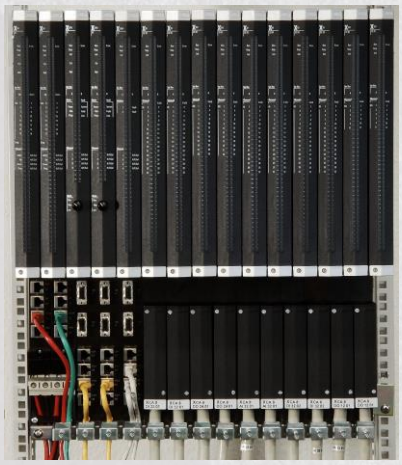


HIMax®

Manuel de sécurité

SAFETY NONSTOP

HIMA

APPLICATIONS FERROVIAIRES

8

Tous les produits et informations contenus dans ce manuel technique sont protégés par la marque HIMA. Sauf stipulation contraire, ceci s'applique également aux autres constructeurs ainsi qu'à leurs produits.

Toutes les indications et consignes figurant dans le présent manuel ont été mises au point avec le plus grand soin et établies à l'appui de mesures de contrôles efficaces. Pour toutes questions, contactez directement les services de HIMA. Toute suggestion relative à des informations qu'il serait bon d'inclure dans le manuel sera la bienvenue.

Sous réserve de modifications techniques. L'entreprise HIMA se réserve le droit de modifier les supports écrits à tout moment et sans préavis.

De plus amples informations sont disponibles sur le DVD documentation de HIMA et sur le site web http://www.hima.de et http://www.hima.com.

Contact

Adresse HIMA :

HIMA Paul Hildebrandt GmbH

Boite postale 1261

D-68777 Brühl

Tél.: +49 6202 709-0

Fax: +49 6202 709-107

E-mail: info@hima.com

Index des mises à jours	Modifications	Type de modification	
		technique	rédactionnelle
5.00	Première édition		

Sommaire

Annex 57

1 Manuel de sécurité

La connaissance des prescriptions et la parfaite mise en application technique des consignes de sécurité figurant dans le présent manuel par du personnel qualifié sont une condition indispensable à la planification, l'étude du projet, la programmation, l'installation, la mise en service, la sécurité de fonctionnement et la maintenance des automates HIMax.

En cas de manipulation non qualifiée des dispositifs, de déconnexion ou d'annulation (by-pass) des fonctions de sécurité et de non-observation des consignes du présent manuel entraînant des perturbations ou endommagements des fonctions de sécurité, HIMA décline toute responsabilité si ces faits sont à l'origine de dommages corporels, matériels ou environnementaux.

Les automates HIMax sont développés, fabriqués et testés en conformité avec les normes de sécurité en vigueur. Ils ne peuvent être utilisés que dans le cadre des applications prévues dans les descriptions et des conditions d'environnement spécifiées.

1.1 Validité et actualité

Version Rév. 5.00	Cette révision s'applique à partir de la version 5 du système HIMax et de SILworX.

Il convient d'utiliser la version la plus récente de ce manuel de sécurité, à savoir celle désignée par le numéro de révision le plus élevé. La dernière version est disponible sur le site *www.hima.com* ou sur le DVD HIMA actuel.

Pour l'application de versions plus anciennes de HIMax et SILworX, il convient d'observer les révisions antérieures de ce manuel.

1.2 Objectifs de ce manuel

Ce manuel contient des informations visant une utilisation conforme et sécurisée des automates HIMax. Il sert d'introduction au concept de sécurité du système HIMax et vise à accroître la prise de conscience du lecteur en matière de sécurité.

Le manuel de sécurité se fonde sur le contenu du certificat et du rapport d'essai attaché au certificat.

1.3 Groupe cible

Ce manuel est destiné aux concepteurs, bureaux d'études et programmeurs d'installations d'automates ainsi qu'aux personnes habilitées à intervenir pour la mise en service, l'exploitation et la maintenance des dispositifs et systèmes. Ces interventions requièrent des connaissances spéciales dans le domaine des systèmes d'automatisation relatifs à la sécurité.

1.4 Conventions typographiques

Afin d'assurer une meilleure lisibilité et compréhension de ce document, les polices suivantes sont utilisées :

Caractères gras	Souligner les passages importants. Noms des boutons, indexes du menu et registres pouvant êtres sélectionnés et utilisés dans SILworX
Italiques	Paramètres système et variables
`Courier`	Entrées textuelles de l'utilisateur
RUN	Les états de fonctionnement sont caractérisés pas des majuscules
Chapitres 1.2.3	Les références croisées sont des liens hypertextes, même s'ils ne sont pas explicitement caractérisés. Leurs formes changent lorsque le curseur est pointé dessus. En un clique le document passe à la destination souhaitée.

Les consignes de sécurité et modes d'emploi sont particulièrement caractérisés.

1.4.1 Consignes de sécurité

Les consignes de sécurité sont présentées comme suit :
Ces notices doivent être strictement respectées afin de réduire le risque au minimum. Le contenu est structuré comme suit :

- Signaux : Avertissement, Précaution, Notices explicatives
- Nature et source du risque
- Suites en cas de non-respect
- Prévention du risque

⚠ SIGNAUX

Nature et source du risque!

Conséquences en cas de non-respect

Prévention du risque

Les signaux ont le sens suivant :

- Avertissement : signifie que toute négligence peut entraîner des lésions corporelles et de mort.
- Précaution : signifie que toute négligence peut entraîner des lésions corporelles légères
- Notices explicatives : signifie que toute négligence peut entraîner des dégâts matériels.

REMARQUE

Nature et source du risque!

Prévention du risque

1.4.2 Mode d'emploi

Les informations complémentaires sont structurées comme suit :

i Le texte contenant les informations complémentaires ce trouve à cet endroit.

Les astuces utiles apparaissent sous cette forme :

ASTUCES Le texte contenant les astuces se trouve ici.

2 Consignes relatives à l'application de systèmes HIMax

Lire impérativement les informations de sécurité, consignes et instructions contenues dans le présent manuel. N'utiliser le produit que si les directives et normes de sécurité sont respectées.

2.1 Utilisation conforme à l'usage prévu

Ce chapitre décrit les conditions d'utilisation des systèmes HIMax.

2.1.1 Domaine d'application

Les automates relatives à la sécurité HIMax peuvent être utilisés jusqu'à un niveau d'intégrité de sécurité SIL 4 selon les normes EN 50128 et EN 50129.

Les automates relatifs à la sécurité HIMax sont certifiés pour des commandes de processus, de brûleur, de machines ainsi que des systèmes de protection.

Le fonctionnement redondant de modules HIMax n'exclut pas le fonctionnement non redondant simultané d'autres modules.

2.1.1.1 Application selon le principe du courant de repos

Les automates ont été conçus selon le principe du courant de repos.

En cas de défaillances, un système fonctionnant selon le principe du courant de repos passe à l'état sans courant ou sans tension (*de-energize-to-trip*) pour exécuter sa fonction de sécurité.

2.1.1.2 Application selon le principe du courant de travail

Les commandes HIMax peuvent être utilisées pour des applications fonctionnant selon le principe du courant de travail.

Un système, fonctionnant selon le principe du courant de travail, active par ex. un actionneur pour exécuter sa fonction de sécurité (*energize-to-trip*).

Lors de la conception de la commande, respecter les exigences des normes d'application, il se peut notamment qu'un diagnostic de ligne des entrées et sorties ou qu'un retour d'information de la fonction de sécurité déclenchée soit nécessaire.

2.1.2 Utilisation non conforme à l'usage prévu

Lors de la transmission de données (importantes pour la sécurité), des règles de sécurité informatiques sont à observer. En cas de transmission par le biais des réseaux publics (par ex. Internet), des mesures complémentaires visant à renforcer la sécurité (par ex. tunnel VPN, pare-feu, etc.) doivent être appliquées.

2.1.3 Conditions d'environnement

Nature de la condition	Domaine de valeurs
Classe de protection	Classe de protection III selon la norme IEC 61131-2
Température ambiante	0...+60 °C
Température de stockage	-40...+85 °C
Pollution	Degré de pollution II selon la norme IEC 61131-2
Altitude	< 2000 m
Boîtier	Par défaut : IP20
Tension d'alimentation	24 VDC

Tableau 1 : Conditions d'environnement

Les conditions d'environnement citées dans le présent manuel doivent être respectées lors de l'exploitation du système HIMax.

2.2 Obligations des fabricants de machines et installations ainsi que de l'exploitant

Les fabricants de machines et installations ainsi que les exploitants sont tenus de garantir l'utilisation sécurisée des systèmes HIMax dans les installations d'automatisation et dans les installations globales.

La programmation correcte des systèmes HIMax doit être amplement validée par les fabricants de machines et installations.

2.2.1 Raccordement de partenaires de communication

Seuls des dispositifs garantissant une isolation électrique sécurisée peuvent être raccordés aux interfaces de communication.

2.2.2 Utilisation de communication relative à la sécurité

Lors des communications relatives à la sécurité entre différents dispositifs, veiller à ce que le temps de réponse complet du système ne dépasse pas le temps de tolérance aux défauts. Les bases des calculs figurant au chapitre 11 doivent être utilisées.

2.3 Mesures de protection CEM

Seul le personnel connaissant les mesures de protection CEM, est autorisé à procéder à des modifications ou extensions du système ou à remplacer les modules.

REMARQUE

Des décharges électrostatiques peuvent endommager les composants électroniques intégrés dans les commandes !

- **Pour exécuter les travaux, utiliser un poste de travail à protection antistatique et porter un bracelet de mise à la terre.**
- **En cas de non-utilisation des modules, les conserver à l'abri de décharges antistatiques, par ex. dans leur emballage.**

Seul le personnel connaissant les mesures de protection CEM, est autorisé à procéder à des modifications ou extensions du système ou à remplacer les modules.

2.4 Autres documents relatifs au système

Pour l'étude et la conception des systèmes HIMax, les documents suivants sont également disponibles :

Nom	Sommaire	Document nº
HIMax Safety Manual	Manuel de sécurité : fonctions de sécurité du système HIMax	HI 801 003 E
HIMax System Manual	Manuel du système : Description du matériel du système modulaire	HI 801 001 E
Certificate Test Report [1)]	Rapport de test : bases de test, exigences en matière de sécurité, résultats	
Manuels des composants	Description de chaque composant	
Communication Manual	Manuel de communication : safe**ethernet** et protocoles standards	HI 801 001 E
SILworX First Step Manual	Manuel d'introduction à SILworX : utilisation de SILworX à des fins de planification, mise en service, test et exploitation	HI 801 103 E
[1)] Fourni uniquement avec un système HIMax		

Tableau 2 : Vue d'ensemble de la documentation du système

Les documents sont disponibles sous forme de fichiers PDF sur le site Internet `www.hima.com`.

3 Concept de sécurité pour l'utilisation de systèmes PE

Ce chapitre traite des questions générales et essentielles relatives à la sécurité de fonctionnement des systèmes HIMax :

- Sécurité et disponibilité
- Temps importants pour la sécurité
- Exigences de sécurité
- Certification

3.1 Sécurité et disponibilité

Les systèmes HIMax ne comportent pas de risques directs.

⚠ AVERTISSEMENT

Risque de dommages corporels liés à des systèmes d'automatisation relatifs à la sécurité, raccordés ou programmés de manière erronée !

Vérifier les raccordements avant la mise en service et tester l'ensemble de l'installation !

HIMA recommande de remplacer le plus rapidement possible les modules défaillants.

Un module de remplacement, utilisé à la place d'un module défaillant, fonctionne sans intervention de l'utilisateur. Il adopte les fonctions du module défaillant à condition qu'il soit du même type ou d'un modèle de remplacement homologué.

3.1.1 Calculs HR

Les calculs HR pour les systèmes HIMax ont été effectués selon IEC 61508.

Les valeurs HR seront communiquées par HIMA sur demande.

Les fonctions de sécurité, se composant d'une boucle relative à la sécurité (entrée, unité de traitement, sortie et communication sécurisée entre les systèmes HIMA), répondent dans toutes les combinaisons à l'ensemble des exigences décrites ci-dessus.

3.1.2 Test automatique et diagnostic de défauts

Le système d'exploitation des modules effectue au démarrage et en cours de fonctionnement de nombreux tests automatiques. Les tests vérifient principalement :

- Les processeurs
- Les zones de mémoire (RAM, random access memory)
- Le chien de garde
- Les connexions entre les modules
- Chaque canal des modules d'E/S

Si, au cours de ces tests, des défauts sont détectés, le module défaillant (ou le canal défaillant en cas de modules d'E/S) est mis hors circuit. Si les tests décèlent dès le démarrage un défaut de module, le module n'est pas mis en marche.

Sur un système sans redondance, cela signifie que les fonctions partielles ou l'ensemble du système PE peuvent être mises hors circuit. En cas de détection de défaut sur un système redondant, la fonction à exécuter est prise en charge par le module redondant ou le canal redondant.

Chaque module HIMax dispose de ses propres DEL qui indiquent les défauts détectés. Cela permet à l'utilisateur de diagnostiquer rapidement un défaut dans un module ou dans le circuit externe si un défaut est signalé.

En outre, le programme utilisateur peut évaluer différentes variables de système qui indiquent l'état des modules.

Un enregistrement de diagnostic complet relatif au comportement du système et des défauts détectés est stocké dans la mémoire de diagnostic du processeur et des autres modules. Après une perturbation du système, l'enregistrement peut être également lu par le biais du PADT.

Pour de plus amples détails sur l'évaluation des messages de diagnostic, se reporter également au manuel du système (HI 801 001 E), chapitre *Diagnosis (Diagnostic)*.

Pour une partie infime des défaillances de composants n'affectant pas la sécurité, le système HIMax ne fournit pas d'information de diagnostic.

3.1.3 PADT

L'utilisateur établit le programme et configure la commande au moyen du PADT. Le concept de sécurité du PADT aide l'utilisateur à appliquer correctement la fonction de commande. Les actions de PADT sont multiples pour vérifier les informations fournies.

3.1.4 Redondance

Pour augmenter la disponibilité, il est possible d'utiliser tous les composants contenant des éléments actifs en montage redondant et de les remplacer en cours d'exploitation.

La redondance ne nuit pas à la sécurité. Le SIL 4 est également garanti dans le cas de composants système redondants.

3.1.5 Montage de systèmes de sécurité selon le principe du courant de travail

Les systèmes de sécurité opérant selon le principe du courant de travail (*energize-to-trip*) ont la fonction suivante :

1. L'état le plus sécurisé d'un module est l'état hors tension. C'est notamment l'état résultant d'un défaut à l'intérieur d'un module.
2. A la demande, la commande peut déclencher la fonction de sécurité en activant un actionneur.

3.1.5.1 Détection de composants défaillants

Le système de sécurité détecte la défaillance de modules au moyen du diagnostic qui s'effectue automatiquement.

3.1.5.2 Fonction de sécurité pendant le fonctionnement selon le principe du courant de travail

L'exécution de la fonction de sécurité consiste à ce que le système de sécurité active (*energize*) un ou plusieurs actionneurs afin d'obtenir l'état de sécurité.

La planification suivante relève de l'utilisateur :

- Paramétrage des groupes de redondance des modules d'entrée et de sortie.
- Surveillance des ruptures de ligne et courts-circuits sur les modules d'entrée et de sortie. Un paramétrage doit être effectué.
- La fonction des actionneurs peut être contrôlée par la recopie de position.

3.1.5.3 Redondance des composants

Un montage redondant des composants peut être nécessaire, se reporter au manuel du système (HI 801 001 E) :

- Alimentation électrique de la commande
- Modules HIMax
- Capteurs et actionneurs

En cas de perte de redondance, la commande doit être réparée dans les plus brefs délais.

Une configuration redondante des modules du système de sécurité n'est pas nécessaire si, en cas de défaillance du système de sécurité, la sécurité requise peut être garantie par d'autres actions notamment sur le plan de l'organisation.

3.2 Temps importants pour la sécurité

Il s'agit de :

- Temps de tolérance aux défauts
- Temps du chien de garde
- Temps de sécurité
- Temps de réponse

3.2.1 Temps de tolérance aux défauts FTT

Le temps de tolérance aux défauts (temps de sécurité du processus) est une caractéristique du processus et décrit le laps de temps pendant lequel le processus peut recevoir des signaux de défaut sans qu'il s'agisse pour autant d'une situation critique pour la sécurité.

3.2.2 Temps du chien de garde de la ressource

Le temps de chien de garde est fixé dans SILworX, dans la boîte de dialogue de paramétrage des propriétés de la ressource. Il s'agit de la durée maximale autorisée d'un cycle de fonctionnement RUN (durée de cycle). Si la durée du cycle dépasse le temps de chien de garde défini, le processeur se met en arrêt pour cause de défaut.

Lors de la mesure du temps de chien de garde, tenir compte des circonstances suivantes :

- Besoin en temps de l'application, à savoir la durée d'un cycle du programme utilisateur.
- Besoin en temps pour la communication des données de processus.
- Besoin en temps pour la synchronisation des processeurs redondants.
- Besoin interne en temps pour l'exécution d'un rechargement.

La plage de réglage du temps de chien de garde de la ressource est de 6 ms à un maximum de 7 500 ms.

Le réglage par défaut est de 200 ms.

Pour le temps de chien de garde, appliquer : **temps de chien de garde ≤ ½ * temps de sécurité**

3.2.2.1 Evaluation du temps de chien de garde

HIMA recommande instamment le réglage suivant pour garantir une disponibilité suffisante :

2 * temps de chien de garde + max. durée de cycle de CPU + 2 * durée de cycle d'E/S ≤ temps de sécurité

La durée de cycle maximale doit être mesurée dans l'application réelle par l'échange d'un processeur redondant. La durée de cycle maximale calculée est à appliquer dans la formule ci-dessus.

Si une évaluation sûre de la durée maximale du cycle du CPU se révèle impossible, paramétrer un temps de sécurité comme suit :

3 * temps de chien de garde + 2 * durée de cycle d'E/S ≤ temps de sécurité

La durée de cycle d'E/S est de 2 ms.

3.2.2.2 Détermination exacte du temps de chien de garde

Elle peut se révéler importante dans le cas d'application à contrainte de temps ou de très grands systèmes.

Afin d'évaluer avec précision le temps de chien de garde pour un projet, celui-ci est à évaluer au moyen d'un test sur l'ensemble du système. Tous les modules du projet sont installés. Le système fonctionne à pleine charge.

Toutes les connexions de communication fonctionnent (safe**ethernet** et protocoles standards).

Détermination du temps de chien de garde

1. Paramétrer un temps de chien de garde élevé en vue du test.
2. Utiliser le système à pleine charge. Pour ce faire, toutes les connexions de communication doivent être opérationnelles, ainsi que celles par le biais de safe**ethernet** ou les protocoles par défaut. Lire à plusieurs reprises la durée de cycle dans le panneau de contrôle et prendre note des variations ou pointes de charge de celle-ci.
3. Retirer puis réinsérer l'un après l'autre les processeurs dans le support de base. Avant de retirer un processeur, attendre que celui qui vient d'être inséré soit synchronisé.

i Lorsqu'il est inséré, un processeur se synchronise automatiquement avec la configuration des processeurs existants. Le temps nécessaire à la synchronisation allonge le cycle de commande à la durée maximale de cycle.

Le temps nécessaire à la synchronisation croît en fonction du nombre de processeurs déjà synchronisés.

Pour la description du montage et démontage d'un processeur, se reporter au manuel X-CPU 01 (HI 801 009 E).

4. Dans l'historique de diagnostic du module non synchronisé, lire la durée de synchronisation des processeurs de n à n+1 à chaque processus de synchronisation. Le plus élevé des temps de synchronisation sera utilisé pour la détermination du temps de chien de garde.
5. Le temps de chien de garde T_{WD} se calcule comme suit :

   $T_{WD} = T_{Sync} + T_{Res} + T_{Com} + T_{Config} + T_{Latence} + T_{Pointe}$, donnent

   T_{Sync} Temps calculé pour la synchronisation d'un processeur

   T_{Res} Réserve de sécurité 12 ms

   T_{Com} Paramètre système configuré *Max.Com. Time Slice ASYNC [ms]*

   T_{Config} Paramètre système configuré *Max. Duration of Configuration Connections [ms]*

   $T_{Latence}$ Paramètre système fixé *Maximum System Bus Latency [µs]* * 4

   T_{Pointe} Pointes de charge observées des programmes utilisateurs

On obtient ainsi une consigne appropriée du temps de chien de garde.

i Le cas échéant, le temps de chien de garde ainsi calculé peut être insuffisant pour un rechargement.

ASTUCES Le temps de chien de garde établi peut être utilisé comme durée maximale de cycle de safe**ethernet**, se reporter au manuel de communication (HI 801 101 E).

3.2.3 Temps de chien de garde du programme utilisateur

Chaque programme utilisateur a un chien de garde et un temps de chien de garde propres.

Le temps de chien de garde du programme utilisateur ne s'ajuste pas immédiatement. HIMax calcule le temps de chien de garde d'un programme utilisateur à partir des paramètres *Watchdog Time [ms]* de la ressource et *Maximum Number of CPU Cycles.* Pour de plus amples détails, se reporter aux chapitres 10.2.3 et 10.2.11.

Veiller à ce que le temps de chien de garde calculé soit au moins aussi élevé que le temps de réponse exigé pour la partie du processus traitée par le programme utilisateur.

3.2.4 Temps de sécurité du système PE

Le temps de sécurité est la durée maximale autorisée, pendant laquelle le système PE doit réagir à une demande. Les demandes sont :

- Modifications des signaux d'entrée du processus.
- Présence d'un défaut dans la commande.

Le système HIMax réagit à un défaut susceptible de conduire la sûreté de fonctionnement en état critique pendant le temps de sécurité paramétré pour le système PE. Il déclenche des réactions aux défauts prédéfinies, mettant en état de sécurité les parties défaillantes. Les conditions requises pour cela sont :

- Aucune temporisation dans le programme utilisateur.
- La réaction se produit au cours d'un cycle du système PE. Le cycle du programme utilisateur est égal au cycle du système PE.
- Aucune tranche de temps de communication n'est paramétrée.

Pour les commandes HIMax, le temps de sécurité peut se paramétrer dans un domaine allant de 20 à 22 500 ms.

Lors de la mesure du temps de sécurité, l'utilisateur doit tenir compte des circonstances suivantes :

- Dans le cas des modules d'entrée et de sortie, prendre en compte le double de la durée de cycle du module d'E/S.

  La durée de cycle des modules d'E/S est de 2 ms.
- La suppression des défauts requiert également une réserve de temps.

Pour le temps de sécurité, choisir un paramètre suffisamment grand pour intégrer tous les effets cités, néanmoins inférieur au FTT du processus.

Le temps de sécurité pour la commande est de :

Temps de sécurité > 2 * temps de chien de garde + durée maximale de cycle + 2 * durée de cycle des modules d'E/S

La durée de cycle maximale doit être mesurée dans l'application réelle par l'échange d'un processeur redondant. La durée de cycle maximale calculée est à appliquer dans la formule ci-dessus.

Un niveau maximal de disponibilité est ainsi garanti.

3.2.5 Temps de sécurité du programme utilisateur

Le temps de sécurité du programme utilisateur ne peut être paramétré. HIMax le calcule à partir des paramètres *Safety Time* de la ressource et *Maximum Number of Cycles.* Pour de plus amples détails, se reporter aux chapitres 10.2.3 et 10.2.11.

3.2.6 Temps de réponse

Le temps de réponse des commandes HIMax à fonctionnement cyclique est le double de la durée de cycle de ces systèmes, s'il n’y a pas de temporisation liée au paramétrage ou à la logique du programme utilisateur.

Le temps de réaction ne doit pas dépasser le temps de tolérance aux défauts.

3.3 Exigences de sécurité

Pour l'utilisation des systèmes PE relatifs à la sécurité du système HIMax, les exigences de sécurité sont les suivantes :

3.3.1 Étude et conception du matériel

Les personnes en charge de l'étude et de la conception du matériel du système HIMax doivent tenir compte des exigences suivantes en matière de sécurité.

Exigences non liées au produit

- Pour des opérations relatives à la sécurité, seuls le matériel à sécurité intrinsèque ainsi que des composants du logiciel homologués doivent être utilisés. Le matériel et les logiciels homologués sont spécifiés dans le document *Version List of Devices and Firmware for HIMax Systems de HIMA Paul Hildebrandt GmbH.* Les révisions actuelles du matériel et logiciels sont disponibles dans l'actuelle liste des révisions détenue par l'organisme d'inspection.
- Les conditions d'application spécifiées relatives à la compatibilité électromagnétique (CEM), aux influences mécaniques, chimiques et climatiques doivent être strictement respectées (voir chapitre 3.4).
- Le matériel et les logiciels n'étant pas à sécurité intrinsèque, néanmoins sans effet rétroactif, doivent être utilisés pour le traitement de signaux n'affectant pas la sécurité et non pour le traitement d'opérations relatives à la sécurité.
- Pour tous les circuits raccordés au système par voie externe, observer le principe du courant de repos.

Exigences liées au produit

- Seuls des dispositifs présentant une isolation sûre à la tension d'alimentation, peuvent être connectés au système.
- Les conditions d'utilisation décrites dans le manuel du système doivent être respectées, notamment celles concernant la tension d'alimentation, la ventilation, etc.
- Seuls des modules relatifs à la sécurité peuvent être utilisés pour le traitement d'opérations relatives à la sécurité.
- Pour assurer le respect des normes de sécurité ayant rapport avec la sécurité électrique et la mise à la terre, le fabriquant des applications spécifiques doit prévoir des mesures de séparations appropriées entre les installations extérieures et intérieures selon la norme EN 50122. Cela permet de protéger les systèmes HIMax contre les influences des équipements extérieurs dans la zone de ligne aérienne de contact ou zone de pantographe et contre le courant de retour de traction. Seuls des équipements d'alimentation homologués pour une utilisation dans le domaine ferroviaire peuvent être employés.

3.3.2 Programmation

Les personnes en charge de la mise en œuvre des programmes utilisateurs doivent tenir compte des exigences suivantes en matière de sécurité.

Exigences non liées au produit

- Dans les applications relevant de la sécurité, assurer la définition exacte des paramètres relatifs à la sécurité du système. Le manuel de sécurité répertorie les paramétrages possibles, se reporter au chapitre 9.3.
- Cela concerne notamment la configuration du système, la durée de cycle maximale, ainsi que le temps de sécurité, voir chapitre 3.2.

3.3.3 Exigences relatives à l'utilisation de l'outil de programmation

- SILworX doit être utilisé pour la programmation.
- Une double compilation dans SILworX, avec comparaison des CRC des deux fichiers obtenus, garantit que la compilation a été correctement effectuée.
- La correcte réalisation des applications spécifiées doit être validée, vérifiée et documentée. Un test complet de la logique doit être effectué en procédant à des essais.

- La réponse du système aux défauts survenant dans les modules d'E/S de sécurité, doit être définie dans la configuration selon les données de sécurité spécifiques aux installations.
- Une fonction de l'outil de programmation SILworX permet de montrer quels changements ont été effectués sur le programme utilisateur ou sur le système de configuration. L'analyse des changements et de leurs effets doit déterminer l'étendue des tests. Cette analyse doit tenir compte des changements après modifications, des résultats obtenus par la fonction de comparaison de SILworX ainsi que des tests de régression.

3.3.4 Communication

- Lors des communications relatives à la sécurité entre différents dispositifs, veiller à ce que le temps de réponse complet du système ne dépasse pas le temps de tolérance aux défauts. Les calculs de base figurant au chapitre 11.2 doivent être utilisés.
- Le transfert des données doit s'effectuer par le biais de systèmes privés de transmission (catégorie 1) au sens de la norme EN 50159.
- L'utilisation de systèmes de transmission de transmission ouverts (catégorie 2 et catégorie 3) au sens de la norme EN 50159 est possible si des mesures supplémentaires sont prises pour garantir la sécurité du canal de transmission (par ex. pare-feu ou cryptage).
- Les protocoles par défaut ne doivent pas être utilisés pour la transmission de données importantes pour la sécurité.
- Seuls des dispositifs garantissant une isolation électrique sécurisée peuvent être raccordés à toutes les interfaces de communication.

3.3.5 Exigences relatives aux applications ferroviaires

- Respecter les normes essentielles concernant les applications ferroviaires.
- Les sorties numériques sont dotées d'une surveillance de court-circuit. Les réactions aux courts-circuits détectés doivent être programmées au sein du programme utilisateur.
- L'état de la température (température de service) des systèmes HIMax doit être évalué dans le programme utilisateur. Les mesures relatives à la sécurité doivent également être appliquées par le biais du programme utilisateur. Pour de plus amples informations, se reporter au manuel du système HIMax (HI 801 001 E), chapitre *Monitoring the Temperature (Surveillance de la température)*.
- Les messages de défaut doivent être évalués par le programme utilisateur. Les défauts sont signalés par les bits d'état et sont disponibles pour le programme utilisateur. En outre, les défauts sont saisis dans la mémoire de diagnostic de la commande et peuvent être lus avec l'outil de programmation. Pour de plus amples informations, se reporter au manuel du système HIMax (HI 801 001 E), chapitre *Diagnosis (Diagnostic)*.
- Une détection de la mise à la terre doit être configurée en externe.

3.4 Conditions d'essai

Les dispositifs ont été testés pour répondre aux exigences en matière de protection climatique et de l'environnement selon les normes CEM suivantes :

Norme	Sommaire
IEC 61131-2 : 2007	Automates programmables, partie 2 Spécifications et essais des équipements
IEC 61000-6-2 : 2005	CEM Norme générique, partie 6-2 Immunité pour les environnements industriels
IEC 61000-6-4 : 2006	Compatibilité électromagnétique (CEM) Norme générique sur l'émission pour les environnements industriels

Tableau 3 : Normes pour la CEM ainsi que la protection du climat et de l'environnement

Pour l'utilisation de systèmes de commande HIMax relatifs à la sécurité, les conditions générales suivantes doivent être observées :

Nature de la condition	Contenu de la condition
Classe de protection	Classe de protection III selon la norme IEC 61131-2
Pollution	Degré de pollution II selon la norme IEC 61131-2
Altitude	< 2000 m
Boîtier	Par défaut : IP20/IP00 S'il doit répondre aux normes applicables (par ex. EN 60204), le dispositif doit être installé dans un boîtier avec indice de protection correspondant (par ex. IP54).

Tableau 4 : Conditions générales

3.4.1 Conditions climatiques

Les essais et valeurs limites les plus importants, applicables aux conditions climatiques, sont répertoriés dans le tableau suivant :

IEC 61131-2	Essais climatiques
	Température de service : 0...+60 °C (Limites d'essai : -10...+70 °C)
	Température de stockage : -40...+85 °C
	Chaleur et froid secs ; essais de durabilité : +70 °C / -25 °C, 96 h, alimentation électrique non raccordée
	Changement de température ; essais de durabilité et de résistance : -25 °C / +70 °C et 0 °C / +55 °C, Alimentation électrique non raccordée
	Cycles avec chaleur humide ; essais de durabilité : +25 °C / +55 °C, 95 % d'humidité relative, Alimentation électrique non raccordée

Tableau 5 : Conditions climatiques

3.4.2 Conditions mécaniques

Les essais et valeurs limites les plus importants, applicables aux conditions mécaniques, sont répertoriés dans le tableau suivant :

IEC 61131-2	Essais mécaniques
	Essais de résistance aux vibrations : 5...9 Hz / 3,5 mm amplitude 9...150 Hz, 1 g, échantillon pendant fonctionnement, 10 cycles par axe
	Essais de résistance aux chocs : 15 g, 11 ms, échantillon pendant fonctionnement, 3 chocs par axe et direction (18 chocs)

Tableau 6 : Essais mécaniques

3.4.3 Conditions CEM

Pour des systèmes relatifs à la sécurité, un niveau plus élevé est exigé lors des interférences. Les systèmes HIMax répondent à ces exigences selon la norme IEC 62061 et IEC 61326-3-1. Voir la colonne *Critère SF* (sécurité fonctionnelle).

Normes d'essais	Essais d'immunité aux interférences	Critère SF
IEC 61000-4-2	Essai CEM : contact 6 kV, décharge dans l'air 8 kV	6 kV, 8 kV
IEC 61000-4-3	Essai RFI (10 V/m) : 80 MHz...2 GHz, 80 % AM Essai RFI (3 V/m) : 2 MHz...3 GHz, 80 % AM Essai RFI (20 V/m) : 80 MHz...1 GHz, 80 % AM	- - 20 V/m
IEC 61000-4-4	Essai par salve : Tension d'alimentation : 2 kV et 4 kV Lignes de signalisation : 2 kV	 4 kV 2 kV
IEC 61000-4-12	Essai avec vibrations amorties : 2,5 kV L-,L+ / PE 1 kV L+ / L -	 - -
IEC 61000-4-6	Haute fréquence, asymétrique : 10 V, 150 kHz...80 MHz, 80 % AM 20 V, fréquences ISM, 80 % AM	 10 V -
IEC 61000-4-3	Impulsion 900 MHz	-
IEC 61000-4-5	Onde de choc : Tension d'alimentation : 2 kV CM, 1 kV DM Lignes de signalisation : 2 kV CM, 1 kV DM avec AC E/S	 2 kV / 1 kV 2 kV

Tableau 7 : Essais d'immunité aux interférences

IEC 61000-6-4	Essais d'émission d'interférences
EN 55011 Classe A	Émission d'interférences : rayonnées, conduites

Tableau 8 : Essais d'émission d'interférences

3.4.4 Tension d'alimentation

Les essais et valeurs limites les plus importants, applicables à la tension d'alimentation des dispositifs, sont répertoriés dans le tableau suivant :

IEC 61131-2	Vérification des propriétés de l'alimentation en courant continu
	Comme solution alternative, l'alimentation électrique doit répondre aux normes suivantes : IEC 61131-2 ou TBTS (très basse tension de sécurité) ou TBTP (très basse tension de protection)
	La protection des dispositifs HIMax doit s'effectuer conformément aux indications du manuel X-BASE PLATE (HI 801 025 E).
	Essai sur la plage de tension 24 VDC, -20...+25 % (19,2...30,0 V)
	Essai relatif à l'immunité contre une brève interruption de l'alimentation électrique externe : DC, PS 2 : 10 ms
	Inversion de polarité de la tension d'alimentation : Note dans le chapitre correspondant du manuel de système ou dans la fiche technique de l'alimentation électrique.
	Durée tampon, essai de résistance : Essai B, 1000 h

Tableau 9 : Vérification des propriétés de l'alimentation en courant continu

3.5 Conditions d'essais supplémentaires pour applications ferroviaires

Le tableau suivant affiche les composants HIMax homologués pour une utilisation dans des applications ferroviaires :

Désignation	Description
X-CPU 01	Processeur
X-SB 01	Module bus système
X-COM 01	Module de communication
X-DI 32 01	Module d'entrées numériques (32 canaux)
X-DI 32 02	Module d'entrées numériques (32 canaux), pour interrupteurs de proximité
X-DI 64 01	Module d'entrées numériques (64 canaux)
X-DO 12 01	Module relais (12 canaux)
X-DO 32 01	Module de sorties numériques (32 canaux)
X-BASE PLATE	Supports de base HIMax

Tableau 10 : Composants HIMax homologués

3.5.1 Conditions climatiques

Les classes climatiques suivantes peuvent être déduites pour le domaine de température de 0...+60 °C du système HIMax conformément à la norme EN 50125-3 :

- Dans un container avec surveillance de la température : T1, T2 et TX
- Dans un bâtiment non climatisé : T1
- Dans un bâtiment climatisé : T1, T2 et TX

3.5.2 Conditions mécaniques

Les essais et valeurs limites les plus importants, applicables aux conditions mécaniques, sont répertoriés dans le tableau suivant :

Normes d'essais	Essais mécaniques
EN 50125-3	Essais de résistance aux vibrations : 2,3 m/s^2 entre 5...2000 Hz, pendant l'exploitation de l'objet testé
	Essais de résistance aux chocs : 20 m/s^2, 11 ms, pendant l'exploitation de l'object testé

Tableau 11 : Essais mécaniques supplémentaires

3.5.3 Conditions CEM

Les essais et valeurs limites les plus importants, applicables aux conditions CEM, sont répertoriés dans le tableau suivant :

EN 50121-4	Essais d'immunité aux interférences
Essai CEM	Contact 6 kV, décharge dans l'air 8 kV
Champ EM	80 MHz…1 GHz : 10 V/m 80 MHz…3 GHz : 10 V/m 800 MHz…1 GHz : 20 V/m
Essai par salve	Tension d'alimentation : 2 kV Lignes d'E/S : 2 kV
Surtension	Tension d'alimentation : 2 kV CM 1 kV DM Lignes d'E/S : 2 kV CM 1 kV DM
Afflux	Tension d'alimentation : 10 V Lignes d'E/S : 10 V
Champ magnétique à la fréquence du réseau	16 2/3 Hz, 50 Hz, 60 Hz : 100 A/m DC : 300 A/m
Champ magnétique, par impulsions	300 A/m

Tableau 12 : Essais CEM supplémentaires

3.5.4 Conditions plus sévères

Pour assurer la protection du système HIMax contre les intempéries de classe 4C3, 4B1 et 4S2, il doit être installé dans une armoire fermée avec indice de protection approprié, par ex. IP54.

4 Processeur

La fonction de sécurité du processeur consiste à exécuter le programme utilisateur au moyen de deux processeurs qui comparent continuellement leurs données. En cas de défaillance, le chien de garde met le module en état de sécurité et rapporte l'état du CPU.

Pour de plus amples détails sur les processeurs, se reporter aux manuels.

4.1 Tests automatiques

Les principales routines de test automatique des processeurs relatifs à la sécurité sont désignées ci-après :

- Test de processeur
- Test de mémoire
- Test de comparateur
- Test CRC dans les mémoires non volatiles
- Test du chien de garde

4.2 Réactions aux défauts dans le processeur

Un mécanisme de comparaison à l'intérieur du processeur vérifie en permanence que les données du système du microprocesseur 1 sont identiques aux données du système microprocesseur 2. Si ce n'est pas le cas ou si les routines de test trouvent des défauts dans le processeur, celui-ci se met automatiquement en ARRÊT.

4.3 Remplacement de processeurs

Avant le remplacement de processeurs, assurez-vous que cela ne provoque pas l'arrêt d'un système HIMax en cours de fonctionnement.

Cela concerne notamment les systèmes opérant selon le principe du courant de travail. Dans de tels cas, une défaillance du système entraîne la perte de la fonction de sécurité.

Des processeurs redondants peuvent être remplacés en cours d'exploitation à condition qu'au moins un processeur soit disponible pour maintenir une exploitation relative à la sécurité pendant le remplacement de l'autre.

REMARQUE

Risque d'interruption des opérations relatives à la sécurité !

L'exploitation de la commande peut être interrompue lors du remplacement d'un processeur sur lequel la DEL Ess **est allumée ou clignote.**

Ne pas retirer les processeurs dont la DEL Ess **est allumée ou clignote !**

La DEL **Ess** allumée ou clignotante indique que le processeur est absolument indispensable au fonctionnement du système.

Même si la DEL n'est pas allumée ou ne clignote pas, les redondances du système auxquelles ce processeur est associé doivent être vérifiées à l'aide de SILworX. Prendre également en compte les connexions de communication gérées par le processeur.

Pour de plus amples détails sur le remplacement de processeurs, se reporter au manuel du processeur (HI 801 009 E) et au manuel du système (HI 801 001 E).

5 Bus système

Un bus système gère un des deux bus systèmes relatifs à la sécurité. Les deux bus systèmes fonctionnent de manière redondante. Chaque bus système relie tous les modules et supports de base entre eux. Les données sécurisées sont transmises par le biais des bus systèmes au moyen d'un protocole relatif à la sécurité.

Un système HIMax ne contenant qu'un seul processeur peut être opérer sous disponibilité réduite avec un seul bus système.

5.1 Rack ID

Le rack ID identifie un support de base au sein d'une ressource et doit être unique pour chacun d'entre eux.

Le rack ID est le **paramètre de sécurité** pour l'adressage de chaque support de base et des modules qui y sont installés !

Le rack ID est enregistré dans le panneau de raccordement du module bus système. Si le rack ID doit être modifié, par ex. en cas de montage d'un nouveau système HIMax, suivre la procédure indiquée dans le manuel du système.

La procédure de réglage du rack ID est décrite dans le manuel du système (HI 801 001 E) et dans le manuel d'introduction à SILworX (HI 801 103 E).

5.2 Responsibility

Seul un des modules bus système par bus système peut avoir l'attribut *Responsible* et, par conséquent, être paramétré en tant que responsable de l'exploitation du bus système.

- Pour le bus système A, l'attribut *Responsible* est alloué au module bus système dans le rack 0, douille 1.
- Pour le bus système B, l'attribut est paramétrable avec SILworX.

Le module bus système responsable doit se trouver soit dans le support de base 0 soit dans le support de base 1, douille 2.

Assurer-vous que les exigences relatives à la sécurité sont remplies avant de démarrer l'exploitation.

La procédure de réglage de l'attribut *Responsible* est décrite dans le manuel d'introduction à SILworX (HI 801 103 E).

⚠ AVERTISSEMENT

Risque de dommages corporels !

Le paramétrage doit être vérifié au moyen de SILworX.

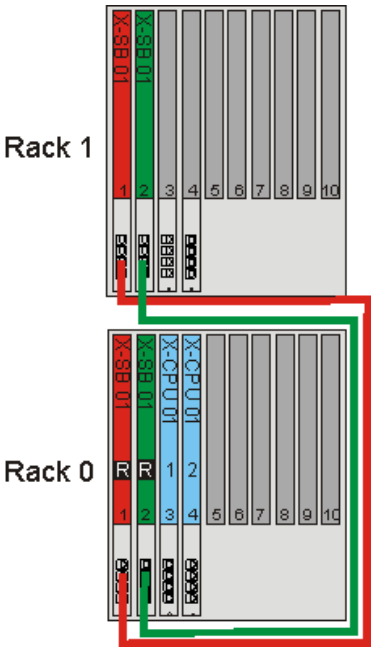
Pour ce faire, observer impérativement la procédure suivante :

- **Dans SILworX, accéder au module bus système au moyen de l'identifiant du module dans rack 0, douille 2**
- **Dans SILworX, accéder au module bus système au moyen de l'identifiant du module dans rack 1, douille 2**
- **Dans les panneaux de commande des deux modules bus système, s'assurer que l'attribut *Responsible* n'est alloué qu'au module bus système approprié (voir Figure 1 et Figure 2) !**

Configurations recommandées :

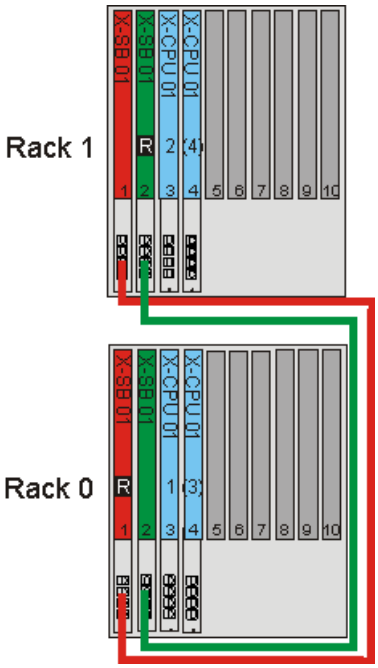
- Si seul le rack 0 contient des processeurs, les deux modules bus système du rack 0 doivent être paramétrés comme *Responsible* (Figure 1).
- Si le rack 1 contient également des processeurs (Figure 2), paramétrer les modules bus système suivants comme *Responsible* :

- dans le rack 0, le module bus système de la douille 1 (automatiquement).
- dans le rack 1, le module bus système de la douille 2.



R Le module bus système est responsable

Figure 1 : Configuration recommandée de tous les processeurs sur rack 0



R Le module bus système est responsable

Figure 2 : Configuration recommandée : processeurs sur rack 0 et rack 1

6 Module de communication

Les modules de communication gèrent tant la transmission de données relative à la sécurité avec d'autres commandes HIMA que celle non relative à la sécurité par le biais des bus de terrain et d'Ethernet

- Le processeur contrôle la transmission des données relative à la sécurité par le biais du protocole relatif à la sécurité safe**ethernet**. Le module de communication transmet les paquets de données aux autres systèmes. Le protocole relatif à la sécurité permet d'assurer la détection de messages corrompus (principe du canal noir).

  Cela permet d'établir une communication relative à la sécurité par des voies de transmission non relative à la sécurité, à savoir des composants de réseau standards.
- Les protocoles standards sont par ex. :
  - Modbus
  - PROFIBUS maître/esclave

Un système HIMax peut être équipé au maximum de 20 modules de communication.

Pour de plus amples détails, se reporter au chapitre 11.1, au manuel du module de communication (HI 801 011 E) et au manuel de communication (HI 801 101 E).

7 Modules d'entrée

Module	Nombre de canaux	Relatif à la sécurité	Canaux sans effet rétroactif	Remarque
X-DI 32 01	32	SIL 4	•	
X-DI 32 02	32	SIL 4	•	Interrupteur de proximité (NAMUR)
X-DI 64 01	64	SIL 4	•	

Tableau 13 : Aperçu des modules d'entrée

7.1 Généralités

Les entrées relatives à la sécurité peuvent être utilisées pour des signaux tant relatifs à la sécurité que non relatifs à la sécurité. Néanmoins, les signaux non relatifs à la sécurité ne peuvent être utilisés pour des fonctions de sécurité !

En ce qui concerne les DEL de diagnostic des modules, les commandes génèrent des messages de défaut et d'état qui sont enregistrés. Le PADT peut lire ces messages enregistrés dans la mémoire de diagnostic.

En cours de fonctionnement, des modules d'entrée relatifs à la sécurité exécutent un test automatique cyclique de haut niveau.

En cas de défaut, la valeur initiale est mise à disposition du programme utilisateur par le biais d'une variable globale et si possible un message détaillé sur le défaut est généré. Ce message peut être lu et évalué par le programme utilisateur.

Pour de plus amples détails sur les modules d'entrée, se reporter aux manuels des modules.

7.2 Sécurité des capteurs, encodeurs et transmetteurs

Dans une application relative à la sécurité, le système PE ainsi que les capteurs, encodeurs et transmetteurs qui y sont raccordés doivent répondre aux exigences en matière de sécurité et atteindre le niveau SIL spécifié.

7.3 Entrées numériques relatives à la sécurité

Le module d'entrées numériques lit ses entrées numériques et fournit des valeurs sécurisées à chaque cycle du processeur. Le module teste la sécurité du fonctionnement des entrées de manière cyclique.

7.3.1 Tests fonctionnels des signaux d'entrée

Les tests fonctionnels vérifient que les canaux d'entrée sont capables de relier les deux niveaux de signaux (signaux 0 et 1) indépendamment des signaux d'entrée émis. Ils sont réalisés chaque fois que des signaux d'entrée sont lus.

7.3.2 Réaction en cas de défaillances

Lorsque les tests fonctionnels détectent un défaut sur une entrée numérique, le module définit la valeur de canal de sorte que la variable globale allouée par l'utilisateur au canal prenne les valeurs suivantes :

- Dans le cas de défauts diagnosticables, la variable globale prend sa valeur initiale configurée. Le module passe de l'état *Channel OK* à FALSE.
- En cas de défauts sécurisés et non diagnosticables, le module ne peut générer aucune entrée de diagnostic.
  Pour ces défauts, la variable globale prend la valeur de sécurité 0.

Si les tests fonctionnels détectent un défaut du sous-module ou du module, le module passe de l'état *Submodule OK* ou *Module OK* à FALSE. En outre, le sous-module ou module passe tous ses canaux de *Channel OK* à FALSE.

Dans tous les cas, le module active la DEL *Error* sur le panneau avant.

7.3.3 Redondance

Il est autorisé de connecter les entrées numériques de manière redondante. La connexion redondante est utilisée afin d'accroître la disponibilité.

D'autres connexions - destinées à augmenter la valeur SIL - requièrent le traitement des états de défaut dans la logique du programme utilisateur.

7.3.4 Surtension au niveau de sorties numériques

En raison de la courte durée de cycle des systèmes HIMax, une impulsion de surtension au sens de la norme EN 61000-4-5 peut être lue comme un bref signal 1 au niveau des entrées numériques.

En cas d'utilisation de câble blindé pour les entrées numériques, aucune autre mesure de prévention n'est nécessaire pour la surtension.

Si le câble utilisé n'est pas blindé, appliquer une temporisation de mise en marche/arrêt du canal, afin d'éviter de telles défaillances. Un signal doit être en suspens pendant un certain temps avant d'être évalué. La temporisation paramétrée + 2 * durée de cycle des E/S doit être ajoutée au temps de réponse et au temps de sécurité paramétré du système PE.

7.4 Entrées analogiques relatives à la sécurité et entrées de l'interrupteur de proximité

Des canaux d'entrée analogiques transforment les courants d'entrée mesurés en une valeur de type DINT (double integer) ; c.-à-d. le paramètre *raw value*, et en un paramètre *process value* de type REAL. Le paramètre *raw value* contient le signal d'entrée mesuré tandis que le paramètre *process value* est une valeur mise à l'échelle.

Les entrées de l'interrupteur de proximité génèrent une valeur numérique en comparant le paramètre *raw value* avec les valeurs seuils paramétrables.

7.4.1 Tests fonctionnels des voies d'entrées

Le module saisit les valeurs analogiques en parallèle et compare leurs résultats. Il teste ensuite de manière cyclique le fonctionnement des voies d'entrées.

7.4.2 Réaction en cas de défaillances

Lorsque les tests fonctionnels détectent un défaut sur une entrée analogique, le module définit la valeur de canal de sorte que la variable globale allouée à le paramètre *process value* du canal prenne sa valeur initiale configurée.

Le module passe de l'état *Channel OK* à FALSE.

Le paramètre *raw value* du canal ne répond pas aux défauts. Si une valeur brute est utilisée, le programme utilisateur doit traiter le défaut.

Si les tests fonctionnels détectent un défaut du sous-module ou du module, le module passe de l'état *Submodule OK* ou *Module OK* à FALSE. En outre, le sous-module ou module passe tous ses canaux de *Channel OK* à FALSE.

Dans tous les cas, la DEL *Error* est activée sur le panneau avant.

7.4.3 Redondance

Il est autorisé de connecter les entrées numériques de manière redondante. La connexion redondante est utilisée afin d'accroître la disponibilité.

D'autres connexions - destinée à augmenter la valeur SIL - requièrent le traitement des états de défaut dans la logique du programme utilisateur.

7.5 Listes de vérification des entrées

HIMA recommande d'utiliser les listes de vérification disponibles pour l'étude, la programmation et la mise en service d'entrées relatives à la sécurité. Les listes de vérification peuvent être utilisées comme documents techniques de conception et font la preuve que la planification a été exécutée avec soin.

Pour les canaux d'entrée relatifs à la sécurité utilisés dans un système ou la mise en service, il convient de remplir la liste de vérification afin de contrôler quelles exigences sont à remplir. Ceci est le seul moyen de s'assurer que les exigences ont été comprises dans leur intégralité. La liste de vérification documente également la cohérence des liens entre le câblage externe et le programme utilisateur.

Les listes de vérification sont disponibles sur le site Internet HIMA en format Microsoft® Word®.

8 Modules de sortie

Module	Nombre de canaux	Relatif à la sécurité	Isolation électrique sécurisée	Remarque
Sorties numériques X-DO 32 01	32	SIL 4	-	
Sorties relais numériques X-DO 12 01	12	SIL 4	•	230 VAC

Tableau 14 : Vue d'ensemble des modules de sortie

8.1 Généralités

Les modules de sorties relatives à la sécurité sont définis une fois dans chaque cycle, les signaux de sortie sont lus et comparés avec les données de sortie fixées.

Dans le cas des sorties, la valeur *0* ou le contact de relais ouvert correspond à l'état de sécurité.

L'utilisation du code défaut correspondant permet en outre de configurer les réactions aux défauts dans le programme utilisateur.

Pour de plus amples détails sur les modules de sorties, se reporter aux manuels de module.

8.2 Sécurité des actionneurs

Dans une application relative à la sécurité, le système PE ainsi que les actionneurs qui y sont raccordés répondent aux exigences en matière de sécurité et au SIL spécifique.

8.3 Sorties numériques relatives à la sécurité

Les canaux de sortie relatifs à la sécurité sont équipés de trois interrupteurs testables connectés série pouvant désactiver chaque canal individuellement. Cela permet la mise en arrêt sécurisée par une deuxième voie indépendante et de répondre à l'exigence de niveau SIL 4. En cas de défaillance, cette mise en arrêt sécurisée met les différents canaux du module de sortie défectueux hors tension (état hors tension).

En outre, le signal de chien de garde du module est la deuxième possibilité de mise à l'arrêt : une panne du signal de chien de garde entraîne le passage immédiat à l'état de sécurité.

8.3.1 Test fonctionnels pour sorties numériques

Les modules sont testés automatiquement pendant l'exploitation. Les principaux tests fonctionnels de test sont :

- Relecture du signal de sortie de l'amplificateur de commutation. Le seuil de commutation d'un signal de niveau bas ayant été relu est en dessous de la valeur de tension valide pour ce type de sortie. Les diodes utilisées empêchent le renvoi des signaux.
- Contrôle de la mise à l'arrêt sécurisée redondante.
- Un test de mise à l'arrêt des sorties est réalisé de manière cyclique tous les 200 µs max.

Si des défauts surviennent, les sorties passent en valeur de sécurité.

8.3.2 Réaction en cas de défauts

Si les tests de fonctionnement détectent un défaut sur un ou plusieurs canaux, le module désactive ces canaux qui passent à l'état de sécurité. Pour ces canaux, le paramètre passe de *Channel OK* à FALSE.

Si les tests fonctionnels détectent un défaut du sous-module ou du module, le module passe de l'état *Submodule OK* ou *Module OK* à FALSE. En outre, le module ou sous-module passe tous ses canaux de *Channel OK* à FALSE.

Si la sortie signalant une interférence est activée, le module de sortie retarde la réaction de mise à l'arrête d'un canal.

⚠ AVERTISSEMENT

Si la sortie signal interférence est activée, les valeurs temporelles paramétrées dans le système HIMax doivent être recalculées.

Observer que la réaction sécurisée à une interférence existante peut être retardée jusqu'à
2 fois le temps de sécurité s'il s'agit de la suppression d'une interférence transitoire par le processeur (X-CPU) et de la suppression complémentaire par la sortie signalant l'interférence.

L'application de sortie interférence est critique et est seulement recommandée que pour des utilisateurs expérimentés.

Dans tous les cas, le défaut est signalé par la DEL *Error* sur le panneau avant.

8.3.3 Comportement en cas de court-circuit externe ou surcharge

En cas de court-circuit de la sortie vers L- ou de surcharge, la testabilité du module est maintenue. Un passage à l'état de sécurité n'est pas nécessaire.

Les sorties sont contrôlées dans cet état de manière cyclique à des intervalles de quelques secondes pour vérifier si la surcharge est encore présente. Si l'état est normal, les sorties sont à nouveau connectées.

8.3.4 Redondance

Il est autorisé de connecter les entrées numériques de manière redondante. La connexion redondante est utilisée afin d'accroître la disponibilité.

D'autres connexions - destinée à augmenter la valeur SIL - requièrent le traitement des états de défaut dans la logique du programme utilisateur.

8.4 Sorties relais relatives à la sécurité

Les modules de sortie relais sont connectés à l'actionneur lorsqu'une ou plusieurs des conditions suivantes sont réunies :

- Isolation électrique est nécessaire.
- Intensités de courant sont plus élevées.
- Des courants alternatifs doivent être connectés.

Sur le module, les sorties sont équipées de deux relais de sécurité avec contacts à guidage forcé. Cela permet d'utiliser les sorties pour des mises à l'arrêt sécurisées conformément à SIL 4.

En outre, le signal du chien de garde du CPU offre une deuxième possibilité de réaliser une mise à l'arrêt de sécurisée : si le signal du chien de garde disparait, le module adopte immédiatement l'état de sécurité.

8.4.1 Tests de fonctionnement pour sorties relais

Le module est testé automatiquement pendant l'exploitation. Les principaux tests fonctionnels sont :

- Relecture des signaux de sortie de l'amplificateur de commutation situé avant le relais.
- Vérification de la connexion du relais avec des contacts à guidage forcé.
- Contrôle de la mise à l'arrêt sécurisée redondante.

8.4.2 Réaction en cas de défaillances

Si un signal erroné est détecté, la sortie concernée du module est mise en état de sécurité par les interrupteurs de sécurité. En cas de défaut du module, toutes les sorties du module sont mises hors tension. Les deux défauts sont en outre signalés par la DEL *FAULT*.

Le nombre des cycles de commutation est limité conformément aux "normes importantes en la matière, par ex. norme EN 50156-1 sur la gestion des brûleurs. Pour de plus amples détails, se reporter au manuel du module (HI 801 023 E).

Lorsque le compteur atteint le nombre de cycles spécifié, remplacer le module !

8.4.3 Redondance

Il est autorisé de connecter les entrées numériques de manière redondante. La connexion redondante est utilisée afin d'accroître la disponibilité.

D'autres connexions - destinée à augmenter la valeur SIL - requièrent le traitement des états de défaut dans la logique du programme utilisateur.

8.5 Listes de vérification des sorties

HIMA recommande d'utiliser les listes de vérification disponibles pour l'étude, la programmation et la mise en service de sorties relatives à la sécurité. Les listes de vérification peuvent être utilisées comme documents techniques de conception et font la preuve que la planification a été exécutée avec soin.

Pour les canaux de sortie relatifs à la sécurité utilisés dans un système ou la mise en service, il convient de remplir la liste de vérification afin de contrôler quelles exigences sont à remplir. Ceci est le seul moyen de s'assurer que les exigences ont été comprises dans leur intégralité. La liste de vérification documente également la cohérence des liens entre le câblage externe et le programme utilisateur.

Les listes de vérification sont disponibles sur le site Internet HIMA en format Microsoft® Word®.

9 Logiciel

Le logiciel pour les automates relatifs à la sécurité des systèmes HIMax est structuré comme suit :

- Système d'exploitation,
- Programme utilisateur,
- Outil de programmation SILworX selon la norme IEC 61131-3.

Le *système d'exploitation* est chargé dans chaque module de la commande. Il est recommandé d'utiliser la version la plus récente pour les applications relatives à la sécurité. Le présent chapitre concerne particulièrement le système d'exploitation du processeur.

Le *programme utilisateur* est mis en œuvre à l'aide de l'outil de programmation SILworX et contient les fonctions spécifiques à l'installation que l'automate doit exécuter. Le paramétrage s'effectue également par le biais de SILworX.

Le programme utilisateur est traduit au moyen du générateur de codes puis transmis par le biais de l'interface Ethernet dans la mémoire non volatile de l'automate.

9.1 Aspects relatifs à la sécurité applicables au système d'exploitation

Chaque système d'exploitation homologué est clairement identifié par le numéro de révision et la signature CRC. Les autres versions du système d'exploitation homologuées par le TÜV pour les automates relatifs à la sécurité et les signatures correspondantes (CRC) sont soumises au contrôle de révision et consignées dans une liste établie conjointement avec le TÜV, à savoir la *Version List of Modules and Firmware for HIMax Systems from HIMA Paul Hildebrandt GmbH*

Une lecture de la version du système d'exploitation actuel est possible à l'aide de l'outil de programmation SILworX. Vérifier si une version homologuée du système d'exploitation est chargée dans les modules (se reporter à 10.3 Liste de vérification destinée à la configuration d'un programme utilisateur).

9.2 Aspects relatifs à la sécurité applicables à la programmation

Lors de la mise en œuvre d'un programme utilisateur, les exigences suivantes doivent être prises en compte.

9.2.1 Concept de sécurité pour l'utilisation de SILworX

Le concept de sécurité de SILworX :

- Lors de l'installation de SILworX, une somme de contrôle CRC sécurise l'intégrité du paquet de programmes sur le parcours du fabricant à l'utilisateur.
- SILworX exécute des tests de plausibilité afin de réduire les défauts lors de la saisie.
- Une double compilation avec comparaison finale des sommes de contrôle CRC atteste que les corruptions de données, dues à des défaillances temporaires dans le PC utilisés, sont détectées.

Double compilation du programme et comparaison des résultats :

1. Démarrer la compilation.
   ☑ Au terme de la compilation, SILworX affiche une somme de contrôle CRC.
2. Redémarrer la compilation.
   ☑ Au terme de la compilation, SILworX affiche une somme de contrôle CRC.

Si les deux sommes de contrôle CRC sont identiques, les résultats n'ont pas été corrompus pendant la compilation.

Lors de la première mise en service d'une commande relative à la sécurité, la sécurité de l'ensemble du système doit être contrôlée par un test fonctionnel exhaustif.

Test fonctionnels de la commande

1. Vérification de la correcte application de la fonction de commande à l'appui des données et flux des signaux.
2. Test complet fonctionnels de logique en procédant à des essais (voir chapitre 9.2.2).

La commande et le programme utilisateur sont suffisamment contrôlés.

Après une modification du programme utilisateur, ne vérifier que les parties de programmes concernées par la modification. À cet effet, le comparateur de révision sécurisé de SILworX peut être utilisé pour déterminer et indiquer quels changement ont été effectués par rapport à la version antérieure :

À chaque mise en service de la commande relative à la sécurité, respecter les exigences des normes d'application en matière de vérification et validation !

9.2.2 Vérification de la configuration et du programme utilisateur

Pour vérifier si le programme utilisateur respecte de la fonction de sécurité spécifiée, l'utilisateur doit réaliser des cas de test appropriés à la spécification du système.

En règle générale, le test indépendant est suffisant pour chaque boucle (composée d'une entrée, des connexions importantes du point de vue de l'application, d'une sortie).

Des cas de test sont également à effectuer pour l'évaluation numérique des formules. Des tests de classe d'équivalence sont parfaitement indiqués. Ce sont des tests réalisés dans des domaines de valeurs définis, aux limites ou dans des domaines non admissibles. Les cas de test doivent être choisis de telle sorte que l'exactitude du calcul peut être attestée. Le nombre nécessaire de cas de tests dépend de la formule utilisée et doit englober des couples de valeurs critiques.

HIMA recommande de procéder à une simulation active avec des sources. Cela atteste d'un câblage correct des capteurs et actionneurs du système, y compris pour ceux connectés par le biais d'E/S déportées. Cela est le seul moyen de contrôler la configuration du système.

Cette procédure est à respecter, tant lors de la première mise en œuvre d'un programme utilisateur que lors de ses modifications.

9.3 Paramètres de la ressource

⚠ AVERTISSEMENT

Risque de dommages corporels lié à une configuration erronée !

Ni l'outil de programmation ni la commande ne sont à même de vérifier certains paramètres fixés et spécifiques au projet. C'est pourquoi, il est impératif de saisir correctement ces paramètres dans l'outil de programmation et de vérifier la saisie effectuée après le téléchargement dans le système PE.

Ces paramètres sont

- **System ID**
- **Rack ID, voir 5.1 et le manuel du système (HI 801 001 E).**
- **Attribut Responsible des modules bus système, voir 5.2**
- **Safety Time**
- **Watchdog Time**
- **Allow Online Settings**
- **Autostart**
- **Start Allowed**
- **Load Allowed**
- **Reload Allowed**
- **Global Forcing Allowed**

Les paramètres suivants sont définis dans SILworX pour les actions autorisées pendant l'exploitation relative à la sécurité de la ressource et sont désignés comme paramètres relatifs à la sécurité.

Les paramètres définis pour l'exploitation relative à la sécurité ne sont pas strictement liés à une classe d'exigence. En effet, chacun d'entre eux doit être approuvé par l'organisme d'inspection compétent pour chacune des applications de l'automate.

9.3.1 Paramètres système de la ressource

Les paramètres système de la ressource peuvent être fixés dans SILworX, dans la boîte de dialogue *Properties* de la ressource.

Paramètre	Description	Valeur par défaut	Installation pour une exploitation sécurisée
Name	Nom de la ressource		À convenance
System ID [SRS]	System ID de la ressource 1...65 535 La valeur allouée à l'ID du système doit différer de la valeur par défaut, dans le cas contraire le projet n'est pas exécutable !	60 000	Valeur significative au sein du réseau des commandes. Ce réseau comprend toutes les commandes susceptible d'être reliées entre elles.
Safety Time [ms]	Temps de sécurité en millisecondes 20...22 500 ms (modifiable en ligne)	600 ms	Spécifique à l'application
Watchdog Time [ms]	Temps de chien de garde en millisecondes 6...7500 ms (modifiable en ligne)	200 ms	Spécifique à l'application
Target Cycle Time [ms]	Durée de cycle souhaitée ou maximale, voir *Target Cycle Time Mode,* 0...7500 ms. La durée maximale du cycle ne doit pas dépasser la durée définie pour le chien de garde moins 6 ms, sinon elle est rejetée par le système PE. Si la valeur par défaut est définie à 0 ms, la durée de cycle n'est pas prise en compte (modifiable en ligne).	0 ms	Spécifique à l'application
Target Cycle Time Mode	Utilisation de la durée du cycle, *Target Cycle Time [ms]* (modifiable en ligne) voir Tableau 16	Fixed-tolerant	Spécifique à l'application

Multitasking Mode	Mode 1 La durée d'un cycle du processeur est basée sur le temps d'exécution nécessaire de tous les programmes utilisateurs. Mode 2 Le processeur met à disposition des programmes utilisateurs à haute priorité, le temps d'exécution en surplus de programmes utilisateurs à basse priorité. Mode d'exploitation pour une disponibilité élevée. Mode 3 Le processeur est en mode attente pendant que le temps d'exécution non nécessaire aux programmes utilisateurs expire, prolongeant ainsi la durée du cycle.	Mode 1	Spécifique à l'application
Max.Com. Time Slice ASYNC [ms]	Valeur maximale en ms de la tranche de temps utilisée pendant le cycle de la ressource pour communiquer, voir manuel de communication (HI 801 101 E), 2...5 000 ms	60 ms	Spécifique à l'application
Max. Duration of Configuration Connections [ms]	Il définit quelle durée est disponible au sein d'un cycle CPU pour la communication des données de processus, 6...5000 ms	6 ms	Spécifique à l'application
Maximum System Bus Latency [µs]	Temporisation maximale d'un message entre un module d'E/S et de processeur 0, 100...50 000 µs i Le paramétrage de la latence maximale du bus système à une valeur > 0 requiert une licence.	0 µs	Spécifique à l'application
Allow Online Settings	ON : Tous les paramètres indiqués sous OFF sont modifiables en ligne avec PADT. OFF : Ces paramètres ne sont **pas** modifiables en ligne : ▪ *System ID* ▪ *Autostart* ▪ *Global Forcing Allowed* ▪ *Global Force Timeout Reaction* ▪ *Load Allowed* ▪ *Reload Allowed* ▪ *Start Allowed* Ces paramètres sont modifiables en ligne, si *Reload Allowed* est sur ON: ▪ *Watchdog Time* (de la ressource) ▪ *Safety Time* ▪ *Target Cycle Time* ▪ *Target Cycle Time Mode* Si *Reload Allowed* est sur OFF, ils ne sont pas modifiables en ligne. i *Allow Online Settings* ne peut être fixé sur *ON* que si le système PE est à l'arrêt !	ON	OFF, recommandé

Paramètre	Description		Valeur par défaut	Installation pour une exploitation sécurisée
Autostart	ON :	Si le processeur est raccordé à la tension d'alimentation, le programme utilisateur démarre automatiquement	OFF	Spécifique à l'application
	OFF :	Après la mise sous tension d'alimentation, pas de démarrage automatique.		
Start Allowed	ON :	Démarrage à froid ou à chaud autorisé par PADT en l'état *RUN* ou *STOP*.	ON	Spécifique à l'application
	OFF :	No Start Allowed		
Load Allowed	ON :	Téléchargement du programme utilisateur autorisé	ON	Spécifique à l'application
	OFF :	Téléchargement du programme utilisateur non autorisé		
Reload Allowed	ON :	Rechargement d'un programme utilisateur autorisé.	ON	Spécifique à l'application
	OFF :	Rechargement non autorisé d'un programme utilisateur Un chargement en cours n'est pas interrompu si l'on commute sur OFF		
Global Forcing Allowed	ON :	Forçage global autorisé pour la ressource	ON	Spécifique à l'application
	OFF :	Forçage global non autorisé pour la ressource		
Global Force Timeout Reaction	Détermine le comportement de la ressource lorsque s'écoule la temporisation du forçage global : ▪ *Stop Forcing* ▪ *Stop Resource*		Stop Forcing	Spécifique à l'application
Minimum Configuration Version	SILworX V2	La génération de code s'effectue comme sur SILworX V2, à l'exception des nouvelles fonctions.	SILworX V5	Spécifique à l'application
	SILworX V3	Génération de code pour HIMax V3.		
	SILworX V4	Génération de code pour HIMax V4.		
	SILworX V5	Génération de code pour HIMax V5. Ce paramètre permet d'assurer la compatibilité avec la version postérieure.		
safeethernet CRC	SILworX V2.36.0	La formation du CRC pour safe**ethernet** s'effectue comme dans SILworX V2.36.0. Ce paramètre est nécessaire à l'échange de données avec les ressources planifiées au moyen de SILworX V2.36 ou versions antérieures.	Version actuelle	Spécifique à l'application
	Version actuelle	La formation du CRC pour safe**ethernet** s'effectue avec l'algorithme actuel.		

Tableau 15 : Les paramètres de système de la ressource

Le tableau suivant décrit l'effet du mode *Target Cycle Time Mode*.

Target Cycle Time Mode	Effet sur les programmes utilisateurs	Effet sur rechargement, synchronisation de processeurs
Fixed	Le PES respecte la durée du cycle *Target Cycle Time* et prolonge le cycle, si nécessaire. Si le temps de traitement des programmes utilisateurs dépasse la durée du cycle *Target Cycle Time*, le cycle est prolongé.	Exécution du rechargement ou synchronisation uniquement si la durée du cycle *Target Cycle Time* est suffisante
Fixed-tolerant	Comme pour *Fixed*.	Prolongation au maximum tous les quatre cycles pour exécuter le rechargement ou la synchronisation
Dynamic-tolerant	Comme pour *Dynamic*.	Prolongation au maximum tous les quatre cycles pour exécuter le rechargement ou la synchronisation
Dynamic	HIMax respecte au mieux la durée du cycle *Target Cycle Time* et exécute le cycle dans un temps aussi court que possible.	Exécution du rechargement ou synchronisation uniquement si la durée du cycle *Target Cycle Time* est suffisante

Tableau 16 : Effet du paramètre Target Cycle Time

9.3.1.1 Calcul de Max. Duration of Configuration Connections [µs]

Si le traitement de la communication ne s'est pas achevé au cours d'un cycle de CPU, il se poursuit immédiatement dans le cycle suivant à partir du point d'interruption.

La communication des données de processus est de ce fait temporisée, néanmoins toutes les connexions avec des partenaires externes sont traitées équitablement et intégralement.

Pour le firmware HIMax CPU V3, la durée maximale des connexions de configuration de SILworX est fixée à 6 ms. Toutefois, la durée de traitement de la communication avec les partenaires externes au cours d'un cycle de CPU peut dépasser la valeur par défaut.

Pour le firmware HIMax CPU V4, la durée max. des connexions de configuration doit être paramétrée en fonction du temps de chien de garde prédéfini.

Valeur appropriée : sélectionner la valeur de telle sorte que les tâches cycliques du processeur puissent être exécutées pendant le temps restant *Watchdog Time - Max. Duration of Configuration Connections [µs]*.

La quantité des données de processus à communiquer dépend de la quantité des E/S déportées configurées, des connexions aux PADT existantes et des modules du système ayant une interface Ethernet.

Un premier paramétrage se calcule comme suit :

$T_{Config} = (n_{Com} + n_{RIO} + n_{PADT}) * 0{,}25\ ms + 2\ ms + 4*T_{Latence}$, où

T_{Config}	Paramètres système *Max. Duration of Configuration Connections [ms]*
n_{Com}	Nombre de modules avec interfaces Ethernet {SB, CPU, COM}
n_{RIO}	Nombre d'E/S déportées configurées
n_{PADT}	Nombre maximal des connexions PADT = 5
$T_{Latence}$	Paramètre système *Maximum System Bus Latency [µs]*

Si le temps calculé est inférieur à 6 ms, il est arrondi à 6 ms. Il est possible de corriger ultérieurement le temps calculé à l'appui de statistiques en ligne ou des propriétés de la ressource, ou de les modifier directement en ligne.

i Lors de la génération de code et de la conversion de projet, un avertissement est donné sur le PADT lorsque la valeur du paramètre *Max. Duration of Configuration Connections* est inférieure au résultat de la formule ci-dessus.

9.3.2 Variable système du matériel

Ces variables servent à modifier le comportement de la commande en cours de fonctionnement et à des états déterminés.

Paramètre	Fonction	Paramètres par défaut	Paramétrage pour une exploitation sécurisée
Force Deactivation	Sert à empêcher et à désactiver immédiatement le forçage	OFF	Spécifique à l'application
Spare 0...Spare 16	Pas de fonction	-	-
Emergency Stop 1... Emergency Stop 4	Interrupteur d'arrêt d'urgence pour désactiver la commande en cas de défaillances détectées par le programme utilisateur	OFF	Spécifique à l'application
Read-only in RUN	Après le démarrage de la commande aucune intervention n'est possible avec SILworX (*Stop, Start, Download*) Exceptions : forçage et rechargement	OFF	Spécifique à l'application
Reload Deactivation	Bloque l'exécution d'un rechargement	OFF	Spécifique à l'application

Tableau 17 : Variable système du matériel

Il est possible d'allouer une variable globale à ces variables de système dans l'éditeur de matériel (Hardware Editor) de SILworX dont la valeur est modifiée par une entrée physique ou la logique du programme utilisateur.

Exemple : fermeture et ouverture du système PE

La **fermeture** du système PE indique le verrouillage des possibilités d'accès de l'utilisateur pendant l'exploitation. Cela protège de toute manipulation non autorisée du programme utilisateur.

L'**ouverture** du système PE indique la désactivation du verrouillage (par ex. afin d'intervenir sur la commande).

Les trois variables système *Read only in Run*, *Reload Deactivation* et *Force Deactivation* sont utilisées pour le verrouillage.

Si les trois variables système sont sur ON, il n'est alors plus possible d'intervenir sur la commande. Dans ce cas, la commande ne peut être remise à l'état STOP qu'en redémarrant le processeur avec mode interrupteur en position *Init*. Le chargement d'un programme utilisateur est alors possible.

Rendre la commande verrouillable

1. Définir une variable globale de type BOOL, mettre la valeur initiale sur FALSE.
2. Allouer la variable globale comme variable de sortie aux trois variables système *Read only in Run*, *Reload Deactivation* et *Force Deactivation*.
3. Allouer la variable globale à la valeur de canal d'une entrée numérique.
4. Raccorder un interrupteur à clé à la sortie numérique.
5. Compiler le programme, le charger sur la commande et le démarrer.

Le détenteur de la clé adéquate peut ouvrir et fermer la commande. En cas de défaut dans le module d'entrée numérique correspondant, la commande est ouverte.

9.4 Forçage

Le forçage indique le remplacement de la valeur actuelle d'une variable par une valeur de forçage. Une variable peut recevoir sa valeur actuelle par le biais d'une entrée physique, une communication ou une connexion logique. Si la variable est forcée, sa valeur ne dépend plus du processus, elle est définie par l'utilisateur.

⚠ AVERTISSEMENT

L'utilisation de la valeur de forçage peut perturber l'exploitation relative à la sécurité !

- **Les valeurs de forçage peuvent être la cause de valeurs de sortie erronées.**
- **Le forçage prolonge la durée de cycle. Cela peut entraîner le dépassement du temps de chien de garde.**

Le forçage n'est autorisé qu'après accord de l'organisme d'inspection compétent et responsable des tests d'acceptation du système.

La personne responsable doit mettre en œuvre d'autres mesures techniques et organisationnelles pour garantir que la surveillance en matière de sécurité du processus est suffisante pendant le forçage. HIMA recommande de limiter le forçage dans le temps.

Pour de plus amples détails sur le forçage, se reporter au manuel du système (HI 801 001 E).

9.4.1 Forçage d'entrées physiques et de données de communication

La modification de l'attribution de variables globales forcées aux sources de données suivantes peut entraîner des résultats inattendus :

- Entrées physiques
- Protocoles de communication

La procédure suivante conduit au forçage involontaire d'une variable :

1. Une variable globale A est allouée à une source de données forcées et est elle aussi forcée.
2. L'allocation est annulée.
3. Une autre variable globale B est allouée à la source de données.
4. Un rechargement est effectué pour charger la modification au niveau du projet dans le système PE.

Résultat : la variable B **nouvellement allouée** est forcée contre toute attente !

Aide : Terminer le forçage de la variable A.

Les canaux ayant été forcés sont représentés dans l'affichage des canaux de l'éditeur de force.

Les variables globales, dont la source de données est le programme utilisateur, conservent la propriété *Forced* (forcé) en cas de modification de l'allocation.

9.5 Comparateur de versions sécurisé

Le comparateur de versions sécurisé de SILworX peut comparer des configurations de ressource entre elles :

- Configuration de ressource chargée dans la commande
- Configuration de ressource présente dans PADT
- Configuration de ressource exportée (archivée)

Le résultat du comparateur est de catégorie SIL 4, car il est généré par les fichiers chargeables, y compris les CRC.

Le comparateur de versions sécurisé doit être utilisé pour vérifier les modifications de programme avant chargement dans la commande.

Il détermine avec précision les parties modifiées de la configuration de ressource. Cela simplifie le contrôle des modifications et la détermination des données de test.

Une programmation structurée et l'utilisation de noms descriptifs depuis la première version de configuration facilitent l'interprétation des résultats comparés.

9.6 Protection contre les manipulations

L'utilisateur doit déterminer avec l'organisme d'inspection compétent les mesures à appliquer pour prévenir les manipulations.

Des mécanismes de protection sont intégrés pour empêcher toute modification fortuite ou non autorisée du système de sécurité dans le système PE et l'outil de programmation SILworX :

- Une modification du programme utilisateur ou de la configuration génère un nouveau CRC. Ces modifications peuvent seulement être transmises au système PE par téléchargement ou rechargement.
- Les possibilités d'intervention dépendent des droits de l'utilisateur connecté au le système PE.
- L'outil de programmation SILworX requiert un mot de passe pour accéder au système PE lorsque l'utilisateur se connecte.
- La connexion entre PADT et PES n'est pas nécessaire en mode RUN.

Les exigences selon les normes de sécurité et d'application relatives à la protection contre les manipulations doivent être respectées. L'autorisation au personnel et les mesures de protection nécessaires relèvent de la responsabilité de l'exploitant.

⚠ AVERTISSEMENT

Risque de dommages corporels lié à une manipulation non autorisée au niveau de la commande !

La commande doit être protégée contre tout accès non autorisé !

p. ex.:

- **modification des paramètres par défaut concernant l'identifiant et le mot de passe**
- **contrôle de l'accès physique à la commande et au PADT !**

L'accès aux données du système PE n'est possible que si le PADT utilisé dispose de l'outil de programmation SILworX et du projet utilisateur en version actuelle (maintenance des archives !).

La connexion entre PADT et PE n'est nécessaire que pour le chargement du programme utilisateur ou le diagnostic. Le PADT n'est pas nécessaire en fonctionnement normal. Une isolation de PADT et de PE pendant la phase d'exploitation normale protège contre tout accès non autorisé.

10 Programme utilisateur

Le présent chapitre aborde les aspects de sécurité applicables aux programmes utilisateurs.

10.1 Procédure générale

Procédure générale de programmation des automates HIMax pour des applications relatives à la sécurité :

1. Spécifications de la fonction de commande.
2. Écriture du programme utilisateur.
3. Compiler le programme utilisateur :
   Le programme utilisateur est sans erreur et peut être exécuté.
4. Vérification et validation.

Ensuite l'utilisateur peut tester le programme utilisateur et le système PE peut commencer l'exploitation sécurisée.

10.2 Cadre d'une application relative à la sécurité

(Pour de plus amples informations sur les spécifications et directives, explications concernant les exigences en matière de sécurité, se reporter au chapitre 3.3)

Le programme utilisateur doit être installé avec l'outil de programmation SILworX. Le système d'exploitation validé pour l'ordinateur personnel est indiqué dans la documentation de validation de la version de SILworX à utiliser.

Éléments essentiels de l'outil de programmation SILworX :

- Saisie (éditeur de programme), surveillance et documentation
- Variables globales avec noms symboliques et type de données (BOOL, UINT, etc.)
- Attribution des commandes du système HIMax (éditeur de matériel)
- Conversion du programme utilisateur en un format chargeable dans le système PE
- Configuration de la communication

10.2.1 Base de la programmation

Les opérations de commande doivent être répertoriées sous forme de spécifications ou de cahier des charges. Cette documentation sert de base pour vérifier la correcte application dans le programme utilisateur. Le format des spécifications dépend des tâches à accomplir. Elles peuvent être :

- *Logique combinatoire*
  - Schéma cause/effet (cause/effect diagram)
  - Logique de la connexion avec les fonctions et blocs fonctionnels
  - Blocs fonctionnels avec propriétés spécifiées
- *Commandes séquentielles (système de contrôle séquentiel)*
  - Description écrite des étapes incluant leurs conditions de progression et les composants externes à contrôler.
  - Plans séquentiels.
  - Format tabellaire ou matriciel des conditions de progression et des composants externes à contrôler.
  - Définition des restrictions, par ex. modes d'exploitation, ARRÊT D'URGENCE, etc.

Le concept d'E/S de l'installation doit inclure l'analyse des circuits d'excitation, c.-à-d. le type de composants externes :

- Composants externes (dispositifs de terrain) :
  - Signal d'entrée en exploitation normale (principe du courant de repos sur les dispositifs numériques)
  - Signal d'entrée en cas de défauts
  - Détermination des redondances requises relatives à la sécurité (1oo2, 2oo3)
  - Surveillance des divergences et réaction
  - Position et amorçage de la commande en exploitation normale
  - Réaction/position sécurisée en cas de coupure ou de panne de courant

Objectifs de la programmation du programme utilisateur :

- Compréhension aisée
- Déduction logique
- Tests simples
- Modifications intuitives

10.2.2 Fonctions du programme utilisateur

La programmation n'est soumise à aucune contrainte liée au matériel. Les fonctions du programme utilisateur sont librement programmables.

Lors de la programmation, le principe du courant de repos doit être pris en compte pour les entrées et sorties physiques. Au sein de la logique, seuls des éléments conformes à la norme IEC 61131-3 ainsi que leurs exigences fonctionnelles respectives, sont utilisés.

- Les entrées et sorties physiques opèrent normalement selon le principe du courant de repos, c.-à-d. que leur état de sécurité est *0*.
- Le programme utilisateur est doté de fonctions logiques et/ou arithmétiques très pertinentes, sans prendre en considération le principe du courant de repos des entrées et sorties physiques.
- La logique doit être explicitement conçue et documentée de manière intelligible afin de faciliter la recherche de défauts. Cela s'applique également à l'utilisation de schémas fonctionnels.
- Pour simplifier la logique, les entrées et sorties de tous les blocs fonctionnels et variables peuvent être inversées à convenance.
- Les signaux de défaut des entrées et sorties ou émanant de modules de logique doivent être évalués par le programmateur.

HIMA recommande d'appliquer le principe de l'encapsulation de fonctions aux blocs fonctionnels et aux fonctions définies par l'utilisateur, basées sur des fonctions de base. Cela permet de structurer clairement un programme utilisateur dans des modules (fonctions, blocs fonctionnels). Chaque module peut être pris en considération et testé individuellement. En regroupant des modules de petites taille à un module plus grand et à un programme utilisateur, l'utilisateur crée une fonction complète et complexe.

10.2.3 Paramètres système du programme utilisateur

Les paramètres suivants d'un programme utilisateur se fixent dans la boîte de dialogue *Properties* du programme utilisateur :

Paramètre	Fonction	Valeur par défaut	Paramétrage pour une exploitation sécurisée
Name	Nom du programme utilisateur		À convenance
Program ID	ID pour identification du programme lors de l'affichage dans SILworX, 1...32	1	Spécifique à l'application
Priority	Priorité du programme utilisateur : 0...31	0	Spécifique à l'application
Program's Maximum Number of CPU Cycles	Nombre maximal de cycles du processeur autorisé pour la durée d'un cycle de programme utilisateur.	1	Spécifique à l'application
Max. Duration for Each Cycle [µs]	Durée d'exécution maximale par cycle de processeur pour un programme utilisateur : 1...7 500 000 µs, 0 : non limité.	0 µs	Spécifique à l'application
Watchdog Time [ms] (calculated)	Temps de surveillance du programme utilisateur, calculé à partir du nombre maximal de cycles et du temps de chien de garde de la ressource Non modifiable !		
Classification	Classement du programme utilisateur : *Safety-related* ou *Standard* (uniquement pour documentation).	Safety-related	Spécifique à l'application
Allow Online Settings	Validation de la modification en ligne sur des paramètres d'autres programmes utilisateurs. N'est effectif que si *Allow Online Settings* de la ressource est sur *ON* !	ON	-
Autostart	Mode validé du démarrage automatique : démarrage à froid (*Cold Start*), démarrage à chaud (*Warm Start*), arrêt (*OFF*).	Cold Start	Spécifique à l'application
Start Allowed	ON : Démarrage du programme utilisateur par le biais du PADT autorisé. OFF : Démarrage du programme utilisateur par le biais du PADT non autorisé.	ON	Spécifique à l'application
Test Mode Allowed	ON : Le mode test est autorisé pour le programme utilisateur. OFF : Le mode test n'est pas autorisé pour le programme utilisateur.	OFF	Spécifique à l'application[1)]
Reload Allowed	ON : Le rechargement du programme utilisateur est autorisé. OFF : Le rechargement du programme utilisateur n'est pas autorisé.	ON	Spécifique à l'application
Local Forcing Allowed	ON : Forçage au niveau du programme autorisé. OFF : Forçage au niveau du programme non autorisé.	OFF	OFF, recommandé
Local Force Timeout Reaction	Comportement du programme utilisateur après expiration du temps de forçage : ▪ *Stop Forcing Only* ▪ *Stop Program*.	Stop Forcing Only	-

Paramètre	Fonction		Valeur par défaut	Paramétrage pour une exploitation sécurisée
Code Generation Compatibility	La génération de code est compatible avec les versions antérieures de SILworX		SILworX V5	
	SILworX V5	La génération de code est compatible avec SILworX V5.		
	SILworX V4	La génération de code est compatible avec SILworX V4.		Spécifique à l'application
	SILworX V3	La génération de code est compatible avec SILworX V3.		
	SILworX V2	La génération de code est compatible avec SILworX V2.		
[1] Après expiration du mode test, il est nécessaire d'effectuer un démarrage à froid du programme avant la reprise de l'exploitation relative à la sécurité !				

Tableau 18 : Paramètres de système du programme utilisateur

10.2.4 Génération de code

Le code est généré après la saisie complète du programme utilisateur et l'assignation des E/S de la commande. Lors de ces étapes, le CRC de configuration, c.-à-d. la somme de contrôle pour les fichiers de configuration, est formé.

Il s'agit d'une signature pour la configuration globale donnée en code hexadécimal, au format 32 bits. Tous les éléments configurables ou modifiables comme la logique, les variables, les paramètres interrupteurs y sont intégrés.

REMARQUE

Risque de défaillance du fonctionnement de la commande !

Avant le chargement du programme utilisateur pour une exploitation relative à la sécurité, l'utilisateur doit impérativement le compiler deux fois. Les deux versions générées doivent présenter les mêmes sommes de contrôle.

La double compilation du système ainsi que la comparaison des sommes de contrôle, assurent la détection des corruptions de données du programme utilisateur causées par des défaillances temporaires dans le matériel ou dans le système d'exploitation du PC utilisé.

Une deuxième compilation avec comparaison des sommes de contrôle est une option activable dans la génération de code.

10.2.5 Téléchargement et démarrage du programme utilisateur

Le chargement d'un PES dans le système HIMax par téléchargement ne peut s'effectuer que s'il a été mis sur STOP auparavant.

Un chargement englobe tous les programmes utilisateurs de la configuration du projet. Le chargement complet d'une configuration de projet est surveillé. Ensuite, le programme utilisateur peut démarrer c.-à-d. que le traitement cyclique des tests de fonctionnement commence.

i Après chaque chargement de programmes utilisateurs dans la commande, HIMA recommande de sauvegarder également les données de projet en utilisant la fonction Rechargement, par ex. sur un support d'enregistrement externe.

Cela permet de garantir la disponibilité permanente des données de projet correspondant à la configuration chargées dans la commande, même si le PADT est défaillant.

HIMA recommande une sauvegarde régulière des données, indépendamment du chargement de programme.

10.2.6 Rechargement

Si des modifications ont été effectuées sur les programmes utilisateurs, celles-ci peuvent être transmises sur le système PE en cours d'exploitation. Après vérification par le système d'exploitation, le programme utilisateur modifié est activé et prend en charge les opérations de commande.

Avant de procéder à un rechargement, le système d'exploitation vérifie si les tâches supplémentaires nécessaires sont susceptibles d'augmenter la durée de cycle des programmes utilisateurs à tel point que le temps de chien de garde fixé peut être dépassé. Si tel est le cas, le rechargement est interrompu avec émission d'un message de défaut et la commande continue de fonctionner avec la configuration de projet utilisée jusque lors.

i **La commande peut interrompre un rechargement**

Pour mener à bien un rechargement, prévoir, lors de la détermination du temps de chien de garde, une réserve pour le rechargement ou augmenter provisoirement le temps de chien de garde de la commande afin d'accroître la réserve.

L'augmentation provisoire du temps de chien de garde doit être approuvé par l'organisme d'inspection compétent.

Un dépassement de la durée de cycle de consigne peut également entraîner une interruption du rechargement.

Un rechargement n'est possible que lorsque le paramètre système *Reload Allowed* se trouve sur ON et que la variable système *Reload Deactivation* se trouve sur OFF.

i Il relève de la responsabilité de l'utilisateur de prévoir des réserves lors de la détermination du temps de chien de garde. Celles-ci doivent permettre de maîtriser les situations suivantes :

- Variations de la durée de cycle du programme utilisateur.
- Fortes charges soudaines du cycle, dues notamment à la communication.
- Expiration du temps limite lors de la communication.

Pour de plus amples informations sur le temps de chien de garde, se reporter au chapitre 3.2.2.

10.2.7 Test en ligne

Dans la logique du programme utilisateur, il est permis d'utiliser des champs de test en ligne (champs OLT) pour afficher des variables pendant l'exploitation de la commande.

Pour de plus amples informations sur l'utilisation des champs OLT, se reporter au mot clé *OLT Field* dans l'aide en ligne de SILworX et dans le manuel d'introduction à SILworX (HI 801 103 E).

10.2.8 Mode pas à pas

Pour diagnostiquer les défauts lors d'un test en ligne, le programme utilisateur peut être exécuté en mode pas à pas, c.-à-d. cycle par cycle. Chaque cycle est déclenché par une commande du PADT.

Cette fonction ne peut être utilisée que lorsque le paramètre système *Freeze Allowed* se trouve sur ON dans le programme utilisateur correspondant.

Etat	Signifié
OFF	Mode pas à pas impossible.
ON	Mode pas à pas possible (paramètre par défaut).

Tableau 19 : Interrupteur programme utilisateur *Freeze Allowed*

REMARQUE

Risque de perturbation des opérations relatives à la sécurité !

Le mode pas à pas n'est pas autorisé en exploitation relative à la sécurité, !

10.2.9 Modification des paramètres système en ligne

Il est possible de modifier les paramètres système du Tableau 20 dans la commande en ligne. Un cas d'application classique est l'augmentation provisoire du temps de chien de garde pour pouvoir effectuer un rechargement.

Avant de fixer des paramètres au moyen d'une commande en ligne, évaluer si cette modification de paramètres peut conduire à un état critique pour la sécurité. Au besoin, prendre des mesures techniques et/ou organisationnelles afin d'écarter tout risque de dommage. Observer les normes d'application !

Les valeurs de temps de sécurité et de temps de chien de garde sont à vérifier par rapport au temps de sécurité requis par l'application ou la durée de cycle réelle. Le système PE ne peut vérifier ces valeurs !

La commande ne permet pas de paramétrer le temps de chien de garde à une valeur inférieure au temps de chien de garde de la configuration chargée dans le système PE.

Paramètre	Modifiable dans l'état du système PE
System ID	STOP
Watchdog Time (de la ressource)	RUN, STOP / VALID CONFIGURATION
Safety Time	RUN, STOP / VALID CONFIGURATION
Target Cycle Time	RUN, STOP / VALID CONFIGURATION
Target Cycle Time Mode	RUN, STOP / VALID CONFIGURATION
Allow Online Settings	ON->OFF : Tous OFF->ON : STOP
Autostart	Tous
Start Allowed	Tous
Load Allowed	Tous
Reload Allowed	Tous
Global Forcing Allowed	Tous
Global Force Timeout Reaction	Tous

Tableau 20 : Paramètres modifiables en ligne

10.2.10 Documentation du programme pour applications relatives à la sécurité

L'outil de programmation SILworX permet l'impression automatique de la documentation d'un projet. Les types de documents les plus importants sont :

- Déclaration d'interfaces
- Liste de signaux
- Logique
- Description des types de données
- Configurations du système, des modules et des paramètres système
- Configuration du réseau
- Liste de références croisées des signaux

La documentation est requise pour les test d'acceptation d'un système soumis à approbation par un organisme d'inspection (par ex. TÜV).

10.2.11 Multitâche

Multitâche désigne la capacité du système HIMax à traiter jusqu'à 32 programmes utilisateurs au sein d'un processeur.

Le démarrage, l'arrêt et le chargement (même le rechargement) des différents programmes utilisateurs peuvent s'effectuer individuellement les uns des autres.

Le cycle d'un programme utilisateur peut durer pendant plusieurs cycles du processeur. Cela peut être contrôlé par les paramètres de la ressource et du programme utilisateur. A partir de ces paramètres, SILworX calcule le temps de chien de garde du programme utilisateur :
Temps de chien de garde$_{\text{Programme utilisateur}}$ = *Temps de chien de garde*$_{\text{Processeur}}$ * *Nombre maximal de cycles*

Les différents programmes utilisateurs fonctionnent généralement sans effet rétroactif. Néanmoins, les influences réciproques peuvent être causées par :

- Utilisation des mêmes variables globales dans plusieurs programmes utilisateurs.
- Longueur imprévisible de la durée d'exécution dans des programmes utilisateurs individuels, si aucune limite n'a été établie au moyen du paramètre *Max. Duration for Each Cycle*.
- La répartition des cycles de programmes utilisateurs sur les cycles de processeurs influence considérablement le temps de réponse du programme utilisateur ainsi que les variables qu'il affiche !
- Un programme utilisateur évalue une variable globale affichée par un autre programme utilisateur, après au moins un cycle du processeur. Dans un pire cas, la temporisation peut être de l'ordre de 32 cycles de processeur. La réaction aux modifications de ces variables globales est proportionnellement temporisée !

REMARQUE

Risque d'influences réciproques entre les programmes utilisateurs !

L'utilisation des mêmes variables globales dans plusieurs programmes utilisateurs peut conduire à une variété de conséquences causées par des influences réciproques au sein des programmes utilisateurs.

- **Planifier avec précision l'utilisation de variables globales dans plusieurs programmes utilisateurs.**
- **Utiliser des références croisées dans SILworX pour vérifier l'utilisation des données globales. Les données globales ne peuvent allouer les valeurs que d'une seule entité, soit d'entrées relatives à la sécurité au sein d'un programme utilisateur, soit par le biais de protocoles de communication relatifs à la sécurité !**

Il relève de la responsabilité de l'utilisateur d'écarter tout risque d'interférences dues à des influences réciproques entre les programmes utilisateurs !

Pour de plus amples détails sur le Multitâche, se reporter au manuel du système (HI 801 001 E).

10.2.12 Tests d'acceptation et Autorité chargée de leurs approbations

HIMA recommande d'impliquer l'autorité compétente aussi tôt que les tests d'acceptation d'un système sont susceptibles d'être soumis à approbation.

L'acceptation fait référence uniquement à la fonction utilisateur et non aux modules relatifs à la sécurité, ni aux automates du système HIMax qui disposent déjà d'une attestation d'examen de type CE.

10.3 Liste de vérification destinée à la configuration d'un programme utilisateur

HIMA recommande de passer en revue la liste de vérification portant sur des aspects de sécurité de programmation avant et après le chargement d'un programme nouveau ou modifié. La liste de vérification peut être utilisée comme base de projet et atteste que la planification a été exécutée avec soin.

La liste de vérification est disponible sur le site Internet HIMA en format Microsoft® Word®.

11 Configuration de la communication

A l'instar des variables d'entrée et de sortie physiques, les valeurs de variables peuvent être également remplacées par le biais d'une connexion de données avec d'autres systèmes. A cet effet, les variables sont déclarées à l'aide de l'outil de programmation SILworX dans la rubrique des protocoles de la ressource correspondante.

11.1 Protocoles standards

Plusieurs protocoles de communication ne permettent qu'une transmission de données non relative à la sécurité. Ces protocoles peuvent être utilisés pour des parties non relatives à la sécurité d'une fonction d'automatisation.

⚠ AVERTISSEMENT

Risque de dommages corporels lié à l'utilisation de données importées non sécurisées !

Ne pas utiliser des données importées de sources non sécurisées pour des fonctions de sécurité du programme utilisateur.

Les protocoles standards suivants sont disponibles :

- Sur les interfaces Ethernet du module de communication :
  - Modbus TCP (maître/esclave).
  - Modbus redondant (esclave).
  - SNTP
  - Send/Receive TCP
  - PROFINET IO (contrôleur, dispositif).
- Sur les interfaces du bus de terrain (RS485) du module de communication selon le modèle de dispositif :
  - Modbus (maître/esclave).
  - Modbus redondant (esclave).
  - PROFIBUS DP (maître/esclave).

11.2 Protocole relatif à la sécurité safe**ethernet**

La surveillance de la communication relative à la sécurité se paramètre dans l'éditeur safe**ethernet**.

Pour de plus amples détails concernant safe**ethernet**, se reporter au manuel de communication (HI 801 101 E).

REMARQUE

Possibilité de transition involontaire à l'état de sécurité !

***ReceiveTMO* est un paramètre relatif à la sécurité !**

ReceiveTMO est le temps de surveillance sur PES 1, pendant lequel une réponse correcte de PES 2 doit être reçue.

i *ReceiveTMO* s'applique également en sens inverse, de PES 2 à PES 1 !

Si aucune réponse correcte du partenaire de communication ne parvient pendant *ReceiveTMO*, HIMax ferme la communication relative à la sécurité. Les variables d'entrée de cette connexion safe**ethernet** se comportent selon les paramètres fixés sous *Freeze Data on Lost Connection [ms]*. Pour des fonctions relatives à la sécurité devant être exécutées par le biais de safe**ethernet**, seul le paramètre *Use Initial Data* doit être utilisé.

i Dans les calculs suivants pour déterminer le temps de réaction maximal au pire cas (Worst Case Reaction Time*)*, il est possible d'utiliser la durée du cycle à atteindre au lieu de celle du temps de chien de garde, si le mode durée du cycle à atteindre est réglé sur *Fixed* ou *Fixed-tolerant*.

11.3 Temps de réaction maximal pour safe**ethernet**

Dans les exemples suivants, les formules pour calculer le temps de réaction maximal s'appliquent à une connexion avec des commandes HIMatrix si le paramètre *Safety Time* est fixé à = 2 * temps de chien de garde. Ces formules sont toujours applicables aux commandes HIMax.

i Le temps de réaction maximal admissible dépend du processus et doit être approuvé en concertation avec l'organisme d'inspection en charge de l'acceptation.

Termes :

ReceiveTMO :	Temps de surveillance dans PES 1 au cours duquel une réponse valide de PES 2 doit être reçue. Dans le cas contraire et après écoulement du temps, la communication relative à la sécurité est fermée.
Production Rate :	Intervalle minimal entre deux envois de données.
Watchdog Time :	Durée maximale autorisée d'un cycle RUN dans une commande. La durée du cycle RUN dépend de la complexité du programme utilisateur et du nombre de connexions safe**ethernet.** Le temps de chien de garde (Watchdog Time - WDT) est à introduire dans les propriétés de la ressource.
Worst Case Reaction Time :	Temps de réaction maximal pour la transmission de la modification de signal d'une entrée physique (In) d'un PES 1 jusqu'à la modification de la sortie physique (Out) d'un PES 2.
Delay :	Temporisation d'une voie de transmission, par ex. en cas de connexion par modem ou satellite. En cas de connexion directe, une temporisation de 2 ms peut tout d'abord être déterminée. La temporisation réelle de la voie de transmission peut être évaluée par l'administrateur de réseau compétent.

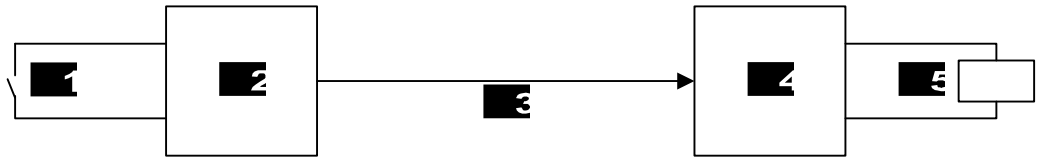
Les calculs postérieurs des temps de réaction maximaux admissibles sont régis par les conditions suivantes :

- Les signaux transmis par le biais de safe**ethernet** doivent être traités dans les commandes correspondantes au cours d'un cycle de CPU.
- Ajouter les temps de réaction des capteurs et actionneurs.

Les calculs s'appliquent également à des signaux en sens inverse.

11.3.1 Calcul du temps de réaction maximal de deux commandes HIMax

Calculer le temps de réaction maximal T_R (worst case reaction time) à partir du changement d'un capteur de la commande 1 (In) jusqu'à la réaction de la sortie (Out) de la commande 2 comme suit :



1 Entrée
2 Commande HIMax 1
3 Protocole relatif à la sécurité
4 Commande HIMax 2
5 Sortie

Figure 3 : Temps de réaction applicable à la connexion de deux commandes HIMax

$T_R = t_1 + t_2 + t_3$

T_R Temps de réaction maximal

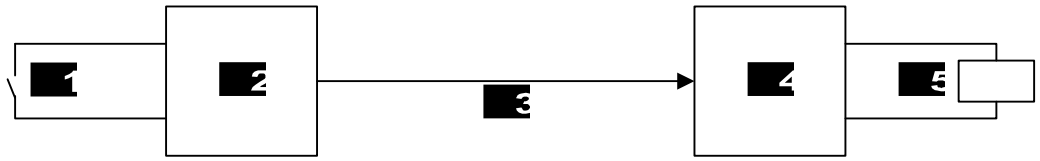
t_1 Temps de sécurité de la commande HIMax 1

t_2 Temps de surveillance, *ReceiveTMO*

t_3 Temps de sécurité de la commande HIMax 2

11.3.2 Calcul du temps de réaction maximal en lien avec une commande HIMatrix

Calculer le temps de réaction maximal T_R (worst case reaction time) à partir du changement d'un capteur (In) de la commande HIMax jusqu'à la réaction de la sortie (Out) de la commande HIMatrix comme suit :



1 Entrée
2 Commande HIMax
3 Protocole relatif à la sécurité
4 Commande HIMatrix
5 Sortie

Figure 4 : Temps de réponse applicable à la connexion d'une commande HIMax avec une commande HIMatrix

$T_R = t_1 + t_2 + t_3$

T_R Temps de réaction maximal

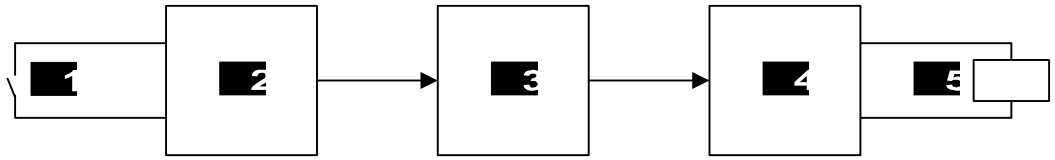
t_1 Temps de sécurité de la commande HIMax

t_2 Temps de surveillance, *ReceiveTMO*

t_3 2 * temps de chien de garde de la commande HIMatrix

11.3.3 Calcul du temps de réaction maximal avec deux commandes HIMatrix ou module d'E/S déportées

Calculer comme suit le temps de réaction maximal T_R (worst case reaction time) à partir du changement d'un capteur (In) dans la première commande HIMatrix ou dans les modules d'E/S déportées (par ex. F3 DIO 20/8 01) jusqu'à la réaction de la sortie dans la deuxième commande HIMatrix (Out) ou dans les modules d'E/S déportées :



1 Entrée
2 Module d'E/S déportées 1
3 Commande HIMax
4 Module d'E/S déportées 2
5 Sortie

Figure 5 : Temps de réponse avec deux modules d'E/S déportées et une commande HIMax

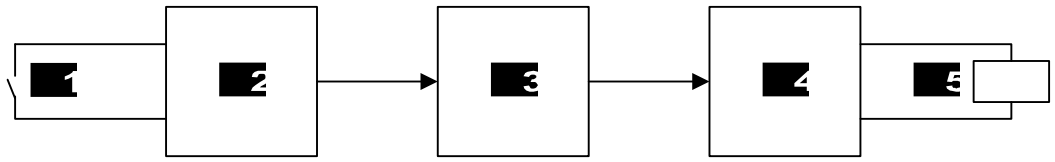
$T_R = t_1 + t_2 + t_3 + t_4 + t_5$

T_R	Temps de réaction maximal
t_1	2 * temps de chien de garde de la commande HIMatrix 1 ou module d'E/S déportées 1
t_2	*ReceiveTMO1*
t_3	2 * temps de chien de garde de la commande HIMax
t_4	*ReceiveTMO2*
t_5	2 * temps de chien de garde de la commande HIMatrix 2 ou module d'E/S déportées 2

i Les deux modules d'E/S déportées 1 et 2 peuvent être identiques. Les temps sont également applicables si l'on utilise une commande HIMatrix au lieu d'un module d'E/S déportées.

11.3.4 Calcul du temps de réaction maximal avec deux commandes HIMax et une commande HIMatrix

Calculer le temps de réaction maximal T_R (worst case reaction time) à partir du changement d'un capteur (In) dans la première commande HIMax jusqu'à la réaction de la sortie (Out) dans la deuxième commande HIMax comme suit :



1 Entrée
2 Commande HIMax 1
3 Commande HIMatrix
4 Commande HIMax 2
5 Sortie

Figure 6 : Temps de réponse avec deux commandes HIMax et une commande HIMatrix

$T_R = t_1 + t_2 + t_3 + t_4 + t_5$

T_R Temps de réaction maximal

t_1 Temps de sécurité de la commande HIMax 1

t_2 *ReceiveTMO1*

t_3 2 * temps de chien de garde de la commande HIMatrix

t_4 *ReceiveTMO2*

t_5 Temps de sécurité de la commande HIMax 2

i Les deux commandes HIMax 1 et 2 peuvent être identiques.
La commande HIMatrix peut être également une commande HIMax.

11.4 Protocole relatif à la sécurité PROFIsafe

Se reporter aux conditions d'utilisation du protocole PROFIsafe dans le manuel de communication (HI 801 101 E). Les conditions indiquées sont à respecter.

Les formules de calcul du temps de réaction sont également répertoriées dans le manuel de communication.

Annex

Glossaire

Terme	Description
Adresse MAC	Media access control address, adresse matérielle d'une connexion réseau
AI	Analog input, entrée analogique
AO	Analog output, sortie analogique
ARP	Address resolution protocol : protocole réseau destiné à l'attribution d'adresses réseaux adresses matérielles
CEI	Commission électrotechnique internationale
CEM	Compatibilité électromagnétique
COM	Module de communication
CRC	Contrôle de redondance cyclique
DI	Digital input, entrée numérique
DO	Digital output, sortie numérique
EN	Norme européenne
ESD	Electrostatic discharge, décharge électrostatique
FB	Fieldbus, bus de terrain
FBD	Function block diagrams, diagramme de blocs fonctionnels
FTT	Fault tolerance time, temps de tolérance aux défauts
ICMP	Internet control message protocol, protocole réseau pour messages concernant l'état et les erreurs
PADT	Programming and debugging tool (selon CEI 61131-3), PC avec SILworX
Panneau de raccordement	Panneau de raccordement pour module HIMax
PE	Protective earth, protection par mise à la terre
PES	Système électronique programmable
R	Read, lecture
R/W	Read/Write
Rack ID	Identification d'un support de base (numéro)
Sans effet rétroactif	Etant supposé que deux circuits d'entrées sont connectés à la même source (par ex. transmetteur). Un circuit d'entrée est qualifié sans effet rétroactif lorsqu'il n'altère pas les signaux d'un autre circuit d'entrée.
SB	Bus système
SFF	Safe failure fraction, part de défaillances sûres
SIL	Safety integrity level, niveau d'intégrité de sécurité (selon CEI 61508)
SILworX	Outil de programmation pour HIMax
SNTP	Simple network time protocol (RFC 1769), protocole d'heure réseau simple
SRS	System.Rack.Slot, adressage connecteurs d'un module
SW	Logiciel
TBTP	Très basse tension de protection
TBTS	Très basse tension de sécurité
TMO	Timeout, temps d'expiration
W	Write, écriture
WD	Watchdog, chien de garde. Temporisateur de surveillance pour modules ou programmes. Si le temps du chien de garde est excédé, le module ou le programme se met en arrêt pour cause de défauts.
WDT	Watchdog time, temps de chien de garde
w_S	Valeur de crête de la tension alternative complète des composants

Index des figures

Index des tableaux

Index

HI 801 351 F

Albert-Bassermann-Str. 28
68782 Brühl, Allemagne
Tél. +49 6202 709-0
Fax +49 6202 709-107
HIMax-info@hima.com
www.hima.com

SAFETY
NONSTOP