HIMax®

Manual de segurança

SAFETY
NONSTOP

HIMA

SEGURANÇA

8

Todos os produtos HIMA mencionados neste manual estão protegidos pela marca registrada da HIMA. A não ser que seja mencionado de outra forma, isso também se aplica aos outros fabricantes e seus produtos mencionados.

Todos os dados e avisos técnicos neste manual foram elaborados com o máximo de cuidado, considerando medidas de controle de garantia de qualidade efetiva. Em caso de dúvidas, dirija-se diretamente à HIMA. A HIMA ficaria grata por quaisquer sugestões, p. ex., informações que ainda devem ser incluídas no manual.

Os dados técnicos estão sujeitos a alterações sem notificação prévia. A HIMA ainda se reserva o direito de modificar o material escrito sem avisar previamente.

Demais informações encontram-se na documentação do DVD HIMA e na nossa homepage em http://www.hima.com.

Contato

Endereço da HIMA:

HIMA Paul Hildebrandt GmbH

Postfach 1261

D-68777 Brühl

Tel.: +49 6202 709-0

Fax: +49 6202 709-107

E-Mail: info@hima.com

Índice de revisão	Alterações	Tipo de alteração	
		técnica	redacional
4.00	Adaptado ao SILworX V4 Edição em português (traduzida)		

Índice

1 Manual de segurança 7
1.1 Validade e atualidade 7
1.2 Objetivos do manual 7
1.3 Grupo alvo 7
1.4 Convenções de representação 7
1.4.1 Avisos de segurança 8
1.4.2 Avisos de utilização 8
2 Utilização prevista 9
2.1 Área de aplicação 9
2.1.1 Aplicação no princípio de circuito fechado 9
2.1.2 Aplicação no princípio de circuito aberto 9
2.1.3 Aplicação em centrais de alarme de incêndio 9
2.2 Utilização não-prevista 9
2.3 Condições de utilização 10
2.3.1 Condições climáticas 10
2.3.2 Requisitos mecânicos 11
2.3.3 Requisitos CEM 11
2.3.4 Alimentação com tensão 12
2.3.5 Medidas de proteção contra ESD 12
2.4 Obrigações dos fabricantes de máquinas e sistemas bem como da empresa operadora 12
2.5 Demais documentações de sistema 13
3 Concepção de segurança para a utilização dos PES 14
3.1 Segurança e disponibilidade 14
3.1.1 Cálculo dos valores PFD e PFH 14
3.1.2 Autoteste e diagnóstico de erros 14
3.1.3 PADT 15
3.1.4 Redundância 15
3.1.5 Estrutura de sistemas de segurança pelo princípio de circuito aberto 15
3.2 Tempos importantes para a segurança 16
3.2.1 Fault tolerance time, tempo de tolerância de falhas (FTT) 16
3.2.2 Tempo de Watchdog do recurso 16
3.2.3 Tempo de Watchdog do programa de aplicação 18
3.2.4 Tempo de segurança do PES 18
3.2.5 Tempo de segurança do programa de aplicação 19
3.2.6 Tempo de reação 19
3.3 Repetição da verificação 19
3.3.1 Execução da repetição da verificação 19
3.3.2 Frequência das repetições da verificação 19
3.4 Requisitos para segurança 20
3.4.1 Configuração do hardware 20

3.4.2 Programação 20
3.4.3 Requisitos para a utilização do sistema de programação 20
3.4.4 Comunicação 21
3.4.5 Trabalhos de manutenção 21
3.5 Certificação 22
4 Módulo processador 24
4.1 Autotestes 24
4.2 Reações a erro no módulo processador 24
4.3 Troca de módulos processadores 24
5 Módulo de barramento de sistema 25
5.1 ID de Rack 25
5.2 Responsibility 25
6 Módulo de comunicação 27
7 Módulos de entrada 28
7.1 Informações gerais 28
7.2 Segurança de sensores, encoders e transmissores 28
7.3 Entradas digitais direcionadas à segurança 29
7.3.1 Rotinas de teste 29
7.3.2 Reação em caso de erro 29
7.3.3 Operação de acordo com o princípio de circuito aberto 29
7.3.4 Redundância 29
7.3.5 Surges em entradas digitais 29
7.4 Entradas analógicas direcionadas à segurança 30
7.4.1 Rotinas de teste 30
7.4.2 Reação em caso de erro 30
7.4.3 Operação de acordo com o princípio de circuito aberto 30
7.4.4 Redundância 30
7.5 Entradas do contador direcionadas à segurança 30
7.5.1 Rotinas de teste 31
7.5.2 Reação em caso de erro 31
7.5.3 No caso do módulo contador X-CI 24 01 observar o seguinte! 31
7.5.4 Operação de acordo com o princípio de circuito aberto 31
7.5.5 Redundância 31
7.6 Listas de verificação das entradas 32
8 Módulos de saída 33
8.1 Informações gerais 33
8.2 Segurança de atuadores 33
8.3 Saídas digitais direcionadas à segurança 33
8.3.1 Rotinas de teste para saídas digitais 33
8.3.2 Reação em caso de erro 34
8.3.3 Comportamento em caso de curto-circuito ou sobrecarga externa 34
8.3.4 Operação de acordo com o princípio de circuito aberto 34

8.3.5 Redundância ... 34
8.4 Saídas de relé direcionadas à segurança ... 34
8.4.1 Rotinas de teste para saídas de relé ... 34
8.4.2 Reação em caso de erro ... 35
8.4.3 Operação de acordo com o princípio de circuito aberto ... 35
8.4.4 Redundância ... 35
8.5 Saídas analógicas direcionadas à segurança ... 35
8.5.1 Rotinas de teste para saídas analógicas ... 35
8.5.2 Reação em caso de erro ... 35
8.5.3 Procedimento em caso de quebra de fio externo ... 36
8.5.4 Observe os seguintes itens se usar o módulo de saída X-AO 16 01! ... 36
8.5.5 Operação de acordo com o princípio de circuito aberto ... 36
8.5.6 Redundância ... 36
8.6 Listas de verificação das saídas ... 36
9 Software ... 37
9.1 Aspectos relacionados à segurança para o sistema operacional ... 37
9.2 Aspectos relacionados à segurança para a programação ... 37
9.2.1 Concepção de segurança do SILworX ... 37
9.2.2 Verificação da configuração e do programa de aplicação ... 38
9.3 Parâmetros do recurso ... 39
9.3.1 Parâmetros de sistema do recurso ... 39
9.3.2 Variáveis de sistema do hardware ... 42
9.4 Forcing ... 43
9.5 Comparador seguro de versão ... 43
9.6 Proteção contra manipulações ... 44
10 Programa de aplicação ... 45
10.1 Sequência geral ... 45
10.2 Âmbito para o uso direcionado à segurança ... 45
10.2.1 Embasamento da programação ... 45
10.2.2 Funções do programa de aplicação ... 46
10.2.3 Parâmetros de sistema do programa de aplicação ... 47
10.2.4 Criação de código ... 48
10.2.5 Fazendo o download e iniciando o programa de aplicação ... 48
10.2.6 Reload ... 48
10.2.7 Teste on-line ... 49
10.2.8 Modo passo-a-passo ... 49
10.2.9 Alteração on-line de parâmetros de sistema ... 50
10.2.10 Documentação do programa para aplicações direcionadas à segurança ... 50
10.2.11 Multitasking ... 50
10.2.12 Vistoria final por órgãos de aprovação ... 51
10.3 Lista de verificação para criação de um programa de aplicação ... 51

11 Configuração da comunicação 52

11.1 Protocolos padrão 52

11.2 Protocolo direcionado à segurança safeethernet 52

11.3 Tempo máximo de reação para safeethernet 53

11.3.1 Cálculo do tempo máximo de reação de dois sistemas de comando HIMax 54

11.3.2 Cálculo do tempo máximo de reação em conexão com um sistema de comando HIMatrix 54

11.3.3 Cálculo do tempo máximo de reação com dois sistemas de comando HIMatrix ou Remote I/Os 55

11.3.4 Cálculo do tempo máximo de reação com dois sistemas de comando HIMax e um sistema de comando HIMatrix 55

11.3.5 Cálculo do tempo máximo de reação de dois sistemas de comando HIMatrix 56

11.3.6 Cálculo do tempo máximo de reação com dois Remote I/Os 57

11.3.7 Cálculo do tempo máximo de reação, dois sistemas de comando HIMatrix, um sistema de comando HIMax 57

11.4 Protocolo PROFIsafe direcionado à segurança 58

Anexo 59

Aumento do SIL de sensores e atuadores 59

Termos e abreviaturas 60

Índice de figuras 61

Lista de tabelas 62

Índice remissivo 63

1 Manual de segurança

O conhecimento das normas e a implementação técnica adequada dos avisos de segurança contidos neste manual por parte do pessoal qualificado são pré-requisitos para o planejamento, o projeto, a programação, instalação e colocação em funcionamento seguros, bem como para a segurança durante a operação dos equipamentos de automação HIMax.

A HIMA não assume nenhuma garantia por graves ferimentos, danos materiais e no meio ambiente que podem ser causados pelo seguinte: trabalhos realizados nos equipamentos por pessoal não qualificado, desligar ou contornar (“bypass”) funções de segurança ou a inobservância dos avisos deste manual (e das avarias ou limitações das funções de segurança resultantes disso).

Equipamentos de automação HIMax são desenvolvidos, fabricados e testados de acordo com os padrões e regulamentos de segurança pertinentes. Eles só podem ser utilizados para as aplicações previstas nas descrições e sob as condições ambientais especificadas.

1.1 Validade e atualidade

Versão Rev. 4.00	Esta revisão deve ser utilizada a partir da versão 4. ou superior do sistema HIMax.

É válida a versão mais nova deste manual de segurança, indicada pelo número de versão mais alto. A versão atual encontra-se na homepage *www.hima.com* ou no DVD HIMA atual.

1.2 Objetivos do manual

Este manual contém informações para o uso dos equipamentos de automação HIMax direcionados à segurança de acordo com as determinações. Ele fornece uma introdução no conceito de segurança do sistema HIMax e deve aumentar a consciência do leitor para a segurança.

O manual de segurança é baseado nos conteúdos do certificado e no relatório de teste para o certificado.

1.3 Grupo alvo

Este manual destina-se a planejadores, projetadores e programadores de sistemas de automação, bem como a pessoas que são autorizadas para realizar a colocação em funcionamento, operação e manutenção dos equipamentos e sistemas. Pressupõem-se conhecimentos especializados na área de sistemas de automatização direcionados à segurança.

1.4 Convenções de representação

Para a melhor legibilidade e para clarificação, neste documento valem as seguintes convenções:

Negrito	Ênfase de partes importantes do texto. Denominações de botões, itens de menu e registros no SILworX que podem ser clicados.
Itálico	Parâmetros de sistema e variáveis
`Courier`	Introdução de dados tal qual pelo usuário
RUN	Denominações de estados operacionais em letras maiúsculas
Cap. 1.2.3	Notas remissivas são híperlinks, mesmo quando não são especialmente destacadas. Ao posicionar o cursor nelas, o mesmo muda sua aparência. Ao clicar, o documento salta para o respectivo ponto.

Avisos de segurança e utilização são destacados de forma especial.

1.4.1 Avisos de segurança

Os avisos de segurança no documento são representados como descrito a seguir. Para garantir o menor risco possível devem ser observados sem excepção. A estrutura lógica é

- Palavra sinalizadora: Perigo, Atenção, Cuidado, Nota
- Tipo e fonte do perigo
- Consequências do perigo
- Como evitar o perigo

⚠ PALAVRA SINALIZADORA

Tipo e fonte do perigo!
Consequências do perigo
Como evitar o perigo

O significado das palavras sinalizadoras é

- Perigo: No caso de não-observância resultam lesões corporais graves até a morte
- Atenção: No caso de não-observância há risco de lesões corporais graves até a morte
- Cuidado: No caso de não-observância há risco de lesões corporais leves
- Nota: No caso de não-observância ha risco de danos materiais

NOTA

Tipo e fonte dos danos!
Como evitar os danos

1.4.2 Avisos de utilização

Informações adicionais são estruturadas de acordo com o seguinte exemplo:

i Neste ponto está o texto das informações adicionais.

Dicas úteis e macetes aparecem no formato:

DICA Neste ponto está o texto da dica.

2 Utilização prevista

Este capítulo descreve as condições para a utilização de sistemas HIMax.

2.1 Área de aplicação

Os sistema de comando HIMax direcionados à segurança estão certificados para sistema de comando de processos, sistemas de proteção, sistemas de queimadores e sistemas de comando de máquinas.

Todos os módulos de Entrada/Saída (módulos E/S) HIMax podem ser operados tanto com módulos processadores individuais quanto com vários módulos processadores redundantes.

Na utilização da comunição direcionada à segurança entre diferentes equipamentos deve ser observado que o tempo total de reação do sistema não ultrapasse o tempo de tolerância a erros. As bases de cálculo listadas no manual de segurança HI 800 241 P devem ser aplicadas.

Apenas podem ser conectados nas interfaces de comunicação equipamentos que garantam uma separação elétrica segura.

2.1.1 Aplicação no princípio de circuito fechado

Os dispositivos de automação foram concebidos para o princípio de circuito fechado.

Um sistema que funciona de acordo com o princípio de circuito fechado não precisa de energia para executar a sua função de segurança (“deenergize to trip” – desenergizar para desligar).

Com sinais de entrada e saída é assumido o estado livre de tensão ou corrente como estado seguro no caso de falhas.

2.1.2 Aplicação no princípio de circuito aberto

Os sistemas de comando HIMax também podem ser utilizados em aplicações pelo princípio de circuito aberto.

Um sistema que funciona de acordo com o princípio de circuito aberto precisa de energia, p. ex., energia elétrica ou pneumática, para executar a sua função de segurança (“energize to trip” – energizar para desligar).

Ao projetar o sistema de comando, os requisitos das normas aplicáveis devem ser observados, p. ex., um diagnóstico de condutores das entradas e saídas pode ser necessário.

2.1.3 Aplicação em centrais de alarme de incêndio

Todos os sistemas HIMax com entradas analógicas foram testados e estão certificados para centrais de alarme de incêndio conforme DIN EN 54-2 e NFPA 72. Nestes sistemas, exige-se que no caso de solicitação o estado ativo para dominar o perigo seja assumido.

Devem ser observadas as condições de utilização!

2.2 Utilização não-prevista

A transmissão de dados relevantes para a segurança por redes públicas (p. ex., internet) não é permitida sem medidas adicionais para aumentar a segurança (p. ex., túnel VPN, Firewall, etc.).

Comunicação direcionada à segurança não é possível com as interfaces de barramento de campo.

Não é permitida a utilização em condições de ambiente fora dos requisitos estabelecidos na continuação.

2.3 Condições de utilização

Os equipamentos foram desenvolvidos para satisfazerem os requisitos das seguintes normas para CEM e requisitos climáticas e de meio-ambiente:

Norma	Conteúdo
IEC/EN 61131-2	Sistemas de controlador lógico programável, Parte 2 Requisitos e verificações de meios operacionais
IEC/EN 61000-6-2	CEM Norma técnica básica, Parte 6-2 Resistência a interferência, ambiente industrial
IEC/EN 61000-6-4	Compatibilidade eletromagnética (CEM) Norma técnica básica emissão de interferências, ambiente industrial

Tabela 1: Normas para requisitos de CEM, climáticas e do meio-ambiente

Para a utilização dos sistemas de comando direcionados à segurança HIMax devem ser respeitados os seguintes requisitos gerais:

Tipo de requisito	Conteúdo do requisito
Classe de proteção	Classe de proteção II conforme IEC/EN 61131-2
Contaminação	Grau de contaminação II conforme IEC/EN 61131-2
Altura de instalação	< 2000 m
Caixa	Padrão: IP 20/IP 00 Se as normas aplicáveis (p. ex., EN 60204) o exigirem, o equipamento deve ser montado numa caixa do grau de proteção exigido (p. ex., IP 54).

Tabela 2: Requisitos gerais

2.3.1 Condições climáticas

Os mais importantes testes e valores limite para os requisitos climáticos são listados na tabela a seguir:

IEC/EN 61131-2	Testes climáticos
	Temperatura de operação: 0…+60 °C (Limites de teste: -10…+70 °C)
	Temperatura de armazenamento: -40…+85 °C
	Calor e frio secos; testes de resistência: +70 °C/-25 °C, 96 h, alimentação de corrente não ligada
	Mudança de temperatura; teste de resistência e insensibilidade: -25 °C/+70 °C e 0 °C/+55 °C, alimentação de corrente não ligada
	Ciclos com calor úmido; testes de resistência: +25 °C/+55 °C, 95% umidade relativa, alimentação de corrente não ligada

Tabela 3: Requisitos climáticos

2.3.2 Requisitos mecânicos

Os mais importantes testes e valores limite para os requisitos mecânicos são listados na tabela a seguir:

IEC/EN 61131-2	Testes mecânicos
	Teste de insensibilidade a oscilações: 5…9 Hz/3,5 mm amplitude 9…150 Hz, 1 g, objeto de teste em operação, 10 ciclos por eixo
	Teste de insensibilidade a choques: 15 g, 11 ms, objeto de teste em operação, 3 choques por eixo e direção (18 choques)

Tabela 4: Testes mecânicos

2.3.3 Requisitos CEM

Para sistemas direcionados à segurança são exigidos níveis mais elevados na resistência contra interferências. Os sistemas HIMax satisfazem estes requisitos conforme IEC 62061 e IEC 61326-3-1. Veja a coluna “Critério SF” (Segurança funcional).

Normas de teste	Testes de resistência contra interferência	Critério SF
IEC/EN 61000-4-2	Teste ESD: 6 kV contato-, 8 kV descarga pelo ar	6 kV, 8 kV
IEC/EN 61000-4-3	Teste de RFI (10 V/m): 80 MHz…2 GHz, 80% AM Teste de RFI (3 V/m): 2 GHz…3 GHz, 80% AM Teste de RFI (20 V/m): 80 MHz…1 GHz, 80% AM	- - 20 V/m
IEC/EN 61000-4-4	Teste Burst: Tensão de alimentação: 2 kV e 4 kV Condutores de sinal: 2 kV	 4 kV 2 kV
IEC/EN 61000-4-12	Teste com oscilações atenuadas: 2,5 kV L-, L+/PE 1 kV L+/L -	 - -
IEC/EN 61000-4-6	Alta frequência, assimétrica: 10 V, 150 kHz…80 MHz, 80% AM 20 V, frequências ISM, 80% AM	 10 V -
IEC/EN 61000-4-3	Pulsos de 900 MHz	-
IEC/EN 61000-4-5	Tensão de choque: Tensão de alimentação: 2 kV CM, 1 kV DM Condutores de sinal: 2 kV CM, 1 kV DM com E/S AC	 2 kV/1 kV 2 kV

Tabela 5: Testes de resistência contra interferência

IEC/EN 61000-6-4	Testes de emissão de interferência
EN 55011 Classe A	Emissão de interferências: por irradiação, via conexão de cabo

Tabela 6: Testes de emissão de interferência

2.3.4 Alimentação com tensão

Os mais importantes testes e valores limite para a alimentação com tensão dos equipamentos são listados na tabela a seguir:

IEC/EN 61131-2	Verificação das características da alimentação com corrente contínua
	Alternativamente, a alimentação com tensão deve satisfazer as seguintes normas: IEC/EN 61131-2 ou SELV (Safety Extra Low Voltage) ou PELV (Protective Extra Low Voltage)
	A proteção dos equipamentos HIMax deve ocorrer de acordo com as indicações deste manual
	Verificação da faixa de tensão: 24 VDC, -20%…+25% (19,2 V…30,0 V)
	Teste de insensibilidade a interrupções por breve tempo da alimentação com corrente externa: DC, PS 2: 10 ms
	Inversão da polaridade da tensão de alimentação: Nota no respectivo capítulo do manual de sistema ou na folha de dados da alimentação com corrente.
	Duração do amortecedor, teste de resistência: Teste B, 1000 h

Tabela 7: Verificação das características da alimentação com corrente contínua

2.3.5 Medidas de proteção contra ESD

Apenas pessoal com conhecimentos sobre medidas de proteção contra ESD pode efetuar alterações ou ampliações do sistema ou a substituição de um módulo.

NOTA

Descargas eletrostáticas podem danificar componentes eletrônicos montados nos sistemas de comando!

- **Usar para os trabalhos um posto de trabalho protegido contra descarga eletrostática e usar uma fita de aterramento.**
- **Guardar módulos protegidos contra descarga eletrostática, p. ex., na embalagem.**

Alterações ou ampliações na fiação do sistema apenas podem ser efetuadas por pessoal que tiver conhecimento de medidas de proteção contra ESD.

2.4 Obrigações dos fabricantes de máquinas e sistemas bem como da empresa operadora

O fabricante de máquinas e sistemas bem como a empresa operadora são responsáveis por garantir a utilização segura dos sistemas HIMax em sistemas de automação e instalações completas.

A programação correta dos sistemas HIMax deve ser validada pelos fabricantes de máquinas e sistemas de forma suficiente.

2.5 Demais documentações de sistema

Além disso, ainda estão disponíveis as seguintes documentações para projetar sistemas HIMax:

Nome	Conteúdo	Nº do documento P = português E = inglês
HIMax Manual de sistema	Descrição do hardware do sistema modular	HI 801 242 P HI 801 001 E
Relatório de teste para o certificado [1)]	Princípios do teste, requisitos de segurança, resultados	
Manuais dos componentes	Descrição dos componentes individuais	
Manual de comunicação	safe**ethernet** e protocolos padrão	HI 801 240 P HI 801 101 E
SILworX Manual de primeiros passos	Uso do SILworX para planejamento, colocação em funcionamento, teste e operação	HI 801 239 P HI 801 103 E

[1)] Fornecido apenas em combinação com um sistema HIMax

Tabela 8: Visão geral da documentação do sistema

Os documentos estão disponíveis como arquivos PDF na homepage *www.hima.com*.

3 Concepção de segurança para a utilização dos PES

Este capítulo trata de questões gerais e importantes da segurança funcional de sistemas HIMax:

- Segurança e disponibilidade
- Tempos importantes para a segurança
- Repetição da verificação
- Requisitos para segurança
- Certificação

3.1 Segurança e disponibilidade

Nenhum perigo iminente resulta dos sistemas HIMax.

⚠ PERIGO

Ferimentos causados por sistemas de automação direcionados à segurança que foram conectados ou programados incorretamente!

Verificar as conexões antes da colocação em funcionamento e testar a instalação completa!

A HIMA recomenda expressamente substituir o mais breve possível módulos que falharam.

Um módulo de reposição, que é utilizado no lugar de um módulo que falhou, começa a operar sem ação de comando. Ele assume a função do módulo que falhou, contanto que seja do mesmo tipo ou de um tipo de reposição autorizado.

3.1.1 Cálculo dos valores PFD e PFH

Os valores PFD e PFH foram calculados para os sistemas HIMax conforme IEC 61508.

Os valores para PFD, PFH e SFF podem ser solicitados à HIMA.

O intervalo para a repetição da verificação para sistemas HIMax é determinado para 10 anos (Offline Proof Test, veja IEC 61508-4, parágrafo 3.8.5).

As funções de segurança, compostas por um loop relacionado à segurança (entrada, unidade de processamento, saída e comunicação segura entre sistemas HIMA), cumprem em todas as combinações os requisitos supracitados.

3.1.2 Autoteste e diagnóstico de erros

O sistema operacional dos módulos realiza durante o início e durante a operação autotestes bastante abrangentes. São testados particularmente:

- Processadores
- Áreas de memória (RAM, memória não volátil)
- Watchdog
- Conexões entre os módulos
- Canais individuais de módulos de E/S

Se forem detectados erros nesses testes, o módulo defeituoso ou os módulos de E/S do canal defeituoso são desligados. Se os testes detectarem erros de módulo já ao iniciar um módulo, então, este módulo não entra em operação.

Em um sistema sem redundância, isso significa que funções parciais ou o PES inteiro podem ser desligados. Em caso de um sistema redundante, o módulo redundante ou o canal redundante assume a função a ser executada em caso de erro detectado.

Todos os módulos HIMax dispõem de LEDs próprios para a indicação dos erros detectados. Assim, em caso de avaria é possível um rápido diagnóstico de erros através de um módulo comunicado como apresentando avarias ou através de um circuito externo.

Além disso, o programa de aplicação pode avaliar diversas variáveis do sistema que indicam o estado dos módulos.

Um registro diagnóstico abrangente do comportamento do sistema e os erros detectados são depositados na memória de diagnóstico do módulo processador e em outros módulos. O registro também pode ser lido após uma falha no sistema via PADT.

Para ver detalhes sobre a avaliação das mensagens de diagnóstico, veja também o Manual de sistema HI 801 242 P, capítulo “Diagnóstico”.

Em caso de quantidade muito pequena das falhas dos componentes que não afetam a segurança, o sistema HIMax não gera nenhuma informação de diagnóstico.

3.1.3 PADT

A PADT permite ao usuário criar o programa e configurar o sistema de comando. O conceito de segurança do PADT auxilia o usuário durante a implementação correta da tarefa do sistema de comando. O PADT executa inúmeras medidas para testar as informações introduzidas.

3.1.4 Redundância

Para o aumento da disponibilidade, é possível utilizar todos os componentes que contêm componentes ativos de forma redundante e trocá-los durante a operação.

A redundância não limita a segurança. Também em casos de componentes de sistema redundantes, o SIL 3 é garantido.

3.1.5 Estrutura de sistemas de segurança pelo princípio de circuito aberto

Sistemas de segurança que operam conforme o princípio de circuito aberto (“energize to trip” – energizar para desligar), p. ex., sistemas de detecção de incêndios, possuem os seguintes «estados seguros»:

1. Estado seguro no desligamento da instalação.
2. Estado que é alcançado sob solicitação, ou seja, ao executar a função de segurança. Neste caso, p. ex., o atuador é ligado.

Na estrutura de sistemas de segurança pelo princípio de circuito aberto deve ser observado o seguinte:

- Garantia da execução da função de segurança no caso de perigo.
- Detectar componentes falhados do sistema e reagir:
  - Comunicação da falha.
  - Comutação automática para um componente redundante, se necessário e possível.

Garantia da função de segurança

O planejador deve garantir que o sistema de segurança possa executar a sua função de segurança no caso de perigo. A execução da função de segurança consiste no sistema de segurança alimentar energia a um ou vários atuadores (“energizar”) para que na consequência seja alcançado um estado seguro, p. ex., fechar uma porta de isolação de incêndio.

Para garantir a função de segurança, pode tornar-se necessária uma estrutura redundante dos componentes do sistema de segurança, veja Manual do sistema HI 801 242 P:

- Alimentação do sistema de comando com corrente.
- Componentes do sistema de comando: módulos HIMax.
- No caso de saídas de relé, a HIMA recomenda configurar as mesmas e a alimentação com corrente dos atuadores como redundantes.
  Justificativa:

- Uma saída de relé não possui supervisão de linha.
- Pode tornar-se necessário para atingir o valor SIL exigido.

Deve ter sido levado em consideração que no caso de perda de redundância possa ocorrer a reparação do componente falhado em breve tempo.

A configuração redundante dos componentes do sistema de segurança não é necessária se a segurança exigida pode ser alcançada por outras medidas, p. ex., organizacionais, no caso da falha do sistema de segurança.

Detectar componentes falhados

O sistema de segurança detecta que componentes estão fora de função e ativa componentes redundantes. Isso é alcançado mediante

- Auto-testes dos módulos HIMax.
- Supervisão de curto de linha e de quebra de fio em módulos de entrada/saída. Estes devem ser parametrizados.
- Entradas adicionais para a supervisão dos atuadores, enquanto necessárias para o projeto.

3.2 Tempos importantes para a segurança

Estes são:

- Fault tolerance time, tempo de tolerância de falhas
- Tempo de Watchdog
- Tempo de segurança
- Tempo de reação

3.2.1 Fault tolerance time, tempo de tolerância de falhas (FTT)

O tempo de tolerância de falhas é uma característica do processo e descreve o período de tempo no qual o processo pode ser influenciado por sinais com erros, sem que aconteça um estado perigoso.

3.2.2 Tempo de Watchdog do recurso

O tempo de Watchdog é especificado como tempo no SILworX no diálogo para o ajuste das características do recurso. Esse tempo é a duração máxima de um ciclo RUN (tempo de ciclo). Se o tempo de ciclo ultrapassar o tempo de Watchdog especificado, o módulo processador reage com parada por erro.

Durante a medição do tempo de Watchdog, os seguintes fatores devem ser considerados:

- Tempo requerido pela aplicação, ou seja, a duração de um ciclo no programa de aplicação.
- Tempo requerido pela comunicação dos dados de processo.
- Tempo requerido para a sincronização dos módulos processadores redundantes.
- Tempo interno requerido para a execução de um Reload.

A faixa de ajuste para o tempo de Watchdog do recurso é de

6 ms até no máximo 7.500 ms.

O ajuste padrão é de 200 ms.

Durante o ajuste do tempo de Watchdog, deve valer o seguinte:
Tempo de Watchdog ≤ ½ * tempo de segurança

i Para uma disponibilidade suficiente, a HIMA recomenda expressamente o seguinte ajuste:

2 * tempo de Watchdog + máx. tempo de ciclo de CPU + 2 * tempo de ciclo E/S ≤ tempo de segurança

Se não for possível fazer uma estimativa segura do máx. tempo de ciclo de CPU, deve-se ajustar um tempo de segurança para o qual é válido o seguinte:

3 * tempo de Watchdog + 2 * tempo de ciclo E/S ≤ tempo de segurança

O tempo de ciclo E/S é de 2 ms.

O tempo de Watchdog para um projeto é determinado através de um teste no sistema completo. Durante isso, todos os módulos processadores projetados estão inseridos. O sistema funciona no modo de operação RUN com carga integral.

Todas as ligações de comunicação estão em funcionamento (safe**ethernet** e protocolos padrão).

Determinação do tempo de Watchdog

1. Ajustar um tempo de Watchdog elevado para o teste.
2. Operar o sistema sob carga integral. Neste momento, todas as conexões de comunicação devem estar em operação, tanto via safeethernet quanto através de protocolos padrão. Ler com frequência o tempo de ciclo no Control Panel e anotar as oscilações, e/ou picos de carga do tempo de ciclo.
3. Sucessivamente remover cada módulo processador e voltar a inseri-lo no suporte básico. Antes de remover um módulo processador, aguardar até que o módulo processador inserido há pouco tenha se sincronizado.

i Ao acrescentar um módulo processador, este se sincroniza automaticamente com a configuração dos módulos processadores presentes. O tempo necessário para a sincronização prolonga o ciclo do sistema de comando para o tempo de ciclo máximo.

O tempo necessário para a sincronização cresce com a quantidade de módulos processadores já sincronizados.

Para mais informações sobre a descrição da montagem e desmontagem de um módulo processador, veja manual X-CPU 01, HI 801 254 P.

4. No histórico de diagnóstico do modulo não sincronizado, ler o tempo de sincronização de n para n+1 módulos processadores a cada procedimento de sincronização. A maior parte destes tempos de sincronização é utilizado para a determinação do tempo de Watchdog.
5. Calcular o mínimo tempo de Watchdog:
   maior tempo de sincronização + 12 ms reserva + reserva para as oscilações anotadas.
6. Calcular o tempo de Watchdog T_{WD} utilizando a seguinte equação:

   T_{WD} = .T_{Sinc} + T_{Margem} + T_{Com} + T_{Config} + T_{Lat} + T_{Pico}, onde

T_{Sinc}	Tempo determinado para a sincronização de um módulo processador
T_{Margem}	Margem de segurança 12 ms
T_{Com}	Parâmetro de sistema configurado *Max. Com.Time Slice ASYNC [ms]*
T_{Config}	Parâmetro de sistema configurado *Max. Duration of Configuration Connections [ms]*
T_{Lat}	Parâmetro de sistema configurado *Maximum System Bus Latency [µs]* * 4
T_{Pico}	Picos de carga observados dos programas de aplicação

Esta equação permite calcular um valor adequado para o tempo de Watchdog.

i Em casos isolados, o tempo de Watchdog determinado desta forma pode ser pequeno demais para um Reload.

DICA O tempo de Watchdog determinado pode ser utilizado como tempo de ciclo máximo para a parametrização da safe**ethernet**, veja Manual de comunicação HI 801 240 P.

3.2.3 Tempo de Watchdog do programa de aplicação

Cada programa de aplicação tem um Watchdog e um tempo de Watchdog próprios.

O tempo de Watchdog do programa de aplicação não pode ser ajustado diretamente. O HIMax calcula o tempo de Watchdog de um programa de aplicação a partir dos parâmetros *Max. Watchdog Time* do recurso e *Maximum Number of Cycles*. Para demais detalhes, veja Capítulo 10.2.3 e 10.2.11.

Deve observar que o tempo de Watchdog calculado seja no máximo tão grande quanto o tempo de reação resultante necessário para a parte do processo processada pelo programa de aplicação.

3.2.4 Tempo de segurança do PES

O tempo de segurança é o tempo máximo permitido, dentro do qual o PES deve reagir a uma solicitação. Solicitações são:

- Alterações de sinais de entrada do processo
- Ocorrência de um erro dentro do sistema de comando.

Para os sistemas de comando HIMax, o tempo de segurança pode ser ajustado na faixa de 20 ms até 22.500 ms.

Dentro do tempo de segurança do sistema de comando, os dispositivos de autoteste detectam erros que podem levar a um estado operacional perigoso. Eles acionam reações de erro definidas que conduzem as peças avariadas para um estado seguro.

Durante a medição do tempo de segurança, o usuário deve considerar as seguintes influências:

- Deve-se considerar nos módulos de entrada:
  Nos retardos de ligação/desligamento configurados para os canais de entrada:
  máximo tempo de retardo ajustado em µs + 2* tempo de ciclo do módulo de E/S
- A supressão de avarias também requer uma margem de tempo.

Para o tempo de segurança, deve-se selecionar um ajuste que seja grande o suficiente para considerar o maior dos fatores citados, mas que seja menor que o FTT do processo. Neste processo, deve-se levar em conta os tempos dos sensores e dos atuadores para a função de segurança.

O tempo de segurança para o sistema de comando é:

Tempo de segurança > 2 * tempo de Watchdog + máximo tempo de ciclo + 2 * tempo de ciclo dos módulos de E/S

O usuário deve medir o máximo tempo de ciclo na aplicação concreta através da troca de um módulo processador redundante. O tempo de ciclo máximo determinado neste processo com o sistema completo deve ser utilizado na fórmula acima. O tempo de ciclo dos módulos de E/S é de 2 ms.

Assim, garante-se o máximo grau de disponibilidade.

3.2.5 Tempo de segurança do programa de aplicação

O tempo de segurança do programa de aplicação não pode ser ajustado diretamente. O HIMax calcula o tempo de segurança de um programa de aplicação a partir dos parâmetros *Max. Safety Time* do recurso e *Max. Safety Time*. Para demais detalhes, veja Capítulo 10.2.3 e 10.2.11.

3.2.6 Tempo de reação

O tempo de reação de sistemas de comando HIMax operando ciclicamente é o dobro do tempo de ciclo desses sistemas, se não houver um retardo através de parametrização ou da lógica do programa de aplicação.

O tempo de ciclo de um sistema de comando é composto pelos seguintes componentes:

- Processamento de entrada.
  - Processamento dos dados de entrada no módulo de entrada.
  - Leitura dos dados de processo a partir das interfaces de comunicação.
  - Leitura dos dados de processo a partir dos módulos de entrada.
- Processamento da lógica do usuário.
- Processamento de saída.
  - Escrita dos dados de processo nos módulos de saída.
  - Escrita dos dados de processo nas interfaces de comunicação.
  - Processamento dos dados de saída nos módulos de saída.
- Processamento adicional
  de ações subsequentes para Reload, módulos processadores acrescentados, etc.

O tempo de reação é válido para um programa de aplicação que dura somente um ciclo do módulo processador. Em programas de aplicação cuja sequência se distribui em vários ciclos do módulo processador, o tempo de reação aumenta para a quantidade de ciclos multiplicada pelo dobro da duração do ciclo. Para demais detalhes, veja Capítulo 10.2.3 e 10.2.11.

3.3 Repetição da verificação

Uma repetição da verificação é uma verificação para detectar erros escondidos em um sistema relacionado à segurança, de modo que o sistema, caso necessário, possa ser restaurado a um estado no qual ele cumpre sua função planejada.

Sistemas de segurança HIMA devem ser submetidos a uma repetição da verificação **em intervalos de 10 anos**. O intervalo pode ser prolongado frequentemente através de uma análise mediante cálculo dos circuitos de segurança realizados.

3.3.1 Execução da repetição da verificação

A execução da repetição da verificação depende como a instalação (EUC = equipment under control – equipamento sob controle) é configurada e do potencial de risco que ela tem, além das normas que são aplicáveis na operação da instalação e exigidas pela instituição de verificação responsável para sua aprovação.

De acordo com as normas IEC 61508 1-7, IEC 61511 1-3, IEC 62061 e VDI/VDE 2180, folhas 1 a 4, a empresa operadora é responsável pela realização da repetição da verificação nos sistemas direcionados à segurança.

3.3.2 Frequência das repetições da verificação

O sistema de comando HIMax pode ser submetido a uma repetição da verificação através da verificação do completo circuito de segurança.

Na prática, um intervalo mais curto é exigido para dispositivos de campo de entrada e de saída para a repetição da verificação (p. ex., a cada 6 ou 12 meses) em relação ao sistema de comando HIMax. Quando o usuário verifica o circuito de segurança completo por causa

do dispositivo de campo, o sistema de comando HIMax é automaticamente incluído neste teste. Portanto, torna-se desnecessário realizar repetições adicionais da verificação para o sistema de comando HIMax.

Caso a repetição da verificação dos dispositivos de campo não incluir o sistema de comando HIMax, é necessário verificar o mesmo pelo menos uma vez a cada 10 anos para SIL 3. Isso pode ser alcançado reiniciando o sistema de comando HIMax.

3.4 Requisitos para segurança

Para a utilização do PES direcionado à segurança do sistema HIMax, são válidos os seguintes requisitos de segurança:

3.4.1 Configuração do hardware

As pessoas que configuram o hardware HIMax devem observar os requisitos de segurança listados abaixo.

Requisitos independentes do produto

- Para assegurar a operação direcionada à segurança, utilizar apenas módulos de hardware e componentes de software à prova de erros e autorizados para tal. Os módulos de hardware e componentes de software autorizados estão especificados na *Lista de Versão dos Módulos e do Firmware dos Sistemas HIMax da firma Paul Hildebrandt GmbH*. As últimas versões encontram-se na lista de versão mantida junta com a instituição de verificação.
- É imprescindível cumprir as condições de utilização especificadas (veja Capítulo Condições de utilização) relativas à CEM, às influências mecânicas, químicas e climáticas.

Requisitos dependentes do produto

- Conectar no sistema apenas equipamentos que tenham um desligamento seguro da rede.
- As condições de utilização mencionadas no manual de sistema devem ser cumpridas, particularmente no que diz respeito à tensão de alimentação, ventilação, etc.
- Para o processamento de tarefas direcionadas à segurança, devem ser utilizados apenas módulos direcionados à segurança.

3.4.2 Programação

As pessoas que criam programas de aplicação devem observar os requisitos de segurança listados abaixo.

Requisitos independentes do produto

- Em aplicações relacionadas à segurança, deve-se observar uma correta parametrização dos tamanhos dos sistemas relacionados à segurança.
- Deve-se observar particularmente a definição da configuração do sistema, do máximo tempo de ciclo e do tempo de segurança.

3.4.3 Requisitos para a utilização do sistema de programação

- Para a programação, deve-se utilizar a ferramenta SILworX.
- Através da dupla compilação no SILworX e comparando os CRCs dos dois arquivos criados, garante-se que a compilação foi realizada corretamente.
- **A implementação correta da especificação da aplicação deve ser validada, verificada e documentada. É necessário realizar uma verificação completa da lógica através de teste.**
- Em caso de alteração da aplicação, verificar no mínimo todos os componentes da lógica que foram atingidos pela alteração.

- A reação de erro do sistema em caso de erros nos módulos de entrada e de saída seguros deve ser determinada de acordo com as características relacionadas à segurança específicas da instalação através da configuração. Exemplos:
  - Reação de erro no programa de aplicação
  - Parametrização de valores iniciais seguros para variável

3.4.4 Comunicação

- Na utilização de comunicação direcionada à segurança entre diversos equipamentos, deve-se observar que o tempo completo de reação do sistema não exceda o tempo de tolerância de falhas FTT. Deve-se utilizar as bases de cálculo listadas no Capítulo 11.2.
- Não é permitida uma transmissão dos dados relacionados à segurança via redes públicas (p. ex., internet) sem medidas de segurança adicionais, p. ex.: túnel VPN.
- Caso a transmissão dos dados seja realizada via redes internas da firma/fábrica, é necessário tomar as devidas medidas administrativas ou técnicas de modo tal que haja proteção suficiente contra manipulação (p. ex., usando um firewall para separar a parte relevante à segurança da rede de outras redes).
- Os protocolos padrão não podem ser utilizados para a transmissão de dados relacionados à segurança.
- Só é permitido conectar equipamentos nas interfaces de comunicação que garantam uma separação elétrica segura.

3.4.5 Trabalhos de manutenção

- Para trabalhos de manutenção é necessário observar as respectivas versões atuais do documento “Maintenance Override” da TÜV Rheinland e TÜV Product Service.
- Sempre que necessário, a empresa operadora deve consultar a respectiva instituição de verificação responsável para a aplicação para definir medidas administrativas para a proteção do acesso aos sistemas.

3.5 Certificação

Os equipamentos de automação HIMA direcionados à segurança (Sistemas Eletrônicos Programáveis – PES) do sistema HIMax devem ser verificados de acordo com as normas para a segurança funcional listadas a seguir e certificadas pela TÜV e em conformidade com CE:

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

Certificado e relatório de teste
Equipamentos de automação direcionados à segurança HIMax

Finalidade de uso: “Safety Related Programmable Electronic System for process control, Burner Management (BMS), emergency shut down and machinery, where the demand safe state is the de-energized state.
Applications, where the demand state is the de-energized or energized state”.
(Sistema Eletrônico programável e direcionado à segurança para sistemas de comando de processo, controle de queimadores (BMS), sistemas de desligamento de emergência e sistemas de comando de máquinas, nos quais o estado seguro de demanda é o estado desenergizado.
Aplicações, nas quais o estado seguro de demanda é o estado desenergizado ou energizado.)

Normas internacionais:		
EN/IEC 61508, partes 1–7: 2000		SIL 3
EN/IEC 61511: 2004		SIL 3
EN/ISO 13849-1: 2008		Performance level e
EN/IEC 62061: 2005	Incl. Ber 1 e Ber 2: 2009	
EN 50156-1: 2006		
EN 12067-2: 2004		
EN 298: 2004	+Ber 1: 2006	
EN 230: 2005		
NFPA 85: 2007		
NFPA 86: 2007		
EN/IEC 61131-2: 2007		
EN/IEC 61000-6-2: 2005		
EN 61000-6-4: 2007		
EN 54-2: 1997	/A1: 2007	
NFPA 72: 2002		

O capítulo “Requisitos operacionais” contém uma lista detalhada de todas as verificações ambientais e de CEM realizadas.

Todos os equipamentos possuem a marca de certificação CE.

Para programar os sistemas de comando HIMax, é utilizado um PADT, ou seja, um PC com o sistema de programação

SILworX

instalado. Ele auxilia o usuário na criação de programas direcionados à segurança com as linguagens de programação Funktionsbausteinsprache (FBS – linguagem de bloco funcional) e a linguagem SFC conforme IEC 61131-3, bem como a operação dos equipamentos de automação. Para demais detalhes, consulte a ajuda on-line do SILworX e o Manual de primeiros passos SILworX HI 801 239 P.

4 Módulo processador

A função de segurança do módulo processador consiste no processamento do programa de aplicação através de dois processadores que comparam seus dados constantemente. Em caso de erros, o Watchdog coloca o módulo no estado seguro e comunica o status de CPU.

Para mais detalhes sobre os módulos processadores, veja os manuais.

4.1 Autotestes

As seções seguintes especificam as rotinas de autotestes mais importantes dos módulos processadores direcionados à segurança:

- Teste de processador
- Teste de memória
- Teste de comparador
- Teste CRC nas memórias não voláteis
- Teste de Watchdog

4.2 Reações a erro no módulo processador

Um comparador de hardware dentro do módulo processador compara constantemente se os dados do sistema de microprocessador 1 são idênticos aos dados do sistema de microprocessador 2. Se este não for o caso, ou se as rotinas de teste encontrarem erros no módulo processador, o sistema de comando passa automaticamente para PARADA POR ERRO e o sinal de Watchdog será desligado. O módulo processador não processa mais nenhum programa de aplicação e coloca as saídas no estado desenergizado e desligado.

4.3 Troca de módulos processadores

Antes da troca de módulos processadores, deve-se observar que um sistema HIMax ainda em funcionamento neste processo não é parado.

Isso se aplica sobretudo a sistemas que funcionam de acordo com o princípio de circuito aberto. Nestes casos, uma falha do sistema causa a perda da função de segurança.

Módulos processadores redundantes podem ser trocados durante o funcionamento, contanto que no mínimo um módulo processador ainda esteja disponível e que mantenha a operação direcionada à segurança durante a troca.

NOTA

É possível a interrupção da operação direcionada à segurança!

A operação do sistema de comando pode ser interrompida através da troca de um módulo processador, no qual o LED Ess **está aceso ou piscando.**

Não remover módulos processadores, nos quais o LED Ess **está aceso ou piscando!**

O LED **Ess** aceso ou piscando é um indício de que o módulo processador está sendo indispensável para o funcionamento do sistema.

Mesmo quando o LED não acender/não piscar, as redundâncias do sistema, das quais este módulo processador participa, devem ser verificadas utilizando o SILworX. Neste processo, também observar as ligações de comunicação que são efetuadas via módulo processador.

Para mais detalhes sobre a troca de módulos processadores, recomenda-se consultar o Manual do módulo processador HI 801 254 P e o Manual de sistema HI 801 242 P.

5 Módulo de barramento de sistema

Um módulo de barramento de sistema administra um dos dois barramentos de sistema direcionados à segurança. Os dois barramentos de sistema operam de forma redundante entre si. Cada barramento de sistema liga todos os módulos e o suporte básico entre si. Através dos barramentos de sistema, os dados são transmitidos utilizando um protocolo direcionado à segurança.

É possível operar um sistema HIMax que contenha **apenas um módulo processador** em caso de disponibilidade reduzida com apenas um barramento de sistema.

5.1 ID de Rack

O ID de Rack identifica um suporte básico dentro de um recurso e precisa ser inequívoco para cada suporte básico.

O ID de Rack é o **parâmetro de segurança** para o endereçamento dos suportes básicos individuais e dos módulos que se encontram neles!

O ID de Rack é armazenado no Connector Board do módulo de barramento de sistema. Se o ID de Rack tiver que ser alterado, p. ex., na instalação de um novo sistema HIMax, deve-se cumprir os procedimentos descritos no manual de sistema.

O procedimento para ajustar o ID de Rack está descrito no manual de sistema HI 801 242 P e no Manual de primeiros passos HI 801 239 P.

5.2 Responsibility

Apenas um dos módulos de barramento de sistema por barramento de sistema pode ter o atributo “responsible” e ser assim parametrizado como o responsável pela operação do barramento de sistema.

- Para o barramento de sistema A, o atributo “responsible” é definido fixamente para o barramento de sistema no rack 0, slot 1.
- Para o barramento de sistema B, é possível ajustar o atributo com SILworX.

O módulo de barramento de sistema “responsible” deve estar no suporte básico 0 ou no suporte básico 1.

Certifique-se de que estes requisitos sejam cumpridos antes de começar a operação direcionada à segurança.

O procedimento para ajustar a Responsibility está descrito no Manual de primeiros passos HI 801 239 P.

⚠ ALERTA

Possibilidade de ferimentos!

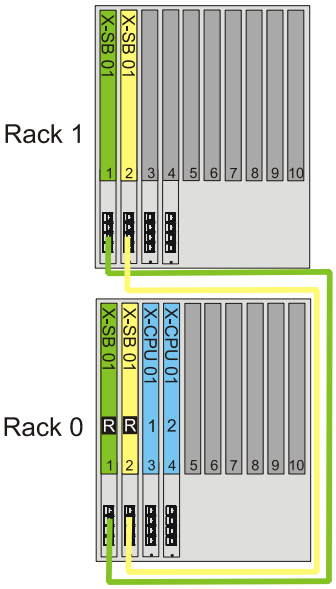
A parametrização deve ser verificada utilizando o SILworX.

Neste processo, é imprescindível proceder da seguinte maneira:

- **Registre-se no SILworX por login de módulo no módulo de barramento de sistema no rack 0, slot 2**
- **Registre-se no SILworX por login de módulo no módulo de barramento de sistema no rack 1, slot 2**
- **Verificar nos Control-Panels dos dois módulos de barramento de sistema para se certificar que o atributo “responsible” só está colocado no módulo de barramento de sistema correto (veja Figura 1 e Figura 2)!**

Configurações recomendadas:

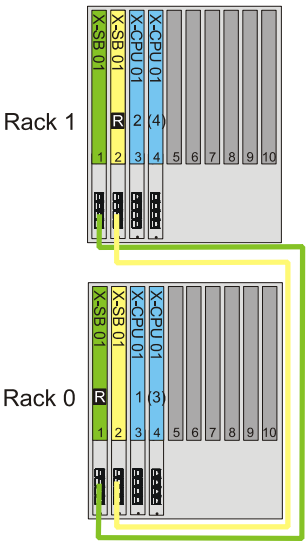
- Se o rack 0 só incluir módulos processadores, os dois módulos de barramento de sistema no rack 0 devem ser colocados em Responsible (Figura 1).
- Se o rack 1 também contiver módulos processadores (Figura 2), colocar os seguintes módulos de barramento de sistema em Responsible:
  - no rack 0 o módulo de barramento de sistema no slot 1.
  - no rack 1 o módulo de barramento de sistema no slot 2.



Rack 0 Suporte básico 0 Rack 1 Suporte básico 1

R Módulo de barramento de sistema colocado no Responsible

Figura 1: Configuração recomendada: Todos os módulos processadores no rack 0



Rack 0 Suporte básico 0 Rack 1 Suporte básico 1

R Módulo de barramento de sistema colocado no Responsible

Figura 2: Configuração recomendada: Módulos processadores no rack 0 e rack 1

6 Módulo de comunicação

Módulos de comunicação realizam tanto a transferência de dados direcionada à segurança com outros sistemas de comando HIMA quanto a transferência de dados direcionada à segurança via barramentos de campo e Ethernet.

- O módulo processador controla a transferência de dados direcionada à segurança através do protocolo de transferência certificado SIL 3 safe**ethernet**. O módulo de comunicação encaminha pacotes de dados para o outro sistema. Através do protocolo direcionado à segurança garante-se que falsificações de mensagens sejam detectadas (Princípio Black Channel).

  Assim é possível a comunicação direcionada à segurança através de caminhos de transmissão não direcionados à segurança, ou seja, componentes de rede padrão.
- O protocolos padrão são p. ex.:
  - Modbus
  - PROFIBUS Master/Slave

Um sistema HIMax só pode ter no máximo 20 módulos de comunicação.

Para mais informações, veja Capítulo 11.1, o Manual do módulo de comunicação HI 801 253 P e o Manual de comunicação HI 801 240 P.

7 Módulos de entrada

Módulo	Quantidade de canais	Direcionado à segurança	Canais livres de efeitos de retro-alimentação	Observação
Entradas digitais				
X-DI 16 01	16	SIL 3	•	120 VCA
X-DI 32 01	32	SIL 3	•	
X-DI 32 02	32	SIL 3	•	Iniciadores (NAMUR)
X-DI 32 03	32	SIL 3	•	48 VCC
X-DI 32 04	32	SIL 3	•	Com registro de sequência de eventos
X-DI 32 05	32	SIL 3	•	Iniciadores (NAMUR), com registro de sequência de eventos
X-DI 32 51	32	-	•	
X-DI 32 52	32	-	•	Iniciadores (NAMUR)
X-DI 64 01	64	SIL 3	•	
X-DI 64 51	64	-	•	
Entradas analógicas				0/4...20 mA
X-AI 16 51	16	SIL 1	•	
X-AI 32 01	32	SIL 3	•	
X-AI 32 02	32	SIL 3	•	Com registro de sequência de eventos
X-AI 32 51	32	-	•	
Entradas do contador				
X-CI 24 01	24	SIL 3	•	
X-CI 24 51	24	-	•	

Tabela 9: Visão geral dos módulos de entrada

7.1 Informações gerais

Entradas direcionadas à segurança podem ser utilizadas tanto para sinais direcionados à segurança como para sinais não direcionados à segurança. Porém, os sinais não direcionados à segurança não podem ser utilizados para funções de segurança!

Além dos LEDs de diagnóstico dos módulos, os sistemas de comando criam mensagens de erro e de status que são salvas. O PADT pode ler estas mensagens salvas na memória de diagnóstico.

Módulos de entrada direcionados à segurança executam automaticamente um autoteste cíclico de alta qualidade durante a operação.

Em caso de erro, um valor inicial é colocado à disposição do programa de aplicação através de uma variável global, e, se possível, é criada uma informação de erro.
Esta informação de erro pode ser avaliada no programa de aplicação através da leitura do código de erro.

Para mais detalhes dos módulos de entrada, veja os manuais de módulo.

7.2 Segurança de sensores, encoders e transmissores

Em uma aplicação direcionada à segurança, tanto o PES como os sensores, encoders e transmissores conectados a ele devem corresponder aos requisitos de segurança e ao SIL especificado. Para tal, veja “Aumento do valor SIL de sensores e atuadores” no anexo.

7.3 Entradas digitais direcionadas à segurança

O módulo de entradas digitais lê suas entradas digitais uma vez em cada ciclo do módulo e salva os valores internamente. O módulo testa ciclicamente se as entradas estão funcionando de forma segura.

Sinais de entrada que existem por um tempo menor do que o tempo entre duas amostragens, p. ex., mais curtos do que um tempo de ciclo do módulo de entrada, em certos casos não são registrados.

7.3.1 Rotinas de teste

As rotinas de teste on-line verificam se os canais de entrada estão em condições de encaminhar os dois níveis de sinal (sinal 0 e 1) independentemente dos sinais de entrada atualmente presentes. Este teste de função é executado em cada leitura dos sinais de entrada.

7.3.2 Reação em caso de erro

Se as rotinas de teste detectarem um erro para uma entrada digital, o módulo coloca o valor de canal de tal modo que a variável global, atribuída ao canal pelo usuário, assume os seguintes valores:

- Nos erros que podem ser diagnosticados, a variável global assume seu valor inicial configurado. O módulo coloca o status Channel OK em FALSE.
- Em caso de erros seguros que não podem ser diagnosticados, o módulo não pode criar itens de diagnóstico.
  Neste tipo de erros, a variável global assume o valor seguro 0.

Se as rotinas de teste detectarem um erro para o módulo ou para o submódulo, o módulo coloca o status *Module OK* e/ou *Submodule OK* em FALSE. Além disso, o módulo ou submódulo coloca *Channel OK* para todos os seus canais em FALSE.

Em todos os casos, o módulo ativa o LED *Error* na placa frontal.

7.3.3 Operação de acordo com o princípio de circuito aberto

É permitido operar entradas digitais conforme o princípio de circuito aberto. Neste caso, deve-se utilizar módulos de entrada com supervisão de linha.

7.3.4 Redundância

É permitido conectar entradas digitais redundantes. A conexão redundante normalmente serve para o aumento da disponibilidade.

Outras conexões – para aumentar o valor SIL – requerem um tratamento dos estados de erro na lógica do programa do usuário.

7.3.5 Surges em entradas digitais

NOTA

Em caso de utilização de cabos blindados para entradas digitais não são necessárias medidas adicionais para proteger contra surges.

Se **não** forem usados cabos blindados, em entradas digitais – devido ao breve tempo de ciclo dos sistemas HIMax – é possível ler um pulso de surge conforme EN 61000-4-5 como sinal 1 de curta duração.

Para evitar tais funções de erro, deve-se aplicar o retardo de ligação/desligamento do canal: um sinal deve estar presente por um determinado período mínimo de tempo antes de ser avaliado. Neste processo, o tempo de Watchdog não pode ser excedido.

7.4 Entradas analógicas direcionadas à segurança

Canais de entrada analógicas convertem as correntes de entrada medidas em um valor do tipo de dados DINT (double integer); o *valor cru (raw value)*, e em um *valor de processo (process value)* do tipo de dados REAL. O *valor cru (raw value)* contém o sinal de entrada medido, enquanto o valor de processo é um valor escalado.

A precisão relacionada à segurança é a precisão garantida da entrada analógica sem reação de erro do módulo. Este valor deve ser levado em conta durante a parametrização de funções de segurança.

7.4.1 Rotinas de teste

O módulo registra os valores analógicos em dois caminhos e compara os resultados entre si. Além disso, ele testa ciclicamente a função dos caminhos de entrada.

7.4.2 Reação em caso de erro

Se as rotinas de teste detectarem um erro para uma entrada analógica, o módulo coloca o valor de canal de tal modo que a variável global, atribuída ao *valor de processo (process value)* do canal, assume os seguintes valores:

- Nos erros que podem ser diagnosticados, a variável global assume seu valor inicial configurado.
- Em caso de erros seguros que não podem ser diagnosticados, o módulo não pode criar itens de diagnóstico.
  Neste tipo de erros, a variável global assume o valor seguro 0.

O módulo coloca o status *Channel OK* em FALSE.

O *valor cru (raw value)* do canal não reage a erro. Em caso de utilização do valor cru, é necessário que o programa de aplicação execute o tratamento de erro.

Se as rotinas de teste detectarem um erro para o módulo ou para o submódulo, o módulo coloca o status *Module OK* e/ou *Submodule OK* em FALSE. Além disso, o módulo ou submódulo coloca *Channel OK* para todos os seus canais em FALSE.

Em todos os casos, o LED *Error* é ativado na placa frontal.

7.4.3 Operação de acordo com o princípio de circuito aberto

É permitido operar entradas analógicas conforme o princípio de circuito aberto.
Neste caso, deve-se utilizar a supervisão de linha.

7.4.4 Redundância

É permitido conectar entradas analógicas redundantes. A conexão redundante normalmente serve para o aumento da disponibilidade.

Outras conexões – para aumentar o valor SIL – requerem um tratamento dos estados de erro na lógica do programa do usuário.

7.5 Entradas do contador direcionadas à segurança

Uma entrada de contador direcionada à segurança pode, dependendo de sua configuração, fornecer os seguintes valores de processo:

- O valor indicado no contador como valor integral ou como valor de ponto flutuante escalado
- Uma rotação ou frequência como valor integral ou como valor de ponto flutuante
- Valores auxiliares adicionais tais como transbordamento.

Para maiores detalhes, veja Manual do módulo HI 801 251 P.

7.5.1 Rotinas de teste

O módulo registra os valores do contador em três caminhos paralelos e compara os resultados entre si. Além disso, ele testa ciclicamente a função dos caminhos de entrada.

7.5.2 Reação em caso de erro

Se as rotinas de teste detectarem um erro para uma entrada do contador, o módulo coloca o valor de canal de tal modo que as variáveis globais, atribuídas pelo usuário ao canal, assumem os seguintes valores:

- As variáveis globais atribuídas ao parâmetro -> *Rotation Speed [mHz] [DINT]* e -> *Rotation Speed [mHz] [DINT]*, assumem o Valor 0.
- As variáveis globais atribuídas ao parâmetro -> *Counter Reading [mHz]* assume o último valor válido.

O módulo coloca o status *Channel OK* em FALSE.

Se as rotinas de teste detectarem um erro para o módulo ou para o submódulo, o módulo coloca o status *Module OK* e/ou *Submodule OK* em FALSE. Além disso, o módulo ou submódulo coloca *Channel OK* para todos os seus canais em FALSE.

Em todos os casos, o LED *Error* é ativado na placa frontal.

7.5.3 No caso do módulo contador X-CI 24 01 observar o seguinte!

Ao utilizar o módulo contador X-CI 24 01, devem ser observadas as seguintes particularidades; veja também o Manual do módulo HI 801 251 P:

- Durante o Reload, é possível a perda de pulsos de entrada dentro dos 3 primeiros ciclos se os seguintes parâmetros forem alterados durante o Reload:
  - Tipo de avaliação de pulsos de contagem
  - Pares de canal utilizados
- Se houver falha do sensor de um canal durante a avaliação de flanco “2 fases, 4 flancos” sem que seja detectada uma quebra de fio ou um curto de linha, o módulo registra a metade da verdadeira frequência.
- Os parâmetros de canal -> *Level* e -> *Count.Read (revolv.)* não podem ser utilizados para aplicações direcionadas à segurança!
- Os pulsos a serem contados podem ser perdidos durante o reinício automático.
- O reinício automático ou manual do módulo deve ser considerado como específico da aplicação.
- Recomendação da aplicação:
  - Recomenda-se a utilização de sensores redundantes em caso de avaliação de multifase e de reconhecimento do sentido de rotação, visto que somente assim é possível reconhecer a falha de sensor.
  - A parametrização da supressão de avarias durante a medição de frequência é irrelevante do ponto de vista relacionado à segurança.

7.5.4 Operação de acordo com o princípio de circuito aberto

É permitido operar entradas do contador de acordo com o princípio de circuito aberto. Neste caso, deve-se utilizar módulos de entrada com supervisão de linha.

7.5.5 Redundância

É permitido conectar entradas do contador redundantes. A conexão redundante normalmente serve para o aumento da disponibilidade.

Outras conexões – para aumentar o valor SIL – requerem um tratamento dos estados de erro na lógica do programa do usuário.

7.6 Listas de verificação das entradas

A HIMA recomenda utilizar as listas de verificação disponíveis para a projetar, programar e colocação em funcionamento de entradas direcionadas à segurança. As listas de verificação podem ser utilizadas como documentos de planejamento, mas servem ao mesmo tempo para demonstrar posteriormente que o planejamento foi realizado criteriosamente.

Para canais de entrada direcionados à segurança utilizados em um sistema dentro do âmbito do projeto e/ou colocação em funcionamento, é útil preencher uma lista de verificação para o controle dos requisitos a serem considerados. Só assim é possível garantir que os requisitos foram registrados inteiramente e de forma clara. A lista de verificação também é uma documentação sobre a relação entre a fiação externa e o programa de aplicação.

As listas de verificação estão disponíveis na homepage da HIMA no formato Microsoft® Word®.

8 Módulos de saída

Módulo	Quantidade de canais	Direcionado à segurança	Isolado eletr. e de forma segura	Observação
Saídas digitais				
X-DO 12 02	12	SIL 3	-	
X-DO 24 01	24	SIL 3	-	
X-DO 24 02	24	SIL 3	-	48 VCC
X-DO 32 01	32	SIL 3	-	
X-DO 32 51	32	-	-	
Saídas de relé digitais				
X-DO 12 01	12	SIL 3	•	230 VCA
X-DO 12 51	12	-	•	
Saídas analógicas				
X-AO 16 01	16	SIL 3	em par	
X-AO 16 51	16	-	-	

Tabela 10: Visão geral dos módulos de saída

8.1 Informações gerais

Os módulos de saída direcionados à segurança são descritos uma vez em cada ciclo; os sinais de saída são relidos e comparados com os dados de saída definidos.

Nas saídas, o valor “0” ou contato de relé aberto é o estado seguro.

Com a utilização do respectivo código de erro, há possibilidades adicionais de programar reações de erro no programa de aplicação.

Para mais detalhes dos módulos de saída, veja os manuais de módulo.

8.2 Segurança de atuadores

Em uma aplicação direcionada à segurança, tanto o PES como atuadores conectados a ele devem corresponder aos requisitos de segurança e ao SIL especificado. Para tal, veja “Aumentar o valor SIL de sensores e atuadores” no anexo.

8.3 Saídas digitais direcionadas à segurança

Nos canais de saída direcionados à segurança, três interruptores que podem ser testados estão integrados em série adicionalmente ao desligamento de canal único. Assim, cumpre-se o requisito para SIL 3 de acordo com uma segunda via independente e segura de desligamento. Este desligamento de segurança integrado desliga de forma segura em caso de erro os canais individuais do módulo de saída defeituoso (estado desenergizado).

Além disso, o sinal de Watchdog do módulo é a segunda via de desligamento: se ocorrer uma falha do sinal de Watchdog, isso resulta em uma transição imediata para o estado seguro.

8.3.1 Rotinas de teste para saídas digitais

Os módulos são testados automaticamente durante a operação. As funções de teste essenciais são:

- Releitura do sinal de saída do amplificador de comutação. O limiar de comutação para um nível Low relido está abaixo do valor de tensão válido para o tipo de saída. Os diodos utilizados impedem uma realimentação de sinais.
- Verificação do desligamento de segurança duplo e integrado.
- Um teste de desligamento das saídas é realizado ciclicamente para no máx. 200 µs.

Se ocorrerem erros, as saídas são colocadas em um valor seguro.

8.3.2 Reação em caso de erro

Se as rotinas de teste detectarem um erro em um ou mais canais, o módulo desliga esses canais, colocando-os em um estado seguro. Para esses canais, coloca-se o parâmetro *Channel OK* em FALSE.

Se as rotinas de teste detectarem um erro para o módulo ou para o submódulo, o módulo coloca o status *Module OK* e/ou *Submodule OK* em FALSE. Além disso, o módulo ou submódulo coloca *Channel OK* para todos os seus canais em FALSE.

Em todos os casos, indica-se adicionalmente o erro com o LED *Error* na placa frontal.

8.3.3 Comportamento em caso de curto-circuito ou sobrecarga externa

Em caso de curto-circuito da saída para L ou em caso de sobrecarga, é mantida a testabilidade do módulo. Não é necessária uma transição para o estado seguro.

As saídas são verificadas ciclicamente neste estado em um intervalo de poucos segundos para detectar se ainda há sobrecarga. Em caso de estado normal, as saídas são religadas.

NOTA

Existe a possibilidade de avarias operacionais!

A tensão induzida durante o desligamento de cargas indutivas poderia causar avarias no sistema de comando ou em outros sistemas eletrônicos nas proximidades do condutor do atuador.

Por esta razão, considera-se uma boa prática conectar cargas indutivas com um circuito de roda livre adequado no participante para atuar contra essas avarias.

8.3.4 Operação de acordo com o princípio de circuito aberto

É permitido operar saídas digitais conforme o princípio de circuito aberto. Neste caso, deve-se utilizar a supervisão de linha.

8.3.5 Redundância

É permitido conectar saídas digitais redundantes. A conexão redundante normalmente serve para o aumento da disponibilidade.

Outras conexões – para aumentar o valor SIL – requerem um tratamento dos estados de erro na lógica do programa do usuário.

8.4 Saídas de relé direcionadas à segurança

Placas de saída de relé são utilizadas quando uma ou mais das seguintes condições para o atuador conectado estiverem presentes:

- Separação elétrica é necessária.
- Amperagens mais elevadas são usadas.
- Conexão de correntes alternadas.

No módulo, as saídas são equipadas com dois relés de segurança com contatos guiados. Assim, as saídas podem ser utilizadas para desligamentos de segurança conforme SIL 3.

Além disso, o sinal Watchdog do módulo também fornece uma segunda possibilidade do desligamento de segurança: se ocorrer uma falha do sinal de Watchdog, isso resulta em uma transição imediata para o estado seguro.

8.4.1 Rotinas de teste para saídas de relé

O módulo é testado automaticamente durante a operação. As funções de teste essenciais são:

- Relendo os sinais de saída do amplificador de comutação do relé,
- Testando a comutação do relé com contatos guiados,
- Verificação do desligamento de segurança duplo e integrado.

8.4.2 Reação em caso de erro

Se for detectado um sinal com erro, a saída afetada do módulo é colocada no estado desenergizado e seguro através do interruptor de segurança. Em caso de erro do módulo, todas as saídas do módulo são desligadas. Os dois tipos de falha são indicados adicionalmente com o LED Error.

NOTA

Existe a possibilidade de avarias operacionais!

A tensão induzida durante o desligamento de cargas indutivas poderia causar avarias no sistema de comando ou em outros sistemas eletrônicos nas proximidades do condutor do atuador.

Por esta razão, considera-se uma boa prática conectar cargas indutivas com um circuito de roda livre adequado no participante para atuar contra essas avarias.

A quantidade de ciclos de manobra é limitado de acordo com as respectivas normas, p. ex., a norma de queimadores EN 50156-1. Para mais detalhes, veja o Manual do módulo HI 801 265 P.

Após o contador de ciclo de manobras ter expirado, deve-se trocar o módulo!

8.4.3 Operação de acordo com o princípio de circuito aberto

É permitido operar saídas de relé digitais conforme o princípio de circuito aberto.

8.4.4 Redundância

É permitido conectar saídas de relé digitais redundantes. A conexão redundante normalmente serve para o aumento da disponibilidade.

Outras conexões – para aumentar o valor SIL – requerem um tratamento dos estados de erro na lógica do programa do usuário.

8.5 Saídas analógicas direcionadas à segurança

Estas encaminham valores determinados no programa de aplicação para os atuadores.

Saídas analógicas direcionadas à segurança releem seus valores de saída e comparam esses valores com os valores a serem emitidos. Em caso de desvios ocorre a reação de erro.

8.5.1 Rotinas de teste para saídas analógicas

Os módulos são testados automaticamente durante a operação. As funções de teste essenciais são:

- Leitura do sinal de saída.
- Verificação do desligamento de segurança duplo e integrado.

Se houver erros, as saídas são colocadas no valor seguro 0 mA.

8.5.2 Reação em caso de erro

Se as rotinas de teste detectarem um erro em um ou mais canais, o módulo desliga esse(s) grupo(s) de canal, colocando-os em um estado seguro. Para esses canais, coloca-se o parâmetro *Channel OK* em FALSE.

Se as rotinas de teste detectarem um erro para o módulo ou para o submódulo, o módulo coloca o status *Module OK* e/ou *Submodule OK* em FALSE. Além disso, o módulo ou submódulo coloca *Channel OK* para todos os seus canais em FALSE.

Em todos os casos, indica-se adicionalmente o erro com o LED *Error* na placa frontal.

8.5.3 Procedimento em caso de quebra de fio externo

Em caso de quebra de fio, o módulo desliga a corrente por aprox. 8 ms e verifica se a quebra de fio ainda permanece. Se este for o caso, ele desliga por aprox. 10 s. Esta sequência pode ser repetida quantas vezes quiser.

8.5.4 Observe os seguintes itens se usar o módulo de saída X-AO 16 01!

Se usar o módulo de saída analógico, é imprescindível observar as seguintes particularidades; veja também o Manual do módulo HI 801 248 P:

- Só são permitidas os tipos de ligação listados no Manual do módulo HI 801 248 P!
- Em caso de redundância serial de mais de dois módulos, a tensão SELV pode ser excedida!
- Em caso de redundância serial, deve-se utilizar apenas um canal de cada grupo de dois canais!
- Se for estabelecida a comunicação HART entre o atuador conectado e um terminal HART, o sinal de saída pode falsificá-los em até 2 % do valor final!
- Em caso de erro, o intervalo de tempo até atingir o estado seguro em Worst Case pode ser de até 16 ms. Considerar este tempo de reação e o tempo de segurança!
- O programa de aplicação não pode descrever saídas analógicas em ciclos menores do que 6 ms.
- Em caso de erro, o módulo emite o valor seguro 0 mA, também se o limite superior da faixa de ajuste for excedida.

8.5.5 Operação de acordo com o princípio de circuito aberto

É permitido operar saídas analógicas conforme o princípio de circuito aberto. Neste caso, deve-se utilizar a supervisão de linha.

8.5.6 Redundância

É permitido conectar saídas analógicas redundantes. A conexão redundante normalmente serve para o aumento da disponibilidade.

Outras conexões – para aumentar o valor SIL – requerem um tratamento dos estados de erro na lógica do programa do usuário.

8.6 Listas de verificação das saídas

A HIMA recomenda utilizar as listas de verificação disponíveis para projetar, programar e colocar em funcionamento saídas direcionadas à segurança. As listas de verificação podem ser utilizadas como documentos de planejamento, mas servem ao mesmo tempo para demonstrar posteriormente que o planejamento foi realizado criteriosamente.

Para canais de entrada direcionados à segurança utilizados em um sistema dentro do âmbito do projeto e/ou colocação em funcionamento, é útil preencher uma lista de verificação para o controle dos requisitos a serem considerados. Só assim é possível garantir que os requisitos foram registrados inteiramente e de forma clara. A lista de verificação também é uma documentação sobre a relação entre a fiação externa e o programa de aplicação.

As listas de verificação estão disponíveis na homepage da HIMA no formato Microsoft® Word®.

9 Software

O software para os equipamentos de automação direcionados à segurança dos sistemas HIMax consiste dos seguintes componentes:

- Sistema operacional,
- Programa de aplicação,
- Sistema de programação SILworX conforme IEC 61131-3.

O *sistema operacional* está carregado em cada módulo do sistema de comando. Recomenda-se utilizar a versão mais atual para a aplicação direcionada à segurança. Este capítulo aborda particularmente o sistema operacional do módulo processador.

O *programa de aplicação* é criado com o *sistema de programação* SILworX e contém as funções específicas da instalação que o dispositivo de automação deve executar. A parametrização também é realizada via SILworX.

O programa de aplicação é compilado com o gerador de código e, em seguida, é transmitido via interface Ethernet para a memória não volátil dos equipamentos de automação.

9.1 Aspectos relacionados à segurança para o sistema operacional

Cada sistema operacional autorizado é inequívoco através do número de revisão e da assinatura CRC. As versões válidas do sistema operacional e as respectivas assinaturas(CRCs), aprovadas pela TÜV para equipamentos de automação direcionados à segurança, estão sujeitas a controle de revisão e são documentadas na *version list of modules and firmware for HIMax systems from HIMA Paul Hildebrandt GmbH (*lista de versão de módulos e firmware dos sistemas HIMax da Firma HIMA Paul Hildebrandt GmbH*),* elaborada em conjunto com a TÜV.

É possível realizar a leitura da versão do sistema operacional em funcionamento com o sistema de programação SILworX. Os usuários devem verificar se a versão do sistema operacional autorizada está carregada nos módulos (compare 10.3 Lista de verificação para criação de um programa de aplicação).

9.2 Aspectos relacionados à segurança para a programação

Durante a criação de um programa de aplicação, devem-se observar os requisitos aqui mencionados.

9.2.1 Concepção de segurança do SILworX

A concepção de segurança do SILworX:

- Durante a instalação do SILworX, garante-se a integridade do pacote de programa no percurso entre o fabricante e o usuário através de uma soma de verificação CRC.
- SILworX realiza verificações de plausibilidade para reduzir erros durante a introdução de dados.
- A compilação dupla com comparação subsequente das somas de verificação CRC criadas garante que falsificações da aplicação sejam reconhecidas através de funções temporárias de erros dos PCs utilizados.

Compilar duplamente o programa e comparar resultados:

1. Iniciar a compilação.
   ☑ Na conclusão da compilação, o SILworX mostra uma soma de verificação CRC.
2. Reiniciar a compilação.
   ☑ Na conclusão da compilação, o SILworX mostra uma soma de verificação CRC.

Se as duas somas de verificação CRC forem iguais, não houve falsificação na compilação.

Na primeira colocação em funcionamento de um sistema de comando direcionado à segurança, deve-se verificar a segurança do sistema completo através de um teste completo de função.

Teste de função do sistema de comando

1. Verificação se houve a implementação correta das tarefas do sistema de comando a partir dos dados e fluxos de sinal.
2. Completa verificação de função da lógica através de teste (veja Capítulo 9.2.2).

O sistema de comando e o programa de aplicação foram suficientemente verificados.

Após uma alteração do programa de aplicação, devem-se testar apenas aqueles componentes do programa que são afetados pela alteração. Para tal, o comparador seguro de revisão do SILworX pode registrar as alterações em relação à versão anterior e exibi-las para o usuário.

9.2.2 Verificação da configuração e do programa de aplicação

Para verificar se o programa de aplicação criado está cumprindo a função de segurança específica, o usuário deve criar casos de teste adequados que abranjam a especificação.

Via de regra, é suficiente o teste independente de cada loop (composto pela entrada, pelos vínculos lógicos importantes do ponto de vista da aplicação e pela saída).

Para a avaliação numérica de fórmulas, também se deve gerar casos de teste adequados. Testes de classe de equivalência são úteis. Estes são testes realizados dentro de áreas definidas de valores, nos limites ou em áreas de valores inadmissíveis. Os casos de teste devem ser selecionados de modo que se possa provar que o cálculo está correto.
A quantidade necessária de casos de teste depende da fórmula utilizada e deve abranger pares de valores críticos.

A HIMA recomenda que não se abra mão de uma simulação ativa com fontes, visto que só assim é possível provar que há uma fiação correta dos sensores e dos atuadores do sistema (também aqueles conectados via comunicação com Remote I/Os). Somente desta maneira é possível verificar a configuração do sistema.

Deve-se cumprir esse procedimento tanto durante a criação de um programa de aplicação como também nas suas alterações.

9.3 Parâmetros do recurso

⚠ PERIGO

Existe a possibilidade de ferimentos devido à configuração errada!

Nem o sistema de programação nem o sistema de comando podem verificar alguns parâmetros definidos fixamente e específicos do projeto. Por esta razão, é imprescindível introduzir esses parâmetros corretamente no sistema de programação e verificar a entrada realizada.

Os parâmetros são colocados em

- **ID de sistema**
- **ID de rack, veja 5.1 e o Manual de sistema HI 801 242 P.**
- **Atributo de responsável de módulos de barramento de sistema, veja 5.2**
- **Tempo de segurança**
- **Tempo de Watchdog**
- **Liberação principal**
- **Autostart**
- **Permitido Início**
- **Permitido Carregar**
- **Permitido Reload**
- **Permitido Forcing global**

Os seguintes parâmetros listados são definidos no SILworX para as ações permitidas em operação direcionada à segurança do recurso e denominados como parâmetros direcionados à segurança.

Os parâmetros que possam ser definidos durante a operação direcionada à segurança não são ligados de forma rígida a uma determinada classe de requisito, mas devem ser aceitos para cada utilização do dispositivo de automação com a respectiva instituição de verificação.

9.3.1 Parâmetros de sistema do recurso

Os parâmetros de sistema do recurso podem ser ajustados no SILworX, no diálogo *Properties* do recurso.

Parâmetros/ interruptores	Descrição	Valor padrão	Ajuste para a operação segura
Nome	Nome do recurso		livre
System ID [SRS]	System-ID do recurso 1…65 535 É necessário atribuir à ID de sistema um outro valor sem ser o valor padrão, caso contrário, o projeto não é executável!	60 000	Valor único dentro da rede de sistemas de comando. Isso inclui todos os sistemas de comando que potencialmente estão ligados uma à outra.
Safety Time [ms]	Tempo de segurança em milissegundos 20…22 500 ms	600 ms	específico da aplicação
Watchdog Time [ms]	Tempo de Watchdog em milissegundos 6…7500 ms	200 ms	específico da aplicação

Parâmetros/ interruptores	Descrição	Valor padrão	Ajuste para a operação segura
Main Enable	ON: Os seguintes interruptores/parâmetros podem ser alterados pelo durante a operação (= RUN): ▪ *System ID* ▪ *Resource Watchdog Time* ▪ *Safety Time* ▪ *Target Cycle Time* ▪ *Target Cycle Time Mode* ▪ *Autostart* ▪ *Global Forcing Allowed* ▪ *Global Force Timeout Reaction* ▪ *Load Allowed* ▪ *Reload Allowed* ▪ *Start Allowed* OFF: Os parâmetros não podem ser alterados durante a operação. i Apenas com PES parado é possível colocar *Main Enable* em ON – não online!	ON	OFF recomendado
Autostart	ON: Se o módulo processador é ligado à tensão de alimentação, o programa de aplicação inicia automaticamente OFF: Não há início automático depois de ligar a tensão de alimentação.	OFF	específico da aplicação
Start Allowed	ON: Arranque a frio ou arranque quente permitidos pelo PADT no estado RUN ou STOP. OFF: Nenhum arranque permitido	ON	específico da aplicação
Load Allowed	ON: Download do programa de aplicação permitido OFF: Download do programa de aplicação não permitido	ON	específico da aplicação
Reload Allowed	ON: Reload de um programa de aplicação permitido. OFF: Reload de um programa de aplicação não permitido. Um Reload em andamento não é interrompido ao comutar para OFF	ON	específico da aplicação
Global Forcing Allowed	ON: Forcing global para este recurso permitido OFF: Forcing global para este recurso não é permitido	ON	específico da aplicação
Global Force Timeout Reaction	Define como o recurso se comporta no momento do Force-Timeout global se esgotar: ▪ Encerrar Forcing ▪ Parar recurso	Stop Forcing	específico da aplicação
Max.Com. Time Slice ASYNC [ms]	Valor máximo em ms da fatia de tempo que é usada dentro do ciclo do recurso para a comunicação, veja manual de comunicação HI 801 240 P, 2…5 000 ms	10 ms	específico da aplicação
Max. Duration of Configuration Connections [ms]	Define quanto tempo dentro de um ciclo de CPU está disponível para a comunicação de dados de processo, 6…5 000 ms	6 ms	específico da aplicação
Target Cycle Time [ms]	Tempo de ciclo desejado ou máximo, veja *Target Cycle Time Mode*, 0…7500 ms. O tempo de ciclo nominal no máximo pode ter o mesmo tamanho do tempo de Watchdog ajustado, 6 ms, caso contrário, é rejeitado pelo PES.	0 ms	específico da aplicação

Parâmetros/ interruptores	Descrição		Valor padrão	Ajuste para a operação segura
Multitasking Mode	Mode 1	O comprimento do ciclo da CPU depende da duração de execução de todos os programas de aplicação.	Mode 1	específico da aplicação
	Mode 2	O processador disponibiliza o tempo não utilizado dos programas de aplicação de baixa prioridade para programas de aplicação de alta prioridade. Modo de operação para alta disponibilidade.		
	Mode 3	O processador aguarda durante o tempo de execução não usado por programas de aplicação e, assim, prolonga o ciclo.		
Sum of UP Max. Duration for Each Cycle [µs]	Soma dos valores indicados em todos os programas de aplicação para *Max. Duration for each Cycle [µs]*; apenas exibição, não pode ser alterado.		-	-
Target Cycle Time Mode	Utilização do *Target Cycle Time [ms]*.		Fixed	específico da aplicação
	Fixed	O PES mantém o tempo de ciclo nominal e prorroga o ciclo, caso necessário. Isso não vale se o tempo de processamento dos programas de aplicação ultrapassar o tempo de ciclo.		
	Fixed-tolerant	Como em *Fixed*, mas ao sincronizar módulos processadores e no 1º ciclo de ativação do Reload o tempo de ciclo nominal não é observado.		
	Dynamic-tolerant	Como em *Dynamic*, mas ao sincronizar módulos processadores e no 1º ciclo de ativação do Reload o tempo de ciclo nominal não é observado.		
	Dynamic	O HIMax respeita o tempo de ciclo nominal se possível, porém, executa o ciclo no menor tempo possível.		
Minimum Configuration Version	SILworX-V2	A geração de código ocorre como no SILworX V2, exceto no caso de novas funções. Com este ajuste, o Reload de um projeto criado com V2 é possível.	SIL-worX-V4	específico da aplicação
	SILworX-V3	Geração de código para HIMax V3. Com este ajuste, a compatibilidade com versões posteriores está garantida.		
	SILworX-V4	Geração de código para HIMax V4. Com este ajuste, a compatibilidade com versões posteriores está garantida.		
Maximum System Bus Latency [µs]	Retardo máximo de uma mensagem entre um módulo de E/S e o módulo processador. 0, 100…50 000 µs		0 µs	específico da aplicação
	i	Para o ajuste do retardo máximo do barramento de sistema a um valor > 0 é necessária uma licença.		
safeethernet CRC	SILworX V.2.36.0	A formação do CRC para safe**ethernet** ocorre como no SILworX V.2.36.0. Este ajuste é necessário para a troca de dados com recursos que foram planejados com SILworX V.2.36 ou anterior.	Versão atual	específico da aplicação
	Versão atual	A formação do CRC para safe**ethernet** ocorre com o algoritmo atual.		

Tabela 11: Os parâmetros de sistema do recurso

Cálculo da *Maximum Duration of Configuration Connections [µs]*

Se o processamento da comunicação num ciclo de CPU não terminar será continuada no próximo ciclo de CPU imediatamente seguinte, no ponto de interrupção.

A comunicação de dados de processo é retardada desta forma, porém, todas as conexões com parceiros externos são processadas com direitos iguais e de forma completa.

Para o firmware HIMax-CPU V3, a duração máxima das conexões de configuração do SILworX e definida com 6 ms. Porém, a duração de processamento da comunicação com parceiros externos em um ciclo de CPU pode ultrapassar a definição.

Para o firmware HIMax-CPU V4, a duração máxima das conexões de configuração do SILworX deve ser ajustado respeitando o tempo de Watchdog definido.

Ajuste adequado: escolher o valor de forma que no tempo restante *Watchdog Time - Max. Duration of Configuration Connections* as tarefas cíclicas do processador ainda possam ser executadas.

A quantidade de dados de processo a serem comunicados depende da quantidade de Remote-IOs configurados, da conexão existente a PADTs e dos componentes no sistema que possuírem uma interface Ethernet.

Um primeiro ajuste pode ser calculado como seque:

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

T_{Config}	Parâmetro de sistema *Max. Duration of Configuration Connections [ms]*
n_{Com}	Quantidade de módulos com interfaces Ethernet {SB, CPU, COM}
n_{RIO}	Quantidade de Remote IOs configurados
n_{PADT}	Quantidade máx. de conexões PADT = 5
T_{Lat}	Parâmetro de sistema *Maximum System Bus Latency [µs]*

Se o tempo calculado for menor do que 6 ms, é arredondado a 6 ms. Mais tarde, é possível corrigir o tempo calculado com ajuda de estatística Online posteriormente, ou nas características do recurso, ou corrigir diretamente online.

i Ao gerar o código e ao converter projetos, é exibido no PADT um aviso se o *Max. Duration of Configuration Connections* for menor do que o calculo em conjunto.

9.3.2 Variáveis de sistema do hardware

Estas variáveis permitem alterar o comportamento do sistema de comando na operação em funcionamento em determinados estados.

Parâmetros/ interruptores	Função	Ajuste padrão	Ajuste para operação segura
Force Deactivation	Permite evitar o Forcing e desligá-lo imediatamente	OFF	específico da aplicação
Spare 0 ... Spare 16	Sem função	-	-
Emergency Stop 1 ... Emergency Stop 4	Interruptor de parada de emergência para desligar o sistema de comando nos casos de falha detectados pelo programa de aplicação	OFF	específico da aplicação
Read-only in RUN	Após iniciar o sistema de comando nenhuma ação de comando (Stop, Início, Download) pode ser mais realizada via SILworX, exceções: Forcing e Reload	OFF	específico da aplicação
Reload Deactivation	Bloqueia a execução de um Reload	OFF	específico da aplicação

Tabela 12: Variáveis de sistema do hardware

É possível atribuir variáveis globais a estas variáveis de sistema no editor de hardware do SILworX, cujo valor será alterado por uma entrada física ou pela lógica do programa de aplicação.

Exemplo: Trancando e destrancado o PES

"Trancar" o PES significa trancar as possibilidades de acesso pelo usuário durante a operação. Isso também evita uma manipulação não autorizada do programa de aplicação.

"Destrancar" o PES significa remover o trancamento ativo, p. ex., para a execução de medidas no sistema de comando.

As três variáveis de sistema *Read only in Run, Reload Deactivation* e *Force Deactivation* servem para trancar o PES.

Se todas as três variáveis de sistema estiverem ON, não é mais possível o acesso ao sistema de comando. Neste caso, só é possível colocar o sistema de comando de volta para o estado STOP através de Reinício de um módulo do processador com o interruptor de modo na posição *Init*. Assim é possível recarregar um programa de aplicação.

Para poder trancar o sistema de comando

1. Definir variável global do tipo BOOL, colocar o valor inicial em FALSE.
2. Atribuir variáveis globais às três variáveis de sistema *Read only in Run*, *Reload Deactivation* e *Force Deactivation* como variáveis de saída.
3. Atribuir variáveis globais ao valor de canal de uma entrada digital.
4. Conectar um interruptor chave na entrada digital.
5. Compilar programa, carregar no sistema de comando e iniciar.

O proprietário de uma chave correspondente pode trancar e destrancar o sistema de comando. Em caso de erro no respectivo módulo de entrada digital, o sistema de comando é destrancado.

9.4 Forcing

Forcing significa a substituição do valor atual de uma variável por um valor Force. Uma variável pode receber o seu valor atual via uma entrada física, pela comunicação ou por um vínculo lógico. Se a variável for forçada, o seu valor não depende mais do processo, mas é definido pelo usuário.

⚠ ALERTA

Valores forçados podem causar avarias na operação direcionada à segurança!

- **Valores forçados podem resultar em valores de saída incorretos.**
- **Forcing aumenta o tempo de ciclo. Desta forma é possível que o tempo de Watchdog seja ultrapassado.**

Forcing apenas é admissível depois de consultar a instituição de verificação responsável pela certificação do sistema.

Durante o Forcing, a pessoa responsável deve garantir a supervisão suficiente de segurança do processo por outras medidas técnicas e organizacionais.
A HIMA recomenda colocar um limite de tempo para o procedimento Forcing.

Mais detalhes sobre o Forcing encontram-se no Manual de sistema HI 801 242 P.

9.5 Comparador seguro de versão

O comparador seguro de versão do SILworX pode comparar configurações de recurso entre si:

- Configuração de recurso carregada no sistema de comando
- Configuração de recurso presente no PADT

- Configuração de recurso exportada (arquivada)

O resultado do comparador tem a qualidade SIL 3, visto que ele é derivado de arquivos que podem ser carregados e incluem os CRCs.

O comparador seguro de versão deve ser utilizado para a verificação de alterações de programa antes de carregá-lo no sistema de comando.

Ele define exatamente as partes alteradas da configuração de recurso. Isso facilita a verificação das alterações e a identificação de dados de teste.

Programação estruturada e a utilização de nomes significativos a partir da primeira versão de configuração ajudam a compreender o resultado da comparação.

9.6 Proteção contra manipulações

O usuário deve definir em trabalho conjunto com a instituição de verificação quais medidas devem ser utilizadas para a proteção contra manipulação.

No PES e no sistema de programação SILworX, estão integrados mecanismos de proteção que evitam alterações feitas por engano ou alterações não autorizadas no sistema de segurança:

- Uma alteração do programa de aplicação ou da configuração resulta em um novo valor de CRC. Essas alterações podem ser transmitidas ao PES através de um Download ou Reload.
- As opções de comando dependem dos direitos do usuário registrado no PES.
- O sistema de programação SILworX requer uma senha do usuário ao fazer o registro para a conexão com PES.
- A conexão entre PADT e PES não é necessária durante a operação RUN.

Deve-se observar os requisitos das normas de segurança e de aplicação relativas à proteção contra manipulação. A autorização de funcionários e as medidas de segurança necessárias estão sob a responsabilidade da empresa operadora.

⚠ PERIGO

Ferimentos devido à manipulação não autorizada no sistema de comando!

O sistema de comando deve ser protegido contra acessos não autorizados!

P. ex.:

- **Alterar os ajustes padrão para login e senha**
- **Controlar o acesso físico do sistema de comando e do PADT!**

O acesso a dados do PES só é possível se o PADT utilizado tiver o sistema de programação SILworX e o projeto do usuário na versão atual em funcionamento (atualização do arquivo!).

A conexão entre PADT e PES só é necessária para carregar o programa de aplicação ou para o diagnóstico. Durante a operação normal, não é necessário o PADT; uma separação do PADT e do PES na fase normal de operação protege contra acessos não permitidos.

10 Programa de aplicação

Este capítulo aborda aspectos relacionados à segurança para programas de aplicação.

10.1 Sequência geral

Sequência geral da programação dos equipamentos de automação HIMax para aplicações relacionadas à segurança:

1. Especificação da função do sistema de comando.
2. Escrita do programa de aplicação.
3. Compilação do programa de aplicação:
   o programa de aplicação foi criado sem erros e pode rodar.
4. Verificação e validação.

Em seguida, o usuário pode testar o programa de aplicação e, em seguida, o PES pode começar a operação segura.

10.2 Âmbito para o uso direcionado à segurança

(Para mais detalhes sobre definição e regras, explicações sobre os requisitos para segurança, veja Capítulo 3.4 “Requisitos para segurança”)

O programa de aplicação deve ser introduzido com o software de programação SILworX. O sistema operacional liberado para o PC encontra-se na documentação de liberação para a versão do SILworX a ser utilizada.

O sistema de programação SILworX contém basicamente:

- Introdução de código (editor de programa), supervisão e documentação
- Variáveis globais com nomes simbólicos e tipo de dado (BOOL, UINT etc.)
- Atribuição dos sistemas de comando do sistema HIMax (editor de hardware)
- Compilação do programa de aplicação em uma forma que pode ser carregada no PES
- Configuração da comunicação

10.2.1 Embasamento da programação

A tarefa do sistema de comando deve estar presente sob a forma de uma especificação ou de um documento de especificação funcional. Esta documentação é a base da verificação da implantação correta no programa de aplicação. O tipo de representação da especificação depende das tarefas a serem realizadas. Estas incluem:

Lógica combinatória

- Esquema de causa/efeito (cause/effect diagram)
- Lógica da conexão com funções e blocos funcionais
- Blocos funcionais com características específicas

Sistemas de comando sequenciais (Sistema de comando da sequência)

Descrição escrita dos passos com as condições para habilitar e atuadores a serem controlados

- Planos de sequência de trabalho
- Forma de matriz ou de tabela das condições para habilitar e dos atuadores a serem controlados
- Definição das condições, p. ex., modos de operação, PARADA DE EMERGÊNCIA etc.

O conceito de E/S da instalação deve incluir uma análise dos circuitos de campo, ou seja, o tipo de sensores e atuadores:

Sensores (digitais ou analógicos)

- Sinal em operação normal (princípio de circuito fechado para sensores digitais, life-zero para sensores analógicos)
- Sinal em caso de erro

Definição de redundâncias necessárias relacionadas à segurança (1oo2, 2oo3) (compare com anexo “Aumentar o valor SIL de sensores e atuadores”)

- Supervisão de discrepância e reação

Atuadores

- Posicionamento e ativação em operação normal
- Reação segura/posicionamento seguro em caso de desligamento ou falta de energia elétrica

Objetivos na programação do programa de aplicação

- Fácil de entender.
- Fácil de seguir.
- Fácil de testar.
- Fácil de alterar.

10.2.2 Funções do programa de aplicação

A programação não está sujeita a limitações de hardware. As funções do programa de aplicação podem ser programadas livremente.

Durante a programação, é necessário considerar o princípio de circuito fechado em caso de entradas e saídas físicas. Somente elementos de acordo com IEC 61131-3 com suas respectivas condições funcionais são utilizados dentro da lógica.

- As entradas e saídas físicas operam geralmente no princípio de circuito fechado, ou seja, seu estado seguro é “0”.
- O programa de aplicação contém funções lógicas e/ou aritméticas úteis sem considerar o princípio de circuito fechado das entradas e saídas físicas.
- A lógica deve ser concebida de forma clara e ser documentada de forma compreensível para facilitar a busca de erros. Isso inclui a utilização de diagramas de função.
- Para facilitar a lógica, é possível inverter aleatoriamente as entradas e saídas de todos os blocos de função e variáveis.
- Sinais de erro de entradas/saídas ou de blocos de lógica devem ser avaliados por programadores.

Recomenda-se o encapsulamento de funções em blocos funcionais e funções criadas pelo usuário, que, por sua vez, são formadas por funções padrão. Assim, é possível estruturar claramente um programa de aplicação em módulos (funções, blocos funcionais). Cada módulo pode ser visto – e testado –. Através do agrupamento dos módulos em um módulo maior e em um programa de aplicação, resulta uma função pronta e complexa.

10.2.3 Parâmetros de sistema do programa de aplicação

Os seguintes interruptores e parâmetros de um programa de aplicação podem ser ajustados na janela de diálogo *Properties* do programa de aplicação:

Interruptores/ parâmetros	Função		Valor padrão	Ajuste para a operação segura
Nome	Nome do programa de aplicação			livre
Safety Integrity Level	Nível de segurança: SIL0…SIL3 (apenas para documentação).		SIL3	específico da aplicação
Start	ON: ON OFF: Iniciar programa de aplicação pelo PADT não é permitido.		ON	específico da aplicação
Program Main Enable	Liberação da alteração em outros interruptores do programa de aplicação. Apenas tem efeito se o interruptor *Main Enable* do recurso estiver em ON!		ON	-
Autostart	Tipo liberado de Autostart: Arranque a frio, arranque quente, desliga.		Cold start	específico da aplicação
Test Mode Allowed	ON OFF OFF Para o programa de aplicação, a operação de teste não é permitida.		OFF	específico da aplicação
Local Forcing Allowed	ON: OFF OFF: Forcing não é permitido no nível do programa.		OFF	OFF recomendado
Reload Allowed	ON: ON OFF: Reload do programa de aplicação não é permitido.		ON	específico da aplicação
Program's Maximum CPU Cycles Count	Número máximo de ciclos de CPU que um ciclo do programa de aplicação pode durar.		1	específico da aplicação
Max. Duration for Each Cycle [µs]	Duração máxima de execução por ciclo do módulo processador para um programa de aplicação: 1…7 500 000 µs, 0: sem limite.		0 µs	específico da aplicação
Local Force Timeout Reaction	Comportamento do programa de aplicação depois do tempo de forcing ter vencido. ▪ Apenas encerrar Forcing. ▪ Parar o programa.		Stop Forcing Only.	-
Program ID	ID para a identificação do programa na exibição no SILworX, 1...32		1	específico da aplicação
Watchdog Time [ms] (calculado)	Tempo de supervisão do programa de aplicação, calculado pelo número de máximo de ciclos e do tempo de Watchdog do recurso Não pode ser alterado!			
Code Generation Compatibility	SILworX V4	SILworX V4	SILworX V4	específico da aplicação
	SILworX V3	Geração de código trabalha em compatibilidade com o SILworX V3.		
	SILworX V2	Geração de código trabalha em compatibilidade com o SILworX V2.		

Tabela 13: Parâmetros de sistema do programa de aplicação

10.2.4 Criação de código

O código é criado após a introdução correta do programa de aplicação e da atribuição das E/S do sistema de comando. Neste processo, é criada a CRC de configuração, ou seja, a soma de verificação via arquivos de configuração.

Esta é uma assinatura para toda a configuração e é emitida como código hexadecimal em formato de 32 bits. Isso inclui todos os elementos que podem ser configurados ou alterados tais como lógica, variáveis, ajustes de interruptores.

NOTA

É possível operação com erros do sistema de comando!

Antes de carregar o programa de aplicação para a operação direcionada à segurança, é imprescindível que o usuário a compile duas vezes. As duas versões criadas devem ter as mesmas somas de verificação.

Realizando a compilação duas vezes e a comparação das somas de verificação, é possível detectar possíveis falsificações do programa de aplicação que são causadas por erros esporádicos no hardware ou no sistema operacional do PC utilizado.

10.2.5 Fazendo o download e iniciando o programa de aplicação

O download de um PES no sistema HIMax não pode ser realizado antes que o estado STOP esteja colocado.

Um procedimento de carregamento abrange todos os programas de aplicação da configuração do projeto. O carregamento completo de uma configuração de projeto é supervisionado. Em seguida, o programa de aplicação pode ser iniciado, ou seja, o processamento cíclico da rotina inicia.

i A HIMA recomenda fazer o backup de dados do projeto, p. ex., em um dispositivo de armazenamento de dados, após cada carregamento de programas de aplicação no sistema de comando, também através de Reload.

Isso é feito para garantir que os dados do projeto respectivos à configuração carregados no sistema de comando continuem disponíveis, mesmo quando há falha no PADT.

A HIMA recomenda executar um backup com regularidade também independentemente de carregar o programa.

10.2.6 Reload

Se os programas de aplicação sofrerem alterações, estas podem ser transferidas para o PES durante a operação. Após verificações através do sistema operacional, o programa de aplicação alterado é ativado e assume a tarefa do sistema de comando.

i **No Reload de sequências de passos deve ser observado:**

A informação de Reload para sequências de passos não considera o status atual da sequência. Por isso, é possível que o Reload de uma determinada alteração da sequência de passos coloque a mesma em um estado não definido. A responsabilidade por isso está com o usuário.

Exemplos:

- Excluir o passo ativo. Depois disso, nenhum passo da sequência de passos possui o estado *active.*
- Renomear o passo inicial enquanto um outro passo está ativo. Isso leva a uma sequência de passos com dois passos ativos!

No Reload de Actions deve ser observado:

Reload carrega Actions com os seus dados completos. Antes do Reload, é importante refletir cuidadosamente quais consequências isso pode surtir.

Exemplos:

- Retirar de um sinal de identificação de um Timer pelo Reload resulta no esgotamento imediato do tempo deste Timer. Através disso, a saída *Q* pode assumir o estado TRUE, dependendo da atribuição restante.
- Retirar o sinal de identificação no caso de elementos que perduram (p. ex., sinal de identificação *S*) que estavam atribuídos faz com que estes elementos continuem atribuídos.
- Retirar um sinal de identificação *P0* atribuído como TRUE dispara o Trigger.

Antes da execução de um Reload, o sistema operacional verifica se o tempo de ciclo dos programas de aplicação em funcionamento aumentaria as tarefas adicionais necessárias de tal forma que o tempo de Watchdog definido seria excedido. Neste caso, o Reload é interrompido com uma mensagem de erro e o sistema de comando continua a funcionar com a atual configuração de projeto.

O sistema de comando pode interromper um Reload.

Para obter um Reload com êxito, durante a definição do tempo de Watchdog deve-se planejar uma reserva para o Reload ou aumentar temporariamente uma reserva do tempo de Watchdog do sistema de comando.

O aumento temporário do tempo de Watchdog deve ser coordenado com a instituição de verificação responsável.

Se o tempo de ciclo nominal for excedido também pode levar à interrupção de um Reload.

O Reload só é possível se o parâmetro de sistema “Reload permitido” estiver ajustado em ON e se a variável de sistema “Desativação de Reload” estiver em OFF.

É de responsabilidade do usuário planejar reservas durante a medição do tempo de Watchdog. Estas devem tornar possível o controle das seguintes situações:

- Oscilações no tempo de ciclo do programa de aplicação
- Fortes cargas súbitas do ciclo, p. ex., através da comunicação
- Sequência de limites de tempo na comunicação.

Para mais detalhes sobre o tempo de Watchdog, veja Capítulo 3.2.2.

10.2.7 Teste on-line

É permitido utilizar campos de teste on-line (campos OLT) para a indicação de variáveis durante a operação do sistema de comando na lógica do programa de aplicação.

Demais informações sobre a utilização de campos OLT encontram-se sob a palavra-chave “campo OLT” na ajuda on-line do SILworX e no Manual de primeiros passos HI 801 239 P.

10.2.8 Modo passo-a-passo

Para busca de erros, é possível executar o programa de aplicação durante o teste on-line, ou seja, ciclo por ciclo. Cada ciclo é acionado por um comando do PADT.

Esta função só pode ser utilizada quando o parâmetro de sistema **Permitido parar** para o respectivo programa de aplicação estiver colocado em ON.

Estado	Significado
OFF	Não é possível o modo passo-a-passo.
ON	Modo passo-a-passo é possível (ajuste padrão).

Tabela 14: Interruptor do programa de aplicação **Permitido parar**

NOTA

É possível uma avaria da operação direcionada à segurança!

Na operação direcionada à segurança, não é permitido o modo passo-a-passo!

10.2.9 Alteração on-line de parâmetros de sistema

É possível alterar on-line alguns parâmetros de sistema no sistema de comando. Um caso de aplicação é um aumento temporário do tempo de Watchdog para poder executar um Reload.

Antes de colocar os parâmetros através de um comando on-line, deve-se ponderar se esta alteração de parâmetro pode resultar em um estado perigoso. Caso necessário, deve-se tomar medidas técnicas ou do ponto de vista da organização para excluir danos.

Os valores do tempo de segurança e do tempo de Watchdog devem ser verificados e comparados com o tempo de segurança exigido pela aplicação e/ou com o tempo de ciclo real. Esses valores não podem ser verificados pelo PES!

Os parâmetros que podem ser alterados on-line estão citados na Tabela 11.

10.2.10 Documentação do programa para aplicações direcionadas à segurança

O sistema de programação SILworX possibilita a impressão automática da documentação de um projeto. Os tipos mais importantes de documentação são:

- Declaração de interfaces
- Lista de sinal
- Lógica
- Descrição dos tipos de dados
- Configurações para sistema, módulos e parâmetros de sistema
- Configuração da rede
- Lista de referências cruzadas

A documentação é parte integrante da vistoria final de funcionamento de uma instalação sujeita à aprovação de uma instituição de verificação (p. ex., TÜV).

10.2.11 Multitasking

Multitasking denomina a capacidade do sistema HIMax de processar até 32 programas de aplicação dentro do módulo processador.

Os programas de aplicação individuais podem ser iniciados, parados e carregados de forma independente um do outro, também por Reload.

O ciclo de um programa de aplicação pode ter a duração de vários ciclos do módulo processador. Isso pode ser controlado por parâmetros do recurso e do programa de aplicação. A partir destes parâmetros, o SILworX calcula o tempo de Watchdog do programa de aplicação:
Tempo de $\text{Watchdog}_{\text{programa de aplicação}}$ = *tempo de* $\textit{Watchdog}_{\text{módulo processador}}$ * *número máximo de ciclos*

Os programas de aplicação individuais em geral são executados sem efeitos de influência mútua entre si. Mesmo assim, a influência mútua é possível através de:

- Utilização das mesmas variáveis globais em vários programas de aplicação.
- Tempos de execução imprevisivelmente longos em programas de aplicação individuais, se nenhum limite estiver parametrizado por *Max Duration for Each Cycle*.

- A distribuição dos ciclos do programa de aplicação nos ciclos do módulo processador afeta fortemente o tempo de reação do programa de aplicação e o tempo de reação das variáveis descritas pelo programa de aplicação!
- Um programa de aplicação avalia variáveis globais, que um outro programa de aplicação descreveu, no mínimo um ciclo do módulo processador mais tarde. Em casos extremos, isso pode ocorrer com um atraso de 32 ciclos do módulo processador. Assim, a reação a alterações de tais variáveis globais é respectivamente atrasada!

NOTA

É possível a influência mútua de programas de aplicação!

A utilização das mesmas variáveis globais em vários programas de aplicação pode resultar na influência mútua de programas de aplicação com diversos efeitos.

- **Planejar com precisão a utilização de variáveis globais em vários programas de aplicação.**
- **Utilizar vínculos remissivos no SILworX para verificar a utilização de dados globais. Dados globais só podem ser sobrescritos em um local com novos valores, ou num programa de aplicação, através de entradas direcionadas à segurança ou via protocolos de comunicação direcionados à segurança!**

É de inteira responsabilidade do usuário excluir avarias de operação através de influência mútua de programas de aplicação!

Para mais detalhes sobre Multitasking, veja Manual de sistema, HI 801 242 P.

10.2.12 Vistoria final por órgãos de aprovação

Ao projetar uma instalação sujeita a certificação final, recomenda-se entrar em contato com os órgãos de certificação o mais cedo possível.

A vistoria final refere-se apenas à função de aplicação mas não aos módulos e equipamentos de automação do sistema HIMax direcionados à segurança que já foram aprovados como protótipo.

10.3 Lista de verificação para criação de um programa de aplicação

A HIMA recomenda utilizar a lista disponível de verificação para o cumprimento de aspectos relacionados à segurança durante a programação, antes e depois de carregar o programa novo ou alterado. A lista de verificação pode ser utilizada como documento de planejamento, mas serve ao mesmo tempo para demonstrar posteriormente que o planejamento foi realizado criteriosamente.

A lista de verificação está disponível na homepage da HIMA sob o formato Microsoft® Word®.

11 Configuração da comunicação

Além das variáveis de entrada e saída físicas, também é possível trocar valores de variáveis com um outro sistema através de uma conexão de dados. Para tal, as variáveis são declaradas com o sistema de programação SILworX na área Protocolos do respectivo recurso.

11.1 Protocolos padrão

Uma série de protocolos de comunicação permite apenas uma transmissão de dados não direcionada à segurança. Estes protocolos podem ser utilizados para aspectos não direcionados à segurança de uma tarefa de automação.

⚠ PERIGO

Ferimentos devido à utilização de dados importados!

Não utilize dados importados de fontes inseguras para as funções de segurança do programa de aplicação!

Os seguintes protocolos padrão estão disponíveis:

- Nas interfaces Ethernet do módulo de comunicação:
  - Modbus-TCP (Master/Slave)
  - Modbus redundante (Slave).
  - SNTP
  - Send/Receive TCP
  - PROFINET-IO (Controller, Device).
- Nas interfaces barramento de campo (RS 485) do módulo de comunicação, dependendo da versão da unidade:
  - Modbus (Master/Slave).
  - Modbus redundante (Slave).
  - PROFIBUS-DP (Master/Slave).

11.2 Protocolo direcionado à segurança safe**ethernet**

A supervisão da comunicação direcionada à segurança deve ser parametrizada no editor safe**ethernet**.

Demais detalhes sobre a safe**ethernet** encontram-se no Manual de Comunicação HI 801 240 P.

NOTA

É possível uma passagem involuntária para o estado seguro!

“ReceiveTMO” é um parâmetro direcionado à segurança!

“ReceiveTMO” é o intervalo de tempo de supervisão em PES 1, dentro do qual uma resposta correta deve ser recebida do PES 2.

i O ReceiveTMO também é válido na direção inversa de PES 2 para PES 1!

Se dentro do *ReceiveTMO* não chegar uma resposta correta do parceiro de comunicação, o HIMax encerra a comunicação direcionada à segurança. As variáveis de Input desta conexão safe**ethernet** se comportam de acordo com o parâmetro ajustado *Freeze Data on Lost Connection [ms]*. Para funções direcionadas à segurança que são realizadas via safe**ethernet**, é possível usar apenas o ajuste **Use Initial Data**.

i Nos seguintes cálculos do máximo tempo de reação (Worst Case Reaction Time), é possível utilizar o tempo de ciclo nominal em vez do tempo de Watchdog, se o modo de tempo de ciclo nominal estiver ajustado em *Fix* ou *Fixed-tolerant*.

11.3 Tempo máximo de reação para safeethernet

Nos seguintes exemplos as fórmulas para o cálculo do tempo máximo de reação no caso de uma conexão com sistemas de comando HIMatrix apenas valem se nos mesmos estiver ajustado o tempo de segurança = 2 * tempo de Watchdog. Para sistemas de comando HIMax, estas fórmulas valem sempre.

i O tempo máximo de reação admissível depende do processo é deve ser autorizado pela respectiva instituição de certificação.

Conceitos:

ReceiveTMO:	Tempo de supervisão no PES 1, dentro do qual deve ser recebido uma resposta válida do PES 2. Caso contrário, a comunicação direcionada à segurança é encerrada depois de esgotar este tempo.
Production Rate:	Distância mínima entre duas missivas de dados.
Watchdog Time:	Duração máxima permitida de um ciclo de RUN num sistema de comando. A duração do ciclo de RUN depende da complexidade do programa de aplicação e do número de conexões safe**ethernet**. O tempo de Watchdog (WDT) deve ser introduzido nas características do recurso.
Worst Case Reaction Time:	Tempo máximo de reação para a transmissão da alteração do sinal de uma entrada física (In) de uma PES 1 até a alteração da saída física (Out) de um PES 2.
Delay:	Retardos de um trajeto de transmissão, p. ex., no caso de conexões por modem ou satélite. No caso de conexões diretas pode ser assumido inicialmente um retardo de 2 ms. O retardo real do trajeto de transmissão pode ser medido pelo administrador responsável da rede.

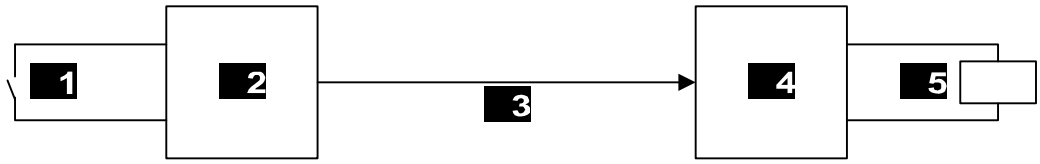
Para os seguintes cálculos dos tempos máximos de reação admissíveis valem as seguintes condições:

- Os sinais que são transmitidos via safe**ethernet** devem ser processados nos respectivos sistemas de comando dentro de um ciclo de CPU.
- Os tempos de reação dos sensores e atuadores devem ser somados adicionalmente.

Os cálculos valem também para sinais na direção inversa.

11.3.1 Cálculo do tempo máximo de reação de dois sistemas de comando HIMax

Calcular o tempo máximo de reação T_R (“Worst Case”) da mudança de estado de um transdutor do sistema de comando 1 (In) até a reação da saída (Out) do sistema de comando 2:



1 Entrada
2 Sistema de comando HIMax 1
3 Protocolo direcionado à segurança
4 Sistema de comando HIMax 2
5 Saída

Figura 3: Tempo de reação ao conectar dois sistemas de comando HIMax

$T_R = t_1 + t_2 + t_3$

T_R Worst Case Reaction Time

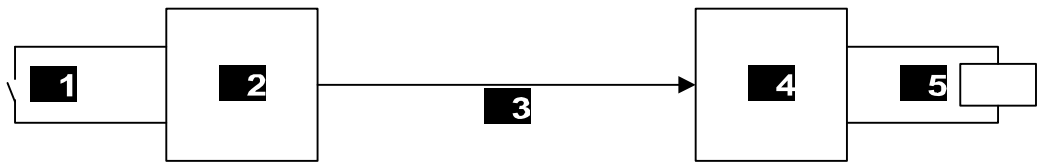
t_1 Tempo de segurança do sistema de comando HIMax 1

t_2 *ReceiveTMO*

t_3 Tempo de segurança do sistema de comando HIMax 2

11.3.2 Cálculo do tempo máximo de reação em conexão com um sistema de comando HIMatrix

Calcular o tempo máximo de reação T_R (“Worst Case”) da mudança de estado de um transdutor (In) do sistema de comando HIMax até a reação da saída (Out) do sistema de comando HIMatrix:



1 Entrada
2 Sistema de comando HIMax
3 Protocolo direcionado à segurança
4 Sistema de comando HIMatrix
5 Saída

Figura 4: Tempo de reação na conexão de um sistema de comando HIMax com um sistema de comando HIMatrix

$T_R = t_1 + t_2 + t_3$

T_R Worst Case Reaction Time

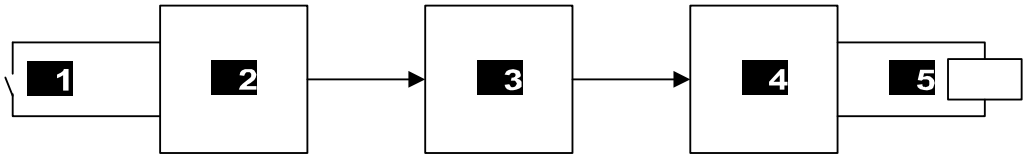
t_1 Tempo de segurança do sistema de comando HIMax

t_2 *ReceiveTMO*

t_3 2 * tempo de Watchdog do sistema de comando HIMatrix

11.3.3 Cálculo do tempo máximo de reação com dois sistemas de comando HIMatrix ou Remote I/Os

Calcular o tempo máximo de reação T_R (“Worst Case”) da mudança de estado de um transdutor (In) no primeiro sistema de comando HIMatrix ou na Remote I/O (p. ex., F3 DIO 20/8 01) até a reação da saída no segundo sistema de comando HIMatrix ou na Remote I/O (Out):



1 Entrada
2 Remote I/O 1
3 Sistema de comando HIMax
4 Remote I/O 2
5 Saída

Figura 5: Tempo de reação com dois Remote I/Os e um sistema de comando HIMax

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

T_R Worst Case Reaction Time

t_1 2 * tempo de watchdog do Remote I/O 1

t_2 *ReceiveTMO1*

t_3 2 * tempo de Watchdog do sistema de comando HIMax

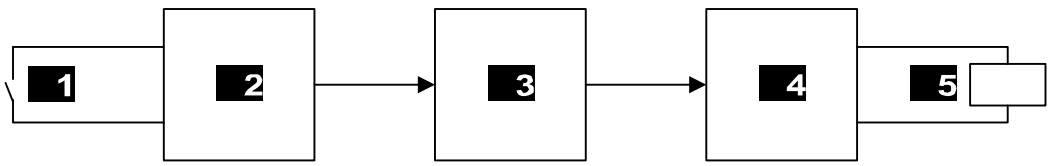
t_4 *ReceiveTMO2*

t_5 2 * tempo de watchdog do Remote I/O 2

i Os dois Remote I/Os 1 e 2 também podem ser idênticos. Os tempos também valem se ao invés de uma Remote I/O um sistema de comando HIMatrix for utilizado.

11.3.4 Cálculo do tempo máximo de reação com dois sistemas de comando HIMax e um sistema de comando HIMatrix

Calcular o tempo máximo de reação T_R (“Worst Case”) da mudança de estado de um transdutor (In) do primeiro sistema de comando HIMax até a reação da saída (Out) do segundo sistema de comando HIMax:



1 Entrada
2 Sistema de comando HIMax 1
3 Sistema de comando HIMatrix
4 Sistema de comando HIMax 2
5 Saída

Figura 6: Tempo de reação com dois sistemas de comando HIMax e um sistema de comando HIMatrix

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

T_R Worst Case Reaction Time

t_1 Tempo de segurança do sistema de comando HIMax 1

t_2 *ReceiveTMO1*

t_3 2 * tempo de Watchdog do sistema de comando HIMatrix

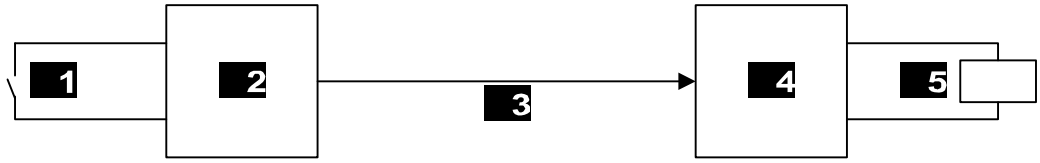
t_4 *ReceiveTMO2*

t_5 Tempo de segurança do sistema de comando HIMax 2

i Os dois sistema de comando HIMax 1 e 2 também podem ser idênticos.
O sistema de comando HIMatrix também pode ser um sistema de comando HIMax.

11.3.5 Cálculo do tempo máximo de reação de dois sistemas de comando HIMatrix

O tempo máximo de reação T_R (“Worst Case”) da mudança de estado de um transdutor do sistema de comando 1 até a reação da saída do sistema de comando 2 pode ser calculado como segue:



1 Entrada
2 Sistema de comando HIMatrix 1
3 Protocolo direcionado à segurança
4 Sistema de comando HIMatrix 2
5 Saída

Figura 7: Tempo de reação ao conectar dois sistemas de comando HIMatrix

$T_R = t_1 + t_2 + t_3$

T_R Worst Case Reaction Time

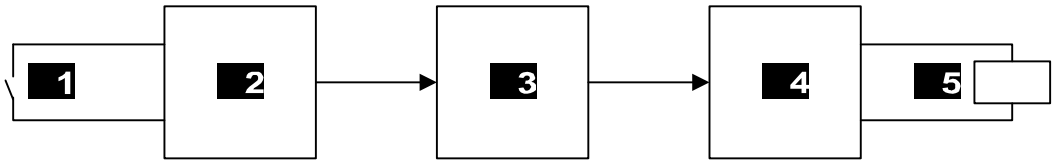
t_1 2 * tempo de Watchdog do sistema de comando HIMatrix 1

t_2 ReceiveTMO

t_3 2 * tempo de Watchdog do sistema de comando HIMatrix 2

11.3.6 Cálculo do tempo máximo de reação com dois Remote I/Os

O tempo máximo de reação T_R (“Worst Case”) da mudança de estado de um transdutor (In) do primeiro sistema de comando HIMatrix ou Remote I/O (p. ex., F3 DIO 20/8 01) até a reação da saída do segundo sistema de comando HIMatrix ou Remote I/O (Out) pode ser calculado como segue:



1 Entrada
2 Remote I/O 1
3 Sistema de comando HIMatrix
4 Remote I/O 2
5 Saída

Figura 8: Tempo de reação com Remote I/Os

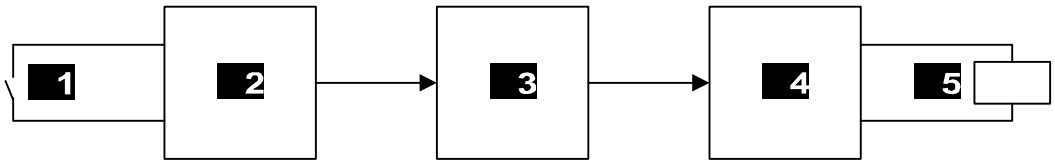
$$T_R = t_1 + t_2 + t_3 + t_4 + t_5$$

T_R Worst Case Reaction Time
t_1 2 * tempo de watchdog do Remote I/O 1
t_2 $ReceiveTMO_1$
t_3 2 * tempo de Watchdog do sistema de comando HIMatrix
t_4 $ReceiveTMO_2$
t_5 2 * tempo de watchdog do Remote I/O 2

Observação: Os dois Remote I/Os 1 e 2 também podem ser idênticos. Os tempos também valem se ao invés de uma Remote I/O um sistema de comando HIMatrix for utilizado.

11.3.7 Cálculo do tempo máximo de reação, dois sistemas de comando HIMatrix, um sistema de comando HIMax

O tempo máximo de reação T_R (“Worst Case”) da mudança de estado de um transdutor (In) do primeiro sistema de comando HIMatrix até a reação da saída do segundo sistema de comando HIMatrix (Out) pode ser calculado como segue:



1 Entrada
2 Sistema de comando HIMatrix 1
3 Sistema de comando HIMax
4 Sistema de comando HIMatrix 2
5 Saída

Figura 9: Tempo de reação com dois sistemas de comando HIMatrix e um sistema de comando HIMax

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

T_R Worst Case Reaction Time
t_1 2 * tempo de Watchdog do sistema de comando HIMatrix 1
t_2 $ReceiveTMO_1$
t_3 2 * tempo de Watchdog do sistema de comando HIMax
t_4 $ReceiveTMO_2$
t_5 2 * tempo de Watchdog do sistema de comando HIMatrix 2

11.4 Protocolo PROFIsafe direcionado à segurança

Os requisitos para a utilização do protocolo PROFIsafe estão especificados no Manual de comunicação HI 801 240 P. Deve-se observar os requisitos.

Fórmulas para o cálculo do tempo de reação também se encontram no Manual de comunicação.

Anexo

Aumento do SIL de sensores e atuadores

Os sistemas de comando HIMax direcionados à segurança podem ser utilizados para aplicações de segurança até o nível de integridade de segurança SIL 3. Um dos requisitos para tal é que os sensores e atuadores utilizados (encoder de sinal e elementos atuadores) atinjam o SIL exigido.

Em alguns casos, sensores e atuadores não estão disponíveis para os requisitos definidos na aplicação, tais como tamanho do processo, faixa de valores, SIL. Neste caso, existe a seguinte solução:

- Para entradas: utilizar sensores disponíveis que sejam suficientes para os requisitos, com exceção do valor SIL. Usar uma quantidade suficiente de sensores de modo que sua combinação forneça um sinal de entrada com o SIL necessário.
- Para saídas: utilizar atuadores disponíveis que sejam suficientes para os requisitos, com exceção do valor SIL. Utilizar uma quantidade suficiente deles de modo que sua combinação afete o processo com o SIL necessário.

Com entradas, associar os valores dos sensores individuais e suas informações de status em uma parte do programa de aplicação de modo tal que, como resultado dessa combinação, uma variável global contenha um valor que o SIL necessário tem.

Com saídas, distribuir o valor de uma variável global em várias saídas de modo que, em caso de avaria, o processo assuma o estado seguro. Além disso, a combinação dos atuadores deve poder atuar de modo adequado no processo (exemplo: conexão serial ou paralela de válvulas).

Em entradas e saídas, deve-se projetar a combinação de vários sensores/atuadores para o mesmo tamanho de processo de modo que a maior segurança possível seja alcançada no processo. Utilizar uma ferramenta de cálculo para calcular o SIL.

i A utilização de vários sensores/atuadores descrita aqui para a entrada/saída de um sinal permite aumentar o SIL e não pode ser confundida com a utilização de entradas/saídas redundantes para o aumento da disponibilidade!

Notas sobre como atingir o SIL necessário para os sensores e atuadores encontram-se, por exemplo, no IEC 61511-1, seção 11.4.

Termos e abreviaturas

Conceito	Descrição
ARP	Address Resolution Protocol: Protocolo de rede para a atribuição de endereços de rede a endereços de hardware
AI	Analog Input: Entrada analógica
Connector Board	Placa de conexão para o módulo HIMax
COM	Módulo de comunicação
CRC	Cyclic Redundancy Check: Soma de verificação
DI	Digital Input: Entrada digital
DO	Digital Output: Saída digital
CEM	Compatibilidade eletromagnética
EN	Normas européias
ESD	ElectroStatic Discharge: descarga eletrostática
FB	Fieldbus: barramento de campo
FBS	Funktionsbausteinsprache: linguagem de bloco funcional
FTT	Fault tolerance time: tempo de tolerância de falhas
ICMP	Internet Control Message Protocol: Protocolo de rede para mensagens de status e de falhas
IEC	Normas internacionais para eletrotécnica
Endereço MAC	Endereço de hardware de uma conexão de rede (Media Access Control)
PADT	Programming and Debugging Tool (conforme IEC 61131-3), PC com SILworX
PE	Terra de proteção
PELV	Protective Extra Low Voltage: Extra baixa tensão funcional com separação segura
PES	Programable Electronic System: Sistema eletrônico programável
PFD	Probability of Failure on Demand: Probabilidade de uma falha ao demandar uma função de segurança
PFH	Probability of Failure per Hour: Probabilidade de uma falha perigosa por hora
R	Read: Ler
Rack-ID	Identificação de um suporte básico (número)
Livre de efeitos de retro-alimentação	Dois circuitos de entrada estão ligados à mesma fonte (p. ex., transmissor). Uma ligação de entrada é chamada de “livre de efeitos de retroalimentação” se ela não interferir com os sinais de uma outra ligação de entrada.
R/W	Read/Write: Ler/Escrever
SB	Systembus: (módulo do) barramento de sistema
SELV	Safety Extra Low Voltage: Tensão extra baixa de proteção
SFF	Safe Failure Fraction: Fração de falhas que podem ser controladas com segurança
SIL	Safety Integrity Level (conf. IEC 61508)
SILworX	Ferramenta de programação para HIMax
SNTP	Simple Network Time Protocol (RFC 1769)
SRS	System.Rack.Slot Endereçamento de um módulo
SW	Software
TMO	Timeout
TMR	Triple Module Redundancy: módulos com tríplice redundância
W	Write
w_S	Valor limite do componente total de corrente alternada
Watchdog (WD)	Supervisão de tempo para módulos ou programas. O ultrapassar o tempo do Watchdog, o módulo ou programa entre em parada por erro.
WDZ	Tempo de Watchdog

Índice de figuras

Figura 1: Configuração recomendada: Todos os módulos processadores no rack 0 26

Figura 2: Configuração recomendada: Módulos processadores no rack 0 e rack 1 26

Figura 3: Tempo de reação ao conectar dois sistemas de comando HIMax 54

Figura 4: Tempo de reação na conexão de um sistema de comando HIMax com um sistema de comando HIMatrix 54

Figura 5: Tempo de reação com dois Remote I/Os e um sistema de comando HIMax 55

Figura 6: Tempo de reação com dois sistemas de comando HIMax e um sistema de comando HIMatrix 55

Figura 7: Tempo de reação ao conectar dois sistemas de comando HIMatrix 56

Figura 8: Tempo de reação com Remote I/Os 57

Figura 9: Tempo de reação com dois sistemas de comando HIMatrix e um sistema de comando HIMax 57

Lista de tabelas

Tabela 1: Normas para requisitos de CEM, climáticas e do meio-ambiente 10
Tabela 2: Requisitos gerais 10
Tabela 3: Requisitos climáticos 10
Tabela 4: Testes mecânicos 11
Tabela 5: Testes de resistência contra interferência 11
Tabela 6: Testes de emissão de interferência 11
Tabela 7: Verificação das características da alimentação com corrente contínua 12
Tabela 8: Visão geral da documentação do sistema 13
Tabela 9: Visão geral dos módulos de entrada 28
Tabela 10: Visão geral dos módulos de saída 33
Tabela 11: Os parâmetros de sistema do recurso 41
Tabela 12: Variáveis de sistema do hardware 42
Tabela 13: Parâmetros de sistema do programa de aplicação 47
Tabela 14: Interruptor do programa de aplicação Permitido parar 49

Índice remissivo

Aumento do SIL de sensores e atuadores 59
Autoteste 14
Campo de teste on-line 49
Concepção de segurança 37
Condições de utilização
  Alimentação com tensão 12
  CEM 11
  climáticas 10
  mecânicas 11
  Proteção contra ESD 12
CRC 48
Editor de hardware 43
Fault tolerance time, tempo de tolerância de falhas 16
ID de Rack 25
LED Ess 24
Lista de versão 37
Multitasking 50
Para poder trancar o sistema de comando 43
Princípio de circuito aberto 9
Princípio de circuito fechado 9
Reação de erro
  saídas analógicas 35
  saídas digitais 34
Reação em caso de erro
  entrada analógica 30
  entrada digital 29
  entrada do contador 31
Redundância 15
Repetição da verificação 19
responsible 25
Tempo de reação 19
Tempo de segurança 18
Tempo de Watchdog
  Determinação 17
  Programa e aplicação 18
  Recurso 16
Teste de função do sistema de comando 38
version list 37

HI 801 241 P

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

HIMA

SAFETY
NONSTOP