# Modicon M580

## Guide de planification du système de sécurité

**Traduction de la notice originale**

**QGH60284.08**
**06/2024**

www.se.com

# 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

## 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**<br>• N'utilisez pas ce logiciel ni les automatismes associés sur des appareils non équipés de protection du point de fonctionnement.<br>• N'accédez pas aux machines pendant leur fonctionnement.<br>**Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.** |

Cet automatisme 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 déréglé 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

Ce guide de planification de système de sécurité décrit les modules du système de sécurité M580, en mettant l'accent sur le respect des exigences de sécurité de la norme CEI 61508. Il fournit des informations détaillées sur l'installation, l'exécution et la maintenance du système qui vous permettent d'assurer la protection des personnes et d'éviter tout dommage sur l'environnement, l'équipement et la production.

Cette documentation s'adresse au personnel qualifié connaissant bien la sécurité fonctionnelle et Control Expert XL 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.

## Champ d’application

Ce document s'applique à EcoStruxure™ Control Expert 16.0 avec ControlExpert_V160_ HF001 M580 Safety ou version ultérieure.

Pour plus d'informations sur la conformité des produits avec les normes environnementales (RoHS, REACH, PEP, EOLI, etc.), consultez le site www.se.com/ww/en/work/support/green-premium/.

Les caractéristiques des produits décrits dans ce document sont censées correspondre aux caractéristiques disponibles sur www.se.com. Toutefois, en application de notre stratégie d'amélioration continue, nous pouvons être amenés à réviser le contenu du document afin de le rendre plus clair et plus précis. Si vous constatez une différence entre les caractéristiques figurant dans ce document et celles fournies sur www.se.com, considérez que le site www.se.com contient les informations les plus récentes.

# Documents à consulter

| Titre de documentation | Référence |
|---|---|
| M580, Conditions d'application liées à la sécurité — Plan de vérification | EIO0000004540 (ENG)<br>EIO0000004741 (FRE)<br>EIO0000004742 (GER)<br>EIO0000004744 (ITA)<br>EIO0000004743 (SPA)<br>EIO0000004745 (CHS) |
| Modicon M580, Manuel de sécurité | QGH46982 (Anglais), QGH46983 (Français), QGH46984 (Allemand), QGH46985 (Italien), QGH46986 (Espagnol), QGH46987 (Chinois) |
| EcoStruxure™ Control Expert - Sécurité, Bibliothèque de blocs | QGH60275 (Anglais), QGH60278 (Français), QGH60279 (Allemand), QGH60280 (Italien), QGH60281 (Espagnol), QGH60282 (Chinois) |
| Cybersécurité des systèmes de contrôleur Modicon, Guide utilisateur | EIO0000001999 (Anglais), EIO0000002001 (Français), EIO0000002000 (Allemand), EIO0000002002 (Italien), EIO0000002003 (Espagnol), EIO0000002004 (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 - Topologies complexes - Guide système | NHA58892 (Anglais), NHA58893 (Français), NHA58894 (Allemand), NHA58895 (Italien), NHA58896 (Espagnol), NHA58897 (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) |
| 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/).

# Informations relatives au produit

**⚠⚠DANGER**

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

- Coupez toutes les alimentations de tous les équipements, y compris les équipements connectés, avant de retirer les caches ou les 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 approprié à cet équipement.
- Utilisez toujours un appareil de mesure de tension réglé correctement pour vous assurer que l'alimentation est coupée conformément aux indications.
- Remettez en place et fixez tous les caches de protection, accessoires, matériels, câbles et fils et vérifiez que l'appareil est bien relié à la terre avant de le remettre sous tension.
- Utilisez uniquement la tension spécifiée pour faire fonctionner cet équipement et tout autre produit associé.

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

# ⚠AVERTISSEMENT

**PERTE DE CONTRÔLE**

- Effectuez une analyse des modes de défaillance et de leurs effets (FMEA - Failure Mode and Effects Analysis) ou une analyse des risques équivalente de votre application et appliquez des contrôles de prévention et de détection avant toute mise en oeuvre.
- 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 liaison de communication et prenez les 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 instructions peut provoquer 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, d'installation et d'exploitation de variateurs de vitesse) ou leur équivalent en vigueur dans votre pays.

| ⚠AVERTISSEMENT |
|---|
| **FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT**<br>• N'utilisez que le logiciel approuvé par Schneider Electric pour faire fonctionner cet équipement.<br>• Mettez à jour votre programme d'application chaque fois que vous modifiez votre configuration matérielle physique.<br>**Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.** |

# Marques commerciales

*QR Code* est une marque déposée de DENSO WAVE INCORPORATED au Japon et dans d'autres pays.

# 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 notamment (mais pas exclusivement) des termes *sécurité*, *fonction de sécurité*, *état sécurisé*, *défaut*, *réinitialisation de défaut*, *dysfonctionnement*, *défaillance*, *erreur*, *message d'erreur*, *dangereux*, etc.

Ces normes incluent entre autres :

| 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.<br>Principes généraux de conception |
| EN 61496-1:2013 Sécurité | Sécurité des machines : Équipement de protection électrosensible.<br>Partie 1 : Exigences générales et tests. |
| ISO 12100:2010 | Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque |

| Norme | Description |
|---|---|
| EN 60204-1:2006 | Sécurité des machines - Equipement électrique des machines - Partie 1 : règles 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 programmable 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 : Exigences concernant les logiciels. |
| 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 |
| 30/2014/UE | Directive sur la compatibilité électromagnétique |
| 35/2014/UE | Directive sur les basses tensions |

En outre, les termes employés dans ce contenu 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 | Réseaux de communication industriels - Spécifications des bus de terrain |

Enfin, le terme *zone de fonctionnement* utilisé dans le contexte de la description de dangers spécifiques a la même signification que les termes "zone dangereuse" et "zone à risque" employés dans la directive Machines (2006/42/CE) et la norme 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.

# Terminologie non inclusive ou non sensible

En tant qu'entreprise responsable et inclusive, nous actualisons nos communications et produits qui contiennent une terminologie non inclusive ou non sensible. Cependant, malgré ces efforts, notre contenu pourra toujours contenir des termes qui pourraient être jugés inappropriés par certains de nos clients.

# Modules pris en charge par le système de sécurité M580

## Présentation

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 s’utiliser avec les UC de sécurité BMEP582040S et BMEH582040S.
- Control Expert XL Safety fournit toutes les fonctionnalités de Control Expert XL et peut s’utiliser avec toutes les UC 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 PAC de sécurité M580 est un système de sécurité certifié par TÜV Rheinland Group, conformément aux normes suivantes :

- SIL3 / IEC 61508 / IEC 61511
- SIL4 / EN 50128 (IEC 62279), EN 50129 (IEC 62245), EN 50126 (IEC 62278)
- 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 révisions du certificat TÜV sont conformes pour une utilisation Sécurité.

Vous trouverez les informations les plus récentes sur les versions certifiées des produits, des micrologiciels et des logiciels sur le site Web de TÜV Rheinland Group, à l'adresse www.certipedia.com ou www.fs-products.com.

Il est basé sur la famille M580 de contrôleurs d'automatisation programmables (PAC, Programmable Automation Controller). Les modules de sécurité M580 suivants de Schneider Electric sont certifiés :

- CPU BMEP582040S autonome
- CPU BMEP584040S autonome
- CPU BMEP586040S autonome
- CPU BMEH582040S redondante
- CPU BMEH584040S redondante
- CPU BMEH586040S redondante
- Coprocesseur BMEP58CPROS3
- Module d'entrées analogiques BMXSAI0410
- Module d'entrées numériques BMXSDI1602
- Module de sorties numériques BMXSDO0802
- Module de sorties relais numériques 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 21 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 PLa, b, c, d.

**NOTE:**

- Chaque fois que le niveau 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 module CPU

Il est possible de remplacer une CPU BME•58•040S par un autre module 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 configuration* du document *Modicon M580 - Redondance d'UC - Guide de planification du système pour architectures courantes* pour une description des applications Control Expert compatibles avec les CPU de sécurité et de redondance d'UC.
- Caractéristiques des performances de la CPU et du coprocesseur de sécurité *M580*, page 58 du document *Modicon M580 - Guide de planification du système de sécurité* pour une description des limites liées à l'UC.

# 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.

## Définition d'un module non perturbateur

**NOTE:** Assurez-vous 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 perturbateur est un module qui ne risque pas de perturber la fonction de sécurité. Pour les modules M580 en rack (BMEx, BMXx, PMXx et PMEx), il existe deux types de modules non perturbateurs :

- **Type 1** : un module de type 1 peut être installé dans le même rack que des modules de sécurité (lorsque le module de sécurité est placé dans le rack principal ou dans un rack d'extension).
- **Type 2** : un module non perturbateur de type 2 ne peut pas être installé dans le même rack principal que des modules de sécurité (lorsque le module de sécurité est placé dans le rack principal ou dans un rack d'extension).

  **NOTE:** Les modules de type 1 et de type 2 sont répertoriés sur le site Web de TÜV Rheinland à l'adresse www.certipedia.com.

  Pour les modules Mx80 qui ne sont pas en rack, 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 actualisée est disponible sur le site Web de TÜV Rheinland à l'adresse www.certipedia.com.

| 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 de rack | 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 |
| 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 | BMEAHI0812 |
| Analogique : HART à courant isolé 4 sorties analogiques | BMEAHO0412 |

| Type de module | Référence du module |
|---|---|
| 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 |
| 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 |

| Type de module | Référence du module |
|---|---|
| | 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 en rack 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 actualisée est disponible sur le site Web de TÜV Rheinland à l'adresse www.certipedia.com.

| 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 |

| Type de module | Référence du module |
|---|---|
| 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 le même rack que les modules de sécurité M580) sont des modules non perturbateurs de type 2.

# Choix de la topologie du système de sécurité M580

## Présentation

Cette section décrit les topologies prises en charge par un système de sécurité M580.

# Conception de la topologie d'un système de sécurité M580

## Prise en charge de PAC autonomes et à redondance d'UC

Un système de sécurité M580 prend en charge les applications SIL3 pour PAC autonomes et redondants. Chaque rack CPU comprend une CPU et un module coprocesseur.

**NOTE:** Pour connaître la description des racks disponibles et leur utilisation autorisée, consultez la rubrique *Utilisation des racks*, page 90.

## Positionnement des modules de sécurité dans l'anneau principal d'E/S distantes (RIO)

Installez les modules de sécurité M580 exclusivement dans l'anneau principal d'E/S distantes (RIO), qui inclut :

- Rack local principal. Les PAC de sécurité autonomes peuvent également comprendre jusqu'à sept racks d'extension locaux facultatifs.
  - Le rack local principal doit inclure une alimentation de sécurité, une CPU de sécurité et un coprocesseur de sécurité.
  - Pour un PAC de sécurité autonome, le rack local principal et les racks d'extension locaux peuvent également inclure les E/S de sécurité. Un PAC redondant M580 ne prend pas en charge les E/S sur le rack principal local ou les racks d'extension locaux.

    **NOTE:** La distance maximale entre le rack principal et le dernier rack d'extension est de 30 m.
- Jusqu'à 31 stations d'E/S distantes (RIO) pour la CPU BME•586040S, 16 stations RIO pour la CPU BME•584040S et 8 stations RIO pour la CPU BME•582040S, chacune composée d'un rack principal distant et d'un rack d'extension distant facultatif.

Tout rack incluant des modules de sécurité requiert également une alimentation de sécurité.

**NOTE:** Un rack incluant des modules de sécurité peut également inclure des modules non perturbateurs de type 1, page 21. Cependant, les modules non perturbateurs de type 2, page 24 ne doivent pas être installés dans le même rack que les modules de sécurité. Les modules non perturbateurs de type 2 peuvent être installés dans les racks exempts de modules de sécurité, par exemple dans les racks d'équipements distribués. Les autres modules non liés à la sécurité ne doivent pas être inclus au système de sécurité M580.

# Extension d'un rack principal

Utilisez des modules d'extension de rack BMXXBE1000 pour relier en chaîne le rack principal et les racks d'extension. Connectez chaque paire de modules d'extension à l'aide de câbles à connecteur BMXXBC•••K et placez une terminaison de ligne TSXELYEX à chaque extrémité de la chaîne.

# Communications dans le rack local avec station RIO

Pour prendre en charge des stations RIO dans un système de sécurité M580 avec micrologiciel de CPU de version 3.10 ou antérieure, configurez la CPU de sécurité M580 en tant que serveur NTP ou bien en tant que client NTP (avec un autre équipement configuré comme serveur NTP). Sans une horloge correctement configurée (NTP), il se peut que la communication des E/S de sécurité ne fonctionne pas correctement.

Utilisez un module adaptateur distant BM•CRA312•0 (un BM•CRA31200 pour un rack hébergeant exclusivement des modules non perturbateurs, et un adaptateur BM•CRA31210 pour un rack distant hébergeant à la fois des modules non perturbateurs et/ou des modules d'E/S de sécurité) pour relier la station RIO à l'anneau principal RIO. Reliez chaque extrémité de l'anneau principal RIO aux deux ports doubles de la CPU de sécurité BME•58•040S.

Si la connexion est effectuée via un câble en cuivre Cat5e, la distance maximale entre les stations est de 100 m.

**NOTE:** Vous pouvez choisir de connecter le rack principal local à l'adaptateur distant BM•CRA312•0 de la station RIO distante en installant un module répéteur à fibre optique BMXNRP020• dans chaque rack. Pour plus d'informations, consultez la rubrique *Utilisation des modules convertisseurs fibre optique* dans le document *Modicon M580 Autonome - Guide de planification du système pour architectures courantes*.

# Connexion de deux PAC de sécurité M580

Un système de sécurité M580 prend également en charge la communication poste à poste par canal noir entre deux PAC de sécurité. En général, cette connexion est effectuée via un BMENOC0321 dans chaque système de sécurité. Pour plus d'informations, consultez la rubrique Communications d'égal à égal dans le document *Modicon M580 - Manuel de sécurité*.

**NOTE:** Pour prendre en charge les communications par canal noir entre deux PAC équipés du micrologiciel CPU de version 3.10 ou antérieure, activez le service NTP dans les deux PAC. Vous pouvez configurer un PAC en tant que serveur NTP, et un autre en tant que client NTP. Vous pouvez choisir de configurer chaque PAC en tant que client NTP, en configurant un autre équipement en tant que serveur NTP.

# Ajout d'équipements distribués à un système de sécurité M580

Vous pouvez inclure un équipement distribué à votre système de sécurité M580. En général, un équipement est connecté en tant que chaînage sans boucle.

Vous pouvez relier une boucle de chaînage d'équipements distribués aux deux ports de réseau de l'un des modules suivants sur l'anneau principal RIO :

- module de communications BMENOC0301/11 Ethernet
- commutateur d'option réseau Ethernet BMENOS0300
- commutateur double anneau ConneXium

Vous pouvez également utiliser le port de service d'un module de communication Ethernet BMENOC0301/11, un commutateur d'options réseau Ethernet BMENOS0300 ou la CPU de sécurité BME•58•040S pour relier l'équipement distribué sous la forme de chaînage sans boucle.

**NOTE:** Dans un réseau d'équipements distribués, vous pouvez installer uniquement des modules non perturbateurs de type 1 et type 2. Vous pouvez installer des modules de sécurité uniquement dans le rack local (principal ou d'extension) et le réseau RIO. Dans un projet lié à la sécurité, excluez tout module non lié à la sécurité qui ne soit pas un module non perturbateur de type 1 ou de type 2.

Consultez la rubrique Choix de la topologie correcte dans le document *Modicon M580 Autonome - Guide de planification du système pour architectures courantes* pour plus d'informations sur la connexion d'équipements distribués à une CPU M580.

# Ajout d'équipements CIP Safety au système de sécurité M580

Il est possible d'ajouter des équipements d'E/S CIP (CSIO) au système de sécurité M580 en tant qu'équipements distribués CSIO.

Les équipements distribués CSIO peuvent être reliés à l'anneau principal RIO via :

- le port de service d'une CPU ou d'un module adaptateur EIO X80 BM•CRA31210,
- un module de sélection d'options de réseau Ethernet BMENOS0300,
- un commutateur double anneau (DRS) ConneXium.

Des restrictions s'appliquent à chaque type d'E/S (CSIO, RIO, DIO). Pour maintenir un niveau de performance acceptable, n'utilisez pas le maximum de tous les types d'E/S dans une même architecture.

Architecture M580 CIP Safety typique basée sur une topologie distante ou distribuée :

Limites pour une **topologie distante** :

| | **Equipements CSIO** | **Equipements DIO** | **Stations RIO** |
|---|---|---|---|
| BMEP582040S | 10 | 10 | 8 |
| BMEP584040S | 32 | 10 | 16 |
| BMEP586040S | (nb CSIO) + 0,5*(nb DIO) + (nb RIO) ≤ 128 | | |

Limites pour une **topologie distribuée** :

| | **Equipements CSIO** | **Equipements DIO** | **Stations RIO** |
|---|---|---|---|
| BMEP582040S | 16 | 61 | 2 |
| BMEP584040S | 64 | 61 | 2 |
| BMEP586040S | (nb CSIO) + 0,5*(nb DIO) + (nb RIO) ≤ 128 | | |

Le temps de cycle CSIO contribue à la tâche SAFE à raison d'environ 100 µs par équipement avec une CPU BMEP584040S ou BMEP586040S et 400 µs par équipement avec une CPU BMEP582040S.

# Topologies de sécurité M580

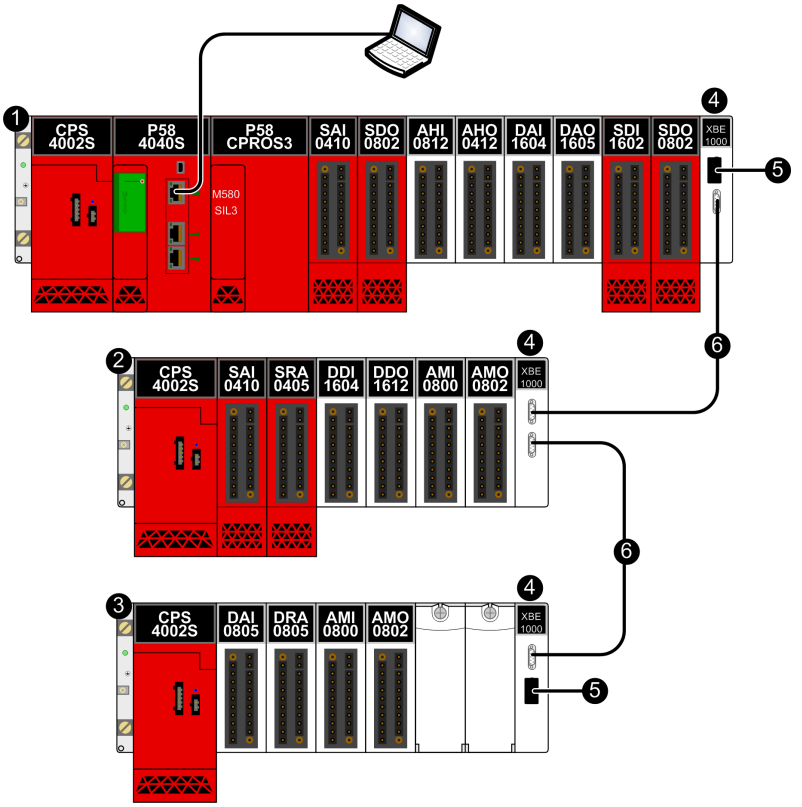
## Introduction

Les schémas suivants présentent des exemples de topologies de sécurité M580. Cette série d'exemples de topologies n'incluent pas toutes les topologies prises en charge par un système de sécurité M580.

Pour plus d'informations sur la conception d'une topologie M580, consultez les documents *Modicon M580 - Autonome - Guide de planification du système pour architectures courantes*, *Modicon M580 - Guide de planification du système pour topologies complexes* et *Redondance d'UC Modicon M580 - Guide de planification du système pour architectures courantes*.

# Extension du rack local principal

Le schéma suivant représente un rack local principal, avec deux racks d'extension. Notez que le système de sécurité M580 prend en charge un seul rack local principal + jusqu'à sept racks d'extension sur une longueur maximale de 30 m :




**1** Rack local principal avec modules de sécurité et modules non perturbateurs de type 1

**2** Rack local d'extension avec modules de sécurité et modules non perturbateurs de type 1

**3** Rack local d'extension avec modules non perturbateurs de type 1

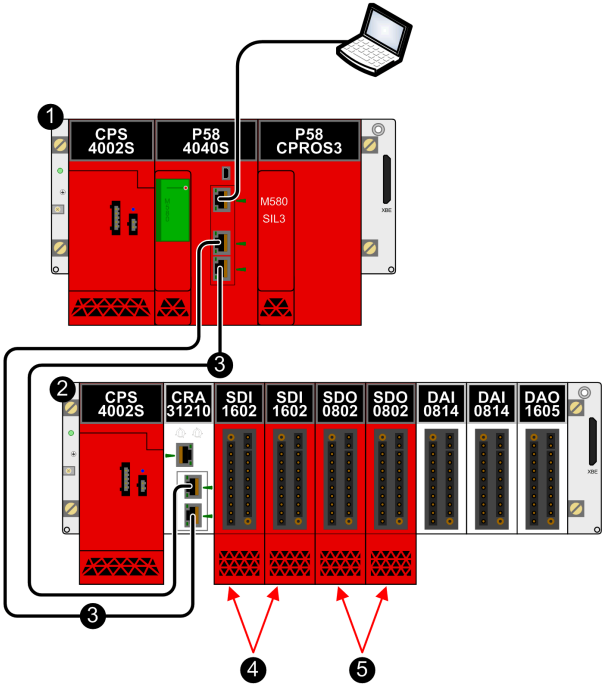
**4** Modules d'extension de rack BMXXBE1000

**5** Terminaisons de ligne TSXELYEX

**6** Câbles de raccordement BMXXBC•••K

# Topologies d'E/S haute disponibilité

Le schéma suivant représente un exemple de modules d'E/S redondants placés dans la même station d'E/S distantes (RIO) :




**1** Rack local principal

**2** Station RIO

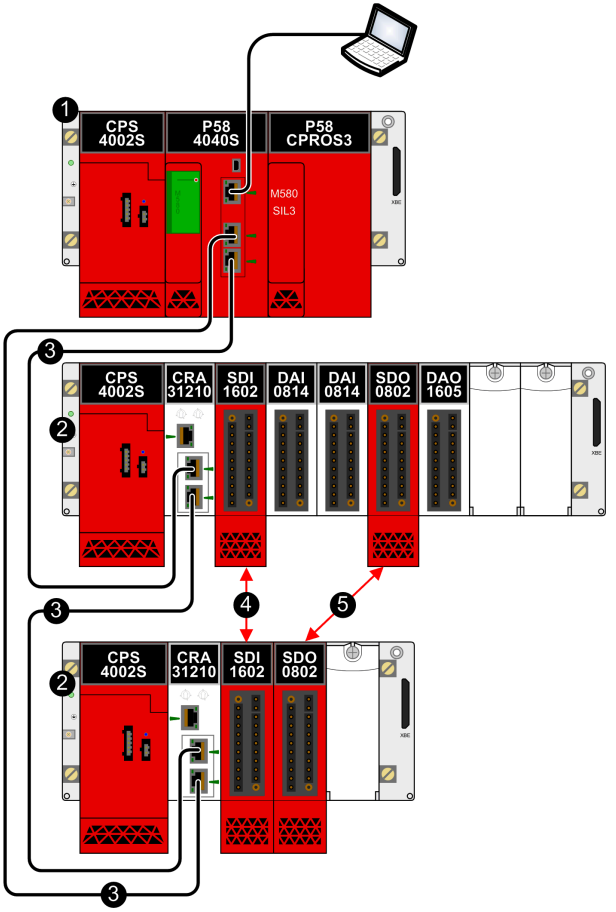
**3** Anneau principal RIO

**4** Deux modules d'entrée redondants dans la même station RIO

**5** Deux modules de sortie redondants dans la même station RIO

**NOTE:** Avec le micrologiciel CPU de version 3.10 ou antérieure, activez le service NTP pour le PAC de sécurité M580 afin de prendre en charge la communication par canal noir entre le rack local principal et les stations RIO de l'anneau principal RIO et configurez l'heure interne du PAC si ce dernier est destiné à servir de serveur NTP. Le PAC de sécurité peut être soit le serveur NTP, soit le client NTP (avec un autre équipement configuré en tant que serveur NTP).

Le schéma suivant représente un exemple de module d'E/S redondant dans deux stations RIO distinctes :




**1** Rack local principal

**2** Station RIO

**3** Anneau principal RIO

**4** Deux modules d'entrée redondants dans deux stations RIO distinctes

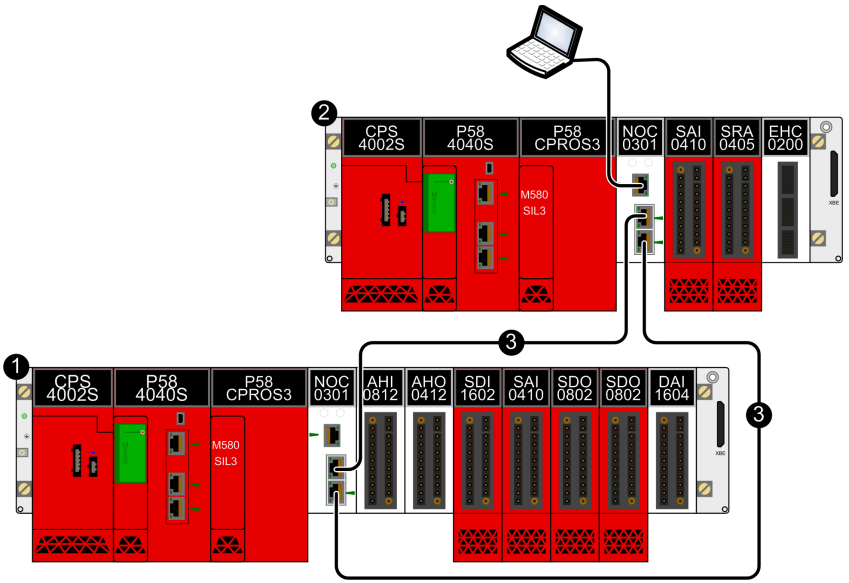
**5** Deux modules de sortie redondants dans deux stations RIO distinctes

**NOTE:**

- Placez les modules d'E/S de sécurité redondants dans des stations RIO distinctes.
- Avec le micrologiciel CPU de version 3.10 ou antérieure, activez le service NTP pour le PAC de sécurité M580 afin de prendre en charge la communication par canal noir entre le rack local principal et les stations RIO de l'anneau principal RIO. Le PAC de sécurité peut être soit le serveur NTP, soit le client NTP (avec un autre équipement configuré en tant que serveur NTP).

# Topologie poste à poste pour deux PAC de sécurité autonomes

Le schéma suivant représente un exemple de connexion de deux PAC de sécurité M580. Dans cet exemple, un capteur lié à un module d'entrée de sécurité dans le PAC 1 peut être configuré pour engendrer une réponse d'un actionneur relié à un module de sortie de sécurité dans un PAC 2 :




**1** PAC 1 de sécurité autonome M580

**2** PAC 2 de sécurité M580

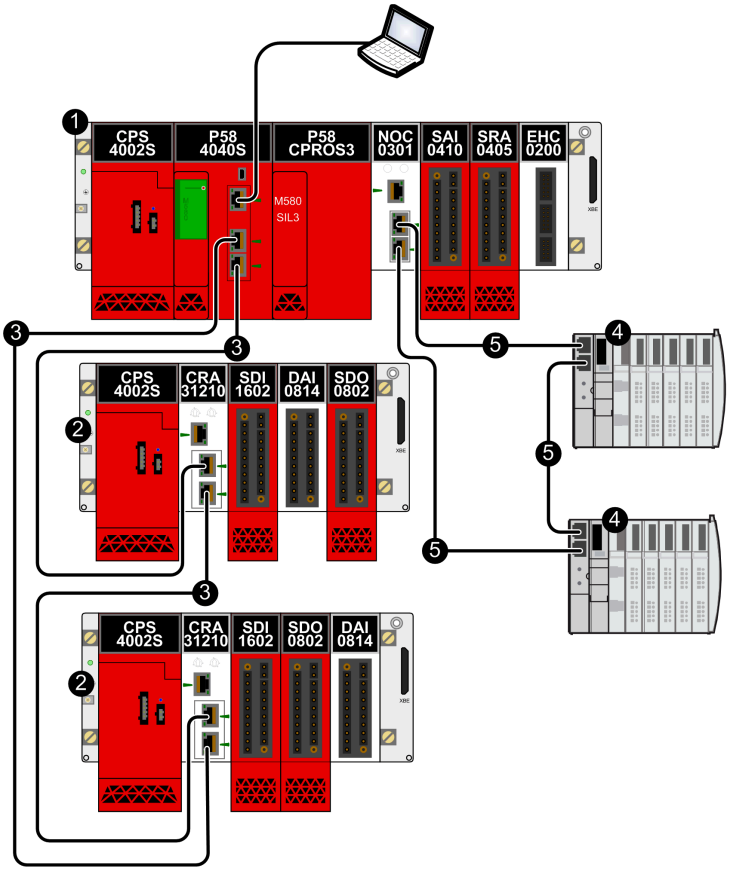
**3** Communication par canal noir entre PAC

**NOTE:** Pour prendre en charge les communications par canal noir entre deux PAC équipés du micrologiciel CPU de version 3.10 ou antérieure, activez le service NTP dans les deux PAC. Vous pouvez configurer un PAC en tant que serveur NTP et l'autre en tant que client NTP. Vous pouvez également choisir de configurer chaque PAC en tant que client NTP, en configurant un autre équipement en tant que serveur NTP.

# Ajout d'équipements distribués au PAC de sécurité M580

Vous pouvez ajouter des modules non perturbateurs de type 1 et type 2 à votre projet de sécurité M580 en tant qu'équipement distribué, dans une conception de type chaînage sans boucle ou boucle de chaînage.

Le schéma suivant décrit un exemple d'équipement distribué ajouté en tant que chaînage sans boucle. Dans cet exemple, le chaînage de l'équipement distribué se connecte au PAC via les ports EIO ETH2 et ETH3 d'un module de communication BMENOC0301/11 Ethernet :




**1** Rack local principal avec embase Ethernet

**2** Station RIO avec modules de sécurité et modules non perturbateurs de type 1

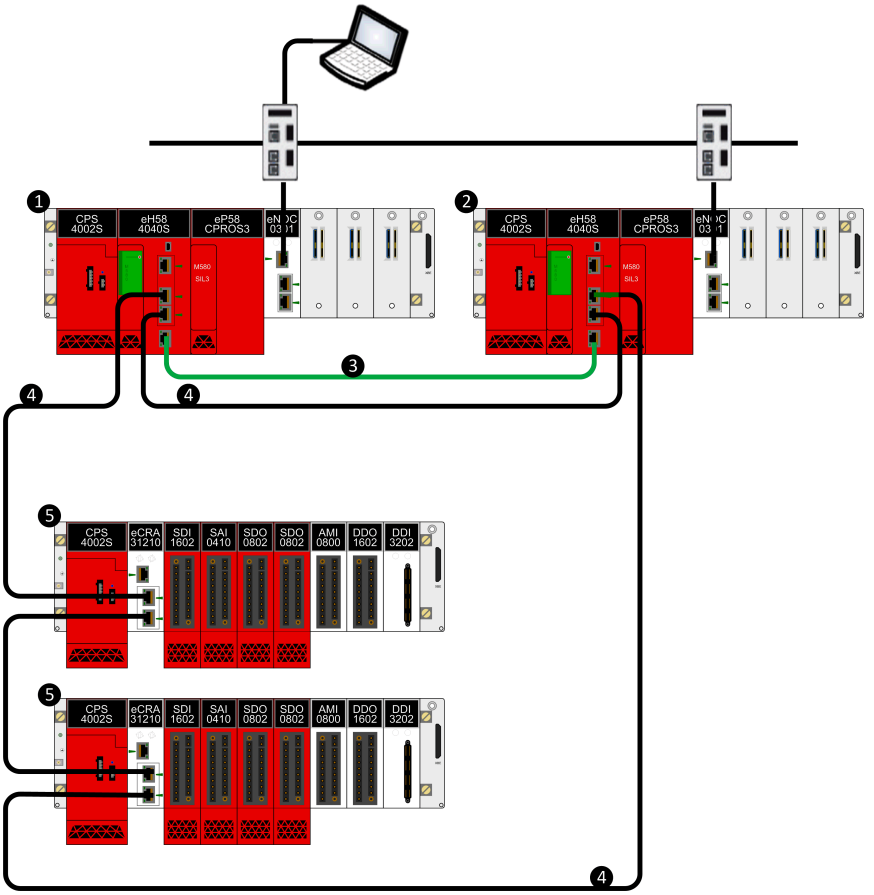
**3** Anneau principal RIO

**4** Equipements distribués

**5** Anneau d'équipements distribués

# Topologie de redondance d'UC

Le schéma suivant représente une topologie à redondance d'UC :




**1** Rack local primaire avec CPU primaire

**2** Rack local redondant avec CPU redondante

**3** Liaison de communication redondante

**4** Anneau principal d'E/S distantes Ethernet

**5** Station d'E/S distantes Ethernet (e)X80

# CPU et coprocesseur de sécurité M580

## Présentation

Ce chapitre décrit les CPU BME•58•040S et le coprocesseur (ou copro) BMEP58CPROS3

# Caractéristiques physiques de la CPU et du coprocesseur de sécurité M580

## Présentation

Cette section décrit les caractéristiques physiques des CPU BME•58•040S et du coprocesseur (copro) BMEP58CPROS3.

## Description physique de la CPU et du coprocesseur de sécurité M580

### Emplacement sur le rack local

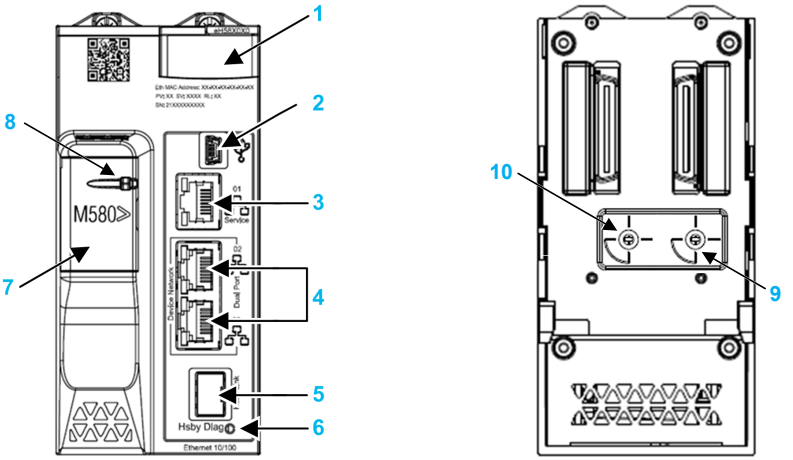
Chaque système de sécurité M580 SIL3 autonome requiert une CPU BME•58•040S et un coprocesseur (Copro) BMEP58CPROS3 La CPU requiert deux emplacements de module : elle est placée dans les emplacements 0 et 1 situés immédiatement à droite de l'alimentation du rack local principal. Le coprocesseur requiert également deux emplacements de module : il est placé dans les emplacements 2 et 3 situés immédiatement à droite de la CPU. Il est impossible de placer la CPU et le coprocesseur dans d'autres emplacements ou sur un autre rack. Si la configuration du rack local comprend des racks d'extension, attribuez l'adresse 00 au rack qui contient la CPU and Copro.

**NOTE:** La CPU et le coprocesseur de sécurité peuvent être installés uniquement sur un rack BMEXBP•••• Ethernet. Pour connaître la description des racks M580 disponibles, consultez la rubrique *Racks locaux et distants* dans le document *Modicon M580 - Manuel de référence du matériel*.

### Vues avant et arrière de la CPU

La CPU de sécurité BME•58•040S prend en charge la scrutation RIO et DIO.

Caractéristiques physiques de la CPU :




Légende :

**1** Panneau d'affichage de diagnostic des voyants (LED)

**2** Port USB mini-B pour la configuration du module via l'instance Control Expert en cours d'exécution sur le PC

**3** Connecteur Ethernet RJ45 pour le port de service

**4** Connecteurs RJ45 servant de port double au réseau Ethernet

**5** Socket SFP pour connecter la liaison redondante en cuivre ou fibre optique

**6** LED d'état de la liaison de redondance d'UC

**7** Emplacement de carte mémoire SD (protégé par un cache)

**8** Cache verrouillable pour carte mémoire SD

**9** Sélecteur rotatif du mode de fonctionnement, avec réglages **Communication Security Reset**, **Secured**, **Standard**

> **NOTE:** Le sélecteur rotatif du mode de fonctionnement sera disponible dans les versions ultérieures du produit. Pour cette version du produit, le mode de fonctionnement est automatiquement réglé sur **Standard**, quelle que soit la position du sélecteur.

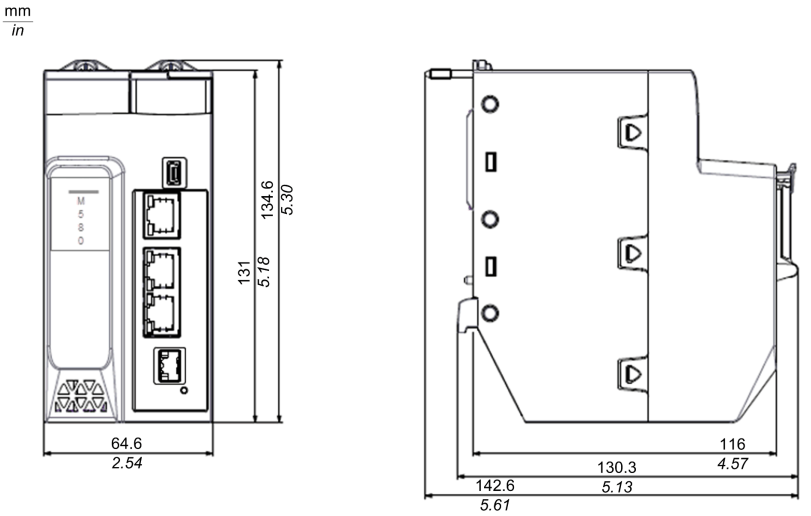
**10** Sélecteur rotatif A/B/Effacer, utilisé pour désigner le PAC comme PAC A ou PAC B, ou pour effacer l'application Control Expert existante

## Face avant du coprocesseur

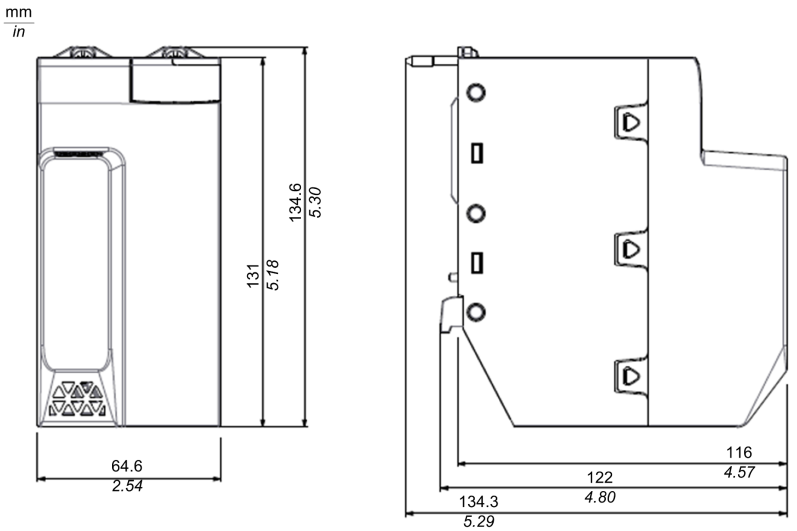
Le coprocesseur BMEP58CPROS3 comporte des voyants uniquement en face avant.

## Dimensions de la CPU et du coprocesseur

Les CPU de sécurité BME•58•040S ont les dimensions physiques suivantes :



Dimensions physiques du coprocesseur BMEP58CPROS3 : Contrairement à la CPU, le coprocesseur ne comporte pas de connecteur physique ni d'étiquette associée

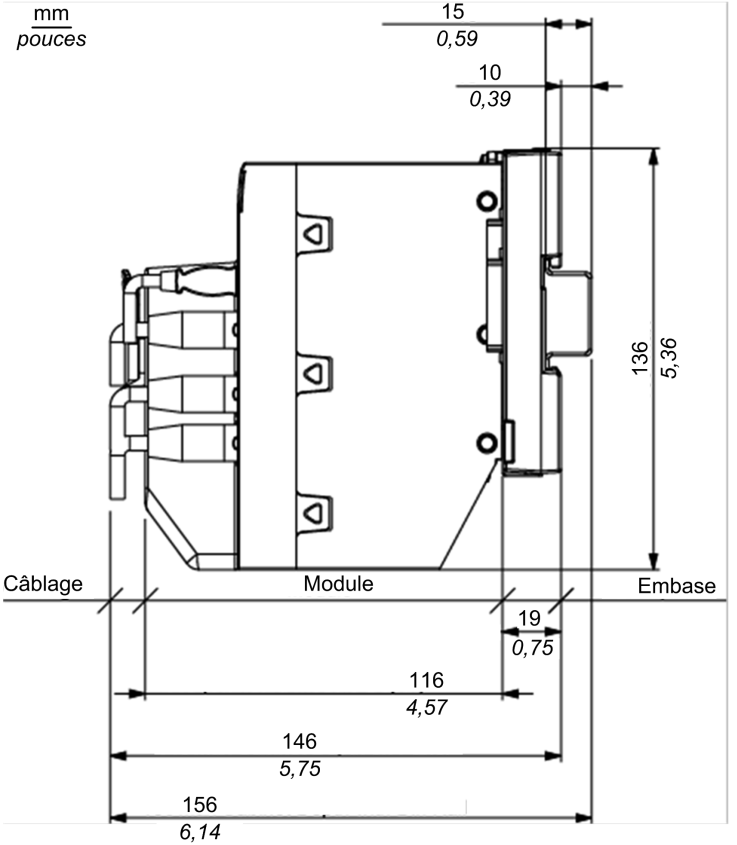



**NOTE:** Tenez compte de la hauteur de la CPU et du coprocesseur lors de la planification de l'installation du rack local. La CPU et le coprocesseur dépassent le bord inférieur du rack de :

- 29,49 mm (1,161 po) pour un rack Ethernet
- 30,9 mm (1,217 po) pour un rack X Bus

# Dimensions de la CPU

Les CPU de sécurité BME•58•040S ont les dimensions suivantes en cas de montage sur un rail DIN avec câblage :

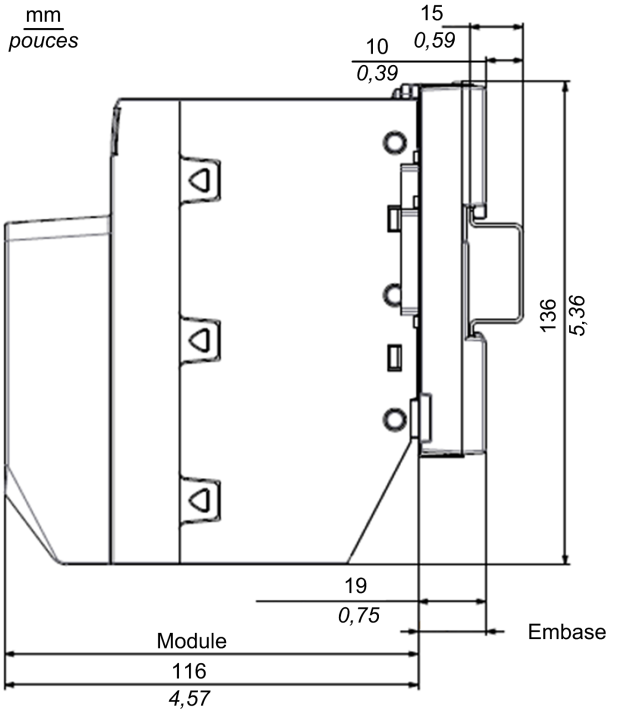



Profondeur globale de la CPU :

- 146 mm avec câblage
- 156 mm avec câblage et rail DIN

# Dimensions du câblage du coprocesseur

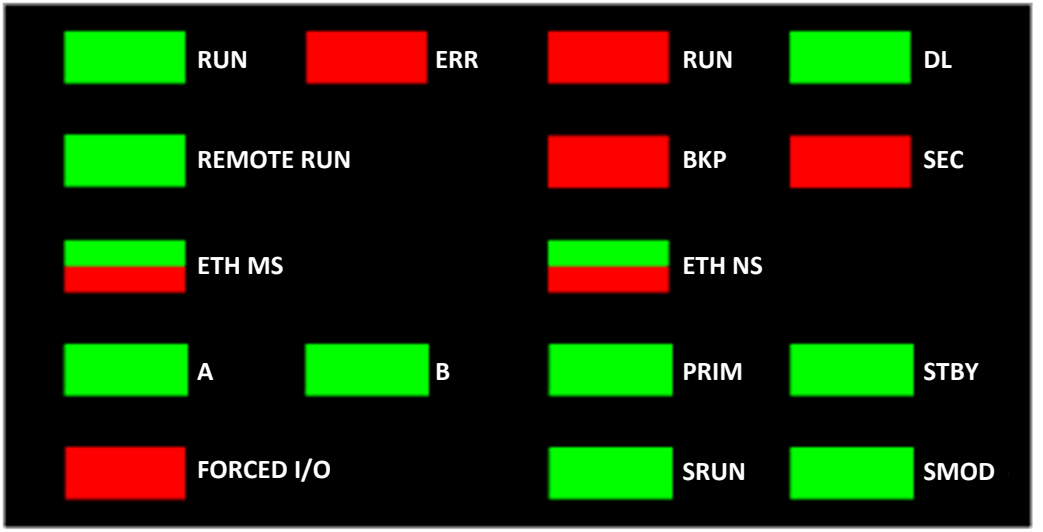
Dimensions du coprocesseur BMEP58CPROS3 lorsqu'il est monté sur un rail DIN :



# Voyants de la CPU et du coprocesseur de sécurité M580

## LED Display de la CPU

La face avant de la CPU comporte des voyants à LED :




**NOTE:** Le voyant **SEC**, indiquant l'état de la communication sécurisée, n'est pas disponible dans cette version.

**NOTE:** Le groupe de voyants du coprocesseur est un sous-ensemble des voyants de la CPU. Il contient les voyants suivants :

- **ERR**
- **DL**
- **SRUN**
- **SMOD**

# Description des voyants à LED

**NOTE:** Consultez les rubriques :

- *Voyants de diagnostic de la CPU de sécurité M580* et *Voyants de diagnostic du coprocesseur M580* dans le document *Modicon M580 - Manuel de sécurité* pour plus d'informations sur l'utilisation des voyants de la CPU et du coprocesseur pour diagnostiquer l'état du PAC de sécurité.
- *Voyants de diagnostic des UC redondantes M580* dans le document *Modicon M580 - Redondance d'UC - Guide de planification du système pour architectures courantes* pour plus d'informations sur l'utilisation des voyants **A**, **B**, **PRIM**, **STBY** et **REMOTE RUN** des CPU à redondance.

| Voyant à LED | Applicable à | | Description |
|---|---|---|---|
| | CPU | Copro | |
| **RUN** | ✓ | – | **Allumé** : La CPU gère ses sorties et au moins une tâche est à l'état RUN. |
| **ERR** | ✓ | ✓ | **Allumé** : La CPU a détecté une erreur d'UC interne (par exemple : aucune configuration, erreur de chien de garde détectée, erreur d'autotest détectée). |
| **I/O** | ✓ | – | **Allumé** : La CPU a détecté une erreur externe dans un ou plusieurs modules d'E/S. |
| **DL** (*téléchargement*) | ✓ | + | • **Allumé** : Une mise à niveau de micrologiciel est en cours vers la CPU, le coprocesseur, l'embase ou un autre module en rack.<br>• **Éteint** : Aucune mise à niveau de micrologiciel n'est en cours. |
| **BKP** | ✓ | – | **Allumé** :<br>• La carte mémoire ou la mémoire flash de la CPU est absente ou inopérante.<br>• La carte mémoire est inutilisable (format incorrect, type non reconnu).<br>• Le contenu de la carte mémoire ou de la mémoire flash de la CPU n'est pas cohérent avec l'application actuelle.<br>• La carte mémoire a été retirée et réinsérée.<br>• Une commande **Automate > Sauvegarde du projet... > Effacer la sauvegarde** a été lancée en l'absence de carte mémoire. Le voyant **BKP** reste **allumé** jusqu'à l'aboutissement de la sauvegarde du projet. |
| | | | **Éteint** : Le contenu de la carte mémoire ou de la mémoire flash de la CPU est valide et l'application en mémoire d'exécution est identique. |
| **ETH MS** | ✓ | – | MOD STATUS (vert/rouge) : Le motif indique l'état de configuration de port Ethernet.<br>**NOTE:** En cas de détection d'une erreur récupérable, le voyant **ETH MS** peut être vert ou rouge, allumé ou éteint. |

| Voyant à LED | Applicable à | | Description |
|---|---|---|---|
| | CPU | Copro | |
| **ETH NS** | ✓ | – | NET STATUS (vert/rouge) : Le motif indique l'état de la connexion Ethernet. |
| **FORCED I/O** | ✓ | – | **Allumé** : Au moins une entrée ou une sortie est forcée sur un module d'E/S numériques. |
| **SRUN** | ✓ | ✓ | **Allumé** : Le PAC gère ses sorties de sécurité et la tâche SAFE est à l'état RUN. |
| **SMOD** | ✓ | ✓ | • **Allumé** : Le PAC fonctionne en mode sécurité, page 121.<br>• **Clignotant** : Le PAC fonctionne en mode maintenance, page 122. |
| ✓ : Applicable<br>– : Non applicable | | | |

# Ports Ethernet

## Introduction

Il y a trois ports RJ45 Ethernet en face avant de la CPU : un port de service et deux ports de réseau d'équipements. Ces ports ont des caractéristiques communes, comme décrit ci-dessous.

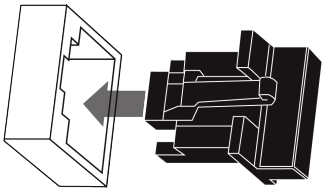
## Caractéristiques communes

Les trois ports présentent le même connecteur RJ45 et utilisent le même type de câbles Ethernet.

**NOTE:** Les trois ports Ethernet sont reliés à la masse du châssis, et le système nécessite une terre équipotentielle.

## Protection anti-poussière

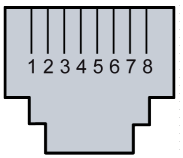
Afin d'éviter toute pénétration de poussière dans les ports Ethernet inutilisés, protégez-les à l'aide du bouchon prévu à cet effet :



## Ports Ethernet

Chaque connecteur RJ45 comporte une paire de voyants LED :


La position des broches, leur affectation et les connexions câblées sont identiques sur les trois ports RJ45 Ethernet :

| Broche | Description | |
|---|---|---|
| 1 | TD+ | Brochage :  |
| 2 | TD- | |
| 3 | RD+ | |
| 4 | non connectée | |
| 5 | non connectée | |
| 6 | RD- | |
| 7 | non connectée | |
| 8 | non connectée | |
| — | Masse du châssis/boîtier | |



**NOTE:** Les broches TD (1 et 2) et les broches RD (3 et 6) sont compatibles auto-MDIX et inversent automatiquement leur fonction selon le matériel connecté (câbles droits ou croisés).

Les ports sont pourvus d'une fonctionnalité MDIX qui détecte automatiquement la direction de la transmission.

Vous avez le choix entre les câbles Ethernet suivants pour la connexion aux ports Ethernet :

- TCSECN3M3M•••• : câble blindé droit Cat 5E Ethernet, pour utilisation industrielle, conforme CE ou UL
- TCSECE3M3M•••• : câble blindé droit Cat 5E Ethernet, pour utilisation industrielle, conforme CE
- TCSECU3M3M•••• : câble blindé droit Cat 5E Ethernet, pour utilisation industrielle, conforme UL

La longueur maximale des câbles de cuivre est de 100 m. Pour les distances supérieures, utilisez des câbles à fibre optique. La CPU ne présente aucun port pour fibre optique. Vous pouvez utiliser des commutateurs double anneau (DRS) ou des modules convertisseurs fibre optique BMX NRP •••• (voir Modicon M580 Autonome, Guide de planification du système pour, architectures courantes) pour gérer la conversion cuivre-fibre.

## Ports Ethernet sur les CPU autonomes

Sur les CPU autonomes, le voyant LED**ACTIVE** est vert. Le voyant (LED) **LNK** s'affiche en vert ou en jaune, selon l'état :

| Voyant | Etat du voyant | Description |
|---|---|---|
| **ACTIVE** | Eteint | Aucune activité n'est signalée sur la connexion Ethernet. |
| | Allumé/ clignotant | Des données sont en cours de transmission et de réception sur la connexion Ethernet. |
| **LNK** | Eteint | Aucune liaison n'est établie au niveau de cette connexion. |
| | Allumé vert | Une liaison 100 Mbits/s* est établie au niveau de cette connexion. |
| | Allumé jaune | Une liaison 10 Mbits/s* est établie au niveau de cette connexion. |
| * Les liaisons 10/100 Mbits/s prennent en charge le transfert de données en semi-duplex et duplex intégral et l'autonégociation. | | |

## Port Service

Le port de service est le plus haut des trois ports Ethernet sur le panneau avant de la CPU. Il peut être utilisé :

- Pour fournir un point d'accès que d'autres équipements ou systèmes peuvent utiliser pour surveiller ou communiquer avec la CPU M580.
- Comme port DIO autonome prenant en charge une topologie d'équipements distribués en étoile ou en boucle de chaînage.
- Pour répliquer les ports CPU pour les diagnostics Ethernet. L'outil de service qui observe l'activité sur le port répliqué peut être un PC ou un terminal IHM.

**NOTE:** N'utilisez pas le port de service pour vous connecter au réseau d'équipements, sauf dans quelques circonstances précises décrites dans le document *Modicon M580, Open Ethernet Network, System Planning Guide*.

Il se peut que le port de service n'offre pas les performances et les fonctionnalités complètes proposées par les ports du **réseau d'équipements** sur la CPU.

La connexion du port de service (directement ou via un commutateur/concentrateur) au réseau d'équipements peut affecter les performances du système.

## Ports doubles du réseau d'équipements

Vous pouvez utiliser un port **Device Network** pour prendre en charge une topologie d'équipements distribués en étoile ou en chaînage. Vous pouvez utiliser les deux ports **Device Network** pour prendre en charge une topologie en anneau.

Lorsqu'ils sont utilisés en tant que ports RIO, ces deux ports connectent la CPU à l'anneau principal dans une boucle ou un anneau de chaînage Ethernet.

Pour plus d'informations sur les architectures RIO/DIO, reportez-vous au chapitre *Système Modicon M580* (voir Modicon M580 Autonome, Guide de planification du système pour, architectures courantes).

## Consignes de mise à la terre

Respectez toutes les normes et consignes de sécurité locales et nationales.

**⚠⚠DANGER**

**RISQUE D'ELECTROCUTION**

Lorsqu'il est impossible de prouver que l'extrémité d'un câble blindé est reliée à la masse locale, ce câble doit être considéré comme dangereux et les équipements de protection individuelle (EPI) doivent être utilisés.

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

# Port USB

## Introduction

Le port USB est un connecteur USB mini-B à vitesse élevée, version 2.0 (480 Mbps) qui peut être utilisé pour un programme Control Expert ou un panneau d'interface homme-machine (HMI). Le port USB peut être connecté à un autre port USB, version 1.1 ou ultérieure.

**NOTE:** Installez les pilotes USB M580 avant de connecter un câble USB entre la CPU et le PC.

## Transparence

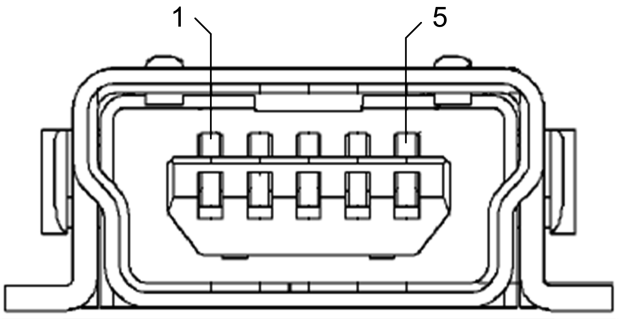
Si votre système requiert la transparence entre l'équipement connecté au port USB et le réseau d'équipements M580, ajoutez un chemin statique persistant dans la table de routage de l'équipement.

Exemple de commande permettant d'adresser un réseau d'équipements avec une adresse IP `X.X.0.0` (pour un PC Windows) : `route add X.X.0.0 mask 255.255.0.0 90.0.0.1 -p`

(`X.X.0.0` correspond à l'adresse du réseau d'équipements M580 et `255.255.0.0` au masque de sous-réseau associé.)

## Brochage

Le port USB présente les positions de broche et affectations suivantes :




Légende :

| Broche | Description |
|---|---|
| 1 | VBus |
| 2 | D- |
| 3 | D+ |
| 4 | non connectée |
| 5 | terre |
| Coque | mise à la terre du châssis |

## Câbles

Utilisez un câble BMX XCA USB H018 (1,8 m/5,91 ft) ou BMX XCA USB H045 (4,5 m/ 14,764 ft) pour raccorder le panneau à la CPU. (Ces câbles présentent un connecteur de type A d'un côté et un connecteur USB mini-B de l'autre.)

Dans un assemblage fixe avec console de type XBT connectée à la CPU, branchez le câble USB à une barre de protection (voir Modicon X80, Racks et modules d'alimentation, Manuel de référence du matériel). Utilisez la partie exposée du blindage ou la cosse métallique du câble BMX XCA pour effectuer ce raccordement.

# Socket SFP

## Connecteur du port de liaison redondante

Chaque module de CPU redondante comporte un socket SFP auquel il est possible de connecter un émetteur-récepteur cuivre ou fibre optique :

Consultez le document *Modicon M580 – Guide de planification de système redondant pour architectures courantes* pour plus d'informations sur l'installation et le retrait d'un socket SFP, et la liste des émetteurs-récepteurs SFP disponibles.

# Carte mémoire SD

## Carte mémoire SD BMXRMS004GPF

La carte mémoire BMXRMS004GPF est une carte de classe 6 de 4 Go adaptée à l'usage industriel. L'emplacement de carte mémoire SD se trouve derrière le le capot en face avant du contrôleur.

Vous pouvez utiliser une carte mémoire BMXRMS004GPF pour le stockage d'applications et de données.

Vous pouvez utiliser une carte mémoire BMXRMS004GPF pour stocker :

- L'application du projet de sécurité M580.
- Données des tâches non liées à la sécurité (MAST, FAST, AUX0, AUX1).

**NOTE:**

- Les données ne peuvent pas être stockées sur la carte mémoire SD pour la tâche SAFE.
- La carte mémoire SD n'est pas incluse dans la boucle de sécurité.

Vous pouvez insérer et extraire la carte lorsque le contrôleur est sous tension et fonctionne en mode RUN. Toutefois, pour éviter les pertes de données, utilisez le bit système %S65 avant d'extraire la carte du contrôleur pour lancer une requête système d'interruption de l'accès à ses données.

**NOTE:** Les autres cartes mémoire, notamment celles utilisées dans les contrôleurs M340, ne sont pas compatibles avec les contrôleurs M580. Si vous insérez une carte mémoire SD incompatible dans le contrôleur :

- Le contrôleur reste dans l'état NOCONF (voir Modicon M580 - Manuel de référence du matériel).
- Le voyant à LED **BKP** du contrôleur s'allume.
- Le voyant à LED d'accès à la carte mémoire clignote.

La carte mémoire BMXRMS004GPF est spécialement formatée pour les contrôleurs M580. Si vous utilisez cette carte avec un autre contrôleur ou un autre outil, elle risque de ne pas être reconnue.

## Caractéristiques de la carte mémoire

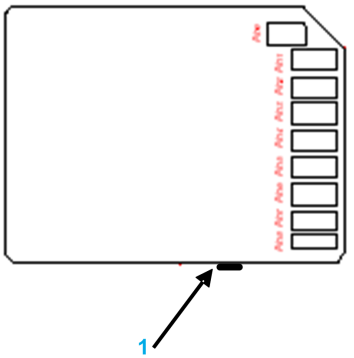
La carte mémoire BMXRMS004GPF présente les caractéristiques suivantes :

| Caractéristique | Valeur |
|---|---|
| Taille globale de la mémoire | 4 Go |
| Taille pour la sauvegarde de l'application | 200 Mo |
| Taille pour le stockage de données | 3,8 Go |
| Cycles d'écriture/d'effacement (en général) | 100 000 |
| Températures de fonctionnement | -40 à +85 °C (-40 à +185 °F) |
| Temps de rétention des fichiers | 10 ans |
| Zone mémoire pour l'accès FTP | Répertoire de stockage de données uniquement |

**NOTE:** Pour des raisons liées au formatage, à l'usure et à d'autres mécanismes internes, la capacité réelle disponible de la carte mémoire est légèrement inférieure à la taille totale.

## Commutateur d'accès en lecture/écriture à la carte

La carte mémoire BMXRMS004GPF est munie d'un commutateur d'accès en lecture/écriture, situé sur le côté non biseauté, qui permet de protéger la carte contre tout accès en écriture non autorisé :




**1** Commutateur d'accès en lecture/écriture

## Formatage de la carte mémoire

La procédure de formatage est décrite dans la section *Formatage de la carte mémoire* du document *Ecostruxure™ Control Expert - Bibliothèque de blocs System*.

# Sceaux anti-altération et cache verrouillable pour carte SD

## Sceaux anti-altération

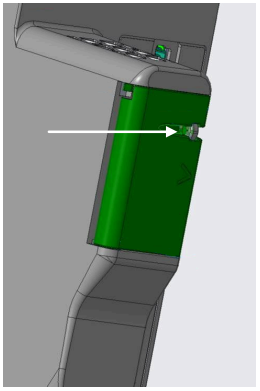
Deux sceaux anti-altération sont placés sur le côté droit des UC M580 autonomes et redondantes, à la jonction entre le cadre (c'est-à-dire la partie avant du conteneur du module) et le boîtier (c'est-à-dire la partie arrière du conteneur du module). Ces sceaux indiquent si le module a été ouvert et éventuellement altéré.

Le conteneur du module n'a pas été ouvert lorsque les sceaux anti-altération se présentent comme suit :


Le conteneur du module a été ouvert lorsque les sceaux anti-altération se présentent comme suit :

## Cache verrouillable pour carte SD

Il est possible de verrouiller ou de plomber le cache qui recouvre l'emplacement de la carte SD.



Pour ce faire, procédez comme suit :

1. Fermez le cache de la carte SD.
2. Insérez l'extrémité d'un fil de plombage (ou le câble d'un cadenas) dans le trou de la partie qui ressort du cache de la carte SD.

   **NOTE:** Vous pouvez utiliser un fil ou un câble d'un diamètre maximum de 1,50 mm (0,06 po).
3. Fermez le plombage (ou verrouillez le cadenas).

**NOTE:** Le plombage ou le cadenas ne sont pas fournis avec le module.

# Caractéristiques des performances de la CPU et du coprocesseur de sécurité M580

## Présentation

Cette section décrit les caractéristiques physiques de la CPU BMEP584040S et du coprocesseur (copro) BMEP58CPROS3

## Performances de la CPU et du coprocesseur M580

### CPU et coprocesseur de sécurité

Voici les caractéristiques des performances de la CPU BME•58•040S et du coprocesseur (ou copro) BMEP58CPROS3 dans une solution de sécurité SIL3 M580 :

| **Caractéristique** | | **BME** | | | | | |
|---|---|---|---|---|---|---|---|
| | | **P582040S** | **P584040S** | **P586040S** | **H582040S** | **H584040S** | **H586040S** |
| Racks locaux | | 4 (1 rack principal + jusqu'à 3 racks d'extension) | 8 (1 rack principal + jusqu'à 7 racks d'extension) | 8 (1 rack principal + jusqu'à 7 racks d'extension) | 1 | 1 | 1 |
| Stations RIO (max. 2 racks par station : rack principal + rack d'extension) | | 8 stations (jusqu'à 2 racks par station) | 16 stations (jusqu'à 2 racks par station) | 31 stations (jusqu'à 2 racks par station) | 8 stations (jusqu'à 2 racks par station) | 16 stations (jusqu'à 2 racks par station) | 31 stations (jusqu'à 2 racks par station) |
| Canaux d'E/S | E/S TOR | 2048 | 4096 | 6144 | 0[1] | 0[1] | 0[1] |
| | E/S analogiques | 512 | 1024 | 1536 | 0[1] | 0[1] | 0[1] |
| | Expertes | 72 | 144 | 216 | 0[1] | 0[1] | 0[1] |
| Ports Ethernet | Embase | 1 | 1 | 1 | 1 | 1 | 1 |
| | Service | 1 | 1 | 1 | 1 | 1 | 1 |
| | RIO | 2 | 2 | 2 | 2 | 2 | 2 |
| Réseau de contrôle | Nombre max. de modules/équipements | 64 | 128 | 128 | 64 | 128 | 128 |
| | Capacité max. d'entrée | 16 Ko | 24 Ko | 24 Ko | 16 Ko | 24 Ko | 24 Ko |

| Caractéristique | | BME | | | | | |
|---|---|---|---|---|---|---|---|
| | | P582040S | P584040S | P586040S | H582040S | H584040S | H586040S |
| | Capacité max. de sortie | 16 Ko | 24 Ko | 24 Ko | 16 Ko | 24 Ko | 24 Ko |
| | Capacité max. d'entrée FAST | 3 Ko | 5 Ko | 5 Ko | 3 Ko | 5 Ko | 5 Ko |
| | Capacité max. de sortie FAST | 3 Ko | 5 Ko | 5 Ko | 3 Ko | 5 Ko | 5 Ko |
| Réseau d'équipements distribués | Nombre max. de modules/équipements | 61 | 61 | 61 | 61 | 61 | 61 |
| | Capacité max. d'entrée | 2 Ko | 8 Ko | 8 Ko | 2 Ko | 2 Ko | 2 Ko |
| | Capacité max. de sortie | 2 Ko | 8 Ko | 8 Ko | 2 Ko | 2 Ko | 2 Ko |
| | Nombre max. d'équipements CIP Safety | 16 | 64 | 128 | – | – | – |
| | Nombre max. de connexions CIP Safety | 32 | 128 | 256 | – | – | – |
| Modules de communication Ethernet sur le rack local | Nb max. de modules de communication Ethernet | 2 | 4 | 4 | 2 | 4 | 4 |
| | Nb max. de BMENOC0301/0311 | 2 | 3 | 3 | 2 | 3 | 3 |
| | Nb max. de BMENOC0321 | 2 | 2 | 2 | 2 | 2 | 2 |
| Allocation de mémoire (max) | Programme d'application non lié à la sécurité | 8 Mo | 16 Mo | 64 Mo[4] | 8 Mo | 16 Mo | 64 Mo[4] |
| | Programme d'application sécurisé | 2 Mo | 4 Mo | 16 Mo[4] | 2 Mo | 4 Mo | 16 Mo[4] |
| | Données non liées à la sécurité | 768 Ko | 2048 Ko | Jusqu'à 65536 Ko[4] | 768 Ko | 2048 Ko | Jusqu'à 65536 Ko[4] |
| | Vol. max. de données conservées configurables | 768 Ko | 2048 Ko | 4096 Ko | 768 Ko | 2048 Ko | 4096 Ko |
| | Vol. max. de données transférées redondantes configurables | – | – | – | 768 Ko | 2048 Ko | 4096 Ko[5] |

| Caractéristique | | BME | | | | | |
|---|---|---|---|---|---|---|---|
| | | P582040S | P584040S | P586040S | H582040S | H584040S | H586040S |
| | Données liées à la sécurité (non conservées) | 512 Ko | 1024 Ko | 1024 Ko[4] | 512 Ko | 1024 Ko | 1024 Ko[4] |
| | Vol. max. de données transférées redondantes liées à la sécurité | – | – | – | 512 Ko | 1024 Ko | 1024 Ko[5] |
| | Partagé : Global -> Sécurisé | 16 Ko | 16 Ko | 16 Ko | 16 Ko[2] | 16 Ko[2] | 16 Ko[2] |
| | Partagé : Sécurisé -> Global | 16 Ko | 16 Ko | 16 Ko | 16 Ko[2] | 16 Ko[2] | 16 Ko[2] |
| | Partagé : Global -> Process | 16 Ko | 16 Ko | 16 Ko | 16 Ko[2] | 16 Ko[2] | 16 Ko[2] |
| | Partagé : Process -> Global | 16 Ko | 16 Ko | 16 Ko | 16 Ko[2] | 16 Ko[2] | 16 Ko[2] |
| | Total stockage de données | 4 Go[6] | 4 Go[6] | 4 Go[6] | 4 Go[6] | 4 Go[6] | 4 Go[6] |

| Caractéristique | | | BME | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | P582040S | P584040S | P586040S | H582040S | H584040S | H586040S |
| Vitesse d'exécution des instructions | Tâches MAST et FAST : | | | | | | | |
| | | Booléen | 40 000 instructions / ms | 40 000 instructions / ms | 50 000 instructions / ms | 40 000 instructions / ms | 40 000 instructions / ms | 50 000 instructions / ms |
| | | Typé | 30 000 instructions / ms | 30 000 instructions / ms | 40 000 instructions / ms | 30 000 instructions / ms | 30 000 instructions / ms | 40 000 instructions/ms |
| | Tâche SAFE : | | | | | | | |
| | | Booléen | 40 000 instructions / ms | 40 000 instructions / ms | 40 000 instructions / ms | 40 000 instructions / ms[3] | 40 000 instructions / ms[3] | 40 000 instructions/ ms[3] |
| | | Typé | 30 000 instructions / ms | 30 000 instructions / ms | 30 000 instructions / ms | 30 000 instructions / ms[3] | 30 000 instructions / ms[3] | 30 000 instructions / ms[3] |

1. Pour les PAC redondants de sécurité M580, le rack local ne prend en charge aucun module d'E/S.

2. Ces données sont incluses dans les zones de données liées ou non liées à la sécurité.

3. Comme la tâche SAFE échange des données via l'embase, les performances en sont affectées. Il faut 1 ms pour transférer 10 Ko pour BMEH584040S et BMEH586040S, et 2 ms pour BMEH582040S.

4. Le volume Programme de l'application (non lié à la sécurité) + Données de l'application (données non liées à la sécurité et non conservées uniquement) + Programme de l'application (lié à la sécurité) + Données de l'application (liées à la sécurité) est inférieur à 64 Mo. La CPU BME•586040S embarque une mémoire globale de 64 Mo pour le programme et les données de l'application.

5. Le volume maximum de données redondantes transférées (liées et non liées à la sécurité) est de 4 Mo.

6. 2 Go sans carte mémoire externe.

# Alimentations de sécurité M580

## Présentation

Cette section décrit les alimentations de sécurité M580.

# Description physique des alimentations M580 de sécurité

## Utilisation dans la boucle de sécurité M580

L'alimentation de sécurité BMXCPS4002S, BMXCPS4022S ou BMXCPS3522S peut être utilisée uniquement dans un rack contenant des modules de sécurité. Vous pouvez utiliser l'alimentation de sécurité dans un X Bus ou un rack Ethernet situé dans :

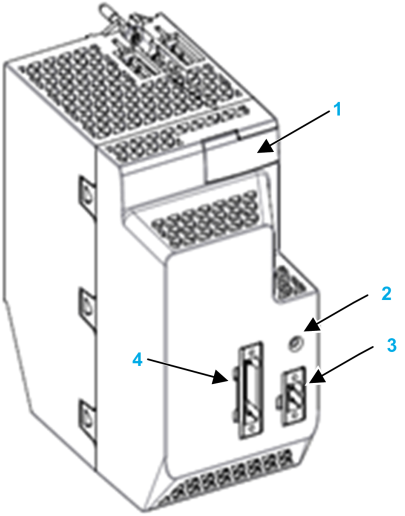
- un rack local principal
- un rack local d’extension
- un rack distant principal
- un rack distant d’extension

Vous pouvez utiliser deux modules d'alimentation de sécurité dans des racks Ethernet qui prennent en charge la redondance : L'alimentation de sécurité requiert deux emplacements de module, situés à l'extrême gauche du rack.

**NOTE:** Pour connaître la description des racks M580 disponibles, consultez la rubrique *Racks locaux et distants* dans le document *Modicon M580 - Manuel de référence du matériel*.

# Face avant de l'alimentation

La face avant des alimentations de sécurité M580 est illustrée ci-après :




**1** Voyants à LED

**2** Bouton RESET

**3** Contact de relais d'alarme

**4** Connecteur 5 broches d'alimentation d'entrée principale

# Voyants à LED

Les modules d'alimentation de sécurité M580 disposent du panneau de voyants illustré ci-après :


Les différents voyants sont :

- **OK** : Etat de fonctionnement
- **ACT** : Activité
- **RD** : Redondance

Chaque voyant peut avoir deux états : Allumé (vert) et Éteint.

Pour plus d'informations sur la signification de ces voyants en vue de diagnostiquer l'état de l'alimentation, reportez-vous à la rubrique *Voyants de diagnostic de l'alimentation* (voir Modicon M580 - Manuel de sécurité) dans le *Manuel de sécurité M580*.

# RESET

Lorsque vous appuyez sur le bouton **RESET** du module d'alimentation, tous les modules situés dans le même rack sont réinitialisés. Si le module d'alimentation de sécurité M580 se trouve dans le rack local principal, l'actionnement du bouton **RESET** entraîne la réinitialisation de la CPU.

**NOTE:** Dans une configuration redondante incluant deux modules d'alimentation de sécurité M580, vous pouvez appuyer sur le bouton RESET sur chacun des modules ou bien sur les deux modules pour exécuter la réinitialisation.

# Connexions de l'alimentation d'entrée

Voici les caractéristiques des broches de chaque alimentation de sécurité M580 :

- 5 points
- Connecteur débrochable :
  - sur le module : tête avec bride filetée
  - bornier enfichable avec bride vissée
- Pas : 5,08 mm
- Section de câble minimale : 0,5 $mm^2$ à 2 $mm^2$

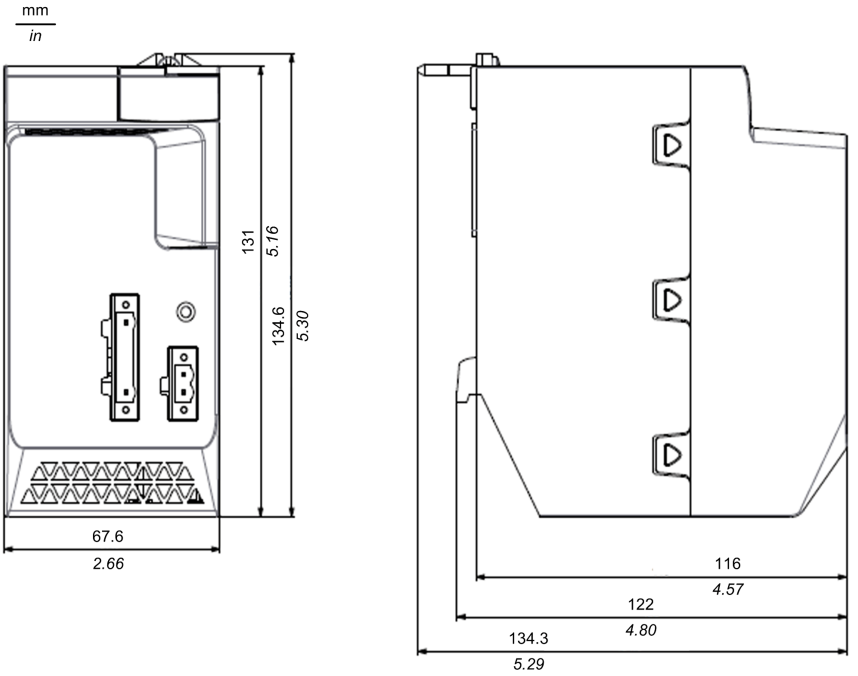
Alimentation d'entrée et affectation des broches pour chaque alimentation de sécurité M580 :

| **Description** | **BMXCPS4002S** | **BMXCPS4022S** | **BMXCPS3522S** |
|---|---|---|---|
| Alimentation d'entrée principale | 100 à 240 VCA | 24 à 48 VCC | 125 VCC |
| Broche 1 | NC | Ligne CC | NC |
| Broche 2 | NC | Ligne CC | NC |
| Broche 3 | PE | Neutre CC | PE |
| Broche 4 | Neutre CA | Neutre CC | Neutre CC |
| Broche 5 | Ligne CA | Terre | Ligne CC |

**NOTE:** Un bornier enfichable est livré avec le module.

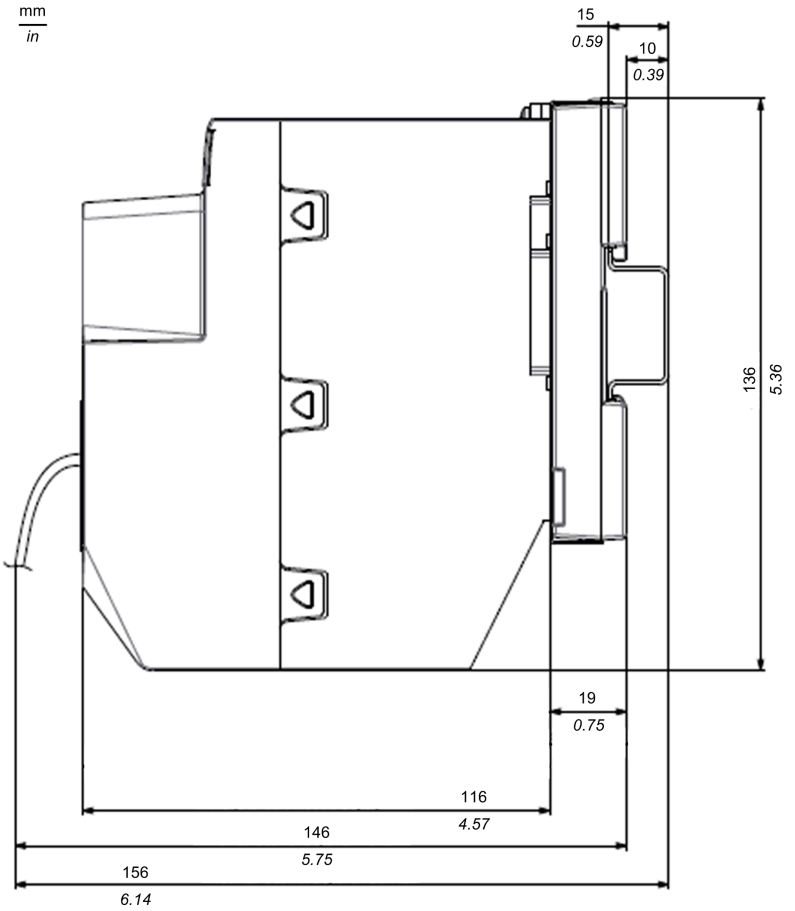
# Dimensions de l'alimentation

Dimensions des alimentations de sécurité M580 :



# Dimensions avec câblage de l'alimentation

Dimensions des alimentations de sécurité M580 en tenant compte du câblage :



# Caractéristiques de performance des alimentations M580 de sécurité

## Alimentation BMXCPS4002S de sécurité

Les caractéristiques des performances de l'alimentation de sécurité BMXCPS4002S sont les suivantes :

| **Caractéristiques des entrées** | | |
|---|---|---|
| Tension nominale | | 100 à 240 Vrms |
| Plage de tension | | 85 à 132 Vrms<br>170 à 264 Vrms |
| Plage de fréquence | | 47 à 63 Hz |
| Coupures de courant d'entrée masquée | | Max 10 ms à 100 Vrms - 15 % et à 200 Vrms - 15 % |
| Energie apparente d'entrée typique | | 130 VA |
| Courant d'entrée typique | | 1,1 Arms à 115 Vrms<br>0,55 Arms à 230 Vrms |
| Courant d'appel à 25°<br>au 1er démarrage à 25 °C | Crête | ≤ 60 A à 24 VCC<br>≤ 60 A à 48 VCC |
| | $I^2t$<br>(pour calibre du fusible externe) | ≤ X $A^2s$ à 24 VCC<br>≤ X $A^2s$ à 48 VCC |
| | It<br>(pour calibre du disjoncteur externe) | ≤ X As à 24 VCC<br>≤ X As à 48 VCC |
| Protection intégrée | | Fusible interne non accessible situé sur entrée L |

| **Caractéristiques des sorties** | | |
|---|---|---|
| Courant de sortie MAX 3V3_BAC | | 5,5 A (18,2 W) |
| Courant de sortie MAX 24V_BAC | | 1,67A (40W) |
| Puissance de sortie totale MAX | | 40W |
| Détection | Surcharge | Oui - Disjonction |
| | Court-circuit | Oui - Disjonction |
| | Surtension | Oui - Disjonction |

| **Autres caractéristiques** | | |
|---|---|---|
| Diélectrique | Primaire / Tous secondaires | SELV/PELV |
| Résistance | Primaire/terre | SELV/PELV |
| Résistance d'isolement | Primaire / Tous secondaires | 100 MΩ |
| | Primaire/terre | 100 MΩ |

# Alimentation du BMXCPS4022S de sécurité

| **Caractéristiques des entrées** | | |
|---|---|---|
| Tension nominale | | 24 à 48 VCC |
| Plage de tension d'entrée | | 18 à 62,4 VCC |
| Efficacité | | pertes max. ≤ 7 W (efficacité ≥ 84,8 %) sous une charge continue maximale, sur toute la plage de tension d'entrée et sur la plage de température |
| Courant d'entrée nominal | | 1,9 A à 24 VCC |
| | | 1 A à 48 VCC |
| Courant d'appel au premier démarrage à 25 °C | Courant de crête | ≤ 60 A à 24 VCC |
| | | ≤ 60 A à 48 VCC |
| | $I^2t$ (pour calibre du fusible externe) | ≤ X $A^2s$ à 24 VCC |
| | | ≤ X $A^2s$ à 48 VCC |
| | It (pour calibre du disjoncteur externe) | ≤ X As à 24 VCC |
| | | ≤ X As à 48 VCC |
| Coupures de courant d'entrée masquées | | Coupures de courant d'entrée durant au maximum : |
| | | • 1 ms en pleine charge et pour une tension de ligne minimale (soit 19,2 VCC) |
| | | • 10 ms en pleine charge et pour une tension de ligne nominale (soit 24 ou 48 VCC) |
| | | Sans incidence sur les caractéristiques de sortie. Période entre deux interruptions d'1 seconde. |
| Protection d'entrée | | • Protection contre le risque d'incendie : fusible monté sur la carte, non accessible, non remplaçable par l'utilisateur, sur l'entrée DC+. Le niveau de protection est sélectionné conformément aux normes de sécurité. La protection ne doit en aucun cas être endommagée lors des tests de résistance au bruit sur la ligne. |

| **Caractéristiques des entrées** | |
|---|---|
| | • Protection contre l'inversion de polarité d'entrée : un circuit intégré doit protéger le module. Le ou les fusibles internes (et éventuellement externes) ne doivent pas sauter. L'alimentation doit démarrer correctement après le rétablissement de la polarité adéquate. |

| **Caractéristiques des sorties :** | |
|---|---|
| Tension nominale de sortie | 24,35 V |
| Plage de tension de sortie (état stationnaire) | 23,3 à 24,7 V sur l'intégralité de la plage de tension d'entrée, de la plage de charge de sortie et de la plage de température |
| Ondulation et bruit en sortie | 240 mV crête à crête (mesure effectuée avec une bande passante ≥ 100 MHz, sur les broches du connecteur du module) |
| Plage de courant de sortie continu | • 1,63 A maximum |
| | • 0 A minimum |
| Courant de sortie transitoire | 1,9 A maximum pendant 500 ms, période de 20 secondes minimum |
| Impédance de sortie et fréquence | 180 mΩ |
| Tension de sortie avec charge transitoire sur 24V_BAC | Charge de sortie transitoire sur 24V_BAC : |
| | • Variation de charge I entre la limite minimale du courant de sortie continu et la limite maximale du courant de sortie transitoire (et inversement). |
| | • Temps de transition 4 µs – largeur d'impulsion 500 ms – période 20 s. |
| | • La tension de sortie transitoire sur 24V_BAC doit être comprise entre 23 et 25 V. Temps de réponse : ≤ 50 ms. |
| | • Pour toute charge capacitive sur 24V_BAC respectant les limites indiquées. |
| Protection contre les courts-circuits et surcharges en sortie | • En cas de court-circuit ou de surcharge sur 24V_BAC (peu importe le niveau, la durée, la température et la tension d'entrée), la carte doit être protégée contre d'éventuels dommages. |
| | • La valeur maximum globale du seuil de détection de surcharge (y compris toutes les tolérances, dérives, etc.) doit être inférieure à Imax. |
| | • Imax = 2 A. |
| Protection contre les surtensions | Disjonction de l'alimentation pour une montée à 30 VCC ±0,8 V de la sortie. |
| Charge capacitive externe | Toutes les conditions ci-dessus doivent être remplies avec la charge capacitive externe suivante, notamment pour assurer la courbe ascendante, la stabilité de la boucle de régulation, la détection des surcharges et la protection contre ces surcharges. |

| **Caractéristiques des sorties :** | |
|---|---|
| | Charge capacitive de 11 500 µF. |

# Alimentation de sécurité BMXCPS3522S

| **Caractéristiques des entrées :** | | |
|---|---|---|
| Tension nominale | | 125 VCC |
| Plage de tension d'entrée | | 100 à 150 VCC |
| Efficacité | | pertes max. ≤ 7 W (efficacité ≥ 84,8 %) sous une charge continue maximale, sur toute la plage de tension d'entrée et sur la plage de température |
| Courant d'entrée nominal | | 0,6 A à 125 VCC |
| Courant d'appel au premier démarrage à 25 °C | Courant de crête | ≤ 60 A à 125 VCC |
| | $I^2t$ (pour calibre du fusible externe) | ≤ 0,15 $A^2s$ à 125 VCC |
| | It (pour calibre du disjoncteur externe) | ≤ 0,025 As à 4 VCC |
| Coupures de courant d'entrée masquées | | Coupures de courant d'entrée durant au maximum : |
| | | • 1 ms en pleine charge et pour une tension de ligne minimale (soit 100 VCC) |
| | | • 10 ms en pleine charge et pour une tension de ligne nominale (soit 125 VCC) |
| | | Ne doivent pas avoir d'incidence sur les caractéristiques de sortie. Période entre deux interruptions d'1 seconde. |
| Protection d'entrée | | • Protection contre le risque d'incendie : fusible monté sur la carte, non accessible, non remplaçable par l'utilisateur, sur l'entrée DC+. Le calibre est sélectionné conformément aux normes de sécurité. La protection ne doit en aucun cas être endommagée lors des tests de résistance au bruit sur la ligne. |
| | | • Protection contre l'inversion de polarité d'entrée : un circuit intégré doit protéger le module. Le ou les fusibles internes (et éventuellement externes) ne doivent pas sauter. L'alimentation doit démarrer correctement après le rétablissement de la polarité adéquate. |

| | **Alimentation haute puissance BMXCPS3522 /S** |
|---|---|
| Tension nominale de sortie | 24,35 V |
| Plage de tension de sortie (état stable) | 23,3 à 24,7 V sur l'intégralité de la plage de tension d'entrée, de la plage de charge de sortie et de la plage de température |
| Ondulation et bruit en sortie | 240 mV crête à crête (mesure effectuée avec une bande passante ≥ 100 MHz, sur les broches du connecteur du module) |
| Plage de courant de sortie continu | • 1,63 A maximum |
| | • 0 A minimum |
| Courant de sortie transitoire | 1,9 A maximum pendant 500 ms, période de 20 secondes minimum |
| Impédance de sortie et fréquence | 180 mΩ |
| Tension de sortie avec charge transitoire sur 24V_BAC | Charge de sortie transitoire sur 24V_BAC : |
| | • Variation de charge I entre la limite minimale du courant de sortie continu et la limite maximale du courant de sortie transitoire (et inversement). |
| | • Temps de transition 4 µs – largeur d'impulsion 500 ms – période 20 s. |
| | • La tension de sortie transitoire sur 24V_BAC doit être comprise entre 23 et 25 V. Temps de réponse : ≤ 50 ms. |
| | • Pour toute charge capacitive sur 24V_BAC respectant les limites indiquées. |
| Protection contre les courts-circuits et surcharges en sortie | • En cas de court-circuit ou de surcharge sur 24V_BAC (peu importe le niveau, la durée, la température et la tension d'entrée), la carte doit être protégée contre d'éventuels dommages. |
| | • La valeur maximum globale du seuil de détection de surcharge (y compris toutes les tolérances, dérives, etc.) doit être inférieure à Imax. |
| | • Imax = 2 A. |
| Protection contre les surtensions | Disjonction de l'alimentation pour une montée à 30 VCC ±0,8 V de la sortie. |
| Charge capacitive externe | Toutes les conditions ci-dessus doivent être remplies avec la charge capacitive externe suivante, notamment pour assurer la courbe ascendante, la stabilité de la boucle de régulation, la détection des surcharges et la protection contre ces surcharges. |
| | Charge capacitive de 11 500 µF. |

# Relais d'alarme des alimentations de sécurité M580

## Performances

Le bornier de relais d'alarme des alimentations de sécurité M580 présente les performances suivantes :

| **Caractéristiques** | |
|---|---|
| Courant/Tension de commutation nominal | 24 VCC, 2 A (charge résistive) |
| | 240 VCA, 2 A (cos φ =1) point |
| Charge de commutation minimum | 5 VCC, 1 mA |
| Tension maximum de commutation | 62,4 VCC |
| | 264 VCA |
| Type de contact | Normalement ouvert |
| Temps d'ouverture/de fermeture du contact | |
| • OFF → ON | 10 ms maximum |
| • ON → OFF | 12 ms maximum |
| Protection intégrée | Contre les surcharges et les courts-circuits : aucune. Insérez un fusible à fusion rapide. |
| | Contre les surtensions inductives en CA : aucune. Utilisez un circuit RC ou un suppresseur MOV (ZNO) (approprié par rapport à la tension) en parallèle sur chaque pré-actionneur. |
| | Contre les surtensions inductives en CC : aucune. Insérez une diode de décharge sur chaque pré-actionneur. |
| Rigidité diélectrique | Contact/terre : 2 000 Veff, 50 Hz, 1 min(altitude de 0 à 2 000 m) |
| Résistance d'isolement | 10 MΩ ou plus sous 500 VCC |

# Modules d'E/S de sécurité M580

## Présentation

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

# Description physique des modules d'E/S de sécurité M580

## Présentation

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

## Description physique des modules d'E/S M580

### Positionnement des modules d'E/S de sécurité

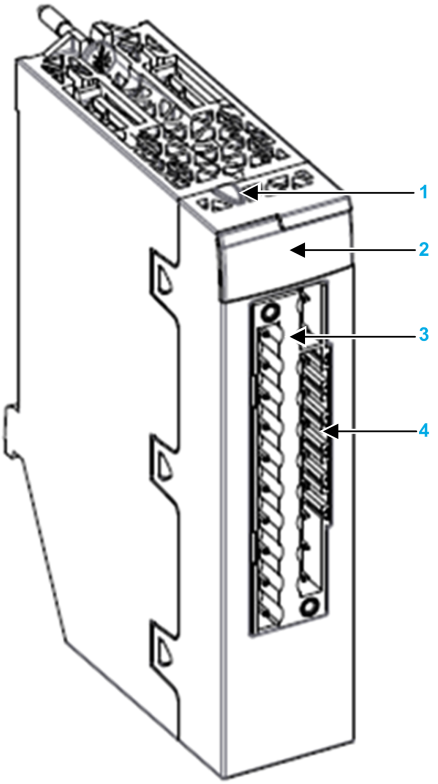
Vous pouvez installer un module d'E/S de sécurité M580 :

- Dans le rack local, dans tout emplacement non réservé à l'alimentation ou à la CPU.
- Dans un rack distant, dans tout emplacement non réservé à l'alimentation ou à l'adaptateur distant.

  **NOTE:** Un module d'E/S de sécurité peut être installé soit dans un rack X Bus BMXXBP•••• soit dans un rack Ethernet BMEXBP••••. Pour connaître la description des racks M580 disponibles, consultez la rubrique *Racks locaux et distants* dans le document *Modicon M580 - Manuel de référence du matériel*.

# Face avant du module d'E/S de sécurité

Caractéristiques de la face avant de chaque module d'E/S de sécurité :




**1** Bouton de verrouillage/déverrouillage de la configuration

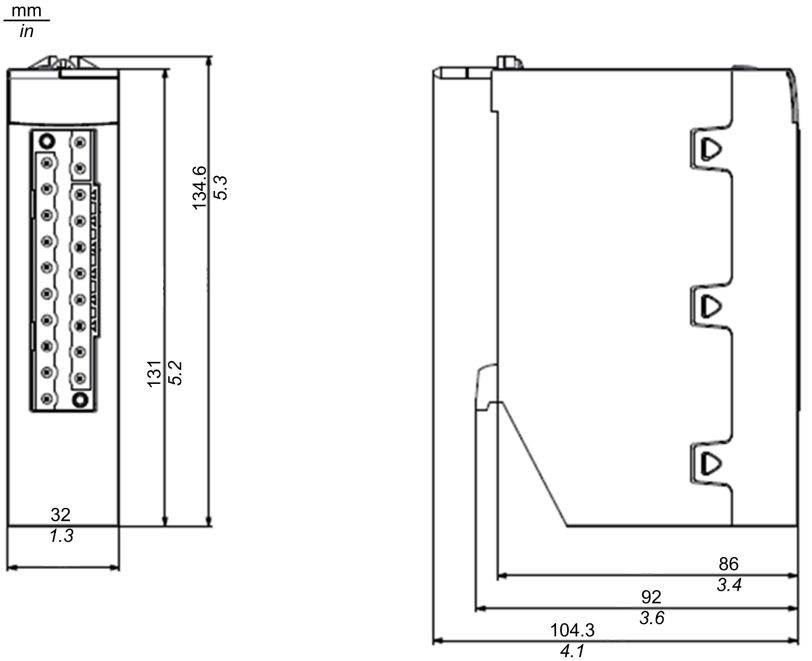
**2** Voyants

**3** Connecteur 20 broches

**4** Emplacements des broches de détrompage

# Dimensions des modules d'E/S de sécurité

Dimensions physiques de chaque module d'E/S de sécurité :

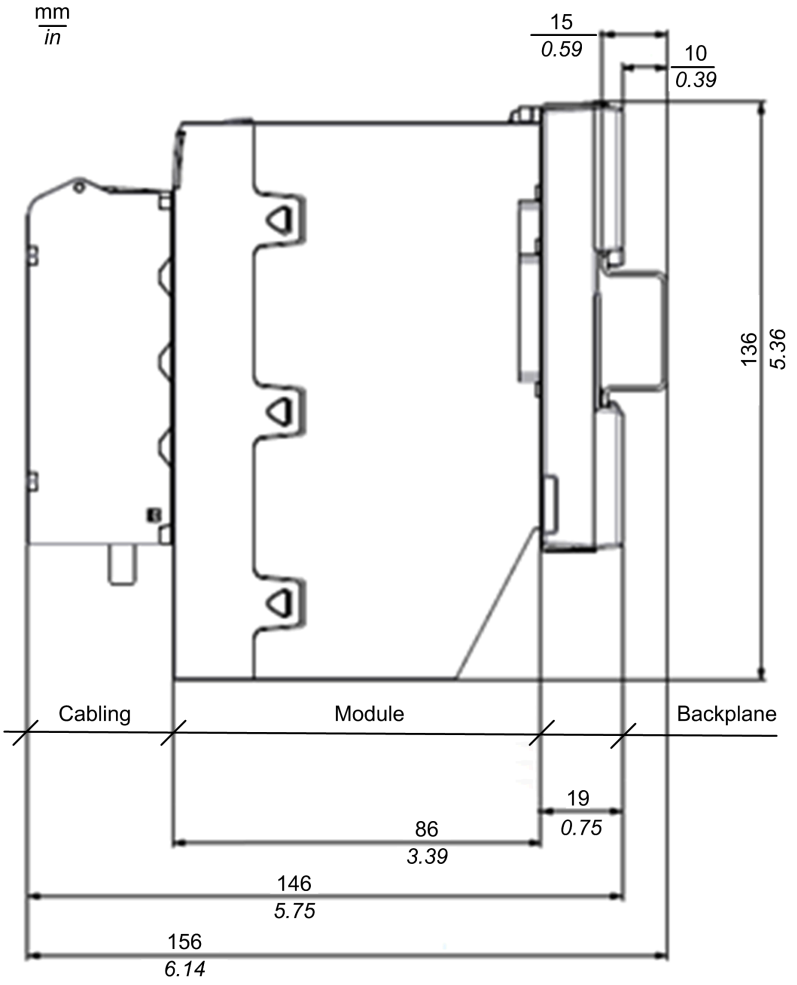



**NOTE:** Tenez compte de la hauteur de chaque module d'E/S de sécurité lors de la planification de l'installation d'un rack. Chaque module d'E/S dépasse le bord inférieur du rack de :

- 29,49 mm (1,161 in.) dans le cas d'un rack Ethernet.
- 30,9 mm (1,217 in.) dans le cas d'un rack X Bus.

# Dimensions du câblage d'E/S de sécurité

Dimensions physiques du câblage de chaque module d'E/S de sécurité :




# Voyants LED

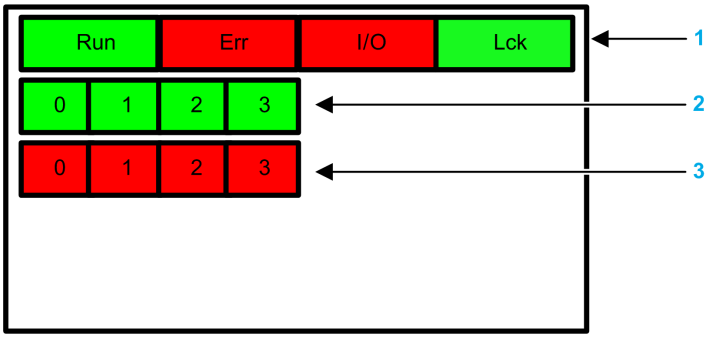
Chaque module d'E/S de sécurité comporte en face avant des voyants LED de diagnostic du module et des canaux :

- Les quatre voyants LED situés en haut (**Run**, **Err**, **I/O** et **Lck**) indiquent l'état du module.

- Les voyants situés en bas associés aux 4 voyants du haut indiquent l'état et l'intégrité de chaque canal d'entrée ou de sortie.

  **NOTE:** Pour plus d'informations sur l'utilisation des voyants LED pour diagnostiquer l'état des modules de sécurité M580, consultez la section *Diagnostics* dans le document *M580 - Manuel de sécurité*.

Voyants LED du module d'entrées analogiques de sécurité BMXSAI0410 et du module de sorties relais numériques de sécurité BMXSRA0405 :

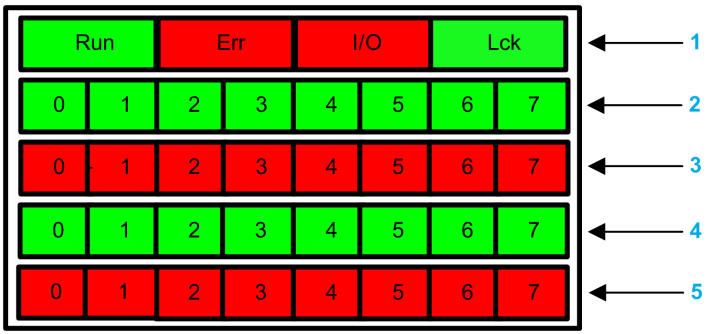



**1** Voyants d'état du module

**2** Voyants d'état des canaux

**3** Voyants d'erreur de canal

Voyants du module d'entrées numériques de sécurité BMXSDI1602 :




**1** Voyants d'état du module

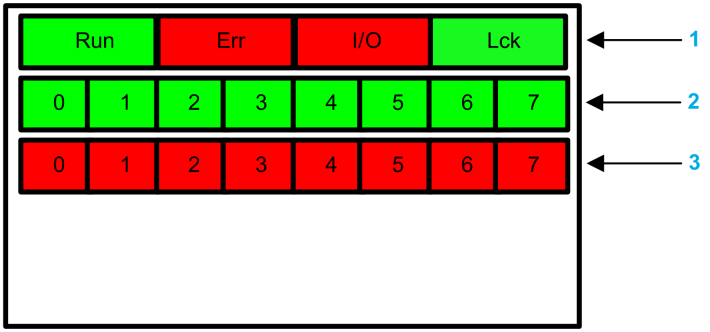
**2** Voyants d'état des canaux (rang A)

**3** Voyants d'erreur des canaux (rang A)

**2** Voyants d'état des canaux (rang B)

**3** Voyants d'erreur des canaux (rang B)

Voyants du module de sorties numériques de sécurité BMXSDO0802 :




**1** Voyants d'état du module

**2** Voyants d'état des canaux

**3** Voyants d'erreur de canal

# Caractéristiques des performances des modules d'E/S de sécurité M580

## Présentation

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

## Caractéristiques de performance des modules d'entrées analogiques de sécurité BMXSAI0410

### Caractéristiques des modules d'entrées analogiques

Les caractéristiques des performances des modules d'entrées analogiques de sécurité BMXSAI0410 sont les suivantes :

| **Caractéristiques statiques** | | **Valeur** |
|---|---|---|
| Impédance d'entrée dans la plage de signal | | 286 Ω |
| Erreur d'entrée analogique | Erreur taille réelle max. à 25 °C | 0,30 % |
| Erreur d'entrée analogique (= tolérance de sécurité) | Erreur maxi. de pleine échelle sur la totalité de la plage de températures - 25 °C à 70 °C | 0,35 % |
| Fiabilité | MTTF à 25 °C | 54,2 ans |
| Plage de mesure linéaire | | 0 à 25 mA et 12 500 comptes (500 ct/mA) |
| Détection hors plage | | < 3,75 mA et > 20,75 mA |
| Résolution numérique | Résolution | 16 bits |
| | Nombre de canaux simultanément convertis | 4 |
| Format de données renvoyé par le programme d'application | | binaire |
| Valeur d'un LSB | | 0,191 µA |
| Surcharge maximale permanente autorisée | | 25 mA |
| Lecture de sorties numériques dans condition de surcharge | La surcharge est signalée à l'application client | I = 25 mA |
| Type d'entrée | Type | 4-20 mA |

| **Caractéristiques statiques** | | **Valeur** |
|---|---|---|
| | Type | Entrées isolées flottantes |
| | Plage maximale d'entrée | 0-25 mA |
| Caractéristiques en mode commun | Réjection du mode commun | à mesurer |

| **Caractéristiques dynamiques** | | **Valeur** |
|---|---|---|
| Caractéristiques du filtre d'entrée | ordre | seconde |
| | Fréquence de coupure à -3 dB | 10,47 Hz |

| **Caractéristiques générales** | | **Valeur** |
|---|---|---|
| Méthode de conversion | | Approximation successive |
| Type de protection | | Diode de protection |
| Potentiel d'isolement en fonctionnement normal | Isolement entre canaux | 500 VCA eff. pendant 1 min. |
| | Isolement canal à embase | 1500 VCA eff. pendant 1 min. |
| Données d'alimentation externe - si nécessaire | | Non requis |
| Type et longueur de câble - règles d'installation pour fournir une immunité aux interférences | | câble blindé |
| Etalonnage ou vérification pour maintenir la précision nominale | | pas d'étalonnage |
| Exemples typiques de connexions externes | | Capteur de température et de pression |

| **Caractéristiques supplémentaires** | | **Valeur** |
|---|---|---|
| Monotonicité sans code manquant | | oui |
| Diaphonie entre CC & CA 50 Hz et CA 60 Hz | | – |
| Non-linéarité | +/- | 0,006 % (LSB) |
| Répétabilité à température constante après temps de stabilisation défini | | – |
| Consommation 3,3 V | Typique | 223 mA |
| | Maximum | 256 mA |
| Consommation 24V | Typique | 92 mA |
| | Maximum | 115 mA |
| Dissipation de puissance | Maximum | 3,98 W |

# Caractéristiques de performance des modules d'entrées numériques de sécurité BMXSDI1602

## Caractéristiques des modules d'entrées numériques

Les caractéristiques des performances des modules d'entrées numériques de sécurité BMXSDI1602 sont les suivantes :

| **Caractéristique** | | **Valeur** |
|---|---|---|
| Entrée nominale | Tension | 24 VCC |
| Alimentation de capteur externe | SELV/PELV, surtension II | (Maxi. 60 V) |
| Courant d'entrée typique | Courant | 3,2 mA |
| Valeurs limites d'entrée | Tension à l'état 1 | ≥ 11 V |
| | Tension à l'état 0 | ≤ 5 V |
| | Courant à l'état 1 | > 2 mA pour U ≥ 11 V |
| | Courant à l'état 0 | < 1,5 mA |
| | Alimentation du capteur<br>(Ondulation incluse) | De 19 à 30 V (Jusqu'à 33 V possible dans la limite de 1 heure par jour) |
| Impédance d'entrée | A la tension typique | 7,5 KΩ |
| Durée de réponse | Typique/Maximum | 100 µs / 250 µs |
| Fiabilité | MTTF à Tamb = 25 °C | 31,5 ans |
| Inversion de polarité | | Protégée |
| IEC 61131-2 - Edition 3.0 (2007) | | Type 3 |
| Compatibilité | (Capteurs de proximité 2 fils, 3 fils) | IEC 947-5-2 |
| Rigidité diélectrique | Primaires/secondaires | 1500 Vrms (à 4000 m) 50/60 Hz pendant 1 minute |
| Résistance d'isolation | | > 10 MΩ (à 500 VCC) |
| Type d'entrée | | Commun plus |
| Parallélisation des entrées (1) | | Oui |
| Tension des capteurs<br>Surveillance de seuil | OK | > 18,6 VCC<br>< 32 VCC |
| | Hors plage de fonctionnement | < 18,6 VCC<br>> 33 VCC |

| Caractéristique | | Valeur |
|---|---|---|
| Temps de réponse surveillance de tension de capteur | À la disparition | 4,4 ms < T < 30 ms |
| | À l'apparition | 0,18 ms < T < 0,3 ms |
| Capacité externe maximale lors de l'utilisation de VS pour détection de court-circuit sur 24 V | Maximum | 80 nF |
| Consommation 3,3 V | Typique | 200 mA |
| | Maximum | 256 mA |
| Consommation 24V | Typique | 63 mA |
| | Maximum | 100 mA |
| Puissance dissipée max. | | 3,57 W |
| **(1)** Cette caractéristique permet de câbler plusieurs entrées sur un même module ou bien sur des modules différents si des entrées redondantes sont nécessaires. | | |

# Caractéristiques de performance des modules de sorties numériques de sécurité BMXSDO0802

## Caractéristiques des modules de sorties numériques

Les caractéristiques des performances des modules de sorties numériques de sécurité BMXSDO0802 sont les suivantes :

| Caractéristique | | Valeur |
|---|---|---|
| Valeurs nominales | Tension | 24 VCC |
| | Courant | 0,5 A |
| Valeurs de limite | Tension | 19 à 30 V(1) |
| | Courant/canal | 0,625 A |
| | Courant/module | 5 A |
| Type d'alimentation d'actionneur externe | | SELV/PELV (60 V maxi.), catégorie de surtension II |
| Puissance d'ampoule à filament de tungstène | max | 6 W |
| Courant de fuite | A l'état 0 | < 0,5 mA |

| **Caractéristique** | | **Valeur** |
|---|---|---|
| Tension résiduelle | A l'état 1 | < 1,2 V |
| Protections | Tension transitoire | oui |
| | Courant de disjonction de surcharge | > 0,625 A |
| | Court-circuit | oui |
| | Polarité incorrecte | oui |
| | Surchauffe | oui |
| Charge minimum Valeur de résistance (pour pré-actionneur) | | 48 Ω |
| Détection complète de rupture de câble : Valeur maximale de la capacité de charge du câble (y compris la capacité des pré-actionneurs) entre la sortie et le pré-actionneur | | 10 nF |
| Temps de réponse(2) | | 1,2 ms |
| Fiabilité : MTTF | | 45,8 ans à 25 °C |
| Fréquence de commutation sur charge inductive | | 0,5 / LI²Hz avec Fmax = 2 Hz |
| Mise en parallèle des sorties | | Oui (2 maximum) |
| Compatibilité avec entrées CC | | Oui (uniquement logique positive de type 3 ou non IEC) |
| Protection intégrée | Contre les surtensions | Oui - TVS interne |
| | Contre l'inversion de polarité | Oui - montage inversé de diode Prévoir un fusible pour le 24 V du pré-actionneur. |
| | Contre courts-circuits et surcharges | Oui, par limiteur de courant et disjoncteur électronique 1,5 In < Id < 2 In |
| Tension préactionneur 24 V<br>Surveillance de seuil | OK | > 19,0 V et < 31,8 V |
| | Hors plage de fonctionnement | < 18,0 V et > 31,8 V |
| Temps de réponse de la surveillance de tension pré-actionneur | À la disparition | 2 ms < T < 5,6 ms |
| | À l'apparition | 10 ms < T < 15,6 ms |
| Consommation 3,3 V | Typique | 240 mA |
| | Maximum | 264 mA |
| Consommation embase 24 V | Typique | 80 mA |
| | Maximum | 90 mA |
| Consommation préactionneur 24 V | Typique | 5 mA |

| Caractéristique | | Valeur |
|---|---|---|
| (sans courant de charge) | Maximum | 15 mA |
| Puissance dissipée | | 4,4 W max |
| Rigidité diélectrique (sortie/terre ou logique interne) | | 1500 Vrms, 50/60 Hz pendant 1 min |
| Résistance d'isolement | | > 10 MΩ à 500 VCC |
| **(1)** 33 V admissible pendant 1 heure par 24 h.<br>**(2)** Toutes les sorties disposent de circuits de démagnétisation rapide pour les électro-aimants. Temps de décharge des électro-aimants < L/R. | | |

# Module de sorties relais numériques de sécurité BMXSRA0405

## Caractéristiques des modules de sorties relais numériques

Les caractéristiques des performances des modules de sorties relais numériques de sécurité BMXSRA0405 sont les suivantes :

| Caractéristique | | Valeur |
|---|---|---|
| Tension/courant de commutation nominal | | 24 VCC 5 A (charge résistive) |
| | | 240 VCA 5 A (cos Φ = 1) |
| Courant max pour les contacts sur charge résistive | | 5 A (DC12 et AC12) |
| Courant max pour les contacts sur charge inductive | | 4A DC13 et 3A AC15 |
| Température de service | | 0 à 60 °C |
| Type d'alimentation d'actionneur externe | | Surtension catégorie II |
| Charge de commutation min | | 5 VCC, 10 mA |
| Charge de commutation max | | 264 VCA 30 VCC |
| Durée de commutation | OFF→ ON (marche) | 12 ms en général |
| | ON →OFF (désactivation) | 6 ms en général |
| Durée de vie (selon relais Elesta SIF3) | Mécanique | 10 millions de cycles ou plus |
| | Electrique | DC12 24 VCC / 5 A → 300 000 cycles |
| | | DC12 24 VCC / 2 A → 500 000 cycles |

| **Caractéristique** | | **Valeur** |
|---|---|---|
| | | DC12 24 VCC / 1 A → 1 000 000 cycles |
| | R/L = 40 s | DC13 24 VCC (0,1 Hz) / 4A → 30 000 cycles |
| | | DC13 24 VCC (0,1 Hz) / 2 A → 50 000 cycles |
| | | DC13 24 VCC (0,1 Hz) / 1 A → 80 000 cycles |
| | – | AC12 250 VCA / 5 A → 70 000 cycles |
| | | AC12 250 VCA / 2 A → 30 000 cycles |
| | | AC12 250 VCA / 1 A → 250 000 cycles |
| | – | AC15 250 VCA / 3A → 40 000 cycles |
| | | AC15 250 VCA / 2 A → 80 000 cycles |
| | | AC15 250 VCA / 1 A → 80 000 cycles |
| Protection intégrée | Contre surcharges et courts-circuits | Aucune - un fusible rapide doit être installé sur chaque canal ou groupe de canaux. |
| | Contre surtensions inductives ~ | Aucune - un circuit RC ou un écrêteur MOV (ZNO) adapté à la tension doit être installé en parallèle sur les bornes de chaque préactionneur. |
| | Contre les surtensions inductives = | Aucune - une diode de décharge doit être installée sur les bornes de chaque préactionneur. |
| Fréquence de commutation max | | 5 cycles par seconde |
| Tension diélectrique maximale entre les canaux | | 3 000 V eff. et 50/60 Hz pendant 1 min |
| Tension diélectrique maximale entre les canaux et l'embase | | 3 000 V eff. et 50/60 Hz pendant 1 min |
| Isolement renforcé | | Isolement de 3 000 VCA entre la partie process (contact de relais) et l'embase |
| Résistance d'isolement | | > 10 MW ou plus par testeur de résistance d’isolement |
| Fiabilité : MTTF à Tamb = 25°C | | 36,9 ans |
| Degré de protection | | IP20 |
| Consommation 3,3 V | Typique | 215 mA |
| | Maximum | 240 mA |
| Consommation courant interne relais 24 V | Typique | 95 mA |
| | Maximum | 130 mA |
| Puissance dissipée | 4 relais alimentés | 3 W typique, 3,9 W maximum |

# Installation du PAC de sécurité M580

## Présentation

Cette section explique comment installer le PAC de sécurité M580.

**NOTE:** Pour plus d'informations sur l'installation des PAC M580, consultez la rubrique *Installation d'un rack local* dans le document *Modicon M580 - Manuel de référence du matériel*.

# Installation de racks et modules d'extension M580

## Présentation

Cette section décrit l'installation d'un rack et de modules d'extension M580 pour un PAC de sécurité M580.

## Planification de l'installation du rack local

### Introduction

La taille et le nombre des racks ainsi que le type des modules qui y sont installés sont des points importants à prendre en compte lors de la planification d'une installation. Cette installation peut être effectuée dans un boîtier ou à l'extérieur. La hauteur, la largeur et la profondeur de la tête de système et l'espacement entre rack local et rack d'extension sont des notions importantes.

**⚠AVERTISSEMENT**

**FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT**

Installez les racks sur le plan horizontal longitudinal pour faciliter la ventilation.

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

Les modules tels que l'alimentation, la CPU, le coprocesseur et les E/S sont refroidis par convection naturelle. Installez-les sur un rack horizontal comme expliqué dans ce manuel pour assurer le refroidissement nécessaire. Les autres positions de montage de rack peuvent provoquer une surchauffe et donc un comportement inattendu de l'équipement.

### Utilisation des racks

Les racks disponibles dans Control Expert et leur utilisation autorisée sont décrits ci-dessous :

| Référence | Emplacements | Bus | Utilisation | | | |
|---|---|---|---|---|---|---|
| | | | Rack principal local | Rack d'extension local | Rack principal distant | Rack d'extension distant |
| **Racks BME :** | | | | | | |
| BME XBP 0400 | 4 | XBus et Ethernet | x | x | x | x |
| BME XBP 0800 | 8 | XBus et Ethernet | x | x | x | x |
| BME XBP 1200 | 12 | XBus et Ethernet | x | x | x | x |
| BME XBP 1600 | 16 | XBus et Ethernet | x | x | x | x |
| BME XBP 0602 | 6 | XBus et Ethernet | x | x | x | x |
| BME XBP 1002 | 10 | XBus et Ethernet | x | x | x | x |
| BME XBP 1402 | 14 | XBus et Ethernet | x | x | x | x |
| **Racks BMX :** | | | | | | |
| BMX XBP 0400 | 4 | XBus | – | x | x | x |
| BMX XBP 0600 | 6 | XBus | – | x | x | x |
| BMX XBP 0800 | 8 | XBus | – | x | x | x |
| BMX XBP 1200 | 12 | XBus | – | x | x | x |
| BMX XBP 1600 | 16 | XBus | – | x | x | x |
| **Racks Premium :** | | | | | | |
| **NOTE:** Les PAC de sécurité M580 ne prennent pas en charge les racks Premium. | | | | | | |
| **Racks Quantum :** | | | | | | |
| 140 XBP 002 00 | 2 | Quantum | – | – | x | x |
| 140 XBP 003 00 | 3 | Quantum | – | – | x | x |
| 140 XBP 004 00 | 4 | Quantum | – | – | x | x |
| 140 XBP 006 00 | 6 | Quantum | – | – | x | x |
| 140 XBP 010 00 | 10 | Quantum | – | – | x | x |
| 140 XBP 016 00 | 16 | Quantum | – | – | x | x |
| X : Autorisé<br>– : Non autorisé | | | | | | |

## Dégagement autour des racks

Ménagez un espace minimum de 12 mm (0,472 po.) sur le côté droit de chaque rack pour permettre le refroidissement.

Si votre plan inclut des racks d'extension, prévoyez un espace minimum de 35 mm (1,378 po.) devant les modules. Le module d'extension de rack BMX XBE 1000 a besoin de ce dégagement pour le connecteur et la terminaison du bus local.

## Espacement requis pour une CPU M580 dans un rack principal local

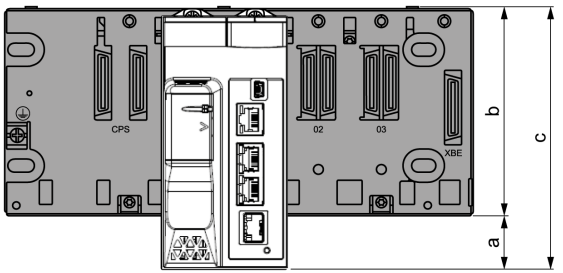
**⚠AVERTISSEMENT**

**SURCHAUFFE ET FONCTIONNEMENT INATTENDU DE L'ÉQUIPEMENT**

Lorsque vous installez les racks, prévoyez des dégagements suffisants pour le refroidissement.

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

Dans le rack local principal, prévoyez un dégagement supplémentaire au fond du rack pour la CPU. Cette illustration indique les dimensions de montage en cas d'utilisation d'un rack X Bus ou Ethernet. La hauteur totale du rack local principal est dans les deux cas de 134,6 mm (5,299 po.).




**a** Espace supplémentaire sous le rack pour tenir compte de la hauteur du module CPU. Pour un rack X Bus, la valeur est 32,0 mm (1,260 po.) ; pour un rack Ethernet la valeur est 30,59 mm (1,204 po.).

**b** Hauteur du rack. Pour un rack X Bus, la hauteur est de 103,7 mm (4,083 po.) ; pour un rack Ethernet, la hauteur est de 105,11 mm (4,138 po.).

**c** Hauteur du rack local principal : 135,7 mm (5,343 po.).

# Remarques concernant la température à l'intérieur d'un boîtier

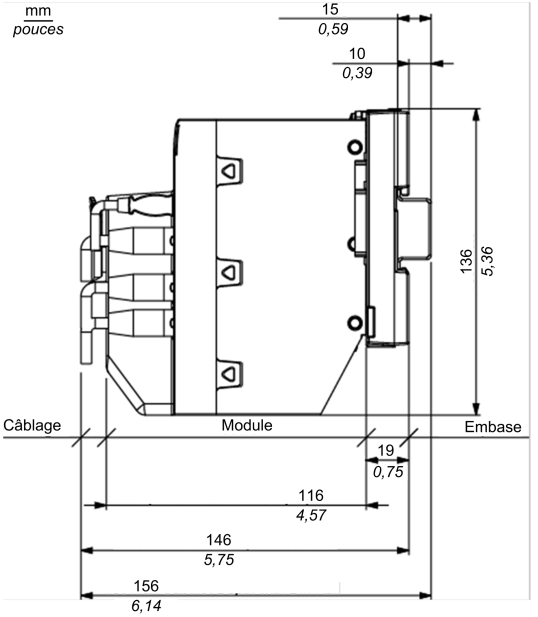
Si les racks sont installés dans un boîtier, il est nécessaire de faciliter la circulation d'air. Utilisez un boîtier permettant les dégagements minimaux suivants :

- 80 mm (3,15 po.) au-dessus des modules installés sur le rack
- 60 mm (2,36 po.) au-dessous des modules installés sur le rack
- 60 mm (2,36 po.) entre les modules et les goulottes de câbles

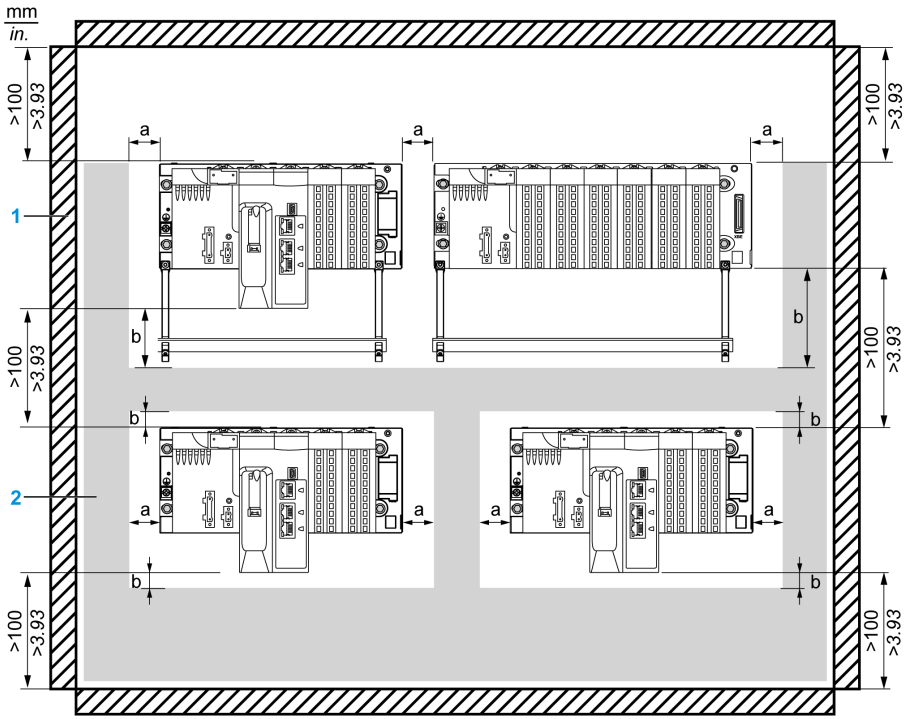
Profondeur minimale du boîtier :

- 150 mm (5,91 po.) si le rack est fixé sur une platine
- 160 mm (6,30 po.) si le rack est monté sur un rail DIN de 15 mm (0,59 po.)
- Si des modules d'extension de rack BMX XBE 1000 sont connectés, utilisez des câbles BMX XBC •••K avec connecteurs à 45°.

Voici une vue latérale d'un rack monté sur rail DIN avec modules et câbles en boîtier :



La figure suivante indique les règles d'installation standard à respecter dans une armoire avec goulottes de câbles :




**1** Appareillage ou enveloppe

**2** Goulotte ou lyre de câblage

**a** Dégagement latéral : > 40 mm (1,57 po.)

**b** Dégagement en haut et en bas avec les objets environnants : > 20 mm (0,79 po.)

**NOTE:** Pour gagner de l'espace, il est possible de rapprocher les racks, aux conditions suivantes :

- Aucune barre de blindage ou gaine ne se trouve entre les racks.
- L’espace entre les racks est d'au moins 40 mm (1,57 po.).
- Vous appliquez une réduction de 5 °C (9 °F) à la température ambiante maximale autorisée, soit 55 °C (131 °F) pour les modules standard et avec revêtement enrobant et 65 °C (149 °F) pour les versions renforcées.

# Montage des racks

## Présentation

Les racks Ethernet et X Bus peuvent être montés sur :

- des rails DIN,
- des murs,
- des platines perforées Telequick.

**NOTE:** montez les racks sur une surface métallique correctement reliée à la terre pour permettre au système PAC de fonctionner convenablement en présence d'interférences électromagnétiques.

**NOTE:** Les vis de montage à gauche de l'embase sont accessibles sans qu'il soit nécessaire de débrancher le module d'alimentation. Montez l'embase à l'aide du trou de fixation situé à l'extrême gauche du panneau.

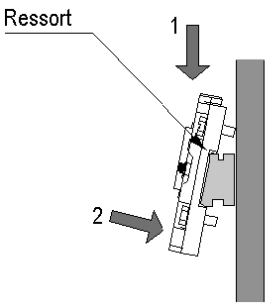
## Montage sur rail DIN

La plupart des racks peuvent être montés sur des rails DIN de 35 mm (1,38 in.) de largeur et 15 mm (0,59 in.) de profondeur.

**NOTE:** les racks d'une longueur supérieure à 400 mm (15,75 in.) et comprenant plus de 8 emplacements de module ne peuvent pas être montés sur un rail DIN. Ne montez pas un rack BMXXBP1200 (PV:02 ou version ultérieure)(H), BMEXBP1002(H) ou BMEXBP1200(H) sur un rail DIN.

**NOTE:** le montage sur rail DIN augmente la contrainte mécanique sur le système.

Montage d'un rack sur un rail DIN :

| Etape | Action | Illustration |
|---|---|---|
| 1 | Positionnez le rack en haut du rail DIN et appuyez sur le dessus du rack pour comprimer les ressorts en contact avec le rail DIN. |  |
| 2 | Faites basculer le fond du rack vers l'arrière pour le plaquer contre le rail DIN. | |
| 3 | Relâchez le rack pour le verrouiller. | |

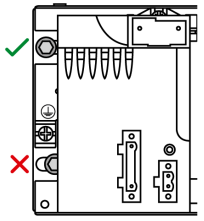
Pour retirer un rack du rail DIN :

| Etape | Action |
|---|---|
| 1 | Appuyez sur le dessus du rack pour comprimer les ressorts en contact avec le rail DIN. |
| 2 | Faites basculer le fond du rack vers l'avant pour le sortir du rail DIN. |
| 3 | Libérez le rack. |

## Montage sur une paroi

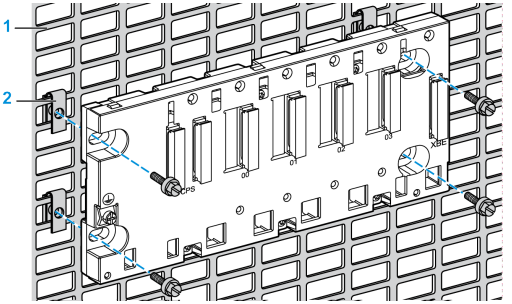
Vous pouvez monter un rack sur une paroi, à l'intérieur ou à l'extérieur d'un boîtier, à l'aide de vis M4, M5, M6 ou UNC #6 insérées dans les trous de fixation.

Placez les deux vis de gauche (près de l'alimentation) le plus près possible du bord gauche du rack. Cela permet d'accéder à ces vis une fois l'alimentation montée.



## Montage sur platines perforées Telequick AM1-PA et AM3-PA

Vous pouvez monter un rack sur une platine perforée Telequick AM1-PA ou AM3-PA à l'aide de vis M4, M5, M6 ou UNC #6.



# Extension d'un rack

## Introduction

Si vous disposez de plus d'un rack dans le rack local ou sur une station distante, installez un module d'extension de rack BMXXBE1000 sur le rack principal et les racks d'extension. Les modules d'extension de rack sont interconnectés par des câbles d'extension X Bus.

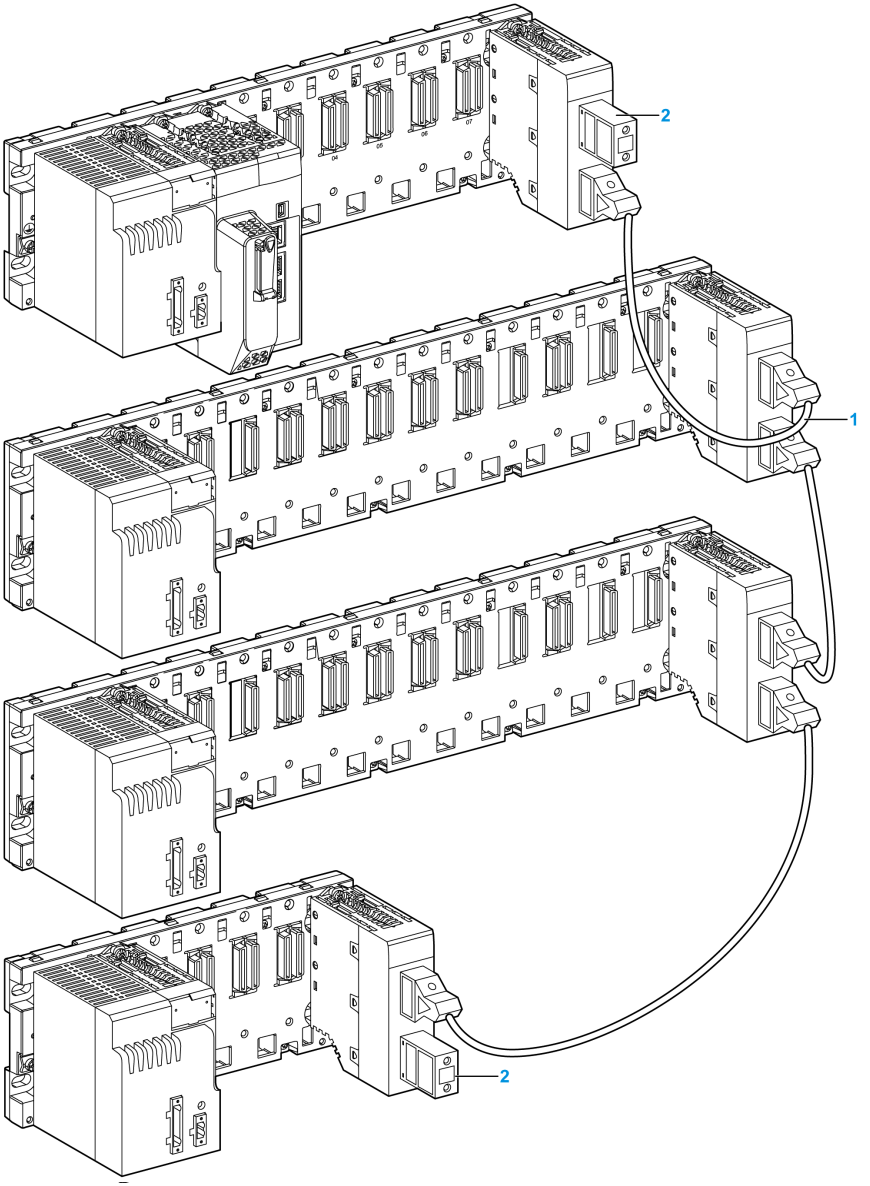
**NOTE:** Pour plus d'informations sur l'installation et la connexion de modules d'extension de rack, consultez la rubrique *Installation de modules d'extension de rack Modicon X80* dans le document *Modicon M580 - Manuel de référence du matériel*.

## Conception d'un système de sécurité M580 en utilisant des racks locaux d'extension

En utilisant des câbles et des modules d'extension BMXXBE1000, vous pouvez ajouter à votre PAC de sécurité M580 :

- jusqu'à sept racks d'extension au rack principal local
- un rack d'extension à un rack principal distant

Exemple de rack principal local Ethernet avec racks d'extension, modules d'extension et câbles :




**1** La même station peut contenir des racks de différentes tailles interconnectés par des câbles d'extension.

**2** Les modules d'extension situés aux extrémités des câbles interconnectés sont munis de terminaisons de ligne.

# Installation d'une CPU, d'un coprocesseur, d'une alimentation et d'un module d'E/S M580

## Présentation

Cette section décrit l'installation d'une CPU de sécurité, d'un coprocesseur, d'une alimentation et d'un module d'E/S M580

## Installation de la CPU et du coprocesseur

### Introduction

Vous pouvez installer la CPU BME•58•040S et le coprocesseur BMEP58CPROS3 dans un rack Ethernet BMEXBP••00 ou BMEXBP••02 uniquement.

### Précautions d'installation

Un module CPU M580 est alimenté par le bus du rack. Vérifiez que l'alimentation du rack est coupée avant d'installer le module CPU.

**⚠⚠ DANGER**

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

- Coupez toutes les alimentations de tous les équipements, y compris les équipements connectés, avant de retirer les caches ou les 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 approprié à cet équipement.
- Utilisez toujours un appareil de mesure de tension réglé correctement pour vous assurer que l'alimentation est coupée conformément aux indications.
- Remettez en place et fixez tous les caches de protection, accessoires, matériels, câbles et fils et vérifiez que l'appareil est bien relié à la terre avant de le remettre sous tension.
- Utilisez uniquement la tension spécifiée pour faire fonctionner cet équipement et tout autre produit associé.

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

Retirez le capot de protection des connecteurs d'emplacement du rack avant d'y brancher le module.

| ⚠AVERTISSEMENT |
| --- |
| **FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT**<br>Assurez-vous que le contrôleur ne contient pas de carte mémoire SD non prise en charge avant de le mettre sous tension.<br>**Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.** |

**NOTE:**

- Vérifiez que la porte du logement de la carte mémoire est fermée après avoir inséré une carte dans le contrôleur.
- Consultez `%SW97` pour vérifier l'état de la carte SD.

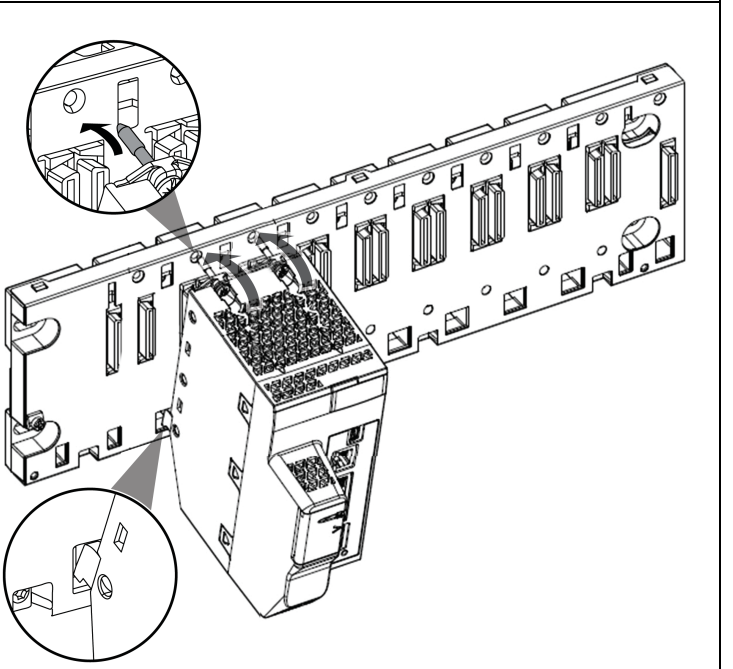
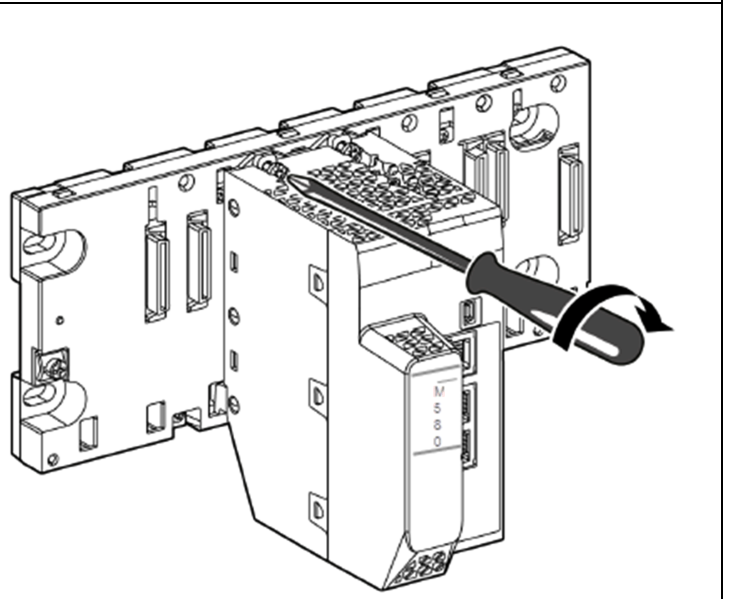
## Installation des modules CPU et coprocesseur dans le rack

Installez la CPU et le coprocesseur dans les emplacements suivants du rack :

- CPU : emplacements **00** et **01**.
- Coprocesseur : emplacements **02** et **03**.

Procédez comme suit pour installer une CPU et un coprocesseur dans un rack :

| Étape | Action |
| --- | --- |
| 1 | Vérifiez que l'alimentation est coupée. |
| 2 | Vérifiez les points suivants :<br>• Si une carte mémoire SD est utilisée, son type est pris en charge par la CPU.<br>• Les capots de protection des connecteurs ont été retirés.<br>• La CPU est placée dans les emplacements marqués **00** et **01**. |

| Étape | Action | |
|---|---|---|
| 3 | Positionnez les ergots de guidage situés à l'arrière du module (partie inférieure) dans les emplacements correspondants du rack. |  |
| 4 | Relevez le module pour le plaquer contre l'arrière du rack.<br><br>Le module est en place. | |
| 5 | Serrez les 2 vis situées sur le dessus de la CPU pour maintenir le module dans le rack.<br><br>Couple de serrage : 0,4 à 1,5 N•m (0,30 à 1,10 lbf-ft) |  |
| 6 | Pour installer le module coprocesseur, placez-le dans les emplacements **02** et **03** et suivez les étapes 3, 4 et 5 ci-dessus. | |

## Mise à la terre

Respectez toutes les normes et consignes de sécurité locales et nationales.

**⚠⚠DANGER**

**RISQUE D'ELECTROCUTION**

Lorsqu'il est impossible de prouver que l'extrémité d'un câble blindé est reliée à la masse locale, ce câble doit être considéré comme dangereux et les équipements de protection individuelle (EPI) doivent être utilisés.

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

Pour plus d'informations sur la mise à la terre de la CPU et du coprocesseur, consultez les *Informations relatives à la mise à la terre* dans le *Manuel de référence du matériel Modicon M580*.

# Installation d'un module d'alimentation

## Introduction

Installez le module d'alimentation de sécurité M580 dans un X Bus ou un rack Ethernet contenant d'autres modules de sécurité M580. Le module d'alimentation de sécurité peut être utilisé dans les racks qui requièrent une seule alimentation ou une double alimentation redondante.

**⚠AVERTISSEMENT**

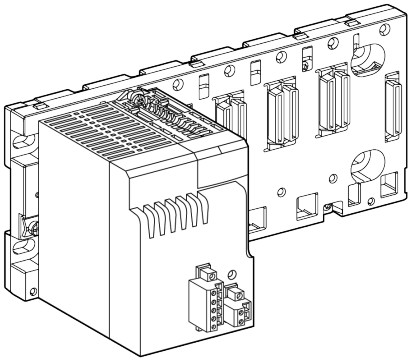
**PERTE DE LA CAPACITE A EXECUTER LA FONCTION DE SECURITE**

Utilisez l'alimentation de sécurité BMXCPS4002S, BMXCPS4022S ou BMXCPS3522S uniquement dans un rack contenant au moins un module de sécurité.

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

Si un rack nécessite une seule alimentation, placez un module d'alimentation M580 de sécurité dans le rack aux deux emplacements marqués **CPS**. Pour un rack à double alimentation BMEXBP••02 (voir le manuel de référence du matériel Modicon M580), placez deux modules d'alimentation M580 de sécurité côte à côte dans les quatre emplacements marqués **CPS**.

Exemple de module d'alimentation unique installé dans un rack BMEXBP0400 :



**NOTE:** La conception du module d'alimentation ne permet de le placer que dans les emplacements marqués **CPS**.

## Précautions d’installation

Le module d'alimentation de sécurité M580 ne peut pas être remplacé à chaud. Vérifiez que le module est hors tension lors de son insertion dans l'embase ou de son retrait de l'embase.

Ne connectez pas ou ne déconnectez pas le bornier amovible de l'alimentation principale lorsque la tension est appliquée au module d'alimentation de sécurité M580. Vérifiez que l'alimentation du module en provenance du disjoncteur en amont est coupée avant d'effectuer ces tâches.

Ne connectez pas ou ne déconnectez pas le bornier amovible du relais d'alarme lorsque le module d'alimentation de sécurité M580 est en cours de fonctionnement. Vérifiez que le module est hors tension avant d'effectuer ces tâches.

**⚠⚠DANGER**

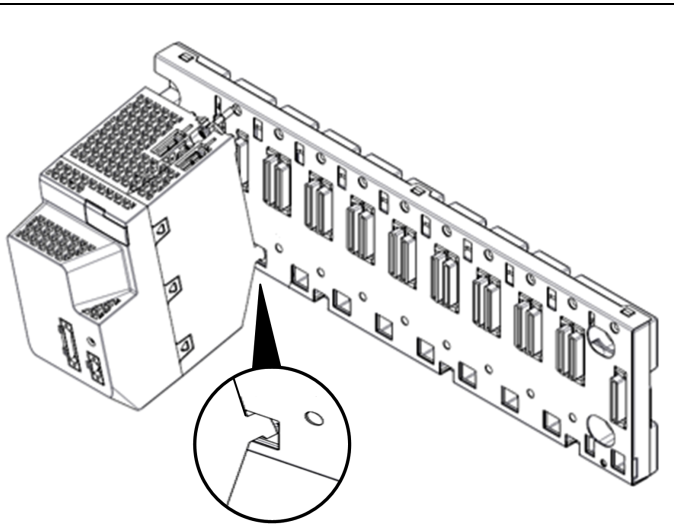
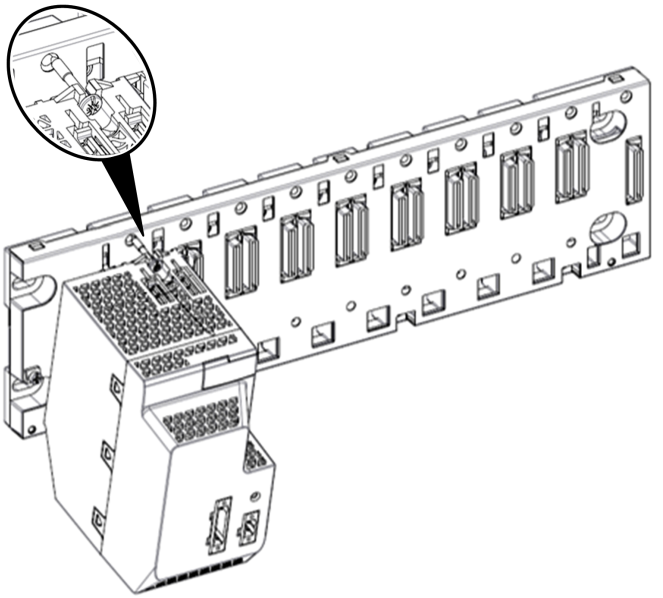
**RISQUE DE CHOC ÉLECTRIQUE, D'EXPLOSION OU D'ARC ÉLECTRIQUE**

- Coupez toutes les alimentations de tous les équipements, y compris les équipements connectés, avant de retirer les caches ou les 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 approprié à cet équipement.
- Utilisez toujours un appareil de mesure de tension réglé correctement pour vous assurer que l'alimentation est coupée conformément aux indications.
- Remettez en place et fixez tous les caches de protection, accessoires, matériels, câbles et fils et vérifiez que l'appareil est bien relié à la terre avant de le remettre sous tension.
- Utilisez uniquement la tension spécifiée pour faire fonctionner cet équipement et tout autre produit associé.

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

## Installation du module d'alimentation dans le rack

Pour installer le module d'alimentation de sécurité dans les emplacements du rack marqués **CPS**, procédez comme suit :

| Étape | Action | |
|---|---|---|
| 1 | Vérifiez que le module d'alimentation est placé dans les emplacements marqués **CPS**. | |
| 2 | Positionnez les ergots de guidage situés à l'arrière du module (partie inférieure) dans les emplacements correspondants du rack. |  |
| 3 | Relevez le module pour le plaquer contre l'arrière du rack.<br><br>Le module est en place. | |
| 4 | Serrez la vis de fixation sur la partie supérieure de l'alimentation afin de maintenir le module en place sur le rack.<br><br>Couple de serrage : 0,4 à 1,5 N•m (0.30 à 1.10 lbf-ft) |  |
| 5 | Pour les racks nécessitant une double alimentation, répétez les étapes 2, 3 et 4 pour la deuxième alimentation. | |

## Mise à la terre du module d'alimentation

Respectez toutes les normes et consignes de sécurité locales et nationales.

**⚠⚠DANGER**

**RISQUE D'ELECTROCUTION**

Lorsqu'il est impossible de prouver que l'extrémité d'un câble blindé est reliée à la masse locale, ce câble doit être considéré comme dangereux et les équipements de protection individuelle (EPI) doivent être utilisés.

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

Pour plus d'informations sur la mise à la terre de l'alimentation, consultez la rubrique *Mise à la terre du rack et du module d'alimentation*.

# Installation d'E/S de sécurité M580

## Introduction

Vous pouvez installer un module d'E/S de sécurité M580 dans tout rack Ethernet ou X Bus, dans tout emplacement non réservé pour l'alimentation de sécurité ou la CPU (en cas de rack local principal).

**NOTE:** Utilisez uniquement l'alimentation de sécurité BMXCPS4002S, BMXCPS4022S ou BMXCPS3522S si le rack contient des modules d'E/S de sécurité.

Vous pouvez effectuer le remplacement à chaud du module d'E/S de sécurité M580.

## Précautions générales relatives au câblage

Pour éviter les interférences entre une charge CC et une source CA, séparez les câbles du circuit d'alimentation (par exemple les câbles de l'alimentation principale) des câbles d'entrée et des câbles de sortie des actionneurs.

Protégez les câbles de connexion entre la CPU et les modules d'E/S avec une gaine à l'intérieur d'un conduit en métal. Placez les câbles d'E/S dans un blindage distinct du blindage des câbles d'alimentation. Placez les câbles blindés dans un conduit distinct des câbles d'E/S. La distance entre les câbles d'alimentation et les câbles d'E/S doit être d'au moins 100 mm.

## Précautions relatives à la mise à la terre

Chaque module d'E/S de sécurité M580 est équipé de contacts de mise à la terre.

Utilisez une barre BMXXSP•••• pour protéger le rack contre les perturbations électromagnétiques.

Pour le module d'entrée analogique de sécurité BMXSAI0410, utilisez une barre BMXXSP••••. Reliez le blindage du câble à la barre de mise à la terre en le fixant à la barre sur le côté du module.

**⚠⚠DANGER**

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

- Vérifiez que chaque bornier reste connecté à la barre de mise à la terre BMXXSP•••• lors du montage ou du retrait des modules d'E/S de sécurité.
- Coupez la tension d'alimentation des capteurs et actionneurs.

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

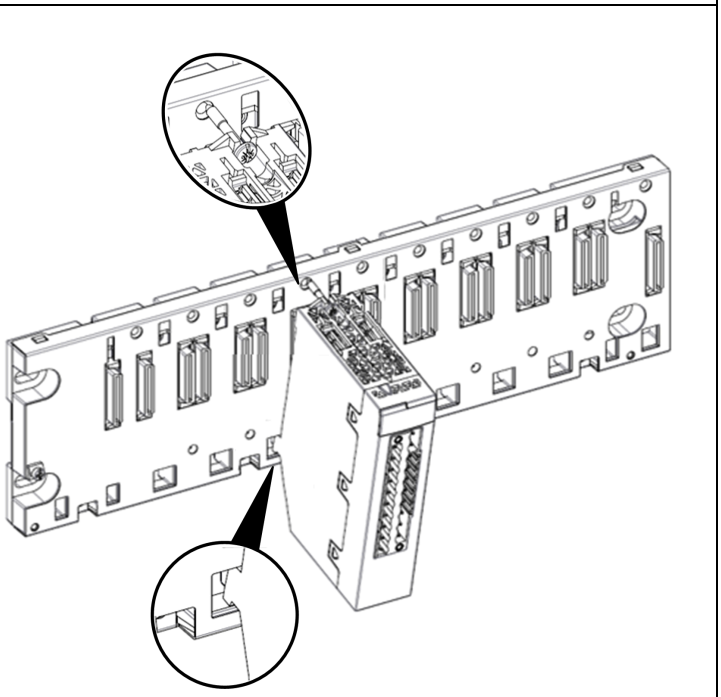
## Positionnement des capteurs des modules d'entrée (en relation avec la mise à la terre)

Lors du placement de capteurs sur votre système :

- Placez les capteurs à proximité l'un de l'autre, à une distance de quelques mètres maximum.
- Définissez un point de référence unique pour tous les capteurs puis reliez ce point à la masse du PAC.

## Installation d'un module d'E/S de sécurité dans le rack

Un module d'E/S de sécurité M580 requiert un seul emplacement de rack. Vous pouvez installer un module d'E/S de sécurité dans tout emplacement non réservé à l'alimentation ou la CPU. Pour installer un module d'E/S de sécurité dans un rack, procédez comme suit :

| Étape | Action | |
|---|---|---|
| 1 | Positionnez les ergots de guidage situés à l'arrière du module dans les emplacements correspondants du rack. |  |
| 2 | Relevez le module pour le plaquer contre l'arrière du rack.<br><br>Le module est en place. | |
| 3 | Serrez la vis de fixation sur la partie supérieure du module afin de maintenir le module en place sur le rack.<br><br>Couple de serrage : 0,4 à 1,5 N•m (0.30 à 1.10 lbf-ft) | |
| 4 | Répétez les étapes 1, 2 et 3 pour chaque module supplémentaire à installer dans le rack. | |

## Mise à la terre des modules d'E/S

Pour plus d'informations sur la mise à la terre, consultez la rubrique *Mise à la terre du rack et du module d'alimentation*.

**NOTE:** Pour le module d'entrée analogique de sécurité BMXSAI0410, utilisez une barre de mise à la terre BMXXSP••••. Pour plus d'informations sur l'installation de cet équipement, reportez-vous à la rubrique *Kit de connexion de blindage*.

# Installation d'une carte mémoire SD dans une CPU

## Présentation

La CPU BME•58•040S est compatible avec la carte mémoire SD 4 Go BMXRMS004GPF.

## Entretien de la carte mémoire

Pour conserver la carte mémoire en bon état de marche :

- Evitez de retirer la carte de son logement lorsque la CPU y accède (voyant vert d'accès à la carte mémoire allumé ou clignotant).
- Evitez de toucher les connecteurs de la carte mémoire.
- Protégez la carte mémoire des sources électrostatiques et électromagnétiques, des sources de chaleur, des rayons de soleil, de l'eau et de l'humidité.
- Evitez tout impact sur la carte mémoire.
- Avant d'envoyer une carte mémoire par courrier, vérifiez les pratiques de sécurité des services postaux. En effet, par mesure de sécurité, les services postaux de certains pays exposent le courrier à de hauts niveaux de radiation. Or, ces hauts niveaux de radiation peuvent effacer le contenu de la carte mémoire et rendre cette dernière inutilisable.
- Si vous retirez une carte mémoire sans générer un front montant du bit %S65 et sans vérifier que le voyant vert d'accès à la carte est éteint, les données qu'elle contient (fichiers, applications, etc.) risquent d'être perdues ou endommagées.

## Procédure d'insertion de la carte mémoire

Procédez comme suit pour insérer une carte mémoire dans une CPU BME•58•040S :

| Etape | Description |
|---|---|
| 1 | Ouvrez le capot de protection de la carte mémoire SD. |
| 2 | Insérez la carte dans son logement. |
| 3 | Poussez la carte mémoire jusqu'à entendre le déclic.<br>**Résultat :** La carte devrait être enclenchée dans son emplacement.<br>**Remarque :** L'insertion de la carte mémoire ne nécessite pas la restauration de l'application. |
| 4 | Fermez le capot de protection de la carte mémoire. |

## Procédure de retrait de la carte mémoire

**NOTE:** Avant d'extraire une carte mémoire, il faut générer un front montant sur le bit %S65. Si vous retirez une carte mémoire sans générer un front montant du bit `%S65` et sans vérifier que le voyant vert d'accès à la carte est éteint, les données risquent d'être perdues.

Procédez comme suit pour retirer une carte mémoire d'une CPU BME•58•040S :

| Etape | Description |
|---|---|
| 1 | Générez un front montant sur le bit %S65. |
| 2 | Vérifiez que le voyant (LED) vert d'accès à la carte mémoire est éteint. |
| 3 | Ouvrez le capot de protection de la carte mémoire SD. |
| 4 | Poussez la carte mémoire jusqu'au déclic, puis relâchez-la.<br><br>**Résultat :** la carte doit se détacher de son emplacement. |
| 5 | Retirez la carte de son emplacement.<br><br>**Remarque :** le voyant LED d'accès à la carte mémoire s'allume lorsque la carte est retirée de la CPU. |
| 6 | Fermez le capot de protection de la carte mémoire. |

# Montée en niveau du micrologiciel du contrôleur de sécurité M580

La procédure diffère en fonction de la version initiale et de la version cible du contrôleur. Un nouveau chargeur de démarrage a été introduit dans la version 4.x. En conséquence, la mise à jour d'une version antérieure (V3.22 ou antérieure) vers une version V4.x ou la rétrogradation d'une version V4.x vers une version antérieure nécessite des procédures spécifiques.

Vous trouverez les procédures détaillées de mise à jour du micrologiciel dans le document *Modicon M580 - Guide d'installation du micrologiciel du contrôleur*.

# Mise à jour du micrologiciel vers la version 4.21

Vous pouvez mettre à niveau le micrologiciel des contrôleurs de sécurité vers la version 4.21 à partir des versions antérieures suivantes :

- 3.30.06 pour les contrôleurs BMEP586040S
- 3.20.05 ou antérieure pour les autres contrôleurs de sécurité M580

La procédure est décrite dans la section *Mise à jour du micrologiciel de v3.x vers v4.x* du Guide d'installation du micrologiciel des contrôleurs Modicon M580.

# Versions de micrologiciel de repli

Si la mise à niveau du micrologiciel vers une version supérieure échoue, le contrôleur de sécurité applique la version de repli suivante :

- 3.30.06 pour le contrôleur BME58P6040S
- 3.20.05 pour les autres contrôleurs de sécurité M580

# Niveau d'application et état de fonctionnement du contrôleur à l'issue de la mise à niveau

Si la mise à niveau réussit, le contrôleur de sécurité redémarre l'application qui y était précédemment chargée et fonctionne à l'état STOP.

**NOTE:** Dans ce cas, le contrôleur fonctionne en mode STOP même lorsque l'option *Démarrage automatique en mode RUN* est sélectionnée.

Si la mise à niveau échoue et que l'application précédemment chargée sur le contrôleur est :

- incompatible avec la version de repli : le contrôleur redémarre à l'état de fonctionnement NOCONF.
- compatible avec la version du micrologiciel de repli : le contrôleur redémarre l'application chargée précédemment et fonctionne à l'état STOP.

# Rétrogradation du micrologiciel à partir de la version 4.21 ou ultérieure

Vous pouvez rétrograder le micrologiciel des contrôleurs de sécurité de la version 4.21 ou ultérieure vers les versions antérieures suivantes :

- Version 3.30.06 pour BMEP586040S
- Version 3.20.05 pour les autres contrôleurs de sécurité M580

La procédure est décrite dans le document *Modicon M580 - Guide d'installation du micrologiciel du contrôleur*, section *Procédure de rétrogradation du micrologiciel*.

# Versions de micrologiciel de repli

Si la rétrogradation du micrologiciel échoue, vous devez utiliser l'outil EADM (Ecostruxure Automation Device Maintenance) pour réactiver le contrôleur en installant un micrologiciel de version 4.21 ou ultérieure.

# Niveau d'application et état de fonctionnement du contrôleur à l'issue d'une rétrogradation

Si la rétrogradation du micrologiciel réussit et que l'application précédemment chargée sur le contrôleur est :

- incompatible avec la version de repli : le contrôleur redémarre à l'état de fonctionnement NOCONF.
- compatible avec la version de repli : le contrôleur redémarre avec l'application précédemment chargée et fonctionne à l'état STOP même lorsque l'option *Démarrage automatique en mode RUN* est sélectionnée.

Si la rétrogradation échoue, le contrôleur conserve son micrologiciel d'origine.

# 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

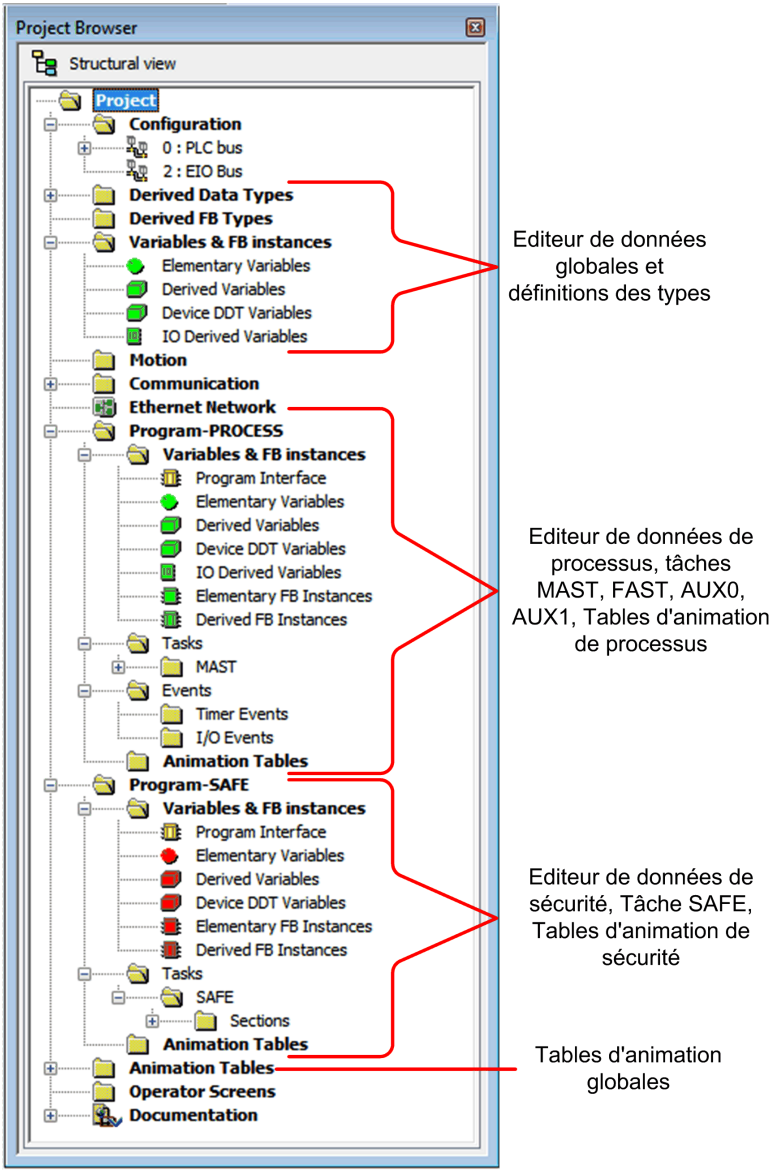
## Introduction

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 :



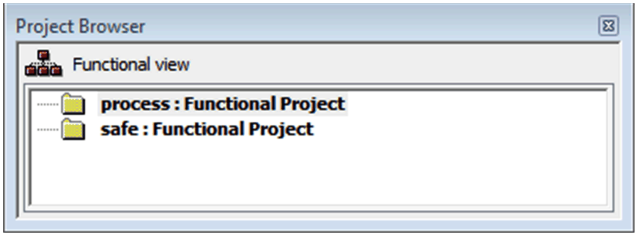

Lors d'une recherche dans le **Navigateur de projet** :

- 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<br>• FBD<br>• LD<br>• Segment LL984<br>• SFC<br>• ST | • MAST<br>• FAST<br>• AUX0<br>• AUX1 |
| **sécurité : projet fonctionnel** | • FBD<br>• 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 PAC de sécurité M580

### Deux modes de fonctionnement

Le PAC 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 la mise au point et la correction du programme d'application ou modifier la configuration.

Le logiciel Control Expert XL Safety est le seul outil qui permet de gérer les transitions entre modes de fonctionnement.

**NOTE:** Le réglage du mode de fonctionnement d'un PAC de sécurité redondant (Hot Standby) – qu'il s'agisse du mode sécurité ou maintenance – n'est pas inclus dans le transfert d'une application du PAC principal au PAC redondant. Lorsqu'un PAC de sécurité redondant devient le PAC principal, le mode sécurité est automatiquement activé.

### Description et limites du mode sécurité

Le mode sécurité est le mode par défaut du PAC de sécurité. Lorsque le PAC 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 PAC de sécurité M580 fonctionne en mode sécurité, les fonctions suivantes ne sont **pas** disponibles :

- Téléchargement d'une configuration modifiée de Control Expert vers le PAC.
- Modification et/ou forçage des valeurs des variables de sécurité et de l'état des E/S de sécurité.

- Mise au point 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 variable non liée à la sécurité sont copiées dans les variables de sécurité.
- A la fin de chaque tâche SAFE, les valeurs de variable de sortie liée à la sécurité sont copiées dans les variables non liées à la sécurité.

## Fonctionnement en mode de maintenance

Le mode maintenance est comparable au mode normal d'une CPU M580 non liée à la sécurité. Il est utilisé uniquement pour effectuer la mise au point et le réglage de la tâche SAFE de l'application. Le mode maintenance est temporaire. En effet, le PAC de sécurité passe automatiquement en mode sécurité si la communication entre Control Expert et le PAC est perdue ou lors de l'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 qui sont 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 PAC de sécurité M580 est en mode maintenance, les fonctions suivantes sont disponibles :

- Téléchargement d'une configuration modifiée de Control Expert vers le PAC.
- Modification et/ou forçage des valeurs des variables de sécurité et de l'état des E/S de sécurité.
- Mise au point 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 de requêtes UMAS (par exemple, via une IHM) 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 de l’automate de sécurité n’est pas maintenu.

## ⚠AVERTISSEMENT

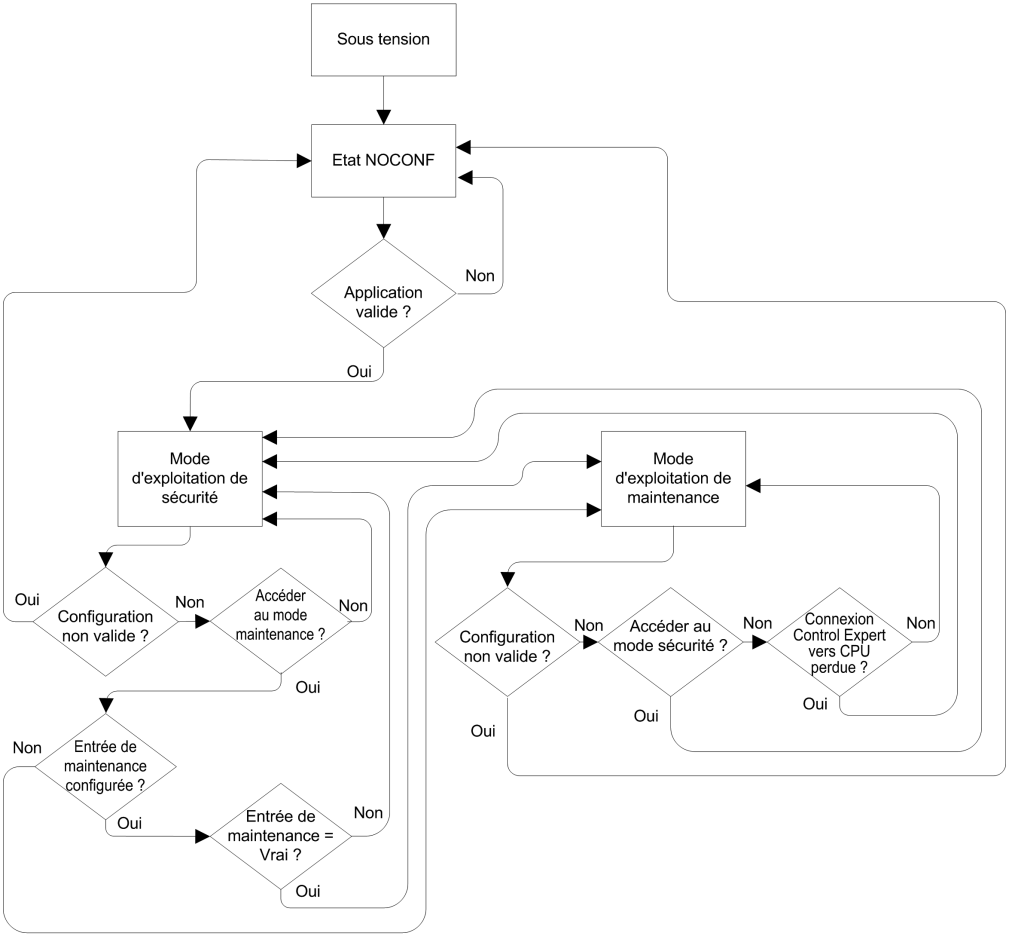
**PERTE DU NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ (SIL)**

Prenez les mesures appropriées pour garantir l'état sécurisé 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.**

# Transitions entre les modes de fonctionnement

Le schéma suivant montre comment le PAC 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 perdure après la transition jusqu'à la transition suivante du mode sécurité au mode maintenance.

- La transition du mode maintenance au mode sécurité peut être effectuée de plusieurs manières :
  - Manuellement, via une commande de menu ou de barre d'outils dans Control Expert.
  - Automatiquement par le PAC de sécurité, lorsque la communication entre Control Expert et le PAC est perdue pendant environ 50 secondes.
- La fonction d'entrée de maintenance, lorsqu'elle est configurée, fonctionne comme une vérification de la transition du mode sécurité au mode maintenance. La fonction d'entrée de maintenance est configurée à l'aide de Control Expert, dans l'onglet **Configuration** de la CPU, de la manière suivante :
  - Sélectionnez le paramètre **Entrée 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 PAC est verrouillé en mode sécurité. Si le bit est défini sur 1 (vrai), une transition vers le mode maintenance est possible.

## Basculement entre le mode sécurité et le mode maintenance dans Control Expert

Il n'est pas possible de basculer le PAC de sécurité du mode maintenance au mode sécurité si :

- Le PAC est en mode mise au point.
- 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 mise au point 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 **Automate > Maintenance** ou
  - Cliquez sur le bouton  dans la barre d'outils.
- Pour passer du mode maintenance au mode sécurité :
  - Sélectionnez **Automate > 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 dans la CPU.

## Identification du mode de fonctionnement

Vous pouvez déterminer le mode de fonctionnement actuel d'un PAC de sécurité M580 en consultant les voyants **SMOD** de la CPU et du coprocesseur ou à l'aide de Control Expert.

Lorsque les voyants **SMOD** de la CPU et du coprocesseur sont :

- *Clignotants* : le PAC est en mode maintenance.
- *Allumés fixement* : le PAC est en mode sécurité.

Quand Control Expert est connecté au PAC, il identifie le mode de fonctionnement du PAC de sécurité M580 de plusieurs manières :

- Les mots système %SW12 (coprocesseur) et %SW13 (CPU), page 225 combinés indiquent le mode de fonctionnement du PAC, comme suit :
  - si la valeur de %SW12 est 16#A501 (hex) et celle de %SW13 est 16#501A (hex), le PAC est en mode maintenance.
  - si la valeur de l'un de ces mots système ou des deux est 16##5AFE (hex), le PAC est en mode sécurité.
- Les sous-onglets **Tâche** et **Informations** de l'onglet **Animation** de la CPU affichent tous les deux le mode de fonctionnement du PAC.
- La barre des tâches située en bas de la fenêtre principale de Control Expert indique le mode de fonctionnement MAINTENANCE ou SECURITE.

# Etats de fonctionnement du PAC de sécurité M580

## Etats de fonctionnement

Le PAC de sécurité M580 présente les états de fonctionnement suivants.

**NOTE:** Pour une description de la relation entre les états de fonctionnement du PAC de sécurité M580 et les états de fonctionnement du PAC redondant M580, consultez le document *Modicon M580 - Redondance d''UC, Guide de planification du système pour architectures courantes* et les rubriques *Etats du système de redondance d'UC* et *Affectation et transition des états de redondance d'UC*.

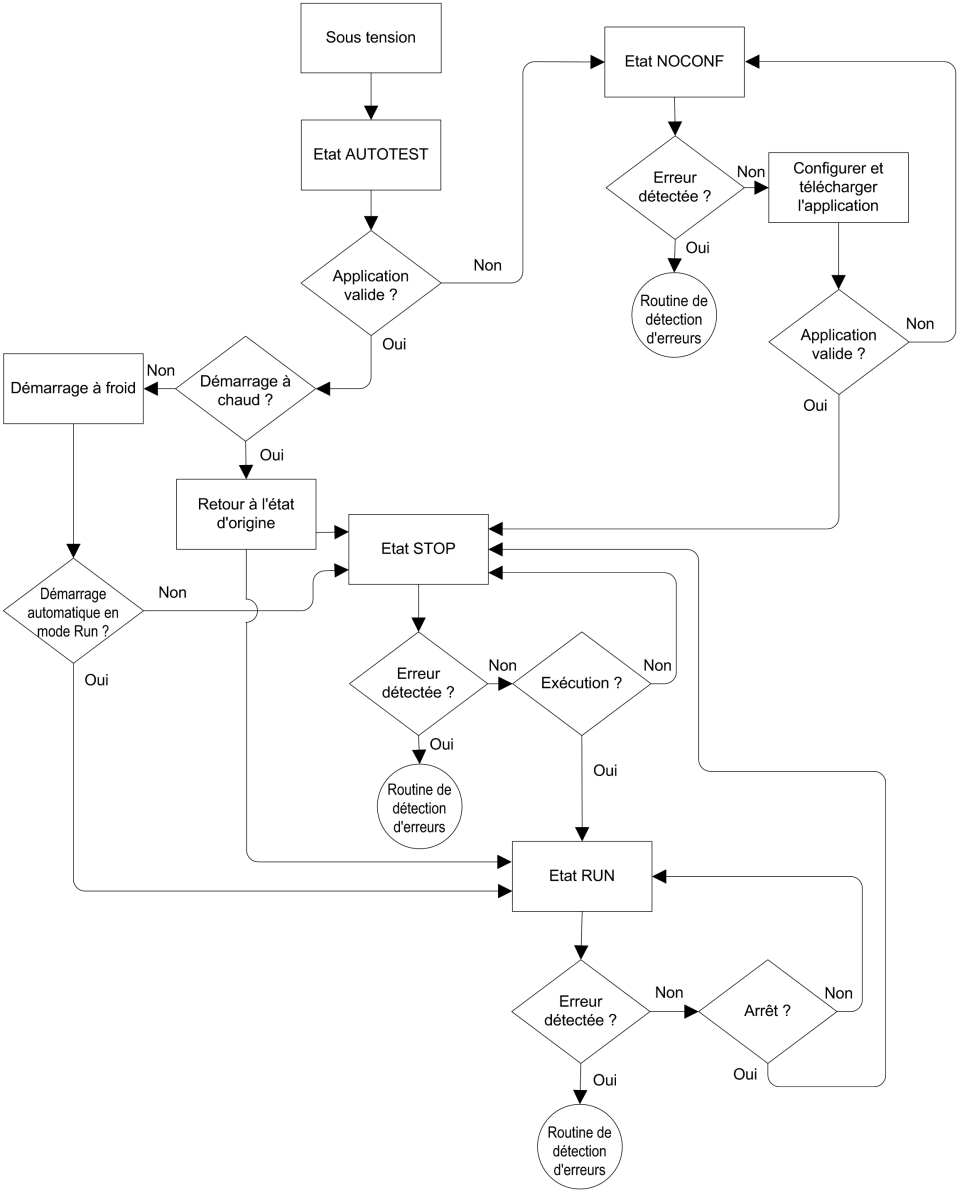
| Etat de fonctionnement | Applicable à | Description |
|---|---|---|
| AUTOTEST | PAC | La CPU exécute des autotests internes.<br>**NOTE:** Si des racks d'extension sont connectés au rack local principal et que les connecteurs inutilisés du module d'extension de rack ne sont pas munis de terminaisons de ligne, la CPU reste à l'état AUTOTEST à l'issue des autotests. |
| NOCONF | PAC | Le programme d'application n'est pas valide. |
| STOP | PAC ou tâche | Le PAC contient une application valide et aucune erreur n'est détectée, mais le fonctionnement s'est arrêté car :<br>• Au démarrage **Démarrage automatique en mode Run** n'est pas défini (mode sécurité, page 121).<br>• Exécution arrêtée par l'exécution de la commande STOP (mode sécurité, page 121 ou maintenance, page 122)<br>• Les points d'arrêt ont été définis en mode maintenance, puis la connexion entre Control Expert et la CPU a été perdue durant plus de 50 secondes.<br>La CPU lit les entrées associées à chaque tâche, mais n'actualise pas les sorties, qui passent à l'état de repli. Vous pouvez redémarrer la CPU lorsque vous êtes prêt.<br>**NOTE:** L'envoi de la commande STOP dans Control Expert arrête toutes les tâches. L'événement STOP est enregistré sur le serveur SYSLOG de la CPU. |
| HALT | Tâche | Le PAC de sécurité M580 peut être dans deux états HALT indépendants :<br>• 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.<br>• L'état SAFE HALT s'applique uniquement à la tâche SAFE. Les tâches de processus ne sont pas affectées par une condition SAFE HALT.<br>Dans chaque cas, les opérations de la tâche sont arrêtées à cause d'une condition bloquante inattendue, entraînant une condition récupérable (voir Modicon M580, Manuel de sécurité).<br>La CPU lit les entrées associées à chaque tâche arrêtée, mais n'actualise pas les sorties, qui sont à l'état de repli. |
| RUN | PAC ou tâche | En présence d'une application valide et en l'absence d'erreur détectée, la CPU lit les entrées associées à chaque tâche, exécute le code associé à chaque tâche, puis actualise les sorties associées.<br>• En mode sécurité, page 121 : la fonction de sécurité est effectuée, et toutes les restrictions sont appliquées.<br>• En mode maintenance, page 122 : le PAC fonctionne comme une CPU non liée 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 de la CPU. |
| WAIT | PAC | La CPU est dans un état transitoire pendant qu'elle sauvegarde ses données quand une condition de mise hors tension est détectée. La CPU démarre à nouveau lorsque l'alimentation est rétablie et que la réserve de courant est remplie.<br><br>Comme l'état WAIT est transitoire, il se peut qu'il ne soit pas visible. La CPU effectue un redémarrage à chaud, page 135 pour sortir de l'état WAIT. |
| ERROR | PAC | La CPU (voir Modicon M580, Manuel de sécurité) est arrêtée suite à la détection d'une erreur matérielle ou système. L'état ERROR déclenche la fonction de sécurité (voir Modicon M580, Manuel de sécurité).<br><br>Lorsque le système est prêt à redémarrer, effectuez un Démarrage à froid, page 135 de la CPU pour quitter l'état ERROR, soit par un redémarrage, soit par une réinitialisation (RESET). |
| OS DOWNLOAD | PAC | Un téléchargement du micrologiciel de la CPU ou du coprocesseur est en cours. |

Consultez les rubriques *M580 - Voyants de diagnostic de la CPU* (voir Modicon M580, Manuel de sécurité) et *M580 - Voyants de diagnostic du coprocesseur de sécurité* (voir Modicon M580, Manuel de sécurité) pour plus d'informations sur les états de fonctionnement du PAC.

# Transitions entre les états de fonctionnement

Les transitions entre les différents états d'un PAC de sécurité M580 sont décrites ci-dessous :



Consultez la rubrique *Traitement des erreurs détectées*, page 130 pour plus d'informations sur la façon dont système de sécurité gère les erreurs.

## Traitement des erreurs détectées

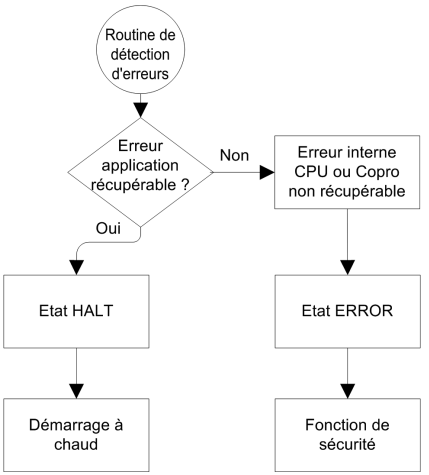
Le PAC de sécurité M580 gère les erreurs détectées par la CPU des types suivants :

- Erreurs récupérables liées à 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 liées à l'application, erreurs internes de la CPU ou du coprocesseur : ces événements font passer le PAC 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 |

| Type de l'erreur détectée | Etat des tâches | | | |
|---|---|---|---|---|
| | **FAST** | **SAFE** | **MAST** | **AUX** |
| 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 la CPU | RUN | HALT[2] | RUN | RUN |
| Dépassement du chien de garde de sécurité[3] | ERROR | ERROR[2] | ERROR | ERROR |
| Détection d'erreur interne de la CPU | 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 PAC 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 :

| Etat 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 PAC de sécurité M580 peut passer à la séquence de démarrage dans les cas suivants :

- À la première mise sous tension.
- En réponse à l'interruption de l'alimentation.

Selon le type de tâche et le contexte de l'interruption de l'alimentation, le PAC de sécurité M580 peut effectuer un nouveau démarrage à froid, page 135 ou un démarrage à chaud, page 135 lorsque l'alimentation est restaurée.

## Démarrage initial

Lors du démarrage initial, le PAC de sécurité M580 exécute 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 l'option **Démarrage automatique en mode RUN** est activée, auquel cas toutes les tâches passent à l'état RUN.

## Démarrage après une coupure de courant

L'alimentation de sécurité M580 constitue une réserve qui continue à alimenter tous les modules du rack pendant 10 ms en cas de coupure de courant. Si la réserve d'alimentation est vide, le PAC de sécurité M580 effectue un cycle d'alimentation complet.

Avant la mise hors tension du système, la CPU 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.

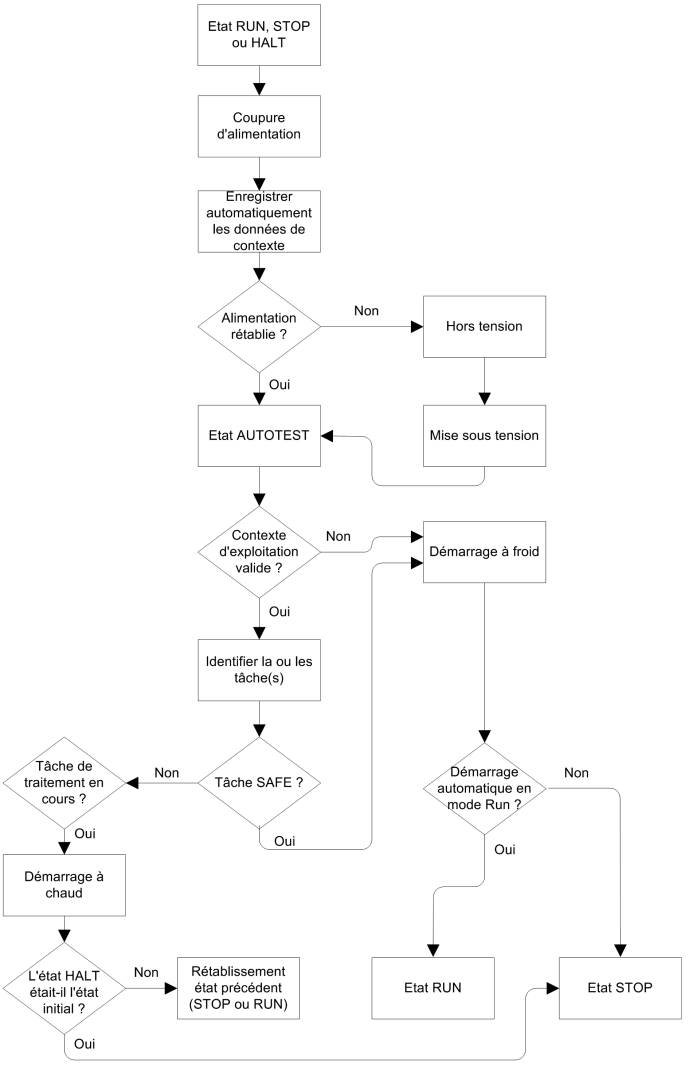
Après une mise hors tension, le démarrage peut être automatique (si l'alimentation a été restaurée avant la fin de la mise hors tension) ou manuel (dans le cas contraire).

Ensuite, le PAC 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

Un démarrage à froid entraîne le passage à l'état STOP de toutes les tâches, y compris la tâche SAFE et les tâches non liées à la sécurité (MAST, FAST, AUX0, AUX1), sauf si l'option **Démarrage automatique en mode RUN** est activée, auquel cas toutes 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.
- Toutes les variables forcées sont initialisées à leur valeur par défaut.

Un démarrage à froid peut être exécuté pour les données, les variables et les fonctions dans l'espace de nom de processus en sélectionnant **Automate > Init** dans Control Expert, page 151 ou en définissant 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 (y compris les tâches MAST, FAST, AUX0 et AUX1) repasse à l'état de fonctionnement où elle se trouvait au moment de la coupure de courant. En revanche, un démarrage à chaud fait passer la tâche SAFE à l'état STOP, sauf si l'option **Démarrage automatique en mode RUN** est sélectionnée.

**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).
- Toutes les variables forcées sont initialisées à leur valeur par défaut.
- Restauration de la dernière valeur des variables de l'application.
- Configuration de %S1 (WARMSTART) sur 1.
- Réinitialisation des connexions entre le PAC et la CPU.

- 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, son exécution reprend depuis le début après le démarrage à chaud.

**⚠AVERTISSEMENT**

**FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT**

Assurez-vous que la sélection de l'option **Démarrage automatique en mode RUN** est compatible avec le comportement correct de votre système ; dans le cas contraire, désactivez-la.

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

# Tâches du PAC de sécurité M580

## Introduction

Un PAC 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 PAC de sécurité M580 prend en charge les tâches suivantes :

- FAST
- SAFE
- MAST
- AUX0
- AUX1

## Caractéristiques des tâches

Caractéristiques des tâches prises en charge par le PAC 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 1500 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 la fonction CCOTF est activée (option **Modification en ligne en mode RUN ou STOP** sélectionnée dans l'onglet **Configuration** de la boîte de dialogue des propriétés de la CPU), la valeur minimale de **Chien de garde** est de 64 ms.

3. Pris en charge par les PAC de sécurité BMEP58•040S autonomes. Non pris en charge par les PAC redondants de sécurité BMEH58•040S.

4. Les PAC de sécurité BMEP58•040S autonomes prennent en charge les modèles temporels cycliques et périodiques. Les PAC de sécurité BMEH58•040S redondants prennent uniquement en charge le modèle périodique.

## Priorité des tâches

Les PAC de sécurité 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) opèrent dans la même zone de mémoire, tandis que la tâche SAFE est exécutée dans une zone de mémoire distincte qui lui est propre. 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), la CPU et le coprocesseur passe 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 la tâche SAFE, définissez un temps d'exécution le plus court possible pour la tâche FAST. Utilisez une valeur de chien de garde FAST peu supérieure à la période d'exécution FAST.

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

## Création d'un projet de sécurité M580

### Création d'un projet de sécurité M580

#### Création d'un projet de sécurité M580

En mode Safety, le menu **Générer** de Control Expert comporte les trois commandes ci-dessous, ainsi qu'une commande de signature SAFE :

| Commande | Description |
|---|---|
| **Générer le projet** | 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.<br>**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.<br>**NOTE:**<br>• Exécutez cette commande uniquement si les modules d'E/S de sécurité sont déverrouillés, page 148.<br>• 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 140 pour l'application sécurisée.<br>**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 PAC de sécurité M580 - autonomes et Hot Standby - incluent un mécanisme permettant de générer une empreinte algorithmique SHA256 de l'application sécurisée : la signature de source SAFE. Lors du transfert de l'application du PC vers le PAC, Control Expert compare la signature de source SAFE du PC à celle du PAC afin de déterminer si l'application sécurisée du PC est identique à celle du PAC ou différente.

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.

**Modifications de configuration :** Les actions de configuration suivantes entraînent une modification de la signature :

| **Équipement** | **Action** |
|---|---|
| CPU de sécurité | Changement de référence de CPU via **Remplacer le processeur...** |
| | Changement de version de CPU via **Remplacer le processeur...** |
| | Modification d'un paramètre de la CPU dans l'onglet **Configuration** ou **Redondance d'UC**. |
| | Modification d'un paramètre dans un onglet quelconque du module de communication Ethernet de la CPU (**Sécurité**, **Configuration IP**, **RSTP**, **SNMP**, **NTP**, **Port de service**, **Safety** ...). |
| Coprocesseur de sécurité | Non applicable, car le coprocesseur n'est pas configurable. |
| Autre module de sécurité | **Ajout**/**Suppression**/**Déplacement** d'un module :<br>• directement (via une commande)<br>• 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** (par exemple, **Détection de court-circuit vers 24 V**, **Détection de fil ouvert**) et dans le volet gauche de l'éditeur (par exemple, **Fonction**, **Repli**). |
| | Modification de l'ID du module via la commande **Renouveler les ID et Regénérer tout**. |
| | Modification du nom de l'instance de DDT d'équipement |
| Module CIP Safety | **Ajout**/**Suppression** d'un module. |

| Équipement | Action |
|---|---|
| | 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 maître de la CPU. |
| | Modification du nom de l'instance de DDT 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 :<br>• Déplacement d'un rack contenant un équipement de sécurité<br>• Déplacement d'un bus ou d'une station contenant un équipement de sécurité |

**Modifications de valeur :** Sauf indication contraire, les éléments suivants interviennent dans le calcul de la signature de source SAFE. Une modification de leur valeur entraîne un changement de signature :

| Type | Eléments |
|---|---|
| Programme | Tâche SAFE et sections de code associées |
| Variables | Variables de zone SAFE et attributs associés |
| DDT | Attributs de DDT SAFE, à l'exception des attributs de date et version |
| | Variables contenues dans chaque DDT, 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 | Toutes les **Options du projet** pour lesquelles **Portée** = sécurité. |
| Paramètres de portée commune | Les **Options du projet** suivantes pour lesquelles **Portée** = commune : |
| | **Variables**<br>• Chiffres en début autorisés<br>• Jeu de caractères<br>• Autoriser l'utilisation du front sur EBOOL<br>• Autoriser INT/DINT à la place de ANY_BIT<br>• Autoriser l'extraction de bits pour BYTE, INT, UINT, DINT, UDINT, WORD et DWORD<br>• Représentation directe des variables de tableau<br>• Activer la scrutation rapide de tendance<br>• Forcer l'initialisation des références |
| | **Programme > Langages > Commun** |

| Type | Eléments |
|---|---|
| | • Autoriser les procédures<br>• Autoriser les commentaires imbriqués<br>• Autoriser les affectations en cascade [a:=b:=c] (ST/LD)<br>• Autoriser les paramètres vides dans les appels informels (ST/IL)<br>• Maintenir les liens de sortie sur les EF désactivées (EN=0)<br>• Afficher les commentaires complets d'élément de structure |
| | **Programme > Langages > LD**<br>• Détection de front par scrutation unique pour EBOOL |
| | **Général > Heure**[1]<br>• Fuseau horaire personnalisé<br>• Fuseau horaire<br>• Décalage<br>• Régler automatiquement l'horloge sur l'heure d'été<br>◦ Tous les paramètres DEBUT et FIN sous Régler automatiquement l'horloge sur l'heure d'été |
| 1. Ces variables ne sont pas exportées, mais toute modification de leurs valeurs modifie la signature partielle de la configuration. | |

## Gestion de la signature de source SAFE

La signature de source SAFE est gérée dans Control Expert en accédant à la fenêtre **Outils > Options du projet**, puis à **Général > Options de génération** et en sélectionnant l'une des options suivantes dans **Gestion de la signature SAFE** :

- **Automatique** (option par défaut) : une nouvelle signature de source SAFE est générée chaque fois qu'une commande **Générer** est exécutée.
- **A la demande de l'utilisateur** : une nouvelle signature de source SAFE est générée lorsque la commande **Générer > Mettre à jour la signature SAFE** est exécutée.

  **NOTE:** Si vous sélectionnez **A la demande de l'utilisateur**, Control Expert génère 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.

## Transfert d'une application du PC vers l'automate

Lorsque vous téléchargez une application du PC vers le PAC, Control Expert compare la signature de source SAFE de l'application téléchargée avec celle de l'application présente dans le PAC. Control Expert se comporte comme suit :

| Nouvelle signature SAFE | Signature SAFE dans le PAC | Control Expert affiche |
|---|---|---|
| Toute valeur | Pas d'application | Confirmation de transfert |
| Toute valeur (sauf 0) | 0 | Confirmation de transfert |
| 0 | 0 | Confirmation de transfert |
| 0 | Toute valeur (sauf 0) | Confirmation de transfert, puis "Cette action réinitialisera la signature SAFE", puis nouvelle confirmation de transfert |
| XXXX = YYYY[2] | YYYY | Confirmation de transfert |
| XXXX ≠ YYYY[3] | YYYY | Confirmation de transfert, puis "Cette action modifiera l'application SAFE", puis nouvelle confirmation de 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 PAC (YYYY) sont IDENTIQUES.

3. L'application sécurisée du PC (XXXX) et l'application sécurisée du PAC (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 :

- Onglet **Propriétés du projet > Identification** : Dans le **Navigateur de projet**, cliquez avec le bouton droit sur **Projet** et sélectionnez **Propriétés**.
- Onglet **Ecran de l'automate > Informations** (voir EcoStruxure™ Control Expert, Modes de fonctionnement) : Dans le **Navigateur de projet**, accédez à **Projet > Configuration > Bus automate > <CPU>**, cliquez avec le bouton droit et sélectionnez **Ouvrir**, puis ouvrez l'onglet **Animation**.
- Boîte de dialogue **Comparaison PC < - - > Automate** (voir EcoStruxure™ Control Expert, Modes de fonctionnement) : Sélectionnez cette commande à partir du menu **Automate**.
- Boîte de dialogue **Transfért du projet vers l'automate** : Sélectionnez cette commande à partir du menu **Automate** (ou dans la boîte de dialogue **Comparaison PC < - - > Automate**.

# Différences entre la signature de source SAFE et le SAId

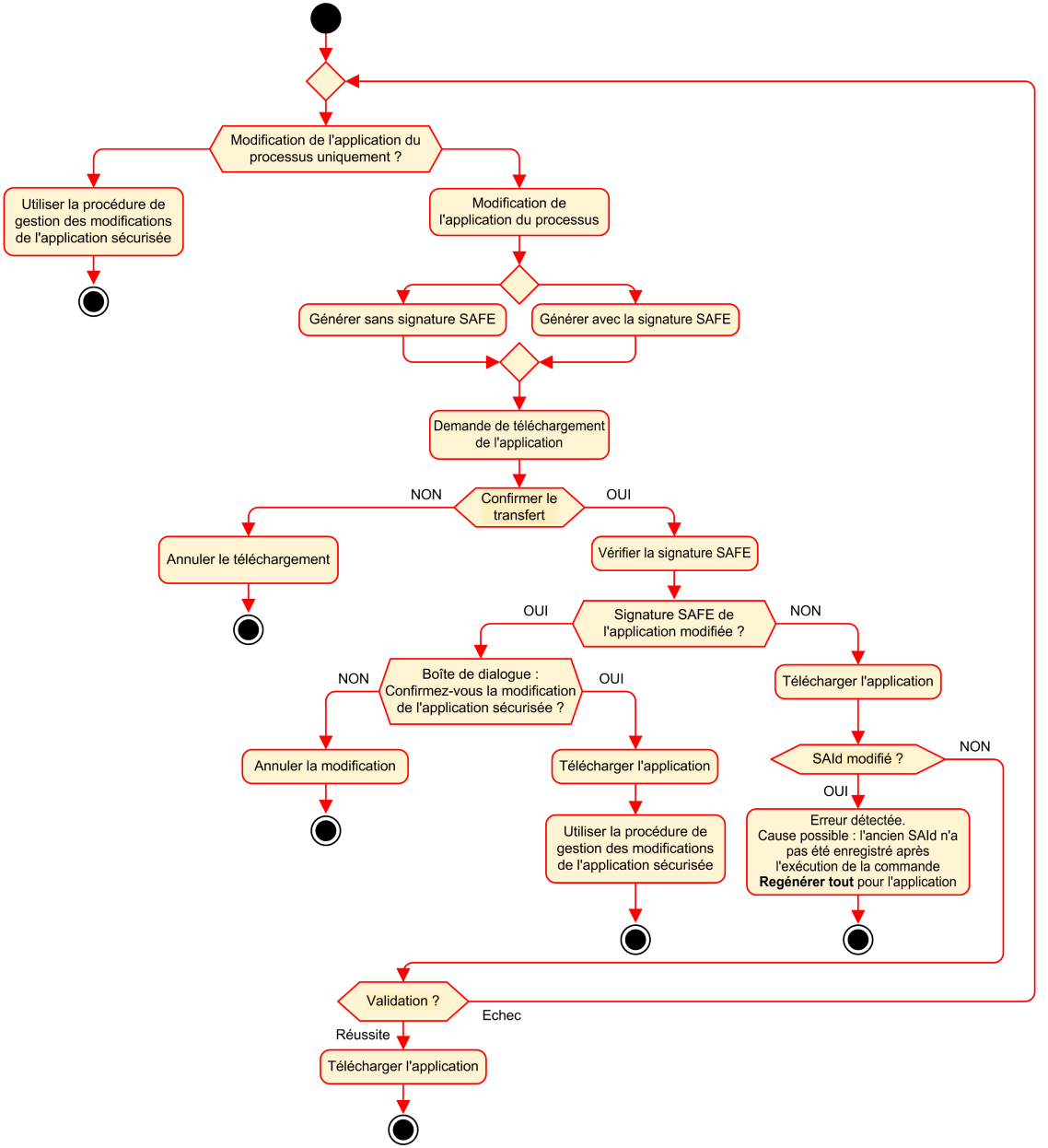
La signature de source SAFE a été introduite afin de vérifier *théoriquement* que l'application sécurisée n'a pas changé. Utilisez cette fonction chaque fois que l'application du processus est modifiée, page 146 pour éviter toute modification indésirable de l'application sécurisée.

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.

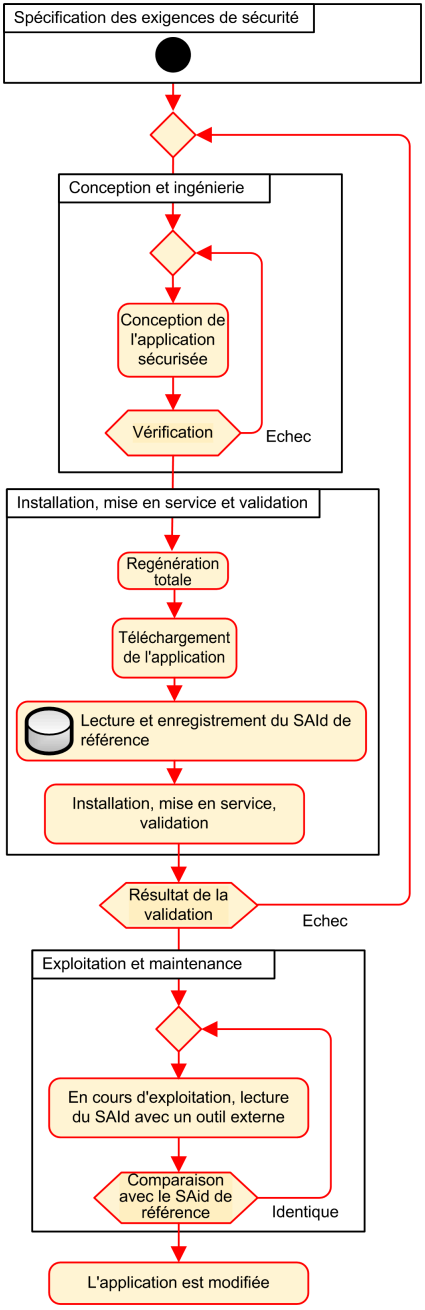
Le SAId peut être évalué en cours d'exécution seulement. Il est calculé deux fois et comparé par la CPU et par le coprocesseur, sur la base du code binaire exécuté par l'application sécurisée. Comme le SAId est sensible à toutes les modifications, y compris celles engendrées par une commande **Regénérer tout** après un changement de génération, utilisez une commande **Regénérer tout** pour créer une version de référence de l'application sécurisée. Ce processus, page 147 vous permet d'utiliser l'option de génération de votre choix (**Regénérer tout**, **Générer le projet** en mode local ou connecté) pour les modifications de l'application de processus qui n'incluent pas de modification du SAId.

Le SAId constitue la meilleure méthode pour vérifier que l'application sécurisée est bien celle qui a été validée. La valeur de SAId n'est pas testée automatiquement par l'application. Pour cette raison, vérifiez régulièrement le SAId par un moyen approprié (par exemple, à l'aide de Control Expert ou d'une IHM) en lisant la sortie du bloc fonction S_SYST_STAT_MX ou le contenu du mot système %SW169, page 225.

# 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 comporte un bouton de verrouillage de configuration, page 77 situé en haut de la face avant du module. Ce bouton de verrouillage permet d'empêcher toute modification indésirable de la configuration du module d'E/S. Par exemple, le verrouillage de la configuration actuelle du module d'E/S peut bloquer une tentative de configuration frauduleuse ou simplement protéger le module contre les erreurs de configuration.

Pour atteindre le niveau d'intégrité de la sécurité (SIL) souhaité, verrouillez chaque module d'E/S de sécurité après sa configuration et avant de commencer ou de reprendre des opérations.

**⚠AVERTISSEMENT**

**PERTE DE NIVEAU D'INTÉGRITÉ DE LA SÉCURITÉ (SIL)**

Verrouillez chaque module d'E/S de sécurité après sa configuration et avant de commencer 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 :

| Étape | Action |
|---|---|
| 1 | Connectez Control Expert au PAC de sécurité M580. |
| 2 | Utilisez la commande **Transférer le projet depuis l'automate** pour charger le projet du PAC dans Control Expert. |
| 3 | Dans la fenêtre **Bus automate** de Control Expert, ouvrez chaque module d'E/S de sécurité de niveau 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 sa configuration est la même qu'à 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, page 77 durant plus de 3 secondes, puis relâchez le bouton. |
| 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 :

| Étape | Action |
|---|---|
| 1 | Remplacez le module d'E/S de sécurité SIL3 par un module neuf. |
| 2 | Connectez Control Expert au PAC de sécurité M580 en mode de maintenance, page 122. |
| 3 | Dans la fenêtre **Bus automate** de Control Expert, ouvrez chaque module d'E/S de sécurité de niveau 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 sa configuration n'a pas changé par rapport à 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, page 77 durant plus de 3 secondes, puis relâchez-le. |
| 6 | Vérifiez dans une 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 :

| Étape | Action |
|---|---|
| 1 | Connectez Control Expert au PAC de sécurité M580 en mode de maintenance, page 122. |
| 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 automate** de Control Expert, ouvrez chaque module d'E/S de sécurité de niveau 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 sa configuration n'a pas changé par rapport à 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, page 77 durant plus de 3 secondes, puis relâchez-le. |
| 7 | Vérifiez dans une 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 **Automate** de Control Expert, commandez au PAC d'entrer en mode de sécurité, page 121. |

# 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 135.

# Utilisation des tables d'animation dans Control Expert

## Tables d'animation et écrans des opérateurs

### Introduction

Un PAC de sécurité M580 prend en charge trois types de tables d'animation, correspondant chacun 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 processus.
- 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 les espaces 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 de sécurité s'affiche sous la forme "SAFE.<nom de variable>".
  - Une variable de données de l'espace de nom de processus s'affiche sous la forme "PROCESS.<nom de variable>".
  - Une variable de données située dans l'espace de nom global (ou d'application) s'affiche sous la forme d'un <nom de variable> uniquement, sans le préfixe d'espace de nom.

Les données de processus et de sécurité d'un PAC 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 dépendent des éléments suivants :

- Espace de nom (sécurité ou processus) où se trouvent les variables de données.

- Mode de fonctionnement (sécurité ou maintenance) du PAC de sécurité M580.

Quand Control Expert est connecté au PAC 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 une table d'animation de processus ou globale lorsque le PAC 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 lorsque le PAC 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 lorsque le PAC 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/exclure les tables d'animation dans le transfert : dans Control Expert, sélectionnez **Outils > Paramètres du projet...** puis, dans la boîte de dialogue **Paramètres du projet...**, accédez à **Paramètres du projet > Général > Données intégrées de l'automate > Informations d'Upload > 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 PAC 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 maintenance 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 propose deux méthodes pour créer des tables d'animation dans 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 l'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 crée une 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 globale dans le **Navigateur de projet** en cliquant avec le bouton droit sur le dossier **Tables d'animation** et en sélectionnant **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 depuis un éditeur de données vers 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 à partir de l'**Editeur de données de sécurité**, de l'**Editeur de données de processus** ou de l'**Editeur de données globales**.
- *Boîte de dialogue Sélection d'instance* : Vous pouvez double-cliquer sur une ligne de la table d'animation, puis cliquer sur le bouton portant des points de suspension 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 sécurité.
  - 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 les données sur un écran d'exploitation (IHM, SCADA ou application FactoryCast, par exemple) de la même manière que vous accédez aux données d'une table d'animation. Les variables de données disponibles pour la sélection sont celles incluses dans le dictionnaire de données Control Expert.

Pour activer le dictionnaire de données, ouvrez la fenêtre **Outils > Paramètres du projet...** puis, dans la zone **Portée > commune**, sélectionnez **Général > Données intégrées de l'automate > Dictionnaire de données**.

Le dictionnaire de données permet à l'opérateur de visualiser les variables de données sur l'écran d'exploitation :

- Les variables de l'espace de nom Sécurité incluent toujours le préfixe "SAFE" et ne sont accessibles qu'en utilisant le format "SAFE.<nom de variable>".
- Les variables de l'espace de nom Global ou Application n'incluent pas de préfixe et sont accessibles en utilisant uniquement le "<nom de variable>".
- L'option **Utilisation de l'espace de nom de processus** détermine la manière d'accéder aux variables d'espace de nom de processus à partir d'un écran d'exploitation.
  - 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 "PROCESS.<nom de variable>".
  - Si vous désélectionnez **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 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 individuels.

| ⚠ AVERTISSEMENT |
| --- |
| **FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT**<br>• Assurez-vous que les paramètres de projet de l'application sont corrects.<br>• Vérifiez la syntaxe permettant d'accéder aux variables dans les différents espaces de nom.<br>**Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou 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 utilisez la syntaxe suivante pour accéder aux variables portant le même nom :
  - "PROCESS.<nom de variable>" pour les variables déclarées dans l'espace de noms de processus.
  - "<nom de 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 *Création et configuration d'une tâche* dans le document *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 prend en charge uniquement 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 : 10 à 500 ms par incréments de 10 ms, avec 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 x Taille_Données_Safe) + 2 ms (pour BME•584040S et BME•586040S)
  - (0,273 x Taille_Données_Safe) + 2 ms (pour BME•582040S)

  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 :
  - $(K1 \times Tâche_{ko} + K2 \times Tâche_{DFB}) / 500$

  Dans cette formule :
  - $Tâche_{DFB}$ = nombre de DFB déclarés dans la partie sécurisée de l'application.
  - $Tâche_{ko}$ = 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'UC 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 Autonome - Guide de planification du système pour architectures courantes*.
- Par défaut, les valeurs Taille_Données_Safe 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. Les valeurs Taille$_{ko}$ et Taille_Données_Safe sont supposées égales. | | | | | |

**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* (voir Modicon M580, Manuel de sécurité).

Pour obtenir des informations sur la priorité d'exécution de la tâche SAFE, consultez la rubrique *Tâches du PAC de sécurité M580*, page 136.

## 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<br>– : 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 *Boîte de dialogue des propriétés pour les 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 %.

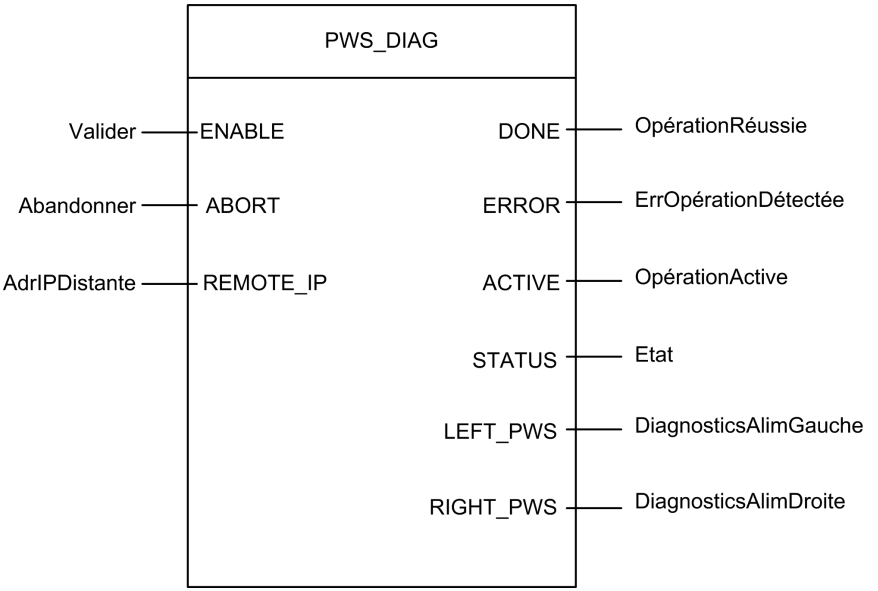
  **NOTE:** Pas de permutation si 0 %.

- 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

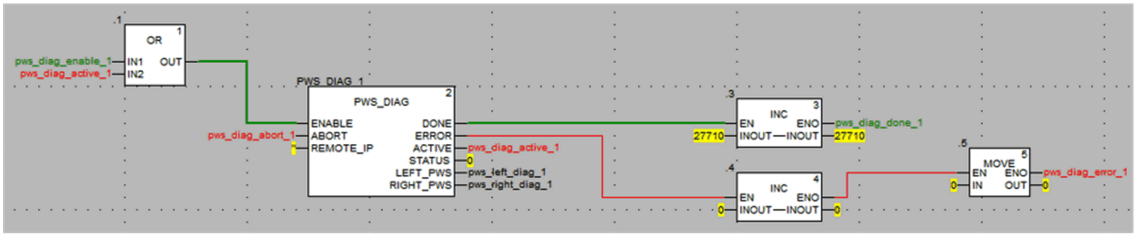
Paramètres d'entrée :

| 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 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

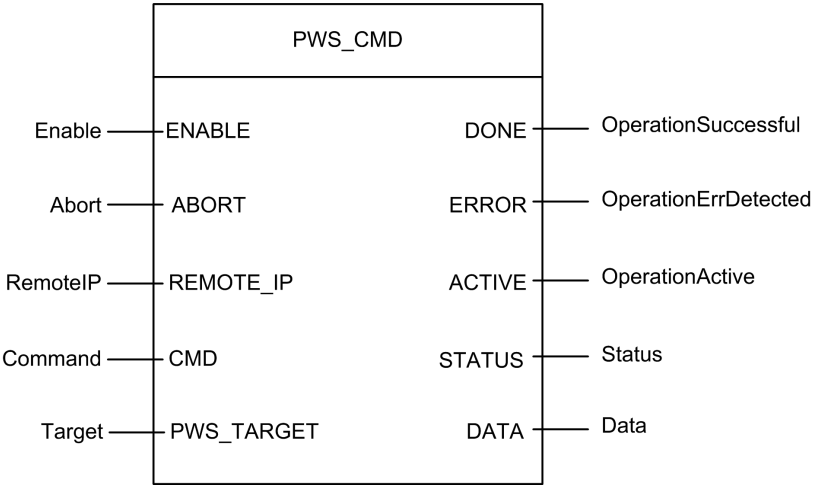
Le bloc fonction PWS_CMD peut être utilisé pour émettre deux commandes :

- 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:

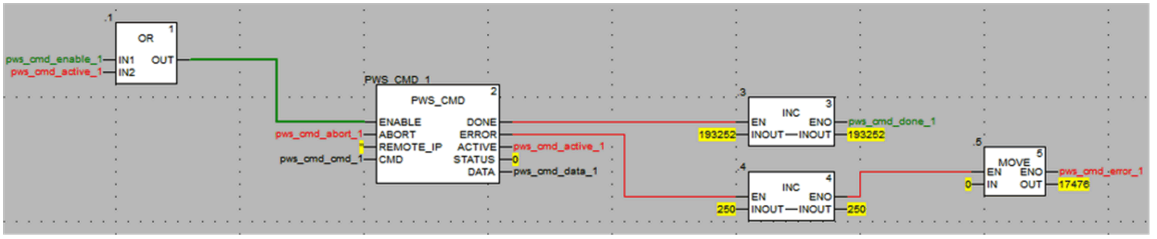
| Nom du paramètre | Type de données | Description |
|---|---|---|
| ENABLE | BOOL | Si ce paramètre est activé, l'opération est activée. |
| ABORT | BOOL | Si ce paramètre est activé, l'opération active est abandonnée. |
| REMOTE_IP | STRING | Adresse IP ("ip1.ip2.ip3.ip4") de la station contenant le 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 :<br>• 1 = permutation<br>• 3 = effacement |
| PWS_TARGET | BYTE | Alimentation vers l'adresse :<br>• 1 = gauche<br>• 2 = droite<br>• 3 = les deux |

Paramètres de sortie:

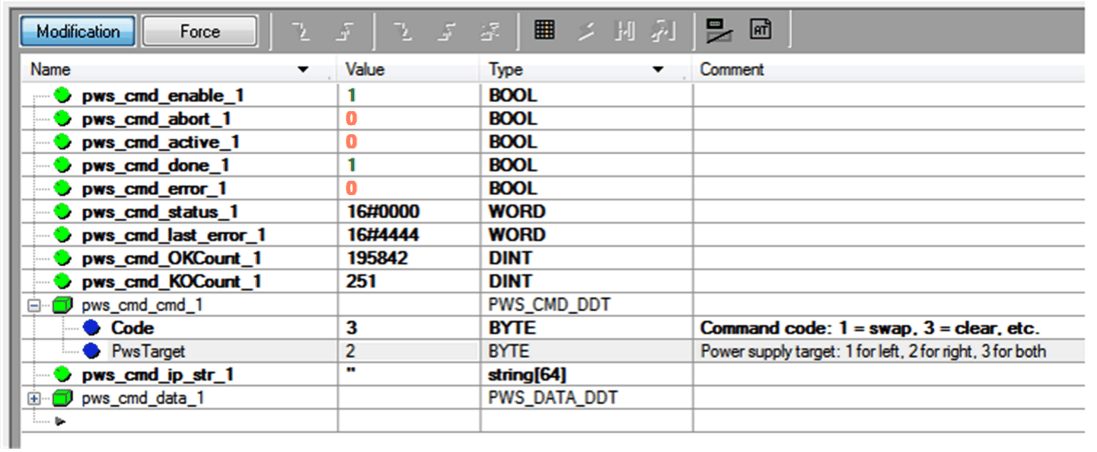
| Nom du paramètre | Type de données | Description |
|---|---|---|
| DONE | BOOL | Activé lorsque l'opération s'est déroulée correctement. |
| ERROR | BOOL | Activé lorsque l'opération a été abandonnée suite à un échec. |
| ACTIVE | BOOL | Activé lorsque l'opération est active. |
| STATUS | WORD | Identifiant 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.

## Protection de l'application

### Présentation

EcoStruxure Control Expert comporte une fonction de protection par mot de passe qui empêche tout accès non autorisé à l'application.

Le mot de passe de EcoStruxure Control Expert protège les actions suivantes :

- Ouvrir l'application dans EcoStruxure Control Expert.
- Se connecter au contrôleur dans EcoStruxure Control Expert.

La définition d'un mot de passe d'application permet d'éviter toute action de modification, de téléchargement ou d'ouverture indésirable des fichiers d'application. Le mot de passe est crypté au sein de l'application.

Outre la définition du mot de passe, vous pouvez crypter les fichiers `.STU`, `.STA` et `.ZEF`. La fonction de cryptage de fichiers dans EcoStruxure Control Expert permet d'éviter les modifications et renforce la protection de la propriété intellectuelle. L'option de cryptage de fichier est protégée par un mécanisme de mot de passe.

**NOTE:** Lorsqu'un contrôleur est géré dans le cadre d'un projet système, le mot de passe de l'application et le cryptage des fichiers sont désactivés dans Control Expert et gérés avec Topology Manager.

### Construction du mot de passe

La construction du mot de passe est conforme à la norme IEEE 1686-2013.

Un mot de passe valide contient au moins 8 caractères et inclut au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère non alphanumérique ($, %, &, etc.).

**NOTE:** Le mot de passe de l'application est effacé lorsque vous exportez un projet non crypté vers un fichier `.XEF` ou `.ZEF`.

# Créer un nouveau projet

Par défaut, une nouvelle application (projet) EcoStruxure Control Expert Classic présente les caractéristiques suivantes :

- Le projet n'est pas protégé par un mot de passe.
- Les fichiers d'application du projet ne sont pas cryptés.

Lorsque vous créez un projet, vous pouvez exercer ces options dans la boîte de dialogue **Application de sécurité** :

- Définissez un mot de passe pour l'application.
- Appliquez le cryptage à vos fichiers d'application via un mot de passe de cryptage de fichier.

Accédez à la boîte de dialogue **Application de la sécurité** dans EcoStruxure Control Expert Classic :

| Étape | Action |
|---|---|
| 1 | Ouvrez la fenêtre **Nouveau projet** dans EcoStruxure Control Expert (**Fichier > Nouveau**). |
| 2 | Sélectionnez un contrôleur pour le projet. |
| 3 | Cliquez sur **OK** pour ouvrir la boîte de dialogue **Application de la sécurité**. |
| 4 | Choisissez de créer un projet avec ou sans mot de passe, puis suivez les instructions dans le tableau correspondant ci-dessous. |

**Aucun mot de passe :** Créez un projet sans mot de passe d'application :

| Étape | Action |
|---|---|
| 1 | Accédez à la boîte de dialogue **Application de la sécurité**. |
| 2 | Dans la boîte de dialogue **Application de la sécurité**, sélectionnez **Je ne souhaite pas définir de mot de passe d'application pour ce projet**. |
| 3 | Cliquez sur **OK** pour continuer. |

**Avec mots de passe :** Utilisez les instructions ci-dessous pour créer un projet avec un mot de passe d'application et un mot de passe de cryptage de fichier (optionnel).

**NOTE:** Vous pouvez configurer une date d'expiration pour ces mots de passe dans l'onglet **Stratégies** de Security Editor.

| Étape | Action |
|---|---|
| 1 | Accédez à la boîte de dialogue **Application de la sécurité**. |
| 2 | Dans la zone **Mot de passe d'application**, créez un mot de passe pour protéger l'application et renforcer la sécurité d'accès au contrôleur :<br>• Saisissez un mot de passe dans le champ **Saisie**.<br>• Saisissez à nouveau le mot de passe dans le champ **Confirmation**. |
| 3 | Dans la zone **Mot de passe cryptage de fichier**, créez un mot de passe pour protéger la propriété intellectuelle :<br>• Saisissez un mot de passe dans le champ **Saisie**.<br>• Saisissez à nouveau le mot de passe dans le champ **Confirmation**.<br>**NOTE:**<br>• Vous ne pouvez configurer un mot de passe de cryptage de fichier qu'après avoir configuré un mot de passe d'application.<br>• Utilisez des mots de passe différents pour le mot de passe d'application et le mot de passe de cryptage de fichier. |
| 4 | Appuyez sur le bouton **OK** pour appliquer vos paramètres de mot de passe et fermer la boîte de dialogue **Application de la sécurité**. |

**NOTE:**

- Si aucun mot de passe n'est entré, les fichiers d'application ne sont pas cryptés. Dans ce cas, lors de la prochaine ouverture de votre projet EcoStruxure Control Expert , la boîte de dialogue **Mot de passe** s'ouvre. Pour accéder à votre projet, ne tapez pas de mot de passe et cliquez sur **OK**. Suivez ensuite les instructions ci-dessous pour définir un mot de passe d'application et activer le cryptage de fichier.
- Vous pouvez créer ou modifier un mot de passe d'application à tout moment, mais vous ne pouvez pas effacer le mot de passe d'application lorsqu'un mot de passe de cryptage de fichier est configuré pour le projet.

## Définir un mot de passe d'application

Définissez le mot de passe d'application :

| Étape | Action |
|---|---|
| 1 | Cliquez avec le bouton droit de la souris sur **Projet** dans le **Navigateur de projet**. |
| 2 | Sélectionnez **Propriétés** dans le menu contextuel pour ouvrir la fenêtre **Propriétés du projet**. |

| Étape | Action |
|---|---|
| 3 | Sélectionnez l'onglet **Protection du projet et du contrôleur**. |
| 4 | Dans le champ **Application**, cliquez sur **Modifier le mot de passe...** pour ouvrir la fenêtre **Modifier le mot de passe**. |
| 5 | Saisissez le nouveau mot de passe dans le champ **Saisie**. |
| 6 | Saisissez la confirmation du nouveau mot de passe dans le champ **Confirmation**. |
| 7 | Cliquez sur **OK** pour confirmer. |
| 8 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer les modifications. |

## Modifier le mot de passe d'application

Modifiez le mot de passe de protection d'application :

| Étape | Action |
|---|---|
| 1 | Cliquez avec le bouton droit de la souris sur **Projet** dans le **Navigateur de projet**. |
| 2 | Sélectionnez la commande **Propriétés** dans le menu contextuel pour ouvrir la fenêtre **Propriétés du projet** . |
| 3 | Sélectionnez l'onglet **Protection du projet et du contrôleur**. |
| 4 | Dans le champ **Application** , cliquez sur **Modifier le mot de passe ...** pour ouvrir la fenêtre **Modifier le mot de passe**. |
| 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 | Saisissez la confirmation du nouveau mot de passe dans le champ **Confirmation**. |
| 8 | Cliquez sur **OK** pour confirmer. |
| 9 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer les modifications. |

## Supprimer le mot de passe d'application

L'effacement du mot de passe de l'application n'est pas autorisé tant que le cryptage des fichiers est activé.

Effacez le mot de passe d'application :

| Étape | Action |
|---|---|
| 1 | Cliquez avec le bouton droit de la souris sur **Projet** dans le **Navigateur de projet**. |
| 2 | Sélectionnez la commande **Propriétés** dans le menu contextuel pour ouvrir la fenêtre **Propriétés du projet**. |
| 3 | Sélectionnez l'onglet **Protection du projet et du contrôleur**. |
| 4 | Dans le champ **Application** , cliquez sur **Effacer le mot de passe ...** pour ouvrir la fenêtre **Mot de passe**. |
| 5 | Saisissez le mot de passe dans le champ **Mot de passe**. |
| 6 | Cliquez sur **OK** pour confirmer. |
| 7 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer les modifications. |

## Fonction de verrouillage automatique

Pour activer l'option de limitation de l'accès à l'outil EcoStruxure Control Expert après une période d'inactivité configurée, sélectionnez (cochez) la case **Verrouillage auto** et saisissez une valeur dans le champ **Minutes avant verrouillage** pour définir le délai d'inactivité.

Une fonction optionnelle de verrouillage automatique limite l'accès à l'outil de programmation du logiciel EcoStruxure Control Expert au terme du délai d'inactivité configuré. Vous pouvez activer la fonction de verrouillage automatique à l'aide de la case à cocher **Verrouillage auto** et sélectionner le délai d'inactivité dans le champ **Minutes avant verrouillage**.

Si la fonction de verrouillage automatique est activée et que le délai d'inactivité configuré est écoulé, une boîte de dialogue s'affiche pour saisir le mot de passe de l'application. Derrière cette boîte de dialogue,, tous les éditeurs restent dans la même position. Par conséquent, toute personne peut lire le contenu des fenêtres EcoStruxure Control Expert , mais ne peut pas poursuivre le travail avec EcoStruxure Control Expert.

**NOTE:** Si vous n'attribuez pas de mot de passe au projet, la boîte de dialogue ne s'affiche pas.

## Condition de demande de mot de passe

**Ouverture d'une application (projet) existante :**

Lorsque vous ouvrez un fichier d'application, une boîte de dialogue **Mot de passe de l'application** s'ouvre.

Saisissez le mot de passe, puis cliquez sur **OK**.

**Résultat** : Si le mot de passe est correct, l'application s'ouvre. Si le mot de passe est incorrect, un message à l'écran indique qu'il n'est pas valide, et une nouvelle boîte de dialogue **Mot de passe de l'application** s'ouvre.

Si vous cliquez sur **Annuler**, l'application n'est pas ouverte.

Accès à l'application dans EcoStruxure Control Expert après un verrouillage automatique, lorsque EcoStruxure Control Expert n'est pas connecté au contrôleur ou lorsque le projet dans EcoStruxure Control Expert est *identique* à celui du contrôleur :

Lorsque le délai de verrouillage automatique est écoulé, une boîte de dialogue **Mot de passe de l'application** s'ouvre.

Saisissez le mot de passe, puis cliquez sur **OK**.

**Résultat** : Si le mot de passe est correct, EcoStruxure Control Expert redevient actif. Si le mot de passe est incorrect, une boîte de message indique qu'il n'est pas valide, et une nouvelle boîte de dialogue **Mot de passe de l'application** s'ouvre.

Cliquez sur **Fermer** pour fermer l'application non enregistrée.

Accès à l'application dans le contrôleur après un verrouillage automatique, lorsque EcoStruxure Control Expert est connecté au contrôleur et que l'application dans EcoStruxure Control Expert est *différente* de celle du contrôleur :

À la connexion, si l'application du logiciel EcoStruxure Control Expert et l'application du contrôleur ne sont pas identiques, une boîte de dialogue **Mot de passe de l'application** s'ouvre.

Saisissez le mot de passe, puis cliquez sur **OK**.

**Résultat** : Si le mot de passe est correct, la connexion est établie. Si le mot de passe est incorrect, une boîte de message indique qu'un mot de passe erroné a été saisi, et une nouvelle boîte de dialogue **Mot de passe de l'application** s'ouvre.

Si vous cliquez sur **Annuler**, la connexion n'est pas établie.

**NOTE:** À la connexion, si l'application logicielle EcoStruxure Control Expert et l'application du contrôleur sont identiques, aucune demande de mot de passe n'est requise. Si aucun mot de passe n'a été saisi initialement (champ laissé vide lors de la création du projet), cliquez sur **OK** pour établir la connexion à l'invite du mot de mot de passe.

**NOTE:**

- Après trois tentatives avec un mot de passe invalide, un délai d'attente croissant est imposé entre les tentatives suivantes. Le délai augmente de 15 secondes à 1 heure, avec un incrément doublant après chaque tentative avec un mot de passe invalide.
- En cas d'oubli du mot de passe, consultez les instructions pour récupérer les mots de passe perdus, page 186.

# Activer l'option de cryptage de fichier

**NOTE:** Définissez un mot de passe pour l'application *avant* d'activer le cryptage des fichiers.

Activez l'option de cryptage de fichiers :

| Étape | Action |
|---|---|
| 1 | Cliquez avec le bouton droit de la souris sur **Projet** dans le **Navigateur de projet**. |
| 2 | Sélectionnez la commande **Propriétés** dans le menu contextuel pour ouvrir la fenêtre **Propriétés du projet**. |
| 3 | Sélectionnez l'onglet **Protection du projet et du contrôleur**. |
| 4 | Cochez la case **Cryptage des fichiers actif** pour ouvrir la fenêtre **Créer un mot de passe** . |
| 5 | Saisissez le mot de passe dans le champ **Saisie**. |
| 6 | Confirmez le mot de passe dans le champ **Confirmation**. |
| 7 | Cliquez sur **OK** pour confirmer. |
| 8 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer les modifications. |

# Désactiver l'option de cryptage de fichiers

Désactivez l'option de cryptage de fichiers :

| Étape | Action |
|---|---|
| 1 | Cliquez avec le bouton droit de la souris sur **Projet** dans le **Navigateur de projet**. |
| 2 | Sélectionnez la commande **Propriétés** dans le menu contextuel pour ouvrir la fenêtre **Propriétés du projet**. |
| 3 | Sélectionnez l'onglet **Protection du projet et du contrôleur**. |
| 4 | Décochez *(décochez)* la case **Cryptage de fichier actif** pour ouvrir la fenêtre **Mot de passe de cryptage de fichier**. |
| 5 | Entrez le mot de passe et cliquez sur **OK** pour confirmer que l'application n'est pas cryptée. |
| 6 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer toutes les modifications. |

# Modifier le mot de passe de cryptage de fichier

Modifiez le mot de passe de cryptage de fichier :

| Étape | Action |
|---|---|
| 1 | Cliquez avec le bouton droit de la souris sur **Projet** dans le **Navigateur de projet**. |
| 2 | Sélectionnez la commande **Propriétés** dans le menu contextuel pour ouvrir la fenêtre **Propriétés du projet**. |
| 3 | Sélectionnez l'onglet **Protection du projet et du contrôleur**. |
| 4 | Dans le champ **Cryptage de fichier**, cliquez sur **Modifier le mot de passe...** pour ouvrir la fenêtre **Modifier le mot de passe**. |
| 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 | Saisissez la confirmation du nouveau mot de passe dans le champ **Confirmation**. |
| 8 | Cliquez sur **OK** pour confirmer. |
| 9 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer les modifications. |

## Effacer le du mot de passe de cryptage de fichier

Effacez le mot de passe de cryptage de fichier :

| Étape | Action |
|---|---|
| 1 | Cliquez avec le bouton droit de la souris sur **Projet** dans le **Navigateur de projet**. |
| 2 | Sélectionnez la commande **Propriétés** dans le menu contextuel pour ouvrir la fenêtre **Propriétés du projet**. |
| 3 | Sélectionnez l'onglet **Protection du projet et du contrôleur**. |
| 4 | Dans le champ **Cryptage de fichier**, cliquez sur **Effacer le mot de passe...** pour ouvrir la fenêtre **Mot de passe**. |
| 5 | Saisissez le mot de passe dans le champ **Mot de passe**. |
| 6 | Cliquez sur **OK** pour confirmer. |
| 7 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer les modifications. |

**NOTE:** En cas d'oubli du mot de passe de cryptage de fichier, consultez les instructions pour récupérer les mots de passe perdus, page 186.

## Règles de compatibilité

Vous ne pouvez pas ouvrir les fichiers d'application `.STA` et `.ZEF` cryptés dans EcoStruxure Control Expert 15.0 Classic ou des versions antérieures.

Vous ne pouvez pas importer des fichiers d'application `.ZEF` cryptés dans EcoStruxure Control Expert avec Topology Manager.

Les règles de compatibilité entre la version de l'application et la version EcoStruxure Control Expert/Unity Pro s'appliquent aux fichiers `.ZEF` exportés sans cryptage.

**NOTE:** Lorsque le cryptage des fichiers est activé pour votre projet, vous ne pouvez pas enregistrer les fichiers d'application archivés (`.STA`) sans cryptage.

# Protection par mot de passe des zones de sécurité

## Présentation générale

Les contrôleurs de sécurité incluent une fonction de protection par mot de passe de la zone de sécurité, qui est accessible dans la boîte de dialogue **Propriétés** du projet. Cette fonction permet de protéger les éléments du projet situés dans la zone de sécurité du projet de sécurité opérationnel.

**NOTE:** Lorsque la fonction de protection par mot de passe de la zone de sécurité est active, les parties sécurisées de l'application ne sont pas modifiables.

Aucune modification des parties de la zone de sécurité n'est autorisée lorsque la fonction de protection par mot de passe de la zone de sécurité est activée :

| **Zone de sécurité** | **Action interdite (hors ligne ET en ligne)** |
|---|---|
| Configuration | Modifier les caractéristiques du contrôleur |
| | Ajouter, supprimer, modifier un module de sécurité dans le rack |
| | Modifier l'alimentation de sécurité |
| Types | Créer, supprimer, modifier un DDT de sécurité |
| | Changer un attribut de DDT : de NOT SAFE->defined SAFE-STATE |
| | Changer un attribut de DDT : de defined SAFE-STATE->NOT SAFE |
| | Créer, supprimer, modifier un bloc de fonction dérivé (DFB, Derived Function Block) de sécurité |
| | Modifier un attribut de DFB : de NOT SAFE->defined SAFE-STATE |
| | Changer un attribut de DFB : de defined SAFE-STATE->NOT SAFE |
| Programme-SAFE | Toute modification sous le nœud **Variables et instances FB** |
| | Créer une tâche |
| | Importer une tâche |
| | Modifier une tâche |
| | Créer une section |

| Zone de sécurité | Action interdite (hors ligne ET en ligne) |
|---|---|
| | Supprimer une section |
| | Importer une section |
| | Modifier une section |
| Paramètres du projet. | Modifier les paramètres du projet SAFE |
| | Modifier les paramètres du projet COMMON |

**NOTE:**

- Si un mot de passe de sécurité est activé, entrez-le pour passer en mode Maintenance.
- Si le mot de passe de l'application et le verrouillage automatique sont activés : lorsque le mot de passe de l'application est demandé en raison d'une inactivité et que EcoStruxure Control Expert Classic est connecté au contrôleur de sécurité en mode Programmation et que le contrôleur de sécurité fonctionne en mode Maintenance, le contrôleur de sécurité passe en mode Sécurité au bout de 5 minutes si vous n'entrez pas le mot de passe.

**NOTE:**

- Si un mot de passe de sécurité est activé, entrez-le pour passer en mode Maintenance.
- Si le mot de passe de l'application et le verrouillage automatique sont activés :

  **Lorsque les conditions suivantes sont vraies, le contrôleur de sécurité passe en mode de sécurité au bout de cinq minutes si vous ne saisissez pas le mot de passe**:

  Le mot de passe de l'application est demandé pour cause d'inactivité.

  Ecostruxure Control Expert Classic est connecté au contrôleur de sécurité en mode Programmation.

  Le contrôleur de sécurité fonctionne en mode Maintenance.

## Cryptage

Le mot de passe de la zone de sécurité utilise le chiffrement standard SHA-256.

# Fonction de mot de passe de la zone de sécurité ou droits utilisateur du projet de sécurité fonctionnel

L'activation du mot de passe de la zone de sécurité et la mise en œuvre des droits utilisateur créés dans l'**Éditeur de sécurité** sont des fonctions mutuellement exclusives, comme suit :

- Si l'utilisateur qui lance EcoStruxure Control Expert s'est vu attribuer un profil d'utilisateur, cet utilisateur peut accéder aux zones de sécurité de l'application de sécurité s'il entre le mot de passe de la zone de sécurité et a reçu des droits d'accès dans l'**Éditeur de sécurité**.
- Si des profils d'utilisateur n'ont pas été attribués, un utilisateur peut accéder aux zones de sécurité de l'application de sécurité s'il entre le mot de passe correspondant.

# Voyants LED de EcoStruxure Control Expert

L'état de la fonction de protection de la zone sécurisée est indiqué dans le nœud **Programme-SAFE** du **du Navigateur de projet** :

- Un cadenas verrouillé indique qu'un mot de passe de sécurité a été créé et activé.
- Un cadenas déverrouillé indique qu'un mot de passe de sécurité a été créé mais pas activé.

  **NOTE:** Si l'application de sécurité est fermée puis rouverte, le mot de passe de la zone de sécurité est automatiquement activé lors de la réouverture.
- L'absence de cadenas indique qu'aucun mot de passe de sécurité n'a été créé.

# Compatibilité

À compter de la version 14.0 de EcoStruxure Control Expert , la fonction de mot de passe de la zone de sécurité existe pour les contrôleurs liés à la sécurité du M580 à partir de la version 2.80 du micrologiciel.

**NOTE:**

- Le programme d'application `.STU`, `.STA`, et les fichiers `.ZEF` (qui sont créés à partir de la version 14.0 de EcoStruxure Control Expert ) ne peuvent pas être ouverts dans version la 13.1 ou une version antérieure de Unity Pro.
- Le remplacement d'un contrôleur de sécurité M580 dans la version 14.0 d'une application EcoStruxure Control Expert a l'impact suivant :
  - La mise à niveau du micrologiciel 2.70 vers la version 2.80 (ou des versions ultérieures prise en charge) ajoute la fonction de mot de passe de la zone de sécurité dans l'onglet **Protection du programme et de la sécurité** de la fenêtre **Propriétés > du projet**.
  - La rétrogradation du micrologiciel 2.80 (et des versions comparables postérieures à la version 2.70) supprime la fonctionnalité de mot de passe de la zone de sécurité.

## Activation de la protection et création du mot de passe

Pour activer la protection des sections et créer le mot de passe, procédez comme suit :

| Etape | Action |
|---|---|
| 1 | Dans le navigateur de projet, cliquez avec le bouton droit sur **Projet**. |
| 2 | Dans le menu contextuel, choisissez la commande **Propriétés**.<br><br>**Résultat** : La fenêtre **Propriétés de projet** apparaît.. |
| 3 | Sélectionnez l'onglet **Protection du programme et Safety**. |
| 4 | Dans la zone **Sécurité**, activez la protection en cochant la case **Protection active**.<br><br>**Résultat** : : la boîte de dialogue **Modification du mot de passe** s'affiche. |
| 5 | Saisissez un mot de passe dans le champ **Saisie**. |
| 6 | Confirmez le mot de passe dans le champ **Confirmation**. |
| 7 | Cliquez sur **OK** pour confirmer. |
| 8 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer toutes les modifications.<br><br>Si vous cliquez sur **Annuler** dans la fenêtre **Propriétés de Projet**, toutes les modifications sont annulées. |

## Changement de mot de passe

Pour modifier le mot de passe de protection des sections du projet, procédez comme suit :

| Etape | Action |
|---|---|
| 1 | Dans le navigateur de projet, cliquez avec le bouton droit sur **Projet**. |
| 2 | Dans le menu contextuel, choisissez la commande **Propriétés**.<br>**Résultat** : La fenêtre **Propriétés de projet** apparaît.. |
| 3 | Sélectionnez l'onglet **Protection du programme et Safety**. |
| 4 | Dans la zone **Sécurité**, cliquez sur **Changer mot de passe...**.<br>**Résultat** : La boîte de dialogue **Modification du mot de passe** s'affiche : |
| 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 | Saisissez la confirmation du nouveau mot de passe dans le champ **Confirmation**. |
| 8 | Cliquez sur **OK** pour confirmer. |
| 9 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer toutes les modifications.<br>Si vous cliquez sur **Annuler** dans la fenêtre **Propriétés de Projet**, toutes les modifications sont annulées. |

## Suppression du mot de passe

Pour supprimer le mot de passe de protection des sections du projet, procédez comme suit :

| Etape | Action |
|---|---|
| 1 | Dans le navigateur de projet, cliquez avec le bouton droit sur **Projet**. |
| 2 | Dans le menu contextuel, choisissez la commande **Propriétés**.<br>**Résultat** : La fenêtre **Propriétés de projet** apparaît.. |
| 3 | Sélectionnez l'onglet **Protection du programme et Safety**. |
| 4 | Dans la zone **Sécurité**, cliquez sur **Effacer mot de passe...**.<br>**Résultat** : la boîte de dialogue **Contrôle d'accès** s'ouvre : |
| 5 | Saisissez l'ancien mot de passe dans le champ **Mot de passe**. |
| 6 | Cliquez sur **OK** pour confirmer. |
| 7 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer toutes les modifications.<br>Si vous cliquez sur **Annuler** dans la fenêtre **Propriétés de Projet**, toutes les modifications sont annulées. |

# Protection des unités de programme, sections et sous-programmes

## Présentation

La fonction de protection est accessible depuis l'écran **Propriétés** du projet en mode local.

Cette fonction permet de protéger les éléments du programme (sections et unités de programme).

**NOTE:** la protection n'est active qu'une fois activée dans le projet.

**NOTE:** la protection du projet s'applique uniquement aux éléments de programme marqués. Elle ne permet pas d'éviter :

- la connexion à l'UC,
- le chargement d'applications à partir de l'UC,
- la modification de la configuration,
- l'ajout d'unités de programme et/ou de sections,
- la modification de la logique au sein d'une nouvelle section (non protégée).

## Activation de la protection et création du mot de passe

Pour activer la protection et créer le mot de passe des sections et unités de programme, procédez comme suit :

| Etape | Action |
|---|---|
| 1 | Dans le navigateur de projet, cliquez avec le bouton droit sur **Projet**. |
| 2 | Dans le menu contextuel, choisissez la commande **Propriétés**.<br>**Résultat** : la fenêtre **Propriétés de Projet** s'ouvre. |
| 3 | Sélectionnez l'onglet **Protection du programme et Safety**. |
| 4 | Dans le champ **Sections et unités de programme**, activez la protection en cochant la case **Protection active**.<br>**Résultat** : la boîte de dialogue **Modification du mot de passe** s'ouvre : |
| 5 | Saisissez un mot de passe dans le champ **Saisie**. |
| 6 | Saisissez la confirmation du mot de passe dans le champ **Confirmation**. |
| 7 | Cochez la case **Chiffré** si une protection renforcée du mot de passe est nécessaire.<br>**NOTE:** Un projet dont le mot de passe est chiffré ne peut pas être édité dans Unity Pro V4.0 et les versions antérieures. |

| Etape | Action |
|---|---|
| 8 | Cliquez sur **OK** pour confirmer. |
| 9 | Cliquez sur **OK** ou sur **Appliquer** dans la fenêtre **Propriétés de Projet** pour confirmer toutes les modifications.<br><br>Si vous cliquez sur **Annuler** dans la fenêtre **Propriétés de Projet**, toutes les modifications sont annulées. |

## Remarques

Si un élément de programme est configuré avec une protection (lecture ou lecture/écriture), un cadenas fermé apparaît au niveau de l'élément lorsque la protection est activée.

Si l'élément de programme est configuré avec une protection mais que celle-ci est désactivée, un cadenas ouvert est affiché au niveau de l'élément.

## Changement de mot de passe

Pour changer le mot de passe de protection des sections et des unités de programme, procédez comme suit :

| Etape | Action |
|---|---|
| 1 | Dans le navigateur de projet, cliquez avec le bouton droit sur **Projet**. |
| 2 | Dans le menu contextuel, choisissez la commande **Propriétés**.<br><br>**Résultat** : la fenêtre **Propriétés de Projet** s'ouvre. |
| 3 | Sélectionnez l'onglet **Protection du programme et Safety**. |
| 4 | Dans le champ **Sections et unités de programme**, cliquez sur **Changer mot de passe**.<br><br>**Résultat** : la boîte de dialogue **Modification du mot de passe** s'ouvre : |
| 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 | Cochez la case **Chiffré** si une protection renforcée du mot de passe est nécessaire.<br><br>**NOTE:** Un projet dont le mot de passe est chiffré ne peut pas être édité dans Unity Pro V4.0 et les versions antérieures.<br><br>Unity Pro est l'ancien nom de Control Expert pour les versions 13.1 et antérieures. |

| Etape | Action |
|---|---|
| 9 | Cliquez sur **OK** pour confirmer. |
| 10 | Cliquez sur **OK** ou sur **Appliquer** dans la fenêtre **Propriétés de Projet** pour confirmer toutes les modifications.<br><br>Si vous cliquez sur **Annuler** dans la fenêtre **Propriétés de Projet**, toutes les modifications sont annulées. |

## Suppression du mot de passe

Pour supprimer le mot de passe de protection des sections et des unités de programme, procédez comme suit :

| Etape | Action |
|---|---|
| 1 | Dans le navigateur de projet, cliquez avec le bouton droit sur **Projet**. |
| 2 | Dans le menu contextuel, choisissez la commande **Propriétés**.<br><br>**Résultat** : la fenêtre **Propriétés de Projet** s'ouvre. |
| 3 | Sélectionnez l'onglet **Protection du programme et Safety**. |
| 4 | Dans le champ **Sections et unités de programme**, cliquez sur **Effacer mot de passe**.<br><br>**Résultat** : la boîte de dialogue **Contrôle d'accès** s'ouvre : |
| 5 | Saisissez l'ancien 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.<br><br>Si vous cliquez sur **Annuler** dans la fenêtre **Propriétés de Projet**, toutes les modifications sont annulées. |

# 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**.<br><br>**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...**.<br><br>**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.<br><br>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**.<br><br>**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...**.<br><br>**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`**.<br><br>Si vous cliquez sur **Annuler** dans la fenêtre **Propriétés de Projet**, toutes les modifications sont annulées. |

# Stockage de données/protection Web

## Présentation

La protection par mot de passe permet d'éviter tout accès indésirable à la zone de stockage des données de la carte mémoire SD (si une carte valide est insérée dans la CPU).

Pour les CPU Modicon M580 dans un projet créé par Control Expert, en fonction de la version :

- Version antérieure à 15.1 : vous pouvez fournir une protection par mot de passe pour l'accès au stockage des données.
- À compter de la version 15.1, vous pouvez fournir une protection par mot de passe pour l'accès aux diagnostics Web et au stockage de données.

  **NOTE:** Lorsqu'un contrôleur est géré dans le cadre d'un projet système, le mot de passe de **Diagnostic Web / Stockage des données** est désactivé dans Control Expert et il doit être géré à l'aide du Topology Manager.

# 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 d'accès au Web/stockage des données est stocké dans le module à condition que l'option **Cryptage de fichier** soit sélectionnée.

# Changement de mot de passe

Vous pouvez modifier un mot de passe à tout moment.

**NOTE:** Le mot de passe d'accès au Web/stockage de données a une valeur par défaut dans l'application Control Expert. Cette valeur par défaut dépend de la version de Control Expert :

- versions antérieures à 15.1 de **`datadownload:`** Control Expert
- versions à partir de 15.1 de **`webuser:`** Control Expert

La modification du mot de passe par défaut est obligatoire ou facultative selon la version de micrologiciel du module :

- À compter du de la version V4.01 du micrologiciel, vous devez modifier le mot de passe par défaut pour le stockage de données/l'accès Web, faute de quoi vous n'aurez plus la possibilité de générer l'application Control Expert.
- Pour le micrologiciel antérieur à la version 4.01, il n'est pas obligatoire mais fortement recommandé de modifier le mot de passe par défaut pour le stockage de données/l'accès Web

Procédez comme suit pour modifier le mot de passe d'accès au stockage de données/Web :

| Etape | Action |
|---|---|
| 1 | Dans le navigateur de projet, cliquez avec le bouton droit sur **Projet**. |
| 2 | Dans le menu contextuel, choisissez la commande **Propriétés**.<br><br>**Résultat** : La fenêtre **Propriétés de projet** apparaît.. |
| 3 | Sélectionnez l'onglet **Protection du projet et du contrôleur**. |
| 4 | Dans le champ **Stockage des données** (ou **Diagnostic Web / Stockage des données**)liquez sur **Modifier le mot de passe...**.<br><br>**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**. |

| Etape | Action |
|---|---|
| 7 | Saisissez la confirmation du nouveau mot de passe dans le champ **Confirmation**. |
| 8 | Cliquez sur **OK** pour confirmer. |
| 9 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer toutes les modifications.<br><br>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 stockage des données/Web dans l'application Control Expert si le mot de passe actuel est confirmé.

Pour réinitialiser le mot de passe, procédez comme suit :

| Etape | Action |
|---|---|
| 1 | Dans le navigateur de projet, cliquez avec le bouton droit sur **Projet**. |
| 2 | Dans le menu contextuel, choisissez la commande **Propriétés**.<br><br>**Résultat** : La fenêtre **Propriétés de projet** apparaît.. |
| 3 | Sélectionnez l'onglet **Protection du projet et du contrôleur**. |
| 4 | Dans le champ **Stockage des données** (ou **Diagnostic Web/Stockage des données**), cliquez sur **Réinitialiser le mot de passe...**.<br><br>**Résultat** : La fenêtre **Mot de passe** apparaît. |
| 5 | Saisissez le mot de passe actuel dans le champ **Mot de passe**. |
| 6 | Cliquez sur **OK** pour confirmer. |
| 7 | Cliquez sur **OK** ou **Appliquer** dans la fenêtre **Propriétés du projet** pour confirmer toutes les modifications. Le nouveau mot de passe est le mot de passe par défaut : **`datadownload`**.<br><br>Si vous cliquez sur **Annuler** dans la fenêtre**Propriétés de Projet**, toutes les modifications sont annulées. |

# 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 `SHIFT+F2`.<br><br>**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.<br><br>**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 `SHIFT+F2`.<br><br>**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.<br><br>**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`.<br><br>**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.<br><br>**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`.<br><br>**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.<br><br>**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.<br><br>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`.<br><br>**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.<br><br>**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.<br><br>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`.<br><br>**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.<br><br>**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.<br><br>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`.<br><br>**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.<br><br>**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.<br><br>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 d'accès **Security Editor** qui permet de limiter et de contrôler l'accès aux stations de travail où le logiciel EcoStruxure Control Expert est installé. Cette section décrit les fonctions de cet outil spécifiquement conçu pour les projets de sécurité M580.

## Gestion de l'accès à EcoStruxure Control Expert

### Introduction

Schneider Electric fournit l'outil de configuration *Security Editor* qui permet de gérer l'accès au logiciel Control Expert installé sur une station de travail. L'utilisation de l'outil de configuration *Security Editor* pour gérer l'accès au logiciel Control Expert est facultative.

**NOTE:** La gestion d'accès s'applique au matériel (généralement une ou plusieurs stations de travail) sur lequel le logiciel EcoStruxure Control Expert est installé et non au projet (qui dispose de son propre système de protection).

Pour plus d'informations, consultez *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. Si vous créez ou modifiez un profil utilisateur, vous devez vérifier que toutes les modifications nécessaires sont correctement effectuées.

### Catégories d'utilisateurs

L'outil **Security Editor** prend en charge deux catégories d'utilisateurs :

- **SecurityAdmin :** L'administrateur de la sécurité (*SecurityAdmin*) est la seule personne pouvant gérer la sécurité d'accès au logiciel. L'utilisateur *SecurityAdmin* spécifie qui peut accéder au logiciel et avec quels droits d'accès. Lors de l'installation du logiciel EcoStruxure Control Expert sur la station de travail, seul l'utilisateur *SecurityAdmin* peut accéder à la configuration de la sécurité sans limitation de droits (sans mot de passe).

  **NOTE:** Le nom d'utilisateur réservé à l'administrateur de la sécurité est *SecurityAdmin*. Cet utilisateur assume le rôle d'administration qui était pris en charge par le *superutilisateur Supervisor* dans les versions héritées (antérieures à la version 15.3) de EcoStruxure Control Expert.

- **Utilisateurs :** Les utilisateurs du logiciel sont définis dans une liste établie par l'utilisateur *SecurityAdmin* si la sécurité d'accès à EcoStruxure Control Expert est active. 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

Le profil utilisateur contient tous les droits d'accès d'un utilisateur. Le profil utilisateur peut être personnalisé par l'utilisateur *SecurityAdmin* ou il peut être créé en appliquant un profil préconfiguré fourni avec l'outil **Security Editor**.

## Profils utilisateur préconfigurés

L'outil **Security Editor** contient les profils 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 ne peut accéder au projet qu'en mode lecture, mais il peut modifier l'adresse du PAC. L'utilisateur peut également copier ou charger le projet. |
| **Marche** | ✓ | — | 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.) du programme de processus. |
| **Sécurité_Marche** | — | ✓ | L'utilisateur a des droits d'accès similaires au profil **Marche** mais par rapport au programme de sécurité, avec les exceptions suivantes :<br>• Le transfert des valeurs de données vers le PAC n'est pas autorisé.<br>• Il est possible de commander au programme de sécurité de passer en mode de maintenance. |
| **Réglage** | ✓ | — | L'utilisateur a les mêmes droits qu'avec le profil **Marche**, plus la possibilité de charger un projet (transfert vers le PAC) et de modifier le mode de marche du PAC (**Run**, **Stop**, etc.). |
| **Sécurité_Réglage** | — | ✓ | L'utilisateur a des droits d'accès similaires au profil **Réglage** mais par rapport au programme de sécurité, avec les exceptions suivantes :<br>• Le transfert des valeurs de données vers le PAC n'est pas autorisé.<br>• Il est possible de commander au programme de sécurité de passer en mode de maintenance. |

| Profil | Type de programme applicable | | Description |
|---|---|---|---|
| | Processus | Sécurité | |
| **Mise au point** | ✓ | — | L'utilisateur a les mêmes droits qu'avec le profil **Réglage**, plus la possibilité d'utiliser les outils de mise au point. |
| **Sécurité_Mise au point** | — | ✓ | L'utilisateur a des droits d'accès similaires au profil **Mise au point** mais par rapport au programme de sécurité, avec les exceptions suivantes :<br>• L'arrêt et le démarrage du programme ne sont pas autorisés.<br>• La mise à jour des valeurs d'initialisation n'est pas autorisée.<br>• Le transfert des valeurs de données vers le PAC n'est pas autorisé.<br>• Le forçage des entrées, sorties ou bits internes n'est pas autorisé.<br>• Il est possible de commander au programme de sécurité de passer en mode de maintenance. |
| **Programme** | ✓ | — | L'utilisateur a les mêmes droits qu'avec le profil **Mise au point**, plus la possibilité de modifier le programme. |
| **Sécurité_ Programme** | — | ✓ | L'utilisateur a des droits d'accès similaires au profil **Programme** mais par rapport au programme de sécurité, avec les exceptions suivantes :<br>• L'arrêt et le démarrage du programme ne sont pas autorisés.<br>• La mise à jour des valeurs d'initialisation n'est pas autorisée.<br>• Le transfert des valeurs de données vers le PAC n'est pas autorisé.<br>• La restauration du projet sur le PAC à partir d'une sauvegarde n'est pas autorisée.<br>• Le forçage des entrées, sorties ou bits internes n'est pas autorisé.<br>• Il est possible de commander au programme de sécurité de passer en mode de maintenance. |
| **Désactivé** | ✓ | ✓ | L'utilisateur ne peut pas accéder au projet. |

## Attribution d'un utilisateur préconfiguré

L'utilisateur *SecurityAdmin* peut attribuer un utilisateur préconfiguré (dérivé d'un profil préconfiguré) à un utilisateur spécifique dans l'onglet **Utilisateurs** de l'outil **Security Editor**. Les utilisateurs préconfigurés disponibles sont les suivants :

- Utilisateur_Sécurité_Réglage

- Utilisateur_Sécurité_Mise au point
- Utilisateur_Sécurité_Marche
- Utilisateur_Sécurité_Programme
- Utilisateur_Réglage
- Utilisateur_Mise au point
- Utilisateur_Marche
- Utilisateur_Programme

Consultez la rubrique *Fonctions utilisateur* (voir EcoStruxure™ EcoStruxure Control Expert, Security Editor, Guide d'exploitation) pour plus d'informations sur la façon dont un utilisateur *SecurityAdmin* peut attribuer un profil préconfiguré.

# Droits d'accès

## Introduction

Cette rubrique présente les droits d'accès disponibles pour chaque profil 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/mise au point
- Bibliothèques
- Modification globale
- Modification élémentaire d'une variable
- Modification élémentaire de données composées DDT
- Modification élémentaire d'un type DFB
- Modification élémentaire d'une instance de DFB
- Editeur de configuration de bus
- Editeur de configuration d'entrées/sorties
- Écrans d’exploitation.
- Cybersécurité
- Sécurité

**NOTE:** Les droits d'accès EcoStruxure Control Expert Classic s'appliquent également à Control Expert.

## Topology Manager

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_Réglage | Mise au point | Sécurité_Mise au point | Marche | Sécurité_Marche | Programme | Sécurité_Programme |
| **Create projet système** | – | – | – | – | – | – | ✓ | ✓ |
| **Modify projet système** | – | – | – | – | – | – | ✓ | ✓ |
| **Import projet système** | – | – | – | – | – | – | ✓ | ✓ |
| **Delete projet système** | – | – | – | – | – | – | ✓ | ✓ |
| **Manage projet système settings** | – | – | – | – | – | – | ✓ | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Services de projet

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_Réglage | Mise au point | Sécurité_Mise au point | Marche | Sécurité_Marche | Programme | Sécurité_Programme |
| **Créer un nouveau projet** | – | – | – | – | – | – | ✓ | ✓ |
| **Ouvrir un projet existant** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Enregistrer un projet** | – | – | – | – | – | – | ✓ | ✓ |
| **Enregistrer sous un projet** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Importer un projet** | – | – | – | – | – | – | ✓ | ✓ |
| **Générer hors ligne** | – | – | – | – | – | – | ✓ | ✓ |

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **Arrêter une génération en ligne** | – | – | – | – | – | – | ✓ | ✓ |
| **Exécuter une génération en ligne** | – | – | – | – | – | – | ✓ | ✓ |
| **Démarrer, arrêter ou initialiser le PAC*** | ✓ | – | ✓ | – | – | – | ✓ | ✓ |
| **Mettre à jour les valeurs d'initialisation avec les valeurs courantes (données non liées à la sécurité uniquement)** | – | – | ✓ | – | – | – | ✓ | ✓ |
| **Transférer un projet depuis le PAC** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Transférer un projet vers le PAC** | ✓ | ✓ | ✓ | ✓ | – | – | ✓ | ✓ |
| **Transférer des valeurs de données depuis un fichier vers le PAC (données non liées à la sécurité uniquement)** | ✓ | – | ✓ | – | ✓ | – | ✓ | ✓ |
| **Restaurer une sauvegarde de projet dans le PAC** | – | – | – | – | – | – | ✓ | ✓ |
| **Enregistrer vers une sauvegarde de projet dans le PAC** | – | – | – | – | – | – | ✓ | ✓ |
| **Définir l'adresse** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Modifier les options** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

* Seules les tâches de processus sont lancées ou arrêtées. Pour un PAC non lié à la sécurité, cela signifie que le PAC est démarré ou arrêté. Pour un PAC de sécurité M580, cela signifie que les tâches autres que SAFE sont démarrées ou arrêtées.

✓ : Inclus

– : Non inclus

## Réglage/Mise au point

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **Modifier les valeurs de variable** | ✓ | – | ✓ | | ✓ | | ✓ | ✓ |
| **Modifier les valeurs des variables de sécurité** | – | ✓ | – | ✓ | – | ✓ | – | ✓ |
| **Forcer les bits internes** | – | – | ✓ | – | – | – | ✓ | ✓ |
| **Forcer les sorties** | – | – | ✓ | – | – | – | ✓ | ✓ |
| **Forcer les entrées** | – | – | ✓ | – | – | – | ✓ | ✓ |
| **Gestion des tâches** | – | – | ✓ | – | – | – | ✓ | ✓ |
| **Gestion de la tâche SAFE** | – | – | – | ✓ | – | – | – | ✓ |
| **Modification de la durée de cycle de la tâche** | ✓ | – | ✓ | | ✓ | – | ✓ | ✓ |
| **Modification de la durée du cycle de la tâche SAFE** | – | ✓ | – | ✓ | – | ✓ | – | ✓ |
| **Suppression de message dans le visualiseur** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Mise au point de l'exécutable** | – | – | ✓ | ✓ | – | – | ✓ | ✓ |
| **Remplacer une variable de projet** | – | – | – | – | – | – | ✓ | ✓ |
| **Remplacer une variable de projet de sécurité** | – | – | – | – | – | – | – | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Bibliothèques

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **Créer des bibliothèques ou des familles** | – | – | – | – | – | – | ✓ | ✓ |
| **Créer des bibliothèques ou des familles de sécurité** | – | – | – | – | – | – | – | ✓ |
| **Supprimer des bibliothèques ou des familles** | – | – | – | – | – | – | ✓ | ✓ |
| **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 dans une bibliothèque** | – | – | – | – | – | – | ✓ | ✓ |
| **Supprimer un objet dans une bibliothèque de sécurité** | – | – | – | – | – | – | – | ✓ |
| **Obtenir un objet d'une bibliothèque** | – | – | – | – | – | – | ✓ | ✓ |
| **Obtenir un objet d'une bibliothèque de sécurité** | – | – | – | – | – | – | – | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Modification globale

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **Modifier la documentation** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Modifier la vue fonctionnelle** | – | – | – | – | – | – | ✓ | ✓ |
| **Modifier les tables d'animation** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Modifier les valeurs des constantes** | ✓ | – | ✓ | – | ✓ | – | ✓ | ✓ |
| **Modifier les valeurs des constantes de sécurité** | – | ✓ | – | ✓ | – | ✓ | – | ✓ |
| **Modifier la structure du programme** | – | – | – | – | – | – | ✓ | ✓ |
| **Modifier la structure du programme de sécurité** | – | – | – | – | – | – | – | ✓ |
| **Modifier les sections du programme** | – | – | – | – | – | – | ✓ | ✓ |
| **Modifier les sections du programme de sécurité** | – | – | – | – | – | – | – | ✓ |
| **Modifier les paramètres du projet** | – | – | – | – | – | – | ✓ | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Modification élémentaire d'une variable

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **Ajout/suppression d'une variable** | – | – | – | – | – | – | ✓ | ✓ |
| **Ajout/suppression d'une variable de sécurité** | – | – | – | – | – | – | – | ✓ |
| **Modification d'attributs principaux d'une variable** | – | – | – | – | – | – | ✓ | ✓ |
| **Modification des attributs principaux d'une variable de sécurité** | – | – | – | – | – | – | – | ✓ |
| **Modification d'attributs secondaires d'une variable** | ✓ | – | ✓ | – | ✓ | – | ✓ | ✓ |
| **Modification des attributs secondaires d'une variable de sécurité** | – | ✓ | – | ✓ | – | ✓ | – | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Modification élémentaire de données composées DDT

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **Ajout/suppression de DDT** | – | – | – | – | – | – | ✓ | ✓ |
| **Modifications de DDT** | – | – | – | – | – | – | ✓ | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Modification élémentaire d'un type DFB

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **Ajout/suppression de type DFB** | – | – | – | – | – | – | ✓ | ✓ |
| **Ajout/suppression de type DFB de sécurité** | – | – | – | – | – | – | – | ✓ |
| **Modification de la structure d'un type DFB** | – | – | – | – | – | – | ✓ | ✓ |
| **Modification de la structure d'un type DFB de sécurité** | – | – | – | – | – | – | – | ✓ |
| **Modification des sections d'un type DFB** | – | – | – | – | – | – | ✓ | ✓ |
| **Modification des sections d'un type DFB de sécurité** | – | – | – | – | – | – | – | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Modification élémentaire d'une instance de DFB

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **Modification d'une instance de DFB** | – | – | – | – | – | – | ✓ | ✓ |
| **Modification d'une instance de DFB de sécurité** | – | – | – | – | – | – | – | ✓ |

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **Modification d'attributs secondaires d'une instance de DFB** | ✓ | – | ✓ | – | ✓ | – | ✓ | ✓ |
| **Modification d'attributs secondaires d'une instance de DFB de sécurité** | – | ✓ | – | ✓ | – | ✓ | – | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Editeur de configuration de bus

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **Modifier la configuration** | – | – | – | – | – | – | ✓ | ✓ |
| **Modifier la configuration de sécurité** | – | – | – | – | – | – | – | ✓ |
| **Apprentissage automatique de la configuration des E/S** | – | – | – | – | – | – | ✓ | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Editeur de configuration d'entrées/sorties

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **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 des paramètres** | – | – | ✓ | – | – | – | ✓ | ✓ |
| **Restaurer des paramètres** | – | – | ✓ | – | – | – | ✓ | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Ecrans d'exploitation

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_ Réglage | Mise au point | Sécurité_ Mise au point | Marche | Sécurité_ Marche | Programme | Sécurité_ Programme |
| **Modifier les écrans** | – | – | – | – | – | – | ✓ | ✓ |
| **Modifier les messages** | – | – | – | – | – | – | ✓ | ✓ |
| **Ajouter/supprimer des écrans ou des familles** | – | – | – | – | – | – | ✓ | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Cybersécurité

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_Réglage | Mise au point | Sécurité_Mise au point | Marche | Sécurité_Marche | Programme | Sécurité_Programme |
| **Créer ou modifier le mot de passe de l'application** | – | – | – | – | – | – | ✓ | ✓ |
| **Accéder au mode de maintenance** | – | ✓ | – | ✓ | – | ✓ | – | ✓ |
| **Adapter la temporisation de verrouillage automatique** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

## Sécurité

Les droits d'accès de cette catégorie sont les suivants :

| Droit d'accès | Profil utilisateur préconfiguré | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Réglage | Sécurité_Réglage | Mise au point | Sécurité_Mise au point | Marche | Sécurité_Marche | Programme | Sécurité_Programme |
| **Accéder au mode de maintenance** | – | ✓ | – | ✓ | – | ✓ | – | ✓ |
| ✓ : Inclus<br>– : Non inclus | | | | | | | | |

# Paramètres de projet de sécurité M580

## Présentation

Cette section décrit les paramètres de projet qui sont uniques pour un projet de sécurité M580 Control Expert.

## Paramètres de projet pour un projet de sécurité M580 dans Control Expert

### Paramètres de projet spécifiques à la portée

Sélectionnez **Outils > Paramètres de projet...** dans le menu principal de Control Expert pour ouvrir la fenêtre permettant de configurer et de visualiser les paramètres d'un projet de sécurité M580. Les paramètres de projet sont divisés en trois groupes en fonction de leur **Portée**, à savoir :

- **commun** : Ces paramètres s'appliquent à l'ensemble de l'application et peuvent avoir un impact sur les zones globales, de processus et de sécurité du projet.
- **processus**: Ces paramètres s'appliquent uniquement à la zone de processus du projet.
- **sécurité**: Ces paramètres s'appliquent uniquement à la zone de sécurité du projet.

Cette rubrique ne décrit que les parties de la fenêtre **Paramètres du projet** qui sont différentes par rapport à un projet M580 non lié à la sécurité. Consultez la section *Paramètres de projet* du manuel *Ecostruxure™ Control Expert - Modes de fonctionnement* pour plus d'informations sur les fonctionnalités communes aux projets M580 de sécurité et non liés à la sécurité.

### Paramètres de projet communs

Les paramètres de **Portée > commune** s'appliquent aux zones de projet globales, de sécurité et de processus, mais pas de la même manière que dans un projet M580 non lié à la sécurité :

| Groupe | Paramètre | Description |
|---|---|---|
| **Paramètres généraux :** | | |
| Options de génération | Mémoire de données libre (en Ko) | Ce champ est désactivé.<br>**NOTE:** Dans un système de sécurité M580, l'allocation des données est effectuée |

| Groupe | Paramètre | Description |
|---|---|---|
| | | dynamiquement, et il n'est pas nécessaire de réserver un bloc de données de taille fixe. |
| | Mode de connexion virtuelle | Le mode de connexion virtuelle est possible mais désactivé par défaut pour les contrôleurs de sécurité M580. Lorsque le mode de connexion virtuelle est activé, les modifications qui ne nécessitent pas de régénération du projet sont autorisées dans les zones du programme qui sont communes, liées au processus et liées à la sécurité. Pour interdire les modifications sur la zone du programme liée à la sécurité lorsque le mode de connexion virtuelle est activé, définissez un mot de passe de sécurité permettant la protection de cette zone.<br>**NOTE:**<br>• Pour les processeurs de sécurité M580, le mode de connexion virtuelle est fonctionnel, mais désactivé par défaut.<br>• L'utilisateur peut activer le mode de connexion virtuelle. Lorsque le mode de connexion virtuelle est actif, les modifications qui ne nécessitent pas de régénération du projet sont autorisées dans les parties du programme qui sont communes, liées au processus et liées à la sécurité. Si vous souhaitez interdire les modifications sur la partie du programme liée à la sécurité lorsque le mode de connexion virtuelle est actif, définissez un mot de passe de sécurité et activez cette protection dans les propriétés du projet. |
| Données intégrées de l'automate | Dictionnaire de données<br>• Utilisation de l'espace de nom de processus | Détermine la façon dont un écran d'exploitation permet d'accéder aux variables d'espace de nom de processus :<br>• Si cette option est sélectionnée, l'écran d'exploitation ne peut lire les variables de la zone de processus qu'en utilisant le format "PROCESS.<nom de variable>".<br>• Si cette option est désactivée, l'écran d'exploitation ne peut lire les variables de la zone de processus qu'en utilisant le format "<nom de variable>", sans le préfixe PROCESS.<br>**NOTE:** Toutes les variables de la zone de sécurité sont accessibles via le format "SAFE.<nom de variable>". |
| | Optimiser la modification en ligne des données | Applicable à :<br>• Programme de processus en mode de fonctionnement sécurité et maintenance.<br>• Programme de sécurité uniquement en mode de fonctionnement maintenance. |

| Groupe | Paramètre | Description |
|---|---|---|
| Diagnostics de l'automate | Informations de diagnostic Visualiseur de rack<br>• Noms de variables Visualiseur de rack | Ces paramètres sont disponibles pour les variables de processus et de sécurité. |
| | Informations Visualiseur de programme | Ce paramètre est disponible pour les sections de code de processus et sécurité. |
| Heure | Mode d'horodatage | Ce paramètre est disponible pour les programmes de processus et de sécurité, excepté que l'horodatage des variables de sécurité n'est pas pris en charge. |
| Paramètres de l'**Ecran d'exploitation** : | | |
| Ecran piloté | Affichage d'écrans pilotés par l'automate | Ce paramètre est disponible dans le PAC de sécurité M580 pour la variable sélectionnée. |

## Paramètres de projet communs qui ne concernent pas la zone de sécurité du projet

Les paramètres de **Portée > commune** suivants s'appliquent au programme de processus mais pas au programme de sécurité dans un projet de sécurité M580 :

| Groupe | Paramètre | Description |
|---|---|---|
| **Paramètres généraux :** | | |
| Fonctionnement de l'automate | Réinitialiser %M sur la transition Arrêt->Marche | Les sections de code LL984 ne sont pas prises en charge dans le programme de sécurité. |
| Configuration | Type de données d'E/S favori M580 (E/S locales) | Seul le type de données DDDT d'équipement est disponible pour les modules d'E/S de sécurité. |
| Paramètres des **Variables** : | | |
| – | Représentation directe des variables de tableau | L'accès %MW n'est pas pris en charge dans le programme de sécurité. |
| | Activer la scrutation rapide de tendance | L'outil d'analyse des tendances n'est pas pris en charge dans le programme de sécurité. Il est pris en charge uniquement dans la tâche MAST du programme de processus. |
| | Forcer l'initialisation des références | Les références ne sont pas autorisées dans le programme de sécurité. |
| Paramètres du **Programme** : | | |
| Langages<br>• Commun | Autoriser les commentaires imbriqués | Pris en charge uniquement pour les tâches non liées à la sécurité (MAST, FAST, AUX0 et AUX1) |

| Groupe | Paramètre | Description |
|---|---|---|
| | Autoriser les affectations en cascade [a:=b:=c] (ST/LD) | • Le langage ST, qui inclut le bloc opération, n'est pas pris en charge par le programme de sécurité.<br>• Le langage LD ne prend pas en charge les affectations en cascade dans le programme de sécurité |
| | Autoriser les paramètres vides dans les appels informels (ST/IL) | Les langages ST et IL ne sont pas pris en charge dans le programme de sécurité. |
| Langages<br>• ST | Autoriser les sauts et les étiquettes | Le langage ST n'est pas pris en charge dans le programme de sécurité. |

## Paramètres de projet ayant un impact différent sur les zones processus et sécurité

Les deux zones **Portée > sécurité** et **Portée > processus** présentent le même ensemble de paramètres de programme. Cependant, les paramètres suivants sont traités différemment dans chaque portée d'un projet de sécurité M580

| Groupe | Paramètre | Description |
|---|---|---|
| **Paramètres généraux :** | | |
| Options de génération | Code optimisé | • Activé pour la portée processus.<br>• Désactivé et désélectionné pour la portée sécurité. |
| | Gestion de la signature SAFE | • Désactivé pour la portée processus.<br>• Activé et réglé sur **Automatique** par défaut, pour la portée sécurité. |
| Diagnostic automate | Diagnostic application<br>• Niveau de diagnostic application | • Activé pour la portée processus.<br>• Désactivé et désélectionné pour la portée sécurité. |
| Paramètres des **Variables** : | | |
| – | Autoriser les tableaux dynamiques | Les paramètres sont :<br>• Activés pour la portée processus.<br>• Désactivés et désélectionnés pour la portée sécurité.<br>**NOTE:** Les tableaux dynamiques ne sont pas pris en charge pour les variables de programme de sécurité. |
| | Inhiber contrôle compatibilité taille tableau | |
| Paramètres du **Programme** : | | |

| Groupe | Paramètre | Description |
|---|---|---|
| Langages | Langage à blocs fonction (FBD) | Activé pour les portées processus et sécurité. |
| | Schéma à contacts (LD) | |
| | Diagramme fonctionnel en séquence (SFC). | • Activé pour la portée processus.<br>• Désactivé et désélectionné pour la portée sécurité. |
| | Liste d'instructions (IL) | |
| | Littéral structuré (ST) | |
| | Schéma à contacts 984 (LL984) | |
| Langages<br>• Commun | Autoriser les sous-programmes | • Activé pour la portée processus.<br>• Désactivé et désélectionné pour la portée sécurité.<br>**NOTE:** Les sous-programmes ne sont pas autorisés dans le programme de sécurité. |
| | Utilisation d'expressions ST (LD/FBD) | • Activé pour la portée processus.<br>• Désactivé et désélectionné pour la portée sécurité.<br>**NOTE:** Les expressions ST ne sont pas prises en charge dans le programme de sécurité. |
| | Permettre la conversion de type implicite | • Activé pour la portée processus.<br>• Désactivé et désélectionné pour la portée sécurité.<br>**NOTE:** Les conversions de type implicite ne sont pas prises en charge dans le programme de sécurité. |

# Annexes

## Contenu de cette partie



# 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



# 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 :

- règlementations 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.

# Modèle 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 4 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 section Niveaux SIL en faible demande, page 219.

## Description des exigences SIL

Pour atteindre la sécurité fonctionnelle, 2 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
- Proportion de défaillances en sécurité
- 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 norme IEC 61508, la valeur SIL est limitée par la proportion de défaillances en sécurité (SFF) et la tolérance aux anomalies matérielles (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 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 | HFT = 0 | HFT = 1 | HFT = 2 |
|---|---|---|---|
| SFF ≤ 60 % | - | SIL1 | SIL2 |
| 60 % < SFF ≤ 90 % | SIL1 | SIL2 | SIL3 |
| 90 % < SFF ≤ 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 en fournissant des procédures d'arrêt indépendantes supplémentaires
- Augmentation de la valeur SFF au moyen de diagnostics supplémentaires

# Description de la relation entre niveaux SIL et demande

La norme IEC 61508 fait la distinction entre le fonctionnement en mode faible demande et en mode 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 1 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 sur demande (PFD) |
|---|---|
| 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

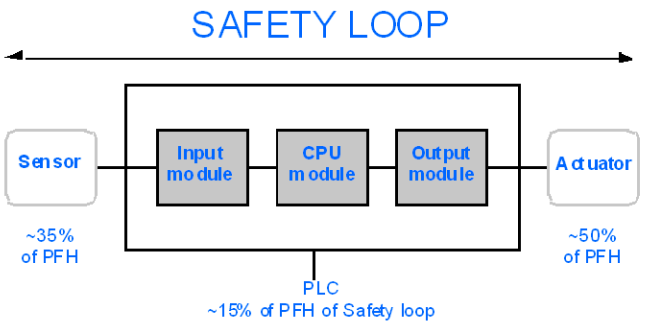
# Description de la boucle de sécurité

La boucle de sécurité de l'automate de sécurité M580 comporte 3 parties :

- Capteurs
- Automate de sécurité M580 avec alimentation, CPU de sécurité, coprocesseur 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 PAC 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 PAC 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 PAC de sécurité à la probabilité totale laisse davantage de marge à l'utilisateur et aboutit aux probabilités requises ci-dessous pour le PAC de sécurité :

- PFD ≥ $10^{-5}$ à < $10^{-4}$ pour une faible demande
- PFH ≥ $10^{-9}$ à < $10^{-8}$ pour une forte demande

# Description de l'équation PFD

La norme IEC 61508 suppose que la moitié des défaillances aboutissent à l'état sécurisé. Par conséquent, le taux de défaillance λ est composé de :

- $\lambda_S$ : défaillance en sécurité

- $\lambda_D$ : défaillance dangereuse, elle même composée de
  - $\lambda_{DD}$ : défaillance dangereuse détectée par le diagnostic interne
  - $\lambda_{DU}$ : 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 :

$\lambda = 1/MTBF$

L'équation de calcul de la probabilité de défaillance sur demande (PFD) est la suivante :

$PFD(t) = \lambda_{DU} \times t$

t représente le temps entre deux tests réguliers.

La probabilité de défaillance par heure implique un intervalle de temps de 1 heure. Par conséquent, l'équation PFD est réduite à la suivante :

$PFH = \lambda_{DU}$

# Objets système

## Contenu de ce chapitre



# 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**<br><br>**Symbole** | **Fonction** | **Description** | **Etat initial** | **Type** |
|---|---|---|---|---|
| %S17<br><br>`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<br><br>`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 :<br>• Résultat supérieur à +32 767 ou inférieur à -32 768, en simple longueur<br>• Résultat supérieur à +65 535, en entier non signé<br>• Résultat supérieur à +2 147 483 647 ou inférieur à -2 147 483 648, en double longueur<br>• Résultat supérieur à +4 294 967 296, en double longueur ou en entier non signé.<br>• Division par 0.<br>• Racine d'un nombre négatif.<br>• Forçage à un pas inexistant sur un programmateur cyclique.<br>• Empilage d'un registre plein, dépilage d'un registre vide. | 0 | R/W |
| %S21<br><br>`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.<br>**NOTE:**<br>• Le premier cycle de l'état de la tâche peut être lu en utilisant la sortie `SCOLD` du bloc fonction système `S_SYST_STAT_MX`.<br>• 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 M580 de sécurité

## Mots système des automates de sécurité M580

Les mots système suivants s'appliquent à l'automate de sécurité M580. Vous trouverez la description des mots système qui s'appliquent au PAC de sécurité M580 et aux PAC M580 non liés à la sécurité dans la présentation des *Mots système* fournie par le document *Ecostruxure™ Control Expert - Bits 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 :<br>• 16#A501 = mode de maintenance<br>• 16#5AFE = mode de sécurité<br>Toute autre valeur est interprétée comme une erreur. | L |
| %SW13 | Indique le mode de fonctionnement de la CPU :<br>• 16#501A = mode de maintenance<br>• 16#5AFE = mode de sécurité<br>Toute autre valeur est interprétée comme une erreur. | L |
| %SW42 | Temps en cours de la tâche SAFE. Indique le temps d'exécution du dernier cycle de la tâche SAFE (en ms) | L |
| %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) | L |
| %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) | L |
| %SW110 | Pourcentage de la charge de l'UC utilisé par le système pour les services internes. | L |
| %SW111 | Pourcentage de la charge de l'UC utilisé par la tâche MAST. | L |
| %SW112 | Pourcentage de la charge de l'UC utilisé par la tâche FAST. | L |
| %SW113 | Pourcentage de la charge de l'UC utilisé par la tâche SAFE. | L |
| %SW114 | Pourcentage de la charge de l'UC utilisé par la tâche AUX0. | L |
| %SW115 | Pourcentage de la charge de l'UC utilisé par la tâche AUX1. | L |
| %SW116 | Charge totale de l'UC du système. | L |

| Mot | Fonction | Type |
|---|---|---|
| %SW124 | Contient la cause de l'erreur non récupérable détectée lorsque l'automate de sécurité M580 est à l'état HALT :<br>• 0x5AF2 : Erreur RAM détectée dans la vérification de mémoire.<br>• 0x5AFB : Erreur détectée dans le code du micrologiciel de sécurité<br>• 0x5AF6 : Erreur de débordement de chien de garde de sécurité détectée sur l'UC.<br>• 0x5AFF : Erreur de débordement de chien de garde de sécurité détectée sur le coprocesseur.<br>• 0x5B01 : Coprocesseur non détecté au démarrage.<br>• 0x5AC03 : Erreur non récupérable de sécurité CIP détectée par l'UC.<br>• 0x5AC04 : Erreur non récupérable de sécurité CIP détectée par le coprocesseur.<br>**NOTE:** La liste ci-dessus n'est pas exhaustive. Pour plus d'informations, consultez le document *EcoStruxure™ Control Expert - Bits et mots système - Manuel de référence*. | L |
| %SW125 | Contient la cause de l'erreur récupérable détectée dans l'automate de sécurité M580 :<br>• 0x5AC0 : La configuration de sécurité CIP n'est pas correcte (détectée par l'UC).<br>• 0x5AC1 : La configuration de sécurité CIP n'est pas correcte (détectée par le coprocesseur).<br>• 0x5AF3 : Erreur de comparaison détectée par l'UC principale.<br>• 0x5AFC : Erreur de comparaison détectée par le coprocesseur.<br>• 0x5AFD : Erreur interne détectée par le coprocesseur.<br>• 0x5AFE : Erreur de synchronisation détectée entre l'UC et le coprocesseur.<br>• 0x9690 : Erreur de somme de contrôle du programme d'application détectée.<br>**NOTE:** La liste ci-dessus n'est pas exhaustive. Pour plus d'informations, consultez le document *EcoStruxure™ Control Expert - Bits et mots système - Manuel de référence*. | L |
| %SW126<br>%SW127 | Ces deux mots système contiennent des informations destinées à un usage interne Schneider Electric pour faciliter l'analyse détaillée des erreurs détectées. | L |
| %SW128 | Avec les UC 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 d'UC SAFE :<br>• Le changement de valeur de 16#1AE5 à 16#E51A force la synchronisation. Consultez la rubrique *Procédure de synchronisation des paramètres d'heure NTP* (voir Modicon M580 - Manuel de sécurité).<br>• Les autres séquences et valeurs ne forcent pas la synchronisation. | L/E |
| %SW142 | Contient la version du micrologiciel COPRO dans le BCD à 4 chiffres : par exemple la version du micrologiciel 21.42 correspond à %SW142 = 16#2142. | L |
| %SW148 | Nombre d'erreurs du code correcteur ECC (Error Correcting Code) détectées par la CPU. | L |

| Mot | Fonction | Type |
|---|---|---|
| %SW152 | Avec le micrologiciel de CPU de version 3.10 ou antérieure : état de l'heure de l'UC NTP mise à jour par le module de communication Ethernet (par ex. BMENOC0301/11) sur l'embase XBus via la fonction de synchronisation forcée de l'heure (en option) :<br>• 0 : L'heure de l'UC n'est pas actualisée par le module de communication Ethernet.<br>• 1 : L'heure de l'UC est actualisée par le module de communication Ethernet. | L |
| %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.<br>**NOTE:**<br>• Si le code de sécurité a été modifié et qu'une commande **Générer le projet** a été exécutée depuis la dernière commande **Regénérer tout** (modifiant ainsi l'ID de l'application de sécurité), l'exécution d'une commande **Regénérer tout** peut de nouveau modifier l'ID de l'application de sécurité.<br>• L'identifiant unique du programme SAFE peut être lu à l'aide de la sortie `SAID` du bloc fonction système `S_SYST_STAT_MX`. | L |
| %SW171 | Etat des tâches FAST :<br>• 0 : Aucune tâche FAST n'existe<br>• 1 : Arrêt<br>• 2 : Exécution<br>• 3 : Point d'arrêt<br>• 4 : Pause | L |
| %SW172 | Etat de la tâche SAFE :<br>• 0 : Aucune tâche SAFE n'existe<br>• 1 : Arrêt<br>• 2 : Exécution<br>• 3 : Point d'arrêt<br>• 4 : Pause | L |
| %SW173 | Etat de la tâche MAST :<br>• 0 : Aucune tâche MAST n'existe<br>• 1 : Arrêt<br>• 2 : Exécution<br>• 3 : Point d'arrêt<br>• 4 : Pause | L |
| %SW174 | Etat de la tâche AUX0 :<br>• 0 : Aucune tâche AUX0 n'existe<br>• 1 : Arrêt<br>• 2 : Exécution<br>• 3 : Point d'arrêt<br>• 4 : Pause | L |

| Mot | Fonction | Type |
|---|---|---|
| %SW175 | Etat de la tâche AUX1 :<br>• 0 : Aucune tâche AUX1 n'existe<br>• 1 : Arrêt<br>• 2 : Exécution<br>• 3 : Point d'arrêt<br>• 4 : Pause | L |
| %SW176 | Etat de comptage des bits forcés pour les variables SAFE du programme :<br>• Incrémenté chaque fois qu'un bit TOR est forcé.<br>• Décrémenté chaque fois qu'un bit TOR est déforcé. | L |

# Références SRAC

Le plan de vérification des conditions d'application liées à la sécurité (SRAC) fournit une trame générique pour justifier que les instructions du manuel d'installation et de sécurité associé sont respectées. Les instructions contenues dans le document *Modicon M580 - Guide de planification du système de sécurité* sont répertoriées comme des exigences.

Le tableau suivant indique le titre du paragraphe où trouver les exigences :

| **Exigences relatives aux messages d'informations sur la sécurité** | |
|---|---|
| **Id** | **Paragraphe** |
| PG 1 | Avant de commencer, page 8 |
| PG 2 | Démarrage et test, page 9 |
| PG 3 | Qu'est-ce qu'un module non perturbateur ?, page 21 |
| PG 4 | Consignes de mise à la terre, page 51 |
| PG 5 | Planification de l'installation du rack local, Introduction, page 90 |
| PG 6 | Espacement requis pour une CPU M580 dans un rack local principal, page 92 |
| PG 7 | Précautions d'installation, page 100 |
| PG 8 | Précautions d'installation, page 100 |
| PG 9 | Mise à la terre, page 103 |
| PG 10 | Installation d'un module d'alimentation, Introduction, page 103 |
| PG 11 | Précautions d'installation, page 104 |
| PG 12 | Précautions d'installation, page 104 |
| PG 13 | Précautions d'installation, page 104 |
| PG 14 | Mise à la terre du module d'alimentation, page 107 |
| PG 15 | Précautions relatives à la mise à la terre, page 108 |

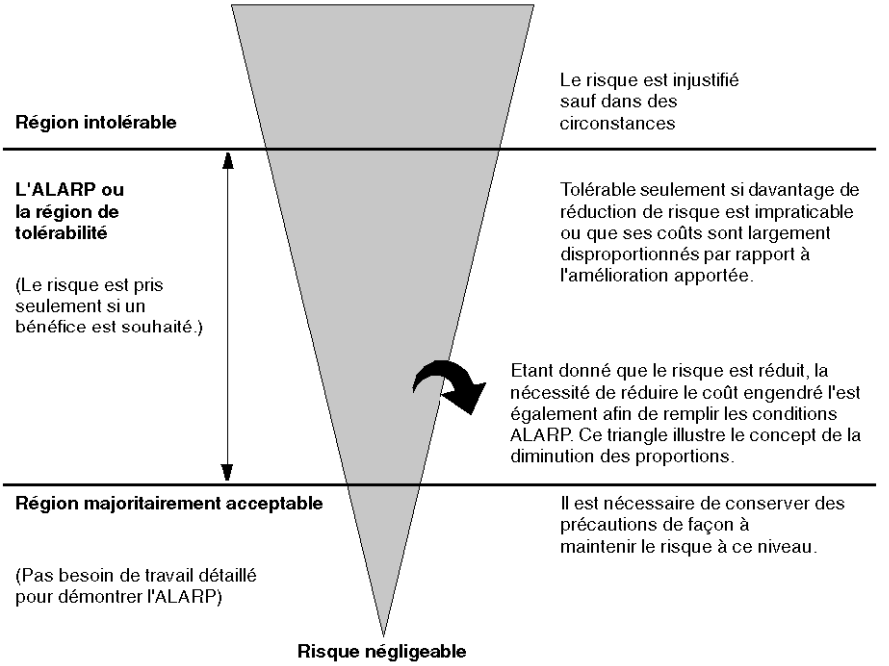
| Exigences relatives aux messages d'informations sur la sécurité | |
|---|---|
| **Id** | **Paragraphe** |
| PG 16 | Fonctionnement du mode de maintenance, page 122 |
| PG 17 | Démarrage à chaud, page 135 |
| PG 18 | Verrouillage de la configuration d'un module d'E/S de sécurité, page 148 |
| PG 19 | Affichage des données sur les écrans d'exploitation, page 155 |

# 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.

## D

**DIO:**

(*E/S distribuées*) Egalement appelé équipement distribué. Les DRSs utilisent des ports DIO pour connecter des équipements distribués.

## F

**FTP:**

Acronyme de *file transfer protocol* (protocole de transfert de fichiers). Protocole qui copie un fichier d'un hôte vers un autre sur un réseau TCP/IP, comme Internet. Le protocole FTP utilise une architecture client-serveur ainsi qu'une commande et des connexions de données distinctes entre le client et le serveur.

## 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.

## S

**SFF:**

Acronyme de *Safe Failure Fraction* (proportion de défaillances en sécurité).

**SRAC:**

(*Safety Related Application Condition*)

# Index



## A



## B



## C



## D

## E



## F



## G



## H



## I



## M



## N



## O

## P



## R



## S



## T



## U



## V

## Z

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.



QGH60284.08