HIMax®

Manual de seguridad

SAFETY
NONSTOP

HIMA

SEGURIDAD

8

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 más información debería incluirse 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 nuestros sitios web http://www.hima.com.

© Copyright 2015, HIMA Paul Hildebrandt GmbH

Todos los derechos reservados.

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
4.00	Adaptación a HIMax V4/SILworX V4 Edición en español (traducción)		

Índice de contenidos

1 Manual de seguridad

El conocimiento de la normativa y la correcta aplicación de las instrucciones de seguridad contenidas en este manual por parte de personal cualificado son requisito indispensable para la planificación, el proyecto, la programación, la instalación, la puesta en servicio exentas de peligro y para la seguridad en el funcionamiento y los trabajos de conservación de los sistemas de automatización HIMax.

En caso de intervenir personal no cualificado, desactivar o puentear (by-pass) funciones de seguridad o hacer caso omiso de las instrucciones de este manual (con las consiguientes perturbaciones y el menoscabo de las funciones de seguridad), pueden producirse situaciones de serio peligro para las personas, los bienes materiales y el medio ambiente, declinando HIMA toda responsabilidad en tales supuestos.

Los dispositivos de automatización HIMax se proyectan, fabrican y ponen a prueba cumpliendo las pertinentes normas de seguridad. Se permite su uso sólo en los casos de aplicación previstos descritos y bajo las condiciones ambientales especificadas.

1.1 Validez y vigencia

Versión Rev. 4.00	Esta revisión tiene validez a partir de la 4ª versión del sistema HIMax.

Es válida siempre la edición más reciente de este manual de seguridad, reconocible por el mayor número de versión. La edición actual puede consultarse en el sitio web *www.hima.com* o en el DVD actual de HIMA.

1.2 Estructuración del manual

Este manual contiene información relativa al uso conforme a la finalidad prevista de los dispositivos de automatización HIMax con función relacionada con la seguridad. Ofrece una introducción al concepto de seguridad del sistema HIMax y tiene como objetivo concienciar al lector en materia de seguridad.

El manual de seguridad se apoya en el contenido del certificado y del informe de ensayos del certificado.

1.3 Destinatarios

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

1.4 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 SILworX sobre los que puede hacerse clic
Cursiva	Variables y parámetros 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 tal, cambiará su aspecto. Haciendo clic en él, se saltará a la correspondiente página del documento.

Las notas de seguridad y uso están especialmente identificadas.

1.4.1 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

1.4.2 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:

SUGE-RENCIA En este punto figura el texto con la sugerencia.

2 Uso conforme a la finalidad prevista

Este capítulo describe las condiciones de uso de sistemas HIMax.

2.1 Ámbito de aplicación

Los sistemas de control HIMax con función relacionada con la seguridad están certificados para el control de procesos, sistemas de protección, quemadores y sistemas de control de máquinas.

Todos los módulos de entrada/salida (módulos de E/S) de HIMax pueden usarse tanto con módulos procesadores individuales como con varios módulos procesadores redundantes juntos.

En la utilización de la comunicación con función relacionada con la seguridad entre diversos dispositivos, deberá observarse que el tiempo total de reacción del sistema no sobrepase el tiempo de tolerancia de fallos. Deberán usarse los fundamentos de cálculo especificados en el manual de seguridad HI 800 196 ES.

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

2.1.1 Aplicación según el principio de corriente de reposo

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

Un sistema que funcione según el sistema de corriente de reposo no necesitará energía para ejecutar su función de seguridad (“deenergize 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.

2.1.2 Aplicación según el principio de corriente de trabajo

Los sistemas de control HIMax pueden usarse también en aplicaciones de corriente de trabajo.

Un sistema que funcione según el sistema de corriente de trabajo necesitará 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

Todos los sistemas HIMax con entradas analógicas están homologados y certificados según DIN EN 54-2 y NFPA 72 para sistemas de alarma de incendios. Estos sistemas deberán poder adoptar su estado activo cuando se solicite, para poder dominar los peligros emergentes.

¡Deben respetarse las condiciones de uso!

2.2 Uso no conforme a la finalidad prevista

No se permite la transmisión de datos con relevancia de seguridad a través de redes públicas (p. ej. internet) sin 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 de seguridad.

No es admisible su uso bajo condiciones que excedan las citadas a continuación.

2.3 Condiciones de uso

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

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

Tabla 1: Normas de compatibilidad electromagnética, clima y medio ambiente

Para hacer uso de los sistemas de control HIMax de 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 de emplazamiento	< 2000 m
Carcasa	Estándar: IP 20/IP 00 Si las normas de aplicación pertinentes (p. ej. EN 60204) así lo exigen, el dispositivo deberá montarse en una carcasa del grado de protección exigido (p. ej. IP 54).

Tabla 2: Condiciones generales

2.3.1 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: -25 °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 3: Condiciones climáticas

2.3.2 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 de amplitud 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 y dirección (18 choques)

Tabla 4: Ensayos mecánicos

2.3.3 Condiciones de compatibilidad electromagnética

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).

Normas de ensayos	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: Tensión de alimentación: 2 kV y 4 kV Líneas de señal: 2 kV	 4 kV 2 kV
IEC/EN 61000-4-12	Ensayo con vibraciones atenuadas: 2,5 kV L-, L+/PE 1 kV L+/L -	 - -
IEC/EN 61000-4-6	Alta frecuencia, asimétrica: 10 V, 150 kHz…80 MHz, 80% AM 20 V, frecuencias ISM, 80% AM	 10 V -
IEC/EN 61000-4-3	Impulsos de 900 MHz	-
IEC/EN 61000-4-5	Tensión transitoria: Tensión de alimentación: 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 5: 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 6: Ensayos de emisión de interferencias

2.3.4 Fuente de alimentación

Los ensayos más relevantes y los valores límite para las fuentes de alimentación de los dispositivos 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 alternativamente las siguientes normas: IEC/EN 61131-2 o SELV (Safety Extra Low Voltage) o PELV (Protective Extra Low Voltage)
	Los cortacircuitos que se usen en los dispositivos HIMax deben 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.
	Duración del búfer, ensayo de durabilidad: Ensayo B, 1000 h

Tabla 7: Evaluación de las características de la fuente de corriente continua

2.3.5 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 de los sistemas de control!

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

Las modificaciones o ampliaciones del cableado del sistema se autorizan sólo a personal con conocimientos sobre medidas de protección contra descargas electrostáticas (ESD).

2.4 Responsabilidades de fabricantes de máquinas y de la empresa usuaria

Los fabricantes de máquinas/equipos y la empresa usuaria de los mismos son responsables de velar por la segura aplicación de sistemas HIMax en plantas de automatización y en plantas globales.

La correcta programación de los sistemas HIMax deberá estar suficientemente validada por los fabricantes de máquinas/equipos.

2.5 Otros documentos del sistema

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

Nombre	Contenido	Nº de documento S = español E = inglés
Manual del sistema HIMax	Descripción de hardware del sistema modular	HI 801 141 ES HI 801 001 E
Informe de ensayos para el certificado [1)]	Principios de ensayos, requisitos de seguridad, resultados	
Manuales de los componentes	Descripción de los distintos componentes	
Manual de comunicación	Protocolos estándar y safe**ethernet**	HI 801 195 ES HI 801 101 E
Manual de primeros pasos de SILworX	Uso de SILworX para planificación, puesta en servicio, pruebas y funcionamiento	HI 801 194 ES HI 801 103 E

1) Se suministra sólo junto a un sistema HIMax

Tabla 8: Sinopsis de documentos del sistema

Los documentos están a su disposición en formato PDF en internet: *www.hima.com*.

3 Concepto de seguridad para el uso del PES

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

- Seguridad y disponibilidad
- Tiempos importantes para la seguridad
- Prueba recurrente
- Obligaciones de seguridad
- Certificación

3.1 Seguridad y disponibilidad

De los sistemas HIMax no se desprende ningún peligro inmediato.

⚠ PELIGRO

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

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

HIMA recomienda encarecidamente sustituir todo módulo averiado a la mayor brevedad.

El módulo de repuesto, una vez instalado en el lugar del módulo averiado, pasará a estar operativo sin necesidad de que intervenga el usuario. Asumirá inmediatamente las funciones del módulo averiado, siempre que sea del mismo tipo o de un tipo de recambio homologado.

3.1.1 Cálculos de PFD y PFH

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

Bajo pedido, HIMA le comunicará los valores de PFD, PFH y SFF.

El intervalo para la prueba recurrente de los sistemas HIMax se establece en 10 años (Offline Proof Test, ver IEC 61508-4, párrafo 3.8.5).

Las funciones de seguridad, que consisten en un bucle relativo a la seguridad (entrada, unidad procesadora, salida y comunicación segura entre sistemas HIMA), cumplen en todas sus combinaciones las exigencias arriba descritas.

3.1.2 Autocomprobación y diagnóstico de errores

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

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

Si se detectan errores en estas comprobaciones, se desactivará el módulo defectuoso o, en el caso de los módulos de E/S, el canal defectuoso. Si se detectan errores de módulo ya en la puesta en marcha de un módulo, éste no se pondrá en funcionamiento.

En el caso de un sistema sin redundancia, esto puede llevar a que se desactiven funciones parciales o todo el sistema programable PES. Si se trata de un sistema redundante, en caso de detectarse un error será el módulo redundante o el canal redundante el que asuma las funciones a ejecutar.

Todos los módulos HIMax 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 módulo detectado como defectuoso.

Además, el programa de usuario podrá evaluar diversas variables del sistema que indican el estado de los módulos.

Un completo registro de diagnóstico del comportamiento del sistema y de los errores detectados se guardará en la memoria de diagnóstico del módulo procesador y de los demás módulos. 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 del sistema HI 801 141 ES, en el Capítulo “Diagnóstico”.

En un porcentaje sumamente reducido de fallos de componentes que no afectan a la seguridad, el sistema HIMax 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.

3.1.4 Redundancia

Para aumentar el grado de disponibilidad, podrán instalarse redundantemente todos los componentes que contengan elementos activos, pudiendo sustituirse sin interrumpir el funcionamiento.

La redundancia no menoscaba la seguridad. El nivel SIL 3 está garantizado también con componentes redundantes del sistema.

3.1.5 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 al desactivarse el equipo.
2. Estado que se adopta por solicitación, 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 del fallo.
  - 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 componentes del sistema de seguridad.
Véase el manual del sistema HI 801 141 ES:

- Fuente de alimentación del sistema de control.
- Componentes del sistema de control: Módulos HIMax.

- Para las salidas de relés, HIMA recomienda implementar redundantemente éstas 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 fallo 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 y activa los respectivos componentes redundantes. Esto se logra mediante

- Autocomprobaciones de los módulos HIMax.
- 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.

3.2 Tiempos importantes para la seguridad

Son:

- Tiempo de tolerancia de errores
- Tiempo de WatchDog
- Tiempo de seguridad
- Tiempo de reacción

3.2.1 Tiempo de tolerancia de errores (FTT)

El tiempo de tolerancia de errores 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 WatchDog del recurso

El tiempo de WatchDog se definirá como valor de tiempo en el cuadro de diálogo de configuración de propiedades del recurso. Es la máxima duración admisible de un ciclo RUN (tiempo de ciclo). Si el tiempo de ciclo sobrepasa el tiempo de WatchDog definido, el módulo procesador adoptará el estado de parada por error.

Al calcular el tiempo de WatchDog habrá que incluir los siguientes aspectos:

- Tiempo que necesita la aplicación, es decir, la duración de un ciclo del programa del usuario.
- Tiempo que necesita la comunicación de datos de proceso
- Tiempo que necesita la sincronización de los módulos procesadores redundantes.
- El tiempo necesario internamente para ejecutar una carga por reload.

El rango de ajuste del tiempo de WatchDog del recurso es

desde 6 ms hasta un máximo de 7500 ms.

El valor configurado por defecto es 200 ms.

Para el tiempo de WatchDog debe cumplirse:
tiempo de WatchDog ≤ ½ * tiempo de seguridad

Para una disponibilidad suficiente, HIMA recomienda la siguiente configuración:

2 * tiempo WatchDog + máx. tiempo ciclo CPU + 2 * tiempo ciclo E/S ≤ tiempo seguridad

Si no puede estimarse con seguridad el máximo tiempo de ciclo de CPU, habrá que aplicar un tiempo de seguridad tal que:

3 * tiempo WatchDog + 2 * tiempo ciclo E/S ≤ tiempo seguridad

El tiempo de ciclo de E/S es de 2 ms.

El tiempo de WatchDog para un proyecto se averiguará mediante una prueba del sistema en su integridad. Para esta prueba se tendrán aplicados todos los módulos procesadores planificados. El sistema funcionará en modo RUN a plena carga.

Todas las conexiones de comunicación estarán en uso (safe**ethernet** y protocolos estándar).

Determinación del tiempo de WatchDog

1. Ajuste un tiempo de WatchDog alto para la prueba.
2. Haga funcionar el sistema a plena carga. Deberán estar en uso todas las conexiones de comunicación, tanto mediante safeethernet como mediante protocolos estándares. Lea frecuentemente el tiempo de ciclo en el panel de control y anote las fluctuaciones y los picos de carga del tiempo del ciclo.
3. Retire, uno tras otro, cada módulo procesador y vuelva a colocarlo en el rack. Antes de retirar cada módulo procesador, aguarde hasta que el módulo procesador recién agregado se haya sincronizado.

Al agregar un módulo procesador, éste se sincronizará automáticamente con la configuración de los módulos procesadores existentes. El tiempo necesario para la sincronización prolongará el ciclo del sistema de control hasta el máximo tiempo de ciclo.

El tiempo necesario para la sincronización aumentará cuanto mayor sea la cantidad de los módulos procesadores ya sincronizados.

La instalación y el desmontaje de un módulo procesador se describen en el manual X-CPU 01, HI 801 208 ES.

4. En el historial de diagnóstico del módulo no sincronizado se leerá el tiempo de sincronización de n a n+1 módulos procesadores en cada sincronización. Con el mayor de estos tiempos de sincronización se determinará el tiempo de WatchDog.
5. El tiempo mínimo de WatchDog se calcula a partir de:
   mayor tiempo de sincronización + 12 ms de reserva + reserva para las fluctuaciones observadas.
6. El tiempo de WatchDog T_{WD} se calcula a partir de:

   $T_{WD} = T_{Sinc} + T_{Res} + T_{Com} + T_{Config} + T_{Lat} + T_{Punta}$, siendo

T_{Sinc}	El tiempo dado para la sincronización de un módulo procesador
T_{Res}	Tiempo de reserva de 12 ms
T_{Com}	Parámetro de sistema configurado *Max. Com. Time Slice ASYNC [ms]*
T_{config}	Parámetro configurado de sistema *Max. Duration of Configuration connections [ms]*
$T_{Latencia}$	Parámetro configurado del sistema *Maximum System Bus Latency [µs]* * 4
T_{Punta}	Puntas de carga observadas de los programas de usuario

Así se calcula un valor de consigna adecuado para el tiempo de WatchDog.

i Es posible que el tiempo de WatchDog así calculado sea insuficiente para una carga por reload.

SUGE-RENCIA El tiempo de WatchDog calculado puede usarse como máximo tiempo de ciclo para la parametrización de safe**ethernet**. Véase el manual de comunicación HI 801 195 ES.

3.2.3 Tiempo de WatchDog del programa del usuario

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

El tiempo de WatchDog del programa del usuario no puede configurarse directamente. HIMax 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*. Hallará más información en el Capítulo 10.2.3 y 10.2.11.

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.

3.2.4 Tiempo de seguridad del sistema PES

El tiempo de seguridad es el tiempo máximo admisible, dentro del cual el PES deberá reaccionar a un requerimiento. Requerimientos son:

- Cambios en las señales de entrada del proceso
- Aparición de un error dentro del sistema de control.

En los sistemas de control HIMax podrá configurarse un tiempo de seguridad desde 20 ms hasta 22 500 ms.

Dentro del tiempo de seguridad del sistema de control, los dispositivos de autocomprobación detectarán los errores que puedan originar estados peligrosos. Estos desencadenan reacciones definidas frente a los errores, poniendo así las partes erróneas en un estado funcional seguro.

Al calcular el tiempo de seguridad, el usuario deberá incluir los siguientes aspectos:

- Para los módulos de entrada habrá que considerar:
  Los retardos de conexión/desconexión configurados en los canales de entrada:
  El tiempo máximo de retardo en µs + 2* tiempo de ciclo del módulo de E/S
- La exploración de fallos también necesita un margen de tiempo de reserva.

Para el tiempo de seguridad habrá que configurar un valor que sea lo suficientemente grande como para considerar el mayor de los aspectos citados, pero menor que el FTT del proceso. Habrá que considerar aquí los tiempos de los sensores y actuadores para la función de seguridad.

El tiempo de seguridad del sistema de control es:

tiempo seguridad > 2 * tiempo WatchDog + máx. tiempo ciclo + 2 * tiempo ciclo módulos E/S

El máximo tiempo de ciclo debería medirlo el usuario empíricamente en su aplicación concreta sustituyendo un módulo procesador redundante. El valor de tiempo máximo de ciclo así averiguado con el sistema en su integridad debería aplicarse en la fórmula anterior. El tiempo de ciclo de los módulos de E/S es de 2 ms.

Ello garantiza altas cotas de disponibilidad.

3.2.5 Tiempo de seguridad del programa del usuario

El tiempo de seguridad del programa del usuario no puede configurarse directamente. HIMax calcula el tiempo de seguridad de un programa de usuario a partir de los parámetros *Safety Time* del recurso y *Maximum Number of Cycles*. Hallará más información en el capítulo 10.2.3 y 10.2.11.

3.2.6 Tiempo de reacción

El tiempo de reacción de sistemas de control HIMax 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:

- Procesado de los datos de introducción.
  - Procesado de los datos de entrada del módulo de entrada.
  - Lectura de los datos de proceso de las interfaces de comunicación.
  - Lectura de los datos de proceso de los módulos de entrada.
- Procesado de la lógica del usuario.
- Procesado de los datos de salida.
  - Escritura de los datos de proceso en los módulos de salida.
  - Escritura de los datos de proceso en las interfaces de comunicación.
  - Procesado de los datos de salida en los módulos de entrada.
- Procesado adicional
  de acciones conclusivas de reload, módulos procesadores agregados, etc.

Este tiempo de reacción será válido para un programa de usuario que dure sólo un ciclo del módulo procesador. En programas de usuario cuya ejecución se extienda a varios ciclos del módulo procesador. el tiempo de reacción aumentará hasta la cantidad de ciclos multiplicada por el doble de la duración del ciclo. Hallará más información en el capítulo 10.2.3 y 10.2.11.

3.3 Prueba recurrente

Una prueba recurrente es una ensayo de prueba que sirve para descubrir errores ocultos en un sistema técnico de seguridad, 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 una prueba recurrente **cada 10 años**. Mediante un análisis por cálculo de los circuitos de seguridad implementados suele poder prolongarse dicho intervalo.

3.3.1 Realización de la prueba recurrente

La realización de la prueba recurrente 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 las pruebas recurrentes es responsabilidad del usuario de los sistemas con funciones orientadas a la seguridad.

3.3.2 Frecuencia de las pruebas recurrentes

El sistema de control HIMax podrá someterse a una prueba recurrente comprobando para ello todo el circuito de seguridad.

En la práctica se exige un intervalo de prueba más corto para la 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 HIMax. Si el usuario comprueba todo el circuito de seguridad debido

al dispositivo de campo, el sistema de control HIMax estará automáticamente incluido en dicha prueba y no se requerirán pruebas recurrentes adicionales para el sistema de control HIMax.

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

3.4 Obligaciones de seguridad

Para usar sistemas programables PES con funciones orientadas a la seguridad del sistema HIMax tienen validez las siguientes obligaciones de seguridad:

3.4.1 Proyecto del hardware

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

Obligaciones no dependientes del producto

- Para el uso con fines orientados a la seguridad podrán emplearse únicamente módulos de hardware y componentes de software a prueba de fallos y homologados a tal fin. Los módulos hardware y los componentes de software homologados se especifican en *Version List of Modules and Firmware for HIMax Systems from HIMA Paul Hildebrandt GmbH* (la lista de versiones de módulos y de firmware de los sistemas HIMax de HIMA Paul Hildebrandt GmbH). Las correspondientes versiones actuales figuran en la lista de versiones presentada junto con la instancia oficial de inspección.
- Son de obligado cumplimiento las condiciones de uso (ver capítulo “Condiciones de uso”) especificadas en lo relativo a la compatibilidad electromagnética y los factores mecánicos, químicos y climáticos.

Obligaciones dependientes del producto

- Al sistema se conectarán sólo dispositivos que dispongan de una separación segura de la red eléctrica. Lo mismo rige para las conexiones de comunicación.
- Deberán cumplirse las condiciones de uso citadas en el manual del sistema, particularmente la tensión de alimentación, la ventilación, etc.
- Para solventar tareas orientadas a la seguridad se usarán únicamente módulos con función orientada a la seguridad.

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.

3.4.3 Condiciones obligatorias para hacer uso del sistema de programación

- Para la programación deberá usarse la utilidad SILworX.
- Mediante una doble compilación en SILworX y la comparación de los CRCs de ambos archivos generados se garantiza que la compilación haya sido correcta.
- **La correcta implementación de lo especificado para la aplicación habrá de validarse, verificarse y documentarse. Deberá realizarse una verificación completa poniendo a prueba la lógica.**
- En caso de modificar la aplicación habrá que probar al menos todas las partes de la lógica afectadas por la modificación.

- La reacción del sistema a errores en módulos de salida/entrada a prueba de fallos deberá definirse mediante la configuración de acuerdo a las circunstancias técnicas de seguridad específicas del equipo o la instalación a controlar. Ejemplos:
  - Reacción a errores en el programa de usuario
  - Parametrización de valores iniciales seguros para variable

3.4.4 Comunicación

- Si se usa la comunicación con función orientada a la seguridad entre diversos dispositivos, deberá observarse que el tiempo total de reacción del sistema no exceda el tiempo de tolerancia a errores. Deberán seguirse los principios de cálculo indicados en el capítulo 11.2.
- No se permite la transmisión de datos con relevancia de seguridad a través de 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 la transmisión de datos con relevancia de seguridad no se permite usar los protocolos estándar.
- A todas las interfaces de comunicación deberán conectarse sólo dispositivos que garanticen una separación eléctrica segura.

3.4.5 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 las medidas administrativas necesarias para proteger el acceso a los sistemas en consulta con las instancias oficiales de homologación.

3.5 Certificación

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

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

Certificado e informe de ensayos
Dispositivos de automatización HIMax con función orientada a la seguridad

Finalidad: “Safety Related Programmable Electronic System for process control, Burner Management (BMS), emergency shut down and machinery, where the demand safe state is the de-energized state.
Applications, where the demand state is the de-energized or energized state”.
Sistema electrónico programable con función orientada a la seguridad para control de procesos, control de quemadores (BMS), sistemas de desconexión de emergencia y control de máquinas, en los que el estado de seguridad a adoptar en caso necesario es el estado sin energía.
Aplicaciones en las que el estado de seguridad a adoptar en caso necesario es el estado sin energía o con energía.

Normas internacionales:		
EN/IEC 61508, Partes 1–7: 2000		SIL 3
EN/IEC 61511: 2004		SIL 3
EN/ISO 13849-1: 2008		Nivel de prestaciones e
EN/IEC 62061: 2005	incl. enmiendas 1 y 2: 2009	
EN 50156-1: 2006		
EN 12067-2: 2004		
EN 298: 2004	+enm. 1: 2006	
EN 230: 2005		
NFPA 85: 2007		
NFPA 86: 2007		
EN/IEC 61131-2: 2007		
EN/IEC 61000-6-2: 2005		
EN 61000-6-4: 2007		
EN 54-2: 1997	/A1: 2007	
NFPA 72: 2002		

El capítulo “Condiciones de uso” especifica detalladamente todas las pruebas realizadas en materia medioambiental y de compatibilidad electromagnética.

Todos los dispositivos llevan marcado el distintivo CE.

Para programar los sistemas de control HIMax se usa un PADT, es decir, un PC que tiene instalado el sistema de programación

SILworX.

Este permite al usuario crear programas con función orientada a la seguridad mediante lenguaje de bloques funcionales (FBD) y tabla de funciones secuenciales (SFC) conforme a 61131-3, así como operar los dispositivos de automatización. Hallará más detalles en la ayuda directa en pantalla de SILworX y en el manual de primeros pasos de SILworX HI 801 194 ES.

4 Módulo procesador

La función de seguridad del módulo procesador consiste en ejecutar el programa del usuario con dos procesadores que comparan continuamente sus datos. En caso de error, el WatchDog pondrá el módulo en estado seguro y comunicará el estado de la CPU.

Hallará más información de los módulos procesadores en los manuales.

4.1 Autocomprobaciones

A continuación se explican las principales rutinas de autocomprobación de los módulos procesadores con función orientada a la seguridad:

- Prueba de procesador
- Prueba de memoria
- Prueba de comparador
- Prueba de verificación CRC de las memorias no volátiles
- Prueba de WatchDog

4.2 Reacción a errores en el módulo procesador

Un comparador de hardware incluido en el módulo procesador compara continuamente que los datos 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 del módulo procesador, el sistema de control adoptará automáticamente el estado seguro frente a fallos y la señal de WatchDog se desactivará. El módulo procesador no procesará ya ningún programa de usuario y pondrá las salidas en estado desactivado, sin energía.

4.3 Sustitución de módulos procesadores

Antes de sustituir módulos procesadores deberá observarse que ello no provoque la detención de un sistema HIMax en funcionamiento.

Esto será especialmente relevante en sistemas que funcionen según el principio de corriente de trabajo. En caso de que un sistema tal deje de funcionar, se perderá la función de seguridad.

Los módulos procesadores redundantes se pueden sustituir sin interrumpirse el funcionamiento, siempre que se disponga de al menos un módulo procesador que permanezca operativo y asuma la función orientada a la seguridad durante la sustitución.

NOTA

¡Posible interrupción del modo con función orientada a la seguridad!

Si se sustituye un módulo procesador cuyo LED Ess **esté encendido o parpadee, es posible que ello interrumpa el funcionamiento del sistema de control.**

¡No sustituya módulos procesadores cuyo LED Ess **esté encendido con luz fija o parpadeante!**

El LED **Ess** encendido o parpadeante indica que el respectivo módulo procesador es imprescindible para que el sistema siga funcionando.

Aun cuando el LED no esté encendido ni parpadee, deberán comprobarse con SILworX las redundancias del sistema en las que participe el módulo procesador dado. Habrá que observar igualmente las conexiones de comunicación que tienen lugar mediante el módulo procesador.

Hallará información más detallada sobre la sustitución de módulos procesadores en el manual de módulo procesador HI 801 208 ES y en el manual del sistema HI 801 141 ES.

5 Módulo de bus de sistema

Un módulo de bus de sistema administra uno de los dos buses de sistema orientados a la seguridad. Ambos buses de sistema funcionan redundantemente entre sí. Cada bus de sistema interconecta todos los módulos y racks. Mediante los buses de sistema se transmiten los datos con ayuda de un protocolo orientado a la seguridad.

Podrá hacerse funcionar un sistema HIMax que **sólo contenga un módulo procesador** con un solo bus de sistema a menor grado de disponibilidad.

5.1 ID de rack

El ID de rack identifica un rack dentro de un recurso y deberá ser único e inequívoco para cada rack.

El ID de rack es el **parámetro de seguridad** para el direccionamiento de los distintos racks y de los módulos que estos contienen.

El ID de rack se guarda en la tarjeta de conexión del módulo de bus de sistema. Si es necesario modificar el ID de rack, p. ej. al montar un nuevo sistema HIMax, deberá seguirse el procedimiento descrito en el manual del sistema.

El procedimiento de ajuste del ID de rack-Id se describe en el manual del sistema HI 801 141 ES y en el manual de primeros pasos HI 801 194 ES.

5.2 Responsibility

Sólo uno de los módulos de bus de sistema podrá tener el atributo “responsible” y parametrizarse como responsable del bus del sistema.

- El bus de sistema A tiene de forma fija el atributo “responsible” para el módulo de bus de sistema 0, slot 1.
- Para el bus de sistema B, el atributo puede configurarse con SILworX.

El módulo de bus de sistema “responsable” deberá encontrarse en el rack 0 o en el rack 1.

Deberá verificarse esta condición antes de la puesta en servicio orientado a la seguridad.

El procedimiento de ajuste de “Responsibility” se describe en el manual de primeros pasos HI 801 194 ES.

⚠ ADVERTENCIA

¡Riesgo de daños personales!

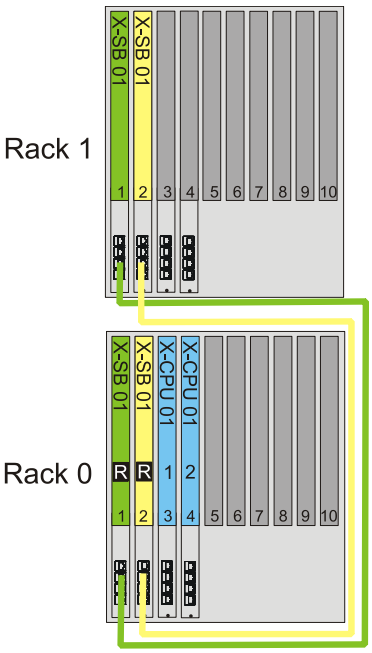
La parametrización debe verificarse con ayuda de SILworX.

A este efecto es indispensable seguir este procedimiento:

- **Ingrese en SILworX por Modul-Login en el módulo de bus de sistema rack 0, slot 2.**
- **Ingrese en SILworX por Modul-Login en el módulo de bus de sistema rack 1, slot 2.**
- **En los paneles de control abiertos de ambos módulos de bus de sistema cerciórese de que el atributo “responsible” esté aplicado sólo al correcto módulo de bus de sistema (ver Fig. 1 y Fig. 2).**

Configuraciones recomendadas:

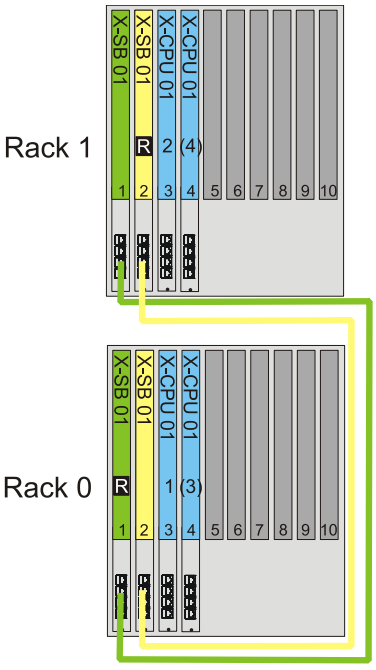
- Si sólo el rack 0 contiene módulos procesadores, deberán aplicarse como “responsables” ambos módulos de bus de sistema del rack 0 (Fig. 1).
- Si también el rack 1 contiene módulos procesadores (Fig. 2), aplique los siguientes módulos de bus de sistema como “responsables”:
  - En el rack 0 el módulo de bus de sistema del slot 1.
  - En el rack 1 el módulo de bus de sistema del slot 2.



Rack 0 Base 0 Rack 1 Base 1

R El módulo de bus de sistema es "responsable"

Fig. 1: Configuración recomendada: Todos los módulos procesadores en el rack 0



Rack 0 Base 0 Rack 1 Base 1

R El módulo de bus de sistema es "responsable"

Fig. 2: Configuración recomendada: Módulos procesadores en el rack 0 y el rack 1

6 Módulo de comunicación

En los módulos de comunicación tiene lugar tanto el tráfico de datos orientado a la seguridad con otros sistemas de control HIMA como también el tráfico de datos no orientado a la seguridad mediante buses de campo y Ethernet.

- El módulo procesador controla el tráfico de datos orientado a la seguridad a través del protocolo de transmisión safe**ethernet** certificado para SIL 3. El módulo de comunicación reenvía los paquetes de datos a los demás sistemas. El protocolo orientado a la seguridad garantiza que se detecten notificaciones falseadas (principio black-channel).

  De esta forma se imposibilita la comunicación orientada a la seguridad mediante vías de transmisión no orientadas a la seguridad, es decir, mediante componentes de red estándar.
- Los protocolos estándar son p. ej.:
  - Modbus
  - PROFIBUS Master/Slave

Un sistema HIMax puede dotarse como máximo con 20 módulos de comunicación.

Más información en el capítulo 11.1, en el manual del módulo de comunicación HI 801 207 ES y en el manual de comunicación HI 801 195 ES.

7 Módulos de entrada

Módulo	Cantidad de canales	Con función orientada a la seguridad	Canales libres de repercusiones	Comentario
Entradas digitales				
X-DI 16 01	16	SIL 3	•	120 VCA
X-DI 32 01	32	SIL 3	•	
X-DI 32 02	32	SIL 3	•	Iniciadores (NAMUR)
X-DI 32 03	32	SIL 3	•	48 VCC
X-DI 32 04	32	SIL 3	•	Con captación de eventos
X-DI 32 05	32	SIL 3	•	Iniciadores (NAMUR), con captación de eventos
X-DI 32 51	32	-	•	
X-DI 32 52	32	-	•	Iniciadores (NAMUR)
X-DI 64 01	64	SIL 3	•	
X-DI 64 51	64	-	•	
Entradas analógicas				0/4...20 mA
X-AI 16 51	16	SIL 1	•	
X-AI 32 01	32	SIL 3	•	
X-AI 32 02	32	SIL 3	•	Con captación de eventos
X-AI 32 51	32	-	•	
Entradas de contadores				
X-CI 24 01	24	SIL 3	•	
X-CI 24 51	24	-	•	

Tabla 9: Sinopsis de módulos de entrada

7.1 Generalidades

Las entradas con función orientada a la seguridad podrán usarse tanto para señales orientadas a la seguridad como para señales no orientadas a la seguridad. ¡Por el contrario, las señales no orientadas a la seguridad no podrán usarse para funciones orientadas a la seguridad!

Los sistemas de control generan mensajes de error y de estado relativos a los LEDs de diagnóstico de los módulos y dichos mensajes se guardan. El PADT podrá leer los mensajes guardados en esta memoria de diagnóstico.

Los módulos de entrada con función orientada a la seguridad realizan cíclicamente una autocomprobación de alta calidad durante el funcionamiento.

En caso de error, el programa del usuario dispondrá del valor inicial a través de una variable global y, de ser posible, se generará información del error. Dicha información del error podrá evaluarse en el programa del usuario leyendo el código de error.

Para más información de los módulos de entrada, véanse sus manuales.

7.2 Seguridad de sensores, codificadores y transmisores

En una aplicación con función orientada a la seguridad, tanto el sistema PES 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 valor SIL de sensores y actuadores” en el anexo.

7.3 Entradas digitales con función orientada a la seguridad

El módulo de entrada digital lee sus entradas digitales una vez en cada ciclo del módulo y guarda el valor internamente. El módulo comprueba cíclicamente la función segura de las entradas.

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 del módulo de entrada) no se captarán.

7.3.1 Rutinas de comprobación

Las rutinas de comprobación on-line verifican que todos los canales de entrada sean capaces de transmitir ambos niveles de señal (0 y 1), independientemente de las señales de entrada actuales. Esta prueba funcional se realiza cada vez que se leen las señales de entrada.

7.3.2 Reacción en caso de error

Si las rutinas de comprobación detectan un error de una entrada digital, el módulo pondrá el valor del canal de forma tal que la variable global que el usuario haya asignado al canal adopte los siguientes valores:

- En el caso de los errores diagnosticables, la variable global adoptará su valor inicial configurado. El módulo pone el estado “Channel OK” en FALSE.
- En caso de errores seguros no diagnosticables, el módulo no podrá generar registros de diagnóstico.
  Con estos errores la variable global adoptará el valor seguro 0.

Si las rutinas de comprobación descubren un error de módulo o submódulo, el módulo pondrá en FALSE el estado *Module OK* o *Submodule OK*. Además el módulo o submódulo pondrá en FALSE el estado *Channel OK* para todos sus canales.

En todos los casos, el módulo activará el LED *Error* en el panel frontal.

7.3.3 Funcionamiento según el principio de corriente de trabajo

Es admisible hacer funcionar las entradas digitales según el principio de corriente de trabajo. En tal caso habrá que usar módulos de entrada con monitoreo de cable.

7.3.4 Redundancia

Es admisible circuitar las entradas digitales de forma redundante. El circuitado redundante sirve normalmente para aumentar el grado de disponibilidad.

Otros circuitados (para aumentar el nivel SIL) requieren de un tratamiento de los estados de error en la lógica del programa de aplicación.

7.3.5 Picos en entradas digitales

NOTA

Si se usan cables apantallados para las entradas digitales, no será necesario tomar otras medidas adicionales para prevenir picos.

Si **no** se usan cables apantallados, es posible que en las entradas digitales (debido al corto tiempo de ciclo de los sistemas HIMax) se interprete como breve señal “1” un impulso de pico de corriente, según se define éste en EN 61000-4-5.

Para evitar semejantes disfunciones habrá que usar el retardo de conexión/desconexión del canal: una señal deberá estar presente al menos un tiempo dado antes de ser evaluada. Hay que cuidar que este tiempo no exceda el tiempo de WatchDog.

7.4 Entradas analógicas con función orientada a la seguridad

Los canales de entrada analógicos convierten las intensidades de entrada en un valor del tipo DINT (double integer), el *Raw Value*, y en un *Process Value* del tipo de dato REAL. El *Raw Value* contiene la señal de entrada medida, mientras que el valor de proceso es un valor puesto a escala.

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

7.4.1 Rutinas de comprobación

El módulo capta los valores analógicos por dos medios y compara los resultados entre sí. Además comprueba cíclicamente la función de las vías de entrada.

7.4.2 Reacción en caso de error

Si las rutinas de comprobación detectan un error de una entrada analógica, el módulo pondrá el valor del canal de forma tal que la variable global asignada al *Process Value* del canal adopte los siguientes valores:

- En caso de errores diagnosticables, la variable global adoptará su valor inicial configurado.
- En caso de errores seguros no diagnosticables, el módulo no podrá generar registros de diagnóstico.
  Con estos errores la variable global adoptará el valor seguro 0.

El módulo pone el estado "*Channel OK*" en FALSE.

El *Raw Value* del canal no reacciona a errores. Si se emplea el valor bruto, el programa del usuario deberá realizar un tratamiento de errores.

Si las rutinas de comprobación descubren un error de módulo o submódulo, el módulo pondrá en FALSE el estado *Module OK* o *Submodule OK*. Además el módulo o submódulo pondrá en FALSE el estado *Channel OK* para todos sus canales.

En todos los casos, se activará el LED *Error* en el panel frontal.

7.4.3 Funcionamiento según el principio de corriente de trabajo

Es admisible hacer funcionar las entradas analógicas según el principio de corriente de trabajo. En tal caso habrá que usar monitoreo de cable.

7.4.4 Redundancia

Es admisible circuitar las entradas analógicas de forma redundante. El circuitado redundante sirve normalmente para aumentar el grado de disponibilidad.

Otros circuitados (para aumentar el nivel SIL) requieren de un tratamiento de los estados de error en la lógica del programa de aplicación.

7.5 Entradas de contador con función orientada a la seguridad

Una entrada de contador orientada a la seguridad podrá proporcionar, según su configuración, los siguientes valores de proceso:

- Una lectura de contador en forma de valor entero o valor escalado de coma flotante.
- Una velocidad o frecuencia en forma de valor entero o valor escalado de coma flotante.
- Otros valores auxiliares, como p.ej. desbordamientos.

Más información en el manual del módulo HI 801 205 ES.

7.5.1 Rutinas de comprobación

El módulo capta los valores de contador paralelamente por tres medios y compara los resultados entre sí. Además comprueba cíclicamente la función de las vías de entrada.

7.5.2 Reacción en caso de error

Si las rutinas de comprobación detectan un error de una entrada de contador, el módulo pondrá el valor del canal de forma tal que las variables globales que el usuario haya asignado al canal adopten los siguientes valores:

- Las variables globales asignadas al parámetro *-> Rotation Speed [mHz] [DINT]* y *-> Rotation Speed (scaled) [REAL]* adoptarán el valor 0.
- La variable global asignada al parámetro *-> Counter Reading* adoptará el último valor válido.

El módulo pone el estado "*Channel OK*" en FALSE.

Si las rutinas de comprobación descubren un error de módulo o submódulo, el módulo pondrá en FALSE el estado *Module OK* o *Submodule OK*. Además el módulo o submódulo pondrá en FALSE el estado *Channel OK* para todos sus canales.

En todos los casos, se activará el LED *Error* en el panel frontal.

7.5.3 ¡A observar en el módulo contador X-CI 24 01!

Si se usa el módulo contador X-CI 24 01 habrá que observar las siguientes particularidades (véase también el manual del módulo HI 801 205 ES):

- Durante una carga por reload es posible que se pierdan impulsos de entrada en los primeros 3 ciclos en caso de modificarse los siguientes parámetros durante el reload:
  - Tipo de evaluación de impulsos de contador
  - Pares de canales utilizados
- Si durante la evaluación de flancos "2 fases, 4 flancos" falla el sensor de un canal sin que se detecte cortocircuito ni interrupción de cable, el módulo registrará la mitad de la frecuencia real.
- ¡No es admisible usar los parámetros de canal *-> Level* y *-> Count.Read (revolv.)* para aplicaciones orientadas a la seguridad!
- Los impulsos a contar pueden perderse en caso de reinicio automático.
- El reinicio automático o manual del módulo habrá que considerarlo específicamente para la aplicación.
- Recomendación de aplicación:
  - Para la evaluación de varias fases y la detección del sentido de giro se recomienda usar sensores redundantes, pues sólo así puede detectarse el fallo de un sensor.
  - La parametrización de la exploración de fallos no es absolutamente problemática para la medición de frecuencia desde el punto de vista de la técnica de control.

7.5.4 Funcionamiento según el principio de corriente de trabajo

Es admisible hacer funcionar las entradas de contadores según el principio de corriente de trabajo. En tal caso habrá que usar módulos de entrada con monitoreo de cable.

7.5.5 Redundancia

Es admisible circuitar las entradas de contador de forma redundante. El circuitado redundante sirve normalmente para aumentar el grado de disponibilidad.

Otros circuitados (para aumentar el nivel SIL) requieren de un tratamiento de los estados de error en la lógica del programa de aplicación.

7.6 Listas de chequeo de entradas

HIMA recomienda usar las listas de chequeo disponibles para proyectar, programar y poner en servicio entradas con función orientada a la seguridad. Las listas de chequeo pueden usarse como documento de planificación, sirviendo al mismo tiempo de comprobante de la realización concienzuda de la planificación.

En el marco de proyección y puesta en servicio, para verificar las exigencias normativas a cumplir, es conveniente cumplimentar una lista de chequeo para cada uno de los canales de entrada orientados a la seguridad que se usen en un sistema. Sólo así podrá Ud. asegurarse de registrar las exigencias completa y claramente. La lista de chequeo es asimismo una forma de documentar la correlación entre el cableado externo y el programa del usuario.

Las listas de chequeo están a su disposición en formato Microsoft® Word® en el sitio web de HIMA.

8 Módulos de salida

Módulo	Cantidad de canales	Con función orientada a la seguridad	Con separación eléctrica segura	Comentario
Salidas digitales				
X-DO 12 02	12	SIL 3	-	
X-DO 24 01	24	SIL 3	-	
X-DO 24 02	24	SIL 3	-	48 VCC
X-DO 32 01	32	SIL 3	-	
X-DO 32 51	32	-	-	
Salidas de relés digitales				
X-DO 12 01	12	SIL 3	•	230 VCA
X-DO 12 51	12	-	•	
Salidas analógicas				
X-AO 16 01	16	SIL 3	por pares	
X-AO 16 51	16	-	-	

Tabla 10: Sinopsis de módulos de salida

8.1 Generalidades

El sistema escribe las salidas con función orientada a la seguridad una vez por ciclo, relee las señales de salida y las compara con los datos de salida que acaba de ordenar.

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

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

Para más información de los módulos de salida, véanse sus manuales.

8.2 Seguridad de actuadores

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

8.3 Salidas digitales con función orientada a la seguridad

En los canales de salida con función orientada a la seguridad se han integrado además tres contactos comprobables en serie para la desconexión monocanal. Así se cumple la exigencia de SIL 3 de una segunda vía de desconexión independiente y segura. Esta vía de desconexión de seguridad desactivará con seguridad (los pondrá en estado sin energía o excitación) los distintos canales del módulo de salida defectuoso en caso de error.

Por lo demás, la señal de WatchDog del módulo es la segunda vía de desconexión: si se pierde la señal de WatchDog, ello hará que se aplique inmediatamente el estado seguro.

8.3.1 Rutinas de comprobación para salidas digitales

Los módulos se comprueban automáticamente durante el funcionamiento. Las funciones de comprobación fundamentales son:

- Relectura de la señal de salida del amplificador de conmutación. El umbral de conmutación para un nivel 0 (low) releído se halla por debajo de la tensión de salida válida para el tipo de salida. Los diodos utilizados impiden el retroceso de señales.
- Comprobación de la doble desconexión integrada de seguridad.

- Una prueba de desconexión de salidas se realiza cíclicamente durante un máximo de 200 µs cada vez.

Si se producen errores, las salidas se pondrán al valor seguro.

8.3.2 Reacción en caso de error

Si las rutinas de comprobación detectan algún error en uno o más canales, el módulo desactivará esos canales, poniéndolos por tanto en el estado seguro. Para esos canales, el parámetro *Channel OK* se pondrá en FALSE.

Si las rutinas de comprobación descubren un error de módulo o submódulo, el módulo pondrá en FALSE el estado *Module OK* o *Submodule OK*. Además el módulo o submódulo pondrá en FALSE el estado *Channel OK* para todos sus canales.

En todos los casos, el error se indicará con el LED *Error* en el panel frontal.

8.3.3 Reacción en caso de sobrecarga o cortocircuito externo

En caso de sobrecarga o de cortocircuitarse la salida con L-, se conservará la comprobabilidad del módulo. No es necesaria una transición al 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.

NOTA

¡Posibilidad de disfunciones!

La tensión inducida por cargas inductivas al desconectar podría causar perturbaciones en el sistema de control u otros sistemas electrónicos en la proximidad de la línea de entrada de los actuadores.

Por tanto, es conveniente conectar las cargas inductivas a un circuito de protección (de marcha en vacío) en el dispositivo consumidor, para anular tales perturbaciones.

8.3.4 Funcionamiento según el principio de corriente de trabajo

Es admisible hacer funcionar las salidas digitales según el principio de corriente de trabajo. En tal caso habrá que usar monitoreo de cable.

8.3.5 Redundancia

Es admisible circuitar las salidas digitales de forma redundante. El circuitado redundante sirve normalmente para aumentar el grado de disponibilidad.

Otros circuitados (para aumentar el nivel SIL) requieren de un tratamiento de los estados de error en la lógica del programa de aplicación.

8.4 Salidas de relé con función orientada a la seguridad

Se usarán tarjetas de salidas de relé cuando se cumpla una o más de las siguientes condiciones para el actuador conectado:

- Separación eléctrica necesaria.
- Altas intensidades de corriente.
- Conmutación de corrientes alternas.

En el módulo las salidas están dotadas de dos relés de seguridad con contactos forzados. Así podrán usarse las salidas para desconexión de seguridad conforme al nivel SIL 3.

La señal de WatchDog del módulo es la segunda posibilidad de desconexión de seguridad: si se pierde la señal de WatchDog, ello hará que se aplique inmediatamente el estado seguro.

8.4.1 Rutinas de comprobación de salidas de relés

El módulo se comprueba automáticamente 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.

8.4.2 Reacción en caso de error

Si se detecta una señal errónea, la salida del módulo afectado se pondrá en estado seguro (sin energía o excitación) mediante el interruptor de seguridad. Si es un error de módulo, se desactivarán todas las salidas del módulo. Ambos tipos de error se indicarán además con el LED “Error”.

NOTA

¡Posibilidad de disfunciones!

La tensión inducida por cargas inductivas al desconectar podría causar perturbaciones en el sistema de control u otros sistemas electrónicos en la proximidad de la línea de entrada de los actuadores.

Por tanto, es conveniente conectar las cargas inductivas a un circuito de protección (de marcha en vacío) en el dispositivo consumidor, para anular tales perturbaciones.

La cantidad de conmutaciones está limitada de acuerdo a la normativa, p. ej. la norma de quemadores EN 50156-1. Más información en el manual del módulo HI 801 219 ES.

¡Al superarse la cantidad de conmutaciones en el contador, habrá que cambiar el módulo!

8.4.3 Funcionamiento según el principio de corriente de trabajo

Es admisible hacer funcionar las salidas digitales de relé según el principio de corriente de trabajo.

8.4.4 Redundancia

Es admisible circuitar las salidas digitales de relé de forma redundante. El circuitado redundante sirve normalmente para aumentar el grado de disponibilidad.

Otros circuitados (para aumentar el nivel SIL) requieren de un tratamiento de los estados de error en la lógica del programa de aplicación.

8.5 Salidas analógicas con función orientada a la seguridad

Éstas reflejan los valores de actuadores obtenidos en el programa del usuario.

Las salidas analógicas con función orientada a la seguridad releen sus valores de salida y comparan estos con los valores a emitir. En caso de divergencia, se activará la reacción a errores.

8.5.1 Rutinas de comprobación para salidas analógicas

Los módulos se comprueban automáticamente durante el funcionamiento. Las funciones de comprobación fundamentales son:

- Relectura de la señal de salida.
- Comprobación de la doble desconexión integrada de seguridad.

Si se producen errores, las salidas se pondrán al valor seguro 0 mA.

8.5.2 Reacción en caso de error

Si las rutinas de comprobación detectan algún error en uno o más canales, el módulo desactivará esos grupos de canales, poniéndolos por tanto en el estado seguro. Para esos canales, el parámetro *Channel OK* se pondrá en FALSE.

Si las rutinas de comprobación descubren un error de módulo o submódulo, el módulo pondrá en FALSE el estado *Module OK* o *Submodule OK*. Además el módulo o submódulo pondrá en FALSE el estado *Channel OK* para todos sus canales.

En todos los casos, el error se indicará con el LED *Error* en el panel frontal.

8.5.3 Reacción en caso de interrupción de cable externa

En caso de interrupción de cable, el módulo conecta la corriente durante unos 8 ms y compruebe si la interrupción de cable persiste. De ser así, se desconecta durante unos 10 s. Esta secuencia puede repetirse indefinidamente.

8.5.4 ¡A observar en el módulo de salida analógico X-AO 16 01!

Si se usa el módulo de salida analógico, habrá que observar las siguientes particularidades (véase también el manual del módulo HI 801 202 ES):

- ¡Son admisibles sólo los circuitos relacionados en el manual del módulo HI 801 202 ES!
- ¡En caso de redundancia en serie de más de dos módulos, es posible que se exceda la baja tensión de seguridad SELV!
- ¡En caso de redundancia en serie, habrá que usar sólo uno de ambos canales de cada grupo!
- Si hay comunicación HART entre el actuador conectado y un terminal HART, es posible que la señal de salida difiera en hasta un 2 % respecto al valor final.
- Si se produce un error, es posible que el tiempo necesario para alcanzar el estado seguro sea de hasta 16 ms en el peor de los casos (Worst Case). Tenga en cuenta este tiempo para el tiempo de reacción y el tiempo de seguridad.
- No se permite que el programa de usuario escriba salidas analógicas en ciclos más cortos que 6 ms.
- En caso de error, el módulo emitirá el valor seguro 0 mA, también si se sobrepasa el límite superior del rango de ajuste.

8.5.5 Funcionamiento según el principio de corriente de trabajo

Es admisible hacer funcionar las salidas analógicas según el principio de corriente de trabajo. En tal caso habrá que usar monitoreo de cable.

8.5.6 Redundancia

Es admisible circuitar las salidas analógicas de forma redundante. El circuitado redundante sirve normalmente para aumentar el grado de disponibilidad.

Otros circuitados (para aumentar el nivel SIL) requieren de un tratamiento de los estados de error en la lógica del programa de aplicación.

8.6 Listas de chequeo de salidas

HIMA recomienda usar las listas de chequeo disponibles para proyectar, programar y poner en servicio salidas con función orientada a la seguridad. Las listas de chequeo pueden usarse como documento de planificación, sirviendo al mismo tiempo de comprobante de la realización concienzuda de la planificación.

En el marco de proyección y puesta en servicio, para verificar las exigencias normativas a cumplir, es conveniente cumplimentar una lista de chequeo para cada uno de los canales de entrada orientados a la seguridad que se usen en un sistema. Sólo así podrá Ud. asegurarse de registrar las exigencias completa y claramente. La lista de chequeo es asimismo una forma de documentar la correlación entre el cableado externo y el programa del usuario.

Las listas de chequeo están a su disposición en formato Microsoft® Word® en el sitio web de HIMA.

9 Software

El software para los dispositivos de automatización con función orientada a la seguridad de los sistemas HIMax se desglosa como sigue:

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

El *sistema operativo* está cargado en cada módulo del sistema de control. Se recomienda utilizar la versión vigente más reciente para aplicaciones con función orientada a la seguridad. En este capítulo se expone particularmente el sistema operativo del módulo procesador.

El *programa del usuario* se crea con el *sistema de programación* SILworX y contiene las funciones específicas del equipo o la instalación que haya de ejecutar el dispositivo de automatización. La parametrización se realiza asimismo mediante SILworX.

El programa del usuario se traduce con el generador de códigos y se transmite a continuación a la memoria no volátil del dispositivo de automatización mediante una interfaz Ethernet.

9.1 Aspectos técnicos de seguridad para el sistema operativo

Todo sistema operativo homologado está inequívocamente identificado con el número de revisión y la signatura CRC. Las respectivas versiones del sistema operativo homologadas por el ente de inspección para los dispositivos de automatización con función orientada a la seguridad y sus respectivas signaturas (CRC) están sujetas a revisión y se documentan en *Version List of Modules and Firmware for HIMax Systems from HIMA Paul Hildebrandt GmbH* (una lista de versiones de módulos y firmware de los sistemas HIMax de HIMA Paul Hildebrandt GmbH) que se redacta conjuntamente con el ente de inspección oficial (TÜV).

La versión instalada del sistema operativo podrá leerse con el sistema de programación SILworX. Habrá que comprobar si en los módulos se ha cargado un versión de sistema operativo homologada (ver 10.3 Lista de chequeo de creación de un programa de usuario).

9.2 Aspectos técnicos de seguridad para la programación

Al crear un programa de usuario habrá que observar las exigencias aquí relacionadas.

9.2.1 Concepto de seguridad de SILworX

El concepto de seguridad de SILworX:

- Al instalar la utilidad SILworX, una suma de verificación CRC preserva la integridad del paquete del programa en su camino desde el fabricante hasta el usuario.
- SILworX realiza pruebas de plausibilidad para minimizar los errores de introducción de datos.
- La doble compilación y la consiguiente comparación de las sumas de verificación de CRC obtenidas permite detectar falseamiento de la aplicación debidas a disfunciones temporales del PC utilizado.

Doble compilación del programa y comparación de los resultados:

1. Inicie la compilación.
   ☑ Al concluir la compilación, SILworX muestra una suma de verificación CRC.
2. Reinicie la compilación.
   ☑ Al concluir la compilación, SILworX muestra 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 orientada a la seguridad habrá que comprobar la seguridad de todo el sistema con 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 (ver capítulo 9.2.2).

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

Si se modifica el programa del usuario, habrá que probar sólo aquellas partes del programa afectadas por la modificación. A este efecto, el comparador de revisiones de SILworX puede detectar y mostrar al usuario las modificaciones respecto a la versión previa.

9.2.2 Comprobación de la configuración y del programa de usuario

Para comprobar si el programa de usuario creado cumple la función de seguridad específica, el usuario deberá crear 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).

Deberán generarse también casos de prueba idóneos para la evaluación numérica de fórmulas. Son muy convenientes las pruebas de clases de equivalencias. Se trata de pruebas dentro de rangos de valores definidos, en sus límites o en rangos de valores inadmisibles. Los casos de prueba se seleccionarán de forma tal que con ellos se demuestre que el cálculo es correcto. La cantidad necesaria de casos de prueba dependerá de la fórmula utilizada y deberá incluir pares de valores críticos.

HIMA recomienda no obviar una activa simulación con fuentes, ya que sólo así puede demostrarse que el cableado de los sensores y los actuadores del sistema es correcto (también en la comunicación a las I/O remotas conectadas). Por lo demás, sólo así podrá comprobarse la configuración del sistema.

Este procedimiento deberá seguirse tanto para crear un programa de usuario como para sus ulteriores modificaciones.

9.3 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 5.1 y el manual del sistema HI 801 141 ES).**
- **Atributo Responsible de módulos de bus de sistema (ver 5.2)**
- **Safety Time**
- **WatchDog Time**
- **Main Enable**
- **AutoStart**
- **Start Allowed**
- **Load Allowed**
- **Reload Allowed**
- **Global Forcing Allowed**

Los parámetros listados a continuación se definen en SILworX para las acciones admisibles en el funcionamiento del recurso con función orientada a la seguridad y se designan como parámetros con función orientada a la seguridad.

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

9.3.1 Parámetros de sistema del recurso

Los parámetros de sistema del recurso podrá Ud. configurarlos 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 tendrá Ud. que 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. Se trata de todos los controles unidos por potencial entre sí.
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 6…7500 ms	200 ms	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 sólo con el sistema PES detenido – no en modo online.	ON	Se recomienda: OFF
AutoStart	ON: Una vez se conecte el módulo 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	ON: Se permite el reload de un programa de usuario. OFF: No se permite el reload de un programa de usuario. Un reload ya en curso no se cancelará por cambiar la opción a OFF.	ON	Específico de la aplicación

Parámetro/ Switch	Descripción	Valor por defecto	Ajuste para funcionamiento seguro
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: ▪ Stop Forcing: Finalizar la función de forzado ▪ Stop resource: Detener recurso	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 ES, 2…5000 ms	10 ms	Específico de la aplicación
Max. Duration of Configuration Connections [ms]	Aquí se define de cuánto tiempo se dispone dentro de un ciclo de CPU para la comunicación de datos de proceso, 6…	6 ms	Específico de la aplicación
Target Cycle Time [ms]	Tiempo de ciclo deseado o máximo. Véase *Target Cycle Time Mode*, 0…7500 ms. El valor del tiempo de ciclo de consigna podrá ser tan grande como el tiempo de WatchDog configurado - 6 ms. De lo contrario, el sistema PES lo rechazará.	0 ms	Específico de la aplicación
Multitasking Mode	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.	Mode 1	Específico de la aplicación
Sum of UP Max. Duration for Each Cycle [µs]	Suma de los valores especificados en todos los programas de usuario para *Max. Duration for Each Cycle [µs]*; sólo lectura, no puede modificarse.	-	-

Target Cycle Time Mode	Utilización del tiempo *Target Cycle Time [ms]*.		Fixed	Específico de la aplicación
	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 la sincronización de módulos procesadores y en el 1er ciclo de activación de reload no se considerará el tiempo de ciclo deseado.		
	Dynamic-tolerant	Igual que *Dynamic*, pero en la sincronización de módulos procesadores y en el 1er ciclo de activación de reload no se considerará el tiempo de ciclo deseado.		
	Dynamic	HIMax mantendrá en lo posible el tiempo de ciclo deseado, pero ejecutará el ciclo tan rápido como sea posible.		
Minimum Configuration Version	SILworX-V2	El código se generará igual que en SILworX V2, salvo para nuevas funciones. Con este ajuste podrá hacerse un reload de un proyecto creado con V2.	SILworX-V4	Específico de la aplicación
	SILworX-V3	El código se generará para HIMax V3. Con este ajuste se garantiza la compatibilidad con versiones posteriores.		
	SILworX-V4	El código se generará para HIMax V4. Con este ajuste se garantiza la compatibilidad con versiones posteriores.		
Maximum System Bus Latency [µs]	Máximo retardo de una notificación entre un módulo de E/S y el módulo procesador. 0, 100…50 000 µs		0 µs	Específico de la aplicación
	i	Para ajustar la máxima latencia del bus del sistema a un valor > 0 se necesita una licencia.		
safeethernet CRC	SILworX V.2.36.0	El 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 CRC para safe**ethernet** se generará con el algoritmo actual.		

Tabla 11: Los parámetros de sistema del recurso

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

Si en un ciclo de CPU no llega a completarse el procesado de comunicación, se proseguirá en el ciclo inmediatamente siguiente de CPU desde el punto de interrupción.

Aunque ello retrasará la comunicación de los datos de proceso, así se procesarán completa y uniformemente todas las conexiones con interlocutores externos.

En el firmware HIMax-CPU V3 obra por defecto una duración máx. de conexiones de configuración de SILworX de 6 ms. No obstante, la duración de procesado de la comunicación con interlocutores externos en un ciclo de CPU podrá sobrepasar dicho valor predeterminado.

En el firmware HIMax-CPU V4 habrá que ajustar una duración máx. de conexiones de configuración teniendo en cuenta el tiempo de WatchDog predefinido.

Configuración adecuada: seleccione el valor de forma tal que puedan ejecutarse las tareas cíclicas del procesador en el tiempo restante *Watchdog Time - Max. Duration of Configuration Connections*.

La cantidad de los datos de proceso a comunicar dependerá de la cantidad de I/Os remotas configurada, de las conexiones existentes a los PADT y de los módulos del sistema que tengan una interfaz Ethernet.

Una primera configuración puede calcularse como sigue:

$T_{config} = (n_{com} + n_{RIO} + n_{PADT}) * 0{,}25\ ms + 2\ ms + 4 * T_{latencia}$, donde

T_{config}	Parámetro de sistema *Max. Duration of Configuration Connections [ms]*
n_{com}	Cantidad de módulos con interfaces Ethernet {SB, CPU, COM}
n_{RIO}	Cantidad de las I/Os remotas configuradas
n_{PADT}	máx. cantidad de conexiones PADT = 5
$T_{latencia}$	Parámetro de sistema *Maximum System Bus Latency [µs]*

Si el tiempo calculado es menor que 6 ms, se redondeará a 6 ms. Es posible modificar más tarde el tiempo calculado en base a la estadística online, bien corrigiéndolo en las propiedades del recurso o directamente en modo online.

i Al generarse el código y al convertir el proyecto aparecerá un mensaje en el PADT, en caso de que el valor configurado de *Max. Duration of Configuration Connections* sea menor que el calculado con la fórmula de arriba.

9.3.2 Variables de sistema del hardware

Estas variables sirven para modificar en ciertas circunstancias la respuesta del sistema de control ya en funcionamiento.

Parámetro/Switch	Función	Config. por defecto	Ajuste para funcionamiento seguro
Force Deactivation	Sirve para impedir y desactivar inmediatamente la función de forzado	OFF	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	OFF	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	OFF	Específico de la aplicación
Reload Deactivation	Inhabilita la realización de recargas por reload	OFF	Específico de la aplicación

Tabla 12: Variables de sistema del hardware

En el editor de hardware de SILworX, a estas variables del sistema podrán asignárseles variables globales, cuyo valor será modificado por una entrada física o por la lógica del programa de usuario.

Ejemplo: Bloqueo/desbloqueo del PES

El bloqueo del PES significa restringir las posibilidades de intervención del usuario durante el funcionamiento. Así se evitan posibles manipulaciones no autorizadas del programa de usuario.

El desbloqueo del PES significa eliminar el bloqueo activo, por ejemplo para realizar trabajos de reglaje del sistema de control.

Para la restricción se usan las tres variables de sistema *Read only in run*, *Reload-Deactivation* y *Force-Deactivation*.

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 mediante el reinicio de un módulo procesador con el selector de modo en la posición *Init*. Entonces se podrá cargar de nuevo un programa de usuario.

Para hacer bloqueable un sistema de control

1. Defina una variable global de tipo BOOLEANO, ponga el valor inicial en FALSE.
2. Asigne variables globales a las tres variables de sistema *Read only in Run*, *Reload Deactivation* y *Force Deactivation* como variable de salida.
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 digital, el sistema de control estará desbloqueado.

9.4 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 orientado a la seguridad debido a 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" sólo tras consultar al ente oficial responsable del acta de aprobación del equipo.

Durante el forzado, la persona responsable deberá garantizar un control tecnológico suficiente de la seguridad mediante otras medidas técnicas y organizativas.
HIMA recomienda limitar temporalmente el forzado.

Más información sobre el forzado en el manual del sistema HI 801 141 ES.

9.5 Comparador de versiones seguro

El comparador de versiones seguro de SILworX puede comparar configuraciones de recurso entre sí:

- Configuración de recurso cargada en el sistema de control
- Configuración de recurso presente en el PADT
- Configuración de recurso exportada (archivada)

El resultado del comparador tienen la calidad SIL 3, pues se genera a partir de los archivos cargables de CRCs.

El comparador de versiones seguro deberá usarse para comprobar las modificaciones del programa antes de cargarlo al sistema de control.

El mismo determina exactamente las partes modificadas de la configuración del recurso. Ello hace más fácil comprobar las modificaciones y determinar los datos de prueba.

La programación estructurada y el uso de nombres significativos desde la primera versión de configuración son de gran ayuda para comprender el resultado de la comparación.

9.6 Protección contra manipulaciones

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

El PES y el sistema de programación SILworX integran mecanismos de protección 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. Dichas modificaciones pueden transferirse al PES mediante las funciones de carga Download o Reload.
- Las posibilidades de intervención dependerán del nivel de derechos de acceso del usuario de la sesión en curso en el PES.
- Para conectarse al PES, el sistema de programación SILworX necesita la contraseña del usuario de la sesión en curso.
- No es necesario tener conectados PADT y PES durante el modo RUN.

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.

⚠ PELIGRO

¡Posibles daños personales por manipulación no autorizada del sistema de control!

¡El sistema de control debe protegerse contra intervenciones no autorizadas!

Por ejemplo:

- **Cambie el nombre y la contraseña originales predeterminadas.**
- **Controle el acceso físico al sistema de control y al PADT.**

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

La conexión entre PADT y PES sólo es necesaria para cargar el programa de usuario o para el diagnóstico. Durante el funcionamiento normal no es necesario tener conectados el PADT y el PES, evitándose posibles intervenciones no autorizadas si se tienen desconectados uno del otro.

10 Programa de usuario

En este capítulo se exponen los aspectos técnicos de seguridad para el programa de usuario.

10.1 Procedimiento general

Procedimiento general de programación de dispositivos de automatización HIMax para aplicaciones con fines de seguridad:

1. Especificación de la función del sistema de control.
2. Escritura del programa de usuario.
3. Traducción del programa de usuario:
   Programa de aplicación creado sin errores y ejecutable.
4. Verificación y validación.

A continuación, el usuario podrá probar su programa de aplicación y finalmente el PES podrá adoptar el funcionamiento seguro.

10.2 Marco de uso con fines de seguridad

(Consignas, reglamentación y obligaciones de seguridad en el capítulo 3.4 “Obligaciones de seguridad”.)

El programa de usuario deberá introducirse con el software de programación SILworX. El sistema operativo autorizado para PC consta en la documentación de habilitación de versión de SILworX a utilizar.

El sistema de programación SILworX contiene básicamente:

- Introducción (editor de programas), monitoreo y documentación.
- Variables globales con nombres simbólicos y tipo de datos (BOOL, UINT etc.).
- Asignación de los sistemas de control del sistema HIMax (editor de hardware).
- Traducción del programa de aplicación del usuario a un formato cargable al PES.
- Configuración de la comunicación

10.2.1 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 técnicas de seguridad requeridas (1oo2, 2oo3) (ver anexo “Aumento del valor 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 probar.
- Fácil de modificar.

10.2.2 Funciones del programa de usuario

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

En la programación deberá tenerse en cuenta el principio de corriente de reposo para las entradas y salidas físicas. 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”.
- 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 funcionales.
- Para simplificar la lógica podrán invertirse como se desee las entradas y salidas de todos los bloques funcionales y las variables.
- El programador deberá evaluar las señales de error de las E/S o de los bloques lógicos.

Es aconsejable encapsular las funciones en bloques funcionales de propia creación y funciones estándares. Así, un programa de usuario podrá estructurarse claramente en módulos (funciones, bloques funcionales). Cada módulo podrá considerarse (y probarse) por separado. Ensamblando los módulos para constituir un módulo mayor o un programa del usuario se obtendrá una función compleja preparada.

10.2.3 Parámetros de sistema del programa de usuario

Los siguientes switches y parámetros de un programa de usuario podrá Ud. configurarlos en el cuadro de diálogo *Properties* del programa de usuario:

Switch/ Parámetro	Función		Valor por defecto	Ajuste para funcionamiento seguro
Name	Nombre del programa de usuario			Cualquiera
Safety Integrity Level	Nivel de seguridad: SIL0…SIL3 (sólo para documentación).		SIL3	Específico de la aplicación
Start	ON:	Se permite iniciar el programa de usuario mediante PADT.	ON	Específico de la aplicación
	OFF:	No se permite iniciar el programa de usuario mediante PADT.		
Program Main Enable	Habilitación de cambios de otros switches del programa de usuario. ¡Tiene efecto sólo con el switch *Main Enable* del recurso en pos. ON!		ON	-
AutoStart	Tipo de AutoStart habilitado: cold start, warm start, off.		Cold start	Específico de la aplicación
Test Mode Allowed	ON	Se permite el modo de prueba para el programa de usuario.	OFF	Específico de la aplicación
	OFF	No se permite el modo de prueba para el programa de usuario.		
Local Forcing Allowed	ON:	Se permite el forzado al nivel del programa.	OFF	Se recomienda: OFF
	OFF:	No se permite el forzado al nivel del programa.		
Reload Allowed	ON:	Se permite el reload del programa de usuario.	ON	Específico de la aplicación
	OFF:	No se permite el reload del programa de usuario.		
Program's Maximum CPU Cycles Count	Máxima cantidad de ciclos de CPU que puede durar un ciclo del programa de usuario.		1	Específico de la aplicación
Max. Duration for Each Cycle [µs]	Máximo tiempo de ejecución por ciclo del módulo procesador para un programa de usuario: 1…7 500 000 µs, 0: sin limitación.		0 µs	Específico de la aplicación
Local Force Timeout Reaction	Reacción del programa de usuario al expirar el tiempo de forzado: ▪ Finalizar sólo la función de forzado (Stop Forcing Only). ▪ Detener el programa (Stop Program).		Stop Forcing Only.	-
Program ID	ID para identificar el programa en la pantalla de SILworX, 1…32		1	Específico de la aplicación
WatchDog Time [ms] (calculated)	Tiempo de monitoreo del programa de usuario, calculado a partir de la máxima cantidad de ciclos y el tiempo WatchDog del recurso ¡No puede modificarse!			
Code Generation Compatibility	SILworX V4	SILworX V4	SILworX V4	Específico de la aplicación
	SILworX V3	La generación del código es compatible con SILworX V3.		
	SILworX V2	La generación del código es compatible con SILworX V2.		

Tabla 13: Parámetros de sistema del programa de usuario

10.2.4 Generación de códigos

Tras completar la introducción del programa de usuario y la asignación de E/S del sistema de control, se generará el código. Se creará el CRC de configuración, la suma de verificación de los archivos de configuración.

Se trata de una signatura de toda la configuración que se genera en código hexadecimal y formato de 32 bits. Abarca todos los elementos configurables o modificables, tales como la lógica, las variables y las posiciones de los switches.

NOTA

¡Posibles disfunciones del sistema de control!

Antes de cargar el programa de aplicación del usuario para el funcionamiento seguro, es indispensable que el usuario lo compile dos veces. Ambas versiones deberán tener idénticas sumas de verificación.

Mediante la segunda compilación y la comparación de las sumas de verificación pueden descubrirse falseamientos del programa del usuario causadas por errores esporádicos del hardware o del sistema operativo del PC utilizado.

10.2.5 Descarga e inicio del programa de usuario

El proceso de carga de un PES del sistema HIMax por download sólo podrá tener lugar cuando previamente se haya colocado en el estado STOP.

Un proceso de carga incluye todos los programas de usuario de la configuración del proyecto. El sistema monitorea que se cargue la configuración del proyecto en su integridad. 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 una unidad de disco) cada vez que se carguen programas de usuario al sistema de control, también en el caso de usar la función reload a tal propósito.

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

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

10.2.6 Reload

Si se efectúan modificaciones en programas de usuario, éstas podrán transferirse al PES sin interrumpir el funcionamiento. Tras haber sido verificado por el sistema operativo, el programa de usuario modificado se activará y asumirá 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.

Al cargar “Actions” por reload, observe:

La función reload carga “Actions” con todos sus datos. Considere concienzudamente 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.

Antes de ejecutar una carga por reload, el sistema operativo comprueba si las tareas adicionales necesarias aumentarán el tiempo de ciclo de los programas de usuario en curso hasta el punto de sobrepasarse el tiempo definido de WatchDog. De ser así, la carga por reload se cancelará con un mensaje de error y el sistema de control seguirá operando en la configuración de proyecto activa hasta ese momento.

El sistema de control puede cancelar una carga por reload.

Para garantizar el éxito del reload, deberá considerarse un margen de tiempo para el mismo al definir el tiempo de WatchDog o aumentar provisoriamente el margen de tiempo de WatchDog del sistema de control.

El aumento provisorio del tiempo de WatchDog habrá que acordarlo con el ente de inspección competente.

Si se sobrepasa el tiempo “Target-Cycle-Time” podrá también cancelarse el reload.

La función de carga reload sólo será posible si el parámetro de sistema “Reload Allowed” está activo (“ON”) y la variable de sistema “Reload Deactivation” está anulada (“OFF”).

Es responsabilidad del usuario planificar márgenes de tiempo de reserva al calcular el tiempo de WatchDog. Estos deberían permitir dominar las siguientes situaciones:

- Fluctuaciones en el tiempo de ciclo del programa de usuario
- Repentinas e intensas solicitaciones del ciclo, p.ej. debido a la comunicación
- Expiración de límites de tiempo durante la comunicación.

Para más información del tiempo de WatchDog, véase el capítulo 3.2.2.

10.2.7 Prueba en línea

En la lógica del programa de usuario es admisible el uso de recuadros OLT (Online-Test) para visualizar variables durante el funcionamiento del sistema de control.

Hallará más información sobre cómo usar los recuadros OLT con ayuda de la palabra clave “OLT Field” en la ayuda directa en pantalla de SILworX y en el manual de primeros pasos HI 801 194 ES.

10.2.8 Modo paso a paso

Para localizar errores, es posible ejecutar paso a paso (es decir, ciclo por ciclo) el programa de usuario en la prueba en línea. Cada ciclo se desencadenará mediante un comando del PADT.

Esta función solamente podrá usarse si está activado (“ON”) el parámetro de sistema **Freeze Allowed** para el respectivo programa de usuario.

Estado	Significado
OFF	No es posible el modo paso a paso.
ON	Es posible el modo paso a paso (opción seleccionada por defecto).

Tabla 14: Switch de programa de usuario **Freeze Allowed**

NOTA

¡Posible perturbación del modo con función orientada a la seguridad!

¡En el funcionamiento orientado a la seguridad no es admisible el modo paso a paso!

10.2.9 Modificación en línea de parámetros del sistema

Es posible modificar algunos parámetros de sistema de control 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.

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.

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!

Los parámetros modificables en línea se relacionan en la Tabla 11.

10.2.10 Documentación de programa para aplicaciones con función orientada a la seguridad

El sistema de programación SILworX 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

La documentación forma parte del acta de aprobación de funciones de un sistema sujeto a autorización por parte de una ente de inspección oficial (p.ej. TÜV).

10.2.11 Multitasking

Multitasking designa la capacidad del sistema HIMax de ejecutar hasta 32 programas de usuario dentro del módulo procesador.

Los programas de usuario podrán iniciarse o detenerse y también cargarse por reload independientemente unos de otros.

El ciclo de un programa de usuario puede durar varios ciclos del módulo procesador. Esto puede controlarse 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:

$\text{Watchdog-Time}_{\text{user program}} = \textit{Watchdog-Time}_{\text{processor module}} * \textit{Maximum Number of Cycles}$

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 haberse limitado estos con el parámetro *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 éste escribe!
- Un programa de usuario evalúa variables globales escritas por otro programa de usuario por lo menos un ciclo más tarde del módulo procesador. En caso extremo, puede demorarse hasta 32 ciclos del módulo procesador. ¡Ello retarda correspondientemente la reacción a modificaciones de tales variables globales!

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 sólo podrán ser escritos con valores en un lugar: bien en un programa de usuario por entradas con función orientada a la seguridad o por protocolos de comunicación orientados a 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 sistema HI 801 141 ES.

10.2.12 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 sólo a la función del usuario, pero no a los módulos de automatización con función orientada a la seguridad del sistema HIMax, pues estos ya han pasado el examen de tipos.

10.3 Lista de chequeo de creación de un programa de usuario

Esta es una lista de chequeo que HIMA recomienda usar para el cumplimiento de los aspectos técnicos de seguridad en la programación, antes y después de cargar el programa nuevo o modificado. La lista de chequeo puede usarse como documento de planificación, sirviendo al mismo tiempo de comprobante de la realización concienzuda de la planificación.

La lista de chequeo está a su disposición en formato Microsoft® Word® en el sitio web de HIMA.

11 Configuración de la comunicación

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

11.1 Protocolos estándar

Toda una serie de protocolos de comunicación permite sólo una transmisión de datos sin función orientada a la seguridad. Podrán usarse para las partes de una tarea de automatización no orientadas a 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 de los siguientes protocolos estándar:

- En las interfaces Ethernet del módulo de comunicación:
  - Modbus-TCP (Master/Slave)
  - Modbus redundante (Slave).
  - SNTP
  - Send/Receive TCP
  - PROFINET-IO (Controller, Device).
- En las interfaces de bus de campo (RS 485) del módulo de comunicación y según ejecución del dispositivo:
  - Modbus (Master/Slave).
  - Modbus redundante (Slave).
  - PROFIBUS-DP (Master/Slave).

11.2 Protocolo con función orientada a la seguridad safe**ethernet**

El monitoreo de la comunicación para funciones de seguridad habrá que parametrizarlo en el editor de safe**ethernet**.

Hallará más información sobre safe**ethernet** en el manual de comunicación HI 801 195 ES.

NOTA

¡Es posible una transición involuntaria al estado seguro!

¡"ReceiveTMO" es un parámetro orientado a la seguridad!

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

i ¡"ReceiveTMO" tiene validez también en el sentido opuesto, desde el PES 2 al PES 1!

Si dentro del tiempo *ReceiveTMO* no se recibe respuesta correcta del interlocutor de comunicación, HIMax cerrará la comunicación con función orientada a 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 de seguridad implementadas mediante safe**ethernet** sólo se permite utilizar la opción **Use Initial Data**.

i En los siguientes cálculos del máximo tiempo de reacción (Worst Case Reaction Time*)* podrá usarse el modo “Target-Cycle-Time” en lugar del “WatchDog-Time”, en caso de haberse configurado el modo “Target-Cycle-Time” como “*fixed*” o “*fixed tolerant*”.

11.3 Máximo tiempo de reacción para safeethernet

En los siguientes ejemplos, las fórmulas de cálculo del máximo tiempo de reacción de una conexión con sistemas de control HIMatrix tendrán validez sólo cuando para estos se haya definido el tiempo de seguridad = 2 * tiempo de WatchDog. Estas fórmulas son siempre válidas para los sistemas de control HIMax.

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

Términos:

ReceiveTMO:	Tiempo de monitoreo en el sistema PES 1, dentro del cual deberá recibirse una respuesta válida del sistema PES 2. De lo contrario, tras expirar este 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. La duración del ciclo RUN dependerá de la complejidad del programa de usuario y de la cantidad de las conexiones safe**ethernet**. El tiempo de WatchDog (WDT) consta en las propiedades del recurso.
Worst Case Reaction Time	Máximo tiempo de reacción para la transmisión del cambio de la señal de una entrada física (IN) de un sistema PES 1 hasta el cambio de la salida física (OUT) de un sistema PES 2.
Delay:	Retardo en una línea de transmisión, p. ej. en conexiones por módem o satélite. En una conexión directa puede suponerse en principio un retardo de 2 ms. El retardo que de hecho se dé en la línea de transmisión podrá ser evaluado por el administrador de la red responsable de ello.

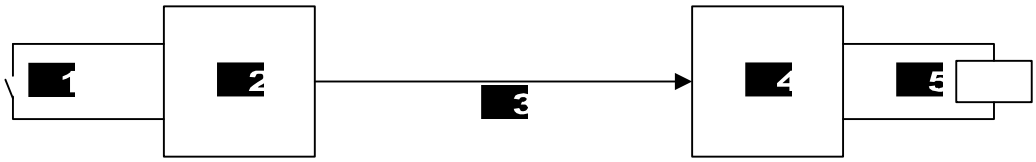
Para los siguientes cálculos de los máximos tiempos de reacción admisibles tienen validez estas condiciones:

- Las señales transmitidas con safe**ethernet** deberán procesarse en los respectivos sistemas de control dentro de un ciclo de CPU.
- Deberán sumarse además los tiempos de reacción de sensores y actuadores.

Los cálculos son válidos también para señales en el sentido opuesto.

11.3.1 Cálculo del tiempo máximo de reacción de dos sistemas de control HIMax

El tiempo máximo de reacción T_R (Worst Case) desde el cambio de estado de un transductor del sistema de control 1 hasta la reacción de la salida del sistema de control 2 puede calcularse como sigue:



1 Entrada
2 Sistema de control HIMax 1
3 Protocolo con función relacionada con la seguridad
4 Sistema de control HIMax 2
5 Salida

Fig. 3: Tiempo de reacción en caso de conectar dos sistemas de control HIMax

$T_R = t_1 + t_2 + t_3$

T_R Worst Case Reaction Time

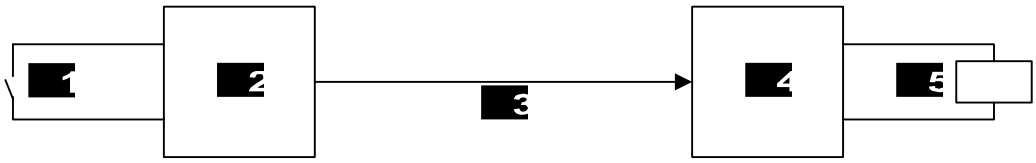
t_1 Tiempo de seguridad del sistema de control HIMax 1

t_2 *ReceiveTMO*

t_3 Tiempo de seguridad del sistema de control HIMax 2

11.3.2 Cálculo del tiempo máximo de reacción en conjunción con un sistema de control HIMatrix

El tiempo máximo de reacción T_R (Worst Case) desde el cambio de estado de un transductor (IN) del sistema de control HIMax hasta la reacción de la salida (OUT) del sistema de control HIMatrix puede calcularse como sigue:



1 Entrada
2 Sistema de control HIMax
3 Protocolo con función relacionada con la seguridad
4 Sistema de control HIMatrix
5 Salida

Fig. 4: Tiempo de reacción de un HIMax en conjunción con un sistema de control HIMatrix

$T_R = t_1 + t_2 + t_3$

T_R Worst Case Reaction Time

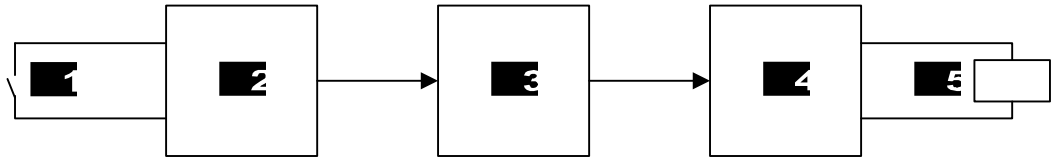
t_1 Tiempo de seguridad del sistema de control HIMax

t_2 *ReceiveTMO*

t_3 2 * tiempo de WatchDog del sistema de control HIMatrix

11.3.3 Cálculo del tiempo máximo de reacción con dos sistemas de control HIMatrix o I/Os remotas

El tiempo máximo de reacción T_R (Worst Case) desde el cambio de estado de un transductor (IN) en el primer sistema de control HIMatrix o en las I/O remotas (p. ej. F3 DIO 20/8 01) hasta la reacción de la salida (OUT) en el segundo sistema de control HIMatrix o en la I/O remota puede calcularse como sigue:



1 Entrada
2 I/O remota 1
3 Sistema de control HIMax
4 I/O remota 2
5 Salida

Fig. 5: Tiempo de reacción con dos I/Os remotas y un sistema de control 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 de la I/O remota 1

t_2 *ReceiveTMO1*

t_3 2 * tiempo de WatchDog del sistema de control HIMax

t_4 *ReceiveTMO2*

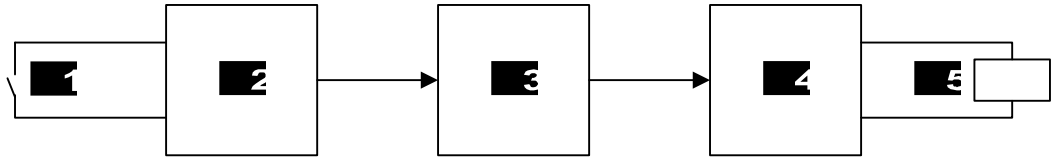
t_5 2 * tiempo de WatchDog de la I/O remota 2

---

i Las dos I/Os remotas 1 y 2 también pueden ser idénticas. Los tiempos serán válidos aun cuando en lugar de una I/O remota se utilice un sistema de control HIMatrix.

11.3.4 Cálculo del tiempo máximo de reacción con dos HIMax y un sistema de control HIMatrix

El tiempo máximo de reacción T_R (Worst Case) desde el cambio de estado de un transductor (IN) en el primer sistema de control HIMax hasta la reacción de la salida (OUT) en el segundo sistema de control HIMax puede calcularse como sigue:



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

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

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

T_R Worst Case Reaction Time

t_1 Tiempo de seguridad del sistema de control HIMax 1

t_2 *ReceiveTMO1*

t_3 2 * tiempo de WatchDog del sistema de control HIMatrix

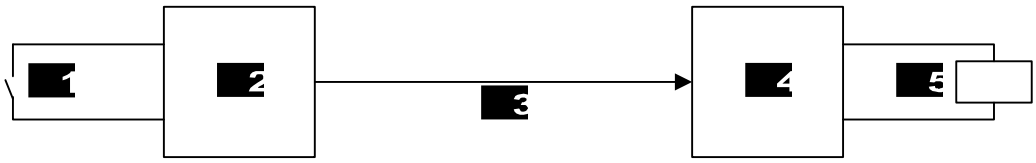
t_4 *ReceiveTMO2*

t_5 Tiempo de seguridad del sistema de control HIMax 2

i Ambos sistemas de control HIMax 1 y 2 también pueden ser idénticos.
El sistema de control HIMatrix también puede ser un sistema de control HIMax.

11.3.5 Cálculo del tiempo máximo de reacción de dos sistemas de control HIMatrix

El tiempo máximo de reacción T_R (Worst Case) desde el cambio de estado de un transductor del sistema de control 1 hasta la reacción de la salida del sistema de control 2 puede calcularse como sigue:



1 Entrada
2 Sistema de control HIMatrix 1
3 Protocolo con función relacionada con la seguridad
4 Sistema de control HIMatrix 2
5 Salida

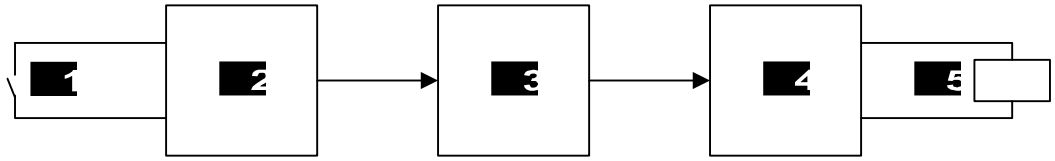
Fig. 7: Tiempo de reacción en caso de conectar dos sistemas de control HIMatrix

$T_R = t_1 + t_2 + t_3$

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

11.3.6 Cálculo del tiempo máximo de reacción con dos I/Os remotas

El tiempo máximo de reacción T_R desde el cambio de estado de un transductor (IN) del primer sistema de control HIMatrix o I/O remota (p. ej. F3 DIO 20/8 01) hasta la reacción del segundo sistema de control HIMatrix o I/O remota puede calcularse de la siguiente forma:



1 Entrada
2 I/O remota 1
3 Sistema de control HIMatrix
4 I/O remota 2
5 Salida

Fig. 8: Tiempo de reacción con I/Os remotas

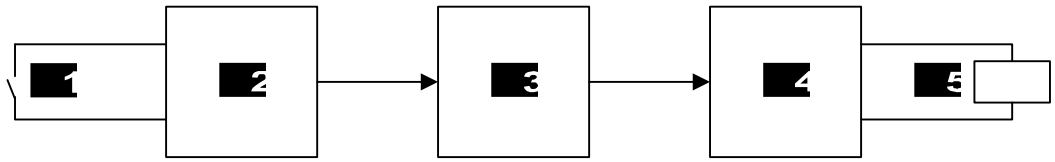
$$T_R = t_1 + t_2 + t_3 + t_4 + t_5$$

T_R Worst Case Reaction Time
t_1 2 * tiempo de WatchDog de la I/O 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 I/O remota 2

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

11.3.7 Cálculo del tiempo máximo de reacción con dos sistemas HIMatrix y un HIMax

El tiempo máximo de reacción T_R desde el cambio de estado de un transductor (IN) del primer sistema de control HIMatrix hasta la reacción de la salida (OUT) del segundo sistema de control 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. 9: 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

11.4 Protocolo con función orientada a la seguridad PROFIsafe

Las obligaciones a cumplir en el uso del protocolo PROFIsafe se indican en el manual de comunicación HI 801 195 ES. Las obligaciones tienen que cumplirse.

Las fórmulas de cálculo del tiempo de reacción se indican asimismo en el manual de comunicación.

Anexo

Aumento del nivel SIL de sensores y actuadores

Los sistemas de control HIMax con función orientada a la seguridad se usan para aplicaciones de seguridad 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. En tales casos se dispone de la siguiente solución:

- 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 éste 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 un programa 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.

Términos y abreviaturas

Término	Descripción
ARP	Address Resolution Protocol: protocolo de red para asignar direcciones de red a direcciones de hardware
AI	Analog input: entrada analógica
Connector Board	Tarjeta de conexión para módulo HIMax
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
FTT	Tiempo de tolerancia de errores
ICMP	Internet Control Message Protocol: protocolo de red para mensajes de estado y de error
IEC	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	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 solicitar una función de seguridad
PFH	Probability of Failure per Hour: probabilidad de una disfunción peligrosa por hora
R	Read
ID de Rack	Identificación (número) de un rack
Sin repercusiones	Suponiendo que hay dos circuitos de entrada conectados a la misma fuente (p. ej. transmisor). Entonces un circuito de entrada se denominará “sin repercusiones”, cuando no falsee las señales del otro circuito de entrada.
R/W	Read/Write
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 HIMax
SNTP	Simple Network Time Protocol (RFC 1769)
SRS	Direccionamiento por “Sistema.Rack.Slot” de un módulo
SW	Software
TMO	TimeOut
TMR	Triple Module Redundancy: módulos de triple redundancia
W	Write
w_S	Valor máximo del total de componentes de corriente alterna
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

HI 801 196 ES
© 2015 HIMA Paul Hildebrandt GmbH
HIMax y SILworX son marcas registradas de:
HIMA Paul Hildebrandt GmbH

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

SAFETY
NONSTOP