

# Modicon M580

## Manual de seguridad

Traducción del manual original

QGH46986.05  
11/2021

# Información legal

La marca Schneider Electric y cualquier otra marca comercial de Schneider Electric SE y sus filiales mencionadas en esta guía son propiedad de Schneider Electric SE o sus filiales. Todas las otras marcas pueden ser marcas comerciales de sus respectivos propietarios. Esta guía y su contenido están protegidos por las leyes de copyright aplicables, y se proporcionan exclusivamente a título informativo. Ninguna parte de este manual puede ser reproducida o transmitida de cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otro), para ningún propósito, sin el permiso previo por escrito de Schneider Electric.

Schneider Electric no concede ningún derecho o licencia para el uso comercial de la guía o su contenido, excepto por una licencia no exclusiva y personal para consultarla "tal cual".

La instalación, utilización, mantenimiento y reparación de los productos y equipos de Schneider Electric la debe realizar solo personal cualificado.

Debido a la evolución de las normativas, especificaciones y diseños con el tiempo, la información contenida en esta guía puede estar sujeta a cambios sin previo aviso.

En la medida permitida por la ley aplicable, Schneider Electric y sus filiales no asumen ninguna responsabilidad u obligación por cualquier error u omisión en el contenido informativo de este material o por las consecuencias derivadas o resultantes del uso de la información contenida en el presente documento.

Como parte de un grupo de empresas responsables e inclusivas, estamos actualizando nuestras comunicaciones que contienen terminología no inclusiva. Sin embargo, hasta que completemos este proceso, es posible que nuestro contenido todavía incluya términos estandarizados del sector que nuestros clientes puedan considerar inapropiados.

---

# Tabla de contenido

Información de seguridad.....	9
Antes de empezar .....	10
Iniciar y probar .....	11
Funcionamiento y ajustes.....	12
Acerca de este libro.....	13
Función de seguridad de M580 .....	15
Función de seguridad de M580.....	16
Normas de certificación .....	20
Certificaciones .....	21
Normas y certificaciones .....	25
Módulos compatibles con el sistema de seguridad M580.....	26
Módulos certificados del sistema de seguridad M580 .....	27
Módulos no interferentes.....	29
Ciberseguridad para el sistema de seguridad M580.....	34
Ciberseguridad para el sistema de seguridad M580 .....	34
Ciclo de vida de la aplicación .....	35
Ciclo de vida de la aplicación.....	35
Módulos de E/S de seguridad M580 .....	45
Características compartidas del módulo de E/S de seguridad M580 .....	46
Presentamos los módulos de E/S de M580seguridad .....	46
Descripción general de diagnósticos para módulos de E/S de seguridad M580 .....	48
Módulo de entrada analógica BMXSAI0410 .....	51
Módulo de entrada analógica de seguridad BMXSAI0410 .....	51
Conector de cableado BMXSAI0410 .....	53
Ejemplos de cableado de aplicación de entrada de BMXSAI0410.....	55
Estructura de datos de BMXSAI0410 .....	61
Módulo de entrada digital BMXSDI1602 .....	65
Módulo de entrada digital de seguridad BMXSDI1602 .....	65
Conector de cableado BMXSDI1602 .....	67
Ejemplos de cableado de aplicación de entrada de BMXSDI1602 .....	73
Estructura de datos de BMXSDI1602 .....	94
Módulo de salida digital BMXSDO0802.....	99

---

Módulo de salida digital de seguridad BMXSDO0802 .....	99
Conector de cableado BMXSDO0802 .....	101
Ejemplos de cableado de aplicación de salida BMXSDO0802 .....	104
Estructura de datos de BMXSDO0802.....	110
Módulo de salida de relé digital BMXSRA0405 .....	115
Módulo de salida de relé digital de seguridad BMXSRA0405.....	115
Conector de cableado BMXSRA0405.....	116
Ejemplos de cableado de aplicación de salida BMXSRA0405 .....	118
Estructura de datos de BMXSRA0405 .....	127
Fuentes de alimentación de seguridad de M580 .....	132
Fuentes de alimentación de seguridad de M580 .....	133
Diagnósticos del módulo de alimentación de seguridad M580.....	136
DDT de seguridad de M580.....	138
Validación de un sistema de seguridad M580 .....	140
Arquitectura del módulo de seguridad M580 .....	141
Arquitectura de seguridad de la CPU y del coprocesador de seguridad de M580 .....	141
Arquitectura de seguridad del módulo de entrada analógica BMXSAI0410.....	145
Arquitectura de seguridad del módulo de entrada digital BMXSDI1602 .....	146
Arquitectura de seguridad del módulo de salida digital BMXSDO0802.....	147
Arquitectura de seguridad del módulo de salida de relé digital BMXSRA0405 .....	149
Valores de SIL y MTTF del módulo de seguridad M580 .....	150
Cálculos del nivel de integridad de seguridad.....	150
Cálculos de tiempo y rendimiento del sistema de seguridad M580.....	157
Tiempo de seguridad del proceso.....	157
Impacto de las comunicaciones de CIP Safety en el tiempo de reacción del sistema de seguridad .....	166
Biblioteca de seguridad .....	169
Biblioteca de seguridad.....	169
Separación de datos en un sistema de seguridad M580 .....	173
Separación de datos en un proyecto de seguridad de M580 .....	174

---

---

Cómo transferir datos entre áreas de espacios de nombres .....	177
Comunicaciones del sistema de seguridad M580.....	179
Sincronización horaria .....	180
Configuración de la sincronización horaria con la versión del firmware de la CPU 3.10 o anterior .....	180
Sincronización horaria para la versión del firmware de la CPU 3.20 o posterior.....	184
Comunicaciones entre pares.....	186
Comunicación entre pares.....	186
Arquitectura entre pares con la versión del firmware de la CPU 3.10 o anterior .....	187
Configuración del DFB S_WR_ETH_MX de la lógica del programa del PAC emisor.....	194
Configuración del DFB S_RD_ETH_MX de la lógica del programa del PAC emisor.....	196
Arquitectura entre pares con la versión del firmware de la CPU 3.20 o posterior.....	200
Configuración del DFB S_WR_ETH_MX2 de la lógica del programa del PAC emisor.....	207
Configuración del DFB S_RD_ETH_MX2 de la lógica del programa del PAC receptor .....	209
Comunicaciones del canal negro de M580.....	213
Comunicación de CPU a E/S de seguridad de M580 .....	216
M580 Comunicaciones de PAC de seguridad a E/S.....	216
Diagnóstico de un sistema de seguridad de M580 .....	218
Diagnósticos de la CPU y coprocesador de seguridad de M580 .....	219
Diagnósticos de condiciones de bloqueo .....	219
Diagnósticos de condiciones sin bloqueo.....	222
LED de diagnóstico de la CPU de seguridad de M580 .....	224
LED de diagnóstico de coprocesador de seguridad M580 .....	227
LED de acceso a la tarjeta de memoria.....	229
Diagnósticos de fuente de alimentación de seguridad de M580.....	232
Diagnóstico mediante LED de la fuente de alimentación .....	232
Diagnósticos de entradas analógicas de BMXSAI0410.....	234
Diagnósticos de DDDT de BMXSAI0410 .....	234

---

---

LED de diagnóstico de entradas analógicas BMXSAI0410 .....	235
Diagnósticos de entrada digital de BMXSDI1602 .....	239
Diagnósticos de DDDT de BMXSDI1602 .....	239
LED de diagnóstico de entradas digitales BMXSDI1602 .....	241
Diagnósticos de salida digital de BMXSDO0802 .....	245
Diagnósticos de DDDT de BMXSDO0802.....	245
LED de diagnóstico de salidas digitales BMXSDO0802 .....	247
Diagnósticos de salida de relé digital BMXSRA0405 .....	251
Diagnósticos de DDDT de BMXSRA0405 .....	251
LED de diagnóstico de salida de relé digital BMXSRA0405 .....	252
Funcionamiento de un sistema de seguridad M580.....	255
Áreas de proceso, seguridad y datos globales en Control Expert.....	256
Separación de datos en Control Expert.....	257
Modalidades de funcionamiento, estados de funcionamiento y tareas .....	261
Modalidades de funcionamiento del PAC de seguridad M580 .....	261
Estados de funcionamiento del PAC de seguridad M580.....	266
Secuencias de arranque.....	272
Tareas del PAC de seguridad M580.....	276
Creación de un proyecto de seguridad de M580 .....	280
Creación de un proyecto de seguridad de M580.....	280
Firma de seguridad .....	280
Bloqueo de configuraciones de módulos de E/S de seguridad de M580.....	288
Bloqueo de configuraciones de módulos de E/S de seguridad de M580 .....	288
Inicialización de datos en Control Expert .....	291
Inicialización de datos en Control Expert para el PAC de seguridad M580 .....	291
Utilización de tablas de animación en Control Expert.....	292
Tablas de animaciones y pantallas de operador .....	292
Adición de secciones de código .....	297
Adición de código a un proyecto de seguridad de M580 .....	297
Petición de diagnóstico .....	301
Comandos de intercambio y borrado .....	304
Gestión de la seguridad de las aplicaciones.....	308
Protección de la aplicación .....	308

---

---

Protección mediante contraseña de área segura.....	316
Protección de unidad de programa, sección y subrutina.....	320
Protección de firmware.....	323
Protección del almacenamiento de datos/web.....	325
Pérdida de la contraseña.....	327
Gestión de la seguridad de la estación de trabajo.....	333
Gestión del acceso a Control Expert.....	333
Derechos de acceso .....	336
Modificaciones en Control Expert para el sistema de seguridad M580 .....	347
Transferencia e importación de proyectos de seguridad y código de M580 en Control Expert.....	347
Almacenamiento y restauración de datos entre un archivo y el PAC.....	348
CCOTF para un PAC de seguridad M580 .....	348
Cambios en las herramientas del PAC de seguridad M580.....	350
CIP Safety .....	352
Introducción a CIP Safety para los PAC de seguridad M580 .....	353
Comunicación CIP Safety.....	353
Configuración de la CPU CIP Safety M580 .....	357
Configuración del OUNID de la CPU .....	357
Configuración del dispositivo de destino CIP Safety .....	359
Resumen de configuración del dispositivo CIP Safety.....	359
Configuración del dispositivo CIP Safety mediante una herramienta facilitada por el proveedor .....	361
Configuración de DTM de dispositivo de seguridad .....	363
Utilización de los DTM.....	363
DTM de dispositivo de seguridad: Información de archivo y proveedor.....	365
DTM de dispositivo de seguridad: Número de red de seguridad.....	367
DTM de dispositivo de seguridad: Comprobar y validar la configuración.....	369
DTM del dispositivo de seguridad: Conexiones de E/S.....	369
DTM de dispositivo de seguridad: Ajustes de conexión de E/S .....	373
Ajustes de dirección IP del dispositivo de seguridad .....	373
Operaciones de CIP Safety .....	375

---

Transferencia de una aplicación CIP Safety de Control Expert al PAC .....	375
Estructura de una petición SafetyOpen de tipo 2 .....	376
Operaciones del dispositivo CIP Safety .....	377
Interacciones entre las operaciones del PAC de seguridad y la conexión de destino .....	379
Comandos del DTM de CIP Safety .....	383
Diagnóstico de CIP Safety .....	385
DDDT del dispositivo CIP Safety .....	385
Códigos de error del dispositivo CIP Safety .....	388
DDDT de la CPU autónoma CIP Safety .....	392
Diagnósticos del DTM de la CPU .....	392
Diagnósticos de conexión del dispositivo CIP Safety .....	393
<b>Apéndices</b> .....	<b>396</b>
IEC 61508 .....	397
Información general sobre IEC 61508 .....	398
Política de SIL .....	400
Objetos de sistema .....	405
Bits del sistema de seguridad M580 .....	406
Palabras del sistema de seguridad M580 .....	408
Referencias de SRAC .....	412
<b>Glosario</b> .....	<b>417</b>
<b>Índice</b> .....	<b>423</b>

# Información de seguridad

## Información importante

Lea atentamente estas instrucciones y observe el equipo para familiarizarse con el dispositivo antes de instalarlo, utilizarlo, revisarlo o realizar su mantenimiento. Los mensajes especiales que se ofrecen a continuación pueden aparecer a lo largo de la documentación o en el equipo para advertir de peligros potenciales, o para ofrecer información que aclara o simplifica los distintos procedimientos.



La inclusión de este icono en una etiqueta “Peligro” o “Advertencia” indica que existe un riesgo de descarga eléctrica, que puede provocar lesiones si no se siguen las instrucciones.



Éste es el icono de alerta de seguridad. Se utiliza para advertir de posibles riesgos de lesiones. Observe todos los mensajes que siguen a este icono para evitar posibles lesiones o incluso la muerte.

### PELIGRO

**PELIGRO** indica una situación de peligro que, si no se evita, **provocará** lesiones graves o incluso la muerte.

### ADVERTENCIA

**ADVERTENCIA** indica una situación de peligro que, si no se evita, **podría provocar** lesiones graves o incluso la muerte.

### ATENCIÓN

**ATENCIÓN** indica una situación peligrosa que, si no se evita, **podría provocar** lesiones leves o moderadas.

### **AVISO**

**AVISO** indica una situación potencialmente peligrosa que, si no se evita, **puede provocar** daños en el equipo.

## Tenga en cuenta

La instalación, manejo, puesta en servicio y mantenimiento de equipos eléctricos deberán ser realizados sólo por personal cualificado. Schneider Electric no se hace responsable de ninguna de las consecuencias del uso de este material.

Una persona cualificada es aquella que cuenta con capacidad y conocimientos relativos a la construcción, el funcionamiento y la instalación de equipos eléctricos, y que ha sido formada en materia de seguridad para reconocer y evitar los riesgos que conllevan tales equipos.

## Antes de empezar

No utilice este producto en maquinaria sin protección de punto de funcionamiento. La ausencia de protección de punto de funcionamiento en una máquina puede provocar lesiones graves al operador de dicha máquina.

### **▲ ADVERTENCIA**

#### **EQUIPO SIN PROTECCIÓN**

- No utilice este software ni los equipos de automatización relacionados en equipos que no dispongan de protección de punto de funcionamiento.
- No introduzca las manos u otras partes del cuerpo dentro de la maquinaria mientras está en funcionamiento.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

Este equipo de automatización y el software relacionado se utilizan para controlar diversos procesos industriales. El tipo o modelo del equipo de automatización adecuado para cada uso varía en función de factores tales como las funciones de control necesarias, el grado de protección requerido, los métodos de producción, la existencia de condiciones poco habituales, las normativas gubernamentales, etc. En algunos usos, puede ser necesario más de un procesador, como en el caso de que se requiera redundancia de respaldo.

Solamente el usuario, el fabricante de la máquina o el integrador del sistema conocen las condiciones y los factores presentes durante la configuración, el funcionamiento y el mantenimiento de la máquina y, por consiguiente, pueden decidir el equipo asociado y las medidas de seguridad y los enclavamientos relacionados que se pueden utilizar de forma adecuada. Al seleccionar los equipos de automatización y control, así como el software relacionado para un uso determinado, el usuario deberá consultar los estándares y las normativas locales y nacionales aplicables. La publicación National Safety Council's Accident Prevention Manual (que goza de un gran reconocimiento en los Estados Unidos de América) también proporciona gran cantidad de información de utilidad.

En algunas aplicaciones, como en el caso de la maquinaria de embalaje, debe proporcionarse protección adicional al operador, como la protección de punto de funcionamiento. Esta medida es necesaria si existe la posibilidad de que las manos y otras partes del cuerpo del operador puedan introducirse y quedar atrapadas en áreas o puntos peligrosos, lo que puede provocar lesiones graves. Los productos de software por sí solos no pueden proteger al operador frente a posibles lesiones. Por este motivo, el software no se puede sustituir por la protección de punto de funcionamiento ni puede realizar la función de esta.

Asegúrese de que las medidas de seguridad y los enclavamientos mecánicos/eléctricos relacionados con la protección de punto de funcionamiento se hayan instalado y estén operativos antes de que los equipos entren en funcionamiento. Todos los enclavamientos y las medidas de seguridad relacionados con la protección de punto de funcionamiento deben estar coordinados con la programación del software y los equipos de automatización relacionados.

**NOTA:** La coordinación de las medidas de seguridad y los enclavamientos mecánicos/eléctricos para la protección de punto de funcionamiento está fuera del ámbito de la biblioteca de bloques de funciones, la guía de usuario del sistema o de otras instalaciones mencionadas en esta documentación.

## Iniciar y probar

Antes de utilizar los equipos eléctricos de control y automatización para su funcionamiento normal tras la instalación, es necesario que personal cualificado lleve a cabo una prueba de inicio del sistema para verificar que los equipos funcionan correctamente. Es importante realizar los preparativos para una comprobación de estas características y disponer de suficiente tiempo para llevar a cabo las pruebas de forma completa y correcta.

### **ADVERTENCIA**

#### **PELIGRO DE FUNCIONAMIENTO DEL EQUIPO**

- Compruebe que se hayan seguido todos los procedimientos de instalación y configuración.
- Antes de realizar las pruebas de funcionamiento, retire de todos los dispositivos todos los bloqueos u otros medios de sujeción temporales utilizados para el transporte.
- Retire del equipo las herramientas, los medidores y el material de desecho que pueda haber.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

Realice todas las pruebas de inicio recomendadas en la documentación del equipo. Guarde la documentación del equipo para consultarla en el futuro.

---

**Las pruebas del software deben realizarse tanto en un entorno simulado como en un entorno real.**

Verifique que no existen cortocircuitos ni conexiones a tierra temporales en todo el sistema que no estén instalados según la normativa local (de conformidad con National Electrical Code de EE. UU., por ejemplo). Si fuera necesario realizar pruebas de tensión de alto potencial, siga las recomendaciones de la documentación del equipo para evitar dañar el equipo fortuitamente.

Antes de dar tensión al equipo:

- Retire del equipo las herramientas, los medidores y el material de desecho que pueda haber.
- Cierre la puerta de la carcasa del equipo.
- Retire todas las conexiones a tierra temporales de las líneas de alimentación de entrada.
- Realice todas las pruebas iniciales recomendadas por el fabricante.

## Funcionamiento y ajustes

Las precauciones siguientes proceden de NEMA Standards Publication ICS 7.1-1995 (prevalece la versión en inglés):

- Aunque se ha extremado la precaución en el diseño y la fabricación del equipo o en la selección y las especificaciones de los componentes, existen riesgos que pueden aparecer si el equipo se utiliza de forma inadecuada.
- En algunas ocasiones puede desajustarse el equipo, lo que provocaría un funcionamiento incorrecto o poco seguro. Utilice siempre las instrucciones del fabricante como guía para realizar los ajustes de funcionamiento. El personal que tenga acceso a estos ajustes debe estar familiarizado con las instrucciones del fabricante del equipo y con la maquinaria utilizada para los equipos eléctricos.
- El operador solo debe tener acceso a los ajustes de funcionamiento que realmente necesita. El acceso a los demás controles debe restringirse para evitar cambios no autorizados en las características de funcionamiento.

# Acerca de este libro

## Presentación

En este manual de seguridad se describen los módulos del sistema de seguridad M580, prestando especial atención en cómo cumplen los requisitos de seguridad de la norma IEC 61508. Proporciona información detallada sobre cómo instalar, ejecutar y mantener el sistema correctamente para ayudar a proteger a las personas, el medio ambiente, los equipos y la producción.

Esta documentación está orientada al personal cualificado familiarizado con la seguridad funcional y con Control Expert Safety. La puesta en marcha y el funcionamiento del sistema de seguridad M580 sólo pueden llevarlos a cabo personas autorizadas para ello de acuerdo con las normas de seguridad funcional vigentes.

### NOTA:

- La versión en lengua inglesa de este manual es la versión original.
- En el caso de que surja una petición de cambio o un problema de calidad relacionado con la oferta de seguridad de M580, póngase en contacto con el centro de asistencia local para obtener soporte técnico. Puede encontrar más información en la sección *Soporte/Contacto* del sitio web de Schneider Electric en:

[www.se.com/b2b/en/support/](http://www.se.com/b2b/en/support/)

## Nota de validez

Este documento es válido para <sup>™</sup>EcoStruxure Control Expert Seguridad 15.0 o posterior.

Para la conformidad de los productos y la información medioambiental (RoHS, REACH, PEP, EOLI, etc.), vaya a [www.se.com/ww/en/work/support/green-premium/](http://www.se.com/ww/en/work/support/green-premium/).

Las características técnicas de los dispositivos que se describen en este documento también se encuentran online. Si desea consultar la información online, visite la página de inicio de Schneider Electric [www.se.com/ww/en/download/](http://www.se.com/ww/en/download/).

Las características que se indican en este manual deben coincidir con las que figuran online. De acuerdo con nuestra política de mejoras continuas, es posible que a lo largo del tiempo revisemos el contenido con el fin de elaborar documentos más claros y precisos. En caso de que detecte alguna diferencia entre el manual y la información online, utilice esta última para su referencia.

## Documentos relacionados

Título de la documentación	Número de referencia
M580 Safety SRAC — SRAC Verification Plan	EIO000004540 (inglés)
Modicon M580, Guía de planificación del sistema de seguridad	QGH60283 (inglés), QGH60284 (francés), QGH60285 (alemán), QGH60286 (español), QGH60287 (italiano), QGH60288 (chino)
EcoStruxure™ Control Expert, Seguridad, Biblioteca de bloques	QGH60275 (inglés), QGH60278 (francés), QGH60279 (alemán), QGH60280 (italiano), QGH60281 (español), QGH60282 (chino)
Ciberseguridad - Plataforma de controladores Modicon - Manual de referencia	EIO000001999 (inglés), EIO000002001 (francés), EIO000002000 (alemán), EIO000002002 (italiano), EIO000002003 (español), EIO000002004 (chino)
Modicon M580 Hot Standby, Guía de planificación del sistema para arquitecturas utilizadas con más frecuencia	NHA58880 (inglés), NHA58881 (francés), NHA58882 (alemán), NHA58883 (italiano), NHA58884 (español), NHA58885 (chino)
Modicon M580, Hardware, Manual de referencia	EIO000001578 (inglés), EIO000001579 (francés), EIO000001580 (alemán), EIO000001582 (italiano), EIO000001581 (español), EIO000001583 (chino)
Modicon M580 autónomo, Guía de planificación del sistema para arquitecturas utilizadas con más frecuencia	HRB62666 (inglés), HRB65318 (francés), HRB65319 (alemán), HRB65320 (italiano), HRB65321 (español), HRB65322 (chino)
Modicon M580, Guía de planificación del sistema para topologías complejas	NHA58892 (inglés), NHA58893 (francés), NHA58894 (alemán), NHA58895 (italiano), NHA58896 (español), NHA58897 (chino)
EcoStruxure™ Automation Device Maintenance, Manual del usuario	EIO000004033 (inglés), EIO000004048 (francés), EIO000004046 (alemán), EIO000004049 (italiano), EIO000004047 (español), EIO000004050 (chino)
Unity Loader, Manual del usuario	33003805 (inglés), 33003806 (francés), 33003807 (alemán), 33003809 (italiano), 33003808 (español), 33003810 (chino)
EcoStruxure™ Control Expert, Modalidades de funcionamiento	33003101 (inglés), 33003102 (francés), 33003103 (alemán), 33003104 (español), 33003696 (italiano), 33003697 (chino)
EcoStruxure™ Control Expert, Palabras y bits de sistema, Manual de referencia	EIO000002135 (inglés), EIO000002136 (francés), EIO000002137 (alemán), EIO000002138 (italiano), EIO000002139 (español), EIO000002140 (chino)

Puede descargar estas publicaciones técnicas, el presente documento y otra información técnica de nuestro sitio web en [www.se.com/en/download/](http://www.se.com/en/download/).

# Función de seguridad de M580

## Contenido de este capítulo

Función de seguridad de M580 .....	16
------------------------------------	----

## Introducción

En este capítulo se presenta la función de seguridad de M580 del sistema de seguridad M580 y para cada módulo de seguridad.

# Función de seguridad de M580

## Introducción de la función de seguridad de M580 de Schneider Electric

Con Control Expert Seguridad, puede realizar la programación, configuración y mantenimiento de una aplicación de seguridad. Al diseñar y programar su aplicación de seguridad, aplique funciones de seguridad sólo a componentes de un bucle de seguridad.

**NOTA:** Incluya sólo módulos de seguridad, sus ajustes de configuración y sus datos en un bucle de seguridad.

Tras la puesta en marcha, mientras su sistema de seguridad M580 funciona en modalidad de seguridad, el sistema de seguridad lee entradas de seguridad, procesa la lógica de seguridad del programa de aplicación, realiza diagnósticos y aplica los resultados de la lógica a las salidas de seguridad.

Si la CPU o los diagnósticos de E/S detectan un error, el sistema de seguridad colocará la parte afectada del sistema en un estado de seguridad. En función de la naturaleza del error detectado, el ámbito de la respuesta puede colocar un solo canal de E/S, un módulo de E/S o todo el sistema en el estado de seguridad.

El estado de seguridad siempre corresponde al estado deenergizado. Por ejemplo:

- Si el módulo de entrada analógica BMXSAI0410 o el módulo de entrada digital BMXSDI1602 detecta una condición interna peligrosa, establece el valor de sus entradas a la CPU en "0" (el estado deenergizado), las cuales mantienen ese estado hasta que se resuelve la condición subyacente.
- Si el módulo de salida digital BMXSDO0802 o el módulo de salida de relé digital BMXSRA0405 detectan una condición interna peligrosa, establece sus salidas en el estado deenergizado, las cuales mantienen ese estado hasta que se resuelve la condición subyacente y se reinicia el módulo.
- Si el módulo de salida digital BMXSDO0802 o el módulo de salida de relé digital BMXSRA0405 detectan un error de comunicación en un enlace de canal negro a la CPU, el módulo de salida establece sus salidas en su estado de retorno.

**NOTA:** Puede utilizar Control Expert Safety para configurar el estado de retorno (energizado, deenergizado o mantener el último valor) por si se pierde la comunicación del canal negro entre la CPU y el módulo de salida.

- Si una CPU BMEP58•040S autónoma o BMEH58•040S Hot Standby detecta un error de comunicación en un enlace de canal negro a un módulo de entrada de seguridad, establece el estado de las entradas afectadas en "0" (estado deenergizado) hasta que el canal negro vuelve a funcionar y la CPU puede volver a leer los valores de entrada reales.

## Bucle de seguridad

Un bucle de seguridad es el conjunto de equipos y lógica que ejecuta un proceso de seguridad. Un proyecto de seguridad puede incluir varios bucles de seguridad. Para cada bucle de seguridad, debe verificar que:

- El tiempo de seguridad del proceso, página 157 sea mayor que el tiempo de reacción del sistema, página 157.
- La suma de los valores de PFD o PFH, página 150 de todos los componentes del bucle de seguridad no supera el valor máximo permitido para los siguientes elementos previstos:
  - Nivel de integridad de seguridad (1, 2, 3 o 4)
  - Modalidad de funcionamiento (baja demanda o alta demanda)
  - Intervalo de prueba

Incluya sólo el equipo de seguridad en un bucle de seguridad. Aunque puede incluir módulos no interferentes, página 29 en el proyecto de seguridad, utilícelos sólo para las tareas no seguras (MAST, FAST, AUX0 o AUX1).

### **▲ ADVERTENCIA**

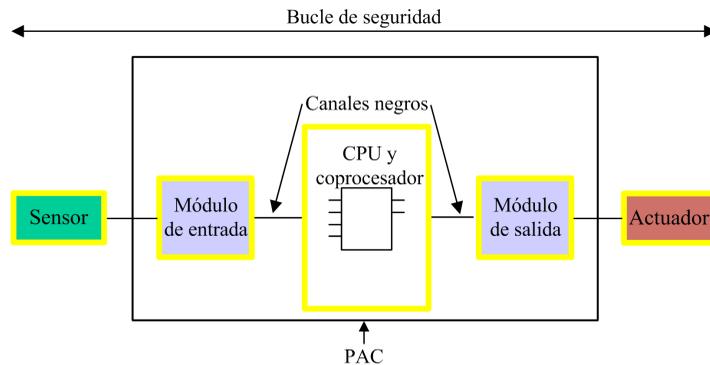
#### **PÉRDIDA DE CAPACIDAD PARA EJECUTAR FUNCIONES DE SEGURIDAD**

- Utilice sólo módulos de seguridad para realizar funciones de seguridad.
- No utilice entradas o salidas de módulos no interferentes para funciones relacionadas con la seguridad.
- No utilice variables del área global para funciones relacionadas con la seguridad.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

Consulte el tema *Separación de datos en un proyecto de seguridad de M580*, página 174 para obtener una descripción de variables del área global.

Bucle de seguridad:



El equipo de seguridad incluye los módulos de seguridad M580 de Schneider Electric:

- CPU BME•58•040S y coprocesador BMEP58CPROS3:

La CPU y el coprocesador realizan conjuntamente las tareas de lectura de entradas de seguridad, procesamiento de la lógica de seguridad, realización de diagnósticos y aplicación de resultados a las salidas. Todas estas tareas forman parte del bucle de seguridad. Los puertos utilizados para las comunicaciones de canal negro también forman parte del bucle de seguridad. Sin embargo, otros componentes de la CPU, como, por ejemplo, el puerto USB, la tarjeta de memoria SD y la memoria de acceso aleatorio estática no volátil (nvSRAM), no forman parte del bucle de seguridad.

**NOTA:** Tanto en un arranque del sistema en frío como en un arranque del sistema en caliente, la CPU y el coprocesador no cargan los datos almacenados en nvSRAM en la tarea de seguridad (los datos nvSRAM se utilizan sólo en las tareas MAST, FAST y AUX no seguras). En su lugar, la CPU y el coprocesador inicialmente aplican ajustes de configuración predeterminados de la tarjeta de memoria SD y luego aplican los valores recibidos directamente desde entradas durante el funcionamiento.

- E/S de seguridad (BMXSAI0410, BMXSDI1602, BMXSDO0802 y BMXSRA0405):

Las funciones de envío de señales de entrada, recepción de señales de salida y realización de diagnósticos forman parte del bucle de seguridad.

- Fuentes de alimentación BMXCPS4002S, BMXCPS4022S y BMXCPS3522S:

Estas fuentes de alimentación de seguridad proporcionan detección de sobretensión como parte del bucle de seguridad. Dado que la fiabilidad de cada fuente de alimentación (es decir, su frecuencia de fallos peligrosos) es más de 100 veces mejor que el umbral de la norma SIL3, estas fuentes de alimentación de seguridad no se incluyen en los cálculos de nivel de integridad de seguridad para el bucle de seguridad.

El bucle de seguridad también incluye el equipo que no es de seguridad siguiente:

- Los sensores y los actuadores, así como el cableado que los conectan a módulos de E/S de seguridad. Las E/S de seguridad realizan diagnósticos de cableado para sensores y actuadores a fin de ayudar a gestionar el bucle de seguridad.

**NOTA:** Cuando diseña su aplicación de seguridad, debe identificar las características del sensor y del actuador (en especial valores de PFD/PFH).

# Normas de certificación

## Contenido de este capítulo

Certificaciones.....	21
Normas y certificaciones .....	25

## Introducción

En este capítulo se describen las normas de certificación que se aplican al sistema de seguridad M580 y sus módulos de componentes.

## Certificaciones

### Normas de certificación del PAC de seguridad M580

El PAC de seguridad M580 está certificado por TÜV Rheinland Group para su uso en aplicaciones de hasta:

- SIL3/IEC 61508/IEC 61511
- SIL4 / EN 50126 (IEC 62278), EN 50128 (IEC 62279), EN 50129 (IEC 62245)
- SIL CL3/IEC 62061
- PLe, Cat. 4/ISO 13849-1

Para obtener información más detallada sobre la clasificación SIL, consulte Descripción de la clasificación SIL, página 401.

### Especificaciones del controlador programable

- IEC 61131-2 Controladores programables. Parte 2: Requisitos y ensayos de los equipos.
- IEC/EN 61010-2-201, UL 61010-2-201, CSA-C22.2 N.º 61010-2-201: Requisitos de seguridad para equipos eléctricos. Parte 2-201: Requisitos específicos para el equipo de control.

### Especificaciones medioambientales

Consulte Normas y certificaciones de M580, página 25 para conocer los niveles de las pruebas de entorno.

### Especificaciones de áreas Ex

**Para EE. UU. y Canadá: Ubicación peligrosa clase I, división 2, grupos A, B, C y D**

- CSA 22.2 N.º 213, ANSI/ISA12.12.01 y FM3611

**Para otros países: CE ATEX (directiva 2014/34/UE) o IECEx en zonas con atmósferas definidas como zona 2 (gas) o zona 22 (polvo)**

- IEC/EN 60079-0; IEC/EN 60079-7; IEC/EN 60079-15

## Especificaciones para sistemas de automatización de compañía eléctrica

- IEC/EN 61000-6-5 Compatibilidad electromagnética. Parte 6-5: Estándares genéricos: inmunidad para los entornos de centrales eléctricas y subestaciones.
- IEC/EN 61850-3 Redes y sistemas de comunicación para la automatización de las compañías eléctricas. Parte 3: Requisitos generales

Consulte M580 Normas y certificaciones, página 25 para ver las restricciones de instalación.

## Especificaciones ferroviarias

- EN 50126/IEC 62278: Aplicaciones ferroviarias: especificación y demostración de fiabilidad, disponibilidad, mantenimiento y seguridad (RAMS).
- EN 50128/IEC 62279: Aplicaciones ferroviarias - Sistemas de comunicación, señalización y procesamiento - Software para sistemas de control y protección ferroviarios.
- EN 50129/IEC 62245: Aplicaciones ferroviarias - Sistemas de comunicación, señalización y procesamiento - Sistemas electrónicos relacionados con la seguridad para la señalización.
- EN 50155/IEC 60571: Aplicaciones ferroviarias. Material rodante. Equipos electrónicos.
- EN 50121-3-2/IEC 62236-3-2: Aplicaciones ferroviarias. Compatibilidad electromagnética. Parte 3-2: Material rodante - Aparatos.
- EN 50121-4/IEC 62236-4: Aplicaciones ferroviarias. Compatibilidad electromagnética. Parte 4: Emisión e inmunidad de los aparatos de señalización y telecomunicaciones.
- EN 50121-5/IEC 62236-5: Aplicaciones ferroviarias. Compatibilidad electromagnética. Parte 5: Emisión e inmunidad de instalaciones y aparatos fijos de suministro de energía.
- EN 50125-1: Ferrocarril - Condiciones ambientales del equipo - Parte 1: Material rodante y equipo incorporado.
- EN 50125-3: Ferrocarril - Condiciones ambientales del equipo - Parte 3: Equipos de señalización y telecomunicaciones.
- EN 50124-1: Ferrocarril - Coordinación de aislamiento - Parte 1: Requisitos básicos: distancias de aislamiento y fuga para todos los equipos eléctricos y electrónicos.

Consulte M580 Normas y certificaciones, página 25 para ver las restricciones de instalación.

## Especificaciones de seguridad funcional

- IEC/EN 61000-6-7 Compatibilidad electromagnética. Parte 6-7: Normas genéricas - Requisitos de inmunidad para equipos diseñados para realizar funciones en un sistema relacionado con la seguridad (seguridad funcional) en ubicaciones industriales.
- IEC 61326-3-1: Equipos eléctricos para medida, control y uso en laboratorio. Parte 3-1: Requisitos de inmunidad para sistemas relacionados con la seguridad y para equipos destinados a realizar funciones relacionadas con la seguridad - Aplicación industrial general.
- IEC 61508: Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad - Parte 1-7, edición 2.0.
- IEC 61511-1: Seguridad funcional - Sistemas instrumentados de seguridad para el sector de la industria de procesos - Parte 1: Programación, definiciones, requisitos de sistema, hardware y software.
- IEC 61511-2: Seguridad funcional - Sistemas instrumentados de seguridad para el sector de la industria de procesos - Parte 2: Directrices para la aplicación de la norma IEC 61511-1.
- IEC 61511-3: Seguridad funcional - Sistemas instrumentados de seguridad para el sector de la industria de procesos - Parte 3: Guía para determinar los niveles de integridad de seguridad requeridos.

## Especificaciones de máquinas de seguridad

- IEC/EN 62061 Seguridad de la maquinaria: seguridad funcional de los sistemas de control eléctricos, electrónicos y electrónicos programables de seguridad
- ISO EN 13849-1: Seguridad de las máquinas - Piezas de los sistemas de control relacionadas con la seguridad - Parte 1: Principios generales del diseño.

## Especificaciones de seguridad funcional en sistemas

- EN 54-2: Sistemas de detección de incendios y de alarma contra incendios Parte 2: Control e indicación del equipo.
- EN 50156-1: Equipos eléctricos para hornos y equipos auxiliares - Parte 1: Requisitos para el diseño y la instalación de la aplicación.
- EN 50130-4: Sistemas de alarma - Parte 4: Compatibilidad electromagnética. Familia de productos: Requisitos de inmunidad para componentes de sistemas de detección de incendios, intrusión, atraco, CCTV, control de accesos y alarmas sociales.
- EN 298: Sistemas automáticos de control de quemadores para quemadores y aparatos que queman combustibles gaseosos o líquidos.

- NFPA 85: Código de riesgos de sistemas de combustión y calderas.
- NFPA 86: Estándar para hornos y hornos.
- NFPA 72: National Fire Alarm and Signaling Code (Código nacional de señalización y alarma de incendios).

## Nota:

Para ver una lista completa de las normas (con sus revisiones y fechas) certificadas por TÜV, consulte el certificado de TÜV en el sitio web:

[www.certipedia.com](http://www.certipedia.com) o [www.fs-products.com](http://www.fs-products.com).

# Normas y certificaciones

## Descargar

Haga clic en el enlace correspondiente al idioma que prefiera para descargar las normas y las certificaciones (formato PDF) aplicables a los módulos de esta línea de productos:

Título	Idiomas
Plataformas Modicon M580, M340 y X80 I/O, Normas y certificaciones	<ul style="list-style-type: none"><li data-bbox="659 431 924 456">• Inglés: EIO0000002726</li><li data-bbox="659 464 942 488">• Francés: EIO0000002727</li><li data-bbox="659 496 938 521">• Alemán: EIO0000002728</li><li data-bbox="659 529 934 553">• Italiano: EIO0000002730</li><li data-bbox="659 561 942 586">• Español: EIO0000002729</li><li data-bbox="659 594 919 618">• Chino: EIO0000002731</li></ul>

# Módulos compatibles con el sistema de seguridad M580

## Contenido de este capítulo

Módulos certificados del sistema de seguridad M580.....	27
Módulos no interferentes .....	29

## Introducción

Un proyecto de seguridad de M580 puede incluir módulos de seguridad y módulos que no sean de seguridad. Se pueden utilizar:

- Módulos de seguridad en la tarea SAFE.
- Módulos que no sean de seguridad sólo para las tareas no seguras (MAST, FAST, AUX0 y AUX1).

**NOTA:** Sólo se pueden añadir a un proyecto de seguridad módulos que no son de seguridad que no interfieran con la función de seguridad.

Utilice sólo el software de programación Control Expert de Schneider Electric para la programación, la puesta en servicio y el funcionamiento de su aplicación de seguridad M580.

- Control Expert L Safety proporciona todas las funciones de Control Expert L y se puede usar con las CPU de seguridad BMEP582040S y BMEH582040S.
- Control Expert XL Safety proporciona todas las funciones de Control Expert XL y se puede utilizar para toda la gama de CPU de seguridad BMEP58•040S y BMEH58•040S.

En este capítulo se ofrece una lista de los módulos de seguridad y los que no son de seguridad compatibles con el sistema de seguridad M580.

# Módulos certificados del sistema de seguridad M580

## Módulos certificados

El PAC de M580seguridad es un sistema relacionado con la seguridad certificado por TÜV Rheinland Group, de acuerdo con:

- SIL3 / IEC 61508 / IEC 61511
- SIL4 / EN 50126 (IEC 62278), EN 50128 (IEC 62279), EN 50129 (IEC 62245)
- SIL CL3 / IEC 62061
- PLe, Cat. 4 / ISO 13849-1
- CIP Safety IEC 61784-3

Se basa en la familia M580 de controladores de automatización programables (PAC, por sus siglas en inglés). Los siguientes módulos de seguridad M580 de Schneider Electric están certificados:

- CPU BMEP582040S autónoma
- CPU BMEP584040S autónoma
- BMEP586040S CPU independiente
- CPU BMEH582040S Hot Standby
- CPU BMEH584040S Hot Standby
- CPU BMEH586040S Hot Standby
- Coprocesador BMEP58CPROS3
- Módulo de entrada analógica BMXSAI0410
- Módulo de entrada digital BMXSDI1602
- Módulo de salida digital BMXSDO0802
- Módulo de salida de relé digital BMXSRA0405
- Fuente de alimentación BMXCPS4002S
- Fuente de alimentación BMXCPS4022S
- Fuente de alimentación BMXCPS3522S

**NOTA:** Además de los módulos de seguridad de la lista anterior, también pueden incluir en su proyecto de seguridad módulos no interferentes que no sean de seguridad, página 29.

**NOTA:** La oferta de seguridad de Modicon es de hasta SIL3 (reg. IEC 61508) y PLe (reg. con capacidad ISO 13849), lo que significa que también es compatible con SIL1/ SIL2 y PLa, b,c,d.

**NOTA:**

- Cada vez que en el documento se menciona SIL2 o SIL3 sin una referencia estándar esto se refiere a IEC 61508 / IEC 61511.
- Cada vez que se menciona SIL2, también se refiere a SIL3 en relación con EN 50126 / EN 50128 / EN 50129.
- Cada vez que se menciona SIL3, también se refiere a SIL4 en relación con EN 50126 / EN 50128 / EN 50129.

La información más reciente acerca de las versiones de productos certificados está disponible en el sitio web de TÜV Rheinland Group: [www.certipedia.com](http://www.certipedia.com) o [www.fs-products.com](http://www.fs-products.com).

## Reemplazo de una CPU

Se puede reemplazar una CPU BME•58•040S por otra BME•58•040S. Sin embargo, la sustitución no funciona si se sobrepasan las limitaciones siguientes:

- Número de E/S
- Número de estaciones de E/S
- Número de variables
- Tamaño de memoria de aplicación

Consulte los temas:

- *de configuraciónCompatibilidad de configuración en Modicon M580 Hot Standby System Planning Guide for Frequently Used Architectures* (Guía de planificación del sistema Modicon M580 Hot Standby para arquitecturasControl ExpertControl Expertcompatibles con las CPU de seguridad y Hot Standby).
- *CharacteristicsM580 CPU & Copro Performance Characteristics in the Modicon M580 Safety System Planning Guide* (Guía de planificación del sistema de seguridad Modicon M580) para obtener una descripción de las limitaciones de la CPU.

## Módulos no interferentes

### Introducción

Un proyecto de seguridad de M580 puede incluir módulos de seguridad y módulos que no sean de seguridad. Sólo puede utilizar módulos que no son de seguridad para tareas no seguras. Sólo se pueden añadir a un proyecto de seguridad módulos que no son de seguridad que no interfieran con la función de seguridad.

### Definición de un módulo no interferente

#### **⚠ ATENCIÓN**

##### **USO INCORRECTO DE DATOS RELACIONADOS CON LA SEGURIDAD**

Confirme que ni los datos de entrada ni los datos de salida de módulos no interferentes se utilizan para controlar salidas relacionadas con la seguridad. Los módulos que no son de seguridad sólo pueden procesar datos que no son de seguridad.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

Un módulo no interferente es un módulo que no puede interferir con la función de seguridad. En el caso de los módulos M580 en bastidor (BME<sub>x</sub>, BMX<sub>x</sub>, PMX<sub>x</sub> y PME<sub>x</sub>), hay dos tipos de módulos no interferentes:

- Tipo 1: Se puede instalar un módulo de tipo 1 en el mismo bastidor que los módulos de seguridad (siempre que se coloque el módulo de seguridad, en el bastidor principal o de extensión).
- Tipo 2: No se puede instalar un módulo no interferente de tipo 2 en el mismo bastidor principal que los módulos de seguridad (siempre que se coloque el módulo de seguridad, en el bastidor principal o de ampliación).

**NOTA:** Los módulos de tipo 1 y tipo 2 se enumeran en el sitio web de TÜV Rheinland en [www.certipedia.com](http://www.certipedia.com).

En el caso de los módulos Mx80 que no están en bastidor, todos los equipos de Ethernet (DIO o DRS) se pueden considerar no interferentes y, por tanto, se pueden utilizar como parte de un sistema de seguridad de M580.

## Módulos no interferentes de tipo 1 para aplicaciones SIL3

Los siguientes módulos que no son de seguridad pueden calificarse como módulos no interferentes de tipo 1 en un sistema de seguridad M580.

**NOTA:** La lista de módulos que no son de seguridad no interferentes de tipo 1 puede cambiar de vez en cuando. Para obtener la lista actual, visite el sitio web de TÜV Rheinland en [www.certipedia.com](http://www.certipedia.com).

Tipo de módulo	Referencia del módulo
4 slots en la placa de conexiones	BMEXBP0400
8 slots en la placa de conexiones	BMEXBP0800
12 slots en la placa de conexiones	BMEXBP1200
4 slots en la placa de conexiones	BMXXBP0400
6 slots en la placa de conexiones	BMXXBP0600
8 slots en la placa de conexiones	BMXXBP0800
12 slots en la placa de conexiones	BMXXBP1200
6 slots en la placa de conexiones con slots duales para las fuentes de alimentación redundantes	BMEXBP0602
10 slots en la placa de conexiones con slots duales para las fuentes de alimentación redundante	BMEXBP1002
Comunicación: Adaptador de estación Ethernet X80 de alto rendimiento 1 canal	BMXCRA31210
Comunicación: Adaptador de estación Ethernet X80 de alto rendimiento 1 canal	BMECRA31210
Comunicación: Módulo Ethernet con servicios web estándar	BMENOC0301
Comunicación: Módulo Ethernet con reenvío de IP	BMENOC0321
Comunicación: Módulo Ethernet con servicios web FactoryCast	BMENOC0311
Comunicación: Módulo de extensión del bastidor.	BMXXBE1000
Comunicación: Interfaz AS	BMXEIA0100
Comunicación: Datos globales	BMXNGD0100
Comunicación: Convertidor de fibra MM/LC de 2 canales y 100 Mb	BMXNRP0200
Comunicación: Convertidor de fibra SM/LC de 2 canales y 100 Mb	BMXNRP0201
Comunicación: Módulo de comunicaciones M580 IEC 61850	BMENOP0300
Comunicación: Servidor OPC UA integrado	BMENUA0100
En conteo: Módulo SSI de 3 canales	BMXEAE0300

Tipo de módulo	Referencia del módulo
En conteo: Contador de alta velocidad de 2 canales	BMXEHC0200
En conteo: Contador de alta velocidad de 8 canales	BMXEHC0800
Movimiento: Salida de tren de pulsos 2 independiente CH	BMXMSP0200
Analógica: HART con 8 entradas de corriente analógicas aisladas	BMEAHI0812
Analógica: HART con 4 salidas de corriente analógicas aisladas	BMEAHO0412
Analógica: 4 entradas analógicas U/I con separación de potencial de alta velocidad	BMXAMI0410
Analógica: 4 entradas analógicas U/I no aisladas de alta velocidad	BMXAMI0800
Analógica: 8 entradas analógicas U/I con separación de potencial de alta velocidad	BMXAMI0810
Analógica: 4 entradas analógicas U/I 4 salidas U/I	BMXAMM0600
Analógica: 2 salidas analógicas U/I aisladas	BMXAMO0210
Analógica: 4 salidas analógicas U/I aisladas	BMXAMO0410
Analógica: 8 salidas de corriente analógicas no aisladas	BMXAMO0802
Analógica: 4 entradas analógicas TC/RTD aisladas	BMXART0414.2
Analógica: 8 entradas analógicas TC/RTD aisladas	BMXART0814.2
Binario: 8 entradas digitales de 220 V CA	BMXDAI0805
Binario: 8 entradas digitales de 100 a 120 V CA aisladas	BMXDAI0814
Binario: Común positivo de 16 entradas digitales de 24 V CA/24 V CC	BMXDAI1602
Binario: 16 entradas digitales de 48 V CA	BMXDAI1603
Binario: 16 entradas digitales de 100 a 120 V CA, 20 pines	BMXDAI1604
Binario: 16 canales de entradas digitales supervisadas de 100 a 120 VCA 40 pines	BMXDAI1614
Binario: 16 canales de entradas digitales supervisadas de 200 a 240 VCA 40 pines	BMXDAI1615
Binario: 16 salidas digitales de Triacs de 100 a 240 V CA 20 pines	BMXDAO1605
Binario: 16 salidas digitales de Triacs de 24 a 240 V CA 40 pins	BMXDAO1615
Binario: Común positivo de 16 entradas digitales de 24 V CC	BMXDDI1602
Binario: Común positivo de 16 entradas digitales de 48 V CC	BMXDDI1603
Binario: Común positivo de 16 entradas digitales de 125 V CC	BMXDDI1604T
Binario: Común positivo de 32 entradas digitales de 24 V CC	BMXDDI3202K
Binario: Común positivo de 64 entradas digitales de 24 V CC	BMXDDI6402K
Binario: Triacs común negativo 8 ent. dig. 24 V CC 8Q	BMXDMM16022

Tipo de módulo	Referencia del módulo
Binario: Relés de 8 entradas digitales de 24 V CC y 8 salidas	BMXDDM16025
Binario: Triacs común negativo 16 ent. dig. 24 V CC 16 Q	BMXDDM3202K
Binario: Origen trans. dig. 16Q 0,5 A	BMXDDO1602
Binario: Común positivo trans. dig. 16 O	BMXDDO1612
Binario: 32 salidas digitales transistor común negativo	BMXDDO3202K
Binario: 64 salidas digitales transistor común negativo	BMXDDO6402K
Binario: 8 salidas digitales de 125 V CC	BMXDRA0804T
Binario: Relés aislados 8Q digitales de 24 V CC o de 24 a 240 V CA	BMXDRA0805
Binario: 16 canales de salidas de relé no aisladas digitales de 5 a 125 V CC o de 25 a 240 V CA	BMXDRA0815
Binario: Relés de 16 salidas digitales	BMXDRA1605
Binario: Salida NC digital 5 a 125 V CC o relés 24 a 240 V CA	BMXDRC0805
Binario: 16 entradas digitales 24/125 V CC TSTAMP	BMXERT1604
Conmutador de opciones de red Mx80	BMENOS0300
Entrada de frecuencia de turbomaquinaria 2 canales	BMXETM0200
Soporte para módulo maestro Profibus DP/DPV1	PMEPXM0100
Módulo RTU avanzado Mx80	BMENOR2200H

## Módulos no interferentes de tipo 2 para aplicaciones SIL2/3

Los siguientes módulos en bastidor que no son de seguridad se pueden considerar módulos no interferentes de tipo 2 en un sistema de seguridad M580.

**NOTA:** La lista de módulos que no son de seguridad no interferentes de tipo 2 puede cambiar de vez en cuando. Para obtener la lista actual, visite el sitio web de TÜV Rheinland en [www.certipedia.com](http://www.certipedia.com).

Tipo de módulo	Referencia del módulo
Comunicación: Adaptador de estación Ethernet X80 estándar de 1 canal	BMXCRA31200
Fuente de alimentación de CA estándar	BMXCPS2000
Fuente de alimentación de CC estándar aislada	BMXCPS2010

Tipo de módulo	Referencia del módulo
Fuente de alimentación de alta potencia aislada de 24 a 48 V CC	BMXCPS3020
Fuente de alimentación de 125 V CC redundante estándar	BMXCPS3522
Fuente de alimentación de 24/48 V CC redundante estándar	BMXCPS4022
Fuente de alimentación de CA redundante estándar	BMXCPS4002
Fuente de alimentación de CA de alta potencia	BMXCPS3500
Fuente de alimentación de CC de alta potencia	BMXCPS3540T
Comunicación: Puerto RS485/232 del módulo de bus 2	BMXNOM0200
Binario: Común positivo o común negativo de 32 entradas digitales de 12/24 V CC	BMXDDI3232
Binario: Común positivo de 32 entradas digitales de 48 V CC	BMXDDI3203
Maestro CANopen X80	BMECXM0100
Módulo de peso	PMESWT0100
Módulo de diagnóstico del participante	PMXCDA0400
Módulo de comunicación universal Ethernet TCP Open	PMEUCM0302

**NOTA:** Todos los equipos autorizados de un sistema M580 que están vinculados a módulos de seguridad por medio de Ethernet se consideran no interferentes. En consecuencia, todos los módulos de rangos Quantum y STB Advantys (no se pueden conectar en el mismo bastidor que los módulos de seguridad M580) son módulos no interferentes de tipo 2.

# Ciberseguridad para el sistema de seguridad M580

## Contenido de este capítulo

Ciberseguridad para el sistema de seguridad M580.....	34
---	----

## Introducción

En este capítulo se hace referencia a materiales disponibles para desarrollar un enfoque relativo a la ciberseguridad para el PAC de seguridad M580.

# Ciberseguridad para el sistema de seguridad M580

## Referencia de ciberseguridad

El propósito de una política de ciberseguridad es reducir, en la medida de lo posible, la vulnerabilidad del sistema de seguridad frente a los ciberataques. Para obtener más información sobre el desarrollo de una política de ciberseguridad para el sistema de seguridadM580, consulte el *manual de referencia de ciberseguridad de la plataforma de controladores de Modicon* (número de referencia EIO0000001999 (EN)).

# Ciclo de vida de la aplicación

## Contenido de este capítulo

Ciclo de vida de la aplicación .....35

## Introducción

# Ciclo de vida de la aplicación

## Introducción

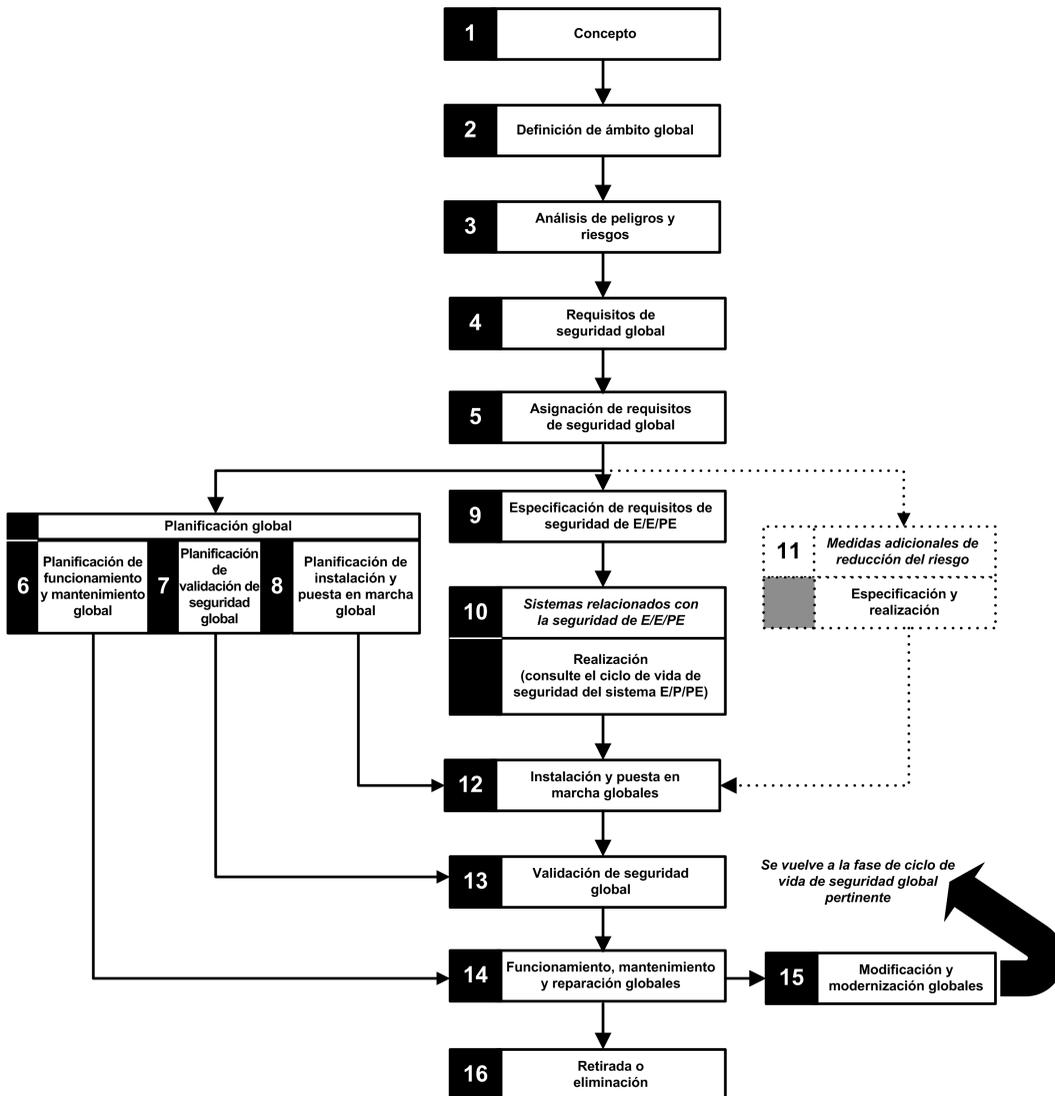
Al diseñar una aplicación segura, deberá seguir la recomendación de una de las normas de seguridad que se aplica al dominio de la aplicación. La mayoría de las normas de aplicación se derivan de o están vinculadas a la norma genérica IEC 61508, incluyendo, por ejemplo, la norma de la industria de procesos (IEC 61511), las normas de la industria de máquinas (IEC 62061 e ISO 13489), la norma de la industria nuclear (IEC 61513), las normas ferroviarias (EN 5012x), etc.

IEC 61508 define el ciclo de vida de una aplicación con una secuencia de pasos. Cada paso tiene un rol definido, necesita documentos de entrada obligatorios y produce documentos de salida. La decisión de utilizar un sistema integridad de seguridad (SIS) se realiza al final del paso Asignación de requisitos de seguridad (paso 5).

En este tema se definen las comprobaciones necesarias, relacionadas con el uso de un sistema de seguridad de M580, que debe realizar en los pasos siguientes:

9.	Especificación de requisitos de seguridad del sistema E/E/PE
10.	Realización de sistemas relacionados con la seguridad E/E/PE
12.	Instalación y puesta en marcha globales
13.	Validación de seguridad global
14.	Funcionamiento, mantenimiento y reparación globales
15.	Modificación y modernización globales

En el diagrama siguiente se muestra el ciclo de vida de seguridad global:



## Paso 9: Especificación de requisitos de seguridad del sistema E/E/PE

Este paso se realiza una vez que el análisis de riesgos ha finalizado y ha proporcionado, entre otras cosas, la información siguiente:

- Definición de funciones integradas de seguridad
- Sus rendimientos necesarios (tiempo, reducción del riesgo, SIL...)
- Sus modalidades de fallo

Debe generar las especificaciones de requisitos de seguridad entre las que se incluyen, al menos, la información siguiente para diseñar una aplicación segura utilizando cualquier tipo de PAC de seguridad:

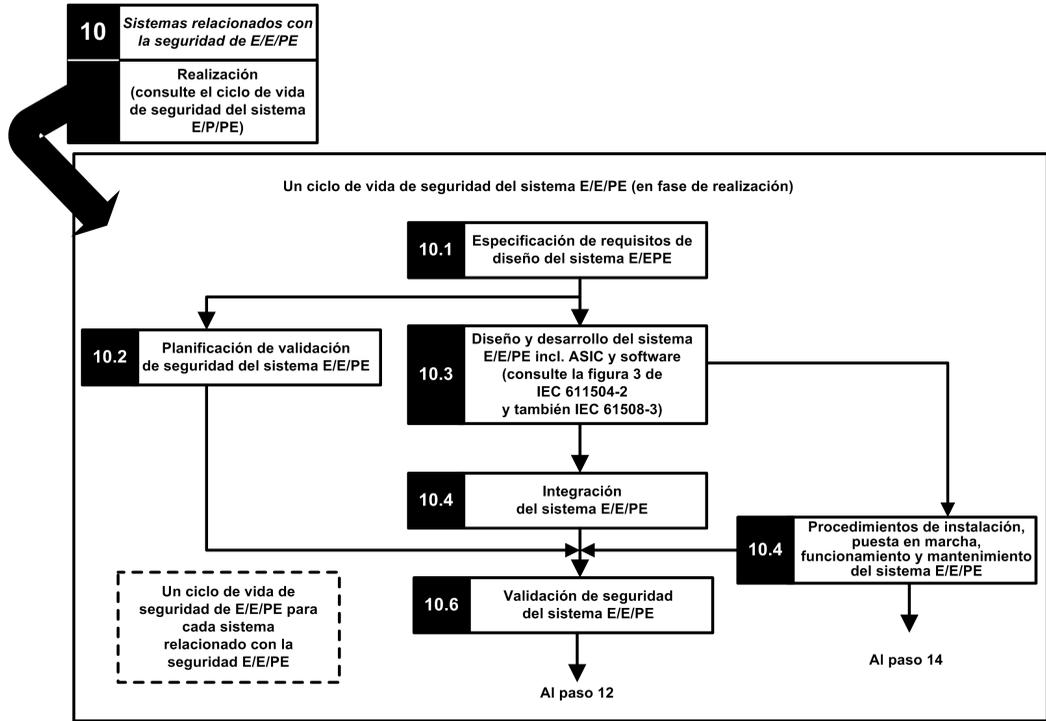
- Estado de seguridad de las funciones integradas de seguridad
- Análisis de la modalidad de funcionamiento de SIS (incluido el comportamiento durante la ejecución, detención, secuencia de encendido, mantenimiento, reparación, etc.)
- Intervalo de prueba del SIF
- MTTR del SIS
- Opción de SIF energizado o deenergizado
- Rendimiento del dispositivo de resolución lógica (tiempo de reacción, precisión, etc.)
- Requisitos de rendimiento
  - Tolerancia de errores
  - Integridad
  - Tasa máxima de falsos disparos
  - Tasa máxima de fallos peligrosos
- Especificación ambiental (CEM, mecánica, química, climática, etc.)

## Paso 10: Realización de sistemas relacionados con la seguridad E/E/PE

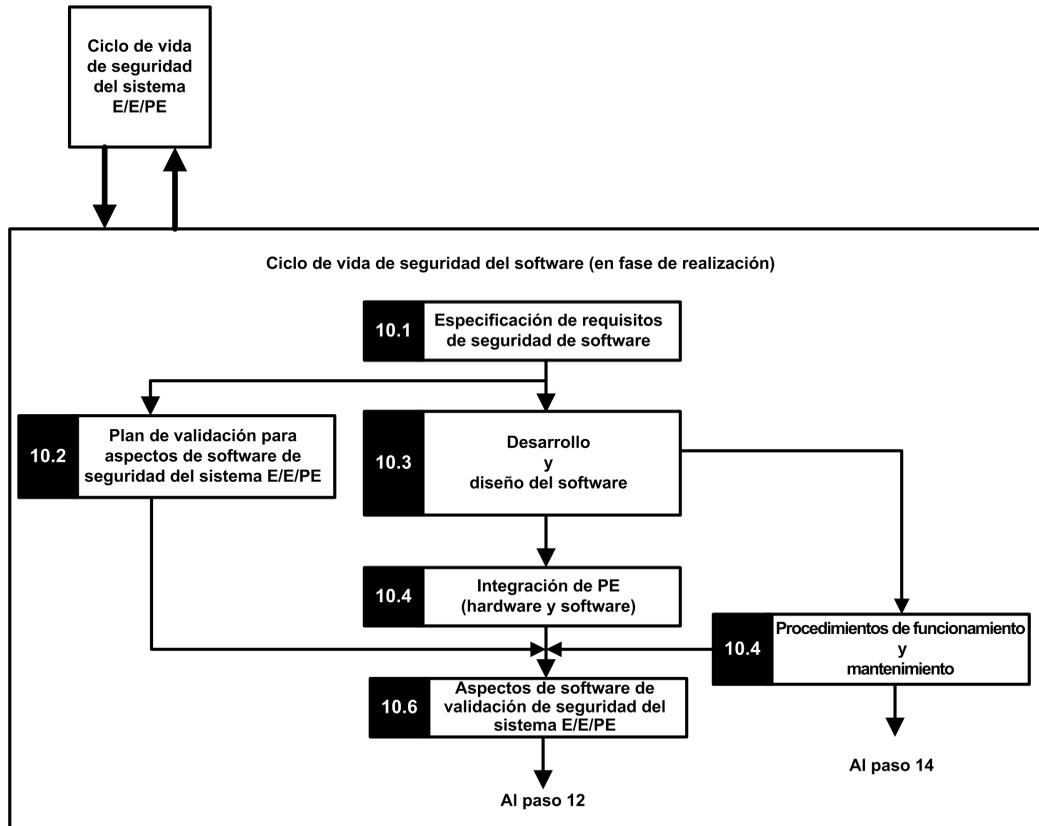
La norma IEC 61508 divide este paso en 2 ciclos de vida secundarios, uno para la realización del sistema y otro para la realización del software.

Realización del sistema:

Del paso 10



Realización del software:



El objetivo de los primeros pasos secundarios (10.1) es convertir los requisitos de seguridad del SIS en las especificaciones del diseño de hardware, de las pruebas de hardware, del diseño de software, de las pruebas de software y de las pruebas de integración. Debe proporcionar al menos la información siguiente necesaria para diseñar una aplicación segura mediante M580 de seguridad:

- Arquitectura de hardware responsable de lo siguiente:
  - El cumplimiento de las reglas de M580 relativas a la combinación de los módulos que no son de seguridad y de seguridad: todos los módulos de seguridad (módulos de E/S seguros y CPU/coprocesador seguros) se colocan en bastidores, en los que el bastidor principal y su extensión se alimentan con una fuente de alimentación segura y contiene sólo módulos seguros o módulos no interferentes del tipo 1.
  - Consumo eléctrico por bastidor.
  - Reglas de reducción.

- Arquitectura de fuente de alimentación:
  - Sólo fuente de alimentación SELV/PELV.
- Arquitectura del software:
  - Incluido el uso de variables globales de M580, una variable global no debe impedir que se active una acción de seguridad a menos que se utilice un "protocolo de aplicación segura".
- Integración de hardware (cableado, armario, etc.).
  - Protección de fusible.
  - Accesorios para diagnóstico de cables.
- Interfaces hombre-máquina
  - Incluido el uso de variables globales de M580, una variable global no debe impedir que se active una acción de seguridad a menos que se utilice un "protocolo de aplicación segura".
- Interfaces eléctricas/numéricas:
  - Estado de seguridad.
  - Sensor y actuador.
- Algoritmo
- Rendimientos, entre los que se incluye la definición de período de tarea, watchdog y timeout, y predicción de un buen comportamiento con la fórmula:

$$\sum_{\text{todas las tareas}} \frac{Ejec.tarea}{Periodo_{tarea}} < 80 \%$$

**NOTA:** Esta fórmula solo se aplica cuando la tarea MAST no está en modalidad cíclica.

- Comportamiento en caso de:
  - Desbloqueo de la configuración
  - Modalidad de mantenimiento
  - Entrada de mantenimiento
  - Canal no válido
  - Fallo de escritura
  - Estado del canal
  - Estado del módulo
- Gestión del UID de los módulos de E/S seguros (definir cuándo se debe cambiar un UID).

- Servidor NTP:
  - Opción del PAC como servidor NTP o servidor NTP externo (en función del uso de marcas de tiempo de E/S en la aplicación del proceso).
  - Redundancia de servidores
  - Pérdida de servidores

Los siguientes pasos secundarios refinan las especificaciones para obtener especificaciones técnicas detalladas, realizan el propio diseño, ejecutan todos los planes de prueba y ofrecen informes.

## Paso 12: Instalación y puesta en marcha globales

El objetivo de este paso es definir los requisitos de instalación, planificación de tareas, procedimiento de puesta en marcha y luego crear el sistema y verificar que esté correcto.

- Para las aplicaciones Hot Standby, verificar que el **timeout de recuperación**, página 160 de los módulos de salida de seguridad encaje con las condiciones definidas para las operaciones de **intercambio**, página 162 y **conmutación**, página 163 y verificar el tiempo de pausa de CRA.
- Verificar que el **timeout de seguridad de recuperación (S\_TO)** para los módulos de salida de seguridad sea, como mínimo, superior a 40 ms o ( $2,5 * T_{SAFE}$ ) (el que sea más grande de los dos), en el que  $T_{SAFE}$  es igual al periodo de tarea SAFE configurado.
- Borre cualquier aplicación existente en el interior del PLC, o utilice una aplicación configurada sin ningún dispositivo CIP Safety antes de instalar el dispositivo de seguridad en una red de seguridad Ethernet (con dispositivos CIP Safety).

En un sistema de seguridad M580, el procedimiento de puesta en marcha debe incluir los puntos siguientes:

- Verificar la integridad de Control Expert, verificar la versión de Control Expert.
- Comprobar corrección de las versiones de firmware de CPU y coprocesador supervisando las palabras de sistema %SW14 (versión del firmware del procesador del PLC) y %SW142 (versión del firmware de coprocesador).
- Comprobar corrección de cada dirección de módulo (posición en el bastidor, conmutadores de CRA).
- Comprobar corrección del cableado:
  - Verificación de punto a punto: de variable interna a módulo de E/S y a actuador/sensor.
  - Fusibles.
  - Equipos para el diagnóstico del cableado.
- Al final del procedimiento, todos los módulos de seguridad están en modalidad de "bloqueo" (se recomienda que la misma aplicación segura compruebe esta condición).

- Comprobar corrección de cada configuración de módulo (incluidos los timeouts).
  - Leer la configuración mediante la pantalla de Control Expert y comparar con la especificación.
- Todas las aplicaciones de seguridad se han regenerado mediante la opción **Regenerar todo el proyecto** y, luego, se han descargado en cada PLC; además, se ha guardado su SAId, así como el archivo de aplicación.
- El periodo de tarea y el watchdog de tarea son correctos.
- Referencias y versión del módulo.
- Uso de SELV/PELV sólo.
- Si se utilizan dispositivos CIP Safety en la aplicación de seguridad:
  - Puede considerarse que la firma de ID de configuración de seguridad (SCID) se ha verificado (opción habilitada en el DTM de CIP Safety de Control Expert) y la configuración de destino se ha bloqueado tras las pruebas del usuario.
  - Para confirmar que la configuración del origen creada por el usuario con la herramienta de software Control Expert se ha enviado correctamente y guardado en el origen CIP Safety M580, compare visualmente todos los valores de parámetros de la configuración del destino CIP Safety que se muestran en los DDDT de destino (en modalidad conectada con el PAC, mediante una tabla de animación) con los valores de parámetros mostrados y configurados en la *ficha Verificación de configuración*, página 369 del DTM de destino. Todos los valores deben ser idénticos.
  - Pruebe todas las configuraciones de conexión de seguridad una vez que se hayan aplicado en el origen CIP Safety M580 para confirmar que cada conexión de destino funciona de la manera prevista.
  - Antes de instalar los dispositivos CIP Safety en la red de seguridad, ponga en marcha todos los dispositivos de seguridad con ID de MAC y Velocidad de transmisión, según sea necesario.
- Las pruebas de usuario son el método con el que se validan las descargas de aplicaciones.

## Paso 13: Validación de seguridad global

El objetivo de este paso es demostrar que el sistema integrado de seguridad cumple sus requisitos. Ejecuta todas las pruebas y genera los informes definidos en el paso 7 del "ciclo de vida de seguridad". Debe incluir lo siguiente:

- Verificar que no exista ninguna condición de desborde durante cualquier estado del sistema (verificación del bit del sistema %S19 en las tareas MAST, FAST, AUX0) y que el tiempo máximo y actual de ejecución de la tarea SAFE (%SW42 y %SW43) se encuentre por debajo del período de la tarea SAFE.

$$\sum_{\text{todas las tareas}} \frac{\text{Ejec. tarea}}{\text{Periodo}_{\text{tarea}}} < 80 \%$$

- Compruebe la fórmula de carga de la CPU:  
**NOTA:** Puede utilizar las palabras de sistema %SW110 a %SW115, página 408 para realizar una evaluación en tiempo real del promedio de carga de las tareas de la CPU (si todas las tareas son periódicas, %SW116 debería ser inferior a 80).
- Verificar las modalidades de funcionamiento especiales (desbloqueo de módulo, entrada de mantenimiento, canal no válido, defecto de cableado).
- En el caso de las aplicaciones Hot Standby, verificar que todas las tareas estén correctamente sincronizadas a través del enlace de Hot Standby comprobando y utilizando los bits de MAST\_SYNCHRONIZED, FAST\_SYNCHRONIZED y SAFE\_SYNCHRONIZED en T\_M\_ECPU\_HSBY DDT. Consulte *Modicon M580 Hot Standby, Guía de planificación del sistema para arquitecturas utilizadas con más frecuencia* para obtener una descripción del DDT T\_M\_ECPU\_HSBY DDT.

## Paso 14: Funcionamiento, mantenimiento y reparación globales

- Ejecute las pruebas en el periodo correcto.
- Supervise el SAId consulte la nota.  
**NOTA:** Mientras no cambie el SAId, tampoco cambiará la parte de seguridad de la aplicación. Consulte el bloque de funciones S\_SYST\_STAT\_MX para obtener información detallada sobre el comportamiento del SAId.
- Supervise el estado de bloqueo de configuración de cada módulo de seguridad.
- Registre las operaciones de reparación.
- Si se sustituye un módulo, el dispositivo sustitutorio deberá configurarse debidamente y el usuario deberá verificar su funcionamiento. Ejecute las operaciones (mínimas) de puesta en marcha relacionadas con este módulo.
- Registre las desviaciones.

## Paso 15: Modificación y modernización globales

Toda modificación debe tratarse como un nuevo diseño. Un análisis del impacto puede ser útil para definir la parte del sistema de seguridad anterior que se puede conservar y la parte que se debe volver a diseñar.

**NOTA:** Si la modificación de una aplicación no afecta a la aplicación SAFE, puede utilizar la opción de firma de origen SAFE para verificar que no se haya introducido ninguna modificación no deseada en el código SAFE. La opción de firma de origen SAFE consiste en una verificación *a priori* de que la aplicación no ha sufrido cambios. La firma de origen SAFE no sustituye al SAId, la única medida que permite confirmar de manera fiable que un PAC está ejecutando la misma aplicación SAFE que la validada.

# Módulos de E/S de seguridad M580

## Contenido de este capítulo

Características compartidas del módulo de E/S de seguridad M580 .....	46
Módulo de entrada analógica BMXSAI0410 .....	51
Módulo de entrada digital BMXSDI1602 .....	65
Módulo de salida digital BMXSDO0802 .....	99
Módulo de salida de relé digital BMXSRA0405.....	115

## Introducción

En este capítulo se describen los módulos de E/S de seguridad M580.

# Características compartidas del módulo de E/S de seguridad M580

## Introducción

En esta sección se describen las características compartidas o comunes de los módulos de E/S de seguridad M580.

## Presentamos los módulos de E/S de M580seguridad

### Introducción

Los siguientes cuatro módulos de E/S de seguridad M580 están certificados para utilizarse en aplicaciones de seguridad:

- BMXSAI0410 (Entrada analógica)
- BMXSDI1602 (Entrada digital)
- BMXSDO0802 (Salida digital)
- BMXSRA0405 (Salida de relé digital)

Use los cuatro módulos de E/S de seguridad para conectar el PAC de seguridad a los sensores y actuadores que forman parte del bucle de seguridad. Cada módulo de E/S de seguridad incorpora un procesador de seguridad dedicado. Puede instalar estos módulos de E/S en la placa de conexiones local o en estaciones RIO.

### Requisitos de instalación y carcasa

Instale tu equipo de M580seguridad de manera que cumpla con:

- El grado de contaminación 2 según la norma IEC 60950 para la seguridad de los equipos de tecnología de la información, y
- la norma IEC 60529 de protección contra entrada IP54, de forma que:
  - la presencia de polvo no interfiera en el funcionamiento del equipo, y
  - las salpicaduras de agua no perjudiquen al equipo ni a las operaciones.

Normalmente estas normas se cumplen al colocar el equipo de seguridad en una carcasa (por ejemplo, un armario).

## Altitud máxima de funcionamiento

La altitud máxima de operación para los módulos de E/S de M580seguridad es de 2000 m sobre el nivel del mar.

## Comunicación entre el PAC y E/S

La CPU de M580seguridad y el cable de cobre controlan todos los intercambios de plano posterior, mientras que la E/S de seguridad responde a los comandos de la CPU y el cable de cobre. Los módulos de E/S de seguridad se pueden instalar en un bastidor X Bus de BMXXBP\*\*\*\* o un bastidor Ethernet de BMEXBP\*\*\*\*.

Las comunicaciones entre el PAC de seguridad y los módulos de E/S de seguridad del bastidor principal local se realizan a través de la placa de conexiones.

Las comunicaciones entre el PAC de seguridad y los módulos de E/S de seguridad instalados en la estación RIO se realizan a través de un módulo adaptador instalado en la estación RIO, ya sea:

- un adaptador BMECRA31210, para un bastidor Ethernet, o bien
- un adaptador BMXCRA31210, para un bastidor X Bus.

**NOTA:** Con la versión del firmware de la CPU 3.20 o posterior, la comunicación entre el PAC y las E/S de seguridad requiere un módulo BM•CRA31210 con la versión del firmware 2.60 o posterior.

**NOTA:** No se puede utilizar un adaptador BMXCRA31200 para conectar los módulos de seguridad de E/S con el PAC de seguridad de M580.

Opcionalmente, puede utilizar los módulos repetidores de fibra óptica BMXNRP0200 o BMXNRP0201 para ampliar el enlace físico entre la CPU y el coprocesador del bastidor local y el adaptador de la estación RIO. Los módulos repetidores de fibra óptica mejoran la inmunidad al ruido de la red de la estación RIO y aumentan la distancia de cableado, al tiempo que mantienen el rango dinámico completo de la red y el nivel de integridad de seguridad.

El protocolo de comunicaciones entre la E/S de seguridad y el PAC de seguridad permite sus intercambios. Permite a los dos dispositivos comprobar la precisión de los datos recibidos, detectar los datos dañados y determinar si el módulo de transmisión pasa a no ser operativo. Así, un bucle de seguridad puede incluir cualquier placa de conexiones y adaptadores RIO no interferentes, página 29.

## Fuente de alimentación externa utilizada con E/S de seguridad digital

Los módulos BMXSDI1602 y BMXSDO0802 digitales requieren una fuente de alimentación externa de bajo voltaje (SELV/PELV) con protección de 24 Vcc para proporcionar energía a los sensores y accionadores. Los módulos de E/S de seguridad supervisan la fuente de alimentación de proceso que no es de seguridad para las condiciones de sobretensión e infratensión.

### PELIGRO

#### **SE REQUIERE FUENTE DE ALIMENTACIÓN SELV/PELV OVERVOLTAGE CATEGORY II**

Use sólo una fuente de alimentación SELV/PELV tipo de sobretensión categoría II, con una salida máxima de 60 Vcc, para alimentar sensores y actuadores.

**Si no se siguen estas instrucciones, se producirán lesiones graves o la muerte.**

## Descripción general de diagnósticos para módulos de E/S de seguridad M580

### Introducción

Cada módulo de E/S de seguridad M580 presenta las siguientes funciones de diagnóstico:

- Autoprueba durante el arranque del módulo
- Autoprueba en tiempo de ejecución integrada continua
- LED de diagnóstico del módulo y del canal

Asimismo, los módulos de E/S de seguridad digitales también realizan diagnósticos de cableado.

### Autoprueba de encendido

Durante el encendido, los módulos de E/S realizan una serie ampliada de autopruebas de encendido. Si el resultado de estas pruebas son:

- Correctas: se considera que los módulos funcionan correctamente y son operativos.
- Incorrectas: se considera que los módulos no funcionan correctamente y no son operativos. En este caso, las entradas se establecen en 0 y las salidas están deenergizadas.

**NOTA:** Si la fuente de alimentación externa de 24 V CC no está conectada a un módulo de entrada digital o salida digital, las autopuebas de arranque no se llevarán a cabo y el módulo no arrancará.

## Pruebas integradas continuas

Durante la ejecución, los módulos de E/S llevan a cabo autopuebas continuamente. Los módulos de entrada verifican que pueden leer datos desde los sensores en el rango completo. Los módulos de salida verifican que el estado real de la salida sea el mismo que el del estado ordenado.

## Indicadores LED

Cada módulo de E/S de seguridad proporciona diagnósticos mediante LED de los módulos y los canales en la parte frontal del módulo:

- Los cuatro LED superiores (**Run**, **Err**, **I/O** y **Lck**) describen conjuntamente el estado del módulo.
- Las dos o cuatro filas inferiores de los LED se combinan con los cuatro LED superiores para describir el estado de cada canal de entrada o salida.

Consulte el tema sobre LED de diagnóstico para los módulos de E/S de seguridad siguientes para obtener más información sobre cómo leer los LED para el módulo en cuestión:

- Módulo de entrada analógica de seguridad, página 235 BMXSAI0410
- Módulo de entrada digital de seguridad, página 241 BMXSDI1602
- Módulo de salida digital de seguridad, página 247 BMXSDO0802
- Módulo de salida de relé digital de seguridad, página 252 BMXSRA0405

## Diagnósticos de cableado para módulos digitales

Tanto el módulo de entrada digital de seguridad como el módulo de salida digital de seguridad pueden detectar las siguientes condiciones de diagnóstico de cableado para canales:

- Cable abierto (o cortado).
- Cortocircuito a la tierra de 0 V.
- Cortocircuito a 24 V CC.
- Cruces entre dos canales.

**NOTA:** La disponibilidad de estas funciones de diagnóstico depende del diseño de cableado específico del módulo para sus dispositivos de campo. Consulte los ejemplos de cableado de la aplicación relativos a los módulos de E/S digitales de seguridad siguientes para obtener más información.

- Módulo de entrada digital de seguridad, página 73 BMXSDI1602
- Módulo de salida digital de seguridad, página 104 BMXSDO0802

# Módulo de entrada analógica BMXSAI0410

## Introducción

En esta sección se describe el módulo de entrada analógica de seguridad BMXSAI0410 M580.

# Módulo de entrada analógica de seguridad BMXSAI0410

## Introducción

El módulo de entrada analógica de seguridad BMXSAI0410 presenta las características siguientes:

- 4 canales de entrada de corriente de 4 a 20 mA analógica aislados.
- Conteos de resolución de 12 500, que abarca el rango de datos de 0 a 25 mA.
- Detección de corriente fuera de rango, para valores de corriente inferior a 3,75 mA o superior a 20,75 mA.
- Admite las normas de SIL3 (IEC 61508) siguientes:
  - El módulo puede alcanzar hasta la Categoría 2 (Cat2)/Nivel de rendimiento d (PLd) mediante 1 canal de entrada (evaluación de una de una [1oo1]). Por lo tanto, Cat1 y Cat2/PL a, b, c y d se pueden alcanzar utilizando 1 canal de entrada.
  - El módulo puede alcanzar hasta la Categoría 4 (Cat4)/Nivel de rendimiento e (PLe) mediante 2 canales de entrada (evaluación de una de dos [1oo2]). Por lo tanto, Cat3 y Cat4/PL d, e se puede conseguir utilizando 2 canales de entrada.
- Pantalla de LED de diagnóstico, página 235 que se proporciona para el módulo y para cada canal de entrada.
- Intercambio bajo tensión de módulos durante el tiempo de ejecución.
- Módulo CCOTF al operar en modalidad de mantenimiento, página 262. (CCOTF no es compatible con la modalidad de seguridad, página 261).

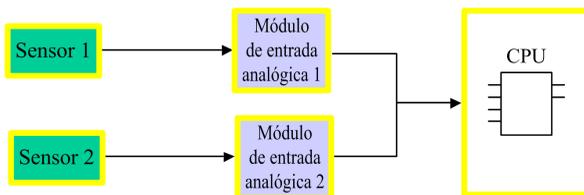
## Alta disponibilidad

Puede diseñar su aplicación de seguridad a niveles cambiantes de rendimiento y disponibilidad utilizando módulos y canales de entrada individuales o redundantes, de la forma siguiente:

Diseño:	Niveles de función de seguridad:			
Canales de entrada => Módulos	SIL	Cat	PL	¿Alta disponibilidad?
Canal de entrada individual a módulo de entrada individual, página 57	SIL3	Cat 2	PLd	–
Canal de entrada individual a módulos de entrada redundantes, página 58	SIL3	Cat 2	PLd	✓
Canales de entrada redundantes a módulo de entrada individual, página 59	SIL3	Cat 4	PLe	–
Canales de entrada redundantes a módulos de entrada redundantes, página 60	SIL3	Cat 4	PLe	✓

✓: Suministrado  
 -: No suministrado

En la figura siguiente se muestra la configuración de entradas analógicas redundantes.



El valor de corriente de entrada analógica del sensor 1 y del sensor 2 se envían mediante el módulo de entrada 1 y el módulo de entrada 2, respectivamente, a través de un canal negro a una CPU de seguridad. La CPU ejecuta un bloque de funciones dedicado (`S_AIHA`) en cada uno de los programas de lógica compilados e independientes para gestionar y seleccionar datos de los dos módulos de entrada. Este bloque de funciones opera de la forma siguiente:

- Si el estado de funcionamiento de los datos de entrada procedentes del módulo 1 es correcto, los datos de entrada de este módulo se utilizan en la función de seguridad.
- Si el estado de funcionamiento de los datos de entrada procedentes del módulo 1 no es correcto, pero el estado de funcionamiento de los datos de entrada procedentes del módulo 2 es correcto, se utilizan los datos de entrada del módulo 2.
- Si el estado de funcionamiento de los datos de entrada tanto del módulo 1 como del módulo 2 no es correcto, el sistema activará la función de seguridad.

# Conector de cableado BMXSAI0410

## Introducción

El módulo de entrada analógica BMXSAI0410 incluye 4 entradas analógicas. El módulo tiene dos pares de pines (dos pines de canal positivo [Ch] y dos pines comunes negativos [Com]) para cada entrada.

Para cada entrada:

- los dos pines de canal ( $Ch_n$ ) están conectados internamente, y
- los dos pines comunes ( $Com_n$ ) también están conectados internamente.

Para conectar un sensor analógico a una entrada, puede utilizar cualquiera de los dos pines de canal y dos pines comunes para esa entrada.

## Bloques de terminales

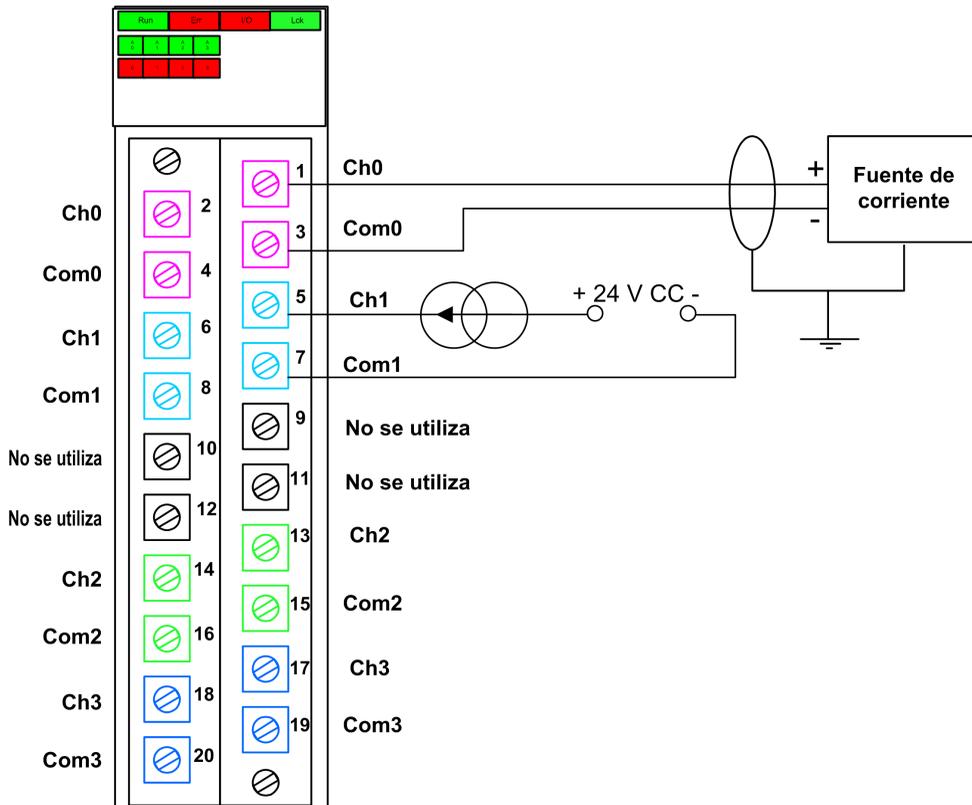
Puede utilizar los bloques de terminales de 20 puntos de Schneider Electric siguientes para montar el conector de 20 pines en la parte frontal del módulo:

- Bloque de terminales con tornillo de presión BMXFTB2010
- Bloque de terminales de abrazadera BMXFTB2000
- Bloque de terminales de resorte BMXFTB2020

**NOTA:** Los bloques de terminales se pueden retirar sólo cuando el módulo está apagado.

## Conector de cableado

En el ejemplo siguiente, se muestra un esquema de cableado genérico para las entradas del módulo:



**NOTA:** El módulo detecta una condición de cable cortado y lo notifica como una condición de fuera de rango (inferior a 3,75 mA) estableciendo el elemento OOR de la estructura `T_U_ANA_SIS_CH_IN`, página 64 en "1".

## Asignación de entradas a pines de conector

A continuación, se ofrece una descripción de cada pin del módulo de entrada analógica BMXSAI0410:

Descripción de los pines	Número de pin en el bloque de terminales		Descripción de los pines
Entrada (+) de canal 0	2	1	Entrada (+) de canal 0
Entrada (-) de canal 0	4	3	Entrada (-) de canal 0
Entrada (+) de canal 1	6	5	Entrada (+) de canal 1
Entrada (-) de canal 1	8	7	Entrada (-) de canal 1
No se utiliza	10	9	No se utiliza
No se utiliza	12	11	No se utiliza
Entrada (+) de canal 2	14	13	Entrada (+) de canal 2
Entrada (-) de canal 2	16	15	Entrada (-) de canal 2
Entrada (+) de canal 3	18	17	Entrada (+) de canal 3
Entrada (-) de canal 3	20	19	Entrada (-) de canal 3

**NOTA:** Puesto que los dos pines positivos para cada entrada están conectados internamente, debe utilizar sólo un pin positivo para un canal de entrada. De la misma forma, puesto que los dos pines negativos para cada entrada están conectados internamente, debe utilizar sólo un pin negativo para cada canal de entrada.

Por ejemplo, para conectar un sensor analógico a un canal de entrada 0, puede conectar:

- El cable positivo del sensor al pin 1 o al pin 2.
- El cable negativo del sensor al pin 3 o al pin 4.

## Ejemplos de cableado de aplicación de entrada de BMXSAI0410

### Introducción

Puede conectar el módulo de entrada analógica de seguridad BMXSAI0410 a sensores analógicos para lograr la conformidad con SIL3 de diversas formas, según:

- La norma requerida de Categoría (Cat2 o Cat4) y Nivel de rendimiento (PLd o PLe)
- Los requisitos de alta disponibilidad de la aplicación

## ▲ ATENCIÓN

### RIESGO DE FUNCIONAMIENTO IMPREVISTO

El nivel de integridad de seguridad (SIL) máximo se determina por medio de la calidad del sensor y la duración del intervalo de prueba de comprobación según IEC 61508. Si utiliza sensores que no cumplen la calidad de la norma de SIL prevista, conecte siempre estos sensores de forma redundante a dos canales.

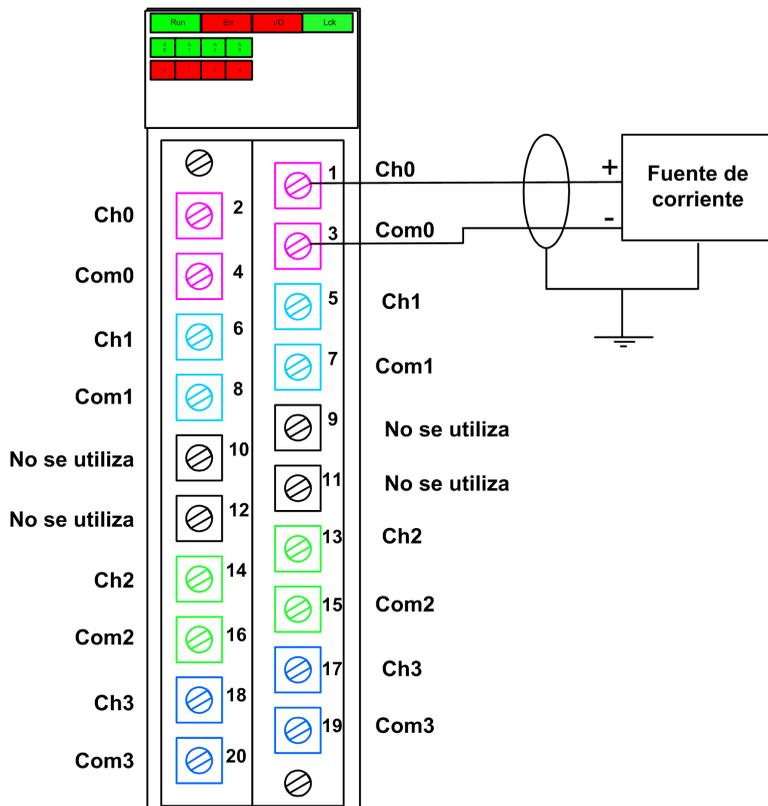
**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

Los siguientes ejemplos de cableado de aplicación de entrada digital SIL3 se describen a continuación.

- Cat2/PLd:
  - un sensor único conectado a una entrada.
- Cat2/PLd con alta disponibilidad:
  - dos sensores conectados a dos puntos de entrada en módulos de entrada diferentes.
- Cat4/PLe:
  - dos sensores, conectados respectivamente a un punto de entrada diferente en el mismo módulo de entrada.
- Cat4/PLe con alta disponibilidad:
  - dos pares de sensores (para un total de cuatro sensores): los sensores del primer par se conectan respectivamente a cada punto de entrada diferente en un módulo, y los sensores del segundo par se conectan respectivamente a un punto de entrada diferente en un segundo módulo.

## SIL3 Cat2/PLd

En el ejemplo siguiente se muestra un sensor único conectado a un punto de entrada en un módulo de entrada individual. La CPU realiza una evaluación 1oo1D en el valor único supervisado:



### ⚠ ATENCIÓN

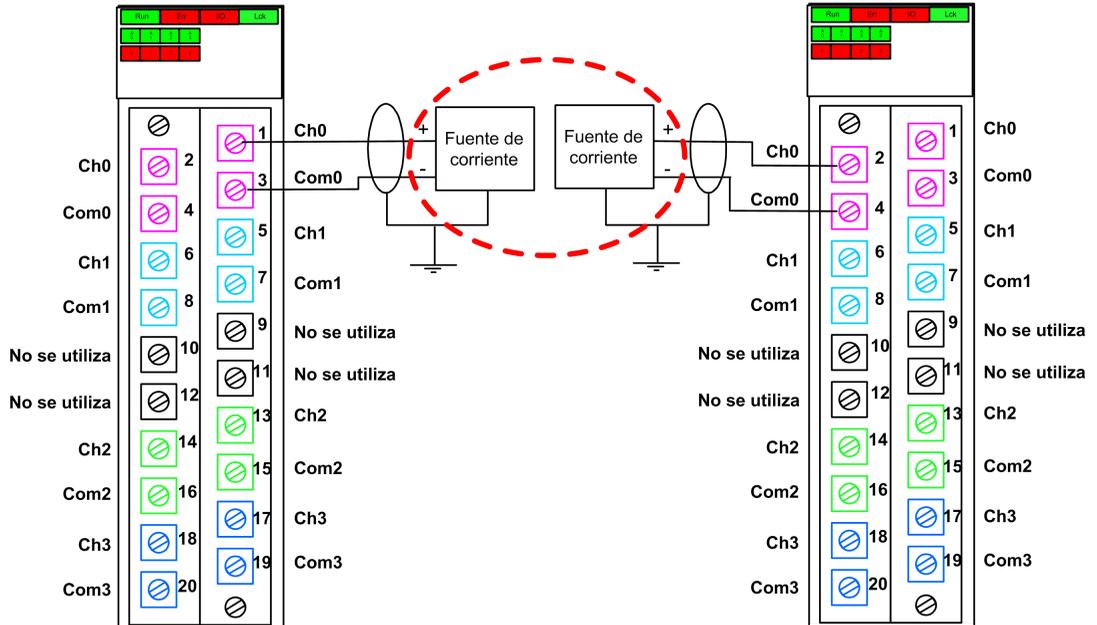
#### RIESGO DE FUNCIONAMIENTO IMPREVISTO

Para lograr SIL3 conforme a IEC 61508 y Categoría 2/Nivel de rendimiento d según ISO 13849 mediante este diseño de cableado, se debe usar un sensor homologado adecuado.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

## SIL3 Cat2/PLd con alta disponibilidad

El ejemplo siguiente muestra dos sensores que supervisan la misma variable de proceso. Cada sensor está conectado a un punto de entrada individual en módulos de entrada diferentes. La CPU realiza una evaluación 1oo1D del valor único supervisado:



**NOTA:** En este diseño, use el bloque de funciones `S_AIHA` de la tarea `SAFE` para gestionar dos valores de variable de proceso notificados por los dos sensores.

### ⚠ ATENCIÓN

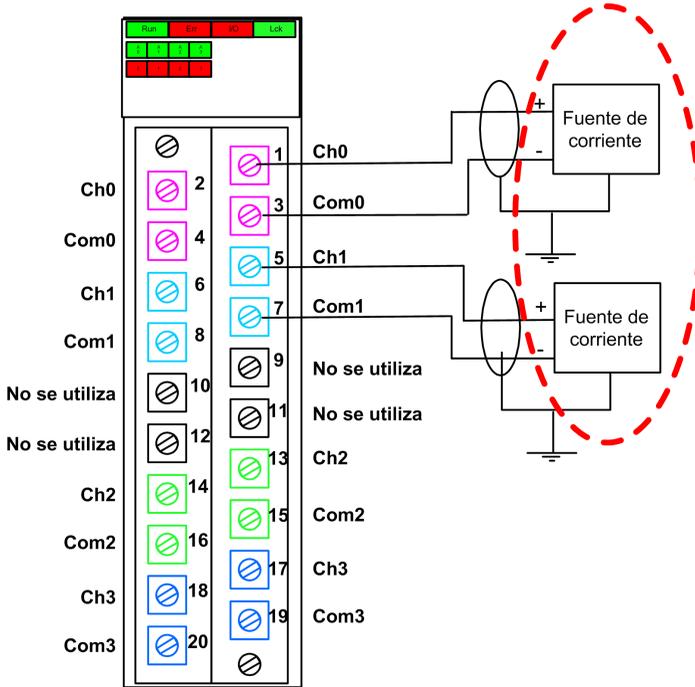
#### RIESGO DE FUNCIONAMIENTO IMPREVISTO

Para lograr SIL3 conforme a IEC 61508 y Categoría 2/Nivel de rendimiento d según ISO 13849 mediante este diseño de cableado, se debe usar un sensor homologado adecuado.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

## SIL3 Cat4/PLe

El ejemplo siguiente muestra dos sensores que supervisan la misma variable de proceso. Cada sensor está conectado a un punto de entrada individual en el mismo módulo de entrada. La CPU realiza una evaluación 1oo2D de los valores competidores proporcionados por los dos sensores para la misma variable de proceso:



**NOTA:** En este diseño, utilice el bloque de funciones `S_AI_COMP` de la tarea `SAFE` para realizar la evaluación 1oo2D de los valores competidores procedentes de los dos sensores.

### ⚠ ATENCIÓN

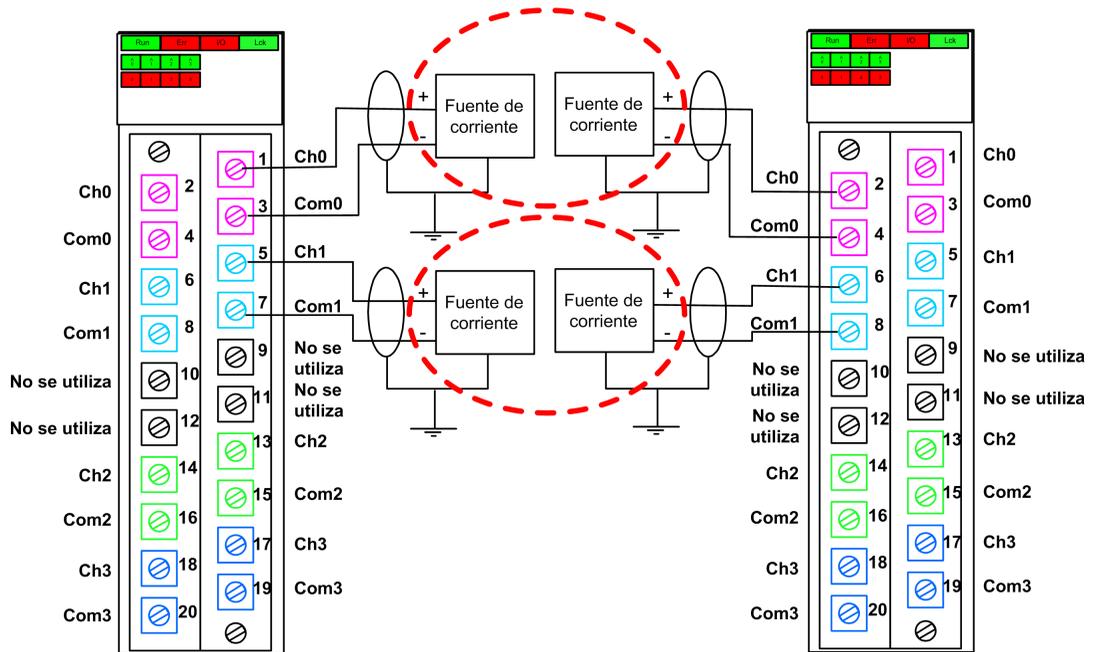
#### RIESGO DE FUNCIONAMIENTO IMPREVISTO

Para lograr SIL3 conforme a IEC 61508 y Categoría 4/Nivel de rendimiento d según ISO 13849 mediante este diseño de cableado, se debe usar un sensor homologado adecuado.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

## SIL3 Cat4/PLe con alta disponibilidad

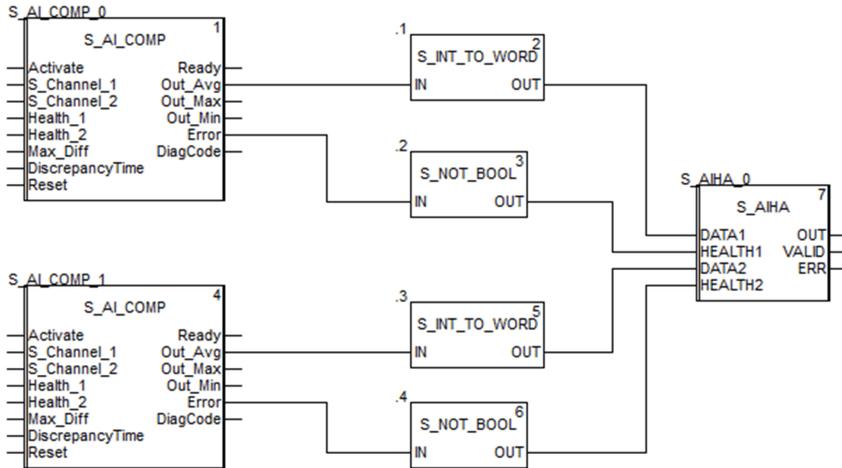
El ejemplo siguiente presenta dos pares de sensores redundantes, que supervisan la misma variable de proceso. Cada sensor está conectado a un punto de entrada individual en dos módulos de entrada diferentes (dos entradas en cada módulo). Este diseño permite que la CPU realice una evaluación 1oo2D:



**NOTA:** En este diseño, debe utilizar los bloques de funciones S\_AI\_COMP y S\_AIHA dentro de la tarea SAFE para gestionar las cuatro señales de entrada:

- S\_AI\_COMP para realizar una evaluación 1oo2 de dos pares de valores de los dos sensores conectados al mismo módulo.
- S\_AIHA para gestionar la característica de alta disponibilidad.

El siguiente diagrama del bloque de funciones muestra el diseño de segmento del código de referencia que aparece más arriba.



## ⚠ ATENCIÓN

### RIESGO DE FUNCIONAMIENTO IMPREVISTO

Para lograr SIL3 conforme a IEC 61508 y Categoría 4/Nivel de rendimiento d según ISO 13849 mediante este diseño de cableado, se debe usar un sensor homologado adecuado.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

## Estructura de datos de BMXSAI0410

### Introducción

El tipo de datos derivados del dispositivo (DDDT) T\_U\_ANA\_SIS\_IN\_4 es la interfaz entre el módulo de entrada analógica BMXSAI0410 y la aplicación que se ejecuta en la CPU. El

DDDT T\_U\_ANA\_SIS\_IN\_4 incorpora los tipos de datos T\_SAFE\_COM\_DBG\_IN y T\_U\_ANA\_SIS\_CH\_IN.

Todas estas estructuras se describen más abajo.

## Estructura del DDDT T\_U\_ANA\_SIS\_IN\_4

La estructura del DDDT T\_U\_ANA\_SIS\_IN\_4 incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso
MOD_HEALTH <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>1: El módulo está funcionando correctamente.</li> <li>0: El módulo no está funcionando correctamente.</li> </ul>	RO
SAFE_COM_STS <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>1: La comunicación del módulo es válida.</li> <li>0: La comunicación del módulo no es válida.</li> </ul>	RO
S_COM_DBG	T_SAFE_COM_DBG_IN	Estructura de depuración para comunicación segura.	RO
CONF_LOCKED	BOOL	<ul style="list-style-type: none"> <li>1: La configuración de módulo está bloqueada.</li> <li>0: La configuración de módulo no está bloqueada.</li> </ul>	RO
CH_IN	ARRAY[0-3] de T_U_ANA_SIS_CH_IN	Matriz de estructuras de canal	–
MUID <sup>2</sup>	ARRAY[0-3] de DWORD	ID exclusivo del módulo (asignado automáticamente por Control Expert)	RO
RESERVED	ARRAY[0-9] de INT	–	–
<p>1. Cuando la tarea SAFE de la CPU no está en modalidad de ejecución, no se actualizan los datos intercambiados entre la CPU y el módulo, y MOD_HEALTH y SAFE_COM_STS se establecen en 0.</p> <p>2. Este valor generado automáticamente se puede cambiar ejecutando el comando <b>Generar &gt; Renovar ID y Regenerar todo</b> en el menú principal de Control Expert.</p>			

## Estructura T\_SAFE\_COM\_DBG\_IN

La estructura T\_SAFE\_COM\_DBG\_IN incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso <sup>1</sup>
S_COM_EST	BOOL	<ul style="list-style-type: none"> <li>1: Se ha establecido comunicación con el módulo.</li> <li>0: No se ha establecido ni se ha interrumpido la comunicación con el módulo.</li> </ul>	RO
M_NTP_SYNC	BOOL	<p>Con la versión del firmware de la CPU 3.10 o anterior:</p> <ul style="list-style-type: none"> <li>1: El módulo se ha sincronizado con el servidor NTP.</li> <li>0: El módulo no se ha sincronizado con el servidor NTP.</li> </ul> <p><b>NOTA:</b> Con la versión del firmware de la CPU 3.20 o posterior, el valor siempre es 1.</p>	RO
CPU_NTP_SYNC	BOOL	<p>Con la versión del firmware de la CPU 3.10 o anterior:</p> <ul style="list-style-type: none"> <li>1: La CPU se ha sincronizado con el servidor NTP.</li> <li>0: La CPU no se ha sincronizado con el servidor NTP.</li> </ul> <p><b>NOTA:</b> Con la versión del firmware de la CPU 3.20 o posterior, el valor siempre es 1.</p>	RO
CHECKSUM	BYTE	Suma de comprobación de trama de comunicación.	RO
COM_DELAY	UINT	<p>Retardo de comunicación entre dos valores recibidos por el módulo:</p> <ul style="list-style-type: none"> <li>1-65534: El tiempo, en ms, desde que la CPU ha recibido la última comunicación del módulo.</li> <li>65535: La CPU no ha recibido ninguna comunicación del módulo.</li> </ul>	RO
COM_TO	UINT	<p>Valor de timeout de comunicación para las comunicaciones procedentes del módulo.</p> <p><b>NOTA:</b> Puede que desee editar este valor de lectura/escritura para igualar o superar el tiempo de comunicación real del módulo (por ejemplo, en una estación RIO remota).</p>	L/E
STS_MS_IN	UINT	Valor de marca de tiempo segura correspondiente a la fracción de un segundo, redondeado al ms más cercano, de los datos recibidos del módulo.	RO
S_NTP_MS	UINT	Valor de marca de tiempo segura correspondiente a la fracción de un segundo, redondeado al ms más cercano, para el ciclo actual.	RO

Elemento	Tipo de datos	Descripción	Acceso <sup>1</sup>
STS_S_IN	UDINT	Valor de marca de tiempo segura en segundos de los datos recibidos del módulo.	RO
S_NTP_S	UDINT	Valor de tiempo seguro en segundos para el ciclo actual.	RO
CRC_IN	UDINT	Valor de CRC para datos recibidos del módulo.	RO

## Estructura T\_U\_ANA\_SIS\_CH\_IN

La estructura T\_U\_ANA\_SIS\_CH\_IN incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso
FCT_TYPE	WORD	<ul style="list-style-type: none"> <li>1: El canal está habilitado.</li> <li>0: El canal no está habilitado.</li> </ul>	RO
CH_HEALTH <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>1: El canal está operativo.</li> <li>0: Se ha detectado un error en el canal, que no está operativo.</li> </ul> <p><b>Fórmula:</b> CH_HEALTH = not (OOR or IC) and SAFE_COM_STS</p>	RO
VALUE	INT	<p>Valor de entrada analógica.</p> <p><b>Fórmula:</b> VALUE = if (SAFE_COM_STS and not (IC)) then READ_VALUE else 0</p>	RO
OOR	BOOL	<ul style="list-style-type: none"> <li>1: El valor de corriente de entrada del canal está fuera de rango, ya sea: <ul style="list-style-type: none"> <li>&lt;3,75 mA</li> <li>&gt;20,75 mA</li> </ul> </li> <li>0: El valor de corriente de entrada del canal no está fuera de rango.</li> </ul>	RO
IC	BOOL	<ul style="list-style-type: none"> <li>1: Canal no válido detectado por el módulo.</li> <li>0: El módulo declara que el canal está operativo de forma interna.</li> </ul>	RO

1. Cuando la tarea SAFE de la CPU no está en modalidad de ejecución, no se actualizan los datos intercambiados entre la CPU y el módulo, y CH\_HEALTH se establece en 0.

# Módulo de entrada digital BMXSDI1602

## Introducción

En esta sección se describe el módulo de entrada digital de seguridad BMXSDI1602 M580.

# Módulo de entrada digital de seguridad BMXSDI1602

## Introducción

El módulo de entrada de seguridad BMXSDI1602 ofrece las características siguientes:

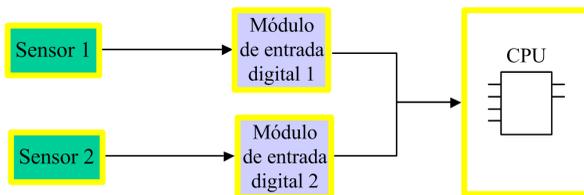
- 16 entradas de tipo 3 (IEC 61131-2), en dos grupos de 8 entradas no aislados galvánicamente.
- Tensión de entrada nominal de 24 V CC.
- Logra lo siguiente:
  - SIL3 IEC 61508, SIL CL3 IEC 62061.
  - SIL4 EN5012x.
  - Categoría 2 (Cat2)/Nivel de rendimiento d (PLd) ISO 13849 mediante 1 canal de entrada (evaluación de una de una [1oo1D]).
  - Categoría 4 (Cat4)/Nivel de rendimiento e (PLE) ISO 13849 mediante 2 canales de entrada (evaluación de una de dos [1oo2D]).
- Compatible con sensores de proximidad de 2 o 3 hilos.
- Proporciona de forma opcional dos salidas de 24 V CC (VS1 y VS2) para cortocircuito a supervisión de 24 V CC:
  - VS1 para supervisar el cortocircuito en las entradas 0-3 (rango A y B).
  - VS2 para supervisar cortocircuito en las entradas 4-7 (rango A y B).
- Supervisar la tensión externa de alimentación del sensor de 24 V CC.
- Pantalla de LED de diagnóstico, página 241 que se proporciona para el módulo y para cada canal de entrada.

- Diagnósticos de cableado de canal (habilitar/deshabilitar) configurables, página 74 que pueden detectar las condiciones siguientes:
  - Cable abierto (o cortado).
  - Cortocircuito a la tierra de 0 V.
  - Cortocircuito a 24 V CC (si se proporciona alimentación al sensor de forma interna).
  - Cruces entre dos canales (si se proporciona alimentación al sensor de forma interna).
- Intercambio bajo tensión de módulos durante el tiempo de ejecución.
- Módulo CCOTF al operar en modalidad de mantenimiento, página 262. (CCOTF no es compatible con la modalidad de seguridad, página 261).

## Alta disponibilidad

Puede utilizar dos sensores conectados a dos canales de entrada diferentes ubicados en módulos de entrada diferentes para supervisar el mismo valor físico y, por tanto, aumentar la disponibilidad del sistema.

En la figura siguiente se muestran las configuraciones de entradas digitales redundantes:



El valor de estado de entrada del sensor 1 y sensor 2 se envían por medio del sensor 1 y sensor 2, respectivamente, a través de un canal negro a una CPU de seguridad. La CPU ejecuta un bloque de funciones dedicado, S\_DIHA, para gestionar y seleccionar los datos de los dos módulos de entrada. Este bloque de funciones opera de la forma siguiente:

- Si el estado de funcionamiento de los datos de entrada procedentes del módulo 1 es correcto, los datos de entrada de este módulo se utilizan en la función de seguridad.
- Si el estado de funcionamiento de los datos de entrada procedentes del módulo 1 no es correcto, pero el estado de funcionamiento de los datos de entrada procedentes del módulo 2 es correcto, se utilizan los datos de entrada del módulo 2.
- Si el estado de funcionamiento de los datos de entrada del módulo 1 y módulo 2 no es correcto, el estado de la entrada se establece en el estado de seguridad ("0") a fin de activar la función de seguridad.

Consulte la descripción de [ejemplos de cableado de la aplicación de entrada](#), página 73 para obtener información detallada sobre cómo conectar el módulo para la alta disponibilidad.

# Conector de cableado BMXSDI1602

## Introducción

El módulo de entrada digital BMXSDI1602 presenta 16 entradas en dos grupos de 8 entradas. El primer grupo consta de entradas 0 a 3 (rango A y B), el segundo grupo consta de entradas 4 a 7 (rango A y B). No hay aislamiento entre estos dos grupos.

Se puede proporcionar alimentación a los sensores, ya sea directamente desde la fuente de alimentación externa o internamente a través de las fuentes de alimentación VS1 y VS2. Cada diseño se muestra más abajo.

## Bloques de terminales

Puede utilizar los bloques de terminales de 20 puntos de Schneider Electric siguientes para montar el conector de 20 pines en la parte frontal del módulo:

- Bloque de terminales con tornillo de presión BMXFTB2010
- Bloque de terminales de abrazadera BMXFTB2000
- Bloque de terminales de resorte BMXFTB2020

**NOTA:** Los bloques de terminales se pueden retirar sólo cuando el módulo está apagado.

## Fuente de alimentación de proceso

Se necesita una fuente de alimentación de proceso de categoría de sobretensión II con tensión extrabaja protegida (SELV/PELV) de 24 V CC. Schneider Electric recomienda una fuente de alimentación que no restablezca automáticamente la alimentación una vez que esta se haya interrumpido.

### PELIGRO

#### **PÉRDIDA DE CAPACIDAD PARA EJECUTAR FUNCIONES DE SEGURIDAD**

Utilice sólo una fuente de alimentación de proceso de tipo SELV/PELV con una salida máxima de 60 V.

**Si no se siguen estas instrucciones, se producirán lesiones graves o la muerte.**

## Fusible

Se necesita un fusible de acción rápida para ayudar a proteger la fuente de alimentación externa contra las condiciones de sobretensión o cortocircuito.

### **AVISO**

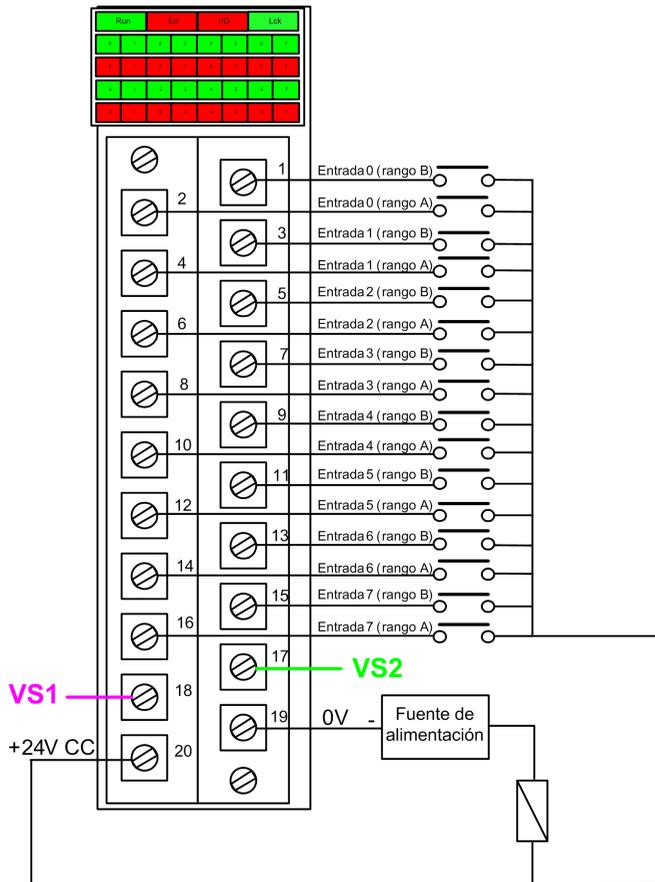
#### **SELECCIÓN DE FUSIBLES INCORRECTOS**

Use fusibles de acción rápida para ayudar a proteger los componentes electrónicos del módulo de entrada digital frente a una condición de sobrecorriente. La selección incorrecta de fusibles puede provocar daños en el módulo de entrada.

**Si no se siguen estas instrucciones, pueden producirse daños en el equipo.**

## Conector de cableado: Sensores alimentados con alimentación externa

En el diseño siguiente, una fuente de alimentación externa alimenta directamente a los sensores:



**fuentes de alimentación:** 24Vdc

**fusible:** fusible de acción rápida de 0,5 A

**NOTA:** Cuando se alimenta externamente a los sensores, se restringen los diagnósticos del canal que puede realizar el módulo. En este diseño de cableado, el módulo puede detectar:

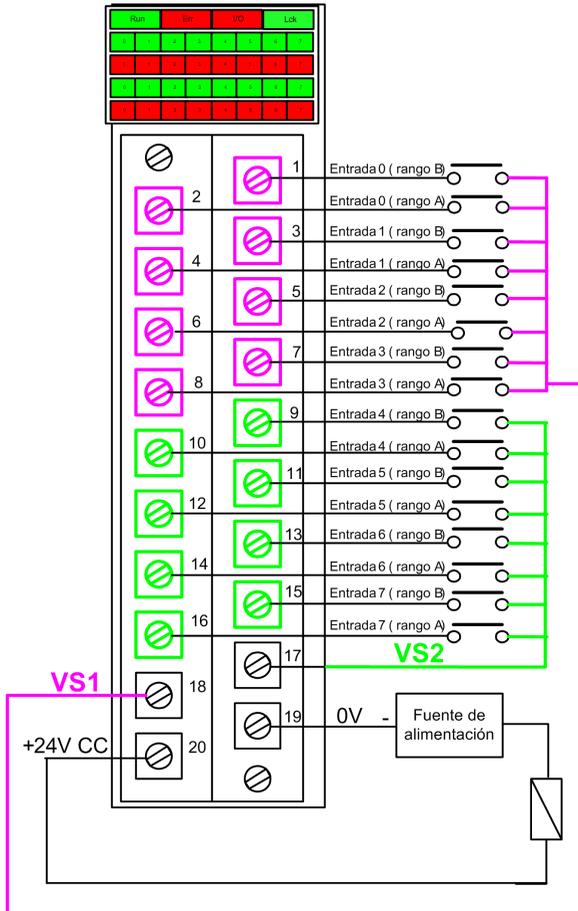
- Una condición de cable cortado (o abierto) (si se habilita para el canal en Control Expert).
- Una condición de cortocircuito a tierra.

Sin embargo, en este diseño, el módulo no detecta:

- Una condición de cortocircuito de 24 V CC.
- Una condición de cruce con otra entrada de cableado.

## Conector de cableado: Sensores alimentados con alimentación VS interna

En el diseño siguiente, la fuente de alimentación VS1 supervisada alimenta a los sensores para los canales 0 a 3 y la fuente de alimentación VS2 supervisada alimenta a los sensores para los canales 4 a 7:



Si utiliza este diseño, aplique alimentación interna a los grupos de canales de la siguiente forma:

- Use VS1 para alimentar a los canales 0 a 3 (rango A y B).
- Use VS2 para alimentar a los canales 4 a 7 (rango A y B).

**NOTA:** En este diseño, el módulo puede detectar:

- Una condición de cortocircuito de 24 V CC (si se habilita para el canal en Control Expert).
- Una condición de cruce con otra entrada de cableado.
- Una condición de cable cortado (o abierto) (si se habilita para el canal en Control Expert).
- Una condición de cortocircuito a tierra.

## Asignación de entradas a pines del conector y canales de Control Expert

A continuación se ofrece una descripción de cada pin del módulo de entrada BMXSDI1602 y se asigna cada pin al canal para ese pin según aparece en la ficha **Configuración** del canal para el módulo en Control Expert Safety:

Canal Control Expert	Descripción de los pines	Número de pin en el bloque de terminales		Descripción de los pines	Canal Control Expert
0	Entrada 0 (rango A)	2	1	Entrada 0 (rango B)	8
1	Entrada 1 (rango A)	4	3	Entrada 1 (rango B)	9
2	Entrada 2 (rango A)	6	5	Entrada 2 (rango B)	10
3	Entrada 3 (rango A)	8	7	Entrada 3 (rango B)	11
4	Entrada 4 (rango A)	10	9	Entrada 4 (rango B)	12
5	Entrada 5 (rango A)	12	11	Entrada 5 (rango B)	13
6	Entrada 6 (rango A)	14	13	Entrada 6 (rango B)	14
7	Entrada 7 (rango A)	16	15	Entrada 7 (rango B)	15
–	Fuente de alimentación VS1	18	17	Fuente de alimentación VS2	–
–	Fuente de alimentación de proceso de 24 V CC	20	19	Fuente de alimentación de proceso de 24 V CC	–

# Ejemplos de cableado de aplicación de entrada de BMXSDI1602

## Introducción

Puede conectar el módulo de entrada digital de seguridad BMXSDI1602 a los sensores para lograr la conformidad con SIL3 de distintas formas, según:

- La norma requerida de Categoría (Cat2 o Cat4) y Nivel de rendimiento (PLd o PLe)
- Los requisitos de alta disponibilidad de la aplicación

### **⚠ ATENCIÓN**

#### **RIESGO DE FUNCIONAMIENTO IMPREVISTO**

El nivel de integridad de seguridad (SIL) máximo se determina por medio de la calidad del sensor y la duración del intervalo de prueba de comprobación según IEC 61508. Si utiliza sensores que no cumplen la calidad de la norma de SIL prevista, conecte siempre estos sensores de forma redundante a dos canales.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

Los siguientes ejemplos de cableado de aplicación de entrada digital SIL3 se describen a continuación.

- Cat2/PLd:
  - Un único sensor conectado una entrada
- Cat2/PLd con alta disponibilidad:
  - Un único sensor conectado a dos puntos de entrada en módulos de entrada diferentes
  - Dos sensores conectados a dos puntos de entrada en módulos de entrada diferentes
- Cat4/PLe:
  - Un único sensor conectado a dos puntos de entrada en el mismo módulo de entrada
  - Dos sensores, conectados respectivamente a un punto de entrada diferente en el mismo módulo de entrada
- Cat4/PLe con alta disponibilidad:
  - Dos sensores, conectados respectivamente a dos puntos de entrada diferentes en módulos de entrada diferentes

## Diagnósticos de cableado configurables en Control Expert

Para el módulo de entrada digital de seguridad BMXSDI1602, utilice su página **Configuración** en Control Expert para:

- Habilitar **Detección de cortocircuito a 24 V** para cada canal energizado. Esta prueba realiza los diagnósticos de cableado del actuador siguientes para un canal:
  - Detección de cortocircuito a 24 V CC.
  - Detección de cruce entre dos canales de salida.

La idea es proporcionar alimentación a los sensores, por grupo de 8 canales (con VS1 para los canales 0 a 3 [rango A y B] y VS2 para los canales 4 a 7 [rango A y B]). Se aplica un pulso a OFF a estas salidas de alimentación de forma periódica con un periodo inferior a 1 segundo y una duración inferior a 1 ms. Durante este pulso, si la lectura de corriente en la entrada no es nula, el módulo considera que la entrada está cortocircuitada.

- Habilitar **Detección de cable abierto** para cada uno de los ocho canales, lo cual realiza los siguientes diagnósticos de cableado para el canal pertinente:
  - Detección de cable abierto (o cortado) (es decir, el canal de entrada no está conectado al sensor).
  - Detección de cortocircuito del cableado a la tierra de 0 V CC.

El principio consiste en crear artificialmente, y luego medir, una corriente de fuga (leakage) en la línea (con una resistencia colocada paralela al sensor) cuando se abre el sensor. Si el módulo no puede medir la corriente de fuga ( $0,4 \text{ mA} < \text{leakage} < 1,3 \text{ mA}$ ) en la línea de entrada, la línea externa se considerará cortada (o cortocircuitada a tierra). El diagnóstico se realiza en un periodo inferior a 10 ms.

- En el caso de un sensor de contacto seco, recomendamos poner una resistencia de 33 kΩ en paralelo con el sensor.
- Al utilizar 2 o 3 cables de DDP, los valores de la corriente de fuga deben estar comprendidos dentro de los límites definidos anteriormente. Debe definir el valor de la resistencia que se debe poner en paralelo con el sensor, teniendo en cuenta la corriente de fuga natural del sensor y la resistencia interna de la entrada (7,5 kΩ).

### ⚠ ADVERTENCIA

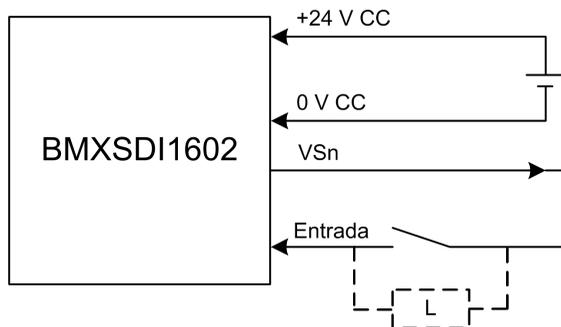
#### RIESGO DE FUNCIONAMIENTO IMPREVISTO

Schneider Electric recomienda habilitar los diagnósticos disponibles que se proporcionan en Control Expert para detectar o excluir las condiciones enumeradas anteriormente. Si una prueba de diagnóstico no está habilitada o no está disponible en Control Expert, deberá aplicar otra medida de seguridad para detectar o excluir estas condiciones.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## SIL3 Cat2/PLd

### Sensor único conectado a una entrada alimentada por la VS interna:



En este ejemplo, si se suministra alimentación interna mediante:

- VS1, use canales 0-3 rangos A y B.
- VS2, use canales 4-7 rangos A y B.

Puesto que se suministra alimentación internamente al sensor a través de un pin VS, se aplican los diagnósticos de cableado de canal siguientes.

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC <sup>1</sup>	Sí	< 1 s
Cruces entre dos canales <sup>1</sup>	Sí	
1. Esta función de diagnóstico se realiza si está habilitada en la ficha <b>Configuración</b> del módulo en Control Expert.		

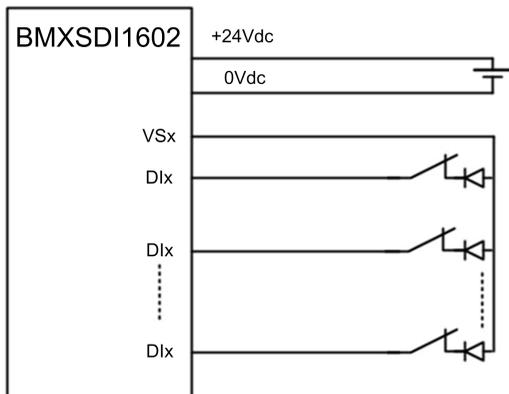
## ⚠ ADVERTENCIA

### RIESGO DE CRUCES ENTRE CANALES DEL MISMO GRUPO

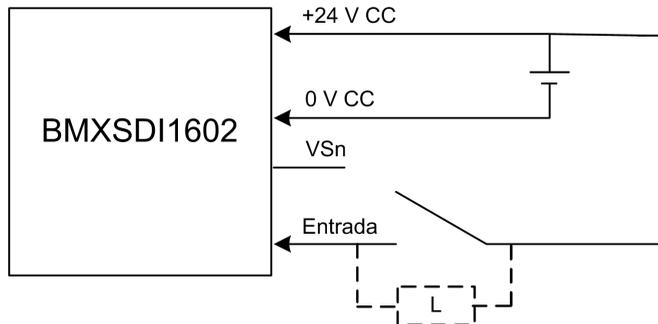
El módulo no puede detectar los cruces entre dos canales del mismo grupo de VS de canales. Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

**NOTA:** Plantéese añadir un diodo Shottky al bucle de entrada, entre el sensor y el punto de entrada, para reducir la probabilidad de que un cortocircuito a 24 V CC en un canal pueda generar la misma situación en un canal adyacente.



**Un solo conector conectado a una entrada, al que se suministra alimentación externa:**



Puesto que se suministra alimentación al sensor de forma externa, se aplican los diagnósticos de cableado de canales siguientes:

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC	Sin	-
Cruces entre dos canales	No	

1. Esta función de diagnóstico se realiza si está habilitada en la ficha **Configuración** del módulo en Control Expert.

## **⚠ ADVERTENCIA**

### **RIESGO DE CRUCES ENTRE CANALES**

El módulo no puede detectar cruces entre dos canales (en el caso de un sensor único conectado a una entrada, al que se suministra alimentación externa, tal como se muestra más arriba). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## **⚠ ADVERTENCIA**

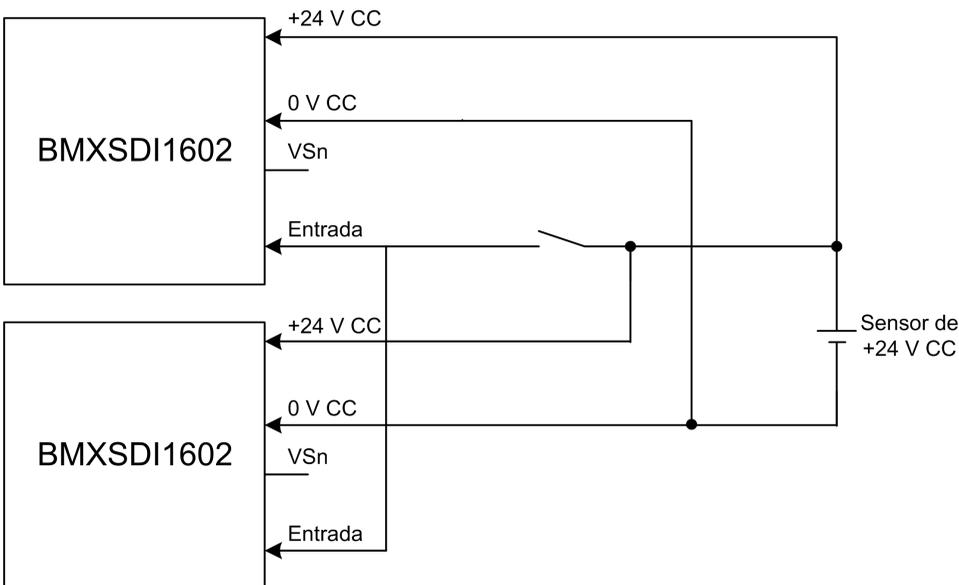
### **RIESGO DE CORTOCIRCUITO A 24 V CC**

El módulo no puede detectar una condición de cortocircuito a 24 V CC (en el caso de un sensor único conectado a una entrada, al que se suministra alimentación externa, tal como se muestra más arriba). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## **SIL3 Cat2/PLd con alta disponibilidad**

**Un sensor único conectado a 2 entradas al que se suministra alimentación externa:**



Puesto que se suministra alimentación al sensor único de forma externa, se aplican los diagnósticos de cableado de canales siguientes:

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sin	-
Cortocircuito a la tierra de 0 V	No	
Cortocircuito a 24 V CC <sup>1</sup>	No	
Cruces entre dos canales	No	

1. Esta función de diagnóstico se realiza si está habilitada en la ficha **Configuración** del módulo en Control Expert.

## ⚠ ADVERTENCIA

### RIESGO DE CRUCES ENTRE CANALES

El módulo no puede detectar cruces entre dos canales (en el caso de un sensor único conectado a dos entradas, al que se suministra alimentación externa, tal como se muestra más arriba). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## ⚠ ADVERTENCIA

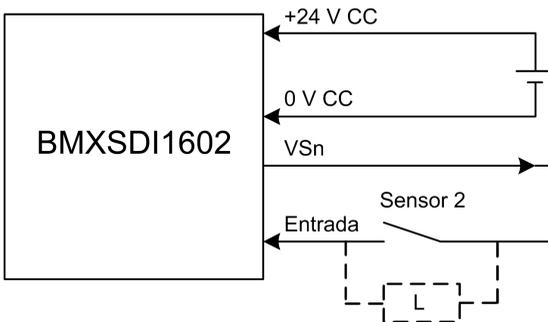
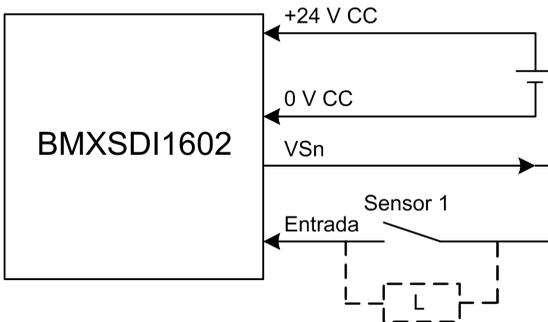
### RIESGO DE CORTOCIRCUITO A 24 V CC

El módulo no puede detectar una condición de cortocircuito a 24 V CC (en el caso de un sensor único conectado a dos entradas, al que se suministra alimentación externa, tal como se muestra más arriba). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

### 2 sensores redundantes conectados a entradas individuales de 2 módulos mediante VS:

En el ejemplo siguiente se muestran dos sensores redundantes (que pueden estar o no conectados mecánicamente) que se utilizan para adquirir la misma variable de proceso. Cada sensor está conectado a un punto de entrada individual en un módulo de entrada diferente, con alimentación suministrada por la fuente de alimentación VS supervisada:



En este ejemplo, si se suministra alimentación interna mediante:

- VS1, use canales 0-3 rangos A y B.

- VS2, use canales 4-7 rangos A y B.

**NOTA:**

- En este diseño, puede utilizar el bloque de funciones S\_DIHA para gestionar las dos señales de entrada.
- Plantéese añadir un diodo Shottky al bucle de entrada, entre el sensor y el punto de entrada, para reducir la probabilidad de que la condición de cortocircuito a 24 V CC de un canal pueda generar la misma condición en un canal adyacente.

Puesto que se suministra alimentación internamente al sensor a través de un pin VS, se aplican los diagnósticos de cableado de canal siguientes.

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC <sup>1</sup>	Sí	< 1 s
Cruces entre dos canales	Sí	
1. Esta función de diagnóstico se realiza si está habilitada en la ficha <b>Configuración</b> del módulo en Control Expert.		

## ADVERTENCIA

### RIESGO DE CRUCES ENTRE CANALES DEL MISMO GRUPO

El módulo no puede detectar los cruces entre dos canales del mismo grupo de VS de canales. Deberá aplicar otra medida de seguridad para detectar y excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

### 2 sensores redundantes conectados a entradas individuales de 2 módulos mediante alimentación externa:

**NOTA:** De forma alternativa, se puede suministrar alimentación a los sensores mediante una fuente de alimentación externa. En este caso, no se detectaría una condición de cortocircuito a 24 V CC ni una condición de cruces entre dos canales.

Puesto que se suministra alimentación internamente al sensor a través de un pin VS, se aplican los diagnósticos de cableado de canal siguientes.

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC	Sin	–

Estado	¿Detectable?	Tiempo de detección típico
Cruces entre dos canales	No	
1. Esta función de diagnóstico se realiza si está habilitada en la ficha <b>Configuración</b> del módulo en Control Expert.		

## ⚠ ADVERTENCIA

### RIESGO DE CRUCES ENTRE CANALES

El módulo no puede detectar los cruces entre dos canales (en el caso de dos sensores redundantes conectados a entradas individuales de dos módulos mediante alimentación externa). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## ⚠ ADVERTENCIA

### RIESGO DE CORTOCIRCUITO A 24 V CC

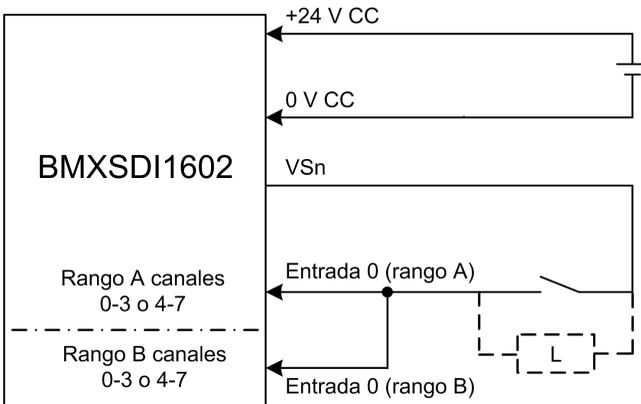
El módulo no puede detectar una condición de cortocircuito a 24 V CC (en el caso de dos sensores redundantes conectados en entradas individuales de dos módulos mediante alimentación externa). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## Cat4/PLe

**Un conector único conectado a 2 entradas del mismo módulo a través de VS:**

En el ejemplo siguiente se muestra un sensor único conectado a dos puntos de entrada del mismo módulo de entrada, con alimentación suministrada a través de la fuente de alimentación VS supervisada:



En este ejemplo, si se suministra alimentación interna mediante:

- VS1, use canales 0-3 rangos A y B.
- VS2, use canales 4-7 rangos A y B.

**NOTA:**

- En este diseño, puede utilizar el bloque de funciones `S_EQUIVALENT` para gestionar las dos señales de entrada.
- Plantéese añadir un diodo Shottky al bucle de entrada, entre el sensor y el punto de entrada, para reducir la probabilidad de que la condición de cortocircuito a 24 V CC de un canal pueda generar la misma condición en un canal adyacente.

Diagnóstico de cableado con sensor único conectado a dos entradas usando tensión del pin VS:

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC <sup>1</sup>	Sí	< 1 s
Cruces entre dos canales	Sí	
1. Esta función de diagnóstico se realiza si está habilitada en la ficha <b>Configuración</b> del módulo en Control Expert.		

## ▲ ADVERTENCIA

### RIESGO DE CRUCES ENTRE CANALES DEL MISMO GRUPO

El módulo no puede detectar los cruces entre dos canales del mismo grupo de VS de canales. Deberá aplicar otra medida de seguridad para detectar y excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

### Sensor único conectado a 2 entradas del mismo módulo mediante fuente de alimentación externa:

**NOTA:** De forma alternativa, se puede suministrar alimentación a los sensores mediante una fuente de alimentación externa. En este caso, no se detectaría una condición de cortocircuito a 24 V CC ni una condición de cruces entre dos canales.

Diagnóstico de cableado con sensor único conectado a dos entradas mediante fuente de alimentación externa:

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC <sup>1</sup>	No	-
Cruces entre dos canales	No	

1. Esta función de diagnóstico se realiza si está habilitada en la ficha **Configuración** del módulo en Control Expert.

## ▲ ADVERTENCIA

### RIESGO DE CRUCES ENTRE CANALES

El módulo no puede detectar cruces entre dos canales (en el caso de un sensor único conectado en dos entradas del mismo módulo mediante una fuente de alimentación externa). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## ⚠ ADVERTENCIA

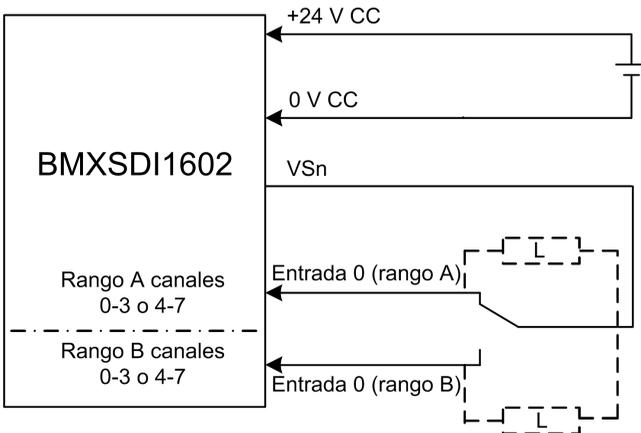
### RIESGO DE CORTOCIRCUITO A 24 V CC

El módulo no puede detectar una condición de cortocircuito a 24 V CC (en el caso de un sensor único conectado a dos entradas del mismo módulo mediante una fuente de alimentación externa). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

### Sensor no equivalente conectado a 2 entradas no equivalentes del mismo módulo a través de VS:

En el ejemplo siguiente se muestra un sensor único no equivalente conectado a dos puntos de entrada del mismo módulo de entrada, con alimentación suministrada a través de la fuente de alimentación VS supervisada: El módulo realizará una evaluación 1oo2D:



En este ejemplo, si se suministra alimentación interna mediante:

- VS1, use canales 0-3 rangos A y B.
- VS2, use canales 4-7 rangos A y B.

#### NOTA:

- En este diseño, puede utilizar el bloque de funciones `S_ANTIIVALENT` para gestionar las dos señales de entrada.
- Plantéese añadir un diodo Shottky al bucle de entrada, entre el sensor y el punto de entrada, para reducir la probabilidad de que la condición de cortocircuito a 24 V CC de un canal pueda generar la misma condición en un canal adyacente.

Diagnóstico de cableado con sensores no equivalentes conectados a dos entradas usando tensión del pin VS:

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC <sup>1</sup>	Sí	< 1 s
Cruces entre dos canales	Sí	
1. Esta función de diagnóstico se realiza si está habilitada en la ficha <b>Configuración</b> del módulo en Control Expert.		

### Sensor no equivalente conectado a 2 entradas no equivalentes del mismo módulo mediante fuente de alimentación externa:

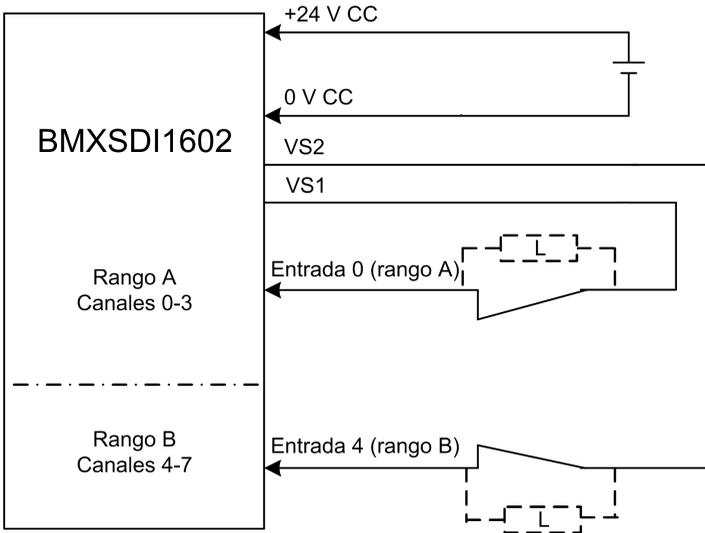
**NOTA:** De forma alternativa, se puede suministrar alimentación a los sensores mediante una fuente de alimentación externa. En este caso, no se detectaría una condición de cortocircuito a 24 V CC ni una condición de cruces entre dos canales.

Diagnóstico de cableado con sensores no equivalentes únicos conectados en dos entradas mediante alimentación externa:

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC <sup>1</sup>	No	-
Cruces entre dos canales	No	
1. Esta función de diagnóstico se realiza si está habilitada en la ficha <b>Configuración</b> del módulo en Control Expert.		

### Adquisición de la misma variable de proceso mediante dos sensores independientes (conectados o no mecánicamente) a través de VS:

En el ejemplo siguiente se muestran dos sensores redundantes (que pueden estar o no conectados mecánicamente) que se utilizan para adquirir la misma variable de proceso. Cada sensor está conectado a un punto de entrada único en el mismo módulo de entrada, con alimentación suministrada por la fuente de alimentación VS supervisada:



**NOTA:**

- Las entradas 0-3 del rango A se utilizan con las entradas 4-7 del rango B.
- Las entradas 0-3 del rango B se utilizan con las entradas 4-7 del rango A.

## ⚠ ADVERTENCIA

### RIESGO DE FUNCIONAMIENTO IMPREVISTO

Para lograr SIL3 conforme a IEC 61508 y Categoría 4/Nivel de rendimiento e según ISO 13849 usando este diseño de cableado, se deben usar sensores homologados adecuados.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

En este ejemplo, si se suministra alimentación interna mediante:

- VS1, use canales 0-3 rangos A y B.
- VS2, use canales 4-7 rangos A y B.

**NOTA:**

- En este diseño, puede utilizar el bloque de funciones S\_EQUIVALENT para gestionar las dos señales de entrada.
- Plántese añadir un diodo Shottky al bucle de entrada, entre el sensor y el punto de entrada, para reducir la probabilidad de que la condición de cortocircuito a 24 V CC de un canal pueda generar la misma condición en un canal adyacente.

Diagnóstico de cableado con sensor único conectado a dos entradas usando tensión del pin VS:

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC <sup>1</sup>	Sí	< 1 s
Cruces entre dos canales	Sí	

1. Esta función de diagnóstico se realiza si está habilitada en la ficha **Configuración** del módulo en Control Expert.

## ▲ ADVERTENCIA

### RIESGO DE CRUCES ENTRE CANALES DEL MISMO GRUPO

El módulo no puede detectar cruces entre dos canales del mismo grupo de VS de canales (en el caso de la adquisición de la misma variable de proceso utilizando dos sensores independientes mediante alimentación suministrada por VS). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## ▲ ADVERTENCIA

### RIESGO DE CORTOCIRCUITO A 24 V CC

El módulo no puede detectar una condición de cortocircuito a 24 V CC (en el caso de la adquisición de la misma variable de proceso utilizando dos sensores independientes mediante alimentación suministrada por VS). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

**Adquisición de la misma variable de proceso utilizando dos sensores independientes (conectados o no mecánicamente) mediante alimentación externa:**

**NOTA:** De forma alternativa, se puede suministrar alimentación a los sensores mediante una fuente de alimentación externa. En este caso, no se detectaría una condición de cortocircuito a 24 V CC ni una condición de cruces entre dos canales.

Diagnóstico de cableado con sensor único conectado a dos entradas mediante alimentación externa:

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC <sup>1</sup>	No	-
Cruces entre dos canales	No	
1. Esta función de diagnóstico se realiza si está habilitada en la ficha <b>Configuración</b> del módulo en Control Expert.		

## ⚠ ADVERTENCIA

### RIESGO DE CRUCES ENTRE CANALES

El módulo no puede detectar cruces entre dos canales (en el caso de la adquisición de la misma variable de proceso utilizando dos sensores independientes mediante alimentación externa). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## ⚠ ADVERTENCIA

### RIESGO DE FUNCIONAMIENTO IMPREVISTO

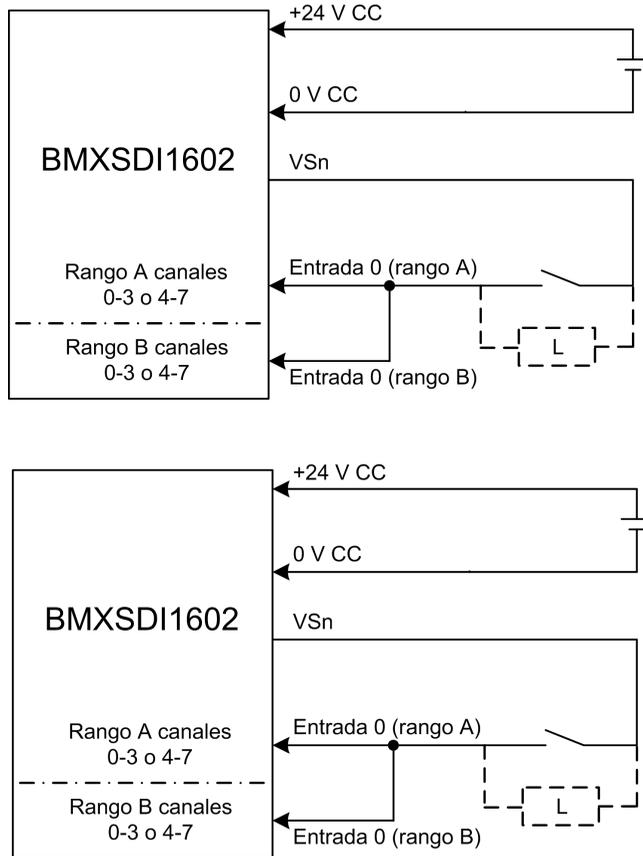
Para lograr SIL3/Cat4/PLe mediante este cableado, debe utilizar un sensor debidamente homologado.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## Cat4/PLe con alta disponibilidad

Esquema de cableado con conexión de único canal de dos sensores de un único canal redundantes mediante VS:

En el ejemplo siguiente se muestran dos sensores de único canal redundantes (que pueden estar o no conectados mecánicamente), conectados respectivamente a dos puntos de entrada en dos módulos de entrada diferentes, con alimentación suministrada por la fuente de alimentación VS supervisada:



En este ejemplo, si se suministra alimentación interna mediante:

- VS1, use canales 0-3 rangos A y B.
- VS2, use canales 4-7 rangos A y B.

**NOTA:**

- En este diseño, puede utilizar los bloques de funciones `S_EQUIVALENT` y `S_DIHA` para gestionar las cuatro señales de entrada.
- Plantéese añadir un diodo Shottky al bucle de entrada, entre el sensor y el punto de entrada, para reducir la probabilidad de que la condición de cortocircuito a 24 V CC de un canal pueda generar la misma condición en un canal adyacente.

Diagnóstico de cableado con sensor único conectado a dos entradas usando tensión del pin VS:

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC <sup>1</sup>	Sí	< 1 s
Cruces entre dos canales	Sí	

1. Esta función de diagnóstico se realiza si está habilitada en la ficha **Configuración** del módulo en Control Expert.

## **⚠ ADVERTENCIA**

### **RIESGO DE CRUCES ENTRE CANALES DEL MISMO GRUPO**

El módulo no puede detectar los cruces entre dos canales del mismo grupo de VS de canales. Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

### **Esquema de cableado con conexión de canal único de dos sensores de canal único redundantes mediante alimentación externa:**

**NOTA:** De forma alternativa, se puede suministrar alimentación a los sensores mediante una fuente de alimentación externa. En este caso, no se detectaría una condición de cortocircuito a 24 V CC ni una condición de cruces entre dos canales.

Diagnóstico de cableado con sensor único conectado a dos entradas mediante alimentación externa:

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC <sup>1</sup>	No	-
Cruces entre dos canales	No	

1. Esta función de diagnóstico se realiza si está habilitada en la ficha **Configuración** del módulo en Control Expert.

## **⚠ ADVERTENCIA**

### **RIESGO DE CRUCES ENTRE CANALES**

El módulo no puede detectar dos cruces entre dos canales (en el caso de una conexión de canal único de dos sensores de canal único redundantes mediante alimentación externa). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## **⚠ ADVERTENCIA**

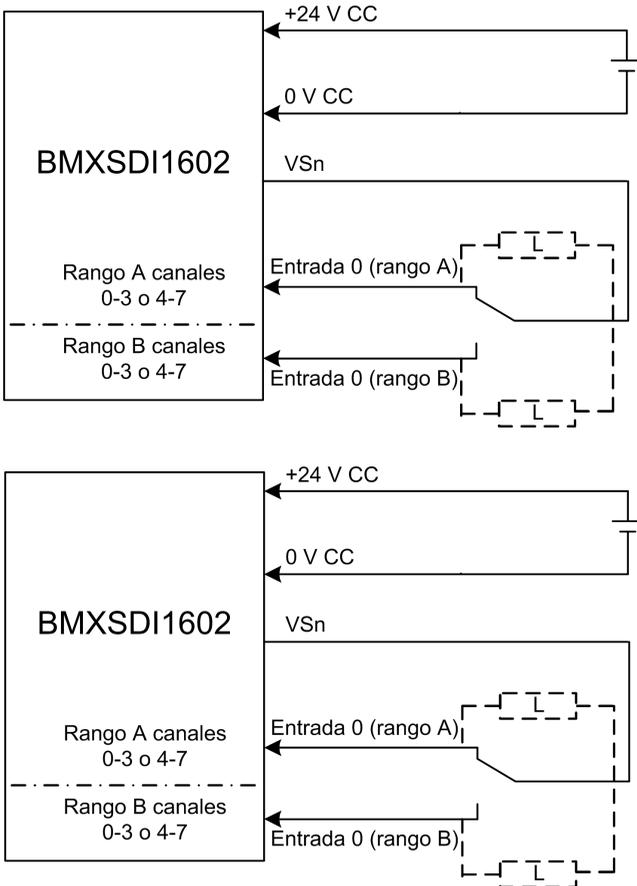
### **RIESGO DE CORTOCIRCUITO A 24 V CC**

El módulo no puede detectar una condición de cortocircuito a 24 V CC (en el caso de una conexión de canal único de dos sensores de canal único redundantes mediante alimentación externa). Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

**Sensor no equivalente (conectado o no mecánicamente) a 2 entradas no equivalentes de dos módulos diferentes mediante VS:**

El ejemplo siguiente muestra dos pares de sensores no equivalentes redundantes (que pueden estar o no conectados mecánicamente), conectados respectivamente a un punto de entrada individual en dos módulos de entrada diferentes (dos en cada módulo), con alimentación suministrada por la fuente de alimentación VS supervisada.



En este ejemplo, si se suministra alimentación interna mediante:

- VS1, use canales 0-3 rangos A y B.
- VS2, use canales 4-7 rangos A y B.

**NOTA:**

- En este diseño, debe utilizar los bloques de funciones S\_ANTIVALENT y S\_DIHA para gestionar las cuatro señales de entrada.
  - S\_ANTIVALENT para realizar una evaluación 1oo2 de dos pares de valores de los dos sensores conectados al mismo módulo.
  - S\_DIHA para gestionar la característica de alta disponibilidad.
- Plantéese añadir un diodo Shottky al bucle de entrada, entre el sensor y el punto de entrada, para reducir la probabilidad de que la condición de cortocircuito a 24 V CC de un canal pueda generar la misma condición en un canal adyacente.

Puesto que se suministra alimentación internamente al sensor a través de un pin VS, se aplican los diagnósticos de cableado de canal siguientes.

Estado	¿Detectable?	Tiempo de detección típico
Cable abierto (o cortado) <sup>1</sup>	Sí	< 10 ms
Cortocircuito a la tierra de 0 V	Sí	
Cortocircuito a 24 V CC <sup>1</sup>	Sí	< 1 s
Cruces entre dos canales	Sí	
1. Esta función de diagnóstico se realiza si está habilitada en la ficha <b>Configuración</b> del módulo en Control Expert.		

## ⚠ ADVERTENCIA

### RIESGO DE CRUCES ENTRE CANALES DEL MISMO GRUPO

El módulo no puede detectar los cruces entre dos canales del mismo grupo de VS de canales. Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

**Sensor no equivalente (vinculado o no mecánicamente) conectado a 2 entradas no equivalentes de dos módulos diferentes mediante alimentación externa:**

**NOTA:** De forma alternativa, se puede suministrar alimentación a los sensores por medio de una fuente de alimentación externa (en el caso de un sensor no equivalente conectado a dos entradas no equivalentes de dos módulos diferentes mediante alimentación externa). En este caso, no se detectaría una condición de cruces entre dos canales.

## ⚠ ADVERTENCIA

### RIESGO DE CRUCES ENTRE CANALES

El módulo no puede detectar cruces entre dos canales. Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## ⚠ ADVERTENCIA

### RIESGO DE FUNCIONAMIENTO IMPREVISTO

Para lograr SIL3 conforme a IEC 61508 y Categoría 4/Nivel de rendimiento e según ISO 13849 usando este diseño de cableado, se deben usar sensores homologados adecuados.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## Estructura de datos de BMXSDI1602

### Introducción

El tipo de datos derivados del dispositivo (DDDT) `T_U_DIS_SIS_IN_16` es la interfaz entre el módulo de entrada digital BMXSDI1602 y la aplicación que se ejecuta en la CPU. El DDDT `T_U_DIS_SIS_IN_16` incorpora los tipos de datos `T_SAFE_COM_DBG_IN` y `T_U_DIS_SIS_CH_IN`.

Todas estas estructuras se describen más abajo.

### Estructura del DDDT `T_U_DIS_SIS_IN_16`

La estructura del DDDT `T_U_DIS_SIS_IN_16` incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso
MOD_HEALTH <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>1: El módulo está funcionando correctamente.</li> <li>0: El módulo no está funcionando correctamente.</li> </ul>	RO
SAFE_COM_STS <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>1: La comunicación del módulo es válida.</li> <li>0: La comunicación del módulo no es válida.</li> </ul>	RO
PP_STS	BOOL	<ul style="list-style-type: none"> <li>1: La fuente de alimentación de proceso está operativa.</li> <li>0: La fuente de alimentación de proceso no es operativa.</li> </ul>	RO
CONF_LOCKED	BOOL	<ul style="list-style-type: none"> <li>1: La configuración de módulo está bloqueada.</li> <li>0: La configuración de módulo no está bloqueada.</li> </ul>	RO
S_COM_DBG	T_SAFE_COM_DBG_IN	Estructura de depuración para comunicación segura.	RO
CH_IN_A	ARRAY[0-7] de T_U_DIS_SIS_CH_IN	Matriz de estructuras de canal de rango A.	–
CH_IN_B	ARRAY[0-7] de T_U_DIS_SIS_CH_IN	Matriz de estructuras de canal de rango B.	–
MUID <sup>2</sup>	ARRAY[0-3] de DWORD	ID exclusivo del módulo (asignado automáticamente por Control Expert)	RO
RESERVED	ARRAY[0-9] de INT	–	–
<p>1. Cuando la tarea SAFE de la CPU no está en modalidad de ejecución, no se actualizan los datos intercambiados entre la CPU y el módulo, y MOD_HEALTH y SAFE_COM_STS se establecen en 0.</p> <p>2. Este valor generado automáticamente se puede cambiar ejecutando el comando <b>Generar &gt; Renovar ID y Regenerar todo</b> en el menú principal de Control Expert.</p>			

## Estructura T\_SAFE\_COM\_DBG\_IN

La estructura T\_SAFE\_COM\_DBG\_IN incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso
S_COM_EST	BOOL	<ul style="list-style-type: none"> <li>1: Se ha establecido comunicación con el módulo.</li> <li>0: No se ha establecido ni se ha interrumpido la comunicación con el módulo.</li> </ul>	RO
M_NTP_SYNC	BOOL	<p>Con la versión del firmware de la CPU 3.10 o anterior:</p> <ul style="list-style-type: none"> <li>1: El módulo se ha sincronizado con el servidor NTP.</li> <li>0: El módulo no se ha sincronizado con el servidor NTP.</li> </ul> <p><b>NOTA:</b> Con la versión del firmware de la CPU 3.20 o posterior, el valor siempre es 1.</p>	RO
CPU_NTP_SYNC	BOOL	<p>Con la versión del firmware de la CPU 3.10 o anterior:</p> <ul style="list-style-type: none"> <li>1: La CPU se ha sincronizado con el servidor NTP.</li> <li>0: La CPU no se ha sincronizado con el servidor NTP.</li> </ul> <p><b>NOTA:</b> Con la versión del firmware de la CPU 3.20 o posterior, el valor siempre es 1.</p>	RO
CHECKSUM	BYTE	Suma de comprobación de trama de comunicación.	RO
COM_DELAY	UINT	<p>Retardo de comunicación entre dos valores recibidos por el módulo:</p> <ul style="list-style-type: none"> <li>1-65534: El tiempo, en ms, desde que la CPU ha recibido la última comunicación del módulo.</li> <li>65535: La CPU no ha recibido ninguna comunicación del módulo.</li> </ul>	RO
COM_TO	UINT	Valor de timeout de comunicación para las comunicaciones procedentes del módulo.	L/E
STS_MS_IN	UINT	Valor de marca de tiempo segura correspondiente a la fracción de un segundo, redondeado al ms más cercano, de los datos recibidos del módulo.	RO
S_NTP_MS	UINT	Valor de marca de tiempo segura correspondiente a la fracción de un segundo, redondeado al ms más cercano, para el ciclo actual.	RO
STS_S_IN	UDINT	Valor de marca de tiempo segura en segundos de los datos recibidos del módulo.	RO

Elemento	Tipo de datos	Descripción	Acceso
S_NTP_S	UDINT	Valor de tiempo seguro en segundos para el ciclo actual.	RO
CRC_IN	UDINT	Valor de CRC para datos recibidos del módulo.	RO

## Estructura T\_U\_DIS\_SIS\_CH\_IN

La estructura T\_U\_DIS\_SIS\_CH\_IN incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso
CH_HEALTH <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>1: El canal está operativo.</li> <li>0: Se ha detectado un error en el canal, que no está operativo.</li> </ul> <b>Fórmula:</b> CH_HEALTH = not (OC or IC or SC) and SAFE_COM_STS	RO
VALUE <sup>2</sup>	EBOOL	<ul style="list-style-type: none"> <li>1: La entrada está energizada.</li> <li>0: La entrada está deenergizada.</li> </ul> <b>Fórmula:</b> VALUE = if (SAFE_COM_STS and not (IC)) then READ_VALUE else 0	RO
OC	BOOL	<ul style="list-style-type: none"> <li>1: El canal está abierto o cortocircuitado a tierra.</li> <li>0: El canal está conectado y no está cortocircuitado a tierra.</li> </ul>	RO
SC	BOOL	<ul style="list-style-type: none"> <li>1: El canal está cortocircuitado a una fuente de 24 V o está cruzado entre dos canales.</li> <li>0: El canal no está cortocircuitado a una fuente de 24 V ni está cruzado entre dos canales.</li> </ul>	RO
IC	BOOL	<ul style="list-style-type: none"> <li>1: Canal no válido detectado por el módulo.</li> <li>0: El módulo declara que el canal está operativo de forma interna.</li> </ul>	RO
V_OC	BOOL	Estado de la configuración de la prueba de circuito abierto o cortocircuito a tierra: <ul style="list-style-type: none"> <li>1: Habilitado.</li> <li>0: Deshabilitado.</li> </ul>	RO

Elemento	Tipo de datos	Descripción	Acceso
V_SC	BOOL	Estado de la configuración de la prueba de cortocircuito a fuente de 24 V: <ul style="list-style-type: none"><li>• 1: Habilitado.</li><li>• 0: Deshabilitado.</li></ul>	RO
<p>1. Cuando la tarea SAFE de la CPU no está en modalidad de ejecución, no se actualizan los datos intercambiados entre la CPU y el módulo, y CH_HEALTH se establece en 0.</p> <p>2. El elemento VALUE puede tener una marca de tiempo proporcionada por BMX CRA o BME CRA.</p>			

# Módulo de salida digital BMXSDO0802

## Introducción

En esta sección se describe el módulo de salida digital de seguridad BMXSDO0802 M580.

## Módulo de salida digital de seguridad BMXSDO0802

### Introducción

El módulo de salida digital de seguridad BMXSDO0802 presenta las características siguientes:

- 8 salidas de 0,5 A no aisladas galvánicamente.
- Tensión de salida nominal de 24 V CC.
- Logra lo siguiente:
  - SIL3 IEC 61508, SIL CL3 IEC 62061.
  - SIL4 EN5012x.
  - Categoría 4 (Cat4)/Nivel de rendimiento e (PLe) ISO 13849.
- Supervisa la fuente de alimentación del preactuador externa.
- Pantalla de LED de diagnóstico, página 247 que se proporciona para el módulo y para cada canal de salida.
- Se proporcionan automáticamente diagnósticos de cableado de canal que pueden detectar las condiciones siguientes cuando la salida está *energizada*:
  - Corriente de sobrecarga
  - Cortocircuito a la tierra de 0 V CC
- Diagnósticos de cableado de canal (habilitar/deshabilitar) configurables, página 105 que pueden detectar las condiciones siguientes:
  - Cable abierto (o cortado).
- Diagnósticos de cableado de canal (habilitar/deshabilitar) configurables que pueden detectar las condiciones siguientes cuando la salida está *deenergizada*:
  - Cortocircuito a la tierra de 0 V.

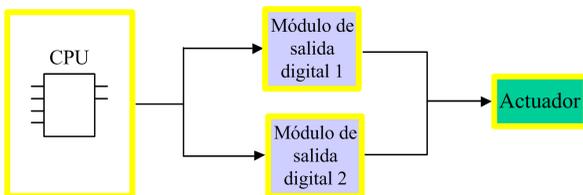
- Diagnósticos de cableado de canal (habilitar/deshabilitar) configurables que pueden detectar las condiciones siguientes cuando la salida está *energizada* o *deenergizada*:
  - Cortocircuito a 24 V CC.
  - Cruces entre dos canales (si se proporciona alimentación al sensor de forma interna).
- Valores de retorno configurables para cada canal que se aplican si se pierde la comunicación entre la CPU y el módulo de salida.
- Intercambio bajo tensión de módulos durante el tiempo de ejecución.
- Módulo CCOTF al operar en modalidad de mantenimiento, página 262. (CCOTF no es compatible con la modalidad de seguridad, página 261).

**NOTA:** Se ejecutará una autoverificación en cada salida para comprobar su capacidad para deenergizarse y alcanzar su estado de seguridad sin que ello afecte de ninguna manera a la carga (pulso de desconexión < 1 ms). Esta autoverificación también se ejecuta, en una salida a la vez, para cada salida con energía con un periodo inferior a 1 segundo. Si la salida está conectada a una entrada estática de un producto, la entrada estática conectada podría detectar este pulso. Para evitar el posible impacto de este pulso en la entrada, un filtro podría resultar de utilidad.

## Alta disponibilidad

Puede conectar la CPU a dos módulos de salida a través del canal negro, luego conectar cada módulo de salida a un solo actuador. No se necesita ningún bloque de funciones, porque la señal de la CPU está conectada los dos canales de salida.

En la figura siguiente se muestra la configuración de salidas digitales redundantes para alta disponibilidad.



El estado de cada módulo de salida se puede leer de los elementos de su estructura de DDDT `T_U_DIS_SIS_OUT_8`, página 111. Puede utilizar estos datos para determinar si es necesario reemplazar un módulo. Si un módulo deja de ser operativo y se debe reemplazar, el sistema continuará funcionando con una configuración conforme a SIL3 mientras se realiza el intercambio de módulos.

Consulte el ejemplo de cableado de salida de alta disponibilidad, página 108 para obtener información detallada sobre este diseño.

# Conector de cableado BMXSDO0802

## Introducción

El módulo de salida BMXSDO0802 digital presenta un único grupo de 8 salidas.

- Los dos pines comunes de fuente de alimentación de +24 V CC (18 y 20) están internamente conectados.
- Todos los pines de 0 V comunes (1, 3, 5, 7, 9, 11, 13, 15, 17 y 19) están internamente conectados.

## Bloques de terminales

Puede utilizar los bloques de terminales de 20 puntos de Schneider Electric siguientes para montar el conector de 20 pines en la parte frontal del módulo:

- Bloque de terminales con tornillo de presión BMXFTB2010
- Bloque de terminales de abrazadera BMXFTB2000
- Bloque de terminales de resorte BMXFTB2020

**NOTA:** Los bloques de terminales se pueden retirar sólo cuando el módulo está apagado.

## Fuente de alimentación de proceso

Se requiere una fuente de alimentación de proceso de sobretensión categoría II de 24 Vcc con protección adicional de bajo voltaje (SELV/PELV). Schneider Electric recomienda una fuente de alimentación que no restablezca automáticamente la alimentación una vez que esta se haya interrumpido.

## Opcional

Se necesita un fusible de acción rápida, 6 A como máximo, para ayudar a proteger la fuente de alimentación externa contra las condiciones de cortocircuito y sobretensión.

## **▲ ATENCIÓN**

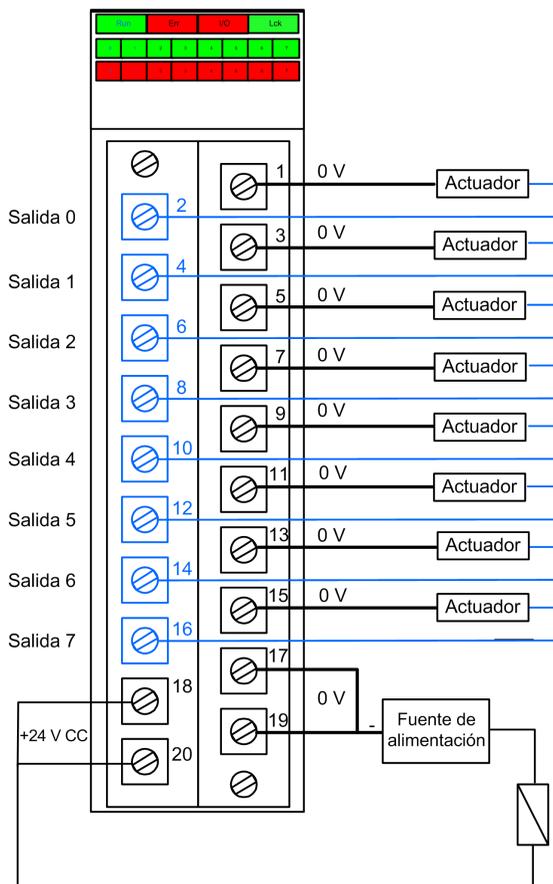
### **SELECCIÓN DE FUSIBLES INCORRECTOS**

Use fusibles de acción rápida para ayudar a proteger los componentes electrónicos del módulo de salida digital frente a una condición de sobrecorriente. La selección incorrecta de fusibles puede provocar daños en el módulo.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

## Pines de conector de cableado

El diagrama de cableado siguiente muestra un módulo de una salida conectado a 8 actuadores:



## Asignación de salidas a pines de conector

A continuación, se ofrece una descripción de cada pin del módulo de salida BMXSDO0802:

Descripción de los pines	Número de pin en el bloque de terminales		Descripción de los pines
Salida 0	2	1	Común 0 V
Salida 1	4	3	Común 0 V
Salida 2	6	5	Común 0 V

Descripción de los pines	Número de pin en el bloque de terminales		Descripción de los pines
Salida 3	8	7	Común 0 V
Salida 4	10	9	Común 0 V
Salida 5	12	11	Común 0 V
Salida 6	14	13	Común 0 V
Salida 7	16	15	Común 0 V
Fuente de alimentación de proceso de 24 V CC	18	17	Común 0 V
Fuente de alimentación de proceso de 24 V CC	20	19	Común 0 V

## Ejemplos de cableado de aplicación de salida BMXSDO0802

### Introducción

Puede conectar el módulo de salida digital de seguridad BMXSDO0802 a actuadores para lograr la conformidad con SIL3 Categoría 4 (Cat4)/Nivel de rendimiento e (PLe) de formas diferentes, en función de sus requisitos de alta disponibilidad.

## ⚠ ATENCIÓN

### RIESGO DE FUNCIONAMIENTO IMPREVISTO

El nivel de integridad de seguridad (SIL) máximo se determina por medio de la calidad del actuador y la duración del intervalo de prueba de comprobación según IEC 61508. Si utiliza actuadores que no cumplen la calidad de la norma de SIL prevista, siempre conecte estos sensores de forma redundante a dos canales.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

Los siguientes ejemplos de cableado de aplicación de salida digital de SIL3 Cat4/PLe se describen a continuación.

- Cat4/PLe:
  - un canal de módulo una salida que controla una variable de proceso. En este diseño se emplea un solo actuador.

- Cat4/PLe con alta disponibilidad:
  - dos módulos de salida redundantes, cada uno provisto de un canal conectado a un actuador independiente, pero que controlan la misma variable de proceso.

## ⚠ ATENCIÓN

### RIESGO DE FUNCIONAMIENTO IMPREVISTO

Cuando el equipo se utiliza en una aplicación de incendios y gases, o cuando el estado de demanda de la salida es energizado:

- Su procedimiento de prueba debe incluir una prueba en la que la detección del cable cortado sea eficaz retirando el bloque de terminales y verificando que se hayan establecido los bits de error correspondientes.
- Verifique la eficacia de la detección del cortocircuito a tierra, ya sea habilitando esta función de diagnóstico **Pulso de prueba a energizado** en la ficha **Configuración** del módulo o implementando otro procedimiento (por ejemplo, estableciendo la salida en 1 y comprobando el diagnóstico, etc.).
- Procure no utilizar los actuadores tipo lámpara, porque su impedancia es muy baja cuando están encendidos, con lo cual existe el riesgo de que se detecte una condición falsa de cortocircuito o sobrecarga.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

## Diagnósticos de cableado configurables en Control Expert

Para el módulo de salida digital de seguridad BMXSDO0802, utilice su página **Configuración** en Control Expert para:

- Habilitar **Detección de cortocircuito a 24 V** para cada canal energizado. Esta prueba realiza los diagnósticos de cableado del actuador siguientes para un canal:
  - Detección de cortocircuito a 24 V CC
  - Detección de cruce entre dos canales de salida
- Habilitar **Detección de cable abierto** para cada uno de los ocho canales, lo cual realiza los siguientes diagnósticos de cableado para el canal pertinente:
  - Detección de cable abierto (o cortado) (es decir, el canal de salida no está conectado al actuador)
  - Detección de cortocircuito del cableado a la tierra de 0 V CC

- Habilitar **Pulso de prueba a energizado** para cada canal de salida. Esta prueba se realiza periódicamente cuando la salida se encuentra en el estado deenergizado y aplica un pulso (duración inferior a 1 ms) a la salida para determinar si puede pasar al estado energizado. Si la corriente supera un umbral de 0,7 A, se notifica que la salida está en una condición de cortocircuito con la tierra de 0 V CC. El periodo de prueba es inferior a 1 s.

## **⚠ ADVERTENCIA**

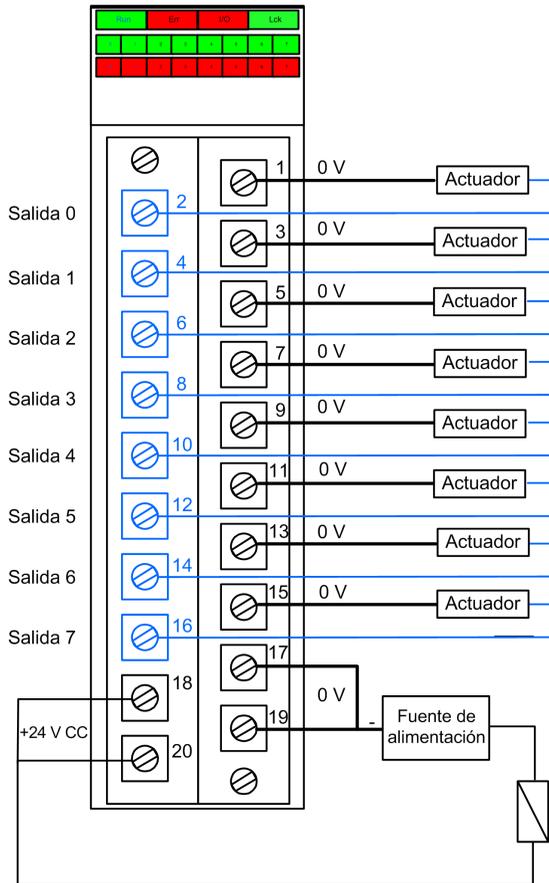
### **RIESGO DE FUNCIONAMIENTO IMPREVISTO**

Schneider Electric recomienda habilitar los diagnósticos disponibles que se proporcionan en Control Expert para detectar y responder a las condiciones enumeradas más arriba. Si una prueba de diagnóstico no está habilitada o no está disponible en Control Expert, deberá aplicar otra medida de seguridad para detectar o excluir estas condiciones.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

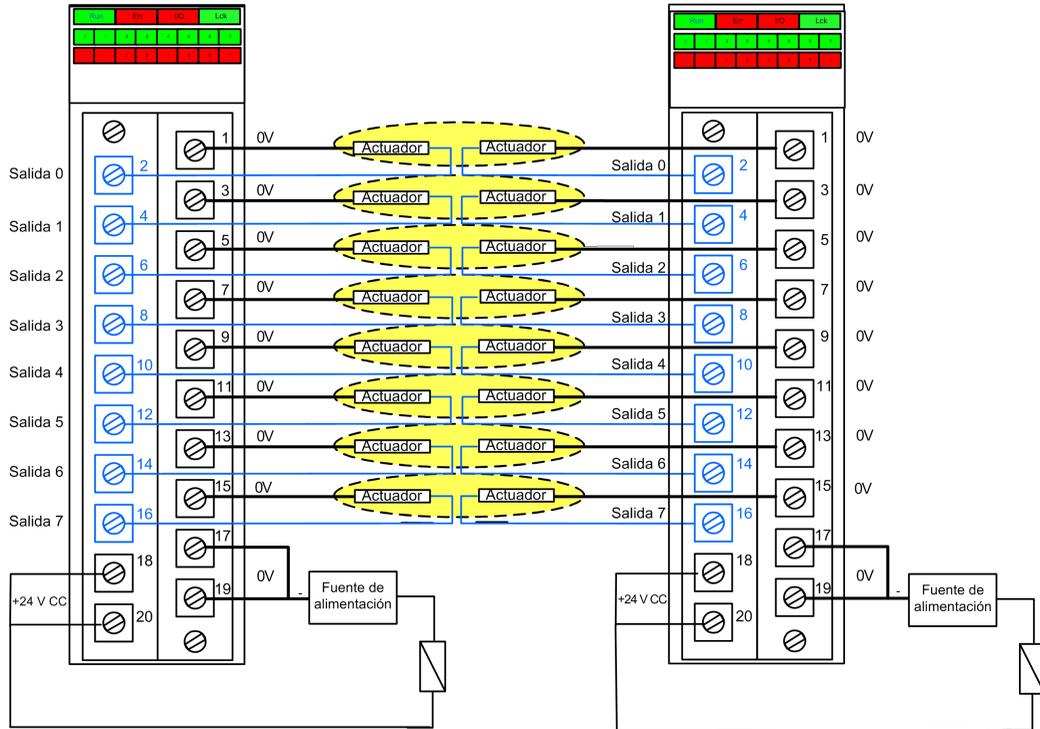
## SIL 3 Cat4/PLe - Ejemplo de módulo de una salida digital

En el ejemplo siguiente se muestra un actuador exclusivo conectado a cada salida en un módulo de una salida. Cada bucle es SIL 3 Cat4/PLe:



## SIL 3 Cat4/PLe - Ejemplo de alta disponibilidad:

En el diagrama de cableado siguiente, dos salidas redundantes ordenan a la misma variable de proceso. Tal como se muestra a continuación, cada salida está conectada a actuadores independientes y cada uno de ellos ejecuta la misma orden, que se envía a través de canales diferentes. Como alternativa, se pueden conectar entre sí las dos salidas redundantes para ordenar al mismo actuador.



## Resumen de diagnóstico de cableado de salida

Los dos diseños proporcionan los diagnósticos de cableado siguientes:

Estado	¿Diagnóstico proporcionado en el estado de salida?	
	Energizado	Deenergizado
Cable abierto (o cortado) <sup>1</sup>	Sí. Se diagnostica en cada ciclo.	Sí. Se diagnostica en cada ciclo.
Salida en sobrecarga <sup>2</sup>	Sí. Se diagnostica en cada ciclo.	No.
Cortocircuito a la tierra de 0 V	Sí. Se diagnostica en cada ciclo.	Sí. Periodo de diagnóstico < 1 s.

Estado	¿Diagnóstico proporcionado en el estado de salida?	
	Energizado	Deenergizado
Cortocircuito a 24 V CC <sup>1</sup>	Sí. Periodo de diagnóstico < 1 s.	Sí. Se diagnostica en cada ciclo.
Cruces entre dos canales	Sí. Periodo de diagnóstico < 1 s.	Sí. Se diagnostica en cada ciclo.
<p>1. Esta función de diagnóstico se realiza si está habilitada en la ficha <b>Configuración</b> del módulo en Control Expert.</p> <p>2. Una vez que se ha resuelto la condición, rearme la salida deenergizándola.</p>		

## ⚠ ADVERTENCIA

### RIESGO DE CORTOCIRCUITO A TIERRA DE 0 V CC

En el caso de la condición de cortocircuito a tierra de 0 V con el estado deenergizado, se recomienda que habilite la opción **Detección de cable abierto** en la ficha **Configuración** del módulo. Como alternativa, deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## ⚠ ADVERTENCIA

### RIESGO DE CORTOCIRCUITO A 24 V CC

En el caso de la condición de cortocircuito a 24 V CC con el estado de salida energizado o deenergizado, se recomienda que habilite la opción **Detección de cortocircuito a 24 V** en la ficha **Configuración** del módulo. Como alternativa, deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## ⚠ ADVERTENCIA

### RIESGO DE CRUCES

El módulo no puede detectar la condición de cruces entre dos canales con el estado de salida deenergizado y el otro canal deenergizado. Deberá aplicar otra medida de seguridad para detectar o excluir esta condición si ocurre cuando el estado de salida cambia a energizado.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

**⚠ ADVERTENCIA****RIESGO DE CRUCES**

En el caso de la condición de cruces entre dos canales con el estado de salida deenergizado y el otro canal energizado, se recomienda que habilite la opción **Detección de cortocircuito a 24 V** en la ficha **Configuración** del módulo. Como alternativa, deberá aplicar otra medida de seguridad para detectar o excluir esta condición cuando el estado de salida cambia a energizado.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

**⚠ ADVERTENCIA****RIESGO DE CRUCES**

El módulo no puede detectar la condición de cruces entre dos canales con el estado de salida energizado y el otro canal deenergizado. Deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

**⚠ ADVERTENCIA****RIESGO DE CRUCES**

En el caso de la condición de cruces entre dos canales con el estado de salida energizado y el otro canal energizado, se recomienda que habilite la opción **Detección de cortocircuito a 24 V** en la ficha **Configuración** del módulo. Como alternativa, deberá aplicar otra medida de seguridad para detectar o excluir esta condición.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## Estructura de datos de BMXSDO0802

### Introducción

El `T_U_DIS_SIS_OUT_8` tipo de datos derivados del dispositivo (DDDT) es la interfaz entre el módulo de salida digital BMXSDO0802 y la aplicación que se ejecuta en la CPU. El DDDT `T_U_DIS_SIS_OUT_8` incorpora los tipos de datos `T_SAFE_COM_DBG_OUT` y `T_U_DIS_SIS_CH_OUT`.

Todas estas estructuras se describen más abajo.

## Estructura del DDDT T\_U\_DIS\_SIS\_OUT\_8

La estructura del DDDT T\_U\_DIS\_SIS\_OUT\_8 incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso
MOD_HEALTH <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>1: El módulo está funcionando correctamente.</li> <li>0: El módulo no está funcionando correctamente.</li> </ul>	RO
SAFE_COM_STS <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>1: La comunicación del módulo es válida.</li> <li>0: La comunicación del módulo no es válida.</li> </ul>	RO
PP_STS	BOOL	<ul style="list-style-type: none"> <li>1: La fuente de alimentación de proceso está operativa.</li> <li>0: La fuente de alimentación de proceso no es operativa.</li> </ul>	RO
CONF_LOCKED	BOOL	<ul style="list-style-type: none"> <li>1: La configuración de módulo está bloqueada.</li> <li>0: La configuración de módulo no está bloqueada.</li> </ul>	RO
S_COM_DBG	T_SAFE_COM_DBG_OUT	Estructura de depuración para comunicación segura.	RO
CH_OUT	ARRAY[0-7] de T_U_DIS_SIS_CH_OUT	Matriz de estructuras de canal	RO
S_TO	UINT	Timeout de seguridad antes de que el módulo pase al estado de retorno.	RO
MUID <sup>2</sup>	ARRAY[0-3] de DWORD	ID exclusivo del módulo (asignado automáticamente por Control Expert)	RO
RESERVED_1	ARRAY[0-8] de INT	–	–
RESERVED_2	ARRAY[0-6] de INT	–	–
<p>1. Cuando la tarea SAFE de la CPU no está en modalidad de ejecución, no se actualizan los datos intercambiados entre la CPU y el módulo, y MOD_HEALTH y SAFE_COM_STS se establecen en 0.</p> <p>2. Este valor generado automáticamente se puede cambiar ejecutando el comando <b>Generar &gt; Renovar ID y Regenerar todo</b> en el menú principal de Control Expert.</p>			

## Estructura T\_SAFE\_COM\_DBG\_OUT

La estructura T\_SAFE\_COM\_DBG\_OUT incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso
S_COM_EST	BOOL	<ul style="list-style-type: none"> <li>1: Se ha establecido comunicación con el módulo.</li> <li>0: No se ha establecido ni se ha interrumpido la comunicación con el módulo.</li> </ul>	RO
M_NTP_SYNC	BOOL	<p>Con la versión del firmware de la CPU 3.10 o anterior:</p> <ul style="list-style-type: none"> <li>1: El módulo se ha sincronizado con el servidor NTP.</li> <li>0: El módulo no se ha sincronizado con el servidor NTP.</li> </ul> <p><b>NOTA:</b> Con la versión del firmware de la CPU 3.20 o posterior, el valor siempre es 1.</p>	RO
CPU_NTP_SYNC	BOOL	<p>Con la versión del firmware de la CPU 3.10 o anterior:</p> <ul style="list-style-type: none"> <li>1: La CPU se ha sincronizado con el servidor NTP.</li> <li>0: La CPU no se ha sincronizado con el servidor NTP.</li> </ul> <p><b>NOTA:</b> Con la versión del firmware de la CPU 3.20 o posterior, el valor siempre es 1.</p>	RO
CHECKSUM	BYTE	Suma de comprobación de trama de comunicación.	RO
COM_DELAY	UINT	<p>Retardo de comunicación entre dos valores recibidos por el módulo:</p> <ul style="list-style-type: none"> <li>1-65534: El tiempo, en ms, desde que la CPU ha recibido la última comunicación del módulo.</li> <li>65535: La CPU no ha recibido ninguna comunicación del módulo.</li> </ul>	RO
COM_TO	UINT	Valor de timeout de comunicación para las comunicaciones procedentes del módulo.	L/E
STS_MS_IN	UINT	Valor de marca de tiempo segura correspondiente a la fracción de un segundo, redondeado al ms más cercano, de los datos recibidos del módulo.	RO
S_NTP_MS	UINT	Valor de marca de tiempo segura correspondiente a la fracción de un segundo, redondeado al ms más cercano, para el ciclo actual.	RO

Elemento	Tipo de datos	Descripción	Acceso
STS_S_IN	UDINT	Valor de marca de tiempo segura en segundos de los datos recibidos del módulo.	RO
S_NTP_S	UDINT	Valor de tiempo seguro en segundos para el ciclo actual.	RO
CRC_IN	UDINT	Valor de CRC para datos recibidos del módulo.	RO
STS_MS_OUT	UINT	Valor de marca de tiempo segura correspondiente a la fracción de un segundo, redondeado al ms más cercano, de los datos que se van a enviar al módulo.	RO
STS_S_OUT	UDINT	Valor de marca de tiempo segura en segundos de los datos que se van a enviar al módulo.	RO
CRC_OUT	UDINT	Valor de CRC para datos que se van a enviar al módulo.	RO

## Estructura T\_U\_DIS\_SIS\_CH\_OUT

La estructura T\_U\_DIS\_SIS\_CH\_OUT incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso
CH_HEALTH <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>1: El canal está operativo.</li> <li>0: Se ha detectado un error en el canal, que no está operativo.</li> </ul> <p><b>Fórmula:</b></p> <p>CH_HEALTH = not (SC or OL or IC or OC) and SAFE_COM_STS and not (módulo en estado de retorno)</p>	RO
VALUE	EBOOL	<p>Comando seguro de canal de salida:</p> <ul style="list-style-type: none"> <li>1: Ordenar el cierre de la salida (energizada).</li> <li>0: Ordenar la apertura de la salida (deenergizada).</li> </ul>	L/E
TRUE_VALUE <sup>2</sup>	BOOL	<p>Valor de relectura del canal de relé de salida:</p> <ul style="list-style-type: none"> <li>1: La salida está cerrada (energizada).</li> <li>0: La salida está abierta (deenergizada).</li> </ul>	RO
OC	BOOL	<ul style="list-style-type: none"> <li>1: El canal está abierto o cortocircuitado a tierra.</li> </ul>	RO

Elemento	Tipo de datos	Descripción	Acceso
		<ul style="list-style-type: none"> <li>0: El canal está conectado y no está cortocircuitado a tierra.</li> </ul>	
SC	BOOL	<ul style="list-style-type: none"> <li>1: El canal está cortocircuitado a una fuente de 24 V o está cruzado con otro canal.</li> <li>0: El canal no está cortocircuitado a una fuente de 24 V ni está cruzado.</li> </ul>	RO
OL	BOOL	<ul style="list-style-type: none"> <li>1: El canal está sobrecargado o cortocircuitado a 0 V.</li> <li>0: El canal no está sobrecargado ni cortocircuitado a 0 V.</li> </ul>	RO
IC	BOOL	<ul style="list-style-type: none"> <li>1: Canal no válido detectado por el módulo.</li> <li>0: El módulo declara que el canal está operativo de forma interna.</li> </ul>	RO
V_OC	BOOL	<p>Estado de la configuración de la prueba de circuito abierto:</p> <ul style="list-style-type: none"> <li>1: Habilitado.</li> <li>0: Deshabilitado.</li> </ul>	RO
V_SC	BOOL	<p>Estado de la configuración de la prueba de cortocircuito a fuente de 24 V:</p> <ul style="list-style-type: none"> <li>1: Habilitado.</li> <li>0: Deshabilitado.</li> </ul>	RO
V_PULSE_ON	BOOL	<p>Estado de la configuración de la prueba del pulso a energizado:</p> <ul style="list-style-type: none"> <li>1: Habilitado.</li> <li>0: Deshabilitado.</li> </ul>	RO
CH_FBC	BOOL	<p>Configuración del ajuste de retorno del canal:</p> <ul style="list-style-type: none"> <li>1: Valor definido por el usuario.</li> <li>0: Mantener último valor.</li> </ul>	RO
CH_FBST	BOOL	<p>Configuración del estado de retorno del canal cuando se seleccionan valores definidos por el usuario:</p> <ul style="list-style-type: none"> <li>1: Energizado</li> <li>0: Deenergizado</li> </ul>	RO
<p>1. Cuando la tarea SAFE de la CPU no está en modalidad de ejecución, no se actualizan los datos intercambiados entre la CPU y el módulo, y CH_HEALTH se establece en 0.</p> <p>2. El elemento TRUE_VALUE puede tener una marca de tiempo con BMX CRA o BME CRA.</p>			

# Módulo de salida de relé digital BMXSRA0405

## Introducción

En esta sección se describe el módulo de salida relé digital de seguridad BMXSRA0405 M580.

## Módulo de salida de relé digital de seguridad BMXSRA0405

### Introducción

El módulo de salida de relé digital de seguridad BMXSRA0405 presenta las características siguientes:

- 4 salidas de relé con corriente de 5 A.
- Tensión de salida nominal de 24 V CC y de 24 a 230 V CA (categoría de sobretensión II).
- Logra una evaluación de hasta SIL4 (EN5012x) / SIL3 (IEC61508) Categoría 4 (Cat4) / Nivel de rendimiento e (PLe).
- Compatibilidad con 8 selecciones de configuración de cableado de aplicación predefinida.
- Supervisión de autoprueba automática configurable de la capacidad de relé para ejecutar el estado de salida ordenado (en función de la configuración de cableado de aplicación seleccionada).
- Ajustes del módulo configurables para modalidad de retorno y timeout de retorno (en ms).
- Pantalla de LED de diagnóstico, página 252 que se proporciona para el módulo y para cada canal de salida.
- Intercambio bajo tensión de módulos durante el tiempo de ejecución.
- Módulo CCOTF al operar en modalidad de mantenimiento, página 262. (CCOTF no es compatible con la modalidad de seguridad, página 261).

# Conector de cableado BMXSRA0405

## Introducción

El módulo de salida de relé digital BMXSRA0405 incluye 4 relés y admite hasta 4 salidas. El módulo presenta un par de pines *a* y *b* para cada relé. Observe que por cada relé:

- los dos pines *a* estén conectados internamente, y
- los dos pines *b* también estén conectados internamente.

## Bloques de terminales

Puede utilizar los bloques de terminales de 20 puntos de Schneider Electric siguientes para montar el conector de 20 pines en la parte frontal del módulo:

- Bloque de terminales con tornillo de presión BMXFTB2010
- Bloque de terminales de abrazadera BMXFTB2000
- Bloque de terminales de resorte BMXFTB2020

**NOTA:** Los bloques de terminales se pueden retirar sólo cuando el módulo está apagado.

## Fuente de alimentación de proceso

Debe instalar la fuente de alimentación de proceso 24 V CC o 24 V CA a 230 V CA.

## Opcional

Se necesita un fusible de acción rápida, 6 A como máximo, que es adecuado para el diseño de aplicación y relé seleccionado. Instale siempre un fusible externo en serie con la fuente de alimentación externa, el relé y la carga.

### **⚠ ADVERTENCIA**

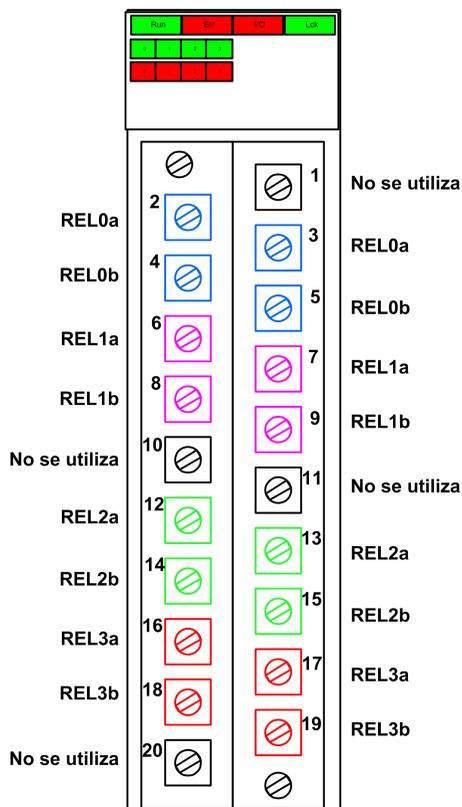
#### **RIESGO DE FUNCIONAMIENTO IMPREVISTO**

Es su responsabilidad implementar diagnósticos de cableado adecuados para detectar y evitar que se produzcan fallos peligrosos en el cableado externo.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## Conector de cableado

En el ejemplo siguiente se presentan los pines del módulo de relé.



## Asignación de entradas a pines de conector

A continuación, se ofrece una descripción de cada pin del módulo de salida de relé digital BMXSRA0405:

Descripción de los pines	Número de pin en el bloque de terminales		Descripción de los pines
Contacto NA, relé 0a	2	1	No se utiliza
Contacto NA, relé 0b	4	3	Contacto NA, relé 0a
Contacto NA, relé 1a	6	5	Contacto NA, relé 0b
Contacto NA, relé 1b	8	7	Contacto NA, relé 1a

Descripción de los pines	Número de pin en el bloque de terminales		Descripción de los pines
No se utiliza	10	9	Contacto NA, relé 1b
Contacto NA, relé 2a	12	11	No se utiliza
Contacto NA, relé 2b	14	13	Contacto NA, relé 2a
Contacto NA, relé 3a	16	15	Contacto NA, relé 2b
Contacto NA, relé 3b	18	17	Contacto NA, relé 3a
No se utiliza	20	19	Contacto NA, relé 3b

**NOTA:** Puesto que los dos pines *a* de cada relé están conectados internamente, sólo debe utilizar un pin *a* para cada relé. De igual forma, puesto que los dos pines *b* de cada relé están conectados internamente, sólo debe utilizar un pin *b* para cada relé.

## Ejemplos de cableado de aplicación de salida BMXSRA0405

### Introducción

Puede configurar el módulo de relé de salida digital de seguridad BMXSRA0405 para lograr la conformidad con SIL2 Categoría 2 (Cat2)/Nivel de rendimiento c (PLc) o SIL3 Cat4/PLe de diferentes formas, según:

- el número de salidas que admitirá el módulo, y
- cómo desea comprobar la capacidad del módulo de poner el actuador en el estado de demanda previsto, ya sea:
  - automáticamente por medio del módulo (en este caso, no hay transición de estado para el actuador) o bien
  - mediante un procedimiento que realice y compruebe una transición diaria de la señal del módulo al actuador (en este caso, la transición afecta al estado del actuador).

Realice esta configuración seleccionando un número de aplicación (que se describe en las tablas más abajo) en la lista **Función** de la ficha **Configuración** del módulo en Control Expert.

Aplicaciones de diseño de cableado SIL2 Cat2/PLc:

Función	Estado de demanda	Relés	Salidas	¿Prueba de señal?		Diagrama de cableado (consulte más abajo)
				¿Prueba de señal automática?¹	¿Transición de señal diaria?	
Aplicación_1	Deenergizado	1	4	Sin	Sí	A
Aplicación_2	Deenergizado	2	2	Sí	Sin	B
Aplicación_3	Energizado	1	4	Sin	Sí	A
Aplicación_4	Energizado	2	2	Sí	Sin	C

1. La prueba de señal automática no afecta al estado del actuador.

### Aplicaciones de diseño de cableado SIL3 Cat4/PLc:

Función	Estado de demanda	Relés	Salidas	¿Prueba de señal?		Diagrama de cableado (consulte más abajo)
				¿Prueba de señal automática?¹	¿Transición de señal diaria?	
Aplicación_5	Deenergizado	2	2	Sin	Sí	C
Aplicación_6	Deenergizado	4	1	Sí	Sin	D
Aplicación_7	Energizado	2	2	Sin	Sí	C
Aplicación_8	Energizado	2	2	Sí	Sin	C

1. La prueba de señal automática no afecta al estado del actuador.

Cada una de estas ocho selecciones de aplicación se describen en los ejemplos de cableado siguientes.

## Aplicación\_1: 4 salidas, SIL2/Cat2/PLc, estado deenergizado, no hay prueba de señal automática

El estado de demanda para este diseño de aplicación es deenergizado. Si el módulo detecta un error interno para una salida, deenergizará esa salida.

## ▲ ATENCIÓN

### PÉRDIDA DE CAPACIDAD PARA EJECUTAR FUNCIONES DE SEGURIDAD

Para lograr SIL2 conforme a IEC 61508 y Categoría 2/Nivel de rendimiento c según ISO 13849 mediante este diseño de cableado, debe realizar una transición de señal diaria del estado energizado al estado deenergizado.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

Consulte el diagrama de cableado A, página 124 más abajo para obtener una representación del diseño de cableado de Aplicación\_1.

## Aplicación\_2: 2 salidas, SIL2 Cat2/PLc, estado deenergizado, prueba de señal automática

El estado de demanda para este diseño de aplicación es deenergizado. Si el módulo detecta un error de salida interno en una de los relés que se utilizan para una salida, deenergizará los dos relés (relé 0 y relé 1 o relé 2 y relé 3) para esa salida.

Su programa de aplicación debe ordenar el mismo estado de salida a todos los relés que activan el mismo actuador.

El módulo realiza secuencialmente una prueba de pulso periódica automática en cada relé. La duración de la prueba es inferior a 50 ms. Debido a la configuración de los dos relés utilizados (en paralelo), la prueba no afectará a la carga de salida (normalmente *energizada*). Puede configurar la frecuencia de la prueba estableciendo el **periodo de supervisión** en la ficha **Configuración** del módulo. Los valores de frecuencia de prueba están comprendidos entre 1 y 1440 minutos.

Consulte el diagrama de cableado B, página 125 más abajo para obtener una representación del diseño de cableado de Aplicación\_2.

## Aplicación\_3: 4 salidas, SIL2/Cat2/PLc, estado energizado, no hay prueba de señal automática

El estado de demanda para este diseño de aplicación es energizado. Si el módulo detecta un error interno para una salida, deenergizará esa salida, que es el estado de seguridad.

## ▲ ATENCIÓN

### **PÉRDIDA DE CAPACIDAD PARA EJECUTAR FUNCIONES DE SEGURIDAD**

Para lograr SIL2 conforme a IEC 61508 y Categoría 2/Nivel de rendimiento c según ISO 13849 mediante este diseño de cableado, debe realizar una transición de señal diaria del estado energizado al estado deenergizado.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

Consulte el diagrama de cableado A, página 124 más abajo, para obtener una representación del diseño de cableado de Aplicación\_3.

## **Aplicación\_4: 2 salidas, SIL2 Cat2/PLc, estado energizado, prueba de señal automática**

El estado de demanda para este diseño de aplicación es energizado. Si el módulo detecta un error de salida interno en una de los relés que se utilizan para una salida, deenergizará los dos relés (relé 0 y relé 1 o relé 2 y relé 3) para esa salida.

Su programa de aplicación debe ordenar el mismo estado de salida a todos los relés que activan el mismo actuador.

El módulo realiza secuencialmente una prueba de pulso periódica en cada relé. La duración de la prueba es inferior a 50 ms. Debido a la configuración de los dos relés utilizados (en paralelo), la prueba no afectará a la carga de salida (normalmente *energizada*). Puede configurar la frecuencia de la prueba estableciendo el **periodo de supervisión** en la ficha **Configuración** del módulo. Los valores de frecuencia de prueba están comprendidos entre 1 y 1440 minutos.

Consulte el diagrama de cableado C, página 126 más abajo para obtener una representación del diseño de cableado de Aplicación\_4.

## **Aplicación\_5: 2 salidas, SIL3/Cat4/PLe, estado deenergizado, no hay prueba de señal automática**

El estado de demanda para este diseño de aplicación es deenergizado. Si el módulo detecta un error de salida interno en una de los relés que se utilizan para una salida, deenergizará los dos relés (relé 0 y relé 1 o relé 2 y relé 3) para esa salida.

Su programa de aplicación debe ordenar el mismo estado de salida a todos los relés que activan el mismo actuador.

## ▲ ATENCIÓN

### PÉRDIDA DE CAPACIDAD PARA EJECUTAR FUNCIONES DE SEGURIDAD

Para lograr SIL3 conforme a IEC 61508 y Categoría 4/Nivel de rendimiento e según ISO 13849 mediante este diseño de cableado, debe realizar una transición de señal diaria del estado energizado al estado deenergizado.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

Consulte el diagrama de cableado C, página 126 más abajo para obtener una representación del diseño de cableado de Aplicación\_5.

## Aplicación\_6: 1 salida, SIL3/Cat4/PLe, estado deenergizado, prueba de señal automática

El estado de demanda para este diseño de aplicación es deenergizado. Si el módulo detecta un error de salida interno en uno de los relés que se utilizan para una salida, deenergizará todos los relés (relé 0 y relé 1 o relé 2 y relé 3) del módulo.

Su programa de aplicación debe ordenar el mismo estado de salida a todos los relés que activan el mismo actuador.

El módulo realiza secuencialmente una prueba de pulso periódica en cada relé. La duración de la prueba es inferior a 50 ms. Debido a la configuración de los cuatro relés utilizados (2 pares de relés en serie puestos en paralelo), la prueba no afectará a la carga de salida (normalmente *energizada*). Puede configurar la frecuencia de la prueba estableciendo el **periodo de supervisión** en la ficha **Configuración** del módulo. Los valores de frecuencia de prueba están comprendidos entre 1 y 1440 minutos.

Consulte el diagrama de cableado D, página 127 más abajo para obtener una representación del diseño de cableado de Aplicación\_6.

## Aplicación\_7: 2 salidas, SIL3/Cat4/PLe, estado deenergizado, no hay prueba de señal automática

El estado de demanda para este diseño de aplicación es energizado. Si el módulo detecta un error de salida interno en una de los relés que se utilizan para una salida, deenergizará los dos relés (relé 0 y relé 1 o relé 2 y relé 3) para esa salida.

Su programa de aplicación debe ordenar el mismo estado de salida a todos los relés que activan el mismo actuador.

## ▲ ATENCIÓN

### **PÉRDIDA DE CAPACIDAD PARA EJECUTAR FUNCIONES DE SEGURIDAD**

Para lograr SIL3 conforme a IEC 61508 y Categoría 4/Nivel de rendimiento e según ISO 13849 mediante este diseño de cableado, debe realizar una transición de señal diaria del estado energizado al estado deenergizado.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

Consulte el [diagrama de cableado C](#), página 126 más abajo para obtener una representación del diseño de cableado de Aplicación\_7.

## **Aplicación\_8: 2 salidas, SIL3/Cat4/PLe, estado energizado, prueba de señal automática**

El estado de demanda para este diseño de aplicación es energizado. Si el módulo detecta un error de salida interno en una de los relés que se utilizan para una salida, deenergizará los dos relés (relé 0 y relé 1 o relé 2 y relé 3) para esa salida.

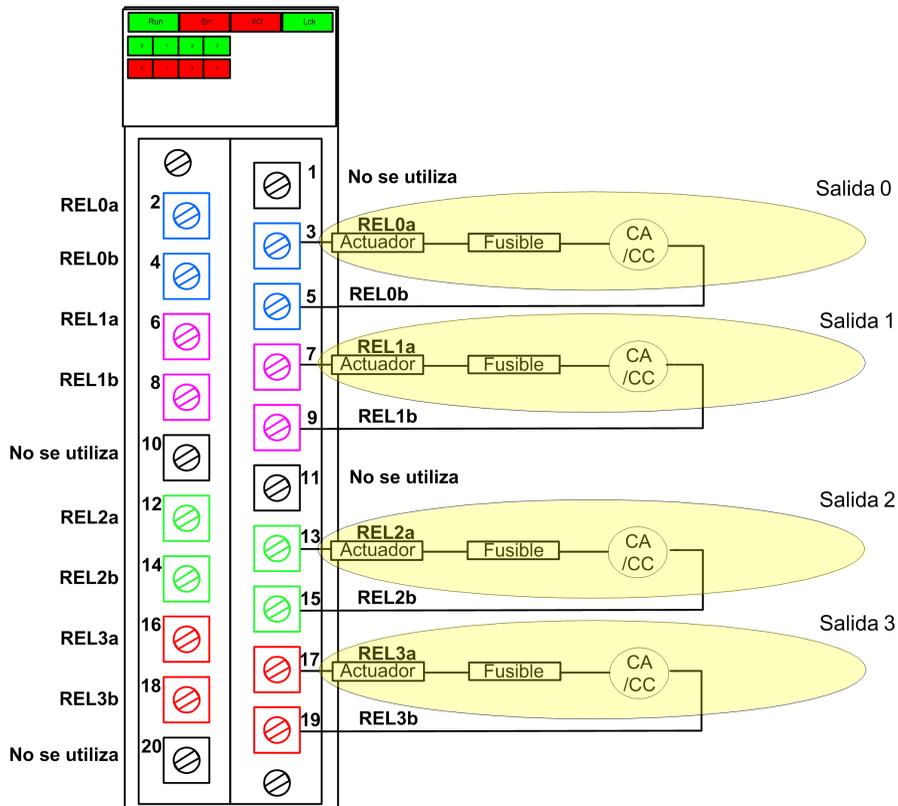
Su programa de aplicación debe ordenar el mismo estado de salida a todos los relés que activan el mismo actuador.

El módulo realiza secuencialmente una prueba de pulso periódica en cada relé. La duración de la prueba es inferior a 50 ms. Debido a la configuración de los dos relés utilizados (en serie), la prueba no afectará a la carga de salida (normalmente *deenergizada*). Puede configurar la frecuencia de la prueba estableciendo el **periodo de supervisión** en la ficha **Configuración** del módulo. Los valores de frecuencia de prueba están comprendidos entre 1 y 1440 minutos.

Consulte el [diagrama de cableado C](#), página 126 más abajo para obtener una representación del diseño de cableado de Aplicación\_8.

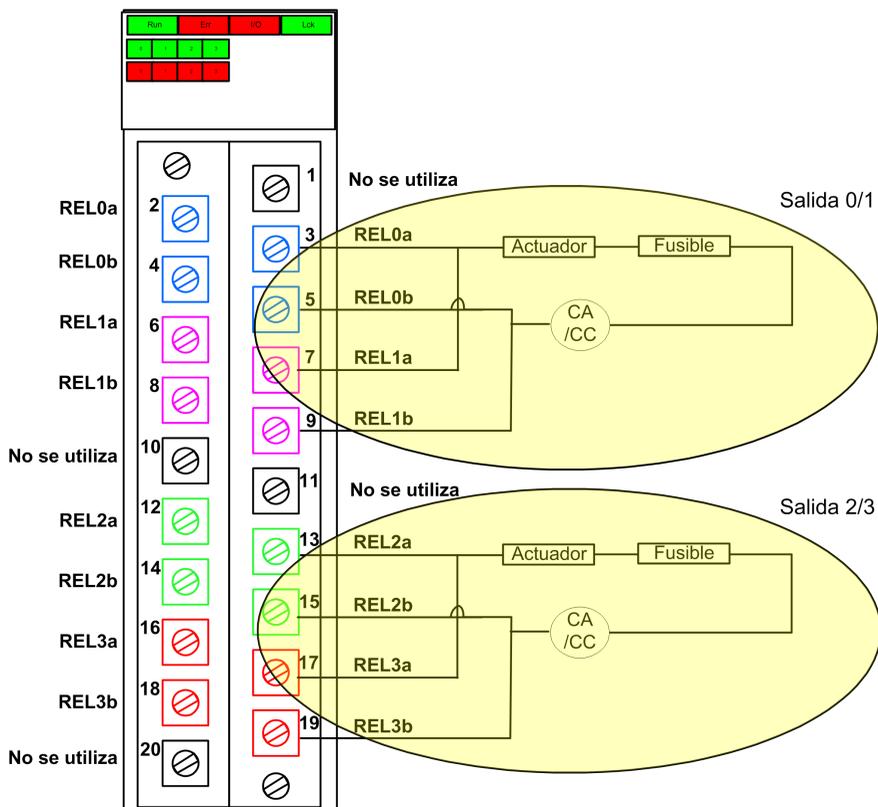
## Diagrama de cableado A

El diagrama de cableado se aplica a Aplicación\_1 y Aplicación\_3:



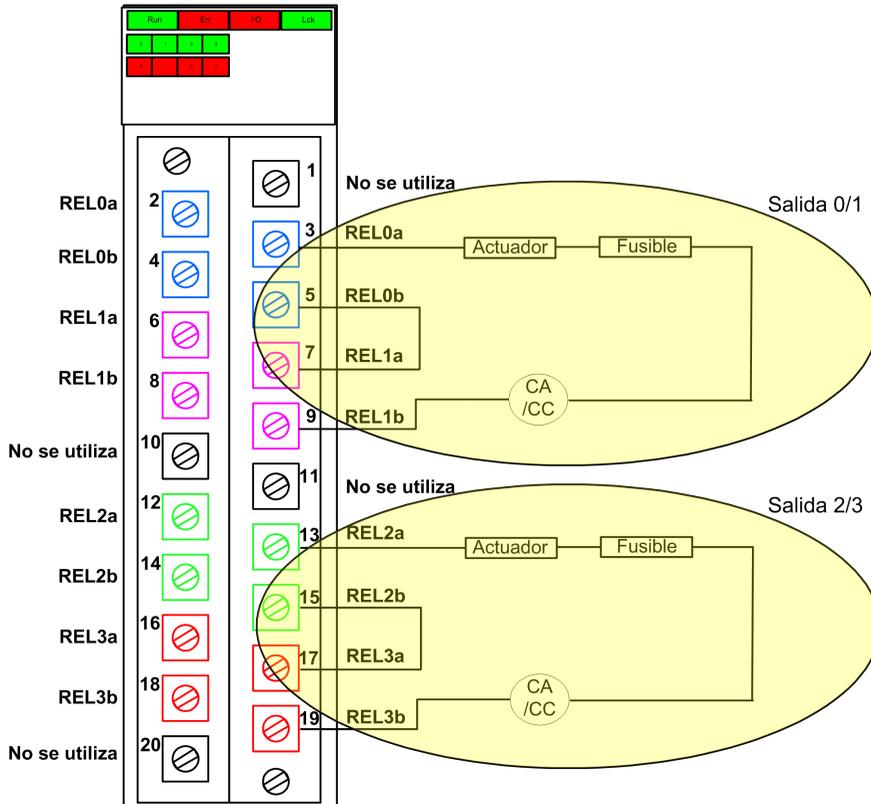
## Diagrama de cableado B

Este diagrama de cableado se aplica a Aplicación\_2:



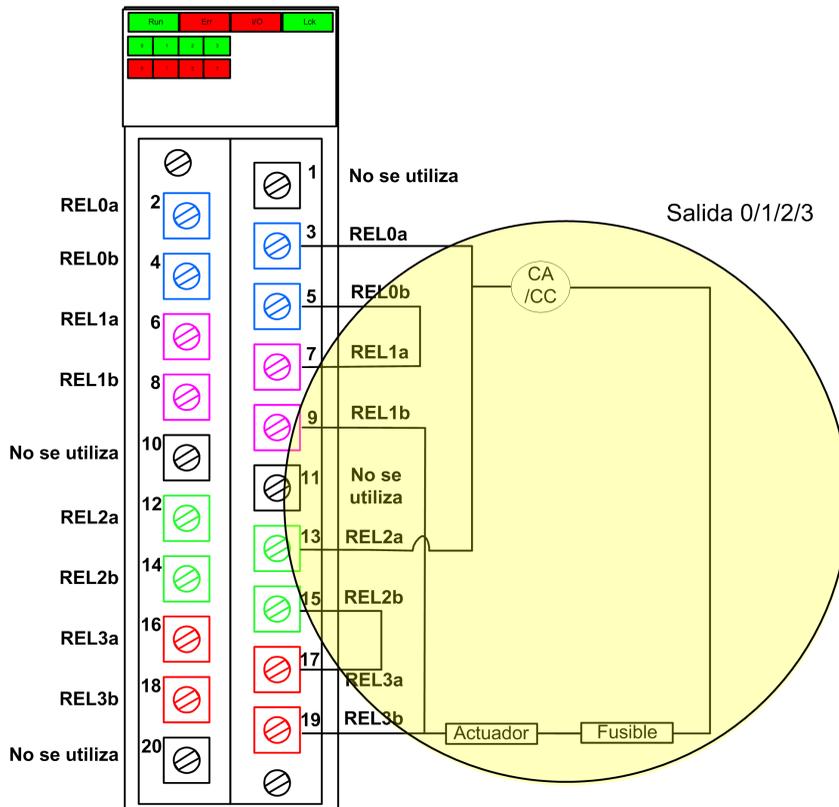
## Diagrama de cableado C

Este diagrama de cableado se aplica a Aplicación\_4, Aplicación\_5, Aplicación\_7 y Aplicación\_8:



## Diagrama de cableado D

Este diagrama de cableado se aplica a Aplicación\_6:



## Estructura de datos de BMXSRA0405

### Introducción

El tipo de datos derivados del dispositivo (DDDT) `T_U_DIS_SIS_OUT_4` es la interfaz entre el módulo de salida del relé BMXSRA0405 y la aplicación que se ejecuta en la CPU. El DDDT `T_U_DIS_SIS_OUT_4` incorpora los tipos de datos `T_SAFE_COM_DBG_OUT` y `T_U_DIS_SIS_CH_ROUT`.

Todas estas estructuras se describen más abajo.

## Estructura del DDDT T\_U\_DIS\_SIS\_OUT\_4

La estructura del DDDT T\_U\_DIS\_SIS\_OUT\_4 incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso
MOD_HEALTH <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>• 1: El módulo está funcionando correctamente.</li> <li>• 0: El módulo no está funcionando correctamente.</li> </ul>	RO
SAFE_COM_STS <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>• 1: La comunicación del módulo es válida.</li> <li>• 0: La comunicación del módulo no es válida.</li> </ul>	RO
CONF_LOCKED	BOOL	<ul style="list-style-type: none"> <li>• 1: La configuración de módulo está bloqueada.</li> <li>• 0: La configuración de módulo no está bloqueada.</li> </ul>	RO
APPLI	UINT	Configuración de aplicación de relé: 1, 2, 3, 4, 5, 6 o 7.	RO
TIME_PERIOD	UINT	Periodo del temporizador para la supervisión automática de relé (en minutos).	RO
S_COM_DBG	T_SAFE_COM_DBG_OUT	Estructura de depuración para comunicación segura.	RO
CH_OUT	ARRAY[0-3] de T_U_DIS_SIS_CH_ROUT	Matriz de estructuras de canal	–
S_TO	UINT	Timeout de seguridad antes de que el módulo pase al estado de retorno.	RO
MUID <sup>2</sup>	ARRAY[0-3] de DWORD	ID exclusivo del módulo (asignado automáticamente por Control Expert)	RO
RESERVED_1	ARRAY[0-7] de INT	–	–
RESERVED_2	ARRAY[0-6] de INT	–	–
<p>1. Cuando la tarea SAFE de la CPU no está en modalidad de ejecución, no se actualizan los datos intercambiados entre la CPU y el módulo, y MOD_HEALTH y SAFE_COM_STS se establecen en 0.</p> <p>2. Este valor generado automáticamente se puede cambiar ejecutando el comando <b>Generar &gt; Renovar ID y Regenerar todo</b> en el menú principal de Control Expert.</p>			

## Estructura T\_SAFE\_COM\_DBG\_OUT

La estructura T\_SAFE\_COM\_DBG\_OUT incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso
S_COM_EST	BOOL	<ul style="list-style-type: none"> <li>1: Se ha establecido comunicación con el módulo.</li> <li>0: No se ha establecido ni se ha interrumpido la comunicación con el módulo.</li> </ul>	RO
M_NTP_SYNC	BOOL	<p>Con la versión del firmware de la CPU 3.10 o anterior:</p> <ul style="list-style-type: none"> <li>1: El módulo se ha sincronizado con el servidor NTP.</li> <li>0: El módulo no se ha sincronizado con el servidor NTP.</li> </ul> <p><b>NOTA:</b> Con la versión del firmware de la CPU 3.20 o posterior, el valor siempre es 1.</p>	RO
CPU_NTP_SYNC	BOOL	<p>Con la versión del firmware de la CPU 3.10 o anterior:</p> <ul style="list-style-type: none"> <li>1: La CPU se ha sincronizado con el servidor NTP.</li> <li>0: La CPU no se ha sincronizado con el servidor NTP.</li> </ul> <p><b>NOTA:</b> Con la versión del firmware de la CPU 3.20 o posterior, el valor siempre es 1.</p>	RO
CHECKSUM	BYTE	Suma de comprobación de trama de comunicación.	RO
COM_DELAY	UINT	<p>Retardo de comunicación entre dos valores recibidos por el módulo:</p> <ul style="list-style-type: none"> <li>1-65534: El tiempo, en ms, desde que la CPU ha recibido la última comunicación del módulo.</li> <li>65535: La CPU no ha recibido ninguna comunicación del módulo.</li> </ul>	RO
COM_TO	UINT	Valor de timeout de comunicación para las comunicaciones procedentes del módulo.	L/E
STS_MS_IN	UINT	Valor de marca de tiempo segura correspondiente a la fracción de un segundo, redondeado al ms más cercano, de los datos recibidos del módulo.	RO
S_NTP_MS	UINT	Valor de marca de tiempo segura correspondiente a la fracción de un segundo, redondeado al ms más cercano, para el ciclo actual.	RO
STS_S_IN	UDINT	Valor de marca de tiempo segura en segundos de los datos recibidos del módulo.	RO

Elemento	Tipo de datos	Descripción	Acceso
S_NTP_S	UDINT	Valor de tiempo seguro en segundos para el ciclo actual.	RO
CRC_IN	UDINT	Valor de CRC para datos recibidos del módulo.	RO
STS_MS_OUT	UINT	Valor de marca de tiempo segura correspondiente a la fracción de un segundo, redondeado al ms más cercano, de los datos que se van a enviar al módulo.	RO
STS_S_OUT	UDINT	Valor de marca de tiempo segura en segundos de los datos que se van a enviar al módulo.	RO
CRC_OUT	UDINT	Valor de CRC para datos que se van a enviar al módulo.	RO

## Estructura T\_U\_DIS\_SIS\_CH\_ROUT

La estructura T\_U\_DIS\_SIS\_CH\_ROUT incluye los elementos siguientes:

Elemento	Tipo de datos	Descripción	Acceso
CH_HEALTH <sup>1</sup>	BOOL	<ul style="list-style-type: none"> <li>1: El canal está operativo.</li> <li>0: Se ha detectado un error en el canal, que no está operativo.</li> </ul> <p><b>Fórmula:</b></p> <p>CH_HEALTH = not (IC) and SAFE_COM_STS and not (módulo en estado de retorno)</p>	RO
VALUE	EBOOL	Comando seguro de canal de salida: <ul style="list-style-type: none"> <li>1: Ordenar el cierre de la salida (energizada).</li> <li>0: Ordenar la apertura de la salida (deenergizada).</li> </ul>	L/E
TRUE_VALUE <sup>2</sup>	BOOL	Valor de relectura del canal de salida de relé: <ul style="list-style-type: none"> <li>1: La salida está cerrada (energizada).</li> <li>0: La salida está abierta (deenergizada).</li> </ul>	RO
IC	BOOL	<ul style="list-style-type: none"> <li>1: Canal no válido detectado por el módulo.</li> <li>0: El módulo declara que el canal está operativo de forma interna.</li> </ul>	RO

<b>Elemento</b>	<b>Tipo de datos</b>	<b>Descripción</b>	<b>Acceso</b>
CH_FBC	BOOL	Configuración del ajuste de retorno del canal: <ul style="list-style-type: none"><li>• 1: Valor definido por el usuario.</li><li>• 0: Mantener último valor.</li></ul>	RO
CH_FBST	BOOL	Configuración del estado de retorno del canal cuando se seleccionan valores definidos por el usuario: <ul style="list-style-type: none"><li>• 1: Energizado</li><li>• 0: Deenergizado</li></ul>	RO
<p>1. Cuando la tarea SAFE de la CPU no está en modalidad de ejecución, no se actualizan los datos intercambiados entre la CPU y el módulo, y CH_HEALTH se establece en 0.</p> <p>2. El elemento TRUE_VALUE puede tener una marca de tiempo con BMX CRA o BME CRA.</p>			

# Fuentes de alimentación de seguridad de M580

## Contenido de este capítulo

Fuentes de alimentación de seguridad de M580.....	133
Diagnósticos del módulo de alimentación de seguridad M580 .....	136
DDT de seguridad de M580 .....	138

## Introducción

En este capítulo se describen los módulos de alimentación de seguridad M580.

# Fuentes de alimentación de seguridad de M580

## Introducción

Las fuentes de alimentación de seguridad siguientes se pueden utilizar con el PAC de seguridad M580

- Fuente de alimentación de seguridad redundante de 100 a 240 V CA de BMXCPS4002S
- Fuente de alimentación de seguridad de alta potencia redundante de 24/48 V CC de BMXCPS4022S
- Fuente de alimentación de seguridad de alta potencia redundante de 125 V CC de BMXCPS3522S

### **⚠ ADVERTENCIA**

#### **PÉRDIDA DE CAPACIDAD PARA EJECUTAR FUNCIONES DE SEGURIDAD**

Utilice sólo una fuente de alimentación BMXCPS4002S, BMXCPS4022S o BMXCPS3522S en cualquier bastidor que incluya un módulo de seguridad M580. Compruebe tanto la instalación física como el proyecto en Control Expert para confirmar que sólo se utilizan módulos de alimentación de seguridad M580.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## Funcionalidad de fuente de alimentación

Cada módulo de alimentación de seguridad M580 convierte la alimentación V CC o V CA en dos tensiones de salida, 24 V CC y 3,3 V CC, tal como se describe más abajo:

Funciones	Fuente de alimentación		
	BMXCPS4002S	BMXCPS4022S	BMXCPS3522S
Entrada de alimentación de red	100-240 V CA, 50-60 Hz	24-48 V CC	100-150 V CC
Salida de límite de potencia a placa de conexiones	40 V CC	40 V CC	40 V CC

Funciones	Fuente de alimentación		
	BMXCPS4002S	BMXCPS4022S	BMXCPS3522S
Temperatura ambiente para límite de potencia	-De 25 °C a +60 °C	-De 25 °C a +60 °C	-De 25 °C a +60 °C
Cable a	<ul style="list-style-type: none"> <li>Red de CA con neutro conectado a la tierra de CA o bien</li> <li>Red de CA con el neutro aislado o impedante respecto a tierra, con protección de neutro CA por el usuario.</li> </ul>	Una red de CC de 24-48 V CC	Una red de CC de 125 V CC

Cada fuente de alimentación detecta las condiciones de sobretensión, sobrecarga y cortocircuito en las líneas de placa de conexión de 3,3 V CC y 24 V CC.

Si se detecta el umbral superior de 40 V CC, el módulo realizará las acciones de respuesta siguientes.

- Se realiza un restablecimiento, lo que provoca que los módulos reciban alimentación de la fuente de alimentación que se va a reinicializar.
- Si se detectara el umbral de tensión superior en:
  - La línea de la placa de conexiones de 24 V CC, el PAC se desconecta.
  - La línea de la placa de conexiones de 3,3 V CC, el PAC deja de funcionar, pero este sigue recibiendo alimentación.

Consulte el tema *Diagnósticos para las tensiones de la placa de conexiones de 24 V CC y 3,3 V CC*, página 136 para obtener información sobre cómo responder ante estas condiciones.

## Módulos de alimentación redundante

Los módulos BMXCPS4002S, BMXCPS4022S y BMXCPS3522S son módulos de alimentación redundantes. Dos de estos módulos de alimentación se pueden instalar, uno como maestro y otro como esclavo, en un bastidor Ethernet redundante. Entre las configuraciones posibles están las siguientes:

Configuración	Funciones		
	Gestionar la redundancia (control de alimentación y señales de LED)	Proporcionar datos a la aplicación	Supervisar y guardar los datos de alimentación
2 fuentes de alimentación en bastidor principal	✓	✓	✓
2 fuentes de alimentación en bastidor de ampliación	✓	X	✓
1 fuente de alimentación en un bastidor heredado	X	X	✓
✓ = Admitido. X = No admitido.			

Para obtener más información acerca de las fuentes de alimentación redundantes, consulte el capítulo *Descripción de los módulos de alimentación de Modicon X80* (véase Modicon X80, Bastidores y fuentes de alimentación, Hardware Manual de referencia).

# Diagnósticos del módulo de alimentación de seguridad M580

## Diagnósticos para las tensiones de la placa de conexiones de 24 V CC y 3,3 V CC

Las fuentes de alimentación de seguridad de BMXCPS4002S, BMXCPS4022S y BMXCPS3522S permiten detectar automáticamente una condición de sobretensión, sobrecarga o cortocircuito que pueda producirse con relación a las tensiones de la placa de conexiones de 24 V CC y 3,3 V CC.

Si la fuente de alimentación detecta una de estas condiciones en la tensión de 24 V CC, se produce lo siguiente:

- La función de conversión eléctrica se apaga para toda la placa de conexiones.
- Se emite un comando RESET para todos los módulos del bastidor.
- Se apaga el LED **OK** de la fuente de alimentación.
- Se apaga todo el PAC.

Si la fuente de alimentación detecta una de estas condiciones en la tensión de 3,3 V CC, se produce lo siguiente:

- La conversión de alimentación se apaga para la tensión de la placa de conexiones de 3,3 V CC.
- Se emite un comando RESET para todos los módulos del bastidor.
- Se apaga el LED **OK** de la fuente de alimentación.
- Se detiene el funcionamiento de todo el programa PAC, aunque algunos circuitos del PAC pueden seguir recibiendo alimentación.

En cualquier caso, para recuperarse de estas condiciones, siga estos pasos:

1. Apague la línea de alimentación principal.
2. Compruebe la compatibilidad entre el consumo de fuente de alimentación estimado del PAC con relación a la capacidad del módulo de alimentación de seguridad M580 en las líneas de placa de conexiones de 24 V CC y 3,3 V CC.
3. Elimine la causa de la condición subyacente.
4. Espere 1 minuto después del apagado.
5. Aplique alimentación a la línea para reiniciar el módulo de alimentación de seguridad M580.

## Diagnósticos del contacto de relé de alarma

Las fuentes de alimentación BMXCPS4002S, BMXCPS4022S y BMXCPS3522S presentan un contacto de relé de alarma de dos pines que puede utilizar para obtener la información siguiente:

- Si el relé está activado (es decir, cerrado):
  - La tensión de la placa de conexiones de 24 V CC y de 3,3 V CC son correctas, y
  - el comando RESET no está activo; y
  - Si la fuente de alimentación se coloca en el bastidor local principal:
    - la CPU está operativa y
    - la CPU está en la modalidad RUN.
- Si el relé está desactivado (es decir, abierto):
  - Si una de las tensiones de la placa de conexiones, o las dos, de 24 V CC o 3,3 V CC, no son correctas; o
  - RESET está activo; o
  - Si la fuente de alimentación se coloca en el bastidor local principal:
    - la CPU no está operativa, o
    - la CPU está en modalidad STOP.

# DDT de seguridad de M580

## Introducción

Los módulos de alimentación de seguridad M580 presentan dos conjuntos de tipos de datos derivados (DDT):

- PWS\_DIAG\_DDT\_V2 para diagnósticos
- PWS\_CMD\_DDT para comandos

## PWS\_DIAG\_DDT\_V2

Offset de bytes	Nombre	Tipo	Comentario
0	Reservado	BYTE	–
1	Reservado	BYTE	–
2	PwsMajorVersion	BYTE	Versión del firmware principal de la fuente de alimentación
3	PwsMinorVersion	BYTE	Versión del firmware menor de la fuente de alimentación
4	Modelo	BYTE	Identificador de modelo Identificador de modelo: <ul style="list-style-type: none"> <li>• BMXCPS4002S = 01</li> <li>• BMXCPS4022S = 02</li> <li>• BMXCPS3522S = 03</li> </ul>
5	Estado	BYTE	Estado de fuente de alimentación
6	I33BacPos	UINT	Corriente medida en placa de conexiones de 3,3 V con rol nominal (productor)
8	V33Buck	UINT	Tensión medida de 3,3 V Buck
10	I24Bac	UINT	Corriente medida de línea de placa de conexiones de 24 V
12	V24Int	UINT	Tensión medida de 24 V Int
14	Temperatura	INT	Medición de temperatura ambiente
16	OperTimeMasterSincePO	UDINT	Tiempo de funcionamiento como maestro desde último encendido
20	OperTimeSlaveSincePO	UDINT	Tiempo de funcionamiento como esclavo desde último encendido

Offset de bytes	Nombre	Tipo	Comentario
24	OperTimeMaster	UDINT	Tiempo de funcionamiento como maestro desde fabricación
28	OperTimeSlave	UDINT	Tiempo de funcionamiento como esclavo desde fabricación
32	Work	UDINT	Trabajo suministrado desde fabricación
36	RemainingLTPC	UINT	Tiempo de vida en porcentaje restante
38	NbPowerOn	UINT	Número de encendidos desde fabricación
40	NbVoltageLowFail	UINT	Número de fallo detectado en tensión primaria por umbral inferior
42	NbVoltageHighFail	UINT	Número de fallo detectado en tensión primaria por umbral superior
44	Reservado	UDINT	–
48	Reservado	UDINT	–
52	RemainingLTMO	UINT	Tiempo de vida útil restante en meses
54	Reservado	BYTE	–
63	Reservado	BYTE	–

## PWS\_CMD\_DDT

Offset de bytes	Nombre	Tipo	Comentario
0	Reservado	BYTE	–
1	Código	BYTE	Código de comando: <ul style="list-style-type: none"> <li>• 1 = intercambiar</li> <li>• 3 = borrar</li> </ul>
2	PwsTarget	BYTE	Destino de fuente de alimentación: 1 para izquierda, 2 para derecha, 3 para las dos  Destino de fuente de alimentación <ul style="list-style-type: none"> <li>• 1 = izquierda</li> <li>• 2 = derecha</li> </ul>
3	Reservado	BYTE	–
15	Reservado	BYTE	–

# Validación de un sistema de seguridad M580

## Contenido de este capítulo

Arquitectura del módulo de seguridad M580 .....	141
Valores de SIL y MTTF del módulo de seguridad M580 .....	150
Cálculos de tiempo y rendimiento del sistema de seguridad M580 .....	157

## Introducción

En este capítulo se muestra cómo realizar cálculos que validen el sistema de seguridad M580.

# Arquitectura del módulo de seguridad M580

## Introducción

En esta sección se muestran las arquitecturas internas de los módulos de seguridad.

## Arquitectura de seguridad de la CPU y del coprocesador de seguridad de M580

### Introducción

El funcionamiento de las CPU BME•58•040S y el coprocesador BMEP58CPROS3 (Copro) como par de procesadores está certificado por el TÜV Rheinland Group para utilizarlos en soluciones de seguridad M580 de nivel de integridad de seguridad 3 (SIL3).

Al funcionar conjuntamente, la CPU y el coprocesador proporcionan las funciones de nivel de seguridad SIL3 siguientes:

- Ejecución doble independiente del código de tarea de seguridad.
- Comparación de los resultados de la ejecución doble de código.
- Autopruebas periódicas.
- Compatibilidad con una arquitectura 1oo2D ("one out of two", una de dos) con diagnóstico.

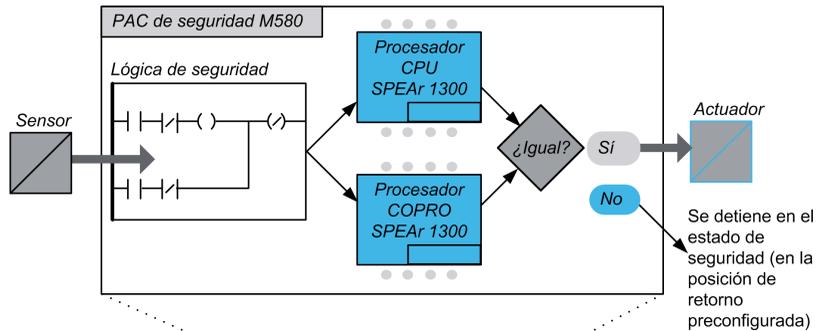
**NOTA:** Además de la funcionalidad de seguridad, las CPU BMEP58•040S también proporcionan funciones comparables de CPU M580 autónomas que no son de seguridad equivalentes, mientras que las CPU BMEH58•040S proporcionan funciones comparables de CPU Hot Standby M580 que no son de seguridad equivalentes. Consulte los manuales *Modicon M580, Hardware, Manual de referencia* y *Modicon M580 Hot Standby, Guía de planificación del sistema para arquitecturas utilizadas con más frecuencia* para obtener información sobre las características que no son de seguridad de estas CPU de seguridad.

## Descripción de la arquitectura interna de la CPU y del coprocesador

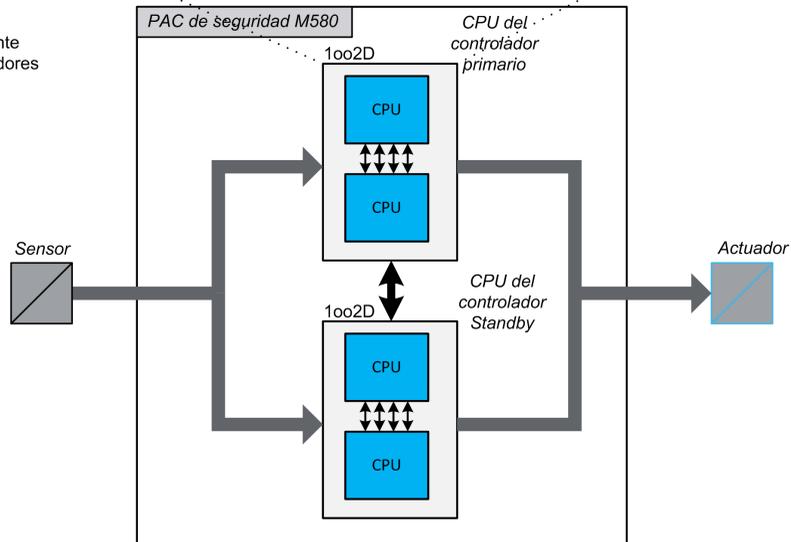
La CPU y el coprocesador de seguridad de M580 contienen respectivamente un procesador SPEAr 1300. Cada procesador ejecuta la lógica de seguridad en su propia área de memoria y compara los resultados de la ejecución al final de la tarea segura.

En las siguientes figuras se muestra la arquitectura interna de la CPU de seguridad de M580 en configuraciones simples y redundantes:

Arquitectura simple basada en 2 procesadores



Arquitectura redundante basada en 4 procesadores



## Generación y ejecución doble de código

Los dos procesadores dentro del PAC de seguridad M580 permiten la generación y ejecución doble de código. Esta diversidad ofrece las ventajas siguientes en cuanto a la detección de errores:

- Se generan dos programas de código ejecutable de forma independiente. El uso de dos compiladores de código independientes es útil para detectar errores sistemáticos en la generación de código.

- Los dos programas de código generados se ejecutan mediante dos procesadores independientes. De esta manera, la CPU puede detectar errores sistemáticos en la ejecución del código y errores aleatorios en el PAC.
- Cada uno de los dos procesadores utiliza sus propia área de memoria independiente. De esta manera, el PAC puede detectar errores aleatorios en la RAM y no es necesario realizar una prueba completa de la RAM en cada exploración.

## Arquitectura 1oo2D

La arquitectura 1oo2D ("one out of two with Diagnostic", una de dos con diagnóstico) significa que dos canales independientes ejecutan la lógica de seguridad y que, si se detecta un error en uno de los canales, el sistema pasa al estado seguro.

## Arquitectura simple

La arquitectura simple de PAC de seguridad de M580 se basa en una arquitectura 1oo2D formada por procesadores duales compatibles con el nivel de integridad de seguridad (SIL3) incluso en arquitecturas no redundantes.

## Arquitectura redundante

El PAC de seguridad de M580 en una arquitectura redundante proporciona una disponibilidad del sistema y tiempo de actividad del proceso máximos al incorporar redundancia total (estructura cuádruple, es decir, cuatro CPU) para control, fuente de alimentación y comunicación.

Una de las CPU (par de procesadores), que funciona como CPU primaria, ejecuta la aplicación al ejecutar la lógica de programa y las E/S operativas. La CPU primaria (del par de procesadores) actualiza la CPU secundaria (del par de procesadores) a fin de que esta esté lista para asumir el control de las E/S.

El sistema se autosupervisa continuamente. En el caso de que se produzca un fallo de control de la CPU primaria, el sistema pasará el control a la CPU secundaria. En esta modalidad degradada, el sistema sigue siendo SIL3. En el caso de que tanto la CPU primaria como la secundaria fallen, el sistema pasará al estado de seguridad contra fallos.

El PAC de seguridad de M580 redundante, basado en una arquitectura cuádruple (4 procesadores), permite aumentar la disponibilidad del sistema y proporciona compatibilidad con el nivel de integridad de seguridad (SIL3).

## Watchdog

Un hardware y un watchdog del firmware comprueban la actividad del PAC y el tiempo requerido para ejecutar la lógica del programa de seguridad.

**NOTA:** Configure el watchdog del software (en el diálogo **Propiedades de SAFE**) para permitir:

- El tiempo de ejecución de aplicación
- El filtrado de cualquier error de comunicación de E/S detectado
- El tiempo de seguridad del proceso

Para obtener más información, consulte el tema *Tiempo de seguridad del proceso*, página 157.

## Comprobación de memoria

La integridad del contenido de memoria estática se pone a prueba mediante la comprobación de redundancia cíclica (CRC) y la ejecución doble de código. La integridad del contenido de memoria dinámica se pone a prueba mediante una ejecución doble de código, una prueba de memoria periódica y un mecanismo de código de corrección de errores (ECC) que detecta y corrige las instancias más habituales de datos internos dañados. Durante el arranque en frío, estas pruebas se reinician y se realizan totalmente antes de que la CPU pase a la modalidad de ejecución o parada.

## Supervisión de sobretensión

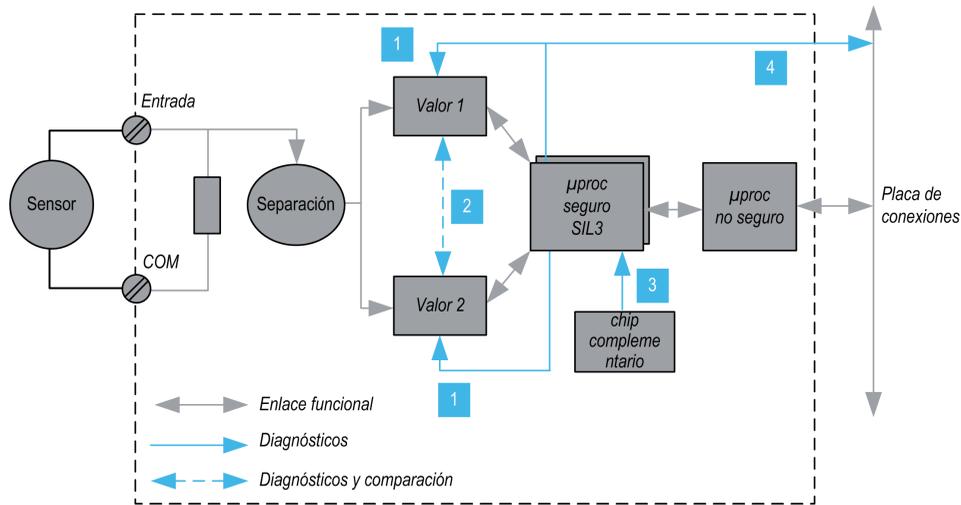
La CPU recibe alimentación del módulo de alimentación de seguridad M580 dedicado a través de la línea de placa de conexiones. El módulo de alimentación proporciona una tensión regulada de 24 V con una tensión máxima absoluta en el rango de 0 a 36 V.

En la CPU hay una función integrada que comprueba las fuentes de alimentación internas. Si se detecta una condición de infratensión o sobretensión, se apagará el PAC.

# Arquitectura de seguridad del módulo de entrada analógica BMXSAI0410

## Arquitectura de función de seguridad

La arquitectura interna del módulo BMXSAI0410 realiza su función de seguridad de la forma siguiente:



**1** Los dispositivos de medición se supervisan habitualmente dada su capacidad para medir, sin que se detecten errores, 10 valores analógicos entre 4 y 20 mA. La linealidad de las etapas de medición se verifica de forma simultánea.

**2** 2 circuitos idénticos adquieren cada valor de entrada. Los valores de medición se comparan mediante el procesador de seguridad. Si los valores son diferentes, se determina que el canal no es válido. Se tolera una como máximo una discrepancia del 0,35 % del rango de escala completo de 20 mA entre los dos valores.

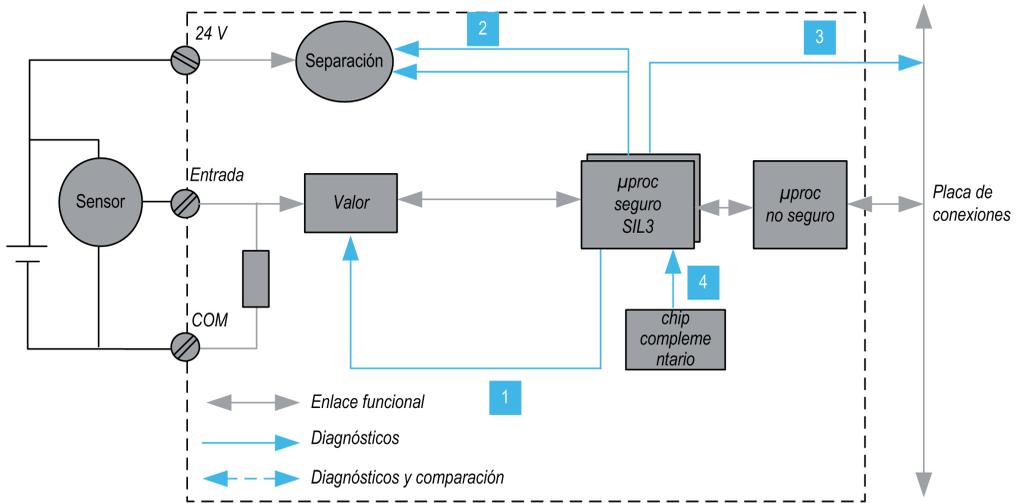
**3** El chip complementario alimenta al procesador de seguridad, diagnostica continuamente el procesador de seguridad y supervisa la tensión de la placa de conexiones.

**4** La tensión de alimentación de la placa de conexiones se supervisa para detectar si se produce una condición de sobretensión o infratensión.

# Arquitectura de seguridad del módulo de entrada digital BMXSDI1602

## Arquitectura de función de seguridad

La arquitectura interna del módulo BMXSDI1602 realiza la función de seguridad de la forma siguiente:



**1** Los dispositivos de medición se supervisan continuamente dada su capacidad para medir un "1" y un "0".

**2** El procesador de seguridad supervisa continuamente la fuente de alimentación de 24 V CC externa. Dos circuitos idénticos adquieren cada valor de entrada. Los valores adquiridos se comparan mediante el procesador de seguridad. Si los valores son diferentes, el canal se declara no válido.

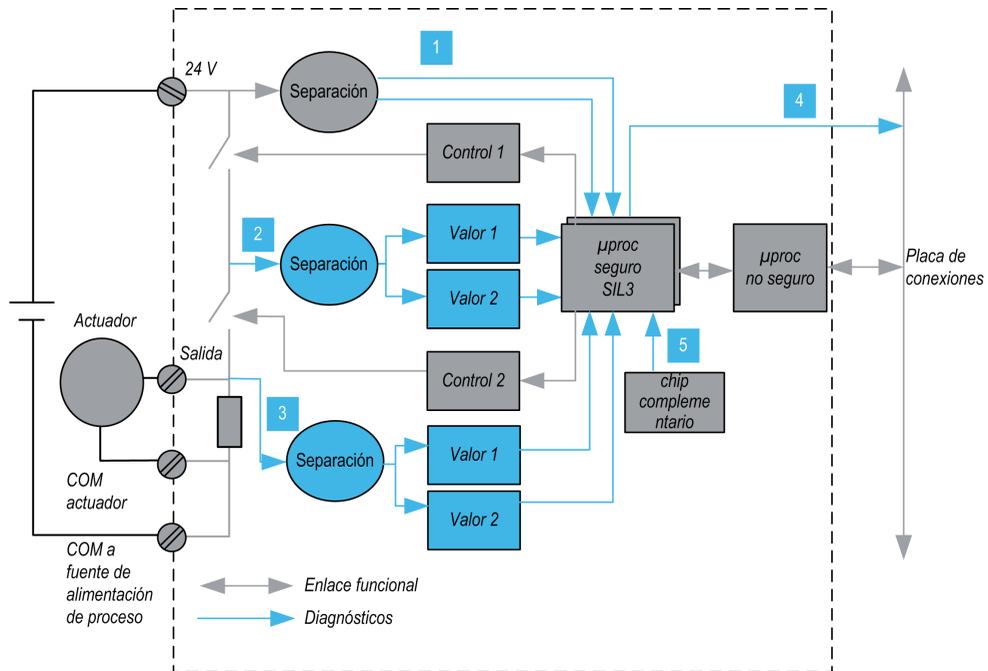
**3** La tensión de alimentación de la placa de conexiones se supervisa para detectar una condición de sobretensión o infratensión.

**4** El chip complementario alimenta al procesador de seguridad, diagnostica continuamente el procesador de seguridad y supervisa la tensión de la placa de conexiones.

# Arquitectura de seguridad del módulo de salida digital BMXSDO0802

## Arquitectura de función de seguridad

La arquitectura interna del módulo BMXSDO0802 realiza la función de seguridad de la forma siguiente:



**1** El procesador de seguridad supervisa continuamente la fuente de alimentación de 24 V CC externa.

**2** Cada salida consta de 2 conmutadores en serie ubicados entre la fuente de alimentación de 24 V CC externa y la tierra. El valor de punto medio (2) se lee y se envía de forma redundante al procesador de seguridad. Los valores de medición de puntos medios se comparan mediante el procesador de seguridad. Si los valores no son los previstos, el canal se declara no válido.

**3** También se supervisa el valor de punto bajo (3) a fin de realizar el diagnóstico de cableado externo.

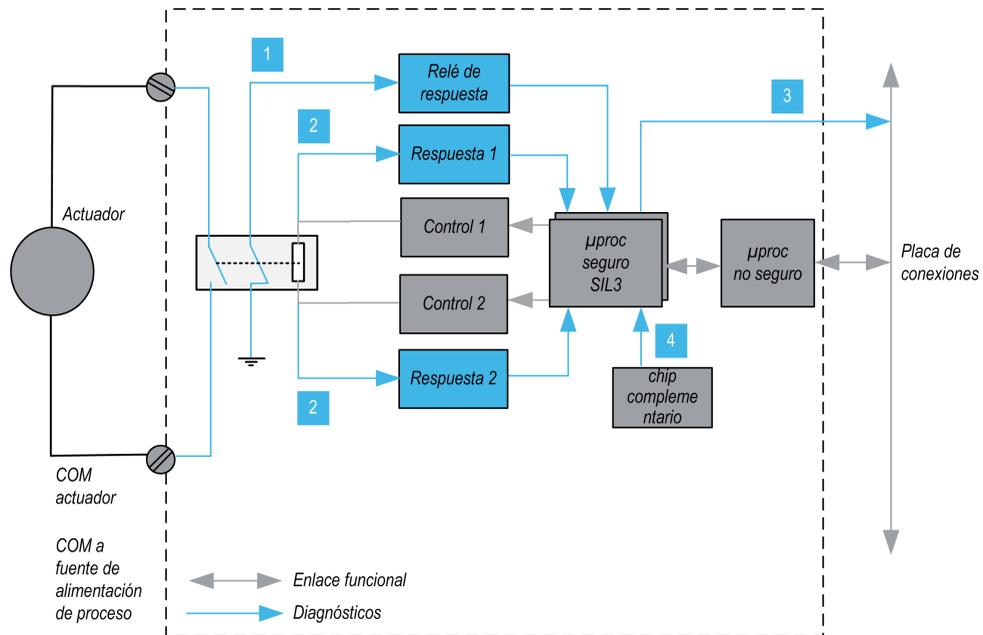
**4** La tensión de alimentación de la placa de conexiones se supervisa para determinar si hay una condición de sobretensión o infratensión.

**5** El chip complementario alimenta al procesador de seguridad, diagnostica continuamente el procesador de seguridad y supervisa la tensión de la placa de conexiones.

# Arquitectura de seguridad del módulo de salida de relé digital BMXSRA0405

## Arquitectura de función de seguridad

La arquitectura interna del módulo BMXSRA0405 realiza la función de seguridad de la forma siguiente:



**1** El estado del relé se supervisa continuamente mediante el procesador de seguridad, que lee el estado de un contacto NC conectado mecánicamente al contacto NA y que está conectado al actuador.

**2** El estado del comando de relé se supervisa continuamente. 2 circuitos idénticos reciben cada entrada. Los valores medidos se comparan mediante el procesador de seguridad. Si los valores son diferentes, el canal se declara no válido.

**3** La tensión de alimentación de la placa de conexiones se supervisa para determinar si hay una condición de sobretensión o infratensión.

**4** El chip complementario alimenta al procesador de seguridad, diagnostica continuamente el procesador de seguridad y supervisa la tensión de la placa de conexiones.

# Valores de SIL y MTTF del módulo de seguridad M580

## Introducción

Esta sección muestra los valores de SIL y MTTF que puede utilizar para los cálculos del módulo de seguridad M580.

## Cálculos del nivel de integridad de seguridad

### Clasificación de los productos de Schneider Electric

El PAC de seguridad M580 puede consistir en:

- Módulos de seguridad, que pueden realizar funciones de seguridad, incluidos:
  - CPU y coprocesador
  - módulos de E/S
  - alimentación
- Módulos no interferentes; , página 29, que no realizan funciones de seguridad, pero le permiten añadir elementos que no son de seguridad a su proyecto de seguridad.

#### **NOTA:**

- Puesto que los módulos no interferentes no forman parte del bucle de seguridad, no forman parte de los cálculos de nivel de integridad de seguridad.
- Un error detectado en un módulo no interferente no afecta negativamente a la ejecución de las funciones de seguridad.
- Las fuentes de alimentación BMXCPS4002S, BMXCPS4022S y BMXCPS3522S están certificadas. Dado que presentan una frecuencia de fallos peligrosos despreciable (<1 % del objetivo de SIL3), la fuente de alimentación no se incluye en los cálculos de nivel de integridad de seguridad para el bucle de seguridad. En consecuencia, no se proporcionan valores de PFH ni de PFD para los módulos de alimentación.

## Valores de PFD/PFH para módulos de seguridad M580

Schneider Electric ofrece los siguientes módulos de seguridad certificados para su uso en aplicaciones de seguridad. Los módulos de seguridad se enumeran con sus valores de probabilidades de fallo, página 153 (PFD/PFH) correspondientes para intervalos de prueba,

página 156 (PTI) diferentes. Los PFD/PFH se expresan como valores que contribuyen a los PFD/PFH globales del bucle de seguridad, página 17 completo.

En las tablas siguientes se enumeran los módulos de seguridad y sus valores de PFD/PFH para las aplicaciones SIL2 y SIL3, cuando sea posible:

Tipo de producto	Referencia del producto	SIL	PTI = 1 año	
			PFD <sub>G</sub>	PFH <sub>G</sub>
CPU con coprocesador	BME•58•040S y BMEP58CPROS3	SIL3 <sup>1</sup>	4,38E-07	1.00E-10
Entrada analógica	BMXSAI0410	SIL3 <sup>2</sup>	5,76E-06	1,31E-09
Entrada digital	BMXSDI1602	SIL3 <sup>2</sup>	6,81E-06	1,56E-09
Salida digital	BMXSDO0802	SIL3 <sup>1</sup>	5,75E-06	1,31E-09
Salida de relé digital	BMXSRA0405	SIL2 <sup>3</sup>	5,85E-06	1,68E-09
		SIL3 <sup>4</sup>	5,84E-06	1,34E-09
		SIL3 <sup>5</sup>	–	1,35E-09
Fuente de alimentación	BMXCPS4002S, BMXCPS4022S, y BMXCPS3522S	SIL3	–	–
1. 1 salida a 80 °C 2. 1 entrada a 80 °C 3. 1 relé por salida a 80 °C 4. 2 relés por salida a 80 °C 5. 4 relés por salida a 80 °C				

Tipo de producto	Referencia del producto	SIL	PTI = 5 años	
			PFD <sub>G</sub>	PFH <sub>G</sub>
CPU y coprocesador	BME•58•040S y BMEP58CPROS3	SIL3 <sup>1</sup>	2,20E-06	1.01E-10
Entrada analógica	BMXSAI0410	SIL3 <sup>2</sup>	2,88E-05	1,31E-09
Entrada digital	BMXSDI1602	SIL3 <sup>2</sup>	3,41E-05	1,56E-09
Salida digital	BMXSDO0802	SIL3 <sup>1</sup>	2,88E-05	1,31E-09
Salida de relé digital	BMXSRA0405	SIL2 <sup>3</sup>	2,92E-05	1,68E-09
		SIL3 <sup>4</sup>	2,92E-05	1,34E-09
		SIL3 <sup>5</sup>	–	1,35E-09

Tipo de producto	Referencia del producto	SIL	PTI = 5 años	
			PFD <sub>G</sub>	PFH <sub>G</sub>
Fuente de alimentación	BMXCPS4002S, BMXCPS4022S, y BMXCPS3522S	SIL3	–	–
1. 1 salida a 80 °C 2. 1 entrada a 80 °C 3. 1 relé por salida a 80 °C 4. 2 relés por salida a 80 °C 5. 4 relés por salida a 80 °C				

Tipo de producto	Referencia del producto	SIL	PTI = 10 años	
			PFD <sub>G</sub>	PFH <sub>G</sub>
CPU y coprocesador	BME•58•040S y BMEP58CPROS3	SIL3 <sup>1</sup>	4,44E-06	1.02E-10
Entrada analógica	BMXSAI0410	SIL3 <sup>2</sup>	5,76E-05	1,31E-09
Entrada digital	BMXSDI1602	SIL3 <sup>2</sup>	6,81E-05	1,56E-09
Salida digital	BMXSDO0802	SIL3 <sup>1</sup>	5,75E-05	1,31E-09
Salida de relé digital	BMXSRA0405	SIL2 <sup>3</sup>	5,84E-05	1,68E-09
		SIL3 <sup>4</sup>	5,84E-05	1,34E-09
		SIL3 <sup>5</sup>	–	1,35E-09
Fuente de alimentación	BMXCPS4002S, BMXCPS4022S, y BMXCPS3522S	SIL3	–	–
1. 1 salida a 80 °C 2. 1 entrada a 80 °C 3. 1 relé por salida a 80 °C 4. 2 relés por salida a 80 °C 5. 4 relés por salida a 80 °C				

Tipo de producto	Referencia del producto	SIL	PTI = 20 años	
			PFD <sub>G</sub>	PFH <sub>G</sub>
CPU y coprocesador	BME•58•040S y BMEP58CPROS3	SIL3 <sup>1</sup>	9.00E-06	1,04E-10
Entrada analógica	BMXSAI0410	SIL3 <sup>2</sup>	1,15E-04	1,31E-09
Entrada digital	BMXSDI1602	SIL3 <sup>2</sup>	1,36E-04	1,56E-09
Salida digital	BMXSDO0802	SIL3 <sup>1</sup>	1,15E-04	1,31E-09

Tipo de producto	Referencia del producto	SIL	PTI = 20 años	
			PFD <sub>G</sub>	PFH <sub>G</sub>
Salida de relé digital	BMXSRA0405	SIL2 <sup>3</sup>	1,17E-04	1,68E-09
		SIL3 <sup>4</sup>	1,17E-04	1,34E-09
		SIL3 <sup>5</sup>	–	1,35E-09
Fuente de alimentación	BMXCPS4002S, BMXCPS4022S, y BMXCPS3522S	SIL3	–	–
1. 1 salida a 80 °C 2. 1 entrada a 80 °C 3. 1 relé por salida a 80 °C 4. 2 relés por salida a 80 °C 5. 4 relés por salida a 80 °C				

## Probabilidades de fallo para aplicaciones SIL3

Para las aplicaciones SIL3, la IEC 61508 define las siguientes probabilidades de fallo a petición (PFD) y probabilidades de fallo por hora (PFH) para cada bucle de seguridad, en función de la modalidad de funcionamiento:

- $PFD \geq 10^{-4}$  a  $< 10^{-3}$  para una modalidad de funcionamiento de baja demanda
- $PFH \geq 10^{-8}$  a  $< 10^{-7}$  para una modalidad de funcionamiento de alta demanda

El PAC de seguridad M580 está certificado para su utilización en sistemas de baja y alta demanda.

## Cálculo de ejemplo de nivel de integridad de seguridad

Este cálculo de ejemplo le muestra cómo determinar:

- La contribución de riesgo de los módulos de seguridad de Schneider Electric a su aplicación de seguridad.
- La cantidad restante de riesgo de que los otros dispositivos del bucle de seguridad (por ejemplo, sensores y actuadores) pueden contribuir a su aplicación de seguridad para un nivel de integridad de seguridad y una modalidad de funcionamiento determinados.

**NOTA:** Al calcular la contribución de riesgo de sensores y actuadores a su aplicación de seguridad, póngase en contacto con los fabricantes de estos dispositivos y obtenga los valores de PFD/PFH para el intervalo de prueba apropiado.

Los módulos de seguridad de Schneider Electric siguientes se incluyen en este ejemplo:

- 1: CPU BMEP584040S
- 1: BMEP58CPROS3 Coprocesador
- 1: BMXSAI0410 Entrada analógica
- 1: BMXSDO0802 Salida digital
- 1: BMXCPS4002S Fuente de alimentación

El cálculo siguiente emplea valores de  $PFH_G$  para una modalidad de funcionamiento de alta demanda para un bucle de seguridad SIL3 con un PTI de 20 años. El valor máximo permisible de PFH para esta aplicación de seguridad es de  $10^{-7}$  (o  $1,0E-7$ ):

Módulo de seguridad		Contribución (notificación científica)	Contribución restante para sensores y actuadores
CPU con coprocesador		7.01E-10	–
Entrada analógica		1,31E-09	
Salida digital		1,31E-09	
Fuente de alimentación		–	
<b>Total</b>	numérico	<b>2,72E-09</b>	<b>97,28E-09</b>
	% máx	<b>2,72%</b>	<b>97,28 %</b>

Nota 1: La salida de relé utiliza cuatro relés para admitir una salida.

## Valores de módulos de seguridad M580 para maquinaria

Schneider Electric ofrece los módulos de seguridad siguientes certificados para usarlos en aplicaciones de maquinaria de seguridad según la norma ISO 13849-1. En la tabla que aparece a continuación se muestran los módulos de seguridad y sus valores, categoría y nivel, si proceden.

Tipo de producto	Referencia del producto	Configuración	Categoría	Nivel de rendimiento	MTTF (años)	DCav
CPU con coprocesador	BME•58•040S y BMEP58CPROS3	N/A	4	e	235	Alto (>99 %)
Entrada analógica	BMXSAI0410	mediante 1 canal	2	d	255	99,66%
		mediante 2 canales	4	e	255	99,66%
Entrada digital	BMXSDI1602	mediante 1 canal	2	d	231	99,69%
		mediante 2 canales	4	e	231	99,69%

Tipo de producto	Referencia del producto	Configuración	Categoría	Nivel de rendimiento	MTTF (años)	DCav
Salida digital	BMXSDO0802	N/A	4	e	253	99,63%
Salida de relé digital	BMXSRA0405	mediante 1 canal	2	c	156	99,77%
		mediante 2 canales	4	e	156	99,77%

## Valores para módulos de seguridad M580 para ferrocarriles

Schneider Electric ofrece los siguientes módulos de seguridad certificados para el sector ferroviario de acuerdo con las normas Cenelec EN50126, EN50128, EN50129. En la tabla siguiente se enumeran los módulos de seguridad y sus valores de fiabilidad:

Tipo de producto	Referencia del producto	SIL	TFFR (PTI = 20 años)
<b>CPU y coprocesador</b>	BME-58-040S y BMEP58CPROS3	SIL4	1,04E-10
Entrada analógica	BMXSAI0410	SIL4	1,31E-09
Entrada digital	BMXSDI1602	SIL4	1,56E-09
Salida digital	BMXSDO0802	SIL4	1,31E-09
Salida de relé digital	BMXSRA0405	SIL3 <sup>1</sup>	1,68E-09
		SIL4 <sup>2</sup>	1,34E-09
		SIL4 <sup>3</sup>	1,35E-09
Fuente de alimentación	BMXCPS4002S, BMXCPS4022S, y BMXCPS3522S	SIL4	–
<p><b>NOTA:</b> Los valores de SIL están a 80 °C</p> <p>1. 1 relé por salida a 80 °C</p> <p>2. 2 relés por salida a 80 °C</p> <p>3. 4 relés por salida a 80 °C</p>			

La suma de TFFR de un módulo de entrada, la CPU y el coprocesador, la fuente de alimentación y un módulo de salida es siempre inferior a 3,5E-09/h, que es inferior a la previsión máxima asignada del 40 % dirigida como la tasa máxima de fallos residuales para una función de seguridad SIL4 que permite integrar otros productos en el bucle de seguridad.

TFFR por hora y función	Atributo SIL
$10^{-9} \leq \text{TFFR} \leq 10^{-8}$	4
$10^{-8} \leq \text{TFFR} \leq 10^{-7}$	3
$10^{-7} \leq \text{TFFR} \leq 10^{-6}$	2
$10^{-60} \leq \text{TFFR} \leq 10^{-5}$	1

## Descripción de los tiempos de seguridad

El PAC de seguridad M580 tiene una duración de ciclo mínima de PAC de 10 ms, que es necesaria para el procesamiento de las señales provenientes de los módulos de E/S, la ejecución de la lógica de programa y la configuración de las salidas. Para calcular el tiempo de reacción máximo del PAC, debe conocer el tiempo de reacción máximo de los sensores y actuadores que se están utilizando. Además, el tiempo de reacción máximo del PAC depende del tiempo de seguridad del proceso (PST), página 157 necesario para el proceso.

## Intervalo de prueba

El texto de prueba es una prueba periódica que debe realizar para detectar fallos en un sistema relacionado con la seguridad de modo que, si es necesario, el sistema pueda restablecerse a una nueva condición o a una condición tan próxima a esta como sea posible. El periodo de tiempo entre estas pruebas es el intervalo de prueba.

El intervalo de prueba depende del nivel de integridad de seguridad de destino, los sensores, los actuadores y la aplicación del PAC. El sistema de seguridad M580 es adecuado para su uso en una aplicación SIL3 en relación con IEC 61508 y un intervalo de prueba de 20 años.

# Cálculos de tiempo y rendimiento del sistema de seguridad M580

## Introducción

En esta sección se muestra cómo calcular el tiempo de reacción del PAC, el tiempo de reacción del sistema y el tiempo de seguridad del proceso para el sistema de seguridad M580.

## Tiempo de seguridad del proceso

### Descripción del tiempo de seguridad del proceso

El tiempo de seguridad del proceso (PST) es una medida fundamental de un proceso ejecutado por un bucle de seguridad. Se define como el periodo comprendido entre el momento en el que se produce fallo en el equipo bajo control (EUC) y el momento en el que se produce un evento peligroso, si no se realiza la función de seguridad (es decir, no se alcanza el estado de seguridad).

**NOTA:** Su proceso de seguridad específico determina el tiempo de seguridad del proceso. Debe verificar que el sistema relacionado con la seguridad puede realizar sus funciones de seguridad durante el tiempo de seguridad del proceso.

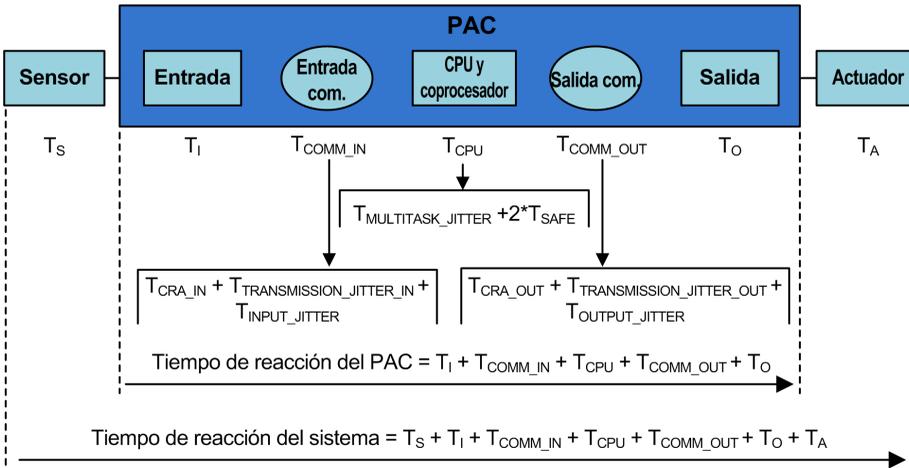
### Descripción del tiempo de reacción del sistema

El tiempo de reacción del sistema es la suma del tiempo de reacción del PAC, más los tiempos de reacción para el sensor seleccionado ( $T_S$ ) y el actuador seleccionado ( $T_A$ ).

**NOTA:**  $T_S$  y  $T_A$  son específicos del dispositivo.

Para cada bucle de seguridad, verifique que el tiempo de reacción del sistema sea inferior al tiempo de seguridad del proceso.

El tiempo de reacción del sistema se muestra más abajo:



Los componentes del tiempo de reacción del sistema pueden incluir lo siguiente:

Componente	Descripción	Valor calculado para el peor de los casos
$T_S$	Tiempo de reacción que necesita el sensor seleccionado para reaccionar ante un evento de proceso.	Específico del dispositivo.
$T_I$	Tiempo máximo que necesita el módulo de entrada para muestrear y confirmar un evento de sensor. Incluye: <ul style="list-style-type: none"> <li>Un periodo de muestreo del módulo de entrada.</li> <li>Varios periodos de muestreo del módulo de entrada para el filtrado.</li> </ul>	6 ms
$T_{COMM\_IN}$	Retardo de comunicación de entrada. Sus componentes se describen en el tema <i>Tiempo de respuesta de la aplicación en Modicon M580 autónomo Guía de planificación del sistema para arquitecturas utilizadas con más frecuencia</i> e incluyen lo siguiente (los números hacen referencia al cálculo de ART en el tema referenciado): <ul style="list-style-type: none"> <li><math>T_{CRA\_IN}</math>: CRA_Drop_Process (2) + CRA Input RPI (3)</li> <li><math>T_{JITTER\_IN}</math>: Network_In_Time (4) + Network_In_Jitter (5) + CPU_In_Jitter (6)</li> </ul>	–
$T_{CPU}$	El tiempo de reacción de la CPU y del coprocesador, que es igual a la suma del retardo provocado por tareas de mayor prioridad pendientes (la tarea FAST) más dos tiempos de exploración de la tarea SAFE, la primera de las cuales corresponde una exploración fallida y la segunda una exploración correcta: <p><math>T_{MULTITASK\_JITTER} + 2 * T_{SAFE}</math>.</p>	–
$T_{MULTITASK\_JITTER}$	El retardo máximo provocado por la ejecución de tareas pendientes de mayor prioridad. En este caso, la tarea FAST.	–

Componente	Descripción	Valor calculado para el peor de los casos
	$T_{MULTITASK\_JITTER} = T_{FAST}$ .	
$T_{SAFE}$	El periodo de la tarea SAFE configurada.	–
$T_{FAST}$	Este valor se incluye porque se prioriza la ejecución de la tarea FAST frente a la tarea SAFE. <b>NOTA:</b> Para simplificar la fórmula, se considera que ninguna tarea del sistema se encuentra en una condición de desborde. Por tanto, este valor es igual al periodo de la tarea FAST configurada o bien 0 si la tarea FAST no está configurada.	–
$T_{COMM\_OUT}$	Retardo de la comunicación de salida. Sus componentes se describen en el tema <i>Tiempo de respuesta de la aplicación en Modicon M580 autónomo Guía de planificación del sistema para arquitecturas utilizadas con más frecuencia</i> e incluyen lo siguiente (los números hacen referencia al cálculo de ART en el tema referenciado): <ul style="list-style-type: none"> <li><math>T_{CRA\_OUT}</math>: CRA_Drop_Process (12)</li> <li><math>T_{JITTER\_IN}</math>: CPU_Out_Jitter (9) + Network_Out_Time (10) + Network_Out_Jitter (11)</li> </ul>	–
$T_O$	Es igual a la suma de los tiempos siguientes: <ul style="list-style-type: none"> <li>Tiempo de retardo entre la lectura y la aplicación del valor de salida de la CPU (de 0 a 3 ms).</li> <li>El tiempo que necesita el módulo de salida de seguridad para modificar la salida física, es decir, propagar el cambio de ram X a la salida física (entre 0 y 3 ms).</li> </ul>	6 ms
$T_A$	Tiempo de reacción para el actuador seleccionado.	Específico del dispositivo.

## Descripción del tiempo de reacción del PAC

En el caso de E/S colocadas en el bastidor principal local (con la CPU), el tiempo de reacción del PAC es la suma de los tiempos de reacción relacionados tanto para el módulo de entrada seleccionado ( $T_I$ ) como el módulo de salida seleccionado ( $T_O$ ), más el tiempo de reacción de CPU y coprocesador ( $T_{CPU}$ ):

$$\text{Tiempo de reacción del PAC (local)} = T_{CPU} + T_I + T_O$$

Si las E/S están ubicadas en un bastidor remoto, el tiempo de reacción del PAC también incluye los tiempos de retardo de comunicación de entrada ( $T_{COMM\_IN}$ ) y de retardo de comunicación de salida ( $T_{COMM\_OUT}$ ):

$$\text{Tiempo de reacción del PAC (remoto)} = T_{CPU} + T_{COMM\_IN} + T_I + T_{COMM\_OUT} + T_O$$

## Descripción del tiempo de reacción de la CPU y del coprocesador

El tiempo de reacción de la CPU y del coprocesador está directamente influido por el periodo de la tarea SAFE y el periodo de la tarea FAST. Verifique que la lógica de seguridad se ejecutará durante el periodo de la tarea SAFE.

Puesto que una señal puede aparecer al inicio del ciclo de ejecución cuando ya se han procesado las señales, es posible que se necesiten dos ciclos de tarea SAFE para reaccionar ante la señal.

Dado que la tarea FAST tiene prioridad sobre la tarea SAFE, también debe tener en cuenta el tiempo para ejecutar la tarea FAST al calcular la fluctuación.

Esto produce la siguiente ecuación para el tiempo de reacción máximo (es decir, para el peor de los casos):

$$\text{Tiempo de reacción de la CPU y del coprocesador} = 2 \times T_{\text{SAFE}} + T_{\text{FAST}}$$

**NOTA:** Si está utilizando una comunicación segura entre pares, página 186 para realizar la función de seguridad, la estimación del tiempo de reacción de la CPU es diferente.

## Descripción del tiempo para módulos de entrada

Los tiempos máximos (para el peor de los casos) para el módulo de entrada digital de seguridad y para el módulo de entrada analógica de seguridad  $T_1$  son 6 ms..

## Descripción del tiempo para módulos de salida

Se calcula que el tiempo máximo  $T_O$  para el módulo de salida digital de seguridad es 6 ms.

Se debe configurar un timeout de seguridad de recuperación  $S\_TO$  para el módulo de salida digital, página 111 y el módulo de salida de relé digital, página 128. En función del periodo de la tarea SAFE configurada ( $T_{\text{SAFE}}$ ), se debe configurar el valor de  $S\_TO$  de la forma siguiente:

- Si  $(2,5 * T_{\text{SAFE}}) \leq 40$  ms, establezca  $S\_TO$  a un valor mínimo de 40 ms.
- Si  $(2,5 * T_{\text{SAFE}}) > 40$  ms, establezca  $S\_TO$  a un valor mínimo de  $(2,5 * T_{\text{SAFE}})$  ms.

## **AVISO**

### **RIESGO DE FUNCIONAMIENTO IMPREVISTO DEL EQUIPO**

Establezca el timeout de seguridad de recuperación (S\_TO) de un módulo de salida de seguridad a, como mínimo, un valor superior a 40 ms o  $(2,5 * T_{SAFE})$ , en el que  $T_{SAFE}$  es igual al periodo de tarea SAFE.

**Si no se siguen estas instrucciones, pueden producirse daños en el equipo.**

En el caso de aplicaciones Hot Standby, tenga en cuenta cuál será el impacto sobre el parámetro (S\_TO) de timeout de seguridad de recuperación a raíz del tiempo adicional ( $T_{SWAP}$ ) que se necesita en un intercambio, página 162 y del tiempo adicional  $T_{SWITCH}$  que se necesita en una conmutación, página 163.

## **Cálculo del tiempo de reacción del sistema**

Si conoce el tiempo de seguridad del proceso (PST) necesario y el tiempo de reacción máximo de los sensores y actuadores, podrá calcular el tiempo de reacción del sistema (SRT) máximo que se tolera en el proceso.

El tiempo de reacción (es decir, para el peor de los casos) máximo del sistema se puede calcular de la siguiente forma:

### **Para sistemas con E/S en estaciones remotas:**

$$\text{SRT máx.} = T_S + T_I + 2 \times T_{CRA} + T_{RPI} + 2 \times T_{SAFE} + T_{FAST} + T_O + T_A.$$

o bien

$$\text{SRT máx.} = 16 \text{ ms} + T_S + 2,5 \times T_{SAFE} + T_{FAST} + T_A.$$

### **Para sistemas con E/S locales:**

$$\text{SRT máx.} = T_S + T_I + 2,5 \times T_{SAFE} + T_{FAST} + T_O + T_A.$$

o bien

$$\text{SRT máx.} = 15 \text{ ms} + T_S + 2,5 \times T_{SAFE} + T_{FAST} + T_A.$$

**NOTA:** En el caso de los PAC Hot Standby, para calcular el tiempo máximo de reacción de seguridad, se deben tener en cuenta los componentes adicionales a los cálculos anteriores:

- Mientras se produce un evento imprevisto y una conmutación, el tiempo máximo de reacción de seguridad puede incrementarse añadiendo el componente, página 163  $T_{SWITCH}$  a los cálculos anteriores.

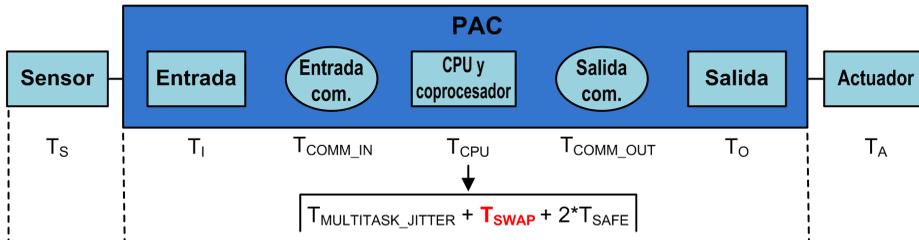
- Mientras el operador del sistema realiza un intercambio, el tiempo máximo de reacción de seguridad puede incrementarse añadiendo un componente, página 162  $T_{\text{SWAP}}$  a los cálculos anteriores.

## Tiempo de reacción del sistema durante un intercambio

Un intercambio es la acción que inicia el operador en un sistema Hot Standby, que provoca que los PAC primario y standby intercambien sus roles. Un intercambio consume tiempo adicional, porque mientras tanto no se puede perder información y todas las salidas del sistema deben tener un timeout de seguridad.

El componente de tiempo de intercambio añadido se suma al tiempo de  $T_{\text{CPU}}$  tras el componente  $T_{\text{JITTER}}$  normal, como se muestra a continuación:

El componente de tiempo  $T_{\text{SWAP}}$  se suma al tiempo de  $T_{\text{CPU}}$  tras el componente  $T_{\text{JITTER}}$  normal. A continuación se muestra esta secuencia. A excepción de la inclusión del componente de intercambio, la descripción del tiempo de reacción del sistema es la misma que la descrita anteriormente, página 157:



El componente de tiempo  $T_{\text{SWAP}}$  es la suma de lo siguiente:

$$T_{\text{ADDITIONAL\_JITTER}} + T_{\text{TRANSFER}}$$

Los componentes específicos del intercambio se describen de la siguiente forma:

Componente	Descripción	Valor calculado para el peor de los casos
$T_{\text{ADDITIONAL\_JITTER}}$	Fluctuación introducida por el sistema multitarea para reiniciar la tarea en el nuevo PAC. Por lo tanto, $T_{\text{ADDITIONAL\_JITTER}} = T_{\text{SAFE}}$ .	–
$T_{\text{TRANSFER}}$	Durante los diagnósticos de la tarea MAST, el PAC acepta el comando de intercambio y empieza a realizar la transferencia de todos los datos más recientes para cada tarea.	Consulte la fórmula a continuación.

$T_{\text{TRANSFER}}$  se puede calcular de la forma siguiente:

$$K3 \times (\text{MAST}_{\text{KB}} + 2 \times \text{SAFE}_{\text{KB}} + \text{FAST}_{\text{KB}}) + K4 \times (\text{MAST}_{\text{DFB}} + 2 \times \text{SAFE}_{\text{DFB}} + \text{FAST}_{\text{DFB}}) / 1000$$

Donde:

- $TASK_{KB}$  = Tamaño de los datos (en Kbytes) intercambiados para la TASK entre el PAC primario y el PAC standby.
- $MAST_{DFB}$  = El número de DFB declarados en la TASK.
- K3 y K4 son constantes con valores determinados por el módulo de CPU específico utilizado en la aplicación, como se muestra a continuación:

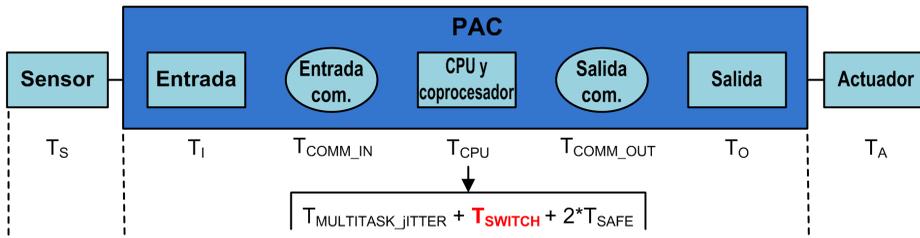
Coeficiente	BMEH582040S	BMEH584040S o BMEH586040S
K3	46,4 $\mu$ s/kB	14,8 $\mu$ s/kB
K4	Instancia de 34,5 $\mu$ s/DFB	Instancia de 11,0 $\mu$ s/DFB

Si el operador del sistema desea realizar un intercambio sin que las salidas del módulo de seguridad pasen al estado de recuperación, establezca el parámetro de timeout de seguridad de recuperación ( $S\_TO$ ) de los módulos de salida de seguridad en, al menos, un valor superior a:  $T_{MULTITASK\_JITTER} + T_{SWAP} + T_{SAFE}$ .

## Tiempo de reacción del sistema durante una conmutación

Una conmutación se produce cuando el PAC standby de un sistema Hot Standby se convierte en el PAC primario en respuesta a un evento imprevisto, por ejemplo, cuando el hardware del PAC primario de repente deja de estar operativo. El objetivo de la conmutación es que el nuevo PAC primario reemplace sin alteraciones al anterior y empiece a operar en el punto en el que el PAC primario antiguo ha dejado de funcionar. No obstante, puede que se vuelva a ejecutar el último ciclo. El objetivo del sistema es lograr la recuperación más rápida posible.

El componente de tiempo  $T_{SWITCH}$  se suma al tiempo  $T_{CPU}$  tras el componente  $T_{JITTER}$  normal. A continuación se muestra esta secuencia. Exceptuando la inclusión del componente de conmutación, la descripción del tiempo de reacción del sistema es la misma que la descrita anteriormente, página 157:



El componente de tiempo  $T_{SWITCH}$  es la suma de lo siguiente:

$$T_{DETECT} + T_{ADDITIONAL\_JITTER}$$

Los componentes específicos de la conmutación se describen de la siguiente forma:

Componente	Descripción	Valor calculado para el peor de los casos
T <sub>DETECT</sub>	El tiempo que utiliza el PAC standby para detectar y confirmar que el PAC primario ya no es operativo.	15 ms
T <sub>ADDITIONAL_JITTER</sub>	Fluctuación introducida por el sistema multitarea para reiniciar la tarea en el nuevo PAC. Por lo tanto, T <sub>ADDITIONAL_JITTER</sub> = T <sub>SAFE</sub> .	–

A diferencia del intercambio, no se necesita tiempo adicional para realizar una transferencia de datos.

Para permitir que el sistema responda a un evento imprevisto y realice una conmutación sin que las salidas del módulo de seguridad pasen al estado de recuperación, establezca el parámetro de timeout de seguridad de recuperación (S\_TO) de los módulos de salida de seguridad en, al menos, un valor superior a: T<sub>JITTER</sub> + T<sub>SWITCH</sub> + T<sub>SAFE</sub>.

## Configuración de los periodos máximos de las tareas SAFE y FAST de la CPU

El PAC de seguridad M580 puede realizar sólo una ejecución periódica de las tareas SAFE y FAST (no se admite la ejecución cíclica para estas tareas).

El **Periodo** de la tarea SAFE y los ajustes máximos permitidos del **Watchdog** de la CPU se configuran en la ficha **General** del diálogo **Propiedades de SAFE**. Los ajustes del **Timeout de recuperación** se configuran de la ficha **Configuración** para el módulo de salida, página 105.

De forma parecida, el **Periodo** de la tarea FAST y los ajustes máximos permitidos del **watchdog** de la CPU se configuran en la ficha **General** del diálogo **Propiedades de FAST**.

### NOTA:

- El rango permitido para los ajustes del periodo de la tarea SAFE es de 10 a 255 ms, con un valor predeterminado de 20 ms.
- El rango permitido para los ajustes del periodo de la tarea FAST es de 1 a 255 ms, con un valor predeterminado de 5 ms.
- El rango permitido para los ajustes del watchdog es de 10 a 500 ms, con un valor predeterminado de 250 ms.
- El rango permitido para los ajustes del timeout de recuperación de salida digital es de 0 a 65 535 ms, con un valor predeterminado de 500 ms.

Verifique que el ajuste del watchdog sea mayor que el periodo de la tarea SAFE.

Compruebe el ajuste del periodo de la tarea SAFE de la CPU al poner en marcha el proyecto. En este momento, Control Expert Safety proporciona los valores en tiempo real del PAC.

Puede encontrar esta información en Control Expert Safety en la ficha **Tarea** utilizando la entrada de menú **Herramientas > Pantalla de PLC**.

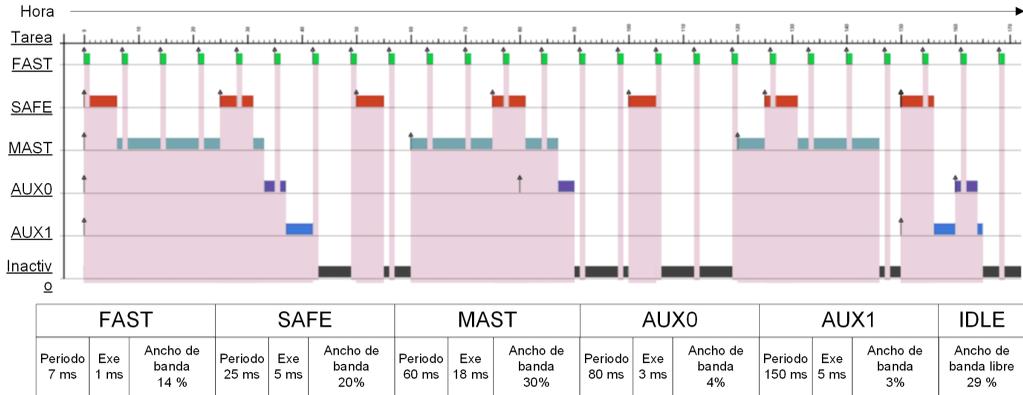
▲ ADVERTENCIA

**RIESGO DE SOBREPASAR EL TIEMPO DE SEGURIDAD DEL PROCESO**

Establezca el periodo máximo de la tarea SAFE de la CPU teniendo en cuenta el tiempo de seguridad del proceso. El periodo de la tarea SAFE de la CPU debe ser inferior al tiempo de seguridad de proceso del proyecto.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

En el esquema siguiente aparece la ejecución de cada tarea en un sistema multitarea y se muestra la priorización de recursos de la CPU en función de la prioridad de tarea.



**NOTA:** Cuando la tarea MAST no esté en modalidad cíclica, y para garantizar un rendimiento óptimo de la CPU, Schneider Electric recomienda dejar inactivo un 20 % del ancho de banda de la CPU.

## Cálculo del impacto de los periodos de ejecución de las tareas sobre el ancho de banda de la CPU

Cada tarea configurada consume una parte del tiempo de procesamiento o el ancho de banda de la CPU. El porcentaje calculado de ancho de CPU que consume una tarea es el resultado (o cociente) del tiempo de ejecución que requiere una tarea ( $E_{TASK}$ ) dividido entre el periodo de ejecución configurado para esa tarea ( $T_{TASK}$ ), y se puede mostrar de la siguiente forma:

$$\text{Ancho de banda de tarea} = E_{TASK} / T_{TASK}.$$

Por tanto, el porcentaje de ancho de banda de la tarea que consume una aplicación es la suma de los porcentajes de ancho de banda de la CPU consumidos para todas las tareas.

**NOTA:** Cuando la tarea MAST no esté en modalidad cíclica, y para garantizar un rendimiento óptimo de la CPU, Schneider Electric recomienda que el porcentaje total de ancho de banda de la CPU consumido por una aplicación no supere el 80 %.

En la tabla siguiente se muestran dos aplicaciones e indica el impacto de las tareas de alta prioridad (FAST y SAFE) sobre el uso de ancho de banda de la CPU.

#	FAST			SAFE			MAST			AUX0			Total
	Per.	Ejec.	% BW	Per.	Ejec.	% BW	Per.	Ejec.	% BW	Per.	Ejec.	% BW	
1	5 ms	1 ms	20 %	20 ms	5 ms	25 %	50 ms	18 ms	35 %	200 ms	30 ms	15 %	96 %
2	7 ms	1 ms	14 %	25 ms	5 ms	20 %	60 ms	18 ms	30 %	200 ms	30 ms	15 %	79 %

Per. = Periodo de tarea ( $T_{TASK}$ )  
Ejec.= Tiempo de ejecución requerido para la tarea ( $E_{TASK}$ )  
% BW = Ancho de banda de la tarea.

## Impacto de las comunicaciones de CIP Safety en el tiempo de reacción del sistema de seguridad

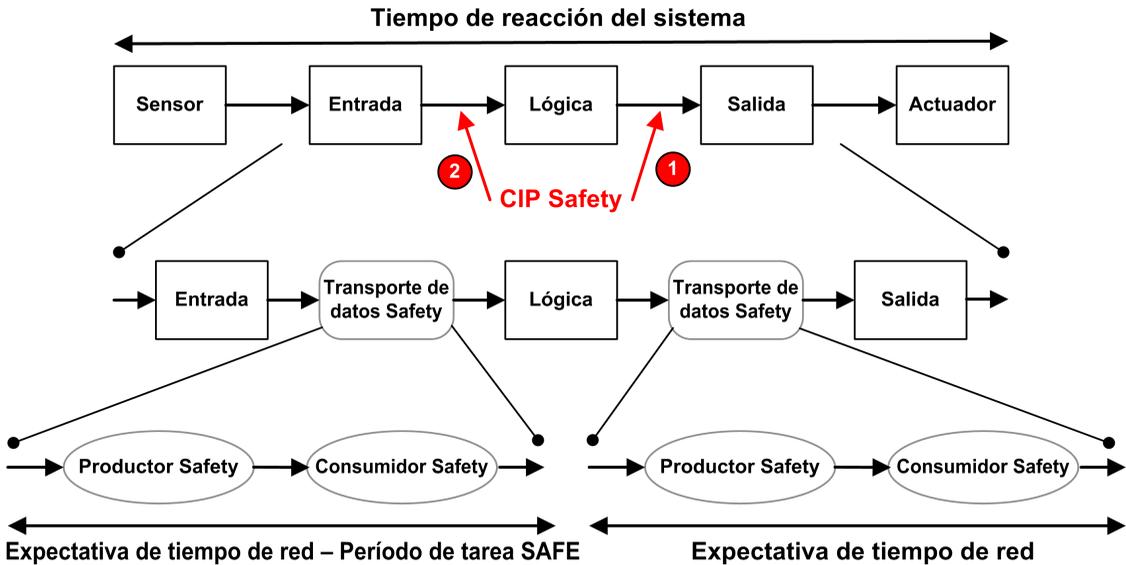
### Introducción

El tiempo consumido por la comunicación de CIP Safety, denominado *expectativa de tiempo de red*, se añade al *tiempo de reacción del sistema*, página 157 para pasar a formar parte de este. La expectativa de tiempo de red representa el periodo de tiempo máximo o, en el peor de los casos, el periodo que comienza cuando el productor de datos de seguridad captura los datos y termina cuando la aplicación de consumo detecta un estado de seguridad. También incluye los errores que se produzcan durante la producción y el consumo.

Si la comunicación CIP Safety tiene lugar entre una entrada y la lógica, sustituya la variable de término TCOMM\_IN en el cálculo del tiempo de seguridad del proceso, página 157 por *Expectativa de tiempo de red - Periodo de tarea SAFE*. Si la comunicación CIP Safety tiene lugar entre la lógica y una salida, sustituya la variable TCOMM\_OUT en el cálculo del tiempo de seguridad del proceso por *Expectativa de tiempo de red*.

Las medidas predeterminadas de la expectativa de tiempo red variarán en función del rol de la CPU de seguridad M580 de productor o consumidor.

En el siguiente diagrama se representan los elementos de la expectativa de tiempo de red, así como su ubicación en el contexto del tiempo de reacción del sistema:



1 CPU CIP Safety como productor

2 CPU CIP Safety como consumidor

## Cálculo de la expectativa de tiempo de red

La expectativa de tiempo de red puede calcularse mediante la siguiente fórmula:

$$\text{Expectativa de tiempo de red} = \text{Multiplicador\_expectativa\_tiempo\_red} * 128 \mu\text{s} > (\text{EPI} * \text{Multiplicador\_timeout} + \text{Tiempo\_mensaje\_seguridad(máx.)} + \text{Tiempo\_mensaje\_coordinación\_horaria(máx.)} + \text{Constante\_corrección\_conexión} * 128 \mu\text{s})$$

Donde:

- **Tiempo\_mensaje\_seguridad(máx.)** es el tiempo real desde que el producto de datos de seguridad captura los datos hasta el momento en que los datos de seguridad se transmiten a la aplicación de consumo para su uso.
- **Tiempo\_mensaje\_coordinación\_horaria(máx.)** es el tiempo máximo que podría tardar la información de coordinación horaria en enviarse del consumidor al productor.
- **Multiplicador\_timeout** es un parámetro empleado en el procesamiento del protocolo CIP Safety que determina el número de mensajes que podrían perderse antes de declararse un error de conexión. Un Multiplicador\_timeout de 1 indica que no puede perderse ningún mensaje.

- **Constante\_corrección\_conexión** es un valor en incrementos de 128  $\mu$ s que se resta de la marca de tiempo para representar el peor error posible a causa de la desviación horaria, la naturaleza asíncrona de los relojes del productor y el consumidor, y el tiempo mínimo que tardará el mensaje de coordinación horaria en transmitirse del consumidor al producto.
- **EPI** es el intervalo de paquetes previsto (expected packet interval); se basa en el periodo de tarea SAFE configurado.
- **Multiplicador\_expectativa\_tiempo\_red** y **Multiplicador\_timeout** son parámetros de comunicación CIP que se configuran para el marco de conexión SafetyOpen de tipo 2, página 376.

## Valores predeterminados de expectativa de tiempo de red

El cálculo predeterminado para el valor de expectativa de tiempo de red dependerá del rol de la CPU CIP Safety de consumidor (caso 2 del diagrama anterior) o productor (caso 1).

### CPU como consumidor (caso 2):

- $\text{Multiplicador\_timeout} = 2$
- $\text{EPI} = \text{Periodo de tarea SAFE} / 2$
- $\text{Tiempo\_mensaje\_seguridad(máx.)} = \text{Periodo de tarea SAFE} + 20 \text{ ms}$  (peor caso)
- $\text{Tiempo\_mensaje\_coordinación\_horaria(máx.)} = \text{Periodo de tarea SAFE} + 20 \text{ ms}$  (peor caso)
- $\text{Constante\_corrección\_conexión} = 0 \text{ ms}$

**Expectativa de tiempo de red =  $1,5 * \text{Expectativa\_tiempo\_red\_mínima} = 1,5 * (3 * \text{Periodo tarea SAFE} + 40 \text{ ms}) = 4,5 * \text{Periodo tarea SAFE} + 60 \text{ ms}$**

### CPU como productor (caso 1):

- $\text{Multiplicador\_timeout} = 2$
- $\text{EPI} = \text{Periodo de tarea SAFE}$
- $\text{Tiempo\_mensaje\_seguridad(máx.)} = \text{Periodo de tarea SAFE} + 20 \text{ ms}$  (peor caso)
- $\text{Tiempo\_mensaje\_coordinación\_horaria(máx.)} = \text{Periodo de tarea SAFE} + 20 \text{ ms}$  (peor caso)
- $\text{Constante\_corrección\_conexión} = 0 \text{ ms}$

**Expectativa de tiempo de red =  $1,5 * \text{Expectativa\_tiempo\_red\_mínima} = 1,5 * (4 * \text{Periodo tarea SAFE} + 40 \text{ ms}) = 6 * \text{Periodo tarea SAFE} + 60 \text{ ms}$**

# Biblioteca de seguridad

## Contenido de este capítulo

Biblioteca de seguridad ..... 169

# Biblioteca de seguridad

## Introducción de la biblioteca de seguridad

Al instalar Control Expert Safety, se incluye automáticamente una biblioteca de seguridad de funciones elementales (EFs), bloques de funciones elementales (EFBs) y bloques de funciones derivadas. Estos EF, EFB y DFB se identifican con el prefijo "S\_" y se reservan para usarlos en secciones de código gestionadas por la tarea SAFE.

**NOTA:** También se instala un conjunto adicional de EF, EFB y DFB. Este es el mismo conjunto de objetos de datos que utilizan los PAC M580 no que no son de seguridad. Estos EF, EFB y DFB sólo se pueden utilizar en secciones de código gestionadas por las tareas de espacio de nombres de proceso (MAST, FAST, AUX0 y AUX1).

Para obtener una descripción de los bloques incluidos en la biblioteca de seguridad M580, consulte el documento *Control Expert* Bibliotecade bloques de seguridad de Control.

## Funciones y bloques de funciones de seguridad certificados

### **▲ ADVERTENCIA**

#### **COMPORTAMIENTO IMPREVISTO DE LA APLICACIÓN**

- No utilice V1.00 del bloque de funciones derivados S\_GUARD\_LOCKING en la aplicación.
- En Unity Pro 13.0 XLS o posterior, actualice el bloque de funciones S\_GUARD\_LOCKING en la aplicación con V1.01 o posterior y regenere la aplicación.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

#### **NOTA:**

Unity Pro es el nombre anterior de Control Expert para la versión 13.1 o anterior.

Estos corresponden al subconjunto de EF y bloques de funciones, que se pueden utilizar en la lógica de seguridad. Estos se proporcionan en la biblioteca de seguridad:

Familia	Grupo o nombre	Tipo	Descripción
Lógica	S_AND_*, S_OR_*, S_XOR_*, S_NOT_*, S_SHL_*, S_SHR_*, S_ROR_*, S_ROL_*	EF	Específico del tipo, por ejemplo, S_AND con 2 a 32 entradas (código en línea)
Lógica	S_RS, S_SR, S_F_TRIG, S_R_TRIG	EFB	–
Matemáticas	S_ADD_*, S_MUL_*, S_SUB_*, S_DIV_*, S_ABS_*, S_SIGN_*, S_NEG_*, S_MOVE, S_SQRT_REAL	EF	Tratamiento de errores detectados específicos del tipo (por ejemplo, desborde) que se deben tener en cuenta (código en línea)
Comparación	S_GT_*, S_GE_*, S_LT_*, S_LE_*, S_NE_*, S_EQ_*	EF	Específico del tipo (código en línea)
Estadística	S_LIMIT_*, S_MAX_*, S_MIN_*, S_MUX_*, S_SEL	EF	Específico del tipo (código en línea)
Tipo a tipo	S_BIT_TO*, S_BOOL_TO*, S_BYTE_TO*, S_DINT_TO*, S_DWORD_TO*, S_INT_TO*, S_REAL_TO*, S_TIME_TO*, S_UDINT_TO*, S_UINT_TO*, S_WORD_TO*	EF	Específico del tipo (código en línea)
Temporizadores y contadores	S_CTU_*, S_CTD_*, S_CTUD_*	EFB	Específico del tipo
Temporizadores y contadores	S_TON, S_TOF, S_TP	EFB	–
Entre pares	S_RD_ETH_MX, S_WR_ETH_MX, S_RD_ETH_MX2, S_WR_ETH_MX2	DFB	Funciones para realizar una comunicación entre pares de seguridad
Conexión de actuador	S_EDM, S_ENABLE_SWITCH, S_ESPE, S_OUTCONTROL, S_GUARD_LOCKING, S_GUARD_MONITORING, S_MODE_SELECTOR	DFB	Bloques de funciones de seguridad de máquinas vinculados a actuadores
Conexión del sensor	S_EQUIVALENT, S_ANTIVALENT, S_EMERGENCYSTOP, S_TWO_HAND_CONTROL_TYPE_II, S_TWO_HAND_CONTROL_TYPE_III, S_MUTING_SEQ, S_MUTING_PAR, S_AI_COMP	DFB	Bloques de funciones de seguridad de máquinas vinculados a sensores
Sistema	S_SYST_STAT_MX, S_SYST_TIME_MX, S_SYST_CLOCK_MX, S_SYST_RESET_TASK_BIT_MX, S_SYST_READ_TASK_BIT_MX	EFB	Bloques de funciones del sistema

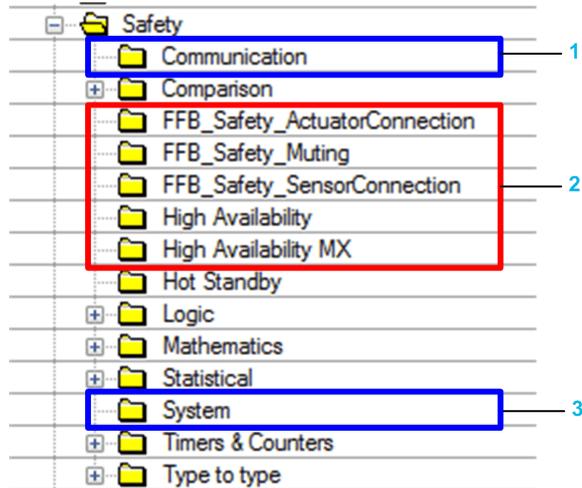
## Funciones y bloques de funciones de seguridad no certificados

Estos corresponden al subconjunto de bloques de funciones derivados (DFB) que se pueden utilizar en la lógica de seguridad. Estos bloques de funciones no están certificados. Su finalidad es proporcionarle bloques de funciones de seguridad de ejemplo que se puedan reutilizar y adaptar fácilmente. Puede copiar y pegar estos bloques de funciones en la aplicación y cambiarlos para satisfacer los requisitos de la aplicación.

Familia	Grupo o nombre	Tipo	Descripción
MX de alta disponibilidad	S_DIHA, S_AIHA	DFB	Función para módulos de entrada digital SIL2 o SIL3 de alta disponibilidad (código en línea)
Conexión del sensor	AI_COMP	DFB	Bloques de funciones de seguridad de máquinas vinculados a sensores

## Visualización de la biblioteca de seguridad en Control Expert

Puede acceder a la biblioteca de seguridad sólo desde la tarea SAFE. Cuando abra la biblioteca de seguridad en el **editor FBD**, la biblioteca de seguridad presenta los grupos de EF, EFB y DFB. Entre algunos de estos grupos se incluyen las versiones de seguridad de funciones y bloques que se encuentran en tareas que no son de seguridad. Otros grupos, que se indican más abajo, contienen funciones y bloques específicos de la tarea SAFE:



1 Bloques para leer y escribir valores de datos de seguridad.

2 Bloques para realizar tareas específicas de seguridad.

3 Bloques para leer y escribir valores del sistema de seguridad.

Para ver un ejemplo de cómo se implementan algunos de estos bloques de seguridad, consulte el ejemplo de configuración de comunicación de PAC a PAC, página 188, que incluye S\_RD\_ETH\_MX y S\_WR\_ETH\_MX.

Consulte también la Biblioteca de Bloques de Seguridad *EcoStruxure™ Control Expert Block Library* para obtener una descripción de cada función y bloque de seguridad disponibles.

# Separación de datos en un sistema de seguridad M580

## Contenido de este capítulo

Separación de datos en un proyecto de seguridad de M580 .....	174
Cómo transferir datos entre áreas de espacios de nombres.....	177

## Introducción

En este capítulo se presenta la división de datos en un sistema de seguridad M580.

# Separación de datos en un proyecto de seguridad de M580

## Ámbito y separación de datos

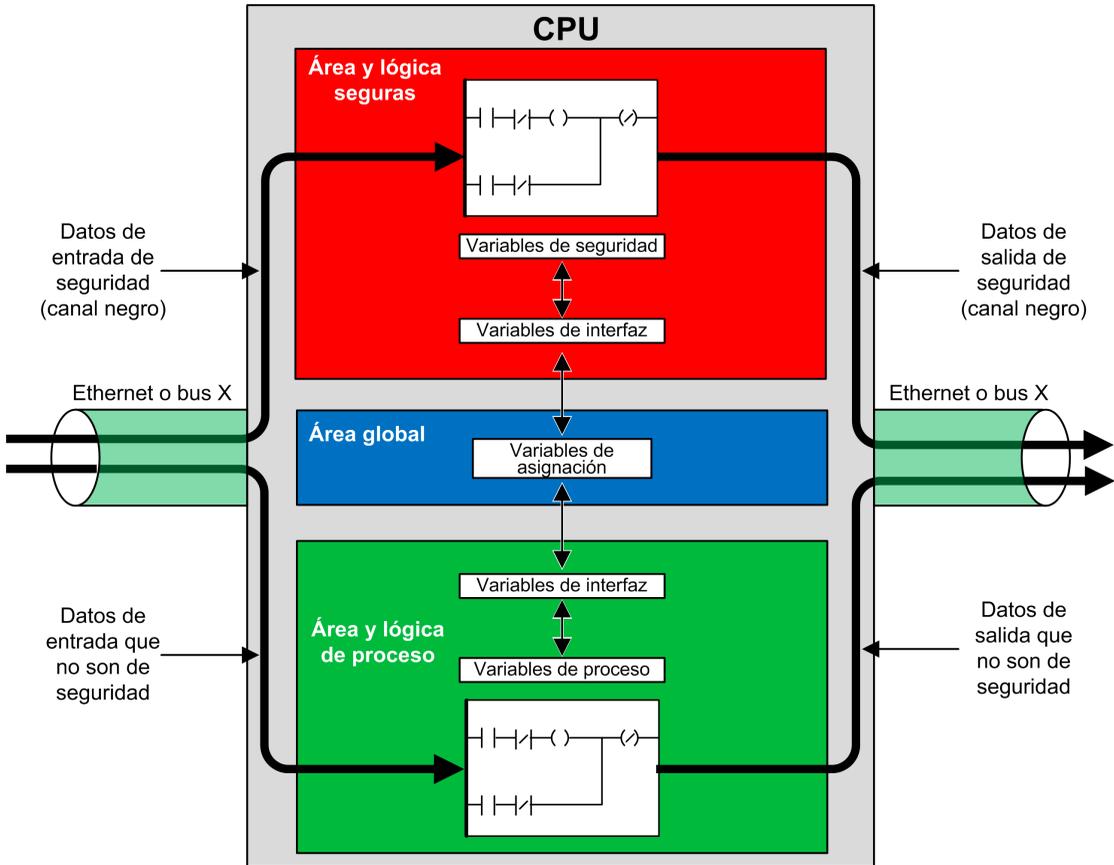
Un proyecto de seguridad de M580 incluye tanto un programa de seguridad como un programa (que no es de seguridad) de proceso. Control Expert aísla la lógica y los datos que utiliza el programa de seguridad de la lógica y los datos que utiliza el programa de proceso. Control Expert lo consigue colocando cada parte del proyecto en su propio espacio de nombres (que también se conoce por área), ya sea *segura* o de *proceso*.

Como resultado de este diseño, el ámbito de una variable de seguridad se limita al área segura y el ámbito de una variable de proceso se limita al área de proceso. Esto resulta evidente cuando añade una lógica de programa a la aplicación.

- Cuando configura una tarea EF O EFB en la tarea SAFE, sólo son visibles las variables creadas en el área segura. Las variables creadas en el área de proceso no son visibles.
- Cuando configura un EF o EFB en una tarea (MAST, FAST, AUX0 o AUX1) no segura, sólo son visibles las variables creadas en el área de proceso. Las variables creadas en el área segura no son visibles.

Para permitir la comunicación entre el área segura y el área de proceso, Control Expert también proporciona un área *global*. El área global se utiliza como paso para las transmisiones de datos entre el área segura y el área de proceso. Este se consigue declarando variables de interfaz en las áreas de seguridad y proceso y, a continuación, vinculándolas a variables de asignación declaradas en el área global.

Esta separación de datos de la CPU y el coprocesador de seguridad M580 se describe gráficamente más abajo:



## Propiedades de área segura, de proceso y global

Las tres áreas de datos de un proyecto de seguridad de M580 tienen las propiedades siguientes:

Área	Tipos de variables admitidas	Ámbito	Acceso externo
Global	Sólo variables no ubicadas. <b>NOTA:</b> Las variables ubicadas no se pueden asignar a una variable de interfaz de seguridad o proceso.	Puede obtener acceso a: <ul style="list-style-type: none"> <li>• Variables de seguridad a través del direccionamiento del espacio de nombres.</li> <li>• Variables de proceso a través de direccionamiento del espacio de nombres.</li> <li>• Otras variables globales.</li> </ul>	Se puede acceder a las variables de las tres áreas con las aplicaciones HMI, SCADA o FactoryCast.  Consulte la nota que aparece más abajo.
Seguro	Sólo variables no ubicadas.	Puede acceder sólo a otras variables de seguridad.	
Proceso	Ambos: <ul style="list-style-type: none"> <li>• Variables ubicadas</li> <li>• Variables no ubicadas</li> </ul>	Puede acceder sólo a otras variables de proceso.	

Cundo un visualizador externo intenta leer una variable de proceso, el formato de direccionamiento depende de si se ha seleccionado el ajuste **Uso del espacio de nombres de proceso** del área **Ámbito > común** de la ventana **Herramientas > Ajustes del proyecto...** Puede seleccionar el ajuste **Uso del espacio de nombres de proceso**:

- Si está seleccionado, la pantalla de operador sólo puede leer variables del área de proceso utilizando el formato "PROCESS.<Nombre de variable>".
- Si no está seleccionado, la pantalla de operador sólo puede leer variables del área de proceso utilizando el formato "<Nombre de variable>" sin el prefijo "PROCESS". En este caso, verifique que cada nombre de variable de proceso sea único y que no haya ninguna variable global con el mismo nombre.

**NOTA:** Si el ajuste **Uso del espacio de nombres de proceso** no está seleccionado, verifique que cada nombre de variable de proceso sea único y que no haya ninguna variable global con el mismo nombre. Si el área global y el área de proceso comparten un nombre de variable, Control Expert detectará un error cuando genere el proyecto.

# Cómo transferir datos entre áreas de espacios de nombres

## Introducción

El PAC de seguridad M580 incluye tres editores de datos diferentes:

- Un **Editor de datos de seguridad** para gestionar los datos utilizados en el espacio de nombres seguro.
- Un **Editor de datos de proceso** para gestionar los datos utilizados en el espacio de nombres de proceso.
- Un **Editor de datos globales** para gestionar variables globales y tipos de datos utilizados en toda la aplicación.

Tanto el **Editor de datos de seguridad** como el **Editor de datos de proceso** incluyen una ficha **Interfaz**. Utilice la ficha **Interfaz** para crear variables no ubicadas en ese espacio de nombres de proceso. La ficha **Interfaz** presenta dos grupos de variables no ubicadas:

- <entradas>: Una variable creada en este grupo se puede vincular a una variable de transferencia de ámbito global y recibir datos de ella en el **Editor de datos globales**.
- <salidas>: Una variable de este grupo se puede vincular a una variable de transferencia de ámbito global y enviar datos a ella en el **Editor de datos globales**.

**NOTA:** Una variable creada en cualquier de estas fichas **Interfaz** debe tener todas las características siguientes:

- Ser una variable de categoría EDT o DDT.
- Pertener al mismo tipo de datos que la variable a la que está vinculada.
- No ser una variable vinculada a un bit extraído de una variable ubicada (por ejemplo, que no sea %MW10.1).

Las variables no ubicadas creadas en los grupos de ficha **Interfaz** del **Editor de datos de seguridad** y del **Editor de datos de proceso** se pueden vincular de la forma siguiente:

Una variable de proceso de este grupo en el Editor de datos de proceso...	Se puede vincular a una variable de seguridad de este grupo en el Editor de datos de seguridad...
<entradas>	<salidas>
<salidas>	<entradas>

Al usar estos tres editores de datos, puede configurar la transferencia de datos entre el espacio de nombres seguro y el espacio de nombres de proceso.

## Transferencia de datos entre espacios de nombres

El proceso de transferencia de datos del espacio de nombres seguro al espacio de nombres de proceso y el proceso inverso son iguales pero invertidos. En el ejemplo siguiente se muestra cómo transferir datos del área de proceso al área segura:

Paso	Acción
1	Abra el <b>Editor de datos de proceso</b> , haga clic en la ficha <b>Interfaz</b> del programa y cree una variable nueva en la parte <b>&lt;salidas&gt;</b> del editor de datos.
2	Abra el <b>Editor de datos de seguridad</b> , haga clic en la ficha <b>Interfaz</b> del programa y cree una variable nueva del mismo tipo que el creado en el paso 1 en la parte <b>&lt;entradas&gt;</b> del editor de datos. A continuación, haga doble clic en el campo <b>Parámetro efectivo</b> . Se abre el cuadro de diálogo <b>Editor de ámbito de datos: Selección de variables</b> .
3	En el menú desplegable de la esquina superior derecha, seleccione el espacio de nombres de destino <b>PROCESS</b> . Se muestran las variables del espacio de nombres PROCESS seleccionado en la parte <b>&lt;salidas&gt;</b> .
4	Seleccione la variable de proceso creada en el paso 1 que se vinculará a la variable segura creada en el paso 2 y luego haga clic en <b>Aceptar</b> . La variable de destino seleccionada se muestra en el campo <b>Parámetro efectivo</b> .
5	<b>Guarde</b> los cambios efectuados.

Después de compilar, descargar y ejecutar el programa de aplicación editado, el valor se transfiere de la forma siguiente:

- Se publican los datos de la ficha **Interfaz** creados en las **<salidas>** al final de la ejecución de la tarea correspondiente.
- Se suscriben los datos de la ficha **Interfaz** creados en las **<entradas>** al principio de la ejecución correspondiente.

# Comunicaciones del sistema de seguridad M580

## Contenido de este capítulo

Sincronización horaria.....	180
Comunicaciones entre pares .....	186
Comunicación de CPU a E/S de seguridad de M580 .....	216

## Introducción

En este capítulo se describen las comunicaciones del sistema de seguridad M580.

# Sincronización horaria

## Introducción

Para PAC con la versión del firmware de la CPU 3.10 o anterior:	Es necesario configurar el servicio NTP para permitir una comunicación segura. Tanto los emisores como los receptores deben tener la hora sincronizada mediante los servicios NTP.
Para PAC con la versión del firmware de la CPU 3.20 o posterior:	La sincronización horaria segura se basa en un reloj interno y "monotónico". La comunicación segura no necesita la sincronización horaria de NTP: <ul style="list-style-type: none"> <li>• La CPU de seguridad comparte su hora segura con todas sus E/S locales y remotas.</li> <li>• El módulo de comunicación de E/S remotas BM•CRA31210 necesita la versión del firmware 2.60 o posterior.</li> <li>• Para la comunicación entre pares, las CPU comparten su hora de seguridad.</li> </ul>

## Configuración de la sincronización horaria con la versión del firmware de la CPU 3.10 o anterior

### Introducción

Si está instalando módulos de E/S de seguridad en una estación RIO, la hora actual debe configurarse para el PAC. Este proceso se puede llevar a cabo en tres diseños distintos con la versión del firmware de la CPU 3.10 o anterior:

1. **Diseño de servidor NTP remoto con CPU como cliente NTP:** Configure un dispositivo en la red de control como servidor NTP, luego configure la CPU de seguridad como cliente NTP.
2. **Diseño del servidor NTP local:** Configure la CPU de seguridad como servidor NTP para los dispositivos en la red Ethernet RIO.
3. **Diseño de servidor NTP remoto con eNOC o eNOP:** Configurar un dispositivo en la red de control como servidor NTP, luego configurar un módulo - ya sea BMENOP0300o BMENOC0301/11 módulos de comunicaciones - en el bastidor principal local y habilitar la función opcional Actualización **de tiempo de CPU > Actualizar tiempo de CPU con este módulo** en el DTM correspondiente. Si se configura una estación RIO con dispositivos de seguridad, configure la CPU de seguridad como servidor NTP, tal como se describe en el caso 2 anterior.

En cualquier diseño, deberá realizar las siguientes acciones adicionales:

- Habilitar el servicio NTP.
- Establecer el periodo de consulta de NTP en 20 s.

Si la CPU de seguridad no está configurada como un servidor NTP o un cliente NTP, tal como se ha descrito anteriormente, no se sincronizarán los ajustes de hora de los módulos de E/S de seguridad remotos y la CPU, y la comunicación del canal negro no funcionará correctamente. Las entradas y salidas de los módulos de E/S de seguridad en estaciones RIO pasarán al estado de seguridad (deenergizado) o de recuperación.

## **▲ ATENCIÓN**

### **RIESGO DE FUNCIONAMIENTO IMPREVISTO**

Si coloca los módulos de E/S en una estación RIO, la hora actual se debe configurar para el PAC con la versión del firmware 3.10 o anterior. Habilite el servicio NTP para su sistema M580 y configure la CPU de seguridad como un servidor NTP o un cliente NTP.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

Schneider Electric recomienda configurar dos fuentes NTP. Estos se pueden configurar de manera redundante con un conjunto como primario y el segundo como servidor de tiempo de espera. Sin embargo, ambos servidores deben sincronizarse a la hora. Cualquier ajuste de tiempo igual o mayor que 2 s en cualquier período de sondeo NTP hará que la CPU y los módulos de I/O de seguridad se desincronicen y se desvíen del servidor de tiempo NTP.

## **Cambio de los ajustes de hora de NTP durante las operaciones**

## **▲ ATENCIÓN**

### **RIESGO DE APAGADO DEL SISTEMA DE SEGURIDAD**

Al utilizar Control Expert V13 o V13.1, o bien al utilizar el firmware de CPU 2.70 o anterior, no cambie el ajuste de hora en el servidor NTP o la CPU.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

Si se cambia la hora durante las operaciones, puede perderse la comunicación y apagarse el sistema de seguridad.

Si se cambia la hora durante el funcionamiento, puede generarse una desincronización horaria con el reloj de referencia. También puede activarse una pérdida de la comunicación de seguridad, por lo que las E/S pasarán al estado de recuperación o de seguridad. Supervise el sistema para ver si se produce la desincronización y, si es así, restaure la sincronización para evitar la pérdida de comunicación. Si se produce la desincronización, utilice el procedimiento siguiente, página 182 para volver a sincronizar el sistema.

**Si utiliza Control Expert V14 o superior y utiliza firmware 2.80, 2.90 ó 3.10 de la CPU:**  
Es posible cambiar la configuración de tiempo en el servidor NTP o en la CPU durante el funcionamiento sin un impacto negativo. Realice esta operación siguiendo el procedimiento que se indica a continuación justo después de modificar la hora.

Consulte el tema *NTP* la ficha NTP en el manual *de referencia de hardware* Modicon M580 para obtener información sobre cómo configurar el servicio NTP para una M580 CPU.

## Procedimiento de sincronización de los ajustes de hora de NTP

Cuando se apague y encienda o se resetee la CPU y esta reciba inicialmente un ajuste de hora procedente de un servidor NTP externo, siga el procedimiento que se indica a continuación para sincronizar la hora de la CPU.

### ⚠ ATENCIÓN

#### RIESGO DE EQUIPO INOPERATIVO

Cuando utilice la función opcional **Actualizar hora de la CPU con este módulo** en un módulo BMENOP0300 o BMENOC0301/11 para actualizar la hora del PAC, una vez que la hora procedente del servidor NTP externo pase a estar operativa (cuando %SW152 pase de 0 a 1), sincronice la hora de seguridad con el servidor NTP externo por medio de %SW128. Siga el procedimiento que se indica a continuación para sincronizar la hora de NTP.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

El siguiente procedimiento es válido con la tarea SAFE en estado RUN (ejecución), con Control Expert V14.0 o posterior y la versión del firmware de la CPU 2.80, 2.90 o 3.10:

Paso	Acción
1	Compruebe que la hora de la CPU o del servidor NTP externo sea válida y estable y funcione correctamente.
2	Si la configuración incluye una o varias estaciones eRIO, después de que el servicio NTP vuelva a funcionar o de que se modifique la hora (lo cual ha generado la desincronización), espere 2 periodos de consulta NTP para que el nuevo valor de hora de referencia se envíe a todos los módulos CRA.
3	Sincronice la hora del sistema en el reloj de referencia mediante la palabra de sistema %SW128: <ul style="list-style-type: none"> <li>Establezca %SW128 en 16#1AE5 durante un mínimo de 500 ms.</li> <li>A continuación, establezca %SW128 en #E51A durante un mínimo de 500 ms.</li> </ul>
4	Compruebe que la hora esté sincronizada. Para ello, verifique que los valores de los parámetros CPU_NTP_SYNC y M_NTP_SYNC en el DDDT de las E/S de seguridad sean verdaderos (1).

Si esta secuencia de sincronización no se ejecuta correctamente, ejecútela de nuevo.

## AVISO

### RIESGO DE APAGADO DE LA SEGURIDAD DEL SISTEMA

- Si utiliza Control Expert V14.0 o posterior y la versión del firmware de la CPU 2.80 o posterior para modificar la hora del PAC, deberá completar dicha modificación siguiendo el procedimiento de sincronización descrito anteriormente.
- Si no realiza un procedimiento de sincronización, las E/S de seguridad podrán acceder a su estado seguro o de recuperación cuando el reloj cambie durante aproximadamente un timeout de retardo de comunicación.

**Si no se siguen estas instrucciones, pueden producirse daños en el equipo.**

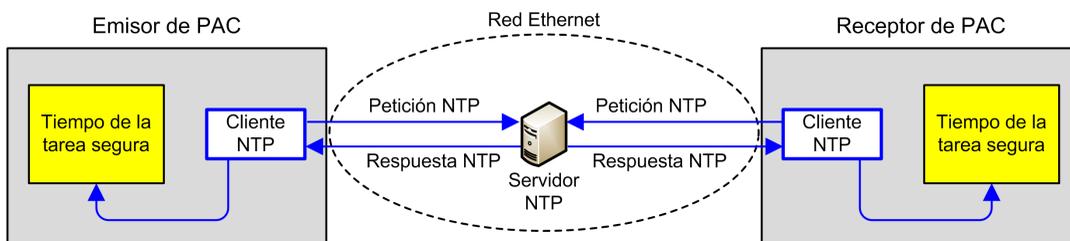
Durante las operaciones de sincronización horaria del paso 3, se deshabilitarán algunos diagnósticos de la comunicación segura durante 500 ms. Schneider Electric recomienda realizar como máximo una modificación y una sincronización al día.

## Servicio NTP para comunicación entre pares

La comunicación Ethernet segura de PAC a PAC requiere que se sincronice la base de tiempo, tanto del PAC emisor como del PAC receptor.

**NOTA:** Schneider Electric recomienda configurar en cada PAC (ya sea la CPU de seguridad, un módulo de comunicaciones BMENOP0300 o un módulo de comunicaciones BMENOC0301/11) un cliente NTP, así como configurar otro dispositivo de red como servidor NTP.

En la figura siguiente se describe el principio de sincronización de base de tiempo de los PAC emisor y receptor:



En Control Expert, configure los parámetros del servicio NTP para cada cliente de la siguiente forma:

- Seleccione **Cliente NTP**.
- Establezca el campo **Dirección IP del servidor NTP primario** en el ajuste de dirección IP para el servidor NTP remoto.
- Schneider Electric recomienda que establecer un valor de **Periodo de consulta** en 20 segundos.

## Coherencia de la hora del servidor NTP y bits del sistema

Coherencia de la hora del servidor NTP:

- Si la hora del servidor NTP es coherente con la hora del PAC interno que muestra el EF `S_SYST_CLOCK`, con menos de 2 segundos de diferencia, el valor de tiempo del EF `S_SYST_CLOCK` se actualiza con la última hora recibida del servidor NTP filtrada con una pendiente de 1 ms/s.
- Si la hora recibida del servidor NTP difiere respecto a la hora del PAC interno que muestra el EF `S_SYST_CLOCK` en más de 2 segundos, entonces:
  - el PAC ignora la última hora recibida del servidor NTP,
  - el valor de tiempo que muestra el EF `S_SYST_CLOCK` se actualiza internamente,
  - el parámetro `status` de `S_SYST_CLOCK` se establece en 0 y
  - el parámetro de salida `SYNCHRO_NTP` de los DFB `S_RD_ETH_MX` y `S_WR_ETH_MX` se establece en 0 para indicar esta condición.

En este caso, puede restablecer la hora del PAC interno realizando una de las acciones siguientes:

- Reinicializar la aplicación con un arranque en frío
- Descargar la aplicación
- Reiniciar el PAC
- Seguir los pasos para cambiar los ajustes de hora de NTP, página 182

**NOTA:** Si se pierde la sincronización de NTP en uno de los dos PAC (parámetro `SYNCHRO_NTP` establecido en 0), tanto la base de tiempo del PAC emisor como del receptor pueden perder la sincronización. En este caso, la comunicación entre pares segura puede dejar de estar operativa (el parámetro de salida `health` del DFB `S_RD_ETH_MX` se establece en 0).

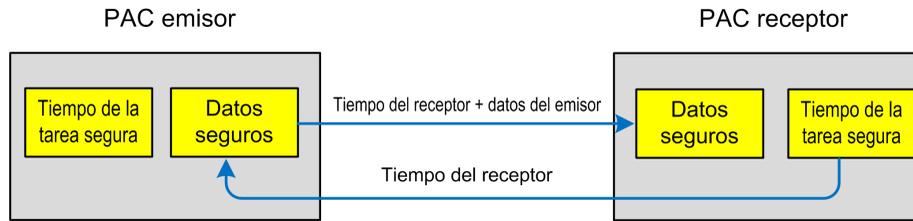
## Sincronización horaria para la versión del firmware de la CPU 3.20 o posterior

### Sincronización horaria para la comunicación entre pares

**NOTA:** Con la versión del firmware de la CPU 3.20 o posterior, no se utiliza el servicio NTP para la sincronización horaria.

La comunicación segura Ethernet de PAC a PAC requiere que tanto el PAC emisor como el PAC receptor compartan una hora segura común.

En la figura siguiente, se describe el principio de hora compartida de los PAC emisor y receptor:



En Control Expert, configure lo siguiente:

- una comunicación para la transmisión de datos del emisor al receptor
- una comunicación para la transmisión de hora segura del receptor al emisor

## Coherencia de la hora

La CPU distribuye una hora de seguridad interna (independiente del protocolo NTP) entre sus módulos de E/S de seguridad locales y remotos.

# Comunicaciones entre pares

## Introducción

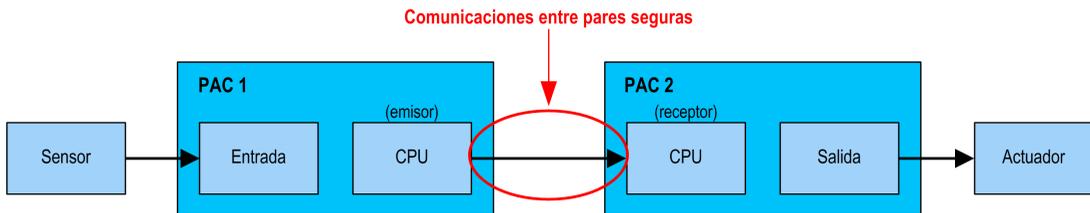
En esta sección se describen las comunicaciones entre pares entre los distintos PAC de seguridad M580.

## Comunicación entre pares

### Introducción

Puede configurar dos PAC de seguridad de M580 para realizar comunicaciones seguras entre pares a través de Ethernet. La configuración se basa en la comunicación de explorador Modbus TCP, incorporada en un canal negro.

A continuación, se ofrece la descripción general funcional de la comunicación entre pares:



Dos bloques de funciones elementales realizan la comunicación desde la biblioteca de bloques de funciones de M580, que gestionan el bucle de seguridad en el nivel de SIL3. El protocolo detecta los errores de transmisión, incluidas las omisiones, las inserciones, las secuencias desordenadas, los retardos, el direccionamiento impreciso y los bits engañosos, y gestiona las retransmisiones.

Esta comunicación entre pares segura solo es posible entre los siguientes elementos:

- dos PAC de seguridad M580, ambos con la versión del firmware de la CPU 3.10 o anterior
- dos PAC de seguridad M580, ambos con la versión del firmware de la CPU 3.20 o posterior

**NOTA:** La comunicación entre pares segura también es posible entre un PLC de seguridad Modicon Quantum y un PLC de seguridad M580 con la versión del firmware de la CPU 3.10 o anterior.

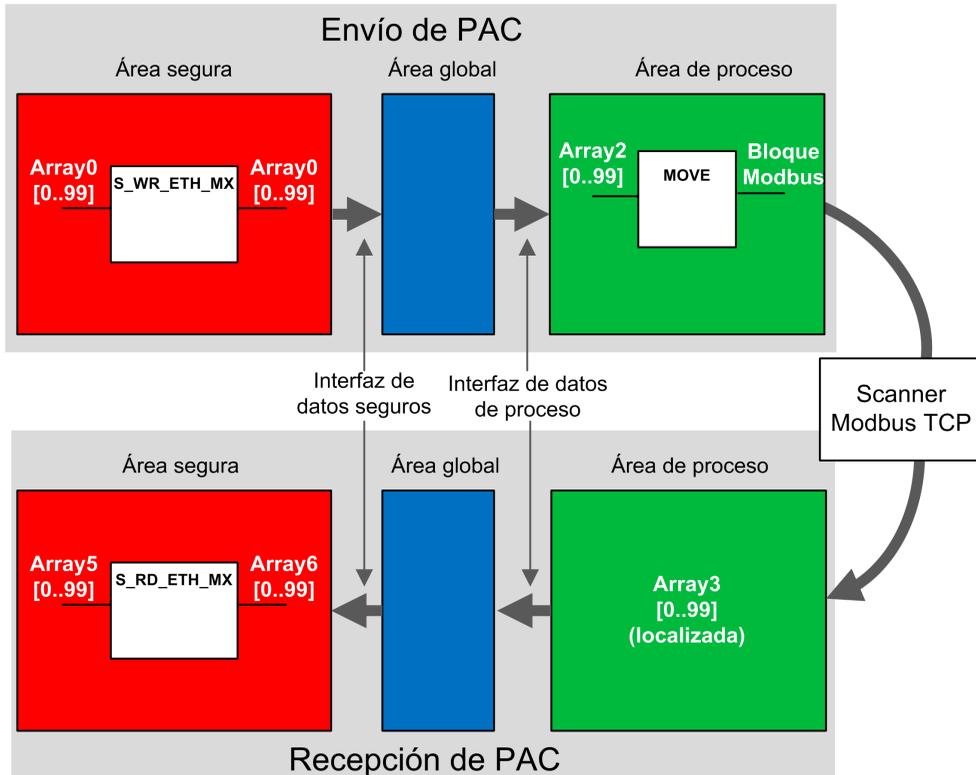
# Arquitectura entre pares con la versión del firmware de la CPU 3.10 o anterior

## Diseño de arquitectura

Con la versión del firmware de la CPU 3.10 o anterior, la arquitectura de la solución se basa en los siguientes elementos:

- Servicio NTP para sincronización horaria.
- Ejecución de 2 DFB (S\_WR\_ETH\_MX y MOVE en el PAC emisor y 1 DFB [S\_RD\_ETH\_MX] en el PAC receptor).
- Exploración a través de Modbus TCP, para transporte de datos.

En la figura siguiente, se muestra la descripción general del proceso que se necesita para realizar la comunicación entre pares segura:

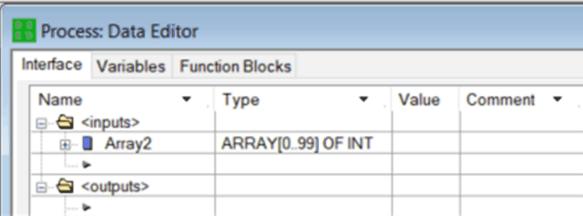
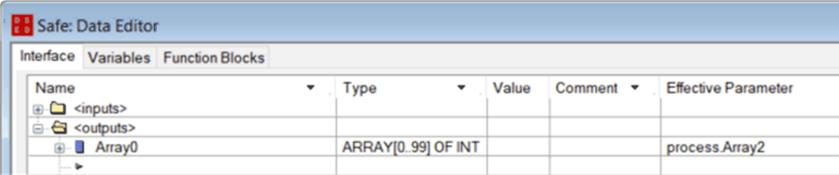


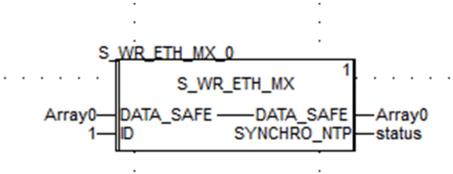
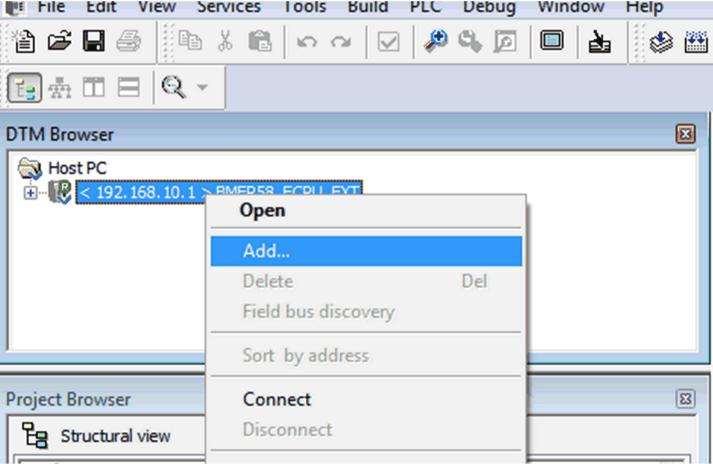
En la figura anterior, Control Expert crea automáticamente (y oculta) las matrices Array 1 y Array 4 en las áreas globales de los PAC homólogos. Desde el punto de vista del usuario, los enlaces van de Array 0 a Array 2, y de Array 3 a Array 5.

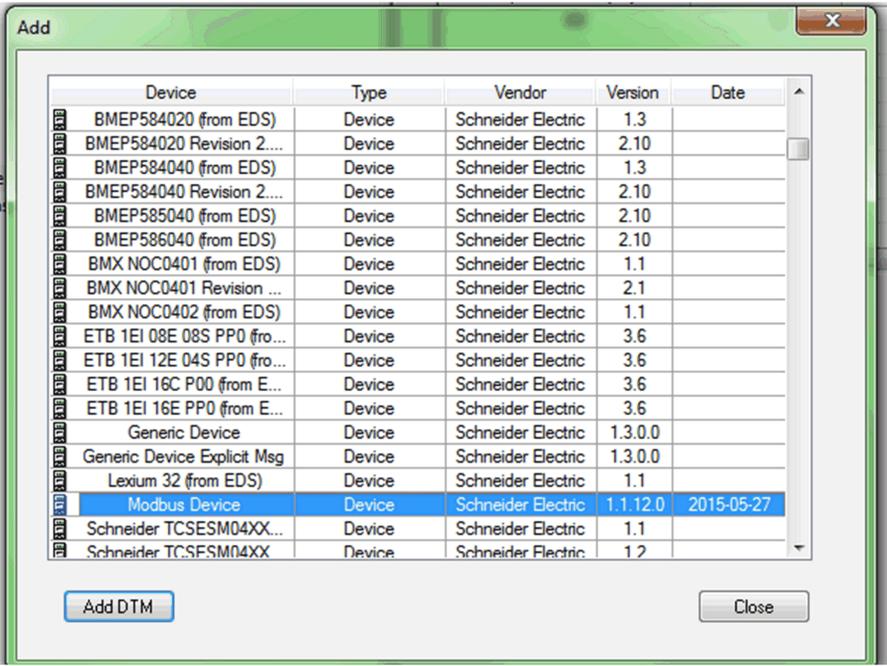
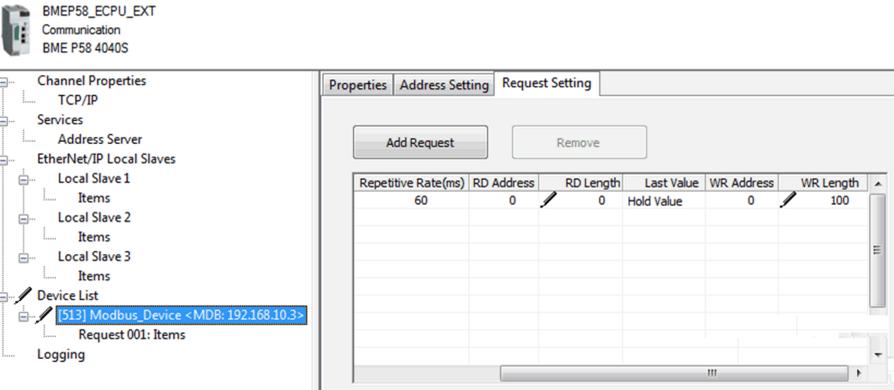
**NOTA:** En la red Ethernet, tiene permiso para mezclar datos relacionados con la seguridad y datos relacionados con la no seguridad sin que ello repercuta en el nivel de integridad de los datos relacionados con la seguridad. No hay restricciones sobre la red Ethernet al utilizar la comunicación entre pares segura.

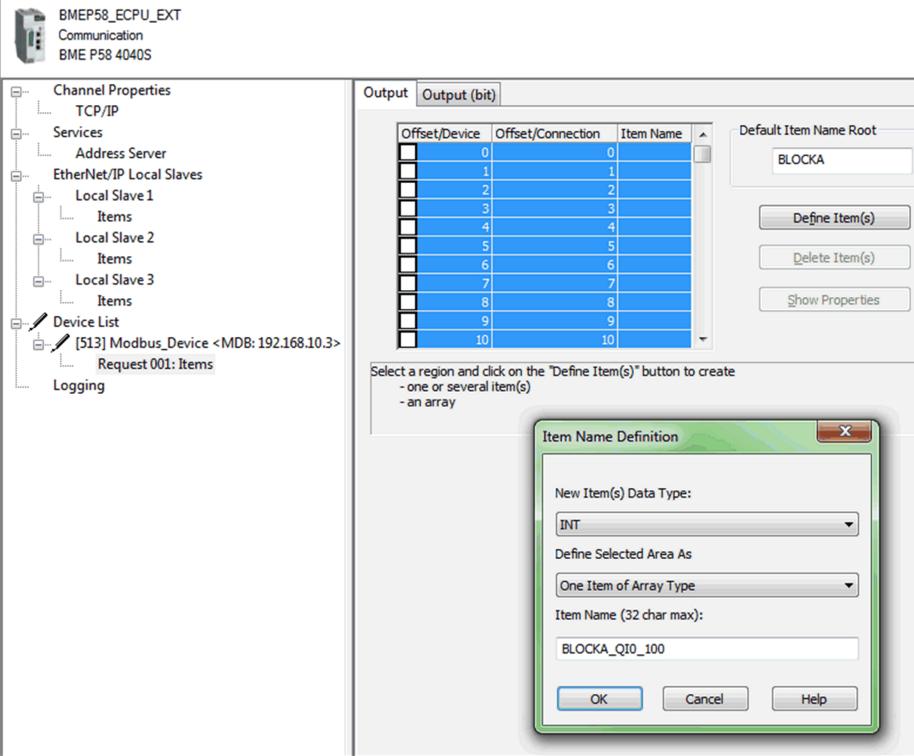
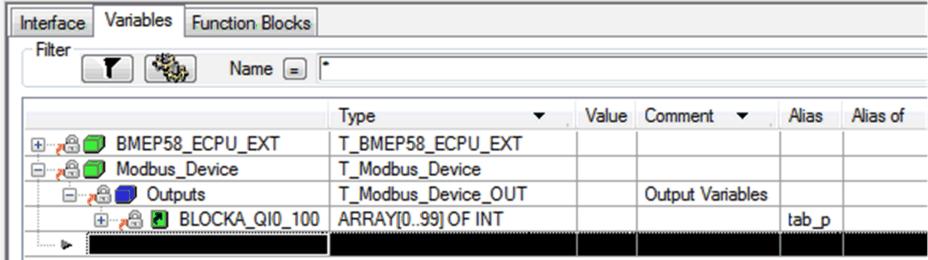
## Detalles de configuración de transferencia de datos entre pares

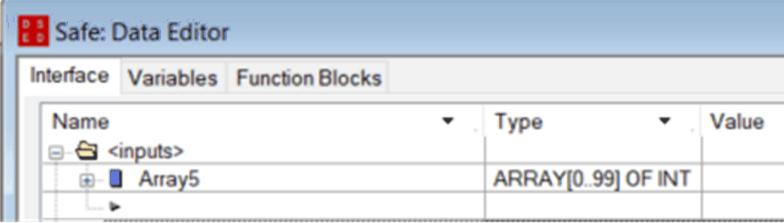
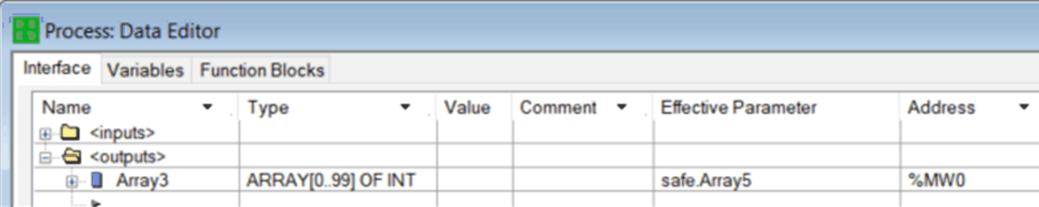
En el siguiente ejemplo, se muestra cómo configurar una transferencia de datos entre pares entre dos PAC de seguridad con la versión del firmware de la CPU 3.10 o anterior y Control Expert 14.1 o anterior:

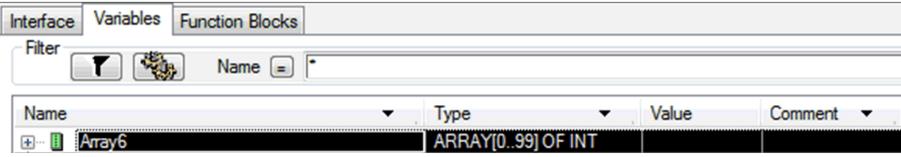
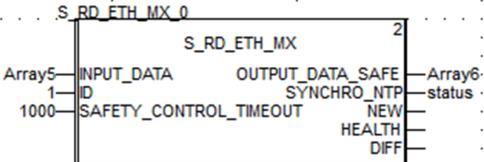
Paso	Acción
1	<p>En el PAC emisor, utilice el <b>Editor de datos de proceso</b> para crear una matriz de 100 enteros como entrada en el área de <b>Interfaz</b>. En este ejemplo, el nombre de la matriz es Array2:</p> 
2	<p>En el PAC emisor, cree otra matriz de 100 enteros como salida en la ficha <b>Interfaz</b> del <b>Editor de datos de seguridad</b> y vincúlela a la matriz del área de proceso de entrada creada en el paso 1 anterior, en la columna <b>Parámetro efectivo</b>. En este ejemplo, el nombre de la matriz es Array0:</p>  <p><b>NOTA:</b> Las variables de enteros correspondientes al índice de 0 a 90 de la matriz incluyen los valores de variables de seguridad que se intercambiarán con el PAC receptor. El área restante se reserva para los datos de diagnóstico generados automáticamente, que incluyen un CRC y una marca de tiempo. El PAC receptor utiliza estos datos de diagnóstico para determinar si los datos transferidos son seguros.</p>

Paso	Acción
3	<p>En el PAC emisor, configure el DFB S_WR_ETH_MX en una sección de la tarea SAFE. Vincule el DFB a Array0:</p> 
4	<p>En el <b>navegador DTM</b> del PAC emisor, seleccione la CPU (de este ejemplo) o un módulo de comunicaciones NOC (si existe) y, a continuación, haga clic en <b>Añadir...</b> para crear un explorador Modbus que pueda enviar datos a través de Modbus TCP del PAC emisor al PAC receptor:</p> 

Paso	Acción																																																																																																				
5	<p>Seleccione <b>Dispositivo Modbus</b> y haga clic en <b>Añadir DTM</b> para añadir el explorador Modbus:</p>  <table border="1" data-bbox="239 316 1005 803"> <thead> <tr> <th>Device</th> <th>Type</th> <th>Vendor</th> <th>Version</th> <th>Date</th> </tr> </thead> <tbody> <tr><td>BMEP584020 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.3</td><td></td></tr> <tr><td>BMEP584020 Revision 2....</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMEP584040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.3</td><td></td></tr> <tr><td>BMEP584040 Revision 2....</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMEP585040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMEP586040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMX NOC0401 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr><td>BMX NOC0401 Revision ...</td><td>Device</td><td>Schneider Electric</td><td>2.1</td><td></td></tr> <tr><td>BMX NOC0402 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr><td>ETB 1EI 08E 08S PP0 (fro...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>ETB 1EI 12E 04S PP0 (fro...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>ETB 1EI 16C PP0 (from E...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>ETB 1EI 16E PP0 (from E...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>Generic Device</td><td>Device</td><td>Schneider Electric</td><td>1.3.0.0</td><td></td></tr> <tr><td>Generic Device Explicit Msg</td><td>Device</td><td>Schneider Electric</td><td>1.3.0.0</td><td></td></tr> <tr><td>Lexium 32 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr><td>Modbus Device</td><td>Device</td><td>Schneider Electric</td><td>1.1.12.0</td><td>2015-05-27</td></tr> <tr><td>Schneider TCSESM04XX...</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr><td>Schneider TCSESM04XX</td><td>Device</td><td>Schneider Electric</td><td>1.2</td><td></td></tr> </tbody> </table>	Device	Type	Vendor	Version	Date	BMEP584020 (from EDS)	Device	Schneider Electric	1.3		BMEP584020 Revision 2....	Device	Schneider Electric	2.10		BMEP584040 (from EDS)	Device	Schneider Electric	1.3		BMEP584040 Revision 2....	Device	Schneider Electric	2.10		BMEP585040 (from EDS)	Device	Schneider Electric	2.10		BMEP586040 (from EDS)	Device	Schneider Electric	2.10		BMX NOC0401 (from EDS)	Device	Schneider Electric	1.1		BMX NOC0401 Revision ...	Device	Schneider Electric	2.1		BMX NOC0402 (from EDS)	Device	Schneider Electric	1.1		ETB 1EI 08E 08S PP0 (fro...	Device	Schneider Electric	3.6		ETB 1EI 12E 04S PP0 (fro...	Device	Schneider Electric	3.6		ETB 1EI 16C PP0 (from E...	Device	Schneider Electric	3.6		ETB 1EI 16E PP0 (from E...	Device	Schneider Electric	3.6		Generic Device	Device	Schneider Electric	1.3.0.0		Generic Device Explicit Msg	Device	Schneider Electric	1.3.0.0		Lexium 32 (from EDS)	Device	Schneider Electric	1.1		Modbus Device	Device	Schneider Electric	1.1.12.0	2015-05-27	Schneider TCSESM04XX...	Device	Schneider Electric	1.1		Schneider TCSESM04XX	Device	Schneider Electric	1.2	
Device	Type	Vendor	Version	Date																																																																																																	
BMEP584020 (from EDS)	Device	Schneider Electric	1.3																																																																																																		
BMEP584020 Revision 2....	Device	Schneider Electric	2.10																																																																																																		
BMEP584040 (from EDS)	Device	Schneider Electric	1.3																																																																																																		
BMEP584040 Revision 2....	Device	Schneider Electric	2.10																																																																																																		
BMEP585040 (from EDS)	Device	Schneider Electric	2.10																																																																																																		
BMEP586040 (from EDS)	Device	Schneider Electric	2.10																																																																																																		
BMX NOC0401 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
BMX NOC0401 Revision ...	Device	Schneider Electric	2.1																																																																																																		
BMX NOC0402 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
ETB 1EI 08E 08S PP0 (fro...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 12E 04S PP0 (fro...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 16C PP0 (from E...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 16E PP0 (from E...	Device	Schneider Electric	3.6																																																																																																		
Generic Device	Device	Schneider Electric	1.3.0.0																																																																																																		
Generic Device Explicit Msg	Device	Schneider Electric	1.3.0.0																																																																																																		
Lexium 32 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
Modbus Device	Device	Schneider Electric	1.1.12.0	2015-05-27																																																																																																	
Schneider TCSESM04XX...	Device	Schneider Electric	1.1																																																																																																		
Schneider TCSESM04XX	Device	Schneider Electric	1.2																																																																																																		
6	<p>Abra el dispositivo Modbus que acaba de añadir, añada una petición y, en la ficha <b>Ajuste de petición</b>:</p> <ul style="list-style-type: none"> <li>Establezca la columna <b>Longitud de escritura</b>, que corresponde a la longitud de los datos que se van a escribir, en un valor de 100.</li> <li>A continuación, establezca la columna <b>Dirección ES</b>, que es la dirección en la que la tabla del PAC receptor escribirá los datos que recibe (en este ejemplo: 0, lo que significa que el PAC emisor escribirá en la tabla empezando por %MW0 en el PAC receptor).</li> </ul>  <p><b>BMEP58_ECPU_EXT</b> Communication BME P58 4040S</p> <p>Channel Properties TCP/IP Services Address Server EtherNet/IP Local Slaves Local Slave 1 Items Local Slave 2 Items Local Slave 3 Items Device List [513] Modbus_Device &lt;MDB: 192.168.10.3&gt; Request 001: Items Logging</p> <p>Properties Address Setting Request Setting</p> <p>Add Request Remove</p> <table border="1" data-bbox="544 1274 1075 1485"> <thead> <tr> <th>Repetitive Rate(ms)</th> <th>RD Address</th> <th>RD Length</th> <th>Last Value</th> <th>WR Address</th> <th>WR Length</th> </tr> </thead> <tbody> <tr> <td>60</td> <td>0</td> <td>0</td> <td>Hold Value</td> <td>0</td> <td>100</td> </tr> </tbody> </table>	Repetitive Rate(ms)	RD Address	RD Length	Last Value	WR Address	WR Length	60	0	0	Hold Value	0	100																																																																																								
Repetitive Rate(ms)	RD Address	RD Length	Last Value	WR Address	WR Length																																																																																																
60	0	0	Hold Value	0	100																																																																																																

Paso	Acción																														
7	<p>Seleccione el nodo <b>Petición 001: Elementos</b> y, a continuación, en la ficha <b>Salida</b>, defina un tipo de matriz de INT (es decir, <math>\geq 100</math> enteros). Esta es la tabla del PAC emisor que se escribirá en el PAC receptor:</p> 																														
8	<p>Después de guardar y crear la configuración, el bloque (BLOCKA_QI0_100 en este ejemplo) se crea automáticamente como una variable de proceso:</p>  <table border="1" data-bbox="194 1144 1122 1404"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Value</th> <th>Comment</th> <th>Alias</th> <th>Alias of</th> </tr> </thead> <tbody> <tr> <td>BMEP58_ECPU_EXT</td> <td>T_BMEP58_ECPU_EXT</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Modbus_Device</td> <td>T_Modbus_Device</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Outputs</td> <td>T_Modbus_Device_OUT</td> <td></td> <td>Output Variables</td> <td></td> <td></td> </tr> <tr> <td>BLOCKA_QI0_100</td> <td>ARRAY[0..99] OF INT</td> <td></td> <td></td> <td>tab_p</td> <td></td> </tr> </tbody> </table>	Name	Type	Value	Comment	Alias	Alias of	BMEP58_ECPU_EXT	T_BMEP58_ECPU_EXT					Modbus_Device	T_Modbus_Device					Outputs	T_Modbus_Device_OUT		Output Variables			BLOCKA_QI0_100	ARRAY[0..99] OF INT			tab_p	
Name	Type	Value	Comment	Alias	Alias of																										
BMEP58_ECPU_EXT	T_BMEP58_ECPU_EXT																														
Modbus_Device	T_Modbus_Device																														
Outputs	T_Modbus_Device_OUT		Output Variables																												
BLOCKA_QI0_100	ARRAY[0..99] OF INT			tab_p																											

Paso	Acción
9	<p>En el PAC emisor, en una sección de código de proceso, utilice el DFB <code>MOVE</code> para copiar el contenido de <code>Array2</code> en la matriz definida más arriba en la estructura del dispositivo Modbus:</p> 
10	<p>En el PAC receptor, utilice el <b>Safe: Editor de datos</b> para crear una matriz de 100 enteros (<code>Array5</code>) como entrada en el área <b>Interfaz</b>:</p> 
11	<p>En el PAC receptor, en el <b>Editor de datos de proceso</b>, cree una matriz (<code>Array3</code>) de 100 INT en la sección <code>&lt;salidas&gt;</code> de la ficha <b>Interfaz</b>. Vincule esta matriz a la matriz del área de datos (<code>Array5</code>, creada en el paso 10) en la columna <b>Parámetro efectivo</b>. Los datos enviados por el PAC emisor se escribirán en esta matriz a través del explorador Modbus, siempre y cuando esta variable esté ubicada en la dirección definida en el explorador del PAC emisor (en este ejemplo, <code>%MW0</code>):</p> 

Paso	Acción
12	<p>En el PAC receptor, utilice el <b>Editor de datos de seguridad</b> para crear una matriz de 100 enteros (Array6):</p> 
13	<p>En el PAC receptor, en una sección de código de la tarea SAFE, instancie el DFB <code>S_RD_ETH_MX</code> con la matriz creada en el paso 10 (Array5) como parámetro de entrada, y con la matriz creada en el paso 12 (Array6) como parámetro de salida:</p> 

## Canal negro entre pares

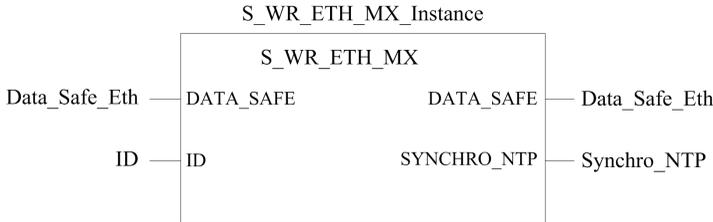
Cada transmisión entre pares consta tanto de *datos de seguridad del usuario*, que incluye el contenido relacionado con las aplicaciones que se transmite, como de *datos reservados*. El PAC de seguridad utiliza *datos reservados* para poner a prueba la fiabilidad de la transmisión, de modo que satisfaga los requisitos de SIL3. Los *datos reservados* constan de los elementos siguientes:

- El PAC emisor calcula un CRC partir de los datos que se van a transmitir. El PAC receptor comprueba el CRC antes de utilizar los datos transmitidos.
- Un identificador de comunicación que se incluye en el cálculo de CRC para impedir los ataques de engaño e inserción en la transmisión de datos de seguridad.
- Una marca de tiempo que contiene el tiempo de la transmisión en ms. Esta marca de tiempo se basa en el valor de tiempo proporcionado por el servicio NTP y se utiliza para sincronizar el PAC emisor y el PAC receptor. Los datos que envía el PAC emisor añaden un valor de tiempo a los datos enviados al PAC receptor. El PAC receptor compara la marca de tiempo recibida con su propio valor de tiempo, y la utiliza para:
  - Comprobar la antigüedad de los datos.
  - Rechazar las transmisiones duplicadas.
  - Determinar el orden cronológico de las transmisiones recibidas.
  - Determinar el tiempo transcurrido entre transmisiones de datos.

## Configuración del DFB `S_WR_ETH_MX` de la lógica del programa del PAC emisor.

### Representación

Representación de DFB:



Para obtener una descripción ampliada de este DFB, consulte *EcoStruxure™ Control Expert, Seguridad, Biblioteca de bloques*.

### Descripción

El DFB `S_WR_ETH_MX` está diseñado para PAC que utilizan la versión del firmware de la CPU 3.10 o anterior. Este DFB calcula datos (datos reservados que contienen un CRC y una marca de tiempo) que necesita el receptor para comprobar y gestionar errores detectados durante la comunicación entre pares segura.

El bloque de funciones DFB `S_WR_ETH_MX` tiene que invocarse en cada ciclo del PAC emisor. Dentro del ciclo, se tiene que ejecutar en la lógica después de llevar a cabo todas las modificaciones necesarias en los datos que se van a enviar. Esto significa que no se pueden modificar los datos que se van a enviar dentro del ciclo después de la ejecución del DFB; en caso contrario, la información de CRC utilizada en el área de datos reservados no será correcta y la comunicación entre pares segura no se realizará correctamente.

Debe asignar un valor exclusivo al parámetro de `ID` que identifique la comunicación entre pares segura entre un emisor y un receptor.

## ⚠ ADVERTENCIA

### PÉRDIDA DE CAPACIDAD PARA EJECUTAR FUNCIONES DE SEGURIDAD

El valor del parámetro `ID` debe ser exclusivo y estar fijado en la red para un par emisor/receptor.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## Descripción de la matriz DATA\_SAFE

Utilice las fichas **Interfaz** del **Editor de datos de seguridad** y del **Editor de datos de proceso** de Control Expert para conectar las variables de proceso y las variables de seguridad.

La conexión de las variables de proceso y de seguridad de este modo permite:

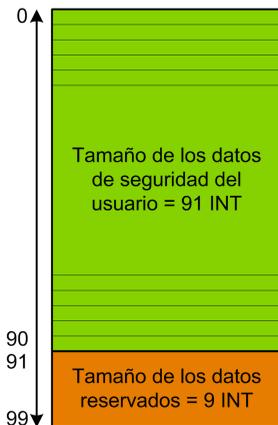
- Transferir el valor de las variables de seguridad a las variables de proceso, a través de variables globales vinculadas.
- Enviar valores de variable del área de proceso del PAC emisor al área de proceso del PAC receptor, a través de mensajes explícitos sobre Modbus TCP.

La matriz DATA\_SAFE se compone de dos zonas:

- La zona **Datos de seguridad del usuario** contiene los datos del área segura del PAC. Esta zona comienza con el índice 0 y finaliza con el índice 90.
- La zona **Datos reservados** se reserva para los datos de diagnóstico generados automáticamente, que incluyen un CRC y una marca de tiempo. El PAC receptor utiliza estos datos para determinar si los datos contenidos en la zona **Datos de seguridad del usuario** son seguros. Esta zona comienza con el índice 91 y finaliza con el índice 99.

**NOTA:** No escriba en la zona **Datos reservados**.

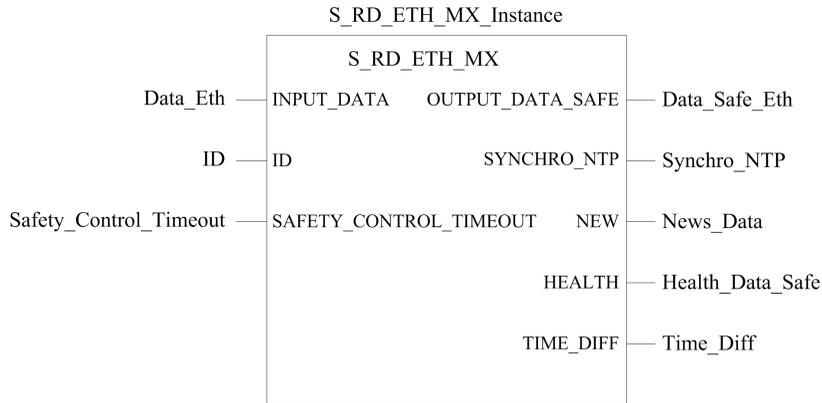
Representación de la estructura de la matriz DATA\_SAFE (array[0..99] of INT):



# Configuración del DFB S\_RD\_ETH\_MX de la lógica del programa del PAC emisor

## Representación

Representación de DFB:



Consulte *EcoStruxure™ Control Expert, Seguridad, Biblioteca de bloques* para obtener una descripción ampliada de este DFB.

## Descripción

El DFB S\_RD\_ETH\_MX está diseñado para PAC que utilizan la versión del firmware de la CPU 3.10 o anterior. Este DFB copia, en el área de seguridad, los datos recibidos en el área de proceso y valida la precisión de los datos recibidos.

## ▲ ADVERTENCIA

### PÉRDIDA DE CAPACIDAD PARA EJECUTAR FUNCIONES DE SEGURIDAD

- El bloque de funciones DFB `S_RD_ETH_MX` se debe invocar en cada ciclo de la lógica del programa del PAC receptor y se debe ejecutar antes de que se utilicen los datos en el ciclo.
- El valor del parámetro `ID` debe ser exclusivo y estar fijado en la red para un par emisor/receptor.
- Debe comprobar el valor de bit `HEALTH` del DFB `S_RD_ETH_MX` en cada ciclo antes usar cualquier dato seguro para gestionar la función de seguridad.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

El bloque de funciones `S_RD_ETH_MX`:

- Copia los datos recibidos en el registro `INPUT_DATA` en el registro `OUTPUT_DATA_SAFE` si se superan las pruebas siguientes:
  - El bloque de funciones comprueba el CRC del último paquete de datos recibido mediante el explorador de E/S a través de Ethernet (Modbus TCP). Si el CRC no es correcto, los datos se consideran no seguros y no se escriben en el registro `OUTPUT_DATA_SAFE` del área de seguridad.
  - El bloque de funciones comprueba los últimos datos recibidos para determinar si son más recientes que los datos ya escritos en el registro `OUTPUT_DATA_SAFE` del área de seguridad (después de comparar las marcas de tiempo). Si los últimos datos recibidos no son más recientes, no se copian en el registro `OUTPUT_DATA_SAFE` del área de seguridad.
- Comprueba la antigüedad de los datos en el área de seguridad. Si su antigüedad es superior al valor máximo configurable establecido en el registro de entrada de `SAFETY_CONTROL_TIMEOUT`, los datos se considerarán no seguros y el bit `HEALTH` se establecerá en 0.

**NOTA:** La antigüedad de los datos es la diferencia entre la hora en la que se calculan los datos en el PAC emisor y la hora en la que se comprueban los datos en el PAC receptor. La referencia base de tiempo se actualiza periódicamente con la hora recibida desde un servidor NTP.

Si el bit `HEALTH` se establece en 0, los datos disponibles en la matriz `OUTPUT_DATA_SAFE` se considerarán no seguros. En este caso, lleve a cabo las medidas oportunas.

## Descripción de las matrices `INPUT_DATA` y `OUTPUT_DATA_SAFE`

Las matrices `INPUT_DATA` se componen de datos procedentes del área de memoria de datos de proceso. Las matrices `OUTPUT_DATA_SAFE` se componen de variables de

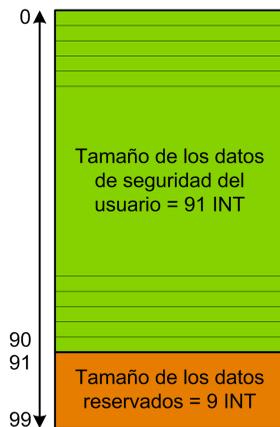
seguridad. Utilice las fichas **Interfaz de datos de seguridad** e **Interfaz de datos de proceso** de Control Expert para conectar las variables de proceso y las variables de seguridad.

Las matrices `INPUT_DATA` y `OUTPUT_DATA_SAFE` constan de dos zonas:

- La zona **Datos de seguridad del usuario** contiene los datos del usuario. Esta zona comienza con el índice 0 y finaliza con el índice 90.
- La zona **Datos reservados** se reserva para los datos de diagnóstico generados automáticamente, que incluyen un CRC y una marca de tiempo. El PAC receptor utiliza estos datos para determinar si los datos contenidos en la zona **Datos de seguridad del usuario** son seguros. Esta zona comienza con el índice 91 y finaliza con el índice 99.

**NOTA:** No se recomienda escribir en la zona **Datos reservados**, ya que si lo hace se sobrescribirán los datos de diagnóstico generados automáticamente.

Representación de la estructura de las matrices `INPUT_DATA` y `OUTPUT_DATA_SAFE` (array[0..99] of INT):



## Cálculo de un valor de SAFETY\_CONTROL\_TIMEOUT

Cuando calcule un valor de `SAFETY_CONTROL_TIMEOUT`, tenga en cuenta lo siguiente:

- Valor mínimo:  $SAFETY\_CONTROL\_TIMEOUT > T1$
- Valor recomendado:  $SAFETY\_CONTROL\_TIMEOUT > 2 * T1$

$T1 = CPU_{sender} \text{ MAST cycle time} + CPU_{sender} \text{ SAFE cycle time} + \text{Repetitive\_rate} + \text{Network transmission time} + CPU_{receiver} \text{ MAST cycle time} + CPU_{receiver} \text{ SAFE cycle time}$

Donde:

- $CPU_{sender} \text{ MAST cycle time}$  es el tiempo de ciclo MAST del PAC emisor.

- $CPU_{sender}$  *SAFE cycle time* es el tiempo de ciclo SAFE del PAC emisor.
- *Repetitive\_rate* es el intervalo de tiempo de la consulta de escritura del explorador de E/S del PAC emisor al PAC receptor.
- *Network transmission time* es el tiempo consumido en la red Ethernet durante la transmisión de datos del PAC emisor al PAC receptor.
- $CPU_{receiver}$  *MAST cycle time* es el tiempo de ciclo MAST del PAC receptor.
- $CPU_{receiver}$  *SAFE cycle time* es el tiempo de ciclo SAFE del PAC receptor.

Observe que el valor definido en el parámetro `SAFETY_CONTROL_TIMEOUT` tiene un efecto directo sobre la solidez y disponibilidad de la comunicación segura entre pares. Si el valor del parámetro `SAFETY_CONTROL_TIMEOUT` supera considerablemente  $T1$ , la comunicación tolerará diversos retrasos (por ejemplo, retrasos en la red) o transmisiones de datos dañados.

Configure su red Ethernet de modo que la carga no provoque un retraso excesivo en la red durante la transmisión de datos, que pueda provocar la caducidad de `timeout`. Para evitar retrasos excesivos en las comunicaciones seguras entre pares a causa de la transmisión de otros datos no seguros en la misma red, puede utilizar una red Ethernet dedicada para el protocolo seguro entre pares.

Cuando ponga en marcha su proyecto, debe calcular el rendimiento de la comunicación segura peer-to-peer; para ello, compruebe los valores proporcionados en el parámetro de salida `TIME_DIFF` y evalúe el margen utilizando el valor definido en el parámetro `SAFETY_CONTROL_TIMEOUT`.

## Descripción del bit `HEALTH`

Cuando el valor del bit `HEALTH` es:

- 1: La integridad de los datos es correcta (CRC) y la antigüedad de los datos es menor que el valor establecido en el registro de entrada `SAFETY_CONTROL_TIMEOUT`.

**NOTA:** La antigüedad de los datos considerados es el tiempo entre:

- El inicio del ciclo en el que los datos se calculan en el PAC emisor.
  - El inicio del ciclo en el que los datos se comprueban en el PAC receptor.
- 0: No se reciben nuevos datos válidos en el intervalo de tiempo exigido (el temporizador caduca y el bit `HEALTH` se establece en 0).

**NOTA:** Si el bit `HEALTH` se establece en 0, los datos de la matriz de salida `OUTPUT_DATA_SAFE` se consideran no seguros; actúe en consecuencia.

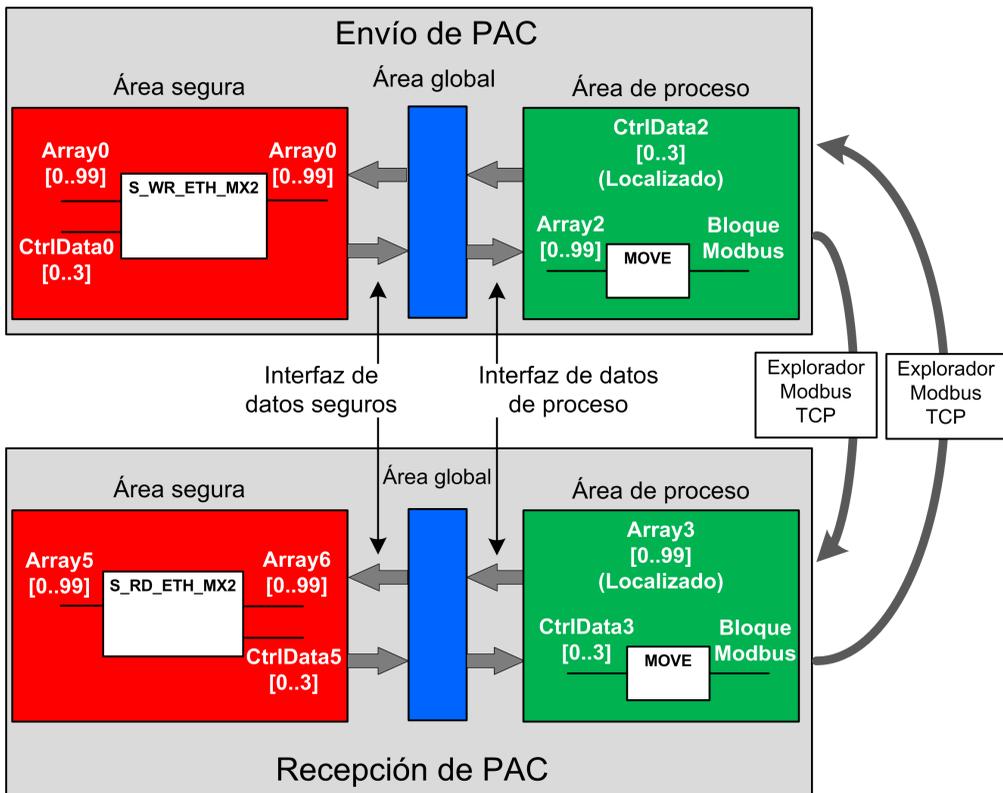
# Arquitectura entre pares con la versión del firmware de la CPU 3.20 o posterior

## Diseño de arquitectura

Con la versión del firmware de la CPU 3.20 o posterior, la arquitectura de la solución se basa en los siguientes elementos:

- Ejecución de 2 DFB (S\_WR\_ETH\_MX2 y MOVE) en el PAC emisor y 2 DFB (S\_RD\_ETH\_MX2 y MOVE) en el PAC receptor.
- Exploración a través de Modbus TCP, para transporte seguro de datos del emisor al receptor.
- Exploración a través de Modbus TCP, para transporte de datos de control del receptor al emisor.

En la figura siguiente, se muestra la descripción general del proceso que se necesita para realizar la comunicación entre pares segura:

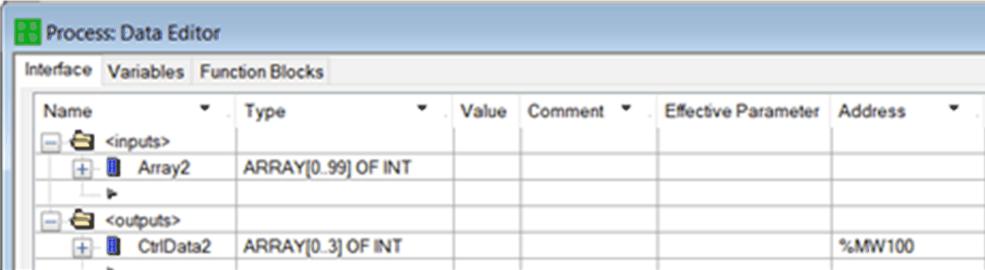


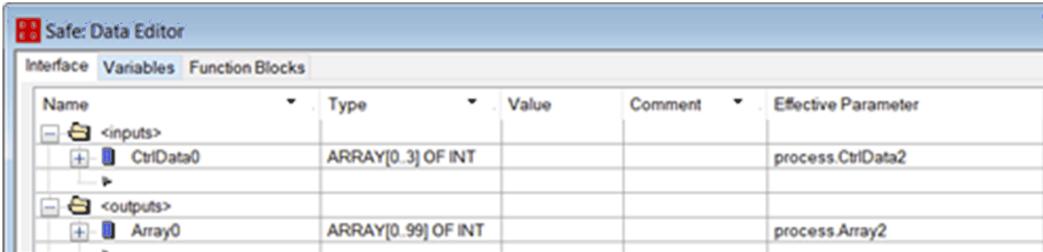
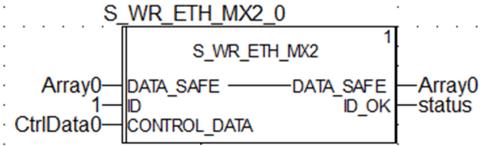
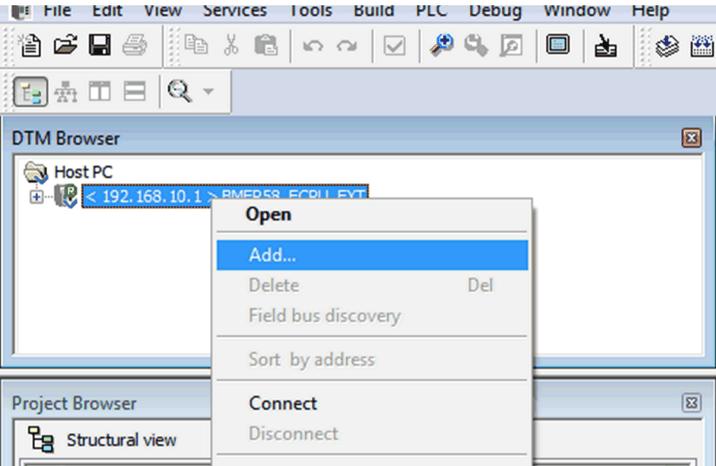
En la figura anterior, Control Expert crea automáticamente (y oculta de la vista externa) las matrices Array1 y Array4 en las áreas globales de los PAC homólogos. Desde el punto de vista del usuario, los enlaces van de Array0 a Array2 y de Array3 a Array5.

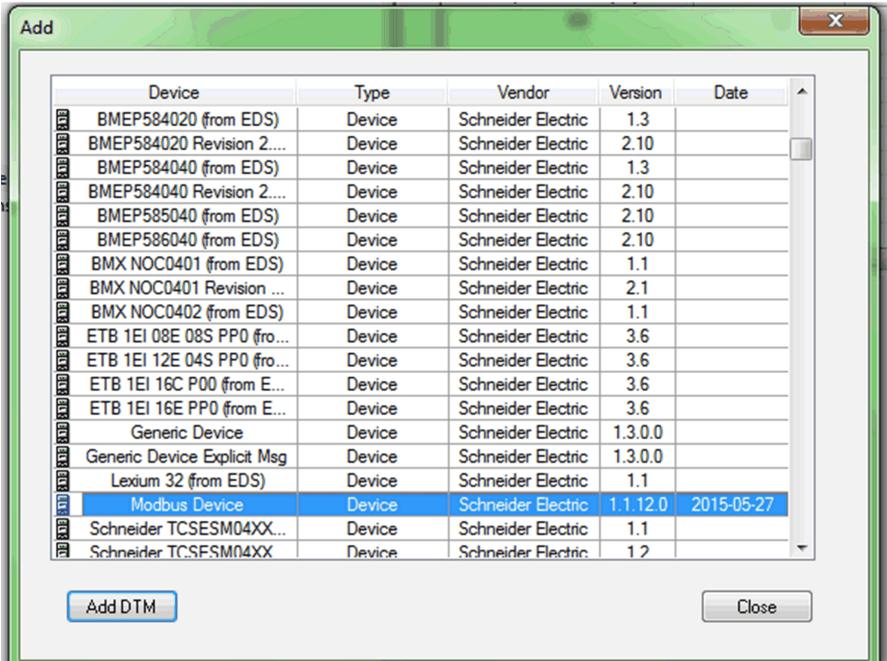
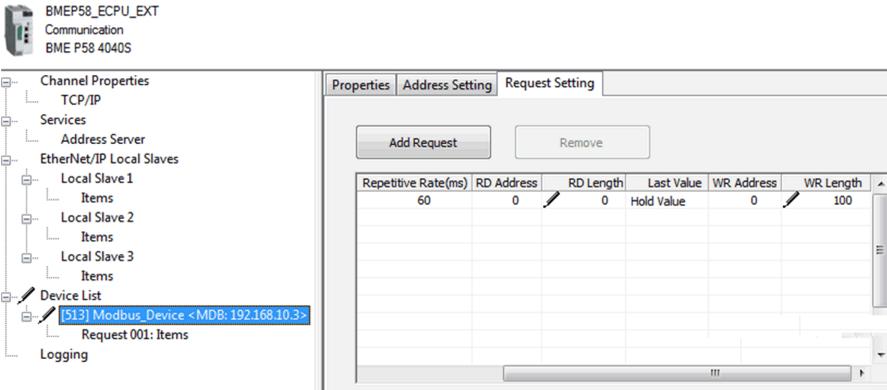
**NOTA:** En la red Ethernet, tiene permiso para mezclar datos relacionados con la seguridad y datos relacionados con la no seguridad sin que ello repercuta en el nivel de integridad de los datos relacionados con la seguridad. No hay restricciones sobre la red Ethernet al utilizar la comunicación entre pares segura.

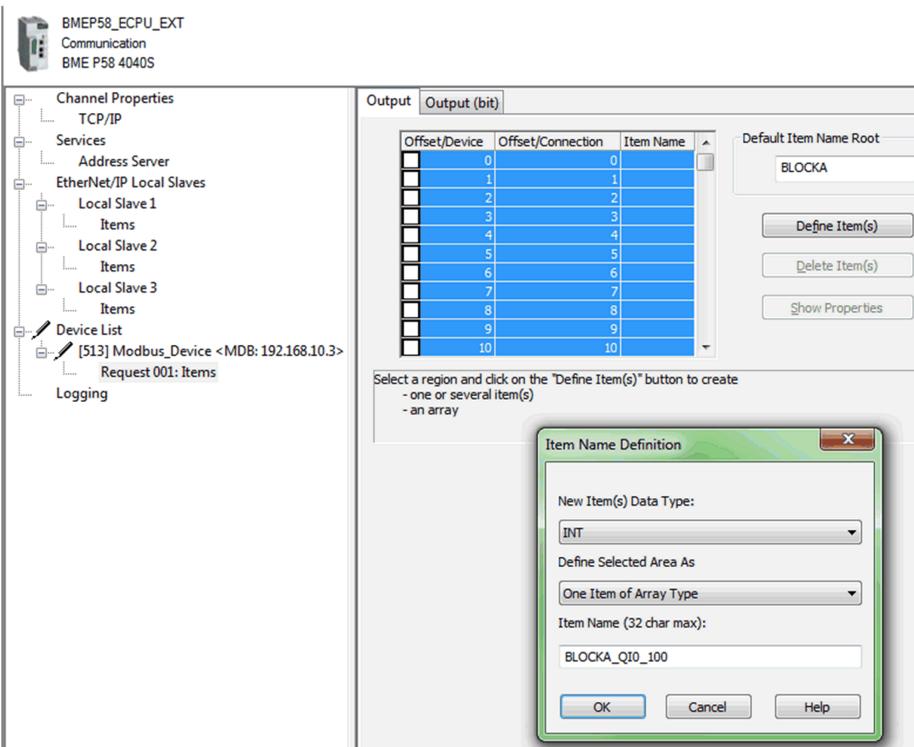
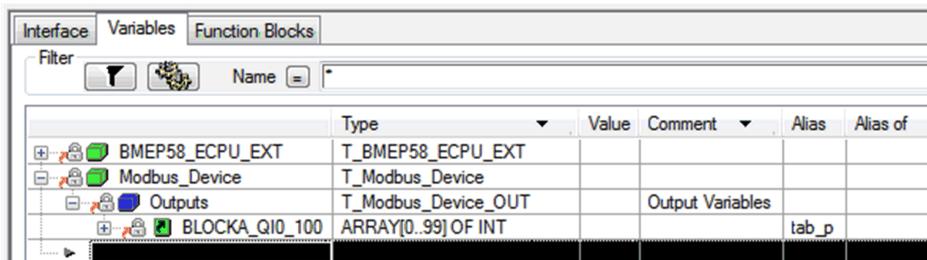
## Detalles de configuración de transferencia de datos entre pares

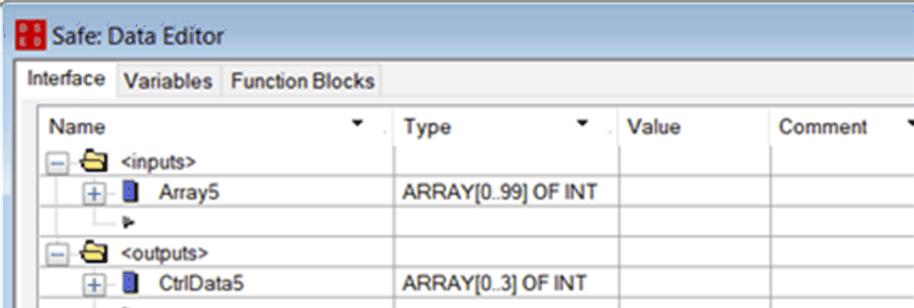
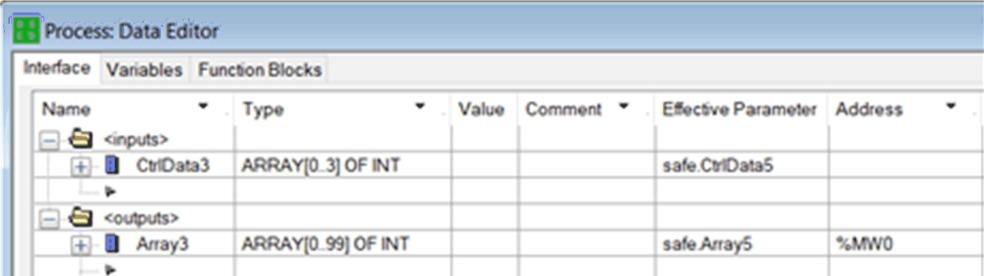
En el siguiente ejemplo se muestra cómo configurar una transferencia de datos entre pares entre dos PAC de seguridad con la versión del firmware 3.20 o posterior y Control Expert 15.0 o posterior:

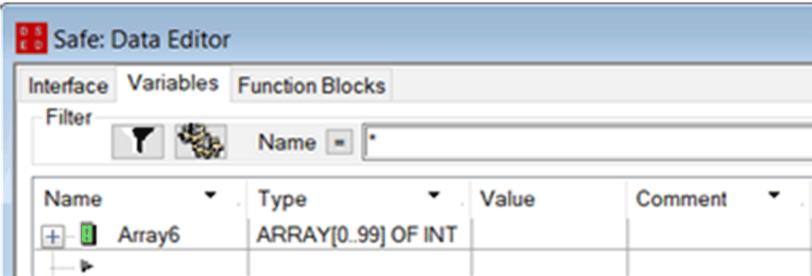
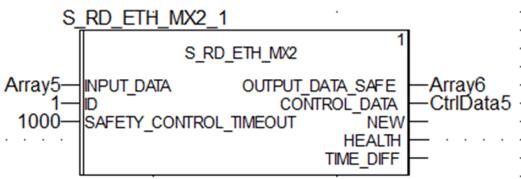
Paso	Acción
1	<p>En el PAC emisor, utilice el <b>Editor de datos de proceso</b> para crear una matriz de 100 enteros (Array2) como entrada en el área Interfaz. En el mismo <b>Editor de datos de proceso</b>, cree una matriz de 4 enteros (CtrlData2) como salida en el área <b>Interfaz</b>.</p> <p>Los datos de control procedentes del PAC receptor se escribirán en esta matriz CtrlData2 a través del explorador Modbus, siempre y cuando esta matriz CtrlData2 esté ubicada en la dirección definida en el explorador del PAC emisor (en este ejemplo, %MW100; consulte el paso 14):</p> 
2	<p>En el PAC emisor, utilice el <b>Safe: Editor de datos</b> para crear otra matriz de 100 enteros (Array0) como salida en el área <b>Interfaz</b> y vincúlela con los datos de process.Array2 creados en el paso 1 anterior, en la columna <b>Parámetro efectivo</b>.</p> <p>En el mismo <b>Safe: Editor de datos</b>, cree una matriz de 4 enteros (CtrlData0) como entrada en el área de seguridad <b>Interfaz</b> y vincúlela con los datos de process.CtrlData2 creados en el paso 1 anterior, en la columna <b>Parámetro efectivo</b>.</p>

Paso	Acción
	 <p><b>NOTA:</b> Las variables enteras correspondientes al índice de 0 a 90 de la matriz incluyen los valores de variables de seguridad que desea intercambiar con el PAC receptor. El área restante se reserva para los datos de diagnóstico generados automáticamente, que incluyen un CRC y una marca de tiempo. El PAC receptor utiliza estos datos de diagnóstico para determinar si los datos transferidos son seguros.</p>
3	<p>En el PAC emisor, configure el DFB S_WR_ETH_MX2 en una sección de la tarea SAFE. Vincule el DFB con Array0 y CtrlData0:</p> 
4	<p>En el <b>navegador DTM</b> del PAC emisor, seleccione la CPU (de este ejemplo) o un módulo de comunicaciones NOC (si existe) y, a continuación, haga clic en <b>Añadir...</b> para crear un explorador Modbus que pueda enviar datos a través de Modbus TCP del PAC emisor al PAC receptor:</p> 

Paso	Acción																																																																																																				
5	<p>Seleccione <b>Dispositivo Modbus</b> y haga clic en <b>Añadir DTM</b> para añadir el explorador Modbus:</p>  <table border="1" data-bbox="235 316 1001 803"> <thead> <tr> <th>Device</th> <th>Type</th> <th>Vendor</th> <th>Version</th> <th>Date</th> </tr> </thead> <tbody> <tr><td>BMEP584020 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.3</td><td></td></tr> <tr><td>BMEP584020 Revision 2....</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMEP584040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.3</td><td></td></tr> <tr><td>BMEP584040 Revision 2....</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMEP585040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMEP586040 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>2.10</td><td></td></tr> <tr><td>BMX NOC0401 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr><td>BMX NOC0401 Revision ...</td><td>Device</td><td>Schneider Electric</td><td>2.1</td><td></td></tr> <tr><td>BMX NOC0402 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr><td>ETB 1EI 08E 08S PP0 (fro...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>ETB 1EI 12E 04S PP0 (fro...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>ETB 1EI 16C P00 (from E...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>ETB 1EI 16E PP0 (from E...</td><td>Device</td><td>Schneider Electric</td><td>3.6</td><td></td></tr> <tr><td>Generic Device</td><td>Device</td><td>Schneider Electric</td><td>1.3.0.0</td><td></td></tr> <tr><td>Generic Device Explicit Msg</td><td>Device</td><td>Schneider Electric</td><td>1.3.0.0</td><td></td></tr> <tr><td>Lexium 32 (from EDS)</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr style="background-color: #e0f0ff;"><td>Modbus Device</td><td>Device</td><td>Schneider Electric</td><td>1.1.12.0</td><td>2015-05-27</td></tr> <tr><td>Schneider TCSESM04XX...</td><td>Device</td><td>Schneider Electric</td><td>1.1</td><td></td></tr> <tr><td>Schneider TCFSM04XX</td><td>Device</td><td>Schneider Electric</td><td>1.2</td><td></td></tr> </tbody> </table>	Device	Type	Vendor	Version	Date	BMEP584020 (from EDS)	Device	Schneider Electric	1.3		BMEP584020 Revision 2....	Device	Schneider Electric	2.10		BMEP584040 (from EDS)	Device	Schneider Electric	1.3		BMEP584040 Revision 2....	Device	Schneider Electric	2.10		BMEP585040 (from EDS)	Device	Schneider Electric	2.10		BMEP586040 (from EDS)	Device	Schneider Electric	2.10		BMX NOC0401 (from EDS)	Device	Schneider Electric	1.1		BMX NOC0401 Revision ...	Device	Schneider Electric	2.1		BMX NOC0402 (from EDS)	Device	Schneider Electric	1.1		ETB 1EI 08E 08S PP0 (fro...	Device	Schneider Electric	3.6		ETB 1EI 12E 04S PP0 (fro...	Device	Schneider Electric	3.6		ETB 1EI 16C P00 (from E...	Device	Schneider Electric	3.6		ETB 1EI 16E PP0 (from E...	Device	Schneider Electric	3.6		Generic Device	Device	Schneider Electric	1.3.0.0		Generic Device Explicit Msg	Device	Schneider Electric	1.3.0.0		Lexium 32 (from EDS)	Device	Schneider Electric	1.1		Modbus Device	Device	Schneider Electric	1.1.12.0	2015-05-27	Schneider TCSESM04XX...	Device	Schneider Electric	1.1		Schneider TCFSM04XX	Device	Schneider Electric	1.2	
Device	Type	Vendor	Version	Date																																																																																																	
BMEP584020 (from EDS)	Device	Schneider Electric	1.3																																																																																																		
BMEP584020 Revision 2....	Device	Schneider Electric	2.10																																																																																																		
BMEP584040 (from EDS)	Device	Schneider Electric	1.3																																																																																																		
BMEP584040 Revision 2....	Device	Schneider Electric	2.10																																																																																																		
BMEP585040 (from EDS)	Device	Schneider Electric	2.10																																																																																																		
BMEP586040 (from EDS)	Device	Schneider Electric	2.10																																																																																																		
BMX NOC0401 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
BMX NOC0401 Revision ...	Device	Schneider Electric	2.1																																																																																																		
BMX NOC0402 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
ETB 1EI 08E 08S PP0 (fro...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 12E 04S PP0 (fro...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 16C P00 (from E...	Device	Schneider Electric	3.6																																																																																																		
ETB 1EI 16E PP0 (from E...	Device	Schneider Electric	3.6																																																																																																		
Generic Device	Device	Schneider Electric	1.3.0.0																																																																																																		
Generic Device Explicit Msg	Device	Schneider Electric	1.3.0.0																																																																																																		
Lexium 32 (from EDS)	Device	Schneider Electric	1.1																																																																																																		
Modbus Device	Device	Schneider Electric	1.1.12.0	2015-05-27																																																																																																	
Schneider TCSESM04XX...	Device	Schneider Electric	1.1																																																																																																		
Schneider TCFSM04XX	Device	Schneider Electric	1.2																																																																																																		
6	<p>Abra el dispositivo Modbus que acaba de añadir y en la ficha <b>Ajuste de petición</b>:</p> <ul style="list-style-type: none"> <li>• Establezca la columna <b>Longitud de escritura</b>, que corresponde a la longitud de los datos que se van a escribir, en un valor de 100.</li> <li>• A continuación, establezca la columna <b>Dirección ES</b>, que es la dirección en la que la tabla del PAC receptor escribirá los datos que recibe (en este ejemplo: 0, lo que significa que el PAC emisor escribirá en la tabla empezando por %MW0 en el PAC receptor).</li> </ul>  <p>Channel Properties TCP/IP Services Address Server EtherNet/IP Local Slaves Local Slave 1 Items Local Slave 2 Items Local Slave 3 Items Device List [513] Modbus_Device &lt;MDB: 192.168.10.3&gt; Request 001: Items Logging</p> <table border="1" data-bbox="537 1274 1068 1485"> <thead> <tr> <th>Repetitive Rate(ms)</th> <th>RD Address</th> <th>RD Length</th> <th>Last Value</th> <th>WR Address</th> <th>WR Length</th> </tr> </thead> <tbody> <tr> <td>60</td> <td>0</td> <td>0</td> <td>Hold Value</td> <td>0</td> <td>100</td> </tr> </tbody> </table>	Repetitive Rate(ms)	RD Address	RD Length	Last Value	WR Address	WR Length	60	0	0	Hold Value	0	100																																																																																								
Repetitive Rate(ms)	RD Address	RD Length	Last Value	WR Address	WR Length																																																																																																
60	0	0	Hold Value	0	100																																																																																																

Paso	Acción																																				
7	<p>Seleccione el nodo <b>Petición 001: Elementos</b> y, a continuación, en la ficha <b>Salida</b>, defina un tipo de matriz de INT (es decir, <math>\geq 100</math> enteros). Esta es la tabla del PAC emisor que se escribirá en el PAC receptor:</p>  <p>The screenshot shows the 'Output (bit)' configuration window with the following table:</p> <table border="1" data-bbox="577 373 900 617"> <thead> <tr> <th>Offset/Device</th> <th>Offset/Connection</th> <th>Item Name</th> </tr> </thead> <tbody> <tr><td>0</td><td>0</td><td></td></tr> <tr><td>1</td><td>1</td><td></td></tr> <tr><td>2</td><td>2</td><td></td></tr> <tr><td>3</td><td>3</td><td></td></tr> <tr><td>4</td><td>4</td><td></td></tr> <tr><td>5</td><td>5</td><td></td></tr> <tr><td>6</td><td>6</td><td></td></tr> <tr><td>7</td><td>7</td><td></td></tr> <tr><td>8</td><td>8</td><td></td></tr> <tr><td>9</td><td>9</td><td></td></tr> <tr><td>10</td><td>10</td><td></td></tr> </tbody> </table> <p>The 'Item Name Definition' dialog box shows:</p> <ul style="list-style-type: none"> <li>New Item(s) Data Type: INT</li> <li>Define Selected Area As: One Item of Array Type</li> <li>Item Name (32 char max): BLOCKA_QI0_100</li> </ul>	Offset/Device	Offset/Connection	Item Name	0	0		1	1		2	2		3	3		4	4		5	5		6	6		7	7		8	8		9	9		10	10	
Offset/Device	Offset/Connection	Item Name																																			
0	0																																				
1	1																																				
2	2																																				
3	3																																				
4	4																																				
5	5																																				
6	6																																				
7	7																																				
8	8																																				
9	9																																				
10	10																																				
8	<p>Después de guardar y crear la configuración, el bloque (BLOCKA_QI0_100 en su ejemplo) se crea automáticamente como una variable de proceso:</p>  <p>The screenshot shows the 'Variables' tab with the following table:</p> <table border="1" data-bbox="201 1234 1102 1396"> <thead> <tr> <th></th> <th>Type</th> <th>Value</th> <th>Comment</th> <th>Alias</th> <th>Alias of</th> </tr> </thead> <tbody> <tr> <td>BMEP58_ECPU_EXT</td> <td>T_BMEP58_ECPU_EXT</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Modbus_Device</td> <td>T_Modbus_Device</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Outputs</td> <td>T_Modbus_Device_OUT</td> <td></td> <td>Output Variables</td> <td></td> <td></td> </tr> <tr> <td>BLOCKA_QI0_100</td> <td>ARRAY[0..99] OF INT</td> <td></td> <td></td> <td>tab_p</td> <td></td> </tr> </tbody> </table>		Type	Value	Comment	Alias	Alias of	BMEP58_ECPU_EXT	T_BMEP58_ECPU_EXT					Modbus_Device	T_Modbus_Device					Outputs	T_Modbus_Device_OUT		Output Variables			BLOCKA_QI0_100	ARRAY[0..99] OF INT			tab_p							
	Type	Value	Comment	Alias	Alias of																																
BMEP58_ECPU_EXT	T_BMEP58_ECPU_EXT																																				
Modbus_Device	T_Modbus_Device																																				
Outputs	T_Modbus_Device_OUT		Output Variables																																		
BLOCKA_QI0_100	ARRAY[0..99] OF INT			tab_p																																	

Paso	Acción
9	<p>En el PAC emisor, en una sección de código de proceso, utilice el DFB <code>MOVE</code> para copiar el contenido de la matriz "tab_p" en la matriz definida más arriba en la estructura de dispositivo del Modbus:</p>  <pre>         .1         MOVE 1         Array2---IN  OUT---Modbus_Device.Outputs:BLOCKA_QI0_100     </pre>
10	<p>En el PAC receptor, utilice el <b>Safe: Editor de datos</b> para crear una matriz de 100 enteros (Array5) como entrada en el área <b>Interfaz</b>.</p> <p>En el mismo <b>Safe: Editor de datos</b>, cree una matriz de 4 enteros (CtrlData5) como salida en el área <b>Interfaz</b>.</p> 
11	<p>En el PAC receptor, en el <b>Editor de datos de proceso</b>, cree una matriz de 100 enteros (Array3) como salida del área <b>Interfaz</b>. Vincule esta matriz Array3 con la matriz Array5 (creada en el paso 10) en la columna <b>Parámetro efectivo</b>. Los datos procedentes del PAC emisor se escribirán en esta matriz Array3 a través del explorador Modbus, siempre y cuando la matriz Array3 esté ubicada en la dirección definida en el explorador del PAC emisor (en este ejemplo, %MW0).</p> <p>En el mismo <b>Editor de datos de proceso</b>, cree una matriz de 4 enteros (CtrlData3) como entrada en el área <b>Interfaz</b>. Vincule esta matriz CtrlData3 con la matriz CtrlData5 (creada en el paso 10) en la columna <b>Parámetro efectivo</b>.</p> 

Paso	Acción
12	<p>En el PAC receptor, utilice el <b>Editor de datos de seguridad</b> para crear una matriz de 100 enteros (Array6):</p> 
13	<p>En el PAC receptor, en una sección de código de la tarea SAFE, instancie el DFB S_RD_ETH_MX2 con la matriz creada en el paso 10 (Array5) como parámetro de entrada, y con las matrices creadas en el paso 10 (CtrlData5) y el paso 12 (Array6) como parámetros de salida:</p> 
14	<p>En el PAC receptor, repita los pasos 4 a 9 a fin de configurar una comunicación de 4 enteros para enviar la matriz CtrlData2 del PAC receptor al PAC emisor.</p> <p>En este ejemplo, CtrlData debe escribirse en el PAC emisor en la dirección %MW100.</p>

## Canal negro entre pares

Cada transmisión entre pares consta tanto de *datos de seguridad del usuario*, que incluye el contenido relacionado con las aplicaciones que se transmite, como de *datos reservados*. El PAC de seguridad utiliza *datos reservados* para poner a prueba la fiabilidad de la transmisión, de modo que satisfaga los requisitos de SIL3. Los *datos reservados* constan de los elementos siguientes:

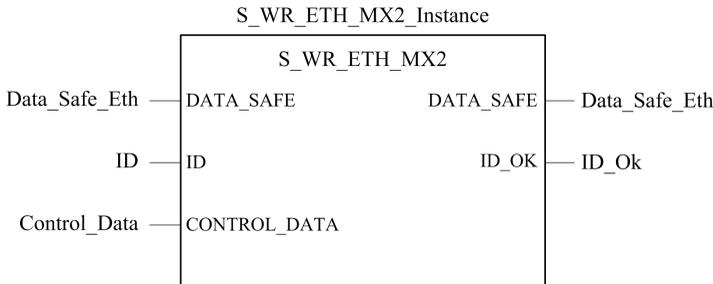
- El PAC emisor calcula un CRC partir de los datos que se van a transmitir. El PAC receptor comprueba el CRC antes de utilizar los datos transmitidos.
- Un identificador de comunicación que se incluye en el cálculo de CRC para impedir los ataques de engaño e inserción en la transmisión de datos de seguridad.

- Una marca de tiempo que contiene el tiempo de la transmisión en ms. Con la versión del firmware de la CPU 3.20 o posterior, esta marca de tiempo corresponde al valor de tiempo seguro proporcionado por la CPU receptora. Los datos que envía el PAC emisor añaden un valor de tiempo a los datos enviados al PAC receptor. El PAC receptor compara la marca de tiempo recibida con su propio valor de tiempo, y la utiliza para:
  - Comprobar la antigüedad de los datos.
  - Rechazar las transmisiones duplicadas.
  - Determinar el orden cronológico de las transmisiones recibidas.
  - Determinar el tiempo transcurrido entre transmisiones de datos.

## Configuración del DFB S\_WR\_ETH\_MX2 de la lógica del programa del PAC emisor

### Representación

Representación de DFB:



Para obtener una descripción ampliada de este DFB, consulte *EcoStruxure™ Control Expert, Seguridad, Biblioteca de bloques*.

### Descripción

El DFB S\_WR\_ETH\_MX2 está diseñado para PAC que utilizan la versión del firmware de la CPU 3.20 o posterior. Este DFB calcula datos (datos reservados que contienen un CRC y una marca de tiempo) que necesita el receptor para comprobar y gestionar errores detectados durante la comunicación entre pares segura.

El bloque de funciones DFB S\_WR\_ETH\_MX2 tiene que invocarse en cada ciclo del PAC emisor. Dentro del ciclo, se tiene que ejecutar en la lógica después de llevar a cabo todas las modificaciones necesarias en los datos que se van a enviar. Esto significa que no se

pueden modificar los datos que se van a enviar dentro del ciclo después de la ejecución del DFB; en caso contrario, la información de CRC utilizada en el área de datos reservados no será correcta y la comunicación entre pares segura no se realizará correctamente.

Debe asignar un valor exclusivo al parámetro de ID que identifique la comunicación entre pares segura entre un emisor y un receptor.

## ⚠ ADVERTENCIA

### PÉRDIDA DE CAPACIDAD PARA EJECUTAR FUNCIONES DE SEGURIDAD

El valor del parámetro ID debe ser exclusivo y estar fijado en la red para un par emisor/receptor.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## Descripción de la matriz DATA\_SAFE

Utilice las fichas **Interfaz** del **Editor de datos de seguridad** y del **Editor de datos de proceso** de Control Expert para conectar las variables de proceso y las variables de seguridad.

La conexión de las variables de proceso y de seguridad de este modo permite:

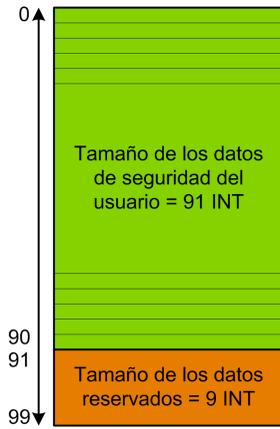
- Transferir el valor de las variables de seguridad a las variables de proceso, a través de variables globales vinculadas.
- Enviar valores de variable del área de proceso del PAC emisor al área de proceso del PAC receptor, a través de mensajes explícitos sobre Modbus TCP.

La matriz DATA\_SAFE se compone de dos zonas:

- La zona **Datos de seguridad del usuario** contiene los datos del área segura del PAC. Esta zona comienza con el índice 0 y finaliza con el índice 90.
- La zona **Datos reservados** se reserva para los datos de diagnóstico generados automáticamente, que incluyen un CRC y una marca de tiempo. El PAC receptor utiliza estos datos para determinar si los datos contenidos en la zona **Datos de seguridad del usuario** son seguros. Esta zona comienza con el índice 91 y finaliza con el índice 99.

**NOTA:** No escriba en la zona **Datos reservados**.

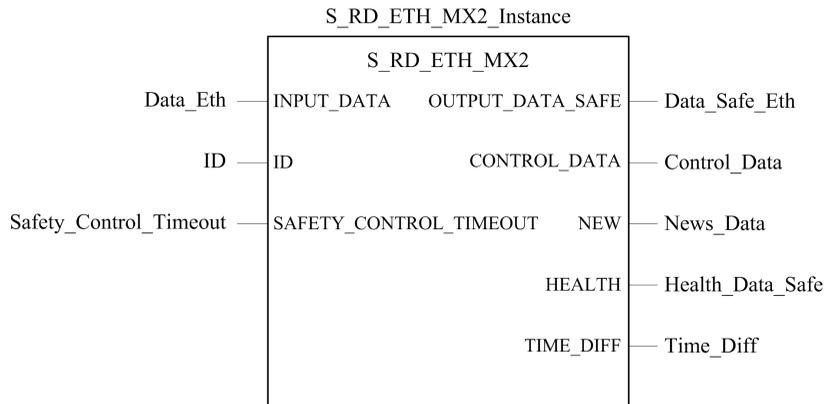
Representación de la estructura de la matriz DATA\_SAFE (array[0..99] of INT):



## Configuración del DFB S\_RD\_ETH\_MX2 de la lógica del programa del PAC receptor

### Representación

Representación de DFB:



Consulte *EcoStruxure™ Control Expert, Seguridad, Biblioteca de bloques* para obtener una descripción ampliada de este DFB.

## Descripción

El DFB `S_RD_ETH_MX2` está diseñado para PAC que utilizan la versión del firmware de la CPU 3.20 o posterior. Este DFB copia, en el área de seguridad, los datos recibidos en el área de proceso y valida la precisión de los datos recibidos.

### ⚠ ADVERTENCIA

#### PÉRDIDA DE CAPACIDAD PARA EJECUTAR FUNCIONES DE SEGURIDAD

- El bloque de funciones DFB `S_RD_ETH_MX2` se debe invocar en cada ciclo de la lógica del programa del PAC receptor y se debe ejecutar antes de que se utilicen los datos en el ciclo.
- El valor del parámetro `ID` debe ser exclusivo y estar fijado en la red para un par emisor/receptor.
- Debe comprobar el valor de bit `HEALTH` del DFB `S_RD_ETH_MX2` en cada ciclo antes usar cualquier dato seguro para gestionar la función de seguridad.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

El bloque de funciones `S_RD_ETH_MX2`:

- Copia los datos recibidos en el registro `INPUT_DATA` en el registro `OUTPUT_DATA_SAFE` si se superan las pruebas siguientes:
  - El bloque de funciones comprueba el CRC del último paquete de datos recibido mediante el explorador de E/S a través de Ethernet (Modbus TCP). Si el CRC no es correcto, los datos se consideran no seguros y no se escriben en el registro `OUTPUT_DATA_SAFE` del área de seguridad.
  - El bloque de funciones comprueba los últimos datos recibidos para determinar si son más recientes que los datos ya escritos en el registro `OUTPUT_DATA_SAFE` del área de seguridad (después de comparar las marcas de tiempo). Si los últimos datos recibidos no son más recientes, no se copian en el registro `OUTPUT_DATA_SAFE` del área de seguridad.
- Comprueba la antigüedad de los datos en el área de seguridad. Si su antigüedad es superior al valor máximo configurable establecido en el registro de entrada de `SAFETY_CONTROL_TIMEOUT`, los datos se considerarán no seguros y el bit `HEALTH` se establecerá en 0.

**NOTA:** La antigüedad de los datos es la diferencia entre la hora en la que se calculan los datos en el PAC emisor y la hora en la que se comprueban los datos en el PAC receptor.

Si el bit `HEALTH` se establece en 0, los datos disponibles en la matriz `OUTPUT_DATA_SAFE` se considerarán no seguros. En este caso, lleve a cabo las medidas oportunas.

## Descripción de las matrices INPUT\_DATA y OUTPUT\_DATA\_SAFE

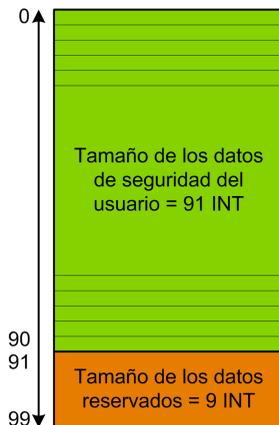
Las matrices INPUT\_DATA se componen de datos procedentes del área de memoria de datos de proceso. Las matrices OUTPUT\_DATA\_SAFE se componen de variables de seguridad. Utilice las fichas **Interfaz de datos de seguridad** e **Interfaz de datos de proceso** de Control Expert para conectar las variables de proceso y las variables de seguridad.

Las matrices INPUT\_DATA y OUTPUT\_DATA\_SAFE constan de dos zonas:

- La zona **Datos de seguridad del usuario** contiene los datos del usuario. Esta zona comienza con el índice 0 y finaliza con el índice 90.
- La zona **Datos reservados** se reserva para los datos de diagnóstico generados automáticamente, que incluyen un CRC y una marca de tiempo. El PAC receptor utiliza estos datos para determinar si los datos contenidos en la zona **Datos de seguridad del usuario** son seguros. Esta zona comienza con el índice 91 y finaliza con el índice 99.

**NOTA:** No se recomienda escribir en la zona **Datos reservados**, ya que si lo hace se sobrescribirán los datos de diagnóstico generados automáticamente.

Representación de la estructura de las matrices INPUT\_DATA y OUTPUT\_DATA\_SAFE (array[0..99] of INT):



## Descripción de la matriz CONTROL\_DATA

La matriz CONTROL\_DATA debe vincularse con variables del área "Global" (definidas a través de la "Interfaz de datos de seguridad") y, a continuación, las variables del área "Global" deben vincularse con las variables ubicadas en el área "Proceso" (definidas a través de la "Interfaz de datos de proceso") para que el explorador de E/S pueda enviar los datos al emisor correspondiente.

## Cálculo de un valor de SAFETY\_CONTROL\_TIMEOUT

Cuando calcule un valor de SAFETY\_CONTROL\_TIMEOUT, tenga en cuenta lo siguiente:

- Valor mínimo:  $\text{SAFETY\_CONTROL\_TIMEOUT} > 2 * T1$
- Valor recomendado:  $\text{SAFETY\_CONTROL\_TIMEOUT} > 3 * T1$

$T1 = \text{CPU}_{\text{sender}} \text{ MAST cycle time} + \text{CPU}_{\text{sender}} \text{ SAFE cycle time} + \text{Repetitive\_rate} + \text{Network transmission time} + \text{CPU}_{\text{receiver}} \text{ MAST cycle time} + \text{CPU}_{\text{receiver}} \text{ SAFE cycle time}$

Donde:

- $\text{CPU}_{\text{sender}} \text{ MAST cycle time}$  es el tiempo de ciclo MAST del PAC emisor.
- $\text{CPU}_{\text{sender}} \text{ SAFE cycle time}$  es el tiempo de ciclo SAFE del PAC emisor.
- $\text{Repetitive\_rate}$  es el intervalo de tiempo de la consulta de escritura del explorador de E/S del PAC emisor al PAC receptor.
- $\text{Network transmission time}$  es el tiempo consumido en la red Ethernet durante la transmisión de datos del PAC emisor al PAC receptor.
- $\text{CPU}_{\text{receiver}} \text{ MAST cycle time}$  es el tiempo de ciclo MAST del PAC receptor.
- $\text{CPU}_{\text{receiver}} \text{ SAFE cycle time}$  es el tiempo de ciclo SAFE del PAC receptor.

Observe que el valor definido en el parámetro SAFETY\_CONTROL\_TIMEOUT tiene un efecto directo sobre la solidez y disponibilidad de la comunicación segura entre pares. Si el valor del parámetro SAFETY\_CONTROL\_TIMEOUT supera considerablemente T1, la comunicación tolerará diversos retrasos (por ejemplo, retrasos en la red) o transmisiones de datos dañados.

Configure su red Ethernet de modo que la carga no provoque un retraso excesivo en la red durante la transmisión de datos, que pueda provocar la caducidad de timeout. Para evitar retrasos excesivos en las comunicaciones seguras entre pares a causa de la transmisión de otros datos no seguros en la misma red, puede utilizar una red Ethernet dedicada para el protocolo seguro entre pares.

Cuando ponga en marcha su proyecto, debe calcular el rendimiento de la comunicación segura peer-to-peer; para ello, compruebe los valores proporcionados en el parámetro de salida TIME\_DIFF y evalúe el margen utilizando el valor definido en el parámetro SAFETY\_CONTROL\_TIMEOUT.

## Descripción del bit HEALTH

Cuando el valor del bit HEALTH es:

- 1: La integridad de los datos es correcta (CRC) y la antigüedad de los datos es menor que el valor establecido en el registro de entrada `SAFETY_CONTROL_TIMEOUT`.

**NOTA:** La antigüedad de los datos considerados es el tiempo entre:

- El inicio del ciclo en el que los datos se calculan en el PAC emisor.
  - El inicio del ciclo en el que los datos se comprueban en el PAC receptor.
- 0: Los nuevos datos válidos no se reciben en el intervalo de tiempo requerido (el temporizador expira y el bit `HEALTH` se establece en 0).

**NOTA:** Si el bit `HEALTH` se establece en 0, los datos de la matriz de salida `OUTPUT_DATA_SAFE` se consideran no seguros; actúe en consecuencia.

## Comunicaciones del canal negro de M580

### Canal negro

El canal negro es el mecanismo que se utiliza para cifrar y validar los datos de seguridad transmitidos:

- Sólo el equipo de seguridad de Schneider Electric puede cifrar y descifrar los datos enviados a través del canal negro en un sistema de seguridad M580.
- El estado de cada transmisión de datos de seguridad se pone a prueba con los módulos de seguridad de recepción y transmisión para cada mensaje transmitido.

El efecto de usar el canal negro es permitir la transmisión de datos de seguridad a través de equipos intermedios no seguros, como, por ejemplo, las placas de conexiones, cableado de Ethernet, adaptadores de comunicaciones, etc. Puesto que las transmisiones del canal negro se cifran, los equipos intermedios no pueden leer ni modificar el contenido de los datos de seguridad transmitidos sin ser detectados.

Las transmisiones del canal negro funcionan al margen del protocolo de comunicaciones que se utiliza para la transmisión:

- Bus X es el portador para las transmisiones de la placa de conexiones entre dispositivos de seguridad ubicados en el mismo bastidor (por ejemplo, de la CPU a E/S locales o de un adaptador remoto de comunicación [CRA] a E/S locales).
- EtherNet/IP es el portador para transmisiones de datos entre bastidores (por ejemplo, de la CPU a un CRA).

Los módulos de E/S de seguridad y la CPU pueden enviar y recibir comunicaciones de canal negro. Para cada transmisión, el dispositivo de transmisión (CPU o E/S) añade la información siguiente al mensaje:

- Una etiqueta CRC que permite comprobar el contenido del mensaje.
- Una marca de tiempo que permite comprobar la cronología de los mensajes.

- Información adicional, incluida la versión de aplicación y la configuración de E/S utilizada, que identifica el módulo de E/S de la transmisión.

Con la versión del firmware 3.10 o anterior, cuando utilice módulos de E/S de seguridad en un bastidor remoto, configure la CPU como cliente NTP o servidor NTP.

Si no se implementa ninguno de estos diseños, no se sincronizarán los ajustes de hora de la CPU y los módulos de E/S de seguridad, y la comunicación del canal negro no funcionará correctamente. Las entradas y salidas de los módulos de E/S de seguridad en estaciones RIO pasarán al estado de seguridad (deenergizado) o de recuperación.

## ⚠ ATENCIÓN

### RIESGO DE FUNCIONAMIENTO IMPREVISTO

Si coloca módulos de E/S de seguridad en una estación RIO, la hora actual se debe configurar para el PAC con una versión del firmware de la CPU 3.10 o anterior. Habilite el servicio NTP para su sistema M580 y configure la CPU de seguridad como un servidor NTP o un cliente NTP.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

El dispositivo de recepción (E/S o CPU) descifra el mensaje y comprueba la precisión de su contenido. Se pueden detectar las condiciones siguientes:

Estado	Descripción
Errores de transmisión	Error detectado en la dirección o enrutamiento del mensaje
Repeticiones	Mensaje enviado varias veces.
Datos eliminados	Falta parte del mensaje o bien se ha perdido.
Datos insertados	Se han añadido datos adicionales al mensaje.
Secuencia incorrecta de datos	Se ha cambiado el orden del mensaje.
Datos dañados	Se han detectado uno o varios errores de bit en el mensaje.
Retardos	El tiempo de entrega del mensaje es excesivamente largo.
Engaño	No se permite enviar datos al origen del mensaje.

Cuando se detecta uno de estos errores, se determina que el canal es defectuoso y se ejecuta la función de seguridad pertinente.

- Si la CPU detecta que una transmisión de un módulo de entrada es defectuoso, la CPU establece los valores de entrada de ese módulo en el estado de seguridad (deenergizado) o de recuperación.

- Si un módulo de salida detecta que una transmisión de la CPU es defectuosa, deja sus salidas en el estado de retorno preconfigurado.

Después de que se haya restablecido la comunicación entre la CPU y el módulo de salida, las salidas pasarán automáticamente al estado ordenado por la CPU.

## **AVISO**

### **CAMBIO DE ESTADO DE SALIDA IMPREVISTO AL RESTABLECERSE LA COMUNICACIÓN**

La lógica de programa debe supervisar el estado de los canales de salida y activar la función de seguridad en consecuencia, estableciendo los comandos de salida en el estado de seguridad.

**Si no se siguen estas instrucciones, pueden producirse daños en el equipo.**

# Comunicación de CPU a E/S de seguridad de M580

## Introducción

En esta sección se describen las comunicaciones entre la CPU de seguridad y los módulos de E/S de seguridad M580.

## M580 Comunicaciones de PAC de seguridad a E/S

### Comunicación entre el PAC y E/S

La CPU y el coprocesador de seguridad de M580 controlan conjuntamente todos los intercambios de la placa de conexiones, mientras que las E/S de seguridad responden a los comandos de la CPU y el coprocesador. Los módulos de E/S de seguridad se pueden instalar en un bastidor X Bus de BMXXBP\*\*\*\* o un bastidor Ethernet de BMEXBP\*\*\*\*.

Las comunicaciones entre el PAC de seguridad y los módulos de E/S de seguridad del bastidor principal local se realizan a través de la placa de conexiones.

Las comunicaciones entre el PAC de seguridad y los módulos de E/S de seguridad instalados en la estación RIO se realizan a través de un módulo adaptador instalado en la estación RIO, ya sea:

- un adaptador BMEXBP31210, para un bastidor Ethernet, o bien
- un adaptador BMXXBP31210, para un bastidor X Bus.

**NOTA:** Con una versión del firmware de la CPU 3.20 o posterior, el módulo adaptador BM•CRA31210 necesita la versión del firmware 2.60 o posterior.

**NOTA:** No se puede utilizar un adaptador BMXXBP31200 para conectar los módulos de seguridad de E/S con el PAC de seguridad de M580.

Las comunicaciones del PAC de seguridad y de los módulos de E/S de seguridad, tanto en el bastidor principal local como en la estación RIO, se realizan a través del canal negro, página 213.

El método de sincronización de la configuración de hora de la CPU y los módulos de E/S de seguridad dependerá de la versión del firmware de la CPU:

- Para PAC con la versión del firmware de la CPU 3.10 o anterior, es necesario configurar el servicio NTP.

**NOTA:** Si instala módulos de E/S de seguridad en el bastidor local (o en una extensión del bastidor local), no es necesario habilitar el servicio NTP.

- Para PAC con la versión del firmware de la CPU 3.20 o posterior, la sincronización horaria segura se basa en un reloj interno y "monotónico".

Para obtener más información, consulte el capítulo *Sincronización horaria*, página 180.

Opcionalmente, puede utilizar los módulos repetidores de fibra óptica BMXNRP0200 o BMXNRP0201 para ampliar el enlace físico entre la CPU y el coprocesador del bastidor local y el adaptador de la estación RIO. Los módulos repetidores de fibra óptica mejoran la inmunidad al ruido de la red de la estación RIO y aumentan la distancia de cableado, al tiempo que mantienen el rango dinámico completo de la red y el nivel de integridad de seguridad.

El protocolo de comunicaciones entre la E/S de seguridad y el PAC de seguridad permite sus intercambios. Permite a los dos dispositivos comprobar la precisión de los datos recibidos, detectar los datos dañados y determinar si el módulo de transmisión pasa a no ser operativo. Así, un bucle de seguridad puede incluir cualquier placa de conexiones y adaptadores RIO no interferentes, página 29.

## Suministro de alimentación a las E/S de seguridad

Las E/S de seguridad reciben alimentación de 24 V CC y 3,3 V CC a través de la placa de conexiones con el módulo de alimentación de seguridad, página 132 M580. El módulo de alimentación de seguridad supervisa la alimentación que proporciona, de modo que no supere los 36 V CC.

### **Alimentación para las funciones que no son de seguridad:**

La alimentación de 5 V CC que proporciona la placa de conexiones se aplica por medio de cada módulo de E/S de seguridad a sus funciones que no son de seguridad.

### **Alimentación externa para E/S de seguridad digital:**

Se necesita una fuente de alimentación externa, no superior a 60 V CC, para los procesos que no son de seguridad (sensor, actuador), y puede ser una fuente de alimentación de tipo tensión extrabaja protegida (SELV/PELV), categoría de sobretensión II. El módulo de E/S supervisa la fuente de alimentación de proceso que no es de seguridad para comprobar si existen condiciones de sobretensión o infratensión.

# Diagnóstico de un sistema de seguridad de M580

## Contenido de este capítulo

Diagnósticos de la CPU y coprocesador de seguridad de M580 .....	219
Diagnósticos de fuente de alimentación de seguridad de M580 .....	232
Diagnósticos de entradas analógicas de BMXSAI0410 .....	234
Diagnósticos de entrada digital de BMXSDI1602.....	239
Diagnósticos de salida digital de BMXSDO0802.....	245
Diagnósticos de salida de relé digital BMXSRA0405.....	251

## Introducción

En este capítulo se ofrece información sobre los diagnósticos que se pueden realizar gracias a las indicaciones del hardware (en función del estado del indicador LED) y a los bits o las palabras de un sistema de seguridad de M580.

# Diagnósticos de la CPU y coprocesador de seguridad de M580

## Introducción

En esta sección se describen los diagnósticos disponibles para las CPU de seguridad de BME•58•040S y el coprocesador de seguridad BMEP58CPROS3.

## Diagnósticos de condiciones de bloqueo

### Introducción

Las condiciones de bloqueo que se generan durante la ejecución del programa de seguridad o proceso se deben a la detección de errores del sistema o al estado HALT de una tarea en la que se ha detectado el error.

**NOTA:** El PAC de seguridad M580 presenta dos estados HALT (pausa) independientes:

- La pausa de proceso se aplica a las tareas no seguras (MAST, FAST, AUX0 y AUX1). Cuando cualquier tarea de proceso entra en el estado HALT, todas las demás tareas de proceso también entran en el estado HALT.
- El SAFE HALT sólo se aplica a la tarea SAFE.

Consulte el tema *Estados de funcionamiento del PAC de seguridad M580*, página 266 para obtener una descripción de los estados HALT y STOP.

### Diagnósticos

Cuando la CPU detecta una condición de bloqueo que produce un error de sistema, se proporciona una descripción del error detectado en la palabra de sistema %SW124.

Cuando la CPU detecta una condición de bloqueo que produce un estado HALT, se proporciona una descripción del error detectado en la palabra de sistema %SW125.

Valores de la palabra de sistema %SW124 y descripción de la condición de bloqueo correspondiente:

Valor (hex) de %sw124	Descripción de la condición de bloqueo
5AF2	Error de RAM detectado en la comprobación de memoria
5AFB	Se ha detectado un error en el código del firmware de seguridad

Valor (hex) de %SW124	Descripción de la condición de bloqueo
5AF6	Se ha detectado un de desborde del watchdog de seguridad en la CPU
5AFF	Se ha detectado un de desborde del watchdog de seguridad en el coprocesador
5B01	Coprocesador no detectado durante el arranque

Valores de la palabra de sistema %SW125 y descripción de la condición de bloqueo correspondiente:

Valor (hex) de %SW125	Descripción de la condición de bloqueo
0...	Ejecución de una función desconocida
0002	Función de firma de la tarjeta SD (utilizada con las funciones <i>SIG_CHECK</i> y <i>SIG_WRITE</i> )
2258	Ejecución de la instrucción HALT
2259	El flujo de ejecución difiere del flujo de referencia
23..	Ejecución de una función CALL hacia una subrutina indefinida
5AF3	La CPU ha detectado un error de comparación
5AF9	Error de instrucción detectado durante el arranque o tiempo de ejecución
5AFA	Error de comparación detectado en el valor de CRC
5AFC	El coprocesador ha detectado un error de comparación
5AFD	Error interno detectado por el coprocesador; subcódigo en %SW126: 1 (resultado desconocido), 2 (aplicación de CRC), 7 (contador de actividad incorrecto)
5AFE	Error de sincronización de coprocesador detectado: sólo CPU; subcódigo en %SW126: 3 (diagnóstico), 4 (fin UL), 5 (comparación), 6 (BC out), 8 (HALT durante UL), 9 HALT durante comparación), 10 (HALT durante BC out).
81F4	Asiento SFC incorrecto
82F4	Código SFC inaccesible
83F4	Área de trabajo SFC inaccesible
84F4	Demasiados pasos SFC iniciales
85F4	Demasiados pasos SFC activos
86F4	Secuencia de código SFC incorrecta
87F4	Descripción incorrecta de código SFC
88F4	Tabla de referencia SFC incorrecta
89F4	Error detectado en el cálculo de índice interno del SFC
8AF4	Estado de paso SFC no disponible

Valor (hex) de %sw125	Descripción de la condición de bloqueo
8BF4	Memoria SFC demasiado pequeña después del cambio por descarga
8CF4	Sección de acción/transición inaccesible
8DF4	Área de trabajo SFC demasiado pequeña
8EF4	Versión del código SFC más antiguo que el intérprete
8FF4	Versión del código SFC más reciente que el intérprete
90F4	Descripción insuficiente de un objeto SFC: puntero NULL
91F4	Identificador de la acción no autorizado
92F4	Definición insuficiente del tiempo para el identificador de acción
93F4	No ha podido encontrarse el paso de macro en la lista de pasos activos para su desactivado
94F4	Desborde en la tabla de acción
95F4	Desborde en la tabla de activado/desactivado de pasos
9690	Error detectado en la comprobación de CRC de la aplicación (suma de control)
DE87	El cálculo ha detectado un error de coma flotante
DEB0	Desborde del watchdog de la tarea (se establecen %S11 y %S19)
DEF0	División entre 0
DEF1	Error detectado de transferencia de cadena de caracteres
DEF2	Se ha excedido la capacidad
DEF3	Desborde de índice
DEF4	periodos de tarea incoherentes
DEF7	Error detectado de ejecución SFC
DEFE	Pasos indefinidos del SFC

## Reinicio de la aplicación

Tras producirse una condición de bloqueo, se deben inicializar las tareas paradas. Si se produce la pausa (HALT) para una:

- Tarea de proceso (MAST, FAST, AUX0 o AUX1): Se realiza una inicialización mediante el comando **PLC > Inic.** de Control Expert o estableciendo el bit %S0 en 1.
- Tarea SAFE: La inicialización se realiza mediante el comando **PLC > Inicialización seguridad** de Control Expert.

Cuando se inicialice, la aplicación se comportará de la manera siguiente:

- Los datos vuelven a sus valores iniciales
- Las tareas se detienen al final del ciclo
- Se actualiza la imagen de entrada
- Las salidas se controlan en posición de retorno

A continuación, el comando RUN permite reiniciar la aplicación o las tareas.

## Diagnósticos de condiciones sin bloqueo

### Introducción

El sistema encuentra una condición sin bloqueo cuando detecta un error de entrada/salida en el bus de la placa de conexiones (X Bus o Ethernet) o a través de la ejecución de una instrucción, que pueda procesar el programa de usuario y no modifica el estado operativo de CPU.

En este se tema describen algunos de los bits y las palabras del sistema que puede utilizar para detectar el estado del sistema de seguridad y sus módulos de componentes.

**NOTA:** Los bits y las palabras del sistema disponibles no incluyen toda la información relativa al estado de módulos de seguridad. Schneider Electric recomienda utilizar la estructura de DDDT de la CPU de seguridad y los módulos de E/S para determinar el estado del sistema de seguridad de M580.

Para obtener más información sobre el DDDT de la CPU de seguridad de M580, consulte el tema *Estructura de datos DDT autónomos para las CPU M580 de Modicon M580 Hardware - Manual de referencia*.

Para obtener más información sobre los DDDT del módulo de E/S de seguridad M580, consulte los temas siguientes:

- Estructura de datos BMXSAI0410, página 61 para el módulo de entrada analógica de seguridad.
- Estructura de datos BMXSDI1602, página 94 para el módulo de entrada digital de seguridad.
- Estructura de datos BMXSDO0802, página 110 para el módulo de salida digital de seguridad.
- Estructura de datos BMXSRA0405, página 127 para el módulo de salida de relé digital de seguridad.

**NOTA:** También puede realizar diagnósticos avanzados de dispositivos Ethernet por medio de mensajes explícitos. Para lograrlo, utilice:

- El bloque de funciones READ\_VAR (véase EcoStruxure™ Control Expert, Comunicación, Biblioteca de bloques) para dispositivos Modbus TCP.

- El bloque de funciones DATA\_EXCH (véase Modicon M580, Hardware, Manual de referencia), especificando el protocolo CIP en el bloque ADDM, para dispositivos EtherNet/IP.

## Condiciones vinculadas al diagnóstico de E/S

Una condición sin bloqueo relacionada con la E/S se diagnostica por medio de las siguientes indicaciones:

- Patrón de indicador LED de **I/O** de la CPU: encendido fijo
- Patrón de indicador LED del módulo **I/O**: encendido fijo
- Bits de sistema (tipo de error detectado):
  - %S10 establecido en 0: error de E/S global detectado en uno de los módulos en el bastidor Ethernet o X Bus local o remoto
  - %S16 establecido en 0: error de E/S detectado en la tarea en curso en un bastidor X Bus
  - %S40 a %S47 establecido en 0: error de E/S detectado en un bastidor X Bus en la dirección 0 a 7
  - %S117 establecido en 0: error de RIO detectado en un bastidor X Bus remoto
  - %S119 establecido en 0: error de E/S detectado en un bastidor X Bus local

**NOTA:** Estos bits (%S10, %S16, %S40...%S47, %S117 y %S119) notifican varios posibles errores detectados (no todos) relacionados con los módulos de E/S de seguridad.
- bits y palabras de sistema combinados con el canal que tiene un error detectado (número de canal de E/S y tipo de error detectado) o información del I/O del módulo de Device DDT (para módulos configurados en la modalidad de dirección del Device DDT):
  - bit %Ir.m.c.ERR establecido en 1: canal de error detectado (intercambios implícitos)
  - palabra %MWr.m.c.2: el valor de la palabra indica el tipo de error detectado en un canal específico y depende del módulo de E/S (intercambios implícitos)

## Condiciones vinculadas a la ejecución del diagnóstico del programa

Se diagnostica una condición sin bloqueo relacionada con la ejecución del programa con los siguientes bits y palabras de sistema:

- Bits de sistema (tipo de error detectado):
  - %S15 establecido en 1: error detectado de manipulación de la cadena de caracteres.
  - %S18 establecido en 1: capacidad desbordada, error detectado en una coma flotante, o división por 0.  
(Consulte el tema *Bits del sistema para la ejecución de la tarea SAFE*, página 406 para obtener más información).  
Cuando %S18 está establecido en 1, %SW17 contiene una descripción del evento causante, página 408.
  - %S20 establecido en 1: índice desbordado.  
**NOTA:** Si el bit del sistema configurable %S78 se establece en el programa, la tarea SAFE pasa al estado HALT cuando el bit del sistema %S18 se establece en 1.
- Palabra de sistema (naturaleza del error detectado):
  - %SW125 (véase Modicon M580, Hardware, Manual de referencia) (siempre actualizado)

## LED de diagnóstico de la CPU de seguridad de M580

### LED de la CPU

Use los LED de la cara frontal de la CPU (véase Modicon M580, Guía de planificación del sistema de seguridad) relacionados con la seguridad, como se describe a continuación, para diagnosticar el estado del PAC.

En *Modicon M580 Hot Standby, Guía de planificación del sistema para arquitecturas utilizadas con más frecuencia*, consulte el tema sobre diagnósticos de LED para CPU M580 Hot Standby para obtener más información sobre cómo realizar el diagnóstico de los LED relacionados con la redundancia, incluidos **[A]**, **[B]**, **[PRIM]**, **[STBY]** y **[REMOTE RUN]**.

**NOTA:** Los indicadores LED no son indicadores fiables, por lo que no pueden garantizar la precisión de la información que proporcionan. Utilícelos únicamente para diagnósticos generales durante la puesta en marcha o la solución de problemas.

## ⚠ ADVERTENCIA

### RIESGO DE IMPRECISIÓN EN EL DIAGNÓSTICO DEL SISTEMA

No utilice los indicadores LED como indicadores operativos.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

Estado del PAC	Nombres y colores del LED:							
	RUN	ERR	E/S <sup>1</sup>	ETH MS	ETH NS	DL	SRUN	SMOD
	Verde	Rojo	Rojo	Verde/ Rojo	Verde/ Rojo	Verde	Verde	Verde
Apagado								
Encendido • Autoprueba								
No configurado					No hay ningún cable enchufado y conectado a otro dispositivo alimentado			
					 De lo contrario			
Configurado: • No se ha detectado ningún error externo							-	-
• Error externo detectado				-	-		-	-
• No hay enlace Ethernet, incluida la placa de conexiones Ethernet							-	-

Estado del PAC	Nombres y colores del LED:							
	RUN	ERR	E/S <sup>1</sup>	ETH MS	ETH NS	DL	SRUN	SMOD
	Verde	Rojo	Rojo	Verde/ Rojo	Verde/ Rojo	Verde	Verde	Verde
• Dirección IP duplicada			—				—	—
• Estado STOP (detenido)			Error detectado en módulo, canal o configuración de E/S		No conectado		Tarea SAFE en ejecución	Modalidad de seguridad o bien
			No se ha detectado ningún error en la entrada/salida configurada		Conectado		Tarea SAFE detenida	Modalidad de mantenimiento
					Sin cable			
• Estado RUN (en ejecución)			—		No conectado		Tarea SAFE en ejecución	Modalidad de seguridad o bien
					Conectado		Tarea SAFE detenida	Modalidad de mantenimiento
					Sin cable			
Estado HALT (error recuperable detectado)			—				Tarea SAFE en ejecución	Modalidad de seguridad

Estado del PAC	Nombres y colores del LED:							
	RUN	ERR	E/S <sup>1</sup>	ETH MS	ETH NS	DL	SRUN	SMOD
	Verde	Rojo	Rojo	Verde/ Rojo	Verde/ Rojo	Verde	Verde	Verde
								
							Tarea SAFE deteni- da	Modalidad de manteni- miento
Estado SAFE (error no recuperable detectado)								
Actualización del SO								
1. No todos los errores detectados para un módulo de E/S de seguridad se notifican mediante LED. Compruebe los DDDT de los módulos de E/S de seguridad para obtener información adicional.								

Legenda:

Símbolo	Descripción	Símbolo	Descripción	Símbolo	Descripción
	Verde fijo		Rojo fijo		OFF
	Verde intermitente (500 ms encendido, 500 ms apagado)		Rojo intermitente (500 ms encendido, 500 ms apagado)	–	No aplicable

## LED de diagnóstico de coprocesador de seguridad M580

### LED de coprocesador

Utilice LED en la parte frontal del coprocesador (véase Modicon M580, Guía de planificación del sistema de seguridad) para diagnosticar el estado del PAC de la forma siguiente

Estado del coprocesador	Nombres y colores del LED:			
	SRUN	ERR	SMOD	DL
	Verde	Rojo	Verde	Verde
Apagado				
Estado WAIT (espere a que se descargue el firmware de la CPU)				
No configurado (sin aplicación)				
Configurado y operativo en modalidad de seguridad: • Tarea SAFE detenida				
• Tarea SAFE en ejecución				
Configurado y operativo en modalidad de mantenimiento: • Tarea SAFE detenida				
• Tarea SAFE en ejecución				
Tarea SAFE en HALT (error recuperable detectado)				
Estado SAFE (error no recuperable detectado)				

Leyenda:

Símbolo	Descripción	Símbolo	Descripción	Símbolo	Descripción
	Verde fijo		Rojo fijo		OFF

Símbolo	Descripción	Símbolo	Descripción	Símbolo	Descripción
	Verde intermitente (500 ms encendido, 500 ms apagado)		Rojo intermitente (500 ms encendido, 500 ms apagado)		

## LED de acceso a la tarjeta de memoria

### Introducción

El LED verde de acceso a la tarjeta de memoria de debajo de la puerta de la tarjeta de memoria SD indica el acceso de la CPU a la tarjeta de memoria cuando se inserta una tarjeta. Este LED puede verse cuando se abre la puerta.

### Estados de LED específicos

Los LEDs de **acceso a la tarjeta de memoria** indican estos estados:

Estados de los indicadores LED	Descripción
ENCENDIDO	Tarjeta de memoria reconocida, pero la CPU no accede a ella.
parpadeo	La CPU está accediendo a la tarjeta de memoria.
intermitente	La tarjeta de memoria no se ha reconocido.
APAGADO	La tarjeta de memoria puede extraerse del slot de la CPU, o la CPU no reconoce la tarjeta de memoria.

**NOTA:** Confirme que el LED esté apagado antes de retirar la tarjeta del slot.

### Significados de los LED combinados

El LED de acceso a la tarjeta de memoria funciona junto con el LED (véase Modicon M580, Hardware, Manual de referencia) de **BACKUP**. Sus patrones combinados indican la siguiente información de diagnóstico:

Estado de la tarjeta de memoria	Condiciones	Estado de la CPU	Indicador LED de acceso a la tarjeta de memoria	LED de BACKUP
No hay ninguna tarjeta de memoria en el slot	—	Sin configuración		
Tarjeta de memoria no correcta	—	Sin configuración		
Tarjeta de memoria sin proyecto	—	Sin configuración		
Tarjeta de memoria con un proyecto incompatible	—	Sin configuración		
Tarjeta de memoria con un proyecto compatible	Se detecta un error cuando se restaura el proyecto desde la tarjeta de memoria a la RAM de la CPU.	Sin configuración	durante la transferencia:  fin de la transferencia: 	durante la transferencia:  fin de la transferencia: 
	No se detecta ningún error cuando se restaura el proyecto desde la tarjeta de memoria a la RAM de la CPU.	—	durante la transferencia:  fin de la transferencia: 	durante la transferencia:  fin de la transferencia: 

– Ningún estado o condición específico de la CPU

En esta leyenda se muestran los diferentes patrones de los LED:

<b>Símbolo</b>	<b>Significado</b>	<b>Símbolo</b>	<b>Significado</b>
	Apagado		rojo permanente
	verde permanente		verde parpadeante

# Diagnósticos de fuente de alimentación de seguridad de M580

## Introducción

En esta sección se describen los diagnósticos disponibles para las fuentes de alimentación de seguridad de M580.

## Diagnóstico mediante LED de la fuente de alimentación

### LED de fuente de alimentación

Las fuentes de alimentación de seguridad BMXCPS4002S, BMXCPS4022S y BMXCPS3522S presentan un panel frontal que incluye los LED de diagnóstico siguientes:

- **OK**: Estado de funcionamiento
- **ACT**: Actividad
- **RD**: Redundancia (para diseños de fuente de alimentación redundante)

Los LED de fuente de alimentación de seguridad M580 pueden presentar la siguiente información de diagnóstico:

LED	Descripción
Aceptar	<ul style="list-style-type: none"> <li>• Encendido (verde) indica que las condiciones siguientes son verdaderas:                             <ul style="list-style-type: none"> <li>◦ La tensión de la placa de conexiones de 24 V CC es correcta.</li> <li>◦ La tensión de la placa de conexiones de 3,3 V CC es correcta.</li> <li>◦ El botón de restablecimiento no se ha activado.</li> </ul> </li> <li>• El parpadeo indica que una de las afirmaciones siguientes es verdadera:                             <ul style="list-style-type: none"> <li>◦ La corriente de la placa de conexiones de 24 V CC no es correcta.</li> <li>◦ La corriente de la placa de conexiones de 3,3 V CC no es correcta y no se ha activado el botón de restablecimiento.</li> </ul> </li> <li>• Apagado indica que al menos una de las condiciones es verdadera:                             <ul style="list-style-type: none"> <li>◦ La tensión de la placa de conexiones de 24 V CC no es correcta.</li> <li>◦ La tensión de la placa de conexiones de 3,3 V CC no es correcta.</li> <li>◦ El botón de restablecimiento se ha activado.</li> </ul> </li> </ul>
ACT	<ul style="list-style-type: none"> <li>• Encendido (verde) indica que la fuente de alimentación está suministrando alimentación. En un diseño de fuente de alimentación redundante, el módulo es el componente primario.</li> <li>• Apagado indica que la fuente de alimentación no está suministrando alimentación. En un diseño de fuente de alimentación redundante, el módulo es el standby.</li> </ul>
RD	<ul style="list-style-type: none"> <li>• Encendido (verde) indica que la comunicación entre los dos módulos de alimentación es correcta.</li> <li>• El parpadeo indica que una de las afirmaciones siguientes es verdadera:                             <ul style="list-style-type: none"> <li>◦ La corriente de la placa de conexiones de 24 V CC no es correcta.</li> <li>◦ La corriente de la placa de conexiones de 3,3 V CC no es correcta.</li> </ul> </li> <li>• Apagado indica que al menos una de las afirmaciones es verdadera:                             <ul style="list-style-type: none"> <li>◦ La comunicación entre los dos módulos de alimentación no es correcta.</li> <li>◦ Se están realizando las autopruuebas.</li> </ul> </li> </ul>

# Diagnósticos de entradas analógicas de BMXSAI0410

## Introducción

En esta sección se describen las herramientas de diagnóstico disponibles para el módulo de entrada analógica de seguridad BMXSAI0410.

## Diagnósticos de DDDT de BMXSAI0410

### Introducción

El módulo de entrada analógica de seguridad BMXSAI0410 proporciona los diagnósticos siguientes utilizando sus elementos DDT de dispositivo `T_U_ANA_SIS_IN_4`, página 62:

- Diagnósticos de entrada
- Detección de error interno
- Diagnósticos de cableado de canal

### Diagnósticos de entrada

Los sensores conectados a cada canal se supervisan dada su capacidad para medir con precisión 10 valores de entrada analógica entre 4 y 20 mA. Si las pruebas de medición de entrada no son correctas, el bit `CH_HEALTH` de la estructura de DDDT `T_U_ANA_SIS_CH_IN`, página 64 se establece en 0, lo que indica que no está operativo.

### Detección de error interno

El módulo procesa el valor de entrada mediante dos circuitos paralelos independientes. Los dos valores se comparan para determinar si un error interno se detecta en el proceso del módulo: Si los valores comparados son diferentes, el bit `IC` de la estructura de DDDT `T_U_ANA_SIS_CH_IN` se establece en 1, lo que indica que no está operativo.

Consulte el diagrama de arquitectura, página 145 para el módulo de entrada analógica de seguridad BMXSAI0410 a fin de obtener una presentación visual de este proceso.

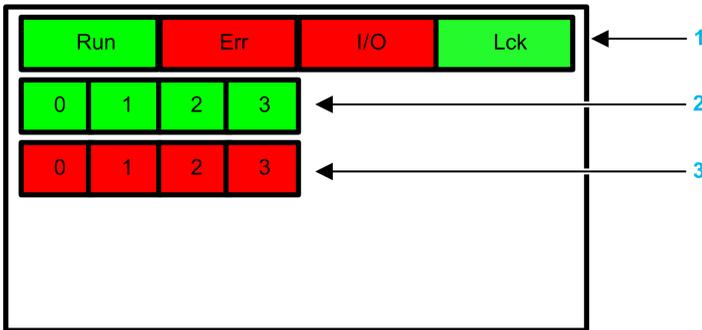
## Diagnósticos de cableado de canal

El cableado del sensor al canal de entrada se diagnostica continuamente para comprobar si hay una condición de cable cortado, lo que se detecta cuando la corriente medida es inferior a 3,75 mA o superior a 20,75 mA. En este caso, el bit `00R` de la estructura de DDDT `T_U_ANA_SIS_CH_IN` se establece en 1.

## LED de diagnóstico de entradas analógicas BMXSAI0410

### Panel de LED

El módulo de entrada analógica BMXSAI0410 presenta el siguiente panel de LED en la parte frontal:



1 Indicadores LED de estado del módulo

2 LED de estado del canal

3 LED de error detectado de canal

#### NOTA:

- Los LED de error detectados de canal sólo son operativos una vez que se ha configurado correctamente el módulo. Cuando se detecta un error de canal, el LED correspondiente se mantiene encendido hasta que se resuelve la condición subyacente.
- Puesto que el módulo de entrada incluye sólo cuatro canales, no se utilizan los LED en las posiciones 4 a 7 y nunca se encienden.

## Diagnóstico de módulos

Utilice los cuatro LED situados en la parte superior del panel de LED para diagnosticar la condición del módulo de entrada analógica BMXSAI0410:

LED del módulo				Estado del módulo	Respuesta recomendada
Run	Err	I/O	LCK		
Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	Autoprueba al encender.	–
Intermitente <sup>1</sup>	ENCENDIDO	OFF	Intermitente <sup>1</sup>	La autoprueba durante el encendido ha detectado un error interno en canales de entrada.	Reemplace el módulo.
Inactiva	ENCENDIDO	Inactiva	Inactiva	Error interno detectado.	Reemplace el módulo si la condición persiste.
OFF	Intermitente <sup>1</sup>	APAGADO	X	Módulo de E/S no configurado.	Configure el módulo a través de la CPU.
X	X	ENCENDIDO	X	Error externo detectado en el canal de entrada.	Consulte <i>Diagnóstico de canal</i> , página 237 (más abajo).
ENCENDIDO	Intermitente <sup>1</sup>	X	X	No hay comunicación entre la CPU y el módulo de E/S.	Verifique que: <ul style="list-style-type: none"> <li>• La CPU es una CPU de seguridad de M580 y esté operativa.</li> <li>• La placa de conexiones esté operativa (si el módulo de E/S se encuentra en el bastidor principal).</li> <li>• El cable entre la CPU y el módulo de E/S esté operativo y esté correctamente conectado (si el módulo de E/S se encuentra en un bastidor ampliado o remoto).</li> </ul>
ENCENDIDO	Parpadeo <sup>2</sup>	X	APAGADO	La comunicación no es segura y la configuración está desbloqueada.	Depure la condición mediante las variables de DDDT, página 61 para la instancia del módulo de E/S.
ENCENDIDO	Parpadeo <sup>2</sup>	X	ENCENDIDO	La comunicación no es segura y la configuración está bloqueada.	Verifique que:

LED del módulo				Estado del módulo	Respuesta recomendada
Run	Err	I/O	LCK		
					<ul style="list-style-type: none"> <li>La configuración bloqueada del módulo sea igual a la configuración del módulo almacenada en la aplicación de la CPU, tal como se ha configurado mediante Control Expert.</li> <li>Depure la condición mediante las variables de DDDT, página 61 para la instancia del módulo de E/S.</li> </ul>
ENCENDIDO	ENCENDIDO	Inactiva	X	Error interno detectado del canal de entrada.	Reemplace el módulo si la condición persiste.
ENCENDIDO	Inactiva	Inactiva	Inactiva	La comunicación con la CPU es correcta y la configuración está desbloqueada.	–
ENCENDIDO	Inactiva	Inactiva	ENCENDIDO	La comunicación con la CPU es correcta y la configuración está bloqueada.	–

X indica que el estado del LED puede ser encendido o apagado.

- Intermitente: 500 ms encendido/500 ms apagado.
- Parpadeo: 50 ms encendido/50 ms apagado.

## Diagnóstico de canal

Use todos los LED en el módulo de entrada analógica BMXSAI0410 para diagnosticar el estado del canal:

LED del módulo				Indicadores LED de canal		Estado del canal	Respuesta recomendada
Run	Err	I/O	LCK	Estado del canal (LED 0-3)	Error detectado (LED 0-3)		
ENCENDIDO	Inactiva	Apagado	X	ENCENDIDO	Inactiva	La corriente de entrada se encuentra en el rango 4-20 mA del canal.	–
ENCENDIDO	Inactiva	EN-	X	Inactiva	Inactiva	La corriente de entrada se encuentra	Verifique que la fuente de alimentación externa,

LED del módulo				Indicadores LED de canal		Estado del canal	Respuesta recomendada
Run	Err	I/O	LCK	Estado del canal (LED 0-3)	Error detectado (LED 0-3)		
		CE-NDI-DO				en el rango 4-20 mA del canal.	el cableado externo y el sensor estén operativos.
EN-CEN-DIDO	EN-CE-NDI-DO	Inac-tiva	X	Inactiva	ENCENDIDO	El canal no está operativo.	Reemplace el módulo si la condición persiste.
X indica que el estado del LED puede ser encendido o apagado.							

# Diagnósticos de entrada digital de BMXSDI1602

## Introducción

En esta sección se describen las herramientas de diagnóstico disponibles para el módulo de entrada digital de seguridad BMXSDI1602.

## Diagnósticos de DDDT de BMXSDI1602

### Introducción

El módulo de entrada digital de seguridad BMXSDI1602 proporciona los diagnósticos siguientes mediante sus elementos DDT de dispositivo T\_U\_DIS\_SIS\_IN\_16, página 94:

- Diagnósticos de entrada
- Detección de error interno
- Diagnósticos de cableado de canal
- diagnósticos de sobretensión e infratensión

### Diagnósticos de entrada

Se prueba la eficacia operativa de cada canal de entrada al iniciar cada ciclo (o exploración). Cada canal se fuerza al estado energizado y se prueba para comprobar que se ha alcanzado el estado energizado. A continuación, el canal se fuerza al estado deenergizado y se vuelve probar para comprobar que se ha alcanzado el estado deenergizado.

Si el canal no conmuta correctamente entre el estado energizado y deenergizado, el bit CH\_HEALTH de la estructura de DDDT T\_U\_DIS\_SIS\_CH\_IN, página 97 se establece en 0, lo que indica que no está operativo.

### Detección de error interno

Cada ciclo, el módulo realiza una secuencia de diagnóstico de entrada. El módulo procesa el valor de entrada mediante dos circuitos idénticos e independientes. Los dos valores se comparan para determinar si existe un error interno en el proceso interno del módulo. Si los valores comparados son diferentes, el bit IC de la estructura de DDDT T\_U\_DIS\_SIS\_CH\_IN se establece en 1, lo que indica que no está operativo.

Consulte el diagrama de arquitectura, página 146 para el módulo de entrada digital de seguridad BMXSDI1602 a fin de obtener una presentación visual de este proceso.

## Diagnósticos de cableado de canal

El cableado del sensor al canal de entrada se puede diagnosticar continuamente para ver si se producen alguna de estas condiciones:

- Cable cortado (circuito abierto)
- Cortocircuito a 24 V CC
- Cortocircuito a 0 V CC
- Cruce entre dos canales paralelos

La disponibilidad de estos diagnósticos depende de la fuente de alimentación que utiliza el diseño de cableado específico, página 73 y de que la función de diagnóstico esté habilitada en la página de configuración del módulo.

Si se detecta una de estas condiciones, la estructura de DDDT `T_U_DIS_SIS_CH_IN` establece el valor de bit asociado en 1, de la manera siguiente:

- El bit `OC` se establece en 1 si se detecta una condición de cable abierto (cortado) o un cortocircuito a tierra de 0 V CC.
- El bit `SC` se establece en 1 si se detecta un cortocircuito a la fuente de 24 V CC o un cruce entre dos canales.

## Diagnósticos de sobretensión e infratensión

El módulo realiza pruebas continuamente para ver si existe una condición de infratensión y sobretensión. Se aplican los valores de umbral siguientes:

- Umbral de infratensión = 18,6 V CC
- Umbral de sobretensión = 33 V CC

Si se detecta una de estas dos condiciones, el módulo establece el bit `PP_STS` del DDT de dispositivo `T_U_DIS_SIS_IN_16` en 0.

# LED de diagnóstico de entradas digitales BMXSDI1602

## Panel de LED

El módulo de entrada digital BMXSDI1602 presenta el siguiente panel de LED en la parte frontal:



- 1 Indicadores LED de estado del módulo
- 2 LED de estado del canal para el Rango A
- 3 LED de error detectado de canal para el Rango A
- 4 LED de estado del canal para el Rango B
- 5 LED de error detectado de canal para el Rango B

**NOTA:** Cuando se detecta un error de canal, el LED correspondiente se mantiene encendido hasta que se resuelve la condición subyacente.

## Diagnóstico de módulos

Utilice los cuatro LED situados en la parte superior del panel de LED para diagnosticar la condición del módulo de entrada digital BMXSDI1602:

LED del módulo				Estado del módulo	Respuesta recomendada
Run	Err	I/O	LCK		
Intermitente	Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	Autopruueba al encender.	–
Intermitente	ENCENDIDO	OFF	Intermitente <sup>1</sup>	La autopruueba durante el encendido ha detectado un error interno en canales de entrada.	Reemplace el módulo.

LED del módulo				Estado del módulo	Respuesta recomendada
Run	Err	I/O	LCK		
Intermitente	ENCENDIDO	ENCENDIDO	Intermitente <sup>1</sup>	<ul style="list-style-type: none"> <li>El módulo de autoprueba durante el encendido ha detectado un error interno en canales de entrada; o bien</li> <li>La fuente de alimentación de 24 V CC externa está fuera del rango.</li> </ul>	Verifique que la fuente de alimentación de 24 V CC del preactuador externa esté operativa y conecte la alimentación de 24 V CC.
Inactiva	ENCENDIDO	Inactiva	Inactiva	Error interno detectado.	Reemplace el módulo si la condición persiste.
OFF	Intermitente <sup>1</sup>	APAGADO	X	Módulo de E/S no configurado.	Configure el módulo a través de la CPU.
X	XX	ENCENDIDO	X	<ul style="list-style-type: none"> <li>La fuente de alimentación de 24 V CC externa está fuera del rango, o bien</li> <li>Error externo detectado en el canal de entrada.</li> </ul>	<ul style="list-style-type: none"> <li>Verifique que la fuente de alimentación de 24 V CC externa del preactuador está operativa.</li> <li>Consulte <i>Diagnóstico de canal</i>, página 243.</li> </ul>
ENCENDIDO	Intermitente <sup>1</sup>	X	X	No hay comunicación entre la CPU y el módulo.	<p>Verifique que:</p> <ul style="list-style-type: none"> <li>La CPU es una CPU de seguridad de M580 y esté operativa.</li> <li>La placa de conexiones esté operativa (si el módulo de E/S se encuentra en el bastidor principal).</li> <li>El cable entre la CPU y el módulo de E/S esté operativo y esté correctamente conectado (si el módulo de E/S se encuentra en un bastidor ampliado o remoto).</li> </ul>
ENCENDIDO	Parpadeo <sup>2</sup>	X	APAGADO	La comunicación no es segura y la configuración está desbloqueada.	Depure la condición mediante las variables de DDDT, página 94 para la instancia del módulo de E/S.

LED del módulo				Estado del módulo	Respuesta recomendada
Run	Err	I/O	LCK		
ENCENDIDO	Parpadeo <sup>2</sup>	X	ENCENDIDO	La comunicación no es segura y la configuración está bloqueada.	<ul style="list-style-type: none"> <li>Verifique que la configuración bloqueada del módulo sea igual a la configuración del módulo almacenada en la aplicación de la CPU, tal como se ha configurado mediante Control Expert.</li> <li>Depure la condición mediante las variables de DDDT, página 94 para la instancia del módulo de E/S.</li> </ul>
ENCENDIDO	ENCENDIDO	Inactiva	X	Error interno detectado de canal de entrada.	Reemplace el módulo si la condición persiste.
ENCENDIDO	Inactiva	Inactiva	Inactiva	La comunicación con la CPU es correcta y la configuración está desbloqueada.	–
ENCENDIDO	Inactiva	Inactiva	ENCENDIDO	La comunicación con la CPU es correcta y la configuración está bloqueada.	–

X indica que el estado del LED puede ser encendido o apagado.

1. Intermitente: 500 ms encendido/500 ms apagado.

2. Parpadeo: 50 ms encendido/50 ms apagado.

## Diagnóstico de canal

Use todos los LED en el módulo de entrada digital BMXSDI1602 para diagnosticar el estado del canal:

LED del módulo				Indicadores LED de canal		Estado del canal	Respuesta recomendada
Run	Err	I/O	LCK	Estado del canal (LED 0-7, rango A/B)	Error detectado (LED 0-7, rango A/B)		
ENCENDIDO	Inactiva	Inactiva	X	ENCENDIDO	Inactiva	Estado de entrada activada.	–
EN-	Inactiva	Inactiva	X	Inactiva	Inactiva	Estado de entrada desactivada.	–

LED del módulo				Indicadores LED de canal		Estado del canal	Respuesta recomendada
Run	Err	I/O	LCK	Estado del canal (LED 0-7, rango A/B)	Error detectado (LED 0-7, rango A/B)		
CE-NDI-DO							
EN-CE-NDI-DO	EN-CE-NDI-DO	Inac-tiva	X	Inactiva	ENCENDIDO	Estado de entrada desactivada. Se ha detectado un error interno en el canal.	Para cambiar el módulo si la condición es permanente
EN-CE-NDI-DO	EN-CE-NDI-DO	EN-CEN-DIDO	X	Inactiva	ENCENDIDO	La fuente de alimentación de 24 V CC externa está fuera de rango.	Verifique que la fuente de alimentación de 24 V CC externa del preactuador está operativa.
EN-CE-NDI-DO	Inac-tiva	EN-CEN-DIDO	X	X	Intermitente <sup>1</sup>	La entrada se encuentra en una de las dos condiciones: <ul style="list-style-type: none"> <li>• Una condición de circuito abierto.</li> <li>• Una condición de cortocircuito con 0 V CC.</li> </ul>	Verifique que el cableado esté operativo y esté correctamente conectado.
EN-CE-NDI-DO	Inac-tiva	EN-CEN-DIDO	X	X	Parpadeo <sup>2</sup>	La entrada se encuentra en una de las dos condiciones: <ul style="list-style-type: none"> <li>• Una condición de cortocircuito con 24 V CC.</li> <li>• Una condición de cortocircuito con 0 V CC.</li> </ul>	Verifique que el cableado esté operativo y esté correctamente conectado.
X indica que el estado del LED puede ser encendido o apagado.							

# Diagnósticos de salida digital de BMXSDO0802

## Introducción

En esta sección se describen las herramientas de diagnóstico disponibles para el módulo de salida digital de seguridad BMXSDO0802.

## Diagnósticos de DDDT de BMXSDO0802

### Introducción

El módulo de salida digital de seguridad BMXSDO0802 proporciona los diagnósticos siguientes mediante sus elementos DDT de dispositivo `T_U_DIS_SIS_OUT_8`, página 111:

- Diagnósticos de salida
- Detección de error interno
- Diagnósticos de cableado de canal
- diagnósticos de sobretensión e infratensión

### Diagnósticos de salida

Se prueba la eficacia operativa de cada canal de salida al iniciar cada ciclo (o exploración). La prueba consiste en conmutar los estados de contacto de salida (de ENCENDIDO a APAGADO, o de APAGADO a ENCENDIDO) durante un tiempo que no sea demasiado largo y evite la respuesta del actuador (inferior a 1 ms). Si el canal no cambia entre el estado energizado y deenergizado, el bit `CH_HEALTH` de la estructura de DDDT `T_U_DIS_SIS_CH_OUT`, página 113 se establece en 0, lo que indica que no está operativo.

### Detección de error interno

El módulo procesa el valor de salida mediante dos circuitos idénticos e independientes. Cada circuito lee la tensión de punto medio en el canal. Se comparan los valores, y si los valores no son los valores previstos, se indica un error detectado interno estableciendo el bit `IC` de la estructura de DDDT `T_U_DIS_SIS_CH_OUT` en 1, lo que indica que no está operativo.

Consulte el diagrama de arquitectura, página 147 para el módulo de salida digital de seguridad BMXSDO0802 a fin de obtener una presentación visual de este proceso.

## Diagnósticos de cableado de canal

El cableado del actuador al canal de salida se puede diagnosticar continuamente para ver si se producen alguna de estas condiciones:

- Cable cortado (circuito abierto)
- Cortocircuito a 24 V CC
- Cortocircuito a 0 V CC
- Cruce entre dos canales paralelos
- Sobrecarga del canal

**NOTA:** La sobrecarga del canal se puede detectar sólo si se ha energizado la salida.

La disponibilidad de estos diagnósticos depende de que la función de diagnóstico esté habilitada en la página de configuración del módulo.

Si se detecta una de estas condiciones, la estructura de DDDT `T_U_DIS_SIS_CH_OUT` establece el valor de bit asociado en 1, de la manera siguiente:

- Si se detecta una condición de cable abierto (cortado), el bit `OC` se establece en 1.
- El bit `SC` se establece en 1 si se detecta un cortocircuito a la fuente de 24 V CC o un cruce entre dos canales.
- El bit `OL` se establece en 1 si se detecta una condición de cortocircuito a la tierra de 0 V CC o sobrecarga de canal.

## Diagnósticos de sobretensión e infratensión

El módulo realiza pruebas continuamente para ver si existe una condición de infratensión y sobretensión. Se aplican los valores de umbral siguientes:

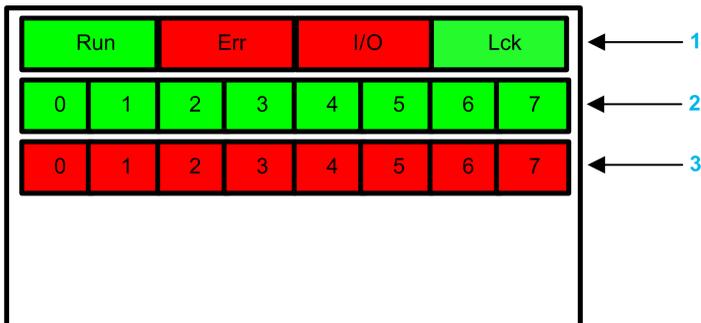
- Umbral de infratensión = 18 V CC
- Umbral de sobretensión = 31,8 V CC

Si se detecta una de estas dos condiciones, el módulo establece el bit `PP_STS` del DDT de dispositivo `T_U_DIS_SIS_OUT_8` en 0.

## LED de diagnóstico de salidas digitales BMXSDO0802

### Panel de LED

El módulo de salida digital BMXSDO0802 presenta el siguiente panel de LED en la parte frontal:



1 Indicadores LED de estado del módulo

2 LED de estado del canal

3 LED de error detectado de canal

**NOTA:** Cuando se detecta un error de canal, el LED correspondiente se mantiene encendido hasta que se resuelve la condición subyacente.

### Diagnóstico de módulos

Utilice los cuatro LED situados en la parte superior del panel de LED para diagnosticar la condición del módulo de salida digital BMXSDO0802:

LED del módulo				Estado del módulo	Respuesta recomendada
Run	Err	I/O	LCK		
Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	Autoprueba al encender.	–
Intermitente <sup>1</sup>	ENCENDIDO	OFF	Intermitente <sup>1</sup>	La autoprueba durante el encendido ha detectado un error interno en canales de salida.	Reemplace el módulo.

LED del módulo				Estado del módulo	Respuesta recomendada
Run	Err	I/O	LCK		
Intermitente <sup>1</sup>	ENCENDIDO	ENCENDIDO	Intermitente <sup>1</sup>	<ul style="list-style-type: none"> <li>El módulo de autoprueba durante el encendido ha detectado un error interno en canales de salida; o bien</li> <li>La fuente de alimentación de 24 V CC externa está fuera del rango.</li> </ul>	Verifique que la fuente de alimentación de 24 V CC del preactuador externa esté operativa y conecte la alimentación de 24 V CC.
Inactiva	ENCENDIDO	Inactiva	Inactiva	Error interno detectado.	Reemplace el módulo si la condición persiste.
OFF	Intermitente <sup>1</sup>	APAGADO	X	Módulo de E/S no configurado.	Configure el módulo a través de la CPU.
X	X	ENCENDIDO	X	<ul style="list-style-type: none"> <li>La fuente de alimentación de 24 V CC externa está fuera del rango, o bien</li> <li>Error externo detectado en el canal de salida.</li> </ul>	<ul style="list-style-type: none"> <li>Verifique que la fuente de alimentación de 24 V CC externa del preactuador está operativa.</li> <li>Consulte <i>Diagnóstico de canal</i>, página 249 (más abajo).</li> </ul>
ENCENDIDO	Intermitente <sup>1</sup>	X	X	No hay comunicación entre la CPU y el módulo. El módulo se encuentra en estado de retorno (o bien se está restableciendo si el módulo no ha funcionado nunca con normalidad).	Verifique que: <ul style="list-style-type: none"> <li>La CPU es una CPU de seguridad de M580 y esté operativa.</li> <li>La placa de conexiones esté operativa (si el módulo de E/S se encuentra en el bastidor principal).</li> <li>El cable entre la CPU y el módulo de E/S esté operativo y esté correctamente conectado (si el módulo de E/S se encuentra en un bastidor ampliado o remoto).</li> </ul>
ENCENDIDO	Parpadeo <sup>2</sup>	X	APAGADO	La comunicación no es segura y la configuración está desbloqueada. El módulo se encuentra en estado de retorno (o bien se está restableciendo si el módulo no ha	Con el fin de verificar las variables disponibles para depurar la comunicación segura en DDDT.

LED del módulo				Estado del módulo	Respuesta recomendada
Run	Err	I/O	LCK		
				funcionado nunca con normalidad).	
ENCENDIDO	Parpadeo <sup>2</sup>	X	ENCENDIDO	La comunicación no es segura y la configuración está bloqueada. El módulo se encuentra en estado de retorno.	<ul style="list-style-type: none"> <li>Verifique que la configuración bloqueada del módulo sea igual a la configuración del módulo almacenada en la aplicación de la CPU, tal como se ha configurado mediante Control Expert.</li> <li>Depure la condición mediante las variables de DDDT, página 110 para la instancia del módulo de E/S.</li> </ul>
ENCENDIDO	ENCENDIDO	Inactiva	X	Error interno detectado en el canal de salida.	Reemplace el módulo si la condición persiste.
ENCENDIDO	Inactiva	Inactiva	Inactiva	La comunicación con la CPU es segura y la configuración está desbloqueada.	–
ENCENDIDO	Inactiva	Inactiva	ENCENDIDO	La comunicación con la CPU es segura y la configuración está bloqueada.	–
<p>X indica que el estado del LED puede ser encendido o apagado.</p> <p>1. Intermitente: 500 ms encendido/500 ms apagado.</p> <p>2. Parpadeo: 50 ms encendido/50 ms apagado.</p>					

## Diagnóstico de canal

Use todos los LED en el módulo de salida digital BMXSDO0802 para diagnosticar el estado del canal:

LED del módulo				Indicadores LED de canal		Estado del canal	Respuesta recomendada
Run	Err	I/O	LCK	Estado de canal (LED 0-7)	Error detectado (LED 0-7)		
ENCENDIDO	Inactiva	Inactiva	X	ENCENDIDO	Inactiva	Estado de salida activo.	–
ENCENDIDO	Inactiva	Inactiva	X	Inactiva	Inactiva	Estado de salida inactivo.	–
ENCENDIDO	ENCENDIDO	Inactiva	X	Inactiva	ENCENDIDO	Estado de salida inactivo. Error interno detectado en el canal de salida.	Reemplace el módulo si la condición persiste.
ENCENDIDO	ENCENDIDO	ENCENDIDO	X	Inactiva	ENCENDIDO	La fuente de alimentación de 24 V CC externa del preactuador está fuera de rango.	Verifique que la fuente de alimentación de 24 V CC está operativa.
ENCENDIDO	Inactiva	ENCENDIDO	X	OFF	Intermitente <sup>1</sup>	La salida se encuentra en: <ul style="list-style-type: none"> <li>• Una condición de circuito abierto.</li> <li>• Una condición de cortocircuito con 0 V CC; o bien</li> <li>• En sobrecarga de tensión.</li> </ul>	Verifique que el cableado esté operativo y esté correctamente conectado.
ENCENDIDO	Inactiva	ENCENDIDO	X	ENCENDIDO	Parpadeo <sup>2</sup>	La salida se encuentra en: <ul style="list-style-type: none"> <li>• Una condición de cortocircuito con 24 V CC.</li> <li>• Una condición de cortocircuito con otro canal de salida activa.</li> </ul>	Verifique que el cableado esté operativo y esté correctamente conectado.

X indica que el estado del LED puede ser encendido o apagado.

1. Intermitente: 500 ms encendido/500 ms apagado.

2. Parpadeo: 50 ms encendido/50 ms apagado.

# Diagnósticos de salida de relé digital BMXSRA0405

## Introducción

En esta sección se describen las herramientas de diagnóstico disponibles para el módulo de salida de relé digital de seguridad BMXSRA0405.

## Diagnósticos de DDDT de BMXSRA0405

### Introducción

El módulo de relé de salida digital de seguridad BMXSRA0405 proporciona los diagnósticos siguientes mediante sus elementos DDT de dispositivo de `T_U_DIS_SIS_OUT_4`, página 128:

- Diagnósticos de contacto de salida
- Detección de error interno

### Diagnósticos de contacto de salida

En función del número de aplicación que se haya configurado para el módulo, este puede poner a prueba su capacidad de conmutar los estados de contacto de salida (de ENCENDIDO a APAGADO o de APAGADO a ENCENDIDO) durante un tiempo que no sea demasiado largo y evite la respuesta del actuador. Si los canales no se conmutan correctamente entre el estado energizado y deenergizado, el bit `CH_HEALTH` de la estructura de DDDT `T_U_DIS_SIS_CH_ROUT`, página 130 se establece en 0, lo que indica un estado no operativo.

**NOTA:** Los números de aplicación 2, 4, 6 y 8 realizan esta prueba de señal automática. Los números de aplicación 1, 3, 5 y 7 no lo hacen, por lo que es necesario hacer una transición manual diaria del estado del canal de salida para confirmar su operabilidad.

### Diagnósticos de comando de salida (detección de error interno)

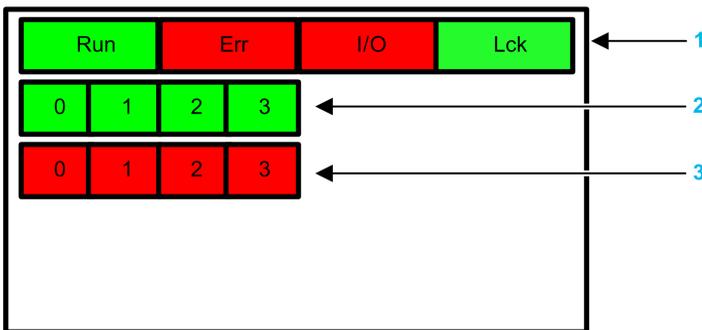
El comando de relé se procesa mediante dos circuitos paralelos e independientes. Se comparan los valores de los circuitos. Si los valores comparados son diferentes, se determina que el canal no está operativo y el bit `IC` de la estructura de DDDT `T_U_DIS_SIS_CH_ROUT` se establece en 1.

Consulte el diagrama de arquitectura, página 149 para el módulo de relé de salida digital de seguridad BMXSRA0405 a fin de obtener una presentación visual de este proceso.

## LED de diagnóstico de salida de relé digital BMXSRA0405

### Panel de LED

El módulo de salida de relé digital BMXSRA0405 presenta el panel de LED siguiente en la parte frontal:



1 Indicadores LED de estado del módulo

2 LED de estado del canal

3 LED de error detectado de canal

#### NOTA:

- Cuando se detecta un error de canal, el LED correspondiente se mantiene encendido hasta que se resuelve la condición subyacente.
- Puesto que el módulo de salida de relé tiene sólo cuatro canales, no se utilizan los LED en las posiciones 4 a 7 y nunca se encienden.

### Diagnóstico de módulos

Utilice los cuatro LED situados en la parte superior del panel de LED para diagnosticar la condición del módulo de salida de relé digital BMXSRA0405:

LED del módulo				Estado del módulo	Respuesta recomendada
Run	Err	I/O	LCK		
Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	Autopruueba al encender.	–
Intermitente <sup>1</sup>	ENCENDIDO	Intermitente <sup>1</sup>	Intermitente <sup>1</sup>	La autopruueba durante el encendido ha detectado un error interno en canales de salida.	–
Inactiva	ENCENDIDO	Inactiva	Inactiva	Error interno detectado.	Reemplace el módulo si la condición persiste.
OFF	Intermitente <sup>1</sup>	APAGADO	X	Módulo de E/S no configurado.	Configure el módulo a través de la CPU.
ENCENDIDO	Intermitente <sup>1</sup>	APAGADO	X	No hay comunicación entre la CPU y el módulo. El módulo se encuentra en estado de retorno.	Verifique que: <ul style="list-style-type: none"> <li>• La CPU es una CPU de seguridad de M580 y esté operativa.</li> <li>• La placa de conexiones esté operativa (si el módulo de E/S se encuentra en el bastidor principal).</li> <li>• El cable entre la CPU y el módulo de E/S esté operativo y esté correctamente conectado (si el módulo de E/S se encuentra en un bastidor ampliado o remoto).</li> </ul>
ENCENDIDO	Parpadeo <sup>2</sup>	Inactiva	Inactiva	No hay comunicación entre la CPU y el módulo. El módulo se encuentra en estado de retorno (o bien se está restableciendo si el módulo no ha funcionado nunca con normalidad).	Depure la condición mediante las variables de DDDT, página 127 para la instancia del módulo de E/S.
ENCENDIDO	Parpadeo <sup>2</sup>	Inactiva	ENCENDIDO	La comunicación no es segura y la configuración está bloqueada. El módulo se encuentra en estado de retorno (o bien se está restableciendo si el módulo no ha funcionado nunca con normalidad).	<ul style="list-style-type: none"> <li>• Verifique que la configuración bloqueada del módulo sea igual a la configuración del módulo almacenada en la aplicación de la CPU, tal como se ha configurado mediante Control Expert.</li> <li>• Depure la condición mediante las variables de DDDT, página 127 para la instancia del módulo de E/S.</li> </ul>
ENCENDIDO	ENCENDIDO	Inactiva	X	Error interno detectado en el canal de salida.	Reemplace el módulo si la condición persiste.

LED del módulo				Estado del módulo	Respuesta recomendada
Run	Err	I/O	LCK		
ENCENDIDO	Inactiva	Inactiva	Inactiva	La comunicación con la CPU es segura y la configuración está desbloqueada.	–
ENCENDIDO	Inactiva	Inactiva	ENCENDIDO	La comunicación con la CPU es segura y la configuración está bloqueada.	–

X indica que el estado del LED puede ser encendido o apagado.

- Intermitente: 500 ms encendido/500 ms apagado.
- Parpadeo: 50 ms encendido/50 ms apagado.

## Diagnóstico de canal

Use todos los LED en el módulo de salida de relé digital BMXSRA0405 para diagnosticar el estado del canal:

LED del módulo				Indicadores LED de canal		Estado del canal	Respuesta recomendada
Run	Err	I/O	LCK	Estado del canal (LED 0-3)	Error detectado (LED 0-3)		
ENCENDIDO	Inactiva	Inactiva	X	ENCENDIDO	Inactiva	El relé de salida está cerrado.	–
ENCENDIDO	Inactiva	Inactiva	X	Inactiva	Inactiva	El relé de salida está abierto.	–
ENCENDIDO	ENCENDIDO	Inactiva	X	Inactiva	ENCENDIDO	El relé de salida no está operativo.	Reemplace el módulo si la condición persiste.

X indica que el estado del LED puede ser encendido o apagado.

# Funcionamiento de un sistema de seguridad M580

## Contenido de este capítulo

Áreas de proceso, seguridad y datos globales en Control Expert.....	256
Modalidades de funcionamiento, estados de funcionamiento y tareas .....	261
Creación de un proyecto de seguridad de M580 .....	280
Bloqueo de configuraciones de módulos de E/S de seguridad de M580.....	288
Inicialización de datos en Control Expert.....	291
Utilización de tablas de animación en Control Expert.....	292
Adición de secciones de código .....	297
Gestión de la seguridad de las aplicaciones.....	308
Gestión de la seguridad de la estación de trabajo.....	333
Modificaciones en Control Expert para el sistema de seguridad M580.....	347

## Introducción

En este capítulo se ofrece información sobre cómo utilizar un sistema de seguridad M580.

# Áreas de proceso, seguridad y datos globales en Control Expert

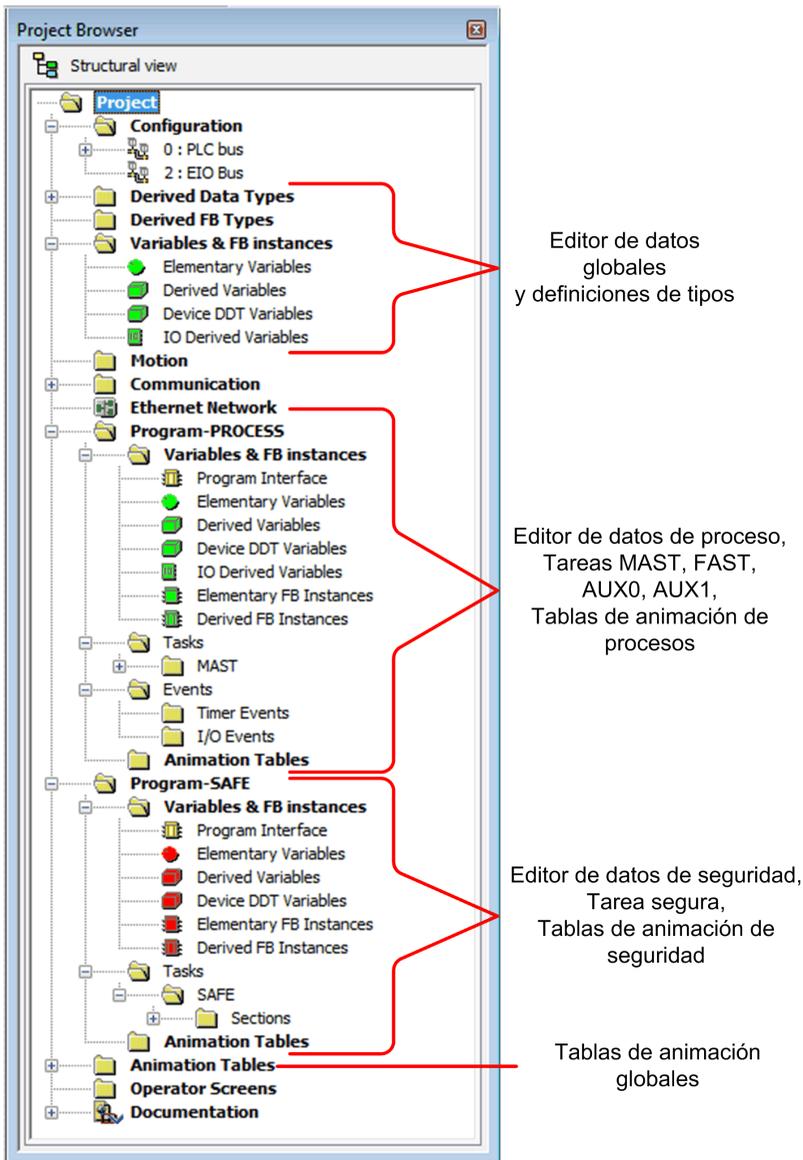
## Introducción

En esta sección se describe la separación de las áreas de datos en un proyecto de seguridad de M580 Control Expert.

## Separación de datos en Control Expert

### Áreas de datos en Control Expert

La **Vista estructural** del **Explorador de proyectos** muestra la separación de datos en Control Expert.. Tal como se muestra a continuación, cada área de datos tiene su propio editor de datos y su conjunto de tablas de animación:



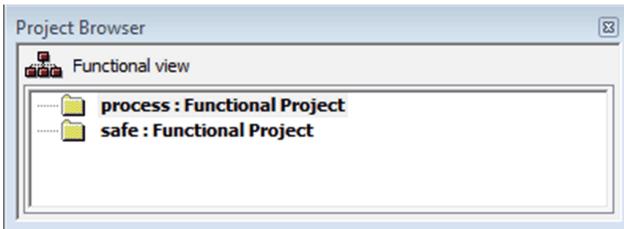
Si observa el **Explorador de proyectos**, verá que:

- El área segura contiene un Editor de datos seguros, lógica de seguridad e instancias de bloques de funciones utilizados por la tarea SAFE. No obstante, observe que:
  - Los eventos de E/S, los eventos de temporizador y las subrutinas no se admiten en un programa de seguridad.
  - La tarea SAFE no admite las variables IODDT, que no están incluidas en el área segura.
  - Los iconos rojos se utilizan para indicar las partes SAFE del programa.
- El área de proceso contiene un Editor de datos de proceso, lógica de proceso e instancias de bloques de funciones utilizados por las tareas no seguras (es decir, MAST, FAST, AUX0 y AUX1).
- El área global contiene un Editor de datos globales, datos derivados y tipos de bloques de funciones instanciados en los programas de proceso y de seguridad.

**NOTA:** El término *Datos globales* utilizado en este tema hace referencia al ámbito de toda la aplicación, o global, de los objetos de datos de un proyecto de seguridad. No hace referencia al servicio de datos globales compatible con muchos módulos Ethernet de Schneider Electric.

## Explorador de proyectos en la vista funcional

La **Vista funcional** del Control Expert. **Explorador de proyectos** para un sistema de seguridad M580 presenta dos proyectos funcionales: uno para el espacio de nombres de proceso y otro para el espacio de nombres seguro:



La gestión de cada proyecto funcional de un sistema de seguridad M580 es igual que la gestión de un proyecto en la vista funcional de un sistema M580 que no sea de seguridad, a excepción de las tablas de animación y las secciones de código.

### Efecto en la vista estructural:

Al añadir una sección de código o una tabla de animación a un proyecto funcional, se asocia al espacio de nombres asociado con dicho proyecto funcional. Al añadir una sección de código o una tabla de animación a:

- **Proceso: Proyecto funcional**, se añade al espacio de nombres de proceso del proyecto en la vista estructural.

- **Seguro: Proyecto funcional**, se añade al espacio de nombres seguro del proyecto en la vista estructural.

**Disponibilidad de selecciones de idioma y de tareas:**

Al crear una nueva sección de código para un proyecto funcional (seleccionando **Crear > Nueva sección**), las selecciones del **Idioma** y la **Tarea** disponibles dependen del proyecto funcional:

Al crear una nueva sección de código para un proyecto funcional (seleccionando **Crear > Nueva sección**), las selecciones del **Idioma** y la **Tarea** disponibles dependen del proyecto funcional asociado:

Proyecto funcional	Lenguajes y tareas disponibles	
	Lenguajes <sup>1</sup>	Tareas <sup>2</sup>
<b>Proceso: Proyecto funcional</b>	<ul style="list-style-type: none"> <li>• IL</li> <li>• FBD</li> <li>• LD</li> <li>• Segmento LL984</li> <li>• SFC</li> <li>• ST</li> </ul>	<ul style="list-style-type: none"> <li>• MAST</li> <li>• FAST</li> <li>• AUX0</li> <li>• AUX1</li> </ul>
<b>Seguro: Proyecto funcional</b>	<ul style="list-style-type: none"> <li>• FBD</li> <li>• LD</li> </ul>	<ul style="list-style-type: none"> <li>• SAFE</li> </ul>

1. Seleccionados en la ficha **General** del diálogo de la nueva sección.

2. Seleccionadas en la ficha **Localización** del diálogo de la nueva sección. La tarea MAST está disponible de forma predeterminada. Otras secciones están disponibles para la selección sólo después de que se hayan creado en el programa de proceso.

## Iconos con códigos de color

Para ayudarlo a distinguir entre las partes seguras y de proceso del proyecto, los iconos de color rojo se utilizan para identificar las partes seguras de su aplicación.

# Modalidades de funcionamiento, estados de funcionamiento y tareas

## Introducción

En esta sección se describen las modalidades de funcionamiento, los estados de funcionamiento y las tareas admitidas por el PAC de seguridad M580.

## Modalidades de funcionamiento del PAC de seguridad M580

### Dos modalidades de funcionamiento

El PAC de seguridad M580 ofrece dos modalidades de funcionamiento:

- Modalidad de seguridad: es la modalidad de funcionamiento predeterminada para las operaciones de seguridad.
- Modalidad de mantenimiento: es una modalidad de funcionamiento opcional en la que se puede entrar temporalmente para depurar y modificar el programa de aplicación o cambiar la configuración.

El software Control Expert Safety es la herramienta exclusiva que puede utilizar para gestionar el paso de una modalidad de funcionamiento a otra.

**NOTA:** El ajuste de modalidad de funcionamiento de un PAC de seguridad Hot Standby, ya sea en la modalidad de seguridad o de mantenimiento, no se incluye en la transferencia de una aplicación del PAC primario al PAC standby. En una conmutación, cuando el PAC de seguridad cambia del PAC standby al PAC primario, la modalidad de funcionamiento se establece automáticamente en la modalidad de seguridad.

### La modalidad de seguridad y sus limitaciones

La modalidad de seguridad es la modalidad predeterminada del PAC de seguridad. Cuando el PAC de seguridad está encendido con una aplicación válida presente, el PAC entra en la modalidad de seguridad. La modalidad de seguridad se utiliza para controlar la ejecución de la función de seguridad. Se puede cargar, descargar, ejecutar y detener el proyecto en modalidad de seguridad.

Cuando el PAC de seguridad M580 funciona en modalidad de seguridad, las siguientes funciones **no** están disponibles:

- Descarga de una configuración modificada de Control Expert al PAC.

- Edición o forzado de valores de variables de seguridad y estados de E/S de seguridad.
- Depuración de lógica de aplicaciones, por medio de puntos de interrupción, puntos de observación y ejecución de código paso a paso.
- Uso de tablas de animación o peticiones UMAS (por ejemplo, desde una HMI) para escribir en variables de seguridad y E/S de seguridad.
- Cambio de los ajustes de configuración de los módulos de seguridad a través de CCOTF. (Tenga en cuenta que se admite el uso de CCOTF para módulos no interferentes).
- Realización de la modificación online de la aplicación de seguridad.
- Uso de animación de conexiones.

**NOTA:** En la modalidad de seguridad, todas las variables de seguridad y los estados de E/S de seguridad son de sólo lectura. No se puede editar directamente el valor de una variable de seguridad.

Puede crear una variable global y utilizarla para pasar un valor entre una variable de proceso vinculada (no segura) y una variable de seguridad vinculada utilizando las fichas de la interfaz del Editor de datos de proceso y el Editor de datos de seguridad. Después de realizar el enlace, la transferencia se ejecuta del modo siguiente:

- Al principio de cada tarea SAFE, los valores de las variables no seguras se copian en las variables seguras.
- Al final de la tarea SAFE, los valores de las variables de salida seguras se copian en las variables no seguras.

## Modalidad de funcionamiento de mantenimiento

La modalidad de mantenimiento es comparable a la modalidad normal de una CPU de M580 de seguridad. Sólo se utiliza para depurar y ajustar la tarea SAFE de la aplicación. La modalidad de mantenimiento es temporal porque el PAC de seguridad entra automáticamente en la modalidad de seguridad si la comunicación entre Control Expert y el PAC se pierde, o al ejecutarse un comando de desconexión. En la modalidad de mantenimiento, las personas con permisos apropiados pueden leer y escribir en variables de seguridad y E/S de seguridad que se hayan configurado para aceptar ediciones.

En modalidad de mantenimiento, se lleva a cabo la ejecución dual de código de tarea SAFE, pero los resultados no se comparan.

Cuando el PAC de seguridad M580 funciona en modalidad de mantenimiento, están disponibles las siguientes funciones:

- Descarga de una configuración modificada de Control Expert al PAC.
- Edición o forzado de valores de variables de seguridad y estados de E/S de seguridad.
- Depuración de lógica de aplicaciones, por medio de puntos de interrupción, puntos de observación y ejecución de código paso a paso.

- Uso de tablas de animación o peticiones UMAS (por ejemplo, desde una HMI) para escribir en variables de seguridad y E/S de seguridad.
- Modificación de la configuración por medio de CCOTF.
- Realización de la modificación online de la aplicación de seguridad.
- Uso de animación de conexiones.

En la modalidad de mantenimiento, no se garantiza el nivel SIL del PLC de seguridad.

## **▲ ADVERTENCIA**

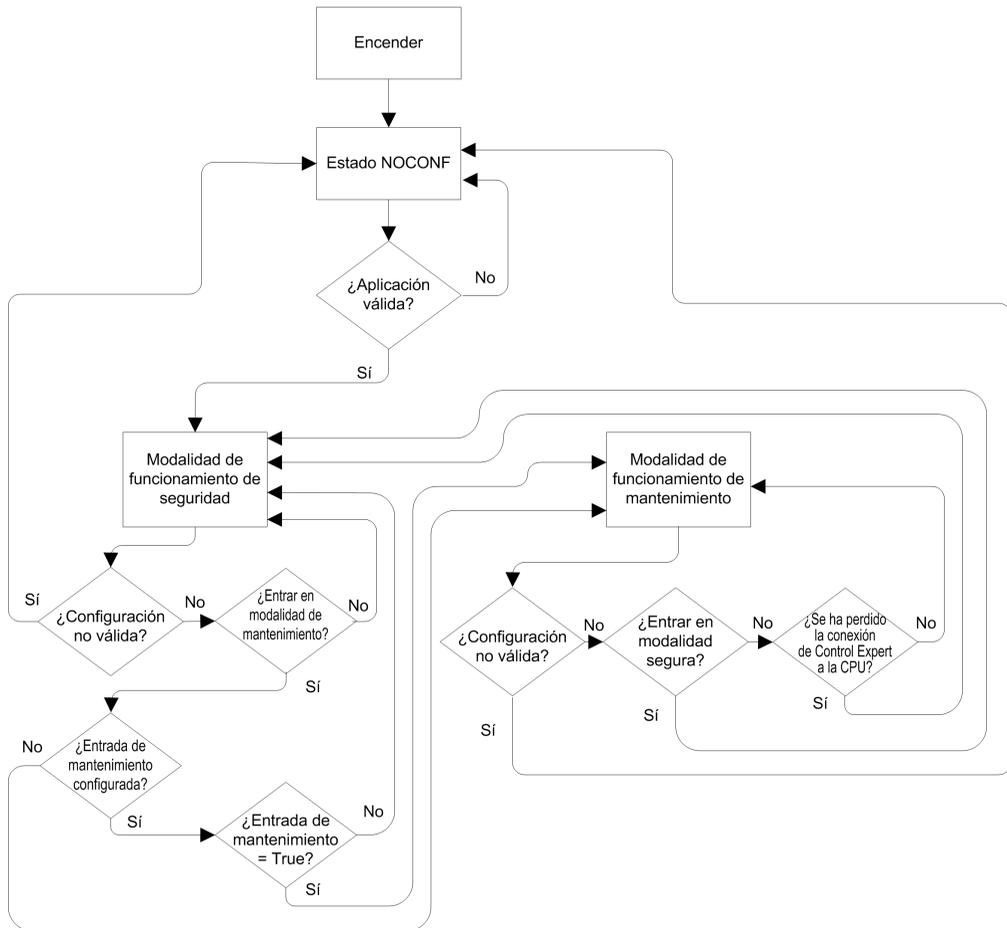
### **PÉRDIDA DEL NIVEL DE INTEGRIDAD DE SEGURIDAD**

Mientras el PAC de seguridad está en la modalidad de mantenimiento, debe tomar las medidas adecuadas para garantizar el estado de seguridad del sistema.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## Transiciones de modalidad de funcionamiento

El diagrama siguiente muestra cómo el PAC de seguridad M580 entra y luego cambia entre la modalidad de seguridad y la de mantenimiento:



Al cambiar entre la modalidad de seguridad y la de mantenimiento:

- Es correcto pasar de la modalidad de mantenimiento a la de seguridad con el forzado activado. En este caso, el valor de la variable forzada o el estado de E/S permanecen forzados tras la transición hasta que se produce otra transición de la modalidad de seguridad a la de mantenimiento.

- La transición de la modalidad de mantenimiento a la modalidad de seguridad se puede llevar a cabo de las siguientes maneras:
  - Manualmente, a través del comando del menú o de la barra de herramientas en Control Expert.
  - Automáticamente, con el PAC de seguridad, cuando la comunicación entre Control Expert y el PAC se pierde durante unos 50 segundos.
- La función de entrada de mantenimiento, cuando está configurada, funciona como una comprobación de la transición de la modalidad de seguridad a la modalidad de mantenimiento. La función de entrada de mantenimiento se configura en Control Expert en la ficha **Configuración** de la CPU de la siguiente manera:
  - Seleccionando el ajuste **Entrada de mantenimiento** y
  - Introduciendo la dirección topológica de un bit de entrada (%I) para un módulo de entrada digital no interferente en el bastidor local.

Cuando se configura la entrada de mantenimiento, la transición de la modalidad de seguridad a la mantenimiento tiene en cuenta el estado del bit de entrada designado (%I). Si el bit se establece en 0 (falso), el PAC se bloquea en modalidad de seguridad. Si el bit se establece en 1 (verdadero), puede producirse una transición a la modalidad de mantenimiento.

## Cambio entre la modalidad de seguridad y la de mantenimiento en Control Expert

El cambio del PAC de seguridad entre la modalidad de mantenimiento y la de seguridad no es posible si:

- El PAC está en modalidad de depuración.
- Hay un punto de interrupción activado en una sección de una tarea SAFE.
- Hay un punto de observación establecido en una sección de una tarea SAFE.

Cuando la modalidad de depuración no está activa, no hay ningún punto de interrupción de tarea SAFE activado y no hay ningún punto de observación de tarea SAFE establecido, se puede activar manualmente una transición entre la modalidad de seguridad y la de mantenimiento de la manera siguiente:

- Para cambiar de la modalidad de seguridad a la mantenimiento:
  - Seleccione **PLC > Mantenimiento**, o bien
  - Haga clic en el botón  de la barra de herramientas.

- Para cambiar de la modalidad de mantenimiento a la de seguridad:
  - Seleccione **PLC > Seguridad**, o bien



- Haga clic en el botón de la barra de herramientas.

**NOTA:** Los eventos de entrada y salida de la modalidad de seguridad se registran en el servidor SYSLOG en la CPU.

## Determinación de la modalidad de funcionamiento

Puede determinar la modalidad de funcionamiento actual de un PAC de seguridad M580 utilizando los LED **SMOD** de la CPU y el coprocesador, o Control Expert.

Cuando los LED **SMOD** de la CPU y el coprocesador están encendidos:

- *Intermitentes*, el PAC está en modalidad de mantenimiento.
- *Fijos*, el PAC está en modalidad de seguridad.

Cuando Control Expert se conecta al PAC, identifica la modalidad de funcionamiento del PAC de seguridad M580 en varios puntos:

- Las palabras del sistema %SW12 (coprocesador) y %SW13 (CPU), página 408 conjuntamente indican la modalidad de funcionamiento del PAC, tal como se indica a continuación:
  - Si la palabra %SW12 está establecida en 16#A501 (hex) y la palabra %SW13 está establecida en 16#501A (hex), el PAC está en modalidad de mantenimiento.
  - Si cualquiera de estas palabras del sistema, o las dos, está establecida en 16#5AFE (hex), el PAC está en modalidad de seguridad.
- Tanto la subficha **Tarea** como la subficha **Información** de la ficha **Animación** de la CPU muestran la modalidad de funcionamiento del PAC.
- La barra de tareas, en la parte inferior de la ventana principal de Control Expert, indica la modalidad de funcionamiento como MANTENIMIENTO o SEGURIDAD.

## Estados de funcionamiento del PAC de seguridad M580

### Estados de funcionamiento

Los estados de funcionamiento del PAC de seguridad M580 se describen a continuación.

**NOTA:** Para ver una descripción de la relación entre los estados de funcionamiento del PAC de seguridad M580 y los estados de funcionamiento del PAC Hot Standby M580, consulte el documento *Modicon M580 Hot Standby, Guía de planificación del sistema para arquitecturas utilizadas con más frecuencia* y los temas *Estados del sistema Hot Standby y Asignaciones y transiciones de estado de Hot Standby*.

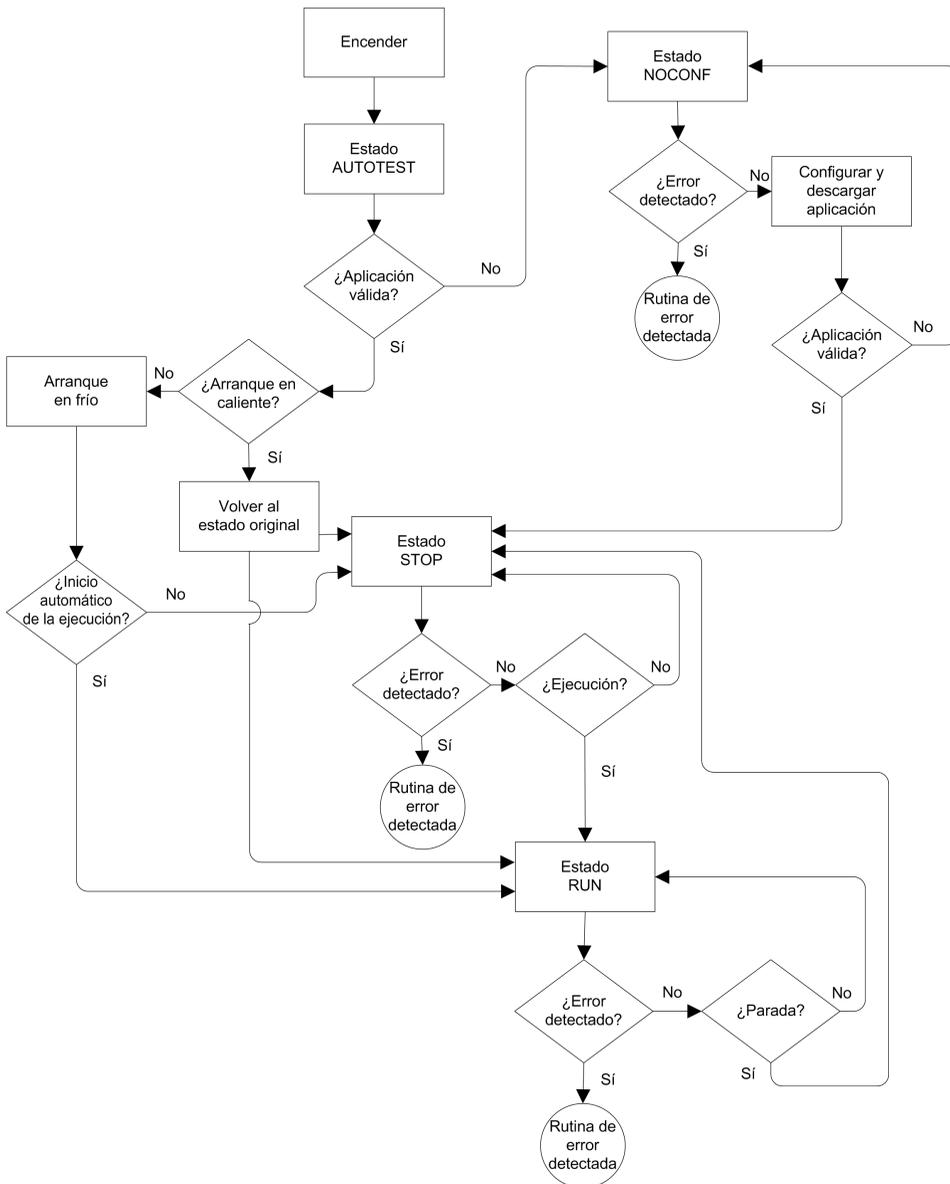
Estado de funcionamiento	Válido para...	Descripción
AUTOTEST	PAC	<p>La CPU está ejecutando autoverificaciones internas.</p> <p><b>NOTA:</b> Si hay bastidores de ampliación conectados al bastidor local y no están conectados los finales de línea en los conectores no utilizados del módulo de ampliación del bastidor, la CPU permanece en AUTOTEST después de que se haya completado la autoverificación.</p>
NOCONF	PAC	El programa de aplicación no es válido.
STOP	PAC o Tarea	<p>El PAC tiene una aplicación válida y no se ha detectado ningún error, pero el funcionamiento se ha detenido porque:</p> <ul style="list-style-type: none"> <li>Al arrancar la opción <b>Inicio automático de la ejecución</b> no está establecida (modalidad de seguridad, página 261).</li> <li>La ejecución se ha detenido mediante la ejecución de un comando de detención (modalidad segura, página 261 o de mantenimiento, página 262).</li> <li>Se han establecido puntos de interrupción en la modalidad de mantenimiento y luego se ha perdido la conexión entre Control Expert y la CPU durante más de 50 segundos.</li> </ul> <p>La CPU lee las entradas asociadas con cada tarea, pero no actualiza las salidas, que entran en estado de recuperación. La CPU se puede reiniciar cuando esté listo.</p> <p><b>NOTA:</b> Al emitir un comando de detención en Control Expert se detienen todas las tareas. El evento de detención se registra en el servidor SYSLOG de la CPU.</p>
HALT	Tarea	<p>El PAC de seguridad M580 presenta dos estados HALT (pausa) independientes:</p> <ul style="list-style-type: none"> <li>La pausa de proceso se aplica a las tareas no seguras (MAST, FAST, AUX0 y AUX1). Cuando cualquier tarea de proceso entra en el estado HALT, todas las demás tareas de proceso también entran en el estado HALT. El estado HALT de proceso no afecta a la tarea SAFE.</li> <li>El SAFE HALT sólo se aplica a la tarea SAFE. El estado SAFE HALT no afecta a las tareas de proceso.</li> </ul> <p>En cada caso, las operaciones de las tareas se paran porque se ha detectado una condición de bloqueo imprevista, lo que ha producido una condición recuperable, página 222.</p> <p>La CPU lee las entradas asociadas con cada tarea en pausa, pero no actualiza las salidas, que están en estado de recuperación.</p>
RUN	PAC o Tarea	Con una aplicación válida y ningún error detectado, la CPU lee las entradas asociadas con cada tarea, ejecuta el código asociado con cada tarea y actualiza las salidas asociadas.

Estado de funcionamiento	Válido para...	Descripción
		<ul style="list-style-type: none"> <li>• en la modalidad de seguridad, página 261: se lleva a cabo la función de seguridad y se aplican todas las limitaciones.</li> <li>• en la modalidad de mantenimiento, página 262: el PAC funciona como cualquier CPU que no sea de seguridad. Se lleva a cabo la ejecución dual de código de tarea SAFE, pero los resultados no se comparan.</li> </ul> <p><b>NOTA:</b> Al emitir un comando de ejecución en Control Expert se inician todas las tareas. El evento de ejecución se registra en el servidor SYSLOG de la CPU.</p>
WAIT	PAC	<p>La CPU está en un estado transitorio mientras hace la copia de seguridad de sus datos cuando se detecta una condición de desconexión. La CPU se inicia de nuevo sólo cuando se restablece la alimentación y se carga la reserva de suministro.</p> <p>Puesto que el estado de espera es transitorio, puede que no resulte visible. La CPU realiza un reinicio en caliente, página 275 para salir del estado WAIT.</p>
ERROR	PAC	<p>La CPU se detiene porque se ha detectado un error de hardware o de sistema no recuperable, página 219. El estado de error activa la función de seguridad, página 16.</p> <p>Cuando el sistema está listo para reiniciarse, realice un arranque en frío, página 275 de la CPU para salir del estado de error, ya sea realizando un ciclo de apagado y encendido o realizando un reset.</p>
Descarga del SO	PAC	Se está realizando una descarga del firmware de la CPU o del coprocesador.

Consulte los temas *Diagnóstico mediante los LED de la CPU de M580*, página 224 y *Diagnóstico mediante los LED del coprocesador de M580*, página 224 para obtener información sobre los estados de funcionamiento del PAC.

## Transiciones entre los estados de funcionamiento

A continuación se describen las transiciones entre los distintos estados de un PAC de seguridad M580:



Consulte el tema *Procesamiento de errores detectados*, página 270 para obtener información sobre cómo trata los errores detectados el sistema de seguridad.

## Procesamiento de errores detectados

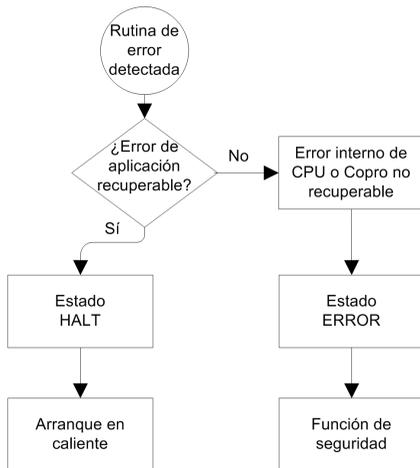
El PAC de seguridad M580 trata los siguientes tipos de errores detectados de la CPU:

- Errores detectados de aplicación recuperables: Estos eventos provocan la entrada de las tareas relacionadas en estado HALT.

**NOTA:** Puesto que las tareas MAST, FAST y AUX funcionan en la misma área de memoria, un evento que provoca la entrada de una de estas tareas en el estado HALT también provoca la entrada de las demás tareas no seguras en el estado HALT. Puesto que la tarea SAFE funciona en un área de memoria distinta, las tareas no seguras no se ven afectadas si la tarea SAFE entra en el estado HALT.

- Errores detectados de aplicación no recuperables: Errores detectados internos de la CPU o el coprocesador: Estos eventos provocan la entrada del PAC en el estado ERROR. La función de seguridad se aplica a la parte afectada del bucle de seguridad.

A continuación se describe la lógica del proceso de tratamiento de errores detectados:



A continuación se describe el impacto de los errores detectados sobre las tareas individuales:

Tipo de error detectado	Estado de tarea			
	FAST	SAFE	MAST	AUX
Desborde del watchdog de la tarea FAST	HALT	RUN <sup>1</sup>	HALT	HALT
Desborde del watchdog de la tarea SAFE	RUN	HALT <sup>2</sup>	RUN	RUN

Tipo de error detectado	Estado de tarea			
	FAST	SAFE	MAST	AUX
Desborde del watchdog de la tarea MAST	HALT	RUN	HALT	HALT
Desborde del watchdog de la tarea AUX	HALT	RUN	HALT	HALT
Error detectado de ejecución de código dual de la CPU	RUN	HALT <sup>2</sup>	RUN	RUN
Desborde el watchdog de seguridad <sup>3</sup>	ERROR	ERROR <sup>2</sup>	ERROR	ERROR
Error interno de CPU detectado	ERROR	ERROR <sup>2</sup>	ERROR	ERROR
<p>1. Puesto que la tarea FAST tiene una prioridad superior a la de la tarea SAFE, el retardo de la tarea FAST puede provocar la entrada de la tarea SAFE en el estado HALT o ERROR en lugar del estado RUN.</p> <p>2. Los estados de ERROR o HALT de la tarea SAFE provocan el establecimiento de las salidas seguras al estado configurable por el usuario (recuperación o mantenimiento).</p> <p>3. El watchdog de seguridad se establece igual a 1,5 veces el watchdog de la tarea SAFE.</p>				

## Visor de estado de seguridad de la barra de tareas

Cuando Control Expert se conecta al PAC de seguridad M580, la barra de tareas incluye un campo que describe los estados de funcionamiento combinados de la tarea SAFE y las tareas de proceso (MAST, FAST, AUX0, AUX1), tal como se indica a continuación:

Estado de las tareas de proceso	Estado de la tarea SAFE	Mensaje
STOP (todas las tareas de proceso en estado STOP)	STOP	STOP
STOP (todas las tareas de proceso en estado STOP)	RUN	RUN
STOP (todas las tareas de proceso en estado STOP)	HALT	SAFE HALT
RUN (al menos una tarea de proceso en estado RUN)	STOP	RUN
RUN (al menos una tarea de proceso en estado RUN)	RUN	RUN
RUN (al menos una tarea de proceso en estado RUN)	HALT	SAFE HALT
HALT	STOP	PROC HALT
HALT	RUN	PROC HALT
HALT	HALT	HALT

# Secuencias de arranque

## Introducción

El PAC de seguridad M580 puede entrar en la secuencia de arranque en las circunstancias siguientes:

- En la conexión inicial.
- En respuesta a una interrupción de la alimentación.

Según el tipo de tarea y el contexto de la interrupción de la alimentación, el PAC de seguridad M580 puede realizar un **arranque en frío**, página 275 o un **arranque en caliente**, página 275 cuando se reanuda la alimentación.

## Arranque inicial

En el arranque inicial, el PAC de seguridad M580 realiza un arranque en frío. Todas las tareas, incluidas la tarea SAFE y todas las tareas no seguras (MAST, FAST, AUX0, AUX1), entran en el estado STOP a menos que se haya habilitado la opción **Inicio automático de la ejecución**, en cuyo caso todas las tareas entran en el estado RUN.

## Arranque tras una interrupción de la alimentación

La fuente de alimentación de seguridad de M580 proporciona una reserva de alimentación que sigue suministrando alimentación a todos los módulos del bastidor hasta 10 ms en caso de una interrupción de la alimentación. Cuando la reserva de alimentación se agota, el PAC de seguridad M580 realiza un ciclo de apagado y encendido completo.

Antes de apagar el sistema, la CPU de seguridad almacena los siguientes datos, que definen el contexto de funcionamiento al apagar el sistema:

- Fecha y hora del apagado (se almacenan en %SW54-%SW58).
- Estado de cada tarea.
- Estado de los temporizadores de eventos.
- Valores de los contadores en funcionamiento.
- Firma de la aplicación.
- Datos de la aplicación (valores actuales de las variables de aplicación)
- Suma de comprobación de la aplicación.

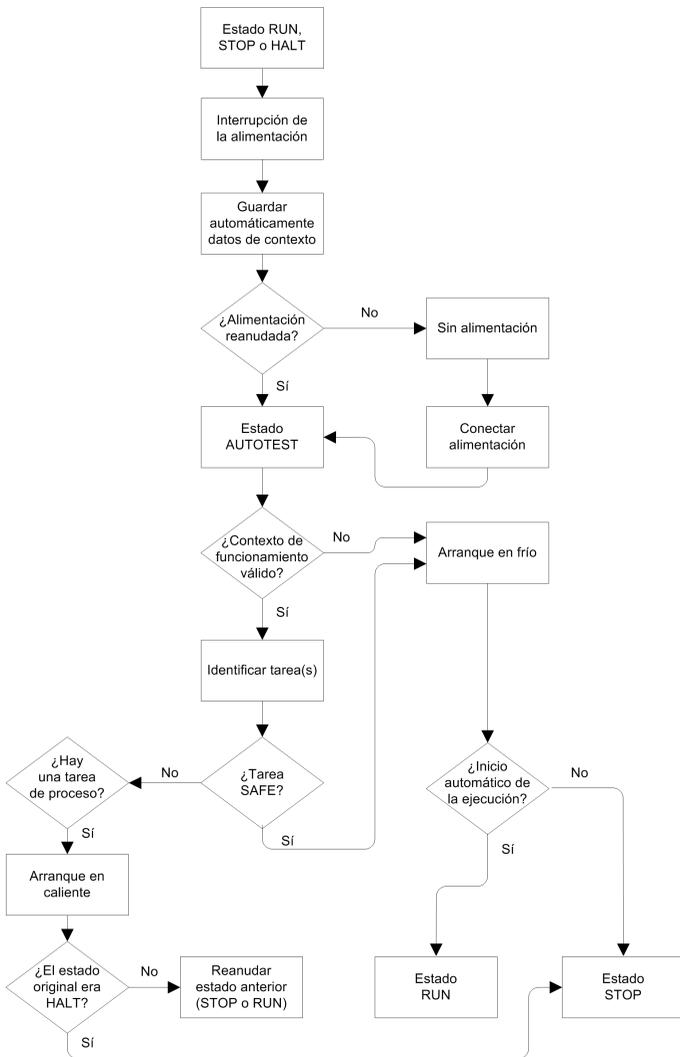
Tras el apagado, el arranque puede ser automático (si la alimentación se ha reanudado antes de que finalizase el apagado) o manual (en caso contrario).

A continuación, el PAC de seguridad M580 realiza autoverificaciones y comprueba la validez de los datos del contexto de funcionamiento guardados durante el apagado, tal como se indica a continuación:

- Se verifica la suma de comprobación.
- Se lee la tarjeta de memoria SD para confirmar que contiene una aplicación válida.
- Si la aplicación de la tarjeta de memoria SD es válida, se comprueban las firmas para confirmar que sean idénticas.
- Se verifica la firma de la aplicación guardada comparándola con la firma de la aplicación almacenada.

Si el contexto de funcionamiento es válido, las tareas no seguras realizan un arranque en caliente. Si el contexto de funcionamiento no es válido, las tareas no seguras realizan un arranque en frío. En cualquiera de los dos casos, la tarea SAFE realiza un arranque en frío.

A continuación se presenta esta secuencia de arranque tras una interrupción de la alimentación:



## Arranque en frío

Un arranque en frío hace que todas las tareas, incluidas las tareas SAFE y las no seguras (MAST, FAST, AUX0, AUX1), entren en el estado STOP, a menos que se haya habilitado la opción **Inicio automático de la ejecución**, en cuyo caso todas las tareas entran en el estado RUN.

Un arranque en frío realiza las operaciones siguientes:

- A los datos de aplicación (incluidos los bits internos, datos de E/S, palabras internas, etc.) se les asignan los valores iniciales definidos por la aplicación.
- Las funciones elementales se establecen en sus valores iniciales.
- Los bloques de función elementales y sus variables se establecen en sus valores predeterminados.
- Los bits y las palabras del sistema se establecen en sus valores predeterminados.
- Inicializa todas las variables forzadas aplicando sus valores predeterminados (inicializados).

Un arranque en frío puede ejecutarse para datos, variables y funciones en el espacio de nombres de proceso seleccionando **PLC > Inic.** en *Control Expert*, página 291 o estableciendo el bit de sistema %S0 (COLDSTART) en 1. El bit de sistema %S0 no tiene ningún efecto en los datos y las funciones pertenecientes al espacio de nombres seguro.

**NOTA:** Tras un arranque en frío, la tarea SAFE no se puede iniciar hasta que se ha iniciado la tarea MAST.

## Arranque en caliente

Un arranque en caliente provoca que todas las tareas de proceso (MAST, FAST, AUX0, AUX1) vuelvan a entrar en su estado de funcionamiento a partir de la interrupción de la alimentación. Por el contrario, un arranque en caliente hace que la tarea SAFE entre en el estado STOP, a menos que se seleccione **Inicio automático de la ejecución**.

**NOTA:** Si una tarea estaba en el estado HALT o en un punto de interrupción en el momento de la interrupción de la alimentación, esa tarea entra en el estado STOP tras el arranque en caliente.

Un arranque en caliente realiza las operaciones siguientes:

- Restaura en las variables del espacio de nombres de proceso el último valor conservado.
- Inicializa todas las variables del espacio de nombres seguro aplicando sus valores predeterminados (inicializados).
- Inicializa todas las variables forzadas aplicando sus valores predeterminados (inicializados).
- Restaura en las variables de aplicación el último valor conservado.

- Establece %S1 (WARMSTART) en 1.
- Las conexiones entre el PAC y la CPU se restablecen.
- Los módulos de E/S se reconfiguran (si es necesario) utilizando sus ajustes almacenados.
- Los eventos, la tarea FAST y las tareas AUX se deshabilitan.
- La tarea MAST se reinicia desde el inicio del ciclo.
- %S1 se establece en 0 al concluir la primera ejecución de la tarea MAST.
- Los eventos, la tarea FAST y las tareas AUX se habilitan.

Si una tarea se estaba ejecutando en el momento de la interrupción de la alimentación, tras el arranque en caliente se reanuda la ejecución al principio de la tarea.

## ▲ ADVERTENCIA

### FUNCIONAMIENTO IMPREVISTO DEL EQUIPO

Es responsabilidad del usuario confirmar que la selección de **Inicio automático de la ejecución** es compatible con el comportamiento correcto de su sistema. En caso contrario, debe desactivar esta función.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

## Tareas del PAC de seguridad M580

### Introducción

Un PAC de seguridad M580 puede ejecutar aplicaciones monotarea y multitarea. A diferencia de una aplicación monotarea, que sólo ejecuta la tarea MAST, una aplicación multitarea define la prioridad de cada tarea.

El PAC de seguridad M580 admite las siguientes tareas:

- FAST
- SAFE
- MAST
- AUX0
- AUX1

## Características de las tareas

Las tareas admitidas por el PAC de seguridad M580 tienen las siguientes características de tarea:

Nombre de tarea	Prioridad	Modelo de tiempo	Rango de periodo	Periodo predeterminado	Rango de watchdog	Watchdog predeterminado
FAST	1	Periódica	De 1 a 255 ms	5 ms	10-500 ms <sup>2</sup>	100 ms <sup>2</sup>
SAFE	2	Periódica	10-255 ms	20 ms	10-500 ms <sup>2</sup>	250 ms <sup>2</sup>
MAST <sup>1</sup>	3	Cíclico <sup>4</sup> o periódico	De 1 a 255 ms	20 ms	10-1500 ms <sup>2</sup>	250 ms <sup>2</sup>
AUX0 <sup>3</sup>	4	Periódica	10-2550 ms	100 ms	100-5000 ms <sup>2</sup>	2000 ms <sup>2</sup>
AUX1 <sup>3</sup>	5	Periódica	10-2550 ms	200 ms	100-5000 ms <sup>2</sup>	2000 ms <sup>2</sup>

1. La tarea MAST es necesaria y no se puede desactivar.

2. Si se habilita CCOTF (seleccionando **Modificación online en RUN o STOP** en la ficha **Configuración** del diálogo de propiedades de la CPU), el ajuste de **Watchdog** mínimo es de 64 ms.

3. Es compatible con los PAC de seguridad BMEP58•040S autónomos. No compatible con los PAC Hot Standby de seguridad BMEH58•040S.

4. Los PAC de seguridad BMEP58•040S autónomos son compatibles con los modelos de tiempo cíclicos y periódicos. Los PAC Hot Standby de seguridad BMEH58•040S sólo son compatibles con el modelo de tiempo periódico.

## Prioridad de la tarea

Los PAC de seguridad M580 ejecutan las tareas pendientes en función de su prioridad. Cuando una tarea se está ejecutando, una tarea con una prioridad relativa superior puede interrumpirla. Por ejemplo, cuando una tarea periódica está programada para ejecutar su código, interrumpiría una tarea de prioridad inferior, pero esperaría a que finalizase una tarea de prioridad superior.

## Consideraciones sobre la configuración de las tareas

Todas las tareas no seguras (MAST, FAST, AUX0 y AUX1) funcionan en la misma área de memoria, mientras que la tarea SAFE funciona en su propia área de memoria independiente. Como resultado:

- Si una tarea no segura supera su valor de watchdog, todas las tareas no seguras entran en estado HALT, mientras que la tarea SAFE sigue en funcionamiento.
- Si la tarea SAFE supera su valor de watchdog, sólo la tarea SAFE entra en estado HALT, mientras que las tareas no seguras siguen en funcionamiento.

Al crear y configurar tareas para su aplicación, tenga en cuenta las siguientes características de las tareas:

**Tarea SAFE:**

Diseñe esta tarea periódica para ejecutar sólo secciones de código relacionadas con la seguridad para módulos de E/S de seguridad. Puesto que la tarea SAFE tiene asignada una prioridad inferior que la tarea FAST, la tarea FAST puede interrumpir la ejecución de la tarea SAFE.

Defina el tiempo de ejecución máximo para la tarea SAFE ajustando el valor de watchdog apropiado. Tenga en cuenta el tiempo necesario para ejecutar código y para leer y escribir datos seguros. Si el tiempo para ejecutar la tarea SAFE supera el ajuste de watchdog, la tarea SAFE entra en el estado HALT y la palabra del sistema %SW125 muestra el código de error detectado 16#DEB0.

**NOTA:**

- Puesto que la tarea FAST tiene una prioridad superior que la tarea SAFE, es recomendable incluir un componente para el tiempo de retardo de la tarea FAST en el ajuste de watchdog de la tarea SAFE.
- Si el desborde de la ejecución de la tarea SAFE es igual al "Watchdog de seguridad" (que es un valor igual a una vez y media el ajuste de watchdog de la tarea SAFE), la CPU y el coprocesador entrarán en estado de ERROR y se aplicará la función de seguridad.

**Tarea MAST:**

Esta tarea se puede configurar como cíclica o periódica. Cuando funcione en modalidad cíclica, defina un tiempo de ejecución máximo introduciendo un valor de watchdog de MAST apropiado. Sume un pequeño intervalo de tiempo a este valor al final de cada ciclo para permitir la ejecución de otras tareas del sistema de prioridad inferior. Puesto que las tareas AUX tienen menos prioridad que MAST, si no se proporciona este intervalo de tiempo, es posible que las tareas AUX nunca se ejecuten. Plantéese sumar un intervalo de tiempo igual al 10 % del tiempo de ejecución del ciclo, con un mínimo de 1 ms y un máximo de 10 ms.

Si el tiempo para la ejecución de una tarea MAST cíclica supera el ajuste de watchdog, la tarea MAST y todas las demás tareas que no son SAFE entran en el estado HALT, y la palabra del sistema %SW125 muestra el código de error detectado 16#DEB0.

Durante el funcionamiento en modalidad periódica, es posible que la tarea MAST supere este periodo. En ese caso, la tarea MAST se ejecuta en modalidad cíclica y se establece el bit del sistema %S11.

**Tarea FAST:**

La finalidad de esta tarea periódica es ejecutar una parte de alta prioridad de la aplicación. Defina un tiempo de ejecución máximo estableciendo el valor de watchdog de FAST. Puesto que la tarea FAST interrumpe la ejecución de todas las demás tareas, incluida la tarea SAFE, se recomienda configurar el tiempo de ejecución de la tarea FAST lo más breve

posible. Se recomienda un valor de watchdog de la tarea FAST no muy superior al periodo de FAST.

Si el tiempo para la ejecución de una tarea FAST supera el ajuste de watchdog, la tarea FAST y todas las demás tareas que no son SAFE entran en el estado HALT, y la palabra del sistema %SW125 muestra el código de error detectado 16#DEB0.

**Tareas AUX:**

AUX0 y AUX1 son tareas periódicas opcionales. Su finalidad es ejecutar es una parte de baja prioridad de la aplicación. Las tareas AUX se ejecutan sólo después de que haya finalizado la ejecución de las tareas MAST, SAFE y FAST.

Defina un tiempo de ejecución máximo para las tareas AUX ajustando el valor de watchdog apropiado. Si el tiempo para la ejecución de una tarea AUX supera el ajuste de watchdog, la tarea AUX y todas las demás tareas que no son SAFE entran en el estado HALT, y la palabra del sistema %SW125 muestra el código de error detectado 16#DEB0.

# Creación de un proyecto de seguridad de M580

## Creación de un proyecto de seguridad de M580

### Creación de un proyecto de seguridad de M580

El menú **Generar** de Control Expert para la seguridad presenta tres comandos de generación diferentes, además de un comando de firma de seguridad. Son los siguientes:

Comando	Descripción
<b>Generar cambios</b>	Compila sólo los cambios que se han realizado en el programa de aplicación desde el comando de generación anterior, y los añade al programa de aplicación generado anteriormente.
<b>Regenerar todo el proyecto</b>	Recompila todo el programa de aplicación, sustituyendo la generación anterior del programa de aplicación.  <b>NOTA:</b> Para los módulos de E/S de seguridad M580, este comando no genera un valor nuevo de identificador unívoco del módulo (MUID). En su lugar, se conserva el valor de MUID generado anteriormente.
<b>Renovar ID y Regenerar todo</b>	Recompila todo el programa de aplicación, sustituyendo la generación anterior del programa de aplicación.  <b>NOTA:</b> <ul style="list-style-type: none"> <li>Ejecute este comando sólo cuando los módulos de E/S de seguridad estén desbloqueados, página 288.</li> <li>Para los módulos de E/S de seguridad M580, este comando genera un valor nuevo de identificador unívoco de módulo (MUID) y sustituye el valor de MUID anterior por el nuevo valor.</li> </ul>
<b>Actualizar firma SAFE</b>	Utilice esta opción para generar manualmente un valor de firma de origen SAFE, página 280 para la aplicación segura.  <b>NOTA:</b> Este comando solo se habilita cuando el parámetro <b>General &gt; Ajustes de generación &gt; Gestión de firmas SAFE</b> está ajustado en <b>A petición del usuario</b> .

## Firma de seguridad

### Introducción

Los PAC de seguridad M580 (tanto autónomos como Hot Standby) incluyen un mecanismo de generación de huellas dactilares algorítmicas SHA256 de la aplicación segura: la firma de origen SAFE. Al transferir la aplicación del PC al PAC, Control Expert compara la firma de origen SAFE del PC con la firma de origen SAFE del PAC para determinar si la aplicación de seguridad del PC es la misma que la del PAC, o bien si es distinta.

La función de firma de seguridad es opcional. El proceso de generación de una firma de origen SAFE puede tomar bastante tiempo, en función del tamaño de la aplicación de seguridad. Mediante las opciones de gestión de firmas de seguridad, puede generar un valor de firma de origen SAFE que cree un valor algorítmico para la aplicación segura en los siguientes casos:

- en cada generación,
- solo cuando desee generar manualmente una firma de origen SAFE y añadirla a la generación más reciente o
- en ningún caso.

## Acciones que modifican la firma de origen SAFE

Las modificaciones en la configuración y los cambios de valores de variables pueden provocar un cambio de la firma de origen SAFE.

**Cambios en la configuración:** Las siguientes acciones de configuración comportan un cambio de firma:

Dispositivo	Acción
CPU de seguridad	Cambiar la referencia de la CPU a través de <b>Sustitución del procesador...</b>
	Cambiar la versión de la CPU a través de <b>Sustitución del procesador...</b>
	Editar cualquier parámetro de las fichas de configuración <b>Configuración</b> o <b>Hot Standby</b> de la CPU.
	Editar cualquier parámetro de cualquier ficha del módulo de comunicaciones Ethernet de la CPU ( <b>Seguridad</b> , <b>Configuración IP</b> , <b>RSTP</b> , <b>SNMP</b> , <b>NTP</b> , <b>ServicePort</b> , <b>Seguridad</b> , etc.).
Coprocador de seguridad	No aplicable, ya que el coprocador no es configurable.
Otro módulo de seguridad	<b>Añadir/Eliminar/Mover</b> un módulo, ya sea: <ul style="list-style-type: none"> <li>• Directamente (a través de un comando)</li> <li>• Indirectamente (por ejemplo, sustituyendo una placa de conexiones Ethernet de 8 slots [con un módulo de seguridad en el slot 7] por una placa de conexiones Ethernet de 4 slots, eliminando de esta forma un módulo)</li> </ul>
	Edición de cualquier parámetro del módulo de seguridad, ubicado en la ficha <b>Configuración</b> (por ejemplo, <b>Detección de cortocircuito a 24 V</b> , <b>Detección de cable abierto</b> ) y en el panel izquierdo del editor (por ejemplo, <b>Función</b> , <b>Retorno</b> ).
	Modificación del ID del módulo a través del comando <b>Renovar ID y Regenerar todo</b> .
	Modificación del nombre de instancia de DDT de dispositivo.

Dispositivo	Acción
Módulo CIP Safety	<b>Añadir/Eliminar</b> un módulo.
	Modificación de cualquier parámetro del módulo CIP Safety en el editor de DTM de dispositivos CIP Safety o de la <b>Lista de dispositivos</b> del editor de DTM maestro de CPU.
	Modificación del nombre de instancia de DDT de dispositivo.
Fuente de alimentación de seguridad	<b>Añadir/Eliminar</b> una fuente de alimentación de seguridad.
Otros equipos relacionados con la seguridad	Modificación de cualquier dirección topológica de equipos que admiten un dispositivo de seguridad, por ejemplo: <ul style="list-style-type: none"> <li>• Mover un bastidor que contiene un dispositivo de seguridad.</li> <li>• Mover un bus o una estación que contiene un dispositivo de seguridad.</li> </ul>

**Cambios de valores:** Excepto cuando se indique, los siguientes elementos se incluyen en el cálculo de firma de origen SAFE. Si se modifican estos valores, el valor de firma de origen SAFE cambia también:

Tipo	Elementos
Programa	Tarea SAFE y secciones de código relacionadas.
VARIABLES	Todas las variables de área segura y sus atributos.
DDT	Cada uno de los atributos de DDT seguro, excepto los atributos de fecha y versión.
	Las variables dentro de cada DDT, incluidos sus atributos.
	Los DDT seguros, aunque no se utilicen en la aplicación segura.
DFB	Cada uno de los atributos de DFB seguro, excepto los atributos de fecha y versión.
	Las variables dentro de cada DFB, incluidos sus atributos.
	Los DFB seguros, aunque no se utilicen en la aplicación segura.
Ajustes de ámbito seguro	Todos los <b>Ajustes del proyecto</b> cuyo <b>Ámbito</b> = seguro.
Ajustes de ámbito común	Los siguientes <b>Ajustes del proyecto</b> cuyo <b>Ámbito</b> = común:
	<b>VARIABLES</b> <ul style="list-style-type: none"> <li>• Permitir cifras antepuestas</li> <li>• Conjunto de caracteres</li> <li>• Permitir el uso de flanco en EBOOL</li> <li>• Permitir INT/DINT en lugar de ANY_BIT</li> <li>• Permitir extracción de bits de INT, WORD y BYTE</li> <li>• Variables de matriz representadas directamente</li> </ul>

Tipo	Elementos
	<ul style="list-style-type: none"> <li>• Habilitar exploración rápida para tendencias</li> <li>• Forzar inicialización de referencias</li> </ul>
	<p><b>Programa &gt; Lenguajes &gt; Común</b></p> <ul style="list-style-type: none"> <li>• Permitir procedimientos</li> <li>• Permitir comentarios intercalados</li> <li>• Permitir asignación múltiple [a:=b:=c] (ST/LD)</li> <li>• Permitir parámetros vacíos en llamadas no formales (ST/IL)</li> <li>• Mantener los enlaces de salida en EF deshabilitada (EN=0)</li> <li>• Mostrar comentarios completos del elemento de estructura</li> </ul>
	<p><b>Programa &gt; Lenguajes &gt; LD</b></p> <ul style="list-style-type: none"> <li>• Detección de flanco de un ciclo para EBOOL</li> </ul>
	<p><b>General &gt; Tiempo<sup>1</sup></b></p> <ul style="list-style-type: none"> <li>• Zona horaria personalizada</li> <li>• Zona horaria</li> <li>• Offset de tiempo</li> <li>• Ajustar automáticamente el reloj al horario de verano                             <ul style="list-style-type: none"> <li>◦ Todos los ajustes de START y END en Ajustar automáticamente el reloj al horario de verano</li> </ul> </li> </ul>
<p>1. Estas variables no se exportan, si bien cualquier cambio en los valores provocará un cambio en la firma parcial de configuración.</p>	

## Gestión de la firma de origen SAFE

La firma de origen SAFE se gestiona en Control Expert, en la ventana **Herramientas > Ajustes del proyecto**. Para ello, seleccione **General > Ajustes de generación** y, a continuación, uno de los siguientes ajustes de **Gestión de firmas SAFE**:

- **Automático** (valor predeterminado): genera una nueva firma de origen SAFE cada vez que se ejecuta un comando **Generar**.
- **A petición del usuario**: genera una nueva firma de origen SAFE cuando se ejecuta el comando **Generar > Actualizar firma SAFE**.

**NOTA:** Si selecciona **A petición del usuario**, Control Expert generará un valor de firma de origen SAFE de 0 con cada generación. Si no ejecuta el comando **Generar > Actualizar firma SAFE**, significa que opta por no utilizar la función de firma de seguridad.

## Transferencia de una aplicación del PC al PLC

Cuando descarga una aplicación del PC al PAC, Control Expert compara la firma de origen SAFE de la aplicación descargada con la del PAC. A continuación se describe el comportamiento de Control Expert:

Nueva firma de seguridad	Firma de seguridad del PAC	Control Expert muestra
Cualquiera	Ninguna aplicación	Confirmación de transferencia
Cualquiera (excepto 0)	0	Confirmación de transferencia
0	0	Confirmación de transferencia
0	Cualquiera (excepto 0)	Confirmación de transferencia, seguida de un aviso "Con esta acción, se restablecerá la firma SAFE", seguido de una nueva confirmación de transferencia
XXXX = YYYY <sup>2</sup>	YYYY	Confirmación de transferencia
XXXX ≠ YYYY <sup>3</sup>	YYYY	Confirmación de transferencia, seguida de un aviso "Con esta acción, se modificará la firma SAFE", seguido de una nueva confirmación de transferencia
<p>1. Un valor de "0" indica que una firma de origen SAFE no se generó de manera automática o manual.</p> <p>2. La aplicación segura del PC (XXXX) y la aplicación segura del PAC (YYYY) son IGUALES.</p> <p>3. La aplicación segura del PC (XXXX) y la aplicación segura del PAC (YYYY) son DIFERENTES.</p>		

## Visualización de la firma de origen SAFE

Cuando se utiliza, cada firma de origen SAFE consta de una serie de valores hexadecimales, por lo que puede resultar muy larga, lo que dificulta en gran medida las lecturas directas y comparaciones de valores al usuario humano. No obstante, es posible copiar el valor de una firma de origen SAFE y pegarlo en una herramienta de texto apropiada para realizar comparaciones. El valor de la firma de origen SAFE se puede encontrar en las siguientes ubicaciones de Control Expert:

- Ficha (véase EcoStruxure™ Control Expert, Modalidades de funcionamiento) **Propiedades del proyecto > Identificación**: En el **Explorador de proyectos**, haga clic con el botón derecho del ratón en **Proyecto** y seleccione **Propiedades**.
- Ficha (véase EcoStruxure™ Control Expert, Modalidades de funcionamiento) **PLCScreen > Información**: En el **Explorador de proyectos**, navegue hasta **Proyecto > Configuración > Bus PLC > <CPU>**, haga clic con el botón derecho del ratón y seleccione **Abrir** y, finalmente, seleccione la ficha **Animación**.
- Cuadro de diálogo (véase EcoStruxure™ Control Expert, Modalidades de funcionamiento) **Comparación PC < - - > PLC**: Seleccione este comando en el menú **PLC**.

- Cuadro de diálogo (véase EcoStruxure™ Control Expert, Modalidades de funcionamiento) **Transferir proyecto al PLC**: Seleccione este comando en el menú **PLC** (o en el cuadro de diálogo **Comparación PC < - - > PLC**).

## Comparación de la firma de origen SAFE con el SAId

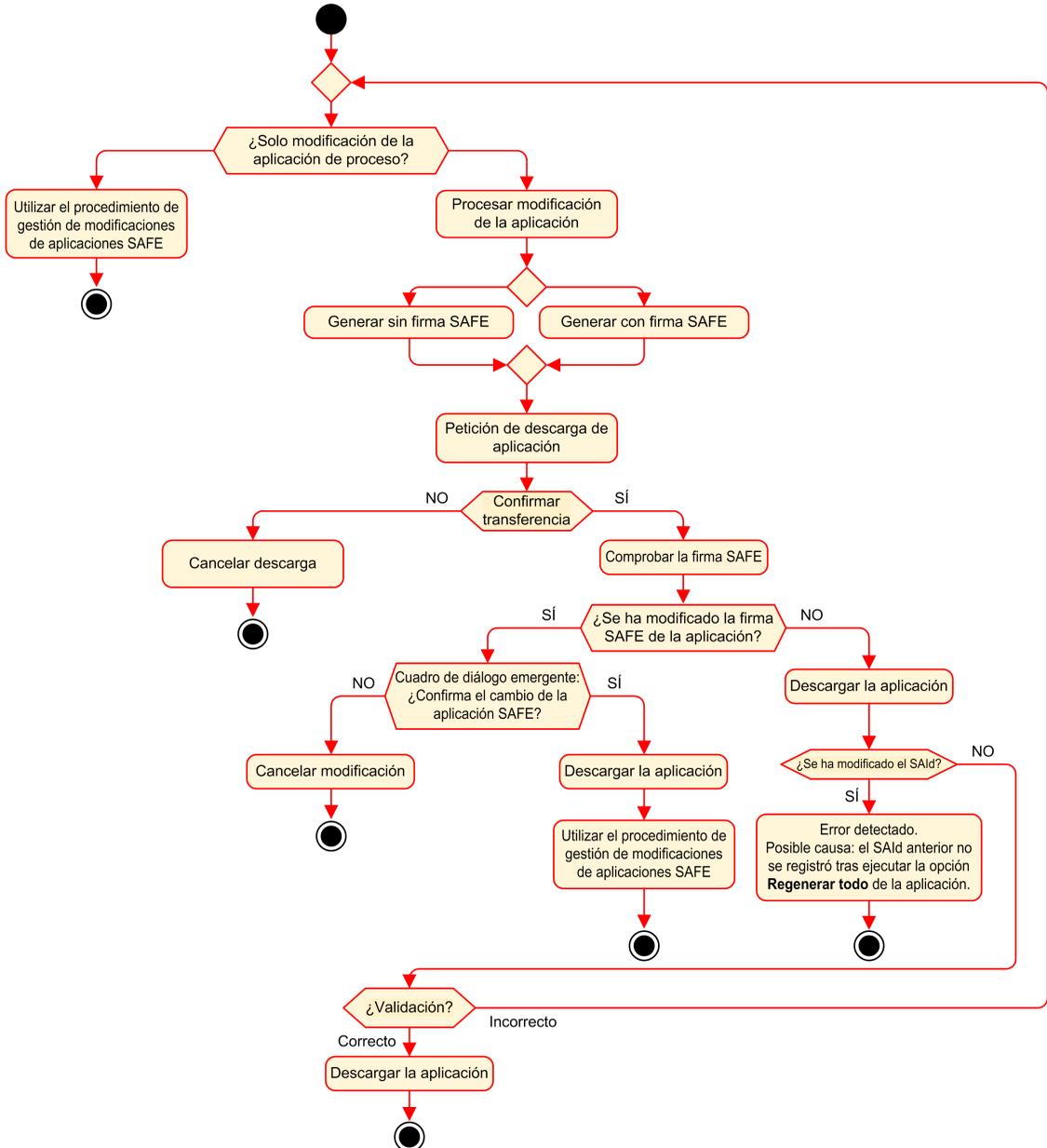
La firma de origen SAFE se introdujo para proporcionar una verificación *a priori* de que la aplicación segura no ha sufrido cambios. Se recomienda utilizar esta función cada vez que se modifique la aplicación del proceso, página 286 a fin de evitar posibles modificaciones accidentales de la aplicación segura.

Si bien la firma de origen SAFE es un mecanismo fiable, no resulta suficiente para las aplicaciones de seguridad, ya que un mismo código fuente puede corresponder a diferentes códigos binarios (ejecutables), en función del tipo de generación utilizada tras la última modificación del código seguro.

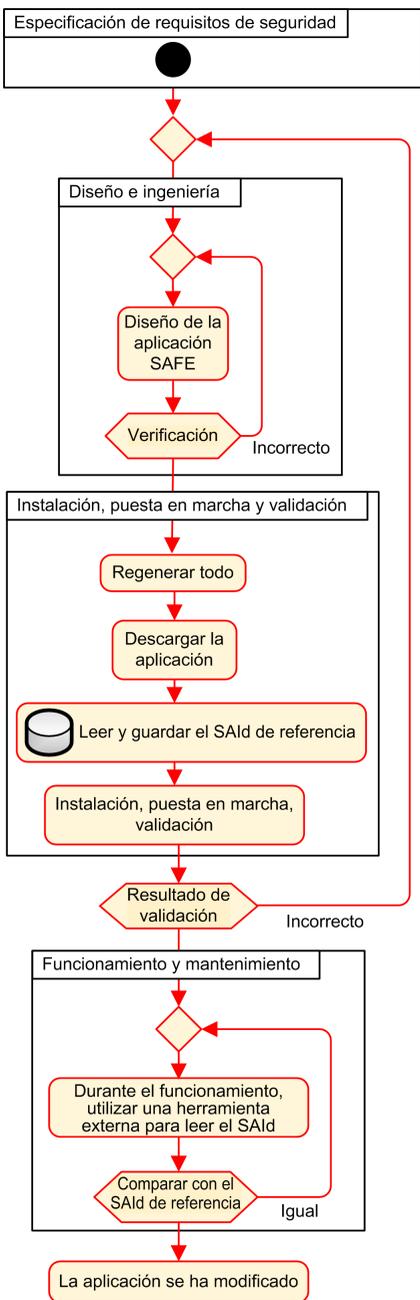
El SAId, página 376 solo puede evaluarse en el tiempo de ejecución. Su cálculo tiene doble ejecución y es comparado tanto por la CPU como por el COPRO, para lo cual se basa en el código binario que ejecuta la aplicación segura. Dado que el SAId es sensible a cualquier modificación, incluidas las que podrían introducirse mediante un comando **Regenerar todo** tras un cambio en la generación, se recomienda utilizar un comando **Regenerar todo** para generar una versión de referencia de la aplicación segura. Este proceso, página 287 permite utilizar cualquier tipo de generación (**Regenerar todo**, **Generar cambios** online u offline) para los cambios de la aplicación del proceso sin que el SAId sufra cambio alguno.

El SAId es el método recomendado para confirmar que la aplicación segura es la que se validó. La aplicación no prueba automáticamente el valor del SAId. Por este motivo, se recomienda verificar periódicamente el SAId por el medio que resulte más práctico (por ejemplo, mediante Control Expert o una HMI) consultando la salida del bloque de funciones S\_SYST\_STAT\_MX o el contenido de la palabra de sistema %SW169, página 408.

## Modificación del proceso simplificado de la aplicación del proceso



## Gestión del SAId



# Bloqueo de configuraciones de módulos de E/S de seguridad de M580

## Bloqueo de configuraciones de módulos de E/S de seguridad de M580

### Bloqueo de la configuración de un módulo de E/S de seguridad

Cada módulo de E/S de seguridad tiene un botón de bloqueo de la configuración (véase Modicon M580, Guía de planificación del sistema de seguridad) que se encuentra en la parte frontal superior del módulo. La finalidad de la función de bloqueo es ayudar a evitar cambios imprevistos de la configuración del módulo de E/S. Por ejemplo, el bloqueo de la configuración actual del módulo de E/S puede evitar un intento de asignar al módulo una configuración falsa, o simplemente ofrecer protección frente a fallos de configuración.

Para lograr el nivel de integridad de seguridad (SIL) previsto, bloquee cada módulo de E/S de seguridad después de configurarlo, pero antes de iniciar o reanudar operaciones.

### **⚠ ADVERTENCIA**

#### **RIESGO DE DEGRADACIÓN IMPREVISTA DEL NIVEL DE INTEGRIDAD DE SEGURIDAD DEL PROYECTO**

Debe bloquear cada módulo de E/S de seguridad después de configurarlo, pero antes de iniciar las operaciones.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

Los mecanismos de bloqueo y desbloqueo funcionan de la manera siguiente:

- Para bloquear la configuración de un módulo de E/S de seguridad, mantenga pulsado el botón de bloqueo durante más de 3 segundos y suéltelo.
- Para de bloquear la configuración de un módulo de E/S de seguridad, mantenga pulsado el botón de bloqueo durante más de 3 segundos y suéltelo.

## Escenarios para el bloqueo de configuraciones de módulos de E/S de seguridad

El procedimiento a seguir para bloquear la configuración de módulos de E/S de seguridad SIL3 variará en función del escenario, que puede ser:

- Primera configuración de módulos de E/S
- Sustitución rápida de dispositivos de módulos de E/S
- Realización de un cambio de configuración sobre la marcha (CCOTF) para módulos de E/S

A continuación se describe el procedimiento para cada escenario.

Primera configuración de módulos de E/S de seguridad SIL3:

Paso	Acción
1	Conecte Control Expert al PAC de seguridad M580.
2	Utilice el comando <b>Transferir proyecto desde PLC</b> para cargar el proyecto del PAC en Control Expert.
3	En la ventana <b>Bus PLC</b> de Control Expert, abra cada módulo de E/S de seguridad SIL3 y confirme que todos estén correctamente configurados.
4	En una tabla de animación en Control Expert, visualice el DDDT de cada módulo de E/S de seguridad SIL3 y confirme que la configuración de cada módulo sea la misma que en el paso 3 anterior.
5	Bloquee la configuración de cada uno de los módulos de E/S de seguridad SIL3 manteniendo pulsado el botón de bloqueo de la configuración (véase Modicon M580, Guía de planificación del sistema de seguridad) durante más de 3 segundos y soltándolo.
6	En una tabla de animación, compruebe la validez del estado del bit de bloqueo (CONF_LOCKED) para cada módulo de E/S SIL3.

Sustitución rápida de dispositivos de un módulo de E/S de seguridad SIL3:

Paso	Acción
1	Sustituya el módulo de E/S de seguridad SIL3 por uno nuevo.
2	Conecte Control Expert al PAC de seguridad M580 en modalidad de funcionamiento de mantenimiento, página 262.
3	En la ventana <b>Bus PLC</b> de Control Expert, abra cada módulo de E/S de seguridad SIL3 y confirme que todos estén correctamente configurados.
4	En una tabla de animación en Control Expert, visualice el DDDT de cada módulo de E/S de seguridad SIL3 y confirme que la configuración de cada módulo no haya cambiado y sea la misma que en el paso 3 anterior.
5	Bloquee la configuración de cada uno de los módulos de E/S de seguridad SIL3 manteniendo pulsado el botón de bloqueo de la configuración (véase Modicon M580, Guía de planificación del sistema de seguridad) durante más de 3 segundos y soltándolo.
6	En una tabla de animación, compruebe la validez del estado del bit de bloqueo (CONF_LOCKED) para cada módulo de E/S SIL3.

Realización de CCOTF para añadir un nuevo módulo de E/S de seguridad SIL3:

Paso	Acción
1	Conecte Control Expert al PAC de seguridad M580 en modalidad de funcionamiento de mantenimiento, página 262.
2	Añada un nuevo módulo de E/S de seguridad SIL3 a la configuración y edite la configuración del módulo, si es necesario.
3	Ejecute el comando <b>Generar &gt; Generar cambios</b> .
4	En la ventana <b>Bus PLC</b> de Control Expert, abra cada módulo de E/S de seguridad SIL3 y confirme que todos estén correctamente configurados.
5	En una tabla de animación en Control Expert, visualice el DDDT de cada módulo de E/S de seguridad SIL3 y confirme que la configuración de cada módulo no haya cambiado y sea la misma que en el paso 3 anterior.
6	Bloquee la configuración de cada uno de los módulos de E/S de seguridad SIL3 manteniendo pulsado el botón de bloqueo de la configuración (véase Modicon M580, Guía de planificación del sistema de seguridad) durante más de 3 segundos y soltándolo.
7	En una tabla de animación, compruebe la validez del estado del bit de bloqueo (CONF_LOCKED) para cada módulo de E/S SIL3.
8	En el menú <b>PLC</b> de Control Expert, ordene al PAC que entre en la modalidad de seguridad, página 261.

## Inicialización de datos en Control Expert

### Inicialización de datos en Control Expert para el PAC de seguridad M580

#### Dos comandos Init

El menú **PLC** de Control Expert proporciona dos comandos distintos para la inicialización de los datos:

- El comando **Init** inicializa los datos para el espacio de nombres de proceso (o no seguro), que puede ser utilizado por las tareas MAST, FAST, AUX0 y AUX1. Puede ejecutar este comando si el PAC funciona en modalidad de mantenimiento mientras el PAC está en el estado STOP. Este comando equivale a establecer el bit del sistema bit %S0 (COLDSTART) en 1.

**NOTA:** Si se establece el bit %S0 en 1, se inicializan los datos sólo en el espacio de nombres de proceso. No afecta a los datos del espacio de nombres seguro.

- El comando **Inicialización seguridad** inicializa los datos sólo para el espacio de nombres seguro, cuyos datos pueden ser utilizados exclusivamente por la tarea SAFE. Este comando sólo se puede ejecutar si la tarea SAFE funciona en modalidad de mantenimiento mientras la tarea SAFE está en el estado STOP o HALT. Si se ejecuta este comando cuando la tarea SAFE está en el estado HALT, la tarea SAFE se reinicia en el estado STOP.

Tanto el comando **Init** como el comando **Inicialización seguridad** realizan un arranque en frío., página 275

# Utilización de tablas de animación en Control Expert

## Tablas de animaciones y pantallas de operador

### Introducción

Un PAC de seguridad M580 admite tres tipos de tablas de animación, cada uno de los cuales está asociado con una de las siguientes áreas de datos:

- Las tablas de animación del área de proceso pueden incluir sólo datos en el espacio de nombres de proceso.
- Las tablas de animación del área de seguridad pueden incluir sólo datos en el espacio de nombres seguro.
- Las tablas de animación globales pueden incluir datos de toda la aplicación, incluidos datos creados para los espacios de nombres seguro y de proceso, y variables globales.

**NOTA:** En una tabla de animación global, los nombres de las variables de datos incluyen un prefijo que indica el espacio de nombres de origen, tal como se indica a continuación:

- Una variable de datos del espacio de nombres seguro se muestra como "SAFE.<Nombre de variable>".
- Una variable de datos del espacio de nombres de proceso se muestra como "PROCESS.<Nombre de variable>".
- Una variable de datos del espacio de nombres global (o de aplicación) sólo muestra su <Nombre de variable>, sin prefijo de espacio de nombres.

Tanto los datos de proceso como los de seguridad de un PAC de seguridad de M580 también resultan accesibles a procesos externos (por ejemplo, SCADA o HMI).

La capacidad de crear y modificar una tabla de animación, y la capacidad de ejecutar funciones de tabla de animación, dependen del espacio de nombres de las variables afectadas y la modalidad de funcionamiento del proyecto de seguridad.

## Condiciones para crear y editar tablas de animación

La creación y la edición de tablas de animación implican la adición o la eliminación de variables de datos. La capacidad de añadir variables de datos a una tabla de animación o eliminarlas de una tabla de animación depende de:

- El espacio de nombres (seguro o proceso) en el que reside la variable de datos.
- La modalidad de funcionamiento (seguridad o mantenimiento) del PAC de seguridad de M580

Cuando Control Expert está conectado al PAC de seguridad M580, se pueden crear y editar tablas de animación tal como se indica a continuación:

- Se pueden añadir variables de espacio de nombres de proceso a una tabla de animación de proceso o global o eliminarlos de dicha tabla mientras el PAC de seguridad M580 funcione en modalidad segura o de mantenimiento.
- Se pueden añadir variables de espacio de nombres seguro a una tabla de animación de seguridad o eliminarlos de dicha tabla mientras el PAC de seguridad de M580 funcione en modalidad de mantenimiento.
- Se pueden añadir variables de espacio de nombres seguro a una tabla de animación de seguridad o eliminarlos de dicha tabla mientras el PAC de seguridad M580 funcione en modalidad de seguridad sólo si la configuración del proyecto no incluye tablas de animación en la información de carga.

**NOTA:** Las tablas de animación se incluyen en la información de carga, o bien se excluyen de ella, en Control Expert seleccionando **Herramientas > Ajustes del proyecto...** para abrir la ventana **Ajustes del proyecto...** y luego navegando a **Ajustes del proyecto > General > Datos incorporados del PLC > Información de carga > Tablas de animación.**

## Condiciones para el funcionamiento de las tablas de animación

Puede utilizar tablas de animación para forzar un valor de variable, cancelar el forzado de una variable, modificar un solo valor de variable o modificar varios valores de variables. La capacidad de llevar a cabo estas funciones dependerá del espacio de nombres en que resida una variable y la modalidad de funcionamiento del PAC de seguridad M580, tal como se indica a continuación:

- Los valores de las variables de proceso o globales se pueden leer o escribir en modalidad de funcionamiento de seguridad y en modalidad de funcionamiento de mantenimiento.
- Los valores de las variables de seguridad se pueden leer o escribir en modalidad de funcionamiento de mantenimiento.
- Los valores de las variables de seguridad sólo se pueden leer en modalidad de funcionamiento de seguridad.

## Proceso para crear tablas de animación en el espacio de nombres de seguridad o de proceso en Control Expert

Control Expert ofrece dos maneras de crear tablas de animación para el espacio de nombres de seguridad o de proceso:

- En una ventana de sección de código de seguridad o de proceso, haga clic con el botón derecho del ratón en la ventana de código y seleccione:
  - **Inicializar tabla de animación** para añadir el objeto de datos a una tabla de animación existente en un espacio de nombres de seguridad o de proceso, o bien
  - **Inicializar nueva tabla de animación** para añadir el objeto de datos a una nueva tabla de animación en el espacio de nombres de seguridad o de proceso.

En cada caso, todas las variables de la sección de código se añaden a la tabla de animación existente o nueva.

- En el **Explorador de proyectos**, ya sea en el área de datos de proceso o de seguridad, haga clic con el botón derecho del ratón en la carpeta **Tablas de animación** y luego seleccione **Nueva tabla de animación**. Control Expert crea una nueva tabla de animación vacía. Luego puede añadir variables individuales del espacio de nombres (de seguridad o de proceso) relacionadas con la tabla.

## Proceso para crear tablas de animación de ámbito global

Para crear una tabla de animación global en el **Explorador de proyectos**, haga clic con el botón derecho del ratón en la carpeta **Tablas de animación** global y luego seleccione **Nueva tabla de animación**. Puede añadir variables a la nueva tabla de animación de varias maneras:

- **Arrastrar y colocar**: Puede arrastrar una variable desde un editor de datos y soltarla en la tabla de animación global. Como el ámbito de la tabla de animación incluye toda la aplicación, puede arrastrar la variable desde el **Editor de datos de seguridad**, el **Editor de datos de proceso** o el **Editor de datos globales**.
- **Cuadro de diálogo Selección de instancias**: Puede hacer doble clic en una fila en la tabla de animación y luego hacer clic en el botón con puntos suspensivos para abrir el diálogo **Selección de instancias**. Utilice la lista de filtrado de la parte superior derecha del diálogo para seleccionar una de las áreas de proyecto siguientes:
  - **SAFE**: Para visualizar objetos de datos relacionados con el área de seguridad.
  - **PROCESO**: Para visualizar objetos de datos relacionados con el área de proceso.
  - **APLICACIÓN**: Para visualizar objetos de datos del ámbito de la aplicación de nivel superior.

Seleccione un objeto de datos y luego haga clic en **Aceptar** para añadir el elemento a la tabla de animación.

**NOTA:** Los objetos de datos añadidos a una tabla de animación global desde:

- El área de proceso llevan el prefijo "PROCESS" junto al nombre de la variable (por ejemplo, PROCESS.variable\_01)
- El área de seguridad llevan el prefijo "SAFE" junto al nombre de la variable (por ejemplo, SAFE.variable\_02)
- El área global no llevan ningún prefijo junto al nombre de la variable.

## Visualización de datos en pantallas de operador

Puede visualizar datos en una pantalla de operador, como una aplicación HMI, SCADA o FactoryCast, del mismo modo que enlaza a datos en una tabla de animación. Las variables de datos disponibles para la selección son las variables incluidas en el diccionario de datos de Control Expert.

Puede habilitar el diccionario de datos abriendo la ventana **Herramientas > Ajustes del proyecto...** y seleccionando luego, en el área **Ámbito > común** de la ventana, **General > Datos incorporados del PLC > Diccionario de datos**.

El diccionario de datos proporciona las variables de datos en las pantallas de operador tal como se indica a continuación:

- Las variables del espacio de nombres seguro siempre incluyen en prefijo "SAFE" y sólo se puede acceder a ellas utilizando el formato "SAFE.<Nombre de variable>".
- Las variables de espacio de nombres global o de aplicación no incluyen ningún prefijo, y sólo se puede acceder a ellas utilizando el "<Nombre de variable>" sin prefijo.
- El ajuste **Uso del espacio de nombres de proceso** determina cómo puede acceder una pantalla de operador a variables de espacio de nombres de proceso.
  - Si selecciona **Uso del espacio de nombres de proceso**, la pantalla de operador puede leer variables del área de proceso únicamente utilizando el formato "PROCESS.<Nombre de variable>".
  - Si anula la selección de **Uso del espacio de nombres de proceso**, la pantalla de operador puede leer variables del área de proceso únicamente utilizando el formato "<Nombre de variable>" sin el prefijo "PROCESS".

**NOTA:** Si se declaran dos variables con el mismo nombre, una en el espacio de nombres de proceso y otra en espacio de nombres global, las aplicaciones HMI, SCADA o Factory Cast sólo pueden acceder a la variable del espacio de nombres global.

Puede utilizar el diálogo **Selección de instancias** para acceder a objetos de datos concretos.

### ⚠ ATENCIÓN

**VALOR DE VARIABLE IMPREVISTO**

- Asegúrese de que la aplicación tenga los ajustes de proyecto correctos.
- Compruebe la sintaxis para acceder a las variables en los distintos espacios de nombres.

**Si no se siguen estas instrucciones, pueden producirse lesiones o daños en el equipo.**

Para evitar acceder a la variable incorrecta:

- Utilice nombres diferentes para las variables que declare en el espacio de nombres de proceso y en el espacio de nombres global, o bien
- seleccione **Uso del espacio de nombres de proceso** y utilice la siguiente sintaxis para acceder a las variables con el mismo nombre:
  - "PROCESS.<nombre de variable>" para las variables declaradas en el espacio de nombres de proceso.
  - "<nombre de variable>" sin ningún prefijo para las variables declaradas en el espacio de nombres global.

## Trending Tool

El uso de la herramienta Trending Tool de Control Expert no es compatible con un proyecto de seguridad de M580.

## Adición de secciones de código

### Adición de código a un proyecto de seguridad de M580

#### Utilización de tareas en Control Expert

En el espacio de nombres del proceso, Control Expert incluye la tarea MAST de forma predeterminada. La tarea MAST no se puede eliminar. No obstante, se pueden añadir las tareas FAST, AUX0 y AUX1. Tenga en cuenta que la creación de una tarea en la parte de proceso de un proyecto de seguridad es igual que la creación de una tarea en un proyecto que no sea de seguridad. Para obtener más información, consulte el tema *tareaCrear y configurar una tarea* en el manual de modos™ de operación de EcoStruxure Control Expert.

En el espacio de nombres seguro, Control Expert incluye la tarea SAFE de manera predeterminada. La tarea SAFE no se puede eliminar y no se pueden añadir otras tareas a la sección **Seguridad del programa** del **Explorador de proyectos** en Control Expert. Puede añadir múltiples secciones a la tarea SAFE.

#### Configuración de las propiedades de la tarea SAFE

La tarea SAFE sólo admite la ejecución periódica de tareas (no se admite la ejecución cíclica). Los ajustes **Periodo** y **Watch Dog** de la tarea SAFE se introducen en el diálogo **Propiedades de SAFE** y pueden admitir el rango de valores siguiente:

- Periodo de tarea SAFE: 10...255 ms con un valor predeterminado de 20 ms.
- Supervisión de tareas SAFE: 10...500 ms, en incrementos de 10 ms, con un valor predeterminado de 250 ms.

Establezca el **Periodo** de la tarea SAFE en un valor mínimo en función del tamaño de datos seguros y del modelo de PLC. El periodo mínimo de la tarea SAFE se puede calcular con las fórmulas siguientes:

- Valor mínimo absoluto necesario para las comunicaciones de E/S:
  - 10 ms
- Tiempo (en ms) necesario para transferir y comparar los datos seguros entre la CPU y el COPRO:
  - $(0,156 \times \text{Data\_Safe\_Size}) + 2$  ms (para BM584040S, BM586040S, BMEH584040S, y BMEH586040S)
  - $(0,273 \times \text{Data\_Safe\_Size}) + 2$  ms (para BM582040S y BMEH582040S)

Donde Data\_Safe\_Size es tamaño en Kbytes de los datos seguros.

- Los PAC Hot Standby necesitan tiempo adicional (en ms) para transferir los datos seguros del PAC primario al PAC standby:
  - $(K1 \times \text{Task}_{kb} + K2 \times \text{Task}_{DFB}) / 500$

En esta fórmula:

- $\text{Task}_{DFB}$  = el número DFB declarados en la parte segura de la aplicación.
- $\text{Task}_{kb}$  = el tamaño (en Kbytes) de los datos seguros intercambiados por la tarea SAFE entre los PAC primario y standby.
- K1 y K2 son constantes, con valores determinados por el módulo de CPU específico utilizado en la aplicación:

Coeficiente	BMEH582040S	BMEH584040S y BMEH586040S
K1	32,0	10,0
K2	23,6	7,4

**NOTA:**

- El valor que se genera en estas fórmulas es un valor mínimo absoluto correspondiente al periodo de tarea SAFE y resulta útil sólo para realizar una primera estimación del límite de tiempo de ciclo SAFE. No incluye el tiempo necesario para ejecutar el código de usuario ni para el margen que se necesita para que el sistema multitarea PAC funcione como se espera. Consulte el tema rendimiento del sistema Consideraciones sobre el rendimiento del sistema en la Guía de planificación del sistema independiente *Modicon M580 para arquitecturas de uso frecuente*.
- De forma predeterminada, los valores  $\text{Data\_Safe\_Size}$  y  $\text{Size}_{kbytes}$  son iguales. Sus valores se pueden ver, respectivamente, en el menú **PLC > Utilización de memoria** y la pantalla **PLC > Hot Standby**.

## Cálculos de ejemplo

A continuación se ofrecen ejemplos de resultados del cálculo del periodo mínimo de la tarea SAFE.

Periodo mínimo de la tarea SAFE (ms)					
$\text{Size}_{kbytes}^1$	$\text{Nb}_{DFB\_Inst}$	BMEP582040S	BMEP584040S o BMEP586040S	BMEH582040S	BMEH584040S o BMEH586040S
0	0	10	10	10	10
50	10	16	10	20	11
100	10	30	18	37	20
150	10	43	25	54	29

Periodo mínimo de la tarea SAFE (ms)					
Size <sub>kbytes</sub> <sup>1</sup>	Nb <sub>DFB_Inst</sub>	BMEP582040S	BMEP584040S o BMEP586040S	BMEH582040S	BMEH584040S o BMEH586040S
200	10	57	33	70	37
250	10	71	41	87	46
300	20	84	49	105	55
350	20	98	57	121	64
400	20	112	64	138	73
450	20	125	72	155	81
500	20	139	80	172	90
550	30	-	88	-	99
600	30	-	96	-	108
650	30	-	103	-	117
700	30	-	111	-	126
750	30	-	119	-	134
800	40	-	127	-	143
850	40	-	135	-	152
900	40	-	142	-	161
950	40	-	150	-	170
1000	40	-	158	-	179

1. Se asume que Size<sub>kbytes</sub> y Data\_Safe\_Size son iguales.

**NOTA:** Configure el watchdog de la tarea SAFE con un valor superior al **Periodo** de la tarea SAFE.

Consulte el tema *Tiempo de seguridad del proceso*, página 157 para obtener información referente a cómo afecta la configuración de la tarea SAFE al tiempo de seguridad del proceso.

Consulte el tema *Tareas del PAC de seguridad M580*, página 276 para obtener información que describe la prioridad de ejecución de la tarea SAFE.

## Creación de secciones de código

Haga clic con el botón derecho del ratón en la carpeta **Sección** de una tarea y seleccione **Nueva sección...** para abrir un diálogo de configuración. Para las tareas de seguridad y de proceso, están disponibles los siguientes lenguajes de programación:

Lenguaje	Tareas de seguridad	Tareas de proceso			
	SAFE	MAST	FAST	AUX0	AUX1
IL	–	✓	✓	✓	✓
FBD	✓	✓	✓	✓	✓
LD	✓	✓	✓	✓	✓
Segmento LL984	–	✓	✓	✓	✓
SFC	–	✓	✓	✓	✓
ST	–	✓	✓	✓	✓
✓ : Disponible – : No disponible					

A excepción de estas limitaciones por lo que respecta a la disponibilidad de lenguajes de programación para la tarea SAFE, el diálogo de configuración de la nueva sección funciona del mismo modo que en el caso de un proyecto de M580 que no sea de seguridad. Consulte el tema *Secciones FBD, LD, IL o ST* en el manual de modos de control™ *EcoStruxure* para obtener más información.

## Adición de datos a secciones de código

Puesto que la tarea SAFE está separada de las tareas de proceso, sólo los datos a los que se puede acceder en el **Editor de datos de seguridad** están disponibles para añadirlos a una sección de código de tarea SAFE. Estos datos incluyen:

- Variables de seguridad no ubicadas (es decir, sin dirección %M o %MW) creadas en el **Editor de datos de seguridad**.
- Objetos de datos que forman parte de estructuras DDT de dispositivos de módulos de seguridad M580.

De manera similar, los datos disponibles para secciones de código de tareas que no son de seguridad incluyen todos los datos dentro del ámbito del espacio de nombres de proceso. Esto incluye todos los datos del proyecto excepto:

- Datos exclusivamente disponibles para el espacio de nombres SAFE (véase más arriba).
- Objetos de datos creados en el **Editor de datos globales**.

## Análisis de código

Cuando se analiza o se genera un proyecto, Control Expert muestra un mensaje de error detectado si:

- Hay datos pertenecientes al espacio de nombres de proceso incluidos en la tarea SAFE.
- Hay datos pertenecientes al espacio de nombres seguro incluidos en una tarea de proceso (MAST, FAST, AUX0, AUX1).
- Hay bits (%M) o palabras (%MW) ubicados incluidos en una sección de una tarea SAFE.

## Petición de diagnóstico

### Introducción

La petición de diagnóstico sólo está disponible para fuentes de alimentación de seguridad M580 ubicadas en el bastidor principal utilizando el bloque de funciones PWS\_DIAG. Un bastidor principal se caracteriza por tener una dirección de 0 y una CPU o un módulo de adaptador de comunicaciones (CRA) en el slot 0 o 1. Un bastidor de extensión no es un bastidor principal.

La CPU puede realizar una petición de diagnóstico de fuentes de alimentación redundantes en el bastidor local y, mediante un adaptador de comunicaciones (CRA), de fuentes de alimentación redundantes en un bastidor remoto. Si las fuentes de alimentación maestra y esclava están operativas, la fuente de alimentación maestra pasará a la modalidad de diagnóstico de maestro y la fuente de alimentación esclava pasará a la modalidad de diagnóstico de esclavo. Los LED indican que la prueba está en curso.

**NOTA:** Esta petición no se implementa al encender.

Una vez que la prueba de diagnóstico ha finalizado, la maestra vuelve a su estado operativo normal y la esclava pasa al estado normal o de error, en función del resultado de las pruebas. Los resultados de la prueba se almacenan en la memoria de la fuente de alimentación.

### Datos devueltos por la petición de diagnóstico

La información de diagnóstico que se envía a la CPU mediante las fuentes de alimentación incluye:

- Temperatura ambiente de la fuente de alimentación.
- Tensión y corriente en la línea de placa de conexiones 3,3 V.
- Tensión y corriente en la línea de placa de conexiones de 24 V.

- Energía acumulada total de la fuente de alimentación desde la fabricación en las líneas de placa de conexiones de 3,3 V y 24 V.
- Tiempo de funcionamiento como maestra desde el último encendido y fabricación.
- Tiempo de funcionamiento total como esclava desde el último encendido y fabricación.
- Tiempo de vida en porcentaje (LTPC, por sus siglas en inglés) restante: el tiempo que debe pasar antes de realizar el mantenimiento preventivo, de 100 % a 0 %.

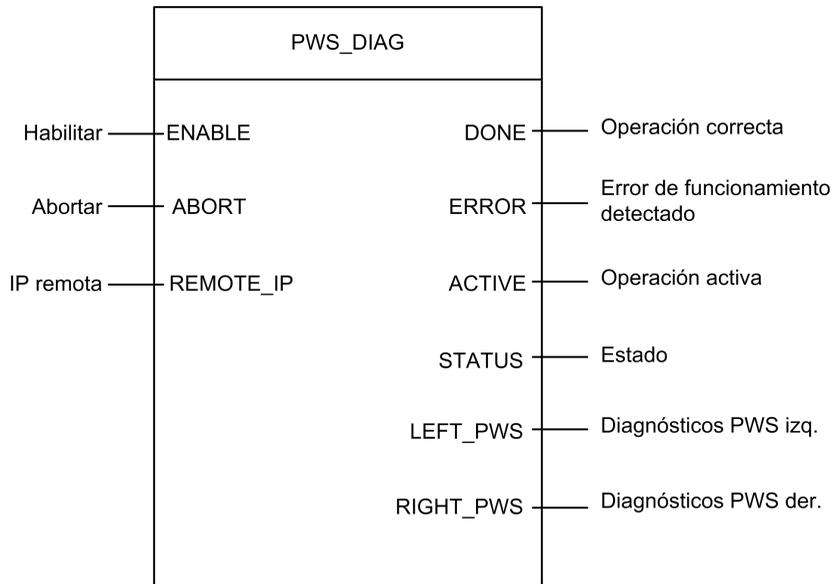
**NOTA:** No hay intercambio cuando el valor es 0 %.

- Número de veces que se ha encendido la fuente de alimentación.

**NOTA:** Desde SCADA, se puede restablecer el número de encendidos desde la instalación y el resto de los diagnósticos.

- Número de veces que la tensión principal de BMXCPS4002S ha caído por debajo del nivel de infratensión 1 (95 V CA).
- Número de veces que la tensión principal BMXCPS4002S supera el nivel de sobretensión 2 (195 V CA).
- Número de veces que la tensión principal de BMXCPS4022S ha caído por debajo del nivel de infratensión 1 (20 V CC).
- Número de veces que la tensión principal de BMXCPS4022S supera el nivel de sobretensión 2 (40 V CC).
- Número de veces que la tensión principal de BMXCPS3522S ha caído por debajo del nivel de infratensión 1 (110 V CC).
- Número de veces que la tensión principal de BMXCPS3522S supera el nivel de sobretensión 2 (140 V CC).
- Estado actual de la fuente de alimentación (maestra/esclava/no operativa).

## Representación en FBD



## Parámetros

Parámetros de entrada:

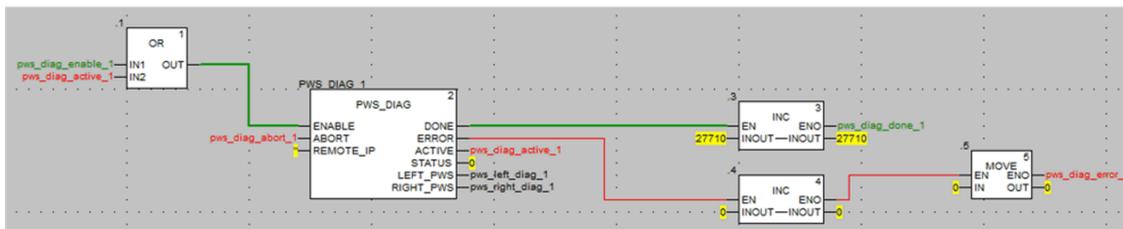
Nombre del parámetro	Tipo de datos	Descripción
ENABLE	BOOL	Cuando está activa, la operación está habilitada.
ABORT	BOOL	Cuando está en ON, se cancela la operación activa en ese momento.
REMOTE_IP	STRING	Dirección IP ("ip1.ip2.ip3.ip4") de la estación que contiene el módulo de alimentación. Deje una cadena vacía ("") en este campo o no asocie ninguna variable a su pin para direccionar la fuente de alimentación del bastidor local.

Parámetros de salida:

Nombre del parámetro	Tipo de datos	Descripción
DONE	BOOL	ON cuando la operación finaliza correctamente.
ERROR	BOOL	ON cuando la operación se cancela sin éxito.
ACTIVE	BOOL	ON cuando la operación está activa.

Nombre del parámetro	Tipo de datos	Descripción
STATUS	WORD	Identificador de error detectado.
LEFT_PWS	ANY	Datos de diagnóstico para fuente de alimentación izquierda. Utilice una variable de tipo PWS_DIAG_DDT_V2, página 138 para realizar una interpretación correcta.
RIGHT_PWS	ANY	Datos de diagnóstico para fuente de alimentación derecha. Utilice una variable de tipo PWS_DIAG_DDT_V2 para realizar una interpretación correcta.

## Ejemplo



		PWS_DIAG_DDT	
+	pws_left_diag_1		PWS_DIAG_DDT
+	pws_right_diag_1		PWS_DIAG_DDT
•	PwsMajorVersion	153	BYTE Power Supply major version
•	PwsMinorVersion	162	BYTE Power Supply minor version
•	Model	0	BYTE Power Supply Model identifier
•	State	12	BYTE Power Supply state
•	I33BacPos	0	UINT Measure current of 3V3 Bac in nominal role (producer)
•	V33Buck	0	UINT Measure voltage of 3V3 Buck
•	I24Bac	0	UINT Measure current of 24V Bac
•	V24Int	0	UINT Measure voltage of 24V Int
•	Temperature	0	INT Measure of Ambient Temperature
•	OperTimeMaster...	16935	DINT Operating Time as Master since last Power ON
•	OperTimeSlaveSi...	2	DINT Operating Time as Slave since last Power ON
•	OperTimeMaster	282128	DINT Operating Time as Master since Manufacturing
•	OperTimeSlave	44	DINT Operating Time as Slave Since Manufacturing
•	Work	0	DINT Work supplied since Manufacturing
•	RemainingLTPC	0	UINT Remaining Life Time in percent
•	NbPowerOn	0	UINT Number of Power ON since Manufacturing
•	NbVoltageLowFail	0	UINT Number of failure detected on Primary Voltage by Low Threshold
•	NbVoltageHighFail	0	UINT Number of failure detected on Primary Voltage by High Threshold

## Comandos de intercambio y borrado

### Introducción

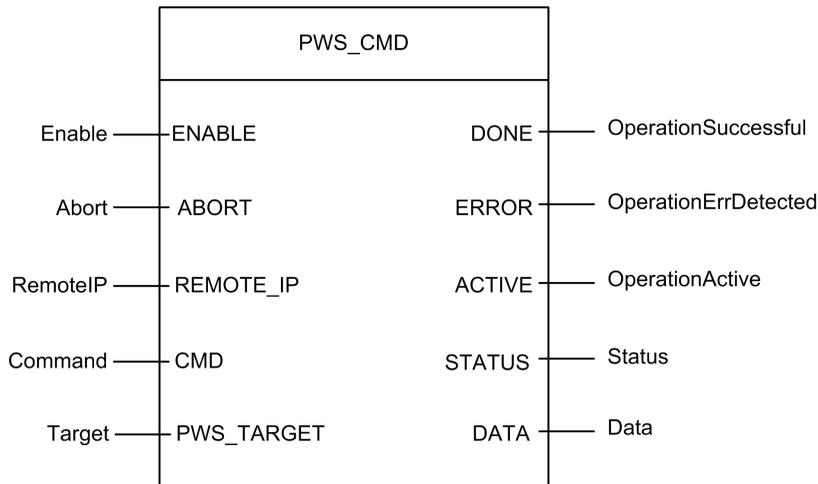
El bloque de funciones PWS\_CMD se puede utilizar para emitir dos comandos.

- Petición de intercambio: este comando especifica la fuente de alimentación que se utiliza como maestra. Si las dos fuentes de alimentación están operativas, la fuente de alimentación especificada se convierte en la maestra y la otra en la esclava.
- Petición de borrado: este comando restablece los contadores del número de estas situaciones:
  - La tensión ha caído por debajo del nivel de infratensión 1.
  - La tensión ha caído por debajo del nivel de infratensión 2.
  - La fuente de alimentación se ha encendido.

Ambas peticiones sólo están disponibles para fuentes de alimentación del bastidor principal. Un bastidor principal se caracteriza por tener una dirección de 0 y una CPU o un módulo de adaptador de comunicaciones (CRA) en el slot 0 o 1. Un bastidor de extensión no es un bastidor principal.

Los LED indican que el comando está en curso. Un registro del evento se almacena en la memoria de la fuente de alimentación.

## Representación en FBD



## Parámetros

Parámetros de entrada:

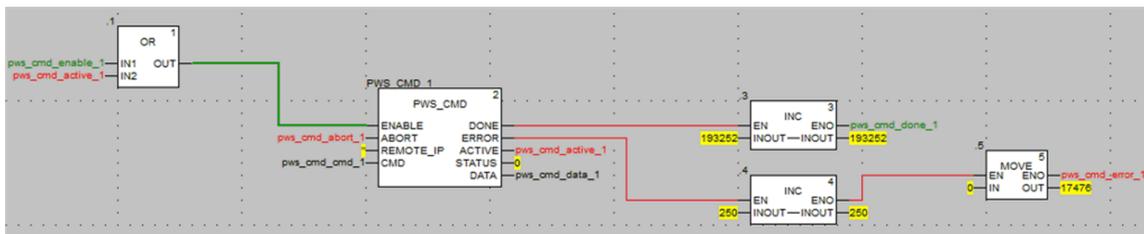
Nombre del parámetro	Tipo de datos	Descripción
ENABLE	BOOL	Cuando está activa, la operación está habilitada.
ABORT	BOOL	Cuando está en ON, se cancela la operación activa en ese momento.
REMOTE_IP	STRING	Dirección IP ("ip1.ip2.ip3.ip4") de la estación que contiene el módulo de alimentación. Deje una cadena vacía ("") en este campo o no asocie ninguna variable a su pin para direccionar la fuente de alimentación del bastidor local.
CMD	ANY	Use una variable del tipo PWS_CMD_DDT para hacer una interpretación correcta. Código de comando disponible: <ul style="list-style-type: none"> <li>• 1 = intercambiar</li> <li>• 3 = borrar</li> </ul>
PWS_TARGET	BYTE	Fuente de alimentación a la que se direcciona: <ul style="list-style-type: none"> <li>• 1 = izquierda</li> <li>• 2 = derecha</li> <li>• 3 = ambas</li> </ul>

Parámetros de salida:

Nombre del parámetro	Tipo de datos	Descripción
DONE	BOOL	ON cuando la operación finaliza correctamente.
ERROR	BOOL	ON cuando la operación se cancela sin éxito.
ACTIVE	BOOL	ON cuando la operación está activa.
STATUS	WORD	Identificador de error detectado.
DATA	ANY	Datos de respuesta (en función del código de comando). No se han notificado datos para los comandos de intercambio y borrado.

## Ejemplo

En el diagrama siguiente se muestra un bloque PWS\_CMD que se utiliza para una petición de intercambio.



En la pantalla del editor de datos siguiente se muestran los valores de variables de una petición de intercambio:

Name	Value	Type	Comment
pws_cmd_enable_1	1	BOOL	
pws_cmd_abort_1	0	BOOL	
pws_cmd_active_1	0	BOOL	
pws_cmd_done_1	1	BOOL	
pws_cmd_error_1	0	BOOL	
pws_cmd_status_1	16#0000	WORD	
pws_cmd_last_error_1	16#4444	WORD	
pws_cmd_OKCount_1	195842	DINT	
pws_cmd_KOCount_1	251	DINT	
pws_cmd_cmd_1		PWS_CMD_DDT	
Code	3	BYTE	<b>Command code: 1 = swap, 3 = clear, etc.</b>
Pws Target	2	BYTE	Power supply target: 1 for left, 2 for right, 3 for both
pws_cmd_ip_str_1	""	string[64]	
pws_cmd_data_1		PWS_DATA_DDT	

# Gestión de la seguridad de las aplicaciones

## Introducción

Control Expert permite restringir el acceso al PAC de seguridad M580 a los usuarios con contraseñas asignadas. Esta sección hace referencia a los procesos de asignación de contraseñas disponibles en Control Expert.

## Protección de la aplicación

### Descripción general

Control Expert ofrece un mecanismo de contraseña para ofrecer protección frente al acceso no autorizado a la aplicación.

Control Expert utiliza la contraseña en las situaciones siguientes:

- Cuando se abre la aplicación en Control Expert.
- Cuando se conecta al PAC en Control Expert.

La configuración de una contraseña de aplicación ayuda a impedir la modificación, la descarga o la apertura no deseada de archivos de aplicación. La contraseña se almacena cifrada en la aplicación.

Además de establecer la contraseña, puede cifrar los archivos `.STU`, `.STA` y `.ZEF`. La función de cifrado de archivos de Control Expert ayuda a impedir las modificaciones por parte de personas malintencionadas y refuerza la protección contra el robo de propiedad intelectual. La opción de cifrado de archivos está protegida por un mecanismo de contraseña.

**NOTA:** Cuando un controlador se gestiona como parte de un proyecto de sistema, la contraseña de la aplicación y el cifrado de archivos se deshabilitan en el editor de Control Expert y deben gestionarse mediante el Administrador de topología.

## Creación de contraseñas

La creación de contraseñas está basada en las recomendaciones de la norma del IEEE 1686-2013.

Una contraseña debe contener al menos 8 caracteres, y combinar como mínimo una mayúscula (A, B, C, ...), una minúscula (a, b, c, ...), un número y un carácter no alfanumérico (!, \$, %, &, ...).

**NOTA:** Al exportar un proyecto no cifrado a un archivo .XEF o .ZEF, se borra la contraseña de la aplicación.

## Creación de nuevos proyectos

De forma predeterminada, un proyecto no está protegido con contraseña y los archivos de aplicación no están cifrados.

En la creación del proyecto, la ventana **Medidas de seguridad** permite:

- Establecer una contraseña de aplicación o
- Establecer una contraseña de aplicación y aplicar cifrado a los archivos de aplicación. La aplicación del cifrado de archivos también requiere la configuración de una contraseña y se recomienda establecer dos contraseñas diferentes.

Si no se introduce ninguna contraseña, no es posible cifrar los archivos de aplicación. En este caso, la próxima vez que abra el proyecto de Control Expert, se abrirá el cuadro de diálogo **Contraseña**. Para acceder al proyecto, no introduzca ningún texto como contraseña, con lo que aceptará la cadena vacía, y haga clic en **Aceptar**. A continuación, puede seguir los pasos que se indican a continuación para establecer una contraseña de aplicación y habilitar el cifrado de archivos.

**NOTA:** Es posible crear o cambiar una contraseña de aplicación en cualquier momento.

La configuración de una contraseña de aplicación es obligatoria para habilitar el cifrado de archivos.

Cuando el cifrado de archivos está habilitado:

- Se permite cambiar la contraseña de la aplicación.
- No se permite borrar la contraseña de la aplicación.

## Configuración de una contraseña de aplicación

Procedimiento para establecer la contraseña de la aplicación:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de proyecto y controlador</b> .
4	En el campo <b>Aplicación</b> , haga clic en <b>Cambiar contraseña...</b> <b>Resultado:</b> Aparecerá la ventana <b>Modificar contraseña</b> .

Paso	Acción
5	Introducir la nueva contraseña en el campo <b>Entrada</b> .
6	Introducir la confirmación de la nueva contraseña en el campo <b>Confirmación</b> .
7	Hacer clic en <b>Aceptar</b> para confirmar.
8	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Modificación de la contraseña de la aplicación

Procedimiento para cambiar la contraseña de protección de la aplicación:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable.  <b>Resultado:</b> aparece la ventana <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de proyecto y controlador</b> .
4	En el campo <b>Aplicación</b> , haga clic en <b>Cambiar contraseña...</b>  <b>Resultado:</b> Aparecerá la ventana <b>Modificar contraseña</b> .
5	Introduzca la contraseña anterior en el campo <b>Contraseña anterior</b> .
6	Introducir la nueva contraseña en el campo <b>Entrada</b> .
7	Introducir la confirmación de la nueva contraseña en el campo <b>Confirmación</b> .
8	Hacer clic en <b>Aceptar</b> para confirmar.
9	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Eliminación de la contraseña de la aplicación

La contraseña de la aplicación no se puede borrar con el cifrado de archivos habilitado.

Procedimiento para borrar la contraseña de protección de la aplicación:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de proyecto y controlador</b> .
4	En el campo <b>Aplicación</b> , haga clic en <b>Borrar contraseña....</b> <b>Resultado:</b> aparece la ventana <b>Contraseña</b> .
5	Introduzca la contraseña en el campo <b>Contraseña</b> .
6	Hacer clic en <b>Aceptar</b> para confirmar.
7	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Función de bloqueo automático

Existe una función opcional de bloqueo automático para limitar el acceso a la herramienta de programación del software Control Expert después de un tiempo de inactividad que haya configurado. Puede activar la función de bloqueo automático con la casilla de verificación **Bloqueo automático** y seleccionar el timeout para el tiempo de inactividad mediante **Minutos antes del bloqueo**.

Los valores predeterminados son:

- La función **Bloqueo automático** no está activada
- La función **Minutos antes del bloqueo** está establecida en 10 minutos (valores posibles: 1 a 999 minutos)

Si la función de bloqueo automático está habilitada y transcurre el tiempo de inactividad configurado, se abre un cuadro de diálogo modal en el que se solicita la introducción de la contraseña de la aplicación. Detrás del cuadro de diálogo modal, todos los editores abiertos siguen abiertos en la misma posición. En consecuencia, cualquiera puede leer el contenido actual de las ventanas de Control Expert pero no puede continuar trabajando con Control Expert.

**NOTA:** Si no ha asignado una contraseña al proyecto, el cuadro de diálogo modal no aparece.

## Condición para la petición de la contraseña

Abra una aplicación existente (proyecto) en Control Expert:

<b>Gestión de contraseñas</b>	
Cuando un archivo de aplicación está abierto, se abre el cuadro de diálogo <b>Contraseña de la aplicación</b> .	
Introduzca la contraseña.	
Haga clic en <b>Aceptar</b> .	Si la contraseña introducida es correcta, se abrirá la aplicación.
	Si la contraseña es incorrecta, un cuadro de mensaje indica que se ha introducido una contraseña incorrecta y se abre un nuevo cuadro de diálogo <b>Contraseña de la aplicación</b> .
Si hace clic en <b>Cancelar</b> , no se abrirá la aplicación.	

Acceso a la aplicación en Control Expert después de un bloqueo automático, cuando Control Expert no está conectado al PAC o cuando el proyecto en Control Expert es IGUAL al proyecto que hay en el PAC:

<b>Gestión de contraseñas</b>	
Cuando haya transcurrido el tiempo del bloqueo automático, se abrirá el cuadro de diálogo <b>Contraseña de la aplicación</b> :	
Introduzca la contraseña.	
Haga clic en <b>Aceptar</b> .	Si la contraseña es correcta, Control Expert se volverá a activar.
	Si la contraseña es incorrecta, un cuadro de mensaje indica que se ha introducido una contraseña incorrecta y se abre un nuevo cuadro de diálogo <b>Contraseña de la aplicación</b> .
Si hace clic en <b>Cerrar</b> , se cerrará la aplicación sin guardar.	

Acceso a la aplicación en el PAC después de un bloqueo automático, cuando Control Expert está conectado al PAC y cuando el proyecto en Control Expert es DIFERENTE de la aplicación que hay en el PAC:

<b>Gestión de contraseñas</b>	
Si, durante la conexión, la aplicación del software Control Expert y la aplicación CPU no son iguales, se abrirá el cuadro de diálogo <b>Contraseña de la aplicación</b> :	
Introduzca la contraseña.	
Haga clic en <b>Aceptar</b> .	Si la contraseña es correcta, se establecerá la conexión.
	Si la contraseña es incorrecta, un cuadro de mensaje indica que se ha introducido una contraseña incorrecta y se abre un nuevo cuadro de diálogo <b>Contraseña de la aplicación</b> .

<b>Gestión de contraseñas</b>
Si hace clic en <b>Cancelar</b> , no se establecerá la conexión.
<b>NOTA:</b> Si, durante la conexión, la aplicación del software Control Expert y las aplicaciones CPU son iguales, no se solicita contraseña. Si no se ha introducido una contraseña en primer lugar (se ha dejado en blanco en la creación del proyecto), haga clic en <b>Aceptar</b> para establecer la conexión en la pantalla de contraseña.

**NOTA:** Después de tres intentos en los que haya introducido una contraseña incorrecta, deberá esperar durante un tiempo, que será cada vez mayor entre cada intento posterior de introducir la contraseña. El tiempo de espera aumenta de 15 segundos a 1 hora, con un incremento del tiempo de espera de un factor de 2 tras cada intento sucesivo con una contraseña incorrecta.

**NOTA:** En caso de pérdida de la contraseña, consulte el procedimiento descrito en el capítulo *Pérdida de la contraseña*, página 327.

## Habilitación de la opción de cifrado de archivos

**NOTA:** Debe establecer una contraseña de aplicación antes de habilitar el cifrado de archivos.

Procedimiento para habilitar la opción de cifrado de archivos:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de proyecto y controlador</b> .
4	Marque la casilla de verificación <b>Cifrado de archivos activo</b> . <b>Resultado:</b> aparece la ventana <b>Crear contraseña</b> .
5	Introduzca la contraseña en el campo <b>Entrada</b> .
6	Introducir la confirmación de la contraseña en el campo <b>Confirmación</b> .
7	Hacer clic en <b>Aceptar</b> para confirmar.
8	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Desactivación de la opción de cifrado de archivos

Procedimiento para deshabilitar la opción de cifrado de archivos:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de proyecto y controlador</b> .
4	Anule la selección de la casilla de verificación <b>Cifrado de archivos activo</b> . <b>Resultado:</b> aparece la ventana <b>Contraseña de cifrado de archivos</b> .
5	Introduzca la contraseña y haga clic en <b>Aceptar</b> para confirmar. <b>NOTA:</b> La aplicación ya no está cifrada.
6	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Modificación de la contraseña de cifrado de archivos

Procedimiento para cambiar la contraseña de cifrado de archivos:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de proyecto y controlador</b> .
4	En el campo <b>Cifrado de archivos</b> , haga clic en <b>Cambiar contraseña....</b> <b>Resultado:</b> aparece la ventana <b>Modificar contraseña</b> .
5	Introduzca la contraseña anterior en el campo <b>Contraseña anterior</b> .
6	Introducir la nueva contraseña en el campo <b>Entrada</b> .
7	Introducir la confirmación de la nueva contraseña en el campo <b>Confirmación</b> .

Paso	Acción
8	Hacer clic en <b>Aceptar</b> para confirmar.
9	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Borrado de la contraseña de cifrado de archivos

Procedimiento para borrar la contraseña de cifrado de archivos:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable.  <b>Resultado:</b> aparece la ventana <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de proyecto y controlador</b> .
4	En el campo <b>Cifrado de archivos</b> , haga clic en <b>Borrar contraseña....</b>  <b>Resultado:</b> aparece la ventana <b>Contraseña</b> .
5	Introduzca la contraseña en el campo <b>Contraseña</b> .
6	Hacer clic en <b>Aceptar</b> para confirmar.
7	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

**NOTA:** En caso de pérdida de la contraseña de cifrado de archivos, consulte el procedimiento descrito en el capítulo *Pérdida de la contraseña*, página 327.

## Reglas de compatibilidad

Los archivos de aplicación cifrados (.STA y .ZEF) no se pueden abrir en Control Expert 15.0 Classic ni en versiones anteriores, y los archivos cifrados (.ZEF) no se pueden importar en Control Expert con el Administrador de topología.

Las reglas de compatibilidad entre la versión de la aplicación y la versión de Control Expert/Unity Pro se aplican a los archivos .ZEF exportados sin opción de cifrado.

**NOTA:** Cuando la opción de cifrado de archivos del proyecto está habilitada, los archivos de aplicación archivados (.STA) no se pueden guardar sin cifrado.

## Protección mediante contraseña de área segura

### Presentación

Las CPU de seguridad incluyen una función de protección de contraseña de área segura a la que se puede acceder desde la pantalla **Propiedades** del proyecto. Esta función se utiliza para ayudar a proteger los elementos que se encuentran en el área segura del proyecto de seguridad.

**NOTA:** Cuando la función de protección de contraseña de área segura está activa, no se pueden modificar las partes seguras de la aplicación.

No se permiten modificaciones en las siguientes partes del área segura cuando la protección de la contraseña del área segura está habilitada:

Parte segura	Acción prohibida (offline y online)
Configuración	Modificar las características de la CPU
	Añadir, eliminar y modificar un módulo de seguridad en el bastidor
	Modificar la alimentación de seguridad
Tipos	Crear, eliminar y modificar un DDT seguro
	Cambiar un atributo de DDT: de no seguro->seguro
	Cambiar un atributo de DDT: de seguro->no seguro
	Crear, eliminar y modificar un DFB seguro
	Cambiar un atributo de DFB: de no seguro->seguro
	Cambiar un atributo de DFB: de seguro->no seguro
Programa SAFE	Cualquier cambio realizado en el nodo <b>Variables e instancias FB</b>
	Crear tarea
	Importar tarea
	Modificar tarea
	Crear sección
	Eliminar sección
	Importar sección
	Modificar sección

Parte segura	Acción prohibida (offline y online)
Ajustes del proyecto	Modificar ajustes del proyecto SAFE
	Modificar ajustes del proyecto COMMON

## Cifrado

La contraseña del área segura utiliza el cifrado estándar SHA-256 con una sal.

## Comparación entre la función de contraseña de área segura y los derechos de usuario de proyecto de seguridad

La activación de la contraseña de área segura y la implementación de derechos del usuario creados en el **Editor de seguridad** son funciones de seguridad que se excluyen mutuamente, de la forma siguiente:

- Si se ha asignado un perfil de usuario al usuario que inicia Control Expert, este podrá acceder a las áreas seguras de la aplicación de seguridad si el usuario conoce la contraseña del área segura y se le han concedido derechos de acceso en el **Editor de seguridad**.
- En el caso de que no se hayan asignado perfiles de usuario, el usuario podrá acceder a las áreas seguras de la aplicación de seguridad si sabe la contraseña de área segura.

## Indicadores visuales en Control Expert

El estado de la función de protección de área segura se puede detectar visualizando el nodo **Programa SAFE** en el **Explorador de proyectos**:

- Un candado cerrado indica que se ha creado y activado una contraseña de área segura.
- Un candado abierto indica que se ha creado una contraseña de área segura pero que no se ha activado.
- Si no hay ningún candado, indica que no se ha creado una contraseña de área segura.

**NOTA:** Si se ha creado la contraseña de área segura, pero no se ha activado, y se cierra la aplicación de seguridad para volverla a abrir posteriormente, la contraseña de área segura se activa automáticamente cuando se vuelve a abrir la aplicación. Este comportamiento es una medida de precaución si la contraseña de área segura no se ha reactivado de forma involuntaria.

## Compatibilidad

La función de contraseña de área segura está disponible en Control Expert V14.0 o posterior para las CPU de seguridad M580 con una versión del firmware 2.80 o posterior.

### NOTA:

- Los archivos `.STU`, `.STA` y `.ZEF` del programa de aplicación, que se crean en Control Expert V14.0 o versiones posteriores, no podrán abrirse en Unity Pro V13.1 o versiones anteriores.
- La sustitución de una CPU de seguridad M580 en una aplicación Control Expert V14.0, produce el efecto siguiente:
  - Al actualizar de la versión 2.70 a la 2.80 (o posterior) del firmware, se añade la funcionalidad de contraseña de área segura a la ficha **Protección de programa y Safety** de la ventana **Propiedades > de proyecto**.
  - Al regresar de la versión 2.80 (o posterior) a la 2.70 del firmware, se elimina la funcionalidad de contraseña de área segura.

## Activación de la protección y creación de contraseñas

Procedimiento para activar la protección de las secciones y crear una contraseña:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana de <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de programa y seguridad</b> .
4	En el área <b>Seguridad</b> , active la protección seleccionando la casilla <b>Protección activa</b> . <b>Resultado:</b> Aparece el cuadro de diálogo <b>Modificar contraseña</b> .
5	Introduzca una contraseña en el campo <b>Entrada</b> .
6	Introducir la confirmación de la contraseña en el campo <b>Confirmación</b> .
7	Hacer clic en <b>Aceptar</b> para confirmar.
8	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Cambio de contraseña

Procedimiento para cambiar la contraseña de protección de las secciones del proyecto:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana de <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de programa y seguridad</b> .
4	En el área <b>Seguridad</b> , haga clic en <b>Cambiar contraseña ....</b> <b>Resultado:</b> aparece el cuadro de diálogo <b>Modificar contraseña</b> .
5	Introduzca la contraseña anterior en el campo <b>Contraseña anterior</b> .
6	Introducir la nueva contraseña en el campo <b>Entrada</b> .
7	Introducir la confirmación de la nueva contraseña en el campo <b>Confirmación</b> .
8	Hacer clic en <b>Aceptar</b> para confirmar.
9	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios. Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Eliminación de la contraseña

Procedimiento para eliminar la contraseña de protección de las secciones del proyecto:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana de <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de programa y seguridad</b> .
4	En el área <b>Seguridad</b> , haga clic en <b>Borrar contraseña...</b> <b>Resultado:</b> aparece el cuadro de diálogo <b>Control de acceso</b> .
5	Introducir la contraseña anterior en el campo <b>Contraseña</b> .

Paso	Acción
6	Hacer clic en <b>Aceptar</b> para confirmar.
7	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Protección de unidad de programa, sección y subrutina

### Presentación

Puede accederse a la función de protección desde la pantalla **Propiedades** del proyecto en modalidad offline.

Esta función se utiliza para proteger los elementos de programa (secciones, unidades de programa).

**NOTA:** La protección no estará activa mientras que no se active en el proyecto.

**NOTA:** La protección del proyecto sólo se aplicará a los elementos de programa señalados. Esto no impedirá:

- Conexión a la CPU
- La carga de la aplicación desde la CPU
- Cambiar la configuración
- Adición de nuevas unidades de programa o secciones
- Cambiar la lógica en una nueva sección (no protegida)

### Activación de la protección y creación de contraseñas

Procedimiento para activar la protección y crear la contraseña para secciones y unidades de programa:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable.  <b>Resultado:</b> aparece la ventana de <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de programa y Safety</b> .

Paso	Acción
4	En el campo <b>Secciones y unidades de programa</b> , active la protección seleccionando la casilla <b>Protección activa</b> .  <b>Resultado:</b> aparece el cuadro de diálogo <b>Modificar contraseña</b> .
5	Introduzca una contraseña en el campo <b>Entrada</b> .
6	Introducir la confirmación de la contraseña en el campo <b>Confirmación</b> .
7	Seleccione la casilla de verificación <b>Cifrado</b> si necesita una contraseña con mayor protección.  <b>NOTA:</b> Los proyectos que tengan una contraseña cifrada no podrán editarse con Unity Pro V4.0 o versiones anteriores.
8	Hacer clic en <b>Aceptar</b> para confirmar.
9	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Notas

Si se configura un elemento de programa con protección (lectura o lectura/escritura) cuando se haya activado la protección, se indicará mediante un candado cerrado en el elemento de programa.

Si el elemento de programa se configura con protección, pero esta protección está desactivada, aparecerá un candado abierto en el elemento de programa.

## Cambio de contraseña

Procedimiento para cambiar la contraseña de protección del proyecto para secciones y unidades de programa:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable.  <b>Resultado:</b> aparece la ventana de <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de programa y Safety</b> .
4	En el campo <b>Secciones y unidades de programa</b> , haga clic en <b>Cambiar contraseña...</b>  <b>Resultado:</b> aparece el cuadro de diálogo <b>Modificar contraseña</b> .
5	Introduzca la contraseña anterior en el campo <b>Contraseña anterior</b> .

Paso	Acción
6	Introducir la nueva contraseña en el campo <b>Entrada</b> .
7	Introducir la confirmación de la nueva contraseña en el campo <b>Confirmación</b> .
8	<p>Seleccione la casilla de verificación <b>Cifrado</b> si necesita una contraseña con mayor protección.</p> <p><b>NOTA:</b> Los proyectos que tengan una contraseña cifrada no podrán editarse con Unity Pro V4.0 o versiones anteriores.</p> <p>Unity Pro es el nombre anterior de Control Expert para la versión 13.1 o anterior.</p>
9	Hacer clic en <b>Aceptar</b> para confirmar.
10	<p>Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.</p> <p>Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b>, se cancelarán todos los cambios.</p>

## Eliminación de la contraseña

Procedimiento para eliminar la contraseña de protección del proyecto para secciones y unidades de programa:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	<p>Seleccione el comando <b>Propiedades</b> en el menú desplegable.</p> <p><b>Resultado:</b> aparece la ventana de <b>Propiedades del proyecto</b>.</p>
3	Seleccione la ficha <b>Protección de programa y Safety</b> .
4	<p>En el campo <b>Secciones y unidades de programa</b>, haga clic en <b>Borrar contraseña...</b></p> <p><b>Resultado:</b> aparece el cuadro de diálogo <b>Control de acceso</b>.</p>
5	Introducir la contraseña anterior en el campo <b>Contraseña</b> .
6	Hacer clic en <b>Aceptar</b> para confirmar.
7	<p>Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.</p> <p>Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b>, se cancelarán todos los cambios.</p>

# Protección de firmware

## Descripción general

La protección del firmware mediante una contraseña ayuda a impedir los accesos no deseados al firmware del módulo.

## Contraseña

La contraseña distingue entre mayúsculas y minúsculas y debe tener entre 8 y 16 caracteres alfanuméricos. La solidez de una contraseña es mayor si contiene una combinación de mayúsculas y minúsculas y caracteres alfanuméricos, numéricos y especiales.

**NOTA:** Al importar un archivo ZEF, la contraseña del firmware se almacena en el módulo únicamente si se ha seleccionado la opción **Cifrado de archivos**.

## Cambio de la contraseña

Se puede cambiar la contraseña en cualquier momento.

**NOTA:** El valor predeterminado de la contraseña del firmware en la aplicación Control Expert es: `fwdownload`.

- Para el firmware V4.01 y posteriores, debe cambiar el valor predeterminado de la contraseña del firmware; de lo contrario, no será posible generar la aplicación Control Expert.
- Para versiones del firmware anteriores a V4.01, no es obligatorio, pero se recomienda encarecidamente cambiar el valor predeterminado de la contraseña del firmware.

Procedimiento para cambiar la contraseña de protección del firmware:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de proyecto y controlador</b> .
4	En el campo <b>Firmware</b> , haga clic en <b>Cambiar contraseña...</b> <b>Resultado:</b> Aparecerá la ventana <b>Modificar contraseña</b> .
5	Introduzca la contraseña anterior en el campo <b>Contraseña anterior</b> .

Paso	Acción
6	Introducir la nueva contraseña en el campo <b>Entrada</b> .
7	Introducir la confirmación de la nueva contraseña en el campo <b>Confirmación</b> .
8	Hacer clic en <b>Aceptar</b> para confirmar.
9	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Restablecimiento de la contraseña

Al restablecer la contraseña, se asigna su valor predeterminado a la contraseña del firmware en la aplicación Control Expert si se confirma la contraseña actual.

Para restablecer la contraseña:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de proyecto y controlador</b> .
4	En el campo <b>Firmware</b> , haga clic en <b>Restablecer contraseña...</b> <b>Resultado:</b> Aparecerá la ventana <b>Contraseña</b> .
5	Introduzca la contraseña actual en el campo <b>Contraseña</b> .
6	Hacer clic en <b>Aceptar</b> para confirmar.
7	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios. La nueva contraseña es la contraseña predeterminada: <code>fwdownload</code> .  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

# Protección del almacenamiento de datos/web

## Descripción general

La protección con contraseña ayuda a impedir los accesos no deseados al área de almacenamiento de datos de la tarjeta de memoria SD (si hay una tarjeta válida insertada en la CPU).

Para las CPU Modicon M580 en un proyecto creado por Control Expert con la versión:

- Antes de la versión 15.1, puede ofrecer protección con contraseña para el acceso al almacenamiento de datos.
- Con la versión 15.1 o posterior, puede ofrecer protección con contraseña para acceso al diagnóstico web y al almacenamiento de datos.

## Contraseña

La contraseña distingue entre mayúsculas y minúsculas y debe tener entre 8 y 16 caracteres alfanuméricos. La solidez de una contraseña es mayor si contiene una combinación de mayúsculas y minúsculas y caracteres alfanuméricos, numéricos y especiales.

**NOTA:** Al importar un archivo ZEF, la contraseña de almacenamiento de datos/web se almacena en el módulo solo si se ha seleccionado la opción **Cifrado de archivos**.

## Cambio de la contraseña

Se puede cambiar la contraseña en cualquier momento.

**NOTA:** La contraseña de almacenamiento de datos/web tiene un valor predeterminado en la aplicación Control Expert. Este valor predeterminado depende de la versión de Control Expert, y es:

- `datadownload` para versiones de Control Expert anteriores a V15.1;
- `webuser` para Control Expert V15.1 y versiones posteriores.

La modificación de la contraseña predeterminada es obligatoria o no en función de la versión del firmware del módulo:

- Para el firmware V4.01 y posteriores, debe cambiar el valor predeterminado de la contraseña de almacenamiento de datos/web; de lo contrario, no será posible generar la aplicación Control Expert.
- Para versiones de firmware anteriores a V4.01, no es obligatorio, pero se recomienda encarecidamente cambiar el valor predeterminado de la contraseña de almacenamiento de datos/web.

Procedimiento para cambiar la contraseña de almacenamiento de datos/web:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de proyecto y controlador</b> .
4	En el campo <b>Almacenamiento de datos</b> (o <b>Diagnóstico web/Almacenamiento de datos</b> ), haga clic en <b>Cambiar contraseña....</b> <b>Resultado:</b> aparece la ventana <b>Modificar contraseña</b> .
5	Introduzca la contraseña anterior en el campo <b>Contraseña anterior</b> .
6	Introducir la nueva contraseña en el campo <b>Entrada</b> .
7	Introducir la confirmación de la nueva contraseña en el campo <b>Confirmación</b> .
8	Hacer clic en <b>Aceptar</b> para confirmar.
9	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Restablecimiento de la contraseña

Al restablecer la contraseña, se asigna su valor predeterminado a la contraseña de almacenamiento de datos/web en la aplicación Control Expert si se confirma la contraseña actual.

Para restablecer la contraseña:

Paso	Acción
1	En el explorador de proyectos, haga clic con el botón derecho en <b>Proyecto</b> .
2	Seleccione el comando <b>Propiedades</b> en el menú desplegable. <b>Resultado:</b> aparece la ventana <b>Propiedades del proyecto</b> .
3	Seleccione la ficha <b>Protección de proyecto y controlador</b> .
4	En el campo <b>Almacenamiento de datos</b> (o <b>Diagnóstico web/Almacenamiento de datos</b> ), haga clic en <b>Restablecer contraseña....</b> <b>Resultado:</b> aparece la ventana <b>Contraseña</b> .
5	Introduzca la contraseña actual en el campo <b>Contraseña</b> .

Paso	Acción
6	Hacer clic en <b>Aceptar</b> para confirmar.
7	Haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana de <b>Propiedades del proyecto</b> para confirmar todos los cambios. La nueva contraseña es la contraseña predeterminada: <code>datadownload</code> .  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Pérdida de la contraseña

### Descripción general

Si ha olvidado su contraseña, proceda como se indica en los pasos siguientes y póngase en contacto con el servicio técnico de Schneider Electric.

**NOTA:** El procedimiento de recuperación de la contraseña de la aplicación varía según si la opción de cifrado de archivos está habilitada o deshabilitada.

### Contraseña de la aplicación Control Expert sin opción de cifrado de archivos

El siguiente procedimiento para restablecer la contraseña de la aplicación es válido cuando la opción de cifrado de archivos está deshabilitada, o para el archivo de aplicación administrado con Control Expert 15.0 Classic o versiones anteriores.

El servicio técnico de Schneider Electric necesitará una cadena de caracteres alfanuméricos que se mostrarán en la ventana emergente **Contraseña olvidada** al pulsar **SHIFT+F2** en el cuadro de diálogo **Contraseña**.

Para acceder al cuadro de diálogo **Contraseña**, se deben cumplir las siguientes condiciones:

- Durante el tiempo de apertura, seleccione la aplicación y se mostrará el cuadro de diálogo **Contraseña**.
- Durante el tiempo de bloqueo automático, se mostrará el cuadro de diálogo **Contraseña**. Si no recuerda la contraseña, seleccione **Cerrar**. Abra de nuevo la aplicación y se mostrará el cuadro de diálogo **Contraseña**.

**NOTA:** Si cierra la aplicación sin introducir una contraseña después del bloqueo automático, se perderán todas las modificaciones.

Procedimiento para resetear la contraseña de la aplicación:

Paso	Acción
1	<b>Condición:</b> Aparece el cuadro de diálogo <b>Contraseña</b> .
2	Pulse <b>SHIFT+F2</b> .  <b>Resultado:</b> Se abrirá la ventana emergente <b>Contraseña olvidada</b> y se mostrará una cadena de caracteres alfanuméricos.
3	Copie esta cadena y facilítesela al servicio técnico de Schneider Electric.
4	Recibirá la nueva contraseña generada por el servicio técnico de Schneider Electric.  <b>NOTA:</b> La contraseña es temporal y estará disponible siempre y cuando no modifique la aplicación.
5	Introduzca la contraseña.
6	Modifique la contraseña (contraseña anterior = contraseña proporcionada por el servicio técnico de Schneider Electric).
7	Haga clic en <b>Generar &gt; Generar cambios</b> .
8	Seleccione <b>Guardar</b> la aplicación.

## Contraseña de la aplicación Control Expert con opción de cifrado de archivos

Si olvida la contraseña de la aplicación con el cifrado de archivos habilitado, deberá enviar el archivo de aplicación al servicio técnico de Schneider Electric. A continuación, recibirá el archivo de aplicación cifrado con una nueva contraseña de aplicación de archivos del servicio técnico de Schneider Electric.

**NOTA:** Se recomienda encarecidamente cambiar la contraseña de la aplicación.

## Contraseña de la aplicación de la CPU

Procedimiento para resetear la contraseña de la aplicación de la CPU si se dispone del archivo \*.STU correspondiente:

Paso	Acción
1	Abra el archivo *.STU correspondiente.
2	Cuando aparezca el cuadro de diálogo <b>Contraseña</b> , pulse <b>SHIFT+F2</b> .  <b>Resultado:</b> Se abrirá la ventana emergente <b>Contraseña olvidada</b> y se mostrará una cadena de caracteres alfanuméricos.
3	Copie esta cadena y facilítesela al servicio técnico de Schneider Electric.
4	Recibirá la nueva contraseña generada por el servicio técnico de Schneider Electric.

Paso	Acción
	<b>Nota:</b> La contraseña es temporal y estará disponible siempre y cuando no modifique la aplicación.
5	Introduzca la contraseña.
6	Modifique la contraseña (contraseña anterior = contraseña proporcionada por el servicio técnico de Schneider Electric).
7	Seleccione <b>Conectar</b> al PLC.
8	Haga clic en <b>Generar &gt; Generar cambios</b> .
9	Seleccione <b>Guardar</b> la aplicación.

Procedimiento para resetear la contraseña de la aplicación de la CPU si no se dispone del archivo \*.STU correspondiente:

Paso	Acción
1	<b>Condición:</b> Durante la conexión, aparece el cuadro de diálogo <b>Contraseña</b> .
2	Pulse <b>SHIFT+F2</b> .  <b>Resultado:</b> Se abrirá la ventana emergente <b>Contraseña olvidada</b> y se mostrará una cadena de caracteres alfanuméricos.
3	Copie esta cadena y facilítesela al servicio técnico de Schneider Electric.
4	Recibirá la nueva contraseña generada por el servicio técnico de Schneider Electric.  <b>Nota:</b> La contraseña proporcionada por el servicio técnico de Schneider Electric es temporal y estará disponible siempre y cuando no modifique la aplicación.
5	Introduzca la contraseña.
6	Cargue la aplicación desde la CPU.
7	Seleccione <b>Guardar</b> la aplicación.
8	Modifique la contraseña (contraseña anterior = la proporcionada por el servicio técnico de Schneider Electric).
9	Haga clic en <b>Generar &gt; Generar cambios</b> .
10	Seleccione <b>Guardar</b> la aplicación.

## Contraseña de cifrado de archivos

El servicio técnico de Schneider Electric necesitará una cadena de caracteres alfanuméricos que se mostrarán en la ventana emergente **Contraseña olvidada** al pulsar **SHIFT+F2** en el cuadro de diálogo **Contraseña**.

Para acceder al cuadro de diálogo **Contraseña**:

- Vaya a **Proyecto > Propiedades del proyecto > Protección de proyecto y controlador**
- En el campo **Cifrado de archivos**, haga clic en **Borrar contraseña....** Aparece el cuadro de diálogo **Contraseña**.

Procedimiento para restablecer la contraseña de cifrado de archivos:

Paso	Acción
1	<b>Condición:</b> Aparece el cuadro de diálogo <b>Contraseña</b> .
2	Pulse <b>SHIFT+F2</b> .  <b>Resultado:</b> Se abrirá la ventana emergente <b>Contraseña olvidada</b> y se mostrará una cadena de caracteres alfanuméricos.
3	Copie esta cadena y facilítesela al servicio técnico de Schneider Electric.
4	Recibirá la nueva contraseña generada por el servicio técnico de Schneider Electric.  <b>Nota:</b> La contraseña es temporal y estará disponible siempre y cuando no modifique la aplicación.
5	Introduzca esta contraseña y haga clic en <b>Aceptar</b> para cerrar el cuadro de diálogo <b>Contraseña</b> .
6	Haga clic en <b>Modificar contraseña</b> y cambie la contraseña (la contraseña anterior equivaldrá a la contraseña proporcionada por el servicio técnico de Schneider Electric).
7	Haga clic en <b>Aceptar</b> para cerrar el cuadro de diálogo <b>Modificar contraseña</b> y luego haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Contraseña de área segura

El servicio técnico de Schneider Electric necesitará una cadena de caracteres alfanuméricos que se mostrarán en la ventana emergente **Contraseña olvidada** al pulsar **SHIFT+F2** en el cuadro de diálogo **Contraseña**.

Para acceder al cuadro de diálogo **Contraseña**:

- Vaya al **Proyecto > Propiedades del proyecto > Protección de programa y Safety**
- En el campo **Safety**, haga clic en **Cambiar contraseña....** Aparece el cuadro de diálogo **Contraseña**.

Procedimiento para restablecer la contraseña de área segura:

Paso	Acción
1	<b>Condición:</b> Aparece el cuadro de diálogo <b>Contraseña</b> .
2	Pulse <b>SHIFT+F2</b> .

Paso	Acción
	<b>Resultado:</b> Se abrirá la ventana emergente <b>Contraseña olvidada</b> y se mostrará una cadena de caracteres alfanuméricos.
3	Copie esta cadena y facilítesela al servicio técnico de Schneider Electric.
4	Recibirá la nueva contraseña generada por el servicio técnico de Schneider Electric. <b>Nota:</b> La contraseña es temporal y estará disponible siempre y cuando no modifique la aplicación.
5	Introduzca esta contraseña y haga clic en <b>Aceptar</b> para cerrar el cuadro de diálogo <b>Contraseña</b> .
6	Haga clic en <b>Modificar contraseña</b> y cambie la contraseña (la contraseña anterior equivaldrá a la contraseña proporcionada por el servicio técnico de Schneider Electric).
7	Haga clic en <b>Aceptar</b> para cerrar el cuadro de diálogo <b>Modificar contraseña</b> y luego haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Contraseña del firmware

El servicio técnico de Schneider Electric necesitará una cadena de caracteres alfanuméricos que se mostrarán en la ventana emergente **Contraseña olvidada** al pulsar **SHIFT+F2** en el cuadro de diálogo **Contraseña**.

Para acceder al cuadro de diálogo **Contraseña**:

- Vaya a **Proyecto > Propiedades del proyecto > Protección de proyecto y controlador**
- En el campo **Firmware**, haga clic en **Restablecer contraseña...** Aparece el cuadro de diálogo **Contraseña**.

Procedimiento para restablecer la contraseña del firmware:

Paso	Acción
1	<b>Condición:</b> Aparece el cuadro de diálogo <b>Contraseña</b> .
2	Pulse <b>SHIFT+F2</b> .  <b>Resultado:</b> Se abrirá la ventana emergente <b>Contraseña olvidada</b> y se mostrará una cadena de caracteres alfanuméricos.
3	Copie esta cadena y facilítesela al servicio técnico de Schneider Electric.
4	Recibirá la nueva contraseña generada por el servicio técnico de Schneider Electric. <b>Nota:</b> La contraseña es temporal y estará disponible siempre y cuando no modifique la aplicación.
5	Introduzca esta contraseña y haga clic en <b>Aceptar</b> para cerrar el cuadro de diálogo <b>Contraseña</b> .

Paso	Acción
6	Haga clic en <b>Modificar contraseña</b> y cambie la contraseña (la contraseña anterior equivaldrá a la contraseña proporcionada por el servicio técnico de Schneider Electric).
7	Haga clic en <b>Aceptar</b> para cerrar el cuadro de diálogo <b>Modificar contraseña</b> y luego haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

## Contraseña del almacenamiento de datos/web

El servicio técnico de Schneider Electric necesitará una cadena de caracteres alfanuméricos que se mostrarán en la ventana emergente **Contraseña olvidada** al pulsar **SHIFT+F2** en el cuadro de diálogo **Contraseña**.

Para acceder al cuadro de diálogo **Contraseña**:

- Vaya a **Proyecto > Propiedades del proyecto > Protección de proyecto y controlador**
- En el campo **Almacenamiento de datos**, haga clic en **Restablecer contraseña...**  
Aparece el cuadro de diálogo **Contraseña**.

Procedimiento para restablecer la contraseña del almacenamiento de datos:

Paso	Acción
1	<b>Condición:</b> Aparece el cuadro de diálogo <b>Contraseña</b> .
2	Pulse <b>SHIFT+F2</b> .  <b>Resultado:</b> Se abrirá la ventana emergente <b>Contraseña olvidada</b> y se mostrará una cadena de caracteres alfanuméricos.
3	Copie esta cadena y facilítesela al servicio técnico de Schneider Electric.
4	Recibirá la nueva contraseña generada por el servicio técnico de Schneider Electric.  <b>Nota:</b> La contraseña es temporal y estará disponible siempre y cuando no modifique la aplicación.
5	Introduzca esta contraseña y haga clic en <b>Aceptar</b> para cerrar el cuadro de diálogo <b>Contraseña</b> .
6	Haga clic en <b>Modificar contraseña</b> y cambie la contraseña (la contraseña anterior equivaldrá a la contraseña proporcionada por el servicio técnico de Schneider Electric).
7	Haga clic en <b>Aceptar</b> para cerrar el cuadro de diálogo <b>Modificar contraseña</b> y luego haga clic en <b>Aceptar</b> o <b>Aplicar</b> en la ventana <b>Propiedades del proyecto</b> para confirmar todos los cambios.  Si hace clic en <b>Cancelar</b> en la ventana de <b>Propiedades del proyecto</b> , se cancelarán todos los cambios.

# Gestión de la seguridad de la estación de trabajo

## Introducción

Schneider Electric proporciona la herramienta de gestión de acceso **Editor de seguridad**, que se puede utilizar para limitar y controlar el acceso a la estación de trabajo en la que está instalado el software Control Expert. En esta sección se describen las funciones de esta herramienta, relacionadas de manera exclusiva con los proyectos de seguridad de M580.

## Gestión del acceso a Control Expert

### Introducción

Schneider Electric proporciona la herramienta de configuración **Editor de seguridad** que permite gestionar el acceso al software Control Expert instalado en una estación de trabajo. El uso de la herramienta de configuración *Editor de seguridad* para gestionar el acceso al software Control Expert es opcional.

**NOTA:** La gestión del acceso está relacionada con el hardware, normalmente una estación de trabajo, en el que está instalado el software Control Expert y no con el proyecto, que tiene su propio sistema de protección.

Para obtener más información, consulte *EcoStruxure™ Control Expert, Editor de seguridad, Guía de funcionamiento*.

**NOTA:** Los perfiles de usuario de seguridad también requieren derechos para acceder a la parte de proceso de la aplicación de seguridad. Al crear o modificar un perfil de usuario, es responsabilidad suya confirmar que se realicen correctamente todas las modificaciones necesarias.

## Categorías de usuarios

El **Editor de seguridad** admite dos categorías de usuarios:

- **Administrador (Supervisor):**

El administrador es la única persona que puede gestionar la seguridad de acceso al software. El administrador especifica quién puede acceder al software y sus derechos de acceso. Durante la instalación de Control Expert en la estación de trabajo, el administrador es el único que puede acceder a la configuración de seguridad sin limitación alguna de sus derechos (sin una contraseña).

**NOTA:** El nombre de usuario reservado al administrador es Supervisor.

- **Usuarios:**

El administrador define los usuarios del software en la lista de usuarios si la seguridad de acceso a Control Expert se encuentra activa. Si su nombre figura en la lista de usuarios, puede acceder a una instancia de software introduciendo su nombre (tal y como aparece en la lista) y su contraseña.

## Perfil de usuario

El perfil de usuario incluye todos los derechos de acceso de un usuario. El perfil de usuario puede definirlo el administrador de manera personalizada o se puede crear aplicando un perfil preconfigurado incluido con la herramienta **Editor de seguridad**.

## Perfiles de usuario preconfigurados

El **Editor de seguridad** ofrece los siguientes perfiles de usuario preconfigurados, que se aplican al programa de seguridad o al programa de proceso:

Perfil	Tipo de programa aplicable		Descripción
	Proceso	Seguridad	
<b>Sólo lectura</b>	✓	✓	El usuario sólo puede acceder al proyecto en modalidad de lectura, a excepción de la dirección del PAC, que puede modificarse. También puede copiar o descargar el proyecto.
<b>Funcionamiento</b>	✓	–	El usuario tiene los mismos derechos que con un perfil <b>Sólo lectura</b> , con la posibilidad adicional de modificar parámetros de ejecución del programa de proceso (constantes, valores iniciales, tiempos de ciclo de tareas, etc.).
<b>Seguridad_ Funcionamiento</b>	–	✓	El usuario tiene derechos similares a los del perfil <b>Funcionamiento</b> , salvo en lo que respecta al programa de seguridad y estas otras excepciones: <ul style="list-style-type: none"> <li>• No se permite la transferencia de valores de datos al PAC.</li> <li>• Se permite ordenar al programa de seguridad que entre en modalidad de mantenimiento.</li> </ul>
<b>Ajuste</b>	✓	–	El usuario tiene los mismos derechos que con un perfil <b>Funcionamiento</b> , con la posibilidad adicional de cargar un proyecto (transferirlo al PAC) y modificar la modalidad de funcionamiento del PAC ( <b>Ejecutar, Detener...</b> ).
<b>Seguridad_Ajuste</b>	–	✓	El usuario tiene derechos similares que con el perfil <b>Ajuste</b> , pero con respecto al programa de seguridad, a excepción de que:

Perfil	Tipo de programa aplicable		Descripción
	Proceso	Seguridad	
			<ul style="list-style-type: none"> <li>No se permite la transferencia de valores de datos al PAC.</li> <li>Se permite ordenar al programa de seguridad que entre en modalidad de mantenimiento.</li> </ul>
<b>Depuración</b>	✓	–	El usuario tiene los mismos derecho que con un perfil <b>Ajuste</b> , con la posibilidad adicional de utilizar las herramientas de depuración.
<b>Seguridad_ Depuración</b>	–	✓	El usuario tiene derechos similares que con el perfil <b>Depuración</b> , pero con respecto al programa de seguridad, a excepción de que: <ul style="list-style-type: none"> <li>No se permite detener o iniciar el programa.</li> <li>No se permite la actualización de valores de inicialización.</li> <li>No se permite la transferencia de valores de datos al PAC.</li> <li>No se permite forzar entradas, salidas o bits internos.</li> <li>Se permite ordenar al programa de seguridad que entre en modalidad de mantenimiento.</li> </ul>
<b>Programa</b>	✓	–	El usuario tiene los mismos derechos que con un perfil <b>Depuración</b> , con la posibilidad adicional de modificar el programa.
<b>Seguridad_ Programa</b>	–	✓	El usuario tiene derechos similares que con el perfil <b>Programa</b> , pero con respecto al programa de seguridad, a excepción de que: <ul style="list-style-type: none"> <li>No se permite detener o iniciar el programa.</li> <li>No se permite la actualización de valores de inicialización.</li> <li>No se permite la transferencia de valores de datos al PAC.</li> <li>No se permite restaurar el proyecto al PAC desde una copia de seguridad guardada.</li> <li>No se permite forzar entradas, salidas o bits internos.</li> <li>Se permite ordenar al programa de seguridad que entre en modalidad de mantenimiento.</li> </ul>
<b>Deshabilitado</b>	✓	✓	El usuario no puede acceder al proyecto.

## Asignación de un usuario preconfigurado

El administrador puede asignar un usuario preconfigurado, derivado de un perfil preconfigurado, a un usuario específico en la ficha **Usuarios** del **Editor de seguridad**. Están disponibles las siguientes selecciones de usuarios preconfigurados:

- seguridad\_usuario\_Ajuste
- seguridad\_usuario\_Depuración
- seguridad\_usuario\_Funcionamiento
- seguridad\_usuario\_Programa
- usuario\_Ajuste
- usuario\_Depuración
- usuario\_Funcionamiento
- usuario\_Programa

Consulte el tema *Funciones de usuario* (véase EcoStruxure™ Control Expert, Editor de seguridad, Guía de funcionamiento) para obtener más información sobre cómo puede asignar un administrador un perfil preconfigurado a un usuario.

## Derechos de acceso

### Introducción

Los derechos de acceso de Control Expert se clasifican según las siguientes categorías:

- servicios de proyecto
- ajuste/depuración
- librerías
- modificación global
- modificación elemental de una variable
- modificación elemental de datos compuestos DDT
- modificación elemental de un tipo de DFB
- modificación elemental de una instancia de DFB
- editor de configuración del bus
- editor de configuración de entrada/salida
- pantallas de ejecución
- ciberseguridad
- seguridad

Este tema presenta los derechos de acceso disponibles para cada uno de los perfiles de usuario preconfigurados.

## Servicios de proyecto

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Crear nuevo proyecto	-	-	-	-	-	-	✓	✓
Abrir proyecto existente	✓	✓	✓	✓	✓	✓	✓	✓
Guardar proyecto	-	-	-	-	-	-	✓	✓
Guardar como proyecto	✓	✓	✓	✓	✓	✓	✓	✓
Importar proyecto	-	-	-	-	-	-	✓	✓
Generar fuera de línea	-	-	-	-	-	-	✓	✓
Generar en línea en modalidad DETENER	-	-	-	-	-	-	✓	✓
Generar en línea en modalidad EJECUTAR	-	-	-	-	-	-	✓	✓
Iniciar, detener o inicializar el PAC*	✓	-	✓	-	-	-	✓	✓
Actualizar los valores de inicialización con los valores actuales (sólo datos no seguros)	-	-	✓	-	-	-	✓	✓
Transferir proyecto desde el PAC	✓	✓	✓	✓	✓	✓	✓	✓
Transferir proyecto al PAC	✓	✓	✓	✓	-	-	✓	✓
Transferir valores de datos de un archivo al PAC (sólo datos no seguros)	✓	-	✓	-	✓	-	✓	✓
Restablecer copia de seguridad de proyecto en el PAC	-	-	-	-	-	-	✓	✓

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Guardar en copia de seguridad del proyecto en el PAC	–	–	–	–	–	–	✓	✓
Establecer dirección	✓	✓	✓	✓	✓	✓	✓	✓
Opciones de modificación	✓	✓	✓	✓	✓	✓	✓	✓
<p>* Sólo se inician o se detienen las tareas de proceso. En el caso de un PAC que no sea de seguridad, esto significa que el PAC se inicia o se detiene. En el caso de un PAC de seguridad M580, esto significa que se inician o se detienen todas las tareas a excepción de la tarea SAFE.</p> <p>✓ : Incluido</p> <p>– : No incluido</p>								

## Ajuste/depuración

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Modificar valores de variable	✓	–	✓		✓		✓	✓
Modificar valores de variables de seguridad	–	✓	–	✓	–	✓	–	✓
Forzar bits internos	–	–	✓	–	–	–	✓	✓
Forzar salidas	–	–	✓	–	–	–	✓	✓
Forzar entradas	–	–	✓	–	–	–	✓	✓
Gestión de tareas	–	–	✓	–	–	–	✓	✓
Gestión de tareas SAFE	–	–	–	✓	–	–	–	✓
Modificación del tiempo de ciclo de tarea	✓	–	✓		✓	–	✓	✓

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Modificación del tiempo de ciclo de tareas SAFE	–	✓	–	✓	–	✓	–	✓
Suprimir mensaje en el visualizador	✓	✓	✓	✓	✓	✓	✓	✓
Depurar ejecutable	–	–	✓	✓	–	–	✓	✓
Reemplazar una variable de proyecto	–	–	–	–	–	–	✓	✓
Sustitución de una variable de proyecto de seguridad	–	–	–	–	–	–	–	✓
✓ : Incluido – : No incluido								

## Librerías

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Crear librerías o familias	–	–	–	–	–	–	✓	✓
Crear familias o bibliotecas de seguridad	–	–	–	–	–	–	–	✓
Eliminar librerías o familias	–	–	–	–	–	–	✓	✓
Eliminar familias o bibliotecas de seguridad	–	–	–	–	–	–	–	✓
Colocar objeto en la librería	–	–	–	–	–	–	✓	✓
Colocar un objeto en la biblioteca de seguridad	–	–	–	–	–	–	–	✓

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Eliminar un objeto de una librería	-	-	-	-	-	-	✓	✓
Eliminar un objeto de la biblioteca de seguridad	-	-	-	-	-	-	-	✓
Obtener un objeto de una librería	-	-	-	-	-	-	✓	✓
Obtener un objeto de la biblioteca de seguridad	-	-	-	-	-	-	-	✓
✓ : Incluido - : No incluido								

## Modificación global

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Modificar la documentación	✓	✓	✓	✓	✓	✓	✓	✓
Modificar la vista funcional	-	-	-	-	-	-	✓	✓
Modificar tablas de animación	✓	✓	✓	✓	✓	✓	✓	✓
Modificar valor de constantes	✓	-	✓	-	✓	-	✓	✓
Modificar valor de constantes de seguridad	-	✓	-	✓	-	✓	-	✓
Modificar estructura del programa	-	-	-	-	-	-	✓	✓
Modificar estructura del programa de seguridad	-	-	-	-	-	-	-	✓

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Modificar secciones de programa	-	-	-	-	-	-	✓	✓
Modificar secciones del programa de seguridad	-	-	-	-	-	-	-	✓
Modificar ajustes del proyecto	-	-	-	-	-	-	✓	✓
✓ : Incluido - : No incluido								

## Modificación elemental de una variable

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Agregar/eliminar variable	-	-	-	-	-	-	✓	✓
Añadir/eliminar variables de seguridad	-	-	-	-	-	-	-	✓
Modificaciones de atributos principales de variable	-	-	-	-	-	-	✓	✓
Modificaciones de atributos principales de variables de seguridad	-	-	-	-	-	-	-	✓
Modificaciones de atributos secundarios de variable	✓	-	✓	-	✓	-	✓	✓
Modificaciones de atributos secundarios de variables de seguridad	-	✓	-	✓	-	✓	-	✓
✓ : Incluido - : No incluido								

## Modificación elemental de datos compuestos DDT

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Agregar/eliminar DDT	-	-	-	-	-	-	✓	✓
Modificaciones de DDT	-	-	-	-	-	-	✓	✓
✓ : Incluido - : No incluido								

## Modificación elemental de un tipo de DFB

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Agregar/eliminar tipo de DFB	-	-	-	-	-	-	✓	✓
Añadir/eliminar tipo DFB de seguridad	-	-	-	-	-	-	-	✓
Modificación de estructura de tipo de DFB	-	-	-	-	-	-	✓	✓
Modificación de estructura del tipo DFB de seguridad	-	-	-	-	-	-	-	✓
Modificación de secciones tipo de DFB	-	-	-	-	-	-	✓	✓

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Modificación de secciones del tipo DFB de seguridad	-	-	-	-	-	-	-	✓
✓ : Incluido - : No incluido								

## Modificación elemental de una instancia de DFB

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Modificación de instancia de DFB	-	-	-	-	-	-	✓	✓
Modificación de instancia de DFB de seguridad	-	-	-	-	-	-	-	✓
Modificación de atributos secundarios de instancia DFB	✓	-	✓	-	✓	-	✓	✓
Modificación de atributos secundarios de instancia de DFB de seguridad	-	✓	-	✓	-	✓	-	✓
✓ : Incluido - : No incluido								

## Editor de configuración del bus

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Modificar la configuración	-	-	-	-	-	-	✓	✓
Modificar la configuración de seguridad	-	-	-	-	-	-	-	✓
Vigilancia de E/S	-	-	-	-	-	-	✓	✓
✓ : Incluido - : No incluido								

## Editor de configuración de entrada/salida

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Modificar la configuración de E/S	-	-	-	-	-	-	✓	✓
Modificar configuración de E/S de seguridad	-	-	-	-	-	-	-	✓
Ajustar la E/S	✓	-	✓	-	✓	-	✓	✓
Ajustar E/S de seguridad	-	✓	-	✓	-	✓	-	✓
Save_param	-	-	✓	-	-	-	✓	✓
Restore_param	-	-	✓	-	-	-	✓	✓
✓ : Incluido - : No incluido								

## Pantallas de ejecución

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Modificar pantallas	–	–	–	–	–	–	✓	✓
Modificar mensajes	–	–	–	–	–	–	✓	✓
Agregar/eliminar pantallas o familias	–	–	–	–	–	–	✓	✓
✓ : Incluido – : No incluido								

## Ciberseguridad

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
Crear o modificar contraseña de la aplicación	–	–	–	–	–	–	✓	✓
Entrar en modalidad de mantenimiento	–	✓	–	✓	–	✓	–	✓
Adaptar tiempo de espera de bloqueo automático	✓	✓	✓	✓	✓	✓	✓	✓
✓ : Incluido – : No incluido								

## Seguridad

Los derechos de acceso de esta categoría son los siguientes:

Derecho de acceso	Perfil de usuario preconfigurado							
	Ajuste	Seguridad_Ajuste	Depuración	Seguridad_Depuración	Funcionamiento	Seguridad_Funcionamiento	Programa	Seguridad_Programa
<b>Entrar en modalidad de mantenimiento</b>	–	✓	–	✓	–	✓	–	✓
✓ : Incluido – : No incluido								

# Modificaciones en Control Expert para el sistema de seguridad M580

## Introducción

En esta sección se describe la funcionalidad Control Expert que se ha modificado o limitado para el sistema de seguridad M580.

## Transferencia e importación de proyectos de seguridad y código de M580 en Control Expert

### Transferencia de un proyecto de seguridad de Control Expert al PAC de seguridad

Puede utilizar el comando **PLC > Transferir proyecto a PLC** para transferir el proyecto de Control Expert al PAC cuando:

- Control Expert esté conectado en modo de programación (véase EcoStruxure™ Control Expert, Modalidades de funcionamiento) al PAC de seguridad M580, y
- Un proyecto está abierto en Control Expert, y
- Todas las tareas de PAC se encuentren en el estado STOP.

**NOTA:** Puede transferir una aplicación segura sólo a un PAC de seguridad. Una aplicación de seguridad no se puede transferir a un PAC que no es de seguridad.

### Transferencia de un proyecto de seguridad del PAC de seguridad a Control Expert

De igual modo, puede utilizar el comando **PLC > Transferir proyecto desde PLC** para transferir el proyecto del PAC a Control Expert cuando:

- Control Expert esté conectado en modo de programación (véase EcoStruxure™ Control Expert, Modalidades de funcionamiento) al PAC de seguridad M580, y
- ningún proyecto esté abierto en Control Expert.

Puede transferir el contenido relacionado con cualquier tarea (SAFE, MAST, FAST, AUX0 o AUX1), ya sea en la modalidad de funcionamiento de seguridad o de mantenimiento.

## Importación de proyectos y secciones de código en Control Expert

Control Expert Safety permite la importación de proyectos enteros (seleccionando **Archivo > Abrir**) y secciones de código (seleccionando **Tareas > Importar...** o **Secciones > Importar...**) en función de las condiciones siguientes:

- En una sección de código gestionada mediante la tarea SAFE sólo pueden incluirse funciones o tipos de bloques de funciones que existan en la biblioteca de seguridad (**Editor del ámbito de datos > <Libset> > Seguridad**) o la biblioteca personalizada (**Editor del ámbito de datos > <Libset> > Biblioteca personalizada**).
- En una sección de código no SAFE gestionada mediante una tarea de proceso (MAST, FAST, AUX0 o AUX1) sólo pueden incluirse funciones o tipos de bloques de funciones que existan en bibliotecas distintas a la biblioteca de seguridad.

## Almacenamiento y restauración de datos entre un archivo y el PAC

### Funciones de guardar y restaurar datos que no son de seguridad

Control Expert admite los comandos **PLC > Guardar datos del PLC al archivo y PLC > Restaurar datos del archivo al PLC** para datos de área global y proceso. Sin embargo, los datos guardados y restaurados no incluyen variables ni instancias de bloque de funciones creadas en el espacio de nombres seguro.

Para obtener información sobre cómo utilizar estos comandos para datos no seguros, consulte el tema *Guardar/Restaurar datos entre un archivo y el PLC* en el documento *Modalidades de funcionamiento de EcoStruxure™ Control Expert*.

## CCOTF para un PAC de seguridad M580

### Cambio de configuración sobre la marcha

La función de cambio de configuración sobre la marcha (CCOTF) permite cambiar una configuración de Control Expert mientras se ejecuta el PAC. Las funciones admitidas incluyen:

- Añadir una estación.
- Añadir un módulo de E/S.
- Eliminar un módulo de E/S.

- Editar la configuración de un módulo de E/S, como:
  - Cambiar el ajuste de un parámetro.
  - Añadir una función de canal.
  - Eliminar una función de canal.
  - Cambiar una función de canal.

**NOTA:** Las funciones CCOTF no se aplican a los dispositivos CIP Safety.

La función CCOTF se habilita seleccionando **Modificación online en RUN (EJECUTAR) o STOP (DETENER)** en la ficha **Configuración** del módulo de la CPU.

La funcionalidad básica de CCOTF se ha implementado en el PAC de seguridad M580 con las limitaciones que se describen más abajo.

Para obtener una descripción completa de CCOTF, consulte *Modicon M580 Cambio de configuración sobre la marcha - Manual del usuario*.

## Limitaciones de CCOTF de un PAC de seguridad M580

La función CCOTF se implementa en el PAC de seguridad M580 con limitaciones que se basan en la función específica y el tipo de módulo de E/S de la siguiente forma:

Función CCOTF	Tipo de módulo de E/S y modalidad de funcionamiento			
	E/S no interferentes		E/S de seguridad SIL3	
	Modalidad de mantenimiento	Modalidad de seguridad	Modalidad de mantenimiento	Modalidad de seguridad
Añadir estación	✓	✓	✓ <sup>1</sup>	✓
Añadir módulo	✓	✓	✓ <sup>1</sup>	X
Eliminar módulo	✓	✓	✓	X
Editar configuración del módulo de E/S	✓	✓	X	X
✓: Se admite X: No se admite  1. Para añadir un módulo de estación y un módulo de seguridad se necesitan dos sesiones CCOTF: una sesión CCOTF para añadir la estación, la segunda sesión CCOTF para añadir el módulo de seguridad. Estas acciones no se pueden realizar en una única sesión de CCOTF.				

**NOTA:** Las ediciones realizadas en una única sesión de CCOTF sólo pueden estar relacionadas con una única tarea (SAFE, MAST, FAST, AUX0 o AUX1).

# Cambios en las herramientas del PAC de seguridad M580

## Introducción

El PAC de seguridad M580 admite el uso de varias herramientas relacionadas. Algunas de estas herramientas se han modificado para usarlas juntamente con el PAC de seguridad M580. Estos temas abordan algunas de estas herramientas.

## Uso de la memoria

La pantalla **Uso de la memoria** presenta la información siguiente:

- La distribución física del PAC (memoria interna y tarjeta de memoria)
- El espacio que un proyecto ocupa en la memoria (datos, programa, configuración, sistema)

Para el PAC de seguridad M580, esta pantalla proporciona específicamente dos parámetros nuevos: **Datos declarados de seguridad** y **Código ejecutable de seguridad**, que se describen más abajo.

**NOTA:** También puede utilizar el comando **Comprimir** en esta pantalla para reorganizar la memoria, cuando sea posible.

Para obtener más información, consulte el tema *Uso de la memoria* en el manual de usuario de *Modalidades de funcionamiento de EcoStruxure™ Control Expert*.

En el caso del PAC de seguridad M580, se muestran los parámetros siguientes:

Parámetro	Descripción
<b>Datos de usuario</b>	<p>Este campo indica el espacio en la memoria (en palabras) que ocupan los datos del usuario (objetos relacionados con la configuración):</p> <ul style="list-style-type: none"> <li>• <b>Datos:</b> datos ubicados asociados con el procesador (%M, %MW, %S, %SW, etc.) o los módulos de entrada/salida.</li> <li>• <b>Datos declarados:</b> Datos no ubicados (declarados en el editor de datos de proceso) que se han guardado después del corte de corriente.</li> <li>• <b>Datos declarados no guardados:</b> Datos no ubicados (declarados en el editor de datos) que no se han guardado después del corte de corriente.</li> <li>• <b>Datos declarados de seguridad:</b> Datos no ubicados (declarados en el editor de datos) que no se han guardado después del corte de corriente.</li> </ul>
<b>Programa de usuario</b>	<p>Este campo indica el espacio en la memoria (en palabras) que ocupa el programa del proyecto:</p> <ul style="list-style-type: none"> <li>• <b>Constantes:</b> Constantes estáticas asociadas al procesador (%KW) y los módulos de entrada/salida; los valores de los datos iniciales.</li> <li>• <b>Código ejecutable:</b> Código ejecutable de la parte del área del proceso del programa de proyecto, EF, EFB y tipos de DFB.</li> </ul>

Parámetro	Descripción
	<ul style="list-style-type: none"> <li>• <b>Información de carga:</b> La información para cargar un proyecto (código gráfico de idiomas, símbolos, etc.).</li> <li>• <b>Código ejecutable de seguridad:</b> Código ejecutable de la parte de área del proceso del programa de proyecto, EF, EFB y tipos de DFB.</li> </ul>
<b>Otros</b>	<p>Este campo indica el espacio en la memoria (en palabras) que ocupan los otros datos relacionados con la configuración y la estructura del proyecto:</p> <ul style="list-style-type: none"> <li>• <b>Configuración:</b> Otros datos relacionados con la configuración (configuración de hardware, configuración de software).</li> <li>• <b>Sistema:</b> Datos utilizados por el sistema operativo (pila de tareas, catálogos, etc.).</li> <li>• <b>Diagnóstico:</b> Información relacionada con el diagnóstico del proceso o del sistema, el búfer de diagnóstico.</li> <li>• <b>Diccionario de datos:</b> Diccionario de variables simbolizadas con sus características (dirección, tipo, etc.).</li> </ul>
<b>Memoria interna</b>	<p>Este campo muestra la organización de la memoria interna del PAC. También indica el espacio disponible en memoria (<b>Total</b>), el mayor espacio contiguo en memoria posible (<b>Mayor</b>) y el nivel de fragmentación (a causa de modificaciones online).</p>

## Visualizador de eventos

El *visualizador de eventos* es una utilidad de MS Windows que captura los eventos registrados por Control Expert. Puede utilizar el *visualizador de eventos* para mostrar un historial de eventos registrados.

Acceda al *visualizador de eventos* de MS-Windows de la carpeta *Herramientas administrativas* del *Panel de control*. Cuando abra la utilidad, seleccione **Mostrar panel de acciones** y haga clic en **Crear vista personalizada** para abrir el diálogo. Aquí, puede crear una vista personalizada para eventos de Control Expert.

**NOTA:** En el cuadro de diálogo **Crear vista personalizada**, en primer lugar seleccione **Por origen** y luego **TraceServer** como la fuente para mostrar los eventos de Control Expert.

---

# CIP Safety

## Contenido de este capítulo

Introducción a CIP Safety para los PAC de seguridad M580 .....	353
Configuración de la CPU CIP Safety M580 .....	357
Configuración del dispositivo de destino CIP Safety.....	359
Configuración de DTM de dispositivo de seguridad .....	363
Operaciones de CIP Safety .....	375
Diagnóstico de CIP Safety .....	385

## Descripción general

En este capítulo se describen las comunicaciones CIP Safety según la norma IEC 61784-3 compatibles con las CPU de seguridad autónomas M580 BMEP58•040S.

# Introducción a CIP Safety para los PAC de seguridad M580

## Comunicación CIP Safety

### Introducción

Las CPU de seguridad autónomas BMEP58•040S admiten la comunicación CIP Safety (IEC 61784-3) y pueden utilizar este protocolo para establecer una conexión con un dispositivo CIP Safety a través de EtherNet/IP.

CIP Safety utiliza el mecanismo consumidor/productor para el intercambio de datos entre nodos seguros a través de EtherNet/IP. (No se admite la comunicación DeviceNet ni Sercos III). La CPU actúa como el origen que establece una conexión EtherNet/IP de unidifusión (uno a uno) con cada uno de los dispositivos de seguridad de destino. La CPU puede establecer una conexión CIP Safety con los dispositivos de destino que admitan el protocolo CIP Safety, así como una conexión CIP (que no sea de seguridad) con los dispositivos de destino que admitan el protocolo CIP.

Al igual que ocurre con cualquier PAC de seguridad, la CPU y el COPRO CIP Safety ejecutan doblemente la pila de CIP Safety de forma paralela y comparan los resultados del procesamiento.

### Arquitecturas compatibles

Las CPU de seguridad M580 independientes son compatibles con dispositivos CIP Safety ubicados en nubes DIO.

**NOTA:** Actualmente, no existe ningún dispositivo CIP Safety que admita RSTP y que pueda instalarse en un bastidor eX80. Por lo tanto, los dispositivos CIP Safety no pueden conectarse actualmente a los puertos duales de red de dispositivos de la CPU, pero sí pueden conectarse al puerto de servicio de esta.

Las nubes DIO requieren una única conexión de cobre (no de anillo), y pueden conectarse a los siguientes elementos:

- Un módulo de conmutación de opción de red BMENOS0300.
- El puerto de servicio de la CPU.
- El puerto de servicio de un módulo adaptador de E/S Ethernet eX80 BM•CRA312•0 de una estación RIO.
- Un puerto de cobre de un conmutador de anillo dual Ethernet.

**NOTA:** Cuando se conecta un dispositivo CIP Safety al puerto de servicio de un módulo adaptador de E/S Ethernet eX80 BM•CRA312•0 de una estación RIO, el dispositivo CIP Safety de destino podría no iniciarse automáticamente mientras el CRA descarga su configuración. Para que las conexiones CIP Safety se abran de la manera prevista, es posible que sea necesario gestionar el bit de control de la conexión CIP Safety en el DDDT de destino (CTRL\_IN o CTRL\_OUT), cambiándolo de False a True una vez que el módulo BM•CRA312•0 haya terminado de cargar su configuración.

Al igual que ocurre con cualquier equipo ubicado en una nube DIO, los dispositivos CIP Safety no se exploran como parte del anillo principal RIO; además, su estado de conexión no se refleja en los indicadores LED de la CPU.

Para obtener más información sobre nubes DIO, consulte los manuales *Modicon M580 autónomo Guía de planificación del sistema para arquitecturas utilizadas con más frecuencia* y *Modicon M580 Guía de planificación del sistema para topologías complejas*.

## Descripción general de la configuración

La configuración de las comunicaciones CIP Safety implica tres tareas de configuración distintas:

- Configurar la CPU autónoma de seguridad M580 con los ajustes de CIP Safety en Control Expert, página 357. Esto incluye la creación de un identificador de red único de origen (OUNID) que identifique de manera unívoca a la CPU. El OUNID se crea en Control Expert como resultado de la concatenación de dos componentes:
  - Número de red de seguridad (SNN): Identificador de la CPU creada en Control Expert.
  - Dirección IP principal de la CPU, especificada en Control Expert como parte de los ajustes de dirección IP de la CPU.

Schneider Electric recomienda configurar una sola vez el OUNID de la CPU en la configuración inicial. Si modifica posteriormente el ajuste del OUNID, deberá volver a configurar también todos los dispositivos CIP Safety conectados a la CPU.

- Configurar el dispositivo CIP Safety, página 361 mediante una herramienta de configuración de red de seguridad (SNCT) facilitada por el proveedor del dispositivo. Esto incluye dos tareas:
  - Creación de un identificador de configuración de seguridad (SCID): También conocido como la firma de configuración, el SCID se crea en la SNCT y lo utiliza Control Expert al configurar la conexión CIP Safety entre el origen (CPU) y el destino (dispositivo CIP Safety).
  - Asignación de un número de red de seguridad (SNN): El SNN lo crea normalmente Control Expert para el dispositivo CIP Safety y lo asigna la SNCT al dispositivo.

- Configurar la conexión CIP Safety entre la CPU y el dispositivo CIP Safety, página 363. La conexión se identifica a través de un TUNID que se crea mediante el DTM de la conexión del dispositivo en Control Expert que utiliza un DTM de CIP Safety, el cual puede estar basado en un archivo EDS facilitado por el fabricante o bien utilizarse solo si no hay disponible ningún archivo EDS.

## Gestión de conexiones de dispositivos CIP Safety

La CPU CIP Safety establece una conexión con un dispositivo CIP configurado y, a continuación, gestiona el dispositivo conectado. Dado que Control Expert admite tanto el protocolo CIP como el protocolo CIP Safety, puede gestionar conexiones CIP con los siguientes elementos:

- dispositivos CIP que implementan CIP a través de EtherNet/IP, pero no CIP Safety.
- dispositivos CIP Safety que implementan CIP Safety a través de EtherNet/IP, pero no CIP.
- dispositivos CIP híbridos que implementan tanto CIP como CIP Safety a través de EtherNet/IP.

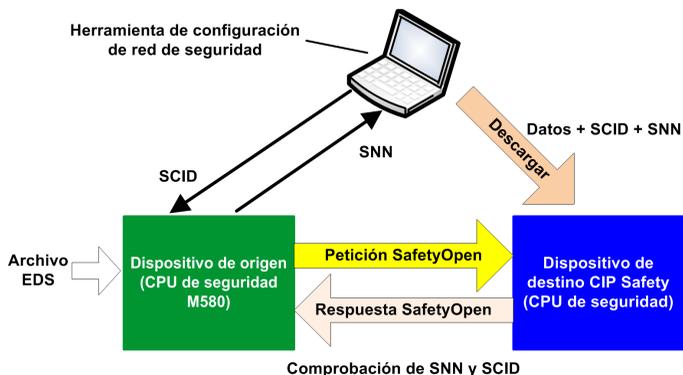
**NOTA:** Los dispositivos CIP y CIP Safety requieren cada uno un único DTM para su configuración. Los dispositivos CIP híbridos, que incorporan los protocolos CIP y CIP Safety, requieren dos DTM: uno configurado como dispositivo CIP y otro como dispositivo CIP Safety.

## Establecimiento de una conexión origen -> destino

La CPU autónoma M580 utiliza únicamente la petición de apertura de seguridad de tipo 2 para establecer una conexión con un dispositivo CIP Safety. Solo será posible establecer una conexión de apertura de seguridad de tipo 2 con un dispositivo de seguridad cuando dicho dispositivo se haya configurado mediante una SNCT. En los casos en los que el dispositivo CIP Safety sea un producto de terceros, Control Expert no dispondrá de ningún archivo de configuración y, por lo tanto, no podrá descargarse en el dispositivo CIP Safety, por lo que no podrá utilizarse como SNCT.

**NOTA:** En cambio, una conexión de apertura de seguridad de tipo 1 proporciona los ajustes de configuración para el dispositivo de seguridad y establece además la conexión. Las CPU CIP Safety M580 no admiten peticiones de conexión de apertura de tipo 1.

En el siguiente diagrama se ofrece una descripción general sobre cómo crear una conexión CIP Safety entre la CPU como origen de la conexión y el dispositivo CIP Safety como destino de la misma:



En este diagrama tienen lugar las siguientes acciones:

1. Control Expert utiliza un archivo EDS facilitado por el proveedor como base para la creación de un DTM para la conexión entre la CPU y el dispositivo CIP Safety.
2. El SNN del dispositivo se crea en Control Expert y, a continuación, se introduce en la SNCT.
3. La SNCT crea el SCID para el dispositivo, que se introduce en Control Expert como parte de la configuración de la conexión.
4. La SNCT descarga los ajustes de configuración en el dispositivo, el SCID creado por la SNCT y el SNN creado mediante Control Expert para la conexión.
5. La CPU como origen envía una petición de apertura de seguridad de tipo 2 al dispositivo.
6. El dispositivo CIP Safety envía una respuesta de apertura de seguridad a la CPU.
7. Si las sumas de comprobación de la petición y la respuesta coinciden, se establece la conexión.

# Configuración de la CPU CIP Safety M580

## Descripción general

En esta sección se describe la configuración de la CPU autónoma CIP Safety como origen de las comunicaciones CIP Safety.

## Configuración del OUNID de la CPU

### CPU como origen

La ficha (véase Modicon M580, Hardware, Manual de referencia) **Seguridad** de la CPU autónoma de seguridad M580 permite configurar la CPU como origen CIP Safety, al asignarle un identificador de red único de origen (OUNID).

Cada OUNID consta de un valor hexadecimal concatenado de 10 bytes, formado por los siguientes elementos:

- Número de red de seguridad (6 bytes)
- Dirección IP (4 bytes)

**NOTA:** El OUNID solo se puede modificar offline. Una vez generada la configuración modificada, la aplicación ya puede descargarse en el PAC.

### Número de red de seguridad

El componente de número de red de seguridad del OUNID puede generarse automáticamente mediante Control Expert o bien por medio del usuario a través de la entrada manual. Para crear el SNN:

- automáticamente, seleccione **Basado en el tiempo** y, a continuación, haga clic en el botón **Generar**. El valor generado automáticamente aparece en el campo **Número**.
- manualmente, seleccione **Manual** y, a continuación, introduzca una cadena hexadecimal de 6 bytes en el campo **Número**.

**NOTA:** El usuario deberá asignar un SNN exclusivo a cada origen de CPU M580 conectado a una misma red de seguridad.

## Dirección IP

Este ajuste de solo lectura se introduce automáticamente, a partir del ajuste configurado en la CPU de **Dirección IP principal** de la ficha (véase Modicon M580, Hardware, Manual de referencia) **IPConfig**.

## OUNID

Una vez creado el OUNID, este se utilizará como parámetro en la petición **SafetyOpen** de tipo 2, página 376 para establecer una conexión entre la CPU como origen y el dispositivo CIP Safety como destino.

# Configuración del dispositivo de destino CIP Safety

## Descripción general

En esta sección se describe el proceso de configuración del dispositivo de destino CIP Safety, incluida la configuración del dispositivo CIP Safety mediante una herramienta de configuración facilitada por el proveedor.

## Resumen de configuración del dispositivo CIP Safety

### Introducción

La configuración del dispositivo de destino CIP Safety comprende dos tareas:

- Configurar los ajustes del dispositivo CIP Safety, página 361 mediante una herramienta de configuración de red de seguridad (SNCT) facilitada por el proveedor.
- Configurar la conexión entre el origen de la CPU CIP Safety y el dispositivo de destino CIP Safety por medio de un DTM en Control Expert. El DTM puede:
  - basarse en un archivo EDS facilitado por el proveedor.
  - ser un DTM genérico de Control Expert, si no hay disponible ningún archivo EDS.

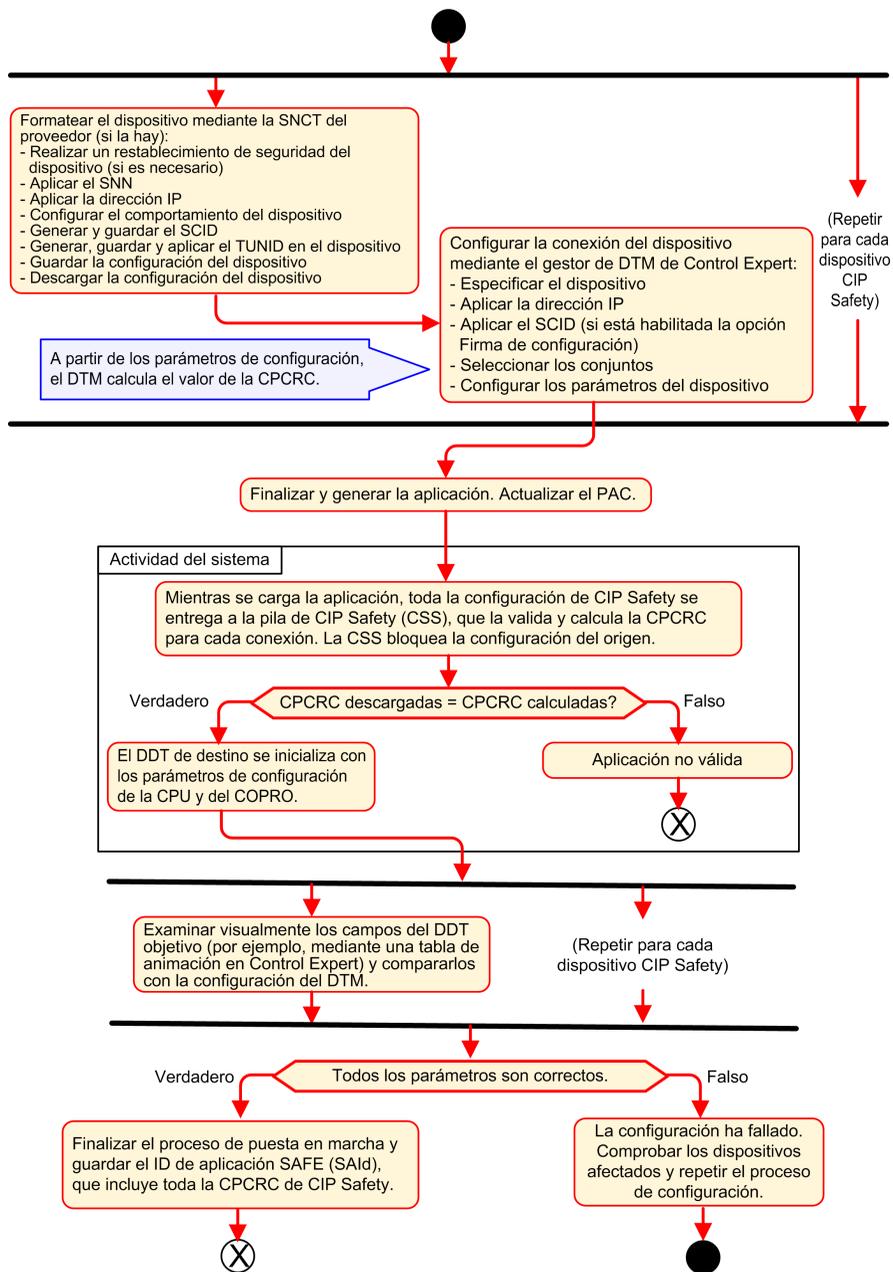
### Doble comprobación de la configuración

Los siguientes dos procesos, juntos, pueden proporcionar una confirmación de gran integridad de que la configuración creada mediante el software Control Expert se ha descargado y guardado correctamente en la CPU M580 CIP Safety como origen:

- Comparación visual realizada por el usuario (una vez finalizada la descarga de la aplicación) de los parámetros de configuración de la conexión CIP Safety que se muestran en el DDDT de destino frente a los parámetros correspondiente que se muestran en el DTM de destino.
- Comparación automática, realizada por la CPU y el COPRO, de la CRC del parámetro de conexión (CPCRC) calculada por el DTM frente a la CPCRC calculada por la pila de CIP Safety (CSS) que se ejecuta en la CPU y el COPRO.

## Resumen del proceso de configuración

Proceso de configuración y validación del dispositivo CIP Safety:



# Configuración del dispositivo CIP Safety mediante una herramienta facilitada por el proveedor

## Introducción

El dispositivo de destino CIP Safety se configura mediante una herramienta de configuración de red de seguridad (SNCT). No se configura mediante el software Control Expert. La SNCT la proporciona el proveedor del dispositivo CIP Safety, por lo que dependerá de este último.

Utilice la SNCT para realizar las siguientes acciones:

- Configurar y descargar en el dispositivo los ajustes necesarios para su funcionamiento.
- Configurar un identificador de configuración de seguridad específico del dispositivo (SCID) y, a continuación, copiarlo y transferirlo al software Control Expert. El SCID también se conoce como la firma de configuración del dispositivo. Se utiliza en Control Expert durante el proceso de configuración de Origen -> Conexión de destino., página 368
- Asignar al dispositivo su TUNID exclusivo, que consta de los siguientes elementos:
  - Número de red de seguridad (SNN), página 367 y
  - Dirección IP exclusiva.

**NOTA:** El SNN lo suele generar el software de configuración Control Expert (como parte de la configuración de conexión de Origen -> Destino), que lo aplica al dispositivo. La dirección IP se introduce en la SNCT y en el DTM de la conexión del dispositivo en Control Expert.

## Configuración del SCID

El SCID se establece en la SNCT y cumple la función de identificador de configuración hexadecimal exclusivo del dispositivo de destino CIP Safety. Está formado por una concatenación de los siguientes elementos:

- CRC de configuración de seguridad (SCCRC): valor de comprobación de redundancia cíclica (CRC) de los ajustes de configuración del dispositivo CIP Safety formado por 4 bytes.
- Marca de tiempo de configuración de seguridad (SCTS): valor de marca de tiempo hexadecimal de fecha y hora formado por 6 bytes.

## AVISO

### RIESGO DE FUNCIONAMIENTO IMPREVISTO DEL EQUIPO

Si configura una CPU M580 como origen CIP Safety, pruebe y verifique el comportamiento funcional de CIP Safety del sistema antes de utilizar la comunicación CIP Safety para controlar la función de seguridad correspondiente. Una vez realizadas correctamente las pruebas y la verificación, habilite la firma de configuración de destino CIP Safety (si la hay) en los DTM de CIP Safety de Control Expert.

**Si no se siguen estas instrucciones, pueden producirse daños en el equipo.**

Una vez creado el SCID mediante la SNCT, ya podrá introducir los elementos del SCID en la ficha **Seguridad** del DTM de dispositivo en Control Expert:

- **ID:** Introduzca el valor de la SCCRC.
- **Fecha:** Introduzca la fecha en la que se creó el SCID (mm/dd/aaaa).
- **Hora:** Introduzca la hora en la que se creó el SCID (hh/mm/ss/ms).

## Secuencia de configuración del dispositivo CIP Safety

En la siguiente secuencia se describe el proceso de configuración habitual de dispositivos CIP Safety:

1. Averigüe el SNN del dispositivo (obtenido de Control Expert).
2. Aplique el SNN en la SNCT del proveedor.
3. Realice un reseteo de seguridad del dispositivo (opcional: en el caso de que el OUNID del origen haya cambiado desde la última vez que se conectó el dispositivo).
4. Aplique el TUNID en el dispositivo.
5. Determine los ajustes de configuración que controlarán el comportamiento del dispositivo.
6. Configure el dispositivo con la SNCT (herramienta de configuración de red de seguridad) del proveedor.
7. Bloquee la configuración y compruebe que sea correcta.
8. Registre y guarde los parámetros para uso futuro en la configuración del origen (SCID, números de conjunto, dirección IP, etc.).
9. Guarde una copia de la configuración del dispositivo para uso futuro (por ejemplo, en el caso de que el dispositivo deba sustituirse).

# Configuración de DTM de dispositivo de seguridad

## Descripción general

En esta sección se describe la configuración de dispositivos de seguridad de destino, así como sus conexiones con la CPU de origen, mediante los DTM de Control Expert.

## Utilización de los DTM

### Utilización de los DTM

La conexión entre el origen de la CPU y el dispositivo de destino CIP Safety se configura por medio de un DTM. Control Expert admite el uso de los siguientes DTM, en función del perfil del dispositivo:

- DTM de CIP Safety: Para configurar una conexión con un dispositivo CIP Safety. Esto puede realizarse con o sin un archivo EDS del proveedor.
- DTM genérico: Para configurar una conexión estándar (es decir, que no es de seguridad) con un dispositivo, a partir de un archivo EDS del proveedor.

Los ajustes especificados mediante un DTM se almacenan en Control Expert en el DDDT, página 386 T\_CIP\_SAFETY\_CONF, y los utiliza la petición SafetyOpen de tipo 2, página 376 para establecer una conexión entre la CPU de origen y el dispositivo de destino.

## Si hay disponible un archivo EDS

Si se dispone de un archivo EDS del proveedor para un dispositivo, utilícelo para crear un nuevo DTM y añadirlo al **Catálogo DTM** de Control Expert. Para ello:

Paso	Acción
1	En Control Expert, seleccione <b>Herramientas &gt; Navegador DTM</b> .
2	En el <b>Navegador DTM</b> , haga clic con el botón derecho del ratón en el DTM de la CPU (BMEP58_ECPU_EXT) para abrir el menú contextual.
3	Desplácese hasta la opción <b>Menú del dispositivo &gt; Funciones adicionales &gt; Añadir EDS a biblioteca</b> y selecciónela. Se abrirá el asistente <b>Adición de EDS</b> .
4	Consulte el tema Adición de un archivo EDS al catálogo de hardware (véase EcoStruxure™ Control Expert, Modalidades de funcionamiento) para obtener instrucciones detalladas sobre cómo llevar a cabo el proceso de adición de un archivo EDS al catálogo DTM.

Una vez que se ha añadido un DTM al **Catálogo DTM**, ya podrá añadirlo al proyecto de Control Expert.

## Si no hay disponible ningún archivo EDS

Control Expert incluye un DTM de seguridad genérico en el **Catálogo DTM**. Utilícelo para configurar un dispositivo CIP Safety cuando no haya disponible ningún archivo EDS para dicho dispositivo.

## Dispositivos híbridos

Un dispositivo híbrido es un dispositivo único que admite tanto conexiones de seguridad como estándar. Cuando añada un dispositivo híbrido al **Catálogo DTM** por medio del comando **Añadir EDS a biblioteca**, se crearán dos DTM en el **Catálogo DTM** para el dispositivo: un DTM estándar y un DTM de seguridad.

Cuando añada un dispositivo híbrido al proyecto, deberá configurar tanto el DTM estándar como el DTM de seguridad para dicho dispositivo.

## Adición de un DTM a un proyecto de Control Expert

Para añadir un DTM a un proyecto de Control Expert:

Paso	Acción
1	En el <b>Navegador DTM</b> , haga clic con el botón derecho del ratón en el DTM de la CPU (BMEP58_ECPU_EXT) y seleccione <b>Añadir....</b> Se mostrará el cuadro de diálogo <b>Añadir</b> .
2	Seleccione el DTM que desea añadir. Este puede ser: <ul style="list-style-type: none"> <li>• Un DTM de CIP Safety creado a partir de un archivo EDS CIP Safety del proveedor, o bien</li> <li>• Un DTM de CIP Safety sin archivo EDS del proveedor.</li> </ul>
3	Haga clic en <b>Añadir DTM</b> . El DTM seleccionado aparece en el <b>Navegador DTM</b> , debajo del DTM de la CPU.
4	Haga clic con el botón derecho del ratón en el nuevo DTM y seleccione <b>Abrir</b> . Se abrirá la ventana de configuración del DTM.

## Configuración del DTM

El DTM de CIP Safety, creado con o sin archivo EDS del proveedor, presenta una serie similar de pantallas de configuración en Control Expert:

Árbol de navegación/fichas de configuración	Tipo de DTM	
	Con EDS del proveedor	Sin EDS del proveedor
<Nodo superior>	✓	✓
Nodo General		
Ficha Dispositivo	✓	X
Ficha Seguridad	✓	✓
<Conexiones>		
Ficha Conexión	✓	✓
Ficha Ajustes de configuración	✓	X
Ficha Verificación de configuración	✓	✓
<p>&lt; &gt; indica el nombre definido por el usuario.</p> <p>✓ = incluido</p> <p>X = no incluido</p>		

En los siguientes temas se describen las diferentes fichas de configuración que incluye Control Expert para cada tipo de DTM.

## DTM de dispositivo de seguridad: Información de archivo y proveedor

### Introducción

En el DTM de CIP Safety, creado o no a partir de un archivo EDS del proveedor, se incluye una descripción del archivo EDS de origen y del proveedor del dispositivo. En el caso de:

- un DTM de CIP Safety creado a partir de un archivo EDS del proveedor: la información es de solo lectura y se puede acceder a ella seleccionando el <Nodo superior> del árbol de navegación de DTM (panel izquierdo).

- un DTM de CIP Safety creado sin archivo EDS del proveedor: la información aparece en dos lugares distintos:
  - Al seleccionar el <Nodo superior>, se muestra la información del archivo EDS de solo lectura.

**NOTA:** La referencia del archivo EDS consiste en un archivo EDS de seguridad genérico interno, con el proveedor Schneider Electric, que utilizará Control Expert para crear el DTM de CIP Safety.
  - Al seleccionar la ficha **General > Dispositivo**, se muestra la información editable del proveedor.

## Información del archivo EDS

La información del archivo EDS incluye los siguientes datos de solo lectura:

- Descripción
- Fecha de creación del archivo
- Hora de creación del archivo
- Fecha de la última modificación
- Hora de la última modificación
- Revisión de EDS

## Información del proveedor

La siguiente información del proveedor es de solo lectura para los DTM de CIP Safety creados a partir de un archivo EDS del proveedor:

- Nombre del proveedor
- Tipo de dispositivo
- Revisión principal
- Revisión secundaria
- Nombre de producto

La siguiente información del proveedor es de lectura y escritura para los DTM de CIP Safety creados sin un archivo EDS del proveedor:

- ID del proveedor
- Tipo de producto
- Código de producto
- Revisión principal
- Revisión secundaria

**NOTA:** En el caso de las configuraciones de DTM realizadas sin la ayuda de un archivo EDS, introduzca los ajustes de información del proveedor con la información facilitada por el proveedor. De manera predeterminada, los valores del proveedor del DTM están establecidos en 0, y los valores de 0 no se admiten.

## DTM de dispositivo de seguridad: Número de red de seguridad

### Número de red de seguridad

La ficha **General > Seguridad** del DTM del dispositivo CIP Safety permite configurar un número de red de seguridad (SNN) para el dispositivo de seguridad. El SNN se emplea para establecer el identificador de red único de destino (TUNID). El TUNID identifica al dispositivo CIP Safety, y constituye un componente esencial de la petición **SafetyOpen** de tipo 2, página 376 emitida por la CPU de origen para iniciar una conexión CIP Safety.

### Configuración del SNN

El SNN consiste en un valor hexadecimal que forma parte tanto de la configuración de conexión CIP Safety (realizada mediante Control Expert) como de la configuración del dispositivo CIP Safety (realizada mediante una SNCT). Por lo general, el SNN se genera en Control Expert, que se copia (o se vuelve a introducir) en la SNCT. A continuación, la SNCT genera el TUNID a partir del SNN y la dirección IP, y transfiere este valor al dispositivo CIP Safety.

También es posible enviar el SNN directamente desde el DTM de la conexión CIP Safety de Control Expert al dispositivo de destino, página 384.

Para configurar el SNN:

Paso	Acción
1	En la ficha <b>General &gt; Seguridad</b> , haga clic en el botón de los puntos suspensivos (...). Se mostrará el cuadro de diálogo <b>Número de red de seguridad</b> .
2	En el cuadro de diálogo <b>Número de red de seguridad</b> , seleccione una de las siguientes opciones: <ul style="list-style-type: none"> <li>• <b>Basado en el tiempo:</b> Para generar un valor hexadecimal a partir del mes, el día, el año, la hora, los minutos, los segundos y los milisegundos en el momento de la generación.</li> <li>• <b>Manual:</b> Para generar un valor a partir de un valor decimal introducido del 1 al 9999, el cual se concatenará con dos valores hexadecimales de la siguiente manera: <ul style="list-style-type: none"> <li>◦ palabra 1: 0004 (fijo)</li> <li>◦ palabra 2: 0000 (fijo)</li> <li>◦ palabra 3: de 0001 a 270F (el valor hexadecimal del valor de la entrada de 1 a 9999)</li> </ul> </li> </ul>

Paso	Acción
	<ul style="list-style-type: none"> <li>• <b>Específico del proveedor:</b> Identificador específico del proveedor basado en 3 palabras hexadecimales de entrada: <ul style="list-style-type: none"> <li>◦ palabra 1: de 05B5 a 2DA7 (procedente del proveedor)</li> <li>◦ palabra 2: 0000 (fijo)</li> <li>◦ palabra 3: de 0001 a 270F (procedente del proveedor)</li> </ul> </li> <li>• Un valor hexadecimal introducido directamente (ya sea escrito o pegado), formado por los siguientes elementos: <ul style="list-style-type: none"> <li>◦ palabra 1: de 2DA8 a FFFE</li> <li>◦ palabras 2 y 3: de 00000000 a 05265BFF</li> </ul> </li> </ul>
3	En el caso de un formato Basado en el tiempo, Manual o Específico del proveedor, haga clic en <b>Generar</b> . Si introduce directamente un valor hexadecimal, haga clic en <b>Establecer</b> .
4	Haga clic en <b>Aceptar</b> para guardar el SNN y cerrar el cuadro de diálogo. El SNN aparece en el campo <b>Número de red de seguridad</b> .

## Configuración del SCID

El SCID, también conocido como firma de configuración, se establece en la herramienta de configuración de red de seguridad facilitada por el proveedor (SNCT) y representa el identificador de configuración hexadecimal exclusivo del dispositivo CIP Safety. Está formado por una concatenación de los siguientes elementos:

- La CRC de configuración de seguridad (SCCRC): Se trata de un valor de comprobación de redundancia cíclica (CRC) de los ajustes de configuración del dispositivo de seguridad, en forma de valor hexadecimal formado por 4 bytes.
- La marca de tiempo de configuración de seguridad (SCTS): Se trata de una marca de tiempo de valor hexadecimal de fecha y hora formada por 6 bytes.

Para introducir el SCID:

Paso	Acción
1	Obtenga la siguiente información de la configuración del dispositivo realizada mediante la SNCT: <ul style="list-style-type: none"> <li>• La SCCRC</li> <li>• La fecha (mm/dd/aaaa) y hora (hh/mm/ss/ms) en las que se realizó la configuración con la SNCT.</li> </ul>
2	Seleccione <b>Firma de configuración</b> .
3	Introduzca la SCCRC en el campo <b>ID</b> .
4	Introduzca los valores de fecha y hora en los campos <b>Fecha</b> y <b>Hora</b> .

**NOTA:** Si configura conexiones de seguridad con un SCID = 0 ("opción de configurar SCID deshabilitada"), tenga en cuenta que deberá responsabilizarse de comprobar que el origen de seguridad M580 y los destinos CIP Safety cuenten con la configuración correcta.

## DTM de dispositivo de seguridad: Comprobar y validar la configuración

### Comprobación visual de la configuración del DTM

Utilice la ficha **General > Verificación de configuración** para el DTM de CIP Safety, creado con o sin archivo EDS del proveedor, para comparar los parámetros definidos en dicho DTM (y que se muestran en esta ficha) con los parámetros configurados para el DDDT del dispositivo de destino. Para ello, utilice una tabla de animación en Control Expert, siempre que este último funcione en modalidad conectada y se encuentre conectado a la CPU.

**NOTA:** Tras la descarga de una aplicación, deberá comprobar visualmente, para cada uno de los destinos CIP Safety, que los diferentes parámetros de configuración de CIP Safety descargados en el origen M580 del destino en cuestión coincidan con los parámetros configurados en el DTM de destino. Para ello, compare los parámetros de configuración que se muestran en el DDDT del destino CIP Safety (por medio de una tabla de animación con Control Expert en modalidad conectada) con los parámetros configurados en el DTM que se muestran en la ficha Verificación de configuración.

### Validación de la configuración descargada

Una vez descargadas las diferentes configuraciones de CIP Safety, deberán validarse las descargas por medio de pruebas realizadas por el usuario. Una de las pruebas de validación consiste en probar las configuraciones de la conexión de seguridad una vez que se han aplicado a un origen para confirmar que la conexión de destino funciona del modo previsto.

## DTM del dispositivo de seguridad: Conexiones de E/S

### Introducción

El DTM de CIP Safety, creado con o sin un archivo EDS del proveedor, presenta los nodos de la conexión de seguridad. Se admiten tanto los nodos de entradas de seguridad como los de salidas de seguridad, según las características de un dispositivo específico. La ficha

**Conexión** presenta los parámetros de conexión correspondientes a la conexión de entrada o salida seleccionada.

En el caso de los DTM creados con un archivo EDS del proveedor, se seleccionan previamente las conexiones predeterminadas. Para adaptar los ajustes de conexión a los requisitos de su aplicación, utilice los comandos **Eliminar conexión** y **Añadir conexión**.

## Ajustes de conexión de entrada de seguridad

Cada conexión de entrada de seguridad presenta los siguientes parámetros:

- **Tamaño de entrada** (lectura/escritura): Tamaño de los datos de entrada configurado en el dispositivo CIP Safety, en bytes. El valor predeterminado es 0.

**NOTA:** Deberá sustituir el valor predeterminado por los ajustes facilitados por el proveedor. No se admite un valor de 0.

- **Intervalo para paquetes requeridos** (lectura/escritura): El RPI representa el período de actualización de la conexión. El valor predeterminado es igual a (período de tarea SAFE)/2.

**NOTA:** El período de tarea SAFE (Tsafe) se ajusta en el cuadro de diálogo **Propiedades de SAFE (Explorador de proyectos > Tareas > SAFE > Propiedades)** de Control Expert.

- **Expectativa tiempo red** (lectura/escritura): El tiempo, en milisegundos, que ha consumido la comunicación, página 166 CIP Safety. Si el valor es inferior a la *expectativa de tiempo de red mínima*, se mostrará un aviso de que se ha detectado un error. De forma predeterminada, el valor debería ser igual a la *expectativa de tiempo de red mínima* \* 1,5.
- **Multiplicador de timeout** (lectura/escritura): Es un componente para la generación de la *expectativa de tiempo de red mínima* y equivale a la expectativa de tiempo de red /128  $\mu$ s. La *expectativa de tiempo de red mínima* = RPI \* Multiplicador de timeout + Tsafe + 40.

- **Máx. transmisión red** (lectura/escritura): Intervalo (en ms) en el peor de los casos (intervalo máximo) de los datos en el momento en que el consumidor recibió el paquete. Este parámetro solo se utiliza para calcular el valor mínimo que hay que introducir en la expectativa de tiempo de red (tal como se describe a continuación). Para precisarlo, compruebe el valor de *Max-data\_age* en el dispositivo consumidor cuando se haya ejecutado la comunicación CIP Safety de red durante un tiempo considerable.

Este parámetro se utiliza en el cálculo del valor mínimo del parámetro de expectativa de tiempo de red, que se realiza de la siguiente manera:

$$\text{Mín. (expectativa de tiempo de red)} = \text{RPI} * \text{Multiplicador de timeout} + \text{Máx. transmisión red}$$

Si se modifica *Tsafe*, el valor del parámetro deberá cambiar y, en consecuencia, el valor mínimo de *expectativa de tiempo de red* también debería cambiar.

A este parámetro se le aplican los siguientes atributos:

- Valor mínimo = 1- ms
- Valor máximo = 5800 ms
- Valor predeterminado = 40 + *Tsafe*

El DTM del dispositivo utiliza estos ajustes de entrada para realizar los siguientes cálculos:

Variable	Valor		
	Predeterminado	Mínimo	Máximo
Período seguro (ms)	20	10	255
Intervalo de paquetes de petición de entrada (ms)	$\text{RPI} = \text{Tsafe} / 2$	5	500
Multiplicador de timeout	2	1	255
Máx. transmisión red (ms)	$40 + 2 * \text{Tsafe}$	10	5800
Expectativa de tiempo de red	Expectativa de tiempo de red mínima * 1,5	$\text{RPI} * \text{Multiplicador de timeout} + \text{Máx. transmisión red}$	5800

## Ajustes de conexión de salida de seguridad

Cada conexión de salida de seguridad presenta los siguientes parámetros:

- **Tamaño de salida** (lectura/escritura): Tamaño de los datos de salida configurado en el dispositivo CIP Safety, en bytes. El valor predeterminado es 0.

**NOTA:** Deberá sustituir el valor predeterminado por los ajustes facilitados por el proveedor. No se admite un valor de 0.

- **Intervalo para paquetes requeridos** (solo lectura): El RPI representa el período de actualización de la conexión. Su valor es igual al período de tarea SAFE (*Tsafe*).

- **Expectativa tiempo red** (lectura/escritura): El tiempo, en milisegundos, que ha consumido la comunicación, página 166 CIP Safety. Si el valor es inferior a la *expectativa de tiempo de red mínima*, se mostrará un aviso de que se ha detectado un error. De forma predeterminada, el valor debería ser igual a la *expectativa de tiempo de red mínima* \* 1,5.
- **Multiplicador de timeout** (lectura/escritura): Es un componente para la generación de la *expectativa de tiempo de red mínima* y equivale a la expectativa de tiempo de red /128  $\mu$ s. La *expectativa de tiempo de red mínima* = RPI \* Multiplicador de timeout + Tsafe + 40.
- **Máx. transmisión red** (lectura/escritura): Intervalo (en ms) en el peor de los casos (intervalo máximo) de los datos en el momento en que el consumidor recibió el paquete. Este parámetro solo se utiliza para calcular el valor mínimo que hay que introducir en la expectativa de tiempo de red (tal como se describe a continuación). Para precisarlo, compruebe el valor de *Max-data\_age* en el dispositivo consumidor cuando se haya ejecutado la comunicación CIP Safety de red durante un tiempo considerable.

Este parámetro se utiliza en el cálculo del valor mínimo del parámetro de expectativa de tiempo de red, que se realiza de la siguiente manera:

Mín. (expectativa de tiempo de red) = RPI \* Multiplicador de timeout + Máx. transmisión red

Si se modifica Tsafe, el valor del parámetro deberá cambiar y, en consecuencia, el valor mínimo de *expectativa de tiempo de red* también debería cambiar.

A este parámetro se le aplican los siguientes atributos:

- Valor mínimo = 1- ms
- Valor máximo = 5800 ms
- Valor predeterminado = 40 + 2\*Tsaf

El DTM del dispositivo utiliza estos ajustes de salida para realizar los siguientes cálculos:

Variable	Valor		
	Predeterminado	Mínimo	Máximo
Período seguro (ms)	20	10	255
Intervalo de paquetes de petición de entrada (ms)	RPI = Tsafe	10	255
Multiplicador de timeout	2	1	255
Máx. transmisión red (ms)	40 + 2 * Tsafe	10	5800
Expectativa de tiempo de red	Expectativa de tiempo de red mínima * 1,5	RPI * Multiplicador de timeout + Máx. transmisión red	5800

# DTM de dispositivo de seguridad: Ajustes de conexión de E/S

## Introducción

El DTM de CIP Safety, cuando se crea sin un archivo EDS del proveedor, incluye la ficha **Ajustes de configuración** del nodo de conexión.

Utilice la ficha **Ajustes de configuración** para completar la configuración de la conexión entre la CPU y el dispositivo remoto.

## Parámetros

La ficha **Ajustes de configuración** incluye los siguientes parámetros:

- **Instancia de entrada:** Número de conjunto específico del dispositivo relacionado con las transmisiones de entrada (D→O).
- **Instancia de salida:** Número de conjunto específico del dispositivo relacionado con las transmisiones de salida (O→D).
- **Instancia de configuración:** Número de conjunto específico del dispositivo relacionado con los ajustes de configuración del dispositivo.

## Ajustes de dirección IP del dispositivo de seguridad

### Edición del DTM maestro de la CPU M580

Los ajustes de dirección IP y DHCP de un dispositivo CIP Safety pueden configurarse en el DTM maestro de la CPU M580.

**NOTA:** A diferencia de otros ajustes de configuración de conexión del dispositivo de destino, la dirección IP del dispositivo no se configura en el DTM de conexión del dispositivo.

## Acceso a los ajustes de dirección IP del dispositivo de seguridad

Siga el procedimiento que se indica a continuación para editar los parámetros de dirección IP y DHCP de un dispositivo CIP Safety:

Paso	Acción
1	Desconecte Control Expert del dispositivo de destino y edite los siguientes elementos offline.
2	En el <b>Navegador DTM</b> de Control Expert, haga doble clic en el DTM maestro de la CPU M580 (BMEP58_ECPU_EXT) para abrir su configuración.
3	En el árbol de navegación, expanda la Lista de dispositivos para ver las instancias de esclavo local asociadas.
4	Seleccione el dispositivo que corresponda al dispositivo CIP Safety.
5	Seleccione la ficha <b>Ajuste de dirección</b> .

## Configuración de los ajustes de dirección IP del dispositivo de seguridad

En la ficha **Ajuste de dirección**, edite los siguientes parámetros para el dispositivo de seguridad seleccionado:

Campo	Parámetro	Descripción
<b>Configuración IP</b>	<b>Dirección IP</b>	Introduzca la dirección IP del dispositivo seleccionado.
	<b>Máscara de subred</b>	Máscara de subred del dispositivo. <b>NOTA:</b> Configure la máscara de subred de modo que la dirección IP del dispositivo se encuentre en la misma subred que la dirección IP principal de la CPU de origen.
	<b>Pasarela</b>	Dirección de pasarela utilizada para llegar a este dispositivo. El valor predeterminado 0.0.0.0 indica que este dispositivo se encuentra en la misma subred que la CPU de origen.
<b>Servidor de direcciones</b>	<b>DHCP para este dispositivo</b>	<ul style="list-style-type: none"> <li>• <b>Deshabilitado</b> (valor predeterminado) desactiva el cliente DHCP en este dispositivo.</li> <li>• <b>Habilitado</b> activa el cliente DHCP en este dispositivo.</li> </ul>
	<b>Identificado por</b>	Si está habilitado el servicio DHCP, seleccione el tipo de identificador del dispositivo: <ul style="list-style-type: none"> <li>• <b>Dirección MAC.</b></li> <li>• <b>Nombre del dispositivo.</b></li> </ul>
	<b>Identificador</b>	Si se ha habilitado el servicio DHCP y seleccionado la opción <b>Nombre del dispositivo</b> , introduzca el valor del nombre del dispositivo.

Para obtener más información acerca de la configuración de los parámetros del dispositivo en el DTM maestro de la CPU M580, consulte el tema Parámetros de la lista de dispositivos (véase Modicon M580, Hardware, Manual de referencia).

# Operaciones de CIP Safety

## Descripción general

En esta sección se describen las operaciones de CIP Safety.

## Transferencia de una aplicación CIP Safety de Control Expert al PAC

### Inicio de la descarga de la aplicación

Utilice el comando **PLC > Transferir proyecto a PLC** para iniciar la descarga.

Si el PLC se configura con una aplicación existente ("aplicación anterior"), esta quedará invalidada cuando se inicie la descarga de la nueva aplicación. Si la aplicación anterior incluye dispositivos configurados, el PAC cerrará las conexiones con dichos dispositivos.

### Fin de la descarga de la aplicación

La configuración de CIP Safety se escribe en la pila de CIP Safety (CSS) de la CPU, que calcula una CRC de parámetros de conexión (CPCRC) para cada conexión. A continuación, el DTM de destino compara cada una de las CPCRC calculadas por la CSS con la CPCRC correspondiente almacenada en la configuración y las calcula. En caso de:

- Discrepancia de la CPCRC, la CSS rechaza la aplicación y el PAC permanece en el estado NOCONF.
- Igualdad:
  - Los valores de los parámetros de conexión y la CPCRC se copian en el DDDT de destino, página 385 correspondiente.
  - El parámetro CSIO\_HEALTH, página 392 del DDDT de la CPU (T\_BMEP58\_ECPU\_EXT) se establece en 0.
  - Los bits de estado funcional (HEALTH) del DDDT del dispositivo, página 385 de destino CIP Safety se establecen en 0.
  - El PAC abre las conexiones de los dispositivos configurados a través de las peticiones SafetyOpen de tipo 2, página 376.

En el caso de que se produzca una discrepancia de CPCRC, la CSS rechaza la aplicación, y el PAC permanece en el estado NOCONF.

## Nuevo cálculo del ID de la aplicación de seguridad

El ID de la aplicación de seguridad (SAID) equivale a una firma de la parte segura de la aplicación de Control Expert. Se almacena como la palabra de sistema %SW169, página 408. La CSS calcula una CRC en todas las instancias de la CPCRC. Esta CRC se añade al cálculo del SAID. Por lo tanto, una modificación de la configuración de un destino CIP Safety supondrá una modificación del valor del SAID.

## Estructura de una petición SafetyOpen de tipo 2

### Estructura de trama de conexión CIP SafetyOpen de tipo 2

Las CPU de seguridad autónomas M580 admiten conexiones CIP Safety creadas mediante peticiones de conexión SafetyOpen de tipo 2. A continuación, se describe la estructura de la trama de petición de conexión:

Nombre del parámetro		Descripción
Connection Timeout Multiplier		Lo utiliza el consumidor de una conexión para determinar si se agota el timeout de alguna de las tres conexiones estándar. El valor de timeout de la conexión se define de la siguiente manera:  RPI de la conexión * (CTM+1) * 4
O_to_T RPI		Intervalo para paquetes requeridos de origen a destino.
T_to_O RPI		Intervalo para paquetes requeridos de destino a origen.
Electronic Key.Vendor ID		Identificador de proveedor de dispositivo
Electronic Key.Prod Type		Tipo de dispositivo
Electronic Key.Prod Code		Código de producto del dispositivo
Electronic Key.Compatible/Major Rev		Revisión principal
Electronic Key.Minor Rev		Revisión secundaria
SCID	Safety Configuration CRC	Identificador de configuración de seguridad: lo facilita la herramienta de configuración de red de seguridad (SNCT); se utiliza durante la puesta en marcha, el establecimiento de la conexión y la sustitución de dispositivos.
	Configuration Date	
	Configuration Time	
TUNID	TUNID Date	Identificador de red único de destino: identifica el destino de la petición SafetyOpen.
	TUNID Time	
	Target Node ID	

Nombre del parámetro		Descripción
OUNID	OUNID Date	Identificador de red único de origen: identifica el origen de la petición SafetyOpen.
	OUNID Time	
	Originator Node ID	
Ping_Interval_EPI_Multiplier		Define el Ping_Count_Interval (intervalo de recuento de ping) de la conexión.
Time_Coord_Msg_Min_Multiplier		Número mínimo de incrementos de 128 $\mu$ s que podría necesitar un mensaje de coordinación horaria para transmitirse del consumidor al productor.
Network_Time_Expectation_Multiplier		Intervalo máximo de los datos de seguridad, medido en incrementos de 128 $\mu$ s, que permite el consumidor en cuestión.
Timeout_Multiplier		Número de reintentos de producción de datos que se incluirá en la ecuación de detección de conexión incorrecta.
Max_Fault_Number		Número de paquetes erróneos que pueden perderse antes de que se cierre la conexión.
Connection Parameters CRC (CPCRC)		CRC de parámetros de conexión. CRC-S32 de los parámetros de conexión de destino incluidos en la petición SafetyOpen de tipo 2.

## Operaciones del dispositivo CIP Safety

### Introducción

En este tema se describen las operaciones del dispositivo CIP Safety, incluidos los mecanismos de detección y respuesta de errores del sistema, y el estado de funcionamiento del dispositivo:

- Autocomprobación durante el encendido
- Respuesta ante error detectado no recuperable
- Error detectado recuperable
- Gestión del estado funcional de la conexión de destino
- Estado de ejecución/inactivo del dispositivo CIP Safety

### Autocomprobación durante el encendido del origen y el destino CIP Safety

Durante el encendido, y cada vez que se carga una nueva aplicación, el sistema CIP Safety ejecuta las siguientes operaciones:

- La CPU transfiere los parámetros de configuración a la pila de CIP Safety (CSS) de la CPU y del COPRO.
- La CSS evalúa, tanto en la CPU como en el COPRO, la CPCRC de cada conexión.
- Para cada conexión, el sistema CIP Safety compara la CPCRC descargada (calculada mediante el DTM de origen) con las calculadas por la CPU y el COPRO.
- La CSS bloquea la configuración del origen.
- La aplicación inicia las peticiones SafetyOpen de tipo 2 de conexión con cada uno de los dispositivos CIP Safety.
- Cada dispositivo CIP Safety:
  - Calcula su CPCRC y la compara con la CPCRC recibida del origen.
  - Compara el SCID recibido con el SCID almacenado internamente (Nota: esta comprobación solo se aplica a dispositivos configurables).

Los intercambios de E/S entre los dispositivos de origen y destino solo se iniciarán si las comprobaciones anteriores no presentan errores.

**NOTA:** Además de las autocomprobaciones durante el encendido mencionadas anteriormente, el sistema ejecuta todas las autocomprobaciones durante el tiempo de ejecución que requiere la norma sobre CIP Safety IEC 61784-3.

## Respuesta ante error detectado no recuperable

Si la CPU o los diagnósticos de E/S detectan un error no recuperable, el sistema de seguridad colocará la parte afectada del sistema en un estado de seguridad. La parte afectada del sistema se apagará y dejará de recibir alimentación. Además, las entradas de seguridad se establecerán en 0. Las diferentes salidas de seguridad que hayan quedado afectadas serán dirigidas a su estado de retorno configurado.

## Respuesta ante error detectado recuperable

Los errores detectados recuperables suelen incluir eventos como, por ejemplo, la pérdida de conexión con el módulo. Estos errores detectados se notifican en el bit de estado funcional del DDDT (T\_CIP\_SAFETY\_IO, página 385) del dispositivo, que contiene el valor AND lógico de los bits de estado funcional Status\_IN y Status\_OUT. En el caso de que se detecte un error recuperable para una entrada, se forzará el valor de dicha entrada al estado de seguridad, que se establecerá en 0.

## Gestión del estado funcional de la conexión de destino

El estado funcional de una conexión con el destino CIP Safety se notifica en el bit de estado funcional de los parámetros Status\_IN y Status\_OUT, tal como se describe en el tipo de

datos T\_CIP\_SAFETY\_STATUS, página 386. El estado funcional de destino puede ser abierto y operativo o bien que se haya detectado un error.

En el caso de las entradas, el validador de seguridad del servidor proporciona el estado de conexión; para las salidas, hace lo propio el validador de seguridad del cliente.

## Ejecución/inactivo

El estado operativo del dispositivo CIP Safety (ejecución o inactivo) se notifica en el bit Run\_Idle del parámetro Status\_IN o Status\_OUT, tal como se describe en el tipo de datos T\_CIP\_SAFETY\_STATUS, página 386.

### **En el caso de un dispositivo de entrada:**

Cuando se establece una conexión con un módulo de entrada, el productor (entrada) establece el bit Run\_Idle en inactivo (0) hasta que finalice correctamente la secuencia de coordinación horaria inicial. A partir de ese momento, el valor del bit podrá ser 1 (estado de ejecución) o 0 (estado inactivo). Si el bit Run\_Idle se establece en 0 (estado inactivo), los valores de los datos de entrada se forzarán a 0 (estado de seguridad).

### **En el caso de un dispositivo de salida:**

El origen (CPU) establecerá el bit Run\_Idle de las salidas en 1 siempre que el PAC se encuentre en estado de ejecución y haya finalizado correctamente la secuencia de coordinación horaria inicial. El origen (CPU) establecerá el estado de ejecución/inactivo de las salidas en 0 cuando el PAC se encuentre en estado de detención o pausa, cuando no haya finalizado correctamente la secuencia de coordinación horaria inicial o cuando se haya cerrado la conexión. Si el bit Run\_Idle se establece en 0 (estado inactivo), se espera que el dispositivo de salida establezca sus salidas en su estado de retorno.

## Interacciones entre las operaciones del PAC de seguridad y la conexión de destino

### Introducción

En este tema se analizan las interacciones que se producen entre los siguientes estados u operaciones del origen de la CPU de seguridad y la conexión del dispositivo de destino:

- Tiempo de reacción del sistema
- Estado de ejecución
- Estado de detención/pausa
- Apagado y encendido/reinicio
- Comando Inicializar SAFE

- Modalidad de mantenimiento
- CCOTF
- Conexión/desconexión/sustitución de un dispositivo

## Tiempo de reacción del sistema

El tiempo consumido por la comunicación CIP Safety (denominado *expectativa de tiempo de red*) se añade al *tiempo de reacción del sistema* de seguridad M580 para pasar a formar parte de él. Para obtener más información, consulte el tema *Impacto de las comunicaciones de CIP Safety en el tiempo de reacción del sistema de seguridad*.

## Estado de ejecución

Cuando el sistema CIP Safety se utiliza en estado de ejecución:

- Los bits de estado funcional del DDDT, página 385 de comunicación del dispositivo CIP Safety se actualizan al inicio del ciclo de tarea SAFE.
- Los valores de entrada se actualizan al inicio del ciclo de tarea SAFE en función del valor recibido más reciente.
- Los valores de salida se actualizan y transmiten tras la ejecución del programa de tarea SAFE.
- El bit Run\_Idle de las salidas del DDDT de comunicación del dispositivo CIP Safety se establece en 1.
- Los bits de estado funcional del DDDT de comunicación del dispositivo CIP Safety se actualizan.

## Estado de detención

Cuando la tarea SAFE pasa al estado de detención, por ejemplo, si se ha detenido la tarea SAFE o ha alcanzado un punto de parada:

- La conexión con el origen o el destino permanece abierta.
- Se ejecutan los intercambios de datos entre la CPU y el dispositivo CIP Safety.
- Los bits de estado funcional del DDDT, página 385 de comunicación del dispositivo CIP Safety continúan actualizándose.
- El bit Run\_Idle de las salidas del DDDT de comunicación del dispositivo CIP Safety se establece en 0 y los dispositivos de salida aplican el ajuste de retorno configurado.

## Estado de pausa

En el estado de pausa, los valores de salida no se envían de la CPU al dispositivo CIP Safety, pero sí se establecen en 0 los bits de estado funcional del dispositivo.

## Apagado e inicio o reseteo

En caso de apagado e inicio o reseteo:

- La parte de seguridad de la aplicación ejecuta un arranque en frío, página 275.
- El PAC ejecuta la misma secuencia de operaciones que la que se ejecuta para la descarga de aplicaciones, página 375.

## Comando Inicializar SAFE

Al ejecutar el comando **PLC > Inicialización Safety** en Control Expert, se inicializan los valores del DDDT, página 385 de comunicación del dispositivo CIP Safety, que se establecen en sus valores predeterminados de fábrica.

## Modalidad de mantenimiento

El uso de la CPU de seguridad M580 en modalidad de mantenimiento, página 262 no afectará a las operaciones del dispositivo CIP Safety. La CPU seguirá comparando los cálculos realizados de manera separada por la CPU y el COPRO. Sin embargo, no habrá comparación adicional con los valores del DDDT de destino. Por consiguiente, el uso del PAC en modalidad de mantenimiento no se considera seguro.

## CCOTF

Los dispositivos CIP Safety no son compatibles con la función de cambio de configuración sobre la marcha (CCOTF). Dado que un dispositivo CIP Safety obtiene sus ajustes de configuración de una herramienta de configuración de red de seguridad (SNCT) facilitada por el proveedor, y no de la CPU de origen, los ajustes del dispositivo no podrán modificarse desde la CPU.

## Conexión/desconexión/sustitución de un dispositivo CIP Safety

De manera predeterminada, al iniciar la aplicación o ejecutar el comando **PLC > Inicialización Safety**, los bits CTRL\_IN y CTRL\_OUT del DDDT, página 385 se establecen en habilitados (1). Cuando se conecta un dispositivo a un PAC en modalidad de detención o

ejecución y el bit CTRL\_IN o CTRL\_OUT del dispositivo está establecido en habilitado (1), el dispositivo inicia automáticamente los intercambios de datos.

**NOTA:** Dado que los bits CTRL\_IN y CTRL\_OUT se establecen en estado habilitado en un apagado e inicio, se recomienda tomar las medidas de precaución apropiadas en la aplicación de la tarea SAFE a fin de evitar un funcionamiento imprevisto al ejecutar un apagado e inicio.

## **▲ ADVERTENCIA**

### **RIESGO DE FUNCIONAMIENTO IMPREVISTO DEL EQUIPO**

No utilice los bits CTRL\_IN o CTRL\_OUT como medida de seguridad para configurar los datos de destino en un estado de seguridad.

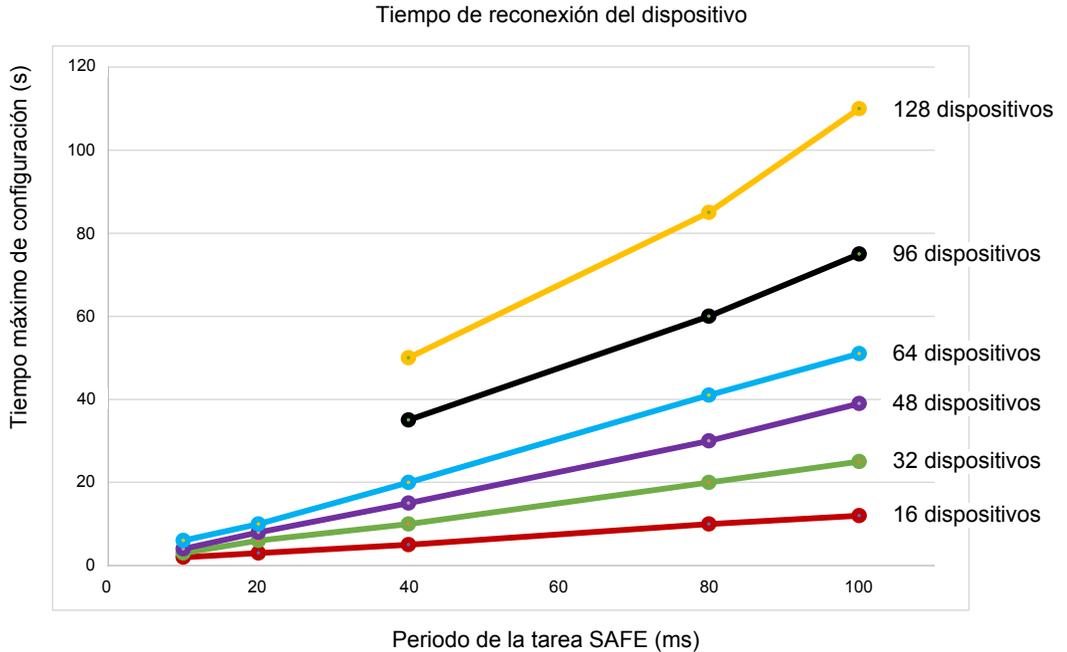
**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

Cuando el PAC detecta un error que requiere la finalización de una conexión de dispositivo, ajusta el bit CTRL\_IN o CTRL\_OUT correspondiente como deshabilitado (0). El dispositivo permanece en estado deshabilitado y solo pasará a estado habilitado (1) si está previsto realizar dicha transición. Por ejemplo, si se soluciona el error y se ejecuta una petición de reapertura de la conexión.

Para ejecutar una petición de reapertura de conexión, vuelva a establecer el bit de control correspondiente (CTRL\_IN o CTRL\_OUT) de deshabilitado (0) a habilitado (1) en el DDDT.

Cuando reconecte un dispositivo, el tiempo que transcurrirá hasta la conexión dependerá del periodo de la tarea SAFE y del número de dispositivos que se conecten:

- En el caso de un único dispositivo con un periodo de tarea SAFE inferior a 100 ms, el tiempo estimado de reconexión es de menos de 2 segundos.
- En el caso de varios dispositivos, consulte el siguiente gráfico para obtener los tiempos estimados de reconexión.



El PAC CIP Safety gestiona la sustitución de un dispositivo de la misma manera que la desconexión y reconexión de un dispositivo. Las operaciones para volver a configurar el nuevo dispositivo con los mismos ajustes que el dispositivo sustituido son locales del dispositivo, por lo que no implican al PAC.

## Comandos del DTM de CIP Safety

### Introducción

El DTM de CIP Safety incluye la ficha **Seguridad**, que contiene los siguientes comandos:

- **Restablecer propiedad**
- **colocar TUNID**

Para acceder a estos comandos, seleccione primero una conexión en el árbol de navegación del DTM. Los comandos solo se habilitarán si el DTM se encuentra conectado al dispositivo CIP Safety que se utiliza online.

## Restablecer propiedad

El comando **Restablecer propiedad** permite restablecer los ajustes de configuración del dispositivo CIP Safety a sus valores predeterminados de fábrica. Solo podrá ejecutar un restablecimiento si se cumplen las siguientes condiciones:

- El comando lo ejecuta la CPU del origen identificada mediante el OUNID almacenado en el dispositivo.
- Los ajustes de configuración del módulo no están bloqueados.

Tras el restablecimiento, el módulo deja de tener propietario, por lo que puede configurarlo otro origen.

**NOTA:** Si se ejecuta un restablecimiento en un módulo con conexiones operativas, el comando de restablecimiento no tendrá efecto.

## colocar TUNID

El comando **colocar TUNID** permite configurar el número de red de seguridad (SNN) en el dispositivo CIP Safety de destino. Al ejecutarse, el número de red de seguridad, página 367 almacenado en la configuración del DTM del dispositivo CIP Safety se transfiere al dispositivo de destino, con lo que se sobrescribe cualquier valor de SNN que existía en el dispositivo.

**NOTA:** Antes de ejecutar este comando, compruebe que ha identificado el dispositivo correcto para recibir el SNN que tiene previsto transferir.

# Diagnóstico de CIP Safety

## Descripción general

En esta sección se presentan las herramientas de diagnóstico para el dispositivo CIP Safety, así como la conexión CIP Safety entre el dispositivo y la CPU autónoma de seguridad M580.

## DDDT del dispositivo CIP Safety

### T\_CIP\_SAFETY\_IO DDDT

Cada instancia de dispositivo CIP Safety se describe mediante un T\_CIP\_SAFETY\_IO DDDT, que consta de los siguientes parámetros:

Parámetro	Tipo de datos	Descripción
Health	BOOL	Estado funcional global = el AND lógico de: <ul style="list-style-type: none"> <li>• Status_IN.Health</li> <li>• Status_OUT.Health</li> </ul> Consulte el tipo de datos T_CIP_SAFETY_STATUS, página 386 para obtener una descripción de estos bits de estado funcional.
Status_IN	T_CIP_SAFETY_STATUS	Estado de entrada.
Status_OUT	T_CIP_SAFETY_STATUS	Estado de salida.
CTRL_IN	BOOL	Habilitar/deshabilitar la conexión de entrada.
CTRL_OUT	BOOL	Habilitar/deshabilitar la conexión de salida.
Conf_In	T_CIP_SAFETY_CONF	Parámetros y firmas CIP para la conexión de entrada.
Conf_Out	T_CIP_SAFETY_CONF	Parámetros y firmas CIP para la conexión de salida.
Input	Matriz[de 0 a n] de BYTE	Valores de entrada. El tamaño depende del tipo de dispositivo. Se alinean 4 bytes del módulo con el tamaño configurado en el DTM.
Output	Matriz[de 0 a m] de BYTE	Valores de salida. El tamaño depende del tipo de dispositivo. Se alinean 4 bytes del módulo con el tamaño configurado en el DTM.

A continuación se describen los tipos de datos de CIP Safety mencionados anteriormente.

## T\_CIP\_SAFETY\_STATUS

El tipo de datos T\_CIP\_SAFETY\_STATUS consta de los siguientes parámetros:

Parámetro	Tipo de datos	Descripción
Health	BOOL	<p>Estado funcional de la entrada o salida:</p> <ul style="list-style-type: none"> <li>• Para la entrada: <ul style="list-style-type: none"> <li>◦ 1: comunicación de entrada abierta y operativa.</li> <li>◦ 0: el validador de seguridad del servidor ha detectado un error en la comunicación de entrada.</li> </ul> </li> <li>• Para la salida: <ul style="list-style-type: none"> <li>◦ 1: comunicación de salida abierta y operativa.</li> <li>◦ 0: el validador de seguridad del cliente ha detectado un error en la comunicación de salida.</li> </ul> </li> </ul>
Run_Idle	BOOL	<p>Estado de las entradas o salidas del dispositivo CIP Safety:</p> <ul style="list-style-type: none"> <li>• Las entradas las configura el productor (entrada): <ul style="list-style-type: none"> <li>◦ 1: si la entrada se encuentra en estado de ejecución.</li> <li>◦ 0: si la entrada se encuentra inactiva o hasta que finalice correctamente la secuencia de coordinación horaria inicial.</li> </ul> </li> <li>• Las entradas las configura el origen (CPU): <ul style="list-style-type: none"> <li>◦ 1: si el PAC se encuentra en estado de ejecución, una vez que haya finalizado correctamente la secuencia de coordinación horaria inicial.</li> <li>◦ 0: si el PAC se encuentra en estado de parada (Stop) o pausa (Halt), si la conexión está cerrada o si no ha finalizado correctamente la secuencia de coordinación horaria inicial.</li> </ul> </li> </ul>
Error_Code	WORD	Consulte la lista de códigos de error detectados, página 388.
Error_Sub_Code	WORD	Consulte la lista de subcódigos de error detectados, página 389.

## T\_CIP\_SAFETY\_CONF

El tipo de datos T\_CIP\_SAFETY\_CONF consta de los siguientes parámetros que se transmiten en la petición SafetyOpen de tipo 2, página 376:

Parámetro	Tipo de datos	Descripción
TO_MULTIPLIER	BYTE	Multiplicador de timeout. Lo utiliza el consumidor de una conexión para determinar si se agota el timeout de alguna de las tres conexiones estándar. El valor de timeout de la conexión se define de la siguiente manera:  RPI de la conexión * (CTM+1) * 4
Output_RPI	UDINT	Intervalo para paquetes requeridos de la conexión O→D.
Input_RPI	UDINT	Intervalo para paquetes requeridos de la conexión D→O.
Device_Vendor_ID	UINT	Identificador del proveedor de la ODVA.
Device_Type	UINT	Agrupación de la ODVA a la que pertenece el dispositivo.
Device_Product_Code	UINT	Código de producto asignado de la ODVA.
Major_Revision	BYTE	Número de revisión principal del firmware del dispositivo.
Minor_Revision	BYTE	Número de revisión secundaria del firmware del dispositivo.
Configuration_Assembly_Nb	UINT	Número de conjunto específico del dispositivo relacionado con los ajustes de configuración del dispositivo.
Output_Assembly_Nb	UINT	Número de conjunto específico del dispositivo relacionado con las transmisiones de salida (O→D).
Input_Assembly_Nb	UINT	Número de conjunto específico del dispositivo relacionado con las transmisiones de entrada (D→O).
SC_CRC	UDINT	CRC de configuración de seguridad. Comprobación de redundancia cíclica (CRC) de la configuración del dispositivo CIP Safety.
Configuration_Date	UINT	Mes, día y año en que se generó la configuración.
Configuration_Time	UDINT	Hora, minutos, segundos y milisegundos en que se generó la configuración.
TUNID_Time	UDINT	Mes, día y año en que se generó el identificador de red único de destino.
TUNID_Date	UINT	Hora, minutos, segundos y milisegundos en que se generó el identificador de red único de destino.
TUNID_NodeID	UDINT	Identificador de red único del dispositivo de destino.
OUNID_Time	UDINT	Mes, día y año en que se generó el identificador de red único de origen.
OUNID_Date	UINT	Hora, minutos, segundos y milisegundos en que se generó el identificador de red único de origen.
OUNID_NodeID	UDINT	Identificador de red único del dispositivo de origen.

Parámetro	Tipo de datos	Descripción
Ping_Interval_EPI_Multiplier	UINT	Define el Ping_Count_Interval (intervalo de recuento de ping) de la conexión.
Time_Coordination_Msg_Min_Mult	UINT	Número mínimo de incrementos de 128 $\mu$ s que podría necesitar un mensaje de coordinación horaria para transmitirse del consumidor al productor.
Network_Time_Expectation_Mult	UINT	Intervalo máximo de los datos de seguridad, medido en incrementos de 128 $\mu$ s, que permite el consumidor en cuestión.
Timeout_Multiplier	BYTE	Número de reintentos de producción de datos que se incluirá en la ecuación de detección de conexión incorrecta.
Max_Fault_Number	UDINT	Número de paquetes erróneos que pueden perderse antes de que se cierre la conexión.
CPCRC	UDINT	CRC de parámetros de conexión. CRC-S32 de los parámetros de conexión de destino incluidos en la petición SafetyOpen de tipo 2.

## Códigos de error del dispositivo CIP Safety

### Códigos de error detectado

Los siguientes códigos y subcódigos de error detectado se aplican al tipo de datos T\_CIP\_SAFETY\_STATUS y se incluyen en los parámetros Status\_IN y Status\_OUT del DDDT del dispositivo CIP Safety.

### Códigos de error detectado

Código de error detectado	Significado
0001	Conexión abierta: sin respuesta.
0002	Conexión abierta: respuesta al error detectado por parte del dispositivo.
0003	Conexión abierta: respuesta no válida por parte del dispositivo.
0004	El servidor (consumidor) no está operativo.
0005	El cliente (productor) no está operativo.

## Subcódigos de error detectado

**NOTA:** Los subcódigos de error detectado que no se incluyan en la lista siguiente son para uso interno de Schneider Electric. En tal caso, notifique el subcódigo de error detectado al servicio de soporte de Schneider Electric.

Subcódigos de error detectado para conexiones abiertas:

Subcódigo de error detectado (hexadecimal)	Significado
0100	Conexión en uso o Forward_Open duplicado.
0103	Combinación de clase de transporte y desencadenador no admitida.
0105	Hay otro origen que ya posee esta configuración.
0106	Hay otro origen que ya posee esta salida.
0107	No se ha encontrado la conexión de destino (Forward_Close).
0108	Parámetro de conexión de red no válido.
0109	Tamaño de conexión no válido.
0110	Dispositivo no configurado.
0111	RPI O->D, RPI D->O o RPI de corrección horaria no admitidos.
0113	Se utilizan todas las instancias del validador de seguridad.
0114	El Device_Vendor_ID (ID del proveedor del dispositivo) o el Device_Product_Code (código de producto del dispositivo) especificados en la clave electrónica no coinciden.
0115	El Device_Type (tipo de dispositivo) especificado en la clave electrónica no coincide.
0116	La Major_Revision (revisión principal) o Minor_Revision (revisión secundaria) especificadas en la clave electrónica no coinciden.
0117	Ruta de aplicación producida o consumida no válida.
0118	Ruta de aplicación de configuración no válida o incoherente.
011A	Objeto de destino sin conexiones.
011B	El RPI es menor que el tiempo de inhibición de producción.
011C	No se admite la clase de transporte.
011D	No se admite el desencadenador de producción.
011E	No se admite la dirección.
0123	Origen no válido para el tipo de conexión de red de destino.
0124	Destino no válido para el tipo de conexión de red de origen.
0126	Tamaño de configuración no válido.

<b>Subcódigo de error detectado (hexadecimal)</b>	<b>Significado</b>
0127	Origen no válido para el tamaño de destino.
0128	Destino no válido para el tamaño de origen.
0129	Ruta de aplicación de configuración no válida.
012A	Ruta de aplicación de consumo no válida.
012B	Ruta de aplicación de producción no válida.
012C	El símbolo de configuración no existe.
012D	El símbolo de consumo no existe.
012E	El símbolo de producción no existe.
012F	Combinación de ruta de aplicación incoherente.
0130	Formato de datos de consumo incoherente.
0131	Formato de datos de producción incoherente.
0203	La conexión ha superado el timeout.
0204	El destino no ha respondido a la petición sin conexión.
0205	Error de parámetro detectado en la petición SafetyOpen.
0207	Confirmación sin conexión y sin respuesta.
0315	Tipo de segmento no válido en la ruta de conexión.
031B	Conexión del módulo ya establecida.
031C	No se aplica ningún otro código de estado ampliado.
031F	No hay más recursos disponibles de consumidor de enlace configurables en el módulo de producción.
0801	Ping_Interval_EIP_Multiplier o Max_Consumer_Number no son válidos en la unión de multidifusión.
0802	Tamaño de conexión de seguridad no válido.
0803	Formato de conexión de seguridad no válido.
0804	Parámetros de conexión de corrección horaria no válidos.
0805	Ping_interval_EIP_Multiplier no válido.
0806	Multiplicador de Time_Coordination_Msg_Min no válido.
0807	Network_Time_Expectation_Mult no válido.
0808	Multiplicador de timeout no válido.
0809	Número de consumidor máximo no válido.

<b>Subcódigo de error detectado (hexadecimal)</b>	<b>Significado</b>
080A	CPCRC no válida.
080B	ID de conexión de corrección horaria no válido.
080C	Discrepancia de SCID.
080D	El TUNID no está configurado.
080E	Discrepancia de TUNID.
080F	Operación de configuración no permitida.

Subcódigos de error detectado para servidor o cliente:

<b>Subcódigo de error detectado (hexadecimal)</b>	<b>Significado</b>
271D	Se recibió un mensaje de coordinación horaria sin el bit Ping_Response configurado.
2730	Mensaje de coordinación horaria: no se ha recibido en el tiempo asignado.
2732	Comprobación de mensaje de coordinación horaria: ya se ha recibido un mensaje procedente de este consumidor con la misma marca de tiempo.
2733	Comprobación de mensaje de coordinación horaria: se ha detectado un error en la comprobación de paridad.
2734	Comprobación de mensaje de coordinación horaria: se ha detectado un error en la comprobación de Ack_Byte_2.
2735	Comprobación de mensaje de coordinación horaria: no se ha recibido dentro del límite de aproximadamente 5 segundos.
2736	Comprobación de mensaje de coordinación horaria: no se ha recibido dentro del mismo intervalo de ping o el siguiente.
2738	Comprobación de mensaje de coordinación horaria: discrepancia de CRC.
2820	Discrepancia de CRC de marca de tiempo.
2821	Valor delta de marca de tiempo igual a cero.
2822	Valor delta de marca de tiempo superior a la expectativa de tiempo de red.
2823	Intervalo de datos de un mensaje erróneo superior a la expectativa de tiempo de red.
2824	Intervalo de datos de un mensaje válido en otros aspectos superior a la expectativa de tiempo de red.
2825	Discrepancia de CRC de datos reales.
2826	Discrepancia de CRC de datos complementados.

Subcódigo de error detectado (hexadecimal)	Significado
282E	Discrepancia de CRC de datos reales (sin cierre de la conexión).
282F	Discrepancia de CRC de datos complementados (sin cierre de la conexión).
2832	Timeout del supervisor de actividad del consumidor.

## DDDT de la CPU autónoma CIP Safety

### Adiciones de CIP Safety a T\_BMEP58\_ECPU\_EXT

El DDDT de la CPU de seguridad autónoma M580 (T\_BMEP58\_ECPU\_EXT) incluye dos variables de CIP Safety:

- CSIO\_SCANNER: estado del bit de control del explorador de E/S CIP Safety. Este campo booleano puede presentar los siguientes valores:
  - 1: Servicio normal.
  - 0: El servicio no funciona con normalidad.

Para obtener información adicional, consulte la lista de parámetros de Modicon M580Modicon M580 .

- CSIO\_HEALTH: estado funcional de los dispositivos CIP Safety vinculados. Esta variable consiste en una matriz de 128 valores booleanos, donde cada bit indica el estado funcional de un único dispositivo vinculado:
  - 1: Servicio normal.
  - 0: El servicio no funciona con normalidad.

Consulte el tema dispositivoEstado del dispositivo (consulte Modicon M580, Hardware, Manual de referencia) para obtener información adicional.

## Diagnósticos del DTM de la CPU

### Diagnósticos a través del DTM de la CPU M580

El DTM de la CPU M580 proporciona los siguientes servicios de diagnóstico:

- Descubrimiento de dispositivos
- Estado funcional del dispositivo de E/S CIP Safety

## Detección de Dispositivos de Seguridad CIP

Cuando se utiliza Control Expert online, puede emplear su servicio de descubrimiento de bus de campo para descubrir dispositivos CIP Safety de primer nivel en la red, es decir, dispositivos que se encuentran directamente conectados a la CPU. Solo podrán descubrirse los dispositivos con un DTM que coincida con un DTM registrado en el **Catálogo DTM** del PC host.

Para descubrir dispositivos, haga clic con el botón derecho del ratón en el DTM de la CPU (BMEP58\_ECPU\_EXT) en el **Navegador DTM** y, a continuación, seleccione **Descubrimiento del bus de campo** para abrir un cuadro de diálogo del mismo nombre en el que se mostrarán los dispositivos descubiertos. Utilice las herramientas de este cuadro de diálogo para añadir DTM de dispositivo al proyecto. Los dispositivos que añada aparecerán bajo la CPU tanto en el **Navegador DTM** como en el árbol de navegación del DTM de la CPU.

Para obtener más información sobre cómo utilizar este servicio, consulte el servicio de detección de bus de Servicio de detección de bus de campo (consulte <sup>™</sup>EcoStruxure Control Expert, Modos de operación) tema.

## Estado de la conexión del dispositivo de seguridad CIP

Cuando se utiliza Control Expert online, se muestra en el árbol de navegación del DTM de la CPU un icono que indica el estado funcional de cada conexión de los dispositivos E/S CIP Safety que se haya añadido al proyecto:

-  indica que la conexión se encuentra en estado RUN (ejecución).
-  indica que la conexión se encuentra en estado STOP (detención), no conectado o desconocido.

Para obtener más información sobre cómo utilizar esta función, consulte el tema DTMI de Control Expert Introducción de diagnósticos en el DTM de Control Expert (consulte Modicon M580, Hardware, Manual de Referencia).

## Diagnósticos de conexión del dispositivo CIP Safety

### Introducción

Los nodos de conexión de un DTM de CIP Safety incluyen dos fichas que permiten identificar y diagnosticar la conexión del dispositivo:

- Información de módulo
- Información de estado

## Ficha Información de módulo

El DTM de CIP Safety presenta la ficha **Información de módulo**, en la que se proporcionan valores estáticos para los siguientes parámetros de identificación de módulos:

- ID del proveedor
- Tipo de producto
- Código de producto
- Revisión de software
- Número de serie
- Nombre de producto
- Dirección MAC

## Ficha Información de estado

El DTM de CIP Safety presenta la ficha **Información de estado**, en la que se proporcionan valores dinámicos para la conexión de la CPU con el dispositivo CIP Safety:

Estado	Descripción
Estado de CIP Safety	<p>Estado actual del dispositivo, según se define en la sección 5-4.2.1.5 "Estado del dispositivo" del estándar CIP Safety:</p> <ul style="list-style-type: none"> <li>• 0: Sin definir</li> <li>• 1: Autoverificación</li> <li>• 2: Inactivo</li> <li>• 3: Excepción de autoverificación</li> <li>• 4: En ejecución</li> <li>• 5: Anular</li> <li>• 6: Fallo grave</li> <li>• 7: Configuración</li> <li>• 8: En espera del TUNID</li> <li>• De 9 a 50: Reservado</li> <li>• 51: En espera del TUNID con par permitido Véase la NOTA</li> <li>• 52: En ejecución con par permitido Véase la NOTA</li> <li>• De 53 a 99: Específico del dispositivo</li> <li>• De 100 a 255: Específico del proveedor</li> </ul> <p><b>NOTA:</b> Solo se permite y define en los perfiles de dispositivos de movimiento de seguridad: 0x2E, 0x2F.</p>
Estado de excepción	<p>Atributo de un solo byte cuyo valor indica el estado de las alarmas y advertencias del dispositivo. Puede proporcionarse en un método básico o ampliado. Para obtener más información, consulte la sección 5-4.2.1.6 "Estado de excepción" del estándar CIP Safety.</p>

<b>Estado</b>	<b>Descripción</b>
Fallo grave	Estado específico del dispositivo. Consulte el manual del dispositivo para obtener más información.
Fallo leve	Estado específico del dispositivo. Consulte el manual del dispositivo para obtener más información.
Dirección IP	Dirección IP del dispositivo CIP Safety, configurada en el DTM de la CPU, página 373 M580.
TUNID	Identificador de red único de destino
OUNID	Identificador de red único de origen, página 357
Estado de bloqueo	Estado de la configuración del dispositivo, realizada mediante una herramienta de configuración de red de seguridad (SNCT): <ul style="list-style-type: none"><li>• Bloqueado: la configuración es de solo lectura.</li><li>• Desbloqueado: la configuración es de lectura/escritura.</li></ul>
Firma de configuración	Identificador de configuración de seguridad (SCID, página 368) de la conexión del dispositivo de destino.

---

# Apéndices

## Contenido de esta parte

IEC 61508 .....	397
Objetos de sistema .....	405
Referencias de SRAC .....	412

## Introducción

Los apéndices contienen información sobre IEC 61508 y su política de SIL. Además, se proporcionan datos técnicos sobre los módulos de seguridad y los no interferentes y se llevan a cabo cálculos de ejemplo.

# IEC 61508

## Contenido de este capítulo

Información general sobre IEC 61508.....	398
Política de SIL .....	400

## Introducción

En este capítulo se proporciona información sobre los conceptos de seguridad de IEC 61508 en general y su política de SIL en particular.

# Información general sobre IEC 61508

## Introducción

Los sistemas relacionados con la seguridad se desarrollan para su uso en procesos en los que el riesgo para las personas, el entorno, los equipos y la producción se deben limitar a un nivel aceptable. El riesgo depende de la gravedad y la probabilidad, que sirven para definir las medidas de protección necesarias.

Por lo que respecta a la seguridad de los procesos, hay 2 aspectos que se deben tener en cuenta:

- Las normativas y los requisitos definidos por las autoridades oficiales para ayudar a proteger a las personas, el entorno, los equipos y la producción
- Las medidas mediante las cuales se cumplen estas normativas y estos requisitos

## Descripción de IEC 61508

La norma técnica que define los requisitos para los sistemas relacionados con la seguridad es

- la IEC 61508.

Aborda la seguridad funcional de sistemas relacionados con la seguridad eléctricos, electrónicos o electrónicos programables. Un sistema relacionado con la seguridad es un sistema necesario para realizar una o varias funciones específicas para garantizar que los riesgos queden limitados a un nivel aceptable. Estas funciones se definen como funciones de seguridad. Un sistema se define como funcionalmente seguro si los fallos aleatorios, sistemáticos y de causa común no provocan el mal funcionamiento del sistema, no producen lesiones o la muerte de personas ni contribuyen a la contaminación del medio ambiente ni a la pérdida de producción o equipos.

La norma define un enfoque genérico para todas las actividades del ciclo de vida para los sistemas que se utilizan para realizar funciones de seguridad. Constituye los procedimientos que se deben utilizar para el diseño, el desarrollo y la validación del hardware y el software que se aplican en los sistemas relacionados con la seguridad. Además, determina reglas por lo que respecta a la gestión de la seguridad funcional y a su documentación.

## Descripción de IEC 61511

Los requisitos de seguridad funcional definidos en IEC 61508 están específicamente adaptados al sector de la industria de procesos en la norma técnica siguiente:

- IEC 61511: Seguridad funcional. Sistemas instrumentados de seguridad para el sector de la industria de procesos

Esta norma orienta al usuario para la aplicación de un sistema relacionado con la seguridad, desde la primera fase de un proyecto y hasta su puesta en marcha, y cubre las modificaciones y las actividades finales de retirada del servicio. En resumen, aborda el ciclo de vida de seguridad de todos los componentes de un sistema relacionado con la seguridad utilizado en la industria de procesos.

## Descripción de riesgo

La norma IEC 61508 se basa en los conceptos de análisis de riesgos y seguridad funcional. El riesgo depende de la gravedad y la probabilidad. Se puede reducir a un nivel tolerable aplicando una función de seguridad que consista en un sistema eléctrico, electrónico o electrónico programable. Además, se debe reducir a un nivel tan bajo como sea razonablemente posible.

En resumen, la norma IEC 61508 considera los riesgos tal como se indica a continuación:

- El riesgo cero nunca puede alcanzarse.
- La seguridad debe considerarse desde el principio.
- Los riesgos intolerables deben reducirse.

# Política de SIL

## Introducción

El valor de SIL evalúa la robustez de una aplicación frente a los fallos, y de este modo indica la capacidad de un sistema para llevar a cabo una función de seguridad dentro de una probabilidad definida. La norma IEC 61508 especifica 4 niveles de rendimiento de seguridad en función del riesgo o de las repercusiones que causa el proceso para el que se utiliza el sistema relacionado con la seguridad. Cuanto más peligrosas sean las posibles repercusiones sobre la comunidad y el entorno, más estrictos serán los requisitos de seguridad para reducir el riesgo.

## Descripción del valor de SIL

Nivel binario (1 de 4 niveles posibles) empleado para especificar los requisitos de integridad de seguridad de las funciones de seguridad que se asignarán a los sistemas relacionados con la seguridad, en el que la integridad de seguridad 4 es la de nivel más alto y la integridad de seguridad 1 es la de nivel más bajo. SIL para baja demanda, página 402.

## Descripción de los requisitos de SIL

Para alcanzar la seguridad funcional, se necesitan dos tipos de requisitos:

- Requisitos de funciones de seguridad, que definen qué funciones se deben llevar a cabo
- Requisitos de integridad de seguridad, que definen el grado de certeza necesario para que se lleven a cabo las funciones de seguridad

Los requisitos de la función de seguridad se derivan del análisis de riesgos y los de integridad de seguridad se derivan de la evaluación de riesgos.

Constan de las cantidades siguientes:

- Tiempo medio entre fallos
- Probabilidades de fallo
- Frecuencias de fallos
- Cobertura del diagnóstico
- Fracción de fallo seguro
- Tolerancia de errores de hardware

En función del nivel de integridad de seguridad, estas cantidades deben estar dentro de los límites definidos.

**NOTA:** Para poder combinar diferentes dispositivos de nivel de integridad de seguridad en una función de red o seguridad, es necesario cumplir estrictamente los requisitos de la norma IEC 61508. Dicha combinación, además, conlleva implicaciones operativas y de diseño.

## Descripción de la clasificación SIL

Tal como se define en la norma IEC 61508, el valor de SIL está limitado por la fracción de fallo seguro (SFF) y la tolerancia de errores de hardware (HFT) del subsistema que lleva a cabo la función de seguridad. Un valor de HFT de  $n$  significa que  $n + 1$  fallos podrían provocar una pérdida de la función de seguridad y que no se pueda entrar en el estado de seguridad. El valor de SFF depende de las frecuencias de fallos y la cobertura de diagnóstico.

En la tabla siguiente se muestra la relación entre SFF, HFT y SIL para los subsistemas relacionados con la seguridad de acuerdo con la norma IEC 61508-2, en que las modalidades de fallo de todos los componentes no se pueden definir por completo:

SFF	HFT = 0	HFT = 1	HFT = 2
$SFF \leq 60 \%$	-	SIL1	SIL2
$60 \% < SFF \leq 90 \%$	SIL1	SIL2	SIL3
$90 \% < SFF \leq 99 \%$	SIL2	SIL3	SIL4
$SFF > 99 \%$	SIL3	SIL4	SIL4

Hay 2 maneras alcanzar un determinado nivel de integridad de seguridad:

- Aumentando el valor de HFT proporcionando circuitos de desconexión independientes adicionales
- Aumentando el valor de SFF mediante diagnósticos adicionales

## Descripción de la relación SIL-demanda

La norma IEC 61508 distingue la modalidad de funcionamiento de baja demanda y la de alta demanda (o continua).

En la modalidad de baja demanda, la frecuencia de demanda para el funcionamiento en un sistema relacionado con la seguridad no es superior a una al año ni al doble de la frecuencia de prueba. El valor de SIL para un sistema relacionado con la seguridad de baja demanda está directamente relacionado con su probabilidad media de fallo para llevar a

cabo su función de seguridad a demanda o, simplemente, la probabilidad de fallo a petición (PFD).

En la modalidad de alta demanda o continua, la frecuencia de demanda para el funcionamiento en un sistema relacionado con la seguridad es superior a una al año y al doble de la frecuencia de prueba. El valor de SIL para un sistema relacionado con la seguridad de alta demanda está directamente relacionado con la probabilidad de que se produzca un fallo peligroso por hora o, simplemente, la probabilidad de fallo por hora (PFH).

## SIL para baja demanda

En la tabla siguiente se enumeran los requisitos para un sistema en una modalidad de funcionamiento de baja demanda:

Nivel de integridad de seguridad («Safety Integrity Level»)	Probabilidad de fallo a petición
4	$De \geq 10^{-5} \text{ a } < 10^{-4}$
3	$De \geq 10^{-4} \text{ a } < 10^{-3}$
2	$De \geq 10^{-3} \text{ a } < 10^{-2}$
1	$De \geq 10^{-2} \text{ a } < 10^{-1}$

## SIL para alta demanda

En la tabla siguiente se enumeran los requisitos para un sistema en una modalidad de funcionamiento de alta demanda:

Nivel de integridad de seguridad («Safety Integrity Level»)	Probabilidad de fallo por hora
4	$De \geq 10^{-9} \text{ a } < 10^{-8}$
3	$De \geq 10^{-8} \text{ a } < 10^{-7}$
2	$De \geq 10^{-7} \text{ a } < 10^{-6}$
1	$De \geq 10^{-6} \text{ a } < 10^{-5}$

Para SIL3, las probabilidades de fallo que se requieren para el sistema integrado de seguridad completo son las siguientes:

- PFD de  $\geq 10^{-4}$  a  $< 10^{-3}$  para baja demanda
- PFH  $\geq$  de  $10^{-8}$  a  $< 10^{-7}$  para alta demanda

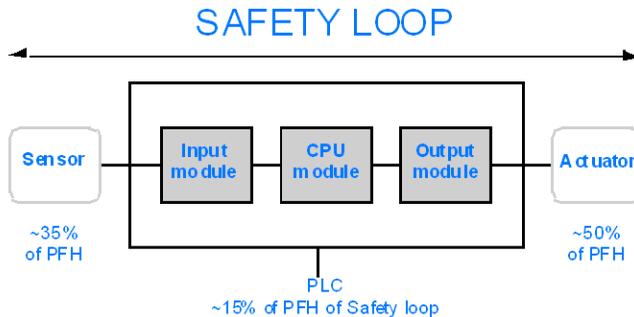
## Descripción del bucle de seguridad

El bucle de seguridad al que pertenece el PAC de seguridad M580 consta de las tres partes siguientes:

- Sensores
- PAC de seguridad M580 con fuente de alimentación de seguridad, CPU de seguridad, coprocesador de seguridad y módulos de E/S de seguridad
- Actuadores

Una placa de conexiones o una conexión remota que incluye un conmutador o un CRA no destruye un bucle de seguridad. Las placas de conexiones, los conmutadores y los módulos CRA forman parte de un "canal negro". Esto significa que los datos que intercambian la E/S y el PAC no se pueden dañar sin que lo detecte el receptor.

La figura siguiente muestra un bucle de seguridad típico:



Tal como se muestra en la figura anterior, la aportación del PAC es sólo del 10-20 % porque la probabilidad de fallo de los sensores y actuadores suele ser bastante elevada.

Una presuposición conservadora del 10 % para la aportación del PAC de seguridad a la probabilidad general deja más margen para el usuario y da como resultado las siguientes probabilidades de fallo requeridas para el PAC de seguridad:

- $PFD \geq \text{de } 10^{-5} \text{ a } < 10^{-4}$  para baja demanda
- $PFH \geq \text{de } 10^{-9} \text{ a } < 10^{-8}$  para alta demanda

## Descripción de la ecuación de PFD

La norma IEC 61508 presupone que la mitad de los fallos termina en un estado de seguridad. Por lo tanto, la frecuencia de fallos  $\lambda$  se divide en

- $\lambda_s$ , el fallo seguro, y

- $\lambda_D$ , el fallo peligroso, que consta a su vez de
  - $\lambda_{DD}$ , el fallo peligroso detectado por el diagnóstico interno, y
  - $\lambda_{DU}$ , el fallo peligroso no detectado.

La frecuencia de fallos se puede calcular utilizando el tiempo medio entre fallos (MTBF), un valor específico del módulo, tal como se indica a continuación:

$$\lambda = 1/\text{MTBF}$$

La ecuación para calcular la probabilidad de fallo a petición es:

$$\text{PFD}(t) = \lambda_{DU} \times t$$

$t$  representa el tiempo entre 2 pruebas.

La probabilidad de fallo por hora implica un intervalo de tiempo de 1 hora. Por lo tanto, la ecuación de PFD se reduce a la siguiente:

$$\text{PFH} = \lambda_{DU}$$

# Objetos de sistema

## Contenido de este capítulo

Bits del sistema de seguridad M580 .....	406
Palabras del sistema de seguridad M580.....	408

## Introducción

En este capítulo se describen los bits y las palabras del PAC de seguridad M580.

**NOTA:** Los símbolos asociados a cada objeto de bit o palabra de sistema a los que se hace referencia en las tablas descriptivas de dichos objetos no están incluidos en el programa, pero se pueden introducir mediante el editor de datos.

## Bits del sistema de seguridad M580

### Bits del sistema para la ejecución de la tarea SAFE

Los siguientes bits del sistema se aplican al PAC de seguridad M580. Para obtener una descripción de los bits de sistema que se aplican tanto al PAC de seguridad M580 como a los PAC M580 que no son de seguridad, consulte la información sobre los *Bits de sistema* en *EcoStruxure™ Control Expert, Palabras y bits de sistema - Manual de referencia*.

Estos bits del sistema están relacionados con la ejecución de la tarea SAFE, pero no se puede acceder directamente a ellos en el código del programa de seguridad. Sólo se puede acceder a ellos a través de los bloques `S_SYST_READ_TASK_BIT_MX` y `S_SYST_RESET_TASK_BIT_MX`.

Bit Icono	Función	Descripción	Estado inicial	Tipo
%S17 CARRY	Salida de desplazamiento circular	Durante una operación de desplazamiento circular en la tarea SAFE, este bit adopta el estado del bit saliente.	0	L/E
%S18 OVERFLOW	Se ha detectado un desborde o un error aritmético	Normalmente en estado 0, este bit pasa a 1 en caso de desborde de la capacidad si: <ul style="list-style-type: none"> <li>El resultado es superior a +32 767 o inferior a -32 768, en longitud simple.</li> <li>El resultado es superior a +65 535, en un entero sin signo.</li> <li>El resultado es superior a +2 147 483 647 o inferior a -2 147 483 648, en longitud doble.</li> <li>El resultado es superior a +4 294 967 296, en longitud doble o entero sin signo.</li> <li>División entre 0.</li> <li>La raíz de un número negativo.</li> <li>Se fuerza un paso inexistente en un programador cíclico.</li> <li>Apilamiento de un registro completo, vaciado de un registro ya vacío.</li> </ul>	0	L/E
%S21 1RSTTASKRUN	Primera exploración de tarea SAFE en RUN	Probado en la tarea SAFE, este bit indica el primer ciclo de esta tarea. Se pone a 1 al comienzo del ciclo y se resetea a 0 al final del ciclo. <b>NOTA:</b> <ul style="list-style-type: none"> <li>El primer ciclo del estado de la tarea se puede leer utilizando la salida <code>SCOLD</code> del bloque de funciones del sistema <code>S_SYST_STAT_MX</code>.</li> <li>Este bit no es efectivo para los sistemas Hot Standby de M580 Safety.</li> </ul>	0	L/E

## Notas relacionadas con los bits de sistema que no son específicos de seguridad

Bit de sistema	Descripción	Notas
%S0	arranque en frío	Sólo se puede utilizar en tareas de proceso (no SAFE) y no influye en la tarea SAFE.
%S9	salidas establecidas en retorno	No influye en los módulos de salida de seguridad.
%S10	error detectado en E/S global	Notifica algunos de los posibles errores detectados (no todos) relacionados con los módulos de E/S de seguridad.
%S11	desborde del watchdog	Tiene en cuenta un desborde en una tarea SAFE.
%S16	error detectado en las E/S de tarea	Notifica algunos de los posibles errores detectados (no todos) relacionados con los módulos de E/S de seguridad.
%S19	desborde de periodo de tareas	La información sobre el desborde de tarea SAFE no está disponible.
%S40-47	Error de E/S detectado en bastidor <i>n</i>	Notifica algunos de los posibles errores detectados (no todos) relacionados con los módulos de E/S de seguridad.
%S78	STOP al detectar un error	Se aplica tanto a las tareas de proceso como a la tarea SAFE. Si el bit está establecido, por ejemplo, si surge un error de desborde %S18, la tarea SAFE pasa al estado HALT.
%S94	Guardar valores ajustados	No se aplica a las variables SAFE. Los valores iniciales SAFE no se pueden modificar con la activación de este bit.
%S117	Error detectado por RIO en red E/S Ethernet	Notifica algunos de los posibles errores detectados (no todos) relacionados con los módulos de E/S de seguridad.
%S119	error general detectado en el bastidor	Notifica algunos de los posibles errores detectados (no todos) relacionados con los módulos de E/S de seguridad.

## Palabras del sistema de seguridad M580

### Palabras del sistema para los PAC de seguridad M580

Las siguientes palabras del sistema se aplican al PAC de seguridad M580. Para ver una descripción de las palabras de sistema que se aplican tanto al PAC de seguridad M580 como a los PAC M580 que no son de seguridad, consulte la información sobre las *Palabras de sistema* en *EcoStruxure™ Control Expert, Palabras y bits de sistema - Manual de referencia*.

Estas palabras y estos valores del sistema están relacionados con la tarea SAFE. Se puede acceder a ellos desde el código del programa de aplicación en las secciones que no son de seguridad (MAST, FAST, AUX0 o AUX1), pero no desde el código de la sección de la tarea SAFE.

Palabra	Función	Tipo
%SW4	Periodo de la tarea SAFE definido en la configuración. El operador no puede modificar el periodo.	L
%SW12	Indica la modalidad de funcionamiento del módulo Copro: <ul style="list-style-type: none"> <li>• 16#A501 = modalidad de mantenimiento</li> <li>• 16#5AFE = modalidad de seguridad</li> </ul> Cualquier otro valor se detecta como un error.	L
%SW13	Indica la modalidad de funcionamiento de la CPU: <ul style="list-style-type: none"> <li>• 16#501A = modalidad de mantenimiento</li> <li>• 16#5AFE = modalidad de seguridad</li> </ul> Cualquier otro valor se detecta como un error.	L
%SW42	Tiempo actual de la tarea SAFE. Indica el tiempo de ejecución del último ciclo de la tarea SAFE (en ms).	L
%SW43	Tiempo máx. de la tarea SAFE. Indica el tiempo de ejecución más largo de la tarea SAFE desde el último arranque en frío (en ms).	L
%SW44	Tiempo mín. de la tarea SAFE. Indica el tiempo de ejecución más corto de la tarea SAFE desde el último arranque en frío (en ms).	L
%SW110	Porcentaje de la carga de la CPU del sistema utilizada por el sistema para los servicios internos.	L
%SW111	Porcentaje de la carga de la CPU del sistema utilizada por la tarea MAST.	L
%SW112	Porcentaje de la carga de la CPU del sistema utilizada por la tarea FAST.	L
%SW113	Porcentaje de la carga de la CPU del sistema utilizada por la tarea SAFE.	L
%SW114	Porcentaje de la carga de la CPU del sistema utilizada por la tarea AUX0.	L
%SW115	Porcentaje de la carga de la CPU del sistema utilizada por la tarea AUX1.	L

Palabra	Función	Tipo
%SW116	Total de la carga de la CPU del sistema.	L
%SW124	<p>Contiene la causa del error detectado no recuperable cuando el PAC de seguridad M580 se encuentra en estado HALT (pausa):</p> <ul style="list-style-type: none"> <li>• 0x5AF2: Error de RAM detectado en la comprobación de memoria.</li> <li>• 0x5AFB: Se ha detectado un error en el código del firmware de seguridad.</li> <li>• 0x5AF6: Se ha detectado un error de desborde del watchdog de seguridad en la CPU.</li> <li>• 0x5AFF: Se ha detectado un error de desborde del watchdog de seguridad en el coprocesador.</li> <li>• 0x5B01: No se ha detectado el coprocesador durante el arranque.</li> <li>• 0x5AC03: Error no recuperable de CIP Safety detectado por la CPU.</li> <li>• 0x5AC04: Error no recuperable de CIP Safety detectado por el coprocesador.</li> </ul> <p><b>NOTA:</b> La lista anterior no es exhaustiva. Para obtener más información, consulte <i>EcoStruxure™ Control Expert, Palabras y bits de sistema - Manual de referencia</i>.</p>	L
%SW125	<p>Contiene la causa del error recuperable detectado en el PAC de seguridad M580:</p> <ul style="list-style-type: none"> <li>• 0x5AC0: La configuración de CIP Safety no es correcta (detectado por la CPU).</li> <li>• 0x5AC1: La configuración de CIP Safety no es correcta (detectado por el coprocesador).</li> <li>• 0x5AF3: La CPU principal ha detectado un error de comparación.</li> <li>• 0x5AFC: El coprocesador ha detectado un error de comparación.</li> <li>• 0x5AFD: El coprocesador ha detectado un error interno.</li> <li>• 0x5AFE: Se ha detectado un error de sincronización entre la CPU y el coprocesador.</li> <li>• 0x9690: Se ha detectado un error de suma de comprobación del programa de aplicación.</li> </ul> <p><b>NOTA:</b> La lista anterior no es exhaustiva. Para obtener más información, consulte <i>EcoStruxure™ Control Expert, Palabras y bits de sistema - Manual de referencia</i>.</p>	L
%SW126	Estas dos palabras del sistema contienen información de uso interno de Schneider Electric para ayudar a analizar un error detectado de manera más detallada.	L
%SW127		
%SW128	<p>Con la versión del firmware 3.10 de la CPU o una versión anterior, fuerza la sincronización horaria entre la hora NTP y la hora SAFE en los módulos de E/S seguros y la tarea de CPU SAFE:</p> <ul style="list-style-type: none"> <li>• El cambio de valor de 16#1AE5 a 16#E51A fuerza la sincronización. Consulte el tema <i>Procedimiento de sincronización de los ajustes de hora de NTP</i>, página 182.</li> <li>• Otros valores y secuencias no fuerzan la sincronización.</li> </ul>	L/E
%SW142	Contiene la versión del firmware COPRO de seguridad en BCD de 4 dígitos: por ejemplo, la versión de firmware 21.42 corresponde a %SW142 = 16#2142.	L

Palabra	Función	Tipo
%SW148	Recuento de errores de código de corrección de errores (ECC) detectados por la CPU.	L
%SW152	Estado de la hora de la CPU de NTP actualizado por el módulo de comunicaciones Ethernet (por ejemplo, BMENOC0301/11) a través de la placa de conexiones X Bus y la función opcional de sincronización de hora forzada: <ul style="list-style-type: none"> <li>• 0: El módulo de comunicaciones Ethernet no actualiza la hora de la CPU.</li> <li>• 1: El módulo de comunicaciones Ethernet actualiza la hora de la CPU.</li> </ul>	L
%SW169	ID de aplicación de seguridad: Contiene un ID de la parte del código de seguridad de la aplicación. El ID se modifica automáticamente cuando se modifica el código de la aplicación segura. <p><b>NOTA:</b></p> <ul style="list-style-type: none"> <li>• Si se ha cambiado el código seguro y se ha ejecutado un comando <b>Generar cambios</b> desde el comando <b>Regenerar todo</b> anterior (con lo que también se cambia el ID de aplicación de seguridad), es posible que, al ejecutar el comando <b>Regenerar todo</b>, vuelva a cambiar el ID de aplicación de seguridad.</li> <li>• El identificador exclusivo del programa SAFE se puede leer utilizando la salida SAID del bloque de funciones del sistema S_SYST_STAT_MX.</li> </ul>	L
%SW171	Estado de las tareas FAST: <ul style="list-style-type: none"> <li>• 0: No hay tareas FAST</li> <li>• 1: Detener</li> <li>• 2: Ejecutar</li> <li>• 3: Punto de parada</li> <li>• 4: Pausa</li> </ul>	L
%SW172	Estado de la tarea SAFE: <ul style="list-style-type: none"> <li>• 0: No hay ninguna tarea SAFE</li> <li>• 1: Detener</li> <li>• 2: Ejecutar</li> <li>• 3: Punto de parada</li> <li>• 4: Pausa</li> </ul>	L
%SW173	Estado de la tarea MAST: <ul style="list-style-type: none"> <li>• 0: No hay ninguna tarea MAST</li> <li>• 1: Detener</li> <li>• 2: Ejecutar</li> <li>• 3: Punto de parada</li> <li>• 4: Pausa</li> </ul>	L

Palabra	Función	Tipo
%SW174	Estado de la tarea AUX0: <ul style="list-style-type: none"><li>• 0: No hay ninguna tarea AUX0</li><li>• 1: Detener</li><li>• 2: Ejecutar</li><li>• 3: Punto de parada</li><li>• 4: Pausa</li></ul>	L
%SW175	Estado de la tarea AUX1: <ul style="list-style-type: none"><li>• 0: No hay ninguna tarea AUX1</li><li>• 1: Detener</li><li>• 2: Ejecutar</li><li>• 3: Punto de parada</li><li>• 4: Pausa</li></ul>	L

# Referencias de SRAC

El plan de verificación de las condiciones de aplicación relacionadas con la seguridad (SRAC) proporciona una trama genérica para justificar que se han cumplido las instrucciones del manual de instalación y seguridad asociado. Estas instrucciones de la documentación del *Modicon M580, Manual de seguridad* se enumeran como requisitos.

En la tabla siguiente se proporciona el título del párrafo donde puede encontrar los requisitos relacionados con el ciclo de vida de la aplicación:

Requisitos del ciclo de vida de la aplicación	
ID	En este lugar
LC #1	Paso 9: Especificación de requisitos de seguridad del sistema E/E/PE, página 37
LC #2	Paso 9: Especificación de requisitos de seguridad del sistema E/E/PE, página 37
LC #3	Paso 10: Realización de sistemas relacionados con la seguridad E/E/PE, página 37
LC #4	Paso 12: Instalación y puesta en marcha globales, página 41
LC #5	Paso 12: Instalación y puesta en marcha globales, página 41
LC #6	Paso 13: Validación de seguridad global, página 42
LC #7	Paso 14: Funcionamiento, mantenimiento y reparación globales, página 43
LC #8	Paso 15: Modificación y modernización globales, página 43

En la tabla siguiente se proporciona el título del párrafo donde puede encontrar los requisitos relacionados con el mensaje de información de seguridad:

Requisito de mensaje de información de seguridad	
ID	En este lugar
SM #1	Antes de empezar, página 10
SM #2	Iniciar y probar, página 11
SM #3	Bucle de seguridad, página 17
SM #4	Módulos no interferentes, página 29

<b>Requisito de mensaje de información de seguridad</b>	
<b>ID</b>	<b>En este lugar</b>
SM #5	Fuente de alimentación externa utilizada con E/S de seguridad digital, página 48
SM #6	Ejemplos de cableado de aplicación de entrada BMXSAI0410, introducción, página 55
SM #7	Ejemplos de cableado de aplicación de entrada BMXSAI0410, SIL3 Cat2/PLd, página 57
#8 SM	Ejemplos de cableado de aplicación de entrada BMXSAI0410, SIL3 Cat2/PLd con alta disponibilidad, página 58
SM #9	Ejemplos de cableado de aplicación de entrada BMXSAI0410, SIL3 Cat4/PLe, página 59
SM #10	Ejemplos de cableado de aplicación de entrada BMXSAI0410, SIL3 Cat4/PLe con alta disponibilidad, página 60
SM #11	Conector de cableado BMXSDI1602, fuente de alimentación de proceso, página 67
SM #12	Conector de cableado BMXSDI1602, fusible, página 68
SM #13	BMXSDI1602 Ejemplos de cableado de aplicación de entrada, introducción, página 73
SM #14	Diagnósticos de cableado configurables en Control Expert, página 74
SM #15	BMXSDI1602 Ejemplos de cableado de aplicación de entrada, SIL3 Cat2/PLd, página 75
SM #16	BMXSDI1602 Ejemplos de cableado de aplicación de entrada, SIL3 Cat2/PLd, página 75
SM #17	BMXSDI1602 Ejemplos de cableado de aplicación de entrada, SIL3 Cat2/PLd, página 75
SM #18	Ejemplos de cableado de aplicación de entrada BMXSDI1602, SIL3 Cat2/PLd con alta disponibilidad, página 77
SM #19	Ejemplos de cableado de aplicación de entrada BMXSDI1602, SIL3 Cat2/PLd con alta disponibilidad, página 77
SM #20	Ejemplos de cableado de aplicación de entrada BMXSDI1602, SIL3 Cat2/PLd con alta disponibilidad, página 77
SM #21	Ejemplos de cableado de aplicación de entrada BMXSDI1602, SIL3 Cat2/PLd con alta disponibilidad, página 77
SM #22	Ejemplos de cableado de aplicación de entrada BMXSDI1602, SIL3 Cat2/PLd con alta disponibilidad, página 77
SM #23	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe, página 81

<b>Requisito de mensaje de información de seguridad</b>	
<b>ID</b>	<b>En este lugar</b>
SM #24	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe, página 81
SM #25	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe, página 81
SM #26	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe, página 81
SM #27	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe, página 81
SM #28	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe, página 81
SM #29	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe, página 81
SM #30	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe, página 81
SM #31	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe con alta disponibilidad, página 88
SM #32	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe con alta disponibilidad, página 88
SM #33	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe con alta disponibilidad, página 88
SM #34	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe con alta disponibilidad, página 88
SM #35	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe con alta disponibilidad, página 88
SM #36	Ejemplos de cableado de aplicación de entrada BMXSDI1602, Cat4/PLe con alta disponibilidad, página 88
SM #37	Conector de cableado BMXSDO0802, fusible, página 101
SM #38	BMXSDO0802 Ejemplos de cableado de aplicación de salida, introducción, página 104
SM #39	BMXSDO0802 Ejemplos de cableado de aplicación de salida, introducción, página 104
SM #40	Diagnóstico de cableado configurable en Control Expert, página 105
SM #41	Resumen de diagnóstico de cableado de salida, página 108
SM #42	Resumen de diagnóstico de cableado de salida, página 108

<b>Requisito de mensaje de información de seguridad</b>	
<b>ID</b>	<b>En este lugar</b>
SM #43	Resumen de diagnóstico de cableado de salida, página 108
SM #44	Resumen de diagnóstico de cableado de salida, página 108
SM #45	Resumen de diagnóstico de cableado de salida, página 108
SM #46	Resumen de diagnóstico de cableado de salida, página 108
SM #47	Conector de cableado BMXSRA0405, fusible, página 116
SM #48	Application_1: 4 salidas, SIL2/Cat2/PLc, estado deenergizado, no hay prueba de señal automática, página 119
SM #49	Application_3: 4 salidas, SIL2/Cat2/PLc, estado deenergizado, no hay prueba de señal automática, página 120
SM #50	Application_5: 2 salidas, SIL3/Cat4/PLe, estado deenergizado, no hay prueba de señal automática, página 121
SM #51	Application_7: 2 salidas, SIL3/Cat4/PLe, estado energizado, no hay prueba de señal automática, página 122
SM #52	Fuentes de alimentación de seguridad de M580, introducción, página 133
SM #53	Descripción del tiempo para módulos de salida, página 160
SM #54	Configuración de los periodos máximos de las tareas SAFE y FAST de la CPU, página 164
SM #55	Funciones y bloques de funciones de seguridad certificados, página 169
SM #56	Configuración de la sincronización horaria con la versión del firmware de la CPU 3.10 o anterior, Introducción, página 180
SM #57	Cambio de los ajustes de hora de NTP durante las operaciones, página 181
SM #58	Procedimiento de sincronización de los ajustes de hora de NTP, página 182
SM #59	Procedimiento de sincronización de los ajustes de hora de NTP, página 182
SM #60	Configuración del DFB S_WR_ETH_MX, página 194
SM #61	Configuración del DFB S_RD_ETH_MX, página 196

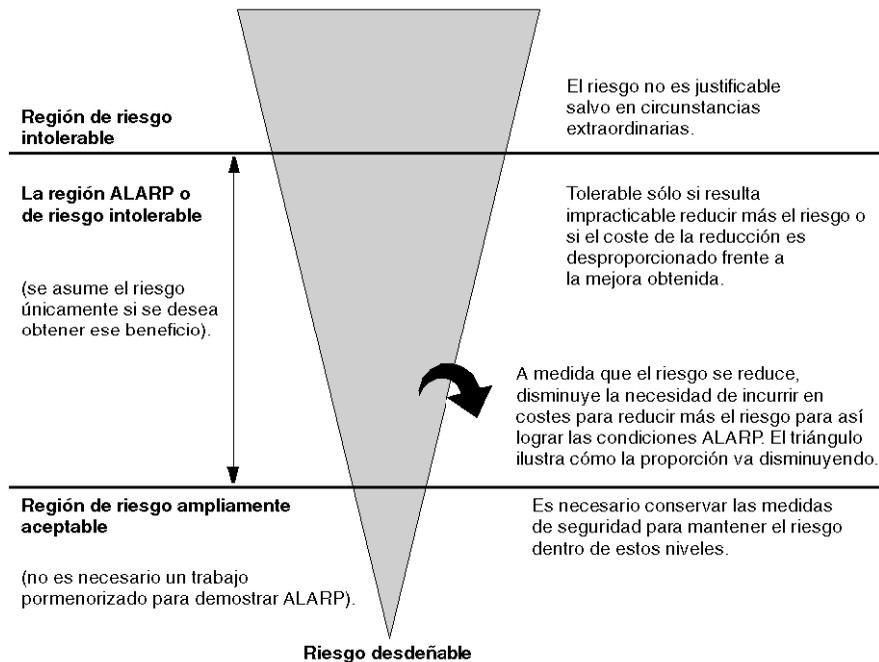
<b>Requisito de mensaje de información de seguridad</b>	
<b>ID</b>	<b>En este lugar</b>
SM #62	Configuración del DFB S_WR_ETH_MX2, página 207
SM #63	Configuración del DFB S_RD_ETH_MX2, página 210
SM #64	Comunicaciones de canal negro de M580, página 213
SM #65	Comunicaciones de canal negro de M580, página 213
SM #66	LED de diagnóstico de la CPU de seguridad de M580, página 224
SM #67	Funcionalidad del modo de mantenimiento, página 262
SM #68	Secuencias de arranque, arranque en caliente, página 275
SM #69	Bloqueo de la configuración de un módulo de E/S de seguridad, página 288
SM #70	Visualización de datos en pantallas de operador, página 295
SM #71	Configuración del dispositivo CIP Safety mediante una herramienta facilitada por el proveedor, página 361
SM #72	Interacciones entre las operaciones del PAC de seguridad y la conexión de destino, página 381

# Glosario

## A

### ALARP:

(del inglés *As Low As Reasonably Practicable*, tan bajo como sea razonablemente posible)  
(Definición IEC 61508)



## C

### CCF:

(del inglés *Common Cause Failure*, fallo de causa común) Fallo que se produce cuando uno o varios eventos causan fallos coincidentes de dos o más canales independientes de un sistema de varios canales, lo que ocasiona un fallo del sistema. (Definición IEC 61508)  
El factor de causa común en un sistema de dos canales es un factor fundamental para el cálculo de la probabilidad de fallo a petición (PFD) de todo el sistema.

---

**CPCRC:**

(*connection parameter cyclic redundancy check, comprobación de redundancia cíclica de parámetros de conexión*) CRC-S32 de los parámetros de la conexión de destino generados por la CSS de cada conexión CIP Safety, e incluida en la petición SafetyOpen de tipo 2.

**D****DDDT:**

(del inglés *Device Derived Data Type*, tipo de datos derivados de dispositivo) Un DDT predefinido por el fabricante y que el usuario no puede modificar. Contiene los elementos del lenguaje de E/S de un módulo de E/S.

**DRS:**

(*conmutador de anillo dual, del inglés, dual-ring switch*) Conmutador gestionado ampliado de ConneXium que se ha configurado para operar en una red Ethernet. Schneider Electric facilita los archivos de configuración predeterminados para descargarlos en un DRS y admitir las funciones especiales de la arquitectura de anillo principal/subanillo.

**DTM:**

(*gestor de tipos de dispositivo, del inglés, device type manager*) Un DTM es un controlador de dispositivos que se ejecuta en el PC host. Ofrece una estructura unificada para acceder a los parámetros de dispositivo, configurar y utilizar los dispositivos, y solucionar problemas de los dispositivos. Los DTM pueden incluir desde una simple interfaz gráfica de usuario (IGU) para configurar parámetros de dispositivo hasta una aplicación sofisticada que permite realizar cálculos complejos en tiempo real con fines de diagnóstico y mantenimiento. En el contexto de un DTM, un dispositivo puede ser un módulo de comunicaciones o un dispositivo remoto de la red.

Consulte FDT.

**E****EDS:**

(*hoja de datos electrónica*) Las EDS son archivos de texto simples en los que se describen las funciones de configuración de un dispositivo. Los archivos EDS los genera y mantiene el fabricante del dispositivo.

**estación RIO:**

Un bastidor de módulos de E/S Ethernet, gestionados por un adaptador RIO, con entradas y salidas incluidas en la exploración RIO de la CPU. Una estación puede ser un bastidor simple o un bastidor principal con un bastidor ampliado.

---

**EUC:**

(del inglés *Equipment Under Control*, equipo bajo control) (Definición IEC 61508) Este término se refiere a equipos, maquinaria, aparatos o plantas utilizados para la fabricación, proceso, transporte, actividades médicas u otras actividades.

**H****HFT:**

(del inglés *Hardware Fault Tolerance*, tolerancia de errores de hardware) (Definición IEC 61508)

Una tolerancia de errores de hardware de valor N indica que N + 1 errores podrían ocasionar la pérdida de la función de seguridad. Por ejemplo:

- HFT = 0: El primer error podría causar una pérdida de la función de seguridad
- HFT = 1: La combinación de dos errores podría causar una pérdida de la función de seguridad. Existen dos rutas diferentes para llegar a un estado de seguridad. La pérdida de la función de seguridad implica que no se puede entrar en un estado de seguridad.

**O****OUNID:**

(*originator unique network identifier, identificador de red único de origen*) Valor que identifica de manera unívoca al dispositivo de origen de una conexión (por lo general, una CPU) en una red CIP Safety. El OUNID consta de:

- un número de red de seguridad (safety network number, SNN), que puede ser una marca de tiempo u otro valor definido por el usuario.
- una dirección de nodo (en el caso de redes EtherNet/IP, la dirección IP).

**P****PST:**

(del inglés *Process Safety Time*, tiempo de seguridad del proceso) El tiempo de seguridad del proceso se define como el intervalo de tiempo entre un fallo que tiene lugar en un EUC o en el sistema de control de EUC (con el potencial suficiente para originar un evento peligroso) y la posibilidad de que se produzca un evento peligroso si la función de seguridad no se ejecuta. (Definición IEC 61508)

---

## R

### Red DIO:

Red que incluye un equipo distribuido, en el que la exploración de E/S se realiza mediante una CPU con un servicio de exploración DIO en el bastidor local. El tráfico de la red DIO se envía después del tráfico RIO, que tiene prioridad en una red de dispositivos.

## S

### SAId:

(*safety application identifier, identificador de aplicación de seguridad*) Firma calculada por algoritmo de la parte segura de una aplicación de Control Expert, almacenada en % SW169.

### SCID:

(*safety configuration identifier, identificador de configuración de seguridad*) Véase TUNID.

### SFF:

(del inglés *Safe Failure Fraction*, fracción de fallo seguro)

### SNCT:

(*safety network configuration tool, herramienta de configuración de red de seguridad*) Herramienta facilitada por el proveedor para configurar los dispositivos CIP Safety. Véase TUNID.

### SRAC:

(*Safety Related Application Condition, Condición de aplicación relacionada con la seguridad*)

### SRT:

(del inglés *System Reaction Time*, tiempo de reacción del sistema) El tiempo de reacción del sistema es el periodo de tiempo entre la detección de una señal en el terminal del módulo de entrada y la reacción de establecer una salida en el terminal del módulo de salida.

## T

### TFFR:

(*Tasa de fallos funcionales tolerable*) Una tasa por hora según las normas EN 5012x para ferrocarriles.

---

**TUNID:**

(*target unique network identifier, identificador de red único de destino*) Valor que identifica de manera unívoca el dispositivo de destino de conexión de una red CIP Safety. El TUNID consta de:

- un número de red de seguridad (safety network number, SNN), que puede ser una marca de tiempo u otro valor definido por el usuario.
- un identificador de configuración de seguridad (SCID), también denominado firma de configuración, creado mediante una herramienta de configuración de red de seguridad (SNCT) facilitada por el proveedor y que consta de:
  - una CRC de configuración de seguridad (SCCRC), que corresponde al valor de CRC de los ajustes de configuración del dispositivo de seguridad, en forma de valor hexadecimal formado por 4 bytes.
  - una marca de tiempo de configuración de seguridad (SCTS), que corresponde a una marca de tiempo de valor hexadecimal de fecha y hora formada por 6 bytes.



# Índice

61508	
IEC .....	398
61511	
IEC .....	398

## A

almacenamiento de datos .....	327
protección .....	325
altitud .....	47
ámbito de datos .....	174
aplicación .....	327
protección .....	308
archivo .....	
cifrado .....	308
área de datos .....	
global .....	175
proceso .....	175
segura .....	175
área segura .....	
contraseña .....	316
arquitectura .....	
BMXSAI0410 .....	145
BMXSDI1602 .....	146
BMXSDO0802 .....	147
BMXSRA0405 .....	149
coprocesador BMEP58CPROS3 .....	141
CPU BMEP58•040S .....	141
arranque .....	272
arranque en caliente .....	275
arranque en frío .....	275
inicial .....	272
tras una interrupción de la alimentación .....	272
arranque en caliente .....	275
arranque en frío .....	275

## B

biblioteca de seguridad .....	
Seguridad de los expertos en control .....	169
bits del sistema de seguridad .....	406
bloquear configuración de E/S .....	288

BMEP58•040S .....	
arquitectura .....	141
BMEP58CPROS3 .....	
arquitectura .....	141
BMXSAI0410 .....	51
aplicaciones .....	55
arquitectura .....	145
conector de cableado .....	53
DDDT .....	61
diagnósticos de DDDT .....	234
LED de diagnóstico .....	235
BMXSDI1602 .....	65
aplicaciones .....	73
arquitectura .....	146
conector de cableado .....	67
DDDT .....	94
diagnósticos de DDDT .....	239
LED de diagnóstico .....	241
BMXSDO0802 .....	99
aplicaciones .....	104
arquitectura .....	147
conector de cableado .....	101
DDDT .....	110
diagnósticos de DDDT .....	245
BMXSRA0405 .....	115
aplicaciones .....	118
arquitectura .....	149
conector de cableado .....	116
DDDT .....	127
diagnósticos de DDDT .....	251
LED de diagnóstico .....	252
bucle de seguridad .....	17
Bucle de seguridad .....	403

## C

canal negro .....	213
carcasa .....	46
CCOTF .....	
limitaciones de un proyecto de seguridad .....	348
certificaciones .....	25
PAC .....	21
ciberseguridad .....	34
ciclo de vida .....	
aplicación .....	35
ciclo de vida de la aplicación .....	35

cifrado	
archivo .....	308
códigos de error .....	388
colocar TUNID .....	384
comando de inicialización de datos	
inicialización seguridad .....	291
Init .....	291
comando generar	
Generar cambios .....	280
Regenerar todo el proyecto .....	280
Renovar ID y Regenerar todo .....	280
comunicación	
PAC a PAC .....	186
Comunicación de PAC a E/S .....	216
comunicación de PAC a PAC .....	186
arquitectura .....	187, 200
configuración .....	188, 201
DFB del PAC emisor .....	194, 207
DFB del PAC receptor .....	196
transmisión de datos .....	193, 206
Comunicación de PAC a PAC	
DFB del PAC receptor .....	209
condiciones de bloqueo .....	219
condiciones sin bloqueo .....	222
conector de cableado	
BMXSAI0410 .....	53
BMXSDI1602 .....	67
BMXSDO0802 .....	101
BMXSRA0405 .....	116
configuración de E/S	
bloquear .....	288
contraseña	
olvido .....	327
pérdida .....	327
sección .....	316
Control Expert	
editor de seguridad .....	336
gestionar acceso a .....	333
guardar datos no seguros .....	348
importar un proyecto de seguridad .....	347
perfiles de usuario predefinidos .....	336
restablecer datos no seguros .....	348
separación de datos .....	257
transferir un proyecto de seguridad .....	347
uso de la memoria .....	350
visualizador de eventos .....	351
coprocesador BMEP58CPROS3	
LED de diagnóstico .....	227

CPU	
comunicación con los módulos E/S de	
seguridad .....	47
CPU BMEP58•040S	
LED de diagnóstico .....	224

## D

DDDT	
BMXSAI0410 .....	61
BMXSDI1602 .....	94
BMXSDO0802 .....	110
BMXSRA0405 .....	127
detección de dispositivos .....	393
diagnostico	
tarjeta de memoria .....	229
diagnóstico	
CIP Safety .....	385
diagnósticos	
BMXSAI0410 DDDT .....	234
BMXSRA0405 DDDT .....	251
condiciones de bloqueo .....	219
condiciones sin bloqueo .....	222
DDDT BMXSDI1602 .....	239
DDDT BMXSDO0802 .....	245
fuente de alimentación .....	232
LED BMXSAI0410 .....	235
LED BMXSDI1602 .....	241
LED BMXSRA0405 LED .....	252
LED de coprocesador	
BMEP58CPROS3 .....	227
LED de la CPU BMEP58•040S .....	224
LED de la fuente de alimentación de	
seguridad de M580 .....	232
módulos de E/S de seguridad .....	48
relé de alarma de fuente de	
alimentación .....	137
tensión de la placa de conexiones .....	136

## E

editor de seguridad .....	333
entrada de mantenimiento .....	265
E/S de seguridad .....	46
E/S de seguridad de M580 .....	216
espacio de nombres	
proceso .....	174

seguro .....	174
transferencia de datos .....	177
estado de conexión del dispositivo .....	393
estados de funcionamiento .....	266
expectativa de tiempo de red .....	166

## F

firma de origen SAFE .....	280
firma de seguridad .....	280
firmware .....	327
protección .....	323
fracción de fallo seguro(SFF) .....	401
frecuencia de fallos .....	403
fuelle de alimentación	
diagnósticos .....	232
diagnósticos de contacto relé de	
alarma .....	137
diagnósticos de tensión de la placa de	
conexiones .....	136
fuelle de alimentación de M580	
LED de diagnóstico .....	232
función de seguridad .....	16

## H

HFT (tolerancia de errores de hardware)....	401
HMI .....	295

## I

IEC 61508	
Seguridad funcional .....	398
IEC 61511	
Seguridad funcional para la industria de	
procesos .....	398
inicializar datos .....	291
intervalo de prueba (PTI) .....	156

## M

modalidad de funcionamiento .....	261
modalidad de funcionamiento de	
mantenimiento .....	262

modalidad de funcionamiento de	
seguridad .....	261
módulos	
certificado .....	27
no interferentes .....	29
tipo 1 no interferente .....	30
tipo 2 no interferente .....	32
módulos de E/S de seguridad	
características comunes .....	46
diagnósticos comunes .....	48
módulos E/S de seguridad	
comunicación con la CPU .....	47
MTBF (tiempo medio entre fallos) .....	403

## N

Nivel de integridad de seguridad (SIL) .....	400
normas .....	25
NTP (protocolo de hora de la red) .....	180

## O

olvido	
contraseña .....	327
OUNID .....	357

## P

palabras del sistema de seguridad .....	408
pérdida	
contraseña .....	327
petición SafetyOpen	
estructura de trama .....	376
PFD (probabilidad de fallo a petición) .....	150, 153, 401
PFH (probabilidad de fallo por hora) ..	150, 153, 401
probabilidad de fallo a petición (PFD) .....	150, 153
probabilidad de fallo a petición(PFD) .....	401
probabilidad de fallo por hora (PFH) ..	150, 153, 401
protección	
almacenamiento de datos .....	325
aplicación .....	308
firmware .....	323

sección .....	320
Unidad de programa .....	320
protocolo de tiempo de red (NTP).....	180
PTI (intervalo de prueba) .....	156

## R

Restablecer propiedad .....	384
RIO .....	46, 216

## S

SCCRC .....	361
SCID .....	361, 368
SCTS .....	361
sección	
protección .....	320
Seguridad de los expertos en control	
biblioteca de seguridad .....	169
separación de datos .....	174
separación de datos en Control Expert .....	257
SFF (fracción de fallo seguro) .....	401
SIL (Nivel de integridad de seguridad) .....	400
sistema	
bits .....	406
palabras .....	408
SNCT .....	361
SNN	
CPU .....	357
dispositivo .....	367

## T

tablas de animación .....	292
Tarea SAFE	
configuración.....	297
tareas.....	276, 297
configurar.....	277
tarjeta de memoria	
diagnóstico.....	229
tiempo de seguridad del proceso.....	157
tiempo medio entre fallos (MTBF).....	403
tolerancia de errores de hardware (HFT)....	401
transferencia de datos entre espacios de	
nombres .....	177
procedimiento.....	178

Trending Tool.....	296
--------------------	-----

## U

Unidad de programa	
protección .....	320
uso de la memoria.....	350

## V

visualizador de eventos .....	351
-------------------------------	-----



Schneider Electric  
35 rue Joseph Monier  
92500 Rueil Malmaison  
France

+ 33 (0) 1 41 29 70 00

[www.se.com](http://www.se.com)

Debido a que las normas, especificaciones y diseños cambian periódicamente, solicite la confirmación de la información dada en esta publicación.

© 2021 Schneider Electric. Reservados todos los derechos.

QGH46986.05