HIMatrix

Sistema de control relacionado con la seguridad

Manual de seguridad

HIMA Paul Hildebrandt GmbH
Automatización Industrial

Rev. 2.00

HI 800 427 S

Todos los productos de HIMA nombrados en el presente manual son marcas registradas. Salvo donde se indique lo contrario, esto se aplicará también a los demás fabricantes aquí citados y a sus productos.

Tras haber sido redactadas concienzudamente, las notas y las especificaciones técnicas ofrecidas en este manual han sido compiladas bajo estrictos controles de calidad. En caso de dudas, consulte directamente a HIMA. HIMA le agradecerá que nos haga saber su opinión acerca de p.ej. qué información falta en el manual.

Reservado el derecho a modificaciones técnicas. HIMA se reserva asimismo el derecho de actualizar el material escrito sin previo aviso.

Hallará más información en la documentación recogida en el DVD de HIMA y en nuestro sitio web http://www.hima.com.

Contacto

Dirección de HIMA:

HIMA Paul Hildebrandt GmbH

Apdo. Postal / Postfach 1261

D-68777 Brühl

Tel: +49 6202 709-0

Fax: +49 6202 709-107

E-Mail: info@hima.com

Índice de revisión	Modificaciones	Tipo de modificación	
		técnica	redaccional
2.00	Edición en español (traducción)		

Índice de contenidos

1 Manual de seguridad

Este manual contiene información sobre el uso conforme a la finalidad prevista de los dispositivos de automatización HIMatrix con función relacionada con la seguridad.

El montaje y la puesta en servicio sin peligros, así como la seguridad en el funcionamiento y el mantenimiento de los sistemas de automatización HIMatrix, requiere:

- Conocimiento de las normativas.
- Implementación técnicamente correcta por parte de personal cualificado de las instrucciones de seguridad contenidas en este manual.

En los siguientes casos pueden producirse situaciones de serio peligro para las personas, los bienes materiales y el medio ambiente a causa de fallos o del menoscabo de las funciones de seguridad, declinando HIMA toda responsabilidad en tales supuestos:

- En caso de intervenir personas no cualificadas en los dispositivos.
- En caso de desactivar o eludir (puentear) funciones de seguridad.
- En caso de no observar las indicaciones de este manual.

HIMA proyecta, fabrica y pone a prueba los sistemas de automatización HIMatrix cumpliendo las pertinentes normas de seguridad. Para hacer uso de los dispositivos tendrán que cumplirse todos los requisitos siguientes:

- Solo para los casos de aplicación previstos descritos.
- Solo en las condiciones ambientales especificadas.
- Solo en combinación con dispositivos autorizados de otros fabricantes.

Por razones de claridad, este manual no recoge todos los detalles de los diversos modelos de dispositivos de automatización HIMatrix. Encontrará información más detallada en sus respectivos manuales.

1.1 Estructuración y uso de la documentación

Este manual de seguridad contiene los siguientes temas:

- Uso conforme a la finalidad prevista
- Concepto de seguridad
- Funciones centrales
- Entradas
- Salidas
- Software
- Aspectos de seguridad instrumentada para el programa de usuario
- Configuración de la comunicación
- Uso en centrales de alarma de incendios
- Anexo:
  - Aumento del nivel SIL de sensores y actuadores
  - Glosario
  - Índices

En el manual se distingue entre las siguientes variantes del sistema HIMatrix:

Utilidad de programación	Sistema operativo del procesador	Sistema operativo de comunicación	Layout del hardware
SILworX	A partir de V.8	A partir de V.13	L3
SILworX	A partir de V.7	A partir de V.12	L2
ELOP II Factory	Hasta V.7	Hasta V.12	L2

Tabla 1: Variantes del sistema HIMatrix

Los sistemas operativos para dispositivos con layout 3 de hardware no valen para dispositivos con layout 2 de hardware y viceversa.

Los dispositivos con layout de hardware L3 tienen en comparación con dispositivos con layout de hardware L2, incluso con idéntica versión de sistema operativo, funciones ampliadas tales como p.ej. Multitasking, Reload. Dichas funciones ampliadas se identifican en el texto o los epígrafes de capítulo de este documento mediante “L3”.

En este manual las variantes se distinguen mediante:

- Subcapítulos separados
- Tablas diferenciadoras de las versiones p.ej. “A partir de V.7”, “Hasta V.7”

i **¡Los proyectos creados con ELOP II Factory no podrán editarse en SILworX y viceversa!**

i Se denominarán como *“devices”* los sistemas de control compactos y las E/S remotas, mientras que las tarjetas de un sistema de control modular se denominarán como *“modules”*.

En SILworX se denomina *modules* a los módulos.

1.2 Destinatarios

Este documento va dirigido a planificadores, proyectadores y programadores de equipos de automatización y al personal autorizado para la puesta en servicio, operación y mantenimiento de dispositivos y sistemas. Se presuponen conocimientos especiales en materia de sistemas de automatización con función relacionada con la seguridad.

1.3 Convenciones de representación

Para una mejor legibilidad y comprensión, en este documento se usa la siguiente notación:

Negrita	Remarcado de partes importantes del texto. Designación de botones de software, fichas e ítems de menús de la utilidad de programación sobre los que puede hacerse clic.
Cursiva	Parámetros y variables del sistema
`Courier`	Entradas literales del operador
RUN	Designación de estados operativos en mayúsculas
Cap. 1.2.3	Las referencias cruzadas son enlaces, aun cuando no estén especialmente marcadas como tales. Al colocar el puntero sobre un enlace, cambiará su aspecto. Haciendo clic en él, se saltará a la correspondiente página del documento.

Las notas de seguridad y uso están especialmente identificadas.

1.3.1 Notas de seguridad

Las notas de seguridad del documento se representan de la siguiente forma.
Para garantizar mínimos niveles de riesgo, deberá seguirse sin falta lo que indiquen.
Los contenidos se estructuran en

- Palabra señalizadora: peligro, advertencia, precaución, nota
- Tipo y fuente de peligro
- Consecuencias del peligro
- Prevención del peligro

⚠ PALABRA SEÑALIZADORA

¡Tipo y fuente de peligro!
Consecuencias del peligro
Prevención del peligro

Las palabras señalizadoras significan

- Peligro: su inobservancia originará lesiones graves o mortales
- Advertencia: su inobservancia puede originar lesiones graves o mortales
- Precaución: su inobservancia puede originar lesiones moderadas
- Nota: su inobservancia puede originar daños materiales

NOTA

¡Tipo y fuente del daño!
Prevención del daño

1.3.2 Notas de uso

La información adicional se estructura como sigue:

i En este punto figura el texto con la información adicional.

Los trucos y consejos útiles aparecen en la forma:

SUGERENCIA En este punto figura el texto con la sugerencia.

2 Notas relativas al uso

En ningún caso omita leer las siguientes informaciones de seguridad, las notas y las instrucciones de este manual. Use el producto cumpliendo siempre todas las directivas y las directrices de seguridad.

2.1 Uso conforme a la finalidad prevista

2.1.1 Ámbito de aplicación

Los sistemas de control HIMatrix con función relacionada con la seguridad podrán usarse hasta el nivel de integridad de seguridad SIL 3 según IEC 61508. En aplicaciones ferroviarias también SIL 4 según EN 50126, EN 50128 y EN 50129 véase el manual de seguridad para las aplicaciones ferroviarias.

Los sistemas HIMatrix están certificados para sistemas de control de procesos, sistemas de protección, control de quemadores y control de máquinas.

Si la comunicación relacionada con la seguridad tiene lugar entre diversos dispositivos, deberá observarse que el tiempo total de reacción del sistema no sobrepase el tiempo de tolerancia a errores. Deberán seguirse los principios de cálculo indicados en el capítulo “Comunicación”.

A las interfaces de comunicación deberán conectarse solamente dispositivos que garanticen una separación eléctrica segura.

Principio de corriente de reposo y principio de corriente de trabajo

Los dispositivos de automatización han sido diseñados para el principio de corriente de reposo.

Un sistema que funciona según el principio de corriente de reposo no necesita energía para ejecutar su función de seguridad (*“de-energize to trip”*).

En caso de fallo, las señales de entrada y salida adoptan como estado seguro su estado sin excitar, es decir, sin corriente ni tensión.

Los sistemas de control HIMatrix pueden usarse igualmente en aplicaciones que funcionen según el principio de corriente de trabajo.

Un sistema que funciona según el sistema de corriente de trabajo necesita energía (p.ej. eléctrica o neumática) para ejecutar su función de seguridad (*“energize to trip”*).

Al concebir el sistema de control habrá que tener en cuenta las exigencias de las normas de aplicación, siendo p.ej. obligatorio un diagnóstico de cables de las entradas y salidas.

Uso en centrales de alarma de incendios

Los sistemas HIMatrix equipados con detección de cortocircuito e interrupción de cable están homologados y certificados según DIN EN 54-2 y NFPA 72 para centrales de alarma de incendios. Estos sistemas deberán poder adoptar su estado activo cuando se requiera, para poder dominar los peligros emergentes.

¡Deben respetarse las condiciones de uso!

2.1.2 Uso no conforme a la finalidad prevista

Para considerar admisible la transmisión de datos relevantes de seguridad a través de redes públicas (p.ej. internet) se deberán tomar medidas adicionales para aumentar el grado de seguridad (p.ej. túnel de red privada virtual, Firewall, etc.).

Con las interfaces de bus de campo no es posible la comunicación relacionada con la seguridad.

2.2 Condiciones de uso

Se permite usar los sistemas HIMatrix solamente bajo condiciones ambientales que no excedan las citadas a continuación.

Los sistemas HIMatrix han sido diseñados de forma que cumplan las exigencias de las siguientes normas en materia de compatibilidad electromagnética, clima y medioambiente:

Norma	Contenido
EC/EN 61131-2: 2006	PLCs, Parte 2 Características exigidas a los equipos de trabajo y ensayos
IEC/EN 61000-6-2: 2005	CEM Norma básica, Parte 6-2 Inmunidad a interferencias, entorno industrial
IEC/EN 61000-6-4: 2006	Compatibilidad electromagnética (CEM) Norma básica de emisión de interferencias, entorno industrial

Tabla 2: Normas de compatibilidad electromagnética, clima y medio ambiente

Para hacer uso de los sistemas de control HIMatrix con función relacionada con la seguridad deben cumplirse las siguientes condiciones generales:

Tipo de condición	Contenido de la condición
Clase de protección	Clase de protección II según IEC/EN 61131-2
Polución	Grado de polución II según IEC/EN 61131-2
Altitud	< 2000 m
Carcasa	Estándar: IP20 Si las normas de aplicación pertinentes (p.ej. EN 60204, EN 15849) así lo exigen, el sistema HIMatrix deberá montarse en una carcasa del grado de protección exigido (p.ej. IP54).

Tabla 3: Condiciones generales

2.2.1 Condiciones climáticas

Los ensayos más relevantes y los valores límite para las condiciones climáticas se relacionan en la siguiente tabla:

IEC/EN 61131-2	Ensayos climáticos
	Temperatura de trabajo: 0…+60 °C (límites de ensayo: -10…+70 °C)
	Temperatura de almacenamiento: -40…+85 °C
	Frío y calor secos, ensayos de durabilidad: +70 °C/-25 °C, 96 h, acometida de corriente no conectada
	Variaciones de temperatura, ensayos de durabilidad e inmunidad: -40 °C/+70 °C y 0 °C/+55 °C, Acometida de corriente no conectada
	Ciclos con calor húmedo, ensayos de durabilidad: +25 °C/+55 °C, 95% de humedad relativa Acometida de corriente no conectada

Tabla 4: Condiciones climáticas

Condiciones de uso que difieran de estas se citarán en los manuales de los dispositivos o los módulos.

2.2.2 Condiciones mecánicas

Los ensayos más relevantes y los valores límite para las condiciones mecánicas se relacionan en la siguiente tabla:

IEC/EN 61131-2	Ensayos mecánicos
	Ensayo de inmunidad frente a vibraciones: 5…9 Hz/3,5 mm 9...150 Hz, 1 g, probeta en funcionamiento, 10 ciclos por eje
	Ensayo de inmunidad frente a choques: 15 g, 11 ms, probeta en funcionamiento, 3 choques por eje (18 choques)

Tabla 5: Ensayos mecánicos

2.2.3 Condiciones de CEM

Para los sistemas con función relacionada con la seguridad se exigen altos niveles frente a interferencias. Los sistemas HIMatrix cumplen estas exigencias según IEC 62061 e IEC 61326-3-1. Véase la columna *Criterio FS* (seguridad funcional).

IEC/EN 61131-2	Ensayos de inmunidad a interferencias	Criterio FS
IEC/EN 61000-4-2	Ensayos de ESD: 6 kV de descarga por contacto, 8 kV al aire	6 kV, 8 kV
IEC/EN 61000-4-3	Ensayos de RFI (10 V/m): 80 MHz…2 GHz, 80% AM Ensayos de RFI (3 V/m): 2 GHz…3 GHz, 80% AM: Ensayos de RFI (20 V/m): 80 MHz…1 GHz, 80% AM	- - 20 V/m
IEC/EN 61000-4-4	Ensayos de ráfagas: alimentación a 2 kV, líneas de señal de 1 kV	4 kV 2 kV
IEC/EN 61000-4-12	Ensayo con vibraciones atenuadas: 2,5 kV CM 1 kV DM	-
IEC/EN 61000-4-6	Alta frecuencia, asimétrica: 10 V, 150 kHz…80 MHz, AM 20 V, 150 kHz…80 MHz, AM: EN 298	 10 V
IEC/EN 61000-4-3	Impulsos de 900 MHz	-
IEC/EN 61000-4-5	Tensión transitoria: alimentación a 2 kV CM, 1 kV DM Líneas de señal: 2 kV CM, 1 kV DM para E/S de CA	2 kV/1 kV 2 kV

Tabla 6: Ensayos de inmunidad a interferencias

IEC/EN 61000-6-4	Ensayos de emisión de interferencias
EN 55011 Clase A	Emisión de interferencias: irradiada, vinculada al cable

Tabla 7: Ensayos de emisión de interferencias

2.2.4 Fuente de alimentación

Las homologaciones más relevantes y los valores límite para fuentes de alimentación de sistemas HIMatrix se relacionan en la siguiente tabla:

IEC/EN 61131-2	Evaluación de las características de la fuente de corriente continua
	La fuente de alimentación debe cumplir las siguientes normas: IEC/EN 61131-2: SELV (Safety Extra Low Voltage) o PELV (Protective Extra Low Voltage)
	Los cortacircuitos que se usen en los sistemas HIMatrix deberán responder a lo especificado en este manual.
	Ensayo del rango de tensiones: 24 V CC, -20%…+25% (19,2 V…30,0 V)
	Ensayo de inmunidad contra breves interrupciones de la fuente de alimentación externa: CC, PS 2: 10 ms
	Inversión de polaridad de la fuente de alimentación: Hallará notas al respecto en el correspondiente capítulo del manual del sistema o en la hoja de características de la fuente de alimentación.

Tabla 8: Evaluación de las características de la fuente de corriente continua

2.2.5 Precauciones contra descargas electrostáticas

Las modificaciones o ampliaciones del sistema, así como la sustitución de módulos, únicamente deberán ser realizas por personal con conocimientos sobre medidas de protección contra descargas electrostáticas.

NOTA

¡Las descargas electrostáticas pueden dañar los componentes electrónicos utilizados en los sistemas HIMatrix!

- **Realice estas tareas en un lugar de trabajo antiestático y llevando una cinta de puesta a tierra.**
- **Guarde bien protegidos electrostáticamente (p.ej. en su embalaje original) los módulos que no tenga en uso.**

2.3 Responsabilidades de fabricantes de máquinas y empresas usuarias

Los fabricantes de máquinas/sistemas y la empresa que los usa son responsables de velar por la segura aplicación de los sistemas HIMatrix en plantas de automatización y en plantas globales.

La correcta programación de los sistemas HIMatrix deberá estar suficientemente validada por los fabricantes de máquinas y sistemas.

2.4 Otros documentos del sistema

Para proyectar sistemas HIMatrix se dispone además de los siguientes documentos:

Nombre	Aplicable	Contenido	Documento Nº	Nº de Ref.
Manual de sistema HIMatrix para sistemas compactos	Todas las versiones	Descripción de los sistemas compactos y datos técnicos	HI 800 495 S	Archivo PDF
Manual de sistema HIMatrix para sistema modular F60	Todas las versiones	Descripción del sistema modular F60 y sus datos técnicos	HI 800 494 S	Archivo PDF
Informe de ensayos para el certificado [1)]	Todas las versiones	Principios de ensayos, requisitos de seguridad, resultados		96 9000104
Manual de comunicación de SILworX (configuración con SILworX)	A partir de S.Op V.7 de CPU	Descripción de los protocolos de comunicación, ComUserTask y forma de proyectarlo en SILworX	HI 801 195 S	Archivo PDF
Ayuda directa en pantalla de SILworX	A partir de S.Op V.7 de CPU	Manejo de SILworX	-	-
Ayuda directa en pantalla de ELOP II Factory	Hasta S.Op. V.7 de CPU	Manejo de ELOP II Factory, protocolo IP Ethernet, protocolo INTERBUS	-	-
Manual de primeros pasos de SILworX	A partir de S.Op V.7 de CPU	Introducción a SILworX	HI 801 194 S	Archivo PDF
Manual de primeros pasos de ELOP II Factory	Hasta S.Op. V.7 de CPU	Introducción a ELOP II Factory	HI 800 496 CSA	Archivo PDF 96 9000013
[1)] Se suministra solamente junto con un sistema HIMatrix				

Tabla 9: Documentación de sistema HIMatrix

Hallará información más detallada sobre los dispositivos y los módulos en sus respectivos manuales.

3 Concepto de seguridad para el uso del PES

Este capítulo trata sobre importantes cuestiones generales de la seguridad funcional de los sistemas HIMatrix:

- Seguridad y disponibilidad
- Tiempos importantes para la seguridad
- Ensayo de prueba
- Obligaciones de seguridad
- Certificación

3.1 Seguridad y disponibilidad

Los sistemas HIMatrix están certificados para su uso en sistemas de control de procesos, sistemas de protección, control de quemadores y control de máquinas.

De los sistemas HIMatrix no se desprende ningún peligro inmediato.

⚠ PELIGRO

¡Daños personales debido a sistemas de automatización con función relacionada con la seguridad mal conectados o mal programados!

Antes de la puesta en servicio, compruebe las conexiones y pruebe todo el sistema.

3.1.1 Cálculos de PFD y PFH

Para los sistemas HIMatrix se realizaron los cálculos de PFD y PFH según IEC 61508.

IEC 61508-1 establece para SIL 3 un PFD de 10^{-4}…10^{-3} y un PFH de 10^{-8}…10^{-7} por hora.

Para el sistema de control programable (PES) se supone un 15% del valor límite dispuesto por la norma para PFD y PFH. Así, como valor límite para la parte del sistema de control resulta: PFD = $1{,}5*10^{-4}$ y PFH = $1{,}5*10^{-8}$ por hora.

El intervalo para el ensayo de prueba recurrente de los sistemas HIMatrix se establece en 10 años, mientras que para E/S remotas y módulos con salidas de relés el período será de 3 años (Offline Proof Test, ver IEC 61508-4, párrafo 3.8.5).

3.1.2 Autocomprobación y diagnóstico de errores

El sistema operativo de los sistemas de control realiza extensas autocomprobaciones durante el inicio y durante el funcionamiento. En estas se comprueban, sobre todo:

- Los procesadores
- Las áreas de memoria (RAM y memoria no volátil)
- El WatchDog
- Los distintos canales de E/S

Si en dichas comprobaciones se detectan errores, el sistema operativo desactivará el módulo defectuoso, la E/S remota afectada o el canal de E/S defectuoso.

En el caso de un sistema sin redundancia, esto puede llevar a que se desactiven funciones parciales o todo el sistema programable PES.

Todos los módulos y los dispositivos HIMatrix disponen de LEDs propios para indicar los errores detectados. De esta forma, en caso de fallo podrá realizarse un rápido diagnóstico de errores del circuito externo o de un dispositivo detectado como defectuoso.

Además, el programa de usuario podrá evaluar diversas variables o señales del sistema que indican el estado de dispositivos y módulos.

Un completo registro de diagnóstico del comportamiento del sistema y de los errores detectados se guardará en la memoria de diagnóstico del sistema de control. Dicho registro podrá leerse mediante PADT aun tras un fallo del sistema.

Hallará información más detallada sobre la evaluación de los mensajes de diagnóstico en el manual de sistemas compactos HI 800 495 S o en el manual de sistemas modulares HI 800 494 S, en el capítulo *"Diagnóstico"*.

En un porcentaje sumamente reducido de fallos de componentes que no afectan a la seguridad, el sistema HIMatrix no generará información de diagnóstico.

3.1.3 PADT

El usuario crea su programa de aplicación y configura el sistema de control mediante PADT. El concepto de seguridad de PADT ayuda al usuario a implementar correctamente las tareas de control. PADT toma toda una serie de medidas para comprobar los datos introducidos por el usuario.

PADT es un PC que tiene instalada la utilidad de planificación.

Para el sistema HIMatrix se dispone de dos utilidades de planificación, según la versión del sistema operativo instalado en el sistema de control:

- Con un sistema operativo a partir de la versión 7 deberá usarse SILworX.
- Con un sistema operativo previo a la versión 7 deberá usarse ELOP II Factory.

3.1.4 Montaje de sistemas de seguridad por principio de corriente de trabajo

Los sistemas de seguridad que funcionan según el principio de corriente de trabajo ("energize to trip"), p.ej. alarmas de incendios, tienen los siguientes "estados seguros":

1. Estado seguro tras desactivar el equipo.
2. Estado que se adopta por requerimiento, es decir, al ejecutar la función de seguridad. En tal caso se activará p.ej. un actuador.

Al montar un sistema de seguridad que actúe según el principio de corriente de trabajo deberá prestarse atención a lo siguiente:

- Garantizar la ejecución de la función de seguridad en caso de peligro.
- Detección de componentes del sistema que hayan fallado y reacción:
  - Notificación de la disfunción.
  - Conmutación automática a componentes redundantes, de ser necesario y posible.

Garantizar la función de seguridad

El planificador deberá asegurarse de que el sistema de seguridad pueda ejecutar su función de seguridad en caso de peligro. La ejecución de dicha función consiste en que el sistema de seguridad haga llegar corriente de excitación ("energize") a uno o más actuadores, de forma que como consecuencia de ello se adopte un estado seguro, p.ej. cerrando una puerta cortafuegos.

Para garantizar que la función de seguridad se ejecutará, es posible que deban implementarse redundantemente estos componentes del sistema de seguridad:

- Fuente de alimentación del sistema de control.
- Componentes del sistema de control: sistemas de control compactos HIMatrix, módulos, E/S remotas.
- Para las salidas de relés, HIMA recomienda implementar redundantemente estas y la fuente de alimentación de los actuadores.
  Motivo:
  - Una salida de relé no tiene monitoreo de cable.
  - Puede ser necesario para satisfacer el nivel SIL requerido.

Deberá hacerse que, siempre que se pierda la redundancia, se realice a la mayor brevedad posible la reparación de los componentes que hayan fallado.

Una implementación redundante de los componentes del sistema de seguridad no será necesaria cuando la seguridad requerida en caso de disfunción del sistema de seguridad pueda garantizarse mediante otras medidas, p.ej. de tipo organizativo.

Detección de componentes que hayan fallado

El sistema de seguridad detecta si hay componentes fuera de servicio. Esto se logra mediante

- Autocomprobaciones de los componentes HIMatrix.
- Monitoreo de interrupciones de cable y cortocircuitos en los módulos de entrada/salida. Deberán parametrizarse.
- Entradas adicionales de monitoreo de actuadores, en la medida necesaria para el proyecto.

El programa de usuario deberá ser capaz de procesar los respectivos estados de error y activar los componentes redundantes.

3.2 Tiempos importantes para la seguridad

Son:

- Tiempo de tolerancia de errores (Fault Tolerance Time)
- Tiempo de WatchDog (Watchdog Time)
- Tiempo de seguridad (Safety Time)
- Tiempo de reacción (Response Time)

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

El tiempo de tolerancia de errores (FTT) es una característica del proceso y describe el período durante el cual el proceso podrá soportar señales erróneas sin que por ello se produzca un estado peligroso.

3.2.2 Tiempo de seguridad del sistema PES

El tiempo de seguridad es el tiempo en el que el sistema programable PES deberá reaccionar (en estado RUN) tras producirse un error interno.

Desde el punto de vista del proceso, el tiempo de seguridad es el tiempo máximo antes del cual el sistema de seguridad deberá reaccionar a una modificación de la señales de entrada activando las respectivas salidas (Response Time).

Versión de sistema operativo	Tiempo de seguridad dentro del rango
A partir de S.Op V.7 de CPU	20…22 500 ms
Hasta S.Op. V.7 de CPU	20…50 000 ms

Tabla 10: Rango de valores del tiempo de seguridad

3.2.3 Tiempo de seguridad del programa de usuario para L3

El tiempo de seguridad (Safety Time) del programa del usuario no es posible ajustarlo directamente. HIMatrix calcula el tiempo de seguridad de un programa de usuario a partir de los parámetros *Max. Safety Time* del recurso y *Maximum Number of Cycles*. Hallará más información en el capítulo 8.2.9.

3.2.4 MOT (Multiple Fault Occurrence Time)

El tiempo de ocurrencia de errores múltiples, MOT, es el período de tiempo en el que será suficientemente pequeña la probabilidad de que se produzcan errores múltiples que, combinados, pueden ser críticos para la seguridad.

El tiempo de ocurrencia de errores múltiples está definido como 24 h en el S.Op.

3.2.5 Tiempo de reacción

El tiempo máximo de reacción (Response Time) de sistemas de control HIMatrix que funcionen cíclicamente será el doble del tiempo de ciclo de tales sistemas, salvo que se produzcan retardos debido a la parametrización o la lógica del programa del usuario.

El tiempo de ciclo de un sistema de control consta básicamente de:

- Lectura de las entradas
- Ejecución del programa de usuario
- Escritura de las salidas
- Comunicación de datos de proceso
- Ejecución de las rutinas de autocomprobación

Además, teniendo en cuenta el peor supuesto posible para todo el sistema, deberán tomarse en consideración los tiempos de conmutación de las entradas y las salidas.

3.2.6 Tiempo de WatchDog del sistema procesador

El tiempo de WatchDog se define como tiempo en el menú de configuración de propiedades del sistema PES. Es la máxima duración admisible de un ciclo RUN (tiempo de ciclo). Si el tiempo de ciclo sobrepasa el tiempo de WatchDog definido, el sistema se desactivará. A continuación el sistema se reiniciará si se tiene parametrizada la función Autostart. Si no se tiene parametrizada la función Autostart, el sistema adoptará el estado STOP/VALID CONFIGURATION.

El tiempo de WatchDog del sistema procesador podrá elegirse como:
≤ ½ * tiempo de seguridad del sistema PES.

Versión de sistema operativo	Rango de valores para el tiempo de WatchDog	Valor por defecto de los sistemas de control	Valor por defecto de E/S remotas
En L3 (a partir de S.Op. V.8 de CPU)	4…5000 ms	200 ms	100 ms
A partir de S.Op V.7 de CPU	8…5000 ms	200 ms	100 ms
Hasta S.Op. V.7 de CPU	2…5000 ms	50 ms	10 ms

Tabla 11: Rango de valores del tiempo de WatchDog

3.2.7 Tiempo de WatchDog del programa del usuario para L3

Cada programa de usuario tiene WatchDog y tiempo de WatchDog propios.

El tiempo de WatchDog del programa del usuario no es posible ajustarlo directamente. HIMatrix L3 calcula el tiempo de Watchdog de un programa de usuario a partir de los parámetros *Max. Watchdog Time* del recurso y *Maximum Number of Cycles*.

Deberá observarse que el tiempo de WatchDog calculado sea como máximo tan grande como el tiempo de reacción resultante exigido para la parte del proceso de la que se ocupa el programa del usuario.

3.3 Ensayo de prueba

Un ensayo de prueba es una prueba que sirve para descubrir errores ocultos en un sistema de seguridad instrumentada, de forma que el sistema, de ser necesario, pueda volver a ponerse en un estado que le permita cumplir sus funciones.

Los sistemas de seguridad de HIMA deben someterse a un ensayo de prueba recurrente cada 10 años. Mediante un análisis por cálculo de los circuitos de seguridad implementados suele poder prolongarse dicho intervalo.

En el caso de las E/S remotas y los módulos con salidas de relés, el ensayo de prueba recurrente para los relés deberá realizarse a intervalos fijos.

3.3.1 Realización del ensayo de prueba

La realización de los ensayos de prueba dependerá de cómo esté constituido el equipo o la instalación a controlar (EUC = equipment under control) y de cuál sea su potencial de riesgo, así como de las normas que encuentren aplicación para el funcionamiento del equipo y las instancias oficiales de inspección como base para su homologación.

Según las normas IEC 61508 1-7, IEC 61511 1-3, IEC 62061 y VDI/VDE 2180, hojas 1 a 4, la realización de los ensayos de prueba es responsabilidad del usuario de los sistemas con función relacionada con la seguridad.

3.3.2 Frecuencia de los ensayos de prueba

El sistema de control HIMatrix podrá someterse a un ensayo de prueba recurrente comprobando para ello todo el circuito de seguridad.

En la práctica se exige un intervalo más corto para el ensayo de prueba recurrente en los dispositivos de campo de entrada y salida (p.ej. cada 6 ó 12 meses) que la exigida para el sistema de control HIMatrix. Si el usuario comprueba todo el circuito de seguridad debido al dispositivo de campo, el sistema de control HIMatrix estará automáticamente incluido en dicha prueba y no se requerirán ensayos de prueba recurrentes adicionales para el sistema de control HIMatrix.

Si en el ensayo de prueba recurrente de los dispositivos de campo no se incluye el sistema de control HIMatrix, el nivel SIL 3 de este deberá comprobarse como mínimo cada 10 años. Ello podrá realizarse reiniciando el sistema de control HIMatrix.

Si para dispositivos especiales rigen exigencias normativas adicionales de ensayo de prueba, deberá observarse lo indicado en el manual del dispositivo dado.

3.4 Obligaciones de seguridad

Para usar sistemas programables PES relacionados con la seguridad del sistema HIMatrix rigen las siguientes obligaciones de seguridad:

3.4.1 Proyecto del hardware

Las personas que elaboren el proyecto del hardware HIMatrix deberán observar las siguientes condiciones de seguridad de obligado cumplimiento.

Obligaciones no dependientes del producto

- Para el funcionamiento relacionado con la seguridad podrá emplearse únicamente el hardware y el software a prueba de fallos homologado a tal fin. El hardware y el software homologados se especifican en la lista de versiones de módulos y de firmware de los sistemas HIMatrix de la casa HIMA Paul Hildebrandt GmbH, Nº de Certificado 968/EZ 128.19/09 *(Version List of Devices and Firmware of HIMatrix Systems of HIMA Paul Hildebrandt GmbH, Certificate-No. 968/EZ 128.19/09).*
  Las correspondientes versiones actuales figuran en la lista de versiones realizada junto con el organismo oficial de inspección.
- Deberán cumplirse las condiciones de uso especificadas (ver capítulo 2.2) en lo relativo a la compatibilidad electromagnética y los factores mecánicos, químicos y climáticos.
- Para procesar señales no relevantes para la seguridad podrá usarse hardware y software que no sea a prueba de fallos, pero que no cause repercusiones en el resto del sistema. No se permite hacerlo para las unidades que deban ejecutar tareas de seguridad instrumentada.
- En todos los circuitos de corriente de seguridad conectados externamente al sistema deberá cumplirse el principio de corriente de reposo.

Obligaciones dependientes del producto

- Al sistema se conectarán solamente dispositivos que dispongan de una separación segura de la red eléctrica.
- La separación eléctrica segura de la alimentación deberá tener lugar en la fuente de 24 V del sistema. Se permite usar únicamente adaptadores de alimentación del tipo PELV o SELV.

3.4.2 Programación

Las personas que creen el programa de usuario deberán observar las siguientes condiciones de obligado cumplimiento.

Obligaciones no dependientes del producto

- En las aplicaciones con relevancia de seguridad deberá prestarse atención a la correcta parametrización de las magnitudes del sistema relevantes para la seguridad.
- Deberá prestarse atención especialmente a la configuración del sistema, la máxima duración del ciclo y el tiempo de seguridad.

Obligaciones dependientes del producto

Condiciones obligatorias para hacer uso de la utilidad de programación

- Para la programación deberá usarse la siguiente utilidad:
  - **SILworX** para versiones de sistema operativo del procesador a partir de V.7.
  - **ELOP II Factory** para versiones de sistema operativo del procesador hasta V.7.
- Tras crear la aplicación deberá realizarse un compilado doble manual y comparar los valores CRC para asegurarse de que la compilación se ha realizado correctamente.
- **La correcta implementación de lo especificado para la aplicación habrá de validarse y verificarse. Deberá realizarse una verificación completa poniendo a prueba la lógica.**
- Deberá repetirse este procedimiento cada vez que se modifique la aplicación.
- La reacción del sistema a errores en E/S remotas y módulos de salida/entrada a prueba de fallos deberá definirse con el programa de usuario de acuerdo a las circunstancias de seguridad instrumentada específicas del equipo o la instalación a controlar.

3.4.3 Comunicación

- Si se usa la comunicación relacionada con la seguridad entre diversos dispositivos, deberá observarse que el tiempo total de reacción del sistema no exceda el tiempo de tolerancia a errores. Siga los principios de cálculo indicados en el cap. 9.2.
- No se permite transmitir datos con relevancia de seguridad por redes públicas (p.ej. internet), salvo que se tomen medidas de seguridad adicionales, p.ej. túnel de red privada virtual.
- Si la transmisión tiene lugar a través de redes internas de la empresa o la planta, deberán tomarse las medidas técnicas y administrativas necesarias para impedir posibles manipulaciones (p.ej. resguardando con Firewall la parte con relevancia de seguridad frente a otras redes).
- Para transmitir datos con relevancia de seguridad no se permite usar protocolos estándar.
- A todas las interfaces de comunicación deberán conectarse solamente dispositivos que garanticen una separación eléctrica segura.

3.4.4 Intervenciones de mantenimiento

- Para las intervenciones de mantenimiento observe la correspondiente versión actual del documento “Maintenance Override” de TÜV Renania y TÜV Product Service.
- De ser necesario, el usuario deberá definir medidas administrativas para proteger el acceso a los sistemas tras consultarlo a los organismos oficiales de homologación.

3.5 Certificación

Los dispositivos de automatización HIMA con función relacionada con la seguridad (sistemas electrónicos programables, PES) del sistema HIMatrix han sido probados según las normas de seguridad funcional citadas a continuación y certificados por el organismo de inspección TÜV como conformes con CE:

3.5.1 Certificado TÜV

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

Certificado e informe de pruebas número 968/EZ 128.19/09
Dispositivos de automatización relacionados con la seguridad
HIMatrix F60, F35, F31, F30, F20, RIO-NC

Normas internacionales:		
EN / IEC 61508, Partes 1–7: 2000		SIL 3
EN / IEC 61511: 2004		SIL 3
EN / ISO 13849-1: 2008		Performance level e
EN / IEC 62061: 2005		
EN 50156-1: 2006		SIL 3
EN 12067-2: 2004		
EN 298: 2004		
EN 230: 2005		
NFPA 85: 2007		
NFPA 86: 2007		
EN / IEC 61131-2: 2007		
EN / IEC 61000-6-2: 2005		
EN 61000-6-4: 2007		
EN 54-2: 1997 + A1:2007	F20, F30, F31, F35, F60, F3 AIO 8/4 01, F3 DIO 16/8 01, F3 DIO 16/8 02, F3 DIO 20/8 01, F3 DIO 8/8 01	
EN 50130-4: 1989 + A1: 1989 +A2: 2003 + Corr. 2003		
NFPA 72: 2007	F20, F30, F31, F35, F60, F3 AIO 8/4 01, F3 DIO 16/8 01, F3 DIO 16/8 02, F3 DIO 20/8 01, F3 DIO 8/8 01	

El capítulo 2.2 especifica detalladamente todas las pruebas realizadas en materia medioambiental y de compatibilidad electromagnética.

Todos los dispositivos llevan marcado el distintivo CE.

3.5.2 Examen de tipo de la CE

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

Examen de tipo de la CE con el número 01/205/0644/09
Gama de sistemas de PLCs de seguridad (PES)
HIMatrix F20, F30, F31, F35, F60, RIO-NC

Normas internacionales:		
EN / IEC 61508, Partes 1–7: 2001		SIL 3
EN / IEC 61511: 2004		
EN ISO 13849-1:2008		
EN 62061: 2005		
EN 50156-1: 2006		SIL 3
EN 12067-2: 2004		
EN 298: 2004		
EN 230: 2005		
EN 61131-2: 2007		
EN 61000-6-2: 2005		
EN 61000-6-4: 2007		
NFPA 85: 2007		
NFPA 86: 2007		
EN 54-2:1997 /A1: 2007	F20, F30, F31, F35, F60, F3 AIO 8/4 01, F3 DIO 16/8 01, F3 DIO 16/8 02, F3 DIO 20/8 01, F3 DIO 8/8 01	
NFPA 72: 2007	F20, F30, F31, F35, F60, F3 AIO 8/4 01, F3 DIO 16/8 01, F3 DIO 16/8 02, F3 DIO 20/8 01, F3 DIO 8/8 01	

4 Funciones centrales

Los sistemas de control y las E/S remotas de los tipos F1…, F2…, F3… son sistemas compactos que no admiten modificaciones.

Los sistemas de control del tipo F60 son sistemas modulares. En estos se pueden usar hasta seis módulos de E/S dentro de un sistema de control, aparte del módulo procesador y el módulo de alimentación.

4.1 Adaptadores de alimentación

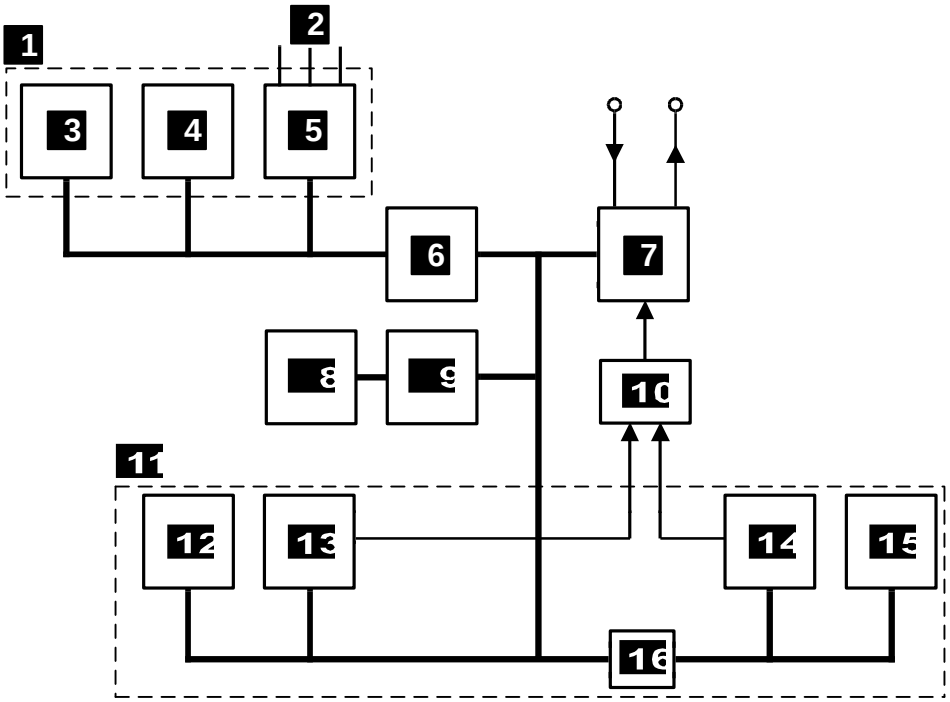
Solamente el F60 tiene un módulo de alimentación. En los sistemas compactos, esta función está integrada en el dispositivo y no puede considerarse modularmente.

El módulo de alimentación PS 01 (para F60) o la función integrada transforma la tensión de alimentación de 24 V CC a 3,3 V CC y 5 V CC (para el bus interno de E/S).

4.2 Descripción funcional del sistema procesador

En el sistema modular F60 el procesador se halla en un módulo propio, mientras que en los sistemas compactos está integrado dentro del sistema de control compacto.

El sistema procesador consta de los siguientes bloques funcionales:



1 Sistema de comunicación
2 Interfaces de comunicación: 2 interf. de bus de campo, switch Ethernet
3 ROM del sistema de comunicación
4 RAM del sistema de comunicación
5 Procesador del sistema de comunicación
6 Dual-Ported RAM
7 Conexión a los módulos de E/S
8 ROM
9 Memoria no volátil (NVRAM)
10 WatchDog
11 Sistema procesador relacionado con la seguridad
12 RAM 1 del sistema procesador
13 Procesador 1 del sistema procesador
14 Procesador 2 del sistema procesador
15 RAM 2 del sistema procesador
16 Comparador

Fig. 1: Representación de bloques funcionales, ejemplo de CPU 01 de F60

Propiedades del módulo procesador CPU 01 de F60

- Dos microprocesadores síncronos (procesador 1 y procesador 2).
- Cada microprocesador tiene su propia memoria RAM.
- Comparador de hardware comprobable para todos los accesos externos de ambos microprocesadores.
- En caso de error, el WatchDog adoptará el estado seguro.
- Flash-EPROM para sistema operativo y programa de usuario, apto para 100 000 ciclos de memoria como mínimo.
- Memoria de datos en NVRAM.
- Multiplexor para conectar bus de E/S, Dual Port RAM (DPR).
- Batería de reserva o Goldcap para fecha y hora.
- Procesador de comunicación para conexiones de bus de campo o Ethernet.
- Interfaz de intercambio de datos entre sistemas de control F3…, F60 y PADT, basado en Ethernet.
- Interfaces opcionales de intercambio de datos por bus de campo.
- Señalización de los estados del sistema mediante LEDs.
- Lógica de bus de E/S para conexión con los módulos de E/S.
- WatchDog seguro (WD).
- Monitoreo de adaptadores de alimentación, comprobable (tensiones de 3,3 V y 5 V CC)

4.3 Autocomprobaciones

Los elementos de autocomprobación detectan diversos errores que podrían causar estados peligrosos y desencadenan reacciones al error dentro de los tiempos de seguridad definidos en el sistema de control, poniendo así las partes erróneas en el estado seguro.

A continuación se explican, por palabras clave, las principales rutinas de autocomprobación de los procesadores con función relacionada con la seguridad de los sistemas de control:

4.3.1 Prueba de microprocesador

Sirve para verificar lo siguiente:

- Todos los tipos de direccionamiento y los comandos empleados.
- La posibilidad de escritura de flags y los comandos condicionados resultantes.
- La posibilidad de escritura y la diafonía de los registros.

4.3.2 Prueba de las áreas de memoria

El sistema operativo, el programa de usuario, las constantes y los parámetros y los datos variables están guardados en áreas de memoria de ambos procesadores y son verificados por un comparador de hardware.

4.3.3 Áreas de memoria aseguradas

Sistema operativo, programa de usuario y rango de parámetros están en sendas memorias. Se aseguran mediante protección contra escritura y comprobación de CRC.

4.3.4 Prueba de RAM

Con una prueba de escritura y lectura se comprueba si hay “stuck-at” o diafonía en las áreas RAM modificables.

4.3.5 Prueba de WatchDog

La señal de WatchDog se desactivará en caso de no ser excitada por ambas CPUs en un intervalo definido, lo mismo que en caso de fallar la prueba del comparador de hardware. Con otra prueba se comprobará la capacidad de desactivarse de la señal de WatchDog.

4.3.6 Prueba del bus de E/S dentro del sistema de control

Se prueba la conexión entre la CPU y las respectivas entradas/salidas (módulos de E/S).

4.3.7 Reacción a errores en el sistema procesador

Un comparador de hardware incluido en el área central compara continuamente que los datos y los comandos del sistema microprocesador 1 sean idénticos a los del sistema microprocesador 2. Si no es así o en las rutinas de autocomprobación se detecta algún error, la señal de WatchDog se desactivará automáticamente. Esto significa que el sistema de control dejará de procesar señales de entrada y las salidas adoptarán el estado desactivado, es decir, sin energía o excitación.

La primera vez que se produzca un error tal, el sistema de control se reiniciará (reboot). Si antes de un minuto tras el reinicio se produce otro error interno, el sistema de control adoptará el estado STOP/INVALID CONFIGURATION y permanecerá en ese estado.

4.4 Diagnóstico de errores

Cada módulo del F60 dispone de un LED propio de indicación de errores en caso de fallos en el módulo o en el circuito externo. De esta forma, en caso de fallo podrá realizarse un rápido diagnóstico de errores de un dispositivo detectado como defectuoso.

En los sistemas compactos F1…, F2…, F3… estos indicadores de error están agrupados en un indicador colectivo de errores.

Adicionalmente, en el programa de usuario podrán evaluarse las diferentes señales de entrada/salida o del sistema de control.

Los errores se señalizarán solamente cuando el error no impida la comunicación con el sistema procesador, es decir, cuando permita aún la evaluación mediante el sistema procesador.

La lógica del programa del usuario puede evaluar los códigos de error de todas las señales de entrada/salida y de las señales del sistema.

Un completo registro de diagnóstico del comportamiento del sistema y de los errores detectados se guardará en la memoria de diagnóstico del procesador y del sistema de comunicación. Dicho registro podrá leerse mediante PADT aun tras un fallo del sistema.

Hallará información más detallada sobre la evaluación de los mensajes de diagnóstico en el manual de sistemas compactos HI 800 495 S o en el manual de sistemas modulares F60, HI 800 494 S, en el capítulo *“Diagnóstico”*.

5 Entradas

Sinopsis de entradas del sistema HIMatrix:

Dispositivo	Tipo	Cantidad de entradas	Relacionadas con la seguridad	Sin repercusiones	Con separación eléctrica
Sistema de control F20	Digital	8	•	•	-
Sistema de control F30	Digital	20	•	•	-
Sistema de control F31	Digital	20	•	•	-
Sistema de control F35	Digital	24	•	•	-
	Contador 24 bits	2	•	•	-
	Analógico	8	•	•	-
E/S remota F1 DI 16 01	Digital	16	•	•	-
E/S remota F3 DIO 8/8 01	Digital	8	•	•	-
E/S remota F3 DIO 16/8 01	Digital	16	•	•	-
E/S remota F3 AIO 8/4 01	Analógico	8	•	•	-
E/S remota F3 DIO 20/8 02	Digital	20	•	•	-
Sistema de control modular F60:					
Módulo DIO 24/16 01	Digital	24	•	•	•
Módulo DI 32 01 (config. para Line Control)	Digital	32	•	•	•
Módulo DI 24 01 (110 V)	Digital	24	•	•	•
Módulo CIO 2/4 01	Contador 24 bits	2	•	•	•
Módulo AI 8 01	Analógico	8	•	•	•
Módulo MI 24 01	Analógico o digital	24	•	•	•

Tabla 12: Sinopsis de entradas del sistema HIMatrix

5.1 Generalidades

Las entradas con función relacionada con la seguridad podrán usarse tanto para señales relacionadas con la seguridad como para señales no relacionadas con la seguridad.

Los sistemas de control transmiten información de errores y de estado como sigue:

- Mediante LEDs de diagnóstico de dispositivos y módulos.
- Mediante señales/variables de sistema evaluables por el programa de usuario.
- Mediante registros en la memoria de diagnóstico que el PADT puede leer.

Los módulos de entrada con función relacionada con la seguridad realizan cíclicamente una autocomprobación de alta calidad durante el funcionamiento. Estas rutinas de comprobación están homologadas por el organismo de inspección TÜV y monitorean el funcionamiento seguro del módulo respectivo.

En caso de error, el sistema de control comunicará al programa de usuario un nivel “low” y, de ser posible, generará información sobre el error (a partir de la versión V.7 del S.Op. de la CPU será el valor inicial predefinido). El programa del usuario podrá evaluar esta información del error leyendo el código del error.

En un porcentaje reducido de fallos de componentes que no afectan a la seguridad, no se generará información de diagnóstico.

5.2 Seguridad de sensores, codificadores y transmisores

En una aplicación con función relacionada con la seguridad, tanto el sistema de control como los sensores, codificadores y transmisores conectados a él deberán cumplir las exigencias normativas de seguridad y el nivel SIL especificado. Véase al respecto “Aumento del nivel SIL de sensores y actuadores” en el anexo.

5.3 Entradas digitales relacionadas con la seguridad

Las propiedades descritas son válidas tanto para los canales de entrada digitales de los módulos del F60 como para los canales de entrada digitales de todos los sistemas compactos, a menos que se indique lo contrario.

5.3.1 Generalidades

Las entradas digitales se leen una vez por ciclo y se guardan internamente, comprobándose su funcionamiento seguro cíclicamente.

Bajo ciertas circunstancias, las señales de entrada que duren menos que el tiempo entre dos exploraciones (es decir, menos que el tiempo de un ciclo) no se captarán.

5.3.2 Rutinas de comprobación

Las rutinas de comprobación on-line verifican que todos los canales de entrada sean capaces de transmitir ambos niveles de señal (LOW y HIGH), independientemente de las señales de entrada actuales. Esta prueba funcional se realiza cada vez que se leen las señales de entrada.

5.3.3 Reacción en caso de error

Si las rutinas de comprobación detectan un error en las entradas digitales, el programa de usuario procesará para el canal defectuoso un nivel “low” de acuerdo al principio de corriente de reposo (“deenergize to trip”).

El programa de usuario deberá tener en cuenta, además del valor de señal del canal, el correspondiente código de error.

Un sistema compacto activará el LED *ERROR*, un módulo F60 el LED *ERR*.

Utilizando el código de error se dispone de posibilidades adicionales de monitorear en el programa de usuario el circuito externo y programar la reacción frente a errores.

Versión	Acceso al código de error	Nombre del código de error
A partir de S.Op V.7 de CPU	En la ficha ...*Channels* de la vista detallada del módulo o dispositivo	*->Error code [Byte]* en la línea del número de canal
Hasta S.Op. V.7 de CPU	En la ventana *Signal Connections…* del módulo o dispositivo	*DI[xx].error code*, *xx* = número de canal

Tabla 13: Códigos de error de las entradas digitales

5.3.4 Picos en entradas digitales

Debido al corto tiempo de ciclo de los sistemas HIMatrix, las entradas digitales podrán leer un impulso pico según EN 61000-4-5 como breve nivel “high”.

Con las siguientes medidas se evitan disfunciones en entornos donde pueden producirse picos:

1. Instalación de cables de entrada apantallados
2. Activación de la inhibición de fallos en el programa de usuario, debiendo una señal estar presente al menos durante dos ciclos antes de ser evaluada.

¡La inhibición de fallos activada alarga el tiempo de reacción del sistema HIMatrix!

Se podrá renunciar a las medidas anteriormente descritas si el equipo se dimensiona de forma tal que puedan descartarse picos en el sistema.

En el dimensionamiento deberán incluirse medidas de protección de sobretensión, descarga de rayos, puesta a tierra y cableado del equipo con base a las especificaciones del manual del sistema (HI 800 495 S o HI 800 494 S) y las normas relevantes.

5.3.5 Entradas digitales parametrizables

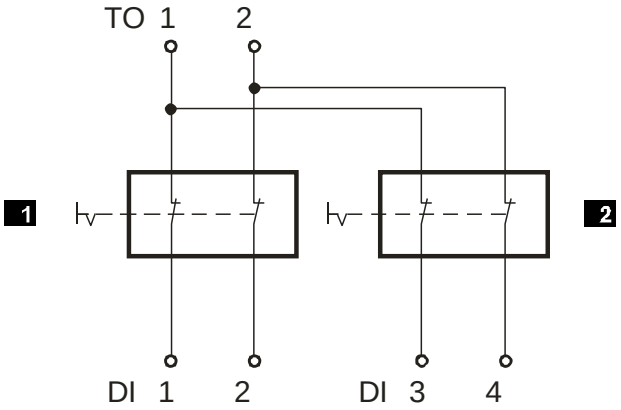
Las entradas digitales del sistema de control F35 y del módulo MI 24 01 funcionan según el principio de las entradas analógicas que, sin embargo, transmiten valores digitales mediante la parametrización de sus umbrales de conmutación.

Para las entradas digitales parametrizables rigen las rutinas de comprobación y las funciones de seguridad descritas en el capítulo 5.4 para las entradas analógicas.

5.3.6 Line Control

Line Control es un detector de cortocircuitos y circuitos abiertos (p.ej. de dispositivos de parada de emergencia) que podrá configurarse en los sistemas HIMatrix con entradas digitales (no con entradas digitales parametrizables).

A este propósito, conecte las salidas digitales TO del sistema a las entradas digitales DI del mismo sistema de la siguiente manera (ejemplo):



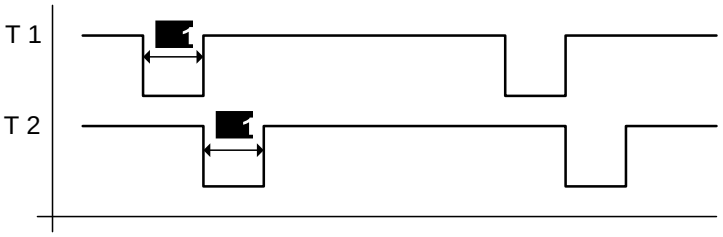
1 Parada de emergencia 1

2 Parada de emergencia 2

Dispositivos de parada de emergencia según EN 60947-5-1 y EN 60947-5-5

Fig. 2: Line Control

El sistema de control hace pulsar las salidas digitales para detectar si hay cortocircuitos o circuitos abiertos en los cables de las entradas digitales. A tal efecto, parametrice en SILworX la variable de sistema *Value [BOOL] ->* y en ELOP II Factory la señal de sistema *DO[01].Value*. Las variables para las salidas de pulsos deberán comenzar en el canal 1 y hallarse una tras la otra (ver señales/variables de sistema en los manuales).



1 Configurable 5…2000 µs

Fig. 3: Señales de pulso T1, T2

Line Control puede detectar los siguientes errores:

- Cortocircuito cruzado entre dos cables paralelos
- Confusión de dos cables (p.ej. TO 2 a DI 3)
- Derivación a tierra de uno de los cables (solo si hay polo de ref. a tierra)
- Si se interrumpen cables o abren contactos (también por pulsar alguna de las paradas de emergencia), parpadeará el LED y se generará un código de error.

Si se produce un error tal, tendrán lugar las siguientes reacciones:

- El LED *FAULT* del panel frontal del sistema de control o del módulo parpadeará.
- Las entradas adoptarán el nivel “low”.
- Se generará un código de error (evaluable).

5.4 Entradas analógicas relacionadas con la seguridad (F35, F3 AIO 8/4 01 y F60)

Los canales de entrada analógicos convierten las intensidades de entrada medidas en un valor ENTERO (INTEGER). El programa de usuario dispone así de valores en forma de variables que se asignan a las siguientes señales/variables de sistema:

Versión de sistema operativo	Valor
A partir de S.Op V.7 de CPU	Variable de sistema -> *Value [INT]*
Hasta S.Op. V.7 de CPU	Señal de sistema *AI[xx].Value* (xx = número de canal).

Tabla 14: Valor de entradas analógicas relacionadas con la seguridad

La exactitud de seguridad instrumentada es la exactitud garantizada de la entrada analógica sin reacción a fallos del módulo. Este valor deberá tenerse en cuenta al parametrizar funciones de seguridad.

Los rangos de valores de las entradas dependen del dispositivo o el módulo:

Sistema de control F35

Canales de entrada	Procedimiento de medición	Corriente, tensión	Rango de valores en la aplicación		Precisión de seguridad instrumentada
			FS1000[1)]	FS2000[1)]	
8	Unipolar	0…+10 V	0…1000	0…2000	2%
8	Unipolar	0…20 mA	0…500[2)] 0…1000[3)]	0…1000[2)] 0…2000[3)]	2%

[1)] Configurable mediante selección de tipo en PADT

[2)] Con adaptador de shunt externo de 250 Ω, Nº de Ref.: 98 2220059

[3)] Con adaptador de shunt externo de 500 Ω, Nº de Ref.: 98 2220067

Tabla 15: Entradas analógicas del sistema de control F35

E/S remota F3 AIO 8/4 01

Canales de entrada	Procedimiento de medición	Corriente, tensión	Rango de valores en la aplicación	Precisión de seguridad instrumentada
8	Unipolar	0…+10 V	0…2000	2%
8	Unipolar	0…20 mA	0…1000[1)] 0…2000[2)]	2%

[1)] Con adaptador de shunt externo de 250 Ω, Nº de Ref.: 98 2220059

[2)] Con adaptador de shunt externo de 500 Ω, Nº de Ref.: 98 2220067

Tabla 16: Entradas analógicas de la E/S remota F3 AIO 8/4 01

Sistema de control F60

Canales de entrada **AI 8 01**	Procedimiento de medición	Corriente, tensión	Rango de valores en la aplicación		Precisión de seguridad instrumentada
			FS1000[1)]	FS2000[1)]	
8	Unipolar	-10…+10 V	-1000…1000	-2000…2000	1%
8	Unipolar	0…20 mA	0…1000[3)]	0…2000[3)]	1%
8	Unipolar	0…20 mA	0…500[2)]	0…1000[2)]	4%
4	Bipolar	-10 V…+10 V	-1000…1000	-2000…2000	1%
MI 24 01					
24	Unipolar	0…20 mA	0…2000[4)]		1%

[1)] Configurable mediante selección de tipo en PADT(F60)

[2)] Con shunt de medición externo de 250 Ω, Nº de Ref.: 00 0710251

[3)] Con shunt de medición externo de 500 Ω, Nº de Ref.: 00 0603501 (exactitud 0,05%, P 1 W)

[4)] Shunts de medición internos

Tabla 17: Entradas analógicas del sistema de control F60

El módulo AI 8 01 del F60 podrá configurarse en el programa de usuario para ocho funciones unipolares o cuatro funciones bipolares. Sin embargo, no se permite mezclar funciones en un módulo.

Las entradas analógicas del sistema de control F35, de la E/S remota F3 AIO 8/4 01 y del módulo AI 8 01 funcionan con medición de tensión. Con las entradas analógicas de F35 y de F3 AIO 8/4 01 podrá monitorearse si hay circuitos interrumpidos en las salidas digitales del propio sistema (F35) u otros sistemas de control HIMatrix. Hallará más información en los manuales de los correspondientes sistemas de control HIMatrix.

En caso de interrupción de cable (el sistema no monitorea los cables), en las entradas altamente óhmicas se procesará cualquier señal de entrada. El valor resultante de esta tensión de entrada fluctuante no es seguro. En las entradas de tensión los canales deberán terminarse con una resistencia de cierre de 10 kΩ. Tenga en cuenta la resistencia interna de la fuente.

Para una medición de intensidad la entrada del shunt se circuitará en paralelo, en cuyo caso no se necesitará la resistencia de 10 kΩ.

Debido al shunt interno de medición, las entradas del módulo MI 24 01 son entradas de intensidad y no podrán usarse como entradas de tensión.

En los canales de entrada que no se usen, la entrada de medición deberá conectarse al potencial de referencia. Así se evitarán repercusiones negativas sobre otros canales en caso de interrupción de cables (valores de tensión fluctuantes).

Versión de sistema operativo	Procedimiento
A partir de S.Op V.7 de CPU	Basta con no asignar variables globales a las entradas que no se usen.
Hasta S.Op. V.7 de CPU	Para la entrada no utilizada, establezca en el administrador de hardware de ELOP II la correspondiente señal *AI[0x].Used* al valor original por defecto *FALSE* ó *0*. Así se ocultará el canal dentro del programa de usuario, es decir, no se dispondrá ya de más mensajes de señal.

Tabla 18: Configuración de entradas no utilizadas

5.4.1 Rutinas de comprobación

El sistema de control procesa valores analógicos de forma paralela mediante dos multiplexores y dos convertidores analógico/digitales con una resolución de 12 bits y coteja unos resultados con otros. Adicionalmente, el sistema de control aplica valores de prueba mediante convertidor digital/analógico, los convierte de nuevo en valores digitales y compara que correspondan a los valores que acababa de ordenar.

En caso de detectar errores, el sistema de control transmitirá para la entrada afectada el valor 0 al programa de usuario y activará el estado de error.

5.4.2 Reacción en caso de error

Si se producen errores de canal en las entradas analógicas, el código de error del canal defectuoso adoptará un valor > 0. Si se trata de errores para todo el módulo, el código de error para el módulo adoptará un valor > 0.

El programa de usuario deberá evaluar, además del valor analógico, el correspondiente código de error. Para un valor > 0 deberá proyectarse una reacción relacionada con la seguridad.

Un sistema compacto activará el LED *FAULT,* un módulo F60 el LED *ERR*.

Utilizando el código de error se dispone de posibilidades adicionales de monitorear en el programa de usuario el circuito externo y programar la reacción frente a errores.

Versión	Acceso al código de error	Nombre del código de error
A partir de S.Op V.7 de CPU	En la ficha …*Channels* de la vista detallada del módulo o dispositivo	->Error code [bytes] en la línea del número de canal
Hasta S.Op. V.7 de CPU	En la ventana *Signal Connections…* del módulo o dispositivo	AI[*xx*].error code, *xx* = número de canal

Tabla 19: Códigos de error de las entradas analógicas

5.5 Contadores relacionados con la seguridad (F35 y F60)

Los puntos aquí indicados valen tanto para el módulo contador CIO 2/4 01 del F60 como para los contadores del F35, salvo que se indique lo contrario.

5.5.1 Generalidades

Un canal de contador podrá parametrizarse como cuenta progresiva/regresiva rápida con resolución de 24 bits o como decodificador en código Gray.

En caso de usarse como contador progresivo/regresivo rápido, en la aplicación se necesitarán como señales la entrada de impulsos y la entrada de sentido de recuento. Se podrán reinicializar solamente en el programa de usuario.

La resolución del codificador de 4 u 8 bits es válida para el módulo de contadores CIO 2/4 01 del F60. En el F35, el codificador tendrá una resolución de 3 ó 6 bits. No será posible una reinicialización.

La agrupación de dos entradas independientes de 4 bits como una entrada de 8 bits (ejemplo para F60) se realiza exclusivamente con el programa de usuario. No se ha previsto una posibilidad de conmutación a este efecto.

La función de codificador monitorea la modificación de los patrones de bits en los canales de entrada. Los patrones de bits en las entradas se transmiten directamente al programa de usuario. En el PADT se representan en forma de un número decimal correspondiente al patrón de bits (*Counter[0x].Value*).

Según la aplicación, este número, que corresponde al patrón de bits del código Gray, podrá convertirse p.ej. en el respectivo valor decimal.

5.5.2 Reacción en caso de error

Si las rutinas de comprobación de la parte de contador del dispositivo/módulo detectan algún error, activarán un bit de estado para la evaluación en el programa de usuario. El programa de usuario podrá considerar además el correspondiente código de error.

Un sistema compacto activará el LED *ERROR*, un módulo F60 el LED *ERR*.

Utilizando el código de error se dispone de posibilidades adicionales de monitorear en el programa de usuario el circuito externo y programar la reacción frente a errores.

Versión	Acceso al código de error	Nombre del código de error
A partir de S.Op V.7 de CPU	En la ficha …*Channels* de la vista detallada del módulo o dispositivo	->Error code [bytes] en la línea del número de canal
Hasta S.Op. V.7 de CPU	En la ventana *Signal Connections…* del módulo o dispositivo	Counter[*xx*].error code, *xx* = número de canal

Tabla 20: Códigos de error de las entradas de contadores

5.6 Lista de chequeo para entradas relacionadas con la seguridad

Esta lista de chequeo es una recomendación para proyectar, programar y poner en servicio entradas con función relacionada con la seguridad. Puede usarse como documento de planificación, sirviendo al mismo tiempo de comprobante de la realización concienzuda de la planificación.

Para cada canal de entrada relacionada con la seguridad que se use en un sistema deberá cumplimentarse una lista de chequeo propia del marco de proyección y puesta en servicio para verificar las exigencias normativas a cumplir. Solamente así podrá Ud. asegurarse de registrar las exigencias completa y claramente. La lista de chequeo es asimismo una forma de documentar la conexión entre el cableado externo y el programa del usuario.

La lista de chequeo *HIMatrix_Checklist_Inputs.doc* está disponible en formato Microsoft© Word©. El archivo ZIP *HIMatrix_Checklists.zip* contiene todas las listas de chequeo y podrá descargarse del sitio www.hima.com.

6 Salidas

Sinopsis de salidas del sistema HIMatrix

Dispositivo	Tipo	Cantidad de entradas	Relacionadas con la seguridad	Con separación eléctrica
Sistema de control F20	Digital	8	•	-
	Pulso	4	-	-
Sistema de control F30 (configurable para Line Control)	Digital	8	•	-
Sistema de control F31 (configurable para Line Control)	Digital	8	•	-
Sistema de control F35		8	•	-
E/S remota F1 DI 16 01	Pulso	4	-	-
E/S remota F2 DO 4 01	Digital	4	•	-
E/S remota F2 DO 8 01	Digital	8	•	•
E/S remota F2 DO 16 01	Digital	16	•	-
E/S remota F2 DO 16 01	Relé	16	•	•
E/S remota F3 DIO 8/8 01	Digital de 1 polo	8	•	-
	Digital de 2 polos	2		
E/S remota F3 DIO 16/8 01	Digital de 1 polo	16	•	-
	Digital de 2 polos	8		
E/S remota F3 AIO 8/4 01	Analógico	4	-	-
E/S remota F3 DIO 20/8 01 y F3 DIO 20/8 02 (configurable para Line Control)	Digital	8	•	-
Sistema de control modular F60:				
Módulo DIO 24/16 01 (configurable para Line Control)	Digital	16	•	•
Módulo DI 32 01 (configurable para Line Control)	Digital	32	•	•
Módulo DO 8 01 (110 V)	Relé	8	•	•
Módulo CIO 2/4 01	Digital	4	•	•
Módulo AO 8 01	Analógico	8	•	•

Tabla 21: Sinopsis de salidas del sistema HIMatrix

6.1 Generalidades

El sistema de control escribe las salidas relacionadas con la seguridad una vez por ciclo, relee las señales de salida y compara que correspondan a los datos de salida que acababa de ordenar.

El estado seguro para las salidas es el valor 0 o el contacto de relé abierto.

En los canales de salida relacionados con la seguridad se han integrado tres contactos en serie comprobables. Con ello, la segunda vía independiente de desconexión requerida en la seguridad instrumentada estará integrada en el canal de salida. Esta vía de desconexión de seguridad desactivará con seguridad (los pondrá en estado sin energía o excitación) todos los canales del módulo de salida defectuoso en caso de error.

La señal de WatchDog de la CPU es la segunda posibilidad de desconexión de seguridad: si se pierde la señal de WatchDog, ello hará que se adopte automáticamente el estado seguro.

Esta función actúa solamente sobre todas las salidas digitales y las salidas de relés de los sistemas de control.

La utilización del respectivo código de error ofrece posibilidades adicionales de configurar reacciones frente a fallos en el programa del usuario.

6.2 Seguridad de actuadores

En una aplicación con función relacionada con la seguridad, tanto el sistema de control como los actuadores conectados a él deberán cumplir las exigencias normativas de seguridad y el nivel SIL especificado. Véase al respecto “Aumento del nivel SIL de sensores y actuadores” *en el anexo.*

6.3 Salidas digitales relacionadas con la seguridad

Los puntos aquí indicados son válidos tanto para los canales de salida digitales de los módulos del sistema F60 como para los canales de salida digitales de los sistemas compactos. Se exceptúan en ambos casos las salidas de relés.

6.3.1 Rutinas de comprobación para salidas digitales

Los dispositivos y los módulos realizan autocomprobaciones durante el funcionamiento. Las funciones de comprobación fundamentales son:

- Relectura de la señal de salida del amplificador de conmutación. El umbral para un nivel “low” releído es de 2 V. Los diodos utilizados impiden el retroceso de señales.
- Comprobación de la doble desconexión integrada de seguridad.
- Una prueba de desconexión de las salidas se realiza dentro del tiempo MOT durante un máximo de 200 µs cada vez. Intervalo mínimo entre dos comprobaciones: ≥ 20 s.

El sistema monitorea su tensión de trabajo y desactiva todas las salidas en caso de baja tensión < 13 V.

6.3.2 Reacción en caso de error

Si el sistema de control detecta una señal errónea, pondrá la salida del dispositivo o del módulo afectado en estado seguro (sin energía o excitación) mediante los interruptores de seguridad. Si es un error de módulo, se desactivarán todas las salidas del módulo. Un sistema compacto indicará además ambos errores con el LED *ERROR*, un módulo del sistema F60 con el LED *ERR*.

6.3.3 Reacción en caso de sobrecarga o cortocircuito externo

En caso de sobrecarga o de cortocircuitarse la salida con L-, se conservará la comprobabilidad del dispositivo o del módulo. No será necesario que se desconecte mediante el circuitado de desconexión de seguridad.

El sistema de control monitorea el consumo total de corriente del dispositivo o del módulo y, en caso de sobrepasarse el umbral, pone todos los canales de salida en estado seguro.

En este estado las salidas se comprueban cíclicamente a intervalos de unos pocos segundos para ver si sigue habiendo sobrecarga. Al recobrarse el estado normal, se volverán a activar las salidas.

6.3.4 Line Control

El sistema de control puede hacer pulsar las salidas digitales relacionadas con la seguridad y usarlas conjuntamente con las entradas digitales relacionadas con la seguridad del mismo sistema (pero no con entradas digitales parametrizables) para detectar interrupciones y cortocircuitos (véase el capítulo 5.3.6 Line Control).

NOTA

¡Son posibles disfunciones de los actuadores conectados!

¡No use salidas de pulsos para las salidas relacionadas con la seguridad, p.ej. para accionar actuadores relacionados con la seguridad!

No podrán usarse salidas de relés como salidas de pulsos.

6.4 Salidas digitales de 2 polos relacionadas con la seguridad

Las características aquí descritas se refieren a salidas digitales de 2 polos de sistemas compactos.

6.4.1 Rutinas de comprobación para salidas digitales de 2 polos

Los dispositivos realizan autocomprobaciones durante el funcionamiento. Las funciones de comprobación fundamentales son:

- Relectura de la señal de salida del amplificador de conmutación. El umbral para un nivel “low” releído es de 2 V. Los diodos utilizados impiden el retroceso de señales.
- Comprobación de la (doble) desconexión integrada de seguridad.
- Una prueba de desconexión de las salidas se realiza dentro del tiempo MOT durante un máximo de 200 µs cada vez. Intervalo mínimo entre dos comprobaciones: ≥ 20 s.
- Diagnóstico de cable para conexión de 2 polos
  F3 DIO 16/8 01:
  - Cortocircuito con L+, L-.
  - Cortocircuito entre conexiones de 2 polos.
  - Interrupción de cable en una de ambas conexiones de 2 polos.
- Diagnóstico de cable para conexión de 2 polos
  F3 DIO 8/8 01: cortocircuito con L+, L-.
- Comprobación de contacto de prueba L- en conexiones de 2 polos con diagnóstico de cable (F3 DIO 16/8 01).
- Monitoreo de la corriente de salida.

El sistema monitorea su tensión de trabajo y desactiva todas las salidas en caso de baja tensión < 13 V.

6.4.2 Conexión de 1 polo / 2 polos (F3 DIO 8/8 01, F3 DIO 16/8 01)

Las salidas digitales podrán configurarse de la siguiente manera:

- Salida digital con conexión de 2 polos con diagnóstico de cable
- Salida digital con conexión de 2 polos sin diagnóstico de cable
- Salida digital con L+ y DO+ conmutante de 1 polo
- Salida digital con L- y DO- conmutante de 1 polo

Conexión de 2 polos

NOTA

¡Es posible una activación inesperada de un relé o actuador conectado a la salida!

En aplicaciones con alto riesgo deberá usarse además la señal de estado de diagnóstico de cable, para poder desconectar las salidas (DO+, DO-) en caso de error.

i

Si no pueden cumplirse las exigencias arriba citadas, deberá observarse el siguiente caso:

Si se da un cortocircuito de cable de DO- a L- es posible que se excite algún relé o actuador, con lo que cambiará su posición de contacto.

Razón: durante el tiempo de monitoreo en curso para el diagnóstico de cable hay un nivel de tensión de 24 V (salida DO+) en el consumidor (relé, actuador conmutante), pudiendo llegar a este suficiente energía como para cambiar de estado.

NOTA

¡Es posible que falle la detección de interrupción de cable!

Si se usa la conexión de 2 polos no deberá haber ninguna entrada DI conectada a una salida DO. Ello impediría detectar interrupciones de cable.

NOTA

¡Es posible que se produzcan fallos en el sistema de control o los dispositivos/sistemas electrónicos adyacentes!

La conexión de cargas inductivas deberá realizarse con un diodo de retorno en el consumidor.

6.4.3 Reacción en caso de error

Salidas DO-

Si se detecta una señal errónea, el dispositivo/módulo pondrá la salida afectada en estado seguro (sin energía) mediante los interruptores de seguridad. Un error del dispositivo/módulo hará que se desactiven todas las salidas. Ambos tipos de error se indicarán en un sistema compacto con el LED *ERROR* y en un módulo del F60 con el LED *ERR*.

Salidas DO+

Si se detecta una señal errónea, el dispositivo/módulo pondrá la salida afectada en estado seguro (sin energía) mediante los interruptores de seguridad. Un error del dispositivo/módulo hará que se desactiven todas las salidas. Ambos errores se indicarán en un sistema compacto con el LED *ERROR* y en un módulo del F60 con el LED *ERR*.

6.4.4 Reacción en caso de sobrecarga o cortocircuito externo

En caso de sobrecarga o de cortocircuitarse la salida con L- o L+, se conservará la comprobabilidad del dispositivo o del módulo. No será necesario que se desconecte mediante el circuitado de desconexión de seguridad.

El consumo total de corriente del dispositivo/módulo se monitorea. En caso de sobrepasarse el umbral, el dispositivo/módulo de salida pondrá todos los canales en estado seguro.

En este estado el dispositivo o módulo comprobará todas las salidas cíclicamente a intervalos de unos pocos segundos para ver si sigue habiendo sobrecarga. Al recobrarse el estado normal, el dispositivo o el módulo volverá a activar las salidas.

6.5 Salidas de relés

Si bien las salidas de relés equivalen funcionalmente a las salidas digitales, ofrecen además separación galvánica y alta tenacidad frente a la tensión.

6.5.1 Rutinas de comprobación de salidas de relés

El dispositivo o el módulo comprueba automáticamente sus salidas durante el funcionamiento. Las funciones de comprobación fundamentales son:

- Relectura de las señales de salida del amplificador de conmutación previo al relé
- Comprobación de la conmutación de los relés con contactos forzados
- Comprobación de la doble desconexión integrada de seguridad.

El sistema monitorea su tensión de trabajo y desactiva todas las salidas en caso de baja tensión < 13 V.

En el módulo DO 8 01 y las E/S remotas F2 DO 8 01 y F2 DO 16 02, las salidas están dotadas con tres relés de seguridad:

- Dos relés con contactos forzados
- Un relé estándar

Así, las salidas pueden usarse para circuitos de desconexión de seguridad.

6.5.2 Reacción en caso de error

Si se detecta una señal errónea, el dispositivo/módulo pondrá la salida afectada en estado seguro (sin energía) mediante los interruptores de seguridad. Si se trata de un error del módulo, este desactivará todas las salidas. Ambos errores se indicarán en un sistema compacto con el LED *ERROR* y en un módulo del F60 con el LED *ERR*.

6.6 Salidas analógicas relacionadas con la seguridad (F60)

El módulo AO 8 01 tiene un sistema procesador relacionado con la seguridad 1oo2 A/D propio con comunicación segura. Este escribe las salidas analógicas una vez por ciclo y guarda los valores internamente. El módulo comprueba él mismo su funcionamiento.

Con los selectores DIP de los módulos de salida analógicos relacionados con la seguridad se pueden configurar las salidas para que actúen por tensión o por corriente. Al hacerlo deberá verificarse que la opción ahí elegida coincida con la que se usa en el sistema y en la parametrización del programa de usuario. La inobservancia hará que el módulo reaccione erróneamente.

NOTA

Funcionamiento erróneo del módulo

Antes de montar el módulo en el sistema, compruebe:

- **Posición de los selectores DIP del módulo.**
- **Parametrización del módulo en el programa de usuario.**

Según el tipo de dispositivo seleccionado (…FS1000, …FS2000) habrá que considerar en la lógica diferentes valores para las señales de salida, para obtener los mismos valores de

salida (véase p.ej. en el manual AO 8 01 HI 800 515 S el capítulo *"Señales y códigos de error de las salidas"*).

Respectivamente hay dos salidas analógicas interconectadas galvánicamente:

- Salidas 1 y 2.
- Salidas 3 y 4.
- Salidas 5 y 6.
- Salidas 7 y 8.

En los circuitos analógicos de salida hay monitoreo de tensión o corriente, canales de prueba y relectura también para circuitos de salida paralelos, así como dos interruptores de seguridad adicionales para desconectar seguramente los circuitos de salida en caso de error. Así se alcanzará el estado seguro (salida de corriente: 0 mA; salida de tensión: 0 V).

6.6.1 Rutinas de comprobación

El módulo realiza autocomprobaciones durante el funcionamiento. Las funciones de comprobación fundamentales son:

- Relectura doble de la señal de salida
- Prueba de diafonía entre las salidas
- Comprobación de la desconexión integrada de seguridad.

6.6.2 Reacción en caso de error

Una vez por ciclo el módulo relee las señales de salida y las compara con las señales de salida internamente guardadas. Si el módulo detecta discrepancias, desactivará el canal de salida erróneo mediante los dos interruptores de seguridad e indicará el error del módulo mediante el LED *ERR*.

La utilización del código de error ofrece posibilidades adicionales de configurar reacciones frente a fallos en el programa del usuario.

Para el tiempo de reacción del peor supuesto posible (Worst Case) de las salidas analógicas, al tiempo de WatchDog (2* WDT_{CPU}) habrá que sumarle el doble del tiempo de WatchDog de AO-CPU (2*$WDT_{AO\text{-}\mu C}$).

El manual especifica el tiempo de reacción para el peor supuesto posible.

6.7 Salidas analógicas con desactivación relacionada con la seguridad (F3 AIO 8/4 01)

La E/S remota escribe las salidas analógicas una vez por ciclo y guarda los valores internamente.

Si bien no se trata de salidas relacionadas con la seguridad, podrán desconectarse conjuntamente de forma segura.

Para satisfacer el nivel SIL 3, deberán releerse los valores de salida mediante entradas analógicas relacionadas con la seguridad y evaluarse en el programa del usuario. En el programa de usuario deberán definirse asimismo reacciones frente a valores de salida erróneos.

6.7.1 Rutinas de comprobación

La E/S remota prueba automáticamente ambos interruptores de seguridad para la desconexión de las cuatro salidas durante el funcionamiento.

6.7.2 Reacción en caso de error

En caso de un error interno de la E/S remota, se desconectarán al mismo tiempo los cuatro canales de salida mediante ambos interruptores de seguridad y el error del módulo se señalizará con el LED *FAULT* en el panel frontal.

La utilización del código de error ofrece posibilidades adicionales de configurar reacciones frente a fallos en el programa del usuario.

6.8 Lista de chequeo para salidas relacionadas con la seguridad

Esta lista de chequeo es una recomendación para proyectar, programar y poner en servicio salidas relacionadas con la seguridad. Puede usarse como documento de planificación, sirviendo al mismo tiempo de comprobante de la realización concienzuda de la planificación.

Para cada canal de salida relacionada con la seguridad que se use en un sistema deberá cumplimentarse una lista de chequeo propia del marco de proyección y puesta en servicio para verificar las exigencias normativas a cumplir. Solamente así podrá Ud. asegurarse de registrar las exigencias completa y claramente. Constituye asimismo una forma de documentar la conexión entre el cableado externo y el programa del usuario.

La lista de chequeo *HIMatrix_Checklist_Outputs.doc* está disponible en formato Microsoft© Word©. El archivo ZIP *HIMatrix_Checklists.zip* contiene todas las listas de chequeo y podrá descargarse del sitio www.hima.com.

7 Software para sistemas HIMatrix

El software para los dispositivos de automatización con función relacionada con la seguridad de los sistemas HIMatrix se desglosa como sigue:

- Sistema operativo
- Programa de usuario
- Utilidad de programación conforme a IEC 61131-3.

El sistema operativo se carga a la unidad central (CPU) del sistema de control y se deberá usar en la respectiva forma válida certificada por el organismo de inspección TÜV para aplicaciones con función relacionada con la seguridad.

La utilidad de programación sirve para crear el programa de usuario, el cual contendrá las funciones específicas para el equipo o la instalación a controlar que hayan de ser ejecutadas por el dispositivo de automatización. La parametrización y el manejo de las funciones del sistema operativo se realiza también mediante la utilidad de programación.

El generador de códigos de la utilidad de programación traduce el programa del usuario al código máquina. La utilidad de programación transmite dicho código máquina mediante una interfaz Ethernet a las memorias Flash-EPROM del dispositivo de automatización.

7.1 Aspectos de seguridad instrumentada para el sistema operativo

Todo sistema operativo homologado lo identifica su designación. Para una mejor diferenciación se especifican la revisión y la signatura CRC. Las respectivas versiones del sistema operativo homologadas por el organismo de inspección para los dispositivos de automatización con función relacionada con la seguridad y sus respectivas signaturas (CRC) están sujetas a revisión y se documentan en una lista que se redacta conjuntamente con el organismo de inspección oficial (TÜV).

La versión instalada del sistema operativo solamente podrá leerse con la utilidad de programación. Se requiere una comprobación por parte del usuario (ver 7.6 “Lista de chequeo de creación de un programa de usuario”).

7.2 Modos y funciones del sistema operativo

El sistema operativo ejecuta el programa de usuario cíclicamente. Para ello ejecuta las siguientes funciones, en forma muy simplificada:

- Lectura de los datos de entrada.
- Procesado de las funciones lógicas que se hayan programado conforme a IEC 61131-3.
- Escritura de los datos de salida.

Además tienen lugar las siguientes funciones fundamentales:

- Extensas autocomprobaciones.
- Pruebas de las entradas y salidas durante el funcionamiento.
- Transmisión de datos.
- Diagnóstico.

7.3 Aspectos de seguridad instrumentada para la programación

7.3.1 Concepto de seguridad de la utilidad de programación

Concepto de seguridad de las utilidades de programación ELOP II Factory y SILworX:

- Al instalar la utilidad de programación, una suma de verificación CRC preserva la integridad del paquete del programa en su camino desde el fabricante hasta el usuario.
- La utilidad de programación realiza pruebas de plausibilidad para minimizar los errores de introducción de datos.

- La doble compilación y la consiguiente comparación de ambas sumas de verificación CRC obtenidas permite detectar falseamientos de la aplicación causados por disfunciones temporales del PC empleado.

Doble compilación del programa y comparación de los resultados:

1. Inicie la compilación.
   ☑ Al concluir la compilación, la utilidad de programación SILworX mostrará una suma de verificación CRC.
2. Reinicie la compilación.
   ☑ Al concluir la compilación, la utilidad de programación SILworX mostrará una suma de verificación CRC.

Si ambas sumas de verificación CRC son idénticas, no habrá habido falseamiento durante la compilación.

En la primera puesta en servicio de un sistema de control con función relacionada con la seguridad habrá que comprobar la seguridad de todo el sistema mediante una prueba funcional completa.

Prueba funcional del sistema de control

1. Comprobación de la correcta implementación de las tareas de control con ayuda de los datos y los flujos de señales.
2. Completa comprobación funcional de la lógica mediante la puesta a prueba (véase la comprobación de la configuración y del programa de usuario).

El sistema de control y el programa de usuario quedan suficientemente probados.

Si se modifica el programa del usuario, habrá que probar solamente aquellas partes del programa afectadas por la modificación.

A partir de S.Op V.7 de CPU

El comparador seguro de revisiones de SILworX puede detectar y mostrar las modificaciones respecto a la versión previa.

7.3.2 Comprobación de la configuración y del programa de usuario

Para comprobar si el programa de usuario creado cumple la función de seguridad específica, deberán crearse casos de prueba adecuados que cubran la especificación.

Por lo general basta con comprobar independientemente cada bucle (compuesto de entrada, nexos importantes desde el punto de vista de la aplicación y salida). La utilidad de programación y las medidas descritas en este manual de seguridad hacen bastante improbable que un código semántica y sintácticamente bien generado pueda originar errores sistemáticos no detectados debidos al proceso de generación de códigos.

Deberán generarse también casos de prueba idóneos para la evaluación numérica de fórmulas. Son muy convenientes las pruebas de clases de equivalencias, es decir, pruebas dentro de rangos de valores definidos, en sus límites o en rangos de valores inadmisibles. Los casos de prueba deberán elegirse de tal forma que demuestren que la lógica del programa es correcta. La cantidad necesaria de casos de prueba dependerá de la lógica de programa utilizada y deberá incluir pares de valores críticos.

Solamente una activa simulación con fuentes puede demostrar que el cableado de los sensores y los actuadores del sistema es correcto (también en la comunicación a las E/S remotas conectadas). Por lo demás, solo así podrá comprobarse la configuración del sistema.

Este procedimiento vale para la primera creación del programa de usuario y también para sus ulteriores modificaciones.

7.3.3 Archivado de un proyecto

HIMA recomienda archivar el proyecto cada vez que se cargue el programa al sistema de control. Esto es válido tanto para cargas por “Download” como por “Reload”.

La forma de archivar un proyecto difiere sustancialmente en la utilidad ELOP II Factory respecto a la utilidad SILworX.

Archivado de un proyecto a partir de la V.7 del S.Op. de la CPU

SILworX crea un proyecto en un archivo de proyecto. Este es idóneo para guardarlo p.ej. en un disco o medio similar.

Creación de un archivo de proyecto hasta la versión V.7 del S.Op.

ELOP II Factory crea un proyecto en una estructura de subdirectorio. Para el archivado, ELOP II Factory puede guardar el contenido de dicha estructura en un archivo de seguridad, el fichero del proyecto. Este fichero de proyecto es idóneo para guardarlo p.ej. en un disco o medio similar.

Creación de un fichero de proyecto

1. Impresión del programa de usuario para cotejar la lógica con las consignas a cumplir.
2. Traducción del programa de usuario para generar CRC de configuración de la CPU.
3. Anotación de la versión de CRC de configuración de la CPU. Para ello se seleccionará el sistema de control dado en el administrador de hardware y las versiones podrán verse en el menú contextual **Configuration Information**. Para determinar una versión:
   - rootcpu.config indica la configuración relacionada con la seguridad de la CPU, el valor CRC de configuración de la CPU.
   - rootcom.config indica la configuración no relacionada con la seguridad de COM.
   - root.config indica la configuración total, incl. las E/S remotas (CPU + COM).
4. Cree un fichero del proyecto en un disco o medio y dótelo con los nombres de los programas de usuario, CRCs de configuración de las CPUs y la fecha.
   Esta medida recomendada no suple la obligación a documentar del usuario.

El fichero del proyecto está creado.

7.3.4 Posibilidad de identificación de configuración y de programa

Los programas de usuario se identifican inequívocamente por los CRCs de configuración del proyecto. Este podrá Ud. compararlo con el CRC de configuración del proyecto cargado.

Archivos de proyecto – A partir de S.Op. V.7 de la CPU

Para asegurarse de que la copia de seguridad del archivo de proyecto guardado no haya sido modificada, compile el recurso que contenga y compare el CRC de configuración con el CRC de la configuración cargada. Esta podrá verse con SILworX.

Archivado – Hasta S.Op. V.7 de la CPU

La designación de un fichero deberá contener los CRCs de configuración de root.config.

Para asegurarse de que el fichero de proyecto empleado no haya sido modificado, compile el recurso tras restaurar el proyecto desde el fichero y compare el CRC de configuración de root.config con el CRC de la configuración cargada, que podrá ver con ELOP II Factory.

Para la comprobación deberá abrirse el menú **Resource → Consistency Check** en el panel de control del recurso.

7.4 Parámetros del recurso

⚠ PELIGRO

¡Una configuración errónea puede llegar a causar daños personales!

Ni el sistema de programación ni el sistema de control pueden comprobar algunos parámetros específicamente definidos para el proyecto. Escriba por tanto dichos parámetros correctamente en el sistema de programación y verifíquelos.

Estos parámetros son:

- **System ID**
- **Rack-ID (ver manuales del sistema HI 800 495 y HI 800 494).**
- **Safety Time**
- **Watchdog Time**
- **Main Enable**
- **Autostart**
- **Start Allowed**
- **Load Allowed**
- **Reload Allowed**
- **Global Forcing Allowed**

Los parámetros listados a continuación se definen en la utilidad de programación para las acciones admisibles en el funcionamiento relacionado con la seguridad del dispositivo de automatización y se designan como parámetros relacionados con la seguridad.

Las posibles definiciones que obren durante el funcionamiento relacionado con la seguridad no están rígidamente vinculadas a una determinada categoría de exigencias normativas, sino que deberán acordarse con el respectivo organismo de inspección oficial para cada finalidad del sistema de control.

7.4.1 Parámetros de sistema a partir de S.Op. V.7 de la CPU

A partir de la versión V.7 del S.Op. de la CPU hay parámetros de sistema del recurso y parámetros de sistema del hardware.

Parámetros de sistema del recurso

Estos parámetros definen cómo responderá el sistema de control durante el funcionamiento y se ajustan en SILworX, en el cuadro de diálogo *Properties* del recurso.

Parámetro/Switch	Descripción	Valor por defecto	Ajuste para funcionamiento seguro
Name	Nombre del recurso		Cualquiera
System ID [SRS]	ID de sistema del recurso 1…65 535 Al ID del sistema deberá Ud. asignarle un valor distinto al valor por defecto, de lo contrario el proyecto no será ejecutable.	60 000	Valor inequívoco dentro de la red de los sistemas de control que puedan estar interconectados unos con otros.
Safety Time [ms]	Tiempo de seguridad, en milisegundos 20…22 500 ms	600 ms	Específico de la aplicación
Watchdog Time [ms]	Tiempo de WatchDog, en milisegundos 8…5000 ms	200 ms/ 100 ms[1)]	Específico de la aplicación

Main Enable	ON: Durante el funcionamiento (= RUN) podrán modificarse los siguientes parámetros/switches con el PADT: ▪ *System ID* ▪ *Resource Watchdog Time* ▪ *Safety Time* ▪ *Target Cycle Time* ▪ *Target Cycle Time Mode* ▪ *Autostart* ▪ *Global Forcing Allowed* ▪ *Global Force Timeout Reaction* ▪ *Load Allowed* ▪ *Reload Allowed* ▪ *Start Allowed* OFF: Durante el funcionamiento no podrán modificarse los parámetros. i El parámetro *Main Enable* podrá ponerse en ON solamente con el sistema PES detenido.	ON	Se recomienda: OFF
Autostart	ON: Una vez se conecte el sistema procesador a la tensión de alimentación, el programa de usuario se iniciará automáticamente. OFF: Sin inicio automático al conectarse la tensión de alimentación.	OFF	Específico de la aplicación
Start Allowed	ON: Se permite el arranque en frío o caliente mediante el PADT en los estados RUN o STOP. OFF: No se permite el inicio	ON	Específico de la aplicación
Load Allowed	ON: Se permite el download del programa de usuario OFF: No se permite el download del programa de usuario	ON	Específico de la aplicación
Reload Allowed	¡Aplicable solamente en L3! ON: Se permite el reload del programa de usuario. OFF: No se permite el reload del programa de usuario. Un reload ya en curso no se cancelará por cambiar la opción a OFF.	ON	-
Global Forcing Allowed	ON: Se permite el forzado global para este recurso OFF: No se permite el forzado global para este recurso	ON	Específico de la aplicación
Global Force Timeout Reaction	Define cómo responderá el recurso tras expirar el force timeout global: ▪ Finalizar la función de forzado (Stop Forcing) ▪ Detener recurso (Stop Resource)	Finalizar la función de forzado (Stop Forcing)	Específico de la aplicación
Max.Com. Time Slice ASYNC [ms]	Valor máximo, en ms, del intervalo de tiempo que se usa para la comunicación dentro del ciclo del recurso. Véase el manual de comunicación HI 801 195 S, 2...5000 ms	10 ms	Específico de la aplicación
Max. Duration of Configuration Connections [ms]	¡Aplicable solamente en L3! Aquí se define de cuánto tiempo se dispone dentro de un ciclo de CPU para la comunicación de datos de proceso, 6…5000	6 ms	

Target Cycle Time [ms]	¡Aplicable solo en L3! El valor del tiempo de ciclo deseado o máximo, véase *Target Cycle Time Mode*, 0…7500 ms. El tiempo de ciclo deseado (Target Cycle Time) podrá ser únicamente tan grande como el tiempo de WatchDog configurado - 6 ms. De lo contrario, el sistema PES lo rechazará.		0 ms	-
Multitasking Mode	¡Aplicable solamente en L3!		Modo 1	-
	Mode 1	La longitud de un ciclo de la CPU se atendrá a la duración de ejecución necesaria para todos los programas de usuario.		
	Mode 2	El procesador pondrá a disposición de los programas de usuario de mayor prioridad el tiempo de ejecución no necesitado por los programas de usuario de menor prioridad. Modo operativo para alta disponibilidad.		
	Mode 3	El procesador aguardará el tiempo de ejecución no necesitado por los programas de usuario y alargará así el ciclo.		
Sum of UP Max. Duration for Each Cycle [µs]	¡Aplicable solamente en L3! Suma de los valores especificados en todos los programas de usuario para *Max. Duration for Each Cycle [µs]*. No modificable.			-
Target Cycle Time Mode	¡Aplicable solamente en L3! Utilización del tiempo *Target Cycle Time [ms].*		Fijo	-
	Fixed	PES mantendrá el tiempo deseado del ciclo y, de ser necesario, prolongará el ciclo. No será válido en caso de que el tiempo de ejecución de los programas de usuario sobrepase el tiempo de ciclo deseado.		
	Fixed-tolerant	Igual que *Fixed*, pero en el 1er ciclo de activación de reload (en L3) no se considerará el tiempo de ciclo deseado (Target Cycle Time).		
	Dynamic-tolerant	Igual que *Dynamic*, pero en el 1er ciclo de activación de reload (en L3) no se considerará el tiempo de ciclo deseado (Target Cycle Time).		
	Dynamic	HIMax mantendrá en lo posible el tiempo de ciclo deseado, pero ejecutará el ciclo tan rápido como sea posible.		
Minimum Configuration Version	Composición de archivos de configuración y generación de código igual que en la versión de SILworX citada (salvo en el caso de funciones más nuevas).		SILworX-V2	-
	SILworX V2	La generación del código tiene lugar igual que en SILworX V2. Este ajuste no cambiará el valor CRC de un proyecto creado con SILworX V2.		
	SILworX V3	Generación del código igual que en SILworX V3. Con este ajuste se garantiza la compatibilidad con versiones posteriores.		
	SILworX V4	Generación del código igual que en SILworX V4. Con este ajuste se garantiza la compatibilidad con versiones posteriores.		
Maximum System Bus Latency [µs]	¡No válido para sistemas de control HIMatrix!		0 ms	Específico de la aplicación

safe**ethernet** CRC	SILworX V.2.36.0	El valor CRC para safe**ethernet** se generará igual que en SILworX V.2.36.0. Este ajuste es necesario para poder intercambiar datos con recursos planificados con SILworX V.2.36 o anteriores.	Versión actual	Específico de la aplicación
	Versión actual	El valor CRC para safe**ethernet** se generará con el algoritmo actual.		
[1] 200 ms para sistemas de control, 100 ms para E/S remotas.				

Tabla 22: Parámetros de sistema del recurso a partir de V.7

Variables de sistema del hardware a partir de S.Op. V.7 de CPU

Estas variables sirven para modificar en ciertas circunstancias la respuesta del sistema de control ya en funcionamiento. Estas variables pueden reajustarse en el editor de hardware de SILworX, en la vista detallada del hardware.

Parámetro/Switch	Función	Config. por defecto	Ajuste para funcionamiento seguro
Force Deactivation	Sirve para impedir y desactivar inmediatamente la función de forzado	FALSE	Específico de la aplicación
Spare 0 ... Spare 16	Sin función	-	-
Emergency Stop 1 ... Emergency Stop 4	Elementos de desactivación de urgencia del sistema de control en caso de fallos detectados por el programa de usuario	FALSE	Específico de la aplicación
Relay Contact 1… Relay Contact 4	¡Aplicable solamente en L3! Sirve para excitar los contactos de relé, en tanto los haya.	FALSE	Específico de la aplicación
Read-only in Run	Una vez iniciado el sistema de control el usuario no podrá intervenir (Stop, Start, Download) mediante SILworX. Excepciones: Forcing y Reload	FALSE	Específico de la aplicación
Reload Deactivation	¡Aplicable solamente en L3! Impide cargar el sistema de control mediante Reload.	FALSE	Específico de la aplicación
User-LED 1… User LED 2	¡Aplicable solamente en L3! Sirve para excitar los LEDs correspondientes, en tanto los haya.	FALSE	Específico de la aplicación

Tabla 23: Variables de sistema del hardware a partir del S.Op. V.7 de CPU

A estas variables del sistema podrá Ud. asignarles variables globales, cuyo valor será modificado por una entrada física o por la lógica del programa de usuario.

Ejemplo: a una entrada digital se ha conectado un interruptor de llave. La entrada digital se ha asignado a una variable global, la cual está asignada a la variable de sistema *Read only in Run*. Entonces el propietario podrá usar su llave para habilitar o impedir las acciones Stop, Start y Download.

7.4.2 Parámetros de sistema hasta S.Op. V.7 de CPU

Switch	Función	Valor por defecto	Ajuste para funcionamiento seguro
Main Enable	Durante el funcionamiento (= RUN) podrán modificarse los siguientes parámetros/switches con el PADT.	ON	OFF [1]
Autostart	Inicio automático tras encender el sistema de control.	OFF	ON / OFF [2]
Start/Restart Allowed	Arranque en frío o caliente mediante el PADT en los estados RUN o STOP.	ON	OFF [1]
Load Allowed	Habilitación de carga para un programa de usuario.	ON	ON
Test Mode Allowed	Se permite o prohíbe el modo de prueba para el programa de usuario. En el modo de prueba se congela o detiene la ejecución cíclica del programa. Las salidas permanecen actuadas y el programa podrá ejecutarse paso por paso.	OFF	OFF
Changing the variables in the OLT allowed	Los valores de las variables pueden verse y modificarse en los recuadros OLT (Online-Test) de la lógica.	OFF	OFF [3]
Forcing Allowed	Se permite introducir y habilitar valores para variables/señales del PES, independientemente del valor actual de la señal de proceso o de la lógica.	OFF	Definido por el organismo de inspección
Stop at Force Timeout	Detención de la CPU si se sobrepasa el tiempo de forzado.	ON	Definido por el organismo de inspección

[1] En el modo RUN solamente podrá cambiarse al valor OFF.

[2] La elección de ON u OFF dependerá de la aplicación.

[3] En el modo RUN solamente podrá cambiarse a ON.

Tabla 24: Parámetros de sistema del recurso hasta la V.7 del S.Op. de la CPU

Para el forzado pueden establecerse otros switches y parámetros.

7.5 Protección contra manipulaciones

El usuario deberá acordar junto con el organismo de inspección cuáles son las medidas de protección a aplicar contra la manipulación.

En el PES y en la utilidad de programación hay mecanismos de protección integrados que evitan modificaciones accidentales o no autorizadas del sistema de seguridad:

- Una modificación del programa de usuario o de la configuración origina un nuevo CRC.
- Los derechos de acceso dependen del nivel del usuario de la sesión en curso en el PES.
- Para conectarse al PES, la utilidad de programación necesita la contraseña del usuario de la sesión en curso.
- No es necesario tener conectados PADT y PES durante el modo RUN y es posible interrumpir la conexión.

Deberán observarse las exigencias de las normas de aplicación y de seguridad relativas a la protección contra manipulación. La autorización del personal y las necesarias medidas de protección a tomar son responsabilidad de la empresa usuaria.

NOTA

¡Al sistema de control HIMatrix deberá acceder solo personal autorizado!

Tome las siguientes medidas para prevenir modificaciones no autorizadas del sistema de control:

- **Cambie el nombre y la contraseña originales predeterminadas.**
- **Cada usuario deberá mantener su contraseña en secreto.**
- **Tras concluir la puesta en servicio, desconecte del sistema de control el PADT y no lo vuelva a conectar hasta que tenga que realizarse alguna modificación.**

Solamente se podrá acceder a los datos del PES si el PADT utilizado dispone de la utilidad de programación y el proyecto del usuario en la versión actual (cuidado de ficheros).

La conexión entre PADT y PES es necesaria solamente para descargar (download) el programa de usuario o para leer las variables/señales. El PADT no es necesario durante el funcionamiento normal. Desconectar el PADT del PES en el estadio del funcionamiento normal evita posibles intervenciones no autorizadas.

7.6 Lista de chequeo de creación de un programa de usuario

Esta es una lista de chequeo recomendada al usuario para el cumplimiento de los aspectos de seguridad instrumentada en la programación, antes y después de cargar el programa nuevo o modificado.

La lista de chequeo *HIMatrix_Checklist_Programm.doc* está disponible en formato Microsoft Word©. El archivo ZIP *HIMatrix_Checklists.zip* contiene todas las listas de chequeo y podrá descargarse del sitio www.hima.com.

8 Aspectos de seguridad instrumentada para el programa de usuario

Procedimiento general de programación de dispositivos de automatización HIMatrix para aplicaciones de seguridad instrumentada:

- Especificación de la función del sistema de control.
- Escritura del programa de usuario.
- Compilar el programa de usuario con el generador de códigos C.
- Traducción doble del programa de usuario y comparación de ambos resultados (CRCs).
- Programa creado sin errores y ejecutable.
- Verificación y validación.

A continuación, el PES podrá adoptar el funcionamiento relacionado con la seguridad.

8.1 Marco de uso relacionado con la seguridad

(consignas, reglamentación y obligaciones de seguridad en el capítulo 3.4)

Introducción del programa de usuario con la utilidad de programación correspondiente:

- SILworX para sistemas operativos a partir de la versión V.7 del S.Op. de la CPU.
- ELOP II Factory para sistemas operativos hasta la versión V.7 del S.Op. de la CPU.

Los sistemas operativos autorizados para PCs pueden consultarse en la lista de la utilidad de programación.

La utilidad de programación contiene básicamente:

- Introducción (editor de bloques funcionales), monitoreo y documentación.
- Variables con tipo de datos y nombres simbólicos (BOOL, UINT etc.).
- Asignación de los sistemas de control del sistema HIMatrix.
- Generador de códigos (traducción del programa del usuario al código máquina).
- Configuración del hardware.
- Configuración de la comunicación.

8.1.1 Base de la programación

El cometido del sistema de control debe constar en forma de una especificación o de un cuaderno de especificaciones. Dicha documentación es la base para comprobar la correcta implementación en el programa de usuario. El tipo de presentación de la especificación depende del planteamiento de tareas. Puede ser:

- Lógica combinatoria
  - Diagrama de causa y efecto.
  - Lógica de los nexos entre funciones y bloques funcionales.
  - Bloques funcionales de propiedades específicas.
- Sistemas de control secuenciales (de desarrollo cíclico).
  - Descripción verbal de los actuadores a controlar y de los pasos con condiciones para la prosecución del proceso.
  - Diagramas de flujo.
  - Tablas o matrices de los actuadores a controlar y de las condiciones para la prosecución del proceso.
  - Definición de las restricciones, p.ej. modos operativos, parada de emergencia, etc.

El concepto de E/S de la instalación o el equipo a controlar deberá contener el análisis de los circuitos de campo, es decir, el tipo de sensores y actuadores:

- Sensores (digitales o analógicos).
  - Señal en el funcionamiento normal (principio de corriente de reposo para sensores digitales, life-zero para sensores analógicos).
  - Señal en caso de error.
  - Definición de las redundancias de seguridad instrumentada requeridas (1oo2, 2oo3) (ver capítulo “Aumento del nivel SIL de sensores y actuadores”).
  - Monitoreo de discrepancias y reacción.
- Actuadores.
  - Posición y actuación en el funcionamiento normal.
  - Reacción segura y posición en caso de desconexión o corte de energía.

Objetivos para la programación del programa de usuario:

- Fácil de entender.
- Fácil de seguir.
- Fácil de modificar.
- Fácil de probar.

8.1.2 Funciones del programa de usuario

La programación no está sujeta a restricciones de hardware. Las funciones del programa de usuario son libremente programables.

- Dentro de la lógica se usan únicamente elementos conforme a IEC 61131-3 con sus correspondientes condiciones funcionales.
- Las E/S físicas funcionan generalmente según el principio de corriente de reposo, es decir, su estado seguro es *0*. Habrá que tenerlo en cuenta para la programación.
- El programa de usuario contiene prácticas funciones lógicas y/o aritméticas sin consideración del principio de corriente de reposo de las E/S físicas.
- La lógica deberá haberse concebido con claridad y estar comprensiblemente documentada para hacer más fácil la localización de errores. Esto incluye la utilización de diagramas de funciones.
- Se admiten las negaciones que se quiera.
- Deberán evaluarse las señales de error de las E/S o de los bloques lógicos.

Es importante encapsular las funciones en bloques funcionales de propia creación y funciones estándares. Así, un programa podrá estructurarse claramente en módulos (funciones, bloques funcionales). Cada módulo podrá contemplarse por separado, constituyendo un módulo mayor o un programa si se ensambla con otros módulos, originando una función compleja preparada.

8.1.3 Declaración de variables y señales

Una variable es un comodín para un valor dentro de la lógica de programación. Mediante el nombre de la variable se direcciona simbólicamente el lugar de memoria con el valor guardado en memoria. Una variable se crea en la declaración de variables del programa o de un bloque funcional.

	Cantidad de caracteres para nombres de variables
A partir de S.Op V.7 de CPU	31
Hasta S.Op. V.7 de CPU	256

Tabla 25: Longitud de los nombres de las variables

La utilización de nombres simbólicos en lugar de direcciones físicas tiene dos ventajas fundamentales:

- En el programa de usuario podrá Ud. usar las mismas designaciones de entradas y salidas de su planta.
- La reasignación de las variables a otros canales de entrada o salida no afectará al programa de usuario.

A partir de la versión V.7 del S.Op. de la CPU ya no hay señales, sino solo variables.

Las variables no inicializadas tienen tras un inicio en frío el valor inicial 0 o FALSE.

Las variables cuya fuente no sea válida, p.ej. por errores de hardware en la entrada física, adoptarán el valor inicial configurado.

Señales – S.Op. de CPU anterior a V.7

Una señal sirve de asignación entre diversas áreas de todo el sistema de control. La señal se crea en el editor de señales y corresponderá al nivel global de una VAR_EXTERNAL del programa, siempre y cuando se haya establecido el vínculo.

8.1.4 Aprobación por parte de las autoridades

HIMA recomienda informar a las autoridades lo más pronto posible en el caso de proyectos que requieran de la aprobación de las autoridades.

8.2 Procedimientos

Este capítulo describe los procedimientos más habituales de realización de programas de usuario para sistemas de control HiMatrix con función relacionada con la seguridad.

8.2.1 Asignación de variables a las entradas/salidas

Las rutinas de comprobación requeridas para canales de E/S, módulos de E/S o dispositivos de E/S con función relacionada con la seguridad las ejecuta automáticamente el sistema operativo.

La asignación de las variables utilizadas en el programa de usuario es diferente en ELOP II Factory y SILworX.

A partir de la versión 7 del sistema operativo

Asignar una variable a un canal de E/S

1. Defina una variable global del tipo apropiado.
2. En la definición especifique un valor inicial apropiado.
3. Asigne la variable global al valor de canal del canal de E/S.
4. Evalúe en el programa de usuario el código de error -> *Error Code [Byte]* y programe una reacción relacionada con la seguridad.

La variable global queda asignada a un canal de entrada/salida.

Hasta la versión 7 del sistema operativo

Si desea asignar el valor de una variable a un canal de E/S, proceda así:

Asignar una variable a un canal de E/S

1. Defina una variable del tipo apropiado.
2. Defina en el editor de señales del administrador de hardware una señal con el mismo nombre que la variable.
3. Arrastre la señal con el ratón hasta la declaración de variables del programa.
4. Arrastre la señal con el ratón hasta la lista de canales del módulo de E/S.
5. Evalúe en el programa de usuario el código de error y programe una reacción relacionada con la seguridad.

La variable queda asignada a un canal de E/S.

El nombre de la señal de sistema para el código de error depende del tipo de canal de E/S.

8.2.2 Bloqueo y desbloqueo del sistema de control

El bloqueo (*Locking*) del sistema de control significa restringir las posibilidades de intervención del usuario durante el funcionamiento. Así se evitan posibles manipulaciones del programa de usuario. El alcance de las restricciones habrá de corresponder a los requisitos de seguridad de uso del PES, pero también podrá acordarse con el respectivo organismo de inspección.

El desbloqueo (*Unlocking*) del sistema de control significa eliminar el bloqueo activo, por ejemplo para realizar trabajos de reglaje del sistema de control.

i ¡El bloqueo y el desbloqueo son posibles solamente para los sistemas de control y la E/S remota F3 DIO 20/8 01, no para otras E/S remotas!

A partir de S.Op V.7 de CPU

Para bloquear se usan tres variables de sistema:

Variable	Función
Read only in Run	ON: Acciones Stop, Start, Download del control inhabilitadas. OFF: Acciones Stop, Start, Download del control habilitadas.
Reload Deactivation	ON: La función Reload está inhabilitada. OFF: La función Reload está habilitada.
Force Deactivation	ON: “Forcing” desactivado. OFF: “Forcing” posible.

Tabla 26: Variables de sistema para bloqueo/desbloqueo del PES

Si las tres variables de sistema están aplicadas (ON), no será posible intervenir en el sistema de control. En tal caso, el sistema de control únicamente podrá ponerse en el estado STOP/VALID CONFIGURATION mediante un reinicio. Entonces se podrá cargar de nuevo un programa de usuario.

Ejemplo de uso de estas variables de sistema:

Para hacer bloqueable un sistema de control

1. Defina una variable global de tipo BOOLEANO y elija OFF como valor inicial.
2. Asigne variables globales a las tres variables de sistema *Read only in Run*, *Reload Deactivation* y *Force Deactivation*.
3. Asigne una variable global al valor de canal de una entrada digital.
4. Conecte un interruptor de llave a la entrada digital.
5. Compile el programa, cárguelo al sistema de control e inícielo.

Quien disponga de la llave adecuada podrá bloquear y desbloquear el sistema de control. En caso de error en el correspondiente módulo de entrada o dispositivo de entrada digital, el sistema de control estará desbloqueado.

Hasta S.Op. V.7 de CPU

Locking: para bloquear el PES debe seguirse este procedimiento:

Bloqueo del sistema de control

1. Ajuste los siguientes valores en el sistema de control antes de compilar (ver capítulo “Generación de códigos”):

Main Enable	en	ON
Forcing Allowed	en	OFF (según aplicación)
Test Mode Allowed	en	OFF
Start/Restart Allowed	en	ON
Load Allowed	en	ON
Autostart	en	ON/OFF
Stop at Force Timeout	en	ON (según aplicación)

2. Tras cargarlo e iniciarlo en el sistema de control, modifique los siguientes switches en este orden:

Start/Restart Allowed	en	OFF
Load Allowed	en	OFF
Main Enable	en	OFF

i Solo tras consultarlo al organismo de inspección podrán cambiarse los valores de los siguientes switches:

Forcing Allowed	en	ON
Stop at Force Timeout	en	ON/OFF
Start/Restart Allowed	en	ON
Autostart	en	ON

El sistema de control está bloqueado.

Unlocking: condición previa para el desbloqueo (Main Enable ON) es que el sistema de control esté detenido (estado STOP). No es posible activar Main Enable para un sistema de control en marcha (estado RUN), pero sí es posible desactivarlo.

Para permitir un nuevo inicio tras inicializarse la CPU (tras un corte de tensión) habrá que proceder de la siguiente manera al desbloquear el PES:

Desbloqueo del sistema de control

1. Ponga Main Enable en ON.
2. Ponga Start/Restart en ON.
3. Inicie el programa de usuario.

El sistema de control está desbloqueado.

8.2.3 Generación de códigos

Tras completar la introducción del programa de usuario y la asignación de E/S del sistema de control, genere el código. El generador de códigos crea el CRC de configuración. Se trata de una signatura de toda la configuración de CPU, E/S y comunicación que se genera en código hexadecimal y formato de 32 bits. La signatura abarca todos los elementos configurables o modificables, tales como: lógica, variables y posiciones de switches.

Para descartar influencias del PC no seguro, genere el código dos veces. El CRC de configuración deberá ser idéntico en ambos casos.

Generación de código para funcionamiento relacionado con la seguridad

1. Inicie el generador de códigos para crear el código de CRC de configuración.
   ☑ Código ejecutable 1 con CRC 1.
2. Vuelva a iniciar el generador de códigos para crear el código de CRC de configuración.
   ☑ Código ejecutable 2 con CRC 2.
3. Compare el CRC 1 y el CRC 2.
   ☑ Ambos son idénticos.

El código generado es utilizable para el funcionamiento relacionado con la seguridad y también para la certificación por parte de los organismos oficiales de inspección.

8.2.4 Carga e inicio del programa de usuario

El proceso de carga (Download) de un PES del sistema HIMatrix solamente podrá tener lugar cuando previamente este haya adoptado el estado STOP.

Versión de hardware	Cantidad de programas de usuario por sistema de control
Hasta L3	1
L3	1…32

Tabla 27: Cantidad de programas de usuario en un PES

El sistema monitorea que el programa de usuario se cargue íntegramente. A continuación podrá iniciarse el programa de usuario, es decir, la ejecución cíclica de la rutina.

i HIMA recomienda hacer una copia de seguridad de los datos del proyecto (p.ej. en un disco) cada vez que se cargue un programa de usuario al sistema de control.

Así quedará garantizado que los datos del proyecto correspondientes a la configuración que obre en el sistema de control sigan disponibles aun en caso de que falle el PADT.

HIMA recomienda realizar también copias de seguridad de datos independientemente de la carga del programa.

8.2.5 Reload – en L3

Si se efectúan modificaciones en programas de usuario, estas podrán transferirse al sistema PES sin interrumpir el funcionamiento. El sistema operativo comprueba y habilita el programa de usuario modificado, tras lo cual este asume el control.

i **Al cargar cadenas de pasos por reload, observe:**

La información de reload de cadenas de pasos no considera el estado actual de la cadena. Por ello es posible que, en caso de cargar por reload una modificación dada de la cadena de pasos, ésta adopte un estado indefinido. Ello será responsabilidad del usuario.

Ejemplos:

- Borrado del paso activo. A continuación no habrá ningún paso de la cadena en estado *active.*
- Cambio del nombre del paso inicial mientras hay otro paso activo. Ello dará lugar a una cadena de pasos con dos pasos activos.

i **Al cargar “Actions” por reload, observe:**

La función reload carga “Actions” con todos sus datos. Considere cuidadosamente las consecuencias resultantes antes de cargar por reload.

Ejemplos:

- Si se elimina el calificador de un temporizador debido al reload, ello hará que el tiempo del temporizador expire inmediatamente. Ello puede originar que la salida *Q* cambie a TRUE según los demás estados asignados.
- La eliminación del calificador en elementos anexos (p. ej. el calificador *S*) que estén aplicados hará que los elementos permanezcan aplicados.
- La eliminación de un calificador *P0* que estuviera en estado TRUE desencadenará el excitador.

8.2.6 Forzado

"Forcing" significa la sustitución del valor actual de una variable por un valor forzado. Una variable puede recibir su valor actual por una entrada física, por comunicación o por un nexo lógico. Si se fuerza la variable, su valor no dependerá ya del proceso, sino del valor que indique el usuario.

⚠ ADVERTENCIA

¡Posible perturbación del funcionamiento relacionado con la seguridad por valores forzados!

- **Los valores forzados pueden dar lugar a falsos valores de salida.**
- **El forzado prolonga la duración del ciclo. Ello puede hacer que se exceda el tiempo de WatchDog.**

Se permite usar la función "Forcing" solamente tras consultar al organismo oficial responsable del acta de aprobación del equipo.

Durante el forzado, la persona responsable deberá garantizar una suficiente supervisión por seguridad instrumentada del proceso mediante otras medidas técnicas y organizativas. HIMA recomienda limitar temporalmente el forzado.

Hallará más información sobre el forzado en los manuales de los sistemas compactos HI 800 495 S y los sistemas modulares HI 800 494 S.

8.2.7 Modificación en línea de parámetros del sistema – A partir de S.Op. V.7

Algunos parámetros/switches de sistema podrá Ud. modificarlos en línea en el sistema de control. Un caso típico sería el aumento provisorio del tiempo de WatchDog para poder realizar una carga mediante la función de reload.

Parámetros modificables en línea:

Parámetro	Layout del hardware	Versión del sistema operativo
System ID	Todos	Todos
Resource Watchdog Time	Todos	Todos
Safety Time	Todos	Todos
Target Cycle Time	Todos	A partir de S.Op V.8 de CPU
Target Cycle Time Mode	L3	A partir de S.Op V.8 de CPU
Main Enable	Todos	Todos
Autostart	Todos	Todos
Start Allowed	Todos	Todos
Load Allowed	Todos	Todos
Reload Allowed	L3	A partir de S.Op V.8 de CPU
Global Forcing Allowed	Todos	Todos
Global Force Timeout Reaction	Todos	Todos

Tabla 28: Parámetros modificables en línea según layout de hardware y versión del sistema operativo

Antes de aplicar los parámetros mediante un comando en línea hay que analizar si esa modificación de parámetros puede originar estados peligrosos. De ser necesario, deberán tomarse medidas organizativas y/o técnicas para descartar posibles casos de daños.

Main Enable permite modificar los demás parámetros. *Main Enable* solamente podrá cambiarse a TRUE en el estado STOP.

Los valores del tiempo de seguridad y del tiempo de WatchDog habrán de cotejarse con el tiempo de seguridad requerido por la aplicación y con el tiempo de ciclo real. ¡El PES no puede verificar estos valores!

En L3 es posible realizar modificaciones, también durante el funcionamiento, mediante carga por reload.

8.2.8 Documentación de programa para aplicaciones relacionadas con la seguridad

La utilidad de programación permite imprimir automáticamente la documentación de un proyecto. Los tipos principales de documentación son:

- Declaración de interfaces
- Lista de señales
- Lógica
- Descripción de los tipos de datos
- Configuraciones de sistema, módulos y parámetros de sistema
- Configuración de la red
- Lista de referencia cruzada de señales
- Información del generador de códigos

La documentación forma parte del acta de aprobación de funciones de un sistema sujeto a autorización por parte de un organismo de inspección oficial (p.ej. TÜV). La aprobación se refiere solamente a la función del usuario, pero no a los módulos y dispositivos de automatización con función relacionada con la seguridad del sistema HIMatrix, pues estos ya han pasado el examen de tipos.

8.2.9 Multitasking – en L3

Multitasking designa la capacidad del sistema HIMatrix Layout3 de ejecutar hasta 32 programas de usuario dentro del sistema procesador.

Los programas de usuario podrán iniciarse, detenerse, cargarse (también por reload) o borrarse independientemente unos de otros.

El ciclo de un programa de usuario puede durar varios ciclos del procesador. Esto puede dirigirse mediante los parámetros del recurso y del programa de usuario. A partir de estos parámetros, SILworX calcula el tiempo de WatchDog del programa de usuario:
WatchDog $\text{Time}_{\text{progr. usuario}}$ = *WatchDog* $\textit{Time}_{\text{mód. procesador}}$ * *Maximum Number of Cycles*

Los distintos programas de usuario se ejecutan generalmente sin repercusiones entre ellos. Sin embargo pueden influir unos sobre otros mediante:

- Utilización de las mismas variables globales en varios programas de usuario.
- Tiempos de ejecución imprevisiblemente largos en algunos programas de usuario en caso de no haber limitación por *Max. Duration for Each Cycle*.
- ¡La distribución de ciclos de programa de usuario a lo largo de ciclos del módulo procesador afecta notablemente al tiempo de reacción del programa de usuario y las variables que este escribe!
- Un programa de usuario evaluará variables globales escritas por otro programa de usuario en tantos ciclos del sistema procesador como defina el parámetro de sistema *Program's Maximum Number of CPU Cycles* para el programa. En casos desfavorables, es posible que se dé la siguiente secuencia:
  - El programa A escribe variables globales que necesita el programa B.
  - El programa A finaliza su ciclo en el mismo ciclo del sistema procesador en el que el programa B inicia su ciclo.
  - Entonces, el programa B no podrá leer hasta su siguiente ciclo los valores escritos por el programa A.

- El ciclo de B recién iniciado podrá durar un tiempo igual a *Program's Maximum Number of CPU Cycles**Cycle Time. Solo en ese momento recibirá B los valores escritos por A.
- Hasta que B reaccione a esos valores pueden transcurrir más ciclos: *Program's Maximum Number of CPU Cycles*.

NOTA

¡Posibles repercusiones recíprocas entre programas de usuario!

La utilización de las mismas variables globales en varios programas de usuario puede originar una influencia recíproca de los programas de usuario con efectos diversos.

- **Planifique exactamente la utilización de variables globales en varios programas de usuario.**
- **Use las referencias cruzadas de SILworX para examinar la utilización de datos globales. ¡Los datos globales solamente podrán ser escritos con valores desde un lugar: bien en un programa de usuario, por entradas relacionadas con la seguridad o por protocolos de comunicación relacionados con la seguridad!**

¡Es responsabilidad del usuario excluir posibles perturbaciones del funcionamiento debido a influencias recíprocas entre programas de usuario!

Más información sobre Multitasking en el manual de sistemas compactos HI 800 495 S o de sistemas modulares HI 800 494 S.

8.2.10 Aprobación por parte de las autoridades

Se recomienda informar a las autoridades lo más pronto posible en el caso de proyectos que requieran de su aprobación.

La aprobación se refiere solo a la función del usuario, pero no a los módulos y dispositivos de automatización con función relacionada con la seguridad del sistema HIMax, pues estos ya han pasado el examen de tipos.

9 Configuración de la comunicación

Además de las variables físicas de entrada y salida, podrán intercambiarse variables también con otro sistema mediante una conexión de datos. Para ello se declaran las variables del respectivo recurso en el editor de protocolos de la utilidad de programación.

Este intercambio de datos puede ser tanto de lectura como de escritura.

9.1 Protocolos estándar

Toda una serie de protocolos de comunicación permite solamente una transmisión de datos no relacionada con la seguridad. Estos podrán usarse para las partes de una tarea de automatización no relacionadas con la seguridad.

⚠ PELIGRO

¡Daños personales a causa del uso de datos importados no seguros!

¡No use datos importados de fuentes no seguras para las funciones de seguridad del programa de usuario!

Se dispone, según variante del sistema de control, de los siguientes protocolos estándar:

- SNTP
- Send/Receive TCP
- Modbus (Master/Slave)
- PROFIBUS DP (Master/Slave)
- INTERBUS.

9.2 Protocolo relacionado con la seguridad (safe**ethernet)**

La comunicación relacionada con la seguridad mediante safe**ethernet** está certificada hasta el nivel SIL 3.

El monitoreo de la comunicación relacionada con la seguridad habrá que parametrizarlo en Editor/Peer-to-Peer-Editor safe**ethernet**.

Para el cálculo de los parámetros safe**ethernet** *Receive Timeout* y *Response Time* rige la siguiente condición:
El intervalo de tiempo de comunicación (Com. Time Slice) deberá ser lo suficientemente grande como para poder procesar en un ciclo de la CPU todas las conexiones safe**ethernet**.

Para las funciones relacionadas con la seguridad implementadas mediante safe**ethernet** solamente se permite configurar la opción *Use Initial Data*.

NOTA

¡Es posible una transición involuntaria al estado seguro!

¡*ReceiveTMO* es un parámetro relacionado con la seguridad!

El valor de una señal deberá estar presente más tiempo que *ReceiveTMO* o ser monitoreado mediante Loop-Back, en caso de desear transmitir cada valor.

ReceiveTMO es el tiempo de monitoreo en el sistema de control 1, dentro del cual deberá recibirse una respuesta correcta del sistema de control 2.

9.2.1 Receive Timeout

ReceiveTMO es el tiempo de monitoreo, en ms, dentro del cual deberá recibirse una respuesta correcta del interlocutor de comunicación.

Si dentro del tiempo *ReceiveTMO* no se recibe respuesta correcta del interlocutor de comunicación, se cerrará la comunicación relacionada con la seguridad. Las variables de entrada de esta conexión safe**ethernet** se comportarán tal y como lo defina el parámetro *Freeze Data on Lost Connection [ms]*.

Para las funciones relacionadas con la seguridad implementadas mediante safe**ethernet** solamente se permite configurar la opción **Use Initial Data**.

Puesto que *ReceiveTMO* es relevante para la seguridad y forma parte del tiempo Worst Case Reaction Time T_R (véase el máximo tiempo de reacción en el apartado 9.2.3 y ss), *ReceiveTMO* deberá calcularse y registrarse en el editor safe**ethernet** de la siguiente forma.

ReceiveTMO ≥ 4*delay + 5*max. cycle time

Condición: el intervalo de tiempo de comunicación (Com. Time Slice) deberá ser lo suficientemente grande para poder procesar en un ciclo de la CPU todas las conexiones safe**ethernet**.

Delay:	Retardo en la línea de transmisión, p.ej. por switch o satélite
Max. Cycle Time	Tiempo máximo de ciclo de ambos sistemas de control

i Si se desea una tolerancia a errores de comunicación, ello podrá lograrse aumentando el tiempo *ReceiveTMO*, siempre y cuando ello sea admisible para el proceso de aplicación desde el punto de vista de los tiempos.

NOTA

El valor máximo admisible para *ReceiveTMO* depende del proceso de aplicación y se ajusta en el editor safe**ethernet junto con el máximo tiempo de respuesta previsto y el perfil.**

9.2.2 Response Time

El valor de *ResponseTime* es el tiempo, en ms, que transcurre hasta que el emisor de una notificación recibe la confirmación de recepción del destinatario.

Para la parametrización con un perfil safe**ethernet** deberá especificarse un tiempo de respuesta esperable (*ResponseTime*) para la línea de transmisión según las circunstancias físicas.

El tiempo *ResponseTime* especificado afectará a la configuración de todos los parámetros de la conexión safe**ethernet** , que deberá Ud. calcular de la siguiente manera:

ResponseTime ≤ ReceiveTMO / n

n = 2, 3, 4, 5, 6, 7, 8…..

La relación entre *ReceiveTMO* y *ResponseTime* afecta a la capacidad de tolerancia de errores, p.ej. en caso de pérdida de paquetes de datos (repetición del paquete perdido) o retardos en la línea de transmisión.

En una red donde puedan producirse pérdidas de paquetes de datos, deberá cumplirse la siguiente condición:

Min. Response Time ≤ ReceiveTMO / 2 ≥ 2*Delay + 2.5*max. Cycle Time

Si se cumple esta condición, podrá cubrirse la pérdida de al menos un paquete de datos sin que se interrumpa la conexión safe**ethernet**.

i Si no se cumple esta condición, la disponibilidad de una conexión safe**ethernet** solamente estará garantizada si se usa en una red libre de perturbaciones y colisiones. ¡En todo caso, ello no representa un problema de seguridad para el módulo procesador!

i ¡Habrá que garantizar que el sistema de comunicación cumpla el tiempo Response-Time parametrizado!

Para los casos en que esto no siempre pueda garantizarse, se dispone de una correspondiente variable de sistema de la conexión para monitorear el tiempo Response-Time. Si no es solo en casos aislados que se excede el tiempo Response-Time medido a lo largo de la mitad del ReceiveTMO, deberá aumentarse el tiempo Response Time parametrizado.

El Receive Timeout deberá adaptarse al Response Time ahora parametrizado.

NOTA

En los siguientes ejemplos, las fórmulas de cálculo del máximo tiempo de reacción de una conexión con sistemas de control HIMatrix tendrán validez solamente cuando para estos se haya definido:

safety time = 2 * watchdog time

9.2.3 Tiempo máximo de ciclo del sistema de control HIMatrix

Para determinar el tiempo máximo de ciclo de un sistema de control HIMatrix, HIMA recomienda el siguiente procedimiento:

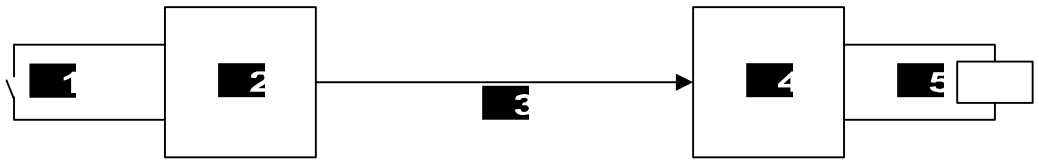
Determinación del tiempo máximo de ciclo del sistema de control HIMatrix

1. Haga funcionar el sistema a plena carga. Deberán estar en uso todas las conexiones de comunicación, tanto por safe**ethernet** como por protocolos estándares. Lea frecuentemente el tiempo de ciclo en el panel de control y anote el tiempo máximo del ciclo.
2. Repita el paso 1 para el interlocutor de comunicación (segundo sistema de control HiMatrix).
3. El mayor de ambos tiempos de ciclo registrados será el máximo tiempo de ciclo buscado.

El tiempo máximo de ciclo queda determinado y se usará para los subsiguientes cálculos.

9.2.4 Cálculo del tiempo máximo de reacción

El tiempo máximo de reacción T_R (*Worst Case Reaction Time*) desde el cambio de estado de una entrada del PES 1 hasta la reacción de la salida del PES 2 puede calcularse como sigue:



1 Entrada
2 Sistema de control HIMatrix - PES 1
3 Protocolo relacionado con la seguridad
4 Sistema de control HIMatrix - PES 2
5 Salida

Fig. 4: Tiempo de reacción en caso de conectar dos sistemas de control HIMatrix

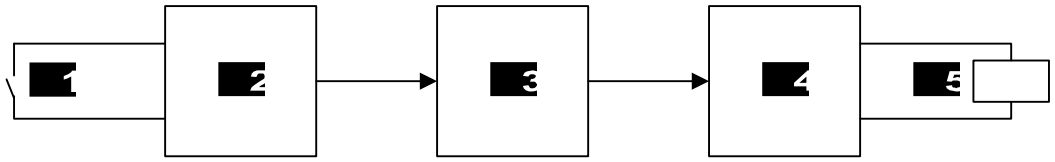
$$T_R = t_1 + t_2 + t_3$$

T_R Worst Case Reaction Time
t_1 2 * tiempo de WatchDog del sistema de control HIMatrix 1
t_2 ReceiveTMO
t_3 2 * tiempo de WatchDog del sistema de control HIMatrix 2

El tiempo máximo de reacción dependerá del proceso y habrá de acordarse con el organismo de inspección oficial que deba emitir su aprobación.

9.2.5 Cálculo del tiempo máximo de reacción con dos E/S remotas

El tiempo máximo de reacción T_R desde el cambio de estado de una entrada del primer PES HIMatrix o la respectiva E/S remota (p.ej. F3 DIO 20/8 01) hasta la reacción del segundo PES HIMatrix o E/S remota puede calcularse de la siguiente forma:



1 Entrada
2 E/S remota 1
3 Sistema de control HIMatrix
4 E/S remota 2
5 Salida

Fig. 5: Tiempo de reacción con E/S remotas

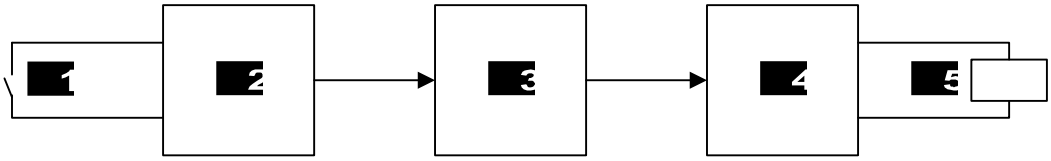
$$T_R = t_1 + t_2 + t_3 + t_4 + t_5$$

T_R Worst Case Reaction Time
t_1 2 * tiempo de WatchDog de la E/S remota 1
t_2 $ReceiveTMO_1$
t_3 2 * tiempo de WatchDog del sistema de control HIMatrix
t_4 $ReceiveTMO_2$
t_5 2 * tiempo de WatchDog de la E/S remota 2

Comentario: las dos E/S remotas 1 y 2 también pueden ser idénticas. Los tiempos serán válidos aun cuando en lugar de una E/S remota se utilice un sistema de control HIMatrix.

9.2.6 Cálculo del tiempo máx. de reacción con 2 sistemas HIMatrix y 1 HIMax

El tiempo máximo de reacción T_R desde el cambio de estado de una entrada del primer PES HIMatrix hasta la reacción de la salida del segundo PES HIMatrix puede calcularse de la siguiente forma:



1 Entrada
2 Sistema de control HIMatrix 1
3 Sistema de control HIMax
4 Sistema de control HIMatrix 2
5 Salida

Fig. 6: Tiempo de reacción con dos sistemas de control HIMatrix y un HIMax

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

T_R	Worst Case Reaction Time
t_1	2 * tiempo de WatchDog del sistema de control HIMatrix 1
t_2	ReceiveTMO$_1$
t_3	2 * tiempo de WatchDog del sistema de control HIMax
t_4	ReceiveTMO$_2$
t_5	2 * tiempo de WatchDog del sistema de control HIMatrix 2

Comentario: el 1er y 3er sistema de control HIMatrix también pueden ser idénticos.

9.2.7 Términos

ReceiveTMO	Tiempo de monitoreo en el sistema de control 1, dentro del cual deberá recibirse una respuesta válida del sistema de control 2. Tras expirar el tiempo se cerrará la comunicación relacionada con la seguridad.
Production Rate	Separación mínima entre dos envíos de datos.
Watchdog Time	Máxima duración admisible del ciclo RUN de un sistema de control
Worst Case Reaction Time	Máximo tiempo de reacción para la transmisión del cambio de la señal de una entrada física de un sistema de control 1 hasta el cambio de la salida física de un sistema de control 2.

9.2.8 Asignación de las direcciones safe**ethernet**

Al asignar las direcciones de red (direcciones IP) para safe**ethernet** observe lo siguiente:

- Las direcciones deberán ser únicas en la red utilizada.
- Al conectar la red safe**ethernet** a otra red (LAN interna de la empresa, etc.), cuide de que no puedan producirse perturbaciones. Posibles fuentes de perturbaciones son p.ej.
  - El tráfico de datos.
  - Acoplamiento a otras redes (p.ej. internet).

En tales casos tome las medidas oportunas (p.ej. switches de Ethernet, Firewall, etc.) para hacer frente a las perturbaciones.

10 Uso en centrales de alarma de incendios

Los sistemas HIMatrix podrán usarse en centrales de alarma de incendios según DIN EN 54-2 y NFPA 72 parametrizando el monitoreo de cable para entradas y salidas.

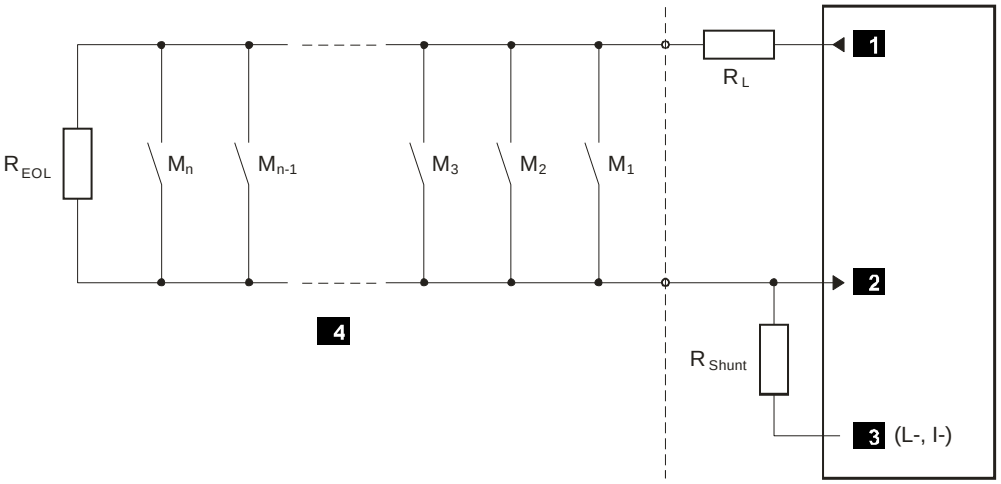
Para ello el programa de usuario deberá cumplir las funcionalidades de centrales de alarma de incendios exigidas por dichas normas.

Los sistemas podrán cumplir fácilmente el tiempo máximo de ciclo de 10 s exigido por la norma DIN EN 54-2 para centrales de alarma de incendios, ya que los tiempos de ciclo de estos sistemas están en el orden de los milisegundos, pudiendo decirse lo mismo del tiempo de seguridad exigido de 1 segundo (tiempo de reacción a errores).

Según EN 54-2, la central de alarma de incendios deberá adoptar el estado de aviso de fallos antes de 100 s tras recibirse el mensaje de fallo en el sistema HIMatrix.

La conexión de la alarma de incendios se realiza según el principio de corriente de trabajo con monitoreo de cortocircuito e interrupción de cables. Para ello podrán usarse los siguientes dispositivos y módulos:

- Las entradas digitales y analógicas del sistema de control F35
- Las entradas analógicas de la E/S remota F3 AIO 8/4 01
- Las entradas y salidas digitales de las E/S remotas F3 DIO 16/8 01 y F3 DIO 8/8 01
- Los módulos de entrada AI 8 01 y MI 24 01 del sistema de control F60



1 Alimentación de sensores
2 Entrada analógica
3 Polo de referencia
4 Bucle de notificación

M Alarma de incendios
R_{EOL} Resistencia de cierre en el último sensor del bucle
R_L Limitación de máx. corriente del bucle
R_{Shunt} Resistencia de medición

Fig. 7: Circuitado de alarmas de incendios

Para esta aplicación, las resistencias R_{EOL}, R_L y R_{Shunt} deberán calcularse según los sensores utilizados y la cantidad de sensores por bucle de notificación. Los datos necesarios al caso pueden consultarse en la respectiva hoja de características del fabricante de los sensores.

Las salidas de alarma para actuar luces de aviso, sirenas, bocinas, etc. se harán funcionar según el principio de corriente de trabajo. En dichas salidas deberá monitorearse el cortocircuito y la interrupción de cables. Esto puede hacerse retroalimentando las señales de salida directamente desde el actuador a las entradas.

La corriente del circuito del actuador puede monitorearse mediante una entrada analógica con un shunt adecuado. Un circuitado en serie del diodo Z y de la resistencia previa protege la entrada frente a sobretensiones en caso de producirse cortocircuitos.

Para la inequívoca detección de interrupción de cables (en salidas DO desexcitadas) deberá usarse, además de las entradas analógicas, una alimentación de transmisores (véase el siguiente croquis):

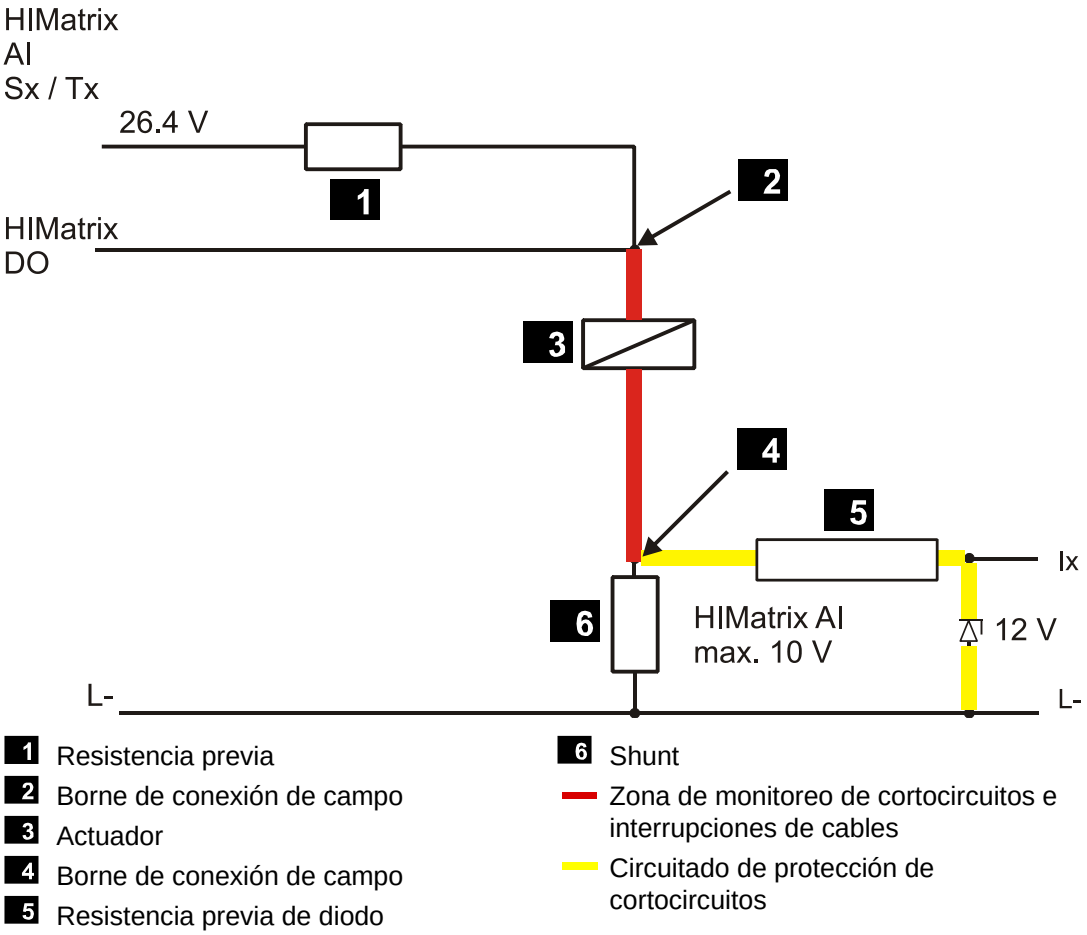


Fig. 8: Ejemplo de monitoreo de cortocircuitos e interrupciones de cables de salidas digitales (circuito de actuador)

En el capítulo *Line Monitoring* del manual de HIMatrix F35 HI 800 148 puede consultarse un ejemplo de parametrización de monitoreo de cortocircuitos con monitoreo adicional de interrupciones de cables de actuadores mediante entradas analógicas.

Con un programa de usuario debidamente adaptado pueden actuarse sistemas de visualización, luces de aviso, LEDs, displays alfanuméricos, alarmas acústicas, etc.

El enrutado de los mensajes de fallo mediante canales de entrada y salida o hacia dispositivos de transmisión de mensajes de fallo deberá realizarse según el principio de corriente de reposo.

La transmisión de las alarmas de incendio desde un sistema HIMatrix a un sistema externo podrá realizarse con el estándar de comunicación Ethernet (OPC) existente. Un posible corte de comunicación deberá detectarse y notificarse.

Los sistemas HIMatrix utilizados como central de alarma de incendios deberán tener alimentación eléctrica redundante. Deberán tomarse asimismo las medidas oportunas para hacer frente a cortes de energía, p.ej. utilizando una bocina con batería de reserva. El cambio de fuente de alimentación desde la red a la fuente de reserva deberá garantizar un funcionamiento exento de interrupciones. Se admiten caídas de tensión de una duración de hasta 10 ms.

En caso de perturbaciones, el sistema operativo escribirá las variables o señales del sistema asignadas en el programa de usuario. Así podrá programarse la señalización de errores en respuesta a los errores detectados por el sistema. En caso de error, el sistema

HIMatrix desactivará las entradas y las salidas relacionadas con la seguridad, con los siguientes efectos:

- Procesado del nivel “Low” en todos los canales de las entradas erróneas.
- Desactivación de todos los canales de las salidas erróneas.

Anexo

Aumento del nivel SIL de sensores y actuadores

Los sistemas de control HIMatrix con función relacionada con la seguridad se usan para aplicaciones de seguridad de hasta un nivel de integridad de seguridad SIL 3. Uno de los requisitos a este respecto es que también los sensores y los actuadores utilizados (transductores de señal y elementos de actuación) satisfagan el nivel SIL exigido.

Puede suceder que no se disponga de sensores o actuadores para los requisitos exigidos en la aplicación, tales como magnitudes de proceso, rango de valores o nivel SIL. De ser así, podrá lograrse el grado SIL requerido de la siguiente manera:

- En las entradas: use los sensores disponibles que satisfagan los requisitos salvo SIL. Use la cantidad necesaria de ellos para que su combinación proporcione una señal de entrada con el nivel SIL requerido.
- En las salidas: use los actuadores disponibles que satisfagan los requisitos salvo SIL. Use la cantidad necesaria de ellos para que su combinación repercuta en el proceso de forma que este satisfaga el nivel SIL requerido.

En las entradas vincule los valores de los distintos sensores y sus informaciones de estado en una parte del programa de usuario de forma que, como resultado de esa combinación, una variable global tenga un valor que satisfaga el nivel SIL.

En las salidas distribuya el valor de una variable global entre varias salidas de forma tal que, en caso de un fallo, el proceso adopte el estado seguro. Para ello, la combinación de actuadores deberá repercutir de forma adecuada en el proceso (ejemplo: conexión en paralelo o en serie de válvulas).

En las entradas y las salidas habrá que planificar la interacción de varios sensores/actuadores para la misma magnitud de proceso de forma tal que ello proporcione la mayor seguridad posible del proceso. Para calcular el nivel SIL use una utilidad de cálculo.

i ¡El uso aquí descrito de varios sensores/actuadores para la entrada/salida de una señal sirve para aumentar el nivel SIL y no debe confundirse con el uso redundante de entradas y salidas para aumentar la disponibilidad del sistema!

En la norma IEC 61511-1, apartado 11.4, hallará más indicaciones para obtener el nivel SIL requerido para los sensores y actuadores.

Glosario

Término	Descripción
ARP	Address Resolution Protocol: protocolo de red para asignar direcciones de red a direcciones de hardware
AI	Analog input: entrada analógica
COM	Módulo de comunicación
CRC	Cyclic Redundancy Check: suma de verificación
DI	Digital input: entrada digital
DO	Digital output: salida digital
CEM	Compatibilidad electromagnética
EN	Normas europeas
ESD	ElectroStatic Discharge: descarga electrostática
FB	Bus de campo
FBS	Lenguaje de bloques funcionales
FTA	Field Termination Assembly
FTT	Tiempo de tolerancia de errores
ICMP	Internet Control Message Protocol: protocolo de red para mensajes de estado y error
IEC	International Electrotechnical Commission: normas internacionales de electrotecnia
Dirección MAC	Dirección de hardware de una conexión de red (Media Access Control)
PADT	Programming and Debugging Tool (según IEC 61131-3), PC con SILworX
PE	Protective Earth: tierra de protección
PELV	Protective Extra Low Voltage: baja tensión funcional con separación segura
PES	Programmable Electronic System
PFD	Probability of Failure on Demand: probabilidad de un fallo al requerir una función de seguridad
PFH	Probability of Failure per Hour: probabilidad de una disfunción peligrosa por hora
R	Read: valor comunicado por señal o variable de sistema, p.ej. al programa de usuario
ID de Rack	Identificación (número) de un rack
Non-reactive: sin repercusiones	Suponiendo que hay dos circuitos de entrada conectados a la misma fuente (p.ej. transmisor). Entonces un circuito de entrada se denominará “*non-reactive*”, cuando no falsee las señales del otro circuito de entrada.
R/W	Read/Write (epígrafe de columna de tipo de señal/variable de sistema)
SB	Bus de sistema (módulo de bus)
SELV	Safety Extra Low Voltage: baja tensión de protección
SFF	Safe Failure Fraction: porcentaje de fallos fácilmente dominables
SIL	Safety Integrity Level (según IEC 61508)
SILworX	Utilidad de programación para sistemas HIMatrix
SNTP	Simple Network Time Protocol (RFC 1769)
S.R.S	Direccionamiento por “Sistema.Rack.Slot” de un módulo
SW	Software
TMO	TimeOut
W	Write: valor ordenado a una señal o variable de sistema, p.ej. desde el programa de usuario
WatchDog (WD)	Control de tiempo para módulos o programas. En caso de excederse el tiempo de WatchDog, el módulo pasará al estado de parada con fallo.
WDT	WatchDog Time

Índice de ilustraciones

Índice de tablas

Índice alfabético

HIMA Paul Hildebrandt GmbH
Apdo. Postal / Postfach 1261
D-68777 Brühl
Tel: +49 6202 709-0
Fax: +49 6202 709-107
E-Mail: info@hima.com Internet: www.hima.com

(1129)