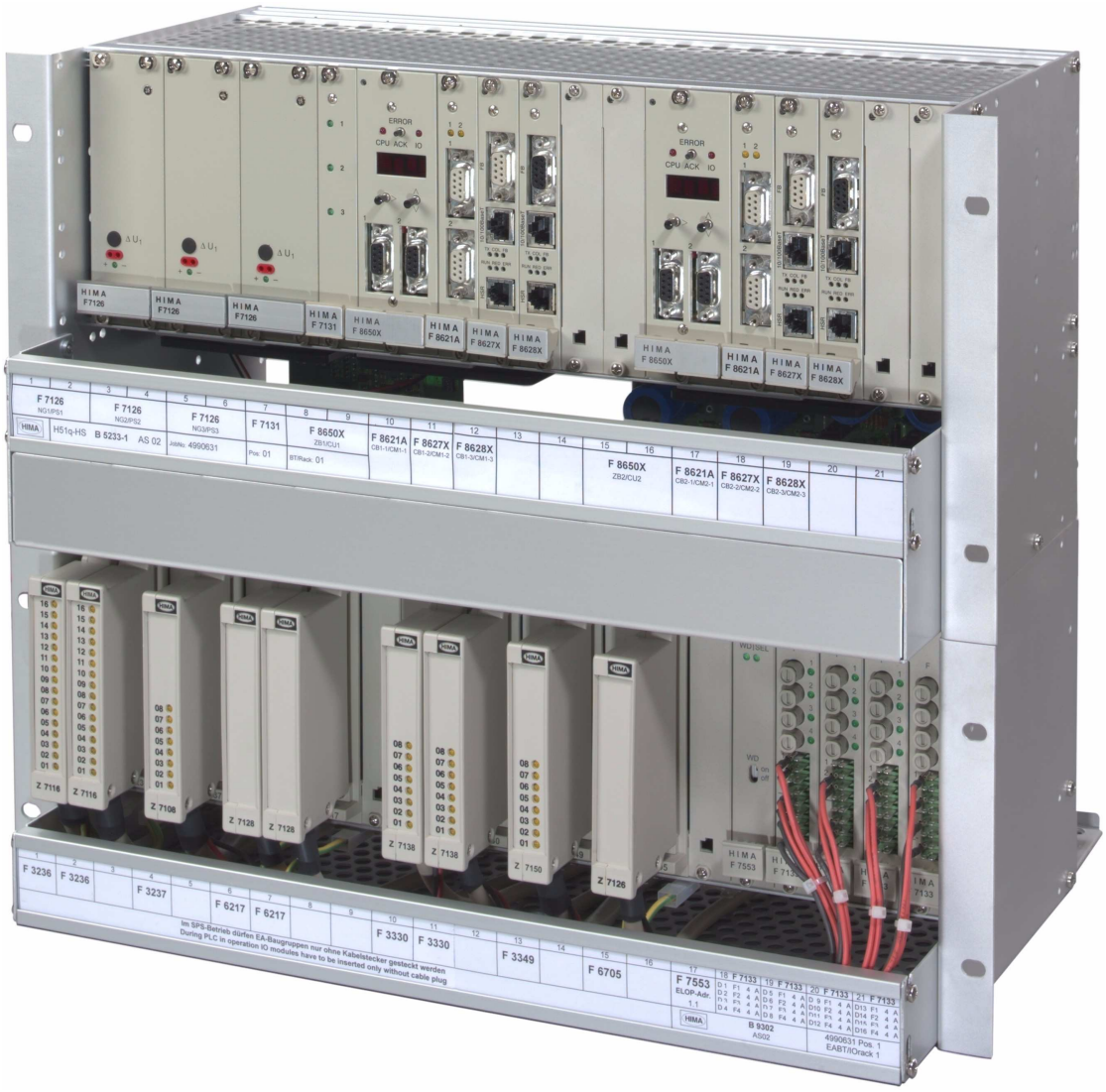
H41q/H51q

Sistema de comando direcionado à segurança

H41q/H51q Manual de segurança



HIMA Paul Hildebrandt GmbH

Automação industrial

Rev.1.00

HI 800 490 PT

Aviso importante

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 a outros fabricantes mencionados e seus produtos.

Os dados técnicos estão sujeitos a alterações sem notificação prévia.

Todos os dados e avisos técnicos neste manual foram elaborados com o máximo de cuidado, considerando medidas efetivas de controle de garantia de qualidade. Mesmo assim, erros não podem ser totalmente excluídos. A HIMA avisa que não pode assumir garantia ou aceitar responsabilidade legal ou direitos de indenização pelas consequências oriundas de informações incorretas. A HIMA agradece a comunicação de eventuais erros.

Contato
Endereço da HIMA:

© HIMA Paul Hildebrandt GmbH
Postfach 1261
D - 68777 Brühl
Telefone +49 06202 709-0
Fax +49 06202 709-107
E-Mail Info@hima.com
Internet http://www.hima.com

Índice de revisões	Alterações	Tipo de alteração	
		técnica	redacional
1.00	Edição em português (tradução)	X	X

Índice

Anexo

1 Introdução

Este manual contém informações para o uso previsto dos equipamentos de automação HIMA H41q e H51q direcionados à segurança.

São pré-requisitos para instalação e colocação em funcionamento seguros, bem como para a segurança durante a operação e manutenção dos equipamentos de automação H41q/H51q:

- 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 H41q/H51q 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
- As condições ambientais especificadas
- Apenas são conectados equipamentos de outros fabricantes se estiverem certificados

Por motivos da estrutura clara, este manual não contém todos os detalhes sobre todas as versões dos dispositivos de automação H41q/H51q.

1.1 Validade e atualidade

Sempre a versão mais recente do manual de segurança possui validade também para versões mais antigas do sistema operacional. As especificidades de determinadas versões são mencionadas no texto.

A versão mais recente está à disposição na homepage www.hima.com.

Alterações abrangentes do manual são identificadas por um novo estado de revisão, modificações menores, por uma nova edição. O estado de revisão encontra-se na capa, atrás do número do documento, a versão pode ser verificada na capa traseira.

1.2 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
Itálico	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 híperlinks, mesmo quando não são especialmente destacadas. Ao posicionar o cursor nelas, o mesmo muda sua aparência. Ao clicar, o documento salta para o respectivo ponto.

Avisos de segurança e utilização são destacados de forma especial.

1.2.1 Avisos de segurança

Os avisos de segurança no documento são representados como descrito a seguir.

Para garantir o menor risco possível devem ser observados sem excepção. A estrutura lógica é

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

⚠ PALAVRA SINALIZADORA

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

AVISO

Aviso! Tipo e fonte dos danos.
Como evitar os danos.

1.2.2 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.

1.3 Grupo alvo

Este manual destina-se a planejadores, projetistas e programadores de sistemas de automação. Pressupõem-se conhecimentos especializados na área de sistemas de automatização direcionados à segurança.

1.4 Perigos residuais

Do equipamento H41q/H51q em si não emana nenhum perigo.

Perigos residuais podem ser causados por:

- Erros do projeto
- Erros no programa de aplicação
- Erros na fiação

2 Utilização prevista

2.1 Área de aplicação

Os equipamentos de automação direcionados à segurança H41q, H41qc e H51q podem ser utilizados até o nível de integridade de segurança SIL 3 (IEC 61508) ou a categoria de segurança Cat 4/PI e (ISO 13849-1).

Todos os grupos de entrada/saída podem ser utilizados tanto com versão redundante quanto mono-canal dos componentes centrais.

Na utilização da comunição direcionada à segurança entre diferentes equipamentos deve ser observado que o tempo total de reação do sistema não ultrapasse o tempo de tolerância a erros. As bases de cálculo listadas no Manual de segurança HI 800 490 P devem ser aplicadas

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

Os sistemas H41q/H51q estão certificados para sistemas de comando de processos, sistemas de proteção, sistemas de queimadores e sistemas de comando de máquinas.

2.1.1 Aplicação no princípio de circuito fechado

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

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

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

2.1.2 Aplicação no princípio de circuito aberto

Os sistemas de comando H41q/H51q 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).

Para este fim, os sistemas de comando H41q/H51q foram verificados e certificados conforme EN54 e NFPA72 para a aplicação em sistemas de detecção de incêndios e sistemas de extinção de incêndios. Nestes sistemas, exige-se que no caso de solicitação o estado ativo para dominar o perigo seja assumido.

2.1.3 Proteção contra explosão

Os equipamentos de automação direcionados à segurança H41q, H41qc e H51q são adequados para a instalação na Zona 2. As respectivas declarações de conformidade estão nas folhas de dados.

Devem ser observadas as condições de utilização listadas abaixo!

2.1.4 Aplicação em centrais de alarme de incêndio

Todos os sistemas H41q/H51q com entradas analógicas podem ser utilizados para centrais de alarme de incêndio conforme DIN EN 54-2 e NFPA 72.

Devem ser observadas as condições de utilização listadas abaixo!

2.2 Utilização não-prevista

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

Comunicação direcionada à segurança com as interfaces de barramento de campo é impossível sem protocolos de barramento de campo direcionados à segurança.

2.3 Condições de utilização

2.3.1 Condições ambientais e dados técnicos

Para a utilização dos sistemas de comando direcionados à segurança H41q/H51q 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
Temperatura de operação	Temperatura de operação: 0...+60 °C
Temperatura de armazenamento	Temperatura de armazenamento: -40...+80 °C (com bateria: apenas -30 °C...+75 °C)
Contaminação	Grau de contaminação II
Altura de instalação	< 2000 m
Caixa	Padrão: IP 20 Se as normas aplicáveis (p. ex., EN 60204, EN 954-1) o exigirem, o equipamento deve ser montado numa caixa do grau de proteção exigido (p.ex., IP 54).
Tensão de entrada fonte de alimentação	24 V DC

Tabela 1: Requisitos de ambiente

Diversos desvios devem ser consultados na respectiva folha de dados.

Os sistemas de comando direcionados à segurança H41q, H41qc e H51q foram desenvolvidos para satisfazerem os requisitos das seguintes normas para CEM e requisitos climáticas e de meio-ambiente.

Norma	Conteúdo
IEC/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

2.3.2 Requisitos climáticos

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...+80 °C (com bateria: apenas -30 °C)
	Calor e frio secos; testes de resistência: +70 °C / -25 °C, 96 h alimentação de corrente não ligada
	Mudança de temperatura; testes de resistência e insensibilidade: -25 °C / +70 °C e 0 °C / +55 °C alimentação de corrente não ligada
	Ciclos com calor úmido; testes de resistência: +25 °C / +55 °C, 95 % umidade relativa alimentação de corrente não ligada

Tabela 3: Requisitos climáticos

2.3.3 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 4: Testes mecânicos

2.3.4 Requisitos CEM

Os mais importantes testes e valores limite para os requisitos de CEM são listados na tabela a seguir.

IEC/EN 61131-2	Testes de resistência contra interferência
IEC/EN 61000-4-2	Teste ESD: 6 kV contato-, 8 kV descarga pelo ar (EN 230, EN 50130)
IEC/EN 61000-4-3	Teste de RFI (10 V/m): 80 MHz...2 GHz, 80 % AM
IEC/EN 61000-4-4	Teste Burst: 2 kV em condutores de alimentação, 1 kV em condutores de sinal, 2 kV em condutores AC

Tabela 5: Testes de resistência contra interferência

IEC/EN 61000-6-2	Testes de resistência contra interferência
IEC/EN 61000-4-6	Alta frequência, assimétrica 10 V, 150 kHz...100 MHz, AM
IEC/EN 61000-4-3	434 MHz-, pulsos de 900 MHz, 20 V/m
IEC/EN 61000-4-5	Tensão de choque: 2 kV, 1 kV em condutores de alimentação

Tabela 6: Testes de resistência contra interferência

IEC/EN 61000-6-4	Testes de emissão de interferência
EN 50011 Classe A	Emissão de interferências: por irradiação, via conexão de cabo

Tabela 7: Testes de emissão de interferência

Todos os componentes dos sistemas H41q e H51q satisfazem os requisitos da diretiva de CEM da União Europeia e exibem a marca CE.

Em caso de interferências acima dos limites indicados, os sistemas reagem de forma direcionada à segurança.

2.3.5 Alimentação com tensão

Os mais importantes testes e valores limite para os requisitos de alimentação com tensão são listados na tabela a seguir.

IEC/EN 61131-2:	Verificação das características da alimentação com corrente contínua
	Alternativamente, a fonte de alimentação com tensão deve satisfazer as seguintes normas: IEC 61131-2 ou SELV (Safety Extra Low Voltage, EN 60950) ou PELV (Protective Extra Low Voltage, EN 60742)
	A proteção dos equipamentos H41q, H41qc e H51q deve ocorrer de acordo com as indicações nas folhas de dados.
	Verificação da faixa de tensão: 24 V DC, -20 %...+25 % (19,2...30,0 V DC)
	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: veja nota no respectivo capítulo do catálogo ou na folha de dados do componente de alimentação com corrente
	Bateria tampão, teste de resistência: Verificação B, 1000 h, bateria de lítio como bateria tampão

Tabela 8: Verificação das características da alimentação com corrente contínua

2.3.6 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.

Descargas eletrostáticas podem danificar os componentes eletrônicos montados nos sistemas.

- Para fins de descarga eletrostática, tocar num objeto aterrado.
- Usar para os trabalhos um posto de trabalho protegido contra descarga eletrostática e usar uma fita de aterramento.
- Se não for usado, guardar o equipamento de forma protegida contra descarga eletrostática, p.ex., na embalagem.

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

2.4 Qualificação to pessoal

Todo pessoal técnico (planejamento, montagem, colocação em funcionamento) deve estar instruído a respeito dos riscos e suas possíveis consequências que podem surgir no caso da manipulação de um sistema de automação direcionado à segurança.

Adicionalmente, planejadores e projetistas devem possuir conhecimentos na seleção e utilização de sistemas de segurança elétricos e eletrônicos em instalações de automação industrial para evitar as consequências de conexões erradas e programação incorreta, por exemplo.

A empresa operadora do sistema é responsável pela qualificação e pelo treinamento de segurança do pessoal de operação e manutenção.

Alterações ou ampliações na fiação do sistema apenas podem ser efetuadas por pessoal qualificado com conhecimentos na tecnologia de comando e regulação, eletrotécnica, eletrônica, utilização de PES e em medidas de proteção contra descargas eletrostáticas ESD.

2.5 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 H41q/H51q em sistemas de automação e instalações completas.

A programação correta dos sistemas H41q/H51q deve ser validada pelos fabricantes de máquinas e sistemas de forma suficiente.

3 Filosofia de segurança e restrições

3.1 Certificação

Os equipamentos de automação direcionados à segurança (PES = sistema eletrônico programável) das famílias de sistemas H41q, H41qc e H51q são certificados como segue:

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

Certificado e relatório de teste Nº 968/EZ 129.16/10

Equipamentos de automação direcionados à segurança
H41q-MS, H41q-HS, H41q-HRS
H41qc-MS, H41qc-HS, H41qc-HRS
H51q-MS, H51q-HS, H51q-HRS

Os equipamentos de automação direcionados à segurança das famílias de sistemas H41q, H41qc e H51q foram verificados e certificados de acordo com as normas para a segurança funcional listadas:

IEC 61508: Partes 1–7: 1998–2000	até SIL 3
IEC 61511: Partes 1–3: 2004	até SIL 3
EN/ISO 13849-1: 2008	Categoria 4, Performance Level e
EN 50156-1: 2004	
EN 12067-2: 2004, EN 298: 2003, EN 230: 2005	
NFPA 85: 2007, NFPA 86: 2007	
EN 61131-2: 2007	
EN 61000-6-2: 2005, EN 61000-6-4: 2007	
EN 54-2:1997, A1: 2006, NFPA 72: 2010	
EN 50130-4: 1998 + A1: 1998 + A2: 2003 + Corr. 2003	

O capítulo 2.3 contém uma lista detalhada de todas as verificações ambientais e de CEM realizadas.

3.2 Segurança e disponibilidade

Já como sistemas mono, as famílias de sistema H41q, H41qc e H51q estão preparadas para o uso até SIL 3, devido à estrutura de microprocessador 1oo2D, em um módulo central.

De acordo com a disponibilidade exigida, os sistemas de automação HIMA podem ser equipados com módulos redundantes na área central e de E/S. Módulos redundantes aumentam a disponibilidade, pois no caso de um defeito de um módulo, ele é retirado da operação automaticamente e o módulo redundante mantém a operação sem interrupção.

3.2.1 Segurança

Para os sistemas relacionados à segurança H41q, H41qc e H51q foram efetuados cálculos de PFD (Probability of Failure on Demand) e PFH- (Probability of Failure per Hour) de acordo com a IEC 61508.

A norma IEC 61508-1 estabelece para SIL 3:

- PFD de $10^{-4}...10^{-3}$
- PFH de $10^{-8}...10^{-7}$ por hora

Para o sistema de comando são assumidos 15 % do valor limite da norma para PFD e PFH. Assim, resultam como valores limite proporcional do sistema de comando:

- PFD = $1{,}5 * 10^{-4}$
- PFH = $1{,}5 * 10^{-8}$ por hora

Como intervalo da repetição da verificação para os sistemas relacionados à segurança H41q, H41qc e H51q estabelecem-se 10 anos [1)].

As funções de segurança compostas do Loop relacionado à segurança (uma entrada, unidade de processamento e uma saída) satisfazem em todas as combinações as exigências.

Informações mais detalhadas estão disponíveis sob solicitação.

3.2.2 Visão geral

A seguinte tabela contém uma visão geral de denominações de sistemas, segurança, disponibilidade e configurações de sistema

Denominação do sistema	H41qc-MS H41q-MS H51q-MS	H41qc-HS H41q-HS H51q-HS	H41qc-HRS H41q-HRS H51q-HRS
SIL / Categoria	SIL 3 / Cat 4	SIL 3 / Cat 4	SIL 3 / Cat 4
Disponibilidade	normal	alta	muito alta
Configuração			
Módulo central	mono	redundante	redundante
Módulos de E/S	mono[1)]	mono[1)]	redundante
barramento de E/S	mono	mono	redundante[2)]

1) Para aumentar a disponibilidade, também é possível usar módulos individuais de E/S de forma redundante ou numa ligação seletiva 2oo3 (veja, p. ex,. Capítulo 7.8.5)

2) A HIMA recomenda no caso de um barramento de E/S redundante não utilizar apenas os módulos de E/S de forma redundante, mas também a periferia (sensores e atuadores na instalação), na medida do possível. Esses elementos em geral possuem uma taxa de falha maior do que os módulos do PES.

Tabela 9: Denominações de sistemas, segurança, disponibilidade e configurações de sistema

1) Restrições no caso do módulo de relé F 3430, veja Capítulo 6.5

Para aumentar a disponibilidade mediante módulos redundantes, três pontos são essenciais:

- Módulos defeituosos devem ser detectados e desligados para que não possam bloquear o sistema.
- A empresa operadora deve receber uma notificação no caso de erros, para a substituição dos módulos.
- Depois da substituição de um módulo ele deve entrar em operação automaticamente.

Essas exigências são satisfeitas pelos sistemas de automação HIMA nas respectivas configurações.

Para a programação dos equipamentos usa-se um PADT (aparelho de programação, PC) com a ferramenta de programação

ELOP II

conforme IEC 61131-3. Ele oferece apoio na elaboração de programas direcionados à segurança e na operação dos dispositivos de automação.

3.3 Tempos de segurança

Erros individuais que possam causar um estado operacional perigoso são detectados pelos dispositivos de autoteste dentro do tempo de tolerância a falhas (mín. 1 s). O tempo de tolerância a falhas é definido como tempo de segurança no menu para o ajuste das propriedades do recurso.

Tempo de tolerância de falhas
Grandeza da técnica de processos que muitas vezes é denominada de tempo de segurança nas diretivas para os usuários.

Tempo de segurança (no PES)
Grandeza que depende da capacidade de sistema

Falhas que apenas possam ter efeitos críticos para a segurança em combinação com erros adicionais são detectados por testes de fundo dento do tempo de ocorrências de falhas múltiplas (MOT – multiple fault occurence time). O tempo de ocorrência de falhas múltiplas é determinado com a parametrização do tempo de segurança e no sistema operacional está definido como tempo 3600 vezes maior.

No caso dos testes há uma diferença entre:

- *Testes dentro do tempo de segurança*
  São executados dentro do tempo de segurança (testes de primeiro plano).
  Tempo de reação: imediatamente, o mais tardar dentro do tempo de segurança.
- *Testes dentro do tempo de ocorrência de falhas múltiplas*
  São executados dentro do tempo de ocorrência de falhas múltiplas e divididos em muitos ciclos (testes de segundo plano).
  Tempo de reação: imediatamente depois da detecção, o mais tardar dentro do tempo de ocorrência de falhas múltiplas.

Exemplo para o tempo de reação: No máximo o dobro do tempo de ciclo. Se para o processo é exigido uma tolerância a falhas (tempo de segurança) de 1 s, o tempo de ciclo não pode ser maior do que 500 ms.

Tempo de reação a falhas

O tempo de reação a falhas de um dispositivo de automação corresponde ao tempo de segurança (≥ 1 s) definido nas propriedades do recurso. Aqui deve ser observado que o tempo de ciclo não seja maior do que a metade do tempo de segurança, pois a reação a erros nos módulos de entrada ocorre dentro de no máx. 2 ciclos. O tempo de ciclo é

influenciado pelo tempo de segurança que define o intervalo de tempo no qual todos os testes de primeiro plano são executados.

Um tempo de segurança curto aumenta o tempo de ciclo e vice versa. No caso de tempos de segurança longos, alguns testes são divididos em vários ciclos.

Exemplo 1: Tempo de segurança = 1 s

Tempo de ciclo do programa de aplicação = 450 ms

Duração dos testes = 100 ms

Dentro do tempo de segurança 2 ciclos são possíveis

100 ms / 2 = 50 ms / ciclo para a duração dos testes

Tempo de ciclo total = **500 ms**

Exemplo 2: Tempo de segurança = 2 s

Tempo de ciclo do programa de aplicação = 450 ms

Duração dos testes = 100 ms

Dentro do tempo de segurança 4 ciclos são possíveis

100 ms / 4 = 25 ms / ciclo para a duração dos testes

Tempo de ciclo total = **475 ms**

i Nas edições do sistema operacional antes de (07.14) o valor 255 s não é permitido para o tempo de segurança!
Apenas a faixa de valores 1 a 254 s é admissível!

3.4 Repetição da verificação

As repetições da verificação detectam erros perigosos escondidos que caso contrário poderiam afetar o funcionamento seguro da instalação.

Sistemas de segurança HIMA devem ser submetidos a uma repetição da verificação **em intervalos de 10 anos**[1)]. Muitas vezes, o intervalo pode ser estendido através de uma análise dos circuitos de segurança realizados mediante uma ferramenta de cálculo.

No caso de módulos de relés, a repetição da verificação para os relés deve ocorrer nos intervalos especificados para o sistema.

3.4.1 Execução da repetição da verificação

A execução da repetição da verificação depende dos seguintes pontos:

- Estado da instalação (EUC = equipment under control – equipamento sob controle)
- Potencial de perigo da instalação
- Normas a serem aplicadas à operação da instalação e a serem usadas pela instituição certificadora como base para a permissão de operação

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

1) Exceção: o módulo F 3430 deve ser verificado em intervalos de 5 anos para SIL 3

3.4.2 Frequência das repetições da verificação

O PES HIMA pode ser submetido a uma repetição da verificação através da verificação do circuito de segurança completo.

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 HIMA está automaticamente incluído neste teste. Portanto, é desnecessário realizar repetições da verificação adicionais para o sistema de comando HIMA.

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

Requisitos adicionais para a repetição da verificação de determinados módulos são descritos na folha de dados do respectivo módulo.

3.5 Requisitos de segurança

Para a utilização dos sistemas de comando direcionados à segurança dos sistemas H41q, H41qc e H51q, são válidos os seguintes requisitos de segurança.

---

i A **empresa operadora** é responsável pela operação segura de uma instalação de acordo com as normas de aplicação em vigor.

3.5.1 Projeto do hardware: requisitos independentes do produto

- Para assegurar a operação direcionada à segurança apenas podem ser utilizados módulos de hardware e componentes de software à prova de erros e certificados para tal. Os módulos de hardware e componentes de software certificados são listados na Lista de acompanhamento das liberações de versões de módulos e firmware da HIMA Paul Hildebrandt GmbH *(Revision List of Devices and Firmware of H41q/H51q Systems of HIMA Paul Hildebrandt GmbH)*. O número do certificado pode ser consultado no último documento de liberação válido. 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 2.3) relativas à CEM, às influências mecânicas, químicas e climáticas.
- Módulos de hardware e componentes de 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.

3.5.2 Projeto do hardware: requisitos relativos ao 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.

3.5.3 Programação: requisitos independentes do produto

- Em aplicações relevantes para a segurança, deve-se observar uma correta parametrização das grandezas de sistema relacionadas à segurança. As possibilidades de parametrização são descritas nos capítulos a seguir. Deve-se observar particularmente a definição da configuração do sistema, do máximo tempo de ciclo e do tempo de segurança.

3.5.4 Programação: requisitos relativos ao produto

- A reação de erro do sistema em caso de erros nos módulos de entrada e de saída à prova de erros deve ser determinada de acordo com as características relacionadas à segurança específicas da instalação através do programa de aplicação.
- Se usar a ferramenta de programação ELOP II, a partir da Rev. 3.5, é possível simplificar a verificação do programa elaborado de acordo com as determinações deste manual de segurança.
- Porém, a validação suficiente do programa precisa ser efetuada, mesmo assim.
- Verificações de função/Testes após alteração da aplicação podem ser limitados às partes alteradas do programa.
- O procedimento descrito no Capítulo 7 durante a elaboração e alteração do programa deve ser observado.

3.5.5 Comunicação: requisitos relativos ao produto

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

3.5.6 Modos de operação especiais: requisitos independentes do produto

- O Reload em aplicações de segurança apenas é admissível depois de consultar a instituição de verificação responsável pela certificação do sistema e com ajuda da ferramenta certificada ELOP II.
- Durante o Reload inteiro, a pessoa responsável deve garantir a supervisão suficiente de segurança do processo por outras medidas técnicas e organizacionais.
- Antes de cada Reload, as alterações de versão em relação ao programa de aplicação ainda em execução devem ser determinadas com ajuda do comparador de código C do ELOP II.
- Durante o Reload de um PES mono, a duração para a alteração completa acrescentando duas vezes o tempo de ciclo não pode ultrapassar o tempo de tolerância a falhas do processo.
- Para a utilização de “Maintenance Override”, deve ser observada a respectiva versão atual do documento *Intervenções de manutenção, Maintenance Override,* na homepage www.tuvasi.com da TÜV Rheinland.
- Mediante o ELOP II, um teste estático offline da lógica é possível. A simulação offline não foi submetida a uma verificação relacionada à técnica de segurança. Portanto, a simulação não pode substituir nenhuma verificação de função da instalação.
- Se necessário, a empresa operadora deve consultar a respectiva instituição de certificação responsável para a aplicação para definir medidas administrativas para a proteção do acesso aos sistemas.

4 Módulos centrais

Os componentes centrais necessários para as diferentes versões dos dispositivos de automação HIMA são unidos em kits. O respectivo kit de um equipamento central funcional consiste em:

- Suporte central de módulos
- Módulos centrais
- Fontes de alimentação
- Acessórios

O volume de fornecimento exato bem com a ligação da tensão de alimentação e a ligação do nível de E/S podem ser consultados nas folhas de dados no catálogo *Sistemas programáveis, famílias de sistemas H41q/H51q*, HI 800 262.

4.1 Módulos centrais e kits para os sistemas H41q e H41qc

Módulo/ Kit	Denominação	direcionado à segurança	sem retroalimentação
F 8652 X	Módulo central, processador duplo 1oo2	•	•
F 8653 X	Módulo central		•
B 4231	Kit equipamento central H41q-MS	•	•
B 4233-1	Kit equipamento central H41q-HS	•	•
B 4233-2	Kit equipamento central H41q-HRS	•	•
B 4235	Kit equipamento central H41cq-MS	•	•
B 4237-1	Kit equipamento central H41cq-HS	•	•
B 4237-2	Kit equipamento central H41cq-HRS	•	•

Tabela 10: Módulos centrais e kits para os sistemas H41q e H41qc

4.2 Módulos centrais e kits para o sistema H51q

Módulo/ Kit	Denominação	direcionado à segurança	sem retroalimentação
F 8650 X	Módulo central, processador duplo 1oo2	•	•
F 8651 X	Módulo central		•
B 5231	Kit equipamento central H51q-MS	•	•
B 5233-1	Kit equipamento central H51q-HS	•	•
B 5233-2	Kit equipamento central H51q-HRS	•	•
B 9302	Suporte de módulos de E/S	•	•

Tabela 11: Módulos centrais e kits para o sistema H51q

4.3 Outros módulos centrais para os sistemas H41q, H41qc e H51q

Módulo/ Kit	Denominação	direcionado à segurança	sem retroalimen-tação
Módulo de distribuição de corrente			
F 7132	Distribuidor de corrente 4x		•
F 7133	Distribuidor de corrente 4x com Supervisão de fusível		•
Módulos adicionais			
F 7126	Módulo de alimentação com corrente		•
F 7130A	Módulo de alimentação com corrente		•
F 7131	Supervisão da fonte de alimentação com baterias tampão para H51q		•
F 8621A	Módulo co-processador para H51q		•
F 8627 F 8627X	Módulo de comunicação para Ethernet		•
F 8628 F 8628X	Módulo de comunicação PROFIBUS-DP (Slave)		•
Conexões de barramento			
F 7553	Módulo de conexão de barramento de E/S para H51q		•
Módulos de ligação de barramento para constituir HIPRO			
H 7505	Conversor de interface RS 485, V.24/20 mA 2 fios/4 fios (HIPRO)		•
H7506	Borne de ligação de barramento para constituir barramentos de 2 fios		•

Tabela 12: Outros módulos centrais para os sistemas H41q, H41qc e H51q

4.4 Informações gerais sobre a segurança e disponibilidade de módulos centrais direcionados à segurança

Para a atribuição do sistema de módulos centrais e fontes de alimentação, bem como componentes do barramento das famílias de sistemas H41q/H51q valem as seguintes exigências:

Sistemas H41q, H41qc	Sistema H51q
No suporte de módulos de sistema do H41q podem ser usados: • dois módulos centrais • 12 módulos de E/S • dois módulos de alimentação com corrente • três módulos de fusíveis No suporte de módulos de sistema do H41qc podem ser usados: • dois módulos centrais • dois módulos de comunicação • 13 módulos de E/S • dois módulos de alimentação com corrente Proteção das entradas/saídas por disjuntores automáticos	No suporte de módulos centrais podem ser encaixados: • dois módulos centrais • para cada módulo central três módulos co-processadores F 8621/A ou cinco módulos de comunicação F 8625, F 8626, F 8627, F 8628 Os componentes básicos para suportes de módulos de E/S são agrupados em kits.

Tabela 13: Segurança e disponibilidade, diferenças H41q, H41qc e H51q

4.4.1 Fontes de alimentação

Em aplicações da técnica relacionada à segurança sempre deve ser utilizada uma fonte de alimentação 24 V = / 5 V = a mais do que seria necessário pelo consumo de corrente. Isso vale para o suporte de módulos centrais e para a alimentação adicional com corrente. As fontes de alimentação são desacopladas por diodos e são monitoradas pelos equipamentos centrais.

4.4.2 Descrição funcional dos módulos centrais direcionados à segurança F 8652 X / F 8650 X

Cada módulo central do tipo F 8652 X ou F 8650 X consiste nos seguintes blocos de função:

- Dois microprocessadores de ciclo sincronizado
- Cada microprocessador possui memória própria
- As memórias de um processador contêm o programa e os dados em formato não invertido, as memórias do outro processador, porém, contêm o programa e os dados em formato invertido
- Comparador de hardware testável para todos os acessos externos dos dois microprocessadores
- Em caso de erros, o Watchdog é colocado no estado seguro e comunicado o status do processador
- Flash EPROMs como memória de programa para sistema operacional e programa de aplicação, adequadas para no mín. 100.000 ciclos de memória
- Memória de dados em SRAM (memória RAM estática)
- Multiplexador para a ligação do barramento de E/S, Dual Port RAM (DPR) e módulo central redundante
- Bateria tampão das SRAMa no módulo central
- 2 interfaces RS485 com separação galvânica, taxa de transmissão: máx. 57600 bps; ajuste para 9600 bps e 57600 bps via interruptor ou ajuste (também de outras taxas de transmissão) por software, sendo que valores do software prevalecem

- Indicador diagnóstico e 2 LEDs para informações do sistema, da área de E/S e do programa de aplicação
- Dual-ported RAM para acesso rápido, mútuo à memória para o segundo módulo central
- Relógio de hardware com bateria tampão
- Lógica de barramento de E/S para conexão com os módulos de E/S
- Watchdog seguro
- Supervisão de fonte de alimentação, testável (tensão de sistema 5 V)
- Supervisão de bateria

4.5 Princípio geral de trabalho de módulos centrais direcionados à segurança

Módulos centrais direcionados à segurança consistem em dois microprocessadores com uma memória RAM cada que processam simultaneamente os mesmos programas, sistema operacional e programa de aplicação. Um comparador continuamente compara os dados nos barramentos entre os microprocessadores e as suas memórias.

O sistema operacional contém rotinas de autoteste que são percorridas sempre de novo. O Watchdog monitora a execução dos programas.

4.5.1 Rotinas de autoteste

Na Tabela 14, são explicadas as rotinas de autoteste dos módulos centrais direcionados à segurança F 8650 X e F 8652X e do acoplamento ao nível de E/S:

Teste	Descrição
Teste de CPU	São verificados: • Tipos de comandos e endereçamento • Capacidade de escrita em flags e comandos acionados por flags • Capacidade de escrita e comunicação cruzada dos registros • Unidade de lógica aritmética (ALU)
Teste das áreas de memória	O sistema operacional, programa de aplicação, constantes e parâmetros, bem como os dados variáveis, são armazenados em cada módulo central de forma direta e invertida e são verificados por um comparador de hardware para detectar anti-valência.
Áreas de memória fixas	Sistema operacional, programa de aplicação e área de parâmetros são armazenados em um Flash EPROM cada e são protegidos por um teste de CRC.
Teste de RAM	As áreas de RAM são verificadas com um teste de escrita / leitura, especialmente para detectar comunicação cruzada.
Teste de Watchdog	O sinal de Watchdog é desligado quando não for disparado num determinado intervalo pelas duas CPUs com padrões de bits antivalentes ou se o comparador de hardware detectar uma diferença entre as duas memórias (direta e invertida). Mediante um outro teste, a capacidade de desligamento do sinal de Watchdog é verificada.

Tabela 14: Rotinas de autoteste

Teste	Descrição
Teste da conexão ao nível de E/S dentro do módulo central	Nos módulos centrais redundantes nos sistemas H41q-HS / H41qc-HS / H51q-HS com barramento de E/S monocanal, o intertravamento recíproco do acesso de E/S aos módulos centrais está garantido. O circuito de intertravamento para este fim é verificado por autotestes. No caso de nível de E/S de dois canais – sistema HR ou HRS – a autorização de acesso de E/S é lida de volta e verificada. No caso de nível de E/S monocanal – sistema M ou MS (módulos de E/S e CPU monocanal) – a autorização de acesso de E/S é lida de volta e verificada.
Teste do módulo de conexão dentro dos suportes de módulos de E/S	O endereçamento é testado ciclicamente após cada processamento de um módulo de E/S direcionado à segurança. Os endereços de todas as posições de módulos de E/S convencionalizadas são lidos de volta e verificados. No módulo F 7553 são testados os interruptores de segurança.

Tabela 14: Rotinas de autoteste

4.5.2 Reação a falhas detectadas nos módulos centrais

As rotinas de teste detectam falhas e desligam o módulo central defeituoso. Simultaneamente, a falha é exibida pelo indicador de diagnóstico e registrado no diagnóstico de sistema.
No caso de um módulo central – sistema MS – isso significa um desligamento total do dispositivo de automação.
No caso de módulos centrais redundantes – sistemas HS e HRS – o módulo central defeituoso é desligado. O segundo módulo central continua a operação sem interrupção.

Se no caso de sistemas redundantes o módulo central defeituoso é substituído por um funcional com o mesmo programa de aplicação e sistema operacional, o novo módulo central recebe os dados atuais do módulo central em operação e o sistema entra novamente na operação redundante.

Sob determinadas condições (entre outras, a mesma versão do sistema operacional, no mínimo V7.0-8 (05.21)), também o programa de aplicação em si é carregado do módulo central ainda em operação para o novo módulo central “vazio” (*self education*). Para detalhes, veja o Capítulo *Self Education* no manual do sistema operacional HI 800 489 P.

4.5.3 Indicador de diagnóstico

O indicador de diagnóstico faz parte do módulo central. O mesmo consiste nas seguintes partes:

- Um indicador alfanumérico de 4 dígitos para textos e valores
- Um LED *CPU* como indicador de falhas nos módulos centrais
- Um LED *IO* como indicador de falhas geral em módulos de E/S direcionados à segurança.

Além disso, há uma tecla de confirmação (ACK) e duas teclas para chamar outras informações de sistema.

No caso de erros no módulo central, o LED *CPU* acende. O indicador de 4 dígitos exibe STOP. É possível visualizar o código de erro mediante um comando. Uma lista dos códigos de erro encontra-se no manual *Funções do sistema operacional* HI 800 489 P.

No caso de erros de módulos direcionados à segurança no nível de E/S acende o LED *IO*. O indicador de 4 dígitos exibe a posição do módulo e eventualmente o canal avariado.

O sistema de diagnóstico disponibiliza todos os códigos de erro para a visualização no sistema de gestão de processo. O sistema de diagnóstico mantém um histórico de erros. O mesmo pode ser exibido no PADT e auxilia na detecção de problemas na instalação.

4.6 Reação a falhas detectadas na área do barramento de E/S

No caso de erros na área do barramento de E/S entre módulo central e módulos de conexão, todos os suportes de módulos de E/S afetados por este erro são desligados.

Se um erro ocorrer na área do barramento de E/S apenas dentro do suporte de módulos de E/S, o módulo de conexão desliga os módulos de saída no suporte de módulos de E/S afetado.

4.7 Aviso para a substituição de módulos centrais

A substituição de módulos defeituosos, tanto na área central quando na área de E/S, pode ser efetuada durante a operação sem que o dispositivo de automação precise ser desligado.

---

i Uma interrupção da operação é possível!
A substituição de módulos centrais defeituosos é urgentemente recomendada.

No caso de erro ou manutenção, devem ser respeitados os seguintes passos de trabalho na substituição:

- Módulos centrais para dispositivos de automação não redundantes com bateria tampão integrada devem ser armazenados sem o programa de aplicação se esse programa contiver variáveis de retenção (Retain variable). As mesmas não são colocadas no valor inicial ao inicializar o sistema.
- Módulos centrais para dispositivos de automação redundantes com bateria tampão integrada podem ser armazenados com o programa de aplicação mesmo se esse programa contiver variáveis de retenção (Retain variable). As mesmas são adotadas pelo módulo central em operação durante a inicialização.

O indicador de diagnóstico do módulo central indica a bateria interna descarregada do módulo central mediante o texto *BATI*.
Uma recomendação para a troca de bateria nos módulos pode ser consultada nas folha de dados.

---

i No caso da falha da bateria e queda de tensão simultaneamente, as variáveis RETAIN perdem os seus valores armazenados. Nesse caso, o sistema inicializa os valores ao rearrancar.

---

5 Módulos de entrada

5.1 Visão geral completa dos módulos de entrada para os sistemas H41q, H41qc e H51q

Módulo		Direcionado à segurança	sem retro-alimentação	(Ex)i	bloco de SW correspondente
Módulos digitais de entrada					
F 3221	16 x módulo de entrada		•		
F 3222	8 x módulo de entrada		•		
F 3223	4 x módulo de entrada		•	•	
F 3224A	4 x módulo de entrada		•	•	
F 3236	16 x módulo de entrada	•	•		
F 3237	8 x módulo de entrada	•	•		HB-RTE-3
F 3238	8 x módulo de entrada	•	•	•	HB-RTE-3
F 3240	8 x módulo de entrada	•	•		
F 3248	16 x módulo de entrada	•	•		
F 5220	2 x módulo de contador	•	•		HF-CNT-3, -4
Módulos analógicos de entrada					
F 6213	4 x módulo analógico de entrada	•	•		HA-RTE-3
F 6215	8 x módulo analógico de entrada		•		
F 6217	8 x módulo analógico de entrada	•	•		
F 6220	8 x módulo termopar	•	•	•	HF-TMP-3
F 6221	8 x módulo analógico de entrada	•	•	•	HF-AIX-3

Tabela 15: Módulos de entrada para os sistemas H41q, H41qc e H51q

5.2 Segurança e disponibilidade de módulos de entrada direcionados à segurança

Devido à sua maior complexidade, alguns tipos de módulos analógicos e digitais de entrada dispõem do seu próprio sistema microprocessador 1oo2 que executa testes direcionados à segurança durante a operação automaticamente e disponibiliza dados seguros para a unidade de processamento segura.

Os módulos de entrada direcionados à segurança permitem a indicação de diagnóstico e, assim, a detecção e localização de erros.

---

i Em sistemas relacionados à segurança é possível utilizar tanto módulos de entrada direcionados à segurança quanto módulos de entrada sem retroalimentação em configuração mista.

Módulos de entrada direcionados à segurança nos sistemas H41q, H41qc e H51q são sujeitos automaticamente a um autoteste cíclico de alta qualidade durante a operação. Os módulos de entrada contêm elementos de circuito que permitem um teste de função do módulo de entrada através de rotinas de teste especiais integradas ao sistema operacional. Essas rotinas de teste são verificadas pela TÜV e garantem a função correta do respectivo módulo. Para cada erro detectado são geradas mensagens de erro. Erros detectados

automaticamente levam à ação direcionada à segurança do sistema. As mensagens de erro são uma informação de diagnóstico para a empresa operadora. Durante o planejamento e a realização da instalação, portanto, pode ser elaborado um sistema de diagnóstico de forma flexível.

Para aumentar a disponibilidade, também é possível utilizar os módulos de entrada direcionados à segurança de forma redundante.

A utilização de módulos de entrada redundantes não reduz a segurança do sistema.

Módulos de entrada direcionados à segurança podem ser utilizadas tanto para sinais direcionados à segurança como para sinais não direcionados à segurança.

Para os slots permitidos para módulos de entrada nos suportes de módulos e nos suporte de módulos de E/S para os sistemas H41q, H41qc e H51q devem ser observadas as seguintes convenções:

Sistema H41q, H41qc	Sistema H51q
Os módulos de entrada são inseridos no suporte de módulos de sistema. Estão à disposição kits com 12 slots (H41q) ou 13 slots (H41qc) para módulos de E/S.	Os módulos de entrada são inseridos nos suportes de módulos de E/S (EABTs) cada um com 16 slots para módulos de E/S. Os componentes básicos necessários para suportes de módulos de E/S são agrupados em kits.

Tabela 16: Slots permitidos

5.2.1 Segurança de sensores, transdutores e transmissores

Apenas se pode falar em sinais direcionados à segurança se os sensores, transdutores ou transmissores externos disporem de uma comprovação de segurança. Se não disporem de comprovação de segurança, a segurança de sensores, transdutores ou transmissores externos também pode ser alcançada mediante uma ligação especial, veja manual *Funções do sistema operacional* HI 800 489 P.

Neste caso, vários sensores devem ser ligados num circuito 1oo2, 2oo3 ou NooM. (Observação: 1oo2 em inglês significa “1 out of 2”, ou seja, “1 entre 2”.)

A segurança e disponibilidade do sistema de sensores podem ser aumentadas pelo tipo de ligação dos sensores. Opções de realização para diferentes circuitos de sensores sob aspectos de segurança e disponibilidade são apresentadas detalhadamente no Capítulo 7.8. O programa de aplicação deve ser configurado de acordo.

Com base na IEC 61508 são viabilizadas as respectivas comprovações de segurança mediante a definição de intervalos de teste offline Proof. As determinações em detalhe para isso devem ser definidas de forma específica para a aplicação.

5.3 Módulos digitais de entrada direcionados à segurança F 3236, F 3237, F 3238, F 3240 e F 3248

5.3.1 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. A cada erro no módulo de entrada, é processado o nível Low (estado seguro) no programa de aplicação.

Adicionalmente, os módulos para iniciadores e contatores com supervisão de linha testam a linha até o transdutor. Um iniciador direcionado à segurança pode ser ligado a estes módulos. Pelos autotestes, todas as exigências para a detecção de limiares dos inciadores direcionados à segurança são satisfeitas.

A supervisão da corrente do transdutor de contato exige a ligação com duas resistências conforme folha de dados.

5.3.2 Reação a falhas detectadas nos módulos digitais de entrada direcionados à segurança

Tipo de erro	Reação do sistema	Observação
Defeito no módulo (módulo de entrada)	FALSE é passado ao programa de aplicação para todos os canais	Assim, garante-se a função segura do sistema pelo princípio de circuito fechado.
Quebra de fio no circuito de sensor	FALSE é lido no canal afetado	No caso de módulos com supervisão de linha é sinalizado falha de linha. Com entradas direcionadas à segurança, este sinal deve ser avaliado pelo bloco de software HB-RTE-3 (veja anexo), para que uma reação de sistema segura seja possível.
Curto de linha no circuito de sensor	TRUE é lido no canal afetado	No caso de módulos com supervisão de linha é sinalizado falha de linha. Com entradas direcionadas à segurança, este sinal deve ser avaliado pelo bloco de software HB-RTE-3 (veja anexo), para que uma reação de sistema segura seja possível.
Informações gerais	O indicador de diagnóstico mostra a posição dos módulos defeituosos. No caso do módulo F 3238 que ocupa dois slots no suporte de módulos é indicada a posição do slot da direita. Ao utilizar módulos de entrada com supervisão de quebra de fio e curto do circuito do sensor, o indicador de diagnóstico exibe além da posição do módulo também o canal falhado do módulo.	

Tabela 17: Reação a falhas em módulos digitais de entrada direcionados à segurança

5.4 Módulo contador direcionado à segurança F 5220

O módulo contador de dois canais possui o seu próprio sistema de processador duplo com uma saída direcionada à segurança por canal. Pode ser utilizado para a contagem de pulsos, medição de frequência ou rotação mediante um tempo ajustável de abertura, bem como para a supervisão do sentido de rotação.

i No caso de alteração do tempo de abertura, o valor de medição correto está à disposição na saída apenas após três tempos de abertura percorridos!

5.4.1 Rotinas de teste

O módulo possui o seu próprio sistema microprocessador 1oo2 que executa testes online direcionados à segurança automaticamente e fornece os dados seguros para o processamento seguro dos sinais no bloco de software HF-CNT-3 ou HF-CNT-4.

5.4.2 Reações a falhas detectadas no módulo contador direcionado à segurança F 5220

Tipo de erro	Reação do sistema em caso de erro	Observação
Erro do módulo	Desligamento das saídas direcionadas à segurança.	No caso de erro, reação apenas na direção segura.
Falha de canal	Desligamento da saída direcionada à segurança atribuída.	No caso de erro, reação apenas na direção segura.
Quebra de fio ou curto de linha no circuito do iniciador ou outros erros.	Desligamento da saída direcionada à segurança atribuída.	Após a eliminação do erro, é necessário um sinal de Reset na entrada do bloco HF-CNT-3 / 4.

Tabela 18: Reações de erro módulo contador direcionado à segurança F 5220

5.5 Módulos analógicos de entrada direcionados à segurança F 6213, F 6214 e F 6217

No caso de redundância de módulos de entrada analógicos direcionados à segurança, em módulos funcionais é processado o valor médio *(apenas dentro das tolerâncias admissíveis)*. O valor médio é gerado no F 6213 e F 6214 pelo bloco correspondente, no F 6217, pelo programa de aplicação. No caso de erro, apenas é processado o valor do módulo funcional.

5.5.1 Rotinas de teste

Os módulos aplicam valores de teste pelo conversor de teste DA e verificam os mesmo pelo conversor AD com o qual também se digitaliza o sinal de entrada.

5.5.2 Reações a falhas detectadas nos módulos analógicos de entrada direcionados à segurança F 6213, F 6214

Tipo de erro	Reação do sistema em caso de erro	Observação
Erro de módulo ou de canal em entradas analógicas de um canal	Processamento do valor configurado no bloco de software HA-RTE-3 (v. Anexo).	No caso de erro, a reação é possível apenas na direção segura.
Erro de módulo ou erro de canal em módulos de entrada analógicos redundantes e transmissores redundantes	No caso de erro de um módulo de entrada, o valor do módulo redundante ou o valor de erro configurado é processado.	Opcionalmente formação do valor mín, máx ou médio mediante o bloco de software HA-RTE-3 (v. Anexo).
Curto no circuito do transmitter	Indicação da posição do módulo e do canal com erro no indicador de diagnóstico	Somente se usar 4...20 mA

Tabela 19: Reação de erro em módulos analógicos de entrada direcionados à segurança F 6213, F 6214

5.5.3 Reações a falhas detectadas nos módulos analógicos de entrada direcionados à segurança F 6217

Tipo de erro	Reação do sistema em caso de erro	Observação
Falha de canal	Valor analógico = 0000 Bit de erro de canal = TRUE	O bit de erro do canal deve ser processado no programa de aplicação de forma direcionada à segurança
Erro do módulo	Todos os valores analógicos = 0000 Todos os bits de erro de canal = TRUE	veja erro de canal, diz respeito a todos os bits de erro de canal
Área de mediação ultrapassada (22 mA)	Valor analógico máx. = 4095 Bit de erro de canal = TRUE	O valor máx. admissível deve ser definido no programa de aplicação.

Tabela 20: Reação de erro em módulos analógicos de entrada direcionados à segurança F 6217

O módulo possui o seu próprio sistema microprocessador 1oo2 que executa testes online direcionados à segurança automaticamente e fornece os dados seguros para a unidade de processamento seguro. Para cada canal existe o valor analógico e um bit de erro de canal correspondente.

⚠ ALERTA

Alerta! Existe a possibilidade de danos pessoais devido a um valor de medição incorreto!

Para cada entrada analógica direcionada à segurança deve ser programada uma reação direcionada à segurança no caso do bit de erro de canal atribuído.

5.6 Módulo de entrada analógico de termopar direcionado à segurança com segurança intrínseca F 6220

O módulo de termopares possui oito canais para a conexão de termopares de diversos tipos (conforme parametrização nos blocos HF-TMP-3) e uma entrada para a conexão de uma termorresistência Pt 100 como entrada de temperatura de comparação. Possui o seu próprio sistema de duplo processador e é parametrizado pelo bloco de software HF-TMP-3 (veja Capítulo 2.12 no Anexo e a ajuda online do ELOP II) para cada canal atribuído.

As entradas também podem ser utilizadas para a medição de tensão baixa, veja folha de dados.

5.6.1 Rotinas de teste

O módulo possui o seu próprio sistema microprocessador 1oo2 que executa testes online direcionados à segurança automaticamente e fornece os dados seguros para o processamento seguro dos sinais no bloco de software HF-TMP-3. Cada um dos 8+1 canais fornece valores de entrada seguros e um status de erro seguro.

5.6.2 Reações a falhas detectadas no módulo de termopares direcionado à segurança F 6220

Estado	Reação do sistema	Observação
Erro do módulo	Saída *erro de canal* no bloco HF-TMP-3 comuta para TRUE.	A reação deve ser realizada no programa de aplicação usando o sinal de saída *erro de canal*.
Falha de canal	Saída *erro de canal* no bloco HF-TMP-3 comuta para TRUE.	A reação deve ser realizada no programa de aplicação.
Transbordamento negativo	Saída *transbordamento negativo* no bloco HF-TMP-3 comuta para TRUE.	A reação deve ser realizada no programa de aplicação.
Transbordamento	Saída *transbordamento* no bloco HF-TMP-3 comuta para TRUE.	A reação deve ser realizada no programa de aplicação.

Tabela 21: Reação de erro módulo de termopares direcionado à segurança F 6220

Os valores limite para transbordamento negativo ou transbordamento são definidos nas entradas *Limiar transbordamento negativo* ou *Limiar transbordamento* do bloco HF-TMP-3. Se o valor de medição ultrapassar ou não alcançar estes valores de limiar parametrizados, o respectivo sinal se torna TRUE, sem que haja um erro no módulo.

5.6.3 Avisos para o projeto

- Entradas não utilizadas devem ser colocadas em curto.
- No nível SIL 3, a temperatura de referência deve ser consultada do programa de aplicação ou determinada como comparação das temperaturas de referência de dois módulos.
- Devem ser observados todos as possíveis desvios e considerados na avaliação dos valores de medição.
- No SIL 3, a temperatura dos termopares deve ser determinada sempre como comparação entre dois termopares.

5.7 Módulo de entrada analógico direcionado à segurança com segurança intrínseca F 6221

O módulo de entrada analógico possui oito canais para a conexão direta de transmitters analógicos da área (Ex). A tensão de alimentação dos transmitters pode ocorrer pelo módulo de saída F 3325 (ou um outro sensor, de acordo com as especificações da folha de dados). Essa tensão de alimentação do transmitter deve ser ligada para a supervisão mediante módulo F 6221.
Cada canal atribuído é parametrizado pelo seu próprio bloco de software HF-AIX-3.

5.7.1 Rotinas de teste

O módulo possui o seu próprio sistema microprocessador 1oo2 que executa testes online direcionados à segurança automaticamente e fornece os dados seguros para o processamento seguro dos sinais no bloco de software HF-AIX-3. Cada um dos oito canais fornece valores de entrada seguros e um status de erro seguro.

5.7.2 Reações a falhas detectadas no módulo analógico de entrada direcionado à segurança F 6221

Estado	Reação do sistema	Observação
Erro do módulo	Saída *valor* (INT) no bloco HF-AIX-3 carrega o valor numérico 0. Saída *erro de canal* no bloco HF-AIX-3 comuta para TRUE.	No programa de aplicação deve ser convencionalizado um valor de erro utilizando o sinal de entrada de bloco *Valor em caso de erro*.
Falha de canal	Saída *erro de canal* no bloco HF-AIX-3 comuta para TRUE.	
Transbordamento negativo	Saída *transbordamento negativo* no bloco HF-AIX-3 comuta para TRUE.	
Transbordamento	Saída *transbordamento* no bloco HF-AIX-3 comuta para TRUE.	

Tabela 22: Reação de erro em módulos analógicos de entrada direcionados à segurança F 6221

Os valores limite para transbordamento negativo ou transbordamento são definidos nas entradas *Limiar transbordamento negativo* ou *Limiar transbordamento* do bloco HF-AIX-3. Se o valor de medição ultrapassar ou não alcançar estes valores de limiar parametrizados, o respectivo sinal se torna TRUE, sem que haja um erro no módulo.

5.7.3 Outros avisos para o projeto

- Entradas de tensão não utilizadas 0...1 V devem ser colocadas em curto na régua de bornes.
- Entradas de corrente não utlizadas são fechadas pelo shunt no conector do cabo.
- Apenas os usos listados na folha de dados F 6221 são permitidos.
- Os regulamentos de proteção Ex e os requisitos de ligação Ex devem ser respeitados.

5.8 Aviso para a troca de módulos de entrada

No caso de erro ou manutenção, devem ser respeitados os seguintes passos de trabalho na substituição:

1. Desparafusar o conector de cabo ou retirar o módulo de entrada com o conector de cabo colocado.
2. Encaixar o novo módulo de entrada sem conector de cabo e aparafusar.
3. Conectar o conector de cabo e aparafusar.
4. Acionar a tecla de confirmar (tecla ACK no módulo central).

---

i Uma interrupção da operação é possível!
A substituição de módulos de entrada defeituosos é urgentemente recomendada.

5.9 Listas de verificação para projetar, programar e colocar em funcionamento módulos de entrada direcionados à segurança

Para cada um dos módulos 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. As listas de verificação servem ao mesmo tempo para demonstrar posteriormente que o projeto foi elaborado cuidadosamente.

As listas de verificação deste manual de segurança podem ser obtidas como arquivos MS Word (*.doc) no DVD HIMA ou na internet, em www.hima.de.

SDIGE-F3236	para módulos digitais direcionados à segurança
SDIGE-F3237	para módulos digitais direcionados à segurança
SDIGE-F3238	para módulos digitais direcionados à segurança
SDIGE-F3240	para módulos digitais direcionados à segurança
SDIGE-F3248	para módulos digitais direcionados à segurança
SDIGE-F5220	para módulos contadores direcionados à segurança
SANAE-F6213 / F6214	para módulos analógicos direcionados à segurança
SANAE-F6217	para módulos analógicos direcionados à segurança
SANAE-F6220	para módulos analógicos direcionados à segurança
SANAE-F6221	para módulos analógicos direcionados à segurança

6 Módulos de saída

6.1 Visão geral completa dos módulos de saída para os sistemas H41q, H41qc e H51q

Módulo	Denominação	Direcionado à segurança	sem retro-alimentação	Capacidade de carga	bloco de SW correspondente
Módulos digitais de saída					
F 3322	16 x módulo digital de saída		•	≤ 0,5 A	
F 3325	6 x dispositivo de alimentação (Ex)		•	22 V ≤ 0,02 A	
F 3330	8 x módulo digital de saída	•	•	≤ 0,5 A	
F 3331	8 x módulo digital de saída	•	•	≤ 0,5 A	HB-BLD-3[1)], HB-BLD-4[1)]
F 3333	4 x módulo digital de saída	•	•	≤ 2 A	
F 3334	4 x módulo digital de saída	•	•	≤ 2 A	HB-BLD-3[1)], HB-BLD-4[1)]
F 3335	4 x módulo digital de saída	•	•	22 V ≤ 0,053 A	
F 3348	8 x módulo digital de saída	•	•	≤ 0,5 A	
F 3349	8 x módulo digital de saída	•	•	≤ 0,5 A ≤ 48 V	HB-BLD-3[1)], HB-BLD-4[1)]
F 3422	8 x módulo de relé		•	≤ 2 A, ≤ 60 V	
F 3430[2)]	4 x módulo de relé	•	•	≤ 4 A, ≤ 250 V	
Módulos analógicos de saída					
F 6705	2 x conversor D/A	•	•	0...20 mA	HZ-FAN-3[3)]
F 6706	2 x conversor D/A		•	0...20 mA	

1) Para indicação de falhas e parametrização dos modos de operação (circuito aberto/fechado)

2) O módulo F 3430 não é certificado conforme EN/ISO 13849-1.

3) Necessário na operação de consumo de corrente para avaliação de erros

Tabela 23: Módulos de saída para os sistemas H41q, H41qc e H51q

6.2 Informações gerais sobre a segurança e disponibilidade de módulos de saída direcionados à segurança

Os módulos de saída direcionados à segurança são inscritos uma vez em cada ciclo; os sinais de saída são relidos e comparados com os dados de saída definidos no programa de aplicação.

Adicionalmente, dentro do tempo de ocorrência de falhas múltiplas (MOT) é executado um teste “walking bit” através de todas as saídas, neste caso o sinal de teste fica ativo por no

máx. 200 µs. Assim, a capacidade de comutação das saídas é verificada sem influenciar a função dos atuadores conectados. O congelamento de cada saída é detectado, mesmo se o sinal de saída for estático.

Os módulos de saída direcionados à segurança com supervisão de linha podem detectar erros na linha de alimentação ao consumidor. A supervisão de linha satisfaz os requisitos de segurança até SIL 1. Isso apenas tem importância se a supervisão de linha for utilizada em circuitos elétricos direcionados à segurança. O sinal de saída pode ser utilizado em todas as aplicações para requisitos de segurança até SIL 3.

Sistema H41q, H41qc	Sistema H51q
Os módulos de saída são inseridos no suporte de módulos de sistema. Estão à disposição kits com 12 slots (H41q) ou 13 slots (H41qc) para módulos de E/S.	Os módulos de saída são inseridos em suportes de módulos de E/S (EABTs) especiais previstos para este fim, com no máximo 16 slots para módulos de E/S. Os componentes básicos necessários para suportes de módulos de E/S são agrupados em kits (veja Capítulo 4, na página 23).

Tabela 24: Slots para módulos de saída em sistemas H41q, H41qc e H51q

6.2.1 Módulos de saída digitais direcionados à segurança

As rotinas de teste detectam um erro mediante comparação dos sinais de saída lidos de volta com os dados de saída internos. O sistema operacional coloca um módulo numa posição detectada como defeituosa no estado seguro e comunica esse fato no indicador de diagnóstico.

No caso de módulos com supervisão do circuito de saída, uma quebra de fio detectada é assinalada mediante indicação do canal com erro do módulo no indicador de diagnóstico. O módulo de saída defeituoso é desligado de forma segura pelo desligamento de segurança integrado.

Adicionalmente, com ajuda do bloco de software H8-STA-3 um ou mais grupos de desligamento podem ser definidos. O defeito de um módulo de saída nesse caso leva à desativação de todos os módulos de saída que pertencem a um grupo de desligamento.

Dependendo dos requisitos de segurança da instalação, também é possível configurar o desligamento total do sistema de comando mediante os parâmetros de E/S, nos ajustes para os recursos.

6.2.2 Módulos de saída analógicos direcionados à segurança

Os módulos de saída analógicos direcionados à segurança podem ser utilizados em operação como *fontes de corrente* ou *consumidores de corrente*.

Na operação como *fonte de corrente*, o desligamento de segurança integrado leva ao estado seguro no caso de erro (corrente de saída 0 mA).

Na operação como *consumidor de corrente*, o estado seguro apenas pode ser alcançado mediante medidas adicionais. O programa de aplicação deve desligar a tensão de alimentação para o circuito de corrente de forma segura. Para fins de avaliação de erro deve ser usado o bloco de software HZ-FAN-3 aqui.

6.3 Princípio geral de trabalho de módulos de saída direcionados à segurança

Nos módulos de saída direcionados à segurança estão três interruptores de semicondutor ligados em série. Assim, o segundo caminho de desligamento independente necessário direcionado à segurança está integrado no módulo 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).

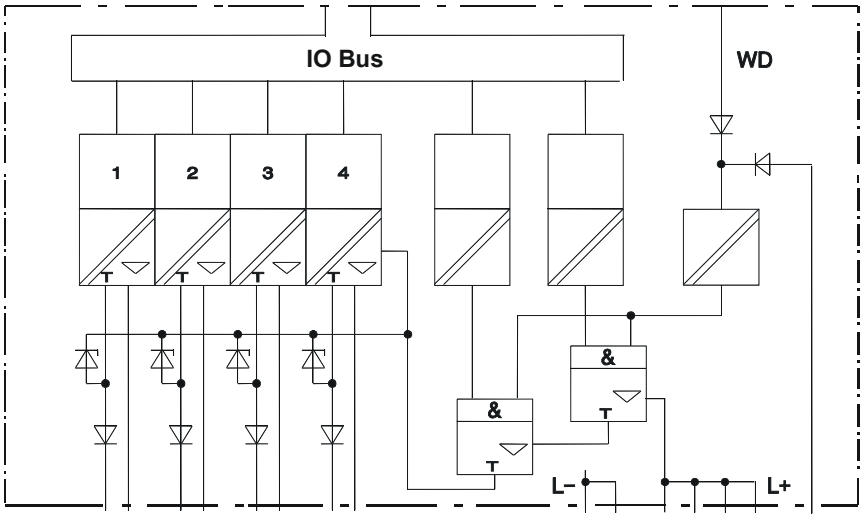


Figura 1: Princípio de ligação dos módulos de saída com desligamento de segurança integrado (aqui com 4 canais de saída)

6.4 Módulos de saída digitais direcionados à segurança F 3330, F 3331, F 3333, F 3334, F 3335, F 3348, F 3349

6.4.1 Rotinas de teste

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

1. Releitura do sinal de saída do amplificador de comutação. O limiar de comutação para um nível Low lido de volta é ≤ 6,5 V.
2. Leitura do diagnóstico de linha dos canais ligados (só com F 3331, F 3334 e F 3349).
3. Ligação de padrões de teste e teste de comunicação cruzada (teste walking bit) dentro do tempo de ocorrência de falhas múltiplas.
4. Leitura do diagnóstico de linha de todos os canais (só com F 3331, F 3334 e F 3349).
5. Verificação do desligamento de segurança integrado.

6.4.2 Reação a falhas detectadas nos módulos digitais de saída direcionados à segurança

- No caso de todos os erros detectados no módulo, o mesmo é colocado no estado seguro, desenergizado, ou seja, o módulo é desligado.
- No caso de curtos que não podem ser diferenciados de erros internos, o módulo também é desligado.
- Erros de linha apenas são sinalizados e não levam ao desligamento.

6.5 Módulo de relé digital direcionado à segurança F 3430

6.5.1 Rotinas de teste

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

1. Releitura do sinal de saída do amplificador de comutação para os interruptores diversitários de relé triplos.
2. Ligação de padrões de teste e teste de comunicação cruzada (teste walking bit) dentro do tempo de ocorrência de falhas múltiplas.
3. Verificação do desligamento de segurança integrado.

6.5.2 Reação a falhas detectadas nos módulos digitais de relé direcionados à segurança

- No caso de todos os erros detectados no módulo, o mesmo é colocado no estado seguro, desenergizado, ou seja, o módulo é desligado.
- No caso de curto-circuito externo, o fusível para o canal relevante é acionado. Não ocorre mensagem de erro.

6.5.3 Aviso para a elaboração do projeto com F 3430

Relés são componentes eletromecânicos e pelo seu princípio construtivo têm uma vida útil limitada. A vida útil de relés depende da potência de ligação dos contatos (corrente/tensão) e da quantidade de ciclos de manobras.

Com condições nominais de operação, a vida útil é de 300 000 ciclos de manobras, com 30 VDC e 4 A.

Para cumprir as exigências conforme IEC 61508 (PFD/PFH, veja Capítulo 3.2.1) vale um intervalo de teste offline Proof dentro de 5 anos para SIL 3 e de 20 anos para aplicações SIL 2.

As verificações necessárias são efetuadas nas instalações do fabricante HIMA.

6.6 Módulo de saída analógico direcionado à segurança F 6705

6.6.1 Rotinas de teste

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

1. Releitura do sinal de saída.
2. Teste da linearidade do conversor DA.
3. Teste de comunicação cruzada entre as saídas.
4. Verificação do desligamento de segurança integrado.

6.6.2 Reações a falhas detectadas no módulo analógico de entrada direcionado à segurança

Ao operar como fonte de corrente, no caso de todos os erros detectados no módulo, o mesmo é colocado no estado seguro, desenergizado, ou seja, o módulo é desligado mediante a função de desligamento de segurança integrada.

Uma quebra de fio externa não pode ser distinguida de erros internos e leva ao desligamento do módulo.

Na operação como consumidor de corrente, o estado desenergizado só pode ser alcançado mediante desligamento externo. O programa de aplicação deve desligar a fonte de tensão para o circuito de corrente de forma segura. Por isso, deve ser utilizado o bloco de software HZ-FAN-3.

6.7 Aviso para a troca de módulos de saída

No caso de erro ou manutenção, devem ser respeitados os seguintes passos de trabalho na substituição:

Substituição de um módulo de saída:

1. Desparafusar o conector de cabo ou retirar o módulo de saída com o conector de cabo colocado.
2. Encaixar o novo módulo de saída sem conector de cabo e aparafusar.
3. Conectar o conector de cabo e aparafusar.
4. Acionar a tecla de confirmar (tecla ACK no módulo central).

O módulo de saída está trocado.

---

i Uma interrupção da operação é possível!
A substituição de módulos de saída defeituosos é urgentemente recomendada.

6.8 Listas de verificação para projetar, programar e colocar em funcionamento módulos de saída direcionados à segurança

Para cada um dos módulos 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 é possível garantir que os requisitos foram registrados inteiramente e de forma clara. As listas de verificação servem ao mesmo tempo para demonstrar posteriormente que o projeto foi elaborado cuidadosamente.

As listas de verificação deste manual de segurança podem ser obtidas como arquivos MS Word (*.doc) no DVD HIMA ou na internet, em www.hima.de.

SDIGA-F3330	para módulos digitais direcionados à segurança
SDIGA-F3331	para módulos digitais direcionados à segurança
SDIGA-F3333	para módulos digitais direcionados à segurança
SDIGA-F3334	para módulos digitais direcionados à segurança
SDIGA-F3335	para módulos digitais direcionados à segurança
SDIGA-F3348	para módulos digitais direcionados à segurança
SDIGA-F3349	para módulos digitais direcionados à segurança
SDIGA-F3430	para módulos digitais direcionados à segurança
SANAA-F6705	para módulos analógicos direcionados à segurança

7 Software

O software para dispositivos de automação direcionados à segurança das famílias de sistema H41q, H41qc e H51q divide-se em três blocos:

- *Sistema operacional*
- *Programa de aplicação*
- *Ferramenta de programação* conforme IEC 61131-3 (ELOP II com ferramenta de segurança integrada).

O *sistema operacional* deve ser utilizado na respectiva forma válida, certificada pela TÜV para aplicações direcionadas à segurança. A respectiva versão válida pode ser consultada no documento conjunto *Lista de versões dos módulos e do firmware do sistema H41q/H51q*. Esse documento é elaborado pelo serviço conjunto de alterações da TÜV Rheinland Industrie Service GmbH e da empresa HIMA.

O *programa de aplicação* é criado com o a ferramenta de programação ELOP II e contém as funções específicas da instalação que o dispositivo de automação deve executar. Para a parametrização de funções do sistema operacional também se usa o ELOP II. Um gerador de código traduz o programa de aplicação para o código de máquina. O ELOP II transfere este código de máquina através de uma interface serial ou Ethernet para as Flash EPROMs no módulo central do dispositivo de automação.

As principais funções do sistema operacional e as especificações para o programa de aplicação baseadas nele são descritas no manual do sistema operacional HI 800 489 P, na tabela *Funções do sistema operacional*.

7.1 Aspectos relacionados à segurança para o sistema operacional

Este capítulo descreve a assinatura e o princípio básico de trabalho do sistema operacional.

7.1.1 Identificação, versão atual liberada para aplicações relacionadas à segurança (assinatura CRC)

Cada novo sistema operacional possui a sua denominação incluindo o estado de edição. Para a identificação mais exata serve a assinatura do sistema operacional que pode ser chamada no indicador de diagnóstico durante a operação do dispositivo de automação.

As versões válidas do sistema operacional e as respectivas assinaturas (CRCs), aprovadas pela TÜV para equipamentos de automação direcionados à segurança podem ser consultadas na Lista de versões dos módulos e do firmware do sistema H41q/H51q *(Revision List of Devices and Firmware of H41q/H51q Systems)*.

7.1.2 Princípio de trabalho e funções do sistema operacional

O sistema operacional processa o programa de aplicação de forma cíclica. De forma muito simplificada, a sequência e esta:

- Leitura dos dados de entrada (entradas de hardware)
- Processar as funções de lógica conforme IEC 61131-3, Seção 4.1.3
- Escrita dos dados de saída (saídas de hardware)

Além disso, há as seguintes funções básicas:

- Autotestes abrangentes
- Testes dos módulos de E/S durante a operação
- Transferência e comparação de dados.

Um ciclo é processado em sete fases. Estas fases são descritas de forma detalhada no manual do sistema operacional HI 800 489 P.

7.2 Aspectos relacionados à segurança do programa de aplicação

Sequência geral da programação dos equipamentos de automação das famílias H41q/H51q para aplicações relacionadas à segurança:

1. Especificação da função do sistema de comando
2. Escrita do programa de aplicação
3. Verificação do programa de aplicação por simulação offline
4. Compilação do programa de aplicação com o gerador de código C
5. O compilador comprovado na prática (GNU-CC) traduz o código C duas vezes e gera o código de destino e o código de comparação.
6. O comparador do código de destino compara o código de destino com o código de comparação. Erros que são causados pelo PC não seguro são detectados e comunicados pelo comparador de código de destino.
7. O programa executável gerado sem erros desta forma é carregado ao sistema H41q ou H51q. Lá, o programa pode ser testado.
8. Depois de encerrar os testes com êxito, o PES inicia a operação segura.

Conceitos

Carregar	Este termo significa que um programa é carregado ao sistema de comando ou mediante Download ou mediante Reload.
Download	Durante o Download de um programa para o sistema de comando, todas as saídas do sistema de comando são resetadas e o sistema de comando é parado.
Reload	Durante o Reload de um programa de aplicação para um sistema de comando redundante, o programa de aplicação alterado é carregado aos módulos centrais de forma sequencial. Neste momento, sempre um módulo central está em operação MONO. Não há desligamento. Com um PES com apenas um módulo central. as saídas são mantidas pela duração da transmissão. O Reload apenas é possível se um código com capacidade de Reload foi gerado.

7.2.1 Especificações e regras para a utilização em aplicações relacionadas à segurança (Requisitos baseados em relatórios de aprovação de tipo, etc.)

O programa de aplicação é introduzido através da ferramenta de programação ELOP II para PC com o sistema operacional Windows®. Adicionalmente, o PC deve estar equipado com um módulo Hardlock da HIMA.

A ferramenta de programação ELOP II contém basicamente:

- Introdução de código (editor de blocos funcionais), supervisão e documentação
- Variáveis com nomes simbólicos e tipo de dado (BOOL, UINT etc.)
- Atribuição do recurso (sistemas de automação HIMA H41q/H51q)
- Gerador de código (compilação do programa de aplicação em código de máquina) com os softwares C-Code Generator e GNU C Compiler.

7.2.1.1 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. O tipo de representação da especificação depende das tarefas a serem realizadas. Estas incluem:

- Lógica combinatória:
  - Esquema de causa/efeito
  - 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 de comutação e atuadores a serem controlados
  - Diagramas sequenciais conforme DIN EN 60848
  - 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 automação 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)
  - Supervisão de discrepância e reação.

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

Os objetivos na programação do programa de aplicação devem ser:

- Fácil compreensão
- Rastreabilidade
- Facilidade de alteração

7.2.2 Aspectos relacionados à segurança para a programação com ELOP II

Para a elaboração dos programas de aplicação usa-se a ferramenta de programação *ELOP II*.
As condições de utilização, p. ex., versão do Windows suportada, podem ser consultadas na documentação da respectiva versão do ELOP II.

O conceito de segurança do ELOP II garante o seguinte:

- A ferramenta de programação trabalha corretamente, ou seja, erros da ferramenta de programação são detectados.
- O usuário utiliza a ferramenta de programação corretamente, ou seja, erros do usuário são detectados.

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. Depois de uma alteração do programa de aplicação, até então, para garantir a segurança era necessário executar novamente um teste de função completo.

A ferramenta de segurança no ELOP II conf. IEC 61131-3 é configurada de forma que após uma alteração do programa de aplicação apenas as alterações precisam ser verificadas. Esta ferramenta de segurança serve para detectar erros do usuário e erros da ferramenta de programação.

A ferramenta de segurança do ELOP II consiste em três componentes importantes para a segurança:

- Comparador de código C
- Comparador de código de destino
- GNU C Compiler comprovado na prática

O comparador de código C identifica alterações no programa de aplicação. O comparador

de código de destino compara dois códigos de destino gerados pelo GNU C Compiler (GNU-CC), um depois do outro. Isso evita erros causados pelo PC não seguro.

Meios auxiliares não direcionados à segurança são:

- A gestão de revisões integrada ao ELOP II. A mesma pode ser utilizada para a identificação inequívoca das versões de projeto relevantes.
- A simulação offline representada no diagrama de fluxo Figura 2: A simulação offline verifica o programa de aplicação em relação à especificação, sem efeitos para o processo.

7.2.2.1 Aplicação da ferramenta de segurança do ELOP II na elaboração de programas

Na Figura 2: encontram-se pontos mencionados no texto abaixo.

1. Elaboração do programa de aplicação de acordo com uma especificação autoritativa (p.ex., conforme IEC 61508, DIN V VDE 0801 ou normas aplicadas correspondentes), no diagrama de fluxo Figura 2: são os pontos (1) a (4).
2. O gerador de código C compila o programa de aplicação para o código C e gera adicionalmente um arquivo de comparação, item (5) no fluxograma.

⚠ PERIGO

Perigo! Existe a possibilidade de danos pessoais devido à falha de função!

Deve ser gerada uma lista de referência cruzada para o programa de aplicação e verificada a utilização correta das variáveis! Deve ser verificado que todas as variáveis apenas são utilizadas onde estão previstas pela especificação.

3. O compilador C comprovado na prática traduz o código C e o arquivo de comparação, itens (6) e (13). É gerado o código de destino e o código de comparação.

⚠ PERIGO

Perigo! Existe a possibilidade de danos pessoais devido à falha de função!

O comparador de código de destino deve estar ativado, ponto (14). Ele compara o código de destino com o código de comparação. O comparador do código de destino detecta e comunica erros causados pelo PC não seguro.

4. O programa executável gerado desta forma é carregado ao sistema H41q ou H51q (item (7)). Lá, o programa deve ser testado por inteiro e liberado (item (8)).
5. Gerar um backup do código de destino.
6. O PES inicia a operação segura.

7.2.2.2 Aplicação da ferramenta de segurança do ELOP II na alteração de programas

1. Modificação do programa de aplicação de acordo com uma especificação autoritativa (p. ex., conforme IEC 61508 ou normas aplicadas correspondentes), no diagrama de fluxo são os pontos (1) a (4).
   Base para a alteração é o backup do programa de aplicação em execução. Este backup contém:
   - Arquivo VGL
   - Código de destino
   - Dados introduzidos
2. O gerador de código C compila o programa de aplicação alterado para o código C (novo), item (5).
3. O comparador de código C deve estar ativado, ponto (12). Ele compara o código C (novo) com o código C (antigo) da versão anterior do programa, item (11). Como arquivo de comparação (código C (antigo)) deve ser escolhido o backup.
4. O resultado da comparação, item (15), é documentado.

5. Verificar se o comparador de código C indica as alterações efetuadas no programa de aplicação. Apenas alterações relevantes para o código são indicadas.
6. Resultado do comparador de código C:
   a) Se comunicar alterações que o usuário não está reconhecendo, isso pode ser as seguintes causas:
      - A alteração efetuada pelo usuário tem como consequência alterações mais abrangentes que não foram previstas
      - Há um erro interno
   b) Se não comunicar alterações efetuadas pelo usuário, o motivo pode ser:
      - Alterações que o comparador de código C não detecta, p. ex., alterações gráficas ou alterações de valores iniciais
      - Alterações que não foram transferidas corretamente
7. O compilador C traduz o código C (novo) e o arquivo de comparação (novo), itens (6) e (13). Ele gera e compara o código de destino com o código de comparação.
8. O comparador de código de destino deve estar ativado, ponto (14). Ele compara o código de destino com o código de comparação. Erros causados pelo PC não seguro são detectados e comunicados.
9. O programa executável gerado desta forma é carregado ao sistema H41q ou H51q. Lá devem ser testadas todas as partes do programa que sofreram uma alteração. O teste da alteração verifica se o código de destino está correto.
10. Se não houver nenhuma falha de função, deve ser criado um backup do novo programa atual. O PES pode iniciar a operação segura.

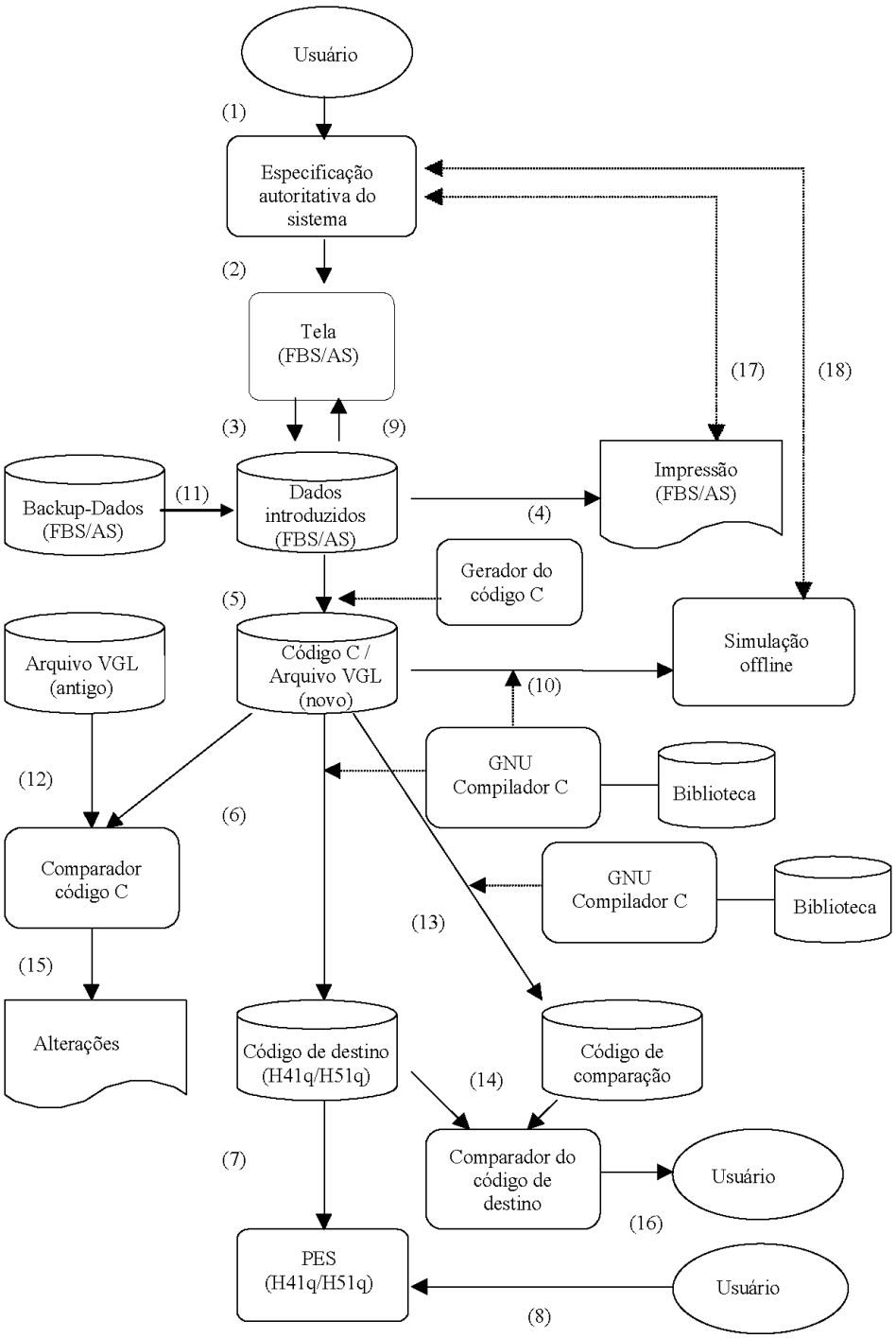


Figura 2: Fluxograma, função da ferramenta de segurança

7.2.3 Utilização de variáveis e nomes PCS

Com ajuda do editor de declaração de variáveis, os nomes de variáveis e os seus tipos de dados são definidos. Todas as variáveis do programa de aplicação são associadas a nomes simbólicos. Esses nomes simbólicos podem consistir no máximo em 256 caracteres.

Para entradas e saídas físicas são usados nomes simbólicos de PCS que também podem conter no máximo 256 caracteres.

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

- No programa de aplicação podem ser utilizadas a denominações de entradas e saídas usadas na instalação.
- Alterações na atribuição dos sinais nos canais de entrada e saída não interferem com o programa de aplicação.

7.2.3.1 Atribuição de nomes PCS aos nomes de variáveis

Como base para a atribuição de nomes PCS aos nomes de variáveis deveria servir a lista de pontos de medição ou uma lista dos sensores e atuadores.

A atribuição de um nome de variável ao hardware utilizado ocorre no diálogo para os recursos em *Process cabinet* – Editar armário. Neste caso, a posição desejada do módulo (1-1 a 1-8 ou 2-1 a 2-8) o tipo do suporte, slot e tipo do módulo exigido bem como os nomes PCS a serem atribuídos aos nomes de variáveis.

DICA Por motivos de praticidade, nomes de variáveis e nomes PCS deveriam ser iguais.

A quantidade de canais (nomes) por módulo depende do tipo de módulo usado. As rotinas de teste necessárias para módulos de E/S direcionados à segurança são executadas pelo sistema operacional automaticamente.

A HIMA recomenda juntar os módulos de entrada e saída nos suportes de módulos de E/S em grupos funcionais.

Pontos de vista para o agrupamento podem ser:

- Agrupamento de acordo com partes da instalação
  Posicionamento semelhante dos módulos nos grupos, p.ex.:
  - Partes digitais/analógicas da instalação
  - Módulos de E/S direcionados à segurança/não direcionados à segurança
- Agrupamentos redundantes nos diferentes suportes de módulos de E/S na mesma sequência
- Módulos de reserva ou canais de reserva para um posterior Reload (código com capacidade de Reload)

7.2.3.2 Tipos de variáveis

De acordo com a unidade de organização do programa (POU) – programa, bloco funcional ou função – podem ser definidos diferentes tipos de variáveis. A seguinte tabela mostra uma visão geral:

Tipo de variável	Programa de aplicação PROG	Bloco funcional FB	Função FUN	Utilização
VAR	X (CONST[1], RETAIN[2])	X (CONST, RETAIN)	X (CONST)	Variável local
VAR_INPUT	-	X	X	Variável de entrada
VAR_OUTPUT	-	X (RETAIN)	X	Variável de saída
VAR_EXTERNAL	-	X (CONST)	-	Externo, de/para outras POU
VAR_GLOBAL	X (CONST, RETAIN)	-	-	Global, de outra POU
VAR_ACTION	X	X	X	No bloco de ação do diagrama sequencial

1) CONST: constante que pode ser alterada no teste online – sem nova compilação do programa de aplicação. Não pode ser escrita pelo programa de aplicação.

2) RETAIN: variável com retenção, ou seja, o valor não se perde após uma queda de tensão / retorno de tensão.

Tabela 25: Tipos de variáveis no ELOP II

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

7.2.3.3 Entradas e saídas digitais para variáveis booleanas

Na definição do recurso diferencia-se entre entradas e saídas digitais e entradas e saídas digitais direcionadas à segurança. Para funções direcionadas à segurança, apenas podem ser utilizados módulos de E/S direcionados à segurança. Para a maioria dos módulos de E/S direcionados à segurança devem ser previstos módulos padrão da HIMA no programa de aplicação, veja no anexo.

Os módulos de E/S não direcionados à segurança são apenas lidos ou escritos no sistema operacional e não são submetidos a outras rotinas de teste. Portanto, um defeito não é detectado pelo sistema operacional e não ocorre nenhuma mensagem de erro. Por isso, a HIMA recomenda utilizar apenas módulos de E/S direcionados à segurança, devido ao diagnóstico mais amplo.

7.2.3.4 Módulos de E/S analógicos

Módulos de entrada analógicos convertem valores analógicos (tensões, correntes) em valores digitais com resolução de 12 bit.

Módulos de saída analógicos convertem valores digitais de 12 bit em correntes de 0...20 mA ou 4...20 mA.

Para a maioria dos módulos de E/S analógicos direcionados à segurança e módulos de E/S não direcionados à segurança devem ser utilizados módulos padrão da HIMA no programa de aplicação, veja no anexo.

7.2.3.5 Variáveis importadas ou exportadas

Os dados das variáveis a serem importadas ou exportadas são transferidas pelas interfaces ou para a comunicação HIMA ou via HIPRO (master PES) a sistemas de outros fabricantes.

Protocolos disponíveis para sistemas de outros fabricantes são Modbus, Modbus TCP, PROFIBUS-DP e 3964R. Os dados também podem ser transferidos via um protocolo Ethernet a um servidor OPC. As variáveis para importação e exportação são processadas no programa de aplicação como variáveis de entrada e saída normais. São definidas na declaração de variáveis da instância do programa.

É possível colocar o atributo de evento em variáveis booleanas. Eventos são mudança de sinal de variáveis booleanas com informações adicionais sobre o momento (data e hora). O carimbo de hora de um evento corresponde à hora do dispositivo de automação com precisão de milissegundos.

7.2.4 Assinaturas do programa de aplicação

Alterações não intencionais ou não autorizadas no programa de aplicação podem ser detectadas através de várias assinaturas de CRC. Essas assinaturas são chamadas de número de versão. No ELOP II, há os seguintes números de versão:

- Número de versão do código
- Número de versão do Run
- Número de versão de dados
- Número de versão de área

7.2.4.1 Número de versão do código

O número de versão do código é formado através das funções da lógica programada. Apenas se a versão o código do programa no sistema de comando e na ferramenta de programação coincidirem é possível monitorar a função do sistema de comando pelo PC.

Os seguintes fatores não influenciam o número de versão do código:

- Escrever ou excluir comentários
- Configurar ou excluir campos de teste online (campos OLT), ou seja, de informações de forcing
- Deslocar linhas ou blocos se a ordem de processamento não for alterada
- Alterações dos parâmetros SIO em si, porém sem ativar/desativar parâmetros SIO
- Parâmetros de barramento

Alterações dos endereços básicos para acoplamento Modbus e de outros sistemas podem levar a uma alteração do número de versão do código. No caso de todas as demais alterações, também o número de versão do código será alterado.

7.2.4.2 Número de versão do Run

O sistema de comando forma o número de versão do Run durante a operação. Através da comparação com um número de versão do Run até então válido e documentado pode ser detectado se o programa dentro do sistema de comando foi influenciado nesse meio-tempo (visível mediante chamada do indicador de diagnóstico).

O número de versão do Run é alterado com:

- Outro número de versão do código (não com todos os tipos de alterações)
- Inserção ou exclusão de módulos
- Outros parâmetros de sistema
- Inserção ou exclusão de VAR_CONST
- Alteração de valores VAR_CONST
- Alteração do tipo de recurso
- Alteração online de ajustes
- Forcing de variáveis de E/S no campo de teste online
- Alteração da posição do interruptor principal de forcing

7.2.4.3 Número de versão de dados

O número de versão de dados se refere à definição de variáveis não direcionadas à segurança importadas ou exportadas e se modifica nos seguintes casos:

- Quando é alterado o nome de uma variável com os atributos para HIPRO-N (não direcionada à segurança).
- Quando tais variáveis são comprimidas ao gerar código sem capacidade de Reload (quando houver lacunas na memória).

7.2.4.4 Número de versão de área

O número de versão de área compreende todas as variáveis definidas dentro do projeto e é alterado nos seguintes casos:

- Ao excluir ou adicionar módulos no armário.
- Se a criação de código com capacidade para Reload estiver ajustada e mais variáveis são atribuídas do que excluídas aos atributos do seguinte tipo: HIPRO-N, HIPRO-S, BUSCOM, Evento, 3964R.
- Se a criação de código sem capacidade para Reload estiver ajustada e variáveis são atribuídas ou excluídas dos atributos do seguinte tipo: HIPRO-N, HIPRO-S, BUSCOM, Evento, 3964R.
- Quando a reorganização da memória for necessária, pois o limite de memória foi alcançado.

Alterações dos endereços básicos para acoplamento Modbus e de outros sistemas podem levar a uma alteração do número de versão de área.

7.2.5 Utilização de blocos funcionais padrão para aplicações relacionadas à segurança

Na lista abaixo são elencados os blocos funcionais padrão HIMA para aplicações relacionadas à segurança. As descrições de função dos blocos estão disponíveis na homepage *www.hima.com* e no DVD HIMA.

7.2.5.1 Blocos funcionais padrão, independentes no nível de E/S

Tipo	Função	Verificação TÜV[1)]	
		direcionado à segurança	sem retro-alimentação
H8-UHR-3	Data e hora		•
HK-AGM-3	Supervisão master PES		•
HK-COM-3	Supervisão módulo de comunicação		•
HK-LGP-3	Avaliação e configuração LGP		•
HK-MMT-3	Modbus Master		•
HA-LIN-3	Linearização de temperatura	•	•
HA-PID-3	Regulador PID	•	•
HA-PMU-3	Conversor de medição parametrizável	•	•

Tabela 26: Blocos funcionais padrão, independentes no nível de E/S

1) O "•" na coluna *Verificação TÜV* significa que para o respectivo bloco existe uma certificação de segurança pela TÜV. Para a aplicação relacionada à segurança dos blocos recomendamos consultar a documentação dos blocos.

7.2.5.2 Blocos funcionais padrão, independentes no nível de E/S

Tipo	Função	Verificação TÜV[1)]	
		direcionado à segurança	sem retro-alimentação
H8-STA-3	Formar grupos direcionados à segurança de saídas testáveis	•	•
HA-RTE-3	Supervisão de módulos analógicos de entrada testáveis F 6213 / F 6214	•	•
HB-BLD-3	Diagnóstico de módulo e condutor de saídas testáveis	•	•
HB-BLD-4	Diagnóstico de módulo e condutor de saídas testáveis	•	•
HB-RTE-3	Supervisão de módulos de entrada binários testáveis	•	•
HF-AIX-3	Supervisão de módulos analógicos de entrada testáveis F 6221	•	•
HF-CNT-3	Bloco contador para módulo F 5220	•	•
HF-CNT-4	Bloco contador para módulo F 5220	•	•
HF-TMP-3	Bloco de configuração para F 6220	•	•
HZ-FAN-3	Indicador de falhas para módulos de E/S testáveis		•
HZ-DOS-3	Diagnóstico sem segurança		•

1) O «•» na coluna *Verificação TÜV* significa que para o respectivo bloco existe uma certificação de segurança pela TÜV. Para a aplicação relacionada à segurança dos blocos recomendamos consultar a documentação dos blocos.

Tabela 27: Blocos funcionais padrão, independentes no nível de E/S

Os seguintes blocos podem ser utilizados em aplicações relacionadas à segurança, porém, não para ações direcionadas à segurança:

- H8-UHR-3
- HK-AGM-3
- HK-LGP-3
- HK-MMT-3
- HZ-FAN-3
- HZ-DOS-3

Outros avisos podem ser consultados na homepage *www.hima.com* e no DVD HIMA.

7.2.6 Parametrização do dispositivo de automação

Os parâmetros listados a seguir determinam o comportamento do dispositivo de automação durante a operação e são ajustados no menu propriedades do recurso.

7.2.6.1 Parâmetros de segurança

Nas propriedades do recurso podem ser ajustados os parâmetros de segurança:

- Os parâmetros para a operação direcionada à segurança do dispositivo de automação
- As ações permitidas com o aparelho de programação durante a operação direcionada à segurança

Parâmetros direcionados à segurança		Ajuste recomendado
Parâmetros podem ser alterados online		Resetar, depende do projeto
Parâmetros de segurança		
	Tempo de segurança em s	Depende do processo
	Tempo de Watchdog em ms	No máximo a metade do tempo de segurança
	Classe de requisição	6, corresponde a SIL 3, depende do projeto
Valores podem ser alterados		
	Constantes	Resetar
	Variáveis	Resetar
	Forcing de E/S	Resetar
Ações permitidas		
	Operação teste	Resetar
	Iniciar	Resetar
	Reload	Depende do projeto

Tabela 28: Parâmetros direcionados à segurança

i Nas edições do sistema operacional antes de (07.14) o valor 255 s não é permitido para o tempo de segurança!
Apenas a faixa de valores 1 a 254 s é admissível!

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

7.2.6.2 Comportamento em caso de erros em canais de saída direcionados à segurança

A seguinte tabela mostra as opções de ajustes do parâmetro *Behavior in Case of Output Faults* – comportamento em caso de erros de saída. O mesmo encontra-se na aba **IO Parameters** da janela de diálogo **Properties** do recurso.

Ajuste	Descrição
Display only – Apenas exibição	Desligamento do amplificador de saída mediante desligamento de segurança integrado. Se não for possível, desligamento do sinal de Watchdog no suporte de módulos de E/S através do módulo de conexão (apenas sistemas H51q). O sinal de Watchdog do módulo central correspondente não é desligado (não há parada por erro). O programa de aplicação e a comunicação continuam. **Apenas admissível até SIL 1!**
Emergency Stop – Parada de emergência	Desligamento do sinal de Watchdog do módulo central correspondente e, assim, desligamento dos canais de saída (parada por erro). O programa de aplicação e a comunicação não continuam a rodar.
Normal operation – Operação normal	Reação como no parâmetro *Display only*, adicionalmente desligamento do grupo correspondente se um grupo está configurado com ajuda do bloco H8-STA-3, Capítulo 2.1 no Anexo. Desligamento do sinal de Watchdog do módulo central correspondente (parada por erro) se não há nenhum grupo configurado ou se o relé do grupo estiver defeituoso. Neste caso, o programa de aplicação e a comunicação não continuam a rodar. **Necessário a partir de SIL 2.** **Ajuste recomendado e usual.**

Tabela 29: Ajuste do parâmetro *Behavior in Case of Output Faults*

A comunicação com o PADT ao surgir um erro independe do ajuste em *Behavior in Case of Output Faults* – comportamento em caso de erros de saída.

7.2.7 Identificação do programa

O programa de aplicação pode ser identificado com ajuda do número de versão do código de forma inequívoca. Assim, o backup correspondente (versão arquivada) sempre pode ser identificado de forma inequívoca.

Se houver incerteza qual Backup é o correto, compilar o Backup em questão com a opção Download e a seguir comparar o código de destino com a versão dp código do programa carregado.

No caso de código com capacidade de Reload, isso apenas é possível se o Backup foi gerado da seguinte forma:

1. Efetuar a última alteração
2. Gerar (compilar) o código com capacidade de Reload, resulta versão de código A
3. Carregar o sistema de comando com a versão de código A
4. Gerar código com capacidade de Reload, resulta versão de código B, pode ser idêntica a A
5. Carregar o sistema de comando com a versão de código B
6. A cada nova geração de código sem alteração resulta a versão de código B.

7.2.8 Verificação do programa de aplicação criado para detectar se respeita a função de segurança específica

Para a verificação deve ser gerado um conjunto adequado de casos de teste que esteja cobrindo a especificação. Nesse caso não é necessário executar 2^{20} casos de teste numa matriz de 20 x E. Via de regra, é suficiente o teste independente de cada entrada e dos vínculos importantes do ponto de vista da aplicação. Esse conjunto de testes é suficiente porque o ELOP II e as medidas definidas neste manual de segurança tornam suficientemente improvável que seja gerado código semantica e sintaticamente correto que ainda contenha erros sistemáticos não detectados resultantes do processo de geração do código.

Também para a avaliação numérica de fórmulas deve ser gerado um conjunto de teste adequado. São úteis, p.ex., testes de classe de equivalência, ou seja, testes dentro das faixas de valores definidas, nos limites e em faixas de valores não admissíveis. Os casos de teste devem ser selecionados de modo que se possa provar que o cálculo está correto. A quantidade necessária de casos de teste depende da fórmula utilizada e deve abranger pares de valores críticos.

O teste online pode ser usado como auxílio aqui, p.ex., para determinar valores e ler valores intermediários. Porém, uma simulação ativa com fontes é necessária, pois apenas desta forma pode ser comprovada a fiação correta de sensores e atuadores. Além disso, só assim a configuração de sistema pode ser verificada.

7.3 Lista de verificação: Medidas para a elaboração de um programa de aplicação

A lista de verificação está disponível como arquivo Word MEAP-0001-D.doc no DVD HIMA e na internet, em www.hima.com.

7.4 Reload (código com capacidade de Reload)

i O Reload apenas é admissível depois de consultar a instituição de verificação responsável pela certificação do sistema. Durante o Reload inteiro, a pessoa responsável deve garantir a supervisão suficiente de segurança do processo por outras medidas técnicas e organizacionais.

⚠ ALERTA

Alerta! Existe a possibilidade de danos pessoais devido à falha de função!

- **Antes de cada Reload, as alterações no programa de aplicação em relação ao programa de aplicação ainda em execução devem ser determinadas com ajuda do comparador de código C na ferramenta de segurança do ELOP II.**
- **As alterações do Reload devem ser testadas criteriosamente em simuladores antes da transmissão ao PES.**

Se o Reload do programa de aplicação no(s) módulo(s) central(ais) for possível, aparece a mensagem *Reloadable Code* durante o ciclo de compilação do gerador de código.

No caso das seguintes alterações no programa de aplicação, perde-se a capacidade de Reload:

- No armário são excluídos módulos ou adicionados módulos novos.
- Aos atributos do seguinte tipo são adicionadas mais variáveis do que excluídas: HIPRO-N, HIPRO-S, BUSCOM, Evento, 3964R
- Os endereços básicos para BUSCOM são alterados, veja Capítulo 7.2.4.4.

- Atribuições a variáveis de sistema são adicionadas ou alteradas.
  Isso não vale para todas as variáveis de sistema (detalhes, veja *Funções do sistema operacional* HI 800 489 P).
- Nomes de variáveis HIPRO-S são alterados.

7.4.1 Sistemas com um módulo central

Durante o tempo de carregar o programa de aplicação não acontece nenhum acesso ao nível de E/S, ou seja, módulos de E/S não são lidos, escritos ou testados.

Ao carregar o programa de aplicação, o mesmo não processa as interfaces do sistema de comando e não ocorre a passagem de variáveis de importação ou exportação pelas interfaces.

Uma interrupção da operação é possível!
Quando efetuar um Reload em sistemas com um módulo central, então o mesmo deve estar concluído dentro do tempo de tolerância a falhas do processo.

7.4.2 Sistemas com módulos centrais redundantes

No caso destes sistemas, o Reload é possível sem as restrições acima listadas para sistemas com um canal.

Sequência de Reload:

1. Ao carregar o primeiro módulo central, o segundo módulo central continua o processamento do programa de aplicação em operação mono.
2. Depois, o módulo central recém carregado recebe os dados atuais do módulo central ainda em execução e assume a operação mono com o novo programa de aplicação.
3. Depois de carregar o segundo módulo central, o mesmo recebe os dados atuais do primeiro e ambos os módulos centrais passam para a operação redundante..

7.4.3 Restrições durante o Reload

Os seguintes pontos devem ser observados durante o Reload:

- Se durante um Reload um elemento da lógica for excluído, p.ex., uma função com controle de uma saída física, então, a imagem do processo não é alterada. Por isso, todas as saídas afetadas pelo Reload devem ser excluídas, ou seja, as saídas afetadas pelo Reload devem estar desativadas antes do Reload.
- Se durante um Reload. a variável de entrada (VAR_INPUT) de um bloco funcional não for mais escrita (p. ex., por que a variável ou a atribuição foi excluída antes do bloco funcional), então, a variável de entrada retém o seu último valor e não é resetada automaticamente a FALSE / 0!
  Esse comportamento diz respeito a todos os blocos funcionais, mas não às funções. A causa para esse comportamento está no fato de que durante o Reload os valores de todas as variáveis permanecem armazenados, para permitir a continuidade do trabalho. As entradas de blocos funcionais padrão ou específicos do usuário são processadas como variáveis internamente.
  Solução: Uma entrada deste tipo deve ser associado a uma nova que está ajustada para o valor desejado.
- Todas as variáveis com o atributo *const* reassumem de novo o seu valor inicial após o Reload, mesmo que tenham sido ajustadas para um outro valor online.
- Todos os parâmetros de sistema reassumem o seu valor configurado durante o Reload, mesmo que tenham sido ajustadas para um outro valor online. Isso tem efeitos para o tempo de Watchdog, tempo de segurança, taxa de Baud das interfaces e muito mais.
- Se num programa de aplicação com uma sequência de passos o passo ativo é excluído e posteriormente um Reload é executado, perde-se a condição de avançar

na comutação ao próximo passo. Isso significa que a sequência de passos não pode mais ser executada.

- Se ao compilar um programa for gerado o CRC 0, o programa não pode ser carregado ao sistema de comando!
  Solução: O programa precisa ser alterado e novamente compilado para gerar um CRC que não seja 0. As alterações não podem alterar a função do programa. Por isso, apenas se deve trocar objetos sem interdependência graficamente, p. ex., as entradas de um bloco E.

7.5 Teste offline

Alterações no programa de aplicação podem ser simuladas com o teste offline no ELOP II. Essa simulação é uma boa ferramenta auxiliar para avaliar os efeitos de uma alteração. Ela não é suficiente para validar as alterações efetuadas nos sistemas de comando direcionados à segurança. Para este fim é necessário um teste no sistema de comando real ou num simulador.

7.6 Forcing

Forcing apenas é admissível depois de consultar a instituição de verificação responsável pela certificação da instalação. Durante o Forcing, a pessoa responsável deve garantir a supervisão suficiente de segurança do processo por outras medidas técnicas e organizacionais.

i Durante o Forcing em sistemas de comando direcionados à segurança, deve ser observada a respectiva versão atual do documento *Intervenções de manutenção, Maintenance Override* da TÜV Rheinland Industrie Service. O documento pode ser descarregado pela internet, na homepage www.tuvasi.com.

Opções durante o Forcing:

- O Forcing pode ser proibido pela configuração. Desta forma, o PES não aceita mais valores de Forcing definidos pelo usuário. Neste caso, novos valores de Forcing apenas podem ser ajustados depois do desligamento do sistema.
- Ao fechar o Control Panel é mostrado se e quantos valores de Forcing ainda estão atribuídos.
- Todas as entradas ou saídas forçadas podem ser resetadas novamente mediante dois interruptores principais de forcing separados.

Mais detalhes sobre o procedimento do Forcing podem ser consultados no manual do sistema operacional HI 800 489 P e na ajuda online do ELOP II.

⚠ PERIGO

Perigo! Existe a possibilidade de danos pessoais devido à falha de função!

Antes de começar a operação direcionada à segurança devem ser removidos todos os marcadores de Forcing do programa de aplicação.

Detalhes sobre marcadores de Forcing são descritos na ajuda Online do ELOP II.

7.7 Proteção contra manipulações

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

1. No PES podem ser ajustados os parâmetros de sistema de forma que uma alteração do programa não seja possível sem recarregar.
2. A ferramenta de programação ELOP II possui um Hardlock e adicionalmente pode ser protegida pelos mecanismos de senha do Windows® contra acessos não autorizados.

---

i Devem-se observar os requisitos das normas de segurança e de aplicação relativas à proteção contra manipulação. A autorização de funcionários e as medidas de segurança necessárias estão sob a responsabilidade da empresa operadora.
A empresa operadora deve definir em trabalho conjunto com a instituição de verificação quais medidas devem ser utilizadas para a proteção contra manipulação.

7.8 Funções do programa de aplicação

A programação não está sujeita a limitações de hardware. As funções do programa de aplicação podem ser programadas livremente. Durante a programação, deve-se considerar o princípio de circuito fechado para as entradas e saídas. Uma quebra de fio, p.ex., leva ao desligamento do respectivo atuador.

- Quebras de fio não precisam ser consideradas dentro do programa de aplicação no caso de sistemas de comando lógico-programável, ao contrário de sistemas de comando de segurança com fiação fixa.
- Negações de diversas formas são admissíveis.
- Sinais ativos para desencadear uma ação (p.ex., pulso de ciclo de deslize para um registro deslizante) podem ser utilizados para aplicações relacionadas à segurança.

No caso de módulos analógicos de entrada direcionados à segurança, no caso de erro é passado um valor definido ao processamento. Informações mais detalhadas a esse respeito podem ser consultadas na descrição dos blocos de software no manual *Tipo de recurso ELOP II*.

Num módulo de E/S digital direcionado à segurança, no caso de erro, a entrada é ajustada ao valor seguro 0, e o módulo digital de saída é desligado mediante o desligamento de segurança integrado. Informações mais detalhadas a esse respeito podem ser consultadas na descrição dos blocos de software em anexo.

Em relação a sistemas de comando com fiação fixa, nos sistemas de comando lógico-programáveis existe uma gama ampliada de funções, especialmente o processamento de byte e palavra.

7.8.1 Desligamento de grupo

Os módulos de saída direcionados à segurança utilizados para uma determinada área da instalação (p.ex., para um queimador) podem ser unidos num grupo. Para esse fim, o bloco de software H8-STA-3 deve ser inserido no programa de aplicação para cada grupo. No bloco de software devem ser ajustadas todas as posições dos módulos de saída que pertencem a um grupo. No caso de um erro em um módulo de saída, todos os módulos de saída que pertencem ao grupo são desligados. Para a segurança do sistema, porém, já é suficiente o desligamento de segurança integrado dos módulos de saída.

7.8.2 Blocos de software para módulos de E/S individuais direcionados à segurança

Módulo de entrada		Módulo de saída	
digital		digital	
Tipo	Bloco de software	Tipo	Bloco de software
F 3237	HB-RTE-3	F 3331	HB-BLD-3 / -4
F 3238	HB-RTE-3	F 3334	HB-BLD-3 / -4
F 5220	HF-CNT-3 / -4	F 3349	HB-BLD-3 / -4
analógico		analógico	
F 6213	HA-RTE-3	F 6705	HZ-FAN-3
F 6214	HA-RTE-3		
F 6220	HF-TMP-3		
F 6221	HF-AIX-3		

Tabela 30: Atribuição de blocos de software a módulos de E/S

Para os módulos de E/S direcionados à segurança, devem ser inseridos no programa de aplicação os blocos de software correspondentes. Informações mais detalhadas a esse respeito, veja no Anexo e na descrição dos blocos de software na ajuda online do ELOP II.

7.8.3 Módulos de E/S redundantes

Para aumentar a disponibilidade sem restrições para a segurança, é possível ligar módulos de entrada ou saída direcionados à segurança em paralelo, como mostrado no esquema abaixo. A disponibilidade máxima é alcançada se neste caso também os dispositivos de automação com dois barramentos de E/S são utilizados e os sinais de E/S redundantes também são conduzidos para módulos de E/S separados.

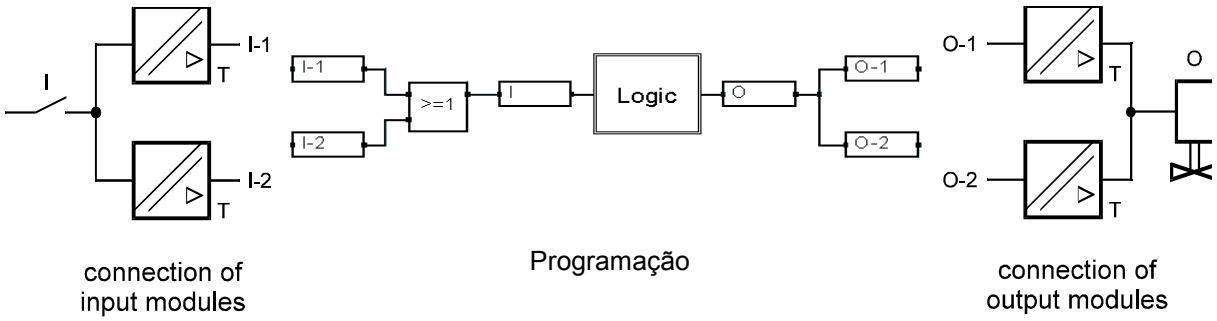


Figura 3: Módulos de E/S redundantes para aumentar a disponibilidade

7.8.3.1 Sensores redundantes, não direcionados à segurança

Hardware

Dependendo do sinal de comando (contato mecânico, iniciador, com / sem segurança intrínseca), devem ser utilizados módulos de entrada do tipo F 3236, F 3237 ou F 3238. Os dois sensores são operados em circuitos 1oo2, ou seja, se um sensor for acionado, o circuito direcionado à segurança é imediatamente desligado. Uma discrepância é comunicada depois de esgotar o tempo especificado. Essa funcionalidade pode ser reunida numa bloco funcional para o módulo de entrada F 3236. Para os módulos F 3237 e F 3238, existe o bloco HB-RTE-3 com supervisão ampliada dos circuitos de iniciadores.

Programa de aplicação, módulo de entrada F 3236

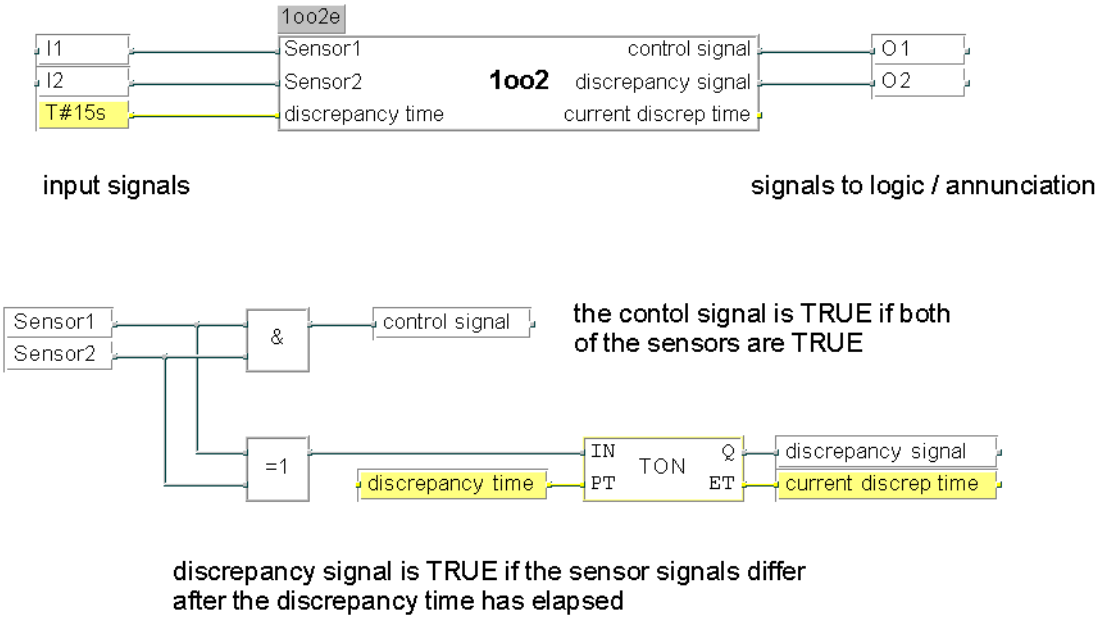


Figura 4: Exemplo de um bloco funcional 1oo2 e lógica do bloco

Programa de aplicação, módulo de entrada F 3237 ou F 3238

Utilização do bloco HB-RTE-3

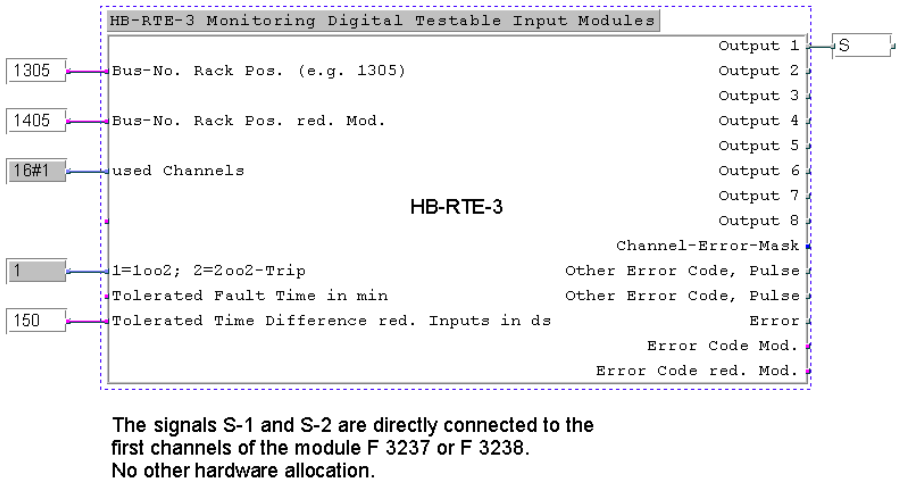


Figura 5: Utilização do bloco HB-RTE-3

Consideração de segurança

Se um dos dois sensores for acionado ou se um componente dentro do sistema falhar, ocorre o desligamento.

Para as aplicações dos sensores, devem ser observadas as normas relevantes, p. ex., IEC 61511.

Consideração de disponibilidade

Não há disponibilidade, pois cada falha de um componente leva ao desligamento.

7.8.4 Sensores analógicos redundantes

Ligação, hardware

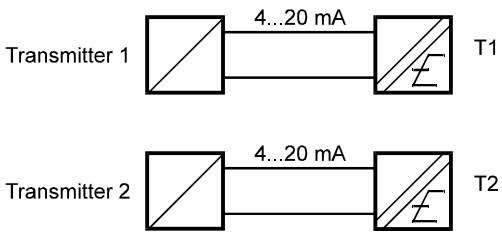
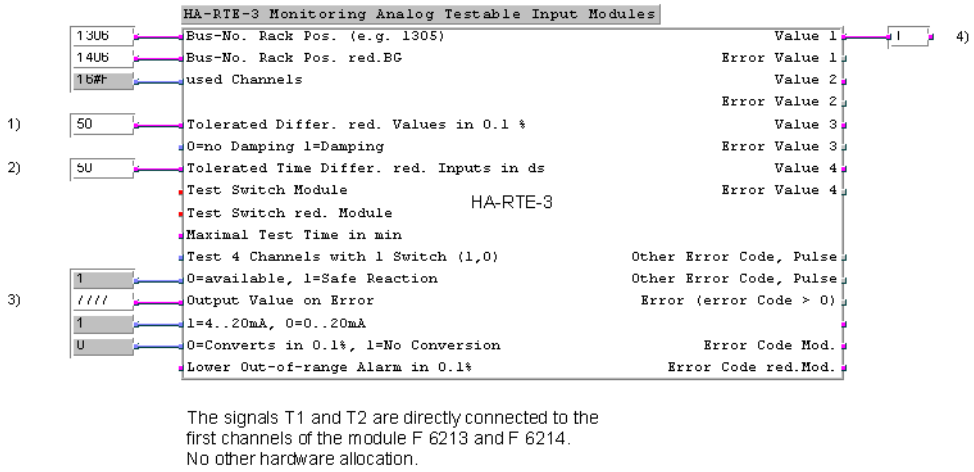


Figura 6: Ligação de sensores redundantes

Programa de aplicação, módulo de entrada F 6213 ou F 6214

Utilização do bloco HA-RTE-3, detalhes sobre o bloco, veja Kapitel 2.5 im Anhang e a ajuda online do ELOP II.



1) p.ex., 50
2) p.ex., 50
3) 7777, se a grandeza física aumentar no caso de perigo (todos os quatro canais do módulo), 0000, se a grandeza física diminuir no caso de perigo (todos os quatro canais do módulo),
4) valores 0...1066

Figura 7: Utilização do bloco HA-RTE-3 com F 6213 ou F 6214

Elemento comparador para alarme ou desligamento ao alcançar o valor limite admissível

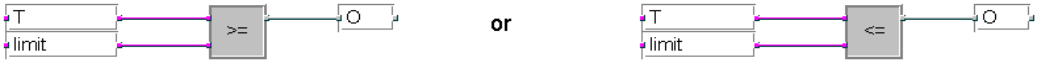


Figura 8: Elemento comparador para alarme ou desligamento ao alcançar o valor limite admissível

Consideração de segurança

Se um dos dois sensores for acionado ou se um componente dentro do sistema falhar, a saída A assume o nível High.

Para as aplicações dos sensores, devem ser observadas as normas relevantes, p. ex., IEC 61511.

Consideração de disponibilidade

Não há disponibilidade, pois cada falha de um componente ou o acionamento de um sensor levam ao desligamento.

7.8.5 Módulos de entrada com ligação 2oo3

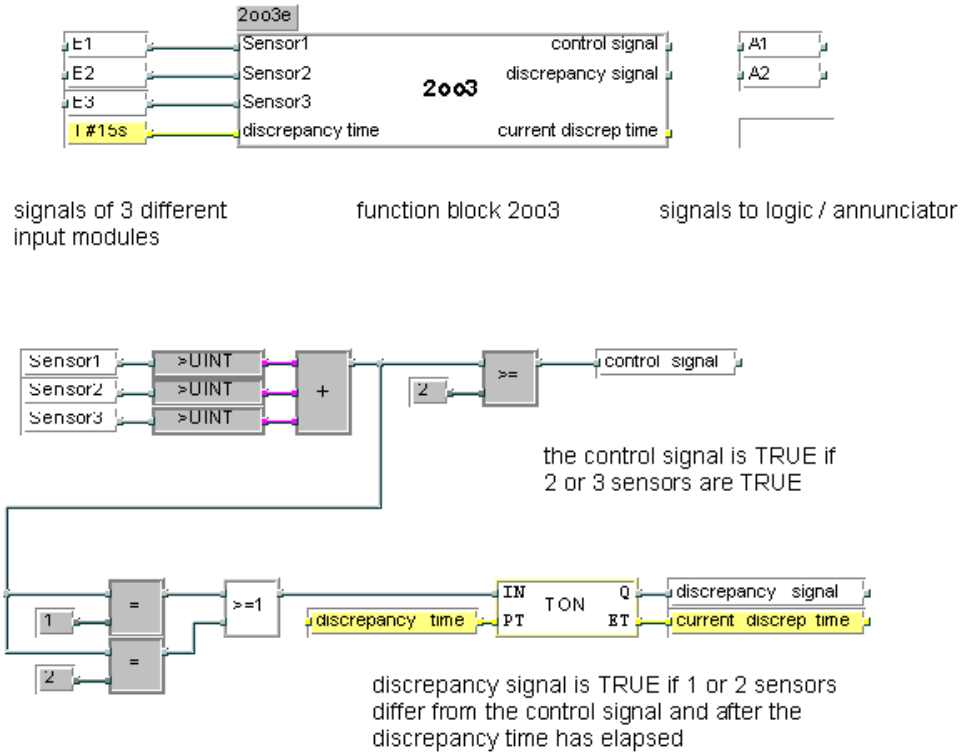


Figura 9: Bloco funcional 2oo3 e lógica do bloco

---

i A ligação mostrada está reunida num bloco funcional *2oo3*, por motivos de praticidade.

Com um PES com dois barramentos de E/S, o sinal do segundo sensor é bifurcado para dois canais de entrada (um canal no barramento de E/S 1 e um canal no barramento de E/S 2) e no programa de aplicação passa por uma função OU. Também é possível ligar todos os sinais de sensores em paralelo em canais de entrada nos dois barramentos de E/S para depois passarem por uma função OU cada um. Depois é utilizado o bloco funcional acima mostrado.

Para as aplicações dos sensores, devem ser observadas as normas relevantes, p. ex., IEC 61511.

7.9 Documentação do programa para aplicações direcionadas à segurança

A ferramenta de programação ELOP II possibilita a impressão automática da documentação de um projeto. Os tipos mais importantes de documentação são:

- Declaração de interfaces
- Lista de variáveis
- Lógica
- Descrição dos tipos de dados
- Configurações para armário, suporte de módulos, módulos e parâmetros de sistema
- Referências cruzadas PCS/variáveis
- Informações do gerador de código

O layout dos diferentes tipos de documentação pode ser definido de forma livre.

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 final refere-se apenas à função de aplicação mas não aos módulos e equipamentos de automação do sistema HIMax direcionados à segurança H41q-MS, H51q-MS, H41q-HS, H51q-HS, H41q-HRS, H51q-HRS que já foram aprovados como tipos.

---

i A HIMA recomenda, ao projetar instalações sujeitas a certificação final, entrar em contato com os órgãos de certificação o mais cedo possível.

7.10 Aspectos relacionados à segurança para a comunicação (transmissão de dados direcionada à segurança)

O protocolo HIPRO-S está certificado para SIL 3.

7.10.1 Comunicação direcionada à segurança

Na janela de diálogo *Properties* para os recursos (aba **HIPRO-S**, **Edit** do recurso marcado), é possível monitorar a troca de dados para recursos atribuídos relacionados à segurança mediante o master PES. Para este fim, é possível indicar um tempo de supervisão como parâmetro *Time interval* – intervalo de tempo – e ativar o comando *Reset imported variables* – resetar variáveis importadas, no caso de ultrapassar o tempo de supervisão.

O tempo de supervisão a ser ajustado depende do processo, devem ser consultadas as autoridades de certificação.

A comunicação direcionada à segurança também pode ocorrer através do protocolo safe**ethernet** certificado pela TÜV, com ajuda dos módulos de comunicação F 8627 X ou F 8628 X.

7.10.2 Exigências de tempo

No caso da conexão serial, a HIMA recomenda por motivos do tempo de transmissão constante um master PES próprio e um barramento próprio para a transmissão de dados direcionada à segurança com uma taxa de transmissão de dados de 57,6 kbit/s.

O tempo de transmissão de dados T_T da troca de um valor de sensor num PES até a reação na saída de um outro PES é:

$$T_T = 2*TC_1 + 2*T_D + 2*TC_2$$

TC_1 Tempo de ciclo do PES 1

TC_2 Tempo de ciclo do PES 2

T_D Tempo de transmissão de dados entre dois PES, depende da conexão de dados utilizada:

Transmissão serial: Aqui deve ser assumido o valor do tempo de ciclo do barramento. Veja sobre o tempo de ciclo do barramento o manual do sistema operacional HI 800 489 P, seção *Transmissão de dados direcionada à segurança via HIPRO-S*.
Transmissão via Ethernet: Nesse caso, deve ser assumido o tempo de transmissão máximo (T_{max}), veja seção *Calcular o tempo de supervisão para conexões HIPRO-S / HIPRO-S DIRECT*, na folha de dados do módulo F 8627 X.

7.10.3 Avisos para a elaboração do programa de aplicação

A configuração da rede Ethernet no ELOP II para HIPRO-S ocorre automaticamente. Mesmo assim, devem ser observados os seguintes avisos para a elaboração do programa de aplicação:

- O nome de recurso no ELOP II deve ser de oito caracteres, os últimos dois sendo números. São admissíveis os números de 1 a 99. Os números devem ser unívocos para que possam ser utilizados sem colisão para detectar o endereço IP do módulo de comunicação.
- A comunicação direcionada à segurança com HIPRO-S no modo NORMAL deve ser ajustada de forma que qualquer dispositivo de automação tenha configurado uma troca de dados direcionada à segurança para qualquer outro. (ou seja, troca de dados vazios, se não são trocados dados do usuário).
  Com a utilização do modo HIPRO-S-DIRECT, isso não se faz necessário (não é preciso transmitir dados vazios). Detalhes, veja folha de dados F 8627 X.
- Para o controle da configuração HIPRO-S, o programa master PES deve ser compilado. Depois devem ser corrigidos os erros ocorridos.
- Para a comunicação direcionada à segurança, zero deve ser o valor seguro para os dados de transmissão.

8 Aplicação em centrais de alarme de incêndio conforme DIN EN 54-2 e NFPA 72

Os sistemas H41q, H41qc e H51q podem ser utilizados para centrais de alarme de incêndio conforme DIN EN 54-2 e NFPA 72.

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 H41q, H41qc e H51q, porque o tempo de ciclo desses sistemas está na faixa de < 0,5 segundos e também o tempo de segurança eventualmente exigido de 1 segundo (tempo de reação de erro).

A ligação dos sensores de incêndio ocorre pelo princípio de circuito aberto com supervisão de linha para curto e quebra de fio. Para esse fim, podem ser utilizados os módulos de entrada F 3237/F 3238 para conexões booleanas ou F 6217/F 6221 para conexões analógicas com a ligação como segue:

Conexões digitais

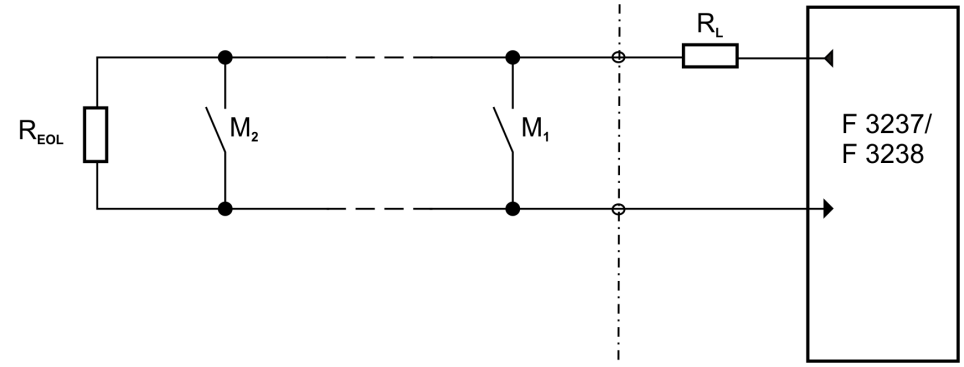


Figura 10: Conexões digitais de sensores de incêndio

Conexões analógicas

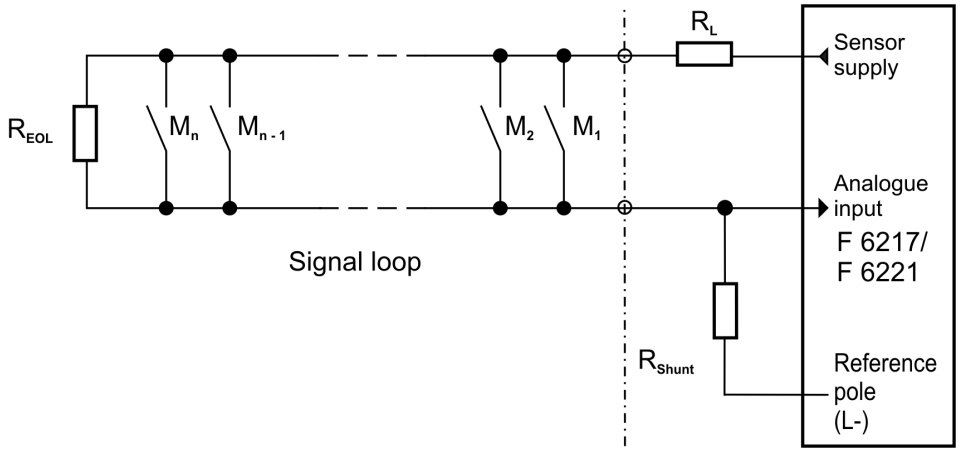


Figura 11: Ligação de sensores de incêndio

Legenda das figuras:

M	Sensor de incêndio
R_{EOL}	Resistência de terminação no último sensor do loop
R_L	Limitação da corrente máxima admissível do loop
R_{Shunt}	Resistência de medição

Para as aplicações devem ser calculadas as resistências R_{EOL}, R_L e R_{Shunt}, dependendo dos sensores utilizados e de sua quantidade por loop de sinalização. Para este fim, também devem ser consideradas as folhas de dados dos fabricantes dos sensores.

Adicionalmente, deve ser observado que os valores de corrente dos módulos F 3237 e F 3238 sejam respeitados (veja folhas de dados). Isso vale especialmente se os sensores de incêndio não tiverem contatos mecânicos, mas saídas eletrônicas.

As saídas de alarmes para comandar lâmpadas, sirenes, buzinas, etc., são operadas no princípio de circuito aberto, ou seja, devem ser utilizados módulos de saída com supervisão dos circuitos para curto de linha e quebra de fio, p.ex., os tipos de módulos F 3331 ou F 3334.

O acionamento de sistemas de visualização, painéis luminosos, indicadores de LED, displays alfanuméricos, alarmes acústicos, etc. pode ser realizado mediante um programa de aplicação adaptado a esta tarefa.

A repassagem de mensagens de avaria através de módulos 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 HIMA a outro pode ser realizada com os padrões de comunicação existentes, como Modbus, HIPRO-S, OPC (Ethernet). A supervisão da comunicação faz parte do programa de aplicação. A HIMA recomenda executar esta comunicação de forma redundante para que no caso de avarias em um componente de um trajeto de transmissão (condutor, erro de hardware, etc.) a comunicação ainda seja garantida. A falha do componente deve ser comunicada e deve ser possível substituir ou reparar o componente defeituoso durante a operação.

Os sistemas H41q, H41qc e H51q 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 ocorrer tão rapidamente que a operação ininterrupta seja garantida. Quedas de tensão até 10 ms são admissíveis.

No caso de avarias do sistema, o sistema operacional escreve nas variáveis de sistema que podem ser avaliadas no programa de aplicação. Assim, a sinalização de erros para os erros detectados pelo sistema pode ser programada. Entradas e saídas direcionadas à segurança são desligadas no caso de erro, ou seja, processamento de níveis Low em todos os canais do módulo de entrada com erro e desligamento de todos os canais do módulo de saída com erro.

No caso de sistema de detecção de incêndios conforme EN 54-2 e NFPA 72 deve ser utilizada uma supervisão de curto a terra.

Anexo

1 Blocos de software padrão para a área central

Para funções dos módulos centrais podem ser chamados e atribuídos blocos de software padrão. Uma descrição detalhada destes blocos encontra-se na ajuda online do respectivo bloco.

1.1 Bloco HK-AGM-3

Com este bloco, é monitorada a função de uma dispositivo de automação H41q ou H51q como master HIPRO.

O bloco não é relevante relacionado à segurança. As saídas do bloco apenas servem fins de informação, não podem ser derivadas ações direcionadas à segurança delas no programa de aplicação.

1.2 Bloco HK-COM-3

Com este bloco, é monitorada a função dos módulos de comunicação num sistema H41q ou H51q.

O bloco não é relevante relacionado à segurança. As saídas do bloco apenas servem fins de informação, não podem ser derivadas ações direcionadas à segurança delas no programa de aplicação.

1.3 Bloco HK-MMT-3

Com este bloco, um dispositivo de automação H41q, H41qc ou H51q pode ser utilizado como master Modbus.

O bloco não é relevante relacionado à segurança. As saídas do bloco apenas servem fins de informação, não podem ser derivadas ações direcionadas à segurança delas no programa de aplicação.

1.4 Bloco H8-UHR-3

O bloco permite o ajuste externo ou a alteração de data e hora do dispositivo de automação.

As saídas do bloco apenas servem fins de informação, não podem ser derivadas ações direcionadas à segurança delas no programa de aplicação.

2 Blocos de software padrão para a área de E/S

Todos os blocos de software descritos na continuação são certificados para a operação em dispositivos de automação direcionados à segurança.

Os avisos especiais de programação descritos neste capítulo devem ser observados.

Para as informações exatas sobre as funções dos blocos de software a atribuição de entradas e saídas deve ser usada a ajuda online do respectivo bloco.

2.1 Bloco H8-STA-3

O bloco é utilizado para a configuração de um desligamento de grupo. Usa-se uma vez para cada grupo de desligamento no programa de aplicação.

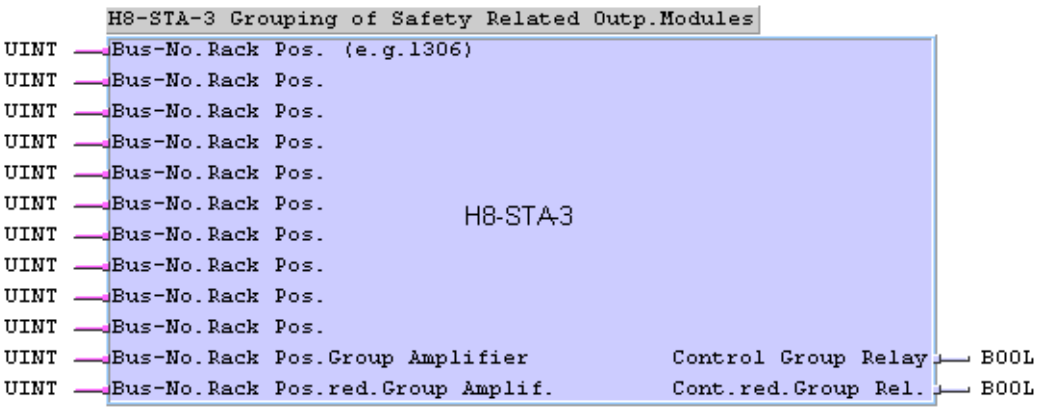


Figura 12: Conexões do bloco H8-STA-3

Sobre o comportamento em caso de erros de canais de saída, veja Capítulo 7.2.6.2

2.1.1 Entradas

As posições dos módulos que pertencem a um grupo de desligamento são introduzidas como número decimal de quatro dígitos, de acordo com a determinação no recurso selecionado.

Exemplo: “1306” significa:

Armário 1, suporte de módulos 3, posição do módulo 06

Ao utilizar módulos com desligamento de segurança integrado, uma das entradas *Bus No. Rack Pos. Group Amplif.* ou *Bus No. Rack Pos. red. Group Amplif.* deve ser atribuída. Aqui deve ser introduzido um slot existente mas não ocupado.

---

i Módulos de saída com desligamento de segurança integrado não necessitam de desligamento de grupo. Porém, também pode ser especificado para estes módulos. Neste caso, um erro em um módulo de saída leva ao desligamento de todos os módulos que pertencem a um grupo (de acordo com as indicações no bloco H8-STA-3).

2.2 Bloco HA-LIN-3

O bloco serve para a linearização de medições de temperatura com termopares e termorresistências Pt 100. A parametrização correta deve ser verificada se os valores são utilizados para o desligamento de circuitos relevantes relacionados à segurança (veja ajuda online do ELOP II).

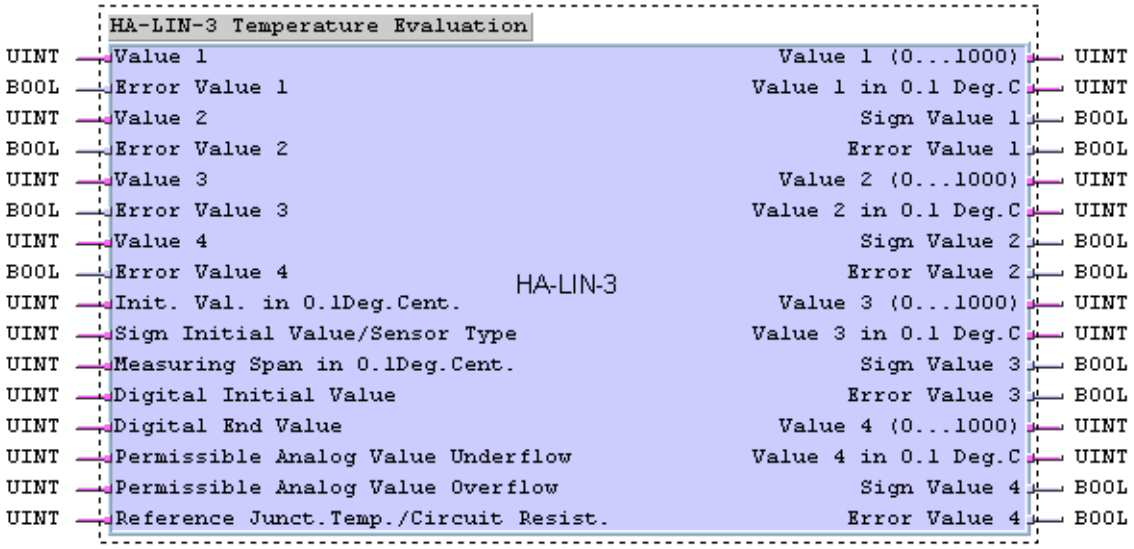


Figura 13: Conexões do bloco HA-LIN-3

2.3 Bloco HA-PID-3

O bloco contém um regulador digital que pode ser operado mediante parametrização nos modos P, I, D, PI, PD e PID.

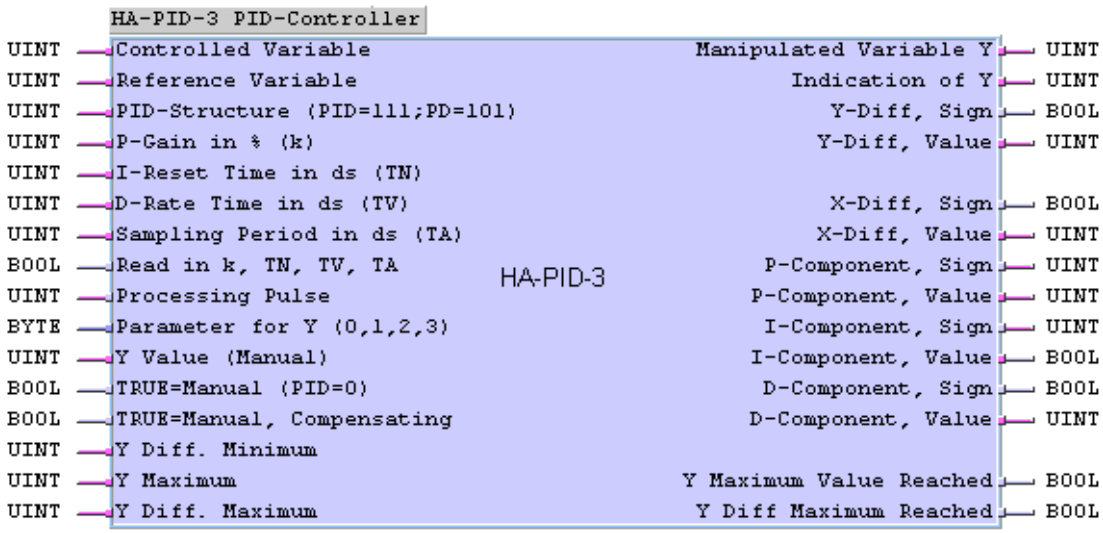


Figura 14: Conexões do bloco HA-PID-3

2.3.1 Entradas

True=operação manual (PID=0), *True=operação manual alinhada*	Na operação direcionada à segurança do bloco regulador, estas entradas não podem ser atribuídas. Desvios desta norma devem ser autorizadas pela instituição de certificação. Alteração de parâmetros e constantes nas entradas de blocos durante a operação em andamento apenas são permitidas com a autorização da instituição de certificação e em operação monitorada. A atribuição das entradas do bloco com variáveis de importação não direcionadas à segurança não é admissível.

2.3.2 Saídas:

Desligamentos de segurança apenas são permitidos mediante:

máx. valor de ajuste alcançado e *máx. diferença de ajuste alcançada*

Desvios desta norma devem ser autorizadas pela instituição de certificação.

---

i O algoritmo de regulação do bloco por si só não pode alcançar em todos os casos o estado seguro de uma instalação. No caso individual, medidas adicionais são necessárias.

2.4 Bloco HA-PMU-3

O bloco serve tanto para a conversão de valores de medição digitalizados em valores de por mil, quanto para a conversão de valores por mil em valores analógicos digitalizados. A parametrização correta deve ser verificada se os valores são utilizados para o desligamento de circuitos relevantes relacionados à segurança (veja ajuda online do ELOP II).

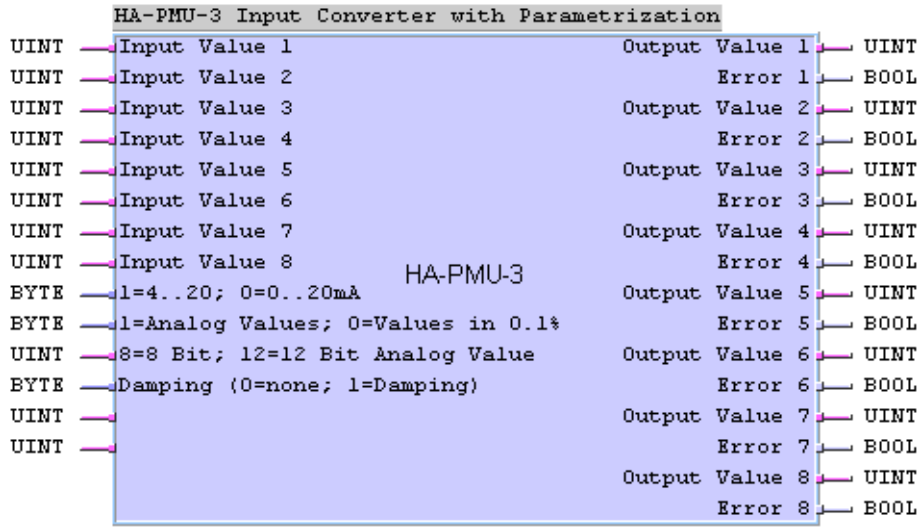


Figura 15: Conexões do bloco HA-PMU-3

2.5 Bloco HA-RTE-3

O bloco serve para o processamento de valores e para a indicação de erros em módulos de entrada analógicos direcionados à segurança na operação monocanal ou redundante. Para cada módulo de entrada analógico direcionado à segurança (F 6213/F 6214), deve ser utilizado uma vez no programa de aplicação. No caso utilizar dois módulos de E/S redundantes, o bloco apenas precisa existir uma vez no programa de aplicação.

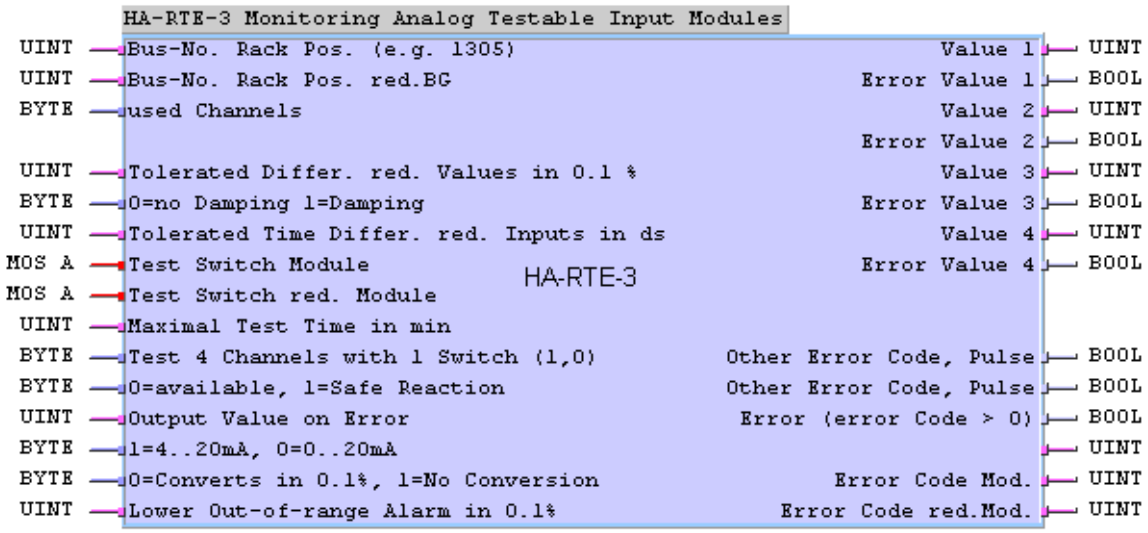


Figura 16: Conexões do bloco HA-RTE-3

2.5.1 Entradas

Bus No. Rack Pos. (p.ex., 1305) *Bus No. Rack Pos. red. Mod* *Módulo*	Posição do módulo de entrada analógico direcionado à segurança e, se equipado, do módulo redundante como número decimal de 4 dígitos: Exemplo: “1305” significa: Armário 1, suporte de módulos 3, posição do módulo 05 (no caso de operação redundante, o módulo redundante deve receber uma posição diferente)
0 = sem; 1 = atenuação	1 só para operação redundante. Diferença entre o valor atual e o valor atual do ciclo anterior soma-se à diferença permitida em ‰ (*Tolerated Differ. red. Values in 0,1 %)*.
Maximum Test Time in min	Limitação do tempo de teste em minutos. Depois de esgotar o tempo de teste, o valor real é processa na lógica da aplicação. Veja também o documento *Intervenções de manutenção Maintenance Override*, na homepage www.tuvasi.com da TÜV Rheinland.

2.5.2 Saídas

Valor 1...4	A utilização dos valores deve ser verificada se eles são usados para o desligamento de circuitos direcionados à segurança.
Erro valor 1...4	As saídas devem ser atribuídas para poder disparar com o seu sinal booleano o desligamento em caso de erro.

As demais saídas apenas servem fins de informação, não podem ser derivadas ações direcionadas à segurança delas no programa de aplicação.

2.6 Bloco HB-BLD-3

O bloco serve à avaliação de erros relacionada ao canal e à indicação de erros para módulos de saída digitais direcionados à segurança F 3331, F 3334 e F 3349. Para cada módulo utilizado apenas pode ser utilizado uma vez.

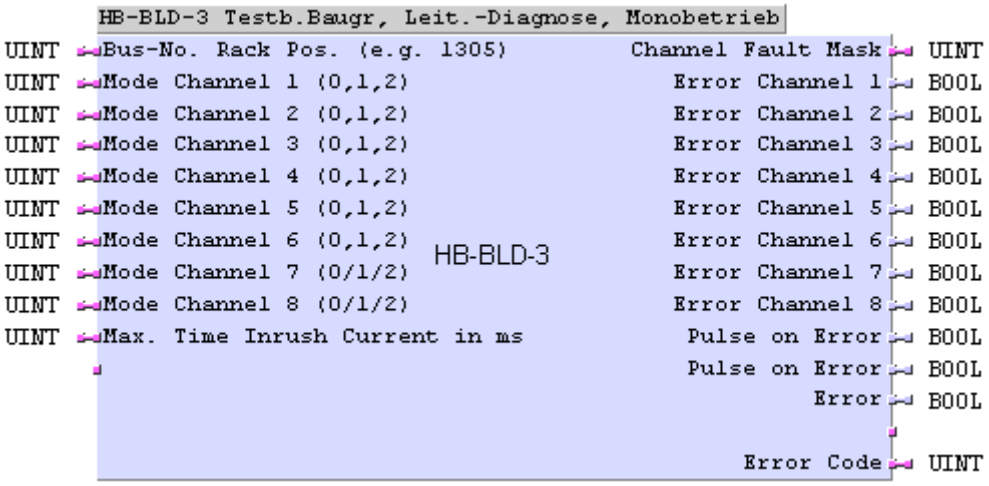


Figura 17: Conexões do bloco HB-BLD-3

2.6.1 Entradas

Bus No. Rack Pos. (p.ex., 1305)

Posição do módulo de saída digital direcionado à segurança como número decimal de 4 dígitos, exemplo: “1305” significa:
Armário 1, suporte de módulos 3, posição do módulo 05

Mode channel n (0/1/2)

Atribuição	Significado
1	Operação normal, erro detectado é comunicado com nível High à saída correspondente *Error Channel n*, o circuito de saída do módulo está fechado.
0	Avaliação de erros, mensagens de erro são suprimidas
2	Apenas permitido de forma específica para a instalação, operação invertida, ou seja, o circuito de saída deve estar aberto
>2	Faixa de valores ultrapassada: o canal é interpretado com erro (TRUE na saída) e uma mensagem de erro relacionada ao canal é emitida.

Em circuitos de comando direcionados à segurança sempre deve ser aplicado o princípio de circuito fechado.

Max. Time Inrush Current in ms

Definição do tempo de espera para a detecção da quebra de fio ou tempo para tolerância do limite de corrente. Durante este tempo, a indicação do erro é suprimida. Um aumento do tempo de espera acarreta um aumento do tempo de ciclo.

2.6.2 Saídas

As saídas *Pulse on Error* (2x), *Error* and *Error Code* apenas servem fins de informação, não podem ser derivadas ações direcionadas à segurança delas no programa de aplicação.

As demais saídas podem ser usadas para ações direcionadas à segurança.

2.7 Bloco HB-BLD-4

O bloco serve à avaliação de erros relacionada ao canal e à indicação de erros para módulos de saída digitais direcionados à segurança F 3331, F 3334 e F 3349 na operação redundante. Apenas pode ser utilizado uma vez para cada par de módulos redundante.

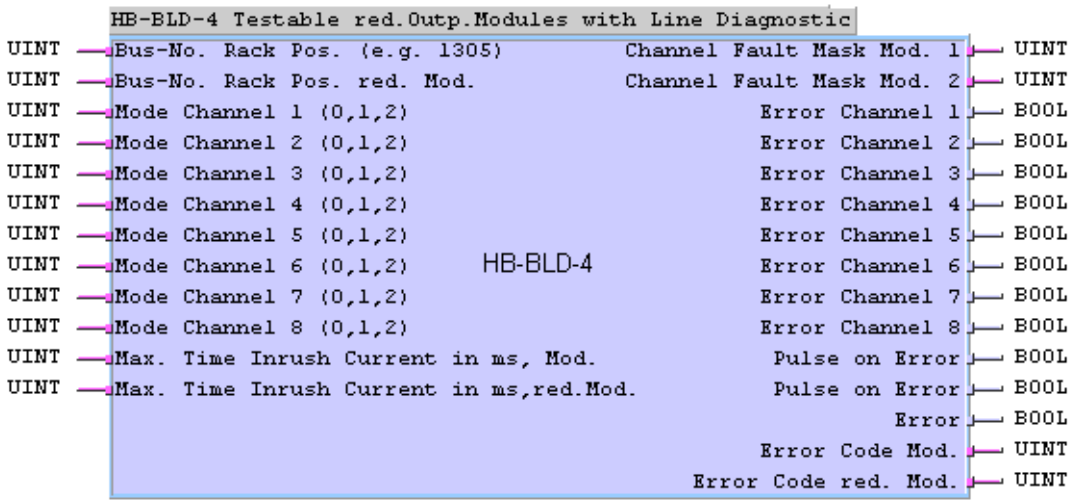


Figura 18: Conexões do bloco HB-BLD-4

2.7.1 Entradas

Bus No. Rack Pos.(p.ex., 1305)
Bus No. Rack Pos. red. Mod.

Posição do módulo de saída digital direcionado à segurança e, se equipado, do módulo redundante como número decimal de 4 dígitos.
Exemplo: “1305” significa:
Armário 1, suporte de módulos 3, posição do módulo 05

Mode channel n (0/1/2)

Atribuição	Significado
1	Operação normal, erro detectado é comunicado com nível High à saída correspondente *Error Channel n*, o circuito de saída do módulo está fechado.
0	Avaliação de erros, mensagens de erro são suprimidas.
2	apenas permitido de forma específica para a instalação, operação invertida, ou seja, o circuito de saída deve estar aberto Um erro detectado é comunicado com nível High à saída correspondente *Error Channel n*.
>2	Faixa de valores ultrapassada: o canal é interpretado com erro (TRUE na saída) e uma mensagem de erro relacionada ao canal é emitida.

Em circuitos de comando direcionados à segurança sempre deve ser aplicado o princípio de circuito fechado.

Max. Time Inrush Current in ms Mod
Max. Time Inrush Current in ms red. Mod

Definição do tempo de espera para a detecção da quebra de fio ou tempo para tolerância do limite de corrente. Durante este tempo, a indicação do erro é suprimida. Um aumento do tempo de espera acarreta um aumento do tempo de ciclo.

2.7.2 Saídas

As saídas *Pulse on Error* (2x), *Error*, *Error Mod.* e *Error Code red. Mod* apenas servem fins de informação, não podem ser derivadas ações direcionadas à segurança delas no programa de aplicação.

As demais saídas podem ser usadas para ações direcionadas à segurança.

2.8 Bloco HB-RTE-3

O bloco serve para a avaliação e para a indicação de erros em módulos de entrada digitais direcionados à segurança na operação monocanal ou redundante. Para cada módulo de entrada direcionado à segurança tipo F 3237 ou F 3238 ou para dois módulos de entrada F 3237 ou F 3238 trabalhando de forma redundante, deve ser utilizado uma vez no programa de aplicação.

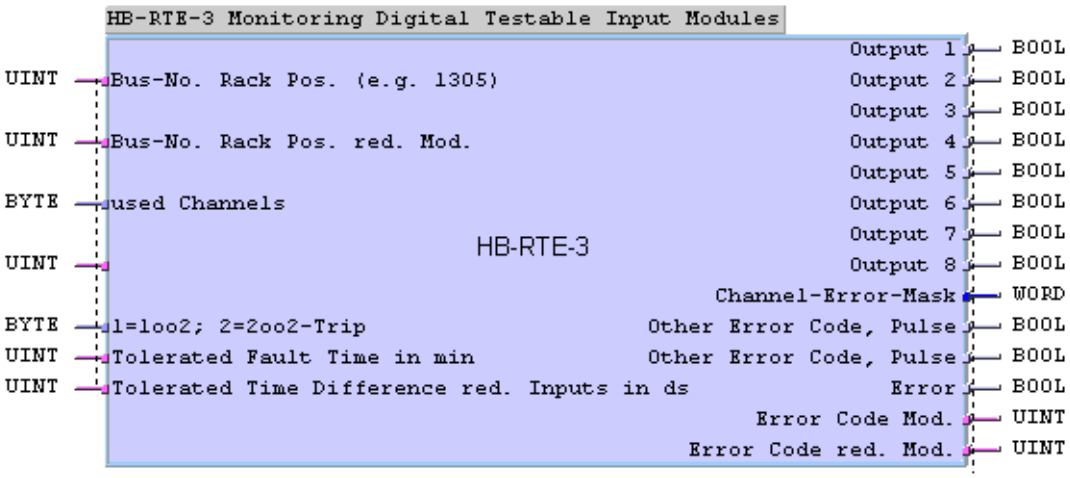


Figura 19: Conexões do bloco HB-RTE-3

2.8.1 Entradas:

Bus No. Rack Pos.(p.ex., 1305) Bus No. Rack Pos. red. Mod.	Posição do módulo de saída digital direcionado à segurança e, se equipado, do módulo redundante como número decimal de 4 dígitos. Exemplo: “1305” significa: Armário 1, suporte de módulos 3, posição do módulo 05

1 = 1 de 2; 2 = 2 de 2 – desligamento

Atribuição	Significado
0	Atribuição na operação monocanal. Introdução de acordo com IEC 1131: 16#00 ou 2#00000000.
1	Desligamento 1 de 2, corresponde ao vínculo E. No caso do desligamento 1 de 2, a redundância dos módulos é utilizada para aumentar a disponibilidade. Se não houver erros dos módulos de entrada e dos circuitos de entrada, os sinais de entrada dos canais 1...8 dos módulos são vinculados às saídas do bloco como E. Se um erro ocorrer num canal, o último estado é mantido na saída correspondente do bloco e depois de esgotar o tempo de erro definido, é resetado para FALSE, se o erro ainda estiver ativo. No caso de FALSE na outra entrada sem erro ou se ocorrerem erros simultaneamente nos dois canais (erro duplo), a saída do bloco é ajustada em FALSE, sem retardo.
2	Desligamento 2 de 2, corresponde ao vínculo OU. No caso do desligamento 2 de 2, a redundância dos módulos é utilizada para aumentar a disponibilidade. Se não houver erros dos módulos de entrada e dos circuitos de entrada, os sinais de entrada dos canais 1...8 dos módulos são vinculados às saídas do bloco como OU. Se ocorrer um erro em um canal, o sinal de entrada do outro canal é transferido à saída do bloco. Apenas no caso da ocorrência simultânea de erros nos dois canais (erro duplo) o último estado é mantido na saída correspondente do bloco e depois de esgotar o tempo de erro definido, é resetado para FALSE, se o erro duplo ainda estiver ativo.

Em circuitos de comando direcionados à segurança sempre deve ser aplicado o princípio de circuito fechado.

Tolerated Fault Time in min
: Dentro do tempo indicado após o teste do sensor, erros de componentes ou condutores não tem efeito sobre o desligamento
Permissão da instituição certificadora é necessária.

Tolerated Time Difference red. Inputs in ds
: A diferença de tempo dos pontos de comutação entre dois sensores redundantes. O tempo depende dos sensores, permissão da instituição certificadora é necessária.

2.8.2 Saídas

As saídas *Channel Error Mask*, *Other Error Code, Pulse* (2x), *Error*, *Error Code Mod.* e *Error Code red. Mod* apenas servem fins de informação, não podem ser derivadas ações direcionadas à segurança delas no programa de aplicação.

As saídas *Output 1* a *Output 8* podem ser usadas para ações direcionadas à segurança.

2.9 Bloco HF-AIX-3

O bloco HF-AIX-3 serve para a parametrização e avaliação de sempre um canal do módulo de entrada analógico (Ex)i direcionado à segurança F 6221 com uma resolução de 0...10 000.

O bloco HF-AIX-3 deve ser utilizado uma vez no programa de aplicação para cada canal do F 6221.

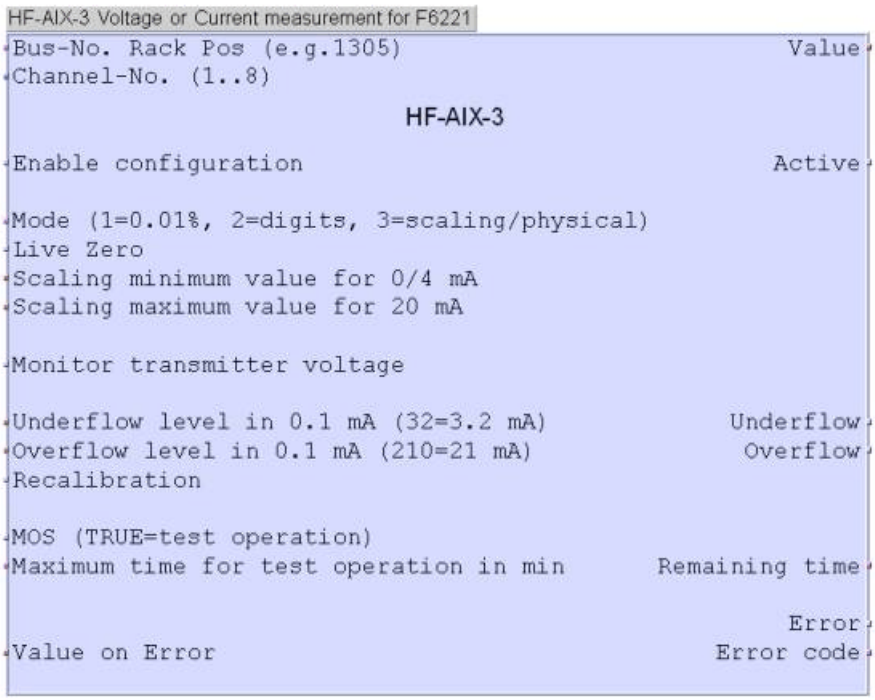


Figura 20: Conexões do bloco HB-AIX-3

O módulo de entrada analógico possui uma saída direcionada à segurança por canal que é controlada de forma independente do ciclo do módulo central. O estado desta saída é indicado na saída do bloco HF-AIX-3 e pode ser usada para processamento posterior no programa de aplicação.

Através dos ajustes de parâmetros, o valor do módulo de entrada analógico pode ser alterado e escalado.

Um valor *Value on error* definido na entrada do bloco é ligado à saída *Value* nos seguintes casos:

- Com falha de canal
- Com erro do módulo
- Com valores fora da área de medição

Nestes casos, o programa de aplicação processa o *Value on error* no lugar do valor de medição.

2.10 Bloco HF-CNT-3

O bloco HF-CNT-3 serve para a parametrização e avaliação dos dois canais do módulo contador direcionado à segurança F 5220 com uma resolução de 24 bit. O módulo contador pode ser utilizado para a contagem de pulsos, detecção de frequências ou rotação, bem como para a detecção do sentido de rotação.

O bloco HF-CNT-3 deve ser utilizado uma vez no programa de aplicação para cada módulo contador F 5220.

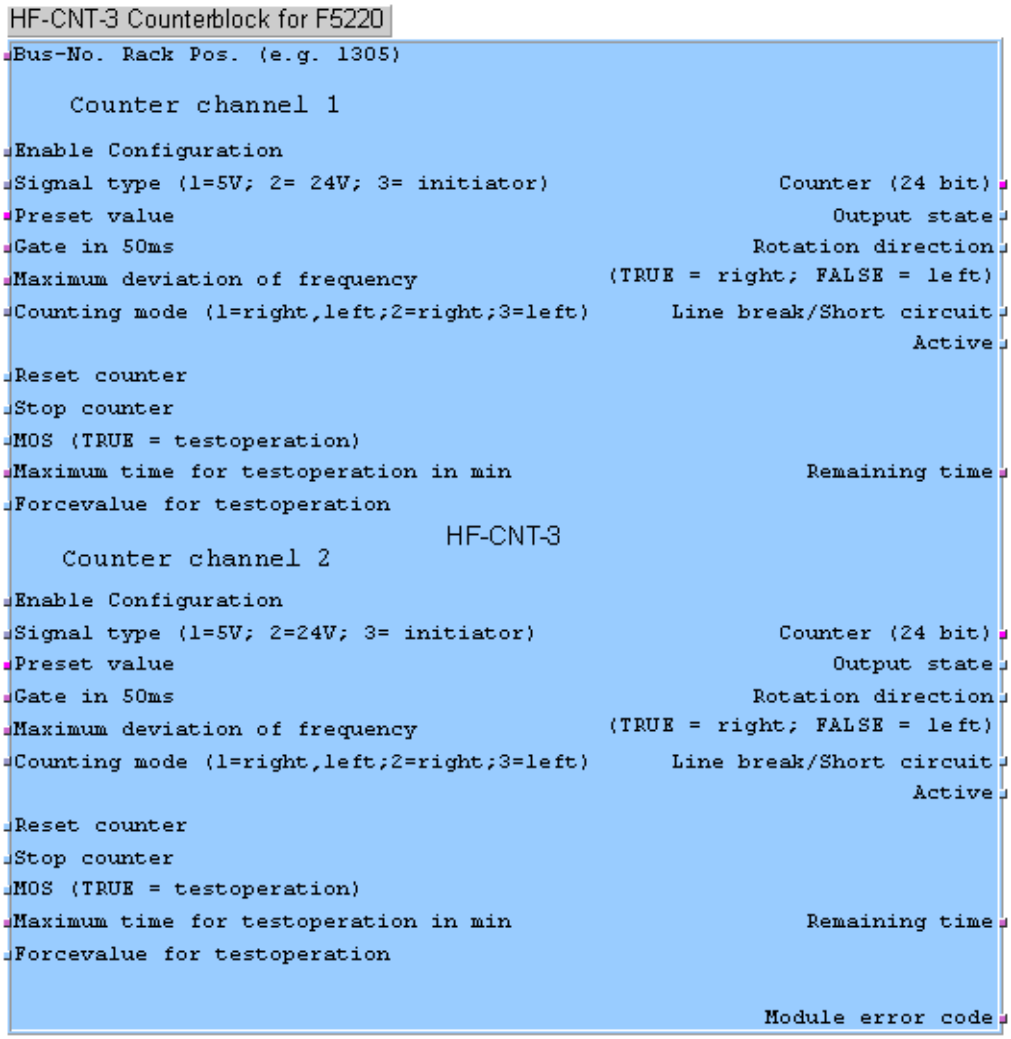


Figura 21: Conexões do bloco HB-CNT-3

O módulo contador possui uma saída direcionada à segurança por canal que é controlada de forma independente do ciclo do módulo central. O *estado da saída* é indicado na saída do bloco HF-CNT-3 e pode ser usada para processamento posterior no programa de aplicação.

Com o sinal TRUE na entrada *MOS* (Maintenance Override Switch), a saída do módulo contador pode ser controlada diretamente para o tempo de operação de teste, ou seja, a saída carrega o sinal atribuído na entrada *Force Value for Test Operation*. Veja também o documento *Intervenções de manutenção Maintenance Override*, na homepage www.tuvasi.com da TÜV Rheinland.

---

i No caso de alteração do tempo de abertura, o valor de medição correto está à disposição na saída apenas após três tempos de abertura percorridos (atualmente ajustados)!

2.11 Bloco HF-CNT-4

Esse bloco corresponde ao bloco HF-CNT-3, mas possui adicionalmente uma saída *Channel Error* por canal.

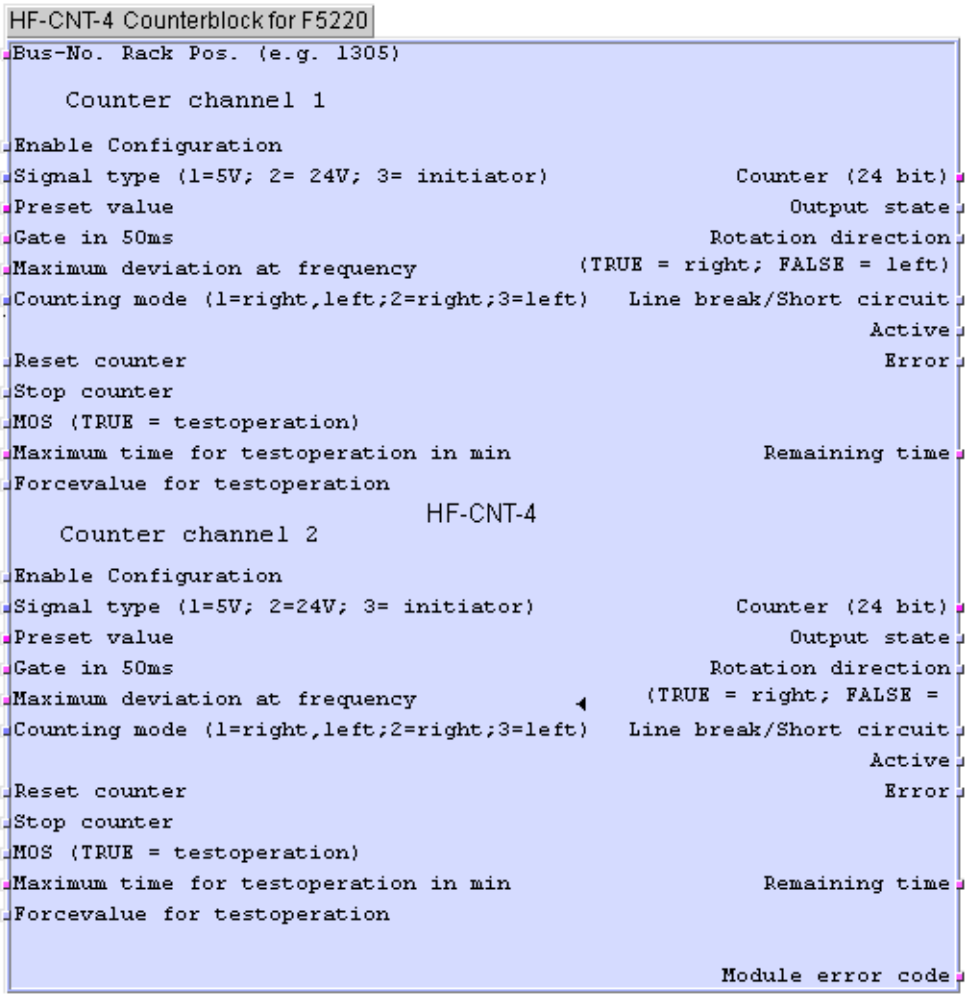


Figura 22: Conexões do bloco HB-CNT-4

As saídas *Channel Error* comunicam um erro de canal:.

Erro de canal=	
TRUE	Há um erro de canal. No caso de um erro de módulo, as duas saídas *Channel Error* são TRUE.
FALSE	O canal trabalha corretamente ou ainda não está parametrizado.

2.12 Bloco HF-TMP-3

O bloco HF-TMP-3 é usado para cada canal do módulo de termopares F 6220. Sem parametrização correta do canal através do bloco HF-TMP-3, o canal não trabalha, ou seja, os valores de saída são 0 ou FALSE. Não existe funcionalidade padrão ou ajuste padrão. O tipo de sensor 1 apenas pode ser introduzido no canal 9.

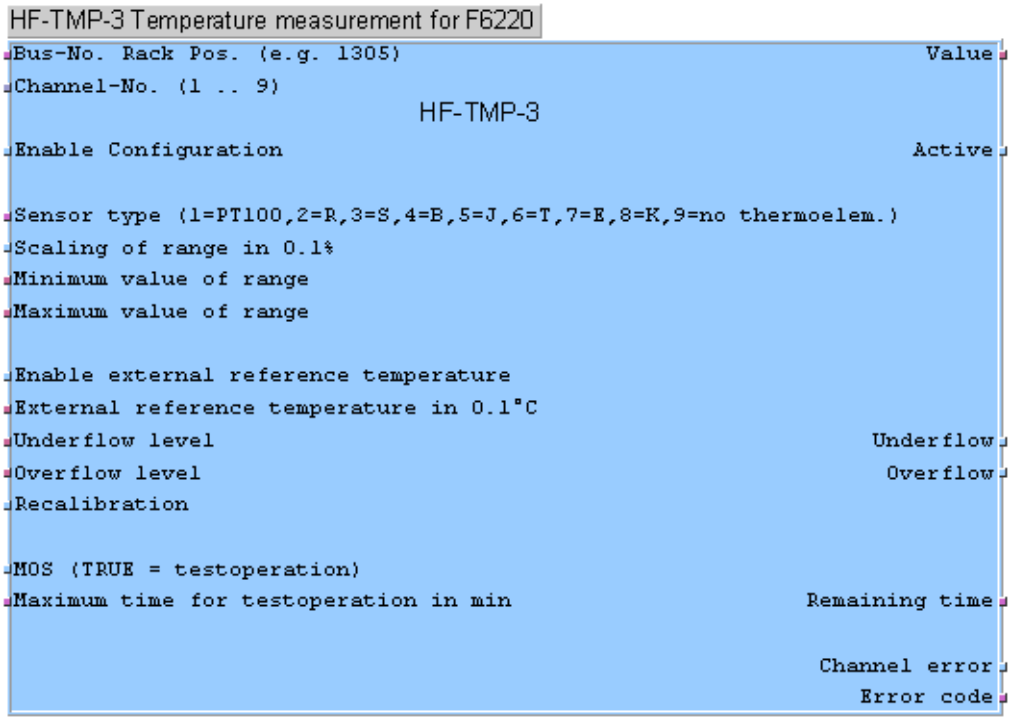


Figura 23: Conexões do bloco HB-TMP-3

O sinal *Enable External Comparison Temperature* apenas é avaliado se o modo de operação *Temperature Measurement* está ajustado (valores 2 a 8 na entrada *Type*). Se esta entrada estiver TRUE, a temperatura presente na entrada *External Reference Temperatura* é utilizada como valor de comparação. Se esta entrada estiver FALSE, o valor de temperatura da termorresistência presente no módulo é processado como temperatura de comparação.

No caso de erro do canal ou do módulo, a saída do bloco *Value* assume o valor 0. Por isso, no caso de erro deve ser avaliada a entrada do bloco *Channel Error* no programa de aplicação para que o valor de erro definido no programa de aplicação seja processado.

No caso de aplicações relacionadas à segurança no SIL 3, a temperatura de referência deve ser avaliada como comparação das temperaturas de referência em dois módulos diferentes, ao mesmo tempo, a temperatura de dois termopares.

A recablibração é executada automaticamente a cada 5 minutos para a detecção automática das condições de ambiente presentes no módulo (p.ex., temperatura). Essa função também pode ocorrer no programa de aplicação mediante sinal TRUE na entrada *Recalibration*. Este sinal apenas pode estar presente durante um ciclo.

Com o sinal TRUE na entrada *MOS* (Maintenance Override Switch), o valor nas entradas do bloco *Value* e *Channel Error* é congelado enquanto correr o tempo para a operação de teste. Veja também o documento *Intervenções de manutenção Maintenance Override*, na homepage www.tuvasi.com da TÜV Rheinland.

2.13 Bloco HK-LGP-3

O bloco serve para a avaliação e configuração do registro de eventos e da comutação entre Modbus e LCL (protocolagem controlada pelo plano lógico – LGP em alemão).

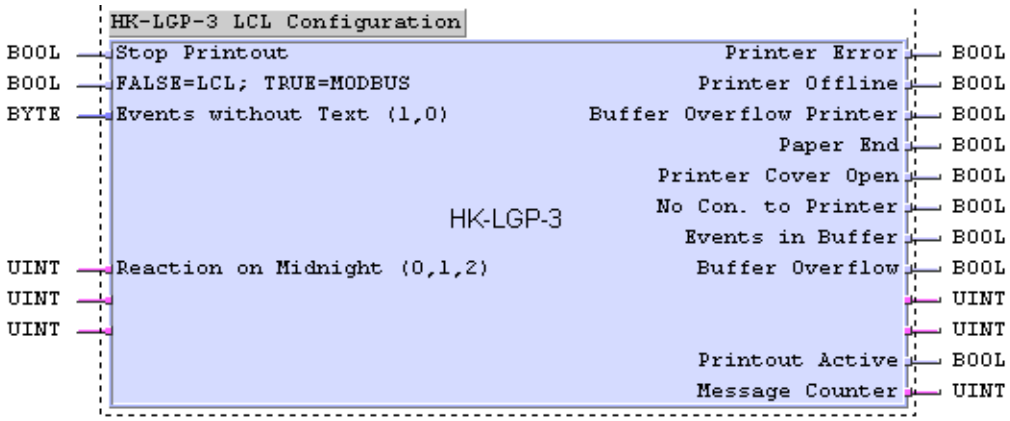


Figura 24: Conexões do bloco HB-LGP-3

O bloco não é relevante relacionado à segurança. As saídas do bloco apenas servem fins de informação, não podem ser derivadas ações direcionadas à segurança delas no programa de aplicação.

2.14 Bloco HZ-DOS-3

O bloco serve para a definição quais módulos de E/S direcionados à segurança apenas devem ser operados no modo de diagnóstico. Com um bloco podem ser monitorados até dezesseis módulos. O bloco pode ser utilizado várias vezes no programa de aplicação.

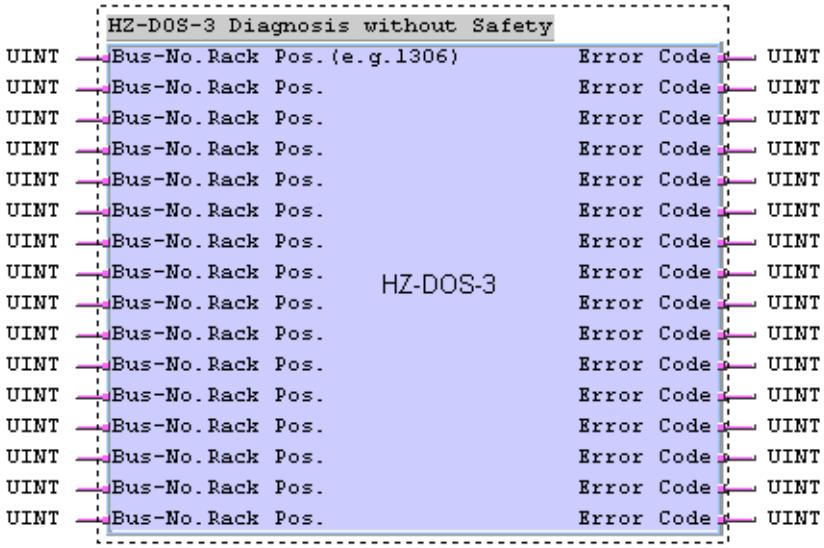


Figura 25: Conexões do bloco HZ-DOS-3

O bloco não é relevante relacionado à segurança. As saídas do bloco apenas servem fins de informação, não podem ser derivadas ações direcionadas à segurança delas no programa de aplicação.

Todos os módulos de E/S direcionados à segurança listados no bloco HZ-DOS-3 não podem ser utilizados para funções de segurança.

2.15 Bloco HZ-FAN-3

O bloco serve para a avaliação e para a indicação de erros em módulos de E/S direcionados à segurança. Com um bloco podem ser monitorados até oito módulos. O bloco pode ser utilizado várias vezes no programa de aplicação.

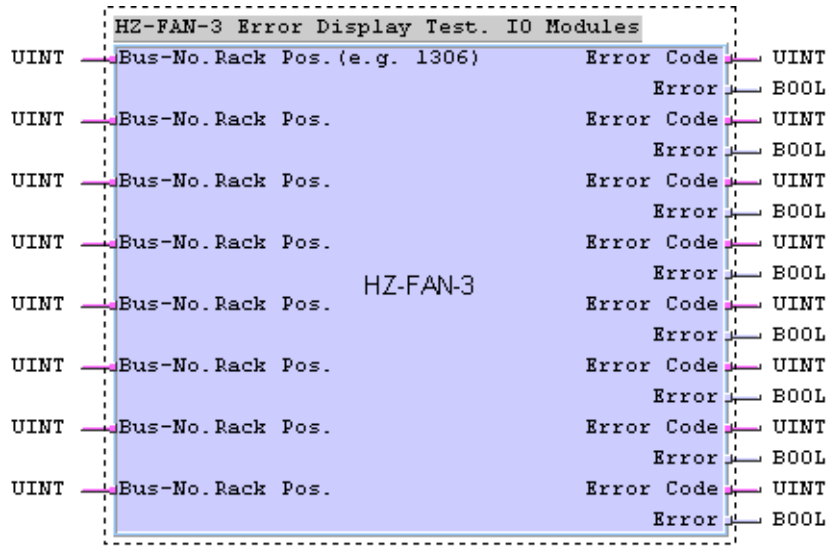


Figura 26: Conexões do bloco HZ-FAN-3

2.15.1 Entradas

Bus No. Rack Pos. (p.ex., 1306)	As posições dos módulos de E/S direcionados à segurança são introduzidas como número decimal de quatro dígitos. Exemplo: “1306” significa: Armário 1, suporte de módulos 3, posição do módulo 06

2.15.2 Saídas

Todas as saídas do bloco apenas servem fins de informação, não podem ser derivadas ações direcionadas à segurança delas no programa de aplicação.

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
Connector Board	Placa de conexão para o módulo HIMax
COM	Módulo de comunicação
CRC	Cyclic Redundancy Check, Soma de verificação
DI	Digital Input, Entrada digital
DO	Digital Output, Saída digital
ELOP II	Ferramenta de programação para H41q/H51q
CEM	Compatibilidade eletromagnética
EN	Normas européias
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	Normas internacionais para eletrotécnica
Endereço MAC	Endereço de hardware de uma conexão de rede (Media Access Control)
PADT	Programming and Debugging Tool (conforme IEC 61131-3), PC com ELOP II
PE	Terra de proteção
PELV	Protective Extra Low Voltage: Extra baixa tensão funcional com separação segura
PES	Programable Electronic System, Sistema eletrônico programável
PFD	Probability of Failure on Demand: Probabilidade de uma falha ao demandar uma função de segurança
PFH	Probability of Failure per Hour: Probabilidade de uma falha perigosa por hora
R	Read, Ler
Livre de efeitos de retroalimentação	Dois circuitos de entrada estão ligados à mesma fonte (p.ex., transmissor). Uma ligação de entrada é chamada de “sem efeito de retroalimentação” se ela não interferir com os sinais de uma outra ligação de entrada.
R/W	Read/Write, Ler/Escrever
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)
SNTP	Simple Network Time Protocol (RFC 1769)
SRS	System.Rack.Slot Endereçamento de um módulo
SW	Software
TMO	Timeout
W	Write
Watchdog (WD)	Supervisão de tempo para módulos ou programas. O ultrapassar o tempo do watchdog, o módulo ou programa entre em parada por erro.
WDT	Tempo de watchdog

Lista de figuras

Lista de tabelas

Remetente:

Empresa:

Nome:

Dept.:

Endereço:

Telefone:

HIMA Paul Hildebrandt GmbH
Automação industrial
Documentação
Postfach 1261

68777 Brühl

Prezados leitores,

tomamos todos os cuidados possíveis para manter os nossos manuais o mais atualizado possível e para evitar erros. Porém, se encontrou erros neste manual ou queria fazer sugestões de melhoria, também dos produtos HIMA, somos muito agradecidos pela sua contribuição.

Utilize esta página ou uma cópia dela para o envio por correio ou fax.

(Fax 0049 6202 709 199)

Assunto: Funções do sistema operacional H41q/H51q

HIMA Paul Hildebrandt GmbH
Automação industrial
Postfach 1261 • 68777 Brühl
Telefone: 0049 (6202) 709-0 • Fax: (06202) 709-107
E-mail: info@hima.com • Internet: www.hima.com

(1045)