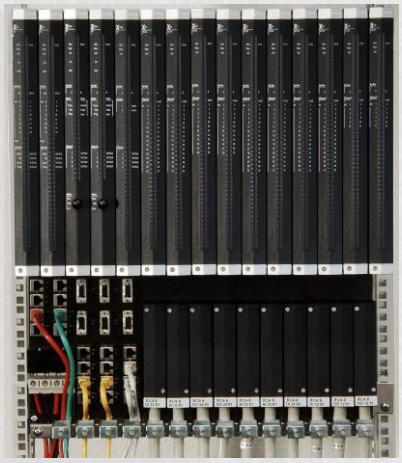


HIMax®

Manuel de sécurité

SAFETY
NONSTOP

HIMA

SÉCURITÉ

8

Contact

Adresse HIMA :

HIMA Paul Hildebrandt GmbH

Boite postale 1261

D-68777 Brühl, Germany

Tél. : +49 6202 709-0

Fax : +49 6202 709-107

E-mail : info@hima.com

Document original	Description
HI 801 002 D, Rev. 7.01 (1530)	Traduction française du document original rédigé en allemand

Sommaire

1 Manuel de sécurité 7
1.1 Validité et version actuelle 7
1.2 Objectifs du manuel 7
1.3 Personnes concernées 8
1.4 Conventions typographiques 8
1.4.1 Consignes de sécurité 8
1.4.2 Mode d'emploi 9
2 Consignes d'utilisation des systèmes HIMax 10
2.1 Utilisation conforme à l'usage prévu 10
2.1.1 Domaine d'application 10
2.1.2 Conditions d'environnement 10
2.2 Obligations des fabricants de machines et d'installations ainsi que des exploitants 10
2.2.1 Raccordement de partenaires de communication 10
2.2.2 Utilisation de la communication de sécurité 10
2.3 Mesures de protection ESD 11
2.4 Autres documentations du système 11
3 Concept de sécurité pour l'utilisation des systèmes PE 12
3.1 Sécurité et disponibilité 12
3.1.1 Calculs des valeurs PFD, PFH et SFF 12
3.1.2 Autotest et diagnostic d'erreurs 12
3.1.3 PADT 13
3.1.4 Redondance 13
3.1.5 Structure des systèmes de sécurité selon le principe de l'émission de courant 13
3.2 Temps importants pour la sécurité 14
3.2.1 Temps de sécurité du processus 14
3.2.2 Temps de chien de garde de la ressource 14
3.2.3 Temps de chien de garde du programme utilisateur 16
3.2.4 Temps de sécurité de la ressource 16
3.2.5 Temps de sécurité du programme utilisateur 16
3.2.6 Temps de réponse 16
3.3 Essai périodique(Proof Test selon IEC 61508) 17
3.3.1 Exécution du test périodique 17
3.3.2 Fréquence des tests périodiques 17
3.4 Exigences de sécurité 17
3.4.1 Étude et conception du matériel 17
3.4.2 Programmation 18
3.4.3 Communication 18
3.4.4 Opérations de maintenance 19
3.4.5 La cyber-sécurité des systèmes HIMax 19
3.5 Certification 21
3.5.1 Conditions d'essai 22
4 Processeur 25
4.1 Tests automatiques 25

4.2 Réponses aux erreurs dans le processeur 25
4.3 Remplacement des processeurs 25
4.4 Processeur X-CPU 01 26
4.5 Processeur X-CPU 31 26
5 Module bus système 27
5.1 Rack ID 27
5.2 Responsibility 27
6 Module de communication 30
7 Modules d'entrée 31
7.1 Généralités 31
7.2 Sécurité des capteurs, encodeurs et transmetteurs 31
7.3 Réaction en cas de défauts 32
7.4 Entrées Tout ou Rien de sécurité 32
7.4.1 Tests fonctionnels des signaux d'entrée 32
7.4.2 Redondance 32
7.4.3 Crêtes sur entrées Tout Ou Rien 32
7.5 Entrées analogiques de sécurité et entrées de l'interrupteur de proximité 32
7.5.1 Procédures de test 32
7.5.2 Redondance 33
7.5.3 État de LL, L, N, H, HH pour X-AI 32 01 et X-AI 32 02 33
7.6 Entrées de compteur de sécurité 33
7.6.1 Procédures de test 33
7.6.2 À prendre en compte pour le compteur X-CI 24 01 ! 33
7.6.3 Redondance 34
7.7 Listes de vérification des entrées 34
8 Modules de sortie 35
8.1 Généralités 35
8.2 Sécurité des actionneurs 35
8.3 Réponse aux erreurs 35
8.4 Sorties Tout ou Rien de sécurité 35
8.4.1 Procédures de test pour sorties Tout Ou Rien 36
8.4.2 Output Noise Blanking 36
8.4.3 Comportement en cas de court-circuit externe ou de surcharge 36
8.4.4 Redondance 36
8.5 Sorties relais de sécurité 36
8.5.1 Tests fonctionnels pour sorties relais 37
8.5.2 Redondance 37
8.6 Sorties analogiques de sécurité 37
8.6.1 Procédures de test pour sorties analogiques 37
8.6.2 Output Noise Blanking 37
8.6.3 Comportement en cas de rupture de ligne externe 37
8.6.4 À prendre en compte pour le module de sortie analogique X-AO 16 01 ! 38
8.6.5 Redondance 38
8.7 Listes de vérification des sorties 38

9	**Modules d'E/S spéciaux**	**39**
9.1	**Module HART X-HART 32 01**	**39**
9.1.1	Fonction de sécurité	39
9.2	**Module de protection contre la survitesse X-MIO 7/6 01**	**39**
9.2.1	Fonction de sécurité	39
9.2.2	Redondance	39
10	**Logiciel**	**40**
10.1	**Aspects relatifs à la sécurité pour le système d'exploitation**	**40**
10.2	**Aspects relatifs à la sécurité pour la programmation**	**40**
10.2.1	Concept de sécurité de SILworX	40
10.2.2	Vérification de la configuration et du programme utilisateur	41
10.3	**Paramètres de la ressource**	**41**
10.3.1	Paramètres système de la ressource	42
10.4	**Forçage**	**47**
10.4.1	Forçage des sources de données	48
10.5	**Comparateur de versions sécurisé**	**48**
11	**Programme utilisateur**	**49**
11.1	**Procédure générale**	**49**
11.2	**Cadre d'une utilisation relative à la sécurité**	**49**
11.2.1	Base de la programmation	49
11.2.2	Fonctions du programme utilisateur	50
11.2.3	Paramètres système du programme utilisateur	51
11.2.4	Génération de codes	52
11.2.5	Chargement et démarrage du programme utilisateur	52
11.2.6	Rechargement	53
11.2.7	Test en ligne	54
11.2.8	Mode test	54
11.2.9	Modification des paramètres système pendant exploitation	55
11.2.10	Documentation du programme pour applications de sécurité	55
11.2.11	Multitâche	56
11.2.12	Essais de réception et organismes en charge de leur approbation	56
11.3	**Liste de contrôle pour la création d'un programme utilisateur**	**56**
12	**Configuration de la communication**	**57**
12.1	**Protocoles standards**	**57**
12.2	**Protocole sécurisé safeethernet**	**57**
12.3	**Temps de réaction maximal pour safeethernet**	**58**
12.3.1	Calcul du temps de réponse maximal entre deux contrôleurs HIMax	59
12.3.2	Calcul du temps de réponse maximal pour une connexion avec un contrôleur HIMatrix	59
12.3.3	Calcul du temps de réponse entre deux contrôleurs HIMatrix ou un contrôleur HIMatrix et un module d'Entrées/Sorties déportées	60
12.3.4	Calcul du temps de réponse maximal pour deux contrôleur HIMax et un contrôleur HIMatrix interconnectés	60
12.4	**Protocole sécurisé PROFIsafe**	**61**
13	**Utilisation dans le cadre d'un système de détection d'incendie**	**62**

14 Utilisation comme dispositif de sécurité, contrôle et régulation avec installation d'alarme pour les concentrations de gaz 64

Annexe 65

Glossaire 65

Index des figures 66

Index des tableaux 67

Index 68

1 Manuel de sécurité

Ce manuel contient des informations pour une utilisation des automates HIMax relatifs à la sécurité.

Les conditions requises garantissant l'installation, la mise en service sans risque, ainsi que la sûreté de fonctionnement et la maintenance des automates HIMax sont :

- Connaissance de la règlementation.
- Mise en œuvre technique rigoureuse des consignes de sécurité contenues dans le présent manuel par du personnel qualifié.

Dans les cas suivants, des perturbations ou endommagements des fonctions de sécurité peuvent être à l'origine de dommages corporels, matériels ou environnementaux pour lesquels HIMA décline toute responsabilité :

- En cas d'interventions non qualifiées sur les automates.
- En cas de désactivation ou de contournement (bypass) des fonctions de sécurité.
- En cas de non-observation des consignes du présent manuel.

HIMA développe, fabrique et teste des systèmes d'automatisation HIMax répondant à toutes les normes de sécurité applicables. L'utilisation des automates n'est autorisée que lorsque toutes les conditions suivantes sont remplies :

- Uniquement dans le cadre des applications prévues dans les descriptions.
- Uniquement dans les conditions environnementales spécifiées.
- Uniquement en association avec les périphériques autorisés.

Dans un souci de lisibilité, le présent manuel ne contient pas l'ensemble des détails concernant tous les modèles d'automates HIMax. Pour de plus amples détails, se reporter, à chaque manuel concerné.

Ce manuel de sécurité fait office de « notice d'instructions originale » au sens de la directive machines (directive 2006/42/CE).

La documentation originale du système HIMA est rédigée en allemand. Les déclarations de la documentation allemande sont valides.

1.1 Validité et version actuelle

Rev. 7.01	Ce manuel de sécurité est à consulter de préférence lorsque les produits suivants sont utilisés : ▪ Système d'exploitation HIMax à partir de la version 7 et ▪ SILworX à partir de la version 7

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'utilisation de versions plus anciennes d'HIMax et SILworX, se reporter aux révisions antérieures du présent manuel.

1.2 Objectifs du manuel

Ce manuel contient des informations pour une utilisation des automates HIMax relatifs à la sécurité. Il propose une introduction au concept de sécurité du système HIMax et doit sensibiliser le lecteur sur la question de la sûreté.

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

1.3 Personnes concernées

Ce manuel s'adresse aux planificateurs, aux ingénieurs de projet et aux programmateurs d'installations d'automatisation ainsi qu'aux personnes en charge de la mise en service, de l'exploitation et de la maintenance des automates et systèmes. Des connaissances spécifiques en matière de systèmes d'automatisation de sécurité sont nécessaires.

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 être sélectionnés et utilisés dans SILworX.
Italiques	Paramètres et variables du système
`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 clic, le document passe à la destination souhaitée.

Les consignes de sécurité et modes d'emploi sont spécialement mis en exergue.

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 :

- Texte de signalisation : Avertissement, Attention, Remarques
- Nature et source du risque
- Conséquences en cas de non-respect
- Prévention du risque

⚠ TEXTE DE SIGNALISATION

Nature et source du risque !

Conséquences en cas de non-respect

Prévention du risque

Les textes de signalisation ont le sens suivant :

- Avertissement : signifie que toute situation potentiellement dangereuse peut entraîner des blessures graves ou mortelles.
- Attention : signifie que toute situation potentiellement dangereuse peut entraîner des blessures légères.
- Remarque : signifie que toute situation potentiellement dangereuse peut entraîner des dommages matériels.

REMARQUE

Nature et source du dommage !

Prévention du dommage

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 conseils utiles apparaissent sous cette forme :

CONSEIL Le texte contenant les conseils se trouve ici.

2 Consignes d'utilisation des systèmes HIMax

Les informations relatives à la sécurité, les consignes et les instructions fournies dans le présent document doivent être strictement respectées. Utiliser le produit uniquement dans le respect des directives générales et de sécurité.

2.1 Utilisation conforme à l'usage prévu

Ce chapitre décrit les conditions requises pour l'utilisation des systèmes HIMax.

2.1.1 Domaine d'application

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

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

2.1.1.1 Application selon le principe de « Mise hors tension pour déclenchement »

Les automates ont été conçus pour le principe de « Mise hors tension pour déclenchement ».

En cas de défaillances, un système fonctionnant selon le principe de « Mise hors tension pour déclenchement » passe à l'état sans courant ou hors tension (de-energize to trip).

2.1.1.2 Application selon le principe de l'émission de courant

Les commandes HIMax peuvent être utilisées pour des applications fonctionnant selon le principe de l'émission de courant.

Un système, fonctionnant selon le principe de l'émission de courant, active par ex. un actionneur (energize to trip).

Lors de la configuration du système, les exigences émanant des normes d'application sont à respecter, par ex. il se peut qu'un diagnostic des entrées et sorties ou une information en retour de la fonction de sécurité déclenchée soit nécessaire.

2.1.1.3 Utilisation dans le cadre d'un système de détection d'incendie

Tous les systèmes HIMax équipés d'entrées analogiques sont testés et certifiés selon les normes DIN EN 54-2 et NFPA 72.

2.1.2 Conditions d'environnement

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

2.2 Obligations des fabricants de machines et d'installations ainsi que des exploitants

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

La programmation des systèmes HIMax doit recevoir l'aval suffisant des fabricants de machines et d'installations.

2.2.1 Raccordement de partenaires de communication

Seuls des automates présentant une isolation électrique sécurisée peuvent être connectés aux interfaces de communication.

2.2.2 Utilisation de la communication de sécurité

Lors des communications de sécurité entre différents automates, veiller à ce que le temps de réponse complet du système ne dépasse pas le temps de sécurité du processus. Les bases des calculs figurant au chapitre 12 doivent être utilisées.

2.3 Mesures de protection ESD

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

REMARQUE

Les décharges électrostatiques peuvent endommager les composants électroniques installés 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, protéger le module des décharges électrostatiques, en le conservant par ex. dans son emballage.**

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

2.4 Autres documentations du système

La documentation suivante est disponible en outre pour la programmation des systèmes HIMax :

Name	Description	Document nº
HIMax System Manual	Description du matériel du système modulaire	HI 801 375 FR
Certificat	Résultat du test	
Liste de versions	Versions du système d'exploitation certifiées par le TÜV	
Manuels des composants	Description des composants individuels	
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
SILworX Online Help	Manuel d'introduction à SILworX	

Tableau 1 : Vue d'ensemble de la documentation du système

Les documents PDF sont disponibles sur le site Internet `www.hima.com` (à l'exception de l'aide en ligne pour SILworX).

3 Concept de sécurité pour l'utilisation des systèmes PE

Ce chapitre traite des questions générales essentielles en matière de sûreté de fonctionnement des systèmes HIMax :

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

3.1 Sécurité et disponibilité

Les systèmes HIMax n'engendrent aucun danger immédiat.

⚠ AVERTISSEMENT

Risques de dommages corporels liés à un raccordement erroné ou une programmation erronée des systèmes d'automatisation relatifs à la sécurité !

Vérifier les raccordements avant la mise en service et tester l'installation dans son intégralité pour vérifier sa conformité aux exigences de sécurité spécifiées !

HIMA recommande de remplacer aussi rapidement que 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 des valeurs PFD, PFH et SFF

Les calculs des PFD, PFH et SFF pour les systèmes HIMax ont été effectués selon IEC 61508.

Les valeurs PFD, PFH et SFF seront communiquées par HIMA sur demande.

L'intervalle entre essais périodiques est fixé à 10 ans pour les systèmes HIMax (Offline Proof Test, voir IEC 61508-4, paragraphe 3.8.5).

Les fonctions de sécurité, se composant d'une boucle de 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 Autotest et diagnostic d'erreurs

Le système d'exploitation des modules exécute au démarrage et en cours de fonctionnement un grand nombre d'autotests. Ces tests concernent essentiellement :

- 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 tension. Si les tests décèlent dès le démarrage un défaut de module, le module ne se met pas en marche.

Dans un système sans redondance, cela signifie que des fonctions partielles ou l'ensemble du système PE peut être désactivé. Pour un système redondant, le module redondant prend en charge la fonction à exécuter si une erreur est détectée.

Chaque module HIMax dispose de ses propres LED 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 du 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 un dysfonctionnement 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 (HIMax System Manual HI 801 375 FR).

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

Avec le PADT, l'utilisateur établit le programme et configure le contrôleur. Le concept de sécurité du PADT aide l'utilisateur à mettre en œuvre le projet d'automatisation. Le PADT exécute un grand nombre d'opérations destinées à vérifier les informations saisies.

3.1.4 Redondance

Pour augmenter la disponibilité, toutes les parties du système contenant des composants actifs peuvent être configurées de manière redondante et, si nécessaire, remplacées en cours de fonctionnement.

La redondance n'influe pas sur la sécurité. Le SIL 3 est également garanti dans le cas de composants système redondants.

3.1.5 Structure des systèmes de sécurité selon le principe de l'émission de courant

Les systèmes de sécurité opérant selon le principe de l'émission de courant (energize to trip) ont la fonction suivante :

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

3.1.5.1 Détection des composants défaillants

Par le biais d'un diagnostic généré automatiquement, le système de sécurité détecte que des modules sont défectueux.

3.1.5.2 Fonction de sécurité selon le principe de l'émission de courant

L'exécution de la fonction de sécurité consiste en l'activation par le système de sécurité d'un ou plusieurs actionneurs (energize) afin de passer à l'état sécurisé.

La planification suivante relève de l'utilisateur :

- Paramétrer les groupes de redondances pour les modules d'E/S.
- Contrôle de court-circuit et d'interruption de ligne sur les modules d'E/S.
  Ces derniers doivent être paramétrés.
- La fonction des actionneurs peut être contrôlée par la recopie de position.

3.1.5.3 Redondance des composants

Une structure redondante des composants peut être nécessaire, se reporter au manuel du système (HIMax System Manual HI 801 375 FR) :

- Alimentation électrique du contrôleur
- Modules HIMax
- Capteurs et actionneurs

En cas de perte de redondance, le contrôleur doit être réparé dans les plus courts délais.

Il n'est pas nécessaire que les modules du système de sécurité soient redondants si la sécurité requise en cas de défaillance du système de sécurité peut être assurée par d'autres mesures, par exemple de nature organisationnelle.

3.2 Temps importants pour la sécurité

Temps importants pour la sécurité :

- Temps de sécurité du processus
- Temps du chien de garde
- Safety Time
- Temps de réponse

3.2.1 Temps de sécurité du processus

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

Une réaction de sécurité du système PE HIMax, y compris toutes les temporisations des capteurs, actionneurs et modules d'E/S, doit avoir lieu dans la limite du temps de sécurité du processus.

3.2.2 Temps de chien de garde de la ressource

Le temps du chien de garde est réglé dans le menu de réglage des caractéristiques du système PE. 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 ERROR STOP (arrêt pour cause de défaut).

Pour la mesure du temps de chien de garde, tenir compte des influences suivantes :

- Temps nécessaire à l'application, c'est-à-dire la durée d'un cycle du programme de l'application.
- Temps nécessaire à la communication des données de processus
- Temps nécessaire pour la synchronisation des processeurs redondants.
- Temps nécessaire en interne pour l'exécution d'un rechargement.

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

Le réglage par défaut est de 200 ms.

Le temps de chien de garde doit respecter : **Temps de chien de garde ≤ ½ * Temps de sécurité**

3.2.2.1 Évaluation du temps de chien de garde

HIMA recommande vivement, pour obtenir une disponibilité suffisante, les réglages suivants :

2 * temps de chien de garde + max. durée de cycle de processeur + 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 aucune évaluation sûre du temps de cycle maximum du processus n'est possible, régler le temps de chien de garde 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 précise du temps de chien de garde

Pour des applications critiques en termes de temps ou de très grands systèmes, il peut être nécessaire de déterminer le temps de chien de garde précisément.

La détermination précise du temps de chien de garde pour un projet s'effectue à l'aide d'un test sur l'ensemble du système. Tous les modules prévus doivent être connectés. Le système fonctionne en mode RUN 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 rack. 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 pour la synchronisation s'allonge avec le nombre de processeurs déjà synchronisés.

Pour la description du montage et démontage d'un processeur, se reporter aux manuels des processeurs (HIMax X-CPU 01 Manual, HI 801 376 FR et HIMax X-CPU 31 Manual, HI 801 355 E).

4. Dans l'historique de diagnostic du module non synchronisé, lire le temps de synchronisation de n à n+1 processeurs pour chaque processus de synchronisation. Le plus long de ces temps de synchronisation servira à déterminer le temps de chien de garde.
5. Calculer le temps de chien de garde T_{WD} :

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

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

   T_{Res} Réserve de sécurité de 12 ms

   T_{Com} Paramètre système configuré *Max.Com. Time Slice ASYNC [ms].* Utiliser le panneau de contrôle pour déterminer la valeur actuelle. Pour de plus amples détails, se reporter au manuel de communication (Communication Manual HI°801°101°E).

   T_{Config} Paramètre système configuré *Max. Duration of Configuration Connections [ms],* pour de plus amples détails, se reporter au chapitre 10.3.1.2.

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

   T_{Pointe} Pointes de charge observées pour les programmes utilisateurs

► Cela indique une valeur appropriée pour le temps de chien de garde.

CONSEIL Le temps du chien de garde configuré peut être utilisé comme durée maximale de cycle de safe**ethernet**, se reporter au manuel de communication (Communication Manual HI°801°101°E).

3.2.3 Temps de chien de garde du programme utilisateur

Chaque programme utilisateur a son propre chien de garde et son propre temps de chien de garde.

Le temps de chien de garde du programme utilisateur ne s'ajuste pas immédiatement. HIMax calcule le temps du 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 11.2.3 et 11.2.11.

Il faut s'assurer 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 de la ressource

Le temps de sécurité de la ressource est la durée maximale autorisée pendant laquelle la ressource doit réagir à une demande. Les exigences sont :

- Modifications des signaux d'entrée du processus
- Erreur dans la ressource

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

- Aucune temporisation des signaux d'entrée à travers les temporisateurs des modules d'entrée (Ton, Toff)
- Aucune temporisation dans le programme utilisateur
- Le programme utilisateur réagit en un cycle du système PE.

Les influences suivantes allongent le temps de sécurité de la ressource et sont à prendre en compte :

- Les temporisations physiques dans les entrées et sorties, par ex. les temps de commutation du relais
- La temporisation des signaux de sortie à travers la suppression des bruits de sortie, voir chapitre 8.4.2

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

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 11.2.3 et 11.2.11.

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.

3.3 Essai périodique (Proof Test selon IEC 61508)

Un essai périodique est un essai qui a pour but de découvrir les erreurs non détectées dans un système de sécurité, afin que le système puisse, le cas échéant, être ramené dans un état qui lui permet de remplir sa fonction initiale.

Les systèmes de sécurité HIMA doivent être soumis **tous les 10 ans** à un test périodique.

L'analyse des boucles de sécurité réalisées par calcul permet souvent d'étendre l'intervalle.

3.3.1 Exécution du test périodique

L'exécution de l'essai périodique dépend de la configuration de l'installation (EUC = equipment under control) et de son potentiel de mise en danger, ainsi que des normes applicables à l'exploitation de l'installation et que l'organisme de contrôle compétent utilisera pour l'agrément.

Selon les normes IEC 61508 1-7, IEC 61511 1-3, IEC 62061 et VDI/VDE 2180 feuillets 1 à 4, l'exploitant a la responsabilité de veiller à ce que le test périodique pour les systèmes de sécurité soit effectué.

3.3.2 Fréquence des tests périodiques

La commande HIMax peut être soumise à un test périodique en testant l'ensemble du circuit de sécurité.

Dans la pratique, pour les appareils d'entrée et de sortie de terrain un intervalle plus court (par ex. tous les 6 ou 12 mois) sera requis que pour le contrôleur HIMax. Si l'utilisateur teste le circuit de sécurité complet avec l'appareil de terrain, cela inclut automatiquement l'automate HIMax. Il n'est donc pas nécessaire de procéder à des tests périodiques supplémentaires pour l'automate HIMax.

Si le test périodique des appareils de terrain ne comprend pas l'automate HIMax, alors sa conformité aux exigences SIL 3 doit être testée au moins tous les 10 ans. Cela peut être effectué en faisant redémarrer l'automate HIMax.

3.4 Exigences de sécurité

Les exigences de sécurité suivantes s'appliquent pour l'utilisation du système PE relatif à la sécurité du système HIMax :

3.4.1 Étude et conception du matériel

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

Exigences non liées au produit

- Pour une opération de sécurité, seuls le matériel et les composants logiciels de sécurité et homologués pour l'utilisation prévue doivent être utilisés. Le matériel et les logiciels homologués sont spécifiés dans le document *Version List of Devices and Firmware for HIMax Systems from 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 2.1.2).

Exigences liées au produit

- Seuls des dispositifs présentant une isolation sécurisée à la tension d'alimentation, peuvent être connectés au système.
- Les conditions d'application mentionnées dans le Manuel du système, particulièrement celles relatives à la tension d'alimentation, ventilation etc. doivent être respectées.
- Pour l'exécution de tâches de sécurité, utiliser uniquement des modules relatifs à la sécurité.
- Pour l'alimentation électrique, seules des unités de courant répondant aux exigences de tension TBTS ou TBTP peuvent être utilisées. La tension d'alimentation délivrée doit être de ≤ 35 V également en cas de défaillance !

3.4.2 Programmation

Les personnes en charge de l'élaboration des programmes utilisateurs doivent prendre en compte les exigences suivantes en matière de sécurité.

Exigences non liées au produit

- Dans les applications relatives à la sécurité, la configuration exacte des paramètres relatifs à la sécurité du système doit être assurée.
- Cela concerne notamment la configuration du système, la durée de cycle maximale, ainsi que le temps de sécurité.

Exigences applicables à l'utilisation de l'outil de programmation

- SILworX doit être utilisé pour la programmation
- **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.**
- En cas de modification de l'application, tester au moins toutes les parties de la logique qui sont affectées par la modification.
- 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. Exemples :
  - Réponse aux erreurs dans le programme utilisateur
  - Paramétrage de valeurs initiales sûres pour les variables

3.4.3 Communication

- Lors des communications de sécurité entre différents dispositifs, veiller à ce que le temps de réponse complet du système ne dépasse pas le temps de sécurité du processus. Les calculs de base figurant au chapitre 12.2 doivent être utilisés.
- Lors de la transmission de données (importantes pour la sécurité), des règles de sécurité informatiques sont à observer.

  Le transfert des données de sécurité par le biais d'un réseau public (par ex. Internet) est autorisé uniquement avec des mesures de sécurité supplémentaires, par ex. tunnel VPN et pare-feu.
- Si le transfert des données s'effectue par le biais d'un réseau interne à l'entreprise/l'usine, des mesures administratives ou techniques doivent être mises en place pour veiller à assurer une protection suffisante contre les manipulations (par ex. cloisonnement des parties du réseau relatives à la sécurité par rapport aux autres réseaux à l'aide d'un pare-feu).
- Les protocoles par défaut ne doivent pas être utilisés pour la transmission de données de sécurité.
- Seuls des automates présentant une isolation électrique sécurisée peuvent être connectés à toutes les interfaces de communication.

3.4.4 Opérations de maintenance

Les opérations de maintenance relèvent de la responsabilité de l'exploitant. L'exploitant doit mettre en place les mesures appropriées pour garantir la sûreté de fonctionnement pendant les opérations de maintenance.

Si nécessaire, l'exploitant doit déterminer avec le site de réception concerné les mesures administratives pour la protection de l'accès au système.

3.4.5 La cyber-sécurité des systèmes HIMax

Les contrôleurs industriels doivent être protégés contre les sources de problèmes informatiques typiques. Ces sources de problèmes sont :

- Une attaque au sein ou à l'extérieur de l'installation du client
- Erreurs d'utilisation
- Erreurs logicielles

Une installation HIMax se compose des parties suivantes, qui doivent être protégées :

- Système PE HIMax
- PADT
- Serveur OPC : X-OPC DA, X-OPC AE (optionnel)
- Connexions de communication vers des systèmes externes (optionnel)

Le system HIMax satisfait déjà de par ses réglages de base aux exigences de la cyber-sécurité (sécurité informatique). Les modules importants ont été testés par l'entreprise canadienne Wurldtech conformément à l'Achilles Level I.

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 :

- Une modification du programme utilisateur ou de la configuration génère un nouveau CRC de la configuration.
- Les possibilités d'intervention dépendent des droits de l'utilisateur connecté au l'automate.
- L'outil de programmation requiert un mot de passe pour la connexion de l'utilisateur au système PE à l'accès.
- L'accès aux données du système PE n'est possible que si le PADT dispose du projet utilisateur dans la version actuellement exécutée (archivage!).
- Une connexion entre le PADT et le système PE n'est pas nécessaire en mode RUN, elle peut être interrompue.

  Pour des travaux de maintenance ou à des fins de diagnostic, le PADT peut être brièvement connecté.

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

⚠ AVERTISSEMENT

Risque de dommages corporels en cas de manipulation non autorisée du contrôleur !

Protéger le contrôleur contre tout accès non autorisé !

p. ex. :

- **Modification des paramètres par défaut pour le nom d'utilisateur et le mot de passe**
- **Contrôler l'accès physique au contrôleur et au PADT !**

Une planification soigneuse devrait détailler les mesures à prévoir. Après l'analyse de risques, appliquer les mesures nécessaires. Ces mesures sont par exemple :

- Répartition des utilisateurs en groupes cohérents

- Des plans de réseau soignés aident à veiller à ce que les réseaux sécurisés soient durablement isolés des réseaux publics et, le cas échéant, qu'un seul passage existe (par ex. à travers un pare-feu ou une DMZ).
- Utilisation de mots de passe appropriés

Il est conseillé de procéder à une révision régulière (par ex. annuelle) des mesures de sécurité.

La mise en œuvre correcte des mesures nécessaires pour l'installation relève de la responsabilité de l'utilisateur !

Pour de plus amples informations, se reporter au manuel sur la cyber-sécurité de HIMA (HIMA Cyber Security Manual HI 801 373 E).

3.5 Certification

Les automates relatifs à la sécurité de HIMA (système PE, programmable électronique) du système HIMax sont testés sur leur sécurité fonctionnelle selon les normes suivantes, et sont certifiés par TÜV et conformes à CE :

TÜV Rheinland Industrie Service GmbH
Automation, Software und Informationstechnologie
Am Grauen Stein
51105 Cologne
Allemagne

Certificat et rapport de test
Automates relatifs à la sécurité HIMax

Utilisation : « Safety Related Programmable Electronic System for process control, Burner Management (BMS), emergency shut down and machinery, where the demand safe state is the de-energized state.
Applications, where the demand state is the de-energized or energized state.
(Système électronique programmable relatif à la sécurité pour commandes de processus, commandes de brûleur (BMS), systèmes d'arrêt d'urgence et commandes de machines pour lesquels l'état de sécurité est l'état hors tension.
Applications pour lesquelles l'état de sécurité est l'état hors tension ou sous tension.)

Normes internationales :	
EN / IEC 61508, parties 1-7: 2010	SIL 3
EN / IEC 61511, parties 1-3: 2004	SIL 3
EN / ISO 13849-1: 2008 + AC:2009	Performance level e
EN / IEC 62061: 2005 + AC:2010 + A1:2013	SIL CL 3
EN 50156-1: 2004	SIL 3
EN 12067-2: 2004	
EN 298: 2012	
EN 230: 2005	
EN 60079-29-1: 2007	
EN 50495: 2010	
NFPA 85: 2011	
NFPA 86: 2011	
EN / IEC 61131-2: 2007	
IEC 61326-3-1:2008	
EN 54-2: 1997 + AC:1999 + A1:2006	
NFPA 72: 2013	

Le chapitre suivant comprend une liste détaillée de tous les tests environnementaux et de compatibilité électromagnétique réalisés.

Tous les automates portent le marquage de certification CE.

Un PADT, c'est-à-dire un PC équipé du système de programmation **SILworX** sera utilisé pour la programmation des contrôleurs HIMax.

Il aide l'utilisateur à créer des programmes utilisateurs de sécurité avec le langage de programmation des boîtes fonctionnelles (FBD) et de graphe de fonction séquentielle (SFC) selon IEC 61131-3, ainsi pour l'utilisation des automates. Consulter l'aide en ligne de SILworX et le manuel d'introduction de SILworX (SILworX Online Help and SILworX First Steps Manual HI 801 103 E).

3.5.1 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	Description
IEC/EN 61131-2	Programmable controllers, Part 2 Equipment requirements and tests
IEC/EN 61000-6-2	EMC Generic standards, Parts 6-2 Immunity for industrial environments
IEC/EN 61000-6-4	Electromagnetic Compatibility (EMC) Generic standards – Emission standard for industrial environments
EN 298	Automatic burner control systems for burners and appliances burning gaseous or liquid fuels
EN 61326-1	Electrical equipment for measurement, control and laboratory use EMC requirements - Part 1: General requirements
EN 61326-3-1	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications
EN 54-2	Fire alarm systems

Tableau 2 : Normes pour la CEM ainsi que la protection du climat et de l'environnement

Pour une utilisation des systèmes de commande de sécurité HIMax, respecter les conditions générales suivantes :

Nature de la condition	Contenu de la condition
Classe de protection	Classe de protection III selon la norme IEC/EN 61131-2
Pollution	Degré de pollution II selon la norme IEC/EN 61131-2
Altitude	< 2000 m
Boîtier	Par défaut : IP20/IP00 Si les normes d'application (par ex. EN 60204) sont exigées, l'automate doit être monté dans un boîtier avec l'degré de protection requis (par ex. IP54).

Tableau 3 : Conditions générales

3.5.1.1 Conditions climatiques

Le tableau suivant répertorie les valeurs limites et les tests les plus importants relatifs aux conditions climatiques :

Norme	Essais climatiques
IEC/EN 61131-2	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 / -40 °C, 16 h, +85 °C, 1 h Alimentation électrique non raccordée
	Changement de température ; essais de durabilité : Changement de température rapide : -40 °C / +70 °C, alimentation électrique non raccordée
	Essai de résistance Changement de température lent : -10 °C / +70 °C, alimentation électrique raccordée
	Cycles avec chaleur humide ; essais de durabilité : +25 °C / +55 °C, 95 % d'humidité relative, Alimentation électrique non raccordée
EN 54-2	Chaleur humide 93 % d'humidité relative, 40 °C, 4 jours en fonctionnement 93 % d'humidité relative, 40 °C, 21 jours, alimentation électrique non raccordée

Tableau 4 : Conditions climatiques

3.5.1.2 Conditions mécaniques

Le tableau suivant répertorie les principaux tests et valeurs limites relatifs aux conditions mécaniques :

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

Tableau 5 : Essais mécaniques

3.5.1.3 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.

Normes d'essais	Essais d'immunité aux interférences	Critère
IEC/EN 61000-4-2	Essai CEM : contact 6 kV, décharge dans l'air 8 kV	FS
IEC/EN 61000-4-3	Essai RFI (20 V/m) : 80 MHz...1 GHz, 80 % AM Essai RFI (10 V/m) : 1 GHz...2 GHz, 80 % AM Essai RFI (3 V/m) : 2 GHz...3 GHz, 80 % AM	FS FS FS
IEC/EN 61000-4-4	Essai par salve : Tension d'alimentation : 3 kV Lignes de signalisation : 2 kV	 FS FS
IEC/EN 61000-4-5	Tension de choc : CC Tension d'alimentation : 2 kV CM, 1 kV DM Lignes de signalisation : 2 kV CM	 FS FS
IEC/EN 61000-4-6	Haute fréquence, asymétrique : 10 V, 150 kHz...80 MHz, 80 % AM	 FS
IEC/EN 61000-4-16	Lignes d'alimentation et de signalisation 1…10 V, 20 dB/décade (1,5…15 kHz) 10 V, (15...150 kHz) 10 V constant (avec CC, $16^2/_3$ Hz, 50/60 Hz, 150/180 Hz) 100 V brièvement (1 s, avec CC, $16^2/_3$ Hz, 50/60 Hz)	 FS FS FS FS

Tableau 6 : Essais d'immunité aux interférences

IEC/EN 61000-6-4	Essais d'émission d'interférences
EN 55011 Classe A	Émission d'interférences : rayonnées, liées au câblage

Tableau 7 : Essais d'émission d'interférences

3.5.1.4 Tension d'alimentation

Le tableau suivant répertorie les principaux tests et valeurs limites relatifs à l'alimentation électrique des automates :

IEC/EN 61131-2	Vérification des caractéristiques de l'alimentation en courant continu
	La tension d'alimentation doit alternativement répondre aux normes suivantes : IEC/EN 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 (HIMax X-BASE PLATE 01 Manual HI 801 025 E).
	Essai sur la plage de tension : 24 V CC, -20...+25 % (19,2...30,0 V)
	Test d'insensibilité aux interruptions de courte durée de la tension d'alimentation externe : CC, PS 2 : 2 ms
	Inversion de polarité de la tension d'alimentation : Note dans le chapitre correspondant du manuel de système ou dans la fiche technique de la tension d'alimentation.
	Durée tampon, essai de durabilité : Essai B, 1000 h

Tableau 8 : Vérification des caractéristiques de l'alimentation en courant continu

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 processeur.

Consulter les manuels relatifs aux processeurs.

4.1 Tests automatiques

Les principaux tests fonctionnels automatiques pour les processeurs relatifs à la sécurité sont détaillés ci-après :

- Test du processeur
- Test de mémoire
- Test de comparaison
- Test CRC pour les mémoires non volatiles
- Test de chien de garde

4.2 Réponses aux erreurs dans le processeur

Un mécanisme de comparaison dans le processeur vérifie en permanence que les données du système microprocesseur 1 sont identiques à celles du système microprocesseur 2. Si les données ne sont pas identiques ou si les tests fonctionnels dans le processeur trouvent des erreurs, le processeur s'arrête automatiquement pour cause de défaut.

Le contrôleur redémarre (reboot) si une telle erreur se produit pour la première fois. Si pendant la minute suivant le redémarrage, une nouvelle erreur interne se produit, le contrôleur passe à l'état STOP/INVALID CONFIGURATION et reste dans cet état.

Si l'on ne souhaite pas procéder à un redémarrage, régler le paramètre *Autostart* de la ressource sur OFF.

4.3 Remplacement des processeurs

Avant le remplacement de processeurs, il faut s'assurer que cela ne provoque pas l'arrêt d'un système HIMax en cours de fonctionnement

C'est particulièrement valable pour les systèmes qui fonctionnent selon le principe de l'émission de courant. Pour ces systèmes, 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

Interruption possible de l'opération de sécurité !

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

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

La LED **Ess** allumée ou clignotante indique que le processeur est absolument nécessaire pour le fonctionnement du système.

Même si la LED 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 des processeurs, se reporter aux manuels des processeurs (HIMax X-CPU 01 Manual HI 801 376 FR et HIMax X-CPU 31 Manual HI 801 355 E), ainsi qu'au manuel du système (HIMax System Manual HI 801 375 FR).

4.4 Processeur X-CPU 01

Le processeur XCPU 01 peut être utilisé pour être redondant jusqu'à 4 fois. Il peut être inséré dans le rack 0 ou 1 aux emplacements 3...6.

4.5 Processeur X-CPU 31

Le processeur X-CPU 31 réunit les fonctions de processeur et de bus système. Il peut donc être utilisé uniquement sur le rack 0, à l'emplacement 1 ou 2. Dans ce cas, aucun autre processeur ne doit être présent sur le rack 0 ou 1 aux emplacements 3...6 !

5 Module bus système

Un Module bus système gère un des deux bus systèmes sécurisé. Les deux bus systèmes fonctionnent de manière redondante. Chaque bus système relie tous les modules et racks entre eux. Les données sécurisées sont transmises par le biais des bus systèmes au moyen d'un protocole de sécurité.

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

À la place des bus système, des processeurs de type X-CPU 31 peuvent également être utilisés dans le rack 0. Les indications de ce chapitre s'y appliquent également. Les processeurs X-CPU 31 nécessitent un panneau de raccordement spécial double largeur.

5.1 Rack ID

Le rack ID identifie un rack 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 des racks individuels et des modules qui s'y trouvent !

Le rack ID est enregistré dans le panneau de raccordement du bus système.

La procédure de réglage du rack ID est décrite dans le manuel du système (HIMax System Manual HI 801 375 FR) et dans le manuel d'introduction à SILworX (SILworX First Steps Manual 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 ou au processeur X-CPU 31 dans le rack 0, emplacement 1.
- Pour le bus système B :
  - En cas d'utilisation du X-SB 01 et du X-CPU 01, l'attribut est réglable à l'aide de SILworX.

  Le module bus système doté de l'attribut *Responsible* doit se trouver soit dans le rack 0, emplacement 2, soit dans le rack 1, emplacement 2.
  - En cas d'utilisation du X-CPU 31, l'attribut est alloué au module dans le rack 0, emplacement 2.

Assurer-vous que la configuration de l'attribut *Responsible* pour les deux systèmes bus a été correctement réalisée avant de démarrer l'exploitation.

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

⚠ AVERTISSEMENT

Risque de dommages corporels !

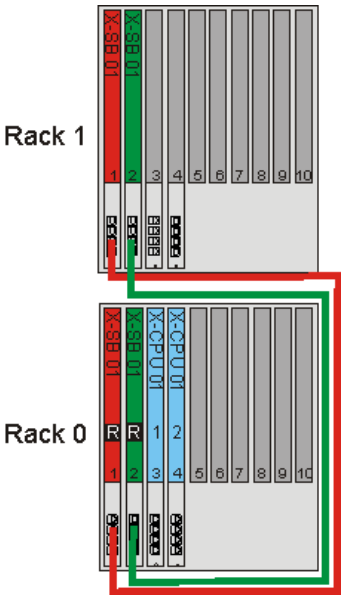
Le paramétrage doit être vérifié à l'aide de SILworX.

Il est impératif de suivre la procédure suivante :

- **Dans SILworX, accéder au module bus système au moyen de l'identifiant du module dans rack 0, emplacement 2**
- **Dans SILworX, accéder au module bus système au moyen de l'identifiant du module dans rack 1, emplacement 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) !**

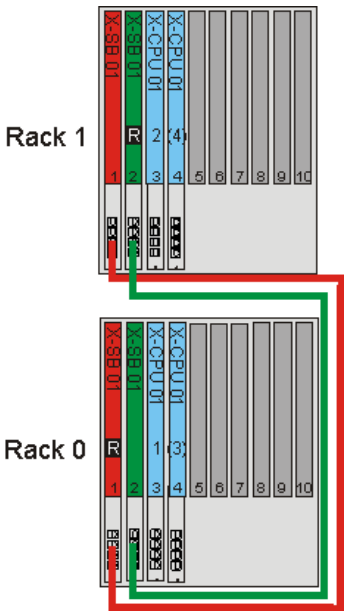
Configurations recommandées :

- Si seul le rack 0 contient des processeurs, les deux modules bus système du rack 0 doivent être dotés de l'attribut *Responsible* (Figure 1).
- Si le rack 1 contient également des processeurs (Figure 2), doter les modules bus système suivants de l'attribut *Responsible* :
  - Dans le rack 0, le module bus système de la douille 1 (automatiquement).
  - Dans le rack 1, le module bus système de l'emplacement 2.



R Le module bus système est responsable

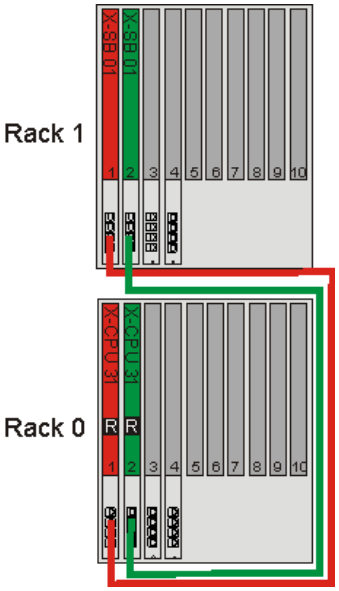
Figure 1 : Configuration recommandée de tous les processeurs sur le rack 0



R Le module bus système est responsable

Figure 2 : Configuration recommandée : processeur X-CPU 01 sur le rack 0 et le rack 1

- En cas d'utilisation de processeurs X-CPU 31 sur le rack 0, emplacements 1 et 2 (Figure 3) les X-CPU 31 sont toujours responsables. Dans ce cas le bus système sur le rack 1, emplacement 2 ne peut pas être responsable !



R Le processeur est responsable

Figure 3 : Configuration avec les processeurs X-CPU 31 sur le rack 0, emplacements 1 et 2

6 Module de communication

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

- Le processeur commande la transmission de sécurité des données par le biais du protocole sécurisé safe**ethernet** certifié SIL 3. Le module de communication transmet les paquets de données aux autres systèmes. Le protocole de sécurité permet d'assurer la détection de messages corrompus (principe du canal noir).

  La communication relative à la sécurité ne peut ainsi pas passer par des canaux de transmission non relatifs à la sécurité, c'est-à-dire des composants de réseau standard.
- Les protocoles standards sont par ex. :
  - Modbus
  - PROFIBUS maître/esclave
  - Send/Receive TCP
  - PROFINET IO
  - SNTP

Pour en savoir plus sur la communication et les modules de communication, se reporter aux documents suivants :

- Chapitre 12.1 du présent manuel
- Manuel du module de communication (HIMax X-COM 01 Manual, HI 801 011 E)
- Manuel de communication (Communication Manual, HI 801 101 E)
- Manuel de système (HIMax System Manual, HI 801 375 FR)

7 Modules d'entrée

Module	Nombre de canaux	Relatif à la sécurité	Canaux sans effet rétroactif	Remarque
Entrées Tout Ou Rien				
X-DI 16 01	16	SIL 3	•	120 VAC
X-DI 32 01	32	SIL 3	•	24 VDC
X-DI 32 02	32	SIL 3	•	Interrupteurs de proximité (NAMUR)
X-DI 32 03	32	SIL 3	•	48 VDC
X-DI 32 04	32	SIL 3	•	Avec saisie des événements
X-DI 32 05	32	SIL 3	•	Interrupteurs de proximité (NAMUR) avec saisie des événements
X-DI 32 51	32	-	•	24 VDC
X-DI 32 52	32	-	•	Interrupteurs de proximité (NAMUR)
X-DI 64 01	64	SIL 3	•	24 VDC
X-DI 64 51	64	-	•	24 VDC
Entrées analogiques				0/4...20 mA
X-AI 16 51	16	SIL 1	•	Thermocouple
X-AI 32 01	32	SIL 3	•	
X-AI 32 02	32	SIL 3	•	Avec saisie des événements
X-AI 32 51	32	-	•	
Entrées du compteur				
X-CI 24 01	24	SIL 3	•	
X-CI 24 51	24	-	•	

Tableau 9 : Aperçu des modules d'entrée

7.1 Généralités

Les entrées de sécurité peuvent être utilisées aussi bien pour des signaux relatifs à la sécurité que pour des signaux non relatifs à la sécurité. Les signaux non relatifs à la sécurité ne peuvent cependant pas être utilisés pour des fonctions de sécurité !

Pendant le fonctionnement, les modules d'entrée relatifs à la sécurité effectuent un test automatique cyclique de grande qualité.

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.

EN plus de l'indication des LEDs de diagnostic sur les modules, les commandes génèrent des messages d'erreur et d'état qui sont enregistrés. Le PADT peut lire ces messages enregistrés dans la mémoire de diagnostic.

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 de 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. Pour obtenir des renseignements pour atteindre le niveau SIL nécessaire pour les capteurs, se reporter par exemple à la norme IEC 61511-1, section 11.4.

7.3 Réaction en cas de défauts

Si les procédures de test détectent un défaut au niveau des entrées, le programme utilisateur traite la valeur initiale des variables globales. Le module active la LED *Error.*

En présence de défauts au niveau de l'ensemble du module d'entrée, le programme utilisateur traite la valeur initiale des variables globales pour toutes les entrées.

Le code de défaut et autres variables de système peuvent être utilisés pour la programmation de réactions aux défauts spécifiques aux utilisateurs. Pour plus de détails, se référer au manuel du module correspondant.

7.4 Entrées Tout ou Rien de sécurité

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

7.4.1 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. Ce test fonctionnel s'effectue chaque fois que des signaux d'entrée sont lus.

7.4.2 Redondance

Il est autorisé de connecter les entrées Tout Ou Rien 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.

7.4.3 Crêtes sur entrées Tout Ou Rien

En raison de la courte durée de cycle des systèmes HIMax, les entrées Tout ou Rien peuvent lire une impulsion de crête selon EN 61000-4-5 comme signal 1 de courte durée.

Si un câble blindé est utilisé pour les entrées Tout Ou Rien, aucune autre mesure n'est nécessaire pour la protection contre les crêtes.

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 de la ressource.

7.5 Entrées analogiques de 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. la *valeur brute*, et en une *valeur de processus* de type REAL. La *valeur brute* contient le signal d'entrée mesuré tandis que la valeur de processus est une valeur mise à l'échelle.

Les entrées de l'interrupteur de proximité génèrent une valeur numérique en comparant la valeur brute avec les valeurs seuils paramétrables.

7.5.1 Procédures de test

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

7.5.2 Redondance

Il est autorisé de connecter les entrées analogiques 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.

7.5.3 État de LL, L, N, H, HH pour X-AI 32 01 et X-AI 32 02

Si, pour une voie d'un module d'entrée X-AI 32 01 ou X-AI 32 02, des événements scalaires sont définis pour les valeurs limites, les variables d'état *-> State LL, -> State L, -> State N, -> State H, -> State HH* doivent être reliées à la variable *Channel OK* **pour assurer des applications relatives à la sécurité ! En cas de défaillance, ces variables d'état fournissent la valeur FALSE.**

7.6 Entrées de compteur de sécurité

Une entrée de compteur de sécurité peut, en fonction de sa configuration, donner les valeurs de processus suivantes :

- Un état de compteur en tant que valeur entière ou en tant que valeur à virgule flottante mise à l'échelle
- Une vitesse ou fréquence en tant que valeur entière ou en tant que valeur à virgule flottante mise à l'échelle
- D'autres valeurs auxiliaires comme le débordement.

Pour de plus amples informations, se reporter au manuel du module (HIMax X-CI 24 01, HI 801 112 E).

7.6.1 Procédures de test

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

7.6.2 À prendre en compte pour le compteur X-CI 24 01 !

En cas d'utilisation du module compteur X-CI 24 01, les particularités suivantes sont à prendre en compte, voir également le manuel du module (HIMax X-CI 24 01_Manual, HI 801 113 E) :

- Pendant le rechargement, des impulsions d'entrée peuvent être perdues lors des 3 premiers cycles si les paramètres suivants ont été modifiés lors du rechargement :
  - Impulsions de compteur d'analyse
  - Paires de canaux utilisées
- Si le capteur d'un canal pour l'exploitation de fronts « 2 Phases, 4 Edges » fait défaut, sans qu'une interruption de ligne ou un court-circuit soient détectés, le module enregistre la moitié de la fréquence effective.
- Les impulsions à compter peuvent être perdues lors du redémarrage automatique.
- Le redémarrage automatique ou manuel du module doit être décidé en fonction de son application.
- Recommandation d'application :
  - l'utilisation de capteurs redondants est recommandée pour l'exploitation multiphase et la reconnaissance du sens de rotation, car c'est le seul moyen de détecter une défaillance de capteur.
  - le paramétrage de la suppression des bruits pour la mesure de fréquence ne pose aucun risque de sécurité.

7.6.3 Redondance

Il est autorisé de connecter les entrées de compteur 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.

7.7 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 de 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. C'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 web de HIMA au format Microsoft® Word®.

8 Modules de sortie

Module	Nombre de canaux	Relatif à la sécurité	À isolation électrique sûre	Remarque
Sorties Tout Ou Rien				
X-DO 12 02	12	SIL 3	-	24 V CC, 2 A
X-DO 24 01	24	SIL 3	-	24 VDC
X-DO 24 02	24	SIL 3	-	48 VDC
X-DO 32 01	32	SIL 3	-	24 VDC
X-DO 32 51	32	-	-	24 VDC
Sorties relais				
X-DO 12 01	12	SIL 3	•	230 VAC
X-DO 12 51	12	-	•	230 VAC
Sorties analogiques				
X-AO 16 01	16	SIL 3	en paires	
X-AO 16 51	16	-	-	

Tableau 10 : Vue d'ensemble des modules de sortie

8.1 Généralités

Les modules de sortie relatifs à la sécurité sont écrits une fois par cycle, les signaux de sortie sont relus et comparés avec les données de sortie fixées.

L'état de sécurité pour les sorties est la valeur « 0 » ou le contact relais ouvert.

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 de sécurité, le système PE ainsi que les actionneurs qui y sont raccordés doivent répondre aux exigences du niveau SIL spécifié. Pour obtenir des renseignements pour atteindre le niveau SIL nécessaire pour les capteurs et les actionneurs, se reporter par exemple à la norme IEC 61511-1, section 11.4.

8.3 Réponse aux erreurs

Si des procédures de test détectent un défaut au niveau des sorties, le contrôleur désactive la sortie correspondante, c.-à-d. active l'état de sécurité. Le module active la LED *Error.*

En présence de défauts au niveau de l'ensemble du module de sortie, toutes les sorties passent à l'état de sécurité.

Le code de défaut et autres variables de système peuvent être utilisés pour la programmation de réactions aux défauts spécifiques aux utilisateurs. Pour plus de détails, se référer au manuel du module correspondant.

8.4 Sorties Tout ou Rien de 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 3. En cas de défaillance, cette mise à l'arrêt de sécurité intégrée désactive les différents canaux du module de sortie défectueux (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.

8.4.1 Procédures de test pour sorties Tout Ou Rien

Les modules sont testés automatiquement pendant le fonctionnement. Les principales fonctions de ces tests sont :

- Relecture du signal de sortie
- Contrôle de la mise à l'arrêt sécurisée redondante
- Test de mise hors tension des sorties
- Surveillance de la tension de service

8.4.2 Output Noise Blanking

Si le Noise Blanking est activé au niveau de la sortie, le module de sortie retarde la coupure de la voie.

Lorsque le Noise Blanking est activé, et qu'une interférence transitoire a été supprimée, un retard au niveau de la réaction *Temps de sécurité – temps de chien de garde* doit être pris en compte.

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

8.4.3 Comportement en cas de court-circuit externe ou de surcharge

En cas de court-circuit de la sortie vers L- ou de surcharge, la sécurité du module est maintenue.

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 actionnées.

8.4.4 Redondance

Il est autorisé de connecter les entrées Tout Ou Rien 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 Sorties relais de 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 3.

En outre, le signal du chien de garde du processeur offre une deuxième possibilité de réaliser une mise à l'arrêt sécurisée : la disparition du signal du chien de garde entraîne le passage immédiat dans l'état de sécurité.

8.5.1 Tests fonctionnels pour sorties relais

Le module est testé automatiquement pendant le fonctionnement. Les principales fonctions de ces tests 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
- Surveillance de la tension de service

8.5.2 Redondance

Il est autorisé de connecter les entrées Tout Ou Rien 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.

8.6 Sorties analogiques de sécurité

Ces sorties transmettent aux actionneurs les valeurs calculées dans le programme utilisateur.

Les sorties analogiques de sécurité lisent leurs valeurs de sortie en retour et les comparent aux valeurs à émettre. Une réponde d'erreur survient en cas d'écart.

8.6.1 Procédures de test pour sorties analogiques

Les modules sont testés automatiquement pendant le fonctionnement. Les principales fonctions de ces tests sont :

- Relecture du signal de sortie.
- Contrôle de la mise à l'arrêt sécurisée redondante.

Si des erreurs surviennent, les sorties passent en valeur de sécurité 0 mA.

8.6.2 Output Noise Blanking

Si le Noise Blanking est activé au niveau de la sortie, le module de sortie retarde la coupure de la voie.

Lorsque le Noise Blanking est activé, et qu'une interférence transitoire a été supprimée, un retard au niveau de la réaction *Temps de sécurité – temps de chien de garde* doit être pris en compte.

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

8.6.3 Comportement en cas de rupture de ligne externe

En cas de rupture de ligne, le module coupe l'alimentation pendant env. 8 ms et vérifie si la rupture de ligne est toujours présente. Dans ce cas, il coupe l'alimentation pour env. 10 s. Ce scénario peut se répéter aussi souvent que nécessaire.

8.6.4 À prendre en compte pour le module de sortie analogique X-AO 16 01 !

En cas d'utilisation du module de sortie analogique, tenir compte impérativement des particularités suivantes, et se reporter également au manuel du module (HIMax X-AO 16 01 Manual HI 801 111 E)

- Seules les connexions figurant dans le manuel du module (HIMax X-AO 16 01 HI 801 111 E) sont autorisées !
- En cas de redondance en série de plus de deux modules, la tension TBTS peut être dépassée !
- En cas de redondance en série, n'utiliser qu'un seul canal dans chaque groupe de deux canaux !
- Si une communication HART a lieu entre l'actionneur raccordé et un terminal HART, elle peut fausser le signal de sortie de jusqu'à 1 % de la valeur finale !
- En cas d'erreur, le temps nécessaire pour atteindre l'état de sécurité peut s'élever à 16 ms dans le pire des cas. Prendre ce temps en compte pour le temps de réaction et le temps de sécurité !
- Le programme utilisateur ne peut pas écrire aux sorties analogiques sur des cycles plus courts que 6 ms.
- En cas d'erreur, le module émet la valeur sûre 0 mA, ainsi que pour le dépassement de la limite supérieure de la plage de réglage.

8.6.5 Redondance

Il est autorisé de connecter les sorties analogiques 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.

8.7 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 de 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. C'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 web de HIMA au format Microsoft® Word®.

9 Modules d'E/S spéciaux

9.1 Module HART X-HART 32 01

Le module HART sert à communiquer avec les capteurs et actionneurs HART.

Pour de plus amples détails, se reporter au manuel du module (HIMax X-HART 32 01 HI 801 307 E).

9.1.1 Fonction de sécurité

La fonction de sécurité du module X-HART comprend les points suivants :

- Désactivation du protocole HART : en état hors tension les canaux HART sont désactivés de façon sûre conformément au niveau SIL 3.
- Filtrage HART : les accès au transmetteur ou aux capteurs HART sont bloqués conformément au niveau SIL 3.
- La communication HART influence la précision de mesure analogique d'env. 1 %.

  Il n'y a pas d'autre répercussion sur les modules analogiques.
- Si le filtrage HART est désactivé sur le module HART, il est possible de reprogrammer les capteurs ou actionneurs analogiques associés. Cela peut compromettre la sécurité.

9.2 Module de protection contre la survitesse X-MIO 7/6 01

Le module à surveiller la vitesse et à déclencher la mise hors tension d'arrêt d'urgence (function trip) d'une turbine. Pour de plus amples détails, se reporter au manuel du module (HIMax X-MIO 7/6 01 Manual HI 801 305 E).

Ce module permet de réaliser des applications conformément à la norme API 670. Le module satisfait aux exigences mentionnées dans la norme API 670 pour la surveillance de la vitesse et les modalités d'arrêt pour les turbines. La surveillance de la vitesse et les modalités d'arrêt de fonctionnent indépendamment du système d'ensemble HIMax et du programme utilisateur.

9.2.1 Fonction de sécurité

Le module surveille la vitesse d'une turbine indépendamment du système d'ensemble HIMax et du programme utilisateur. Le module exécute de façon autonome la mise hors tension de la turbine et des sorties Tout Ou Rien.

Selon l'entrée de mesure le module enregistre la vitesse et le sens de rotation d'un capteur avec une précision conforme à la sécurité. Trois capteurs par turbine sont prévus pour la détermination de la vitesse. Le module effectue une évaluation 2oo3 des valeurs de vitesse transmises par les trois capteurs. Le résultat est à la disposition du processeur relatif à la sécurité du X-MIO 7/6 01 et du programme utilisateur.

En cas de défaillance d'un signal de capteur, le module émet un avertissement. En cas de défaillance de deux des trois signaux, la fonction d'arrêt d'urgence se déclenche.

Le module comprend des sorties Tout Ou Rien de sécurité comme décrit dans le chapitre 8.3.

La fonction de sécurité de toutes les entrées et sorties est exécutée conformément à SIL 3. La sortie de relais est un contact de signalisation exempt de potentiel (à deux directions) non relatif à la sécurité.

9.2.2 Redondance

Pour une plus grande disponibilité, configurer le module de manière redondante. Des panneaux de raccordement doubles sont disponibles à cet effet.

10 Logiciel

Le logiciel pour les automates de 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 du contrôleur. Il est conseillé d'utiliser la dernière version valide pour les applications de sécurité. Ce 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.

10.1 Aspects relatifs à la sécurité pour le système d'exploitation

Chaque système d'exploitation homologué est clairement identifié par le numéro de révision et la signature CRC. Toutes les versions du système d'exploitation homologuées par le TÜV pour les automates de 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.*

Le système de programmation SILworX permet de lire la version actuelle du système d'exploitation. Vérifier si une version autorisée du système d'exploitation est chargée dans le module (cf. 11.3).

10.2 Aspects relatifs à la sécurité pour la programmation

Pour la création d'un programme utilisateur, prendre en compte les exigences mentionnées ici.

10.2.1 Concept de sécurité de SILworX

Le concept de sécurité de SILworX:

- Lorsque SILworX est installé, un control par Checksum CRC permet de garantir l'intégrité sur l'ensemble des programmes lors de la transmission entre le fabriquant et l'utilisateur.
- SILworX mène des contrôles de plausibilité afin de réduire les erreurs de saisie.

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

- Vérification de la correcte application de la fonction de commande à l'appui des données et flux des signaux.
- Test fonctionnel complet de la logique au moyen d'essais (voir chapitre 10.2.2).

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 changements ont été effectués par rapport à la version antérieure.

À chaque mise en service du contrôleur de sécurité, respecter les exigences des normes d'application en matière de vérification et validation !

10.2.2 Vérification de la configuration et du programme utilisateur

Pour vérifier si le programme utilisateur respecte 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 de chaque boucle (composé de l'entrée, des interconnexions dans l'application et de la sortie) est suffisant.

Des tests élémentaires 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 tests élémentaires doivent être choisis de telle sorte que l'exactitude du calcul peut être attestée. Le nombre nécessaire de tests élémentaires 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.

SILworX peut servir comme aide au contrôle :

- Contrôle des entrées
- Forçage des sorties

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

10.3 Paramètres de la ressource

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

⚠ AVERTISSEMENT

Risque de dommages corporels lié à une configuration défectueuse !

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

Ces paramètres sont

- **Rack ID, voir 5.1 et le manuel du système (HIMax System Manual HI 801 375 FR).**
- **Attribut Responsible des modules bus système ou processeur, voir 5.2**
- **Les paramètres mis en valeur dans le Tableau 11**

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.

10.3.1 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	Paramétrage pour un fonctionnement sécurisé
Name	Nom de la ressource		À convenance
System ID [SRS] [1)]	ID du système 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 susceptibles d'être reliées entre elles.
Safety Time [ms] [1)]	Temps de sécurité en millisecondes 20...22 500 ms (modifiable en ligne)	600 ms	Spécifique à l'application
Watchdog Time [ms] [1)]	Temps du 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 (Target Cycle Time) 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. Voir chapitre 10.3.1.1 (modifiable en ligne)	0 ms	Spécifique à l'application
Target Cycle Time Mode	Utilisation de *Target Cycle Time [ms]* (modifiable en ligne) voir chapitre 10.3.1.1.	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 de haute priorité, le temps d'exécution en surplus de programmes utilisateurs de 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 (Communication Manual HI 801 101 E), 2...5 000 ms	60 ms	Spécifique à l'application
Max. Duration of Configuration Connections [ms]	Il définit la durée disponible dans un cycle de processeur pour les connexions de configuration de processus, 2...3500. Voir chapitre 10.3.1.2.	12 ms	Spécifique à l'application

Paramètre	Description	Valeur par défaut	Paramétrage pour un fonctionnement sécurisé
Maximum System Bus Latency [µs]	Temporisation maximale d'un message entre un module d'E/S et de processeur. 0, 100...50 000 µs	0 µs	Spécifique à l'application
	i Une licence est nécessaire pour régler la latence maximale du bus système sur une valeur > 0.		
Allow Online Settings [1]	ON : **Tous** les paramètres/commutateurs cités sous OFF sont modifiables en ligne au moyen du PADT. Cela vaut uniquement si la variable système *Read-only in RUN* a la valeur OFF.	ON	OFF, recommandé
	OFF : Les paramètres suivants **ne sont pas** modifiables en ligne : ▪ *System ID* ▪ *Autostart* ▪ *Global Forcing Allowed* ▪ *Global Force Timeout Reaction* ▪ *Load Allowed* ▪ *Reload Allowed* ▪ *Start Allowed* — Les paramètres suivants sont modifiables en ligne si *Reload Allowed* est 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* peut être fixé sur ON si le système PE est à l'arrêt et par rechargement.		
Autostart [1]	ON : Si le processeur est raccordé à la tension d'alimentation, le programme utilisateur démarre automatiquement.	OFF	Spécifique à l'application
	OFF : Pas de démarrage automatique après connexion de la tension d'alimentation.		
Start Allowed [1]	ON : Démarrage à froid ou à chaud autorisé par PADT à l'état RUN ou STOP.	ON	Spécifique à l'application
	OFF : Démarrage non autorisé.		
Load Allowed [1]	ON : Téléchargement de la configuration autorisé.	ON	Spécifique à l'application
	OFF : Téléchargement de la configuration non autorisé.		
Reload Allowed [1]	ON : Rechargement de la configuration autorisé.	ON	Spécifique à l'application
	OFF : Rechargement de la configuration non autorisé. Un processus de rechargement en cours n'est pas interrompu en cas de commutation sur OFF.		
Global Forcing Allowed [1]	ON : Forçage général autorisé pour cette ressource.	ON	Spécifique à l'application
	OFF : Forçage général non autorisé pour cette ressource.		

Paramètre	Description		Valeur par défaut	Paramétrage pour un fonctionnement sécurisé
Global Force Timeout Reaction	Détermine le comportement de la ressource en cas d'expiration de la temporisation de forçage général : ▪ Stop Forcing ▪ Stop Resource		Stop Forcing	Spécifique à l'application
Minimum Configuration Version	Avec ce réglage, il est possible de générer un code compatible avec des versions trop anciennes ou trop récentes du système d'exploitation HIMax en fonction des exigences du projet. Voir chapitre 0.		SILworX V7 pour de nouveaux projets	Spécifique à l'application
	SILworX V2	La compilation du programme s'effectue comme avec SILworX V2 pour HIMax avec versions antérieures à V3.		
	SILworX V3	La compilation du programme s'effectue comme avec SILworX V3 pour HIMax avec versions antérieures à V3.		
	SILworX V4	La compilation du programme s'effectue comme avec SILworX V4 pour HIMax avec versions antérieures à V4.		
	SILworX V5	La compilation du programme s'effectue comme avec SILworX V5 pour HIMax avec versions antérieures à V5.		
	SILworX V6	La compilation du programme s'effectue comme avec SILworX V6.48 pour HIMax V6.		
	SILworX V6b	La compilation du programme s'effectue comme avec SILworX V6.114 pour HIMax V6.		
	SILworX V7	La compilation du programme s'effectue comme avec SILworX V7 pour HIMax avec versions antérieures à V7.		
Fast Start-Up	Non applicable pour HIMax		OFF	OFF
[1] **Les paramètres de sécurité** sont en caractères gras.				

Tableau 11 : Les paramètres système de la ressource

10.3.1.1 Utilisation des paramètres *Target Cycle Time* et *Target Cycle Mode*

Ces paramètres peuvent être utilisés pour maintenir le temps de cycle de façon aussi constante que possible sur la valeur *Target Cycle Time [ms].* Ce paramètre doit pour ce faire être réglé sur une valeur > 0. Dans ce cas, HIMax limite les activités de rechargement et de synchronisation des modules redondants de façon à respecter le temps de cycle maximal.

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		Prolongation au maximum tous les cinq cycles lors du rechargement. Prolongation d'un seul cycle lors de la synchronisation.
Dynamic-tolerant	HIMax exécute le cycle dans un temps aussi court que possible.	Prolongation au maximum tous les cinq cycles lors du rechargement. Prolongation d'un seul cycle lors de la synchronisation.
Dynamic		Exécution du rechargement ou synchronisation uniquement si la durée du cycle Target Cycle Time est suffisante

Tableau 12 : Effet du paramètre *Target Cycle Time Mode*

10.3.1.2 Calcul de *Max. Duration of Configuration Connections [ms]*

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

La communication 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 processeur peut dépasser la valeur par défaut.

Pour le firmware HIMax-CPU V4 ou supérieur, régler la durée maximale des connexions de configuration de façon à respecter le temps de chien de garde fixé.

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*.

La quantité des données de configuration 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 réglage peut se calculer comme suit :

Pour X-CPU 01 : $T_{Config} = (n_{Com} + n_{RIO} + n_{PADT}) * 0{,}25\ ms + 2\ ms + 4*T_{Latence}/1000$

Pour X-CPU 31 : $T_{Config} = n_{Com} + n_{RIO} * 0{,}25\ ms + n_{PADT} + 2\ ms + 4*T_{Latence}/1000$

Les paramètres signifient :

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
$T_{Latence}$	Le paramètre système *Maximum System Bus Latency [µs]* est à diviser par 1 000 pour le convertir en ms

Si le temps calculé est inférieur à 6 ms, l'arrondir à 6 ms. Le temps calculé peut être corrigé ultérieurement d'après les statistiques en ligne ou dans les propriétés de la ressource, ou modifié directement en ligne.

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 Connexions* est inférieure au résultat de la formule ci-dessus.

i Si la *Max. Duration of Configuration Connections* est réglée à une valeur trop basse, la communication entre le PADT et le système PE est très lente et une défaillance totale peut survenir !

10.3.1.3 Remarques concernant le paramètre *Minimum Configuration Version* :

- En cas de création d'un nouveau projet, la version sélectionnée est toujours la plus récente *Minimum Configuration Version*. Vérifier si ce réglage est compatible avec la version de système d'exploitation utilisée.
- Dans le cas d'un projet converti à partir d'une version antérieure de SILworX, la valeur paramètre de la version antérieure est conservée pour *Minimum Configuration Version*. Cela garantit que le CRC de configuration résultant de la génération de code est le même que celui de la version antérieure et que la configuration déterminée reste compatible avec le système d'exploitation du module.

  Pour cette raison, il est recommandé de ne modifier la *Minimum Configuration Version* de projets convertis qu'en lien avec d'autres modifications au niveau de la ressource concernée.
- SILworX génère automatiquement une *Minimum Configuration Version* si, dans le projet, des utilités sont exploitées ne mettant à disposition qu'une version de configuration supérieure. SILworX, l'affiche dans les résultats de la génération de code. Les modules refusent le chargement de versions de configuration supérieures non compatibles avec leurs systèmes d'exploitation.

  Pour remédier à ce type d'incompatibilités, il peut s'avérer utile de faire un rapprochement entre les informations fournies par le comparateur de version et la vue d'ensemble des caractéristiques du module.
- Pour l'utilisation de processeurs X-CPU 31, régler *Minimum Configuration Version* sur *SILworX V6* ou supérieure.

10.3.1.4 Variables du système du rack

Ces variables servent à modifier le comportement du contrôleur pendant le fonctionnement en fonction de certains états.

Paramètre / commutateur	Fonction	Paramètres par défaut	Paramétrage pour un fonctionnement sécurisé
Force Deactivation	Permet d'éviter le forçage et son arrêt immédiat	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 le contrôleur en cas de défauts détectés par le programme utilisateur	OFF	Spécifique à l'application
Read-only in RUN	Après le démarrage du contrôleur 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 13 : Variables système du rack

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

10.3.1.5 Exemple : ouverture et fermeture 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 le contrôleur.

Les trois variables système *Read only in Run*, *Reload Deactivation* et *Force Deactivation* sont utilisées pour le verrouillage, voir Tableau 13.

Si les trois variables de système sont sur ON, il n'est plus possible d'intervenir sur le contrôleur. Dans ce cas, le contrôleur ne peut être remise à l'état STOP qu'en redémarrant le processeur avec mode commutateur en position *Init*. Le rechargement d'un programme utilisateur est ensuite possible. L'exemple décrit le cas simple d'une clé permettant de verrouiller ou d'autoriser tous les accès au système PE.

Rendre l'automate 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 Tout Ou Rien.
4. Raccorder un interrupteur à clé à une entrée Tout Ou Rien.
5. Compiler le programme, le charger sur le contrôleur et le démarrer.

► Le détenteur de la clé adéquate peut ouvrir et fermer le contrôleur. En cas de défaut dans le module d'entrée Tout Ou Rien correspondant, le contrôleur est ouvert.

L'utilisation de plusieurs variables globales, d'entrées Tout Ou Rien et de commutateurs à clé permet de modifier cet exemple simple de telle sorte que les habilitations de forçage, de rechargement et les fonctions Arrêt + Démarrage + Téléchargement sont réparties entre diverses clés/personnes.

10.4 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 le temps de cycle. Cela peut provoquer un dépassement du temps de chien de garde.**

Le forçage n'est autorisé qu'après concertation avec l'organisme de contrôle compétent et responsable des tests d'acceptation de l'installation.

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 (HIMax System Manual HI 801 375 FR).

10.4.1 Forçage des sources de données

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

- Entrées physiques
- Protocoles de communication
- Variables de système

La séquence suivante mène au forçage involontaire d'une variable :

1. Une variable globale A est allouée à une des sources de données forcées et est de ce fait, elle aussi, forcée. La source de données est ainsi réellement forcée !
2. L'allocation est annulée. La source de données maintient la caractéristique *forcée*.
3. La source de données est allouée à une autre variable globale B.
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 *forcée (Forced)* en cas de modification de l'allocation.

10.5 Comparateur de versions sécurisé

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

- Configuration de ressource chargée dans le contrôleur
- Configuration de ressource présente dans le PADT
- Configuration de ressource exportée (archivée)

Le résultat de la comparaison atteint le niveau SIL 3, car il est généré à partir des fichiers chargeables y compris du CRC.

Utiliser le comparateur de versions sécurisées pour vérifier les modifications de programme avant le chargement sur le contrôleur.

Il détermine avec précision quelles parties de la configuration de la ressource sont modifiées. Cela facilite la vérification des modifications et la détermination des données de test.

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

11 Programme utilisateur

Ce chapitre traite des aspects relatifs à la sécurité pour le programme utilisateur.

11.1 Procédure générale

Procédure générale de programmation des automates HIMax pour des applications de sécurité :

1. Spécifications des fonctionnalités du contrôleur.
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 puis l'automate peut assurer la sûreté de fonctionnement.

11.2 Cadre d'une utilisation 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 3.4.

Saisir le programme utilisateur à l'aide de l'outil de programmation SILworX. Le système d'exploitation validé pour ordinateur personnel est disponible dans la documentation de validation pour la version à utiliser de SILworX.

L'outil de programmation SILworX se compose essentiellement des fonctions suivantes :

- Saisie (éditeur de programme, éditeur de texte structuré), surveillance et documentation
- Variables globales avec noms symboliques et types de données (BOOL, UINT, etc.)
- Assignation des commandes du système HIMax (Hardware Editor)
- Traduction du programme utilisateur sous une forme qui peut être chargée sur l'automate
- Configuration de la communication

11.2.1 Base de la programmation

Les fonctions 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 combinaison des fonctions et modules de fonctions
  - Blocs fonctionnels avec caractéristiques spécifiées
- Commandes séquentielles (système de contrôle séquentiel)
  - Description écrite des étapes incluant leurs conditions de progression et les actionneurs à contrôler
  - Plans séquentiels
  - Forme matricielle ou tabulaire des conditions de progression et des actionneurs 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 capteurs et actionneurs :

- Capteurs (Tout Ou Rien ou analogiques)
  - Signal en exploitation normale (principe de courant de repos pour les capteurs Tout Ou Rien, valeur de repli pour les capteurs analogiques)
  - Signal en cas d'erreur
  - Détermination des redondances requises et relatives à la sécurité (1oo2, 2oo3)
  - Contrôle des incohérences et réponse
- *Actionneurs*
  - Position et amorçage du contrôleur en exploitation normale
  - Réponse/position sécurisée en cas de coupure ou de panne de courant

Objectifs de la programmation du programme utilisateur

- Compréhension aisée.
- Suivi aisé.
- Tests aisés.
- Modifications aisées.

11.2.2 Fonctions du programme utilisateur

Le matériel ne suppose aucune restriction pour la programmation. Les fonctions du programme utilisateur sont librement programmables.

Lors de la programmation, le principe de « Mise hors tension pour déclenchement » 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 en règle générale selon le principe de « Mise hors tension pour déclenchement », c.-à-d. que leur état de sécurité est « 0 ».
- Le programme utilisateur peut être constitué de fonctions logiques et/ou arithmétiques, sans prendre en considération le principe de « Mise hors tension pour déclenchement » 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.
- Afin de simplifier la logique, les entrées et sorties de tous les blocs fonctionnels et variables peuvent être inversées au choix.
- Les signaux d'erreur d'entrées et sorties ou de blocs logiques doivent être évalués par le programmateur.

HIMA recommande d'encapsuler des fonctions dans des blocs spécifiques créés par l'utilisateur ainsi que des fonctions basées sur des fonctions standards. 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 petite taille à un module plus grand et à un programme utilisateur, l'utilisateur crée une fonction complète et complexe.

11.2.3 Paramètres système du programme utilisateur

Les paramètres du programme contenus dans le tableau ci-dessous peuvent être configurés via la boite de dialogue *Properties* du programme utilisateur:

Paramètre	Fonction	Valeur par défaut	Réglage pour fonctionnement sécurisé
Name	Nom du programme utilisateur		À convenance
Program ID	ID pour Identifiant SILworX du programme, 0…4 294 967 295. Si le paramètre *(Generation Compatibility)* est configuré pour la version 2 de SILworX *(SILworX V2)*, seule la valeur "1" est permise.	0	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 du processeur pour un programme utilisateur: 1...4 294 967 295 µs. Réglage sur 0 : sans limitation.	0 µs	Spécifique à l'application
Watchdog Time [ms] (calculated)	Temps de surveillance du programme utilisateur calculé à partir de nombre maximal de cycles et du temps de chien de garde de la ressource Non modifiable !		
Classification	Classement du programme utilisateur : sécurité positive ou standard (uniquement pour documentation).	Safety-related	Spécifique à l'application
Allow Online Settings	Autorise le changement des paramètres pendant le fonctionnement (mode en ligne) N'est effectif que si *Allow Online Settings* de la ressource est sur ON !	ON	-
Autostart	Valide le démarrage automatique: démarrage à froid, démarrage à chaud, off.	Cold Start	Spécifique à l'application
Start Allowed	ON : Le PADT peut être utilisé pour démarrer le programme utilisateur. OFF : Le PADT ne peut pas démarrer le programme utilisateur.	ON	Spécifique à l'application
Test Mode Allowed	ON Mode test autorisé pour le programme utilisateur. OFF Mode test non autorisé pour le programme utilisateur.	OFF	Spécifique à l'application[1)]
Reload Allowed	ON : Le rechargement en ligne du programme utilisateur est autorisé. OFF : Le rechargement en ligne du programme utilisateur n'est pas autorisé.	ON	Spécifique à l'application
Local Forcing Allowed	ON : Forçage autorisé au niveau de programme. OFF : Forçage non autorisé au niveau de programme.	OFF	OFF, recommandé
Local Force Timeout Reaction	Comportement du programme utilisateur après expiration du temps de forçage : ▪ Arrêt du forçage seulement. ▪ Arrêt du programme.	Stop Forcing Only	-

Code Generation Compatibility	Le programme compilé est compatible avec les versions antérieures de SILworX		*SILworX V5* pour de nouveaux projets	Spécifique à l'application
	SILworX V7 et postérieure	Le programme compilé est compatible avec SILworX V7.		
	SILworX V4 – V6b	Le fonctionnement de la génération de code est compatible avec SILworX V4 jusqu'à SILworX V6b.		
	SILworX V3	Le fonctionnement de la génération de code est compatible avec SILworX V3.		
	SILworX V2	Le fonctionnement de 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 afin d'assurer une reprise de fonctionnement sécurisé !				

Tableau 14 : Paramètres système du programme utilisateur

Remarques concernant le paramètre *Code Generation Compatibility* :

- Dans un nouveau projet, SILworX sélectionne la valeur la plus récente pour le paramètre *Code Generation Compatibility*. Cela permet d'activer les paramètres actuels optimisés et d'assurer la prise en charge des versions les plus récentes des modules et de leur système d'exploitation. Vérifier si ce réglage est compatible avec le matériel utilisé.
- Dans le cas d'un projet converti à partir d'une version antérieure de SILworX, la valeur du paramètre *Code Generation Compatibility* est conservée. Cela garantit que le CRC lié à la configuration ne change pas durant la compilation et que la configuration générée est compatible avec le système d'exploitation des modules.

  C'est pourquoi il est recommandé de ne pas modifier le paramètre *Code Generation Compatibility* des projets convertis.
- Si le paramètre de la ressource *Minimum Configuration Version* est configuré en *SILworX V4* (voir ci-dessus), le paramètre *Code Generation Compatibility* des programmes utilisateur doit être configuré sur *SILworX V4*.

11.2.4 Génération de codes

La génération du code intègre le programme utilisateur ainsi que l'assignation des Entrées/Sorties. Lors de ces étapes, le CRC de la configuration, représentant le checksum/CRC des différents fichiers de configuration, est créé.

Celui-ci est codé sur 32 bits en Hexadécimal et représente la signature numérique du programme utilisateur. Tous les éléments configurables ou modifiables comme la logique, les variables et les paramètres de configuration y sont intégrés.

Avant le chargement dans l'automate de sécurité et le démarrage de l'installation, le programme utilisateur doit être impérativement compilé deux fois. Les deux versions générées doivent présenter les mêmes CRC.

Si l'option *CRC Comparison* est sélectionnée, SILworX génère automatiquement cette double compilation de la ressource puis effectue la comparaison entre les CRC. Cette option est pré-configurée.

Le résultat de la comparaison CRC est disponible dans le journal du registre (menu «View > Logbook»).

La double compilation du système ainsi que la comparaison des CRCs assurent la détection de défaillances temporaires au niveau du matériel ou du système d'exploitation du PC utilisé.

11.2.5 Chargement et démarrage du programme utilisateur

Le chargement du programme utilisateur dans l'automate de sécurité HIMax ne peut se faire que dans l'état STOP.

Le chargement comprend l'ensemble des programmes utilisateur ainsi que les configurations liées à la ressource (automate de sécurité). Le système surveille que le chargement de la configuration de la ressource s'est déroulé correctement. Ensuite, le programme utilisateur peut démarrer c.-à-d. que le traitement cyclique des tâches commence.

i Le PADT ne peut agir sur la ressource, par ex. procéder à un rechargement et à un forçage, que si le projet chargé sur la ressource est ouvert dans SILworX. Si le projet n'est pas dans SILworX, seul STOP de la ressource est possible !

HIMA recommande de sauvegarder le projet sur un support externe après chaque chargement du programme utilisateur. Ceci s'applique également dans le cadre d'un rechargement (ressource en mode RUN).

Cela permet de garantir que le projet correspondant à la configuration chargées dans l'automate reste accessible, y compris en cas de défaillance du PADT.

HIMA recommande également de faire une sauvegarde régulière du projet, indépendamment des chargements du programme.

11.2.6 Rechargement

Si des modifications ont été effectuées sur le programme utilisateur, celles-ci peuvent être transférer sur la ressource pendant fonctionnement. Après vérification par le système, le programme utilisateur modifié est activé et prend en charge les nouvelles opérations.

i **Lors du rechargement des fonctions séquentielles, prendre en compte les aspects suivants :**

Les informations de rechargement des fonctions séquentielles ne tiennent pas compte de l'état actuel de la fonction. En conséquence, il est possible, par rechargement d'une modification de la fonction, de la mettre involontairement dans un état indéfini. L'utilisateur en assume alors la responsabilité.

Exemples :

- Suppression de l'étape active. Après cela aucune étape de la fonction séquentielle n'a l'état *Active.*
- Renommer l'étape initiale, pendant qu'une autre étape est active.
  Cela occasionne une fonction séquentielle à deux étapes actives !

i **Lors du rechargement des actions, prendre en compte les aspects suivants :**

Lors du rechargement, les actions sont chargées avec leurs données correspondantes. Toute conséquence potentielle doit être soigneusement prise en compte.

Exemples :

- Si un bloc de temporisation est supprimé à cause du rechargement, le temps restant expire immédiatement. La sortie *Q* peut, de ce fait, en fonction des paramètres utilisés, passer à TRUE.
- Si un bloc de temporisation est supprimé pour un élément défini (par ex. *S*), cet élément reste défini.
- La suppression d'un élément *P0*, ayant pour état la valeur TRUE, active le déclenchement de la fonction.

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 d'erreur et l'automate continu de fonctionner avec la configuration de la ressource précédente.

L'automate peut interrompre un rechargement

Afin d'assurer la fonction de rechargement, il faut prévoir une réserve de temps suffisante lors de la configuration du temps de chien de garde, ou augmenter provisoirement celui-ci via la configuration des paramètres de sécurité en mode en ligne.

L'augmentation provisoire du temps de chien de garde doit être approuvée par l'organisme de contrôle compétent.

Un dépassement du temps de cycle peut également provoquer l'interruption d'un rechargement.

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

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

- Variation du temps de cycle du programme utilisateur
- Sollicitations soudaines et importantes du cycle, par ex. dues 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.

11.2.7 Test en ligne

Les champs de test en ligne (OLT Fields) peuvent être utilisés pour afficher la valeur des variables pendant l'exploitation.

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 (SILworX First Steps Manual, HI 801 103 E).

11.2.8 Mode test

Pour diagnostiquer les défauts en mode test, 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. Pendant l'intervalle entre deux cycles, les variables globales affichées par ce programme utilisateur sont « gelées ». Les sorties physiques et données de communication attribuées ne réagissent ainsi plus aux modifications du processus !

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

État	Signifié
OFF	Le mode test est désactivé (réglage par défaut).
ON	Le mode test est activé.

Tableau 15 : Paramètre programme utilisateur **Test Mode Allowedat**

REMARQUE

Ce mode peut engendrer des problèmes de sécurité !

Si le programme utilisateur est maintenu en mode test, il ne peut plus piloter ses sorties en fonction de ses entrées! Les valeurs de sorties ne sont pas modifiables, l'automate ne peut donc plus assurer ses fonctions de sécurité.

C'est pourquoi ce mode n'est pas autorisé pendant l'exploitation des installations!

Le paramètre Test Mode Allowed **doit être réglé sur OFF!**

11.2.9 Modification des paramètres système pendant exploitation

Il est possible de modifier les paramètres système du Tableau 16 pendant l'exploitation (online). Un cas d'application classique est l'augmentation provisoire du temps de chien de garde pour permettre un rechargement.

Avant de modifier les paramètres système en mode en ligne, il faut s'assurer que le changement de configuration ne générera pas un état dangereux pour l'installation. Au besoin, prendre des mesures techniques et/ou organisationnelles afin d'écarter tout risque de dommage. Observer les normes en vigueur !

La configuration du temps de sécurité et du hien de garde dans le programme utilisateur doit être en cohérence avec les spécifications de l'application et son temps de cycle réel. Le système PE ne peut vérifier ces valeurs !

L'automate empêche de configurer un temps de chien de garde inférieur à celui préalablement chargé

Paramètre	Modifiable dans l'état du contrôleur
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 : All OFF->ON : STOP
Autostart	All
Start Allowed	All
Load Allowed	All
Reload Allowed	All
Global Forcing Allowed	All
Global Force Timeout Reaction	All

Tableau 16 : Paramètres modifiables en ligne

Les modifications des paramètres système pendant le fonctionnement sont également possibles par rechargement.

11.2.10 Documentation du programme pour applications de sécurité

Le système de programmation SILworX permet l'impression automatique de la documentation d'un projet. Les types de documents principaux 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 tests de réception d'un système soumis à l'approbation par un organisme de contrôle (par ex. TÜV).

11.2.11 Multitâche

Le terme Multitâche désigne la capacité du système HIMax à traiter jusqu'à 32 programmes utilisateurs au sein d'un module CPU.

Le démarrage et l'arrêt des différents programmes utilisateurs peuvent s'effectuer séparément.

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. À partir de ces paramètres, SILworX calcule le temps de chien de garde du programme utilisateur :
watchdog time $_{\text{user program}}$ = *watchdog time* $_{\text{processor module}}$ * *maximum number of cycles*

Les différents programmes utilisateurs fonctionnent généralement sans interférence et indépendamment les uns des autres. Néanmoins, des 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 entre les cycles des programmes utilisateur et les cycles des processeurs influence considérablement le temps de réponse du programme et de l'écriture des variables !
- Un programme utilisateur évalue une variable globale affichée par un autre programme utilisateur, après au moins un cycle du processeur. En fonction du réglage *Maximum Number of CPU Cycles* dans les programmes, la lecture peut se produire avec un retard de plusieurs cycles du processeur. La réaction aux modifications de ces variables globales est proportionnellement retardée !

Pour de plus amples détails sur le Multitâche, se reporter au manuel du système (HIMax System Manual, HI 801 375 FR)

11.2.12 Essais de réception et organismes en charge de leur approbation

HIMA recommande d'impliquer l'autorité compétente dès que les tests de validation d'un système sont susceptibles d'être soumis à approbation.

Ces tests de validation concernent uniquement les fonctionnalités implémentées par l'utilisateur et non pas les modules et autres appareils liés système HIMax étant déjà homologués.

11.3 Liste de contrôle pour la création d'un programme utilisateur

HIMA conseille d'utiliser la liste de vérification disponible afin que les aspects relatifs à la sécurité soient observés lors de la programmation, avant et après le chargement du programme nouveau ou modifié. La liste de vérification peut être utilisée comme documentation technique de conception et atteste une planification exécutée avec soin.

La liste de vérification est disponible sur le site web de HIMA au format Microsoft® Word®.

12 Configuration de la communication

A l'instar des variables d'entrée et de sortie physiques, les valeurs de variables peuvent être également échangées par le biais d'une liaison de données avec d'autres systèmes. Dans ce cas, les variables sont déclarées à l'aide du logiciel de programmation SILworX dans le menu protocoles s de la ressource correspondante.

12.1 Protocoles standards

Une série de protocoles communication offrent des transmissions de données non sécurisé. Ceux -ci sont généralement utilisés pour des tâches d'automatisation non liées aux fonctions de sécurité.

⚠ 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 de bus de terrain (RS485) du module de communication selon le modèle:
  - Modbus (maître/esclave).
  - Modbus redondant (esclave).
  - PROFIBUS DP (maître/esclave).

12.2 Protocole sécurisé safeethernet

La communication de sécurité via safe**ethernet** est certifiée jusqu'à SIL 3.

La surveillance de la communication sécurisée se paramètre dans l'éditeur safe**ethernet**.

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

REMARQUE

Transition involontaire à l'état de sécurité possible!

***Receive Timeout* est un paramètre de sécurité !**

Le paramètre *Receive Timeou*t d'un PES 1 représente, lors d'un échange de données, la surveillance du temps de réponse d'un partenaire PES 2.

i *Receive Timeout* est également valable dans le sens contraire, du PE 2 vers le PE 1 !

Si aucune réponse correcte du partenaire de communication ne parvient pendant *Receive Timeout*, HIMax ferme la communication de 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 de sécurité devant être exécutées par le biais de safe**ethernet**, seul le paramètre **Use Initial Data** doit être utilisé.

Les équations énoncées ci-dessous démontrent qu'il est possible de déterminer le temps de réponse maximal (Worst Case Reaction Time*)* en utilisant le paramètre *Target Cycle Time* à la place du *Watchdog Time*, uniquement s'il est garanti que le processeur respecte la durée maximale du cycle, y compris lors du rechargement et de la synchronisation.

Dans ce cas, pour le réglage du *Target Cycle Time Mode* sur *Fixed-Tolerant* ou *Dynamic-Tolerant*, les conditions suivantes s'appliquent :

1. *Watchdog Time* ≤ 1,5**Target Cycle Time*
2. Receive Timeout ≤ 5**Target Cycle Time* + 4*Latence

   La latence correspond à la temporisation sur la ligne de transmission.
3. Pour le rechargement, il existe soit un seul programme utilisateur soit plusieurs programmes utilisateur dont le cycle se limite à un cycle du processeur.

12.3 Temps de réaction maximal pour safeethernet

Les exemples d'équation ci-dessous pour le calcul du temps de réponse maximal ne s'appliquent, pour une connexion entre des systèmes HIMatrix, que si aucune suppression de bruits n'a été programmée sur ces systèmes. Ces équations s'appliquent dans tous les cas pour les automates de sécurité 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 la validation.

Termes :

Receive Timeout :	Temps de surveillance d'un système PE 1 au cours duquel une réponse valide d'un partenaire PES 2 doit être reçue. Après expiration du temps, la communication sécurisée est fermée.
Production Rate :	Intervalle minimum entre deux envois de données.
Watchdog Time:	Durée maximale de cycle autorisée par l'automate. Cette durée dépend de la complexité du programme utilisateur et du nombre de connexions safe**ethernet.** Le temps du chien de garde (Watchdog Time) doit obligatoirement être configuré dans les propriétés de la ressource.
Worst Case Reaction Time :	Temps de réaction maximal entre le changement d'une entrée physique d'un PES 1 et la réaction d'une sortie physique d'un PES 2.
Delay :	Temporisation d'un canal de communication, par ex. en cas de connexion par modem ou satellite. En cas de connexion directe, une temporisation de 2 ms est acceptable. La temporisation réelle du canal de communication peut être évaluée par l'administrateur de réseau compétent.

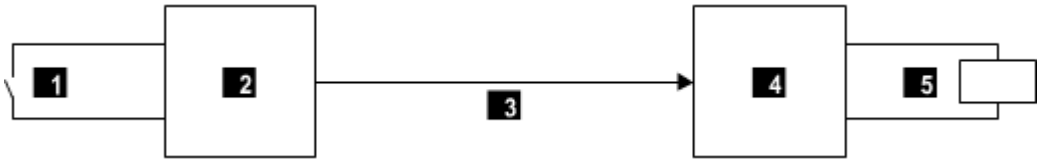
Les conditions suivantes sont applicables aux calculs du temps de réaction maximal indiquées ci-dessous :

- Les données transmises par le protocole safe**ethernet** doivent être traitées par le processeur en un cycle.
- Ajouter les temps de réaction des capteurs et des actionneurs.

Ces calculs sont également applicables aux données transmises par le partenaire.

12.3.1 Calcul du temps de réponse maximal entre deux contrôleurs HIMax

Le temps de réponse maximal T_R (« Worst Case ») correspond à la durée entre le changement d'état d'une entrée du contrôleur 1 (In) et la bascule de la sortie du contrôleur 2 (Out), et se calcule de la manière suivante:



1 Entrée
2 Contrôleur HIMax 1
3 Protocole de sécurité
4 Contrôleur HIMax 2
5 Sortie

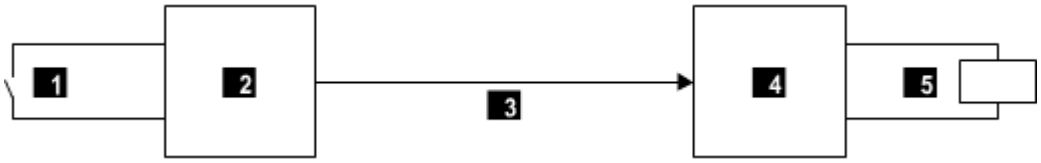
Figure 4 : Temps de réponse entre deux contrôleurs HIMax interconnectés

$T_R = t_1 + t_2 + t_3$

T_R Temps de réponse maximal
t_1 Temps de sécurité du contrôleur HIMax 1
t_2 *Receive Timeout*
t_3 Temps de sécurité du contrôleur HIMax 2

12.3.2 Calcul du temps de réponse maximal pour une connexion avec un contrôleur HIMatrix

Le temps de réponse maximal TR (« Worst Case ») correspond à la durée entre le changement d'état d'une entrée du contrôleur HIMax 1 (In) et la bascule de la sortie du contrôleur HIMatrix 2 (Out), et se calcule de la manière suivante:



1 Entrée
2 Contrôleur HIMax
3 Protocole de sécurité
4 Contrôleur HIMatrix
5 Sortie

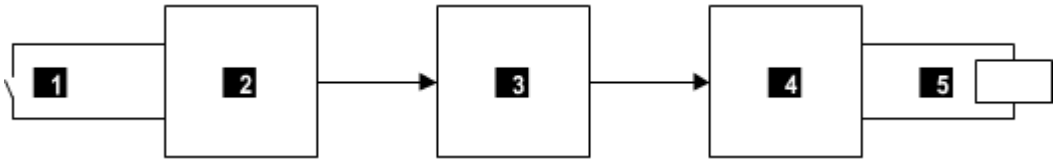
Figure 5 : Temps de réponse applicable à la connexion d'une commande HIMax avec une commande HIMatrix

$T_R = t_1 + t_2 + t_3$

T_R Temps de réponse maximal
t_1 Temps de sécurité du contrôleur HIMax 1
t_2 *Receive Timeout*
t_3 2 * Temps de chien de garde du contrôleur HIMatrix

12.3.3 Calcul du temps de réponse entre deux contrôleurs HIMatrix ou un contrôleur HIMatrix et un module d'Entrées/Sorties déportées

Le temps de réponse maximal T_R (« Worst Case ») correspond à la durée entre le changement d'état d'une entrée du contrôleur HIMatrix 1 (In) et/ou du module d'E/S déportées (par ex. F3 DIO 20/8 01) et la bascule de la sortie du contrôleur HIMatrix 2 (Out) et/ou du module d'E/S déportées. Il se calcule de la manière suivante:



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

Figure 6 : Temps de réponse entre deux contrôleurs HIMax/modules d'E/S déportées et un contrôleur HIMatrix

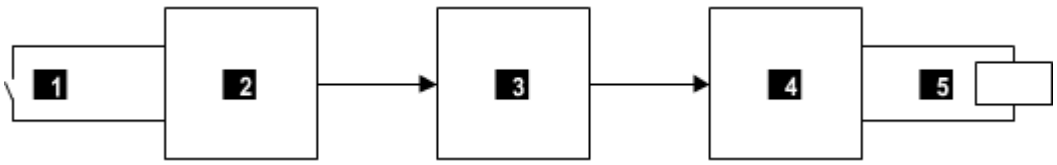
$T_R = t_1 + t_2 + t_3 + t_4 + t_5$

T_R	Temps de réponse maximal
t_1	2 * temps de chien du contrôleur HIMatrix ou module d'E/S déportées 1
t_2	*Receive Timeout1*
t_3	2 * Temps de chien de garde du contrôleur HIMax
t_4	*Receive Timeout2*
t_5	2 * temps de chien du contrôleur HIMatrix 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 un contrôleur HIMatrix au lieu d'un module d'E/S déportées.

12.3.4 Calcul du temps de réponse maximal pour deux contrôleur HIMax et un contrôleur HIMatrix interconnectés

Le temps de réponse maximal TR (« Worst Case ») correspond à la durée entre le changement d'état d'une entrée du premier contrôleur HIMax 1 (In) et la bascule de la sortie du deuxième contrôleur HIMax 2 (Out), et se calcule de la manière suivante:



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

Figure 7 : Temps de réponse entre deux contrôleur HIMax et un contrôleur HIMatrix interconnectés

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

T_R	Temps de réponse maximal
t_1	Temps de sécurité du contrôleur HIMax 1
t_2	*Receive Timeout1*
t_3	2 * Temps de chien de garde du contrôleur HIMatrix
t_4	*Receive Timeout2*
t_5	Temps de sécurité du contrôleur HIMax 2

i Les deux contrôleurs HIMax 1 et 2 peuvent également être identiques.
Le contrôleur HIMatrix peut également être un contrôleur HIMax.

12.4 Protocole sécurisé PROFIsafe

Se reporter aux conditions d'utilisation du protocole PROFIsafe dans le manuel de communication (Communication Manual HI 801 101 E). Les exigences indiquées doivent être respectées.

Les équations relatives au calcul du temps de réponse sont également disponibles dans le manuel de communication.

13 Utilisation dans le cadre d'un système de détection d'incendie

Les automates de sécurité HIMax peuvent être utilisés pour la détection d'incendie selon les normes DIN EN 54-2 et NFPA 72 si la surveillance de ligne est paramétrée pour les entrées et les sorties.

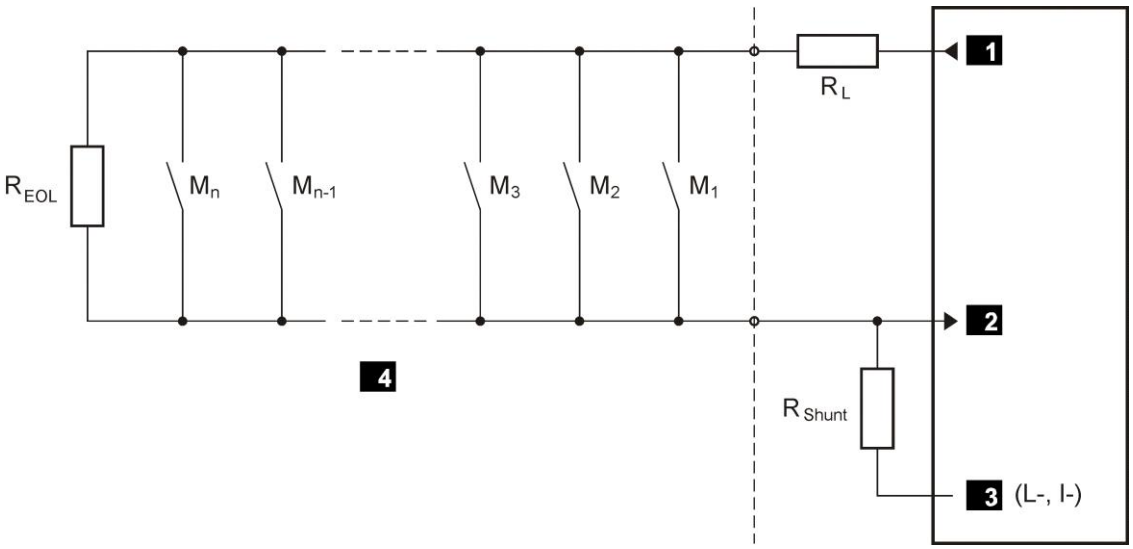
Le programme utilisateur doit pour ce faire remplir les exigences des systèmes conformément aux normes en vigueur précédemment mentionnées.

Le temps de cycle maximal de 10 secondes exigé par la norme DIN EN 54-2 ainsi que le temps de sécurité d'une seconde requis dans certains cas peut être facilement garanti par le système HIMax dont le temps de cycle se calcul en millisecondes.

D'après la norme EN 54-2, le système de détection d'incendie doit être dans l'état spécifié au maximum 100 secondes après détection du problème par le contrôleur HIMax.

Le raccordement des détecteurs d'incendie suit le principe de l'émission de courant (energized to trip) avec surveillance de ligne pour les courts-circuits et ruptures de ligne. Utiliser pour ce faire les entrées et les sorties suivantes :

- Les entrées tout ou rien et analogiques des modules d'entrée avec surveillance de ligne
- Les sorties tout ou rien des modules de sortie avec surveillance de ligne



1 Alimentation capteur
2 Entrée analogique
3 Pôle de référence
4 Boucle de signalisation

M Détecteur d'incendie
R_{EOL} Résistance de terminaison de ligne sur le dernier capteur de la boucle
R_L Limitation du courant maximal de la boucle
R_{Shunt} Résistance de mesure (voir le manuel du module)

Figure 8 : Raccordement des détecteurs d'incendie

Pour l'application, les résistances R_{EOL}, R_L et R_{Shunt} doivent être calculées en fonction des capteurs utilisés et du nombre de capteurs par boucle de signalisation. Les données nécessaires sont disponibles dans les fiches techniques du fabricant du capteur.

Les sorties d'alarme pour le contrôleur des lampes, sirènes, avertisseurs, etc. fonctionnent selon le principe de l'émission de courant. Ces sorties doivent être surveillées contre les courts-circuits et ruptures de ligne. Configurer pour ce faire la surveillance de ligne des modules de sortie et la traiter dans le programme utilisateur.

Un programme utilisateur adapté en conséquence peut commander des systèmes de visualisation, tableaux de signaux lumineux, affichages LED ou alphanumériques, alarmes sonores, etc.

Le routage des signaux de défaut via les modules d'entrées/sorties ou les modules de communication doivent être implémentés selon le principe de mise hors tension pour déclenchement (de-energize to trip)

La transmission des signaux d'incendie d'un système HIMax à un système externe peut se réaliser à l'aide du protocole de communication Ethernet existant (OPC). La perte de la communication doit être détectée.

Les systèmes HIMax utilisés comme système de détection d'incendie doivent être équipés d'une alimentation électrique redondante. Des dispositions doivent également être prises contre la défaillance de l'alimentation électrique, par ex. un avertisseur à batterie. La commutation entre l'alimentation secteur et l'alimentation auxiliaire doit garantir la continuité du fonctionnement. Des chutes de tension de jusqu'à 10 ms sont autorisées.

En cas de mauvais fonctionnement du système, l'automate de sécurité change l'état des variables système correspondantes. Le programme d'utilisateur peut ainsi détecter des erreurs système et réagir en conséquence.
En cas de défaillance sur les modules d'entrées/Sorties, l'automate HIMax réagit de la manière suivante :

- Mise à «0» (Low Pegel) des voies d'entrée défectueuses
- Mise hors tension des voies de sortie défectueuses

14 Utilisation comme dispositif de sécurité, contrôle et régulation avec installation d'alarme pour les concentrations de gaz

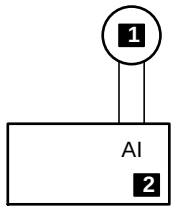
Les modules HIMax sont appropriés pour une utilisation conforme à l'usage prévu dans des applications industrielles sous environnement dangereux jusqu'en zone 2 (gaz, vapeur, brouillard). En tant que composants du système de sécurité HIMax, les modules HIMax X-AI 32 01 et X-AI 32 02 sont testés pour l'utilisation comme dispositif de sécurité, contrôle et régulation avec installation d'alarme pour les concentrations de gaz. Une attestation CE de type fondée sur la directive ATEX est disponible.

L'application est à créer et tester conformément aux exigences des principales normes anti-déflagration.

IEC / EN 60079-0
IEC / EN 60079-29-1

Des capteurs certifiés et testés pour la mesure des concentrations de gaz sont raccordés aux modules HIMax. Respectez les consignes du fabricant en la matière.

En cas d'utilisation en zone 2, le module HIMax et le capteur sont directement connectés l'un à l'autre, voir Figure 9 :

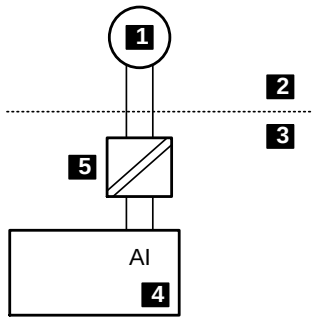


1 Capteur 4…20 mA

2 X-AI 32 01 ou X-AI 32 02

Figure 9 : Utilisation en zone 2

Figure 10 montre une utilisation en zone 1. Le module HIMax est situé en zone 2 et est connecté au capteur en zone 1 par le biais d'un amplificateur-séparateur.



1 Capteur 4…20 mA

2 Zone 1

3 Zone 2

4 X-AI 32 01 ou X-AI 32 02

5 Amplificateur-séparateur, par ex. H 6200A

Figure 10 : Utilisation en zone 1

Le programme d'application peut être créé avec SILworX. Les exigences du fabricant de capteur et des normes sont à respecter lors du paramétrage des seuils.

La fonction de sécurité du système PE HIMax avec les capteurs raccordés est le contrôle des différents gaz inflammables. Les fonctions d'alarme, de régulation et de contrôle de sécurité sont à programmer dans l'application. Avant de démarrer l'exploitation, testez l'application de manière exhaustive.

Annexe

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 aux adresses matérielles
COM	Module de communication
CRC	Contrôle de redondance cyclique
DI	Digital input, entrée tout ou rien
DO	Digital output, sortie tout ou rien
EMC	Electromagnetic compatibility, compatibilité électromagnétique
EN	Norme européenne
ESD	Electrostatic discharge, décharge électrostatique
FB	Fieldbus, bus de terrain
FBD	Function block diagrams, diagramme de blocs fonctionnels
ICMP	Internet control message protocol, protocole réseau pour messages concernant l'état et les erreurs
IEC	Commission électrotechnique internationale
PADT	Programming and debugging tool (selon IEC 61131-3), PC avec SILworX
Panneau de raccordement	Panneau de raccordement pour module HIMax
PE	Protection par mise à la terre
R	Read, lecture
R/W	Read/Write
Rack ID	Identification du rack de l'automate de sécurité
r_P	Valeur de crête de la tension alternative complète des composants
Sans effet rétroactif	Les entrées ont été conçues pour fonctionner sans effet rétroactif et peuvent être implémentées dans des circuits assurant des fonctions de sécurité.
SB	System bus, bus système
SFF	Safe failure fraction, part de défaillances sûres
SIL	Safety integrity level, niveau d'intégrité de sécurité (selon IEC 61508)
SILworX	Outil de programmation pour HIMax
SNTP	Simple network time protocol (RFC 1769), protocole d'heure réseau simple
SRS	System.Rack.Slot, identifiant système d'une ressource
SW	Software, logiciel
Système PE	Système électronique programmable, Programmable Electronic System
TBTP	Très basse tension de protection
TBTS	Très basse tension de sécurité
TMO	Timeout, temps d'expiration
W	Write, écriture
Watchdog (WD)	Chien de garde (surveillance du temps de cycle automate) Si le temps du chien de garde est dépassé, le module ou le programme se met en arrêt pour cause de défauts.
WDT	Temps du chien de garde

Index des figures

Figure 1 : Configuration recommandée de tous les processeurs sur le rack 0 28

Figure 2 : Configuration recommandée : processeur X-CPU 01 sur le rack 0 et le rack 1 28

Figure 3 : Configuration avec les processeurs X-CPU 31 sur le rack 0, emplacements 1 et 2 29

Figure 4 : Temps de réponse entre deux contrôleurs HIMax interconnectés 59

Figure 5 : Temps de réponse applicable à la connexion d'une commande HIMax avec une commande HIMatrix 59

Figure 6 : Temps de réponse entre deux contrôleurs HIMax/modules d'E/S déportées et un contrôleur HIMatrix 60

Figure 7 : Temps de réponse entre deux contrôleur HIMax et un contrôleur HIMatrix interconnectés 60

Figure 8 : Raccordement des détecteurs d'incendie 62

Figure 9 : Utilisation en zone 2 64

Figure 10 : Utilisation en zone 1 64

Index des tableaux

Tableau 1 :	**Vue d'ensemble de la documentation du système**	**11**
Tableau 2 :	**Normes pour la CEM ainsi que la protection du climat et de l'environnement**	**22**
Tableau 3 :	**Conditions générales**	**22**
Tableau 4 :	**Conditions climatiques**	**23**
Tableau 5 :	**Essais mécaniques**	**23**
Tableau 6 :	**Essais d'immunité aux interférences**	**24**
Tableau 7 :	**Essais d'émission d'interférences**	**24**
Tableau 8 :	**Vérification des caractéristiques de l'alimentation en courant continu**	**24**
Tableau 9 :	**Aperçu des modules d'entrée**	**31**
Tableau 10 :	**Vue d'ensemble des modules de sortie**	**35**
Tableau 11 :	**Les paramètres système de la ressource**	**44**
Tableau 12 :	**Effet du paramètre *Target Cycle Time Mode***	**45**
Tableau 13 :	**Variables système du rack**	**46**
Tableau 14 :	**Paramètres système du programme utilisateur**	**52**
Tableau 15 :	**Paramètre programme utilisateur Test Mode Allowedat**	**54**
Tableau 16 :	**Paramètres modifiables en ligne**	**55**

Index

Autotest 12
Champ de test en ligne 54
Concept de sécurité 40
Conditions d'essai
  CEM 24
  climatique 23
  mécaniques 23
  tension d'alimentation 24
CRC 52
Détecteur d'incendie 62
Fonction de sécurité 39
Hardware Editor 47
Installation d'alarme pour les concentrations de gaz 64
LED Ess 25
Liste de versions 40
Multitâche 56
Output Noise Blanking 36, 37
Principe de « Mise hors tension pour déclenchement » 10
Principe de l'émission de courant 10
Procédure de verrouillage du contrôleur 47
Protection ESD 11
Rack ID 27
Réactions aux erreurs
  entres 32
  sorties 35
Redondance 13
responsable 27
Temps de chien de garde
  détermination 15
  programme utilisateur 16
  ressource 14
Temps de réponse 16
Temps de sécurité 16
Temps de sécurité du processus 14
Test fonctionnel du contrôleur 40
Test périodique 17
Zone 1 64
Zone 2 64

HI 801 436 FR

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

HIMA

SAFETY
NONSTOP