IEC 61508 définit quatre niveaux de performances de la sécurité en fonction des risques ou des impacts engendrés par le processus pour lequel est utilisé le système lié à la sécurité. Plus les impacts possibles sont dangereux sur la communauté et l'environnement, plus les exigences de la sécurité doivent être élevées pour réduire les risques.

Description de la valeur SIL

Le niveau TOR (1 sortie sur 4 possibles) permet de définir les exigences d'intégrité de la sécurité des fonctions de sécurité à allouer aux systèmes de sécurité, où le niveau 4 correspond au plus haut niveau d'intégrité de la sécurité et le niveau 1 au plus faible niveau d'intégrité de la sécurité. Reportez-vous à la rubrique Niveaux SIL en faible demande.

Description des exigences SIL

Pour atteindre la sécurité fonctionnelle, deux types d'exigences sont requis :

- Exigences des fonctions de sécurité, qui définissent les fonctions de sécurité à réaliser
- Les exigences de l'intégrité de la sécurité, qui définissent le degré de certitude nécessaire pour réaliser les fonctions de sécurité

Les exigences des fonctions de sécurité sont issues de l'analyse des risques, et les exigences de l'intégrité de la sécurité de l'évaluation des risques.

Les risques sont quantifiés comme suit :

- délai moyen entre les défaillances
- probabilités de défaillance
- taux de défaillance
- Couverture du diagnostic
- Acronyme de « safe failure fraction ». Proportion de défaillances en sécurité.
- Acronyme de « hardware fault tolerance ». Tolérance aux anomalies matérielles.

Selon le niveau d'intégrité de la sécurité, ces valeurs doivent être comprises dans des seuils définis.

NOTE: La combinaison d'équipements associés à différents niveaux d'intégrité de la sécurité sur un réseau ou pour une fonction de sécurité nécessite d'extrêmes précautions, conformément à la norme IEC 61508, et a des répercussions sur la conception et l'exploitation.

Description des niveaux SIL

Comme défini dans la section IEC 61508, la valeur SIL est limitée par le taux de défaillances non dangereuses (SFF) et la tolérance aux défauts matériels (HFT) du sous-système qui exécute la fonction de sécurité. Si la valeur de HFT est n , les défaillances $n+1$ peuvent entraîner la perte de la fonction de sécurité, l'état sécurisé défini ne peut pas être atteint. La valeur SFF dépend du taux de défaillance et de la couverture du diagnostic.

Le tableau ci-dessous montre la relation entre les valeurs SFF, HFT et SIL pour les sous-systèmes de sécurité complexes selon la norme IEC 61508-2, dans laquelle les modes de défaillance de tous les composants ne peuvent pas être totalement définis :

SFF (taux de défaillances non dangereuses)	HFT = 0	HFT = 1	HFT = 2
$SFF \leq 60 \%$	-	SIL1	SIL2
$60 \% < SFF \leq 90 \%$	SIL1	SIL2	SIL3
$90 \% < SFF \leq 99 \%$	SIL2	SIL3	SIL4
$SFF > 99 \%$	SIL3	SIL4	SIL4

Un certain niveau d'intégrité peut être atteint de deux manières :

- augmentation de la valeur HFT (Tolérance aux défauts matériels) en fournissant des procédures d'arrêt indépendantes supplémentaires
- augmentation de la valeur SFF (taux de défaillances non dangereuses) au moyen de diagnostics supplémentaires

Description de la relation entre niveaux SIL et demande

Le IEC 61508 fait la distinction entre le mode à faible demande et le mode de fonctionnement à forte demande (ou continu).

En mode de faible demande, la fréquence de la demande de fonctionnement sur un système lié à la sécurité n'est pas supérieure à 1 par an et n'est pas supérieure à deux fois la fréquence du test périodique. La valeur SIL d'un système lié à la sécurité en faible demande est directement liée à la probabilité moyenne de défaillance du système dans l'exécution de la fonction de sécurité sur demande, ou simplement à la probabilité de défaillance sur demande (PFD).

En mode de forte demande (ou mode continu), la fréquence de la demande de fonctionnement sur un système lié à la sécurité est supérieure à un par an et supérieure à deux fois la fréquence du test périodique. La valeur SIL d'un système lié à la sécurité en forte demande est directement liée à la probabilité moyenne de défaillance dangereuse du système par heure, ou simplement à la probabilité de défaillance par heure (PFH).

Niveaux SIL en faible demande

Le tableau ci-dessous répertorie les exigences d'un système dans le mode de fonctionnement en faible demande :

Niveau d'intégrité de la sécurité	Probabilité de défaillance à la demande
4	$\geq 10^{-5}$ à $< 10^{-4}$
3	$\geq 10^{-4}$ à $< 10^{-3}$
2	$\geq 10^{-3}$ à $< 10^{-2}$
1	$\geq 10^{-2}$ à $< 10^{-1}$

Niveaux SIL en forte demande

Le tableau ci-dessous répertorie les exigences d'un système dans le mode de fonctionnement en forte demande :

Niveau d'intégrité de la sécurité	Probabilité de défaillance par heure (PFH)
4	$\geq 10^{-9}$ à $< 10^{-8}$
3	$\geq 10^{-8}$ à $< 10^{-7}$
2	$\geq 10^{-7}$ à $< 10^{-6}$
1	$\geq 10^{-6}$ à $< 10^{-5}$

Pour SIL3, les probabilités de défaillance requises pour un système à sécurité intégré :

- PFD $\geq 10^{-4}$ à $< 10^{-3}$ pour une faible demande
- PFH $\geq 10^{-8}$ à $< 10^{-7}$ pour une forte demande

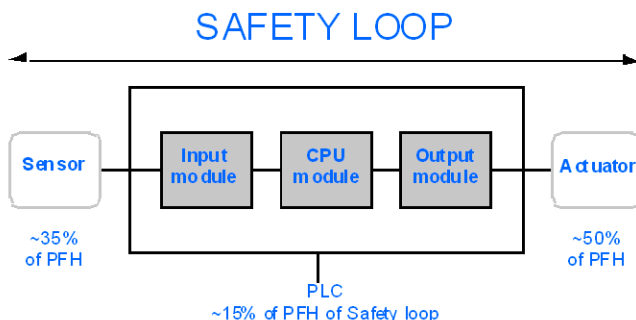
Description de la boucle de sécurité

La boucle de sécurité à laquelle le contrôleur de sécurité M580 appartient se compose des 3 parties suivantes :

- Capteurs
- Contrôleur de sécurité M580 avec alimentation, CPU de sécurité, contrôleur de sécurité et modules d'E/S de sécurité
- Actionneurs

Une embase ou une connexion distante incluant un commutateur ou un CRA ne détruit pas une boucle de sécurité. Les embases, les commutateurs et les modules CRA font partie du « canal noir ». Cela signifie que les données échangées par les E/S et le contrôleur ne peuvent pas être corrompues sans que le récepteur ne le détecte.

L'illustration suivante représente une boucle de sécurité classique :



Comme le montre la figure ci-dessus, la contribution du contrôleur n'est que de 10 à 20 % car la probabilité de défaillance des capteurs et des actionneurs est assez élevée en général.

L'hypothèse prudente de 10 % pour la contribution du contrôleur de sécurité à la probabilité totale laisse davantage de marge à l'utilisateur et aboutit aux probabilités requises ci-dessous pour le contrôleur de sécurité :

- $PFD \geq 10^{-5}$ à $< 10^{-4}$ pour une faible demande
- $PFH \geq 10^{-9}$ à $< 10^{-8}$ pour une forte demande

Description de l'équation PFD

La norme IEC 61508 suppose que la moitié des défaillances se terminent dans un état sécurisé défini. Par conséquent, le taux de défaillance λ est composé de :

- λ_S : défaillance en sécurité
- λ_D : défaillance dangereuse, elle-même composée de
 - λ_{DD} : défaillance dangereuse détectée par le diagnostic interne
 - λ_{DU} : défaillance dangereuse non détectée.

Le taux de défaillance peut être calculé à partir du délai moyen entre les défaillances (MTBF), une valeur spécifique au module, comme suit :

$$\lambda = 1/\text{MTBF}$$

L'équation de calcul de la probabilité de défaillance sur demande (PFD) est la suivante :

$$\text{PFD}(t) = \lambda_{\text{DU}} \times t$$

t représente le temps entre deux tests périodiques.

La probabilité de défaillance par heure implique un intervalle de temps de une heure. Par conséquent, l'équation PFD est réduite à la suivante :

$$\text{PFH} = \lambda_{\text{DU}}$$

Objets système

Contenu de ce chapitre

M580 - Bits système de sécurité..... 417
Mots système de sécurité du système M580 419

Présentation

Ce chapitre décrit les mots et les bits système de l'automate de sécurité M580.

NOTE: les symboles associés à chaque objet bit ou mot système mentionné dans les tableaux descriptifs de ces objets ne sont pas implémentés en standard dans le logiciel, mais ils peuvent être saisis à l'aide de l'éditeur de données.

M580 - Bits système de sécurité

Bits système pour l'exécution de la tâche SAFE

Les bits système suivants s'appliquent à l'automate de sécurité M580. Vous trouvez la description des bits système de l'automate de sécurité M580 et des autres automates M580 dans la présentation des *Bits système* dans le document *EcoStruxure™ Control Expert - Bits et mots système - Manuel de référence*.

Ces bits système sont liés à l'exécution de la tâche SAFE, mais ils ne sont pas directement accessibles dans le code du programme de sécurité. Ils sont accessibles uniquement via les blocs `S_SYST_READ_TASK_BIT_MX` et `S_SYST_RESET_TASK_BIT_MX`.

Bit Symbole	Fonction	Description	Etat initial	Type
%S17 CARRY	Sortie décalage circulaire	Lors d'une opération de décalage circulaire dans la tâche SAFE, ce bit prend l'état du bit sortant.	0	R/W
%S18 OVERFLOW	Détection de dépassement ou d'erreur arithmétique	Normalement à l'état 0, ce bit est réglé sur 1 en cas de dépassement de capacité dans les cas suivants : • Résultat supérieur à +32 767 ou inférieur à -32 768, en simple longueur • Résultat supérieur à +65 535, en entier non signé • Résultat supérieur à +2 147 483 647 ou inférieur à -2 147 483 648, en double longueur • Résultat supérieur à +4 294 967 296, en double longueur ou en entier non signé. • Division par 0. • Racine d'un nombre négatif. • Forçage à un pas inexistant sur un programmeur cyclique. • Empilage d'un registre plein, dépilage d'un registre vide.	0	R/W
%S21 1RSTTASKRUN	Première scrutation de tâche SAFE en mode RUN	Testé dans la tâche SAFE, ce bit indique le premier cycle de cette tâche. Il est mis à 1 en début de cycle et remis à 0 en fin de cycle. NOTE: • Le premier cycle de l'état de la tâche peut être lu en utilisant la sortie <code>SCOLD</code> du bloc fonction système <code>S_SYST_STAT_MX</code>. • Ceci ne concerne pas les systèmes redondants de sécurité M580.	0	R/W

Remarques concernant les bits système non liés à la sécurité

Bit système	Description	Remarques
%S0	Démarrage à froid	N'est utilisable que dans les tâches de processus (autres que SAFE) et n'a aucune influence sur la tâche SAFE.
%S9	Sorties réglées en mode de repli	N'a aucune influence sur les modules de sortie de sécurité.
%S10	Erreur détectée d'E/S globales	Signale certaines (mais pas l'ensemble) des erreurs détectées possibles liées aux modules d'E/S de sécurité.
%S11	Débordement du chien de garde	Prend en compte un dépassement sur la tâche SAFE.
%S16	Erreur détectée d'E/S de tâche	Signale certaines (mais pas l'ensemble) des erreurs détectées possibles liées aux modules d'E/S de sécurité.
%S19	Dépassement période de tâche	Des informations sur le dépassement de la tâche SAFE ne sont pas disponibles.
%S40 à %S47	Erreur détectée d'E/S du rack n	Signale certaines (mais pas l'ensemble) des erreurs détectées possibles liées aux modules d'E/S de sécurité.
%S78	STOP en cas d'erreur détectée	S'applique aux tâches de processus et à la tâche SAFE. Si ce bit est défini, par exemple si une erreur de débordement de %S18 survient, la tâche SAFE prend l'état HALT.
%S94	Enregistre les valeurs réglées	Ne s'applique pas aux variables de SAFE. L'activation de ce bit ne modifie pas les valeurs initiales de SAFE.
%S117	Erreur d'E/S distantes sur le réseau d'E/S Ethernet	Signale certaines (mais pas l'ensemble) des erreurs détectées possibles liées aux modules d'E/S de sécurité.
%S119	erreur détectée générale dans le rack	Signale certaines (mais pas l'ensemble) des erreurs détectées possibles liées aux modules d'E/S de sécurité.

Mots système de sécurité du système M580

Mots système pour les contrôleurs de sécurité M580

Les mots système suivants s'appliquent au contrôleur de sécurité M580. Vous trouvez la description des mots système du contrôleur de sécurité M580 et des autres contrôleurs M580 dans la présentation des *mots système* dans le document *EcoStruxure™ Control Expert - Mot et mots système - Manuel de référence*.

Ces mots système et valeurs sont liés à la tâche SAFE. Ils sont accessibles dans le code du programme d'application, dans les sections autres que les sections de sécurité (MAST, FAST, AUX0 ou AUX1), mais pas dans le code de la section de la tâche SAFE.

Mot	Fonction	Type
%SW4	Période de la tâche SAFE définie dans la configuration. La période n'est pas modifiable par l'opérateur.	L
%SW12	Indique le mode de fonctionnement du module coprocesseur : 16#A501 = mode de maintenance 16#5AFE = mode de sécurité Toute autre valeur est interprétée comme une erreur.	R
%SW13	Indique le mode de fonctionnement du contrôleur : 16#501A = mode de maintenance 16#5AFE = mode de sécurité Toute autre valeur est interprétée comme une erreur.	R
%SW42	Temps en cours de la tâche SAFE. Indique le temps d'exécution du dernier cycle de la tâche SAFE (en ms)	R
%SW43	Temps maximal de la tâche SAFE. Indique le temps d'exécution le plus long de la tâche SAFE depuis le dernier démarrage à froid (en ms)	R
%SW44	Temps minimal de la tâche SAFE. Indique le temps d'exécution le plus court de la tâche SAFE depuis le dernier démarrage à froid (en ms)	R
%SW110	Pourcentage de la charge du contrôleur système utilisé par le système pour les services internes.	R
%SW111	Pourcentage de la charge du contrôleur système utilisé par la tâche MAST.	R
%SW112	Pourcentage de la charge du contrôleur système utilisé par la tâche FAST.	R
%SW113	Pourcentage de la charge du contrôleur système utilisé par la tâche SAFE.	R
%SW114	Pourcentage de la charge du contrôleur système utilisé par la tâche AUX0.	R
%SW115	Pourcentage de la charge du contrôleur système utilisé par la tâche AUX1.	R
%SW116	Charge totale du contrôleur système.	R

Mot	Fonction	Type
%SW124	Contient la cause de l'erreur non récupérable détectée lorsque le contrôleur de sécurité M580 est à l'état HALT : 0x5AF2 : Erreur RAM détectée dans la vérification de mémoire. 0x5AFB : Erreur détectée dans le code du micrologiciel de sécurité 0x5AF6 : Erreur de débordement de chien de garde de sécurité détectée sur le contrôleur. 0x5AFF : Erreur de débordement de chien de garde de sécurité détectée sur le coprocesseur. 0x5B01 : Coprocesseur non détecté au démarrage. 0x5AC03 : Erreur non récupérable de sécurité CIP détectée par le contrôleur. 0x5AC04 : Erreur non récupérable de sécurité CIP détectée par le coprocesseur. NOTE: La liste ci-dessus n'est pas exhaustive. Pour plus d'informations, consultez le document <i>EcoStruxure™ Control Expert - Bits et mots système - Manuel de référence</i>.	R
%SW125	Contient la cause de l'erreur récupérable détectée dans le contrôleur de sécurité M580 : 0x5AC0 : La configuration de sécurité CIP n'est pas correcte (détectée par le contrôleur). 0x5AC1 : La configuration de sécurité CIP n'est pas correcte (détectée par le coprocesseur). 0x5AF3 : Erreur de comparaison détectée par le contrôleur principal. 0x5AFC : Erreur de comparaison détectée par le coprocesseur. 0x5AFD : Erreur interne détectée par le coprocesseur. 0x5AFE : Erreur de synchronisation détectée entre le contrôleur et le coprocesseur. 0x9690 : Erreur de somme de contrôle du programme d'application détectée. NOTE: La liste ci-dessus n'est pas exhaustive. Pour plus d'informations, consultez le document <i>EcoStruxure™ Control Expert - Bits et mots système - Manuel de référence</i>.	R
%SW126	Ces deux mots système contiennent des informations destinées à un usage interne Schneider Electric pour faciliter l'analyse détaillée des erreurs détectées.	R
%SW127		
%SW128	Avec les contrôleurs dont la version du micrologiciel est égale à 3.10 ou antérieure, forcer la synchronisation horaire entre heure NTP et heure SAFE vers les modules d'E/S sécurisés et la tâche de contrôleur SAFE : - Le changement de valeur de 16#1AE5 à 16#E51A force la synchronisation. Consultez la rubrique <i>Procédure de synchronisation des paramètres temporels NTP</i>, page 187. - Les autres séquences et valeurs ne forcent pas la synchronisation.	L/E
%SW142	Contient la version du micrologiciel du coprocesseur de sécurité dans le BCD à quatre chiffres : par exemple la version du micrologiciel 21.42 correspond à %SW142 = 16#2142.	R
%SW148	Nombre d'erreurs du code correcteur ECC (Error Correcting Code) détectées par le contrôleur.	R

Mot	Fonction	Type
%SW152	Avec les contrôleurs dont la version du micrologiciel est égale à 3.10 ou antérieure, état de l'heure du contrôleur NTP mise à jour par le module de communication Ethernet (par ex. BMENOC0301 ou BMENOC0311) sur l'embase X Bus via la fonction de synchronisation forcée de l'heure en option : 0 : le module de communication Ethernet n'actualise pas l'heure du contrôleur. 1 : L'heure du contrôleur est actualisée par le module de communication Ethernet.	R
%SW169	ID de l'application de sécurité : Contient l'ID de la partie code de sécurité de l'application. Cet ID est automatiquement modifié en cas de modification du code de l'application sécurisée. NOTE: - Si le code sécurisé a été modifié et qu'une commande Générer le projet a été exécutée depuis la dernière commande Régénérer tout (modifiant ainsi l'ID de l'application de sécurité), l'exécution d'une commande Régénérer tout peut de nouveau modifier l'ID de l'application de sécurité. - L'identifiant unique du programme SAFE peut être lu en utilisant la sortie SAID du bloc fonction système S_SYST_STAT_MX.	R
%SW171	Etat des tâches FAST : 0 : Aucune tâche FAST n'existe 1 : Arrêt 2 : Exécution 3 : Point d'arrêt 4 : Pause	R
%SW172	Etat de la tâche SAFE : 0 : Aucune tâche SAFE n'existe 1 : Arrêt 2 : Exécution 3 : Point d'arrêt 4 : Pause	R
%SW173	Etat de la tâche MAST : 0 : Aucune tâche MAST n'existe 1 : Arrêt 2 : Exécution 3 : Point d'arrêt 4 : Pause	R
%SW174	Etat de la tâche AUX0 : 0 : Aucune tâche AUX0 n'existe 1 : Arrêt 2 : Exécution 3 : Point d'arrêt	R

Mot	Fonction	Type
	• 4 : Pause	
%SW175	État de la tâche AUX1 : • 0 : Aucune tâche AUX1 n'existe • 1 : Arrêt • 2 : Exécution • 3 : Point d'arrêt • 4 : Pause	R
%SW176	État de comptage des bits forcés pour les variables SAFE du programme : • s'incrémente chaque fois qu'un bit TOR est forcé. • décrémente chaque fois qu'un bit TOR est déforcé.	R

Références SRAC

Le plan de vérification des conditions d'utilisation relatives à la sécurité (SRAC) fournit un cadre générique permettant de justifier que les instructions du manuel d'installation et de sécurité concerné sont respectées. Ces instructions du document *Modicon M580 - Manuel de sécurité* sont répertoriées comme des exigences.

Le tableau suivant fournit le titre du paragraphe dans lequel vous trouverez les exigences relatives au cycle de vie de l'application :

Exigences relatives au cycle de vie de l'application	
Id	À cet endroit
LC #1	Étape 9 : Spécification des exigences de sécurité des systèmes E/E/PE, page 42
LC #2	Etape 9 : Spécification des exigences de sécurité des systèmes E/E/PE, page 42
LC #3	Etape 10 : Réalisation de systèmes liés à la sécurité E/E/PE, page 42
LC #4	Etape 12 : Installation et mise en service globales, page 46
LC #5	Etape 12 : Installation et mise en service globales, page 46
LC #6	Étape 13 : Validation de sécurité globale, page 48
LC #7	Étape 14 : Exploitation, maintenance et réparation générales, page 48
LC #8	Étape 15 : Modification et modernisation générales, page 49

Le tableau suivant fournit le titre du paragraphe dans lequel vous trouverez les exigences relatives au message d'information de sécurité :

Exigences relatives aux messages d'informations de sécurité	
Id	À cet endroit
SM #1	Avant de commencer, page 10
SM #2	Démarrage et test, page 11
SM #3	Boucle de sécurité, page 22
SM #4	Modules non perturbateurs, page 34

Exigences relatives aux messages d'informations de sécurité	
Id	À cet endroit
SM #5	Alimentation externe utilisée avec les modules d'E/S de sécurité numériques, page 53
SM #6	Exemples de câblage d'application d'entrée BMXSAI0410, Introduction, page 60
SM #7	Exemples de câblage d'application d'entrée BMXSAI0410, SIL3 Cat2/PLd, page 62
#8 SM	Exemples de câblage d'application d'entrée BMXSAI0410, SIL3 Cat2/PLd avec haute disponibilité, page 63
SM #9	Exemples de câblage d'application d'entrée BMXSAI0410, SIL3 Cat4/PLe, page 64
SM #10	Exemples de câblage d'application d'entrée BMXSAI0410, SIL3 Cat4/PLe avec haute disponibilité, page 65
SM #11	Connecteur de câblage BMXSDI1602, alimentation process, page 72
SM #12	Connecteur de câblage BMXSDI1602, fusible, page 73
SM #13	Exemples de câblage d'application d'entrée BMXSDI1602, Introduction, page 78
SM #14	Diagnostics de câblage configurables dans Control Expert, page 79
SM #15	Exemples de câblage d'application d'entrée BMXSDI1602, SIL3 Cat2/PLd, page 80
SM #16	Exemples de câblage d'application d'entrée BMXSDI1602, SIL3 Cat2/PLd, page 80
SM #17	Exemples de câblage d'application d'entrée BMXSDI1602, SIL3 Cat2/PLd, page 80
SM #18	Exemples de câblage d'application d'entrée BMXSDI1602, SIL3 Cat2/PLd avec haute disponibilité, page 82
SM #19	Exemples de câblage d'application d'entrée BMXSDI1602, SIL3 Cat2/PLd avec haute disponibilité, page 82
SM #20	Exemples de câblage d'application d'entrée BMXSDI1602, SIL3 Cat2/PLd avec haute disponibilité, page 82
SM #21	Exemples de câblage d'application d'entrée BMXSDI1602, SIL3 Cat2/PLd avec haute disponibilité, page 82
SM #22	Exemples de câblage d'application d'entrée BMXSDI1602, SIL3 Cat2/PLd avec haute disponibilité, page 82
SM #23	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe, page 86

Exigences relatives aux messages d'informations de sécurité	
Id	À cet endroit
SM #24	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe, page 86
SM #25	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe, page 86
SM #26	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe, page 86
SM #27	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe, page 86
SM #28	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe, page 86
SM #29	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe, page 86
SM #30	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe, page 86
SM #31	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe avec haute disponibilité, page 92
SM #32	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe avec haute disponibilité, page 92
SM #33	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe avec haute disponibilité, page 92
SM #34	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe avec haute disponibilité, page 92
SM #35	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe avec haute disponibilité, page 92
SM #36	Exemples de câblage d'application d'entrée BMXSDI1602, Cat4/PLe avec haute disponibilité, page 92
SM #37	Connecteur de câblage BMXSDO0802, fusible, page 105
SM #38	Exemples de câblage d'application de sortie BMXSDO0802, Introduction, page 107
SM #39	Exemples de câblage d'application de sortie BMXSDO0802, Introduction, page 107
SM #40	Diagnostics de câblage configurables dans Control Expert, page 108
SM #41	Récapitulatif des diagnostics de câblage des sorties, page 111
SM #42	Récapitulatif des diagnostics de câblage des sorties, page 111

Exigences relatives aux messages d'informations de sécurité	
Id	À cet endroit
SM #43	Récapitulatif des diagnostics de câblage des sorties, page 111
SM #44	Récapitulatif des diagnostics de câblage des sorties, page 111
SM #45	Récapitulatif des diagnostics de câblage des sorties, page 111
SM #46	Récapitulatif des diagnostics de câblage des sorties, page 111
SM #47	Connecteur de câblage BMXSRA0405, fusible, page 119
SM #48	Application_1 : 4 sorties, SIL2 / Cat2 / PLc, état non alimenté, pas de test de signal automatique, page 122
SM #49	Application_3 : 4 sorties, conformité SIL2 et Cat2/PLc, état alimenté, pas de test de signal automatique, page 123
SM #50	Application_5 : 2 sorties, conformité SIL3 et Cat4/PLc, état non alimenté, pas de test de signal automatique, page 124
SM #51	Application_7 : 2 sorties, conformité SIL3 et Cat4/PLc, état alimenté, pas de test de signal automatique, page 125
SM #52	Alimentations de sécurité M580, introduction, page 136
SM #53	Description du temps nécessaire aux modules de sortie, page 164
SM #54	Configuration des périodes maximum des tâches SAFE et FAST de la CPU, page 168
SM #55	Fonctions et blocs fonction de sécurité certifiés, page 174
SM #56	Configuration de la synchronisation horaire avec le micrologiciel de CPU de version 3.10 ou antérieure, Introduction, page 185
SM #57	Modification des paramètres temporels NTP durant les opérations, page 186
SM #58	Procédure de synchronisation des paramètres temporels NTP, page 187
SM #59	Procédure de synchronisation des paramètres temporels NTP, page 187
SM #60	Configuration du DFB S_WR_ETH_MX, page 200
SM #61	Configuration du DFB S_RD_ETH_MX, page 203

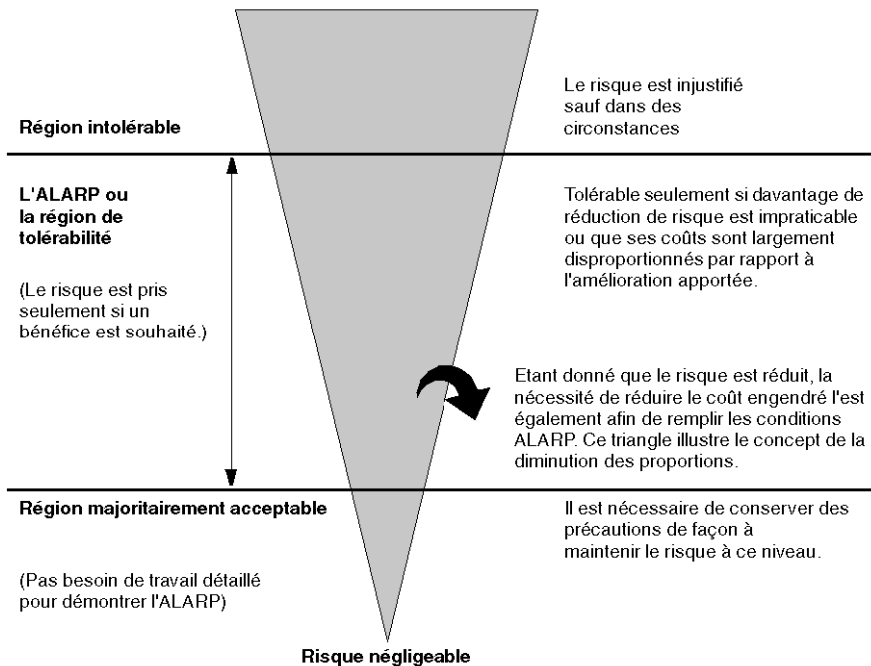
Exigences relatives aux messages d'informations de sécurité	
Id	À cet endroit
SM #62	Configuration du DFB S_WR_ETH_MX2, page 214
SM #63	Configuration du DFB S_RD_ETH_MX2, page 217
SM #64	Communications par canal noir M580, page 221
SM #65	Communications par canal noir M580, page 221
SM #66	Diagnostics par LED de la CPU de sécurité M580, page 231
SM #67	Fonctionnement du mode de maintenance, page 269
SM #68	Séquences De Démarrage, Démarrage À Chaud, page 282
SM #69	Verrouillage de la configuration d'un module d'E/S de sécurité, page 295
SM #70	Affichage des données sur les écrans d'exploitation, page 302
SM #71	Configuration de l'équipement CIP Safety à l'aide d'un outil fourni par le fabricant, page 369
SM #72	Interactions entre les opérations du PAC de sécurité et la connexion cible, page 391

Glossaire

A

ALARP:

Acronyme de *As Low As Reasonably Practicable* (aussi faible que raisonnablement réalisable). (Définition IEC 61508)



C

CCF:

Acronyme de *Common Cause Failure* (défaillance de cause commune). Défaillance résultant d'un ou de plusieurs événements qui, en provoquant des défaillances simultanées de deux ou plusieurs canaux séparés dans un système multicanal, conduit à la défaillance du système. (Définition IEC 61508) Le facteur de cause commune d'un système à deux canaux est un facteur crucial de la probabilité de défaillance sur demande (PFD) sur l'ensemble du système.

CPCRC:

Acronyme de *Connection Parameter Cyclic Redundancy Check* (contrôle de redondance cyclique des paramètres de connexion). Valeur CRC-S32 des paramètres de connexion cible générée par la CSS pour chaque connexion CIP Safety, et contenue dans la requête SafetyOpen de type 2.

D**DDDT:**

Acronyme de *Device Derived Data Type* (type de données dérivé d'équipement). DDT prédéfini par le fabricant, non modifiable par l'utilisateur. Il contient les éléments de langage d'E/S d'un module d'E/S.

DRS:

Acronyme de *dual-ring switch* (commutateur double anneau). Commutateur géré à extension ConneXium qui a été configuré pour fonctionner sur un réseau Ethernet. Des fichiers de configuration prédéfinis sont fournis par Schneider Electric pour téléchargement vers un DRS en vue de prendre en charge les fonctionnalités spéciales de l'architecture à anneau principal/sous-anneau.

DTM:

Acronyme de *device type manager*DTM (gestionnaire de type d'équipement). Pilote d'équipement exécuté sur le PC hôte. Il offre une structure unifiée pour accéder aux paramètres de l'équipement, le configurer et l'utiliser, et pour remédier aux problèmes. Les DTM peuvent présenter différents visages, d'une simple interface graphique permettant de configurer les paramètres de l'équipement jusqu'à une application très perfectionnée susceptible d'effectuer des calculs complexes en temps réel à des fins de diagnostic et de maintenance. Dans le contexte d'un DTM, un équipement peut être un module de communication ou un équipement distant sur le réseau.

Voir FDT.

E**EDS:**

Acronyme de *electronic data sheet* (fiche de données électronique). Les EDS sont de simples fichiers texte qui décrivent les fonctions de configuration d'un équipement. Les fichiers EDS sont générés et gérés par le fabricant de l'équipement.

EUC:

Acronyme de *IEC 61508 Equipment Under Control* (équipement commandé). (Définition)
Ce terme désigne les équipements, les machines, les appareils ou les installations utilisés pour les activités de fabrication, de traitement, de transport, médicales ou d'autres activités.

H

HFT:

Acronyme de *Hardware Fault Tolerance* (tolérance aux anomalies matérielles). (Définition IEC 61508)

Une tolérance aux anomalies matérielles de N signifie que N + 1 anomalies peuvent engendrer une perte de la fonction de sécurité. Par exemple :

- HFT = 0 : la première défaillance pourrait entraîner une perte de la fonction de sécurité.
- HFT = 1 : une association de deux défaillances pourrait entraîner une perte de la fonction de sécurité. Deux méthodes différentes permettent d'atteindre un état sécurisé. La perte de la fonction de sécurité signifie l'impossibilité d'atteindre un état sécurisé.

O

OUNID:

Acronyme de *Originator Unique Network Identifier* (identifiant de réseau source unique). Valeur identifiant de manière unique l'équipement source de la connexion (généralement une CPU) sur un réseau CIP Safety. L'identifiant OUNID est constitué :

- d'un numéro de réseau de sécurité (SNN), correspondant à un horodatage ou à une autre valeur définie par l'utilisateur ;
- d'une adresse de nœud (adresse IP pour les réseaux EtherNet/IP).

P

PST:

Acronyme de *Process Safety Time* (délai de sécurité du processus). Le délai de sécurité du processus est défini comme la période comprise entre une défaillance survenant au niveau du matériel commandé (EUC) ou du système de commande EUC (possibilité de provoquer un événement dangereux) et l'irruption d'un événement dangereux si la fonction de sécurité n'est pas exécutée. (Définition IEC 61508)

R

Réseau DIO:

Réseau contenant des équipements distribués dans lequel la scrutation d'E/S est effectuée par une UC CPU dotée d'un service de scrutation des E/S distribuées DIO sur le rack local. Le trafic réseau DIO est traité après le trafic RIO, qui est prioritaire sur un réseau d'équipements.

S

SAId:

Acronyme de *Safety Application Identifier* (identifiant d'application de sécurité). Signature de la partie sécurisée d'une application Control Expert calculée selon un algorithme et stockée dans le mot %SW169.

SCID:

Acronyme de *Safety Configuration Identifier* (identifiant de configuration de sécurité). Voir TUNID.

SFF:

Acronyme de *Safe Failure Fraction* (proportion de défaillances en sécurité).

SNCT:

Acronyme de *Safety Network Configuration Tool* (outil de configuration du réseau de sécurité). Outil de configuration des équipements CIP Safety fourni par le fabricant. Voir TUNID.

SRAC:

(*Safety Related Application Condition*)

SRT:

Acronyme de *System Reaction Time* (temps de réaction du système). Le temps de réaction du système est la période de temps entre la détection d'un signal sur la borne du module d'entrée et la réaction au niveau d'une sortie sur la borne du module de sortie.

Station RIO:

Rack de modules d'E/S Ethernet, gérés par un adaptateur d'E/S distantes (RIO), avec entrées et sorties incluses à la scrutation RIO de la CPU. Une station peut se présenter sous la forme d'un rack unique ou d'un rack principal associé à un rack d'extension.

T

TFFR:

Acronyme de *Tolability Functional Failure Rate*, taux de défaillance fonctionnelle tolérable. Taux horaire selon les normes EN 5012x pour les chemins de fer.

TUNID:

Acronyme de *Target Unique Network Identifier* (identifiant de réseau cible unique). Valeur identifiant de manière unique l'équipement cible de la connexion sur un réseau CIP Safety. L'identifiant TUNID est constitué :

- d'un numéro de réseau de sécurité (SNN), correspondant à un horodatage ou à une autre valeur définie par l'utilisateur ;
- d'un identifiant de configuration de sécurité (SCID), ou signature de la configuration, généré par un outil de configuration du réseau de sécurité (SNCT) fourni par le fabricant et constitué :
 - d'un CRC de configuration de sécurité (SCCRC), représentant la valeur CRC des paramètres de configuration d'un équipement de sécurité sous la forme d'une valeur hexadécimale de 4 octets ;
 - d'un horodatage de configuration de sécurité (SCTS), représentant une valeur hexadécimale de date et heure de 6 octets.

Index

61508	
IEC	409
61511	
IEC	409

A

alimentation	
diagnostics	239
diagnostics de tension d'embase	139
diagnostics du contact de relais d'alarme	140
alimentation M580	
diagnostics par LED	239
altitude	52
application	332
protecting	314
architecture	
BMXSAI0410	148
BMXSDI1602	149
BMXSDO0802	150
BMXSRA0405	152
coprocesseur BMEP58CPROS3	144
CPU BMEP58-040S	144

B

bibliothèque de sécurité	
Control Expert Safety	174
bilan mémoire	358
bits système de sécurité	417
BMEP58-040S	
architecture	144
BMEP58CPROS3	
architecture	144
BMXSAI0410	56
Applications	60
architecture	148
connecteur de câblage	58
DDDT	66
diagnostics DDDT	241
diagnostics de voyant LED	242
BMXSDI1602	70

applications	78
architecture	149
connecteur de câblage	72
DDDT	98
diagnostics DDDT	246
diagnostics de voyant LED	248
BMXSDO0802	103
Applications	107
architecture	150
connecteur de câblage	105
DDDT	113
diagnostics DDDT	252
BMXSRA0405	118
Applications	121
architecture	152
connecteur de câblage	119
DDDT	130
diagnostics DDDT	258
diagnostics de voyant LED	259
boîtier	51
boucle de sécurité	22, 413

C

canal noir	221
carte mémoire	
diagnostics	236
CCOTF	
limitations au sein d'un projet de sécurité	356
certifications	30
contrôleur d'automatisation programmable (PAC)	26
codes d'erreur	398
commande d'initialisation de données	
initialisation	298
commande d'initialisation des données	
initialisation de la sécurité	298
commande de génération	
Générer des modifications	287
Regénérer tout le projet	287
Renouveler les ID et Regénérer tout	287
communication	
contrôleur à contrôleur	192
communication de contrôleur à contrôleur	192

bloc de fonction dérivé (DFB, Derived Function Block) DFB du contrôleur	
expéditeur	200
bloc DFB du contrôleur expéditeur	214
bloc DFB du contrôleur récepteur	202
communication de PAC à PAC	
architecture	193, 206
configuration	194, 207
transmission de données	199, 213
Communication entre contrôleur d'automatisation programmable (PAC) et contrôleur d'automatisation programmable (PAC)	
bloc de fonction dérivé (DFB, Derived Function Block) du contrôleur d'automatisation programmable (PAC)	
récepteur	216
Communication PAC vers E/S	223
conditions bloquantes	226
conditions non bloquantes	229
Configuration d'E/S	
verrouillage	295
connecteur de câblage	
BMXSAI0410	58
BMXSDI1602	72
BMXSDO0802	105
BMXSRA0405	119
Control Expert	
bilan mémoire	358
enregistrement de données non sécurisées	356
importation d'un projet de sécurité	355
observateur d'événements	359
restauration de données non sécurisées	356
séparation des données	264
transfert d'un projet de sécurité	355
Control Expert	
gestion de l'accès à	339
profils d'utilisateur prédéfinis	342
security editor	342
Control Expert Safety	
bibliothèque de sécurité	174
contrôleur	
les communications avec les modules d'E/S de sécurité	52
coprocesseur BMEP58CPROS3	
diagnostics par LED	234

CPU BMEP58-040S	
diagnostics de voyant LED	231
cybersécurité	39
cycle de vie	
application	40
cycle de vie des applications	40

D

data storage	
protecting	330
DDDT	
BMXSAI0410	66
BMXSDI1602	98
BMXSDO0802	113
BMXSRA0405	130
de l'équipement distant ;	
vérification d'identité	381
délai de sécurité du processus	161
délai moyen entre les défaillances (MTBF, Mean Time Between Failures)	414
démarrage	279
après coupure de courant	279
Démarrage à chaud	282
démarrage à froid	282
Initial	279
Démarrage à chaud	282
démarrage à froid	282
Détection d'équipements	403
diagnostic	
CIP Safety	395
diagnostics	
alimentation	239
carte mémoire	236
conditions bloquantes	226
conditions non bloquantes	229
DDDT du BMXSAI0410	241
DDDT du BMXSDI1602	246
DDDT du BMXSDO0802	252
DDDT du BMXSRA0405	258
modules d'E/S de sécurité	53
relais d'alarme de l'alimentation	140
tension d'embase	139
Voyants de la CPU BMEP58-040S	231
Voyants du BMXSAI0410	242
Voyants du BMXSDI1602	248
Voyants du BMXSRA0405	259

voyants LED de l'alimentation de sécurité M580.....	239	mode de fonctionnement	268
voyants LED du coprocesseur BMEP58CPROS3	234	mode de fonctionnement de maintenance	269
E		mode de fonctionnement de sécurité	268
encryption		modules	
file	314	certifiés	32
entrée de maintenance	272	Non interférent.....	34
E/S de sécurité	51	non perturbateurs de type 1	35
E/S de sécurité M580	223	non perturbateurs de type 2	37
espace de nom		modules d'E/S de sécurité	
processus	179	caractéristiques communes	51
sécurité.....	179	communications avec le contrôleur	52
Transfert des données	182	diagnostics communs.....	53
état de connexion de l'appareil	403	mot de passe	
états de fonctionnement	273	oubli	332
		perte	332
		mots système de sécurité	419
		MTBF (délai moyen entre défaillances)	414
F		N	
file		network time protocol (NTP).....	185
encryption	314	normes.....	30
fonction de sécurité	21	NTP (Network Time Protocol).....	185
H		O	
HFT (tolérance aux anomalies matérielles).....	412	observateur d'événements.....	359
I		oubli	
IEC 61508		mot de passe.....	332
sécurité fonctionnelle	409	OUNID	365
IEC 61511		outil d'analyse des tendances	303
Sécurité fonctionnelle des processus industriels.....	409	P	
IHM.....	302	password	
initialisation des données.....	298	section	321
intervalle entre tests périodiques (PTI)	160	perte	
M		mot de passe.....	332
micrologiciel.....	332	PFD (probabilité de défaillance sur demande)	153, 157, 412
protection	328	PFH (probabilité de défaillance par heure).....	153, 157, 412
		placer TUNID.....	394
		portée des données.....	179

probabilité de défaillance par heure (PFH)	153, 157, 412
probabilité de défaillance sur demande (PFD)	153, 157, 412
Program Unit	
protecting	325
protecting	
application.....	314
data storage	330
Program Unit.....	325
section	325
protection	
micrologiciel	328
PTI (intervalle entre tests périodiques)	160

R

REINITIALISER la propriété.....	394
requête SafetyOpen	
structure de trame.....	386
RIO	51, 223

S

Safety Integrity Level (SIL).....	411
safety-related area	
password	321
SCCRC	369
SCID	369, 376
SCTS	369
section	
protecting	325
Security Editor	339
séparation des données	179
séparation des données dans Control	
Expert.....	264
SFF (taux de défaillances non	
dangereuses).....	412
signature du source SAFE	287
signature SAFE.....	287
SIL (Safety Integrity Level)	411
SNCT	369
SNN	
CPU	365
équipement	375
stockage de données	332
système	

bits	417
mots	419

T

tables d'animation	299
Tâche SAFE	
configuration	304
tâches	283, 304
configuration	284
taux de défaillance	414
Taux de défaillances non dangereuses	
(SFF).....	412
temps réseau attendu.....	170
tolérance aux anomalies matérielles HFT	
(Tolérance aux anomalies matérielles)	412
transfert de données entre espaces de	
nom.....	182
procédure	183

V

Verrouillage de la configuration des	
modules dE/S.....	295

Z

zone de données	
globale.....	180
processus	180
sécurité	180

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Les normes, spécifications et conceptions pouvant changer de temps à autre,
veuillez demander la confirmation des informations figurant dans cette publication.

© 2024 Schneider Electric. Tous droits réservés.

QGH46983.10