

HIMatrix

Sistema de comando direcionado à segurança

Manual de segurança



HIMA Paul Hildebrandt GmbH
Automação industrial

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 efetivas de controle de garantia de qualidade. 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 aviso prévio.

Informações mais detalhadas encontram-se na documentação do DVD HIMA e na nossa homepage em <http://www.hima.com>.

© Copyright 2011, HIMA Paul Hildebrandt GmbH

Todos os direitos reservados

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
2.00	Edição em português (tradução)		

Índice

1	Manual de segurança.....	7
1.1	Estrutura e utilização da documentação	7
1.2	Grupo alvo	8
1.3	Convenções de representação	8
1.3.1	Avisos de segurança.....	9
1.3.2	Avisos de utilização	9
2	Avisos para a utilização	10
2.1	Utilização prevista	10
2.1.1	Área de aplicação	10
2.1.2	Utilização não-prevista.....	10
2.2	Condições de utilização	11
2.2.1	Condições climáticas	11
2.2.2	Requisitos mecânicos	12
2.2.3	Requisitos CEM	12
2.2.4	Alimentação com tensão.....	13
2.2.5	Medidas de proteção contra ESD	13
2.3	Obrigações dos fabricantes de máquinas e sistemas bem como da empresa operadora.....	13
2.4	Demais documentações de sistema	14
3	Concepção de segurança para a utilização dos PES	15
3.1	Segurança e disponibilidade	15
3.1.1	Cálculo dos valores PFD e PFH	15
3.1.2	Autoteste e diagnóstico de erros	15
3.1.3	PADT	16
3.1.4	Estrutura de sistemas de segurança pelo princípio de circuito aberto	16
3.2	Tempos importantes para a segurança	17
3.2.1	Fault Tolerance Time (FTT, veja DIN VDE 0801, Anexo A1 2.5.3)	17
3.2.2	Tempo de segurança do PES.....	17
3.2.3	Safety Time do programa de aplicação com L3	17
3.2.4	Multiple Fault Occurrence Time (MOT).....	17
3.2.5	Response Time	18
3.2.6	Tempo de watchdog do sistema processador	18
3.2.7	Tempo de Watchdog do programa de aplicação para L3.....	18
3.3	Repetição da verificação	18
3.3.1	Execução da repetição da verificação	19
3.3.2	Frequência das repetições da verificação	19
3.4	Requisitos para segurança	19
3.4.1	Projeto do hardware.....	19
3.4.2	Programação	20
3.4.3	Comunicação	20
3.4.4	Trabalhos de manutenção	20
3.5	Certificação	21
3.5.1	Certificado TÜV.....	21
3.5.2	Verificação de tipo CE	22

4	Funções centrais	23
4.1	Fontes de alimentação	23
4.2	Descrição da função do sistema processador	23
4.3	Autotestes	24
4.3.1	Teste de microprocessador	24
4.3.2	Teste das áreas de memória	24
4.3.3	Áreas de memória protegidas	24
4.3.4	Teste de RAM	24
4.3.5	Teste de Watchdog	24
4.3.6	Teste do barramento de E/S dentro do sistema de comando	25
4.3.7	Reações a erros no módulo processador	25
4.4	Diagnóstico de erros	25
5	Entradas	26
5.1	Informações gerais	26
5.2	Segurança de sensores, encoders e transmissores	27
5.3	Entradas digitais direcionadas à segurança	27
5.3.1	Informações gerais	27
5.3.2	Rotinas de teste	27
5.3.3	Reação em caso de erro	27
5.3.4	Surges em entradas digitais	27
5.3.5	Entradas digitais parametrizáveis	28
5.3.6	Line Control	28
5.4	Entradas analógicas direcionadas à segurança (F35, F3 AIO 8/4 01 e F60)	29
5.4.1	Rotinas de teste	31
5.4.2	Reação em caso de erro	31
5.5	Contadores direcionados à segurança (F35 e F60)	32
5.5.1	Informações gerais	32
5.5.2	Reação em caso de erro	32
5.6	Lista de verificação para entradas direcionadas à segurança	33
6	Saídas	34
6.1	Informações gerais	34
6.2	Segurança de atuadores	35
6.3	Saídas digitais direcionadas à segurança	35
6.3.1	Rotinas de teste para saídas digitais	35
6.3.2	Reação em caso de erro	35
6.3.3	Comportamento em caso de curto-circuito ou sobrecarga externa	35
6.3.4	Line Control	35
6.4	Saídas digitais direcionadas à segurança de 2 pinos	36
6.4.1	Rotinas de teste para saídas digitais de 2 pinos	36
6.4.2	Conexão de 1/2 pinos (F3 DIO 8/8 01, F3 DIO 16/8 01)	36
6.4.3	Reação em caso de erro	37
6.4.4	Comportamento em caso de curto-circuito ou sobrecarga externa	38
6.5	Saídas de relé	38
6.5.1	Rotinas de teste para saídas de relé	38
6.5.2	Reação em caso de erro	38

6.6	Saídas analógicas direcionadas à segurança (F60)	39
6.6.1	Rotinas de teste	39
6.6.2	Reação em caso de erro.....	39
6.7	Saídas analógicas com desligamento direcionado à segurança (F3 AIO 8/4 01)	40
6.7.1	Rotinas de teste	40
6.7.2	Reação em caso de erro.....	40
6.8	Lista de verificação para saídas direcionadas à segurança.....	40
7	Software para sistemas HIMatrix	41
7.1	Aspectos relacionados à segurança para o sistema operacional	41
7.2	Princípio de trabalho e funções do sistema operacional	41
7.3	Aspectos relacionados à segurança para a programação	41
7.3.1	Concepção de segurança da ferramenta de programação	41
7.3.2	Verificação da configuração e do programa de aplicação	42
7.3.3	Arquivar um projeto.....	43
7.3.4	Opções de identificação de programa e configuração.....	43
7.4	Parâmetros do recurso.....	44
7.4.1	Parâmetros de sistema a partir de CPU OS V.7	44
7.4.2	Parâmetros de sistema anterior a CPU OS V.7.....	48
7.5	Proteção contra manipulações.....	48
7.6	Lista de verificação para criação de um programa de aplicação.....	49
8	Aspectos relacionados à segurança para o programa de aplicação	50
8.1	Âmbito para o uso direcionado à segurança	50
8.1.1	Embasamento da programação.....	50
8.1.2	Funções do programa de aplicação.....	51
8.1.3	Declaração de variáveis e sinais	51
8.1.4	Vistoria final por órgãos de aprovação	52
8.2	Procedimentos	52
8.2.1	Atribuição de variáveis a entradas/saídas	52
8.2.2	Trancar e destrancar o sistema de comando	53
8.2.3	Criação de código	54
8.2.4	Carregar e iniciar o programa de aplicação.....	55
8.2.5	Reload – com L3.....	55
8.2.6	Forcing	56
8.2.7	Alteração on-line de parâmetros de sistema – a partir de CPU OS V.7	56
8.2.8	Documentação do programa para aplicações direcionadas à segurança	57
8.2.9	Multitasking – com L3	57
8.2.10	Vistoria final por órgãos de aprovação	58
9	Configuração da comunicação	59
9.1	Protocolos padrão	59
9.2	Protocolo direcionado à segurança (safeethernet)	59
9.2.1	Receive Timeout.....	60
9.2.2	ResponseTime	60
9.2.3	Tempo de ciclo máximo do sistema de comando HIMatrix	61
9.2.4	Cálculo do tempo máximo de reação	61
9.2.5	Cálculo do tempo máximo de reação com dois Remote I/Os.....	62

9.2.6	Cálculo do tempo máximo de reação, dois sistemas de comando HIMatrix, um sistema de comando HIMax	62
9.2.7	Conceitos	63
9.2.8	Atribuição dos endereços safeethernet	63
10	Aplicação em centrais de alarme de incêndio	64
	Anexo	67
	Aumento do SIL de sensores e atuadores	67
	Glossário	68
	Lista de figuras	69
	Lista de tabelas	70
	Índice remissivo	71

1 Manual de segurança

Este manual contém informações para o uso dos equipamentos de automação HIMatrix direcionados à segurança em concordância com o uso previsto.

São pré-requisitos para instalação e colocação em funcionamento seguros, bem como para a segurança durante a operação e manutenção dos equipamentos de automação HIMatrix:

- Conhecimento de regulamentos.
- Implementação técnica adequada dos avisos de segurança contidos neste manual por parte do pessoal qualificado.

Nos seguintes casos, devido a avarias ou restrições de funções de segurança, podem ocorrer graves danos pessoais, danos materiais ou no meio ambiente pelos quais a HIMA não pode assumir nenhuma responsabilidade legal:

- No caso de intervenções não qualificadas nos equipamentos.
- No caso de desligamento ou desativação (bypass) de funções de segurança.
- No caso da não-observância dos avisos deste manual.

A HIMA desenvolve, fabrica e verifica os equipamentos de automação HIMatrix de acordo com os regulamentos de segurança aplicáveis. A utilização dos equipamentos apenas é admissível se todos os requisitos seguintes estão satisfeitos:

- Os casos de utilização previstos nas descrições exclusivamente.
- As condições ambientais especificadas exclusivamente.
- Em combinação com equipamentos de outros fornecedores apenas se os mesmos são autorizados.

Por motivos da estrutura clara, este manual não contém todos os detalhes sobre todas as versões dos dispositivos de automação HIMatrix. Outros detalhes encontram-se nos respectivos manuais.

1.1 Estrutura e utilização da documentação

Este manual de segurança contém os seguintes temas:

- Utilização prevista
- Concepção de segurança
- Funções centrais
- Entradas
- Saídas
- Software
- Aspectos relacionados à segurança para o programa de aplicação
- Configuração da comunicação
- Aplicação em centrais de alarme de incêndio
- Anexo:
 - Aumento do SIL de sensores e atuadores
 - Glossário
 - Diretórios/Índice

O manual diferencia as seguintes variantes do sistema HIMatrix:

Ferramenta de programação	Sistema operacional do processador	Sistema operacional de comunicação	Layout do hardware
SILworX	A partir da V.8	A partir da V.13	L3
SILworX	A partir da V.7	A partir da V.12	L2
ELOP II Factory	Anterior a V.7	Anterior a V.12	L2

Tabela 1: Variantes do sistema HIMatrix

Os sistemas operacionais para equipamentos com o Layout de hardware 3 não podem ser utilizados no lugar de equipamentos com Layout de hardware 2 e vice-versa.

Equipamentos com Layout de hardware L3 possuem capacidades ampliadas em relação a equipamentos com o Layout de hardware L2, mesmo com a mesa versão de sistema operacional, p. ex., Multitasking, Reload. Essas capacidades ampliadas são marcadas neste documento no título do capítulo ou no texto mediante «L3».

As variantes são diferenciadas no manual através de:

- Subcapítulos separados
- Tabelas com diferenciação das versões, p. ex., a partir de V.7, anterior a V.7

i

Projetos elaborados com o ELOP II Factory não podem ser editados no SILworX e vice-versa!

i

Sistemas de comando compactos e Remote I/Os são chamados de *devices*, placas de um sistema de comando modular são denominadas de *modules*.

No SILworX, os módulos são chamados de *Modules*.

1.2 Grupo alvo

Este documento dirige-se a planejadores, projetistas e programadores de sistemas de automação, bem como pessoas autorizadas para colocação em funcionamento, operação e manutenção dos equipamentos e do sistema. Pressupõem-se conhecimentos especializados na área de sistemas de automatização direcionados à segurança.

1.3 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 na ferramenta de programação que podem ser clicados
<i>Itálico</i>	Parâmetros e variáveis de sistema
Courier	Introdução de dados tal qual pelo usuário
RUN	Denominações de estados operacionais em letras maiúsculas
Cap. 1.2.3	Notas remissivas são hiperlinks, 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.

1.3.1 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 exceção. 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 há risco de danos materiais

NOTA



Tipo e fonte dos danos!

Como evitar os danos

1.3.2 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 Avisos para a utilização

É imprescindível ler as informações de segurança, avisos e instruções neste manual. Apenas utilizar o produto observando todos os regulamentos e normas de segurança.

2.1 Utilização prevista

2.1.1 Área de aplicação

Os sistemas de comando HIMatrix direcionados à segurança podem ser utilizados para aplicações de segurança até o nível de integridade de segurança SIL 3, conforme IEC 61508, no caso de aplicações de banda também SIL 4 conforme EN 50126, EN 50128 e EN 50129, veja Manual de segurança para aplicações de banda.

Os sistemas HIMatrix estão certificados para sistemas de comando de processos, sistemas de proteção, sistemas de queimadores e sistemas de comando de máquinas.

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. Devem ser utilizadas as bases de cálculo listadas no capítulo comunicação.

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

Princípio de circuito fechado/princípio de circuito aberto

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).

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

Os sistemas de comando HIMatrix 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.

Aplicação em centrais de alarme de incêndio

Os sistemas HIMatrix com detecção de quebra de fio e curto de linha 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!

2.1.2 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.

2.2 Condições de utilização

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

Os sistemas HIMatrix foram desenvolvidos para satisfazerem os requisitos das seguintes normas para CEM e requisitos climáticos e de meio-ambiente:

Norma	Conteúdo
EC/EN 61131-2: 2006	Sistemas de controlador lógico programável, Parte 2 Requisitos e verificações de meios operacionais
IEC/EN 61000-6-2: 2005	CEM Norma técnica básica, Parte 6-2 Resistência a interferência, ambiente industrial
IEC/EN 61000-6-4: 2006	Compatibilidade eletromagnética (CEM) Norma técnica básica emissão de interferências, ambiente industrial

Tabela 2: Normas para requisitos de CEM, climáticas e do meio-ambiente

Para a utilização dos sistemas de comando direcionados à segurança HIMatrix 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: IP20 Se as normas aplicáveis (p. ex., EN 60204, EN 15849) o exigirem, o sistema HIMatrix deve ser montado numa caixa do grau de proteção exigido (p. ex., IP 54).

Tabela 3: Requisitos gerais

2.2.1 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: -40 °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 4: Requisitos climáticos

2.2.2 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 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 (18 choques)

Tabela 5: Testes mecânicos

2.2.3 Requisitos CEM

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

IEC/EN 61131-2	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 escova: Linha de alimentação: 2 kV e 4 kV Linhas de sinal: 1 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, 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: Linha de alimentação: 2 kV CM, 1 kV alimentação DM Linhas de sinal: 2 kV CM, 1 kV DM com E/S AC	2 kV/1 kV 2 kV

Tabela 6: 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 7: Testes de emissão de interferência

2.2.4 Alimentação com tensão

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

IEC/EN 61131-2	Verificação das características da alimentação com corrente contínua
	A alimentação com tensão deve satisfazer as seguintes normas: IEC/EN 61131-2: SELV (Safety Extra Low Voltage) ou PELV (Protective Extra Low Voltage)
	A proteção dos sistemas HIMatrix 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.

Tabela 8: Verificação das características da alimentação com corrente contínua

2.2.5 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 HIMatrix!

- Usar para os trabalhos um posto de trabalho protegido contra descarga eletrostática e usar uma fita de aterramento.
- Se não forem usados, guardar módulos de forma protegida contra descarga eletrostática, p. ex., na embalagem.

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

Os fabricantes de máquinas e sistemas bem como a empresa operadora são responsáveis por garantir a utilização segura dos sistemas HIMatrix em sistemas de automação e instalações completas.

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

2.4 Demais documentações de sistema

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

Nome	Aplicável	Conteúdo	Nº do documento	Número de peça
Manual de elaboração do projeto HIMatrix	Todas as versões	Planejamento e construção de sistemas HIMatrix	HI 800 529 PT	Arquivo PDF
Manual de sistema HIMatrix Sistemas compactos	Todas as versões	Descrições dos sistemas compactos com dados técnicos	HI 800 528 PT	Arquivo PDF
Manual de sistema HIMatrix Sistema modular F60	Todas as versões	Descrição do sistema modular F60 com dados técnicos	HI 800 527 PT	Arquivo PDF
Relatório de teste para o certificado ¹⁾	Todas as versões	Princípios do teste, requisitos de segurança, resultados		96 9000104
Manual de comunicação (Configuração com SILworX)	A partir de CPU OS V.7	Descrição dos protocolos de comunicação, ComUserTask e como projetar os mesmos no SILworX	HI 801 240 PT	Arquivo PDF
Ajuda Online SILworX	A partir de CPU OS V.7	Operação do SILworX	-	-
Ajuda Online ELOP II Factory	Anterior a CPU OS V.7	Operação do ELOP II Factory, Protocolo IP Ethernet, protocolo INTERBUS	-	-
SILworX Manual Primeiros passos	A partir de CPU OS V.7	Introdução ao SILworX	HI 801 239 PT	Arquivo PDF
ELOP II Factory Manual Primeiros passos	Anterior a CPU OS V.7	Introdução ao ELOP II Factory	HI 800 529 CPA	Arquivo PDF 96 9000013
¹⁾ Fornecido apenas em combinação com um sistema HIMatrix				

Tabela 9: Documentação de sistema HIMatrix

Detalhes sobre os equipamentos e módulos encontram-se nos respectivos manuais.

3 Concepção de segurança para a utilização dos PES

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

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

3.1 Segurança e disponibilidade

Os sistemas HIMatrix estão certificados para sistemas de comando de processos, sistemas de proteção, sistemas de queimadores e sistemas de comando de máquinas.

Nenhum perigo iminente resulta dos sistemas HIMatrix.

PERIGO



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

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

3.1.1 Cálculo dos valores PFD e PFH

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

A norma IEC 61508-1 define para SIL 3 um valor PFD de $10^{-4} \dots 10^{-3}$ e um valor PFH de $10^{-8} \dots 10^{-7}$ por hora.

Para o sistema de comando (PES) são assumidos 15% do valor limite da norma para PFD e PFH. Assim, resultam como valores limite proporcional do sistema de comando $PFD = 1,5 \cdot 10^{-4}$ e $PFH = 1,5 \cdot 10^{-8}$ por hora.

O intervalo para a repetição da verificação para sistemas HIMatrix é determinado para 10 anos, para Remote IOs e módulo com saídas de relé, o intervalo é de 3 anos (Offline Proof Test, veja IEC 61508-4, parágrafo 3.8.5).

3.1.2 Autoteste e diagnóstico de erros

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

- Processadores
- Áreas de memória (RAM, memória não volátil)
- Watchdog
- Os canais individuais de módulos de E/S

Se estes testes constatarem erros, o sistema operacional desliga o módulo ou Remote IO ou o canal de E/S que estão defeituosos.

Em um sistema sem redundância, isso significa que funções parciais ou o PES inteiro podem ser desligados.

Todos os respectivos equipamentos HIMatrix 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 equipamento comunicado como apresentando avarias ou através de um circuito externo.

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

Um registro diagnóstico abrangente do comportamento do sistema e os erros detectados são depositados na memória de diagnóstico dos sistemas de comando. 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 Sistema compacto HI 800 528 PT, ou Manual Sistemas modulares, HI 800 527 PT, capítulo *Diagnóstico*.

Em caso de quantidade muito pequena das falhas dos componentes que não afetam a segurança, o sistema HiMatrix 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.

O PADT é um PC no qual foi instalada a ferramenta de planejamento.

Há duas ferramentas de planejamento para o sistema HiMatrix, dependendo da versão do sistema operacional no sistema de comando:

- Com um sistema operacional a partir da versão 7, deve ser usado o SILworX.
- Com um sistema operacional anterior à versão 7, deve ser usado o ELOP II Factory.

3.1.4 Estrutura de sistemas de segurança pelo princípio de circuito aberto

Sistemas de segurança que trabalham 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 após 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 isolamento de incêndio.

Para garantir a função de segurança pode ser necessário configurar os componentes do sistema de segurança como redundantes:

- Alimentação do sistema de comando com corrente.
- Componentes do sistema de comando: sistemas de comando compactos HiMatrix, módulos, E/S remotas.
- 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. Isso é alcançado mediante

- Autotestes dos componentes HIMatrix.
- 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.

O programa de aplicação deve ter condições de processar o respectivo status de erro e ativar componentes redundantes.

3.2 Tempos importantes para a segurança

Estes são:

- Tempo de tolerância a falhas (Fault Tolerance Time)
- Tempo de watchdog (Watchdog Time)
- Tempo de segurança (Safety Time)
- Tempo de reação (Response Time)

3.2.1 Fault Tolerance Time (FTT, veja DIN VDE 0801, Anexo A1 2.5.3)

O tempo de tolerância de falhas (FTT) 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 segurança do PES

O tempo de segurança é o tempo dentro do qual o PES no estado RUN deve reagir depois de ocorrer um erro interno.

Olhando a partir do ponto de vista do processo, o tempo de segurança é o tempo máximo dentro do qual o sistema de segurança deve reagir nas saídas no caso de uma alteração de sinais de entrada (response time).

Versão do sistema operacional	Tempo de segurança na faixa de
A partir de CPU OS V.7	20...22 500 ms
Anterior a CPU OS V.7	20...50 000 ms

Tabela 10: Faixas de valores do tempo de segurança

3.2.3 Safety Time do programa de aplicação com L3

O tempo de segurança do programa de aplicação não pode ser ajustado diretamente. O HIMatrix calcula o tempo de segurança de um programa de aplicação a partir dos parâmetros *Max. Safety Time* do recurso e do *Maximum Number of Cycles*. Para consultar detalhes, veja Capítulo 8.2.9.

3.2.4 Multiple Fault Occurrence Time (MOT)

O tempo de ocorrência para falhas múltiplas é o intervalo de tempo dentro do qual a probabilidade para a ocorrência de falhas múltiplas que são críticas para a segurança é suficientemente reduzida.

O tempo de ocorrência de falhas múltiplas no sistema operacional está definido para 24 horas.

3.2.5 Response Time

O tempo máximo de reação de sistemas de comando HIMatrix 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:

- Leitura das entradas
- Processamento do programa de aplicação
- Escrita das saídas
- Comunicação de dados de processo
- Execução das rotinas de teste

Adicionalmente, devem ser considerados os tempos de comutação das entradas e saídas para a análise do pior caso possível - Worst Case.

3.2.6 Tempo de watchdog do sistema processador

O tempo de Watchdog é especificado como tempo no menu para o ajuste das características do PES. 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 sistema desliga. Depois disso, o sistema reinicia se Autostart foi parametrizado. Se Autostart não foi parametrizado, o sistema entra no estado STOP/VALID CONFIGURATION.

O tempo de Watchdog do sistema processador pode ser ajustado para:
 $\leq \frac{1}{2} \cdot \text{tempo de segurança do PES.}$

Versão do sistema operacional	Faixa de valores do tempo de Watchdog	Valor padrão de sistemas de comando	Valor padrão Remote I/Os
Com L3 (a partir de CPU-BS V.8)	4...5 000 ms	200 ms	100 ms
A partir de CPU OS V.7	8...5 000 ms	200 ms	100 ms
Anterior a CPU OS V.7	2...5 000 ms	50 ms	10 ms

Tabela 11: Faixa de valores do tempo de Watchdog

3.2.7 Tempo de Watchdog do programa de aplicação para L3

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 HIMatrix L3 calcula o tempo de watchdog de um programa de aplicação a partir dos parâmetros *Max. Watchdog Time* do recurso e do *Maximum Number of Cycles*.

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.

3.3 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.

No caso de RemotelOs e módulos com saídas de relé, a repetição da verificação para os relés deve ocorrer nos intervalos especificados para a instalação.

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 HIMatrix pode ser submetido a uma repetição da verificação através da verificação do completo circuito de segurança.

Na prática, é exigido um intervalo mais curto para a repetição da verificação (p. ex., a cada 6 ou 12 meses) para dispositivos de campo de entrada e de saída do que para o sistema de comando HIMA. Quando o usuário verifica o circuito de segurança completo por causa do dispositivo de campo, o sistema de comando HIMatrix é automaticamente incluído neste teste. Portanto, torna-se desnecessário realizar repetições adicionais da verificação para o sistema de comando HIMatrix.

Caso a repetição da verificação dos dispositivos de campo não inclua o sistema de comando HIMatrix, 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 HIMatrix.

Se houver requisitos adicionais para a repetição da verificação, deve ser observado o manual do respectivo equipamento.

3.4 Requisitos para segurança

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

3.4.1 Projeto do hardware

As pessoas que elaboram o projeto do hardware HIMatrix devem observar os requisitos de segurança listados abaixo.

Requisitos independentes do produto

- Para assegurar a operação direcionada à segurança, utilizar apenas hardware e software à prova de erros e autorizados para tal. O hardware e software autorizado está listado na Lista de versões dos módulos e do firmware dos sistemas HIMatrix da HIMA Paul Hildebrandt GmbH, número do certificado 968/EZ 128.19/09 (*Version List of Devices and Firmware of HIMatrix Systems of HIMA Paul Hildebrandt GmbH, Certificate-No. 968/EZ 128.19/09*). 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 2.2) relativas à CEM, às influências mecânicas, químicas e climáticas.
- Hardware e software que não são à prova de erros, porém, sem retroalimentação podem ser utilizados para o processamento de sinais não relevantes para a segurança, mas não para o processamento de tarefas relacionadas à segurança.
- Em todos os circuitos elétricos de segurança externos ligados ao sistema deve ser respeitado o princípio de circuito fechado.

Requisitos dependentes do produto

- Apenas é permitido conectar ao sistema equipamentos que tenham dispositivos de separação segura da rede.
- A separação elétrica segura da alimentação com corrente deve ocorrer na alimentação de 24 V do sistema. Apenas podem ser utilizadas fontes de alimentação nas versões PELV ou SELV.

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 das grandezas relacionadas à segurança do sistema.
- Deve-se observar particularmente a definição da configuração do sistema, do máximo tempo de ciclo e do tempo de segurança.

Requisitos dependentes do produto

Requisitos para a utilização da ferramenta de programação

- Para a programação, deve-se utilizar a seguinte ferramenta:
 - A partir da versão V.7 do sistema operacional do processador: **SILworX**.
 - Anterior à versão V.7 do sistema operacional do processador: **ELOP II Factory**.
- Depois da elaboração da aplicação, deve ser garantido mediante compilação manual dupla e comparação dos CRCs que a compilação ocorreu corretamente.
- **A implementação correta da especificação da aplicação deve ser validada e verificada. É necessário realizar uma verificação completa da lógica através de teste.**
- Após cada alteração da aplicação, este procedimento deve ser repetido.
- A reação de erro do sistema em caso de erros nos módulos de entrada e saída e das RemotesOs à prova de erros deve ser determinada de acordo com as características relacionadas à segurança específicas da instalação através do programa de aplicação.


3.4.3 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 9.2.
- 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.

3.4.4 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 HIMatrix devem ser verificados de acordo com as normas para a segurança funcional listadas a seguir e certificadas pela TÜV e em conformidade com .

3.5.1 Certificado TÜV



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

Certificado e relatório de teste Nº 968/EZ 128.19/09
Equipamentos de automação direcionados à segurança
HIMatrix F60, F35, F31, F30, F20, RIO-NC

Normas internacionais:

EN / IEC 61508, parte 1–7: 2000

SIL 3

EN / IEC 61511: 2004

SIL 3

EN / ISO 13849-1: 2008

Performance level e

EN / IEC 62061: 2005

EN 50156-1: 2006

SIL 3

EN 12067-2: 2004

EN 298: 2004

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

F20, F30, F31, F35, F60,
F3 AIO 8/4 01, F3 DIO 16/8 01,
F3 DIO 16/8 02,
F3 DIO 20/8 01, F3 DIO 8/8 01


EN 50130-4: 1989 + A1: 1989

+A2: 2003 + Corr. 2003

NFPA 72: 2007

F20, F30, F31, F35, F60,
F3 AIO 8/4 01, F3 DIO 16/8 01,
F3 DIO 16/8 02,
F3 DIO 20/8 01, F3 DIO 8/8 01

O capítulo 2.2 contém uma lista detalhada de todas as verificações ambientais e de CEM realizadas.

Todos os equipamentos possuem a marca de certificação .

3.5.2 Verificação de tipo CE



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

Atestado de verificação de tipo CE, nº 01/205/0644/09
CLP (PES) de segurança da família de sistema
HiMatrix F20, F30, F31, F35, F60, RIO-NC

Normas internacionais:

EN / IEC 61508, parte 1–7: 2001

SIL 3

EN / IEC 61511: 2004

EN ISO 13849-1:2008

EN 62061: 2005

EN 50156-1: 2006

SIL 3

EN 12067-2: 2004

EN 298: 2004

EN 230: 2005

EN 61131-2: 2007

EN 61000-6-2: 2005

EN 61000-6-4: 2007

NFPA 85: 2007

NFPA 86: 2007

EN 54-2:1997 /A1: 2007

F20, F30, F31, F35, F60, F3 AIO 8/4 01,
F3 DIO 16/8 01, F3 DIO 16/8 02,
F3 DIO 20/8 01, F3 DIO 8/8 01

NFPA 72: 2007

F20, F30, F31, F35, F60, F3 AIO 8/4 01,
F3 DIO 16/8 01, F3 DIO 16/8 02,
F3 DIO 20/8 01, F3 DIO 8/8 01

4 Funções centrais

No caso de sistemas de comando e RemotelOs dos tipos F1..., F2..., F3..., trata-se de sistemas de comando compactos que não podem ser modificados.

No caso dos sistemas de comando do tipo F60, trata-se de sistemas modulares. Neste caso, podem ser utilizados dentro de um sistema de comando até seis módulos de E/S, além do módulo da fonte de alimentação e do módulo processador.

4.1 Fontes de alimentação

Apenas no modelo F60 há um módulo de fonte de alimentação. Nos sistemas compactos, esta função está integrada ao equipamento e não pode ser considerada como um módulo.

O módulo de fonte de alimentação PS 01 (para F60) ou a função integrada converte a tensão de alimentação de 24 VDC em 3,3 VDC e 5 VDC (utilização para o barramento de E/S interno).

4.2 Descrição da função do sistema processador

No caso do sistema modular F60, o sistema processador encontra-se num módulo separado; nos sistemas compactos, dentro do sistema de comando compacto.

O sistema processador consiste nos seguintes blocos de função:

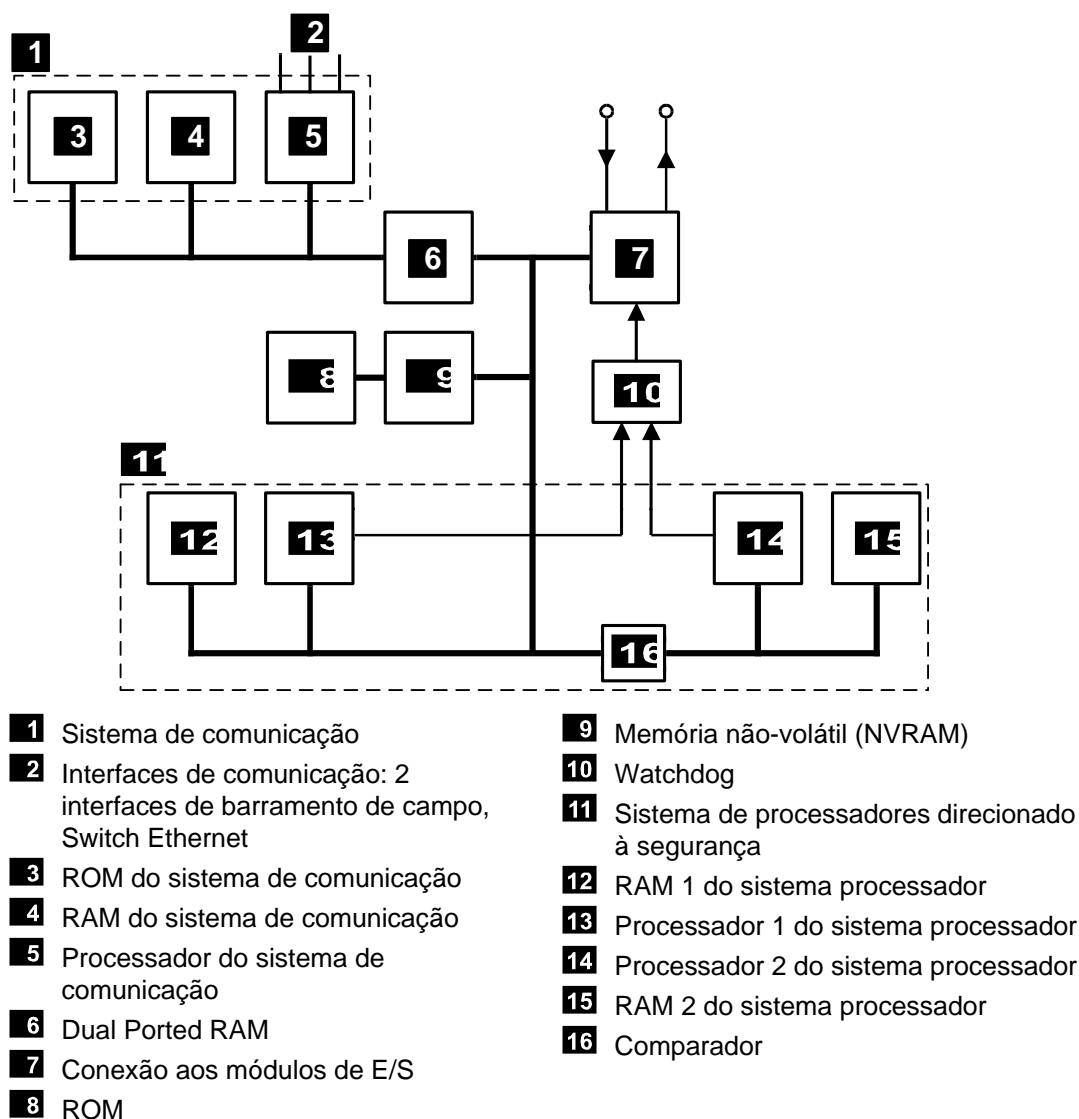


Figura 1: Representação dos blocos de função no exemplo da CPU 01 do F60

Características do módulo processador CPU 01 do F60

- Dois microprocessadores de ciclo sincronizado (processador 1 e processador 2).
- Cada microprocessador possui um memória RAM própria.
- Comparador de hardware testável para todos os acessos externos dos dois microprocessadores.
- Em caso de erro, o Watchdog é colocado no estado seguro.
- Flash EPROMs para sistema operacional e programa de aplicação, adequadas para no mín. 100.000 ciclos de memória.
- Memória de dados em NVRAM.
- Multiplexador para a ligação do barramento de E/S, Dual Port RAM (DPR).
- Bateria tampão ou Goldcap para data/hora.
- Processador de comunicação para conexões do barramento de campo e Ethernet.
- Interface para a troca de dados entre sistemas de comando F3..., F60 e o PADT, baseada em Ethernet.
- Interface(s) opcional(is) para a troca de dados via barramento de campo.
- Sinalização dos estados de sistema pelos LEDs.
- Lógica de barramento de E/S para conexão com os módulos de E/S.
- Watchdog seguro (WD).
- Supervisão de fonte de alimentação, testável (3,3 V = / 5 V = tensão de sistema).

4.3 Autotestes

Os dispositivos de autoteste detectam erros individuais que podem levar a um estado de operação perigoso e disparam dentro do tempo de segurança do sistema de comando as reações de erro definidas que conduzem as partes afetadas pelo erro ao estado seguro.

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

4.3.1 Teste de microprocessador

Verifica o seguinte:

- Todos os tipos de comandos e endereçamento utilizados.
- A capacidade de escrita em flags e comandos acionados por flags.
- A capacidade de escrita e comunicação cruzada dos registos.

4.3.2 Teste das áreas de memória

O sistema operacional, programa de aplicação, constantes e parâmetros, bem como os dados variáveis, são armazenados nas áreas de memória de ambos os processadores e são verificados por um comparador de hardware.

4.3.3 Áreas de memória protegidas

Sistema operacional, programa de aplicação e área de parâmetros são armazenados em uma memória cada. São protegidos por proteção contra escrita e por um teste de CRC.

4.3.4 Teste de RAM

Um teste de escrita e leitura verifica as áreas modificáveis de RAM, especialmente para detectar Stuck-at e comunicação cruzada.

4.3.5 Teste de Watchdog

O sinal de Watchdog se desliga se não for acionado dentro de uma determinada janela de tempo pelas duas CPUs e também se o teste dos comparadores de hardware falhar. Mediante um outro teste, a capacidade de desligamento do sinal de Watchdog é verificada.

4.3.6 Teste do barramento de E/S dentro do sistema de comando

A conexão entre a CPU e as entradas e saídas correspondentes (módulos de E/S) é verificada.

4.3.7 Reações a erros no módulo processador

Um comparador de hardware dentro da área central compara constantemente se os comandos e 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 um erro, o sinal de Watchdog desliga automaticamente. Isso significa que o equipamento não processa mais os sinais de entrada e que as saídas entram no estado seguro, desenergizado.

No caso de um erro deste tipo, o sistema de comando reiniciará (Reboot). Se dentro de um minuto depois de reinicializar ocorrer um outro erro interno, o sistema de comando entra no estado STOP/INVALID CONFIGURATION e permanece neste estado.

4.4 Diagnóstico de erros

Todos os módulos do F60 dispõem sobre o seu próprio LED para a indicação de erros no caso de avarias no módulo ou no circuito externo. Assim, em caso de avaria é possível um rápido diagnóstico de erros através de um módulo comunicado como apresentando avarias.

No caso dos sistemas compactos F1..., F2..., F3..., estes indicadores de erros são reunidos numa mensagem de erro coletivo.

Adicionalmente, é possível avaliar no programa de aplicação os diferentes sinais de sistema das entradas e saídas.

A sinalização do erro apenas ocorre se o erro não afetar a comunicação com o sistema processador, ou seja, a avaliação pelo sistema processador ainda é viável.

A lógica no programa de aplicação pode avaliar os códigos de erro de todos os sinais de entrada e saída e dos sinais de sistema.

Um registro diagnóstico abrangente do comportamento do sistema e os erros detectados são depositados na memória de diagnóstico do sistema processador e do sistema de comunicação.. 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 Sistemas compactos HI 800 528 PT, ou Manual Sistema modular F60, HI 800 527 PT, capítulo *Diagnóstico*.

5 Entradas

Visão geral das entradas do sistema HIMatrix:

Equipamento	Tipo	Quantidade de entradas	Direcionado à segurança	Sem retroalimentação	Separação elétrica
Sistema de comando F20	Digital	8	•	•	-
Sistema de comando F30	Digital	20	•	•	-
Sistema de comando F31	Digital	20	•	•	-
Sistema de comando F35	Digital	24	•	•	-
	Contador 24 bit	2	•	•	-
	Analógico	8	•	•	-
Remote I/O F1 DI 16 01	Digital	16	•	•	-
Remote I/O F3 DIO 8/8 01	Digital	8	•	•	-
Remote I/O F3 DIO 16/8 01	Digital	16	•	•	-
Remote I/O F3 AIO 8/4 01	Analógico	8	•	•	-
Remote I/O F3 DIO 20/8 02	Digital	20	•	•	-
Sistema de comando modular F60:					
Módulo DIO 24/16 01	Digital	24	•	•	•
Módulo DI 32 01 (Line Control configurável)	Digital	32	•	•	•
Módulo DI 24 01 (110 V)	Digital	24	•	•	•
Módulo CIO 2/4 01	Contador 24 bit	2	•	•	•
Módulo AI 8 01	Analógico	8	•	•	•
Módulo MI 24 01	Analógico ou digital	24	•	•	•

Tabela 12: Visão geral das entradas do sistema HIMatrix

5.1 Informações gerais

É possível usar entradas direcionadas à segurança tanto para sinais direcionados à segurança como para sinais não direcionados à segurança.

Os sistemas de comando fornecem informação de status e erro das seguintes maneiras:

- Mediante LEDs de diagnóstico dos equipamentos e módulos.
- Através de sinais de sistema ou variáveis de sistema que o programa de aplicação pode avaliar.
- Mediante entradas na memória diagnóstica que o PADT pode ler.

Módulos de entrada direcionados à segurança executam automaticamente um autoteste cíclico de alta qualidade durante a operação. Essas rotinas de teste são verificadas pela TÜV e monitoram a função segura do respectivo módulo.

No caso de um erro, o sistema de comando fornece um sinal de nível Low ao programa de aplicação – a partir de CPU OS V.7, o valor inicial definido – e gera uma informação de

erro se for possível. O programa de aplicação pode avaliar essa informação através da leitura do código de erro.

Em caso de quantidade pequena das falhas dos componentes que não afetam a segurança, não é gerada nenhuma informação de diagnóstico.

5.2 Segurança de sensores, encoders e transmissores

Em uma aplicação direcionada à segurança, tanto o sistema de comando quanto os sensores, encoders e transmissores conectados a ele devem corresponder aos requisitos de segurança e ao SIL especificado. Veja a este respeito “Aumento do SIL de sensores e atuadores”, no anexo.

5.3 Entradas digitais direcionadas à segurança

As características descritas valem tanto para os canais digitais de entrada dos módulos do F60 quanto para os canais digitais de entrada de todos os sistemas compactos, se não houver identificações específicas.

5.3.1 Informações gerais

As entradas digitais são lidas uma vez por ciclo e armazenadas internamente; sua função segura é testada ciclicamente.

Sinais de entrada ativos por um tempo menor do que o tempo entre duas amostragens (ou seja, mais curtos do que um tempo de ciclo), em certos casos não são registrados.

5.3.2 Rotinas de teste

As rotinas de teste online verificam se os canais de entrada estão em condições de encaminhar os dois níveis de sinal (nível LOW e HIGH) independentemente dos sinais de entrada atualmente presentes. Este teste de função é executado em cada leitura dos sinais de entrada.

5.3.3 Reação em caso de erro

Se as rotinas de teste detectarem um erro numa entrada digital, o programa de aplicação processa um nível Low para o canal com erro, de acordo com o princípio de circuito fechado.

Além do valor de sinal do canal, o programa de aplicação precisa considerar o respectivo código de erro.

Um sistema compacto ativa o LED *ERROR*, um módulo F60, o LED *ERR*.

Com a utilização do respectivo código de erro, há possibilidades adicionais de monitorar os circuitos externos e programar reações de erro no programa de aplicação.

Version	Acesso ao código de erro	Nome do código de erro
A partir de CPU OS V.7	No registro ... <i>Channels</i> na visualização de detalhes do módulo ou da parte do equipamentos	-> <i>Error code [Byte]</i> na linha com o número do canal
Anterior a CPU OS V.7	Na janela <i>Signal Connections...</i> do módulo ou parte do equipamento	<i>DI[xx].error code</i> , xx = número do canal

Tabela 13: Códigos de erro com entradas digitais

5.3.4 Surges em entradas digitais

Devido ao curto tempo de ciclo dos sistemas HIMatrix, pode acontecer de entradas digitais lerem um pulso de Surge conforme EN 61000-4-5 como nível High temporário.

As seguintes medidas evitam falhas de função em ambientes onde Surge pode ocorrer:

1. Instalação de linhas de entrada blindadas

2. Ativar a supressão de avarias no programa de aplicação, um sinal deve estar presente por no mínimo dois ciclos antes de ser avaliado.

i

A ativação da supressão de avarias aumenta o tempo de reação do sistema HIMatrix!

i

A medida acima citada não é necessária se a configuração da instalação consegue excluir a possibilidade de Surges no sistema.

Essa configuração deve incluir especialmente medidas de proteção contra sobretensão e raio, aterramento e fiação da instalação com base nas indicações no Manual de sistema (HI 800 528 PT ou HI 800 527 PT) e nas normas relevantes.

5.3.5 Entradas digitais parametrizáveis

As entradas digitais do sistema de comando F35 e do módulo MI 24 01 trabalham pelo princípio de entradas analógicas que mesmo assim fornecem um valor digital através da parametrização de um limiar de comutação.

Para entradas digitais parametrizáveis valem as rotinas de teste e funções de segurança mencionadas para entradas analógicas, como listadas no Capítulo 5.4.

5.3.6 Line Control

Line Control é uma detecção de curto de linha e quebra de fio, por exemplo, de equipamentos de parada de emergência, que pode ser configurada em sistemas HIMatrix com entradas digitais (não com entradas digitais parametrizáveis).

Para este fim, as saídas digitais TO do sistema são ligadas às entradas digitais DI do mesmo sistema como segue (exemplo):

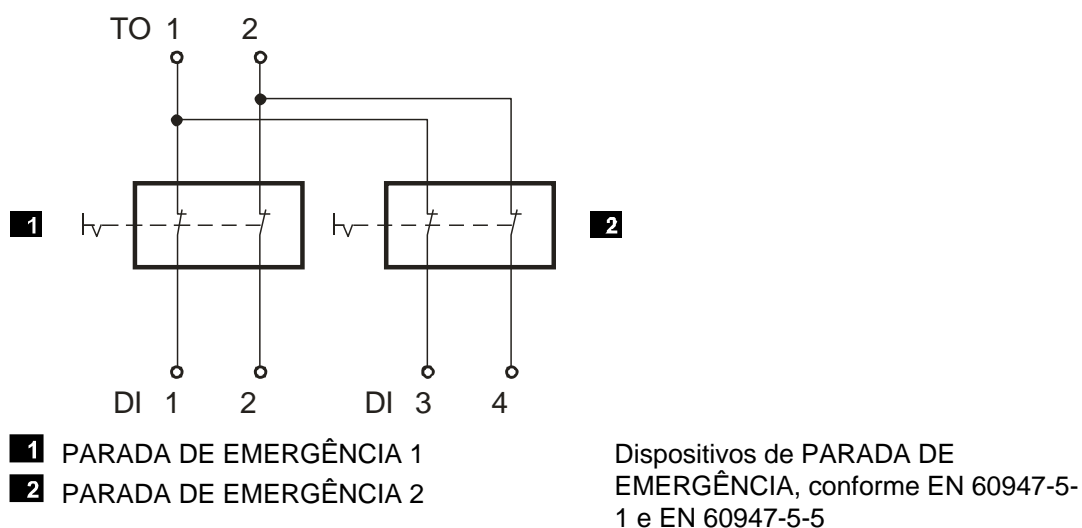
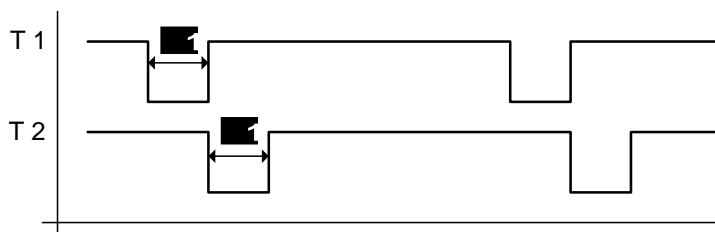


Figura 2: Line Control

O sistema de comando opera os ciclos das saídas digitais para detectar curto de linha e quebra de fio dos condutores para as entradas digitais. Para este fim, parametrizar no SILworX a variável de sistema *Value [BOOL]* -> e no ELOP II Factory o sinal de sistema *DO[01].Value*. As variáveis para emitir pulsos de ciclo devem iniciar com o canal 1 e devem estar em adjacência (veja variáveis / sinais de sistema nos manuais).



1 Configurável 5...2 000 µs

Figura 3: Sinais de ciclo T1, T2

O Line Control consegue detectar os seguintes erros:

- Curto transversal entre duas linhas paralelas.
- Inversão de duas linhas (p.ex., TO2 para DI 3).
- Curto para terra de uma das linhas (apenas com o pólo de referência aterrado).
- Quebra de fio ou abertura de contatos, ou seja, mesmo quando um dos interruptores de PARADA DE EMERGÊNCIA acima mostrados for acionado, o LED pisca e o código de erro é gerado.

Se um erro desse tipo acontecer, ocorrem as seguintes reações:

- O diodo luminoso *FAULT* na placa frontal do sistema de comando ou do módulo está piscando.
- As entradas são colocadas no nível LOW.
- Um código de erro (que pode ser avaliado) é gerado.

5.4 Entradas analógicas direcionadas à segurança (F35, F3 AIO 8/4 01 e F60)

Os canais de entrada analógicos convertem as correntes de entrada medidas em um valor do tipo de dados INTEGER. Os valores estão disponíveis para o programa de aplicação em forma de variáveis que são atribuídas às variáveis / aos sinais de sistema a seguir:

Versão do sistema operacional	Valor
A partir de CPU OS V.7	Variável de sistema -> <i>Value [INT]</i>
Anterior a CPU OS V.7	Sinal de sistema <i>AI[xx].Value</i> (xx = número de canal).

Tabela 14: Valore de entradas analógicas direcionadas à segurança

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.

As faixas de valores das entradas dependem do equipamento ou módulo:

Sistema de comando F35

Canais de entrada	Método de medição	Corrente, tensão	Faixa de valores na aplicação		Precisão de segurança técnica
			FS1000 ¹⁾	FS2000 ¹⁾	
8	unipolar	0...+10 V	0...1000	0...2000	2%
8	unipolar	0...20 mA	0...500 ²⁾ 0...1000 ³⁾	0...1000 ²⁾ 0...2000 ³⁾	2%
¹⁾ ajustável via seleção do tipo no PADT ²⁾ com adaptador externo de Shunt 250 Ω, número de peça: 98 2220059 ³⁾ com adaptador externo de Shunt 500 Ω, número de peça: 98 2220067					

Tabela 15: Entradas analógicas do sistema de comando F35

Remote I/O F3 AIO 8/4 01

Canais de entrada	Método de medição	Corrente, tensão	Faixa de valores na aplicação	Precisão de segurança técnica
8	unipolar	0...+10 V	0...2000	2%
8	unipolar	0...20 mA	0...1000 ¹⁾ 0...2000 ²⁾	2%
¹⁾ com adaptador externo de Shunt 250 Ω, número de peça: 98 2220059 ²⁾ com adaptador externo de Shunt 500 Ω, número de peça: 98 2220067				

Tabela 16: Entradas analógicas da Remote I/O F3 AIO 8/4 01

Sistema de comando F60

Canais de entrada	Método de medição	Corrente, tensão	Faixa de valores na aplicação		Precisão de segurança técnica
			FS1000 ¹⁾	FS2000 ¹⁾	
AI 8 01					
8	unipolar	-10...+10 V	-1000...1000	-2000...2000	1%
8	unipolar	0...20 mA	0...1000 ³⁾	0...2000 ³⁾	1%
8	unipolar	0...20 mA	0...500 ²⁾	0...1000 ²⁾	4%
4	bipolar	-10 V...+10 V	-1000...1000	-2000...2000	1%
MI 24 01					
24	Unipolar	0...20 mA	0...2000 ⁴⁾		1%
¹⁾ ajustável via seleção do tipo no PADT (F60) ²⁾ com Shunt de medição externo 250 Ω, número de peça: 00 0710251 ³⁾ com Shunt de medição externo 500 Ω, número de peça: 00 0603501 (precisão 0,05%, P 1 W) ⁴⁾ Shunts de medição internos					

Tabela 17: Entradas analógicas do sistema de comando F60

O módulo AI 8 01 do F60 pode ser configurado no programa de aplicação para oito funções unipolares ou quatro funções bipolares. Porém, não é admissível misturar as funções em um módulo.

As entradas analógicas do sistema de comando F35, da Remote I/O F3 AIO 8/4 01 e do módulo AI 8 01 trabalham com medição de tensão. Com as entradas analógicas do F35 e do F3 AIO 8/4 01 é possível monitorar as saídas digitais do próprio sistema (F35) ou de outros sistemas de comando HIMatrix para detectar quebra de fio. Mais detalhes encontram-se nos manuais dos respectivos sistemas de comando HIMatrix.

Em caso de quebra de fio (não ocorre supervisão de linha pelo sistema), são processados quaisquer sinais de entrada nas entradas de alta resistência. O valor resultante desta tensão de entrada flutuante não é seguro; no caso de entradas de tensão, os canais precisam ser terminados com uma resistência de 10 k Ω . A resistência interna da fonte deve ser observada aqui.

Para uma medição de corrente, o Shunt é ligado em paralelo à entrada, neste caso, não é necessária a resistência de 10 k Ω .

Devido ao Shunt de medição interno, as entradas do módulo MI 24 01 são entradas de corrente e não podem ser usadas como entradas de tensão.

No caso de canais de entrada não usados, a entrada de medição deve ser ligada ao potencial de referência. Influências negativas sobre outros canais no caso de uma quebra de fio (valores flutuantes de tensão) são evitadas desta forma.

Versão do sistema operacional	Procedimento
A partir de CPU OS V.7	É suficiente não atribuir nenhuma variável global às entradas não usadas.
Anterior a CPU OS V.7	Colocar o respectivo sinal <i>AI[0x].Used</i> para a entrada não usada no ELOP II Hardware Management no seu valor padrão <i>FALSE</i> ou <i>0</i> . Desta forma, o canal é suprimido dentro do programa de aplicação, ou seja, as mensagens de sinais não estão mais disponíveis.

Tabela 18: Configuração de entradas não usadas

5.4.1 Rotinas de teste

O sistema de comando processa valores analógicos em paralelo via dois multiplexadores e dois conversores analógico/digital com resolução de 12 bits e compara os resultados entre si. Adicionalmente, o sistema de comando liga valores de teste via conversor digital/analógico, reconverte os mesmos em valores digitais e compara os mesmos com os valores iniciais.

Se um erro for detectado, o sistema de comando repassa para a entrada o valor 0 para o processamento no programa de aplicação e atribui o status de erro.

5.4.2 Reação em caso de erro

Se ocorrerem erros de canal em entradas analógicas, o código de erro do canal com erro é ajustado para um valor > 0. Se o erro for do módulo inteiro, o código de erro para o módulo é ajustado para um valor > 0.

Além valor analógico, o programa de aplicação precisa avaliar o código de erro. No caso de um valor > 0 deve ter sido projetada uma reação direcionada à segurança.

Um sistema compacto ativa o LED *FAULT*, um módulo F60, o LED *ERR*.

Com a utilização do respectivo código de erro, há possibilidades adicionais de monitorar os circuitos externos e programar reações de erro no programa de aplicação.

Versão	Acesso ao código de erro	Nome do código de erro
A partir de CPU OS V.7	No registro ... <i>Channels</i> na visualização de detalhes do módulo ou da parte do equipamentos	->Error code [Byte] na linha com o número do canal
Anterior a CPU OS V.7	Na janela <i>Signal Connections...</i> do módulo ou parte do equipamento	AI[xx].código de erro, xx = número de canal

Tabela 19: Códigos de erro com entradas analógicas

5.5 Contadores direcionados à segurança (F35 e F60)

Os pontos listados valem tanto para o módulo contador CIO 2/4 01 do F60 quanto para os contadores do F35, exceto onde especificado de forma diferente.

5.5.1 Informações gerais

Um canal de contador pode ser parametrizado para a operação como contador rápido para frente/trás com resolução de 24 bit ou como decoder no código Gray.

Para a utilização como contador rápido para frente/trás são necessários como sinais a entrada de pulsos e a entrada de direção de contagem na aplicação. O reset ocorre apenas no programa de aplicação.

A resolução do encoder de 4 ou 8 bits vale para o módulo contador CIO 2/4 01 do F60, no caso do F35, o encoder possui resolução de 3 ou 6 bits. O reset é possível.

O vínculo entre duas entradas independentes de 4 bits para criar uma entrada de 8 bits (exemplo para F60), ocorre exclusivamente pelo programa de aplicação. Não foi prevista uma opção de comutação para esta finalidade.

A função de encoder monitora a alteração dos padrões de bits nos canais de entrada. Os padrões de bits nas entradas são diretamente repassados ao programa de aplicação. A representação no PADT ocorre em forma de um número decimal que corresponde ao padrão de bit (*Counter[0x].Value*).

Dependendo da aplicação, esse número que corresponde ao padrão de bit do Gray Code pode ser convertido, p. ex., no valor decimal correspondente.

5.5.2 Reação em caso de erro

Se as rotinas de teste na parte do contador do equipamento ou do módulo detectarem um erro, colocam um bit de status para a avaliação no programa de aplicação. Além disso, o programa de aplicação pode também considerar o respectivo código de erro.

Um sistema compacto ativa o LED *ERROR*, um módulo F60, o LED *ERR*.

Com a utilização do respectivo código de erro, há possibilidades adicionais de monitorar os circuitos externos e programar reações de erro no programa de aplicação.

Versão	Acesso ao código de erro	Nome do código de erro
A partir de CPU OS V.7	No registro ... <i>Channels</i> na visualização de detalhes do módulo ou da parte do equipamentos	->Error code [Byte] na linha com o número do canal
Anterior a CPU OS V.7	Na janela <i>Signal Connections...</i> do módulo ou parte do equipamento	Contador[xx].código de erro, xx = número de canal

Tabela 20: Códigos de erro em entradas de contador

5.6 Lista de verificação para entradas direcionadas à segurança

Esta lista de verificação é uma recomendação para projetar, programar e colocar em funcionamento entradas direcionadas à segurança. Ela pode ser utilizada como documento de planejamento, mas serve ao mesmo tempo para demonstrar posteriormente que o planejamento foi realizado criteriosamente.

Para cada um dos canais de entrada direcionados à segurança utilizados em um sistema dentro do âmbito do projeto e/ou colocação em funcionamento, deve-se preencher uma lista de verificação separada 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.

A lista de verificação *HIMatrix_Checklist_Inputs.doc* está disponível como documento no formato do Microsoft® Word®. O arquivo zipado *HIMatrix_Checklists.zip* contém todas as listas de verificação e pode ser descarregado na homepage da HIMA www.hima.com.

6 Saídas

Visão geral sobre as saídas do sistema HIMatrix

Equipamento	Tipo	Quantidade de entradas	Direcionado à segurança	Separação elétrica
Sistema de comando F20	Digital	8	•	-
	Ciclo	4	-	-
Sistema de comando F30 (configurável para Line Control)	Digital	8	•	-
Sistema de comando F31 (configurável para Line Control)	Digital	8	•	-
Sistema de comando F35		8	•	-
Remote I/O F1 DI 16 01	Ciclo	4	-	-
Remote I/O F2 DO 4 01	Digital	4	•	-
Remote I/O F2 DO 8 01	Digital	8	•	•
Remote I/O F2 DO 16 01	Digital	16	•	-
Remote I/O F2 DO 16 01	Relé	16	•	•
Remote I/O F3 DIO 8/8 01	Digital 1 pino	8	•	-
	Digital 2 pinos	2		
Remote I/O F3 DIO 16/8 01	Digital 1 pino	16	•	-
	Digital 2 pinos	8		
Remote I/O F3 AIO 8/4 01	Analógico	4	-	-
Remote I/O F3 DIO 20/8 01 e F3 DIO 20/8 02 (configurável para Line Control)	Digital	8	•	-
Sistema de comando modular F60:				
Módulo DIO 24/16 01 (configurável para Line Control)	Digital	16	•	•
Módulo DI 32 01 (configurável para Line Control)	Digital	32	•	•
Módulo DO 8 01 (110 V)	Relé	8	•	•
Módulo CIO 2/4 01	Digital	4	•	•
Módulo AO 8 01	Analógico	8	•	•

Tabela 21: Visão geral sobre as saídas do sistema HIMatrix

6.1 Informações gerais

O sistema de comando escreve nas saídas direcionadas à segurança uma vez em cada ciclo, relé os sinais de saída e compara os mesmos com os dados de saída definidos.

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

Nos canais de saída direcionados à segurança, três interruptores que podem ser testados estão integrados. Assim, o segundo caminho de desligamento independente necessário direcionado à segurança está integrado no canal de saída. Este desligamento de segurança integrado desliga de forma segura em caso de erro todos os canais do módulo de saída defeituoso (estado desenergizado).

Além disso, o sinal de Watchdog da CPU 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.

Essa função apenas tem efeito para todas as saídas digitais e saídas de relé dos sistemas de comando.

A utilização do respectivo código de erro, oferece possibilidades adicionais de configurar reações de erro no programa de aplicação.

6.2 Segurança de atuadores

Em uma aplicação direcionada à segurança, tanto o sistema de comando quanto os atuadores conectados a ele devem corresponder aos requisitos de segurança e ao SIL especificado. Veja a este respeito Aumento do SIL de sensores e atuadores, *no anexo*.

6.3 Saídas digitais direcionadas à segurança

Os pontos listados valem tanto para os canais digitais de saída dos módulos do F60 quanto para os canais digitais de saída de todos os sistemas compactos. Excepção são nos dois casos as saídas de relé.

6.3.1 Rotinas de teste para saídas digitais

Os equipamentos e módulos testam-se 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 é de 2 V. Os diodos utilizados impedem uma realimentação de sinais.
- Verificação do desligamento de segurança duplo e integrado.
- Um teste de desligamento das saídas é realizado dentro do MOT para no máx. 200 µs. A distância mínima entre duas verificações é de ≥ 20 segundos.

O sistema monitora a sua tensão de operação e desliga todas as saídas no caso de subtensão < 13 V.

6.3.2 Reação em caso de erro

Se o sistema de comando detectar um sinal com erro, o mesmo coloca a saída afetada do módulo no estado desenergizado e seguro através do interruptor de segurança. Em caso de erro do módulo, todas as saídas do módulo são desligadas. Um sistema compacto indica ambos os erros adicionalmente pelo LED *ERROR*, um módulo F60, pelo LED *ERR*.

6.3.3 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 equipamento ou módulo. O desligamento via desligamento de segurança não é necessário.

O sistema de comando monitora o consumo de corrente total do equipamento ou módulo e ao ultrapassar o limiar, coloca todos os canais de saída no 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 ligadas novamente.

6.3.4 Line Control

O sistema de comando pode pulsar os ciclos de saídas digitais direcionadas à segurança e usar as mesmas junto com as entradas digitais direcionadas à segurança do mesmo sistema (porém, não com entradas digitais parametrizáveis) para a detecção de curto de linha e quebra de fio (veja Capítulo 5.3.6 Line Control).

NOTA

Falhas de função dos atuadores ligados são possíveis!

Saídas pulsadas de ciclo não podem ser usadas como saídas direcionadas à segurança, p. ex., para comandar atuadores direcionados à segurança!

Saídas de relé não podem ser usadas como saídas pulsadas de ciclo.

6.4 Saídas digitais direcionadas à segurança de 2 pinos

As características aqui descritas referem-se a saídas digitais de 2 pinos dos sistemas compactos.

6.4.1 Rotinas de teste para saídas digitais de 2 pinos

Os equipamentos testam-se 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 é de 2 V. Os diodos utilizados impedem uma realimentação de sinais.
- Verificação do desligamento de segurança (duplo) integrado.
- Um teste de desligamento das saídas é realizado dentro do MOT para no máx. 200 µs. A distância mínima entre duas verificações é de ≥ 20 segundos.
- Diagnóstico de linha com conexão de 2 pinos
F3 DIO 16/8 01:
 - Curto circuito contra L+, L-.
 - Curto circuito entre conexões de 2 pinos.
 - Quebra de fio em uma das duas conexões de 2 pinos.
- Diagnóstico de linha com conexão de 2 pinos
F3 DIO 8/8 01: curto circuito contra L+, L-.
- Teste do interruptor de teste L- com conexão de 2 pinos com diagnóstico de linha (F3 DIO 16/8 01).
- Supervisão da corrente de saída.

O sistema monitora a sua tensão de operação e desliga todas as saídas no caso de subtensão < 13 V.

6.4.2 Conexão de 1/2 pinos (F3 DIO 8/8 01, F3 DIO 16/8 01)

As saídas digitais podem ser configuradas como segue:

- Saída digital com conexão de 2 pinos com diagnóstico de linha
- Saída digital com conexão de 2 pinos sem diagnóstico de linha
- Saída digital com conexão de 1 pino DO+ comutando L+
- Saída digital com conexão de 1 pino DO- comutando L-

Conexão de 2 pinos

NOTA

É possível é um relé ou atuador conectado à saída seja ligado de forma não-intencional!

Em aplicações com risco elevado, o sinal de status do diagnóstico de linha deve ser usado para desligar as saídas (DO+, DO-) no caso de erro.

i

Se os requisitos acima não podem ser satisfeitos, deve ser observado o seguinte caso:
No caso de um curto de linha de DO- para L-, um relé pode armar ou um outro atuador pode ser colocado num estado de comutação diferente.

Causa: Durante o tempo de supervisão para o diagnóstico de linha há um nível de tensão de 24 V (saída DO+) no consumidor (relé, atuador de comutação), assim que o mesmo poderia derivar o suficiente de energia elétrica para comutar a um outro estado.

NOTA

Avaria na detecção de quebra de fio é possível!

No caso da ligação por dois pinos, nenhuma entrada DI pode estar ligada a uma saída DO. Isso impediria a detecção da quebra de fio.

NOTA

Avarias do sistema de comando ou de equipamentos/sistema eletrônicos são possíveis!

A ligação de cargas indutivas deve ocorrer sem diodo roda-livre no consumidor.

6.4.3 Reação em caso de erro**Saídas DO-**

Ao detectar um sinal com erro, o equipamento ou módulo coloca a saída afetada do módulo no estado desenergizado e seguro através do interruptor de segurança. Um erro do equipamento ou do módulo leva ao desligamento de todas as saídas. Um sistema compacto indica ambos os erros adicionalmente pelo LED *ERROR*, um módulo F60, pelo LED *ERR*.

Saídas DO+

Ao detectar um sinal com erro, o equipamento ou módulo coloca a saída afetada do módulo no estado desenergizado e seguro através do interruptor de segurança. Um erro do equipamento ou do módulo leva ao desligamento de todas as saídas. Um sistema compacto indica ambos os erros adicionalmente pelo LED *ERROR*, um módulo F60, pelo LED *ERR*.

6.4.4 Comportamento em caso de curto-circuito ou sobrecarga externa

Em caso de curto-circuito da saída para L-, L+ ou em caso de sobrecarga, é mantida a testabilidade do equipamento ou módulo. O desligamento via desligamento de segurança não é necessário.

O consumo de corrente total do equipamento ou módulo é monitorado. Ao ultrapassar o limiar, o equipamento de saída / o módulo coloca todos os canais no estado seguro.

O equipamento ou módulo verifica neste estado ciclicamente em intervalos de poucos segundos se a sobrecarga das saídas ainda permanecer. No estado normal, o equipamento ou módulo liga as saídas novamente.

6.5 Saídas de relé

As saídas de relé correspondem a saídas digitais funcionais, porém, oferecem separação galvânica e uma maior resistência a tensão.

6.5.1 Rotinas de teste para saídas de relé

O equipamento ou módulo testa automaticamente as suas saídas durante a operação. As funções de teste essenciais são:

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

O sistema monitora a sua tensão de operação e desliga todas as saídas no caso de subtensão < 13 V.

No caso do módulo DO 8 01 e das Remote I/Os F2 DO 8 01 e F2 DO 16 02, as saídas são equipadas com três relés de segurança:

- Dois relés com contatos guiados
- Um relé padrão

Assim, as saídas podem ser utilizadas para os desligamentos de segurança.

6.5.2 Reação em caso de erro

Ao detectar um sinal com erro, o equipamento ou módulo coloca a saída afetada do módulo no estado desenergizado e seguro através do interruptor de segurança. No caso de um erro de módulo, o mesmo desliga todas as saídas. Um sistema compacto indica ambos os erros adicionalmente pelo LED *ERROR*, um módulo F60, pelo LED *ERR*.

6.6 Saídas analógicas direcionadas à segurança (F60)

O módulo AO 8 01 possui o seu próprio sistema microprocessador 1oo2 A/D direcionado à segurança com comunicação segura. Este escreve nas saídas analógicas uma vez por ciclo e armazena os valores internamente. O próprio módulo verifica o seu funcionamento.

Chaves DIP nos módulos de saída direcionados à segurança podem ajustar as saídas em saída de corrente ou de tensão. Aqui deve ser garantido que estes ajustes correspondam à utilização no sistema e à parametrização no programa de aplicação. Não-observância causa um comportamento incorreto do módulo.

NOTA



Falhas de função do módulo

Verificar antes de inserir o módulo no sistema:

- Ajustes de chaves DIP do módulo.
- Parametrização do módulo no programa de aplicação.

De acordo com a seleção do tipo de equipamento (...FS1000, ...FS2000) durante a configuração, na lógica devem ser considerados valores diferentes para os sinais de saída para se obterem os mesmos valores de saída (veja, p. ex., Manual AO 8 01 HI 800 548 PT, Capítulo *Sinais e códigos de erro das saídas*).

Sempre duas saídas analógicas estão ligadas galvanicamente entre si:

- Saída 1 e 2.
- Saída 3 e 4.
- Saída 5 e 6.
- Saída 7 e 8.

Os circuitos analógicos de saída contém supervisão de corrente e tensão, canais de releitura e teste também para circuitos de saída paralelos, bem como dois interruptores de segurança adicionais para o desligamento seguro dos circuitos de saída no caso de erro. Assim, o estado seguro (saída de corrente: 0 mA, saída de tensão: 0 V) é alcançado.

6.6.1 Rotinas de teste

O próprio módulo se testa automaticamente durante a operação. As funções de teste essenciais são:

- Releitura dupla do sinal de saída.
- Teste de comunicação cruzada entre as saídas.
- Verificação do desligamento de segurança integrado.

6.6.2 Reação em caso de erro

Uma vez em cada ciclo o módulo relê os sinais de saída e compara os mesmos com os dados de saída internamente armazenados. Se o módulo detectar uma discrepância, desliga o canal de saída com erro pelos dois interruptores de segurança e comunica o erro de módulo pelo LED *ERR*.

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

Para o tempo de reação do Worst Case das saídas analógicas, deve ser somado ao dobro do tempo de Watchdog ($2 \cdot \text{WDT}_{\text{CPU}}$) ainda o dobro do tempo de Watchdog da CPU AO ($2 \cdot \text{WDT}_{\text{AO-}\mu\text{C}}$).

No manual é indicado o tempo de reação do pior caso - Worst Case.

6.7 Saídas analógicas com desligamento direcionado à segurança (F3 AIO 8/4 01)

A Remote IO escreve nas saídas analógicas uma vez por ciclo e armazena os valores internamente.

As saídas não são direcionadas à segurança, porém, podem ser desligadas em conjunto de forma segura.

Para alcançar SIL 3, os valores das saídas devem ser relidas por entradas analógicas direcionadas à segurança e avaliadas no programa de aplicação. No programa de aplicação também devem ser definidas as reações após valores de saída com erros.

6.7.1 Rotinas de teste

A Remote IO verifica os dois interruptores de segurança para o desligamento de todas as quatro saídas automaticamente durante a operação.

6.7.2 Reação em caso de erro

No caso de um erro interno da Remote IO, a mesma desliga todos os quatro canais de saída simultaneamente pelos dois interruptores de segurança e comunica o erro de módulo pelo LED *FAULT*, na placa frontal.

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

6.8 Lista de verificação para saídas direcionadas à segurança

Esta lista de verificação é uma recomendação para projetar, programar e colocar em funcionamento saídas direcionadas à segurança. Ela pode ser utilizada como documento de planejamento, mas serve ao mesmo tempo para demonstrar posteriormente que o planejamento foi realizado criteriosamente.

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

A lista de verificação *HIMatrix_Checklist_Inputs.doc* está disponível como documento no formato do Microsoft® Word®. O arquivo zipado *HIMatrix_Checklists.zip* contém todas as listas de verificação e pode ser descarregado na homepage da HIMA www.hima.com.

7 Software para sistemas HIMatrix

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

- Sistema operacional,
- programa de aplicação,
- ferramenta de programação conf. IEC 61131-3.

O sistema operacional é carregado para a parte central (CPU) do sistema de comando e deve ser utilizado na respectiva forma válida, certificada pela TÜV para aplicações direcionadas à segurança.

A ferramenta de programação serve para a criação do programa de aplicação que contém as funções específicas da instalação que o dispositivo de automação deve executar. A parametrização e operação de funções do sistema operacional também é realizada pela ferramenta de programação.

Um gerador de código da ferramenta de programação traduz o programa de aplicação para o código de máquina. A ferramenta de programação transfere este código de máquina através de uma interface Ethernet para as Flash EPROMs do dispositivo de automação.

7.1 Aspectos relacionados à segurança para o sistema operacional

Cada sistema operacional autorizado é identificado através a sua denominação. Para a melhor diferenciação, indicam-se a revisão e a assinatura de CRC. As respectivas versões válidas do sistema operacional e as assinaturas(CRCs) correspondentes, aprovadas pela TÜV para equipamentos de automação direcionados à segurança, estão sujeitas a controle de revisão e são documentadas na lista, elaborada em conjunto com a TÜV.

A leitura da versão do sistema operacional em funcionamento apenas é possível com a ferramenta de programação. O controle pelo usuário é necessário (veja: 7.6, Lista de verificação para criação de um programa de aplicação).

7.2 Princípio de trabalho e funções do sistema operacional

O sistema operacional processa o programa de aplicação de forma cíclica. Neste caso, executa as seguintes funções: de forma muito simplificada:

- Leitura dos dados de entrada.
- Processamento das funções lógicas que foram programadas em conformidade com a normal EC 61131-3.
- Escrita dos dados de saída.

Além disso, há as seguintes funções básicas:

- Autotestes abrangentes.
- Testes das entradas e saídas durante a operação.
- Transmissão de dados.
- Diagnóstico.

7.3 Aspectos relacionados à segurança para a programação

7.3.1 Concepção de segurança da ferramenta de programação

A concepção de segurança das ferramentas de programação ELOP II Factory e SILworX:

- Durante a instalação da ferramenta de programação, garante-se a integridade do pacote de programa no percurso entre o fabricante e o usuário através de uma soma de verificação CRC.

- A ferramenta de programação 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, a ferramenta de programação mostra uma soma de verificação CRC.
2. Reiniciar a compilação.
 - ☒ Na conclusão da compilação, a ferramenta de programação 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 Verificação da configuração e do programa de aplicação).

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.

A partir de CPU OS V.7

O comparador seguro de revisão do SILworX pode registrar as alterações em relação à versão anterior e exibi-las.

7.3.2 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). A ferramenta de programação e as medidas definidas neste manual de segurança tornam suficientemente improvável que seja gerado código semântica e sintaticamente correto que ainda contenha erros sistemáticos não detectados resultantes do processo de geração do código.

Para a avaliação numérica de fórmulas, também se deve gerar casos de teste adequados. São úteis testes de classe de equivalência; 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 a lógica do programa está correta. A quantidade necessária de casos de teste depende da lógica de programa utilizada e deve abranger pares de valores críticos.

Apenas uma simulação ativa com fontes pode provar que há uma fiação correta dos sensores e dos atuadores do sistema (também aqueles conectados via comunicação com Remote I/Os). Além disso, só assim a configuração de sistema pode ser verificada.

Esse procedimento diz respeito tanto à criação inicial de um programa de aplicação como também às suas alterações.

7.3.3 Arquivar um projeto

A HIMA recomenda fazer o backup da configuração de projeto após cada carregamento de um programa de aplicação no sistema de comando. Isso para Download tanto quanto para Reload.

Arquivar um projeto diverge de forma básica entre as ferramentas ELOP II Factory e SILworX.

Arquivar um projeto a partir de CPU OS V.7

O SILworX cria um projeto num arquivo do projeto. O mesmo é adequado, p. ex., para se salvar num meio de armazenamento de dados.

Criação de um arquivo de projeto anterior a CPU OS V.7

O ELOP II Factory cria um projeto numa estrutura de subdiretórios. Para a arquivagem, o ELOP II Factory pode salvar o conteúdo desta estrutura num arquivo no de projeto. Este arquivo de projeto é adequado, p. ex., para se salvar num meio de armazenamento de dados.

Criação de um arquivo de projeto

1. Impressão do programa de aplicação para comparar a lógica com as especificações.
2. Compilação do programa de aplicação para criar o CRC da configuração da CPU.
3. Anotação da versão do CRC da configuração da CPU. Para este fim, seleciona-se na gestão do hardware o sistema de comando e no menu de contexto **Configuration Information** são exibidas as versões. Para determinar uma versão é necessário:
 - rootcpu.config mostra a configuração direcionada à segurança da CPU, o CRC da configuração da CPU.
 - rootcom.config mostra a configuração direcionada à segurança do módulo COM.
 - root.config mostra a configuração total, inclusive Remote I/Os (CPU + COM).
4. Criar um arquivo do projeto num meio de armazenar dados e colocar o nome dos programas de aplicação, CRCs de configuração das CPUs e a data.
Esta recomendação não substitui as necessidades internas de documentação a empresa operadora.

O arquivo do projeto foi criado.

7.3.4 Opções de identificação de programa e configuração

Os programas de aplicação são identificados de forma inequívoca pelas somas de CRC do projeto. As mesmas podem ser comparadas com o CRC de configuração do projeto carregado.

Arquivos de projeto – a partir de CPU OS V.7

Para garantir que o arquivo de projeto salvo está inalterado, compilar o recurso contido e comparar o CRC de configuração com o CRC da configuração carregada. O mesmo pode ser exibido no SILworX.

Arquivações – vor CPU-BS V.7

A denominação de um projeto arquivado deve conter o CRC de configuração do root.config.

Para garantir que o arquivo de projeto utilizado está inalterado, compilar o recurso contido depois da restauração do projeto a partir do arquivo e comparar o CRC de configuração do root.config com o CRC da configuração carregada que pode ser exibido pelo ELOP II Factory.

Para fins de controle, abrir no Control Panel do recurso o menu **Resource → Consistency Check**.

7.4 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.

Estes parâmetros são:

- System ID
- Rack ID, veja manuais de sistema HI 800 528 PT e HI 800 527 PT.
- Safety Time
- Watchdog Time
- Main Enable
- Autostart
- Start Allowed
- Load allowed
- Reload Allowed
- Global Forcing Allowed

Os seguintes parâmetros listados abaixo são definidos na ferramenta de programação para as ações permitidas em operação direcionada à segurança do equipamento de automação 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 adaptados para cada utilização do sistema de comando com a respectiva instituição de verificação.

7.4.1 Parâmetros de sistema a partir de CPU OS V.7

A partir de CPU OS V.7 há uma divisão entre parâmetros de sistema do recurso e parâmetros de sistema do hardware.

Parâmetros de sistema do recurso

Estes parâmetros determinam o comportamento do sistema de comando durante a operação e são ajustados no SILworX, na janela de diálogo *Propriedades* do recurso.

Parâmetros / interruptores	Descrição	Valor padrão	Ajuste para a operação segura
Name	Nome do recurso		livre
System ID [SRS]	System-ID do recurso 1...65 535 É necessário atribuir ao ID de sistema um outro valor sem ser o valor padrão, caso contrário, o projeto não é executável!	60 000	Valor inequívoco dentro da rede de sistemas de comando que potencialmente estão conectados entre si.
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 8...5 000 ms	200 ms/ 100 ms ¹⁾	específico da aplicação

Parâmetros / interruptores	Descrição	Valor padrão	Ajuste para a operação segura
Main Enable	<p>ON: Os seguintes interruptores/parâmetros podem ser alterados pelo PADT durante a operação (= RUN):</p> <ul style="list-style-type: none"> ▪ ID de sistema ▪ Tempo de watchdog do recurso ▪ Tempo de segurança ▪ Tempo de ciclo nominal ▪ Target Cycle Time Mode ▪ Autostart ▪ Global Forcing Allowed ▪ Global Force Timeout Reaction ▪ Load Allowed ▪ Reload Allowed ▪ Start Allowed <p>OFF: Os parâmetros não podem ser alterados durante a operação.</p> <p>i A alteração para ON na <i>liberação principal</i> é possível somente se o PES estiver parado!</p>	ON	OFF recomendado
Autostart	<p>ON: Ao ligar o módulo processador à tensão de alimentação, o programa de aplicação inicia automaticamente</p> <p>OFF: Não há início automático depois de ligar a tensão de alimentação.</p>	OFF	específico da aplicação
Start Allowed	<p>ON: Arranque a frio ou arranque quente permitidos pelo PADT no estado RUN ou STOP.</p> <p>OFF: Nenhum arranque permitido</p>	ON	específico da aplicação
Load Allowed	<p>ON: Download do programa de aplicação permitido</p> <p>OFF: Download do programa de aplicação não permitido</p>	ON	específico da aplicação
Reload Allowed	<p>Apenas aplicável com L3!</p> <p>ON: Reload do programa de aplicação permitido</p> <p>OFF: Reload de um programa de aplicação não permitido. Um Reload em andamento não é interrompido ao comutar para OFF</p>	ON	-
Global Forcing Allowed	<p>ON: Forcing global para este recurso permitido</p> <p>OFF: Forcing global para este recurso não é permitido</p>	ON	específico da aplicação
Global Force Timeout Reaction	<p>Define como o recurso se comporta no momento do Force-Timeout global se esgotar:</p> <ul style="list-style-type: none"> ▪ Encerrar Forcing ▪ Parar recurso 	Encerrar 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 801 100 PT, 2...5000 ms	60 ms	específico da aplicação
Max. Time Config. Connects [ms]	<p>Apenas aplicável com L3!</p> <p>Define quanto tempo dentro de um ciclo de CPU está disponível para a comunicação de dados de processo, 6...5 000</p>	6 ms	

Parâmetros / interruptores	Descrição	Valor padrão	Ajuste para a operação segura
Target cycle time [ms]	Tempo de ciclo máximo ou desejado, veja <i>Target Cycle Time Mode</i> , 0...7 500 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	-
Multitasking Mode	Apenas aplicável com L3! Mode 1 O comprimento do ciclo da CPU depende da duração de execução de todos os programas de 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.	Mode 1	-
Target Cycle Time Mode	Utilização do <i>Target Cycle Time [ms]</i> . Com L3 todos os valores podem ser utilizados, para L2 somente os <i>fixos</i> ! fixo 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. fixo com tolerância Como em <i>fixo</i> , mas no 1º ciclo de ativação do Reload – com L3 – o tempo de ciclo nominal não é observado. dinâmico com tolerância Como em <i>dinâmico</i> , mas no 1º ciclo de ativação do Reload – com L3 – o tempo de ciclo nominal não é observado. dinâmico O HIMax respeita o tempo de ciclo nominal se possível, porém, executa o ciclo no menor tempo possível.	fixed	-
Minimum Configuration Version	A estrutura dos arquivos de configuração e a geração de código são como na versão indicada do SILworX (exceto no caso de funções mais novas). SILworX V2 A geração de código ocorre como no SILworX V2. Com esse ajuste o CRC de um projeto elaborado com SILworX V2 não muda. SILworX V3 Geração de código como no SILworX V3. Com este ajuste, a compatibilidade com versões posteriores está garantida. SILworX V4 Geração de código como no SILworX V4. Com este ajuste, a compatibilidade com versões posteriores está garantida.	SILworX-V4	-
Maximum System Bus Latency [µs]	Não aplicável para sistemas de comando HIMatrix!	0 ms	-

Parâmetros / interruptores	Descrição		Valor padrão	Ajuste para a operação segura
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.		
1) 200 ms com sistemas de comando, 100 ms com Remote I/Os.				

Tabela 22: Os parâmetros de sistema do recurso a partir de CPU-BS V.7

Variáveis de sistema do hardware a partir de CPU OS V.7

Estas variáveis permitem alterar o comportamento do sistema de comando na operação em funcionamento em determinados estados. Estas variáveis podem ser ajustadas no Hardware Editor do SILworX, na visualização de detalhes do hardware.

Parâmetros / interruptores	Função	Ajuste padrão	Ajuste para a operação segura
Force Deactivation	Permite evitar o Forcing e desligá-lo imediatamente	FALSE	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	FALSE	específico da aplicação
Relay Contact 1... Relay Contact 4	Apenas aplicável com L3! Comanda os respectivos contatos de relé, se presentes.	FALSE	específico da aplicação
Read-only in Run	Após iniciar o sistema de comando nenhuma ação de comando (Stop, Start, Download) pode ser mais realizada via SILworX, exceções: Forcing e Reload	FALSE	específico da aplicação
Reload Deactivation	Apenas aplicável com L3! Impede carregar o sistema de comando mediante Reload.	FALSE	específico da aplicação
User-LED 1... User LED 2	Apenas aplicável com L3! Comanda o respectivo LED, se presente.	FALSE	específico da aplicação

Tabela 23: Variáveis de sistema do hardware a partir de CPU OS V.7

É possível atribuir variáveis globais a estas variáveis de sistema, cujo valor será alterado por uma entrada física ou pela lógica do programa de aplicação.

Exemplo: Um interruptor chave está ligado a uma entrada digital. A entrada digital está atribuída a uma variável global que está atribuída à variável de sistema *Read only in Run*. Então o proprietário de uma chave pode permitir ou bloquear as ações de operação Stop, Start e Download mediante o interruptor chave.

7.4.2 Parâmetros de sistema anterior a CPU OS V.7

Interruptor	Função	Valor padrão	Ajuste para operação segura
Main enable	Os seguintes interruptores/parâmetros podem ser alterados pelo PADT durante a operação (= RUN).	ON	OFF ¹⁾
Autostart	Iniciação automática após Power ON do sistema de comando.	OFF	ON / OFF ²⁾
Start/Restart allowed	Arranque a frio, arranque “morno” e “quente” pelo PADT no estado RUN ou STOP.	ON	OFF ¹⁾
Load allowed	Liberação para carregar um programa de aplicação.	ON	ON
Test mode allowed	Modo de teste para o programa de aplicação é permitido ou proibido. Durante o modo de teste, o processamento do programa é congelada ou parada. As saídas permanecem comandadas e o processamento do programa pode ser executado em passos de ciclos individuais.	OFF	OFF
Changing the variables in the OLT allowed	Valores de variáveis podem ser exibidos e alterados nos campos de teste online (OLT).	OFF	OFF ³⁾
Forcing allowed	Introdução e ativação de valores para variáveis/sinais do PES são permitidas, independente do valor atual do sinal de processo ou sinal da lógica.	OFF	Definido pela instituição de certificação
Stop at Force Timeout	Parar a CPU depois de ultrapassar o tempo de Forcing.	ON	Definido pela instituição de certificação
¹⁾ Na operação RUN apenas é possível mudar para o valor OFF. ²⁾ O ajuste de ON ou OFF é específico da aplicação. ³⁾ Na operação RUN apenas é possível mudar para o valor ON.			

Tabela 24: Parâmetros de sistema do recurso anterior a CPU OS V.7

Para o Forcing definir outros interruptores e parâmetros.

7.5 Proteção contra manipulações

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

No PES e na ferramenta de programação, 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.
- As opções de comando dependem do usuário logado no PES.
- A ferramenta de programação 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 e pode ser interrompida.

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

NOTA



Apenas pessoal autorizado pode ter acesso ao sistema de comando HIMatrix!

Tomar as seguintes medidas de proteção contra alterações não autorizadas no sistema de comando:

- **Alterar os ajustes padrão para nome de usuário e senha.**
- **Cada usuário deve manter segredo da sua senha.**
- **Separar o PADT do sistema de comando depois de encerrar a colocação em funcionamento e apenas conectar de novo quando alterações forem necessárias.**

O acesso a dados do PES só é possível se o PADT utilizado tiver a ferramenta de programação 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 ou para ler variáveis/sinais. Durante a operação normal, não é necessário o PADT. Uma separação do PADT e do PES na fase normal de operação protege contra intervenções não permitidas.

7.6 Lista de verificação para criação de um programa de aplicação

Esta lista de verificação é uma recomendação 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 *HIMatrix_Checklist_Program.doc* está disponível como documento no formato do Microsoft® Word®. O arquivo zipado *HIMatrix_Checklists.zip* contém todas as listas de verificação e pode ser descarregado na homepage da HIMA www.hima.com.

8 Aspectos relacionados à segurança para o programa de aplicação

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

- Especificação da função do sistema de comando.
- Escrita do programa de aplicação.
- Compilação do programa de aplicação com o gerador de código C.
- Compilar duas vezes o programa de aplicação, ambos os resultados (CRC) devem ser comparados.
- O programa foi criado sem erros e pode rodar.
- Verificação e validação.

A seguir, o PES pode iniciar a operação direcionada à segurança.

8.1 Âmbito para o uso direcionado à segurança

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

O programa de aplicação deve ser introduzido com a ferramenta de programação admissível:

- SILworX para sistemas operacionais com uma versão a partir de CPU OS V.7.
- ELOP II Factory para sistemas operacionais com uma versão anterior a CPU OS V.7.

Os sistemas operacionais liberados para PC podem ser consultados nos avisos de liberação da ferramenta de programação.

A ferramenta de programação contém basicamente:

- Introdução de código (editor de blocos funcionais), supervisão e documentação.
- Variáveis com nomes simbólicos e tipo de dado (BOOL, UINT etc.).
- Atribuição dos sistemas de comando do sistema HIMatrix.
- Gerador de código (compilação do programa de aplicação em código de máquina).
- Configuração do hardware.
- Configuração da comunicação.

8.1.1 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 de conexão com funções e blocos funcionais.
 - Blocos funcionais com características especificadas.
- Sistemas de comando sequenciais (Sistema de comando sequencial).
 - Descrição escrita dos passos com as condições para habilitar e atuadores a serem controlados.
 - Esquemas de fluxo.
 - Forma de matriz ou de tabela das condições de comutação 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) (Conferir Capítulo Aumento do 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 alterar.
- Fácil de testar.

8.1.2 Funções do programa de aplicação

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

- 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. Isso deve ser considerado durante a programação.
- 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 localização de erros. Isso inclui a utilização de diagramas de função.
- Negações de diversas formas são admissíveis.
- Sinais de erro de entradas/saídas ou de blocos de lógica devem ser avaliados.

É importante 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 em módulos (funções, blocos funcionais). Cada módulo pode ser considerado individualmente e através do agrupamento dos módulos em um módulo maior e em um programa, resulta uma função pronta e complexa.

8.1.3 Declaração de variáveis e sinais

Uma variável é um representante para um valor dentro da lógica do programa. Pelo nome da variável, o local na memória com o valor armazenado é simbolicamente endereçado. Uma variável é criada na declaração de variáveis do programa ou do bloco funcional.

	Quantidade de caracteres para nomes de variáveis
A partir de CPU OS V.7	31
Anterior a CPU OS V.7	256

Tabela 25: Comprimento de nomes de variáveis

A utilização de nomes simbólicos ao invés do endereço físico possui duas vantagens decisivas:

- No programa de aplicação podem ser utilizadas as denominações de entradas e saídas usadas na instalação.
- Alterações na atribuição da variável aos canais de entrada e saída não interferem com o programa de aplicação.

A partir de CPU OS V.7, não existem mais sinais, apenas variáveis.

Variáveis não inicializadas são colocadas ao valor inicial 0 ou FALSE depois de um arranque a frio.

Variáveis cuja fonte é inválida, p. ex., por causa de um erro de hardware na entrada física, assumem o valor inicial configurado.

Sinais – anterior a CPU OS V.7

Um sinal serve como atribuição entre diferentes áreas do sistema de comando inteiro. O sinal é criado no editor de sinais e corresponde ao nível global de uma VAR_EXTERNAL do programa, se esta relação foi criada.

8.1.4 Vistoria final por órgãos de aprovação

A HIMA recomenda, ao projetar uma instalação sujeita a certificação final, entrar em contato com os órgãos de certificação o mais cedo possível.

8.2 Procedimentos

Este capítulo descreve procedimentos típicos para o desenvolvimento de programas de aplicação para sistemas de comando HIMatrix direcionados à segurança.

8.2.1 Atribuição de variáveis a entradas/saídas

As rotinas de teste necessárias para equipamentos de E/S, módulos de E/S ou canais de E/S direcionados à segurança são executadas pelo sistema operacional automaticamente.

A atribuição de variáveis utilizadas no programa de aplicação diverge entre ELOP II Factory e SILworX.

A partir da versão 7 do sistema operacional

Atribuir uma variável a um canal de E/S

1. Definir uma variável global do tipo adequado.
2. Indicar um valor inicial adequado durante a definição.
3. Atribuir a variável global ao valor do canal da entrada.
4. Avaliar no programa de aplicação o código de erro -> *Error Code [Byte]* e programar uma reação de erro direcionada à segurança.

A variável global foi atribuída a um canal de entrada/saída.

Anterior à versão 7 do sistema operacional

Se o valor de uma variável deve ser atribuído a um canal de E/S, proceder como segue:

Atribuir uma variável a um canal de E/S

1. Definir uma variável do tipo adequado.
2. Definir no editor de sinais da gestão do hardware um sinal com o mesmo nome da variável.
3. Puxar o sinal mediante Drag&Drop para a declaração de variáveis do programa.
4. Puxar o sinal mediante Drag&Drop para a lista de canais do módulo de E/S.
5. Avaliar no programa de aplicação o código de erro e programar uma reação de erro direcionada à segurança.

A variável está atribuída a um canal de E/S.

O nome do sinal de sistema para o código de erro depende do tipo do canal de E/S.

8.2.2 Trancar e destrancar o sistema de comando

Locking do sistema de comando significa trancar funções e travar as opções de intervenção pelo usuário durante a operação. Evita-se uma manipulação do programa de aplicação desta forma. A abrangência do travamento depende dos requisitos de segurança para a utilização do PES, mas também pode ocorrer consultando a instituição responsável pela certificação da instalação.

Unlocking do sistema de comando significa remover o travamento ativo, p. ex., para a execução de medidas no sistema de comando.

i

Trancar e destrancar apenas é possível com sistemas de comando e Remote I/O F3 DIO 20/8 01, não no caso de outras Remote I/Os!

A partir de CPU OS V.7

Três variáveis de sistema servem para trancar:

Variável	Função
Read only in Run	ON: Start, Stop e Download do sistema de comando estão trancados. OFF: Start, Stop e Download do sistema de comando são possíveis.
Reload Deactivation	ON: Reload está bloqueado. OFF: Reload é possível.
Force Deactivation	ON: Forcing é desligado. OFF: Forcing é possível.

Tabela 26: Variáveis de sistema para trancar e destrancar 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 ao estado STOP/VALID CONFIGURATION ao reiniciar. Assim, é possível recarregar um programa de aplicação.

Exemplo para a utilização destas variáveis de sistema:

Para poder trancar o sistema de comando

1. Definir variável global do tipo BOOL, colocar o valor inicial em OFF.
2. Atribuir variáveis globais às três variáveis de sistema *Read only in Run*, *Reload Deactivation* e *Force Deactivation*.
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 equipamento de entrada digital ou módulo de entrada digital, o sistema de comando é destrancado.

Anterior a CPU OS V.7

Locking: Para trancar o PES, é imprescindível proceder da seguinte maneira:

Trancar o sistema de comando

1. Ajustar os seguintes valores no sistema de comando antes de compilar (veja também Capítulo Criação de código):

Main Enable	em	ON
Forcing allowed	em	OFF (depende da aplicação)
Test mode allowed	em	OFF
Start/Restart allowed	em	ON
Load allowed	em	ON
Autostart	em	ON/OFF
Stop at Force Timeout	em	ON (depende da aplicação)

2. Depois de carregar e iniciar o sistema de comando online, alterar os seguintes interruptores nesta ordem:

Start/Restart allowed	em	OFF
Load allowed	em	OFF
Main Enable	em	OFF

i

Os seguintes interruptores apenas podem ser colocados em outros valores depois de consultar a instituição de certificação. =:

Forcing allowed	em	ON
Stop at Force Timeout	em	ON/OFF
Start/Restart allowed	em	ON
Autostart	em	ON

O sistema de comando está trancado.

Unlocking: Condição para destrancar (Main Enable em ON) é o estado de STOP do sistema de comando. A ativação da Main Enable de um sistema de comando em operação (no estado RUN) não é possível; por outro lado, é possível desativar a Main Enable no estado de RUN.

Para permitir um novo arranque depois de inicializar a CPU (depois de uma queda de tensão), proceder como segue ao destrancar o PES:

Destrancar o sistema de comando

1. Colocar a Main Enable em ON.
 2. Colocar Start/Restart em ON.
 3. Iniciar o programa de aplicação.
- O sistema de comando está destrancado.

8.2.3 Criação de código

Criar o código após a introdução correta do programa de aplicação e da atribuição das E/S do sistema de comando. Nesse momento, o gerador de código gera a soma CRC da configuração. Esta é uma assinatura para toda a configuração de CPU entradas/saídas e comunicação e é emitida como código hexadecimal em formato de 32 bits. A assinatura inclui todos os elementos que podem ser configurados ou alterados tais como lógica, variáveis, ajustes de interruptores.

Para excluir interferências pelo PC não seguro, gerar o código duas vezes. A soma CRC da configuração deve ser idêntica nas duas passagens.

Gerar o código para a operação direcionada à segurança

1. Iniciar o gerador de código para criar o código com CRC da configuração.
 - ☒ Código executável 1 com CRC 1.
2. Reiniciar o gerador de código para criar o código com CRC da configuração.
 - ☒ Código executável 2 com CRC 2.
3. Comparar CRC 1 com CRC 2.

- ☒ Ambos são idênticos.

O código gerado pode ser usado para a operação direcionada à segurança, também para certificação pelas instituições responsáveis por isso.

8.2.4 Carregar e iniciar o programa de aplicação

O processo de carregar (Download) um PES do sistema HIMatrix apenas pode ser realizado se antes o estado STOP foi ajustado.

Versão do hardware	Quantidade de programas de aplicação por sistema de comando
Anterior a L3	1
L3	1...32

Tabela 27: Quantidade de programas de aplicação num PES

O processo de carregar completo do programa de aplicação é monitorado. Em seguida, o programa de aplicação pode ser iniciado, ou seja, o processamento cíclico da rotina inicia.

i

A HIMA recomenda fazer o backup da configuração de projeto, p. ex. em um meio de armazenamento de dados amovível, após cada carregamento de um programa de aplicação no sistema de comando.

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.

8.2.5 Reload – com L3

Se os programas de aplicação sofrerem alterações, estas podem ser transferidas para o PES durante a operação. O sistema operacional verificar e ativa o programa de aplicação alterado, que depois assume a tarefa 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!

i

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.

8.2.6 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.

Informações mais detalhadas sobre o Forcing, veja os manuais de sistema dos sistemas compactos HI 800 528 PT, e dos sistemas modulares HI 800 527 PT.

8.2.7 Alteração on-line de parâmetros de sistema – a partir de CPU OS V.7

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

Parâmetros que podem ser alterados online:

Parâmetro	Layout do hardware	Versão do sistema operacional
System ID	Todos	Todos
Resource Watchdog Time	Todos	Todos
Safety Time	Todos	Todos
Target Cycle Time	Todos	A partir de CPU OS V.8
Target Cycle Time Mode	L3	A partir de CPU OS V.8
Main Enable	Todos	Todos
Autostart	Todos	Todos
Start Allowed	Todos	Todos
Load Allowed	Todos	Todos
Reload Allowed	L3	A partir de CPU OS V.8
Global Forcing Allowed	Todos	Todos
Global Force Timeout Reaction	Todos	Todos

Tabela 28: Parâmetros que podem ser alterados online, dependendo do layout de hardware e da versão do sistema operacional

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, devem-se tomar medidas técnicas e/ou organizacionais para evitar danos.

Main Enable permite a alteração dos demais parâmetros. *Main Enable* apenas pode ser colocado em TRUE no estado STOP.

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!

Com L3, alterações em parâmetros de sistema são possíveis durante a operação, também mediante Reload.

8.2.8 Documentação do programa para aplicações direcionadas à segurança

A ferramenta de programação 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
- Informações do gerador de código

A documentação é parte integrante da vistoria final de funcionamento de uma instalação sujeita à aprovação de uma instituição de verificação (p. ex., TÜV). A vistoria funcional final refere-se apenas à função de aplicação mas não aos módulos e equipamentos de automação do sistema HIMatrix direcionados à segurança que já foram aprovados como protótipo.

8.2.9 Multitasking – com L3

Multitasking denomina a capacidade do sistema HIMatrix Layout3 de processar até 32 programas de aplicação dentro do sistema processador.

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

O ciclo de um programa de aplicação pode durar vários ciclos do 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:

$$\text{Watchdog time}_{\text{programa de aplicação}} = \text{watchdog time}_{\text{módulo processador}} * \text{maximum number of cycles}$$

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 não ocorre limite parametrizado mediante *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 escritas pelo programa de aplicação!
- Um programa de aplicação avalia variáveis globais, que um outro programa de aplicação escreveu, até tantos ciclos do sistema processador mais tarde quanto for ajustado o parâmetro de sistema *Program's Maximum Number of CPU Cycles*. No caso mais desfavorável é possível que ocorra a seguinte sequência de eventos:
 - Programa A escreve variáveis globais que o programa B necessita.
 - O programa A encerra o seu ciclo naquele ciclo do sistema processador no qual o programa B iniciar o seu ciclo.
 - Nesse caso, o programa B apenas pode ser os valores escritos por A no início do seu próximo ciclo.
 - O ciclo recém iniciado de B pode demorar *Program's Maximum Number of CPU Cycles**tempo de ciclo. B recebe os valores escritos por A apenas nesse momento.
 - Até ocorrer uma reação de B a esses valores, podem se passar outra vez *Program's Maximum Number of CPU Cycles* ciclos do sistema processador!

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 detalhes sobre Multitasking, veja Manual de sistema dos sistemas compactos, HI 800 528 PT, ou o Manual de sistema dos sistemas modulares HI 800 527 PT.

8.2.10 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.

9 Configuração da comunicação

Além das variáveis de entrada e saída físicas, também é possível trocar variáveis com um outro sistema através de uma conexão de dados. Para tal, as variáveis do respectivo recurso são declaradas no editor de protocolos da ferramenta de programação.

Esta troca de dados pode ser do tipo leitura como também escrita.

9.1 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, de acordo com a versão do sistema de comando:

- SNTP
- Send/Receive TCP
- Modbus (master/slave)
- PROFIBUS DP (master/slave)
- INTERBUS.

9.2 Protocolo direcionado à segurança (safeethernet)

A comunicação direcionada à segurança via **safeethernet** é certificada até SIL 3.

A supervisão da comunicação direcionada à segurança deve ser parametrizada no editor **safeethernet** / Peer-to-Peer Editor.

Para o cálculo dos parâmetros **safeethernet Receive Timeout** e **Response Time** vale a seguinte condição:

A fatia de tempo de comunicação deve ser suficientemente grande para processar em um ciclo de CPU todas as conexões **safeethernet**.

Para funções direcionadas à segurança que são realizadas via **safeethernet**, apenas pode ser usado o ajuste *Use Initial Data*.

NOTA



É possível uma passagem involuntária para o estado seguro!

***ReceiveTMO* é um parâmetro direcionado à segurança!**

O valor de uma sinal deve ser mais comprido do que ***ReceiveTMO*** estiver ativo ou sendo monitorado via Loop-Back se todos os valores devem ser transmitidos.

ReceiveTMO é o intervalo de tempo de supervisão no sistema de comando 1, dentro do qual uma resposta correta deve ser recebida do sistema de comando 2.

9.2.1 Receive Timeout

ReceiveTMO é o tempo de supervisão em milissegundos (ms) dentro do qual uma resposta correta do parceiro de comunicação precisa ser recebida.

Se dentro do *ReceiveTMO* não chegar uma resposta correta do parceiro de comunicação, a comunicação direcionada à segurança é encerrada. As variáveis de Input destas conexão **safeethernet** se comportam de acordo com o parâmetro ajustado *Freeze Data on Lost Connection [ms]*.

Para funções direcionadas à segurança que são realizadas via **safeethernet**, é possível usar apenas o ajuste **Use Initial Data**.

Como o *ReceiveTMO* é relevante para a segurança e faz parte do Worst Case Reaction Time T_R (tempo máximo de reação, veja Capítulo 9.2.3 e continuação), o *ReceiveTMO* deve ser calculado como segue e introduzido no **safeethernet** Editor.

ReceiveTMO $\geq 4 \cdot \text{delay} + 5 \cdot \text{max. cycle time}$

Condição: A fatia de tempo de comunicação deve ser suficientemente grande para processar em um ciclo de CPU todas as conexões **safeethernet**.

Delay: Retardo no trajeto de transmissão, p.ex., causado por Switch, Satélite

Max. Cycle Time Tempo máximo do ciclo dos dois sistemas de comando

i

Uma tolerância desejável a falhas da comunicação pode ser alcançada mediante aumento do *ReceiveTMO*, caso seja admissível para o processo de aplicação em termos de tempo.

NOTA



O valor máximo admissível para *ReceiveTMO* depende do processo de aplicação e é ajustado no editor **safeethernet** junto com o Response Time máximo a ser esperado e o perfil.

9.2.2 ResponseTime

O *ResponseTime* é o tempo em milissegundos (ms) que passa até o remetente de uma mensagem receber a confirmação do recebimento do destinatário.

Para a parametrização com uso de um perfil de **safeethernet**, deve ser definido um *ResponseTime* previsto de acordo às características físicas do trajeto de transmissão.

O *ResponseTime* definido influencia a configuração de todos os parâmetros da conexão **safeethernet** que devem ser calculados como segue:

$$\text{ResponseTime} \leq \text{ReceiveTMO} / n$$

$$n = 2, 3, 4, 5, 6, 7, 8, \dots$$

A relação entre o *ReceiveTMO* e o *ResponseTime* influencia a capacidade de tolerância de falhas, p. ex., no caso de perdas de pacotes (repetição de pacotes de dados perdidos) ou no caso de atrasos no trajeto de transmissão.

Numa rede onde podem ocorrer perdas de pacotes deve ser satisfeito o seguinte requisito:

$$\text{min. Response Time} \leq \text{ReceiveTMO} / 2 \geq 2 \cdot \text{Delay} + 2.5 \cdot \text{max. Cycle Time}$$

Se este requisito for satisfeito, a perda de ao menos um pacote de dados pode ser amortecida sem interromper a conexão safe**ethernet**.

i

Se este requisito não for satisfeito, a disponibilidade de uma conexão safe**ethernet** apenas pode ser garantida numa rede sem colisões ou interferências. Porém, isso não significa um problema de segurança para o módulo processador!

i

Deve ser garantido que o sistema de comunicação respeite o Response Time parametrizado!

Para os casos onde isso nem sempre pode ser garantido, há uma variável de sistema da conexão à disposição para a supervisão do Response-Time. Se o Response-Time medido é ultrapassado não apenas em casos raros pela metade do ReceiveTMO, então, o Response-Time parametrizado deve ser aumentado.

O Receive Timeout deve ser adaptado ao novo Response Time parametrizado.

NOTA



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

$$\text{safety time} = 2 * \text{watchdog time}$$

estiver ajustado.

9.2.3

Tempo de ciclo máximo do sistema de comando HIMatrix

Para determinar o tempo de ciclo máximo (tempo de Watchdog mínimo) para um sistema de comando HIMatrix, a HIMA recomenda o seguinte procedimento:

Determinar o tempo de ciclo máximo do sistema de comando HIMatrix

1. Operar o sistema sob carga total. Neste momento, todas as conexões de comunicação devem estar em operação, tanto via safe**ethernet** quanto através de protocolos padrão. Ler com frequência o tempo de ciclo no Control Panel e anotar o tempo de ciclo máximo.
2. Repetir passo 1 para o parceiro de comunicação (segundo sistema de comando HIMatrix).
3. O maior dos dois tempos de ciclo máximos determinados é o tempo de ciclo máximo procurado.

O tempo de ciclo máximo está determinado e entra nos cálculos posteriores.

9.2.4

Cálculo do tempo máximo de reação

O tempo máximo de reação T_R (*Worst Case Reaction Time*) da mudança de estado de um transdutor do PES 1 até a reação da saída do PES 2 pode ser calculado como segue:

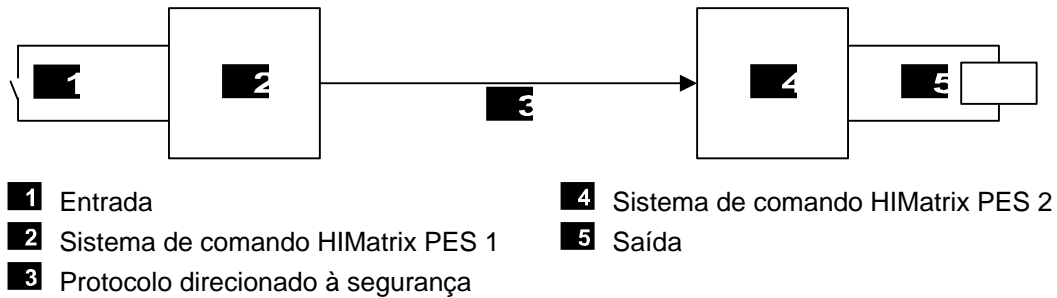


Figura 4: Tempo de reação ao conectar dois sistemas de comando HIMatrix

$$T_R = t_1 + t_2 + t_3$$

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

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

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

O tempo máximo de reação T_R da mudança de estado de uma entrada do primeiro PES ou Remote I/O HIMatrix (p. ex., F3 DIO 20/8 01) até a reação da saída do segundo PES ou Remote I/O HIMatrix pode ser calculado como segue:

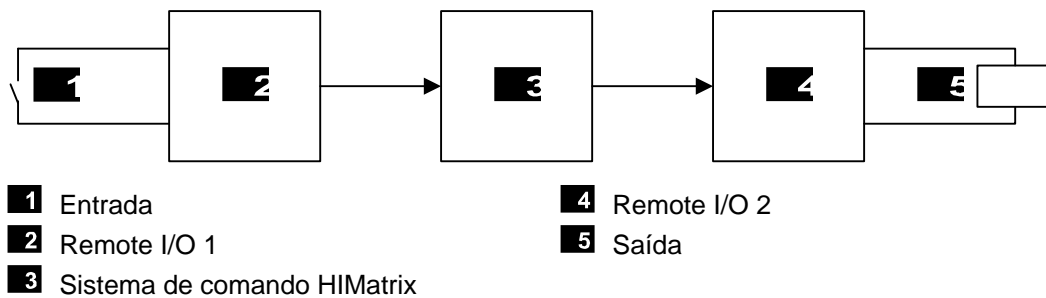


Figura 5: Tempo de reação com Remote I/Os

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

T_R Worst Case Reaction Time

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

t_2 ReceiveTMO₁

t_3 2 * tempo de Watchdog do sistema de comando HIMatrix

t_4 ReceiveTMO₂

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.

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

O tempo máximo de reação T_R da mudança de estado de uma entrada do primeiro PES HIMatrix até a reação da saída do segundo PES HIMatrix pode ser calculado como segue:

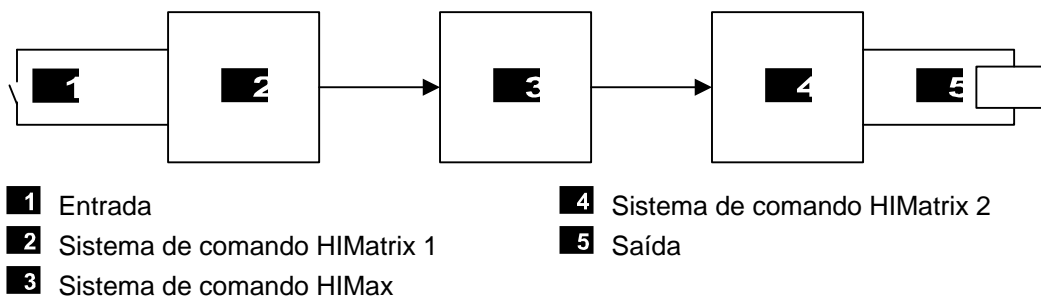


Figura 6: Tempo de reação com dois sistemas de comando HIMatrix e um sistema de comando HIMax

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

T_R Worst Case Reaction Time

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

t_2 ReceiveTMO₁

t_3 2 * tempo de Watchdog do sistema de comando HIMax

t_4 ReceiveTMO₂

t_5 2 * tempo de Watchdog do sistema de comando HIMatrix 2

Observação: Os dois sistema de comando HIMatrix 1 e 3 também podem ser idênticos.

9.2.7

Conceitos

ReceiveTMO

Tempo de supervisão no sistema de comando 1, dentro do qual deve ser recebido uma resposta válida do sistema de comando 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.

Worst Case
Reaction Time

Tempo máximo de reação para a transmissão da alteração do sinal de uma entrada física de um sistema de comando 1 até a alteração da saída física de um sistema de comando 2.

9.2.8

Atribuição dos endereços **safeethernet**

Ao atribuir os endereços de rede (endereços IP) para **safeethernet**, devem ser observados os seguintes pontos:

- Os endereços devem ser inequívocos na rede usada.
- Ao conectar a **safeethernet** com uma outra rede (Lan interno da empresa), deve ser observado que não possam ocorrer interferências. Possíveis fontes de interferências são, p. ex.,
 - a troca de dados lá.
 - Acoplamento a outras redes (p. ex., internet).

Nestes casos, tomar medidas adequadas, p. ex., uso de Switch Ethernet, Firewall, para evitar interferências.

10 Aplicação em centrais de alarme de incêndio

Os sistemas HIMatrix podem ser utilizados para centrais de alarme de incêndio conforme DIN EN 54-2 e NFPA 72 se para as entradas e saídas uma supervisão de linha estiver parametrizada.

Para esse fim, é necessário que o programa de aplicação satisfaça as funcionalidades para centrais de alarme de incêndio de acordo com as normas listadas.

O tempo de ciclo máximo exigido na DIN EN 54-2 para centrais de alarme de incêndio de 10 segundos pode ser facilmente satisfeito com os sistemas, porque o tempo de ciclo desses sistemas está na faixa de milissegundos e também o tempo de segurança eventualmente exigido de 1 segundo (tempo de reação de erro).

Conforme EN 54-2, a central de alarme de incêndio deve assumir o estado de comunicação de avaria dentro de 100 segundos depois de receber a mensagem de avaria no sistema HIMatrix.

A ligação dos sensores de incêndio ocorre pelo princípio de circuito aberto com supervisão de linha para curto e quebra de fio. Para este fim, podem ser usados os seguintes equipamentos e módulos:

- As entradas digitais e analógicas do sistema de comando F35
- As entradas analógicas da Remote I/O F3 AIO 8/4 01
- As entradas e saídas digitais das Remote I/Os F3 DIO 16/8 01 e F3 DIO 8/8 01
- Os módulos de entrada AI 8 01 e MI 24 01 do sistema de comando F60

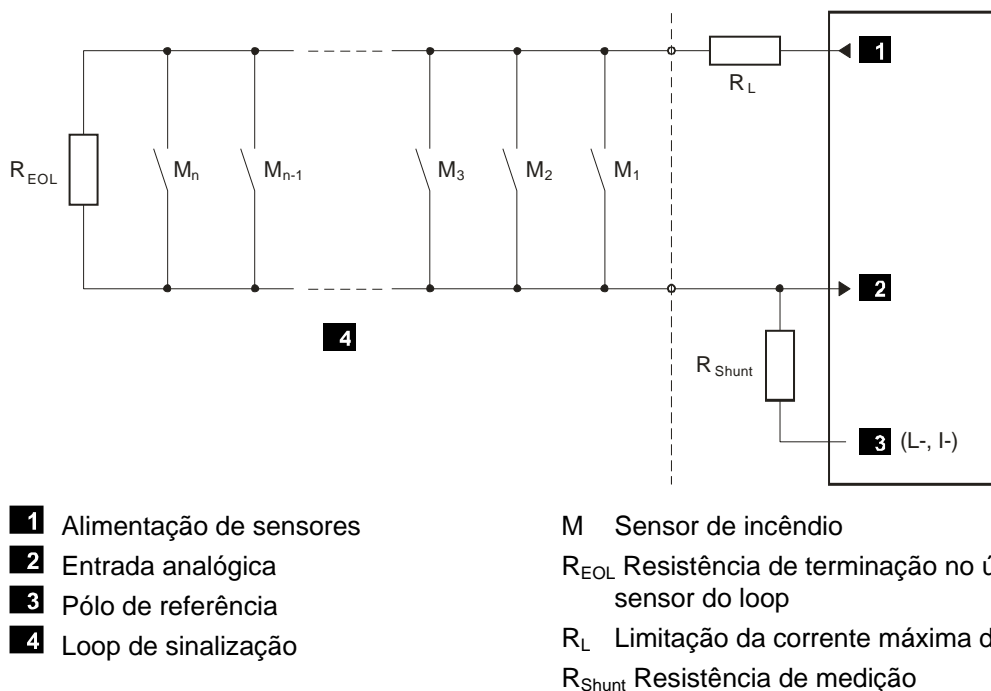


Figura 7: Ligação de sensores de incêndio

Para a aplicação devem ser calculadas as resistências R_{EOL} , R_L e R_{Shunt} , dependendo dos sensores utilizados e da quantidade de sensores por loop de sinalização. Os dados necessários para isso devem ser consultados na respectiva folha de dados do fabricante do sensor.

As saídas de alarme para comandar lâmpadas, sirenes, buzinas, etc., são operadas pelo princípio de circuito aberto. Esas saídas devem ser monitoradas para detectar quebra de fio e curto de linha. Isso pode ocorrer por retorno dos sinais de saída diretamente do atuador para entradas.

A corrente no circuito atuador pode ser monitorada por uma entrada analógica com um Shunt adequado. Uma ligação em série de diodo Z e resistência de entrada protege a entrada de sobretensão no caso de um curto de linha.

Para uma detecção inequívoca da quebra de fio (com as saídas DO desligadas), adicionalmente às entradas analógicas é necessária uma alimentação do transmitter (veja esboço abaixo):

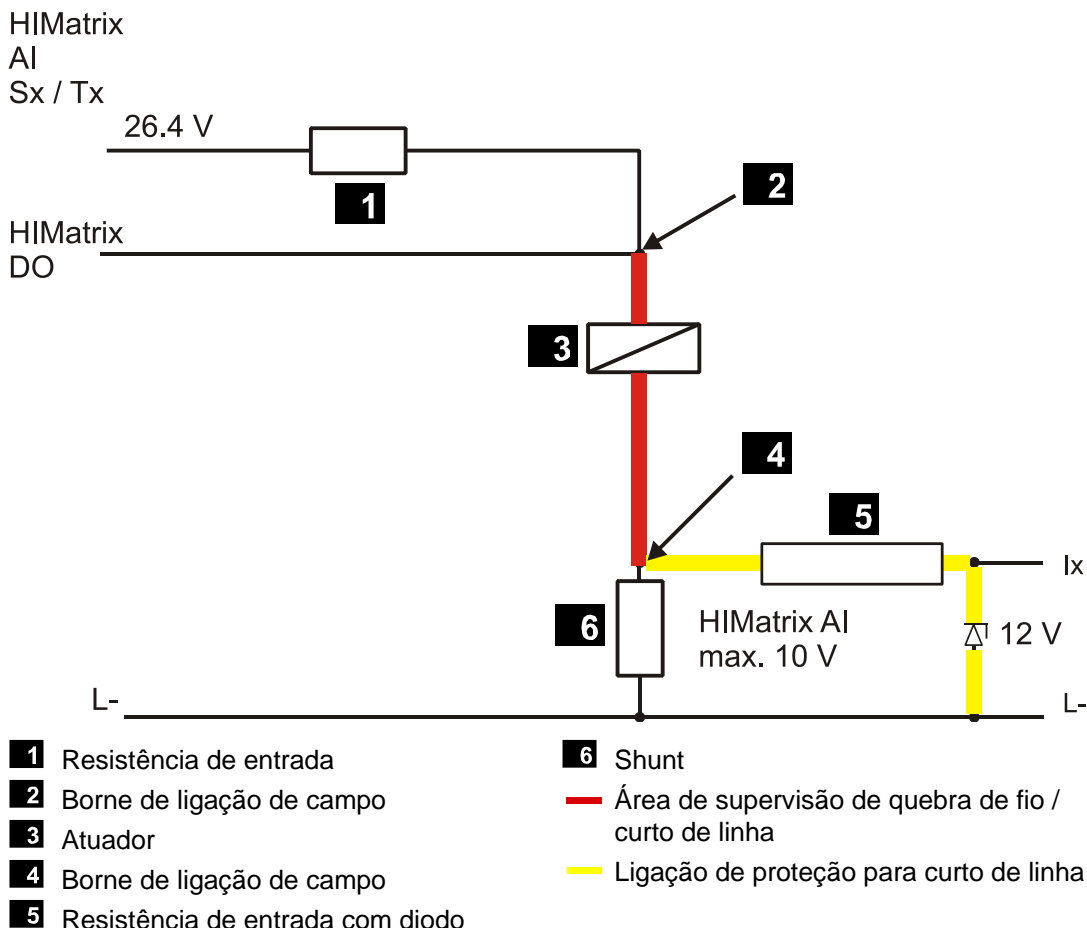


Figura 8: Exemplo da supervisão de quebra de fio e curto de linha de saídas digitais (circuito atuador)

Um exemplo de parametrização para a supervisão de curto de linha com supervisão adicional de quebra de fio de atuadores mediante entradas analógicas encontra-se no Capítulo *Line Monitoring* no manual HIMatrix F35 HI 800 547 PT.

Um programa de aplicação especialmente adaptado a esta tarefa pode realizar o acionamento de sistemas de visualização, painéis luminosos, indicadores de LED, displays alfanuméricos, alarmes acústicos, etc.

A repassagem de mensagens de avaria através de canais de entrada / saída ou até os dispositivos de transmissão para mensagens de avarias deve ocorrer no princípio de circuito fechado.

A transmissão de mensagens de incêndio de um sistema HIMatrix para um sistema de outros fabricantes pode ser realizada com o padrão comunicação existente Ethernet (OPC). A queda da comunicação deve ser comunicada.

Os sistemas HIMatrix que são utilizados como central de alarme de incêndio devem possuir uma alimentação com corrente redundante. Também devem ser tomadas medidas contra uma queda da alimentação com energia, p. ex., uma buzina alimentada por bateria. A comutação entre alimentação de rede e alimentação com corrente de reserva deve

garantir a operação ininterrupta. Quedas de tensão até uma duração de 10 ms são admissíveis.

No caso de avarias do sistema, o sistema operacional escreve as variáveis/os sinais atribuídos no programa de aplicação. Assim, a sinalização de erros para os erros detectados pelo sistema pode ser programada. O sistema HIMatrix desliga no caso erro as entradas e saídas direccionadas à segurança, com as seguintes consequências:

- Processamento do nível Low em todos os canais das entradas com erro.
- Desligamento de todos os canais das saídas com erro.

Anexo

Aumento do SIL de sensores e atuadores

Os sistemas de comando HIMatrix 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, o valor SIL exigido pode ser alcançado da seguinte maneira:

- 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.

Glossário

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
COM	Módulo de comunicação
CRC	Cyclic Redundancy Check, Soma de verificação
DI	Digital Input, Entrada digital
DO	Digital Output, Saída digital
EMC	ElectroMagnetic Compatibility – Compatibilidade eletromagnética
EN	Normas europeias
ESD	ElectroStatic Discharge, descarga eletrostática
FB	Fieldbus, barramento de campo
FBS	Funktionsbausteinsprache, linguagem de bloco funcional
FTA	Field Termination Assembly
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	International Electrotechnical Commission: Normas internacionais para eletrotécnica
MAC Address	Endereço de hardware de uma conexão de rede (Media Access Control)
PADT	Programming and Debugging Tool (conforme IEC 61131-3), PC com SILworX
PE	Protective Earth: 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: Variável/sinal de sistema, fornece valores, p. ex., ao programa de aplicação
Rack ID	Identificação de um suporte básico (número)
Non-reactive/ sem retroalimentação	Dois circuitos de entrada estão ligados à mesma fonte (p. ex., transmissor). Uma ligação de entrada é chamada de <i>sem efeito de retroalimentação</i> se ela não interferir com os sinais de uma outra ligação de entrada.
R/W	Read/Write (Ler/Escriver, título de coluna para tipo de variável/sinal de sistema)
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 sistemas HiMatrix
SNTP	Simple Network Time Protocol (RFC 1769)
S.R.S	System.Rack.Slot Endereçamento de um módulo
SW	Software
TMO	Timeout
W	Write: Variável/sinal de sistema, é alimentado com valores, p. ex., do programa de aplicação
Watchdog (WD)	Supervisão de tempo para módulos ou programas. O ultrapassar o tempo do watchdog, o módulo ou programa entra em parada por erro.
WDT	Watchdog Time

Lista de figuras

Figura 1:	Representação dos blocos de função no exemplo da CPU 01 do F60	23
Figura 2:	Line Control	28
Figura 3:	Sinais de ciclo T1, T2	29
Figura 4:	Tempo de reação ao conectar dois sistemas de comando HIMatrix	62
Figura 5:	Tempo de reação com Remote I/Os	62
Figura 6:	Tempo de reação com dois sistemas de comando HIMatrix e um sistema de comando HIMax	63
Figura 7:	Ligação de sensores de incêndio	64
Figura 8:	Exemplo da supervisão de quebra de fio e curto de linha de saídas digitais (circuito atuador)	65

Lista de tabelas

Tabela 1:	Variantes do sistema HIMatrix	8
Tabela 2:	Normas para requisitos de CEM, climáticas e do meio-ambiente	11
Tabela 3:	Requisitos gerais	11
Tabela 4:	Requisitos climáticos	11
Tabela 5:	Testes mecânicos	12
Tabela 6:	Testes de resistência contra interferência	12
Tabela 7:	Testes de emissão de interferência	12
Tabela 8:	Verificação das características da alimentação com corrente contínua	13
Tabela 9:	Documentação de sistema HIMatrix	14
Tabela 10:	Faixas de valores do tempo de segurança	17
Tabela 11:	Faixa de valores do tempo de Watchdog	18
Tabela 12:	Visão geral das entradas do sistema HIMatrix	26
Tabela 13:	Códigos de erro com entradas digitais	27
Tabela 14:	Valore de entradas analógicas direcionadas à segurança	29
Tabela 15:	Entradas analógicas do sistema de comando F35	30
Tabela 16:	Entradas analógicas da Remote I/O F3 AIO 8/4 01	30
Tabela 17:	Entradas analógicas do sistema de comando F60	30
Tabela 18:	Configuração de entradas não usadas	31
Tabela 19:	Códigos de erro com entradas analógicas	31
Tabela 20:	Códigos de erro em entradas de contador	32
Tabela 21:	Visão geral sobre as saídas do sistema HIMatrix	34
Tabela 22:	Os parâmetros de sistema do recurso a partir de CPU-BS V.7	47
Tabela 23:	Variáveis de sistema do hardware a partir de CPU OS V.7	47
Tabela 24:	Parâmetros de sistema do recurso anterior a CPU OS V.7	48
Tabela 25:	Comprimento de nomes de variáveis	51
Tabela 26:	Variáveis de sistema para trancar e destrancar o PES	53
Tabela 27:	Quantidade de programas de aplicação num PES	55
Tabela 28:	Parâmetros que podem ser alterados online, dependendo do layout de hardware e da versão do sistema operacional	56

Índice remissivo

Condições de utilização		
Alimentação com tensão.....	13	
CEM.....	12	
climáticas.....	11	
mecânicas.....	12	
Proteção contra ESD.....	13	
Destrançar o sistema de comando anterior a CPU OS V.7.....	54	
Fault tolerance time, tempo de tolerância de falhas.....	17	
Hardware Editor.....	47	
Multitasking.....	57	
Para poder trancar o sistema de comando a partir da V.7.....	53	
Princípio de circuito aberto.....	10	
Princípio de circuito fechado.....	10	
Reações de erro		
entradas analógicas.....	31	
Entradas de contador.....	32	
entradas digitais.....	27	
saídas analógicas.....	39, 40	
Saídas de relé.....	38	
saídas digitais.....	35	
saídas digitais de 2 pinos.....	37	
Repetição da verificação.....	18	
Tempo de segurança.....	17	
Tempo de Watchdog		
Programa e aplicação.....	18	
Teste de função do sistema de comando	42	
Trancar o sistema de comando anterior a CPU OS V.7.....	53	
Watchdog Time.....	18	



SAFETY
NONSTOP

HIMA Paul Hildebrandt GmbH

Postfach 1261

D-68777 Brühl

Tel: +49 6202 709-0

Fax: +49 6202 709-107

E-Mail: info@hima.com

Internet: www.hima.com

(1129)

HI 800 526 PT © by HIMA Paul Hildebrandt GmbH