HIMatrix®

Contrôleurs de sécurité

Manuel de sécurité
pour Applications Ferroviaires

SAFETY
NONSTOP

HIMA

Contact

Adresse HIMA :

HIMA Paul Hildebrandt GmbH

Boite postale 1261

68777 Brühl, Germany

Tél. : +49 6202 709-0

Fax : +49 6202 709-107

E-mail : info@hima.com

Document original	Description
HI 800 436 D, rév. 3.01 (1632)	Traduction française du document original rédigé en allemand

Sommaire

1 Introduction 7

1.1 Structure et usage de la documentation 7

1.2 Personnes concernées 8

1.3 Conventions typographiques 8

1.3.1 Consignes de sécurité 8

1.3.2 Mode d'emploi 9

2 Consignes d'utilisation 10

2.1 Utilisation conforme à l'usage prévu 10

2.1.1 Domaine d'application 10

2.1.1.1 Principe de «Mise hors tension pour déclenchement» 10

2.1.1.2 Principe de l'émission de courant 10

2.1.2 Utilisation non conforme 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 relative à la sécurité 11

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 THR 12

3.1.2 Autotest et diagnostic d'erreurs 12

3.1.3 PADT 13

3.1.4 Structure des systèmes de sécurité selon le principe de l'émission de courant 13

3.1.4.1 Détection des composants défaillants 13

3.1.4.2 Fonction 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 sécurité du contrôleur 14

3.2.3 Temps de sécurité du programme utilisateur 14

3.2.4 Temps de réponse maximal 14

3.2.5 Temps du chien de garde de la ressource 15

3.2.5.1 Calcul d'un temps de chien de garde adapté 15

3.2.5.2 Estimation conservatrice du temps du chien de garde au moyen d'un test 15

3.2.6 Temps du chien de garde du programme utilisateur 16

3.3 Exigences de sécurité 17

3.3.1 Étude et conception du matériel 17

3.3.2 Programmation 17

3.3.3 Exigences applicables à l'utilisation de l'outil de programmation : 18

3.3.4 Communication 18

3.3.5 Exigences applicables aux applications ferroviaires 18

3.3.6 La cyber-sécurité des systèmes HIMatrix 18

3.4 Conditions d'essai 20

3.5 Conditions d'essai supplémentaires pour applications ferroviaires 20

3.5.1 Plage de hauteur 20
3.5.2 Conditions climatiques 21
3.5.2.1 Déclassement des sorties Tout Ou Rien 22
3.5.3 Conditions mécaniques 22
3.5.3.1 Application dans technique de signalisation 22
3.5.3.2 Applications ferroviaires 22
3.5.4 Conditions CEM 23
3.5.5 Conditions plus sévères 24
3.5.6 Tension d'alimentation 24
3.5.6.1 Conditions s'appliquant à la tension d'alimentation sur les véhicules ferroviaires 24

4 Fonctions centrales 25

4.1 Modules d'alimentation 25

4.2 Description du fonctionnement du processeur 25

4.3 Tests automatiques 26

4.3.1 Test de microprocesseur 26
4.3.2 Test des zones de mémoire 26
4.3.3 Zones de mémoire sécurisées 26
4.3.4 Test de la RAM 26
4.3.5 Test du chien de garde 27
4.3.6 Test du bus E/S dans le contrôleur 27

4.4 Réponses aux erreurs dans le système processeur 27

4.5 Diagnostic d'erreurs 27

5 Entrées 28

5.1 Généralités 28

5.2 Sécurité des capteurs, encodeurs et transmetteurs 28

5.3 Réaction en cas de défauts 29

5.4 Entrées "Tout Ou Rien" relatives à la sécurité 29

5.4.1 Généralités 29
5.4.2 Procédures de test 29
5.4.3 Crêtes sur entrées numériques 29
5.4.4 Entrées Tout Ou Rien paramétrables 29
5.4.5 Line Control 30

5.5 Entrées analogiques relatives à la sécurité (F35 03, F3 AIO 8/4 01 et F60) 31

5.5.1 Procédures de test 32

5.6 Compteurs de sécurité (F35 03 et F60) 32

5.6.1 Généralités 32

5.7 Liste de contrôle pour les entrées Tout Ou Rien de sécurité 33

6 Sorties 34

6.1 Généralités 34

6.2 Sécurité des actionneurs 35

6.3 Réaction en cas de défauts 35

6.4 Sorties Tout Ou Rien de sécurité 35

6.4.1 Procédures de test pour sorties numériques 35
6.4.2 Comportement en cas de court-circuit externe ou de surcharge 35
6.4.3 Line Control 35

6.5 Sorties Tout Ou Rien de sécurité bipolaires 36

6.5.1	Comportement en cas de court-circuit externe ou de surcharge	37
6.6	**Sorties relais**	**37**
6.6.1	Tests fonctionnels pour sorties relais	37
6.7	**Sorties analogiques de sécurité (F60)**	**37**
6.7.1	Procédures de test	38
6.8	**Sorties analogiques avec mise hors tension de sécurité (F3 AIO 8/4 01)**	**38**
6.8.1	Procédures de test	38
6.9	**Liste de contrôle pour les sorties de sécurité**	**38**
7	**Logiciel pour systèmes HIMatrix**	**39**
7.1	**Aspects relatifs à la sécurité pour le système d'exploitation**	**39**
7.2	**Mode opérationnel et fonctions du système d'exploitation**	**39**
7.3	**Aspects relatifs à la sécurité pour la programmation**	**40**
7.3.1	Concept de sécurité de l'outil de programmation	40
7.3.2	Vérification de la configuration et du programme utilisateur	40
7.3.3	Archivage d'un projet	41
7.3.4	Possibilité d'identification au programme et à la configuration	41
7.4	**Paramètres de la ressource**	**41**
7.4.1	Paramètres système de la ressource	42
7.4.1.1	Utilisation des paramètres *Target Cycle Time* et *Target Cycle Mode*	44
7.4.1.2	Calcul de *Max. Duration of Configuration Connections [ms]*	45
7.4.1.3	Remarques sur les paramètres *Allow Online Settings* et *Reload Allowed*	45
7.4.1.4	Remarques concernant le paramètre *Minimum Configuration Version* :	46
7.4.1.5	Remarque sur le paramètre *Démarrage rapide*	46
7.4.2	Variable système du matériel	47
7.5	**Protection contre manipulations**	**48**
7.6	**Liste de contrôle pour la création d'un programme utilisateur**	**48**
8	**Aspects relatifs à la sécurité pour le programme utilisateur**	**49**
8.1	**Cadre d'une utilisation relative à la sécurité**	**49**
8.1.1	Base de la programmation	49
8.1.2	Fonctions du programme utilisateur	50
8.1.3	Déclaration des variables	50
8.1.4	Essais de réception et organismes en charge de leur approbation	51
8.2	**Procédures**	**51**
8.2.1	Assignation de variables aux entrées et sorties	51
8.2.2	Ouverture et fermeture du contrôleur	51
8.2.3	Génération de codes	52
8.2.4	Comparateur de versions sécurisé	53
8.2.5	Chargement et démarrage du programme utilisateur	53
8.2.6	Rechargement	53
8.2.7	Forçage	55
8.2.7.1	Forçage des sources de données	55
8.2.8	Modification des paramètres système pendant exploitation	55
8.2.9	Documentation du programme pour applications de sécurité	56
8.2.10	Multitâche	56
8.2.11	Essais de réception et organismes en charge de leur approbation	57
9	**Configuration de la communication**	**58**

9.1 Protocoles standards 58
9.2 Protocole sécurisé safeethernet 58
9.2.1 Receive Timeout 59
9.2.2 Response Time 59
9.2.3 Calcul du temps de réponse maximal 61
9.2.4 Calcul du temps de réponse avec deux modules d'E/S déportées 61
9.2.5 Terminologie 62
9.2.6 Attribution des adresses safe**ethernet** 62
Annexe 63
Glossaire 63
Index des figures 64
Index des tableaux 65
Index 66

1 Introduction

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

Les conditions requises garantissant l'installation sans risque, la mise en service ainsi que la sûreté de fonctionnement et la maintenance des automates HIMatrix 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 HIMatrix 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 HIMatrix. 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 Structure et usage de la documentation

Ce manuel de sécurité couvre les thèmes suivants :

- Utilisation conforme à l'usage prévu
- Concept de sécurité
- Fonctions centrales
- Entrées
- Sorties
- Logiciel
- Aspects relatifs à la sécurité pour le programme utilisateur
- Configuration de la communication
- Annexe :
  - Glossaire
  - Listes/Index

i Les commandes compactes et modules d'E/S déportées sont désignés en tant qu'*Appareil*, les cartes d'extension d'une commande modulaire en tant que *Module*.

Dans SILworX, les sous-groupes sont désignés en tant que *module.*

1.2 Personnes concernées

Ce document 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 de l'installation et systèmes. Des connaissances spécifiques en matière de systèmes d'automatisation de sécurité sont nécessaires.

1.3 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, index du menu et onglets cliquables dans l'outil de programmation
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.

1.3.1 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

1.3.2 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

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 HIMatrix.

2.1.1 Domaine d'application

Les commandes relatives à la sécurité HIMatrix peuvent être utilisées jusqu'à un niveau d'intégrité de sécurité SIL 4 selon les normes EN 50126, EN 50128 et EN 50129.

Les systèmes HIMatrix sont homologués pour des commandes de processus, des systèmes de protection, des commandes de brûleurs et des commandes de machine.

2.1.1.1 Principe de «Mise hors tension pour déclenchement»

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

Un système fonctionnant à manque de tension ne requiert pas d'énergie pour exécuter sa fonction de sécurité (de-energize to trip).

En présence d'un défaut, les signaux d'entrée et de sortie adoptent l'état de sécurité hors tension ou hors circuit.

2.1.1.2 Principe de l'émission de courant

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

Un système, fonctionnant selon le principe de l'émission de courant, requiert de l'énergie, par ex. de l'énergie électrique ou pneumatique, pour exécuter sa fonction de sécurité (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.

2.1.2 Utilisation non conforme

La transmission des données essentielles pour la sécurité par le biais des réseaux publics (par ex. Internet) est autorisée avec des mesures complémentaires visant à renforcer la sécurité (par ex. tunnel VPN, pare-feu, etc.).

Une communication relative à la sécurité n'est pas autorisée au moyen d'interfaces de bus de terrain.

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 HIMatrix dans les systèmes d'automatisation et dans l'ensemble des installations.

La programmation des systèmes HIMatrix 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 relative à la 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 9 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 systèmes HIMatrix !

- **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.**

2.4 Autres documentations du système

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

Manuel	Description	Document nº
HIMatrix Safety Manual	Fonctions de sécurité du système HIMatrix	HI 800 023 E
HIMatrix System Manual	Description du système HIMatrix	HI 800 641 FR
Certificats	Résultats des Tests	-
Liste de versions	Versions du système d'exploitation certifiées par le TÜV	-
Manuels des composants	Description des composants individuels	
Communication Manual	Description du protocole de communication ComUserTask et de sa programmation dans SILworX	HI 801 001 E
SILworX Online Help	Instructions sur la manière d'utiliser SILworX	-
SILworX First Step Manual	Introduction à l'utilisation de SILworX : utilisation de SILworX à des fins de planification, mise en service, test et exploitation	HI 801 203 FR

Tableau 1 : Documentation du système HIMatrix

Les documents actuels sont disponibles sur les sites HIMA www.hima.de et www.hima.com (sauf l'aide en ligne SILworX). L'indice de révision en bas de page permet de vérifier si les manuels existants sont à jour par rapport à la version disponible sur Internet.

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 HIMatrix :

- Sécurité et disponibilité
- Temps importants pour la sécurité
- Exigences de sécurité
- Certification
- Conditions d'essai
- Conditions d'essai supplémentaires pour applications ferroviaires

3.1 Sécurité et disponibilité

Les systèmes HIMatrix sont homologués pour des commandes de processus, des systèmes de protection, des commandes de brûleurs et des commandes de machine.

Les systèmes HIMatrix en soi ne présentent aucun risque immédiat.

⚠ AVERTISSEMENT

Possibles 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 !

3.1.1 Calculs THR

Un calcul THR a été effectué pour les systèmes HIMatrix, conformément à la norme EN 50129.

La norme EN 50129 établit un THR de 10^{-9}…10^{-8} par heure (SIL 4).

Les fonctions de sécurité, se composant d'une boucle relative à la sécurité (entrée, unité de traitement, sortie et communication entre les systèmes HIMatrix), répondent dans toutes les combinaisons à l'ensemble des exigences décrites ci-dessus. Les commandes, les E/S déportées et les modules s'ajustent à ces exigences.

3.1.2 Autotest et diagnostic d'erreurs

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

- Les processeurs
- Les zones de mémoire (RAM, mémoire vive)
- Le chien de garde
- Chaque canal E/S

Si ces tests détectent des erreurs, le système d'exploitation désactive l'appareil défectueux, le module défectueux ou le canal E/S défectueux.

Dans un système sans redondance, cela signifie que des fonctions partielles ou l'ensemble du système PE peut être désactivé.

Tous les modules HIMatrix, automates et modules disposent de ses propres LED qui indiquent les défauts détectés. En cas de dérangement, cela permet un diagnostic rapide des erreurs d'un appareil ou d'un circuit externe signalé comme défectueux.

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

Un enregistrement du diagnostic complet relatif au comportement du système et des défauts détectés est stocké dans la mémoire de diagnostic des commandes. 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 (HIMatrix System Manual Compact Systems HI 800 641 FR).

Pour une partie infime des défaillances de composants n'affectant pas la sécurité, le système HIMatrix 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.

Le PADT est un ordinateur personnel sur lequel l'outil de programmation est installé.

3.1.4 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 les fonctions suivantes :

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

3.1.4.1 Détection des composants défaillants

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

3.1.4.2 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 de sécurité.

La planification suivante relève de l'utilisateur :

- Contrôle de court-circuit et d'interruption de ligne sur les automates d'entrées/de sorties. Ces fonctions doivent être paramétrées.
- La fonction des actionneurs peut être contrôlée par la recopie de position.

3.2 Temps importants pour la sécurité

Temps importants pour la sécurité :

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

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.

3.2.2 Temps de sécurité du contrôleur

Le temps de sécurité est le temps pendant lequel le contrôleur en état RUN doit réagir après l'apparition d'un défaut interne.

Du point de vue du processus, le temps de sécurité est la durée maximale pendant laquelle le système de sécurité doit fournir une réponse au niveau des sorties après modification des signaux d'entrée (temps de réponse en cas de défaut). Le temps de sécurité est réglable dans une plage de 20 à 22 500 ms.

3.2.3 Temps de sécurité du programme utilisateur

Le temps de sécurité du programme utilisateur ne peut s'ajuster immédiatement. HIMatrix calcule le temps de sécurité à partir des paramètres *Safety time* de la ressource et *Maximum Number of Cycles*. Pour de plus amples détails, se reporter au chapitre 8.2.10.

3.2.4 Temps de réponse maximal

Le temps de réponse maximal s'applique pour un système fonctionnant sans anomalies. Il s'agit du temps maximal que peut prendre le système HIMatrix pour réagir à la modification d'un signal d'entrée par un signal de sortie correspondant. Dans le cas des commandes HIMatrix en fonctionnement cyclique, le temps de réponse maximal est le double du temps de cycle maximal. Les conditions requises pour cela sont :

- La logique du programme utilisateur est exécutée de façon à empêcher les temporisations, par ex. dues à une séquence de traitement incorrecte.
- L'exécution de la totalité du programme utilisateur doit se faire dans un cycle de processeur.
- Les données décisives pour la réaction ne sont pas transmises entre des programmes utilisateurs différents.

La durée de cycle d'un contrôleur comprend l'exécution des tâches suivantes :

- Lecture des entrées
- Traitement du programme utilisateur ou des programmes utilisateurs
- Écriture des sorties
- Communication des données de processus
- Exécution des procédures de test

3.2.5 Temps du 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 du chien de garde défini, le système se désactive. Ensuite, le système redémarre si le démarrage automatique a été paramétré. Si le démarrage automatique n'a pas été paramétré, le système passe à l'état STOP/VALID CONFIGURATION.

Régler le temps du chien de garde du système processeur sur un temps de sécurité de l'automate ≤ ½ ∗.

Plage de valeurs pour le temps du chien de garde	Commandes de valeur standard	Valeur standard des E/S déportées
4…5000 ms	200 ms	100 ms

Tableau 2 : Plage de valeurs pour le temps du chien de garde

i Le temps de sécurité et le temps du chien de garde doivent être déterminés pour l'installation à contrôler.

3.2.5.1 Calcul d'un temps de chien de garde adapté

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

Les calculs suivants se font à partir de réseaux d'automatisation typiques relatifs à la sécurité. Ces réseaux sont presque exclusivement composés d'appareils HIMA des gammes HIMatrix et HIMax.

Les réseaux étendus, en plus des appareils HIMA, contiennent de nombreux autres participants. Dans le cas des réseaux étendus, les activités des autres participants peuvent allonger fortement le temps de cycle de l'automate HIMatrix. Par exemple, une diffusion à tous les participants, potentiellement plus de 1 000, peut allonger le temps de cycle de 20 à 40 ms.

Pour la mesure du temps du chien de garde, tenir compte aussi de ce type d'influences !

Les réseaux étendus sont l'exception.

3.2.5.2 Estimation conservatrice du temps du chien de garde au moyen d'un test

L'estimation suivante est valable à la condition suivante :

L'appareil HIMatrix se trouve dans un réseau qui n'est ni saturé ni en dérangement. Les sollicitations exceptionnelles, par ex. par des télégrammes de diffusion fréquents ou des appareils défectueux, sont exclues.

Dans le cas d'un réseau homogène contenant uniquement des automates de sécurité, on peut partir du principe que cette condition est remplie.

Dans tous les cas, il convient ici de vérifier le temps du chien de garde estimé pendant le Factory Acceptance Test (FAT, soit le test de réception en usine) et le Site Acceptance Test (SAT, test de réception chez le client) avec les temps de cycle réels par une évaluation des statistiques de temps de cycle.

Si l'on obtient des valeurs inattendues, ou si la condition mentionnée ne peut pas être remplie avec certitude, HIMA recommande de contacter le service client HIMA.

Pour déterminer une configuration appropriée, HIMA recommande d'effectuer un test aussi complet que possible sur l'ensemble du système :

- Le matériel HIMatrix est entièrement monté, par ex. le rack F60 contient tous les modules prévus.
- Les partenaires de communication sont présent, y compris les modules d'E/S déportées.
- La logique du programme utilisateur est aussi complète que possible.

Déterminer une valeur minimale pour le temps du chien de garde

1. Utiliser le système à pleine charge. La communication doit elle aussi fonctionner à pleine charge.
2. Indiquer les données d'entrée de façon à faire fonctionner en continu des chemins de programme aussi longs que possible. À cet effet, des séquences de valeurs d'entrée peuvent être nécessaires.
3. Réinitialiser les statistiques de temps de cycle dans le panneau de configuration.
4. Procéder à plusieurs rechargements si la ressource s'y prête.
5. Tenir compte des valeurs maximales des temps de cycle dans le panneau de configuration.
   ☑ T_{Zyklus} est calculé.
6. Faire fonctionner le système pendant un certain temps et noter les temps de cycle les plus longs des programmes utilisateurs avec une charge de base et avec des charges extrêmes.
   ☑ ΔT_{Spitze} est calculé.
7. Calculer le temps du chien de garde minimum T_{WD} :
   $T_{WD} = T_{Zyklus +} T_{Res} + T_{Komm} + T_{Konfig} + \Delta T_{Spitze}$, donne
   - T_{Zyklus} Temps de cycle maximal observé (charge de base, contient déjà des parts de T_{Com} et T_{Config})
   - T_{Res} Réserve de sécurité de 6 ms
   - T_{Com} Paramètre système configuré *Max.Com. Time Slice ASYNC [ms]*
     Dans cette situation, il ne faut pas reprendre la valeur prédéfinie mais, conformément à l'intensité de communication prévisible (par ex. safe**ethernet**, Modbus), fixer une valeur judicieuse pour le projet !
   - T_{Config} Paramètres système configuré *Max. Duration of Configuration Connections [ms]*
     Dans cette situation, il ne faut pas reprendre la valeur prédéfinie mais fixer une valeur calculée pour le projet, voir chapitre 7.4.1.2 !
   - ΔT_{Spitze} Charges extrêmes observées moins la charge de base observée, voir étape 6.

► Le temps de chien de garde défini doit être : valeur minimale calculée + supplément pour les futures modifications ou extensions.

Les valeurs maximales de temps de cycle en cas de rechargement dépendent du temps défini pour le chien de garde. Pour optimiser l'automate à un temps de chien de garde aussi court que possible, il faut réduire de plus en plus la valeur du temps **défini** pour le chien de garde dans une série de mesure.

3.2.6 Temps du chien de garde du programme utilisateur

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

Le temps du chien de garde du programme utilisateur ne s'ajuste pas immédiatement. HIMatrix 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.*

Il faut s'assurer que le temps du chien de garde calculé 2 fois soit au moins aussi élevé que le temps de réponse exigé pour la partie du processus traitée par le programme utilisateur.

3.3 Exigences de sécurité

Les exigences de sécurité suivantes s'appliquent en cas d'utilisation des composants relatifs à la sécurité du système HIMatrix :

3.3.1 Étude et conception du matériel

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

Exigences non liées au produit

- Pour des opérations relatives à la sécurité, seuls le matériel et les logiciels à sécurité intrinsèque homologués peuvent être utilisés. Le matériel et les logiciels homologués sont spécifiés dans le document *Revision List of Devices and Firmware of HIMatrix-Systems of HIMA Paul Hildebrandt GmbH*.
  Les révisions actuelles sont disponibles dans l'actuelle liste des révisions détenue par l'organisme d'inspection. La liste des versions actuelles est disponible sur le site HIMA.
- Les conditions d'utilisation spécifiées (voir chapitres 3.5) relatives à la compatibilité électromagnétique (CEM), aux influences mécaniques, chimiques et climatiques doivent être respectées.
- Un matériel ou des logiciels sans sécurité intrinsèque, toutefois sans effet rétroactif, peuvent être utilisés pour le traitement de signaux non relatifs à la sécurité. Néanmoins, ne pas les utiliser pour le traitement d'opérations liées à la technique de sécurité.

Exigences liées au produit

- Seuls des dispositifs présentant une isolation sécurisée à la tension d'alimentation peuvent être connectés au système.
- L'isolation électrique sûre doit être assurée au sein de l'alimentation 24 V du système. N'utiliser que des modules d'alimentation assurant la possibilité d'un fonctionnement du contrôleur et des E/S déportées à basse tension 24 V.
- Pour assurer le respect des normes de sécurité ayant trait à la sécurité électrique et la mise à la terre, le fabricant des applications spécifiques doit prévoir des mesures de séparations appropriées entre les installations extérieures et intérieures selon la norme EN 50122. Cela permet de protéger les systèmes HIMatrix contre les influences des équipements extérieurs dans la zone de ligne aérienne de contact ou zone de pantographe et contre le courant de retour de traction. N'utiliser que des équipements d'alimentation homologués pour une utilisation dans le domaine ferroviaire.

3.3.2 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 de sécurité du système doit être assurée. Pour consulter les différentes possibilités de paramétrage, se reporter au manuel de sécurité, voir chapitre 7.4.
- Cela concerne notamment la configuration du système, la durée de cycle maximale ainsi que le temps de sécurité, voir chapitre 3.2.

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

- Utiliser **SILworX** pour la programmation.
- Après avoir créé l'application, compiler deux fois le programme et comparer les deux CRC de configuration obtenus, afin de s'assurer que la compilation a été effectuée correctement.
- La correcte réalisation des applications spécifiées doit être validée et vérifiée. Un test complet de la logique doit être effectué en procédant à des tests.
- La réponse du système aux défauts survenant dans les modules d'E/S de sécurité, doit être définie dans le programme utilisateur selon les données de sécurité spécifiques aux installations.
- Une fonction de l'outil de programmation SILworX permet de montrer quels changements ont été effectués sur le programme utilisateur ou sur le système de configuration. L'analyse des changements et de leurs effets doit déterminer l'étendue des tests. Cette analyse doit tenir compte des changements après modifications, des résultats obtenus par la fonction de comparaison de SILworX ainsi que des tests de régression.

3.3.4 Communication

- Lors des communications relatives à la sécurité entre différents automates, veiller à ce que le temps de réponse complet du système ne dépasse pas le temps de réponse autorisé. Les calculs de base figurant au chapitre 9.2 doivent être utilisés.
- Le transfert des données doit s'effectuer par le biais de systèmes privés de transmission (catégorie 1) au sens de la norme EN 50159.
- L'utilisation de systèmes de transmission ouverts (catégorie 2 et catégorie 3) au sens de la norme EN 50159 est possible si des mesures supplémentaires sont prises pour garantir la sécurité du canal de transmission (par ex. pare-feu ou cryptage).
- Pour ce type d'extensions, les interfaces sérielles s'utilisent exclusivement à des fins non relatives à la sécurité.
- Seuls des automates présentant une isolation électrique sécurisée peuvent être connectés à toutes les interfaces de communication.

3.3.5 Exigences applicables aux applications ferroviaires

- Appliquer les normes concernant les applications ferroviaires.
- Les sorties Tout Ou Rien sont dotées d'une surveillance de court-circuit. Les réactions aux courts-circuits détectés doivent être programmées par le biais du programme utilisateur.
- L'état de la température (température de fonctionnement) des systèmes HIMatrix doit être évalué dans le programme utilisateur. Les mesures relatives à la sécurité doivent également être appliquées par le biais du programme utilisateur. Pour de plus amples informations, se reporter au manuel du système (HIMatrix System Manual Compact Systems HI 800 641 FR).
- Les messages de défaut doivent être évalués par le programme utilisateur. Les défauts sont signalés par les bits d'état et sont disponibles pour le programme utilisateur. En outre, les défauts sont saisis dans la mémoire de diagnostic du contrôleur et peuvent être lus avec l'outil de programmation utilisé. Pour de plus amples informations, se reporter au manuel du système (HIMatrix System Manual Compact Systems HI 800 641 FR).
- Une détection de la mise à la terre doit être configurée en externe.

3.3.6 La cyber-sécurité des systèmes HIMatrix

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 HIMatrix se compose des parties suivantes, qui doivent être protégées :

- Automate HIMatrix
- PADT
- Serveur OPC : X-OPC DA, X-OPC AE (optionnel)
- Connexions de communication vers des systèmes externes (optionnel)

Le system HIMatrix satisfait déjà de par ses réglages de base aux exigences de la cyber-sécurité (sécurité informatique).

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 nom ainsi qu'un mot de passe pour la connexion de l'utilisateur au système PE à l'accès.
- L'accès aux variables 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 les opérations de maintenance ou de diagnostic, il est possible de connecter ponctuellement le PADT.

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 !

Exemples :

- **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 (Cyber Security Manual HI 801 373 E).

3.4 Conditions d'essai

Pour plus d'informations concernant les normes selon lesquelles le système HIMatrix a été testé et certifié pour un usage industriel, se reporter au manuel de sécurité HIMatrix Safety Manual HI 800 023 E.

3.5 Conditions d'essai supplémentaires pour applications ferroviaires

Le tableau suivant montre les variantes HIMatrix homologuées pour une utilisation dans des applications ferroviaires :

Commandes compactes
F30 034
F35 034
Modules d'E/S déportées
F1 DI 16 014
F2 DO 4 014 [1)]
F2 DO 8 014
F2 DO 16 014
F2 DO 16 024 [1)]
F3 AIO 8/4 014
F3 DIO 8/8 014
F3 DIO 16/8 014
F3 DIO 20/8 023
F3 DIO 20/8 024
Système modulaire F60
PS 014
CPU 034
AI 8 014
CIO 2/4 014
DI 24 014
DI 32 014
DIO 24/16 014
MI 24 014
GEH 014
[1)] Seulement autorisé pour une plage de température 0…+60 °C

Tableau 3 : Variantes HIMatrix disponibles pour applications ferroviaires

Les variantes HIMatrix pour applications ferroviaires ont été mises au point pour répondre en outre aux exigences en matière de CEM ainsi que de protection climatique et de l'environnement.

3.5.1 Plage de hauteur

Les classes qui s'appliquent pour la plage de hauteur des variantes HIMatrix sont les suivantes :

- Pour une utilisation en technique de signalisation selon EN 50125-3 : AX jusqu'à 2 000 m
- Pour une utilisation à bord de véhicules ferroviaires selon EN 50125-1 : AX jusqu'à 2 000 m

3.5.2 Conditions climatiques

Tous les appareils sur pied de la gamme d'automates HIMatrix sont prévus et testés pour une plage de température allant de 0 à 60 °C et pour une hygrométrie relative allant de 10 à 95 % (sans condensation). Pour une application ferroviaire selon EN 50125-3, les classes de température qui en résultent sont donc les suivantes :

HIMatrix	En extérieur	Dans une armoire électrique	Dans un container		En intérieur	
			N.T.C	T.C	N.C.C.	C.C
Standard	-	-	-	T1, T2, TX	T1	T1, T2, TX

Tableau 4 : Classes de température des appareils HIMatrix standard selon EN 50125-3

Les appareils standard de la gamme d'automates HIMatrix ne sont pas autorisés pour une utilisation à bord de véhicules ferroviaires selon EN 50155 car ils ne possèdent pas de laquage de protection.

Les variantes HIMatrix pour applications ferroviaires sont conçues pour une plage de température de -25 à +70 °C. Toutes les variantes HIMatrix pour les applications ferroviaires ont été testées selon EN 50125-3 et EN 50155 et sont utilisables dans les classes de température suivantes :

HIMatrix	En extérieur	Dans une armoire électrique	Dans un container		En intérieur	
			N.T.C	T.C	N.C.C.	C.C
F30 034	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F35 034	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F1 DI 16 014	T1, T2	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX	T1, T2, TX
F2 DO 4 014	-	-	-	T1, T2, TX	T1	T1, T2, TX
F2 DO 8 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F2 DO 16 014	T1, T2	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX	T1, T2, TX
F2 DO 16 024	-	-	-	T1, T2, TX	T1	T1, T2, TX
F3 AIO 8/4 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F3 DIO 8/8 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F3 DIO 16/8 014	T1, T2	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX	T1, T2, TX
F3 DIO 20/8 024	T1, T2	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX	T1, T2, TX
PS 014	T1, T2	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX	T1, T2, TX
CPU 034	T1, T2	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX	T1, T2, TX
AI 8 014	T1, T2	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX	T1, T2, TX
CIO 2/4 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
DI 24 014	T1, T2	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX	T1, T2, TX
DI 32 014	T1, T2	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX	T1, T2, TX
DIO 24/16 014	T1, T2	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX	T1, T2, TX
MI 24 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX

Tableau 5 : Classes de température selon EN 50125-3

HIMatrix	Classes de température
F30 034	T1
F35 034	T1
F1 DI 16 014	T1, T2, T3, TX
F2 DO 4 014	- [1)]
F2 DO 8 014	T1
F2 DO 16 014	T1, T2, T3, TX
F2 DO 16 024	- [1)]
F3 AIO 8/4 014	T1
F3 DIO 8/8 014	T1
F3 DIO 16/8 014	T1, T2, T3, TX
F3 DIO 20/8 024	T1, T2, T3, TX
PS 014	T1, T2, T3, TX
CPU 034	T1, T2, T3, TX
AI 8 014	T1, T2, T3, TX
CIO 2/4 014	T1
DI 24 014	T1, T2, T3, TX
DI 32 014	T1, T2, T3, TX
DIO 24/16 014	T1, T2, T3, TX
MI 24 014	T1
[1)] Seulement autorisé pour une plage de température 0…+60 °C	

Tableau 6 : Classes de température selon EN 50125-3

3.5.2.1 Déclassement des sorties Tout Ou Rien

En cas de température ambiante supérieure à 60 °C, la charge des sorties Tout Ou Rien doit être diminuée (déclassement/derating). Dans ce cas, les sorties peuvent être sollicitées à un maximum de 0,5 A, voir les manuels des automates.

3.5.3 Conditions mécaniques

Les composants HIMatrix ont été testés selon EN 50125-3 et EN 50155.

3.5.3.1 Application dans technique de signalisation

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

EN 50125-3	Essais mécaniques
	Essai de vibrations : 2,3 m/s^2 entre 5...2000 Hz, objet testé en fonctionnement
	Essais de résistance aux chocs : 20 m/s^2, 11 ms, objet testé en fonctionnement

Tableau 7 : Conditions mécaniques pour application dans technique de signalisation

3.5.3.2 Applications ferroviaires

Les automates et modules figurant dans le Tableau 3 ont été soumis à un test mécanique EN 50155 et sont appropriés pour les applications ferroviaires. Le test a été effectué selon EN 61373, catégorie 1, classe B.

3.5.4 Conditions CEM

Les tableaux suivants répertorient les valeurs limites et les tests les plus importants applicables aux conditions CEM:

Normes de tests	Nature du test	Essais d'immunité aux interférences
EN 61000-4-2	Essai ESD	Contact 6 kV, décharge dans l'air 8 kV
EN 61000-4-3	Champ EM	80…1000 MHz : 10 V/m 800…1000 MHz : 20 V/m 1400…2000 MHz : 10 V/m 2000…2700 MHz : 5 V/m 5100…6000 MHz : 3 V/m
EN 61000-4-4	Essai par salve	Tension d'alimentation : 2 kV Lignes d'E/S : 2 kV Mise à la terre : 1 kV
EN 61000-4-5	Crête [1)]	Tension d'alimentation : 2 kV CM 1 kV DM Lignes d'E/S : 2 kV CM 1 kV DM Lignes blindées : 2 kV CM
EN 61000-4-6	Afflux	Tension d'alimentation : 10 V Lignes d'E/S : 10 V Mise à la terre : 10 V
EN 61000-4-8	Champ magnétique à la fréquence du réseau	16 2/3 Hz, 50 Hz, 60 Hz : 300 A/m CC 300 A/m
[1)] Le filtre externe H 7013 est impératif dans les systèmes compacts HIMatrix. Des parafoudres d'autres fabricants peuvent être utilisés si les caractéristiques de la fiche technique sont identiques ou supérieures.		

Tableau 8 : Conditions CEM pour application dans technique de signalisation selon EN 50121-4

i De même, des filtres de surtension externes sont obligatoires pour toutes les lignes d'entrée et de sortie non blindées si elles sont reliées à des lignes en-deçà de la plage des 3 m ou par des lignes de plus de 30 m en-deçà de la plage des 10 m.

Normes de tests	Nature du test	Essais d'immunité aux interférences
EN 61000-4-2	Essai ESD	Contact 6 kV, décharge dans l'air 8 kV
EN 61000-4-3	Champ EM	80…1000 MHz : 20 V/m 1400…2000 MHz : 10 V/m 2000…2700 MHz : 5 V/m 5100…6000 MHz : 3 V/m
EN 61000-4-4	Essai par salve	Tension d'alimentation : 2 kV Lignes d'E/S : 2 kV
EN 61000-4-5	Crête [1)]	Tension d'alimentation : 2 kV CM 1 kV DM
EN 61000-4-6	Afflux	Tension d'alimentation : 10 V Lignes d'E/S : 10 V
[1)] Le filtre externe H 7013 est impératif dans les systèmes compacts HIMatrix. Des parafoudres d'autres fabricants peuvent être utilisés si les caractéristiques de la fiche technique sont identiques ou supérieures.		

Tableau 9 : Conditions CEM pour applications ferroviaires selon EN 50121-3-2

Les automates et modules figurant dans le Tableau 3 ont passé avec succès le test relatif aux exigences CEM des normes EN 50121-4 et EN 50121-3-2.

3.5.5 Conditions plus sévères

Les modules d'E/S déportées F3 DIO 20/8 023 répondent aux exigences plus élevées en matière de brouillard salin, conformément à la norme IEC 60068-2-11 (5 % pour une durée de 96 heures).

Un test a certifié son adéquation.

3.5.6 Tension d'alimentation

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

IEC/EN 61131-2	Test d'insensibilité aux anomalies de tension d'alimentation
	Essai sur la plage de tension : 24 VCC, -20...+25 % (19,2...30,0 V)
	Test d'insensibilité aux interruptions de courte durée de la tension d'alimentation externe : CC, PS 2 : 10 ms
	Inversion de polarité de la tension d'alimentation : testée pour 10 s

Tableau 10 : Test d'insensibilité aux anomalies de tension d'alimentation

3.5.6.1 Conditions s'appliquant à la tension d'alimentation sur les véhicules ferroviaires

L'alimentation électrique de l'automate HIMatrix est fournie par une batterie d'accumulateurs dont la tension nominal est de 24 V.

Les valeurs suivantes s'appliquent à la tension d'alimentation du HIMatrix: 24 VCC, -15…+20%, 5 % d'ondulation.

Ce qui se traduit en valeur de tolérance suivante:

- Tension minimale: 19,2 V (0,8 UN)
- Tension nominale: 24 V (UN)
- Tension assignée: 27,6 V (1,15 UN)
- Tension maximale: 30 V (1,25 UN)

Les variantes HIMatrix mentionnées dans le Tableau 3 ont été testées selon la norme EN 50155, chapitre 5.1.

L'utilisateur doit s'assurer qu'une tension minimum de 0,8 UN est maintenue en prenant des mesures externes, sans quoi les appareils isolés ou le système entier exécuteront un redémarrage.

Les écarts de tension supérieurs à 1,25 UN doivent pouvoir être interceptés en prenant des mesures externes selon EN 50155, chapitre 5.1.1.1.

Les automates HIMatrix sont conçus pour une tenue aux interruptions jusqu'à 20 ms. De ce fait HIMatrix répond aux exigences de classe S2 selon EN 50155, chapitre 5.1.1.2.

L'automate HIMatrix répond aux conditions pour le taux d'ondulation de la tension continue selon EN 50155, chapitre 5.1.1.4.

Si un convertisseur ou un transformateur réversible est utilisé pour alimenter le système, HIMatrix répond aux conditions pour une exploitation normale selon EN 50155, chapitre 5.1.2. Pour les écarts de tension autorisés selon la norme, des mesures externes doivent être prises par l'utilisateur.

Cela ne répond pas aux conditions de commutation entre deux tension d'alimentation selon EN 50155, chapitre 5.1.3. Des mesures externes doivent être prises par l'utilisateur.

4 Fonctions centrales

Sur les automates de type F1.., F2.., F3.., il s'agit de systèmes compacts ne pouvant être modifiés.

Sur les commandes de type F60, il s'agit de systèmes modulaires permettant d'utiliser au sein d'une commande avec processeur et de module d'alimentation jusqu'à six modules d'E/S.

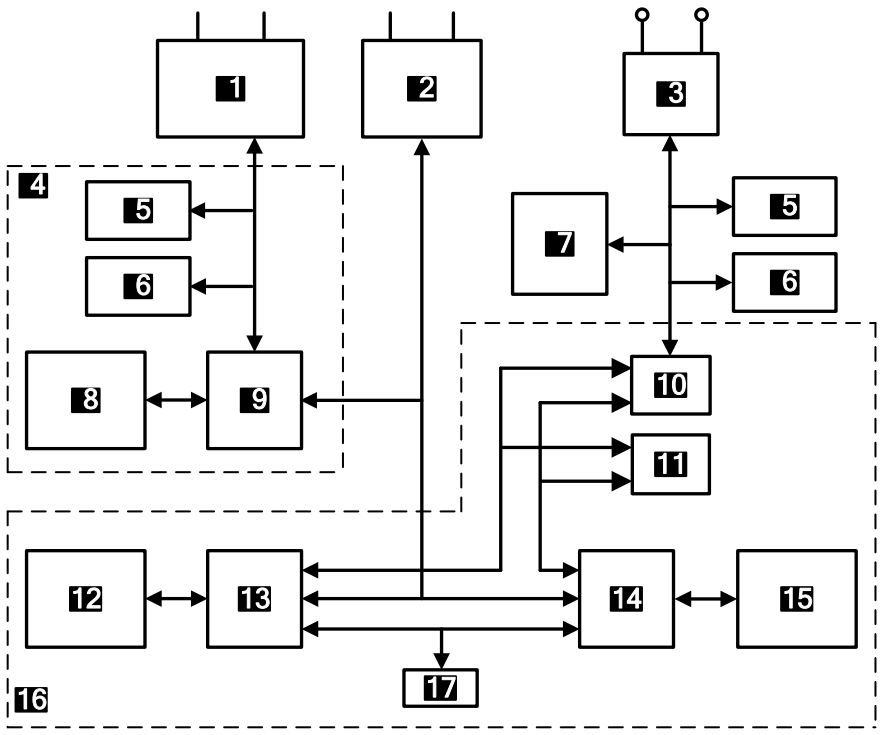
4.1 Modules d'alimentation

L'alimentation des systèmes HIMatrix doit provenir des modules d'alimentation qui fournissent aux commandes et E/S déportées une basse tension de 24 V.

Le respect des limites de tension du contrôleur assure le fonctionnement conforme du contrôleur.

4.2 Description du fonctionnement du processeur

Le processeur est le composant central du contrôleur. Il se compose des blocs de fonctions suivants :



1 Interfaces bus de terrain
2 Interfaces Ethernet
3 Module de bus E/S
4 Système de communication
5 NVSRAM
6 Flash
7 V_{CC} et surveillance de température
8 SDRAM du système de communication
9 Processeur du système de communication
10 Mécanisme de comparaison
11 Chien de garde
12 SDRAM 1 du processeur
13 Processeur 1 du système processeur
14 Processeur 2 du système processeur
15 SDRAM 2 du système processeur
16 Système processeur de sécurité
17 Horloge temps réel

Figure 1 : Représentation des blocs de fonctions fondée sur le processeur 03 de la F60

Caractéristiques du système processeur

- Deux microprocesseurs synchrones (processeur 1 et processeur 2)
- Chaque processeur a sa propre mémoire SDRAM
- Mécanisme de comparaison testable pour tous les accès externes des deux microprocesseurs.
- En cas de défaillance, le chien de garde se met en état de sécurité.
- Flash EPROM, la mémoire pour les systèmes d'exploitation et le programme utilisateur, appropriée pour un minimum de 100 000 cycles de mémoire.
- Mémoire de données dans NVSRAM.
- Goldcap pour la mise en mémoire tampon de la date/de l'heure.
- Processeur de communication pour connexions bus de terrain et Ethernet.
- Interface pour échange des données entre les automates, commandes F60 et le PADT, basé sur Ethernet.
- Interface(s) en option pour échange de données par bus de terrain.
- Signalisation des états du système par les LEDs.
- Logique bus E/S pour connexions avec les modules d'E/S.
- Chien de garde de sécurité (WD).
- Surveillance de module d'alimentation, testable (1,8 V CC / 3,3 V CC).
- Surveillance de la température.

4.3 Tests automatiques

Les dispositifs de tests automatiques détectent les défaillances uniques susceptibles de provoquer un état de fonctionnement critique pour la sécurité et déclenchent, pendant l'intervalle de sécurité du contrôleur, des réponses prédéfinies aux erreurs mettant en sécurité les composants défaillants.

Les principaux tests fonctionnels automatiques pour les systèmes processeur de sécurité sont brièvement expliquées ci-après.

4.3.1 Test de microprocesseur

Portée du test :

- Tous les ordres et types d'adressage
- L'inscriptibilité des drapeaux et les commandes qu'ils génèrent.
- l'inscriptibilité et la diaphonie des registres.

4.3.2 Test des zones de mémoire

Le système d'exploitation, le programme utilisateur, les constantes et les paramètres ainsi que les données variables sont sauvegardés dans les zones de mémoire des deux processeurs et sont testés par un mécanisme de comparaison.

4.3.3 Zones de mémoire sécurisées

Le système d'exploitation, le programme utilisateur et la zone des paramètres sont chacun sauvegardés dans une mémoire. Ils sont protégés en écriture et par un test CRC.

4.3.4 Test de la RAM

Les zones de RAM modifiables sont vérifiées, en particulier pour le blocage (stuck at) et la diaphonie, par un test d'écriture et de lecture.

4.3.5 Test du chien de garde

Le signal du chien de garde est désactivé s'il n'est pas déclenché par les deux processeurs dans un intervalle défini ou si le test du mécanisme de comparaison échoue. Un test supplémentaire détermine la capacité de désactiver le signal du chien de garde.

4.3.6 Test du bus E/S dans le contrôleur

La connexion entre le processeur et les entrées ainsi que les sorties correspondantes (modules E/S) est testée.

4.4 Réponses aux erreurs dans le système processeur

Un mécanisme de comparaison dans le système processeur vérifie en permanence que les données du microprocesseur 1 sont identiques à celles du microprocesseur 2. Si les données ne sont pas identiques ou si les tests fonctionnels dans le processeur trouvent une erreur, le signal du chien de garde se désactive. Cela signifie que le contrôleur ne traite plus aucun signal d'entrée et que les sorties sont mises hors tension.

La commande 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.

4.5 Diagnostic d'erreurs

Chaque module F60 dispose d'une LED d'affichage des défauts en cas de dysfonctionnement du module ou du circuit externe. En cas de dérangement, cela permet un diagnostic rapide des erreurs d'un module signalé comme défectueux.

Dans les systèmes compacts F1.., F2.., F3.., ces erreurs sont résumées et s'affichent dans un seul message de défaut.

En outre, une évaluation de différentes variables de système des entrées et sorties ou du contrôleur peut s'effectuer dans le programme utilisateur.

Une signalisation d'erreur ne se produit que lorsque l'erreur n'entrave pas la communication avec le système de processeur, à savoir qu'elle permet encore une évaluation via le système de processeur.

Dans le programme utilisateur, la logique peut analyser les codes d'erreur de tous les signaux d'entrée et de sortie ainsi que des variables système.

Un enregistrement du diagnostic complet relatif au comportement du système et des erreurs détectées est stocké dans la mémoire de diagnostic des systèmes du processeur et de communication. 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 au manuel du système HI 800 641 FR.

5 Entrées

Vue d'ensemble des entrées du système HIMatrix :

Appareil / Module	Type	Quantité	de sécurité	Sans effet rétroactif	À isolation électrique
Systèmes compacts					
F30 03	Numérique	20	•	•	– [1)]
F35 03	Numérique	24	•	•	– [1)]
	Compteur 24 bits	2	•	•	– [1)]
	Analogique	8	•	•	– [1)]
F1 DI 16 01	Numérique	16	•	•	– [1)]
F3 DIO 8/8 01	Numérique	8	•	•	– [1)]
F3 DIO 16/8 01	Numérique	16	•	•	– [1)]
F3 AIO 8/4 01	Analogique	8	•	•	– [1)]
F3 DIO 20/8 02	Numérique	20	•	•	– [1)]
Système modulaire F60					
DIO 24/16 01	Numérique	24	•	•	•
DI 32 01 (configurable avec Line Control)	Numérique	32	•	•	•
DI 24 01 (110 V)	Numérique	24	•	•	•
CIO 2/4 01	Compteur 24 bits	2	•	•	•
AI 8 01	Analogique	8	•	•	•
MI 24 01	Analogique ou Tout Ou Rien	24	•	•	•
[1)] Potentiel de référence L-					

Tableau 11 : Vue d'ensemble des entrées

5.1 Généralités

Il est possible d'utiliser des entrées relatives à la sécurité pour des signaux relatifs à la sécurité ou non relatifs à la sécurité.

Les commandes fournissent les informations d'état et d'erreur de la manière suivante :

- Par LED de diagnostic des automates et modules.
- Par des variables système que le programme utilisateur peut analyser.
- Par des entrées dans la mémoire de diagnostic que le PADT peut lire.

Pendant le fonctionnement, les modules d'entrée relatifs à la sécurité effectuent un test automatique cyclique de grande qualité. Ces procédures de test ont la certification TÜV et contrôle le fonctionnement sécurisé de chaque module.

Pour une partie infime des défaillances de composants n'affectant pas la sécurité, aucune information de diagnostic n'est fournie.

5.2 Sécurité des capteurs, encodeurs et transmetteurs

Dans une application relative à la sécurité, le contrôleur 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.

5.3 Réaction en cas de défauts

Si les tests fonctionnels constatent une erreur, cela déclenche les réactions suivantes :

- Le programme utilisateur traite la valeur initiale des variables globales pour les entrées.
- Le code d'erreur et d'autres variables de système peuvent être utilisés pour programmer des réactions personnalisées aux erreurs selon les utilisateurs. Pour plus de détails, se référer au manuel du module correspondant.

En cas d'erreur, un système compact active la LED *ERROR* et un module F60 active la LED *ERR*.

5.4 Entrées "Tout Ou Rien" relatives à la sécurité

Sauf spécifications contraires, les caractéristiques décrites s'appliquent tant aux canaux d'entrées Tout Ou Rien du F60 qu'aux canaux d'entrées Tout Ou Rien de tous les systèmes compacts.

5.4.1 Généralités

Les entrées Tout Ou Rien sont lues une fois dans chaque cycle et enregistrées en interne ; leur sûreté de fonctionnement est testée de manière cyclique.

Dans certaines circonstances, les signaux d'entrée plus courts que l'intervalle de temps entre deux balayages (c.-à-d. plus courts que la durée d'un cycle) ne sont pas enregistrés.

5.4.2 Procédures de test

Les procédures de test vérifient que les canaux d'entrée sont capables de relier les deux niveaux de signaux (bas et haut) indépendamment des signaux d'entrée émis. Ce test fonctionnel s'effectue chaque fois que des signaux d'entrée sont lus.

5.4.3 Crêtes sur entrées numériques

En raison de la courte durée de cycle des systèmes HIMatrix, les entrées Tout Ou Rien peuvent lire une impulsion de crête selon EN 61000-4-5 comme un niveau haut de courte durée.

Les mesures suivantes sont destinées à éviter des dysfonctionnements dans des environnements sujets aux crêtes :

1. Installation de lignes d'entrée blindées
2. Programmation de suppression d'impulsions parasites dans le programme utilisateur. Un signal doit être en suspens pendant au moins deux cycles avant d'être évalué. Le temps de réponse maximal s'en trouve rallongé.

i On peut s'abstenir des mesures ci-dessus si la conception de l'installation permet d'exclure des crêtes dans le système.

La configuration suppose la mise en œuvre de mesures de protection relatives à la surtension, la foudre, la mise à la terre et le câblage de l'installation en application des indications du manuel de système HI 800 641 FR et des normes concernées.

5.4.4 Entrées Tout Ou Rien paramétrables

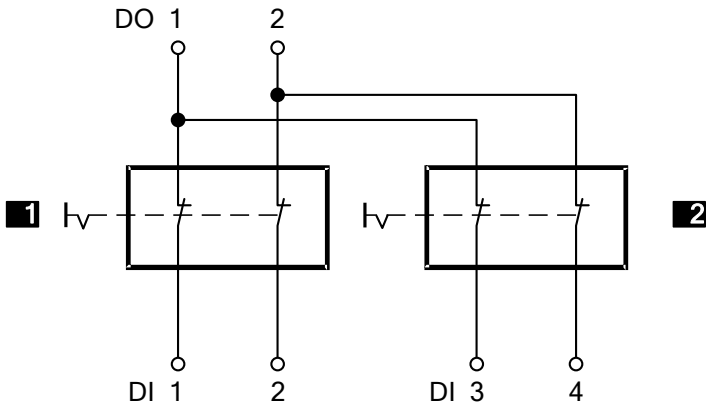
Les entrées tout ou riens du contrôleur F35 03 et du module MI 24 01 travaillent selon le principe des entrées analogiques, mais fournissent une valeur numérique lorsque des seuils de commutation sont configurés.

Les procédures de test et les fonctions de sécurité indiquées pour les entrées analogiques sont également applicables aux entrées Tout Ou Rien comme mentionné dans le chapitre 5.5.1.

5.4.5 Line Control

Line Control sert à détecter les courts-circuits et interruptions de ligne, entre autres sur les automates d'arrêt d'urgence. Elle peut être configurée dans des systèmes HIMatrix à entrées Tout Ou Rien (sauf avec le contrôleur F35 03 et le module MI 24 01).

Pour ce faire, connecter comme suit les sorties Tout Ou Rien du système avec les entrées Tout Ou Rien du même système (exemple) :

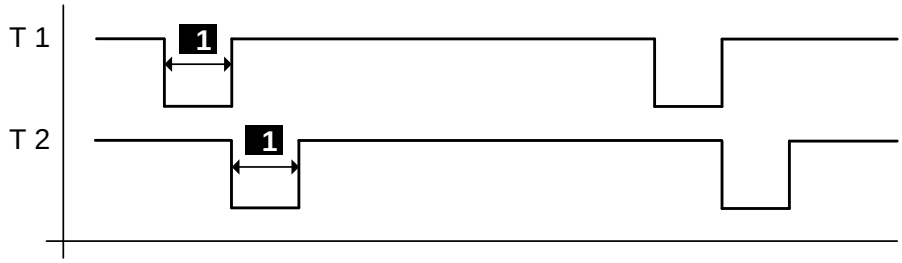


1 ARR.URG 1
2 ARR.URG 2

Interrupteur d'arrêt d'urgence répondant aux normes EN 60947-5-1 et EN 60947-5-5

Figure 2 : Line Control

La commande synchronise les sorties Tout Ou Rien afin de détecter un court-circuit ou une rupture de ligne des entrées Tout Ou Rien. Pour ce faire, paramétrer dans SILworX la variable de système *Value [BOOL] ->*. Les sorties à impulsions peuvent être affectées à n'importe quelles entrées Tout Ou Rien.



1 Configurable 5...2000 µs

Figure 3 : Signaux d'horloge T1, T2

Un code d'erreur (analysable) est généré lorsque les erreurs suivantes se produisent :

- Court-circuit transversal entre deux lignes parallèles,
- Permutation de deux lignes (par ex. DO 2 après DI 3),
- Défaut à la terre de l'une des lignes (uniquement en cas de potentiel de référence mis à la terre),
- Rupture de ligne ou ouverture des contacts.

Pour plus de détails et une description de la configuration de Line Control, consulter le manuel du système HI 800 641 FR.

5.5 Entrées analogiques relatives à la sécurité (F35 03, F3 AIO 8/4 01 et F60)

Des canaux d'entrée analogiques transforment les courants d'entrée mesurés en une valeur INTEGER. Les valeurs sont disponibles pour le programme utilisateur dans les variables assignées comme suit aux variables de système -> *Value [INT]* :

Les plages de valeurs des entrées sont fonction de l'appareil ou du module:

- Contrôleur F35 03 :

Voies d'entrée	Procédé de mesure	Courant, tension	Plage de mesures dans application	
			FS1000 [1]	FS2000 [1]
8	unipolaire	0…+10 V	0…1000	0…2000
8	unipolaire	0–20 mA	0…500 [2] 0…1000 [3]	0…1000 [2] 0…2000 [3]

[1] réglable par sélection de types dans PADT
[2] avec adapteur de shunt externe 250 Ω
[3] avec adapteur de shunt externe 500 Ω

Tableau 12 : Entrées analogiques du contrôleur F35

- Module d'E/S déportées F3 AIO 8/4 01 :

Voies d'entrée	Procédé de mesure	Courant, tension	Plage de mesures dans application
8	unipolaire	0…+10 V	0…2000
8	unipolaire	0/4…20 mA	0…1000 [1] 0…2000 [2]

[1] avec adapteur de shunt externe 250 Ω
[2] avec adapteur de shunt externe 500 Ω

Tableau 13 : Entrées analogiques du module d'E/S déportées F3 AIO 8/4 01

- Contrôleur F60 :

Voies d'entrée	Procédé de mesure	Courant, tension	Plage de mesures dans application	
			FS1000 [1]	FS2000 [1]
AI 8 01				
8	unipolaire	-10…+10 V	-1000…1000	-2000…2000
8	unipolaire	0–20 mA	0…1000 [3]	0…2000 [3]
8	unipolaire	0–20 mA	0…500 [2]	0…1000 [2]
4	bipolaire	-10…+10 V	-1000…1000	-2000…2000
MI 24 01				
	unipolaire	0–20 mA	0…2000 [4]	

[1] réglable par sélection de types dans PADT (F60)
[2] avec shunt de mesure externe 250 Ω
[3] avec shunt de mesure externe 500 Ω (précision 0,05 %, 1 W). N'est plus disponible chez HIMA.
[4] shunts de mesure internes

Tableau 14 : Entrées analogiques du contrôleur F60

Le module AI 8 01 du HIMatrix F60 peut être configuré dans le programme utilisateur pour huit fonctions unipolaires ou quatre fonctions bipolaires. Il est cependant interdit de combiner les fonctions d'un module.

Les entrées analogiques du contrôleur F35 03, des E/S déportées F3 AIO 8/4 01 et du module AI 8 01 fonctionne avec mesure de tension. Les entrées Tout Ou Rien du F35 03 et du F3 AIO 8/4 01 peuvent être utilisées pour surveiller les interruptions de ligne des sorties Tout

Ou Rien du propre système F35 03 ou d'autres commandes HIMatrix. Pour en savoir plus, se reporter aux manuels des commandes HIMatrix correspondantes.

Si le système ne surveille pas la ligne, n'importe quel signal d'entrée est traité sur une sortie de haute impédance en cas d'interruption de ligne. La valeur résultant de cette tension d'entrée sinusoïdale n'est pas fiable, en cas d'entrées de tension, les canaux doivent être connectés à une résistance 10 kΩ. La résistance interne de la source doit être prise en compte.

Afin de mesurer le courant, le shunt est connecté en parallèle à une entrée ; de cette manière une résistance de 10 kΩ n'est pas nécessaire. n'est pas nécessaire.

Les entrées du module MI 24 01 sont, en raison de shunt interne, des entrées de courant et ne peuvent être utilisées comme entrées de tension.

Si les canaux d'entrée ne sont pas utilisés, l'entrée de mesure doit être connectée au potentiel de référence. Des influences négatives sur d'autres canaux peuvent ainsi être évitées en cas d'interruption de ligne (valeur de tension flottante). Il suffit de ne pas assigner une variable globale aux entrées inutilisées.

5.5.1 Procédures de test

Les valeurs analogiques sont traitées en parallèle par le biais de deux multiplexeurs et de deux convertisseurs analogiques/Tout Ou Rien avec une résolution à 12 bits et les résultats sont comparés. En outre, des valeurs tests utilisées par les convertisseurs analogiques/Tout Ou Rien existants, sont reconverties en valeurs numériques puis comparées à la valeur par défaut.

5.6 Compteurs de sécurité (F35 03 et F60)

Sauf indication contraire, les points cités s'appliquent tant au module compteur des F60 qu'aux compteurs des F35 03.

5.6.1 Généralités

Un canal compteur est paramétrable en mode compteur ou décompteur rapide à une résolution de 24 bits ou en mode décodeur en code Gray.

S'il est utilisé comme compteur/décompteur rapide, l'impulsion du signal d'entrée et d'entrée de sens de comptage est nécessaire au sein de l'application. La réinitialisation se fait seulement au sein du programme utilisateur.

Les encodeurs des compteurs ont les résolutions suivantes :

- F60 CIO 2/4 01 : résolution de 4 ou 8 bits.
- F35 03 : résolution de 3 ou 6 bits.

Une réinitialisation est possible.

Deux entrées 4 bits indépendantes l'une de l'autre peuvent seulement être connectées a une entrée 8 bits (exemple du F60) à l'aide du programme utilisateur. Une option de commutation n'est pas prévue à cette fin.

La fonction codeur surveille la modification de la configuration binaire au niveau des canaux d'entrée. Les configurations binaires des entrées sont directement transférées au programme utilisateur. Elles sont représentées dans le PADT sous la forme de chiffres décimaux correspondant à la configuration binaire (*Counter[0x].Value*).

En fonction de l'application, ce chiffre (équivalent à la configuration binaire du code de Gray) peut, p. ex., être converti à la valeur décimale correspondante.

5.7 Liste de contrôle pour les entrées Tout Ou Rien de sécurité

HIMA recommande d'utiliser les listes de vérification disponibles pour l'étude, la programmation et la mise en service d'entrées de sécurité. La liste de vérification peut être utilisée comme documentation technique de conception et atteste une planification exécutée avec soin.

Pour chaque canal d'entrée relatif à la sécurité utilisé dans un système, il convient de remplir la liste de vérification afin d'assurer le correct suivi des exigences à satisfaire dans le cadre d'une étude ou d'une mise en service. 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 connexions entre le câblage externe et le programme utilisateur.

La liste de vérification *HIMatrix_Checklist_Inputs.doc* est un document disponible au format Microsoft© Word©. Le fichier zip *HIMatrix_Checklists.zip* contient toutes les listes de contrôle et peut être téléchargé sur les sites Internet HIMA www.hima.de et www.hima.com.

6 Sorties

Vue d'ensemble des sorties du système HIMatrix :

Automates	Type	Quantité	de sécurité	isolées galvaniquement
Systèmes compacts				
F30 03 (configurable pour Line Control)	Numérique	8	•	–[1)]
F35 03	Numérique	8	•	–[1)]
F1 DI 16 01	Cycle	4	-	–[1)]
F2 DO 4 01	Numérique	4	•	–[1)]
F2 DO 8 01	Relais	8	•	
F2 DO 16 01	Numérique	16	•	–[1)]
F2 DO 16 02	Relais	16	•	
F3 DIO 8/8 01	Numérique unipolaire	8	•	–[1)]
	Numérique bipolaire	2		
F3 DIO 16/8 01	Numérique unipolaire	16	•	–[1)]
	Numérique bipolaire	8		
F3 AIO 8/4 01	Analogique	4	-	–[1)]
F3 DIO 20/8 02 (configurable pour Line Control)	Numérique	8	•	–[1)]
Système modulaire F60				
DIO 24/16 01 (configurable pour Line Control)	Numérique	16	•	
CIO 2/4 01	Numérique	4	•	
[1)] Potentiel de référence L-				

Tableau 15 : Vue d'ensemble des sorties

6.1 Généralités

Le contrôleur écrit sur les sorties relatives à la sécurité une fois par cycle, les signaux de sortie sont lus et comparés avec les données de sortie fixées.

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

Les canaux de sortie relatifs à la sécurité sont équipés de trois interrupteurs testables connectés en série. Le deuxième moyen de mise à l'arrêt indépendant requis pour la technique de sécurité est ainsi intégré au module de sortie. En cas de défaut, cette mise à l'arrêt de sécurité intégrée désactive tous les canaux du module de sortie défectueux de manière sécurisée (état hors tension).

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

Cette fonction est effective pour toutes les sorties Tout Ou Rien et sorties relais des commandes.

L'utilisation du code d'erreur correspondant offre des possibilités supplémentaires de configuration des réponses aux erreurs dans le programme utilisateur.

6.2 Sécurité des actionneurs

Dans une application relative à la sécurité, le contrôleur 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 actionneurs, se reporter par exemple à la norme IEC 61511-1, section 11.4.

6.3 Réaction en cas de défauts

Si les tests fonctionnels constatent une erreur au niveau des sorties, le contrôleur désactive la sortie concernée en cas d'erreur et la met donc en état de sécurité.

Le code d'erreur et d'autres variables de système peuvent être utilisés pour programmer des réactions personnalisées aux erreurs selon les utilisateurs. Pour plus de détails, se référer au manuel du module correspondant.

En cas d'erreur, un système compact active la LED *ERROR* et un module F60 active la LED *ERR*.

6.4 Sorties Tout Ou Rien de sécurité

Les points spécifiés s'appliquent autant aux canaux des sorties Tout Ou Rien des modules F60 qu'aux canaux des sorties Tout Ou Rien des systèmes compacts. Dans les deux cas, les modules relais font exception à cette règle, sauf spécifications contraires.

6.4.1 Procédures de test pour sorties numériques

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

- Relecture du signal de sortie de l'amplificateur de commutation. Le seuil de commutation d'un signal de niveau bas ayant été relu est de 2 V. Les diodes utilisées empêchent le renvoi des signaux.
- Contrôle de la mise à l'arrêt sécurisée redondante.
- En tant que test d'arrière-plan, un test de mise à l'arrêt des sorties est réalisé tous les 200 µs max. L'intervalle minimum entre deux tests est de ≥ 20 secondes.

La tension d'alimentation de l'ensemble du système est surveillée. Toutes les sorties sont mises hors tension en cas de tension insuffisante < 13 V.

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

En cas de court-circuit de la sortie vers L- ou de surcharge, la testabilité du module est maintenue. Une désactivation via la mise à l'arrêt sécurisée n'est pas nécessaire.

Le contrôleur surveille le courant global consommé de l'appareil ou du module et bascule tous les canaux de sortie à l'état de sécurité en cas de dépassement du seuil.

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.

6.4.3 Line Control

Le contrôleur peut cadencer des sorties Tout Ou Rien ou des sorties spéciales à impulsions relatives à la sécurité et les utiliser avec des entrées Tout Ou Rien relatives à la sécurité du même système (sauf avec des entrées Tout Ou Rien de F35 ou F60 MI 24 01) pour une détection de courts-circuits et d'interruptions de ligne, voir chapitre 5.4.5.

REMARQUE

Dysfonctionnements possibles des actionneurs raccordés !

Les sorties cycliques ne doivent pas être utilisées comme des sorties relatives à la sécurité, par ex. pour la commande d'actionneurs relatifs à la sécurité !

Les sorties de relais ne peuvent pas être utilisées comme sorties cycliques.

6.5 Sorties Tout Ou Rien de sécurité bipolaires

Les caractéristiques décrites ici font référence aux sorties Tout Ou Rien bipolaires des modules d'E/S déportées F3 DIO 8/8 01 et F3 DIO 16/8 01.

Les automates se testent automatiquement pendant le fonctionnement. Les principales fonctions de ces tests sont :

- Relecture du signal de sortie de l'amplificateur de commutation. Les diodes utilisées empêchent le renvoi des signaux.
- Contrôle de la mise à l'arrêt sécurisée redondante
- En tant que test d'arrière-plan, un test de mise à l'arrêt des sorties est réalisé tous les 200 µs max. L'intervalle minimum entre deux tests est de ≥ 20 secondes.
- Diagnostic de ligne pour connexion bipolaire
  F3 DIO 16/8 01 :
  - Court-circuit contre L+, L-
  - Court circuit entre connexions bipolaires
  - Interruption de ligne dans une des 2 connexions bipolaires

  F3 DIO 8/8 01 :
  - Court-circuit contre L+, L-

Le système surveille sa tension de service et commande toutes les sorties en cas de sous-tension < 13 V.

Dans le cas d'une connexion bipolaire, tenir compte des remarques suivantes :

i Possibilité d'une activation involontaire d'un relais ou d'un actionneur raccordé à la sortie !

En cas d'applications dans la sécurité des machines, désactiver les sorties DO+, DO- pour la détection de courts-circuits.

i Si les exigences ci-dessus ne peuvent être remplies, tenir compte du cas suivant :

En cas de court-circuit de DO- vers L-, un relais peut s'exciter ou un autre actionneur basculer dans un autre état de communication.

Motif : pendant l'écoulement du temps de surveillance pour le diagnostic de ligne, le consommateur (relais, actionneur commutant) enregistre un niveau de tension de 24 V (sortie DO+) de sorte qu'il pourrait absorber une énergie électrique suffisante pour passer à un autre état.

Le temps de surveillance doit être paramétré de sorte qu'un actionneur d'impulsion de test pour le diagnostic de ligne ne puisse être activé.

i Possibilité de dysfonctionnement de la détection d'interruption de ligne !

En cas de connexion bipolaire, ne pas connecter d'entrée DI à une sortie DO. Cela empêcherait la détection d'une rupture de ligne.

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

En cas de court-circuit de la sortie vers L-, L+ ou de surcharge, la testabilité du module est maintenue. Une désactivation via la mise à l'arrêt sécurisée n'est pas nécessaire.

Le courant absorbé total de l'appareil est contrôlé. En cas de dépassement du seuil, l'appareil bascule tous les canaux à l'état de sécurité.

Dans cet état, l'appareil contrôle de manière cyclique, à des intervalles de quelques secondes, si la surcharge est encore présente. Si l'état est normal, l'appareil actionne à nouveau les sorties.

6.6 Sorties relais

De par leur fonction, les sorties relais sont comparables aux sorties Tout Ou Rien, néanmoins elles sont galvaniquement isolées et plus résistantes à la tension.

6.6.1 Tests fonctionnels pour sorties relais

L'appareil ou le module teste automatiquement ses sorties 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.

Le système surveille sa tension de service et commande toutes les sorties en cas de sous-tension < 13 V.

Dans le cas du module DO 8 01 et des modules d'E/S déportées F2 DO 8 01 et F2 DO 16 02, les sorties sont équipées de trois relais de sécurité :

- Deux relais avec contacts à guidage forcé
- Un relais standard

Cela permet d'utiliser les sorties pour des mises à l'arrêt sécurisées.

6.7 Sorties analogiques de sécurité (F60)

Le module AO 8 01 a son propre système microprocesseur de sécurité 1oo2 A/N avec communication sécurisée. Les sorties analogiques sont définies une fois par cycle et leurs valeurs sont enregistrées. Le module teste lui-même sa fonction.

Les interrupteurs DIP sur les sorties analogiques du module peuvent être utilisés pour définir les sorties sous tension ou courant de sortie. Pour ce faire, s'assurer que leurs réglages sont compatibles avec l'utilisation dans le système et le paramétrage dans le programme utilisateur. La non-observation de ces points impliquerait un dysfonctionnement du module.

REMARQUE

Dysfonctionnement du module

Avant l'utilisation du module dans le système, vérifier :

- **Les paramètres de commutation DIP du module.**
- **Le paramétrage du module dans le programme utilisateur.**

Selon le choix du type d'appareil (...FS1000, ...FS2000), lors de la configuration, différentes valeurs sont à prendre en compte dans la logique pour maintenir des valeurs de sortie identiques (voir par ex. manuel AO 8 01, HI 800 196 D).

Les sorties analogiques sont galvaniquement connectées entre elles deux par deux :

- Sorties 1 et 2
- Sorties 3 et 4.
- Sorties 5 et 6.
- Sorties 7 et 8.

Les circuits de sorties analogiques disposent d'une surveillance de la tension ou du voltage, de canaux test et de relecture (même pour des circuits de sortie parallèle), ainsi que de deux interrupteurs de sécurité supplémentaires pour la mise à l'arrêt sécurisée des circuits de sortie en cas d'erreur. Cela permet de basculer à l'état de sécurité (courant de sortie : 0 mA, tension de sortie : 0 V).

6.7.1 Procédures de test

Le module est testé automatiquement pendant le fonctionnement. Les principales fonctions de ces tests sont :

- Double relecture du signal de sortie.
- Test de chevauchement (diaphotie) entre les sorties.
- Contrôle de la mise à l'arrêt sécurisée intégrée.

6.8 Sorties analogiques avec mise hors tension de sécurité (F3 AIO 8/4 01)

Les modules d'E/S déportées définissent les sorties analogiques une fois par cycle et leurs valeurs sont enregistrées en interne.

Les sorties ne sont pas relatives à la sécurité, mais elles peuvent être mises hors tension conjointement.

Pour atteindre le niveau SIL 4, les valeurs de sortie doivent être relues via des entrées analogiques relatives à la sécurité, puis analysées dans le programme utilisateur. Les réactions aux valeurs de sorties erronées doivent y être également définies.

6.8.1 Procédures de test

Le module d'E/S déportées teste les deux interrupteurs de sécurité destinés à désactiver automatiquement les quatre sorties pendant le fonctionnement.

6.9 Liste de contrôle pour les sorties de sécurité

HIMA recommande d'utiliser les listes de vérification disponibles pour l'étude, la programmation et la mise en service d'entrées relatives à la sécurité. La liste de vérification peut être utilisée comme documentation technique de conception et atteste une planification exécutée avec soin.

Pour chaque canal de sortie relatif à la sécurité utilisé dans un système, il convient de remplir la liste de vérification afin d'assurer le correct suivi des exigences à satisfaire dans le cadre d'une étude ou d'une mise en service. 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 connexions entre le câblage externe et le programme utilisateur.

La liste de vérification *HIMatrix_Checklist_Outputs.doc* est un document disponible au format Microsoft© Word©. Le fichier zip *HIMatrix_Checklists.zip* contient toutes les listes de contrôle et peut être téléchargé sur les sites Internet HIMA www.hima.de et www.hima.com.

7 Logiciel pour systèmes HIMatrix

Le logiciel pour les automates de sécurité des systèmes HIMatrix s'articule autour des blocs suivants :

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

Le *système d'exploitation* est chargé dans la partie centrale (CPU) du contrôleur. Il est conseillé d'utiliser la dernière version valide pour les applications relatives à la sécurité.

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.

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

Chaque système d'exploitation homologué est caractérisé par sa désignation. La révision et la signature CRC permettent de mieux le distinguer. 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 par HIMA conjointement avec le TÜV.

L'outil de programmation SILworX permet de lire la version actuelle du système d'exploitation. L'utilisateur est tenu d'effectuer un contrôle, voir chapitre 7.6.

7.2 Mode opérationnel et fonctions du système d'exploitation

Le système d'exploitation utilise le programme utilisateur de manière cyclique. Les fonctions suivantes sont alors exécutées de manière très simplifiée :

- Lecture des données d'entrée.
- Traitement des fonctions logiques programmées conformément à la norme IEC 61131-3.
- Écriture des données de sortie.

À cela s'ajoutent les fonctions principales suivantes :

- Autotests étendus.
- Tests des modules d'E/S pendant le fonctionnement.
- Transmission des données.
- Diagnostic.

7.3 Aspects relatifs à la sécurité pour la programmation

7.3.1 Concept de sécurité de l'outil de programmation

Le concept de sécurité de l'outil de programmation SILworX :

- Lorsque l'outil de programmation est installé, un control par Checksum CRC permet de garantir l'integrité sur l'ensemble des programmes lors de la transmission entre le fabriquant et l'utilisateur.
- L'outil de programmation exécute des contrôles de cohérence afin de réduire les erreurs de saisie.
- Une double compilation avec comparaison finale des sommes de contrôle CRC atteste que les altérations de données, dues à des dysfonctionnements temporaires du PC utilisé, sont détectées.
- L'outil de programmation et les mesures définies dans le présent manuel de sécurité rendent hautement improbable qu'un code correctement généré d'un point de vue sémantique et syntaxique contienne des erreurs systémiques non détectées survenues lors de la création du code.

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

- Vérification de la correcte application de la fonction du contrôleur à l'appui des données et flux des signaux.
- Test fonctionnel complet de la logique au moyen de tests (voir chapitre 7.3.2).

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 utiliser pour déterminer et indiquer quels changements ont été effectués par rapport à la version antérieure :

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

7.3.2 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 (à savoir entrée, concaténation du point de vue de l'application et sortie) est suffisant.

Des tests élémentaires sont également à effectuer pour l'évaluation numérique des formules. Sont recommandés des tests de classes d'équivalence, à savoir des tests réalisés dans des plages de valeurs définies, aux limites ou dans des plages 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 d'exécuter une simulation active avec sources. HIMA recommande de procéder à une simulation active avec des sources. Cela atteste un câblage correct des capteurs et actionneurs du système, y compris pour ceux connectés par le biais de modules 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 concerne la mise en œuvre d'un programme utilisateur ainsi que ses modifications.

7.3.3 Archivage d'un projet

Après chaque chargement du programme, HIMA recommande d'archiver le projet dans le contrôleur.

SILworX crée un projet dans un fichier de projet. Il est recommandé de sauvegarder ce dernier par ex. sur un support d'enregistrement.

i Si le fichier de projet est supprimé ou endommagé, il n'est plus possible d'accéder au programme et aux variables d'un automate !

C'est pourquoi il est fortement conseillé d'archiver et de classer les données sur un deuxième support de données !

7.3.4 Possibilité d'identification au programme et à la configuration

Les programmes utilisateurs sont clairement identifiés dans les CRC de configuration du projet. Ce dernier peut être comparé au CRC de configuration du projet chargé.

Pour s'assurer que le fichier de projet sauvegardé n'a pas été modifié, compiler la ressource contenue et comparer le CRC de configuration avec le CRC de configuration chargé. Celui-ci peut s'afficher dans SILworX.

i Lors de la première mise en service ou d'une modification du programme utilisateur d'un contrôleur de sécurité, effectuer un test fonctionnel exhaustif.

Créer une archive de projet.

7.4 Paramètres de la ressource

⚠ AVERTISSEMENT

Risque de dommages corporels lié à une configuration défectueuse !

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

Ces paramètres sont :

- **Rack ID, voir le manuel du système (HIMatrix System Manual Compact Systems HI 800 641 FR).**
- **Les paramètres signalées dans le Tableau 16 comme étant des paramètres de sécurité.**

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

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

7.4.1 Paramètres système de la ressource

Les paramètres système de la ressource déterminent le comportement du contrôleur pendant le fonctionnement et se règlent dans SILworX, dans la boîte de dialogue *Properties* de la ressource. Les paramètres peuvent aussi être modifiés en ligne, sauf la *Minimum Configuration Version*.

Paramètre	S [1)]	Description	Paramétrage pour un fonctionnement sécurisé
Name	-	Nom de la ressource.	À convenance
System ID [SRS]	Y	ID du système de la ressource 1...65 535, valeur par défaut : 60 000 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 !	Valeur significative au sein du réseau des commandes. Ce réseau comprend toutes les commandes susceptibles d'être reliées entre elles.
Safety Time [ms]	Y	Temps de sécurité en millisecondes 20...22 500 ms, valeur par défaut : 600 ms pour les commandes, 400 ms pour les modules d'E/S.	Spécifique à l'application
Watchdog Time [ms]	Y	Durée Watchdog Time en millisecondes : 4...5000 ms. Valeur par défaut : 200 ms pour les commandes, 100 ms pour les modules d'E/S.	Spécifique à l'application
Target Cycle Time [ms]	N	Durée de cycle souhaitée ou maximale, voir *Target Cycle Time Mode,* 0...5000 ms. La valeur de la durée maximale du cycle ne doit pas dépasser la valeur : *durée Watchdog Time définie [ms]* – valeur minimale définie pour la durée *Watchdog Time [ms]*. Autrement, c'est l'automate qui la définit. Valeur par défaut 0 ms Si la valeur par défaut est définie à 0 ms, la durée de cycle n'est pas prise en compte. Voir chapitre 7.4.1.1.	Spécifique à l'application
Target Cycle Time Mode	N	Utilisation de *Target Cycle Time [ms]*, voir chapitre 7.4.1.1. Valeur par défaut : *Fixed-tolerant*	Spécifique à l'application
Multitasking Mode	N	Mode 1 La durée d'un cycle du processeur est basée sur le temps d'exécution nécessaire de tous les programmes utilisateurs.	Spécifique à l'application
		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.	
Max.Com. Time Slice ASYNC [ms]	N	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, valeur par défaut : 60 ms.	Spécifique à l'application
Max. Duration of Configuration Connections [ms]	N	Il définit la durée disponible dans un cycle de processeur pour traiter les connexions de configuration de processus, 2...3500 ms, voir chapitre 7.4.1.2. Valeur par défaut 12 ms	Spécifique à l'application
Maximum System Bus Latency [µs]	N	Non applicable aux commandes HIMatrix ! (Valeur par défaut 0 µs).	-

Paramètre	S [1)]	Description	Paramétrage pour un fonctionnement sécurisé
Allow Online Settings	Y	Indique si les paramètres et fonctions en ligne suivants peuvent être modifiés avec le PADT : ▪ *System ID.* ▪ *Autostart.* ▪ *Global Forcing Allowed.* ▪ *Global Force Timeout Reaction.* ▪ *Load Allowed.* ▪ *Reload Allowed.* ▪ *Start Allowed.* ▪ *Multitasking Mode.* ▪ *Démarrage rapide.* ▪ Régler le mode Mono / Redondance. ▪ Module : régler la date / l'heure. ▪ Tous les paramètres du programme utilisateur. L'action sur les autres paramètres est décrite au chapitre 7.4.1.3.	OFF, recommandé
		ON : Les paramètres et fonctions en ligne peuvent être modifiés en ligne.	
		OFF : Les paramètres et fonctions en ligne ne peuvent pas être modifiés en ligne.	
		i *Allow Online Settings* peut être réglé sur ON si l'automate est à l'arrêt ou par rechargement.	
		Valeur par défaut ON	
Autostart	Y	Démarrage automatique du programme utilisateur dans les cas suivants : ▪ Activation de la tension d'alimentation ▪ Redémarrage de l'automate à la suite d'une erreur.	Spécifique à l'application
		ON : Le programme utilisateur démarre automatiquement.	
		OFF : Le programme utilisateur ne démarre pas automatiquement.	
		Valeur par défaut OFF.	
Start Allowed	Y	ON : Démarrage à froid ou à chaud autorisé par PADT à l'état RUN ou STOP.	Spécifique à l'application
		OFF : Démarrage non autorisé.	
		Valeur par défaut : ON	
Load Allowed	Y	ON : Téléchargement de la configuration autorisé.	Spécifique à l'application
		OFF : Téléchargement de la configuration non autorisé.	
		Valeur par défaut ON	
Reload Allowed	Y	Indique si un rechargement de la configuration est possible. L'action sur les autres paramètres est décrite au chapitre 7.4.1.3.	Spécifique à l'application
		ON : Rechargement de la configuration autorisé.	
		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	Y	ON : Forçage général autorisé pour cette ressource	Spécifique à l'application
		OFF : Forçage général non autorisé pour cette ressource	
		Valeur par défaut : ON	
Global Force Timeout Reaction	N	Détermine le comportement de la ressource en cas d'expiration de la temporisation de forçage général : ▪ Stop Forcing. ▪ Stop Resource. Valeur par défaut : Stop Forcing Only.	Spécifique à l'application

Paramètre	S [1)]	Description		Paramétrage pour un fonctionnement sécurisé
Minimum Configuration Version	N	Avec ce réglage, il est possible de générer un code compatible avec des versions trop anciennes ou trop récentes du système d'exploitation du processeur en fonction des exigences du projet. Le code généré correspond au code généré par la version SILworX mentionnée. Voir chapitre 7.4.1.4. Valeur par défaut : SILworX V8 pour de nouveaux projets		Spécifique à l'application
		SILworX V2, SILworX V3	Non applicable aux commandes HIMatrix !	
		SILworX V4, SILworX V5, SILworX V6	La compilation du programme s'effectue comme avec SILworX V4, V5, ou V6.48. Le code généré est compatible avec la version V8 du système d'exploitation du processeur.	
		SILworX V6b	La compilation du programme s'effectue comme avec SILworX V6 114. Le code généré est compatible avec la version V10 du système d'exploitation du processeur.	
		SILworX V7	La compilation du programme s'effectue comme avec SILworX V7. Le code généré est compatible avec la version V11 du système d'exploitation du processeur.	
		SILworX V8	La compilation du programme s'effectue comme avec SILworX V8. Le code généré est compatible avec la version V12 du système d'exploitation du processeur.	
Fast Start-Up	Y	La ressource démarre plus rapidement en cas d'activation de la tension d'alimentation, < 10 s. Voir chapitre 7.4.1.5. Valeur par défaut OFF		Spécifique à l'application

[1)] Paramètre système relatif à la sécurité oui/non (Y/N)

Tableau 16 : Les paramètres système de la ressource

7.4.1.1 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, HIMatrix limite l'activité de rechargement 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 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 uniquement si la durée du cycle Target Cycle Time est suffisante.
Fixed-tolerant		Prolongation au maximum tous les cinq cycles pour exécuter le rechargement.
Dynamic-tolerant	HIMatrix exécute le cycle dans un temps aussi court que possible.	Prolongation au maximum tous les cinq cycles pour exécuter le rechargement.
Dynamic		Exécution du rechargement uniquement si la durée du cycle Target Cycle Time est suffisante.

Tableau 17 : Effet du paramètre Target Cycle Time Mode

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

Si le traitement de la communication des données de configuration 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 avec le module d'E/S et les PADT est de ce fait temporisée, néanmoins toutes les connexions avec des partenaires externes sont traitées équitablement et intégralement.

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 :

$T_{Konfig} = (n_{Kom} + n_{RIO} + n_{PADT}) * 0{,}25\ ms + 2\ ms$, ou

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

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

i Si le paramètre *Max. Duration of Configuration Connections* est configuré trop bas, la communication entre le PADT et le PES est très lente pouvant aller jusqu'à une défaillance totale!

7.4.1.3 Remarques sur les paramètres *Allow Online Settings* et *Reload Allowed*

Les paramètres suivants ne peuvent pas être modifiés en ligne si *Allow Online Settings* **et** *Reload Allowed* sont réglés sur OFF :

- *Watchdog Time [ms]*
- *Safety Time [ms]*
- *Target Cycle Time [ms]*
- *Target Cycle Time Mode*

Si *Allow Online Settings* ou *Reload Allowed* est réglé sur ON, les paramètres peuvent être modifiés en ligne :

7.4.1.4 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 le Hardware et 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 lié à la configuration ne change pas durant la compilation et que la configuration générée est compatible avec le système d'exploitation du matériel.

  C'est pourquoi il est recommandé de ne modifier la *Minimum Configuration Version* des projets convertis qu'en corrélation avec d'autres changements 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. La ressource refuse le chargement d'une version de configuration supérieure incompatible avec son système d'exploitation.

  De telles incompatibilité peuvent être éliminées en rapprochant les informations fournies par le comparateur de version et la vue d'ensemble des caractéristiques de module.

7.4.1.5 Remarque sur le paramètre *Fast Start-Up*

Ce paramètre existe à partir de la version SILworX V7 et requiert une ressource avec un système d'exploitation CPU à partir de la V11 et avec un système d'exploitation COM à partir de la V16. En outre, la ressource doit disposer d'un chargeur d'amorçage CPU à partir de la V11.2 et d'un chargeur d'amorçage COM à partir de la V16.8. Le chargeur d'amorçage se distingue du chargeur OS (chargeur d'urgence) et ne peut pas être remplacé par l'utilisateur.

Le démarrage rapide n'a d'effet qu'à l'activation de la tension d'alimentation de l'automate. Le fonctionnement avec SIL 3 reste garanti.

Le démarrage rapide est obtenu :

- par un Autotest raccourci
- par une absence de contrôle sur les adresses IP en double

  En omettant la détection des adresses IP en double, des adresses IP en double peuvent être actives dans le réseau en cas d'erreur de configuration réseau !

  Le paramétrage doit veiller à ce qu'il n'y ait pas d'adresses IP en double dans le réseau !

Si l'on souhaite effectuer un test LED au démarrage, régler le paramètre *Fast Start-Up* sur OFF !

7.4.2 Variable système du matériel

Ces variables servent à modifier le comportement du contrôleur pendant le fonctionnement en fonction de certains états. Ces variables sont paramétrables dans l'éditeur de matériel de SILworX, dans la vue détaillée du matériel.

Variable	S [1)]	Fonction	Réglage par défaut	Paramétrage pour un fonctionnement sécurisé
Force Deactivation	Y	Permet d'éviter le forçage et son arrêt immédiat	FALSE	Spécifique à l'application
Spare 0... Spare 16	N	Pas de fonction	-	-
Emergency stop 1 ... Emergency stop 4	Y	Pour désactiver le contrôleur en cas de défauts détectés par le programme utilisateur	FALSE	Spécifique à l'application
Relay contact 1... Relay contact 4	N	Uniquement applicable aux F60 ! OU variables de système connexes qui contrôlent le relais du contact FAULT sur la F60 PS 01. Le relais est un inverseur avec le contact commun 2, le contact d'ouverture 3 et le contact de fermeture 1. ▪ Si la F60 est en statut RUN et si les variables de système du *Relay Contact1...4* sont FALSE, le contact 1-2 est fermé (contact 2-3 ouvert). ▪ Si la F60 est en statut RUN et s'il n'y a pas de variables globales associées aux variables de système du *Relay Contact1...4*, le contact 1-2 est fermé (contact 2-3 ouvert). ▪ Si la F60 est en statut RUN et si au moins une variable de système du *Relay Contact1...4* est TRUE, le contact 1-2 est ouvert (contact 2-3 fermé). ▪ Si la F60 n'est pas en statut RUN, le contact 1-2 est ouvert (contact 2-3 fermé). ▪ Si la F60 est hors tension, le contact 1-2 est ouvert (contact 2-3 fermé).	-	Spécifique à l'application
Read-only in RUN	Y	Après le démarrage du contrôleur, les droits d'accès sont ramenés au niveau d'accès *Read*. Exceptions : Forçage et Reload.	FALSE	Spécifique à l'application
Reload Deactivation	Y	Évite un chargement du contrôleur au moyen de Reload.	FALSE	Spécifique à l'application
User LED 1, User LED 2	N	Uniquement applicable à certaines commandes ! Commande la LED correspondante, si présente.	0	-
[1)] Paramètre système relatif à la sécurité oui/non (Y/N)				

Tableau 18 : Les variables de système du matériel

À ces variables de système, il est possible d'assigner une variable globale dont la valeur est modifiée par une entrée physique ou la logique du programme utilisateur.

Exemple : un interrupteur à clé est raccordé à une entrée Tout Ou Rien. L'entrée Tout Ou Rien est assignée à des variables globales, elles-mêmes allouées aux variables de système *Read only in Run*. À l'aide de l'interrupteur à clé, le détenteur d'une clé peut autoriser ou verrouiller les fonctions *Stopp*, *Start* et *Download*.

7.5 Protection contre manipulations

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

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

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

Les exigences selon les normes de sécurité et d'application relatives à la protection contre les manipulations doivent être respectées. L'autorisation 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 !**

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

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

7.6 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 *HIMatrix_Checklist_Outputs.doc* est un document disponible au format Microsoft© Word©. Le fichier zip *HIMatrix_Checklists.zip* contient toutes les listes de contrôle et peut être téléchargé sur les sites Internet HIMA www.hima.de et www.hima.com.

8 Aspects relatifs à la sécurité pour le programme utilisateur

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

- Spécifications des fonctionnalités du contrôleur.
- Écriture du programme utilisateur.
- Compilation du programme utilisateur avec le générateur de code C.
- Seconde compilation du programme utilisateur, comparer les deux résultats (CRC).
- Le programme est sans erreur et peut être exécuté.
- Vérification et validation.

Ensuite, l'automate peut commencer à fonctionner de manière sécurisée.

8.1 Cadre d'une utilisation relative à la sécurité

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

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 se compose essentiellement des fonctions suivantes :

- Saisie (éditeur de programme), surveillance et documentation.
- Variables avec noms symboliques et types de données (BOOL, UINT, etc.).
- Assignation des commandes du système HIMatrix (Hardware Editor).
- Générateur de codes (compilation du programme utilisateur dans le code machine).
- Configuration de la communication.

8.1.1 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 composants externes à contrôler.
  - Plans séquentiels.
  - Forme matricielle ou tabulaire des conditions de progression et des composants externes à contrôler.
  - Définition des restrictions, par ex. modes d'exploitation, arrêt d'urgence, etc.

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

- Composants externes (automates de terrain)
  - Signal d'entrée en exploitation normale (principe de « Mise hors tension pour déclenchement » sur les appareils de terrain numériques)
  - Signal d'entrée en cas de défauts
  - Détermination des redondances requises et relatives à la sécurité (1oo2, 2oo3)
  - Contrôle des incohérences et réponse
  - 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.
- Modifications aisées.
- Tests aisés.

8.1.2 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 du courant de repos, c.-à-d. que leur état de sécurité est *0*.
- Le programme utilisateur est doté de fonctions logiques et/ou arithmétiques très pertinentes, sans prendre en considération le principe 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 fonction 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.

8.1.3 Déclaration des variables

Une variable est un caractère de substitution d'une valeur au sein de la logique du programme. Le nom de variable est utilisé pour adresser symboliquement l'emplacement mémoire contenant la valeur enregistrée. Une variable est créée dans la déclaration de variable du programme ou du module de fonction.

L'utilisation de noms symboliques au lieu d'adresses physiques présente deux avantages :

- Dans le programme utilisateur, les désignations d'installation des entrées et sorties peuvent être utilisées.
- Les modifications de l'affectation des signaux aux canaux d'entrée et de sortie n'ont aucune incidence sur le programme utilisateur.

Les variables, dont la source n'est pas valide, par ex. en raison d'erreurs de matériel dans le cas d'une entrée physique, prennent la valeur initiale configurée. Si aucune valeur initiale n'est configurée, les variables ont comme valeur initiale par défaut 0 ou FALSE.

⚠ ATTENTION

Risque d'influences réciproques entre des parties du programme utilisateur !

L'utilisation des mêmes variables globales dans plusieurs parties d'un programme utilisateur, par exemple des blocs fonctionnels ou des fonctions, peut avoir diverses conséquences imprévues causées par des influences réciproques des différentes parties.

- **Implémenter avec précision l'utilisation de variables globales au sein des différentes parties d'un programme utilisateur.**
- **Utiliser des références croisées dans SILworX pour vérifier l'utilisation des données globales. Les valeurs assignées par les données globales ne peuvent être que d'une seule entité, soit dans une partie d'un programme utilisateur via la communication, soit à partir du matériel !**

8.1.4 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.

8.2 Procédures

Ce chapitre décrit les procédures classiques destinées à la mise au point de programmes utilisateurs pour des commandes HIMatrix relatives à la sécurité.

8.2.1 Assignation de variables aux entrées et sorties

Les procédures de test requises pour les automates d'E/S, les modules d'E/S et les canaux d'E/S sont automatiquement exécutées par le système d'exploitation.

Assignation d'une variable à un canal d'E/S

1. Définir une variable globale d'un type approprié.
2. Indiquer une valeur initiale appropriée lors de la définition.
3. Assigner la variable globale à la valeur de canal du canal d'E/S.
4. Dans le programme utilisateur, analyser le code d'erreur -> *Error Code [Byte]* et programmer une réponse relative à la sécurité.

► La variable globale est assignée à un canal d'entrée/de sortie.

8.2.2 Ouverture et fermeture du contrôleur

La fonction *Locking* du contrôleur indique le verrouillage des possibilités d'accès de l'utilisateur pendant l'exploitation. Cela protège de toute manipulation non autorisée du programme utilisateur. La portée des verrouillages est à établir en fonction des exigences de sécurité liées à l'utilisation de l'automate, elles peuvent également être concertées avec l'organisme de contrôle en charge de la réception de l'installation.

La fonction *Unlocking* de l'automate indique la désactivation du verrouillage, par ex. afin d'intervenir sur le contrôleur.

i La fermeture et l'ouverture ne sont possibles que sur les commandes et les modules d'E/S déportées F3 DIO 20/8 01 et non pas sur d'autres modules d'E/S !

Trois variables de système sont utilisées pour le verrouillage :

Variable	Fonction
Read only in RUN	TRUE : le démarrage, l'arrêt et le téléchargement du contrôleur sont verrouillés. FALSE : le démarrage, l'arrêt et le téléchargement du contrôleur sont possibles.
Reload Deactivation	TRUE : le rechargement est verrouillé. FALSE : le rechargement est possible.
Force Deactivation	TRUE : le forçage est déconnecté. FALSE : le forçage est possible.

Tableau 19 : Variable système pour ouverture et fermeture de l'automate

Si les trois variables de système sont sur TRUE, il n'est plus possible d'intervenir sur le contrôleur pour effectuer des modifications.

Exemple : ouverture et fermeture de l'automate

Procédure de verrouillage de l'automate

1. Définir une variable globale de type BOOL, mettre la valeur initiale sur FALSE.
2. Assigner une variable globale aux trois variables de 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 l'appareil d'entrée Tout Ou Rien ou de module d'entrée Tout Ou Rien correspondant, le contrôleur est ouvert.

Cet exemple simple peut être décliné en utilisant plusieurs variables globales et plusieurs entrées ou sorties Tout Ou Rien de façon à répartir entre différentes clés / personnes les droits d'accès pour le forçage, le rechargement et les fonctions Arrêt, Démarrage et Téléchargement.

8.2.3 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 la checksum 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.

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

En configuration par défaut, SILworX génère automatiquement cette double compilation de la ressource puis effectue la comparaison entre les CRC.

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 CRC assurent la détection de défaillances aléatoires au niveau du matériel ou du système d'exploitation du PC utilisé.

8.2.4 Comparateur de versions sécurisé

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

- 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 sécurisé 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, et sert de justificatif pour les organismes de contrôle.

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

Pour plus de détails sur le comparateur de versions sécurisé, se reporter au manuel du comparateur de versions HI 801 285 D.

8.2.5 Chargement et démarrage du programme utilisateur

Le chargement du programme utilisateur dans l'automate de sécurité HIMatrix 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 du programme utilisateur s'est déroulé correctement. Ensuite, le programme utilisateur peut démarrer, c.-à-d. que le traitement cyclique des tâches commence.

i Après chaque chargement du programme utilisateur, HIMA recommande de sauvegarder le projet, par ex. sur un support d'enregistrement externe.

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.

8.2.6 Rechargement

L'utilisation de la fonction Rechargement pour modifier la configuration des ressources doit être approuvée par l'organisme de contrôle compétent !

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.

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 !

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 du chien de garde fixé peut être dépassé. Si tel est le cas, le rechargement est interrompu avec émission d'un message de défaut et l'automate continu de fonctionner avec la configuration de projet précèdente.

La commande peut interrompre un rechargement.

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

L'augmentation provisoire du temps du 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 du 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.

L'utilisation de la fonction Rechargement nécessite une licence. Pour de plus amples détails sur le rechargement, se reporter au manuel du système HI 800 641 FR.

8.2.7 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 du 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 informations sur le forçage, se reporter aux manuels des systèmes HI 800 641 FR.

8.2.7.1 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 système

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

1. Une variable globale A forcée est allouée à une des sources de données citées. De ce fait, la source de données est elle aussi forcée !
2. L'allocation est annulée. La source de données contient la propriété *Forced*.
3. Une autre variable globale B est allouée à la source de données.
4. Un rechargement est effectué pour charger la modification au niveau du projet dans l'automate.

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.

8.2.8 Modification des paramètres système pendant exploitation

Il est possible de modifier quelques paramètres système du contrôleur en ligne. Un cas d'application classique est l'augmentation provisoire du temps du chien de garde pour permettre un rechargement.

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

La configuration du temps de sécurité et du chien 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 du chien de garde inférieur à celui préalablement chargé.

Les paramètres suivants peuvent être modifiés en ligne :

- System ID
- Watchdog Time (de la ressource)
- Safety time
- Target Cycle Time
- Target Cycle Time Mode
- Allow Online Settings
- Autostart
- Start Allowed
- Load Allowed
- Reload Allowed
- Global Forcing Allowed
- Global Force Timeout Reaction

Allow Online Settings permet de modifier les autres paramètres. *Allow Online Settings* ne peut être mis sur TRUE qu'à l'état STOP.

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

8.2.9 Documentation du programme pour applications de sécurité

L'outil 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 pour système, modules et paramètres système
- Configuration du réseau
- Liste de références croisées des signaux
- Informations sur le générateur de code

La documentation est requise pour les tests de réception d'un système soumis à l'approbation par un organisme de contrôle (par ex. TÜV). Ces tests de validation concernent uniquement les fonctionnalités implémentées par l'utilisateur et non pas les modules et autres appareils liés système HIMatrix étant déjà homologués.

8.2.10 Multitâche

Multitâche désigne la capacité des systèmes HIMatrix à traiter jusqu'à 32 programmes utilisateurs au sein d'un système processeur.

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 système processeur. Cela peut être contrôlé par les paramètres de la ressource et du programme

utilisateur. SILworX calcule le temps du chien de garde du programme utilisateur à partir des paramètres :

Watchdog Time$_{\text{user programm}}$ = *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 paramétrée au moyen de *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 des variables globales écrites par un autre programme utilisateur jusqu'à atteindre le nombre de cycles du système processeur défini pour le programme par le paramètre système *Maximum Number of CPU Cycles*. Dans le cas du pire scénario, la séquence suivante est possible :
  - Le programme A écrit les variables globales requises par le programme B.
  - Le programme A termine son cycle au cours du cycle du système de processeur pendant lequel le programme B commence son cycle.
  - Le programme B ne peut lire les valeurs écrites par A qu'au début de son prochain cycle.
  - Le cycle de B qui vient de commencer peut avoir la même durée de cycle que celui établi par *Program's Maximum Number of CPU cycles**. B ne reçoit les valeurs écrites par A qu'à ce moment-là.
  - Jusqu'à ce que B fournisse une réponse à ces valeurs, d'autres cycles *Program's Maximum Number of CPU Cycles* du système de processeur peuvent s'écouler !

⚠ ATTENTION

Risque d'influences réciproques entre les programmes utilisateurs !

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

- **Implémenter avec précision l'utilisation de variables globales au sein des différents programmes utilisateurs.**
- **Utiliser des références croisées dans SILworX pour vérifier l'utilisation des données globales. Les variables globales ne doivent récupérer leur valeur que par le biais d'une entité unique, quelle soit liée à une entrée physique ou à un protocole de communication sécurisé.!**

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

Pour de plus amples détails sur le Multitâche, se reporter au manuel du système HI 800 641 FR.

8.2.11 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 HIMatrix étant déjà homologués.

9 Configuration de la communication

À l'instar des variables d'entrée et de sortie physiques, les 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 de l'outil de programmation SILworX dans le menu protocoles de la ressource correspondante.

Cet échange de données peut s'effectuer tant en mode lecture qu'en mode écriture.

9.1 Protocoles standards

Une série de protocoles de communication n'offre qu'une transmission de données non sécurisée. 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 selon le modèle de commande :

- SNTP
- Send/Receive TCP
- Modbus (maître/esclave)
- PROFIBUS DP (maître/esclave)
- PROFINET et PROFIsafe (CPU BS V7 et postérieures)

Tous les protocoles standards sont sans effet rétroactif sur le système de processeur sécurisé.

9.2 Protocole sécurisé safeethernet

Le réseau safe**ethernet** doit être utilisé pour l'échange de données relatif à la sécurité entre des composants relatifs à la sécurité.

Le réseau safe**ethernet** est certifié jusqu'au niveau SIL 4 en tant que composant système de l'appareil HIMatrix.

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

Appliquer la condition suivante pour le calcul des paramètres safe**ethernet** *Receive Timeout* et *Response Time* :
La tranche de temps de communication doit être suffisamment grande pour traiter toutes les connexions safe**ethernet** dans un seul cycle de processeur.

Pour des fonctions de sécurité devant être exécutées par le biais de safe**ethernet**, seul le paramètre **Use Initial Data** doit être utilisé.

REMARQUE

Transition involontaire à l'état de sécurité possible!

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

La valeur d'un signal doit être supérieure à *Receive Timeout* ou être surveillée par bouclage si chaque valeur doit être transmise.

9.2.1 Receive Timeout

Le paramètre *Receive Timeout* représente, lors d'un échange de données, la surveillance du temps de réponse en millisecondes (ms) d'un partenaire.

Si aucune réponse correcte du partenaire de communication ne parvient pendant *Receive Timeout*, la communication relative à la sécurité se ferme. Les variables d'entrée de cette connexion safe**ethernet** se comportent selon les paramètres fixés sous *Freeze Data on Lost Connection [ms]*.

Étant donné que *Receive Timeout* est relatif à la sécurité et élément du Worst Case Reaction Time T_R (temps maximal de réponse, voir chapitres 3.2.4 et suivants), *Receive Timeout* doit être calculé comme suit et saisi dans l'éditeur safe**ethernet**.

Receive Timeout ≥ 4*Delay + 5*max. cycle time

Condition : la tranche de temps de communication doit être suffisamment grande pour traiter toutes les connexions safe**ethernet** dans un seul cycle de processeur.

Delay :	Temporisation sur la ligne de transmission, par ex. par commutateur, satellite
Max. cycle time :	Durée de cycle maximale des deux commandes

i Une tolérance aux erreurs souhaitée de la communication peut être obtenue par le biais d'une augmentation de *Receive Timeout* si celle-ci est admissible en termes de durée pour le processus d'application.

REMARQUE

La valeur maximale autorisée pour *Receive Timeout* dépend du processus d'application et est paramétrée dans l'éditeur safe**ethernet conjointement avec le temps de réponse maximal escompté et le profil.**

9.2.2 Response Time

ResponseTime est la durée en millisecondes (ms) qui s'écoule jusqu'à ce que l'émetteur d'un message reçoive l'accusé de réception du récepteur.

Pour le paramétrage au moyen d'un profil safe**ethernet**, une durée *ResponseTime* escomptée en fonction des conditions physiques de la ligne de transmission doit être fixée.

La durée *ResponseTime* fixée a des répercussions sur la configuration de tous les paramètres de la connexion safe**ethernet** et elles doivent être calculées comme suit :

ResponseTime ≤ Receive Timeout / n

n = 2, 3, 4, 5, 6, 7, 8.....

Le rapport entre *Receive Timeout* et *ResponseTime* agit sur la capacité de tolérance des erreurs, par ex. en cas de pertes de paquets de données (répétition de paquets de données perdues) ou de temporisations sur la ligne de transmission.

Dans un réseau pouvant enregistrer des pertes de paquets, la condition suivante doit être remplie :

min. ResponseTime ≤ Receive Timeout / 2 ≥ 2*Delay + 2,5*max. cycle time

Si cette condition est remplie, la perte d'au moins un paquet de données peut être interceptée sans que la connexion safe**ethernet**/connexion peer-to-peer soit interrompue.

i Si cette condition n'est pas remplie, la disponibilité d'une connexion safe**ethernet** ne peut être garantie que dans un réseau sans collision et sans perturbation. Néanmoins, cela ne représente aucun problème de sécurité pour le processeur !

i S'assurer que le système de communication respecte le temps de réponse paramétrée (response time) !

Si ce point ne peut pas toujours être garanti, une variable de système appropriée est disponible pour la surveillance du temps de réponse. Si un dépassement du temps de réponse n'est plus un fait exceptionnel et qu'il est supérieur à la moitié du Receive Timeout, le temps de réponse doit être augmenté.

Le Receive Timeout doit être adapté au nouveau temps de réponse paramétré.

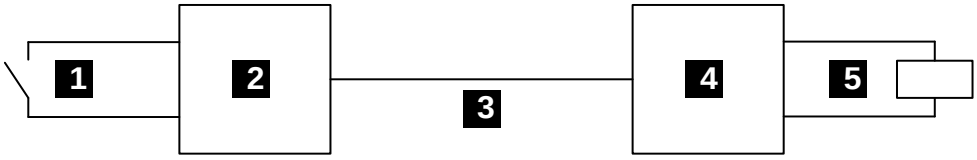
REMARQUE

Les exemples d'équations ci-dessous ne s'appliquent, pour une connexion entre des systèmes HIMatrix, que si le

Temps de Sécurité est fixé à = 2 * temps du chien de garde

9.2.3 Calcul du temps de réponse maximal

Le temps de réponse maximal T_R (*Worst Case*) depuis le changement d'un composant de terrain du contrôleur 1 (In) jusqu'à la réaction de la sortie (Out) du contrôleur 2 peut être calculé comme suit :



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

Figure 4 : Temps de réponse entre deux contrôleurs HIMatrix interconnectés

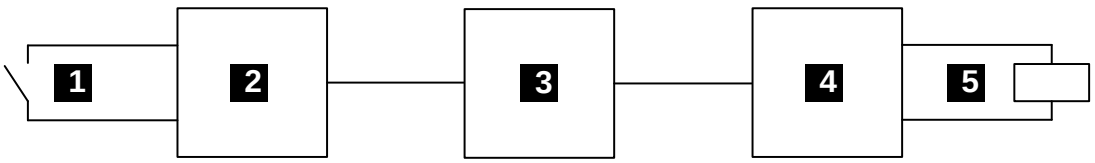
$$\mathbf{T_R = t_1 + t_2 + t_3}$$

T_R	Temps de réponse maximal
t_1	2 ∗ Temps du chien de garde du contrôleur 1
t_2	Receive Timeout
t_3	2 ∗ Temps du chien de garde du contrôleur 2

Le temps de réponse maximal dépend du processus et doit être approuvé en concertation avec l'organisme d'inspection en charge de la validation.

9.2.4 Calcul du temps de réponse avec deux modules d'E/S déportées

Le temps de réponse maximal T_R depuis le changement d'un composant de terrain (In) du premier module d'E/S déportées jusqu'à la réaction de la sortie (Out) du deuxième module d'E/S déportées peut être calculé comme suit :



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

Figure 5 : Temps de réponse avec module d'E/S déportées

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

T_R	Temps de réponse maximal
t_1	2 ∗ Temps du chien de garde du module d'E/S déportées 1
t_2	Receive Timeout $_1$
t_3	2 ∗ Temps du chien de garde du contrôleur
t_4	Receive Timeout $_2$
t_5	2 ∗ Temps du chien de garde du module d'E/S déportées 2

Remarque : les deux modules d'E/S déportées 1 et 2 peuvent être identiques. Les temps sont également applicables si l'on utilise un contrôleur au lieu d'un module d'E/S déportées.

9.2.5 Terminologie

Receive Timeout	Temps de surveillance dans le contrôleur 1, au cours duquel une réponse valide du contrôleur 2 doit être reçue. Après expiration du temps, la communication sécurisée est fermée.
Receive Timeout $_1$	Module d'E/S déportées 1 → Commande
Receive Timeout $_2$	Commande → Module d'E/S déportées 2
Watchdog Time	Durée maximal de cycle autorisée par l'automate.
Worst Case	Temps de réponse maximal pour la transmission de la modification de signal d'une entrée physique (In) d'un contrôleur 1 jusqu'à la modification de la sortie physique (Out) d'un contrôleur 2.

La transmission de données s'effectue avec un protocole de sécurité.

9.2.6 Attribution des adresses safe**ethernet**

Lors de l'attribution d'adresses de réseau (adresses IP) pour safe**ethernet**, observer les points suivants :

- Les adresses doivent être uniques dans le réseau utilisé.
- En cas de connexion de safe**ethernet** avec un autre réseau (LAN interne à l'entreprise, etc.), veiller à ce qu'aucune interférence ne se produise. De possibles sources de perturbations sont par ex. :
  - Trafic de données existant.
  - Couplage avec d'autres réseaux (par ex. Internet).

Dans de tels cas, prendre des mesures appropriées, par ex. utilisation de commutateurs Ethernet, pare-feux, pour neutraliser les perturbations.

---

i L'exploitant est tenu d'assurer une protection suffisante de l'Ethernet utilisé pour les communications safe**ethernet** / peer-to-peer contre d'éventuelles manipulations (par ex. par des pirates informatiques).

La nature et la portée des mesures sont à concerter avec l'organisme de contrôle en charge de la réception.

Annexe

Glossaire

Terme	Description
AI	Analog input : entrée analogique
AO	Analog output : sortie analogique
ARP	Address Resolution Protocol : protocole réseau destiné à l'attribution d'adresses de réseau aux adresses matérielles
COM	Communication (-module)
CRC	Contrôle de redondance cyclique : checksum
DI	Digital input : entrée Tout Ou Rien
DO	Digital output : sortie Tout Ou Rien
EMC	Compatibilité électromagnétique
EN	Norme européenne
ESD	ElectroStatic Discharge : décharge électrostatique
FB	Fieldbus, bus de terrain
FBD	Function block diagrams, diagramme de blocs fonctionnels
HW	Matériel
ICMP	Internet Control Message Protocol : protocole réseau pour messages concernant l'état et les erreurs
IEC	Commission électrotechnique internationale
LS/LB	LS/LB (LS = court-circuit, LB = rupture de ligne)
MAC	Media Access Control : adresse matérielle d'une connexion réseau
PADT	Programming and Debugging Tool (selon IEC 61131-3), PC avec SILworX
PE	Protective Earth : protection par mise à la terre
R	Read, lecture d'une variable
R/W	Read/Write (titre de colonne pour le type de variable de système)
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.
SFF	Safe Failure Fraction : part de défaillances sûres
SIL	Safety Integrity Level (selon IEC 61508)
SILworX	Outil de programmation
SNTP	Simple Network Time Protocol (RFC 1769)
SRS	System.Rack.Slot: Adressage d'un module
SW	Logiciel
Système PE / PES	Système électronique programmable (Programmable Electronic System)
TBTP	Protective Extra Low Voltage : basse tension de fonctionnement avec isolation sécurisée
TBTS	Safety Extra Low Voltage : très basse tension de sécurité
TMO	Timeout, temps d'expiration
W	Write : une valeur est assignée à la variable, provenant par ex. du programme utilisateur
WD	Watchdog : contrôle du fonctionnement pour les systèmes. Signal pour un processus sans erreurs
WDT	Temps du chien de garde

Index des figures

Figure 1 : Représentation des blocs de fonctions fondée sur le processeur 03 de la F60 25

Figure 2 : Line Control 30

Figure 3 : Signaux d'horloge T1, T2 30

Figure 4 : Temps de réponse entre deux contrôleurs HIMatrix interconnectés 61

Figure 5 : Temps de réponse avec module d'E/S déportées 61

Index des tableaux

Tableau 1 :	Documentation du système HIMatrix	11
Tableau 2 :	Plage de valeurs pour le temps du chien de garde	15
Tableau 3 :	Variantes HIMatrix disponibles pour applications ferroviaires	20
Tableau 4 :	Classes de température des appareils HIMatrix standard selon EN 50125-3	21
Tableau 5 :	Classes de température selon EN 50125-3	21
Tableau 6 :	Classes de température selon EN 50125-3	22
Tableau 7 :	Conditions mécaniques pour application dans technique de signalisation	22
Tableau 8 :	Conditions CEM pour application dans technique de signalisation selon EN 50121-4	23
Tableau 9 :	Conditions CEM pour applications ferroviaires selon EN 50121-3-2	23
Tableau 10 :	Test d'insensibilité aux anomalies de tension d'alimentation	24
Tableau 11 :	Vue d'ensemble des entrées	28
Tableau 12 :	Entrées analogiques du contrôleur F35	31
Tableau 13 :	Entrées analogiques du module d'E/S déportées F3 AIO 8/4 01	31
Tableau 14 :	Entrées analogiques du contrôleur F60	31
Tableau 15 :	Vue d'ensemble des sorties	34
Tableau 16 :	Les paramètres système de la ressource	44
Tableau 17 :	Effet du paramètre Target Cycle Time Mode	44
Tableau 18 :	Les variables de système du matériel	47
Tableau 19 :	Variable système pour ouverture et fermeture de l'automate	52

Index

Conditions d'Application
protection ESD 11
Conditions d'essai 20
Hardware Editor 47
Multitâche 56
principe de «Mise hors tension pour
déclenchement» 10
Principe de l'émission de courant 10
Procédure de verrouillage de l'automate 52
Réactions aux erreurs 29
Safety time 14
Temps de sécurité du processus 14
Temps du chien de garde 15
Temps du chien de garde
programme utilisateur 16
Test fonctionnel du contrôleur 40

HI 800 675 FR

HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28 | 68782 Brühl
Téléphone: +49 6202 709-0 · Fax: +49 6202 709-107
info@hima.com | www.hima.de

SAFETY
NONSTOP

Pour obtenir une liste détaillée de toutes les filiales et représentations consultez le site www.hima.de/kontakt