Manual de referencia de seguridad

Traducción de las instrucciones originales

# Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380

Números de catálogo 1756-L81ES, 1756-L82ES, 1756-L83ES, 1756-L84ES, 1756-L8SP, 1756-L81ESK, 1756-L82ESK, 1756-L83ESK, 1756-L84ESK, 1756-L8SPK, 5069-L306ERMS2, 5069-L306ERS2, 5069-L310ERMS2, 5069-L310ERS2, 5069-L320ERMS2, 5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2K, 5069-L330ERMS2, 5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2K, 5069-L340ERMS2, 5069-L340ERS2, 5069-L350ERMS2, 5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2K, 5069-L380ERMS2, 5069-L380ERS2, 5069-L3100ERMS2, 5069-L3100ERS2

Allen-Bradley • Rockwell Software

Rockwell Automation

## Información importante para el usuario

Lea este documento y los documentos que se indican en la sección Recursos adicionales sobre instalación, configuración y operación de este equipo antes de instalar, configurar, operar o dar mantenimiento a este producto. Los usuarios tienen que familiarizarse con las instrucciones de instalación y cableado, y con los requisitos de todos los códigos, las leyes y las normas vigentes.

Es necesario que las actividades que incluyan instalación, ajustes, puesta en servicio, uso, montaje, desmontaje y mantenimiento sean realizadas por personal debidamente capacitado de conformidad con el código de prácticas aplicable.

Si este equipo se utiliza de forma distinta a la indicada por el fabricante, la protección proporcionada por el equipo podría verse afectada.

En ningún caso, Rockwell Automation Inc. será responsable de los daños indirectos o derivados del uso o de la aplicación de este equipo.

Los ejemplos y diagramas incluidos en este manual tienen exclusivamente un fin ilustrativo. Debido a las numerosas variables y requisitos asociados con cada instalación en particular, Rockwell Automation, Inc. no puede asumir ninguna responsabilidad ni obligación por el uso basado en los ejemplos y los diagramas.

Rockwell Automation, Inc. no asume ninguna obligación de patente respecto al uso de la información, los circuitos, los equipos o el software descritos en este manual.

Se prohíbe la reproducción total o parcial del contenido de este manual sin la autorización escrita de Rockwell Automation, Inc.

Este manual contiene notas de seguridad en cada circunstancia en que se estimen necesarias.

| | |
|---|---|
|  | **ADVERTENCIA:** Identifica información acerca de prácticas o circunstancias que pueden causar una explosión en un ambiente peligroso que, a su vez, podría ocasionar lesiones personales o la muerte, daños materiales o pérdidas económicas. |
|  | **ATENCIÓN:** Identifica información sobre prácticas o circunstancias que pueden provocar lesiones personales, la muerte, daños materiales o pérdidas económicas. Las notas de atención le ayudan a identificar un peligro, a evitarlo y a reconocer las posibles consecuencias. |
| **IMPORTANTE** | Identifica información crítica para la correcta aplicación y comprensión del producto. |

También puede haber etiquetas sobre el equipo o dentro del mismo, con el fin de recomendar precauciones específicas.

| | |
|---|---|
|  | **PELIGRO DE CHOQUE:** Puede haber etiquetas en el exterior o en el interior del equipo (por ejemplo, en un variador o un motor) para advertir sobre la posible presencia de voltajes peligrosos. |
|  | **PELIGRO DE QUEMADURA:** Puede haber etiquetas en el exterior o en el interior del equipo (por ejemplo, en un variador o un motor) para advertir sobre superficies que pueden alcanzar temperaturas peligrosas. |
|  | **PELIGRO DE ARCO ELÉCTRICO:** Puede haber etiquetas en el exterior o en el interior del equipo (por ejemplo, en un centro de control de motores) para alertar al personal sobre la posibilidad de que se produzca un arco eléctrico. Un arco eléctrico provocará lesiones graves o la muerte. Use el equipo de protección personal (PPE) apropiado. Cumpla con TODOS los requisitos normativos en lo que respecta a las prácticas de trabajo seguras y al equipo de protección personal (PPE). |

## Capítulo 5

**Características de tags de seguridad, tarea de seguridad y programas de seguridad**



## Capítulo 6

**Desarrollo de la aplicación de seguridad**



## Capítulo 7

**Monitoreo de estado y manejo de fallos**

**Listas de verificación de aplicaciones de seguridad GuardLogix**

**Apéndice D**



**Datos de seguridad de sistemas GuardLogix**

**Apéndice E**



**Aplicación Studio 5000 Logix Designer, versión 31 y posteriores, instrucciones deaplicación de seguridad**

**Apéndice F**

Este manual describe los sistemas controladores GuardLogix® 5580 y Compact GuardLogix 5380, cuyo tipo se ha aprobado y cuentan con certificación para su uso en aplicaciones de seguridad tal como se describe en Certificación SIL en la página 11.

Utilice este manual para el desarrollo, el manejo y el mantenimiento de un sistema de seguridad basado en controladores GuardLogix 5580 o Compact GuardLogix 5380 que utilice la aplicación Studio 5000 Logix Designer®. Lea y comprenda los conceptos de seguridad y los requisitos que se presentan en este manual. También debe familiarizarse con la normativa aplicable (por ejemplo, las normas IEC 61508, IEC 62061, IEC 61511 e ISO 13849-1) antes de poner en marcha un sistema de seguridad basado en controlador GuardLogix 5580 o Compact GuardLogix 5380.

## Resumen de cambios

Este manual contiene información nueva y actualizada tal como se describe en la tabla siguiente.

| Tema | Página |
|---|---|
| Se ha actualizado el texto de introducción del prefacio | 7 |
| Se ha actualizado el texto Homólogo de seguridad | 18 |
| Se ha añadido una tabla Importante en la sección Hardware del controlador Compact GuardLogix 5380 | 19 |
| Se ha actualizado la sección Suposiciones sobre el concepto de seguridad | 49 |
| Se ha actualizado el título de Tabla 9 | 74 |
| Se ha actualizado la sección Tasas de fallos de los productos | 98 |

## Terminología

Esta sección define los términos usados en este manual.

En esta publicación, los términos “controlador GuardLogix” o “sistema GuardLogix” se aplican a los controladores GuardLogix 5580 y Compact GuardLogix 5380 a menos que se indique algo diferente.

Además, el término “SIL 2” corresponde a SIL 2, SIL CL2 y PLd, mientras que “SIL 3” corresponde a SIL 3, SIL CL3 y PLe.

Para ver las abreviaturas habituales y otras definiciones, consulte el Glosario en la página 105.

## Recursos adicionales

Los documentos que se indican a continuación incluyen más información acerca de productos de Rockwell Automation relacionados.

| Recurso | Descripción |
|---|---|
| ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543 | Proporciona información acerca de cómo instalar, configurar, programar y usar los controladores ControlLogix® 5580 y GuardLogix 5580 en proyectos de Studio 5000 Logix Designer. |
| Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001 | Proporciona información acerca de cómo instalar, configurar, programar y usar los controladores CompactLogix™ 5380 y Compact GuardLogix 5380. |
| 1756 ControlLogix and GuardLogix Controllers Technical Data, publicación 1756-TD001 | Presenta las especificaciones y las certificaciones de productos de los controladores ControlLogix y GuardLogix. |
| CompactLogix 5380 and Compact GuardLogix 5380 Controllers Specifications Technical Data, publicación 5069-TD002 | Presenta las especificaciones y las certificaciones de productos de los controladores CompactLogix 5380 y Compact GuardLogix 5380. |
| ControlLogix Chassis and Power Supply Installation Instructions, publicación 1756-IN005 | Proporciona información sobre cómo instalar varios chasis y fuentes de alimentación eléctrica ControlLogix. |
| Controladores Compact GuardLogix 5380 SIL 2 Instrucciones de instalación, publicación 5069-IN014 | Proporciona información sobre cómo instalar controladores CompactLogix 5380. |
| Replacement Guidelines: Logix5000 Controllers Reference Manual, publicación 1756-RM100 | Proporciona pautas acerca de cómo sustituir los siguientes controladores:<br>• Sustituir un controlador ControlLogix 5560 o 5570 por un controlador ControlLogix 5580<br>• Sustituir un controlador CompactLogix 5370 L3 por un controlador CompactLogix 5380 |
| Conjunto de instrucciones de aplicación de seguridad GuardLogix Manual de referencia, publicación 1756-RM095 | Proporciona información acerca del conjunto de instrucciones de las aplicaciones de seguridad GuardLogix. |
| Controladores GuardLogix 5580 Instrucciones de instalació, publicación 1756-IN048 | Proporciona información sobre cómo instalar los controladores GuardLogix 5580. |
| Kinetix 5700 Safe Monitor Functions Safety Reference Manual, publicación 2198-RM001 | Describe las funciones integradas de paro y las funciones de monitoreo seguro con un controlador Logix5000™ y servovariadores Kinetix® 5700. |
| Compact 5000 Safety Sinking Input Module Installation Instructions, publicación 5069-IN020 | Describe cómo instalar el módulo 5069-IB8S. |
| Compact 5000 Configurable Safety Output Module Installation Instructions, publicación 5069-IN021 | Describe cómo instalar el módulo 5069-OBV8S. |
| Módulos de E/S digitales serie 5000 en los sistemas de control Logix5000 Manual del usuario, publicación 5000-UM004 | Describe cómo utilizar los módulos de E/S de seguridad de E/S de seguridad y digitales Compact 5000™, incluyendo cómo utilizar algunos de los módulos en aplicaciones de seguridad. |
| Módulos de seguridad Guard I/O DeviceNet Manual del usuario, publicación 1791DS-UM001 | Proporciona información sobre cómo usar los módulos Guard I/O™ DeviceNet Safety. |
| Módulos de seguridad EtherNet/IP Guard I/O Manual del usuario, publicación 1791ES-UM001 | Proporciona información sobre cómo usar los módulos Guard I/O EtherNet/IP Safety. |
| Módulos de seguridad POINT Guard I/O Manual de instalación y uso, publicación 1734-UM013 | Proporciona información sobre cómo instalar y usar los módulos POINT Guard I/O™. |
| Servovariadores Kinetix 5500 Manual del usuario, publicación 2198-UM001 | Proporciona información sobre cómo instalar y usar los servovariadores Kinetix 5500. |
| Servovariadores Kinetix 5700 Manual de usuario, publicación 2198-UM002 | Proporciona información sobre cómo instalar y usar los servovariadores Kinetix 5700. |
| Variador de CA de frecuencia ajustable PowerFlex 527 Manual del usuario, publicación 520-UM002 | Proporciona información sobre cómo instalar y usar los variadores PowerFlex® 527. |
| Instrucciones generales de los controladores Logix5000 Manual de referencia, publicación 1756-RM003 | Proporciona información sobre el conjunto de instrucciones Logix5000 que incluye instrucciones generales, de movimiento y de procesos. |
| Logix 5000 Controllers Common Procedures, Programming Manual, publicación 1756-PM001 | Proporciona información sobre cómo programar los controladores Logix5000, y sobre cómo administrar los archivos del proyecto, organizar tags, programar y probar rutinas y manejar fallos. |
| Logix5000 Controllers Add On Instructions Programming Manual, publicación 1756-PM010 | Proporciona información sobre cómo crear y usar instrucciones Add-On estándar y de seguridad en aplicaciones Logix. |
| DeviceNet Network Configuration User Manual, publicación DNET-UM004 | Proporciona información sobre cómo usar el módulo 1756-DNB en un sistema de control Logix5000. |
| Configuración de la red EtherNet/IP Manual del usuario, publicación ENET-UM001 | Proporciona información sobre cómo usar el módulo 1756-ENBT en un sistema de control Logix5000. |
| ControlNet Network Configuration User Manual, publicación CNET-UM001 | Proporciona información sobre cómo usar el módulo 1756-CNB en sistemas de control Logix5000. |
| Execution Time and Memory Use for Logix5000 Controller Instructions Reference Manual, publicación 1756-RM087 | Proporciona información sobre cómo calcular el tiempo de ejecución y el uso de memoria para las instrucciones. |
| Logix 5000 Controllers Import/Export Reference Manual, publicación 1756-RM084 | Proporciona información sobre cómo usar la utilidad de importación/exportación de Studio 5000 Logix Designer. |
| Pautas de cableado y conexión a tierra de equipos de automatización industrial Datos de aplicación, publicación 1770-4.1 | Proporciona las pautas generales para instalar un sistema industrial de Rockwell Automation®. |
| Sitio web de certificaciones de productos, http://www.rockwellautomation.com/global/certification/overview.page | Presenta declaraciones de conformidad, certificados y otros detalles de certificación. |

Puede ver o descargar publicaciones de http://www.rockwellautomation.com/global/literature-library/overview.page.

Para solicitar copias impresas de la documentación técnica, comuníquese con el distribuidor de AllenBradley o la oficina de ventas de Rockwell Automation correspondientes a su localidad.

## Notas:

# Concepto de nivel de integridad de seguridad (SIL)



## Certificación SIL

En esta sección se indican las certificaciones SIL y los niveles de rendimiento de los controladores.

| Sistema controlador | IEC 61508 | IEC 62061 | ISO 13849-1 |
|---|---|---|---|
| | Tipo aprobado y certificado para uso en aplicaciones de seguridad hasta: | Adecuado para su uso en aplicaciones de seguridad hasta: | Adecuado para su uso en aplicaciones de seguridad hasta: |
| Sistemas controladores GuardLogix 5580 | SIL 2(2)<br>SIL 3(3) | SIL CL2(2)<br>SIL CL3(3) | Nivel de rendimiento PLd (Cat. 3)(2)<br>Nivel de rendimiento PLe (Cat. 4)(3) |
| Sistemas controladores Compact GuardLogix 5380 SIL 2(1) | SIL 2 | SIL CL2 | Nivel de rendimiento PLd (cat. 3) |

(1) Los números de catálogo de controladores Compact GuardLogix 5380 con un "2" al final, por ejemplo, 5069-L3*xxxxx*S2, se utilizan en aplicaciones de seguridad hasta SIL 2.

(2) Controlador primario que se utiliza sin un homólogo de seguridad.

(3) Controlador primario que se utiliza con un homólogo de seguridad.

**IMPORTANTE** En el resto de esta publicación:

- SIL 2 significa SIL 2, SIL CL2 y PLd
- SIL 3 significa SIL 3, SIL CL3 y PLe

TÜV Rheinland ha aprobado los sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 para uso en aplicaciones relacionadas con la seguridad donde se considera que el estado desenergizado es el estado de seguridad.

Todos los ejemplos de E/S de este manual se basan en conseguir la desenergización como el estado de seguridad en sistemas habituales de parada de emergencia (ESD) y de seguridad de máquinas.

**IMPORTANTE** Como usuario del sistema, usted es responsable de los siguientes aspectos:

- Configuración, clasificación SIL y validación de los sensores o accionadores conectados al sistema GuardLogix
- Administración del proyecto y pruebas de funcionamiento
- Control de acceso al sistema de seguridad, incluido el manejo de contraseñas
- Programación de la aplicación y de las configuraciones del dispositivo de acuerdo con la información contenida en este manual de referencia de seguridad y en estas publicaciones:
  - ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543
  - Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001

Al aplicar la seguridad funcional, restrinja el acceso solo a personal calificado y autorizado que cuente con la debida capacitación y experiencia.

Utilice la aplicación Studio 5000 Logix Designer para crear programas para los controladores GuardLogix 5580 y Compact GuardLogix 5380. Solo se pueden utilizar tareas de seguridad, no tareas estándar, para las funciones de seguridad.

## Pruebas de calidad

La norma IEC 61508 estipula que usted debe realizar varias pruebas de calidad del equipo que se usa en el sistema. Las pruebas de calidad se realizan en momentos definidos por el usuario. Por ejemplo, las pruebas de calidad pueden realizarse una vez al año, una vez cada 15 años o cualquier otro intervalo adecuado.

Los controladores GuardLogix 5580 y Compact GuardLogix 5380 tienen una vida útil de 20 años, sin necesidad de ninguna prueba de calidad. Otros componentes del sistema, como dispositivos de E/S de seguridad, sensores y accionadores, pueden tener vidas útiles diferentes.

**IMPORTANTE** Sus aplicaciones específicas determinan el intervalo de vida útil.

## Arquitectura GuardLogix

En esta sección se presentan ejemplos de sistemas SIL 3 y SIL 2, incluidos los siguientes:

- Función general de seguridad
- Porción de GuardLogix de la función general de seguridad
- Cómo se conectan otros dispositivos (por ejemplo, HMI), mientras operan fuera de la función

**Figura 1 - Ejemplo de sistema SIL 3**

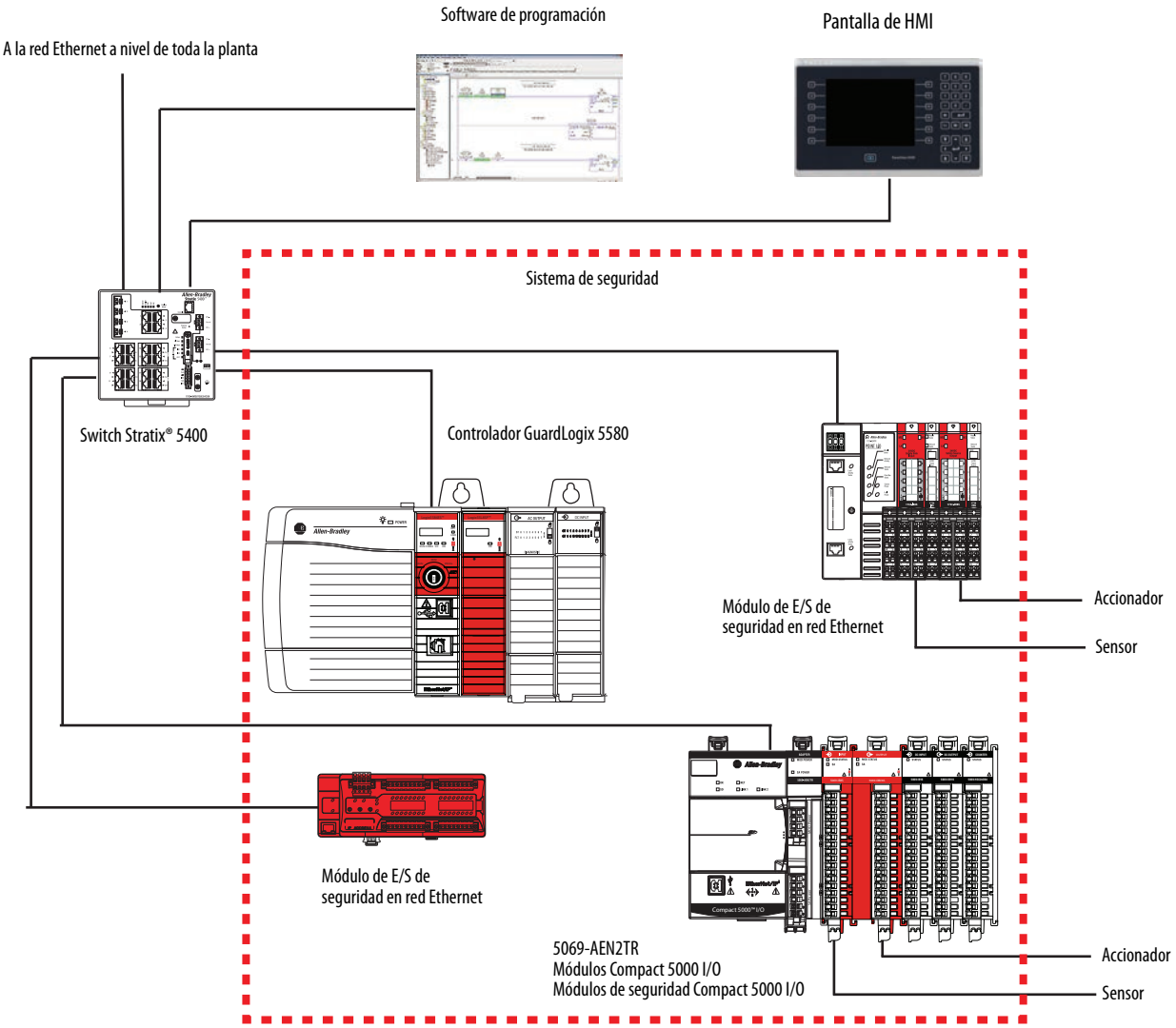
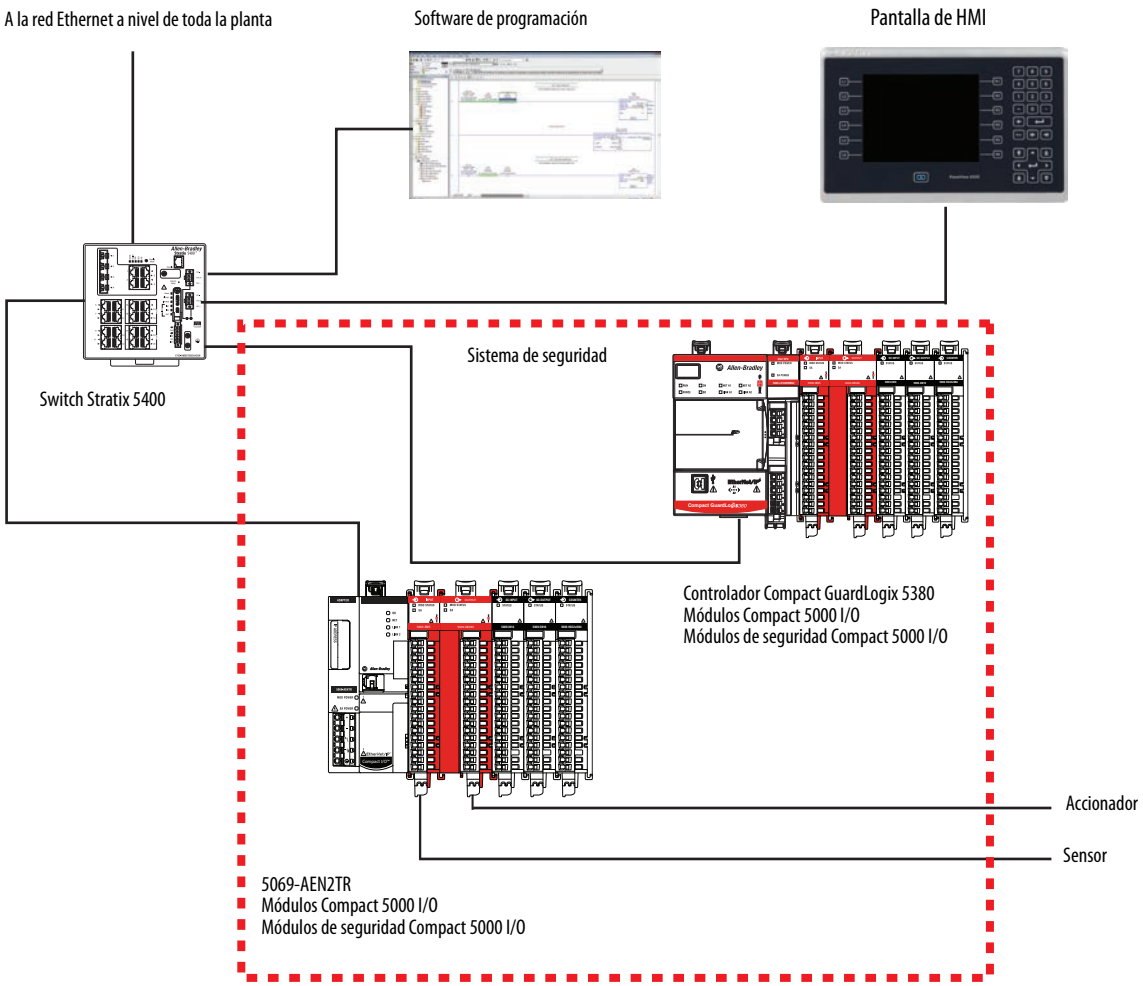


**Figura 2 - Ejemplo de sistema SIL 2**



## Especificaciones del controlador

Estas publicaciones indican las especificaciones y las certificaciones de los productos:

- 1756 ControlLogix and ControlLogix Controllers Technical Data, publicación 1756-TD001
- CompactLogix 5380 and CompactLogix 5380 and Compact GuardLogix 5380 Controllers Specifications Technical Data, publicación 5069-TD002

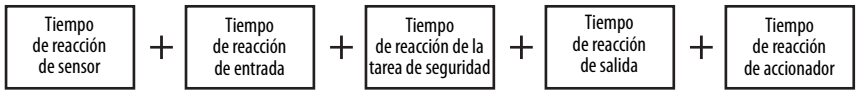
Las certificaciones también se indican en las etiquetas de los productos.

Consulte http://www.rockwellautomation.com/global/certification/overview.page for Declarations of Conformity, Certificates, and other certification details.

## Tiempo de reacción del sistema

El tiempo de reacción del sistema es el tiempo transcurrido, en el peor de los casos, desde que se produce un evento relacionado con la seguridad como entrada al sistema o como fallo dentro del sistema, hasta el momento en que el sistema queda en estado de seguridad.

Esta definición de peor caso incluye los efectos de comunicaciones asíncronas y varios fallos posibles, que se produzcan dentro del sistema. Es posible que los tiempos de reacción reales sean menores.




Cada uno de los tiempos de reacción depende de factores como, por ejemplo, el tipo de dispositivo de E/S y las instrucciones utilizadas en el programa.

**IMPORTANTE** Para obtener más información sobre cómo calcular el tiempo de reacción, consulte el Apéndice C en la página 81.

### Tiempo de reacción de la tarea de seguridad

El tiempo de reacción de la tarea de seguridad es el retardo que puede producirse en el peor caso entre el momento en que se presenta cualquier cambio a la entrada del controlador y el momento en que el productor de la salida establece la salida procesada. Utilice la siguiente ecuación para determinar el tiempo de reacción de la tarea de seguridad:

Tiempo de reacción de la tarea de seguridad = (período de la tarea de seguridad + temporizador de vigilancia de la tarea de seguridad) × 1.01

El multiplicador se usa para la posible deriva del reloj.

### Período de la tarea de seguridad y temporizador de vigilancia de la tarea de seguridad

El período de la tarea de seguridad es el intervalo en que se ejecuta la tarea de seguridad.

El tiempo del temporizador de vigilancia de la tarea de seguridad es el tiempo máximo permisible para el procesamiento de la tarea de seguridad. Si el tiempo que tarda en procesarse una tarea de seguridad supera el tiempo del temporizador de vigilancia de la tarea de seguridad, se produce un fallo de seguridad no recuperable en el controlador, lo que ocasiona una transición al estado de seguridad (apagado).

Usted define el tiempo del temporizador de vigilancia de la tarea de seguridad, que debe ser menor o igual al período de la tarea de seguridad.

El tiempo del temporizador de vigilancia de la tarea de seguridad se establece en la ventana de propiedades de tareas de la aplicación Studio 5000 Logix Designer. Este valor puede ser modificado en línea, independientemente del modo en que se encuentre el controlador, pero no se puede cambiar cuando el controlador esté en bloqueo de seguridad o una vez que se haya creado una firma de seguridad.

## Información de contacto si se produce un fallo en el dispositivo

Si experimenta un fallo con cualquier dispositivo de seguridad, comuníquese con la oficina de ventas de Rockwell Automation o distribuidor de Allen-Bradley correspondiente a su localidad para iniciar las siguientes acciones:

- Devolver el dispositivo a Rockwell Automation para que el fallo quede registrado para el número de catálogo afectado y se guarde un informe del fallo.
- Solicitar un análisis del fallo (en caso necesario) para intentar determinar el motivo del fallo.

# Sistema controlador GuardLogix

| Tema | Página |
|---|---|
| Hardware del controlador GuardLogix 5580 | 17 |
| Hardware del controlador Compact GuardLogix 5380 | 19 |
| Comunicación de red | 20 |
| Descripción general de la programación | 24 |

Para obtener información sobre certificados de seguridad, consulte http://www.rockwellautomation.com/global/certification/safety.page. Utilice los filtros para buscar sus productos.

Consulte Recursos adicionales en la página 8 para buscar información sobre la instalación de los controladores GuardLogix 5580 y Compact GuardLogix 5380.

## Hardware del controlador GuardLogix 5580

El controlador GuardLogix consiste en un controlador primario (ControlLogix 558*x*S), que se puede utilizar solo en aplicaciones SIL 2, y un homólogo de seguridad (ControlLogix 558SP), que se añade para crear un controlador con capacidad SIL 3.

Tanto el controlador primario como el homólogo de seguridad realizan pruebas diagnósticas funcionales, tanto al momento del encendido como durante la ejecución, de todos los componentes del controlador relacionados con la seguridad.

- Un controlador primario que se utiliza sin un homólogo de seguridad tendrá proporciona conformidad hasta SIL 2.
- Un controlador primario que se utiliza con un homólogo de seguridad proporciona conformidad hasta SIL 3.

| Controlador | N.º de cat. |
|---|---|
| Controlador GuardLogix 5580 | 1756-L81ES, 1756-L82ES, 1756-L83ES, 1756-L84ES, 1756-L8SP, 1756-L81ESK, 1756-L82ESK, 1756-L83ESK, 1756-L84ESK, 1756-L8SPK |

Para ver la lista más actualizada de controladores GuardLogix, y de series certificadas de dispositivos de E/S de seguridad y revisiones del firmware, consulte los certificados de seguridad en http://www.rockwellautomation.com/global/certification/safety.page.

Las revisiones del firmware están disponibles en el sitio web de asistencia técnica del Centro de compatibilidad y descarga de productos (PCDC) de Rockwell Automation en http://www.rockwellautomation.com/global/support/pcdc.page.

Puede llenar las ranuras del chasis de un sistema SIL 2 o SIL 3 que no utiliza el sistema GuardLogix SIL 2 o SIL 3 con otros módulos ControlLogix (1756) certificados que estén certificados de acuerdo con las directivas de baja tensión y compatibilidad electromagnética (EMC).

Para buscar los certificados de los controladores y los módulos de E/S, consulte http://www.rockwellautomation.com/global/certification/overview.page.

## Controlador primario

El controlador primario es el procesador que realiza funciones de control estándar y de seguridad, y que se comunica con el homólogo de seguridad para las funciones relacionadas con la seguridad del sistema de control GuardLogix. El controlador primario consta de un procesador central, una interface de E/S y una memoria.

## Homólogo de seguridad

Para cumplir los requisitos de SIL 3, debe instalar un homólogo de seguridad ControlLogix 558SP en la ranura situada justo a la derecha del controlador primario. El homólogo de seguridad es un coprocesador que proporciona arquitectura 1oo2 para las funciones relacionadas con la seguridad del sistema. El sistema 1oo2 no funciona cuando se degrada. Si los dos procesadores no concuerdan o no pueden comunicarse entre sí, el resultado es un fallo mayor no recuperable del controlador. Para obtener información sobre cómo responder a esta situación, consulte el artículo 63983 de la Knowledgebase de Rockwell Automation®.

Para satisfacer los requisitos de SIL 2, no instale un homólogo de seguridad.

El controlador primario configura el homólogo de seguridad. Solo es necesaria una sola descarga del programa de usuario al controlador primario. El controlador primario controla el modo de funcionamiento del homólogo de seguridad.

## Chasis

El chasis proporciona las conexiones físicas entre los módulos y el sistema GuardLogix 1756. Cualquier fallo, aunque improbable, sería detectado como fallo por uno o más de los componentes activos del sistema. Por tanto, el chasis es irrelevante para el análisis de seguridad.

## Fuente de alimentación eléctrica

No es necesario contar con configuraciones ni con cableados adicionales para el funcionamiento SIL 2 o SIL 3 de las fuentes de alimentación eléctrica ControlLogix. Cualquier fallo sería detectado como tal por uno o más de los componentes activos del sistema GuardLogix. Por lo tanto, la fuente de alimentación eléctrica es irrelevante para el análisis de seguridad.

## Hardware del controlador Compact GuardLogix 5380

El controlador Compact GuardLogix 5380 es un controlador con capacidad SIL 2 que realiza las funciones de control estándar y de seguridad para las funciones relacionadas con la seguridad de un sistema de control Compact GuardLogix.

| Controlador | N.º de cat. |
|---|---|
| Controlador Compact GuardLogix 5380 | 5069-L306ERMS2, 5069-L306ERS2, 5069-L310ERMS2, 5069-L310ERS2, 5069L320ERMS2, 5069L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2K, 5069-L330ERMS2, 5069-L330ERS2, 5069L330ERS2K, 5069-L330ERMS2K, 5069-L340ERMS2, 5069-L340ERS2, 5069-L350ERMS2, 5069-L350ERS2, 5069L350ERS2K, 5069-L350ERMS2K, 5069-L380ERMS2, 5069-L380ERS2, 5069-L3100ERMS2, 5069-L3100ERS2 |

**IMPORTANTE** Este equipo se suministra como equipo de tipo abierto para uso en ambientes interiores. Debe montarse dentro de un envolvente con el diseño adecuado para esas condiciones ambientales específicas y estar apropiadamente diseñado para evitar lesiones personales durante el acceso a piezas energizadas.

El envolvente debe tener propiedades retardadoras de llama adecuadas para evitar o minimizar la propagación de llamas, y cumplir así con una clasificación de dispersión de llamas de 5VA o estar aprobado para la aplicación si no fuese metálico. El acceso al interior del envolvente solo deberá ser posible mediante el uso de una herramienta.

Para obtener más información sobre las clasificaciones de tipos de envolventes específicos que se necesitan para cumplir determinadas certificaciones de seguridad de productos, consulte el documento Controladores Compact GuardLogix 5380 SIL 2 Instrucciones de instalación, publicación 5069-IN014.

Para ver la lista más actualizada de controladores GuardLogix y de series certificadas de dispositivos de E/S de seguridad y revisiones del firmware, consulte los certificados de seguridad en http://www.rockwellautomation.com/global/certification/safety.page.

Las revisiones de firmware están disponibles en el sitio web de asistencia del Centro de compatibilidad y descarga de productos (PCDC) de Rockwell Automation en http://www.rockwellautomation.com/global/support/pcdc.page.

Las ranuras expansoras del bus del sistema se pueden rellenar con módulos expansores Compact 5000 I/O certificados de acuerdo con las directivas de baja tensión y compatibilidad electromagnética (EMC), si se rellenan según las instrucciones que aparecen en Fuente de alimentación eléctrica.

Para buscar los certificados de los controladores y los módulos de E/S, consulte http://www.rockwellautomation.com/global/certification/overview.page.

### Fuente de alimentación eléctrica

Para aplicaciones de seguridad funcional, se requieren fuentes de alimentación SELV/PELV tanto para la alimentación de módulo (MP) como la alimentación de sensor/accionador (SA).

Tenga en cuenta lo siguiente al elegir una fuente de alimentación eléctrica:

- La alimentación MP del controlador Compact GuardLogix 5380 debe suministrarla una fuente de alimentación eléctrica de 24 VCC SELV/PELV.
- Todas las E/S de seguridad de 24 VCC locales deben recibir alimentación de una fuente de alimentación eléctrica clasificada como SELV/PELV.
- Si se utiliza el conector de alimentación SA del controlador Compact GuardLogix 5380 debe recibir la alimentación de una fuente de alimentación eléctrica de 24 VCC SELV/PELV.
- Si se utilizan E/S de 120/240 VCA en el chasis Compact GuardLogix 5380, su alimentación de SA de 120/240 VCA debe conectarse a un módulo con número de catálogo 5069-FPD.
- Si se utilizan E/S estándar que no reciben la alimentación de una fuente de alimentación eléctrica SELV/PELV, su alimentación de E/S debe conectarse a un módulo con número de catálogo 5069-FPD.

**IMPORTANTE** Para obtener más información sobre cómo suministrar alimentación a la plataforma 5069 cuando se emplea un controlador CompactLogix o Compact GuardLogix, consulte el documento Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001.

## Comunicación de red

En esta sección se proporcionan ejemplos de configuraciones de comunicación de red.

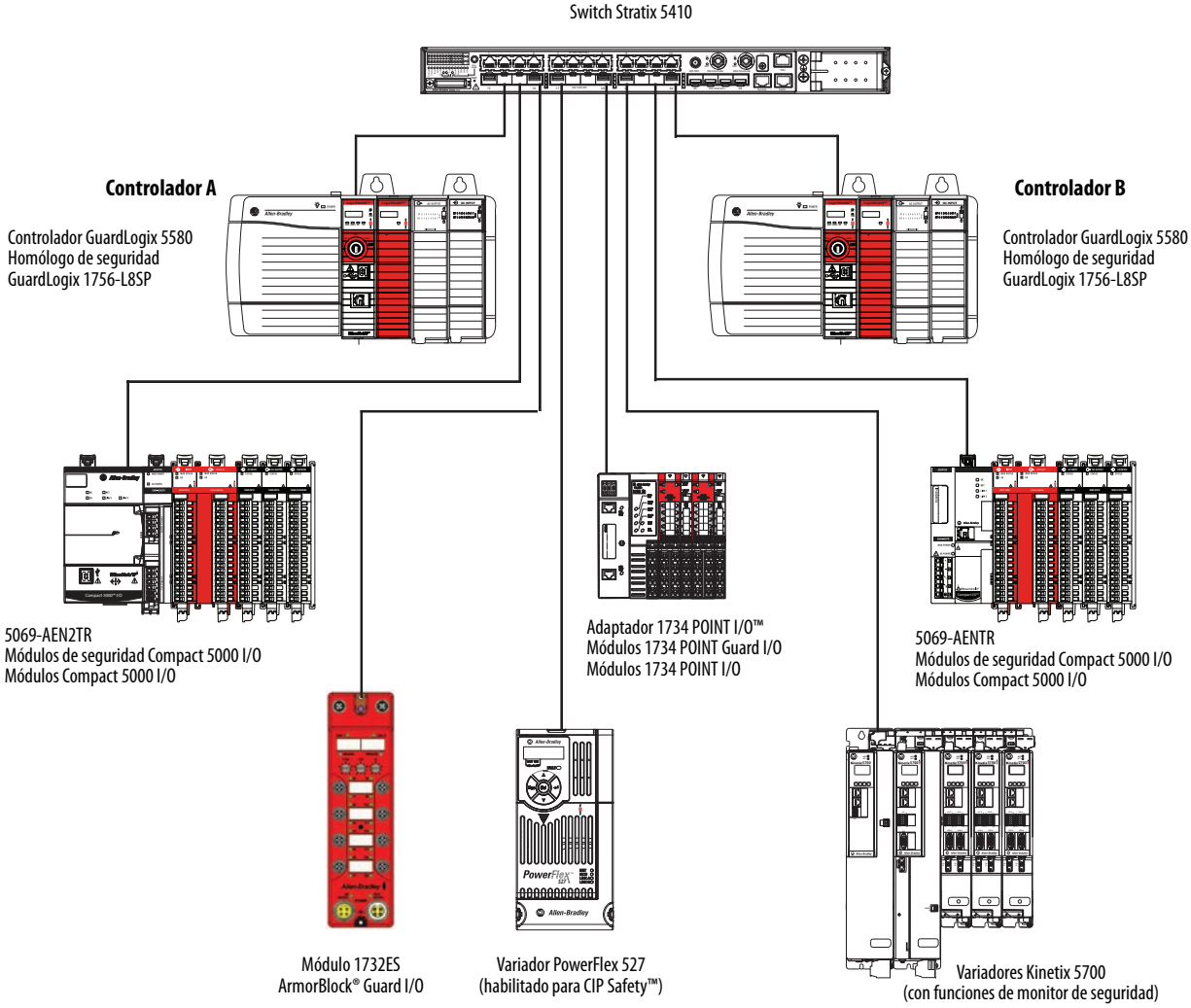
### Red EtherNet/IP

El controlador GuardLogix 5580 se conecta directamente a una red EtherNet/IP mediante el puerto Ethernet incorporado y admite velocidades de red de 10/100/1000 MBps. No se requiere un módulo de comunicación Ethernet aparte, pero se puede utilizar en el chasis local.

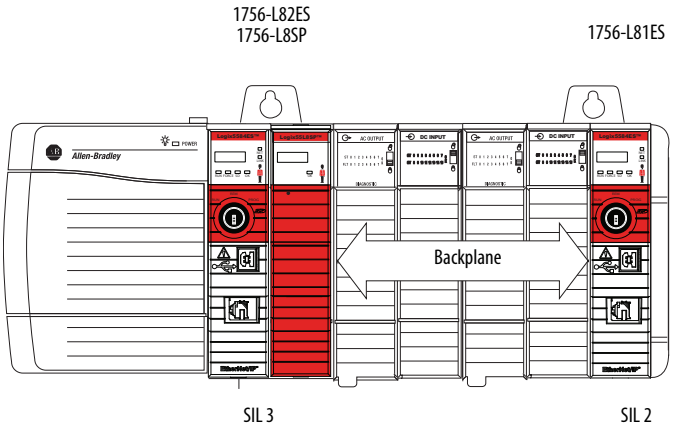
Comuníquese con la oficina de ventas de Rockwell Automation o distribuidor de Allen-Bradley correspondiente a su localidad para ver los otros módulos de interface de comunicación disponibles para uso en el sistema GuardLogix 5580.

La comunicación de seguridad de igual a igual entre controladores GuardLogix es posible mediante la red Ethe rNet/IP. Los controladores GuardLogix pueden controlar e intercambiar datos de seguridad con dispositivos de E/S de seguridad en una red EtherNet/IP, mediante los puertos Ethernet incorporados o puentes EtherNet/IP.

**Figura 3 - Comunicación de igual a igual del GuardLogix 5580 mediante la red EtherNet/IP**

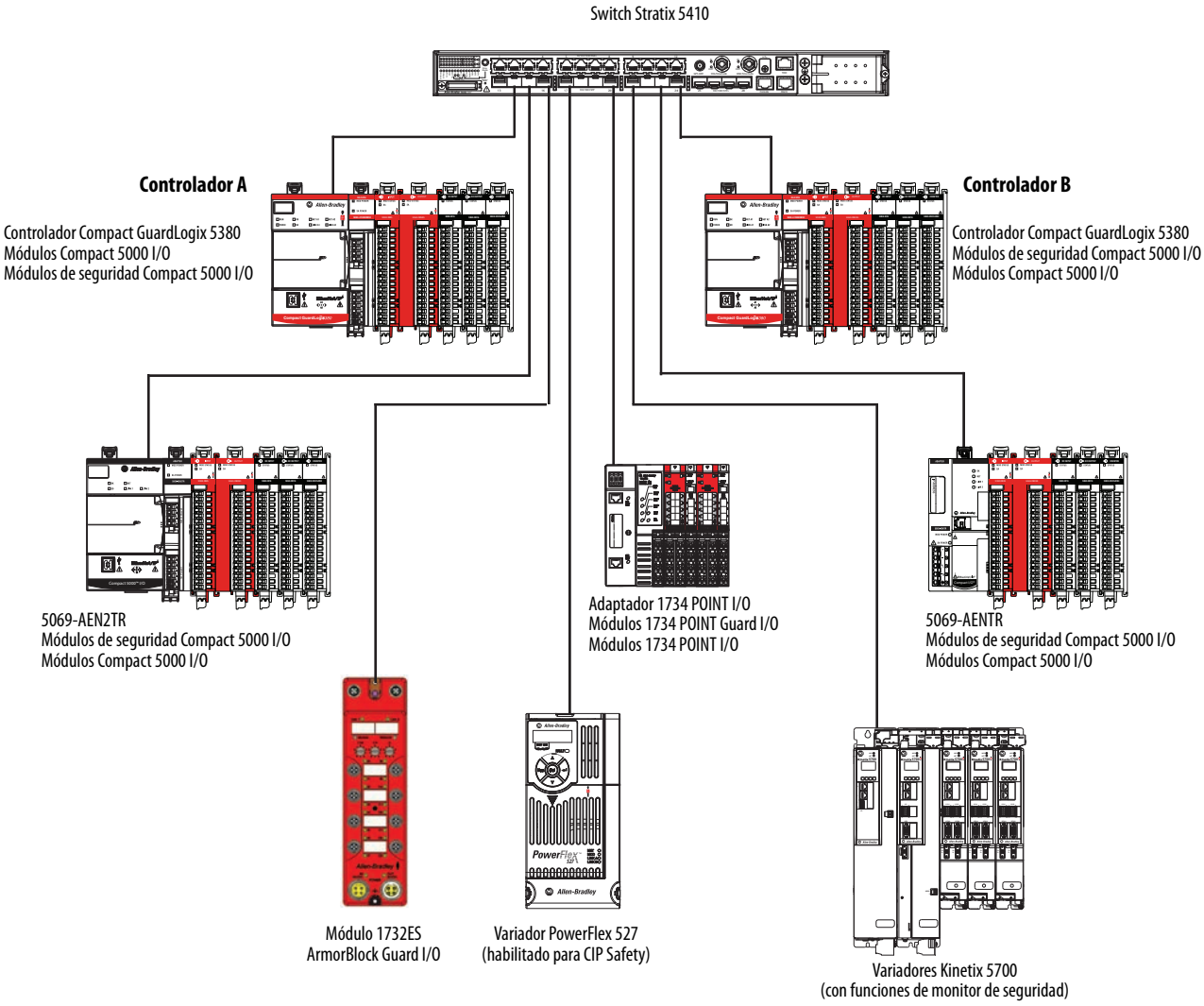



**SUGERENCIA** La comunicación de seguridad de igual a igual entre dos controladores GuardLogix 5580 en el mismo chasis también es posible a través del backplane.



Los controladores Compact GuardLogix 5380 se conectan directamente a la red EtherNet/IP mediante los puertos Ethernet incorporados. También admiten velocidades de red de 10/100/1000 Mbps. No se utiliza un módulo de comunicación Ethernet local.

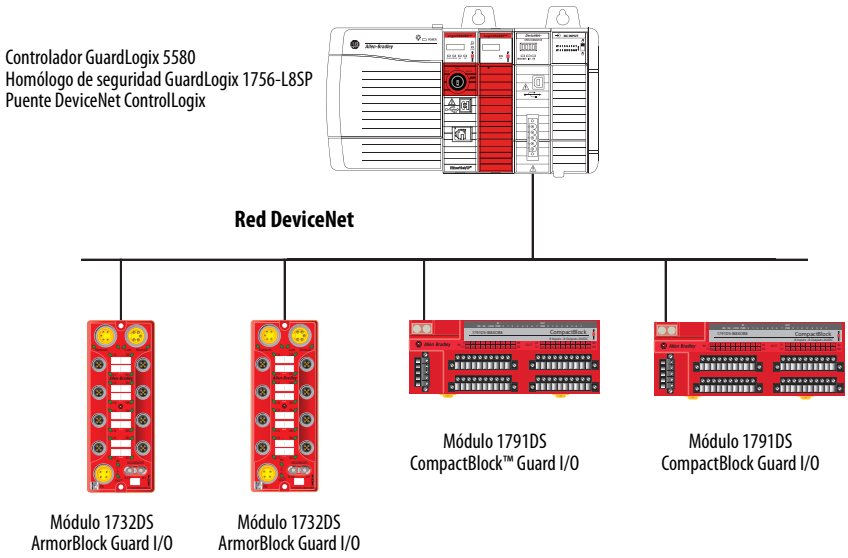
**Figura 4 - Comunicación de igual a igual del Compact GuardLogix 5380 mediante la red EtherNet/IP**



## Red de seguridad DeviceNet

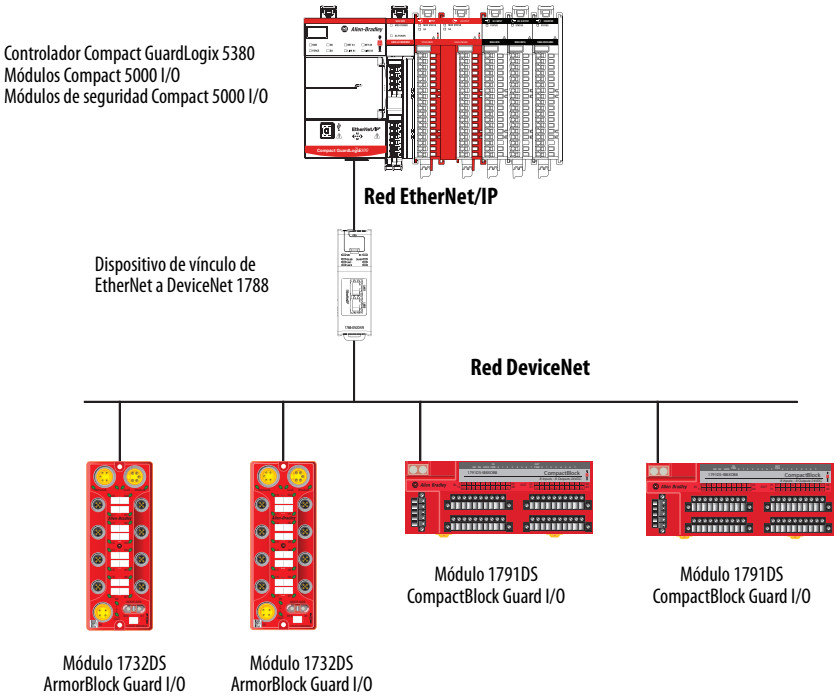
El puente DeviceNet permite al controlador GuardLogix controlar e intercambiar datos de seguridad con módulos de E/S de seguridad en una red DeviceNet.

**Figura 5 - Comunicación de GuardLogix 5580 mediante un puente DeviceNet**




Los controladores Compact GuardLogix 5380 pueden comunicarse con los dispositivos de seguridad en una red DeviceNet mediante un dispositivo de vínculo de EtherNet/IP a DeviceNet 1788-EN2DNR.

**Figura 6 - Controlador Compact GuardLogix 5380 con una red DeviceNet**



## Descripción general de la programación

Utilice la aplicación Studio 5000 Logix Designer para programar los controladores de seguridad GuardLogix.

Use la aplicación Studio 5000 Logix Designer para definir la ubicación, la propiedad y la configuración de los dispositivos de E/S y controladores, así como para crear, probar y depurar la lógica del programa. Solo el diagrama de lógica de escalera es compatible con la tarea de seguridad GuardLogix.

Consulte el Apéndice A en la página 71 para obtener información acerca del conjunto de instrucciones lógicas disponibles para proyectos de seguridad.

**IMPORTANTE** Cuando el controlador GuardLogix está en modo de marcha Run o de programación Program, y el programa de aplicación no ha sido validado, usted es responsable de mantener las condiciones de seguridad.

# E/S de seguridad del sistema de control GuardLogix



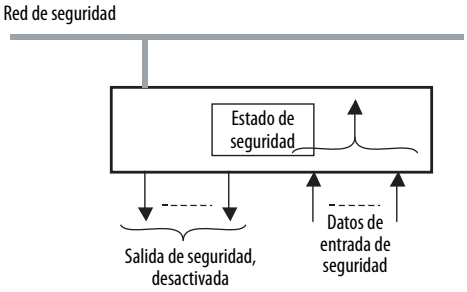
Antes de poner en marcha un sistema de seguridad GuardLogix con dispositivos de E/S de seguridad, primero debe leer, entender y seguir toda la información de seguridad de la documentación del producto correspondiente a dichos productos.

Los dispositivos de E/S de seguridad se pueden conectar a dispositivos de entradas y salidas de seguridad, como sensores y accionadores. El controlador GuardLogix monitorea y controla los dispositivos. En el caso de datos de seguridad, las comunicaciones de E/S se realizan mediante conexiones de seguridad utilizando el protocolo CIP Safety; la lógica de seguridad se procesa en el controlador GuardLogix.

## Funciones de seguridad típicas de los dispositivos de E/S de seguridad

Los dispositivos de E/S de seguridad tratan lo siguiente como estado de seguridad:

- Salidas de seguridad: desactivadas
- Datos de entrada de seguridad al controlador: desactivados




Los dispositivos de E/S de seguridad deben utilizarse para aplicaciones que estén en estado de seguridad cuando se desactive la salida de seguridad.

### Diagnósticos

Los dispositivos de E/S de seguridad realizan autodiagnósticos cuando se conecta la alimentación eléctrica y periódicamente durante el funcionamiento. Si se detecta un fallo de diagnóstico, los datos de entrada de seguridad (al controlador) y las salidas de seguridad locales se establecen en su estado seguro (desactivado).

### Datos de estado

Además de los datos de entrada y de salida de seguridad, los dispositivos de E/S de seguridad aceptan datos de estado para monitorear el buen estado de los circuitos de E/S y del dispositivo. Consulte la documentación del producto correspondiente a su dispositivo para ver las capacidades del producto concreto.

### Indicadores de estado

Los dispositivos de E/S de seguridad incluyen indicadores de estado. Para obtener información detallada acerca del funcionamiento de los indicadores de estado, consulte la documentación del producto relacionada con el dispositivo específico.

### Función de retardo a la conexión o a la desconexión

Algunos dispositivos de E/S de seguridad admiten funciones de retardo a la conexión y a la desconexión para las señales de entrada. En algunas aplicaciones, debe incluir un retardo a la desconexión, un retardo a la conexión o ambos, a la hora de calcular el tiempo de reacción del sistema.

Por ejemplo, el filtro de retardo de la conexión a la desconexión ayuda a filtrar el ruido que afecta el nivel de la lógica de entrada.

Consulte el Apéndice C en la página 81 para obtener información acerca del tiempo de reacción del sistema.

## Tiempo de reacción

El tiempo de reacción de entrada es el tiempo que transcurre desde que la señal cambia en un terminal de entrada hasta que se envían datos de seguridad al controlador GuardLogix.

El tiempo de reacción de salida es el tiempo que transcurre desde que se reciben datos de seguridad del controlador GuardLogix hasta que el terminal de salida cambia de estado.

Para obtener información sobre cómo determinar los tiempos de reacción de entrada y de salida, consulte la documentación del producto relacionada con el dispositivo de E/S de seguridad específico.

Consulte el Apéndice C en la página 81 para obtener información sobre cómo calcular el tiempo de reacción del sistema.

## Consideraciones de seguridad en torno a los dispositivos de E/S de seguridad

Debe poner en servicio todos los dispositivos con dirección de nodo o dirección IP y velocidad de comunicación, de ser necesario, antes de instalarlos en una red de seguridad.

### Propiedad

Un controlador GuardLogix es el propietario de cada dispositivo de E/S de seguridad de un sistema GuardLogix. Es posible usar múltiples controladores GuardLogix y múltiples dispositivos de E/S de seguridad sin restricciones en chasis o en redes, según sea necesario. Cuando un controlador es el propietario de un dispositivo de E/S, almacena los datos de configuración que se definan para dicho dispositivo. Esta configuración controla la forma en que operan los dispositivos en el sistema.

Desde el punto de vista del control, un controlador controla los dispositivos de salida de seguridad. Un controlador es propietario de cada dispositivo de entrada de seguridad. No obstante, los datos de entrada de seguridad pueden ser compartidos (consumidos) por varios controladores GuardLogix.

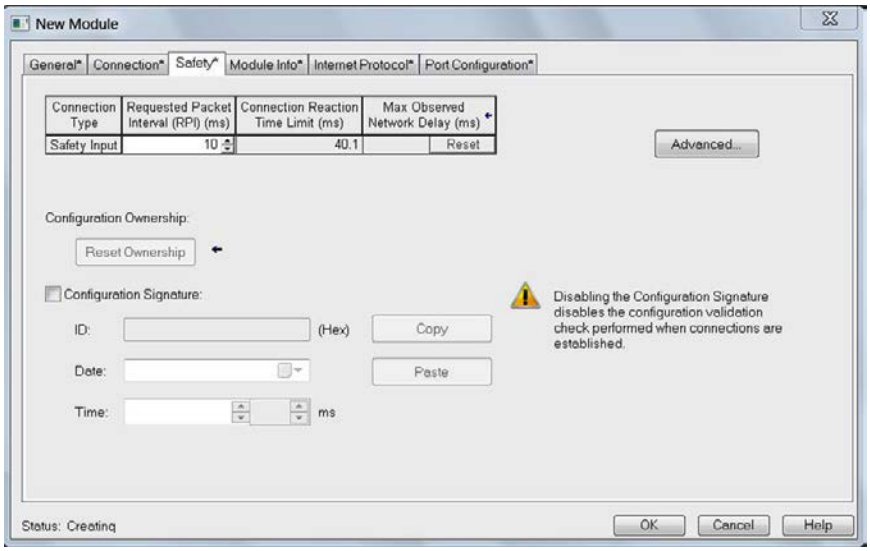
### Firma de configuración de E/S de seguridad

**IMPORTANTE** Las firmas de configuración de E/S de seguridad se aplican a los módulos de seguridad individuales. Esta es diferente de la firma de seguridad del controlador, que se aplica a la parte de seguridad del controlador.

La firma de configuración se calcula a partir de la configuración del dispositivo de E/S de seguridad. La firma de configuración se utiliza para verificar que el dispositivo se ha configurado tal como esperaba la aplicación de seguridad. Cuando se utiliza un controlador GuardLogix, no es necesario monitorear esta firma. El controlador GuardLogix monitorea automáticamente la firma. Si la firma de configuración cambia de manera inesperada, se interrumpe la conexión de seguridad entre el controlador y el módulo de E/S, lo que hace que el módulo de E/S entre en su estado de seguridad.

Al utilizar un módulo de otro fabricante, si se conecta a un dispositivo de E/S de seguridad sin una firma de configuración, deberá verificar que existe una configuración válida en el dispositivo de E/S de seguridad.

**IMPORTANTE** Los módulos de E/S de seguridad de Rockwell Automation normalmente utilizan de manera predeterminada la firma de configuración y no permiten que un sistema funcione sin una firma de configuración.




## Sustitución de un dispositivo de E/S de seguridad

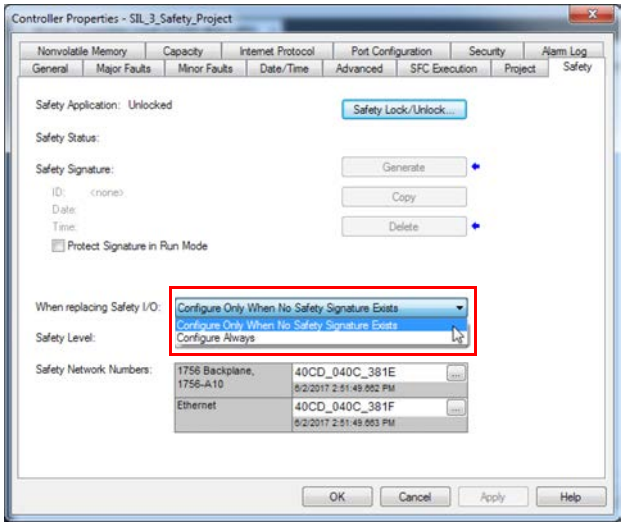
La sustitución de dispositivos de seguridad obliga a configurar correctamente el dispositivo sustituto y verificar su funcionamiento.

**ATENCIÓN:** Durante el reemplazo o las pruebas de funcionamiento de un dispositivo, la seguridad del sistema no debe depender en ninguna parte del dispositivo afectado.

Hay dos opciones disponibles de dispositivos de E/S de repuesto en la ficha Safety del cuadro de diálogo Controller Properties de la aplicación Studio 5000 Logix Designer:

- Configure Only When No Safety Signature Exists
- Configure always

**Figura 7 - Opciones de sustitución de E/S de seguridad**




*Configure Only When No Safety Signature Exists*

Esta opción instruye al controlador GuardLogix para que configure un dispositivo de seguridad cuando la tarea de seguridad no tiene una firma de seguridad y el dispositivo sustituto están en su condición original sin ningún número de red de seguridad.

Si el controlador tiene una firma de seguridad, el controlador GuardLogix configura automáticamente el dispositivo de E/S de seguridad sustituto si se cumplen todas las condiciones siguientes:

- El dispositivo ya tiene el número de red de seguridad correcto.
- La codificación electrónica del dispositivo es correcta.
- El nodo o dirección IP es correcto.

Para establecer el número de red de seguridad (SNN) adecuado cuando existe una firma de seguridad del controlador, es necesario descargar manualmente el SNN correcto. Entre en línea en el controlador GuardLogix o CompactGuardLogix con la aplicación Studio 5000 Logix Designer, abra el cuadro de diálogo Module Properties, vaya a la ficha General y haga clic en el botón "..." que está junto al número de red de seguridad. Utilice el botón Set para escribir manualmente el SNN en el módulo. Tras esta operación manual, el resto de la configuración se descarga automáticamente.

Para obtener información detallada, consulte el procedimiento de sustitución de dispositivos de E/S de seguridad que aparece en el manual del usuario del controlador:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543
- Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001

*Configure always*

El controlador GuardLogix intenta configurar automáticamente un dispositivo de E/S de seguridad sustituto si el dispositivo está en su condición original. (Cuando no hay un número de red de seguridad en el dispositivo de seguridad sustituto y el número de nodo y la codificación del dispositivo de E/S coinciden con la configuración del controlador).

**ATENCIÓN:** Habilite la función Configure Always solo si no confía en que todo el sistema de control de seguridad encaminable pueda mantener la conformidad con el nivel SIL 2 o SIL 3 durante el reemplazo y las pruebas funcionales de un dispositivo. Consulte Sistema CIP Safety encaminable en la página 32.

Si se confía en otros componentes del sistema de control de seguridad para mantener el nivel SIL 2 o SIL 3, asegúrese de inhabilitar la característica Configure Always del controlador.

Es su responsabilidad implementar un proceso que asegure que se mantenga la funcionalidad de seguridad adecuada durante la sustitución del dispositivo.

**ATENCIÓN:** Para colocar un dispositivo en su condición original en una red de seguridad cuando se ha habilitado la característica Configure Always, siga el procedimiento de sustitución del dispositivo del manual del usuario:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543
- Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001

# CIP Safety y números de red de seguridad



## Referencia única de nodo

Los sistemas de control CIP Safety están compuestos por dispositivos CIP Safety que se interconectan mediante redes de comunicación. Estas redes están formadas por dispositivos (switches, puentes, adaptadores, etc.) que podrían no tener la certificación SIL 2 o SIL 3. Por lo tanto, los dispositivos CIP Safety deben contar con una protección intrínseca frente a errores de entrega de la red.

El protocolo CIP Safety es un protocolo de seguridad entre nodos finales. Esta configuración permite el encaminamiento de mensajes CIP Safety desde y hacia dispositivos CIP Safety a través de puentes, switches y encaminadores no certificados.

Un elemento clave del protocolo CIP Safety es el concepto de referencia única de nodo (también denominado ID único de nodo o UNID). Cada dispositivo CIP Safety debe tener un valor UNID asignado a cada puerto compatible con CIP Safety.

**IMPORTANTE** Es su responsabilidad asegurarse de que todos los UNID sean realmente únicos dentro del ámbito de todos los dispositivos que puedan comunicarse entre sí.

## Números de red de seguridad (SNN)

Las comunicaciones en el interior de un sistema de control recorren subredes que están interconectadas con componentes de puente o encaminamiento. Ejemplos de subredes:

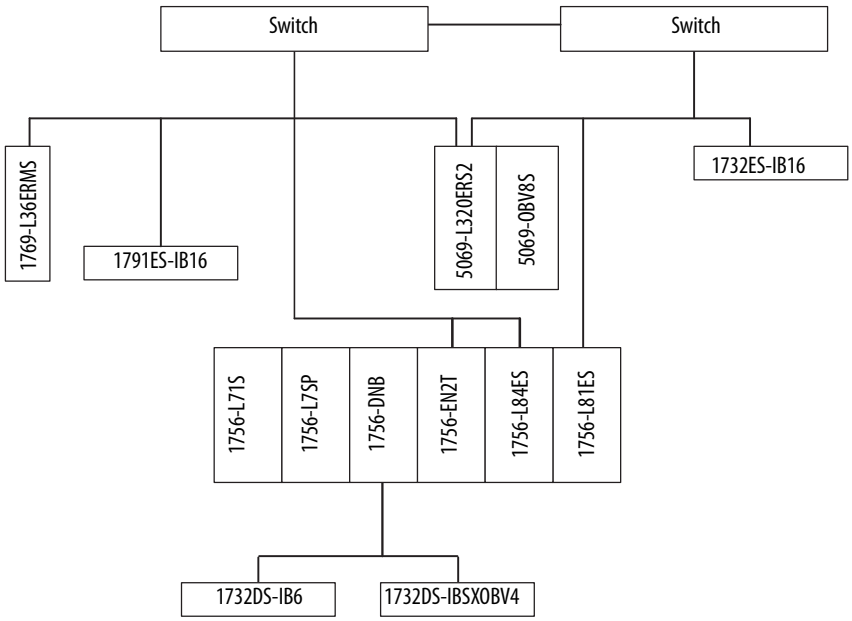
- El backplane de un chasis
- Un banco de módulos de E/S
- Una subred Ethernet dentro de una LAN

En lugar de crear directamente un UNID para cada dispositivo CIP Safety (un proceso que sería propenso a errores en un sistema de grandes dimensiones), a cada subred se le asigna un número de red de seguridad (SNN) único y el UNID se crea a partir del SNN + la dirección del nodo.

## Sistema CIP Safety encaminable

El sistema de ejemplo de la figura 8 no está interconectado a otro sistema CIP Safety mediante una conexión principal Ethernet más grande a nivel de toda la planta. Por lo tanto, la figura 8 ilustra la extensión de un sistema CIP Safety encaminable.

**Figura 8 - Ejemplo de sistema de seguridad**




En este ejemplo:

- Para un puerto del backplane, se asigna un SNN al backplane y la dirección de nodo es el número de ranura del dispositivo.
- Para un puerto Ethernet, se asigna un SNN a la red EtherNet/IP y la dirección de nodo es la dirección IP del dispositivo.
- El 5069-L320ERS2 está en modo Dual-IP y conectado a dos redes EtherNet/IP diferentes. No deben compartir los valores SNN ya que los switches podrían encaminar incorrectamente paquetes entre ellos.

## Consideraciones para asignar SNN

Al crear proyectos de controlador, la aplicación Studio 5000 Logix Designer genera automáticamente un valor de SNN cada vez que reconoce una nueva subred que contiene dispositivos CIP Safety:

- A cada puerto compatible con CIP Safety del controlador se le asigna un SNN.
- Si hay un puente o un dispositivo adaptador en el árbol de E/S y se añade un dispositivo CIP Safety secundario, a la subred creada por el puente o el adaptador se le asigna un SNN.

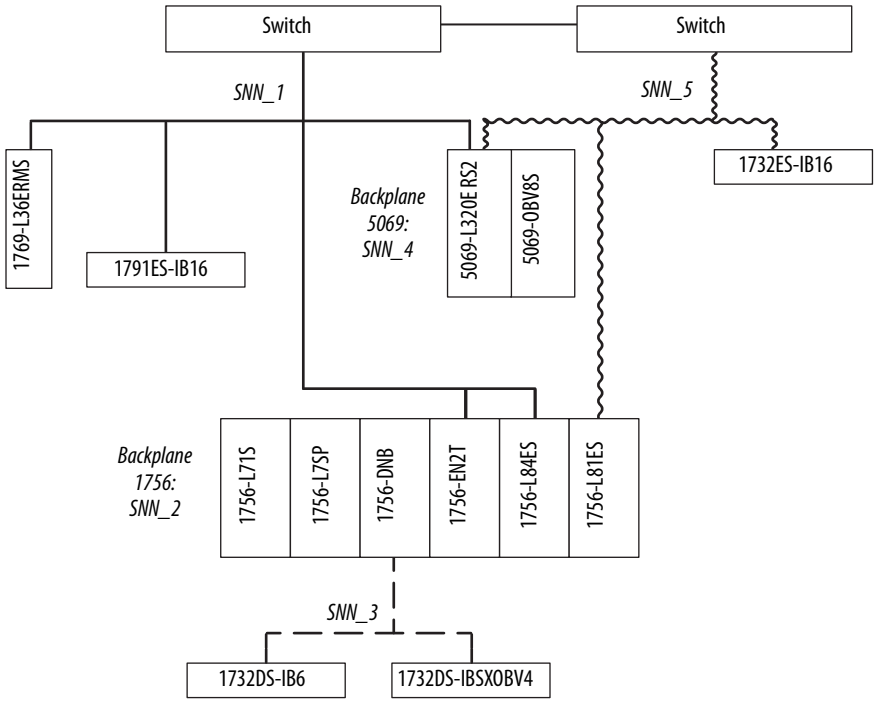
Si el sistema CIP Safety completo consiste en un proyecto de controlador, será suficiente con los valores SNN que se generan automáticamente.

Si hay varios controladores que deben obtener acceso o interactuar con las mismas E/S de seguridad, el diseñador del sistema CIP Safety debe coordinar los valores SNN entre los diversos archivos de proyecto. La aplicación Studio 5000 Logix Designer permite copiar/pegar las asignaciones de SNN para facilitar esta coordinación.

También puede optar por establecer un mapa de todo el sistema encaminable (o quizá de la planta completa) y asignar manualmente valores SNN a cada subred. La aplicación Studio 5000 Logix Designer ofrece un método de introducción manual para asignar valores SNN y hacer posible esta metodología de diseño.

La figura 9 muestra un ejemplo de cómo se pueden asignar SNN a las subredes.

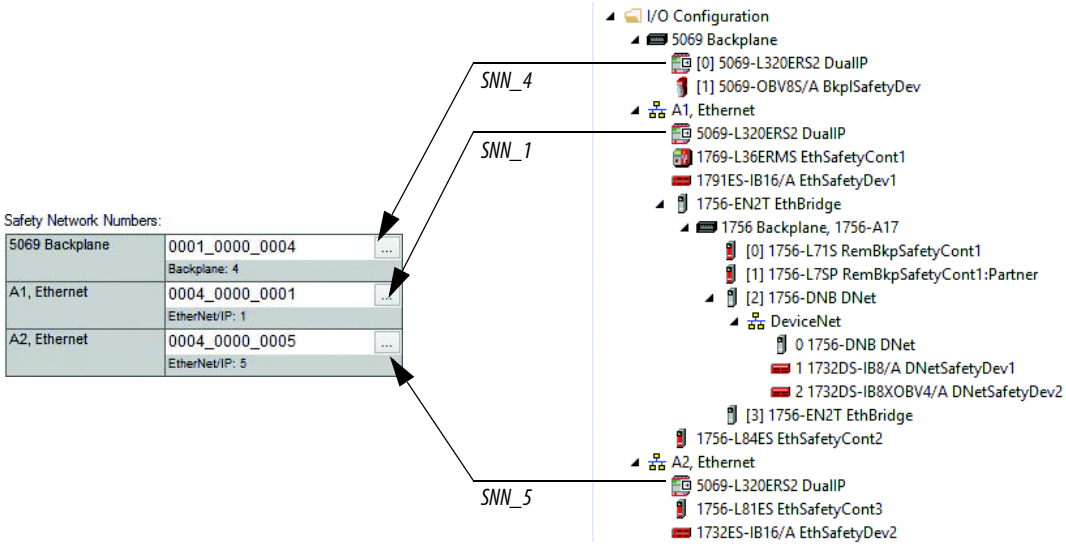
**Figura 9 - Ejemplo de asignación de SNN**




| Subred | Tipo | Línea | Asignación de SNN |
|---|---|---|---|
| SNN_1 | EtherNet/IP | ——— | Puerto Ethernet 1769-L36ERMS, 1791ES-IB16, puerto A1 Ethernet 5069-L320ERS2 (la figura 10 muestra la asignación de SNN 0004_0000_0001 a este puerto), 1756-EN2T y puerto Ethernet 1756-L84ES |
| SNN_2 | Backplane | Ninguno | 1756-L71S, puerto de backplane 1756-L84ES y puerto de backplane 1756-L81ES |
| SNN_3 | DeviceNet | _ — _ | 1732DS-IB6, 1732DS-IBSX0BV4 |
| SNN_4 | Backplane | Ninguno | Backplane 5069-L320ERS2 (la figura 10 muestra la asignación del SNN 0001_0000_0004 a este puerto) y 5069-OBV8S |
| SNN_5 | EtherNet/IP | ~~~ | Puerto A2 Ethernet 5069-L320ERS2 (la figura 10 muestra la asignación del SNN 0004_0000_0005 a este puerto) y 1732ES-IB16 y el puerto Ethernet 1756-L81ES. |

La figura 10 en la página 34 muestra cómo el ejemplo anterior se relaciona con el árbol de E/S del Controller Organizer de Compact GuardLogix 5380 (número de catálogo 5069-L320ERS2).

**Figura 10 - Controller Organizer**




El perfil de configuración de cada dispositivo CIP Safety del árbol de E/S incluye un parámetro para el valor SNN que el controlador utiliza cuando abre la conexión CIP Safety con dicho dispositivo. Este parámetro adopta automáticamente el valor SNN que ya se ha establecido por los SNN que el proyecto conoce:

- Los dispositivos de seguridad (incluidos los controladores de seguridad) que son secundarios directos de un controlador GuardLogix adoptan el SNN que coincide con el controlador del puerto que se utiliza para conectarse con el módulo de seguridad.
  - Los dispositivos de seguridad que están directamente bajo el puerto del backplane adoptan el SNN del puerto del backplane del controlador GuardLogix.
  - Los dispositivos de seguridad que están directamente bajo un puerto Ethernet adoptan el SNN del puerto Ethernet del controlador GuardLogix.
- Los dispositivos de seguridad (incluidos los controladores de seguridad) de una subred remota adoptan el valor SNN que ya se ha asignado a dicha subred, o se genera un nuevo SNN para el primer dispositivo CIP Safety de esa subred.

Le recomendamos que asigne cada SNN de controlador al SNN ya establecido para la subred, lo que permite que la aplicación Studio 5000 Logix Designer asigne el SNN correcto a cada módulo de E/S de seguridad y controlador de seguridad que se añadan al proyecto.

## Cómo los SNN llegan a los dispositivos de seguridad

La mayoría de los módulos de E/S CIP Safety (en el estado predeterminado de fábrica) aceptan el SNN que les asigna el controlador que es propietario de dicho módulo. El valor SNN adoptado automáticamente por la aplicación Studio 5000 Logix Designer para la conexión de ese módulo se acepta cuando el controlador abre la conexión inicial con el módulo.

**IMPORTANTE** Los módulos de E/S CIP Safety conservan su UNID (SNN + nodo) una vez que se les ha asignado y es necesario restablecerlos antes de que se puedan reutilizar con otro valor.

Algunos dispositivos, como otros controladores de seguridad del árbol de E/S, reciben su configuración SNN de una estación de trabajo de programación. Para estos dispositivos, es necesario configurar manualmente la conexión para que utilice el mismo SNN que se ha programado en el dispositivo si la aplicación Studio 5000 Logix Designer no ha asignado automáticamente el SNN correcto.

## Formatos de SNN

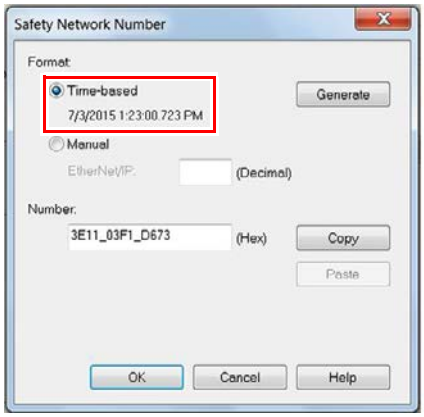
Los SNN que utiliza el sistema son números hexadecimales de 6 bytes. Los SNN pueden establecerse y verse en uno de dos formatos:

- Basado en tiempo
- Manual

### Formato y asignación de SNN basados en tiempo

Cuando se selecciona el formato basado en tiempo, el SNN representa una fecha y una hora concretas.

**Figura 11 - Formatos de SNN**




La asignación de los SNN basados en tiempo es automática cuando se crea un proyecto de controlador de seguridad GuardLogix o se añade EtherNet/IP cambiando el modo IP (solamente Compact GuardLogix 5380) o el tipo de controlador. Los SNN basados en tiempo generados por el software son siempre únicos para el proyecto, ya sea que se generen al crear el proyecto o al cambiar el modo IP. Los dispositivos que se crean directamente bajo el puerto del controlador tienen de manera predeterminada el mismo SNN que el puerto del controlador.

**IMPORTANTE** Si tiene un diagrama de red para su aplicación (por ejemplo, figura 9), debe editar los SNN del controlador para que coincidan con su diagrama de red. Le recomendamos que edite los SNN antes de añadir dispositivos a la configuración de E/S en Controller Organizer.

Los nuevos dispositivos de E/S CIP Safety añadidos a los puertos que están bajo un adaptador (a diferencia de aquellos que están bajo un controlador) siguen reglas similares.

- Si ningún otro dispositivo bajo el puerto utiliza un SNN, se asigna automáticamente un SNN basado en tiempo.
- De no ser así, se asigna al dispositivo el mismo SNN asignado al primer dispositivo por orden de dirección que tiene un SNN.

## Formato y asignación manuales de SNN

Cuando se selecciona el formato manual, el SNN representa un tipo de red y debe tener un valor decimal de 1...9999.

**Figura 12 - Formatos de SNN**


La manipulación manual de un SNN es necesaria en las siguientes situaciones:

- Para asegurarse de que cada puerto de controlador de seguridad de la misma subred tiene el mismo SNN en todos los proyectos.
- Al copiar proyectos de seguridad.

**ATENCIÓN:** Si se copia un proyecto de seguridad en otro proyecto con hardware diferente o en otra ubicación física, y el nuevo proyecto está dentro del mismo sistema de seguridad encaminable, todos los números de red de seguridad deben cambiarse en el segundo sistema. Los valores de SNN no pueden repetirse. Consulte los siguientes manuales del usuario para obtener información sobre cómo cambiar el SNN:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543
- Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001

**IMPORTANTE** Si asigna un SNN manualmente, asegúrese de que la ampliación del sistema no ocasione una duplicación de las combinaciones de SNN y referencias únicas de nodos.

Aparecerá una advertencia si su proyecto contiene combinaciones duplicadas de SNN y referencias únicas de nodos. Aún así, podrá verificar el proyecto, pero le recomendamos que resuelva las combinaciones duplicadas.

No obstante, puede haber dispositivos de seguridad en la red de seguridad encaminable que tengan el mismo SNN y dirección de nodo y que no estén en el proyecto. En este caso, estos dispositivos de seguridad son desconocidos para la aplicación Studio 5000 Logix Designer y no se le mostrará ninguna advertencia.

Si hay referencias únicas de nodos duplicadas, como usuario del sistema usted es el responsable de demostrar que no puede derivar en una condición insegura.

## SNN para dispositivos en su condición original

Los dispositivos de E/S CIP Safety en su condición original no tienen un SNN. El SNN se establece cuando el controlador GuardLogix que es el propietario del dispositivo le envía una configuración al dispositivo.

**IMPORTANTE** Para añadir un dispositivo de E/S CIP Safety a un sistema GuardLogix configurado (el SNN está presente en el controlador GuardLogix), es necesario aplicar el SNN correcto al dispositivo de E/S CIP Safety de reemplazo antes de que se añada a la red CIP Safety.

Para obtener información detallada, consulte el procedimiento de sustitución de dispositivos de E/S de seguridad que aparece en el manual del usuario del controlador:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543
- Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001

## Notas:

# Características de tags de seguridad, tarea de seguridad y programas de seguridad



## Diferenciación entre estándar y seguridad

Puesto que se trata de un controlador Logix, en el sistema de control GuardLogix se pueden utilizar tanto componentes estándar (no relacionados con la seguridad) como componentes relacionados con la seguridad.

Dentro de un proyecto GuardLogix se puede realizar control de automatización estándar de tareas estándar. Los controladores GuardLogix 5580 y los controladores Compact GuardLogix 5380 ofrecen la misma funcionalidad que otros controladores. La diferencia entre estos controladores y los controladores estándar es que estos controladores también proporcionan una tarea de seguridad compatible con SIL 2 o SIL 3.

Sin embargo, es necesario hacer una distinción lógica y visible entre la porción estándar y la porción relacionada con la seguridad de la aplicación. La aplicación Studio 5000 Logix Designer proporciona esta diferenciación mediante la tarea de seguridad, los programas de seguridad, las rutinas de seguridad, los tags de seguridad y los dispositivos de E/S de seguridad.

- Los controladores GuardLogix 5580 permiten proporcionar los niveles SIL 2 y SIL 3 de control de seguridad con la tarea de seguridad. Consulte Certificación SIL en la página 11.
- Los controladores Compact GuardLogix 5380 permiten proporcionar el nivel SIL 2 de control de seguridad con la tarea de seguridad. Consulte Certificación SIL en la página 11.

# Tarea de seguridad

**IMPORTANTE** Solo se pueden utilizar en la tarea de seguridad las instrucciones que se indican en el Apéndice A en la página 71.

Al crear un proyecto GuardLogix se crea automáticamente una sola tarea de seguridad. La tarea de seguridad tiene estas características adicionales:

- Los controladores GuardLogix son los únicos controladores que aceptan la tarea de seguridad.
- La tarea de seguridad no se puede eliminar.
- Los controladores GuardLogix admiten una tarea de seguridad.
- Dentro de la tarea de seguridad se pueden usar varios programas de seguridad, compuestos a su vez por varias rutinas de seguridad.
- No es posible ejecutar rutinas estándar desde dentro de la tarea de seguridad.

La tarea de seguridad es una tarea periódica, por lo que es necesario configurar el período y la prioridad de la tarea de seguridad. La tarea de seguridad se puede interrumpir de acuerdo con las mismas reglas que las tareas estándar (incluidas las interrupciones de la tarea de movimiento, que siempre tiene una prioridad superior a la de cualquier tarea del usuario).

La configuración de la tarea de seguridad con una prioridad mayor (un número más bajo) puede reducir las fluctuaciones en tiempo de ejecución, lo cual puede permitir un ajuste más bajo del temporizador de vigilancia de la tarea de seguridad, que mejora el tiempo de reacción del sistema de seguridad.

**IMPORTANTE** Una gran cantidad de tags de seguridad asignados o una gran cantidad de datos de tags de seguridad producidos/consumidos pueden producir fluctuaciones en el tiempo de escán de la tarea de seguridad del controlador.

## Limitaciones de la tarea de seguridad

Usted especifica tanto el período de la tarea de seguridad como el temporizador de vigilancia de la tarea de seguridad. El período de la tarea de seguridad es el intervalo de tiempo que hay entre ejecuciones sucesivas de la tarea de seguridad. El temporizador de vigilancia de la tarea de seguridad es el tiempo máximo permitido desde el inicio de la ejecución priorizada de la tarea de seguridad hasta que la misma se completa.

Si desea obtener más información acerca del temporizador de vigilancia de la tarea de seguridad, consulte el Apéndice C en la página 81.

El período de la tarea de seguridad está limitado a 500 ms como máximo y no se puede modificar en línea. Asegúrese de que la tarea de seguridad tenga suficiente tiempo para completarse antes de que se vuelva a activar. El tiempo de espera del temporizador de vigilancia de la tarea de seguridad se sobrepasa, se produce un fallo de seguridad no recuperable en el controlador GuardLogix si la tarea de seguridad no termina antes de que caduque el temporizador de vigilancia.

Para obtener más información, consulte el Capítulo 7 en la página 65.

## Detalles de ejecución de la tarea de seguridad

La tarea de seguridad se ejecuta de la misma forma que las tareas periódicas estándar, con las siguientes excepciones:

- Los tags de entrada de seguridad y los tags consumidos de seguridad se actualizan únicamente al principio de la ejecución de la tarea de seguridad. Este proceso implica que, aunque el RPI de E/S pueda ser más breve que el período de la tarea de seguridad, los datos del tag de entrada de seguridad solo se actualizarán una vez al principio de cada ejecución de la tarea de seguridad. La entrada de seguridad y los paquetes consumidos que llegan después del inicio de la tarea de seguridad se almacenarán en un búfer hasta la siguiente ejecución de la tarea de seguridad.
- El tiempo se congela al comienzo de la ejecución de la tarea de seguridad. Como resultado, las instrucciones relacionadas con el temporizador, tales como TON y TOF, no se actualizan durante una ejecución de la tarea de seguridad. Mantienen el tiempo exacto de una ejecución de una tarea a otra, pero el tiempo acumulado no cambia durante la ejecución de la tarea de seguridad.

**ATENCIÓN:** Este comportamiento es diferente de la ejecución de tareas Logix estándar.

- Para los tags estándar asignados a tags de seguridad, los valores de los tags estándar se copian a los tags de seguridad al comienzo de la tarea de seguridad.
  - Es posible que el tag estándar siga cambiando.

**IMPORTANTE** La adición de más tags asignados puede aumentar el tiempo de escán.

  - El código del usuario puede cambiar el tag de seguridad en la tarea de seguridad, pero dicho cambio no se reflejará en el tag estándar.
- Los valores de los tags de salida de seguridad se pueden cambiar durante el escán de la tarea de seguridad mediante el código del la aplicación de seguridad del usuario; el valor final se transmite a los módulos de seguridad al final del escán de la tarea de seguridad. De la misma manera, los valores de seguridad producidos se transmiten a los controladores de seguridad consumidores al final del escán de la tarea de seguridad.

**IMPORTANTE** Mientras que el controlador esté en desbloqueo de seguridad y sin una firma de seguridad, este impedirá el acceso simultáneo de escritura a la memoria de seguridad desde la tarea de seguridad y desde comandos de comunicación. Como resultado, la tarea de seguridad puede permanecer retenida hasta que se complete la actualización de comunicación. El tiempo necesario para la actualización varía de acuerdo al tamaño del tag. Por lo tanto, es posible que expiren la conexión de seguridad y el temporizador de vigilancia de seguridad. (Por ejemplo, si realiza ediciones en línea cuando la tasa de la tarea de seguridad está establecida en 1 ms, podría expirar el temporizador de vigilancia de seguridad).

Para compensar por el tiempo de retención debido a una actualización de comunicación, debe prolongarse el tiempo del temporizador de vigilancia de seguridad.

Dependiendo de la edición, es posible que la tarea de seguridad no tenga suficiente tiempo para finalizar la operación y que expire el temporizador de vigilancia.

Cuando el controlador está en bloqueo de seguridad o cuando existe una firma de seguridad, no puede ocurrir la situación descrita en esta nota.

## Diferencias entre las aplicaciones de seguridad SIL 2 y SIL 3

Una evaluación de riesgos determina si una función de seguridad requiere SIL 2 o SIL 3. Por ejemplo, una máquina tiene varias funciones de seguridad, con un riesgo máximo que solo requiere SIL 2. En tal caso, puede admitirse un controlador con capacidad SIL 2. Mientras tanto, otra máquina cuenta con varias funciones de seguridad, con al menos una que requiere SIL 3. En tal caso, se necesita un controlador compatible con SIL 3.

Tal como se ha comentado en esta publicación, un controlador GuardLogix 5580 SIL 2 solo requiere el controlador primario y un controlador GuardLogix 5580 SIL 3 requiere tanto el controlador primario como el homólogo de seguridad.

**IMPORTANTE** Si se está trabajando por encima de 55 °C (131 °F) en una aplicación SIL 2, los módulos de más de 6.2 W no deben instalarse en ranuras que estén situadas cerca del controlador.

Independientemente de si utiliza una solución SIL 2 o SIL 3, se requiere una firma de seguridad para ambos niveles de integridad de seguridad. Consulte Generación de la firma de la tarea de seguridad en la página 54 para obtener información adicional.

**IMPORTANTE** La tarea de seguridad puede contener varias funciones de seguridad. Para que una determinada función sea SIL 3, la cadena completa de dispositivos y programación desde el sensor hasta el accionador debe ser SIL 3. Tenga cuidado de no utilizar una señal de entrada SIL 2 para una función de seguridad que requiera SIL 3.

## Módulos de E/S de seguridad

Una diferencia entre los niveles de integridad de seguridad es que puede haber disponibles dispositivos de E/S de un solo canal para SIL 2, pero para SIL 3 normalmente se necesitan dispositivos de E/S de doble canal.

Desde el punto de vista de la arquitectura de seguridad, el uso de un solo canal implica que la tolerancia a fallos de hardware (HFT) es cero. Cuando la HFT es cero, hay pautas que indican que los fallos deben detectarse y que la función de seguridad debe llevarse a un estado de seguridad dentro del tiempo de seguridad del proceso. Hay una excepción cuando la tasa de pruebas de diagnóstico es 100 veces la tasa de demanda. Si se utilizan módulos de E/S de seguridad en aplicaciones SIL 2 de un solo canal, debe tenerse en cuenta lo siguiente:

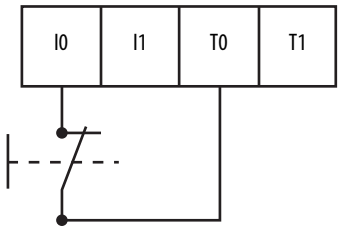
- El canal de entrada o salida debe configurarse para la prueba de impulsos de seguridad.
- El tiempo de seguridad del proceso debe ser superior a 600 ms (el intervalo de prueba de impulsos de E/S de seguridad habitual) o la tasa de demanda debe ser inferior a una demanda por minuto (por ejemplo, una por hora).

Los módulos de entrada de seguridad CompactBlock Guard I/O (serie 1791), ArmorBlock Guard I/O (serie 1732), POINT Guard I/O (serie 1734) y Compact 5000 I/O Safety (serie 5069) admiten circuitos de entrada de seguridad de un solo canal SIL 2 (consulte las consideraciones anteriores) y de doble canal SIL 3. Dado que estos módulos son aptos para el funcionamiento SIL 2 y SIL 3, puede combinar circuitos SIL 2 y SIL 3 en el mismo módulo.

La figura 13 indica cómo cablear circuitos de seguridad SIL 2 a módulos de entrada de seguridad Guard I/O.

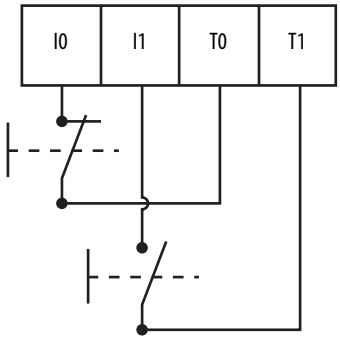
**IMPORTANTE** La fuente de prueba debe configurarse para pruebas de impulsos.

**Figura 13 - Ejemplo de cableado de entrada**



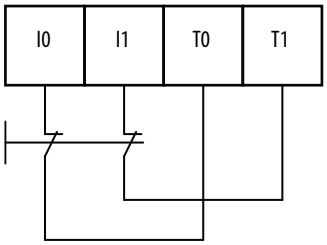

Si dispone de dos circuitos de seguridad SIL 2, puede añadir un segundo como se muestra en la figura 14.

**Figura 14 - Ejemplo de cableado de entradas en parejas**



En la figura 15 se muestra un diagrama de cableado SIL 3 habitual.

**Figura 15 - Cableado SIL 3**




**IMPORTANTE** Estos esquemas de cableado son ejemplos de posibles configuraciones de cableado. Dependiendo de su dispositivo de E/S y la configuración del sistema, es posible que también se puedan emplear otras configuraciones de cableado.

**IMPORTANTE** Las salidas de prueba de impulso incorporadas (T0. . .Tx) generalmente se usan con dispositivos de campo que tienen contactos mecánicos. Si se usa un dispositivo de seguridad que tiene salidas electrónicas (para alimentar entradas de seguridad), dichas salidas deben tener las clasificaciones de seguridad apropiadas.

## Uso de interfaces operador-máquina

Siga estas precauciones y pautas para usar dispositivos HMI en sistemas GuardLogix con clasificación SIL.

### Precauciones

Tome medidas de precaución e implemente técnicas específicas en los dispositivos HMI. Estas precauciones incluyen, entre otras, las siguientes:

- Acceso limitado y protección
- Especificaciones, pruebas y validación
- Restricciones de datos y de acceso
- Límites de datos y de parámetros

Para obtener más información sobre cómo los dispositivos HMI encajan en un lazo SIL típico, consulte Arquitectura GuardLogix en la página 13.

Use técnicas seguras en el software de aplicación dentro de la HMI y el controlador.

### Acceso a los sistemas relacionados con la seguridad

Las funciones relacionadas con la HMI llevan a cabo básicamente dos actividades: leer y escribir datos.

### *Lectura de parámetros en sistemas relacionados con la seguridad*

La lectura de datos no está restringida porque la lectura no afecta el comportamiento del sistema de seguridad. Sin embargo, el número, la frecuencia y el tamaño de los datos que se leen pueden afectar la disponibilidad del controlador. Para evitar falsos disparos relacionados con la seguridad, use buenas prácticas de comunicación para limitar el efecto del procesamiento de comunicaciones en el controlador. No establezca las velocidades de lectura en el valor más rápido posible.

### *Cambio de parámetros en sistemas con clasificación SIL*

Se permite un cambio de parámetro en un lazo relacionado con la seguridad mediante un dispositivo externo (es decir, fuera del lazo de seguridad), por ejemplo, una HMI, con las siguientes restricciones:

- Solo personal especialmente capacitado y autorizado (operadores) puede cambiar los parámetros en sistemas relacionados con la seguridad mediante las HMI.
- El operador que haga cambios en un sistema relacionado con la seguridad mediante una HMI es responsable del efecto de dichos cambios en el lazo de seguridad.
- Usted debe documentar claramente las variables que vayan a ser modificadas.
- Se debe usar un procedimiento de operador claro, completo y explícito para hacer cambios relacionados con la seguridad mediante una HMI.
- Pueden aceptarse cambios en un sistema relacionado con la seguridad solo si ocurre la siguiente secuencia de eventos:
  a. El nuevo valor del parámetro debe enviarse dos veces a dos tags diferentes; es decir, no deben escribirse ambos valores con un comando.
  b. Los dos tags estándar que reciben el valor del parámetro de la HMI deben asignarse a dos tags de seguridad.
  c. El código relacionado con la seguridad que se ejecuta en el controlador debe verificar la equivalencia de ambos tags de seguridad y asegurarse de que estén dentro del rango (verificaciones de límites).
  d. Las dos nuevas variables deben volver a leerse y mostrarse en el dispositivo HMI (la pantalla de la HMI debe leer los tags de seguridad que han recibido los valores de los tags asignados desde los tags estándar).
  e. Los operadores capacitados deben confirmar visualmente que ambas variables sean iguales y que tengan el valor correcto.
  f. Los operadores capacitados deben confirmar manualmente que los valores sean los correctos en la pantalla de la HMI que envía un comando a la lógica de seguridad, lo cual permite que se usen los nuevos valores en la función de seguridad.

  En cada caso el operador debe confirmar la validez del cambio antes de aceptarlo y aplicarlo en el lazo de seguridad.
- Pruebe todos los cambios como parte del procedimiento de evaluación de seguridad.

- Documente de manera suficiente todos los cambios relacionados con la seguridad hechos mediante la HMI, incluidos los siguientes:
  - Autorización
  - Análisis de impacto
  - Ejecución
  - Información de prueba
  - Información de revisión
- Los cambios de la seguridad del proceso al sistema relacionado con la seguridad deben cumplir los requisitos de la norma IEC 61511.
- Los cambios de la seguridad de las máquinas al sistema relacionado con la seguridad deben cumplir los requisitos de la norma IEC 62061.
- El desarrollador debe seguir las mismas técnicas de desarrollo y los mismos procedimientos seguros usados para otro desarrollo de software de aplicación, incluidas la verificación y las pruebas de la interface de operador y su acceso a otras partes del programa. En el software de aplicación del controlador cree una tabla que sea accesible por la HMI y limite el acceso únicamente a los puntos de datos requeridos.
- De modo similar al programa del controlador, el software de HMI se protege y mantiene la conformidad con el nivel SIL después de que el sistema haya sido validado y probado.

## Programas de seguridad

Un programa de seguridad tiene los atributos de un programa estándar, con la excepción de que solo se puede programar en la tarea de seguridad. Un programa de seguridad también puede definir tags de seguridad cubiertos por el programa. Un programa de seguridad puede ser priorizado o no priorizado.

Un programa de seguridad solo puede contener componentes de seguridad. Todas las rutinas de un programa de seguridad son rutinas de seguridad. Un programa de seguridad no puede contener rutinas estándar ni tags estándar.

## Rutinas de seguridad

Las rutinas de seguridad tienen los atributos de las rutinas estándar, con la excepción de que solo pueden existir en los programas de seguridad, no pueden leer ni escribir tags estándar, y solo se pueden crear en lógica de escalera. Una rutina de seguridad debe designarse como la rutina principal de cada programa de seguridad. Otra rutina de seguridad puede designarse como la rutina de fallo de dicho programa de seguridad. En las rutinas de seguridad solo se utilizan instrucciones certificadas de seguridad.

Para consultar la lista de instrucciones de seguridad, remítase al Apéndice A en la página 71.

## Tags de seguridad

El sistema de control GuardLogix admite el uso de tags estándar y tags de seguridad en el mismo proyecto. Sin embargo, el software de programación diferencia desde el punto de vista operativo los tags estándar de los tags de seguridad.

Los tags de seguridad tienen los atributos de los tags estándar, con la adición de mecanismos que proporcionan integridad de los datos al nivel SIL configurado (SIL 2 o SIL 3).

Los tags de seguridad pueden estar compuestos de lo siguiente:

- Todos los tipos de datos primitivos (por ejemplo, BOOL, SINT, INT, DINT, LINT, REAL)
- Los tipos predefinidos que se utilizan para las instrucciones de aplicaciones de seguridad
- Matrices o tipos de datos definidos por el usuario compuestos por los dos tipos anteriores

La aplicación Studio 5000 Logix Designer ayuda a evitar la creación directa de tags no válidos en un programa de seguridad. Si los tags no válidos son importados, no podrán verificarse.

**IMPORTANTE** Los alias entre tags estándar y de seguridad están prohibidos en las aplicaciones de seguridad.

Los tags son clasificados como tags de seguridad que puede ser, o bien cubiertos por el controlador, o bien cubiertos por el programa. La lógica estándar o de seguridad, así como otros dispositivos de comunicación, pueden leer tags de seguridad cubiertos por el controlador, pero solo la lógica de seguridad u otro controlador de seguridad GuardLogix mediante un tag consumido pueden escribir los tags de seguridad cubiertos por el controlador. Solo las rutinas de seguridad locales pueden tener acceso a los tags de seguridad cubiertos por el programa. Estas rutinas residen en un programa de seguridad.

Los tags asociados con E/S de seguridad y los datos de seguridad producidos o consumidos deben ser tags de seguridad cubiertos por el controlador.

**IMPORTANTE** Los tags de entrada de seguridad y los tags consumidos de seguridad pueden ser leídos por cualquier rutina estándar, pero la velocidad de actualización está basada en la ejecución de la tarea de seguridad. Estos tags se actualizan al principio de la ejecución de la tarea de seguridad, lo que difiere del comportamiento estándar de los tags.

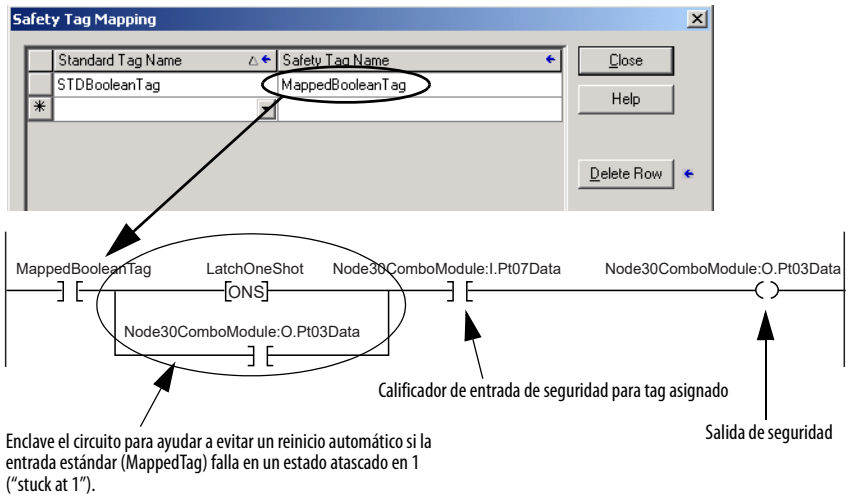
## Tags estándar en rutinas de seguridad (asignación de tags)

Los tags estándar cubiertos por el controlador se pueden asignar a tags de seguridad, lo que proporciona un mecanismo para sincronizar las acciones estándar y las de seguridad.

**ATENCIÓN:** Cuando utilice datos estándar en una rutina de seguridad, usted será responsable de proporcionar una forma más confiable de garantizar que los datos se utilicen de manera apropiada. El uso de datos estándar en un tag de seguridad no los convierte en datos de seguridad. No se debe controlar directamente una salida de seguridad con datos de tag estándar.

Este ejemplo ilustra cómo calificar los datos estándar con datos de seguridad.

**Figura 16 - Calificación de datos estándar con datos de seguridad**



# Desarrollo de la aplicación de seguridad



## Suposiciones sobre el concepto de seguridad

El concepto de seguridad parte de los siguientes requisitos:

- Si usted es responsable de crear, operar y mantener la aplicación, debe estar debidamente calificado y especialmente capacitado, y tener experiencia en sistemas de seguridad.
- Usted aplica la lógica correctamente, lo que significa que los errores de programación pueden detectarse mediante un cumplimiento estricto de las especificaciones, la programación y las reglas de nombrado que pueden detectar errores de programación.
- Usted realiza un análisis crítico de la aplicación y hace uso de todas las medidas posibles para detectar un fallo.
- Usted confirma todas las descargas de la aplicación mediante la verificación manual de la firma de seguridad.
- Antes de poner en marcha un sistema relacionado con la seguridad, usted realiza una prueba de funcionamiento completa de todo el sistema. Esta prueba incluye, entre otras, las siguientes:
  - Validación de la funcionalidad global de las funciones de seguridad implementadas, incluyendo la configuración de E/S realizada por los perfiles Add-On (AOP), más allá de los límites de los dispositivos individuales (pruebas de límites).
  - Verificación de que se utilizan las versiones correctas del software.

**Tabla 1 - Efecto de los modos del controlador sobre la ejecución de seguridad**

| Modo de controlador | Comportamiento del controlador |
|---|---|
| Programa | • Las conexiones de entrada y salida de seguridad se establecen y se mantienen:<br>– Los tags de entrada de seguridad se actualizan para reflejar los valores de entrada de seguridad.<br>• La lógica de la tarea de seguridad no se está escaneando. |
| Prueba | • Las conexiones de entrada y salida de seguridad se establecen y se mantienen:<br>– Los tags de entrada de seguridad se actualizan para reflejar los valores de entrada de seguridad.<br>• La lógica de la tarea de seguridad se está escaneando. |
| Marcha | • Las conexiones de entrada y salida de seguridad se establecen y se mantienen:<br>– Los tags de entrada de seguridad se actualizan para reflejar los valores de entrada de seguridad.<br>– El controlador envía paquetes de salida de seguridad de "marcha".<br>• La lógica de la tarea de seguridad se está escaneando.<br>• Toda la lógica del proceso de la tarea de seguridad y las salidas de lógica de comparación cruzada. Se escriben salidas lógicas a las salidas de seguridad. |

**Tabla 2 - Estado de la aplicación de seguridad**

| Estado de la tarea de seguridad | Seguridad[1] (hasta) | Comportamiento del controlador |
|---|---|---|
| Desbloqueado<br>Sin firma | Solo para fines de desarrollo | • Puede haber forzados de E/S de seguridad.<br>• Pueden modificarse los forzados de E/S de seguridad.<br>• Se admite la edición en línea de seguridad.<br>• La memoria de seguridad está aislada, pero no está protegida (lectura/escritura). |
| Bloqueada<br>Sin firma | Solo para fines de desarrollo | • No se admiten forzados de E/S de seguridad (los forzados de E/S de seguridad deben eliminarse antes de que sea posible el bloqueo).<br>• No se admite la edición en línea de la tarea de seguridad.<br>• La memoria de seguridad está protegida (lectura solamente). |
| Desbloqueado<br>Con firma | SIL 3/PLe/cat. 4<br>Control confiable | • No se admiten forzados de E/S de seguridad. (Los forzados de E/S de seguridad deben eliminarse antes de que se pueda generar una firma).<br>• No se admite la edición en línea de la tarea de seguridad.<br>• La memoria de seguridad está protegida (lectura solamente).<br>• La firma de seguridad permite la recuperación desde un fallo de seguridad no recuperable sin repetir la descarga.<br>• La firma de seguridad no está protegida y cualquiera con acceso al controlador puede eliminarla. |
| Bloqueado<br>Con firma | SIL 3/PLe/cat. 4<br>Control confiable | • No se admiten forzados de E/S de seguridad.<br>• No se admite la edición en línea de la tarea de seguridad.<br>• La memoria de seguridad está protegida (lectura solamente).<br>• La firma de seguridad permite la recuperación desde un fallo de seguridad no recuperable sin repetir la descarga.<br>• La firma de seguridad está protegida. Los usuarios deben introducir la contraseña de desbloqueo para desbloquear el controlador antes de eliminar la firma de seguridad. |

(1) Para lograr este nivel, debe cumplir los requisitos de seguridad que se definen en este manual de referencia de seguridad.

## Nociones básicas de desarrollo y pruebas de aplicaciones

Le recomendamos que un integrador de sistemas o un usuario con capacitación y experiencia en aplicaciones de seguridad desarrolle el programa de aplicación para el sistema SIL 2 o SIL 3 previsto. El especialista en desarrollo debe seguir buenas prácticas de diseño:

- Usar especificaciones funcionales, tales como diagramas de flujo, diagramas de temporización y diagramas de secuencia.
- Hacer una revisión de la lógica de la tarea de seguridad.
- Hacer la validación de la aplicación.

El ambiente Studio 5000® es un conjunto de herramientas que cuenta con certificación como herramienta fuera de línea según la cláusula 7.4.4 de la norma

IEC 61508-3. Cuando desarrolle su aplicación de seguridad, tenga en cuenta lo siguiente:

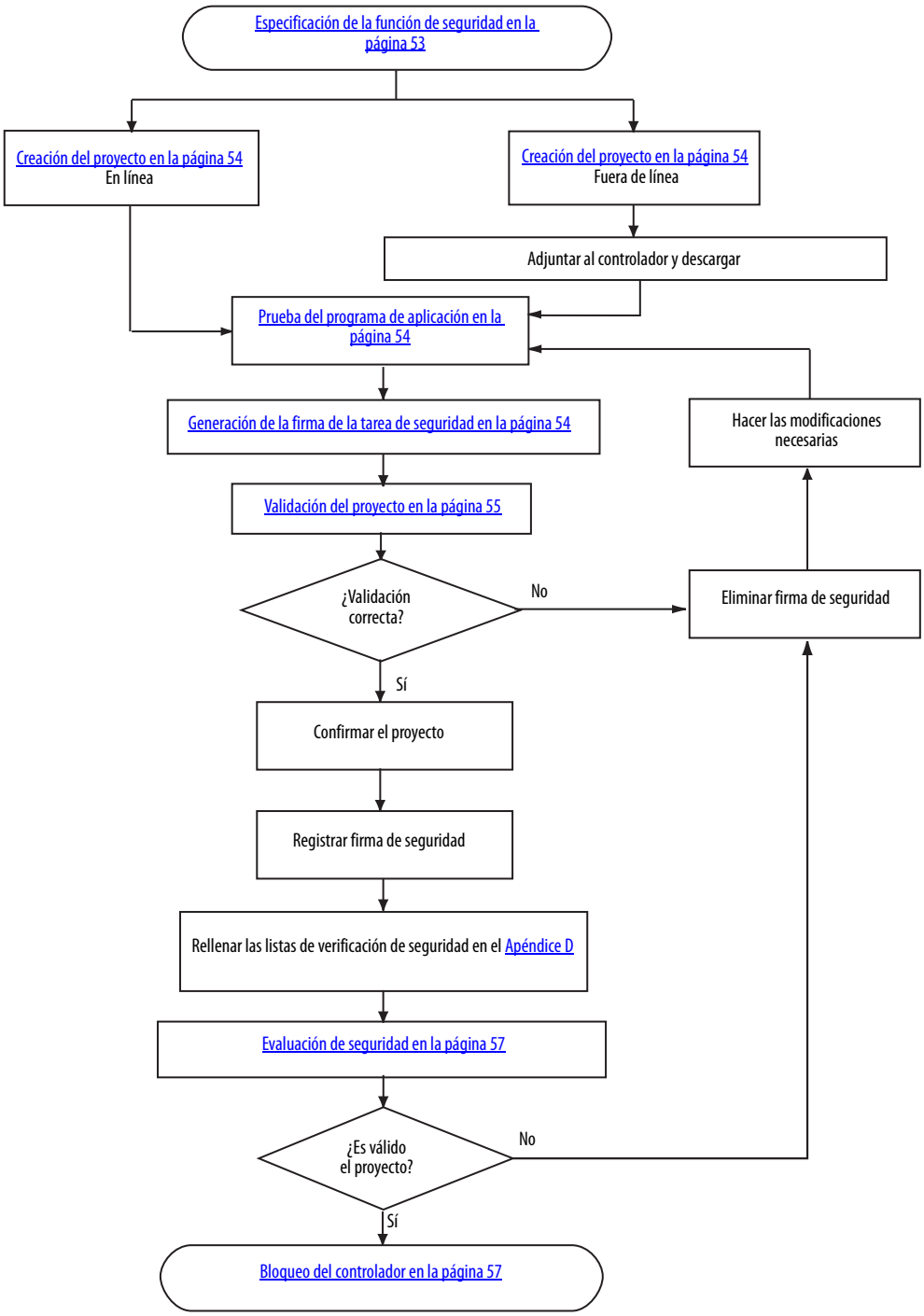
**IMPORTANTE**

- La aplicación Studio 5000 Logix Designer se ha certificado según la cláusula 7.4.4 de la norma IEC 61508-3, 2.ª edición, y puede utilizarse durante el ciclo de vida de codificación de aplicaciones basadas en GuardLogix y también como ayuda en las fases del ciclo de vida de prueba de módulo, prueba de integración y prueba de validación. Como resultado, no se necesita ninguna justificación adicional para su uso durante estas fases del ciclo de vida. No obstante, si se utilizan otras herramientas, ya sea por sí solas o con la aplicación Studio 5000 Logix Designer, es posible que se necesite una justificación adicional para esas otras herramientas. Es su responsabilidad verificar que las demás herramientas fuera de línea que se utilizan durante todas las fases del ciclo de vida se seleccionan como un componente coherente de las actividades de desarrollo de software.
- Es su responsabilidad llevar a cabo una evaluación para determinar el nivel de confiabilidad que se concede a la aplicación Studio 5000 Logix Designer y los posibles mecanismos de fallo que pueden afectar al software ejecutable cuando la aplicación Studio 5000 Logix Designer se emplea de una manera diferente a la que se especifica en la documentación del producto.
- Debe verificar que toda la información de programación y configuración que se introduce en la aplicación Studio 5000 Logix Designer y se descarga al controlador cumple los requisitos de su aplicación. Consulte Confirmación del proyecto en la página 56 para obtener más información.
- Según requiera el nivel de integridad de seguridad, la representación del diseño o el software deben coincidir con las características de la aplicación.
- Según requiera el nivel de integridad de seguridad, la representación del diseño o el software debe ser compatible con las características que admiten la aplicación Studio 5000 Logix Designer y los controladores GuardLogix. Es su responsabilidad verificar que la representación de diseño y el software deseados seon compatibles con la aplicación Studio 5000 Logix Designer y los controladores GuardLogix.
  Por ejemplo: si el diseño se representa en forma de diagrama de flujo, es su responsabilidad convertir dicho diseño en un diagrama de lógica de escalera.
- El uso de herramientas de otros fabricantes o desarrolladas internamente para generar la lógica automáticamente a fin de importarla a la aplicación Studio 5000 Logix Designer para su compilación y descarga a un controlador GuardLogix requiere evaluar su idoneidad en el punto del ciclo de desarrollo donde se selecciona.

## Ciclo de vida de puesta en marcha

El diagrama de flujo muestra los pasos necesarios para poner en marcha un sistema GuardLogix. Consulte los vínculos para ver una explicación de dichos temas.

**Figura 17 - Puesta en servicio del sistema**



## Especificación de la función de seguridad

Debe crearse una especificación para la función de seguridad. Utilice esta especificación para verificar que la lógica del programa aborda de manera correcta y completa los requisitos de control de seguridad y funcionales de su aplicación. En algunas aplicaciones, la especificación puede presentarse en diversos formatos. No obstante, la especificación debe ser una descripción detallada que incluya lo siguiente (si corresponde):

- Secuencia de operaciones
- Diagramas de flujo y de temporización
- Diagramas de secuencias
- Descripción del programa
- Copia impresa del programa
- Descripciones por escrito de los pasos con condiciones de pasos y accionadores que deben controlarse, lo que incluye lo siguiente:
  - Definiciones de las entradas
  - Definiciones de las salidas
  - Referencias y diagramas de cableado de E/S
  - Definición del funcionamiento
- Matriz o tabla de condiciones por pasos, y los accionadores que deben controlarse, incluidos los diagramas de secuencia y de temporización
- Definición de condiciones marginales; por ejemplo, modos de operación y de paro de emergencia

La porción de E/S de la especificación debe contener el análisis de los circuitos de campo, es decir, el tipo de sensores y de accionadores.

- Sensores (digitales o analógicos)
  - Señal en operación estándar (en el caso de sensores digitales, si están desactivados no se transmiten señales)
  - Determinación de las redundancias que son necesarias para los niveles SIL
  - Monitoreo y visualización de discrepancias, incluida la lógica de diagnóstico
- Accionadores
  - Posición y activación en la operación estándar (normalmente activado)
  - Reacción/posicionamiento de seguridad cuando se conmuta a desactivado o cuando se produce un fallo en la energía eléctrica
  - Monitoreo y visualización de discrepancias, incluida la lógica de diagnóstico

## Creación del proyecto

La lógica y las instrucciones que se utilizan en la programación de la aplicación deben ser como sigue:

- Fáciles de comprender
- Fáciles de rastrear
- Fáciles de cambiar
- Fáciles de probar

Revise y pruebe toda la lógica. Mantenga separadas la lógica relacionada con la seguridad de la lógica estándar.

*Etiquetado del programa*

Utilice estas etiquetas para identificar claramente el programa de aplicación:

- Nombre
- Fecha
- Revisión
- Cualquier otra información útil

## Prueba del programa de aplicación

Este paso consta de cualquier combinación de los modos Run y Program, ediciones en línea o fuera de línea, cargas y descargas, y pruebas informales necesarias para que la aplicación funcione debidamente en preparación para la prueba de validación del proyecto.

## Generación de la firma de la tarea de seguridad

**ATENCIÓN:** Se necesita una firma de seguridad para que el controlador pueda funcionar con una clasificación SIL 2 o SIL 3. El funcionamiento sin firma de seguridad solo es aceptable durante el desarrollo.

**IMPORTANTE** Debe emplearse una de las siguientes ediciones de la aplicación Studio 5000 Logix Designer para generar una firma de seguridad: Professional, Full, Lite Edition o un editor de GuardLogix 9324-RLDGLXE independiente.

La firma de seguridad se aplica a toda la porción de seguridad del controlador e identifica de manera única cada proyecto, incluida su lógica, datos y configuración. La firma de seguridad está compuesta por el ID (número de identificación), la fecha y la hora.

La firma de seguridad puede generarse si se cumplen las siguientes condiciones:

- La aplicación Studio 5000 Logix Designer está en línea con el controlador.
- El controlador está en modo de programa.
- El controlador está en desbloqueo de seguridad.

- El controlador no tiene forzados de seguridad ni ediciones de seguridad pendientes en línea.
- El estado de la tarea de seguridad es OK.

Una vez finalizadas las pruebas del programa de aplicación, debe generar la firma de seguridad. El software de programación carga automáticamente la firma de seguridad una vez que ha sido generada.

**IMPORTANTE** Cuando se ha validado la aplicación de seguridad, es posible que haya ocasiones que requieran que se repita la descarga (por ejemplo, al modificar la aplicación estándar) aunque no se haya cambiado la aplicación de seguridad.

Para verificar que se haya descargado la aplicación de seguridad correcta, registre manualmente la firma de seguridad después de la creación inicial y compruebe la firma de seguridad después de cada descarga para asegurarse de que coincide con la original.

Se puede eliminar la firma de seguridad solo cuando el controlador GuardLogix está en desbloqueo de seguridad y, si está en línea, cuando el interruptor de llave está en la posición REM o PROG. Cuando está seleccionado Protect Signature in Run mode, el controlador no permite eliminar la firma de seguridad en modo de marcha.

No se puede actualizar el firmware cuando existe una firma de seguridad.

Cuando existe una firma de seguridad no se pueden realizar las siguientes acciones dentro de la tarea de seguridad:

- Programación o edición en línea o fuera de línea de componentes de seguridad
- Forzado de E/S de seguridad
- Manipulación de datos de componentes de seguridad (excepto mediante la lógica de rutina o de otro controlador GuardLogix)

## Validación del proyecto

Para comprobar si el programa de aplicación cumple las especificaciones es necesario generar un conjunto adecuado de escenarios de prueba que cubran la aplicación. El conjunto de escenarios de prueba debe archivarse y conservarse como especificación de prueba.

Es necesario incluir un grupo de pruebas para comprobar la validez de los cálculos (fórmulas) utilizados en la lógica de la aplicación. Es aceptable utilizar pruebas de rangos equivalentes. Estas son pruebas dentro de los rangos de valores definidos, en los límites, o en rangos de valores no válidos. El número necesario de escenarios de prueba depende de las fórmulas que se utilicen y debe incluir pares de valores críticos.

También se debe incluir una simulación activa con fuentes (dispositivos de campo), ya que es la única forma de verificar que los sensores y los accionadores del sistema estén cableados correctamente. Verifique la operación de las funciones programadas manipulando manualmente los sensores y los accionadores.

También debe incluir pruebas para verificar la reacción frente a fallos de cableado y fallos de comunicación en red.

La validación del proyecto incluye pruebas de rutinas de fallo y canales de entrada y salida, a fin de asegurarse de que el sistema de seguridad funcione adecuadamente.

Para realizar una prueba de validación del proyecto en el controlador GuardLogix es necesario realizar una prueba completa de la aplicación. Es necesario alternar cada sensor y accionador que se utilicen en cada función de seguridad. Es necesario asegurarse de probar todas las funciones de desactivación, ya que estas funciones generalmente no se ejecutan durante la operación normal.

Además, tenga presente que una prueba de validación del proyecto es válida solo para la aplicación específica que se esté probando. Si la aplicación de seguridad se traslada a otra instalación, deberá realizar la puesta en marcha y la validación del proyecto en la aplicación de seguridad en el contexto de los nuevos sensores, accionadores, cableado, redes y equipos físicos del sistema de control.

## Confirmación del proyecto

Se debe imprimir o ver el proyecto y comparar las E/S de seguridad cargadas y las configuraciones del controlador, los datos de seguridad y la lógica del programa de la tarea de seguridad para asegurarse de que los componentes de seguridad adecuados hayan sido descargados, probados y conservados en el programa de aplicación de seguridad.

Si el programa de aplicación contiene una instrucción Add-On de seguridad que haya sido sellada con una firma de instrucción, también es necesario comparar la firma de la instrucción, la fecha/hora y la firma de la instrucción de seguridad frente a los valores registrados al sellar la instrucción Add-On.

Consulte el Apéndice B en la página 75 para obtener información sobre la creación y el uso de las instrucciones Add-On de seguridad en aplicaciones SIL 3.

Los siguientes pasos ilustran un método para confirmar el proyecto.

1. Mientras esté en línea con el controlador, y teniendo el controlador en modo de programa, guarde el proyecto.
2. Responda Yes cuando aparezca Upload Tag Values.
3. Con la aplicación Studio 5000 Logix Designer fuera de línea, guarde el proyecto con un nuevo nombre, como Offlineprojectname.ACD, donde “projectname” es el nombre del proyecto. Este archivo es el nuevo archivo del proyecto maestro probado.
4. Cierre el proyecto.
5. Mueva el archivo de proyecto original fuera de su directorio actual. Puede eliminar este archivo o guardarlo en una ubicación de almacenamiento. Se requiere este paso porque si la aplicación Studio 5000 Logix Designer encuentra projectname.ACD en este directorio, lo correlaciona con el proyecto del controlador y no realiza una verdadera carga.

6. Con el controlador todavía en el modo de programa, cargue el proyecto desde el controlador.
7. Guarde el proyecto cargado como Onlineprojectname.ACD, donde "projectname" es el nombre de su proyecto.
8. Responda Yes cuando aparezca Upload Tag Values.
9. Use la utilidad de comparación de programas de Studio 5000 Logix Designer para realizar estas comparaciones:
   - Compare todas las propiedades del controlador GuardLogix y los de dispositivos de E/S CIP Safety.
   - Compare todas las propiedades de la tarea de seguridad, de los programas de seguridad y de las rutinas de seguridad.
   - Compare toda la lógica de las rutinas de seguridad.
10. Verifique que toda la configuración del controlador y las E/S cumplen los requisitos de la especificación de la aplicación.

## Evaluación de seguridad

Es posible que sea necesario que un tercero revise el sistema de seguridad antes de que este quede aprobado para funcionar. Es posible que se requiera una certificación independiente a cargo de un tercero para los niveles SIL 2 o SIL 3 de IEC 61508.

## Bloqueo del controlador

Le recomendamos que realice un bloqueo de seguridad del controlador GuardLogix para contribuir a impedir que se modifiquen los componentes del control de seguridad. No obstante, el bloqueo de seguridad del controlador no es un requisito para SIL 2 o SIL 3. La característica de bloqueo de seguridad solo se aplica a los componentes de seguridad, como la tarea de seguridad, los programas de seguridad, las rutinas de seguridad, los tags de seguridad, las instrucciones Add-On de seguridad, las E/S de seguridad y la firma de seguridad. No obstante, el bloqueo de seguridad por sí solo no satisface los requisitos de SIL 2 o SIL 3.

Ningún aspecto de seguridad puede ser modificado mientras el controlador esté en el estado de bloqueo de seguridad. Cuando el controlador está en bloqueo de seguridad no se permiten las siguientes acciones dentro de la tarea de seguridad:

- Actualización del firmware
- Programación o edición en línea o fuera de línea
- Forzado de E/S de seguridad
- Manipulación de datos de componentes de seguridad (excepto mediante la lógica de rutina o de otro controlador GuardLogix)
- Creación o edición de instrucciones Add-On de seguridad
- Generación o eliminación de la firma de seguridad

| **IMPORTANTE** | Si existe una firma de seguridad y el controlador está en bloqueo de seguridad, solo se podrán descargar al controlador los proyectos con una firma de seguridad que coincida. |
|---|---|

El estado predeterminado del controlador es el estado de desbloqueo de seguridad. Puede colocar la aplicación de seguridad en un estado de bloqueo de seguridad independientemente de si usted está en línea o fuera de línea, o si tiene la fuente original del programa. Sin embargo, no puede haber forzados de seguridad ni ediciones pendientes de seguridad. El estado de bloqueo o de desbloqueo de seguridad no se puede modificar cuando el interruptor de llave está en la posición RUN.

Para contar con una capa adicional de protección es posible utilizar contraseñas para realizar el bloqueo o desbloqueo de seguridad del controlador. Las contraseñas son opcionales.

Para obtener más información acerca de la característica de bloqueo de seguridad, consulte el manual del usuario del controlador:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543
- Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001

## Descarga del programa de aplicación de seguridad

Al realizar la descarga es necesario realizar pruebas de la aplicación, a no ser que exista una firma de seguridad.

| | |
|---|---|
| **IMPORTANTE** | Para verificar que se ha descargado o restaurado la aplicación de seguridad correcta desde una tarjeta de memoria, debe comprobar manualmente que la firma de seguridad coincide con la firma original que aparece en la documentación de seguridad. |

Las descargas a un controlador GuardLogix con bloqueo de seguridad solo se permiten si la firma de seguridad y la revisión de firmware del proyecto fuera de línea coinciden con el contenido del controlador GuardLogix de destino y el estado de la tarea de seguridad del controlador es OK.

| | |
|---|---|
| **IMPORTANTE** | Si la firma de seguridad no coincide y el controlador está en bloqueo de seguridad, será necesario desbloquear el controlador para la descarga. En este caso, la descarga al controlador elimina la firma de seguridad. Como resultado, será necesario volver a validar la aplicación. |

## Carga del programa de aplicación de seguridad

Si el controlador GuardLogix contiene una firma de seguridad, dicha firma de seguridad se carga al guardar en línea el proyecto. Como resultado, todos los valores de los tags de seguridad fuera de línea se actualizan a los valores de la copia dinámica guardados en el momento en que se generó la firma. En este caso, la opción de cargar los valores de los tags solo afecta los valores de los tags estándar.

## Almacenamiento y carga de un proyecto desde una tarjeta de memoria

Los controladores GuardLogix y Compact GuardLogix admiten actualizaciones de firmware, así como almacenamiento y recuperación del programa de usuario con una tarjeta de memoria. En un sistema GuardLogix, solo el controlador primario usa una tarjeta de memoria.

Para almacenar un proyecto de seguridad en una tarjeta de memoria, le recomendamos que seleccione Remote Program como modo de carga, es decir, el modo al que entra el controlador después de la carga. Antes de que la máquina pueda ponerse en funcionamiento es necesario que el operador intervenga para arrancar la máquina.

Es posible iniciar una carga desde una tarjeta de memoria solo bajo estas condiciones:

- Si el tipo de controlador especificado por el proyecto almacenado en la tarjeta de memoria coincide con su tipo de controlador.
- Si las revisiones mayor y menor del proyecto alojadas en la tarjeta de memoria coinciden con las revisiones mayor y menor del controlador.

**IMPORTANTE** Una desigualdad en la revisión ayuda a evitar únicamente cargas iniciadas por el usuario. Las cargas iniciadas por el controlador sobrescriben el firmware del controlador con el contenido de la tarjeta de memoria.

- Si su controlador no está en el modo de marcha.

La carga de un proyecto a un controlador con bloqueo de seguridad está permitida solo cuando la firma de seguridad del proyecto almacenado en la tarjeta de memoria coincide con el proyecto en el controlador. Si las firmas no coinciden o el controlador tiene bloqueo de seguridad sin una firma de seguridad, primero debe desbloquear el controlador antes de actualizar el controlador mediante una tarjeta de memoria.

**IMPORTANTE** Si usted desbloquea el controlador e inicia una carga desde la tarjeta de memoria, el estado de bloqueo de seguridad, las contraseñas y la firma de seguridad se establecen con los valores contenidos en la tarjeta de memoria una vez concluida la carga.

## Forzado de datos

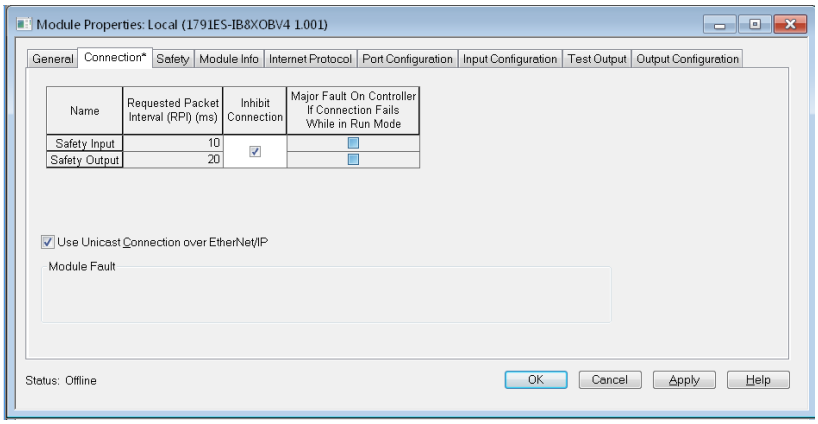
Todos los datos contenidos en un tag de seguridad de E/S, producido o consumido, incluido CONNECTION_STATUS, pueden ser forzados mientras el proyecto está en desbloqueo de seguridad y no existe una firma de seguridad. Sin embargo, los forzados no solo deben ser inhabilitados sino también eliminados en todos los tags de seguridad para que el proyecto de seguridad pueda estar en bloqueo de seguridad o para que se pueda generar una firma de seguridad. Los tags de seguridad no se pueden forzar mientras el proyecto esté en bloqueo de seguridad ni cuando exista una firma de seguridad.

**SUGERENCIA** Es posible instalar y eliminar los forzados en los tags estándar, independientemente de si el estado es de bloqueo o de desbloqueo de seguridad.

## Inhibición de un dispositivo

No es posible inhibir o desinhibir dispositivos de E/S de seguridad ni controladores productores si el programa de aplicación está en bloqueo de seguridad o si existe una firma de seguridad. Siga estos pasos para inhibir un dispositivo específico de E/S de seguridad.

1. En la aplicación Studio 5000 Logix Designer, haga clic con el botón derecho del mouse en el dispositivo y seleccione Properties.
2. En el cuadro de diálogo Module Properties, haga clic en la ficha Connection.
3. Seleccione Inhibit Connection y haga clic en Apply.




El dispositivo está inhibido siempre que la casilla de verificación esté seleccionada. Si un dispositivo de comunicación está inhibido, todos los dispositivos en la rama descendente también están inhibidos.

## Edición en línea

La edición en línea de la lógica estándar no se ve afectada por el estado de seguridad.

**SUGERENCIA** Las ediciones en línea en las rutinas estándar no se ven afectadas por el estado de bloqueo o de desbloqueo de seguridad.

**ATENCIÓN:** La realización de una modificación en línea (a la lógica, los datos o la configuración) puede afectar la función de seguridad del sistema si la modificación se realiza mientras se está ejecutando la aplicación. Las modificaciones en línea solo deben realizarse si son imprescindibles. Si la modificación no se realiza correctamente, puede detener la aplicación. Por lo tanto, antes de realizar una modificación en línea, deben emplearse medidas de seguridad alternativas durante la actualización.

La edición en línea de la lógica de seguridad solo puede realizarse cuando el controlador está en desbloqueo de seguridad y no está firmado. Siga estas pautas para editar la lógica de seguridad en línea:

- Si el controlador está bloqueado con ediciones de seguridad, deberá desbloquearlo para ensamblar o cancelar las ediciones.
- Para las rutinas de seguridad, no es posible bloquear el controlador cuando hay una edición pendiente, pero sí puede bloquearse cuando hay una edición de prueba.
- Al cambiar los parámetros de configuración de una instrucción de seguridad existente, debe cambiar el controlador al modo de programa y regresar al modo de marcha antes de que los cambios surtan efecto.

No se pueden editar instrucciones estándar ni instrucciones Add-On de seguridad mientras se está en línea.

## Edición de la aplicación de seguridad

Las siguientes reglas se aplican al cambio del programa de aplicación de seguridad en la aplicación Studio 5000 Logix Designer:

- Solo personal autorizado y con la debida capacitación puede realizar ediciones en los programas. Este personal debe utilizar todos los métodos de supervisión disponibles como, por ejemplo, protecciones con contraseña para el software e interruptor de llave para el controlador.
- Cuando las ediciones en los programas están a cargo de personal debidamente autorizado y capacitado, este personal asume la responsabilidad de la seguridad central mientras se realizan los cambios. Este personal también debe mantener la operación segura de la aplicación.
- Al realizar una edición en línea es necesario utilizar un mecanismo de protección alternativo para mantener la seguridad del sistema.
- Es necesario documentar suficientemente todas las ediciones del programa, lo que incluye lo siguiente:
  - Autorización
  - Análisis de impacto
  - Ejecución
  - Información de prueba
  - Información de revisión
- Si existen ediciones en línea solo en las rutinas estándar, no es necesario validar esas ediciones antes de volver a la operación normal.
- Es necesario asegurarse de que los cambios en la rutina estándar, relativos a la temporización y a la asignación de tags, sean aceptables para su aplicación de seguridad.
- Es posible editar la porción lógica de su programa, ya sea en línea o fuera de línea, tal y como se describe en las siguientes secciones.

### Ediciones fuera de línea

Cuando se realizan ediciones fuera de línea solamente a elementos del programa estándar y si la firma de seguridad coincide tras una descarga, es posible reanudar la operación.

Cuando las ediciones fuera de línea afectan al programa de seguridad, antes de reanudar el funcionamiento es necesario volver a validar todos los elementos afectados de la aplicación, según lo determinado por el análisis de impacto.

La figura 18 en la página 63 ilustra el proceso de edición fuera de línea.

### Ediciones en línea

Si las ediciones en línea afectan el programa de seguridad, antes de reanudar la operación es necesario volver a validar todos los elementos afectados de la aplicación, según lo determinado por el análisis de impacto. La figura 18 en la página 63 muestra el proceso de edición en línea.

**SUGERENCIA** Limite las ediciones en línea a modificaciones menores en los programas, como cambios de puntos de ajuste o adiciones, eliminaciones y modificaciones menores en la lógica.

Las características de bloqueo de seguridad y firma de seguridad del controlador GuardLogix afectan las ediciones en línea.

Consulte Generación de la firma de la tarea de seguridad en la página 54 y Bloqueo del controlador en la página 57 para obtener más información.

Para obtener información detallada acerca de cómo editar la lógica de escalera en la aplicación Studio 5000 Logix Designer mientras está en línea, consulte el documento Logix5000 Controllers Quick Start, publicación 1756-QS001.

## Modificación de la prueba de impacto

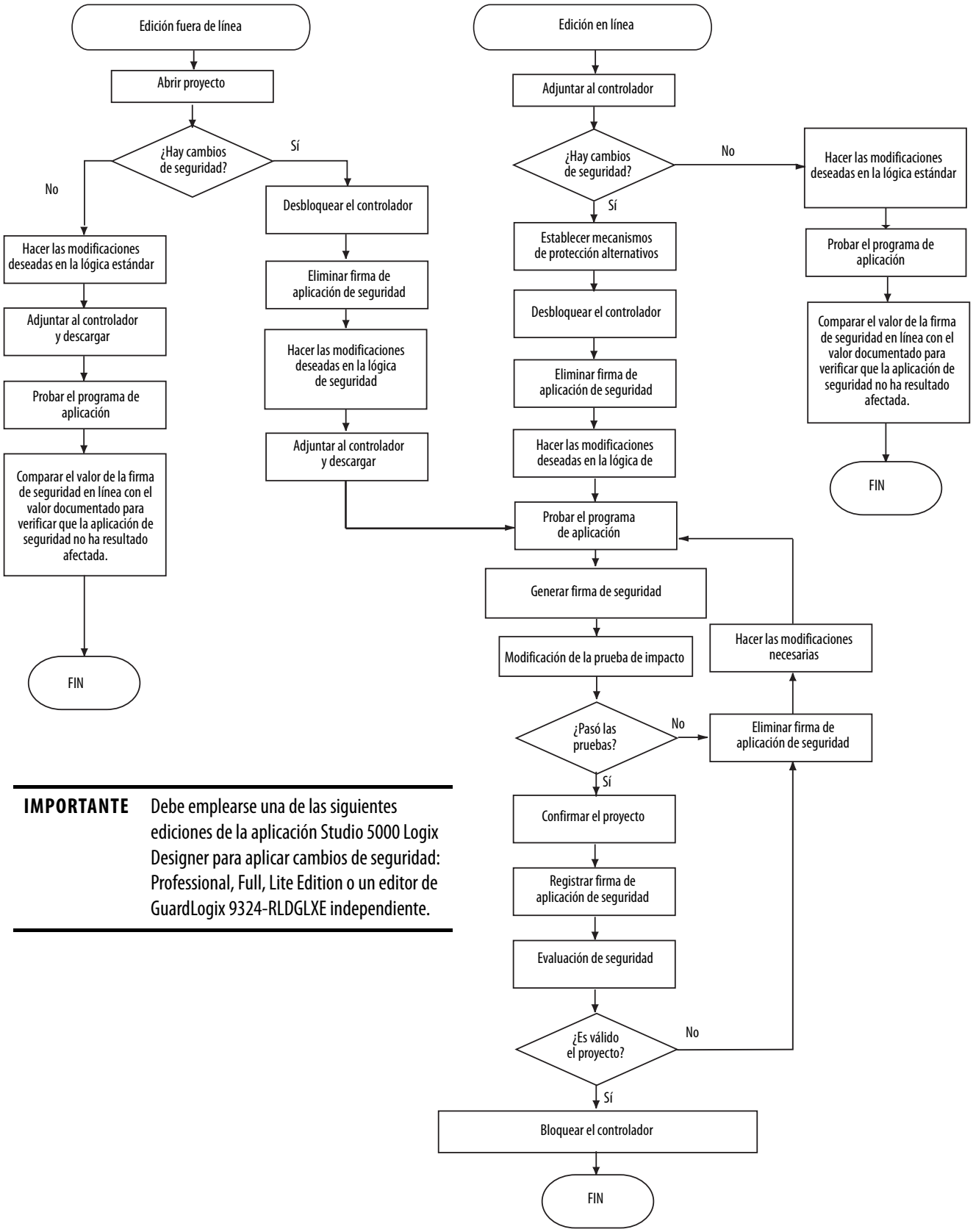
Cualquier modificación, mejora o adaptación de su software validado debe planificarse y analizarse para determinar el impacto en el sistema de seguridad funcional. Todas las fases apropiadas del ciclo de vida de seguridad del software deben realizarse según lo indicado por el análisis de impacto.

Como mínimo, debe realizar las siguientes acciones:

- Pruebas funcionales de todo el software afectado.
- Documentar todas las modificaciones de las especificaciones del software.
- Documentar todos los resultados de las pruebas.

Para obtener información detallada, consulte la norma IEC 61508-3, Sección 7.8, modificación del software.

**Figura 18 - Proceso de edición en línea y fuera de línea**




**IMPORTANTE** Debe emplearse una de las siguientes ediciones de la aplicación Studio 5000 Logix Designer para aplicar cambios de seguridad: Professional, Full, Lite Edition o un editor de GuardLogix 9324-RLDGLXE independiente.

## Notas:

# Monitoreo de estado y manejo de fallos



La arquitectura GuardLogix le proporciona muchas formas de detectar fallos del sistema y reaccionar ante ellos. La primera forma en que usted puede manejar los fallos consiste en verificar que ha rellenado las listas de verificación de su aplicación (consulte el Apéndice D en la página 91).

## Indicadores de estado

Para obtener información detallada acerca del funcionamiento de los indicadores de estado, consulte el manual del usuario del controlador:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543
- Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001

**IMPORTANTE** Los indicadores de estado no son indicadores confiables de las funciones de seguridad. Deben utilizarse solo para realizar diagnósticos generales durante la puesta en servicio o la resolución de problemas. No intente utilizar los indicadores de estado para determinar el estado de operación.

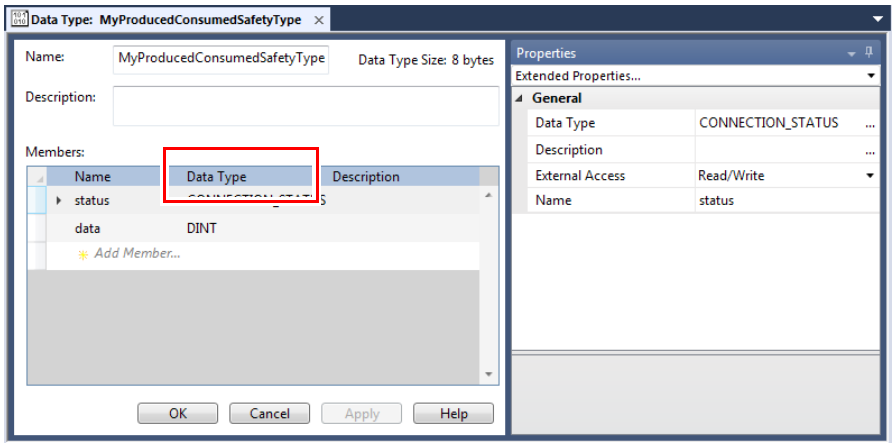
## Monitoreo del estado del sistema

Se puede ver el estado de las conexiones de tags de seguridad. También se puede determinar el estado operativo actual al interrogar varios objetos de dispositivos. Es su responsabilidad determinar qué datos son los más adecuados para iniciar una secuencia de desactivación.

### Datos de CONNECTION_STATUS

El primer miembro de la estructura de tags asociada con datos de entrada de seguridad y con datos de tags de seguridad producidos/consumidos contiene el estado de la conexión. Este miembro es un tipo de datos predefinido que se denomina CONNECTION_STATUS.

**Figura 19 - Cuadro de diálogo Data Type**




Los primeros dos bits del tipo de datos CONNECTION_STATUS contienen los bits de estado RunMode y ConnectionFaulted de un dispositivo. La tabla 3 describe las combinaciones de los estados RunMode y ConnectionFaulted.

**Tabla 3 - Estado de la conexión de seguridad**

| Estado RunMode | Estado ConnectionFaulted | Operación de conexión de seguridad |
|---|---|---|
| 1 = Marcha | 0 = Válido | El dispositivo productor está controlando activamente los datos. El dispositivo productor se encuentra en el modo de marcha. |
| 0 = Inactivo | 0 = Válido | La conexión está activa y el dispositivo productor está en estado de inactividad. Los datos de seguridad se restablecen al estado de seguridad. |
| 0 = Inactivo | 1 = Fallo | Fallo en la conexión de seguridad. Se desconoce el estado del dispositivo productor. Los datos de seguridad se restablecen al estado de seguridad. |
| 1 | 1 | Estado no válido. |

**ATENCIÓN:** Las conexiones de E/S de seguridad y las conexiones producidas/consumidas no se pueden configurar automáticamente para que produzcan un fallo en el controlador si se pierde una conexión y el sistema realiza la transición al estado seguro. Por tanto, si debe detectar un fallo en el dispositivo para asegurarse de que el sistema mantiene el nivel SIL requerido, debe monitorear los bits de CONNECTION_STATUS de E/S de seguridad e iniciar el fallo a través de la lógica del programa.

## Diagnósticos de entrada y salida

Los módulos de Guard I/O proporcionan capacidades de prueba de impulsos y de monitoreo. Si el módulo detecta un fallo, establece la entrada o la salida perturbadora en su estado de seguridad e informa del fallo al controlador. La indicación de fallo se realiza mediante el estado de entrada o salida, y se mantiene durante un período de tiempo configurable después de que se repara el fallo.

**IMPORTANTE** Usted es responsable de proporcionar la lógica de la aplicación para enclavar estos fallos de E/S y para verificar que el sistema se reinicie correctamente.

## Estado de conexión de dispositivo de E/S

El protocolo CIP Safety permite que los destinatarios de los datos de E/S determinen el estado de dichos datos:

- El controlador detecta los fallos de la conexión de entrada, que establecen todos los datos de entrada en el estado de seguridad y el estado de la entrada asociada en fallo.
- El dispositivo de salida detecta los fallos de la conexión de salida, que es responsable de desenergizar sus salidas.
- Por lo general, el controlador de seguridad también tiene conexiones de entrada procedentes de dispositivos de salida; el controlador de seguridad determina el estado de estas conexiones de entrada; no obstante, el estado de la conexión de entrada no es el mecanismo primario para desenergizar las salidas.

**IMPORTANTE** Usted es responsable de que la lógica de la aplicación enclave estos fallos de E/S y de verificar que el sistema se reinicie correctamente.

## Sistema de desenergizar para activar

Los controladores GuardLogix forman parte de un sistema de desenergizar para activar, lo cual significa que cero es el estado de seguridad. Algunos fallos del dispositivo de E/S de seguridad, aunque no todos, hacen que todas las entradas o salidas del dispositivo se establezcan en el estado de seguridad. Los fallos asociados a un canal de entrada específico hacen que dicho canal específico se establezca en el estado de seguridad; por ejemplo, un fallo de prueba de impulso específico del canal 0 hace que los datos de entrada del canal 0 se establezcan en el estado de seguridad. Si un fallo es general para el dispositivo y no corresponde a un canal específico, el bit de estado combinado muestra el estado del fallo y todos los datos del dispositivo se establecen en el estado de seguridad.

Para obtener información sobre cómo usar las instrucciones de aplicación de seguridad consulte el Apéndice F en la página 99 y el Manual de referencia – Conjunto de instrucciones de aplicación de seguridad GuardLogix Manual de referencia, publicación 1756-RM095.

## Instrucciones GSV (obtener valor del sistema) y SSV (establecer valor del sistema)

Las instrucciones GSV y SSV permiten obtener (GSV) y establecer (SSV) datos del sistema controlador que están almacenados en objetos de dispositivos. Cuando se introduce una instrucción GSV o SSV, el software de programación muestra las clases válidas de objetos, los nombres de objetos y los nombres de atributos de cada instrucción. Existen restricciones en cuanto al uso de las instrucciones GSV y SSV con componentes de seguridad.

| | |
|---|---|
| **IMPORTANTE** | La tarea de seguridad no puede realizar operaciones GSV o SSV en atributos estándar.<br>Los atributos de los objetos de seguridad que la tarea estándar puede escribir son únicamente para fines de diagnóstico. No afectan la ejecución de la tarea de seguridad. |

Para obtener más información sobre los atributos de seguridad a los que se puede obtener acceso mediante las instrucciones GSV y SSV, consulte el manual del usuario de su controlador:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543
- Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001

Si desea obtener información general acerca del uso de las instrucciones GSV y SSV consulte el Manual de referencia – Instrucciones generales de los controladores Logix5000 Manual de referencia , publicación 1756-RM003.

## Fallos de seguridad

Los fallos de los sistemas GuardLogix 5580 y Compact GuardLogix® 5380 pueden ser:

- Fallos de controlador recuperables
- Fallos de controlador no recuperables
- Fallos de seguridad no recuperables en la aplicación de seguridad
- Fallos de seguridad recuperables en la aplicación de seguridad

### Fallos de controlador no recuperables

Estos fallos se producen cuando los diagnósticos internos del controlador descubren un fallo. Si se produce un fallo del controlador no recuperable, se detiene la ejecución de las tareas estándar y de seguridad, así como las conexiones de salida. Los dispositivos de E/S de seguridad responden a la pérdida de datos de salida cambiando al estado de seguridad. Para la recuperación es necesario que se vuelva a descargar el programa de aplicación.

### Fallos de seguridad no recuperables en la aplicación de seguridad

Si se produce un fallo de seguridad no recuperable en la aplicación de seguridad, se interrumpen la lógica de seguridad y el protocolo de seguridad. Los fallos del temporizador de vigilancia de la tarea de seguridad y los fallos de la asociación de control se incluyen en esta categoría.

Cuando la tarea de seguridad encuentra un fallo de seguridad no recuperable, también se registra un fallo recuperable mayor estándar y el controlador procede a ejecutar el gestor de fallos del controlador, si existe. Si el gestor de fallos del controlador gestiona este fallo, las tareas estándar continuarán ejecutándose, aunque la tarea de seguridad continúe con un fallo.

**ATENCIÓN:** La anulación de un fallo de seguridad no elimina el fallo. Si anula un fallo de seguridad, es su responsabilidad asegurarse de que el funcionamiento del sistema siga siendo seguro.

Debe demostrar a la agencia certificadora que el sistema puede seguir funcionando de forma segura tras anular un fallo de seguridad.

Si existe una firma de la tarea de seguridad, puede borrar el fallo para que la tarea de seguridad se pueda ejecutar. Si no existe una firma de la tarea de seguridad, la tarea de seguridad no puede volver a ejecutarse mientras no se descargue de nuevo toda la aplicación.

## Fallos de seguridad recuperables en la aplicación de seguridad

Si se produce un fallo recuperable en el programa de seguridad, el sistema puede detener la ejecución de la tarea de seguridad, dependiendo de si el gestor de fallos del programa de seguridad (si existe) gestiona el fallo.

Si se borra un fallo recuperable mediante programación, la tarea de seguridad continúa sin interrupción.

Si no se borra un fallo recuperable en la aplicación de seguridad como parte de la programación, se produce un fallo de seguridad recuperable de Tipo 14, Código 2. La ejecución de la tarea de seguridad se detiene y las conexiones del protocolo de seguridad se cierran y se vuelven a abrir para reinicializarlas. Las salidas de seguridad se ponen en estado de seguridad, y el productor de tags consumidos de seguridad ordena a los consumidores ponerlos también en estado de seguridad.

Si no se gestiona el fallo de seguridad recuperable, también se registra un fallo recuperable mayor estándar y el controlador procede a ejecutar el gestor de fallos del controlador, si existe. Si el gestor de fallos del controlador gestiona este fallo, las tareas estándar continuarán ejecutándose, aunque la tarea de seguridad continúe con un fallo.

La aparición de fallos recuperables es indicativa de que el código de la aplicación no se está protegiendo frente a condiciones o valores de los datos no válidos. Considere la posibilidad de modificar la aplicación para eliminar estos fallos, en lugar de gestionarlos durante la ejecución.

**ATENCIÓN:** La anulación de un fallo de seguridad no elimina el fallo. Si anula un fallo de seguridad, es su responsabilidad asegurarse de que el funcionamiento del sistema siga siendo seguro.

Debe demostrar a la agencia certificadora que el sistema puede seguir funcionando de forma segura tras anular un fallo de seguridad.

## Visualización de fallos

El cuadro de diálogo Recent Faults de la ficha Major Faults del cuadro de diálogo Controller Properties contiene dos subfichas: una para fallos estándar y otra para fallos de seguridad.

La pantalla de estado del controlador también muestra los códigos de fallo con un breve mensaje de estado. Para obtener más información sobre los indicadores de estado, consulte:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543
- Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001

## Códigos de fallo

La tabla 4 muestra los códigos de fallo específicos de los controladores GuardLogix 5580 y Compact GuardLogix® 5380. El tipo y el código corresponden al tipo y al código que aparecen en la ficha Major Faults del cuadro de diálogo Controller Properties, así como en el objeto PROGRAM, atributo MAJORFAULTRECORD (o MINORFAULTRECORD).

**Tabla 4 - Fallos mayores de seguridad (tipo 14)**

| Código | Causa | Estado | Acción correctiva |
|---|---|---|---|
| 01 | Expiró el temporizador de vigilancia de tareas. La tarea del usuario no se ha completado en el período especificado. Un error del programa ha causado un bucle infinito, el programa es demasiado complejo para ejecutarse a la velocidad especificada o hay tareas de mayor prioridad o ejecutadas en segundo plano que impiden que esta tarea finalice. | No recuperable | Borre el fallo.<br>Si existe una firma de la tarea de seguridad, la memoria de seguridad se reinicializa mediante la firma de seguridad y la tarea de seguridad empieza a ejecutarse.<br>Si no existe una firma de la tarea de seguridad, se debe volver a descargar el programa para que la tarea de seguridad pueda ejecutarse.<br>Si la aplicación lo permite, aumente el tiempo del temporizador de vigilancia. |
| 02 | Hay un error en una rutina de la tarea de seguridad. | Recuperable | Corrija el error en la lógica del programa de usuario. |
| 07 | No se puede ejecutar la tarea de seguridad.<br>Este fallo se produce cuando la lógica de seguridad no es válida o no está disponible. | No recuperable | Borre el fallo.<br>Si existe una firma de la tarea de seguridad, la memoria de seguridad se reinicializa mediante la firma de la tarea de seguridad y la tarea de seguridad empieza a ejecutarse.<br>Si no existe una firma de la tarea de seguridad, se debe descargar de nuevo el programa para que la tarea de seguridad pueda ejecutarse. |

El documento Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publicación 1756-PM014, contiene descripciones de los códigos de fallo comunes a todos los controladores Logix.

# Fallo de homólogo de seguridad

El homólogo de seguridad tiene un indicador de estado OK.

Si la configuración SIL se ha establecido en SIL 2 y se ha instalado un homólogo de seguridad en la ranura situada junto al primario de seguridad, se producen estas acciones:

- En el homólogo de seguridad, el indicador de estado OK parpadea en rojo.
- El controlador registra un fallo menor de Tipo 14, Código 12, que indica que el controlador se ha configurado para SIL 2 y hay un homólogo de seguridad presente.
- La aplicación Studio 5000 Logix Designer rechaza la descarga de una aplicación SIL 2.

# Instrucciones de seguridad

**ATENCIÓN:** Estas instrucciones de seguridad son las únicas instrucciones que se pueden emplear en las tareas de seguridad de aplicaciones SIL 2 o SIL 3.

Para ver la información más reciente sobre las instrucciones certificadas, consulte nuestros certificados de seguridad y la lista de lanzamientos de revisiones en http://www.rockwellautomation.com/global/certification/safety.page.

## Instrucciones de seguridad

Las siguientes tablas indican las instrucciones de aplicaciones de seguridad que cuentan con certificación para uso en aplicaciones SIL 2 o SIL 3.

**Tabla 5 - Instrucciones generales de aplicaciones de seguridad**

| Mnemónico | Nombre | Finalidad |
|---|---|---|
| CROUT | Salida redundante configurable | Controla y monitorea salidas redundantes. |
| DCA | Entrada de doble canal – Analógica (versión de números enteros) | Monitorea la tolerancia de rango y desviación de dos valores analógicos. |
| DCAF | Entrada de doble canal – Analógica (versión de punto flotante [coma flotante]) | |
| DCS | Entrada de doble canal – Paro | Monitorea dispositivos de seguridad de entrada doble cuyo propósito principal es proporcionar una función de paro como, por ejemplo, un paro de emergencia, cortina de luz o interruptor de puerta. |
| DCST | Entrada de doble canal – Paro con prueba | Monitorea dispositivos de seguridad de entrada doble cuyo propósito principal es proporcionar una función de paro como, por ejemplo, un paro de emergencia, cortina de luz o interruptor de puerta. Incluye la capacidad adicional de iniciar una prueba funcional del dispositivo de paro. |
| DCSTL | Entrada de doble canal – Paro con prueba y bloqueo | Monitorea dispositivos de seguridad de entrada doble cuyo propósito principal es proporcionar una función de paro como, por ejemplo, un paro de emergencia, cortina de luz o interruptor de puerta. Incluye la capacidad adicional de iniciar una prueba funcional del dispositivo de paro. Puede monitorear una señal de retroalimentación proveniente de un dispositivo de seguridad y emitir una petición de bloqueo a un dispositivo de seguridad. |
| DCSTM | Entrada de doble canal – Paro con prueba y silenciamiento | Monitorea dispositivos de seguridad de entrada doble cuyo propósito principal es proporcionar una función de paro como, por ejemplo, un paro de emergencia, cortina de luz o interruptor de puerta. Incluye la capacidad adicional de iniciar una prueba funcional del dispositivo de paro, y además la capacidad de silenciar el dispositivo de seguridad. |
| DCM | Entrada de doble canal – Monitoreo | Monitorea dispositivos de seguridad de entrada doble. |
| DCSRT | Entrada de doble canal – Arranque | Energiza dispositivos de seguridad de entrada doble cuya función principal es arrancar una máquina de manera segura como, por ejemplo, una consola colgante habilitante. |
| SMAT | Tapete de seguridad | Indica si el tapete de seguridad está ocupado. |
| THRSe | Estación de mando a dos manos – Con características mejoradas | Monitorea dos entradas de seguridad diversas: una desde un botón pulsador para la mano derecha y otra desde un botón pulsador para la mano izquierda, a fin de controlar una salida. Permite configurar el tiempo de discrepancia canal por canal, y capacidad mejorada para evitar una estación de mando a dos manos. |
| TSAM | Muting asimétrico de dos sensores | Inhabilita automáticamente la función de protección de una cortina de luz temporalmente, mediante dos sensores de muting dispuestos de forma asimétrica. |
| TSSM | Muting simétrico de dos sensores | Inhabilita automáticamente la función de protección de una cortina de luz temporalmente, mediante dos sensores de muting dispuestos de forma simétrica. |
| FSBM | Silenciamiento bidireccional de cuatro sensores | Inhabilita automáticamente la función de protección de una cortina de luz temporalmente mediante cuatro sensores dispuestos secuencialmente antes y después del campo de detección de la cortina de luz. |

**Tabla 6 - Instrucciones de aplicaciones de seguridad en formado de metales**

| Mnemónico | Nombre | Finalidad |
|---|---|---|
| CBCM | Embrague/freno – Modo continuo | Se usa en aplicaciones de prensa cuando se selecciona la operación continua. |
| CBIM | Embrague/freno – Modo de avance a pasos | Se usa en aplicaciones de prensas que requieren ajustes menores del carro como, por ejemplo, durante la configuración de la prensa. |
| CBSSM | Embrague/freno – Modo de un solo ciclo | Se usa en aplicaciones de prensa de un solo ciclo. |
| CPM | Monitor de posición de cigüeñal | Se usa para determinar la posición del carro de la prensa. |
| CSM | Monitor de árbol de levas | Monitorea el movimiento en operaciones de arranque, paro y marcha de un árbol de levas. |
| EPMS | Selector de modo de ocho posiciones | Monitorea ocho entradas de seguridad para controlar una de las ocho salidas que corresponden a la entrada activa. |
| AVC | Control de válvula auxiliar | Controla una válvula auxiliar que se usa con una válvula principal. |
| MVC | Control de válvula principal | Controla y monitorea una válvula principal. |
| MMVC | Control manual de válvula en mantenimiento | Se usa para accionar manualmente una válvula durante las operaciones de mantenimiento. |

Para obtener más información sobre las instrucciones de RSLogix 5000®, consulte el Apéndice F en la página 99.

**Tabla 7 - Descripciones de las instrucciones de aplicaciones de seguridad de RSLogix 5000**

| Mnemónico | Nombre | Finalidad |
|---|---|---|
| ENPEN | Habilitar colgante | Monitorea dos entradas de seguridad para controlar una salida y tiene un valor de tiempo de espera tras incoherencia en las entradas de 3 s. |
| ESTOP | Paro de emergencia | Monitorea dos entradas de seguridad para controlar una salida y tiene un valor de tiempo de espera tras incoherencia en las entradas de 500 ms. |
| RIN | Entrada redundante | Monitorea dos entradas de seguridad para controlar una salida y tiene un valor de tiempo de espera tras incoherencia en las entradas de 500 ms. |
| ROUT | Salida redundante | Monitorea el estado de una entrada para controlar y monitorear dos salidas. |
| DIN | Entrada diversa | Monitorea dos entradas de seguridad diversas para controlar una salida y tiene un valor de tiempo de espera tras incoherencia en las entradas de 500 ms. |
| FPMS | Selector de modo de 5 posiciones | Monitorea cinco entradas de seguridad para controlar una de las cinco salidas que corresponden a la entrada activa. |
| THRS | Estación de mando a dos manos | Monitorea dos entradas de seguridad diversas: una desde un botón pulsador para la mano derecha y otra desde un botón pulsador para la mano izquierda, a fin de controlar una salida. |
| LC | Cortina de luz | Monitorea dos entradas de seguridad procedentes de una cortina de luz para controlar una salida. |

Las rutinas de la tarea de seguridad pueden usar estas instrucciones de seguridad de diagrama de lógica de escalera.

**Tabla 8 - Instrucciones de seguridad de diagrama de lógica de escalera**

| Tipo | Mnemónico | Nombre | Finalidad |
|---|---|---|---|
| Matriz (archivo) | COP(1) | Copia | Copia los datos binarios de un tag a otro (sin conversión de tipo). |
| | FAL(2) | Aritmética y lógica de archivo | Realiza operaciones de copia, aritméticas, lógicas y de función en los datos almacenados en una matriz. |
| | FLL | Llenado de archivo | Llena los elementos de una matriz con el valor de origen, sin cambiar el valor de origen. |
| | FSC | Búsqueda y comparación de archivo | Compara los valores de una matriz, elemento por elemento. |
| | SIZE | Dimensionar elementos | Busca la magnitud de una dimensión de una matriz. |
| Bit | XIC | Examinar si está cerrado | Examina el bit de datos para establecer o borrar la condición del renglón. |
| | XIO | Examinar si está abierto | Examina el bit de datos para establecer o borrar la condición del renglón. |
| | OTE | Energizar salida | Controla un bit (realizar las operaciones de establecer y borrar en función del estado del renglón). |
| | OTL | Enclavamiento de salida | Establece un bit (retentivo). |
| | OTU | Desenclavamiento de salida | Borra un bit (retentivo). |
| | ONS | Un impulso | Permite que un evento se produzca una vez. |
| | OSR | Un impulso en flanco ascendente | Establece un bit de salida para un escán con el flanco (ascendente) de falso a verdadero del estado del renglón. |
| | OSF | Un impulso en flanco descendente | Establece un bit de salida para un escán con el flanco (descendente) de verdadero a falso del estado del renglón. |

**Tabla 8 - Instrucciones de seguridad de diagrama de lógica de escalera (continuación)**

| Tipo | Mnemónico | Nombre | Finalidad |
|---|---|---|---|
| Temporizador | TON | Temporizador de retardo a la conexión | Contabilizar el tiempo que un temporizador está habilitado. |
| | TOF | Temporizador de retardo a la desconexión | Contabilizar el tiempo que un temporizador está inhabilitado. |
| | RTO | Temporizador retentivo activado | Acumular tiempo. |
| | CTU | Conteo progresivo | Conteo progresivo. |
| | CTD | Conteo regresivo | Conteo regresivo. |
| | RES | Restablecimiento | Restablecer un temporizador o un contador. |
| Comparación | CMP(2) | Comparación | Realizar una comparación en las operaciones aritméticas que se especifican en la expresión. |
| | EQU | Igual a | Probar si dos valores son iguales. |
| | GEQ | Mayor o igual que | Probar si un valor es mayor o igual a un segundo valor. |
| | GRT | Mayor que | Probar si un valor es mayor a un segundo valor. |
| | LEQ | Menor o igual que | Probar si un valor es menor o igual a un segundo valor. |
| | LES | Menor que | Probar si un valor es menor a un segundo valor. |
| | MEQ | Comparación enmascarada de igualdad | Pasar la fuente, comparar los valores a través de una máscara y determinar si son iguales. |
| | NEQ | Desigual a | Probar si un valor no es igual a un segundo valor. |
| | LIM | Prueba de límite | Probar si un valor está dentro de un rango determinado. |
| Movimiento | CLR | Borrar | Borrar un valor. |
| | MOV | Movimiento | Copiar un valor. |
| | MVM | Mover con máscara | Copiar una parte específica de un entero. |
| | SWPB | Intercambio de byte | Reacomodar los bytes de un valor. |
| Lógico | AND | Función Y a nivel de bits | Realizar la función Y a nivel de bits. |
| | NOT | Función NO a nivel de bits | Realizar la función NO a nivel de bits. |
| | OR | Función O a nivel de bits | Realizar la función O a nivel de bits. |
| | XOR | Función O exclusivo a nivel de bits | Realizar la función O exclusivo a nivel de bits. |
| Control de programa | JMP | Salto a etiqueta | El escán de la lógica salta a una ubicación etiquetada dentro de la misma rutina. |
| | LBL | Etiqueta | Identifica una ubicación de destino para una instrucción JMP. |
| | JSR | Salto a subrutina | Saltar a otra rutina. |
| | RET | Retorno | Retornar los resultados de una subrutina. |
| | SBR | Subrutina | Aceptar los datos que se pasan a una subrutina mediante la instrucción JSR. |
| | TND | Fin temporal | Marcar un fin temporal que detiene la ejecución de la rutina. |
| | Relé de control maestro | Restablecimiento de control maestro | Fuerza a que todos los renglones de una sección de la lógica se ejecuten en estado falso. |
| | AFI | Instrucción siempre falso | Fuerza un renglón a falso (el renglón sigue ejecutándose). |
| | NOP | Ninguna operación | Insertar un indicador de posición en la lógica. |
| | EVENT(3) | Activación de tarea de evento | Activa la ejecución de una tarea de evento. |
| Matemáticas/ cálculo | ADD | Suma | Sumar dos valores. |
| | CPT (2) | Cálculo | Realizar la operación aritmética definida en la expresión. |
| | SUB | Resta | Restar dos valores. |
| | MUL | Multiplicación | Multiplicar dos valores. |
| | DIV | División | Dividir dos valores. |
| | MOD | Modulus | Determinar el residuo después de que un valor se divide entre un segundo valor. |
| | SQR | Raíz cuadrada | Calcular la raíz cuadrada de un valor. |
| | NEG | Negar | Tomar el signo opuesto de un valor. |
| | ABS | Valor absoluto | Tomar el valor absoluto de un valor. |
| E/S | GSV(4) | Obtener valor del sistema | Obtener información de estado del controlador. |
| | SSV(4) | Establecer valor del sistema | Establecer información de estado del controlador. |

(1) Al utilizar la instrucción COP en una rutina de seguridad, debe verificar que el operando de longitud sea una constante y que la longitud del origen y del destino sean iguales.
(2) No se admiten operandos avanzados, tales como SIN, COS y TAN, en las rutinas de seguridad.
(3) La instrucción del evento acciona un escán de la tarea estándar.
(4) Para ver las consideraciones especiales para utilizar las instrucciones GSV y SSV, consulte el documento ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543, o el documento Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001.

**Tabla 9 - Instrucciones de seguridad del variador (1)**

| Mnemónico | Nombre | Finalidad |
|---|---|---|
| SS1 | Paro seguro 1 | La instrucción de paro seguro 1 monitorea la desaceleración de un eje de acuerdo con la rampa de velocidad especificada a velocidad cero y controla su salida (O1) para iniciar la desconexión de par segura (STO). |
| SS2 | Paro seguro 2 | La instrucción de paro seguro 2 inicia y monitorea la desaceleración del motor dentro de los límites establecidos para verificar que el motor se lleva a un paro operacional. Una vez parado, SS2 continúa monitoreando el paro operacional del motor. |
| SOS | Paro seguro de la operación | La instrucción de paro seguro de la operación monitorea la velocidad o la posición de un motor o eje para verificar que la desviación respecto a la velocidad o posición de reposo no supera una cantidad definida. |
| SLS | Velocidad límite segura | La instrucción de velocidad límite segura monitorea la velocidad de un eje y establece la salida de límite de SLS si la velocidad supera el valor de entrada de límite activo de la instrucción. |
| SLP | Posición limitada segura | La instrucción de posición limitada segura monitorea la posición de un motor o eje para verificar que la posición no se desvíe por encima o por debajo de los límites establecidos. |
| SDI | Dirección segura | La instrucción de dirección segura monitorea la posición de un motor o eje para detectar un movimiento superior a una cantidad definida en una dirección no deseada. |
| SBC | Control de freno seguro | La instrucción de control de freno seguro (SBC):<br>• Controla las salidas de seguridad que accionan un freno.<br>• Establece la temporización entre el freno y las salidas de solicitud de desconexión de par.<br>• Monitorea la retroalimentación del freno y el estado de E/S. |
| SFX | Escalado de retroalimentación seguro | La instrucción de interface de retroalimentación de seguridad convierte la retroalimentación de velocidad y posición del motor procedente de un módulo variador a las unidades de escalado del usuario. También define una posición de referencia absoluta. |

(1) Las instrucciones de seguridad de movimiento están disponibles cuando se utiliza un controlador GuardLogix 5580, un Compact GuardLogix 5380 y variadores Kinetix 5700 ERS4 con la aplicación Studio 5000 Logix Designer (versiones 31 y posteriores).

**IMPORTANTE** Si utiliza los comandos directos de movimiento con un variador Kinetix 5500, un servovariador Kinetix 5700 o un variador PowerFlex 527, consulte el manual del usuario del variador para obtener información sobre cómo utilizar esta función en las aplicaciones de seguridad.

- Servovariadores Kinetix 5500 Manual del usuario, publicación 2198-UM001
- Servovariadores Kinetix 5700 Manual de usuario, publicación 2198-UM002
- Variador de CA de frecuencia ajustable PowerFlex 527 Manual del usuario, publicación 520-UM002

Consulte las siguientes publicaciones para obtener más información.

**Tabla 10 - Recursos adicionales**

| Recurso | Descripción |
|---|---|
| Conjunto de instrucciones de aplicación de seguridad GuardLogix Manual de referencia, publicación 1756-RM095 | Proporciona más información acerca de las instrucciones de aplicaciones de seguridad. |
| Instrucciones generales de los controladores Logix5000 Manual de referencia, publicación 1756-RM003 | Proporciona información sobre el conjunto de instrucciones Logix5000 que incluye instrucciones generales, de movimiento y de procesos. |

# Creación y uso de una instrucción Add-On de seguridad

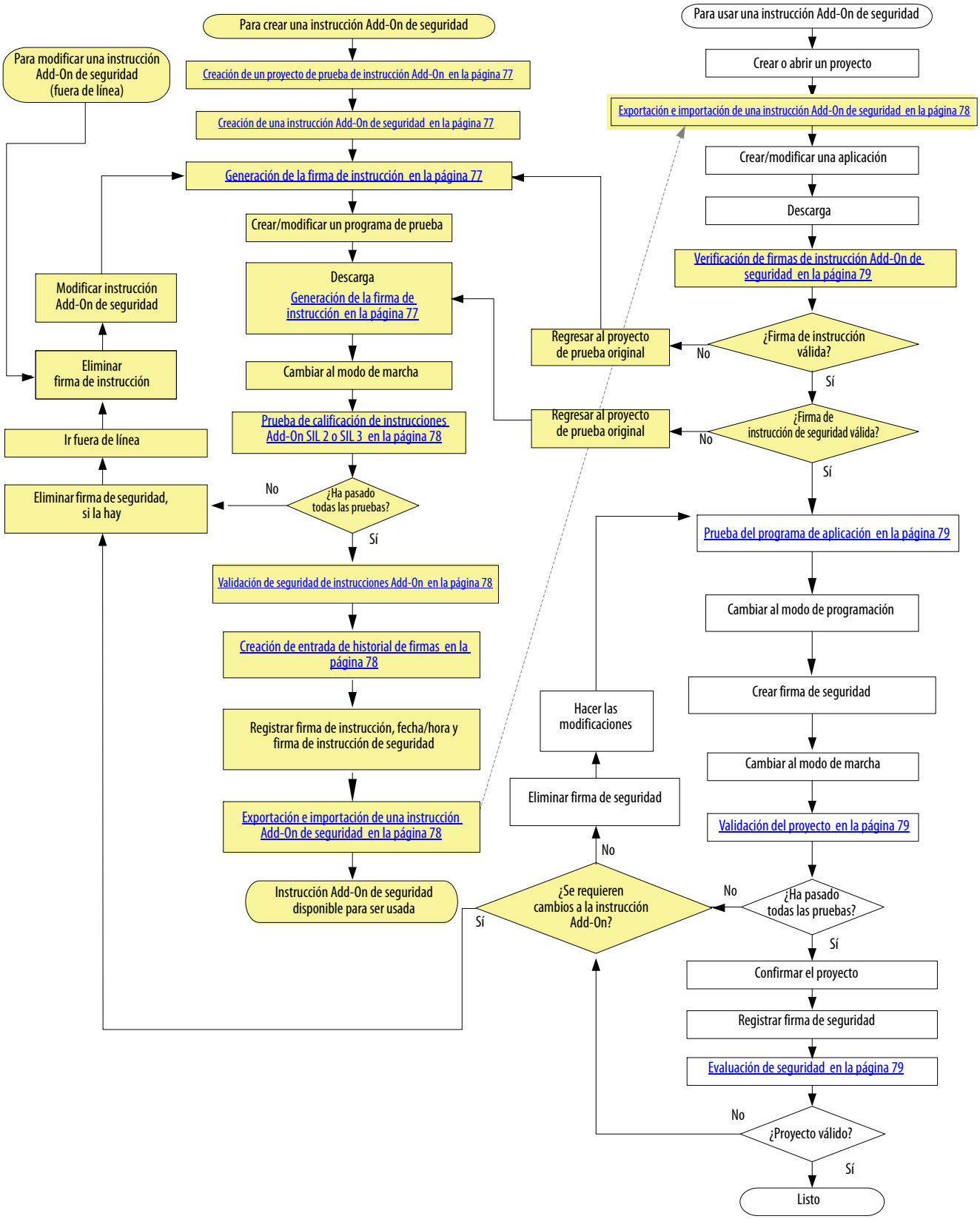


Con la aplicación Studio 5000 Logix Designer, se pueden crear instrucciones AddOn de seguridad. Las instrucciones Add-On de seguridad permiten encapsular en una sola instrucción la lógica de seguridad usada comúnmente, lo que la hace modular y más fácil de reutilizar.

Las instrucciones Add-On de seguridad usan la firma de instrucción de las instrucciones Add-On de alta integridad además de una firma de instrucción de seguridad para uso en funciones relacionadas con la seguridad hasta el nivel SIL 3.

La figura 20 en la página 76 muestra los pasos requeridos para crear una instrucción Add-On de seguridad y posteriormente usarla en un programa de aplicación de seguridad. Los ítems sombreados son pasos exclusivos de instrucciones Add-On. Consulte los vínculos para ver una explicación de dichos temas.

**Figura 20 - Diagrama de flujo para crear y usar instrucciones Add-On de seguridad**



## Creación de un proyecto de prueba de instrucción Add-On

Usted debe crear un proyecto de prueba único, específicamente para crear y probar la instrucción Add-On de seguridad. Este proyecto debe ser un proyecto independiente y dedicado para minimizar las influencias inesperadas.

Siga las pautas para proyectos descritas en la sección Creación del proyecto en la página 54.

## Creación de una instrucción Add-On de seguridad

Para obtener información sobre cómo crear instrucciones Add-On, consulte el documento Logix5000 Controllers Add-On Instruction Programming Manual, publicación 1756-PM010.

## Generación de la firma de instrucción

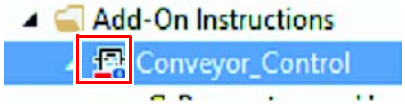
La firma de instrucción le permite determinar rápidamente si la instrucción ha sido modificada. Cada instrucción Add-On puede tener su propia firma. La firma de una instrucción se requiere cuando se usa una instrucción Add-On en funciones relacionadas con la seguridad y a veces puede que se requiera en industrias reguladas. Úsela cuando su aplicación requiera un nivel más alto de integridad.

La firma de instrucción está formada por un número de identificación y un sello de hora que identifican el contenido de la instrucción Add-On en un momento dado.

Una vez que ha sido generada, la firma de instrucción sella la instrucción Add-On, lo que ayuda a evitar que la instrucción se edite mientras la firma esté implementada. Esta restricción incluye comentarios de renglón, descripciones de tags y toda documentación de instrucción que haya sido creada. Cuando la instrucción está sellada solo se pueden realizar las siguientes acciones:

- Copiar la firma de instrucción
- Crear o copiar una entrada de historial de firmas
- Crear instancias de la instrucción Add-On
- Descargar la instrucción
- Retirar la firma de instrucción
- Imprimir informes

Cuando se ha generado una firma de instrucción, la aplicación Studio 5000 Logix Designer muestra la definición de la instrucción con el icono de sello.




**IMPORTANTE** Si protege una instrucción Add-On con la función de protección de origen de la aplicación Studio 5000 Logix Designer, habilite la protección de origen antes de generar la firma de la instrucción.

## Firma de instrucción de seguridad

Cuando se descarga por primera vez una instrucción Add-On de seguridad, se genera automáticamente una firma de instrucción de seguridad. La firma de instrucción de seguridad es un número de identificación que identifica las características de ejecución de la instrucción Add-On de seguridad.

## Prueba de calificación de instrucciones Add-On SIL 2 o SIL 3

Las pruebas de las instrucciones Add-On de seguridad deben ejecutarse en una aplicación independiente y dedicada para asegurarse de que se reducen al mínimo las influencias inesperadas. Usted debe seguir un plan de prueba bien diseñado y realizar una prueba de unidad de la instrucción Add-On de seguridad que cubra todas las rutas de ejecución posibles a través de la lógica, incluidos los rangos válidos y no válidos de todos los parámetros de entrada.

## Validación de seguridad de instrucciones Add-On

Puede que sea necesario que un tercero realice una revisión independiente de la instrucción Add-On de seguridad antes de que dicha instrucción quede aprobada para su uso. Es posible que se requiera una validación independiente a cargo de un tercero para obtener una certificación de seguridad funcional.

## Creación de entrada de historial de firmas

El historial de firmas proporciona un registro para referencia futura. Una entrada de historial de firmas consta de la firma de la instrucción, del nombre del usuario, del valor del sello de hora y de una descripción definida por el usuario. Es posible almacenar hasta seis entradas de historial. Es necesario estar fuera de línea para crear una entrada de historial de firmas.

**SUGERENCIA** El informe de listado de firmas de la aplicación Studio 5000 Logix Designer imprime la firma de instrucción, el sello de hora y la firma de instrucción de seguridad. Para imprimir el informe, haga clic con el botón derecho del mouse en la instrucción Add-On en Controller Organizer y elija Print > Signature Listing.

## Exportación e importación de una instrucción Add-On de seguridad

Cuando vaya a exportar una instrucción Add-On de seguridad, seleccione la opción para incluir todas las instrucciones Add-On referenciadas y todos los tipos definidos por el usuario en el mismo archivo de exportación. Incluir las instrucciones Add-On referenciadas facilita la conservación de las firmas.

Al importar las instrucciones Add-On considere las pautas siguientes:

- No es posible importar una instrucción Add-On de seguridad a un proyecto de controlador estándar.
- No es posible importar una instrucción Add-On de seguridad a un proyecto de controlador de seguridad que tenga un bloqueo de seguridad o una firma de seguridad.
- No es posible importar una instrucción Add-On de seguridad mientras se está en línea.
- Si se importa una instrucción Add-On con una firma de instrucción en un proyecto donde las instrucciones Add-On referenciadas o los tipos de datos definidos por el usuario no están disponibles, quizás sea necesario eliminar la firma.

Para obtener más información, consulte el documento Logix 5000 Controllers Import/Export Programming Manual, publicación 1756-PM019.

## Verificación de firmas de instrucción Add-On de seguridad

Después de descargar el proyecto de aplicación que contiene la instrucción Add-On de seguridad importada, es necesario comparar el valor de la firma de instrucción, la fecha y el sello de hora, y los valores de firmas de instrucción de seguridad con los valores originales registrados antes de exportar la instrucción Add-On de seguridad. Si coinciden, la instrucción Add-On de seguridad es válida y usted puede continuar con la validación de su aplicación.

## Prueba del programa de aplicación

Este paso consta de cualquier combinación de modo de marcha y de programación, ediciones de programa en línea o fuera de línea, carga y descarga, y pruebas informales necesarias para que la aplicación funcione debidamente.

## Validación del proyecto

Realice una prueba de ingeniería de la aplicación, incluido el sistema de seguridad.

Consulte Validación del proyecto en la página 55 para obtener más información sobre los requisitos.

## Evaluación de seguridad

Puede que sea necesario que un tercero independiente revise el sistema de seguridad antes de que este quede aprobado para funcionar. Es posible que se requiera una validación independiente a cargo de un tercero para obtener una certificación de seguridad funcional.

Para obtener más información sobre las evaluaciones de seguridad, consulte el documento Machinery SafeBook 5.

## Notas:

# Tiempos de reacción



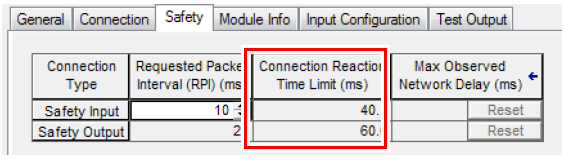
## Límite de tiempo de reacción de la conexión

El límite de tiempo de reacción de la conexión corresponde a la longevidad máxima de los paquetes de seguridad en la conexión asociada. Si la longevidad de los datos que utiliza el dispositivo consumidor supera el límite de tiempo de reacción de la conexión, se produce un fallo de conexión. Las siguientes ecuaciones determinan el límite de tiempo de reacción de la conexión:

> Límite de tiempo de reacción de la conexión de entrada =
> RPI de entrada x [multiplicador de interrupciones + multiplicador de retardo de red]
>
> Límite de tiempo de reacción de la conexión de salida =
> período de la tarea de seguridad x [multiplicador de interrupciones + multiplicador de retardo de red 1]

El límite de tiempo de reacción de la conexión se muestra en la ficha Safety del cuadro de diálogo Module Properties.

**Figura 21 - Límite de tiempo de reacción de la conexión**



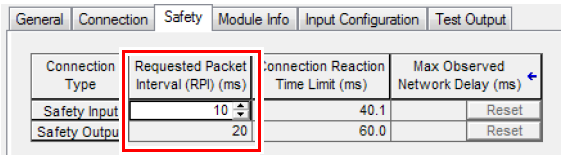
## Especificación del intervalo solicitado entre paquetes (RPI)

El RPI especifica el período en que se actualizan los datos a través de una conexión. Por ejemplo, un módulo de entrada produce datos al RPI que usted asigne.

En el caso de las conexiones de entrada de seguridad, puede definir el RPI en la ficha Safety del cuadro de diálogo Module Properties. El RPI se introduce en incrementos de 1 ms.

El límite de tiempo de reacción de la conexión se ajusta inmediatamente al cambiar el RPI con la aplicación Studio 5000 Logix Designer.

**Figura 22 - Intervalo solicitado entre paquetes**




En el caso de las conexiones de salida de seguridad, el RPI se fija en el período de la tarea de seguridad. Si el límite de tiempo de reacción de la conexión correspondiente no es satisfactorio, puede ajustar el período de la tarea de seguridad en el cuadro de diálogo Safety Task Properties.

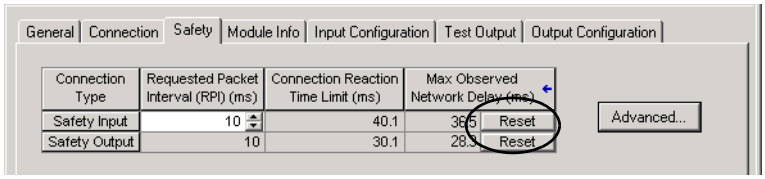
Consulte Tiempo de reacción del sistema en la página 15 para ver los detalles del período de la tarea de seguridad.

Para las aplicaciones habituales, los valores predeterminados del límite de tiempo de reacción de la conexión para conexiones de entrada de 4 x RPI y del límite de tiempo de reacción de la conexión para conexiones de salida de 3 x RPI normalmente es suficiente. Para requisitos más complejos, utilice el botón Advanced para modificar los parámetros del límite de tiempo de reacción de la conexión tal y como se describe en la página 86.

## Visualización del retardo de red máximo observado

El retardo de red máximo observado se visualiza en la ficha Safety del cuadro de diálogo Module Properties. Si está trabajando en línea, haga clic en Reset para restablecer el retardo de red máximo observado.

**Figura 23 - Restablecimiento del retardo de red máximo observado**

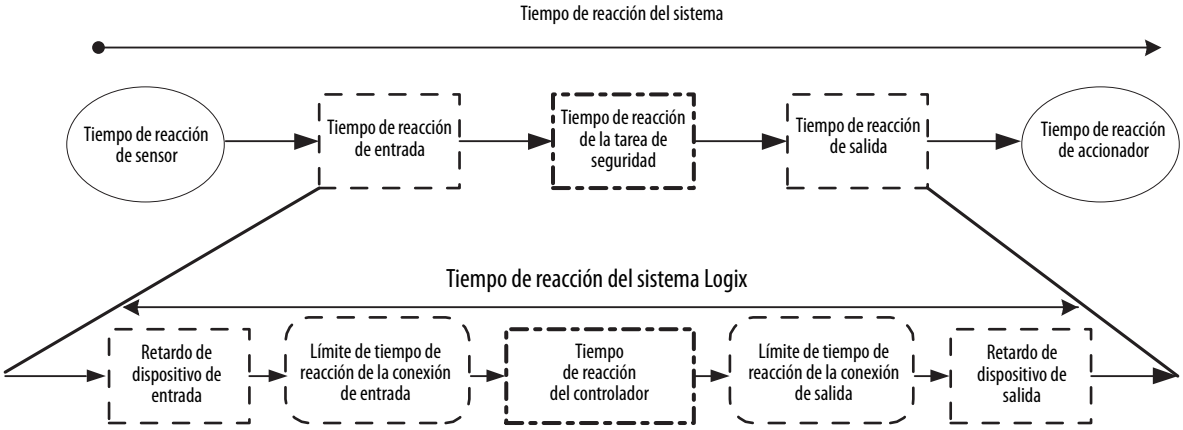


## Tiempo de reacción del sistema

Para determinar el tiempo de reacción del sistema (consulte Tiempo de reacción del sistema en la página 15 para ver los detalles) de cualquier cadena de control, es necesario sumar los tiempos de reacción de todos los componentes de la cadena de seguridad.

> Tiempo de reacción del sistema = Tiempo de reacción de sensores + Tiempo de reacción del sistema Logix + Tiempo de reacción de accionadores

**Figura 24 - Tiempo de reacción del sistema**



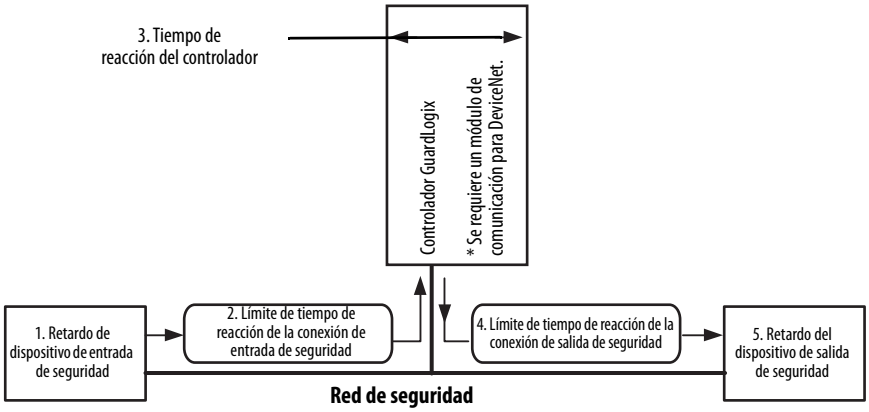

## Tiempo de reacción del sistema Logix

Las siguientes secciones proporcionan información acerca de cómo calcular el tiempo de reacción del sistema Logix de una cadena sencilla de entrada-lógica-salida y de una aplicación más compleja utilizando tags de seguridad producidos/consumidos en la cadena lógica.

### Cadena sencilla de entrada-lógica-salida

En esta sección se describe el tiempo de reacción del sistema Logix para cualquier cadena sencilla de entrada a lógica a salida.

**Figura 25 - Tiempo de reacción en el peor de los casos del sistema Logix de una entrada sencilla a lógica y a salida**



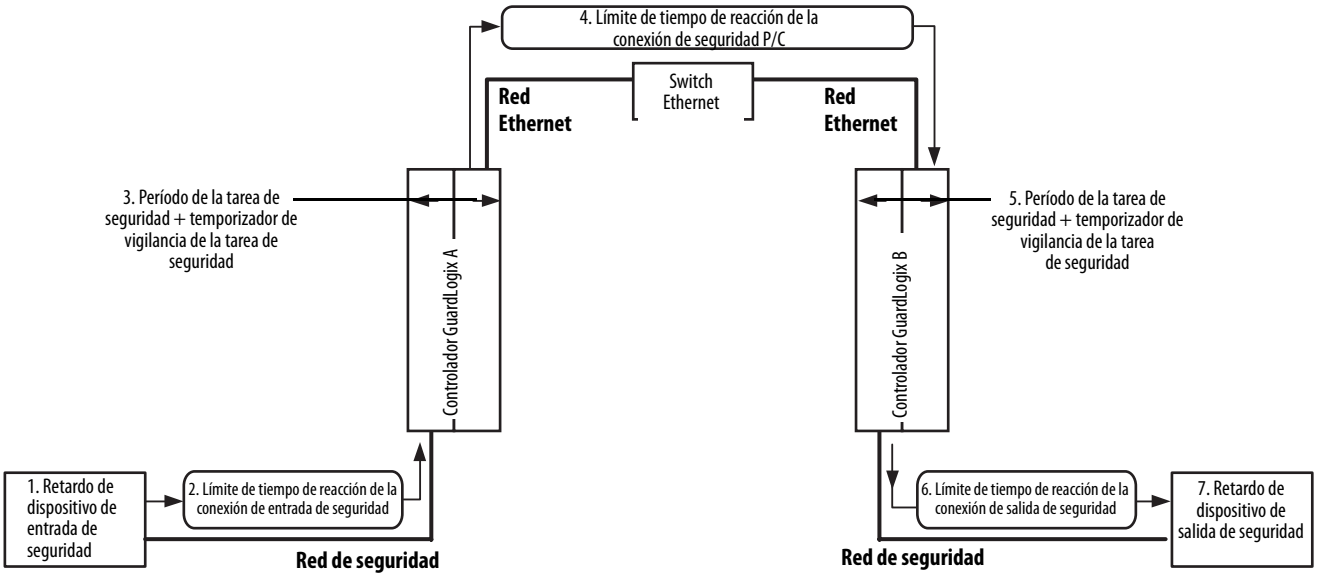
El tiempo de reacción del sistema Logix para cualquier cadena sencilla de entrada-lógica-salida consta de los cinco componentes siguientes:

1. Tiempo de reacción del dispositivo de entrada de seguridad (más tiempo de retardo de entrada, si corresponde)
2. Límite de tiempo de reacción de la conexión de entrada de seguridad (leído desde el cuadro de diálogo Module Properties de la aplicación Studio 5000 Logix Designer, este valor es un múltiplo del RPI de la conexión del dispositivo de entrada de seguridad).
3. Tiempo de reacción del controlador (consulte Tiempo de reacción de la tarea de seguridad en la página 15)
4. Límite de tiempo de reacción de la conexión de salida de seguridad (leído desde el cuadro de diálogo Module Properties de la aplicación Studio 5000 Logix Designer, este valor es un múltiplo del período de la tarea de seguridad).
5. Tiempo de reacción del dispositivo de salida de seguridad

## Cadena lógica que utiliza tags de seguridad producidos/consumidos

En esta sección se describe el tiempo de reacción del sistema Logix para cualquier cadena de entrada a lógica de controlador A a lógica de controlador B a salida.

**Figura 26 - Tiempo de reacción del sistema Logix de una cadena de entrada a controlador A, lógica a controlador B, lógica a salida**




El tiempo de reacción del sistema Logix de una cadena de entrada a controlador A, lógica a controlador B, lógica a salida consta de los siguientes siete componentes:

1. Tiempo de reacción del dispositivo de entrada de seguridad (más tiempo de retardo de entrada, si corresponde)
2. Límite de tiempo de reacción de la conexión de entrada de seguridad

3. Período de la tarea de seguridad más temporizador de vigilancia de la tarea de seguridad para el controlador A
4. Límite de tiempo de reacción de la conexión de seguridad producida/consumida (leído de la ficha Safety de la conexión de tags consumidos).
5. Período de la tarea de seguridad más temporizador de vigilancia de la tarea de seguridad para el controlador B
6. Límite de tiempo de reacción de la conexión de salida de seguridad
7. Tiempo de reacción del dispositivo de salida de seguridad

## Factores que afectan a los componentes del tiempo de reacción Logix

Varios factores pueden influir en los componentes del tiempo de reacción Logix que se han descrito en las secciones anteriores.

**Tabla 11 - Factores que afectan el tiempo de reacción del sistema Logix**

| Estos componentes de tiempo de reacción | Son influenciados por los siguientes factores |
|---|---|
| Retardo de dispositivo de entrada | Tiempo de reacción de dispositivo de entrada |
| | Ajustes de retardo de activado a desactivado y de desactivado a activado para cada canal de entrada, si corresponde |
| Límite de tiempo de reacción de la conexión de entrada de seguridad | Ajustes del dispositivo de entrada para:<br>• Intervalo solicitado entre paquetes (RPI)<br>• Multiplicador de interrupciones<br>• Multiplicador de retardo de red |
| | Cantidad de tráfico de comunicación en la red(1) |
| | El ambiente de compatibilidad electromagnética (EMC) del sistema(1) |
| Período de la tarea de seguridad y temporizador de vigilancia de la tarea de seguridad | Configuración del período de la tarea de seguridad |
| | Configuración del temporizador de vigilancia de la tarea de seguridad |
| | Número y tiempo de ejecución de las instrucciones en la tarea de seguridad(2) |
| | Cualquier tarea de mayor prioridad que pueda impedir la ejecución de la tarea de seguridad(2) |
| Límite de tiempo de reacción de la conexión de seguridad de datos producidos/consumidos | Ajustes de tag consumido para:<br>• Intervalo solicitado entre paquetes (RPI)<br>• Multiplicador de interrupciones<br>• Multiplicador de retardo de red |
| | Cantidad de tráfico de comunicación en la red(1) |
| | El ambiente de compatibilidad electromagnética (EMC) del sistema(1) |
| Límite de tiempo de reacción de la conexión de salida | Configuración del período de la tarea de seguridad |
| | Ajustes del dispositivo de salida para:<br>• Multiplicador de interrupciones<br>• Multiplicador de retardo de red |
| | Cantidad de tráfico de comunicación en la red(1) |
| | El ambiente de compatibilidad electromagnética (EMC) del sistema(1) |
| Retardo del módulo de salida | Tiempo de reacción del módulo de salida |

(1) El tráfico de red y el ruido electromagnético determinan el límite inferior de los valores que se pueden utilizar correctamente para el multiplicador de interrupciones y el multiplicador de retardo de red.

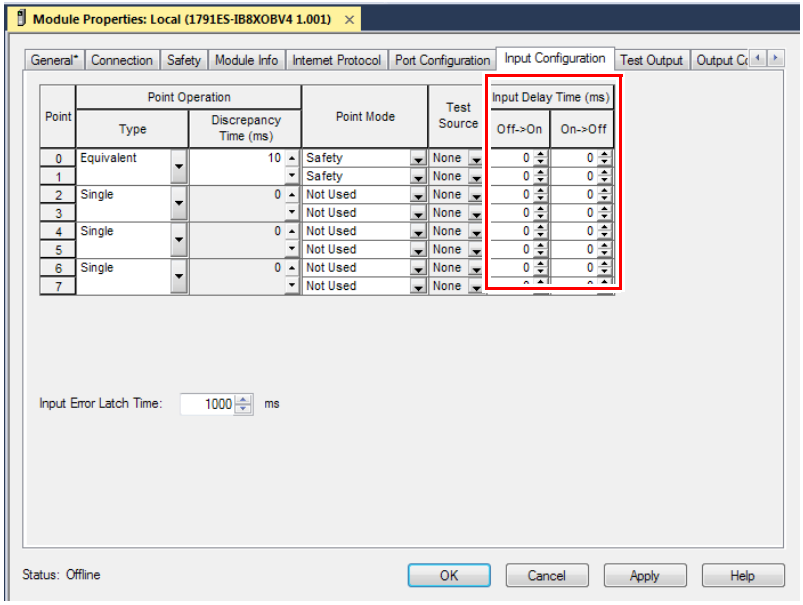
(2) Las instrucciones de la tarea de seguridad y cualquier tarea de mayor prioridad del controlador determinan el límite inferior de los valores que se pueden utilizar correctamente para el período de la tarea de seguridad y el temporizador de vigilancia de la tarea de seguridad.

Las siguientes secciones describen cómo obtener acceso a datos o a ajustes de muchos de estos factores.

## Configuración de ajustes de tiempo de retardo del módulo de entrada Guard I/O

Siga estos pasos para configurar el tiempo de retardo del módulo de entrada en la aplicación Studio 5000 Logix Designer.

1. En el árbol de configuración haga clic con el botón derecho del mouse en módulo Guard I/O y seleccione Properties.
2. Haga clic en la ficha Input Configuration.
3. Ajuste el tiempo de retardo de entrada según lo necesario para su aplicación.




## Configuración o visualización de los límites de tiempo de reacción de la conexión de seguridad de entrada y salida

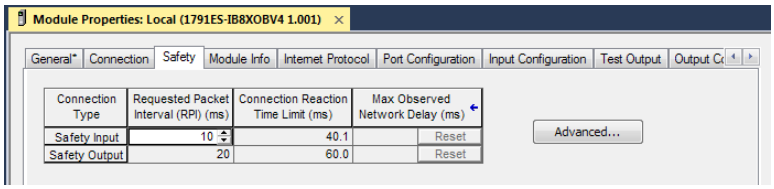
Los tres valores siguientes definen el límite de tiempo de reacción de la conexión (CRTL).

| Valor | Descripción |
|---|---|
| Requested Packet Interval (RPI) | Cuán a menudo se colocan los paquetes de entrada y de salida en el cable (la red). |
| Timeout Multiplier | El multiplicador de interrupciones es el número de reintentos antes de que se sobrepase el tiempo de espera. |
| Network Delay Multiplier | El valor de Network Delay Multiplier tiene en cuenta los retardos conocidos en el cable. Cuando ocurren estos retardos pueden evitarse los tiempos de espera mediante este parámetro. |

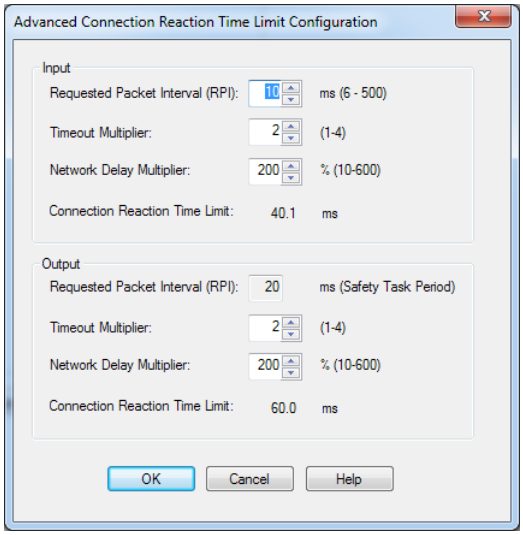
Si ajusta estos valores, podrá ajustar el límite de tiempo de reacción de la conexión. Si no se recibe un paquete válido en el CRTL, la conexión de seguridad sobrepasa el tiempo de espera y los datos de entrada y salida se colocan en el estado de seguridad.

Para ver o configurar estos ajustes, siga estos pasos.

1. En el árbol de configuración haga clic con el botón derecho del mouse en el dispositivo de E/S de seguridad y seleccione Properties.
2. Haga clic en la ficha Safety.




3. Haga clic en Advanced para abrir el cuadro de diálogo Advanced Connection Reaction Time Limit.



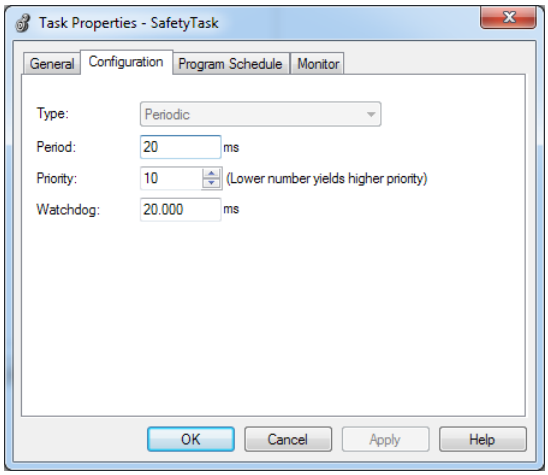

**IMPORTANTE** Los valores Timeout Multiplier y Network Delay Multiplier ofrecen resiliencia frente a las variaciones en la confiabilidad y el rendimiento de la red.

Tenga cuidado al reducir los valores de estos parámetros, ya que al hacerlo aumenta la posibilidad de que se produzcan falsos disparos.

## Configuración del período de la tarea de seguridad y el temporizador de vigilancia

La tarea de seguridad es una tarea periódica temporizada. El período de la tarea, la prioridad y el tiempo del temporizador de vigilancia se seleccionan en el cuadro de diálogo Task Properties – Safety Task del proyecto Studio 5000 Logix Designer.

Para obtener acceso a los ajustes del período de la tarea de seguridad y del tiempo del temporizador de vigilancia haga clic con el botón derecho del mouse en Safety Task y seleccione Properties.

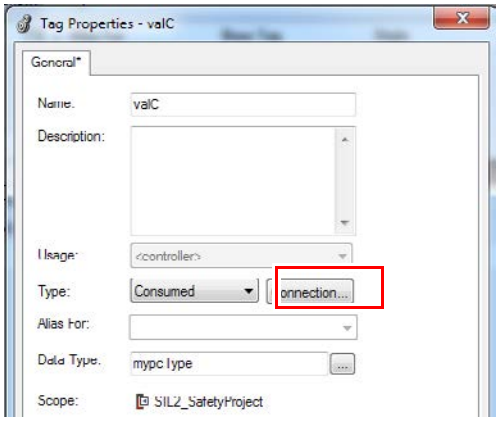



La prioridad de la tarea de seguridad no es un problema para la seguridad, ya que el temporizador de vigilancia de la tarea de seguridad monitorea si una tarea de mayor prioridad interrumpe la tarea.

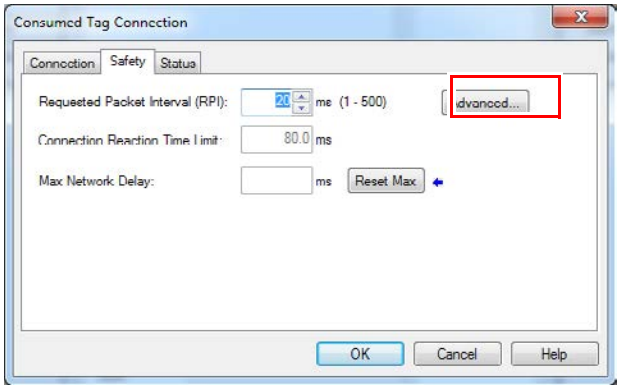
## Acceso a datos de tags producidos/consumidos

Para ver o configurar los datos de conexión de tag de seguridad, siga estos pasos.

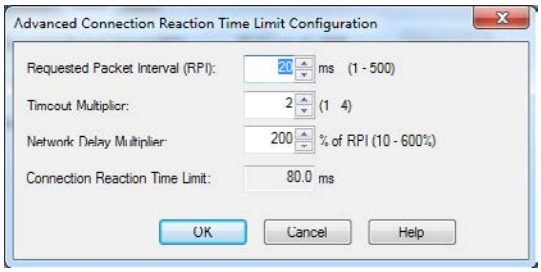
1. En el árbol de configuración haga clic con el botón derecho del mouse en Controller Tags y seleccione Edit Tags.
2. En el Tag Editor haga clic con el botón derecho del mouse en el nombre del tag y seleccione Edit Properties.
3. Haga clic en Connection.



4. En la ficha Safety, haga clic en Advanced.




5. Puede ver o editar los ajustes actuales en el cuadro de diálogo Advanced.




Consulte las siguientes publicaciones para obtener más información.

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publicación 1756-UM543
- Controladores CompactLogix 5380 Manual del usuario, publicación 5069-UM001

## Notas:

# Listas de verificación de aplicaciones de seguridad GuardLogix



Las listas de verificación de este apéndice son necesarias para planificar, programar y poner en marcha una aplicación de seguridad GuardLogix. Pueden utilizarse como guías de planificación, así como durante las pruebas de validación del proyecto. Si se utilizan como guías de planificación, las listas de verificación se pueden guardar como registro del plan.

Las listas de verificación en las siguientes páginas proporcionan una muestra de las consideraciones de seguridad y no fueron concebidas como una lista exhaustiva de puntos a verificar. Su aplicación de seguridad en particular puede tener requisitos de seguridad adicionales, para los que hemos contemplado un espacio en las listas de verificación.

**SUGERENCIA** Haga copias de las listas de verificación y guarde estas páginas para uso futuro.

# Listas de verificación del sistema controlador GuardLogix

| Lista de verificación del sistema GuardLogix | | | | |
|---|---|---|---|---|
| **Empresa** | | | | |
| **Ubicación** | | | | |
| **Definición de la función de seguridad** | | | | |
| **Número** | **Requisitos del sistema** | **Completada** | | **Comentario** |
| | | **Sí** | **No** | |
| 1 | ¿Está utilizando únicamente los componentes certificados para su nivel SIL, con la correspondiente versión del firmware, según se indica en http://www.rockwellautomation.com/global/certification/safety.page? | ☐ | ☐ | |
| 2 | ¿Ha calculado el tiempo de respuesta de seguridad del sistema para cada función de seguridad? | ☐ | ☐ | |
| 3 | ¿Incluye el tiempo de respuesta del sistema tanto el tiempo del temporizador de vigilancia del programa de la tarea de seguridad definido por el usuario (temporizador de vigilancia de software) como la velocidad/período de la tarea de seguridad? | ☐ | ☐ | |
| 4 | ¿Está el tiempo de respuesta del sistema en la proporción adecuada con respecto al tiempo de seguridad del proceso? | ☐ | ☐ | |
| 5 | ¿Se han calculado los valores de probabilidad (PFD/PFH) para cada función de seguridad? | ☐ | ☐ | |
| 6 | ¿Se han realizado todas las pruebas de validación del proyecto correspondientes? | ☐ | ☐ | |
| 7 | ¿Se ha determinado cómo puede manejar los fallos su sistema? | ☐ | ☐ | |
| 8 | ¿Tiene cada red del sistema de seguridad un SNN único? | ☐ | ☐ | |
| 9 | ¿Está configurado cada dispositivo de seguridad con el SNN correcto? | ☐ | ☐ | |
| 10 | ¿Se ha generado una firma de seguridad? | ☐ | ☐ | |
| 11 | ¿Se ha cargado y registrado la firma de seguridad para compararla posteriormente? | ☐ | ☐ | |
| 12 | Después de una descarga, ¿se ha verificado que la firma de seguridad del controlador coincide con la firma de seguridad registrada? | ☐ | ☐ | |
| 13 | ¿Se ha dispuesto un mecanismo alternativo para preservar la integridad de seguridad del sistema al realizar ediciones en línea? | ☐ | ☐ | |
| 14 | ¿Se han tenido en cuenta las listas de verificación para utilizar las entradas y las salidas SIL que aparecen en la página 93 y la 94? | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |

## Lista de verificación de entradas de seguridad

Para la programación o puesta en marcha, es posible rellenar una lista de verificación específica para cada entrada de seguridad del sistema. Este método constituye la única forma de asegurarse de que los requisitos se implementen total y claramente. Esta lista de verificación también se puede utilizar como documentación de la conexión del cableado externo al programa de aplicación.

| **Lista de verificación de entradas del sistema GuardLogix** | | | | |
|---|---|---|---|---|
| **Empresa** | | | | |
| **Ubicación** | | | | |
| **Definición de la función de seguridad** | | | | |
| **Canales de entrada SIL** | | | | |
| | | **Completada** | | |
| **Número** | **Requisitos del dispositivo de entrada** | **Sí** | **No** | **Comentario** |
| 1 | ¿Se han seguido las instrucciones de instalación y las precauciones de conformidad con los estándares de seguridad aplicables? | ☐ | ☐ | |
| 2 | ¿Se han realizado pruebas de validación del proyecto en el sistema y en los dispositivos? | ☐ | ☐ | |
| 3 | ¿Se ejecutan las funciones de control, de diagnóstico y de alarma en secuencia en la lógica de la aplicación? | ☐ | ☐ | |
| 4 | ¿Se ha cargado y comparado la configuración de cada dispositivo con la configuración enviada por la herramienta de configuración? | ☐ | ☐ | |
| 5 | ¿Se han cableado los dispositivos de acuerdo con el estándar de destino y el nivel de seguridad necesario? | ☐ | ☐ | |
| 6 | ¿Se ha verificado que las especificaciones eléctricas del sensor y de la entrada sean compatibles? | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |

## Lista de verificación de salidas de seguridad

Para la programación o puesta en marcha, es posible rellenar una lista de verificación de requisitos específica para cada salida de seguridad del sistema. Este método constituye la única forma de asegurarse de que los requisitos se implementen total y claramente. Esta lista de verificación también se puede utilizar como documentación de la conexión del cableado externo al programa de aplicación.

| **Lista de verificación de salidas del sistema GuardLogix** | | | | |
|---|---|---|---|---|
| **Empresa** | | | | |
| **Ubicación** | | | | |
| **Definición de la función de seguridad** | | | | |
| **Canales de salida SIL** | | | | |
| | | **Completada** | | |
| **Número** | **Requisitos del dispositivo de salida** | **Sí** | **No** | **Comentario** |
| 1 | ¿Se han seguido las instrucciones de instalación y las precauciones de conformidad con los estándares de seguridad aplicables? | ☐ | ☐ | |
| 2 | ¿Se han realizado pruebas de validación del proyecto en los dispositivos? | ☐ | ☐ | |
| 3 | ¿Se ha cargado y comparado la configuración de cada dispositivo con la configuración enviada por la herramienta de configuración? | ☐ | ☐ | |
| 4 | ¿Se ha verificado que las salidas de prueba no se estén utilizando como salidas de seguridad? | ☐ | ☐ | |
| 5 | ¿Se han cableado los dispositivos de acuerdo con el estándar de destino y el nivel de seguridad necesario? | ☐ | ☐ | |
| 6 | ¿Se ha verificado que las especificaciones eléctricas del accionador y de la salida son compatibles? | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |

# Lista de verificación para desarrollar un programa de aplicación de seguridad

Utilice la siguiente lista de verificación para ayudar a mantener la seguridad al crear o modificar un programa de aplicación de seguridad.

| Lista de verificación del desarrollo de un programa de aplicación GuardLogix | | | | |
|---|---|---|---|---|
| **Empresa** | | | | |
| **Ubicación** | | | | |
| **Definición del proyecto** | | | | |
| **Número** | **Requisitos del programa de aplicación** | **Completada** | | **Comentario** |
| | | **Sí** | **No** | |
| 1 | ¿Se está utilizando la versión 31 o una superior[1][2] de la aplicación Studio 5000 Logix Designer, la herramienta de programación del sistema GuardLogix? | ☐ | ☐ | |
| 2 | ¿Se siguieron las pautas de programación que aparecen en el Capítulo 6 en la página 49 durante la creación del programa de aplicación de seguridad? | ☐ | ☐ | |
| 3 | ¿Contiene el programa de aplicación de seguridad solo un diagrama de lógica de escalera? | ☐ | ☐ | |
| 4 | ¿Contiene el programa de aplicación de seguridad solo las instrucciones que aparecen en el Apéndice A en la página 71 como adecuadas para la programación de una aplicación de seguridad? | ☐ | ☐ | |
| 5 | ¿Distingue el programa de aplicación de seguridad claramente entre tags de seguridad y tags estándar? | ☐ | ☐ | |
| 6 | ¿Se utilizan solo tags de seguridad para las rutinas de seguridad? | ☐ | ☐ | |
| 7 | ¿Se ha verificado que las rutinas de seguridad no intenten leer tags estándar o escribir a ellos? | ☐ | ☐ | |
| 8 | ¿Se ha verificado que ningún tag de seguridad esté vinculado mediante alias a tags estándar, y viceversa? | ☐ | ☐ | |
| 9 | ¿Está cada tag de salida de seguridad configurado correctamente y conectado a un canal de salida física? | ☐ | ☐ | |
| 10 | ¿Se ha verificado que todos los tags asignados hayan sido condicionados en la lógica de la aplicación de seguridad? | ☐ | ☐ | |
| 11 | ¿Se han definido los parámetros del proceso que monitorean las rutinas de fallo? | ☐ | ☐ | |
| 12 | ¿Se ha sellado alguna instrucción Add-On de seguridad con una firma de instrucción y registrado la firma de la instrucción de seguridad? Opcional para instrucciones Add-On para usar una sola vez. Las instrucciones Add-On necesarias se reutilizan en varias aplicaciones. | ☐ | ☐ | |
| 13 | ¿Ha revisado el programa un revisor de seguridad independiente (si es necesario)? | ☐ | ☐ | |
| 14 | ¿Ha sido documentada y firmada la revisión? | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |
| | | ☐ | ☐ | |

(1) La aplicación Studio 5000 Logix Designer, versión 31 y posteriores, admite controladores GuardLogix 5580 y Compact GuardLogix 5380.

(2) Para obtener las versiones más recientes del software y del firmware, consulte el sitio web de asistencia del Centro de compatibilidad y descarga de productos (PCDC) de Rockwell Automation en http://www.rockwellautomation.com/global/support/pcdc.page.

## Notas:

# Datos de seguridad de sistemas GuardLogix



Los siguientes ejemplos muestran la probabilidad de un fallo peligroso a demanda (PFD) y la probabilidad de un fallo peligroso por hora (PFH) de un sistema GuardLogix 1oo1 SIL 2 o un sistema 1oo2 SIL 3.

Para consultar los datos de seguridad, que incluyen los valores de PFD y PFH de los módulos de E/S de seguridad, remítase a los manuales de dichos dispositivos. Para obtener más información, consulte Recursos adicionales en la página 8.

## Vida útil

La vida útil de los controladores GuardLogix es de 20 años.

## Datos de seguridad

Para ver los datos de seguridad de dispositivos de E/S, incluidos los valores de PFD y PFH, consulte los manuales de dichos productos.

Los datos de los productos de seguridad de máquinas de Rockwell Automation ahora están disponibles en forma de un archivo de biblioteca que puede utilizarse con la herramienta Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA).

El archivo de biblioteca puede descargarse de:
http://www.marketing.rockwellautomation.com/safety-solutions/ en/MachineSafety/ToolsAndDownloads/sistema_download.

## Tasas de fallos de los productos

Los datos de las siguientes tablas corresponden a tiempos de misión de hasta 20 años.

**Tabla 12 - Parámetros de seguridad**

| Atributo | Controladores y homólogo de seguridad GuardLogix 5580[2] [3] | Controlador GuardLogix 5580[2] [3] | Controlador Compact GuardLogix 5380[3] |
|---|---|---|---|
| Arquitectura de función de seguridad (HFT) [1] | 1 | 0 | 0 |
| Tasa de fallos con ninguna pieza/ningún efecto detectado ($\lambda_{NPED}$) [hora] | 2.80E-06 | 2.58E-06 | 4.04E-06 |
| Tasa de fallos de seguridad ($\lambda_S$) [fallos/hora] | 7.24E-07 | 6.61E-07 | 7.33E-07 |
| Tasa de fallos peligrosos ($\lambda_D$) [fallos/hora] | 7.10E-07 | 6.61E-07 | 7.33E-07 |
| Tasa de fallos peligrosos detectados ($\lambda_{DD}$) [fallos/hora] | 7.10E-07 | 6.54E-07 | 7.26E-07 |
| Tasa de fallos peligrosos no detectados ($\lambda_{DU}$) [fallos/hora] | 7.38E-11 | 6.40E-09 | 7.23E-09 |
| Intervalo de prueba de diagnóstico automático ($T_D$) [hora] | — | <SRT | <SRT |
| Vida útil [años] | 20 | 20 | 20 |
| Capacidad sistemática (SC) | 3 | 3 | 3 |

(1) La HFT aquí especificada es la HFT interna.
(2) Estos valores son las tasas de fallos de productos que deben utilizarse cuando el producto se represente como un bloque en el diagrama de bloques de confiabilidad (RBD).
(3) Estas tasas de fallos de productos son válidas para temperaturas ambiente de hasta 60 °C (140 °F) y altitudes de hasta 2000 m (6561.7 pies). Consulte las publicaciones 1756-TD001 y 1756-IN048.

**Tabla 13 - Cálculos de seguridad**

| Attribute | Controladores y homólogo de seguridad GuardLogix 5580 | Controlador GuardLogix 5580 | Controlador Compact GuardLogix 5380 |
|---|---|---|---|
| $PFD_{ave}$ (tiempo de misión de 20 años) | 6.46E-06 | 5.61E-04 | 6.33E-04 |
| PFH | 7.38E-11 | 6.40E-09 | 7.23E-09 |
| STR | 4.23E-06 | 3.90E-06 | 5.50E-06 |
| $MTTF_d$ [años] | 160.82 | 172.74 | 155.66 |

Suposiciones para los cálculos de seguridad:

- Las tasas de fallos de componentes son constantes durante la vida útil del producto.
- Todos los fallos detectados (seguros y peligrosos) ocasionan un estado de seguridad (MRT = 0).
- Tiempo de misión de ejemplo de 10 o 20 años. Dentro de la vida útil especificada (20 años), no se requiere ninguna prueba de calidad.

$$PFD_{ave} = (\lambda_{DU} + \lambda_{DD})t_{CE}$$

$$STR = \lambda_S + \lambda_{DD} + \lambda_{NPED}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$MTTF = \frac{1}{\lambda_D}$$

$$PFH = \lambda_{DU}$$

# Aplicación Studio 5000 Logix Designer, versión 31 y posteriores, instrucciones deaplicación de seguridad



**IMPORTANTE** Recomendamos utilizar las instrucciones de la aplicación de seguridad generales (tabla 5 en la página 71) en lugar de las instrucciones que se indican en este apéndice.

## Sistema de desenergizar para activar

Todos los valores de entrada de seguridad que están asociados a una conexión concreta se establecen en el estado de seguridad cuando se detecta una condición de fallo de la conexión CIP Safety. Cuando se utilizan pares de entradas diversas, una de las entradas utiliza un valor de uno para iniciar la función de seguridad. Esto que requiere una lógica de seguridad que evalúe las condiciones de fallo, por lo que se ejecuta la función de seguridad cuando se produce un fallo de entrada (aunque el valor de entrada permanezca en cero).

## Uso de los datos de estado de conexión para iniciar un fallo mediante programación

Los siguientes diagramas proporcionan ejemplos de la lógica de aplicación requerida para enclavar y restablecer fallos de E/S. Los ejemplos muestran la lógica necesaria para módulos de entrada solamente, y para módulos combinados de entrada y salida. Los ejemplos usan la función Combined Status de los módulos de E/S, la cual presenta el estado de todos los canales de entrada en una variable booleana. Otra variable booleana representa el estado de todos los canales de salida. Este enfoque reduce la cantidad de lógica de condicionamiento de E/S requerida, y fuerza la lógica a desactivar todos los canales de entrada o de salida del módulo afectado.

Use el Diagrama de flujo de enclavamiento y restablecimiento de fallo de salida en la página 100 para determinar qué renglones de lógica se requieren para diferentes situaciones de la aplicación. El Ejemplo de diagrama de lógica de escalera 1 en la página 101 muestra la lógica que sobrescribe las variables de tags de entrada actuales mientras exista una condición de fallo. Si se requiere el estado de entrada para la resolución de problemas mientras el fallo de entrada está enclavado, use la lógica mostrada en el Ejemplo de diagrama de lógica de escalera 2 en la página 102. Esta lógica usa tags internos que representan las entradas que se van a usar en la lógica de la aplicación. Mientras el fallo de entrada esté enclavado, los tags internos se establecen en su estado de seguridad. Mientras el fallo de entrada no esté enclavado, los valores de entrada actuales se copian a los tags internos.

Use el Diagrama de flujo de enclavamiento y restablecimiento de fallo de salida en la página 103 para determinar qué renglones se requieren de la lógica de aplicación en el Ejemplo de diagrama de lógica de escalera 3 en la página 103.

**Figura 27 - Diagrama de flujo de enclavamiento y restablecimiento de fallo de salida**

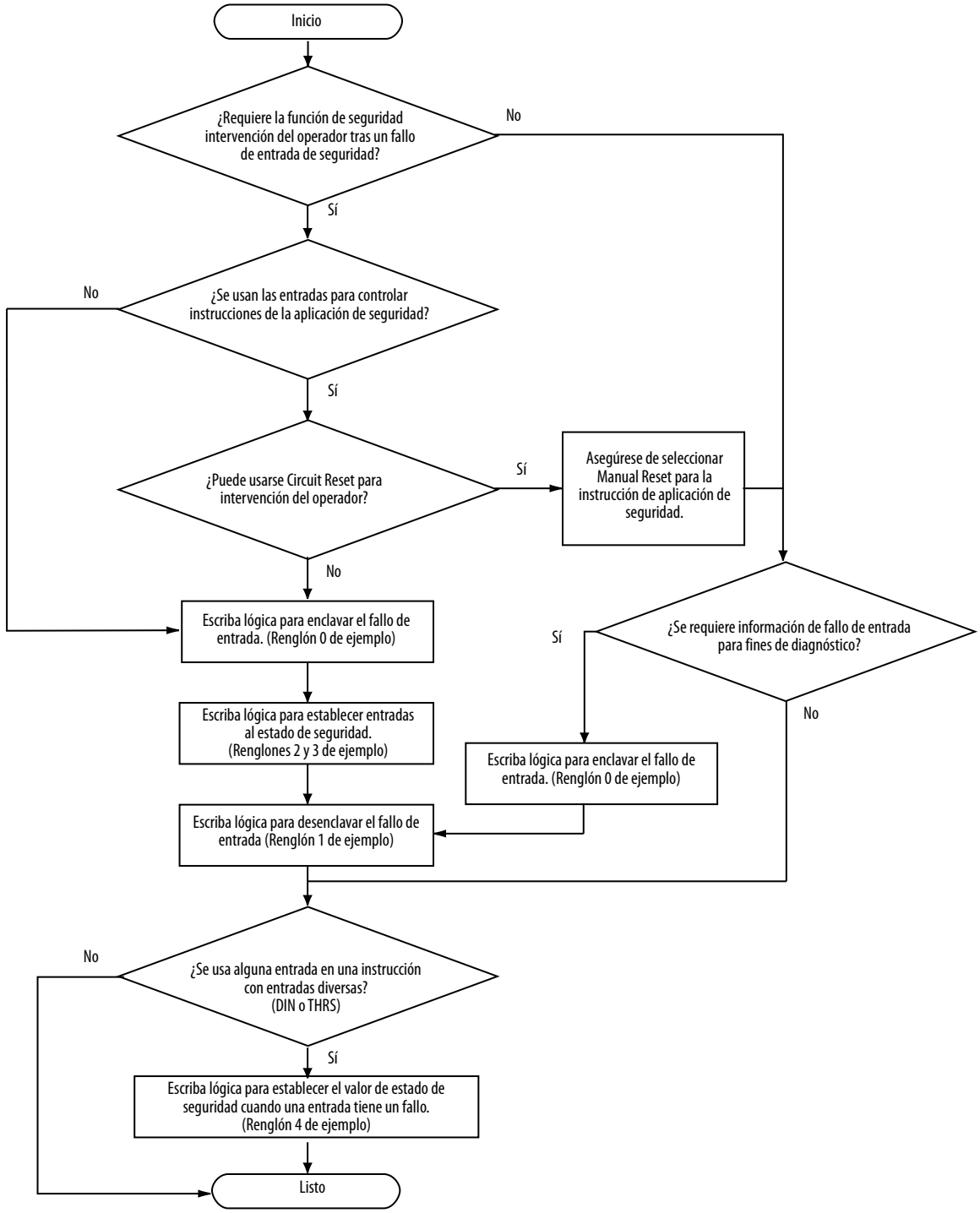


**Figura 28 - Ejemplo de diagrama de lógica de escalera 1**

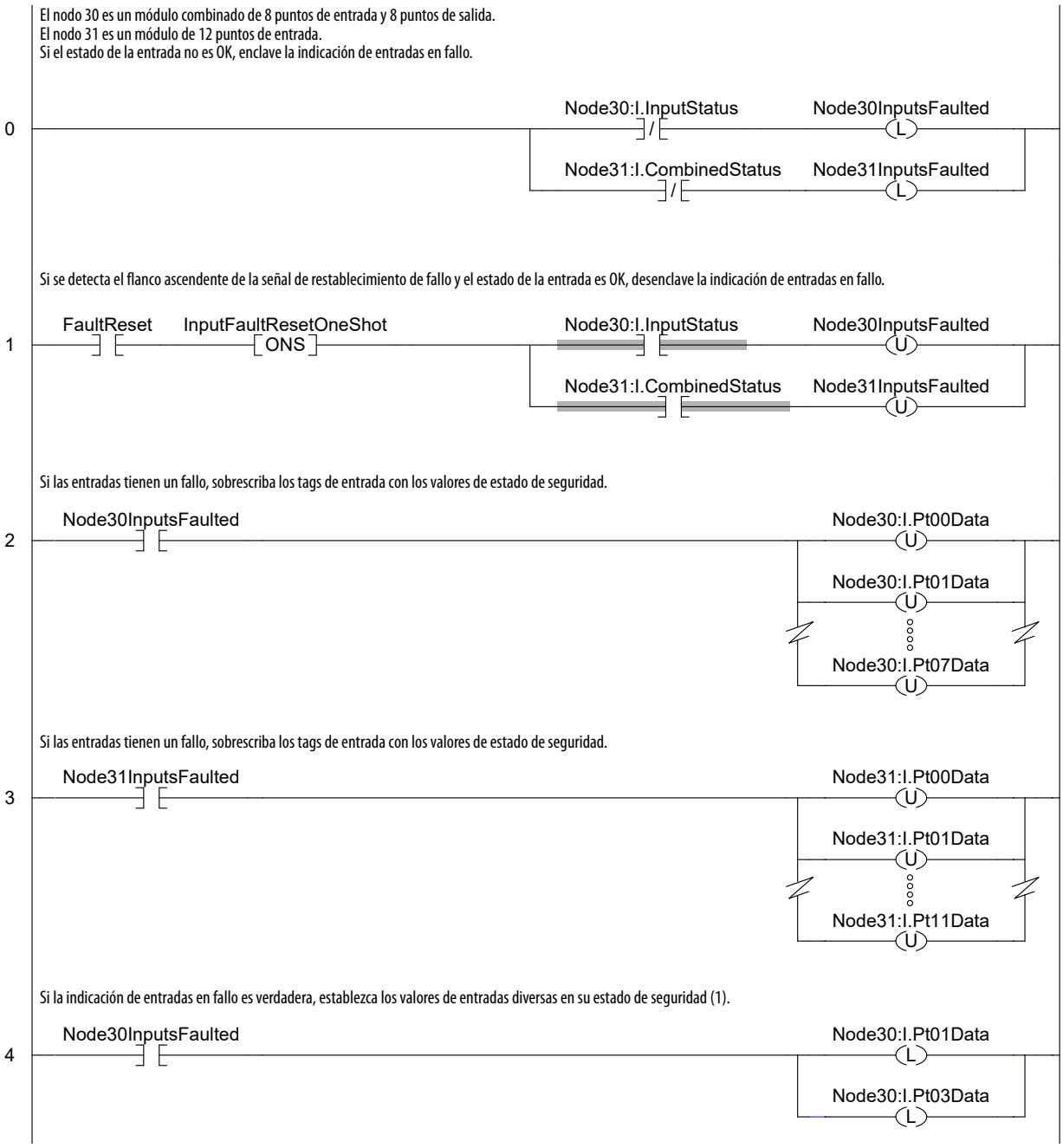


**Figura 29 - Ejemplo de diagrama de lógica de escalera 2**

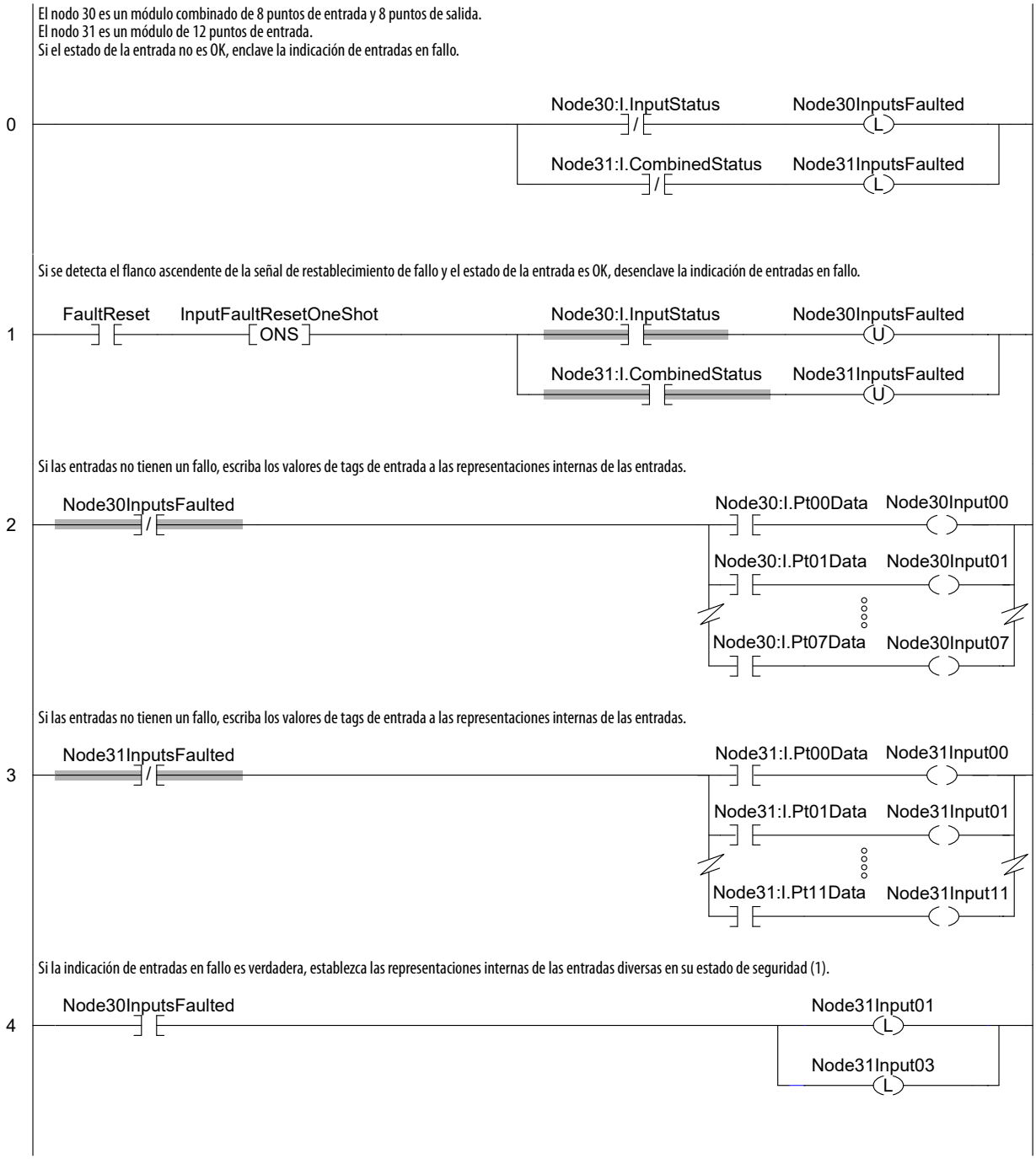


**Figura 30 - Diagrama de flujo de enclavamiento y restablecimiento de fallo de salida**

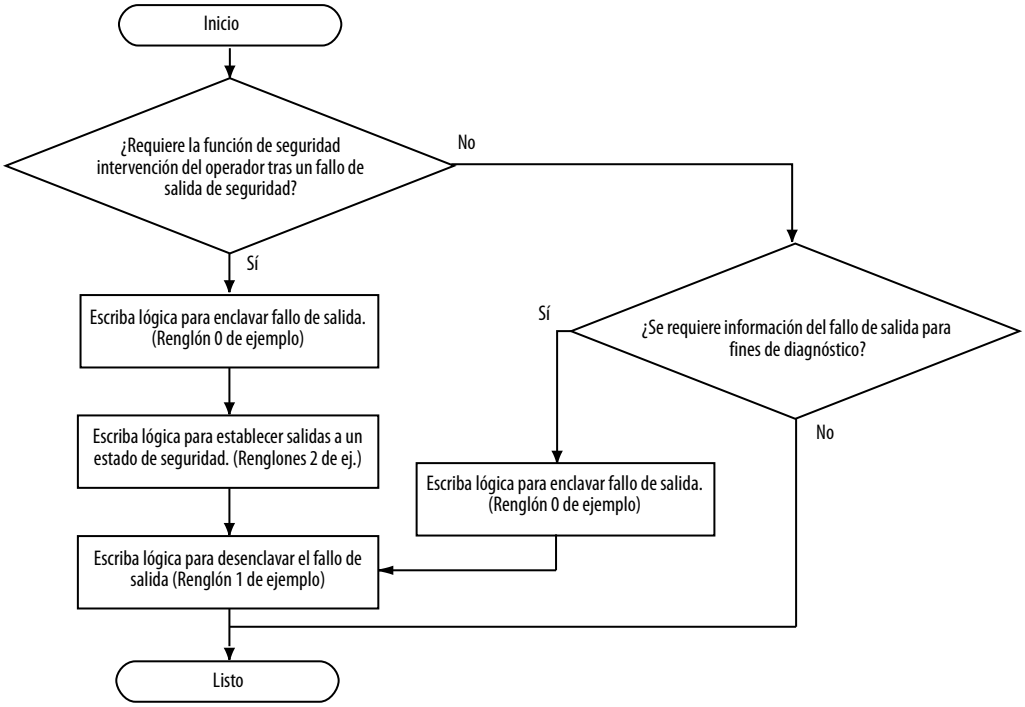
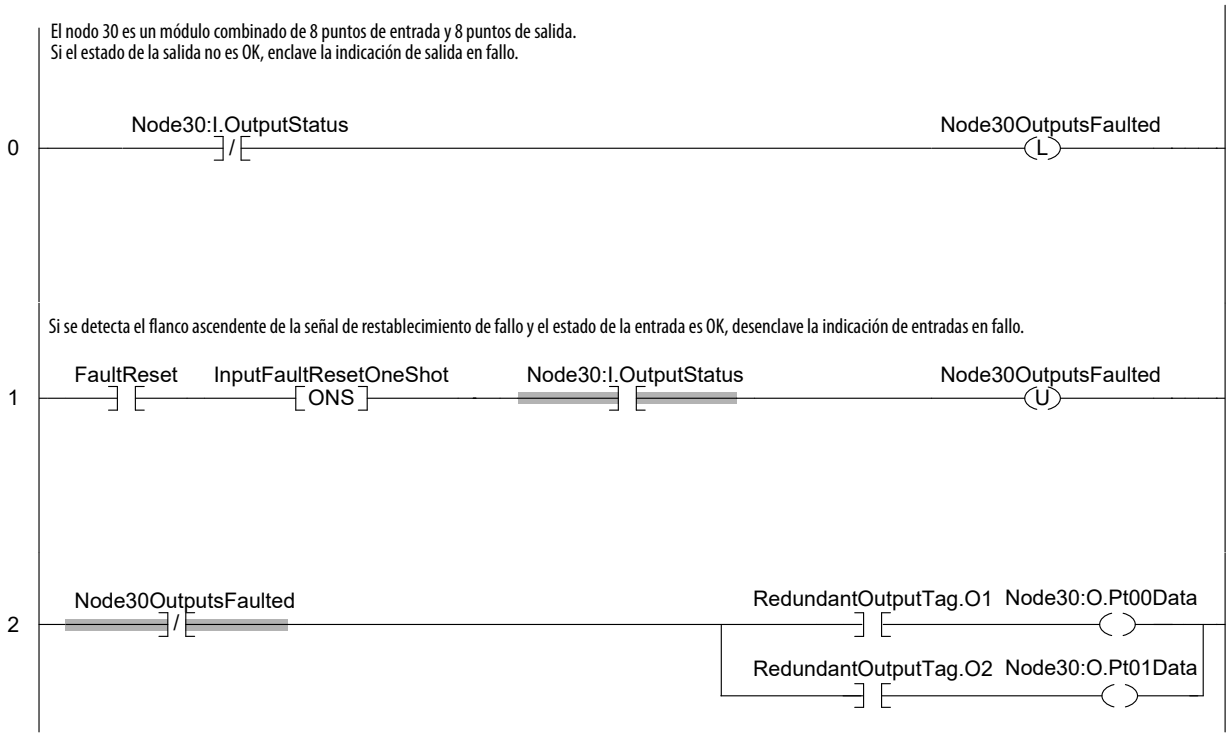



**Figura 31 - Ejemplo de diagrama de lógica de escalera 3**



## Notas:

En este manual se utilizan los siguientes términos y las siguientes abreviaturas. Para consultar las definiciones de términos no incluidos aquí consulte el documento Allen-Bradley Industrial Automation Glossary, publicación AG-7.1.

**1oo1 (uno de uno)** Identifica la arquitectura del controlador electrónico programable. 1oo1 es un sistema de un solo canal.

**1oo2 (uno de dos)** Identifica la arquitectura del controlador electrónico programable. 1oo2 es un sistema de dos canales.

**aceptar ediciones** Acción realizada para aceptar y descargar ediciones en línea. Consulte también componente estándar.

**asociación** Para que se establezca una asociación deben estar presentes en SIL 3 el controlador primario y el homólogo de seguridad, y el hardware y el firmware deben ser compatibles.

**cancelar ediciones** Acción realizada para rechazar y eliminar cualquier edición en línea que no haya sido ensamblada.

**cancelar prueba de ediciones** Una vez aceptadas las ediciones en línea, hay dos versiones de la lógica del usuario en la memoria del controlador. El comando Untest Edits de la aplicación Studio 5000 Logix Designer hace que el controlador ejecute la versión original sin editar de la lógica del usuario. La versión nueva editada de la lógica del usuario sigue en la memoria del controlador, pero no se ejecuta. Consulte ediciones de prueba.

**capacidad sistemática (SC)** Confianza en que la integridad sistemática del sistema cumpla los requisitos del nivel de integridad de seguridad (SIL) especificado. (según la norma IEC 61508-4)

**CIP (protocolo industrial común)** Un protocolo de comunicación industrial usado por los sistemas de automatización basados en Logix5000 en las redes de comunicación EtherNet/IP, ControlNet y DeviceNet.

**CIP Safety (protocolo industrial común – certificado de seguridad)** Versión con clasificación SIL 2 o SIL 3 de CIP.

**cobertura del diagnóstico (DC)** Relación entre la tasa de fallos peligrosos detectados y la tasa de fallos peligrosos.

**componente de seguridad** Cualquier objeto, tarea, programa, rutina, tag o módulo que esté marcado como ítem relacionado con la seguridad.

**componente estándar** Todo objeto, tarea, tag, programa, etc., que no está marcado como ítem relacionado con la seguridad.

**computadora personal (PC)** Computadora utilizada para servir de interface y controlar un sistema basado en Logix mediante el ambiente Studio 5000.

**Conexión válida** La conexión de seguridad está abierta y activa, y no tiene errores.

**controlador estándar** En este documento, un controlador estándar se refiere en términos genéricos a un controlador ControlLogix o CompactLogix.

**controlador primario** Procesador en un controlador con dos procesadores que realiza la funcionalidad de controlador estándar y que se comunica con el homólogo de seguridad para realizar funciones relacionadas con la seguridad.

**direccionamiento simbólico** Método de direccionamiento que proporciona una interpretación ASCII del nombre del tag.

**ediciones de prueba** Una vez aceptadas las ediciones en línea, hay dos versiones de la lógica del usuario en la memoria del controlador. El comando Test Edits de la aplicación Studio 5000 Logix Designer hace que el controlador ejecute la versión nueva y editada de la lógica del usuario. La versión original sin editar de la lógica del usuario sigue en la memoria del controlador, pero no se ejecuta. Consulte cancelar prueba de ediciones.

**ediciones pendientes** Cambio a una rutina que se ha realizado en la aplicación Studio 5000 Logix Designer, pero que todavía no ha sido comunicado al controlador mediante la aceptación de la edición.

**en línea** Situación en la que usted está monitoreando o modificando el programa en el controlador.

**ensamblar ediciones** Se ensamblan ediciones cuando se ha editado en línea el programa del controlador y se desea que estas ediciones sean permanentes, porque ya no se necesita la capacidad de hacer pruebas, deshacer pruebas y anular ediciones.

**entrada de seguridad** Combinación de tags de seguridad producidos y consumidos, entradas de seguridad asignadas y entradas provenientes de módulos de seguridad.

**E/S de seguridad** Las E/S de seguridad tienen la mayoría de los atributos de las E/S estándar, con la excepción de que incorporan mecanismos con certificación SIL 2 o SIL 3 para integridad de los datos.

**estándar** Cualquier objeto, tarea, tag, programa o componente del proyecto que no está relacionado con la seguridad (por ej., un controlador estándar se refiere de manera genérica a un controlador ControlLogix o CompactLogix).

**fallo de controlador no recuperable** Fallo que fuerza la finalización de todo procesamiento y precisa la desconexión y la conexión de la alimentación al controlador. El programa de usuario no se conserva, y es necesario volver a descargarlo.

**fallo de seguridad no recuperable** Fallo que, a pesar de haber sido manejado adecuadamente por los mecanismos de manejo de fallos proporcionados por el controlador de seguridad e implementado por el usuario, termina todo el procesamiento de la tarea de seguridad y precisa una acción externa del usuario para reiniciar la tarea de seguridad.

**fallo detectado** Fallo que detectan las pruebas de diagnóstico, las pruebas de calidad, la intervención del operador o el funcionamiento normal.

**fallo no detectado** Fallo que no resulta detectado por las pruebas de diagnóstico, las pruebas de calidad, la intervención del operador o mediante el funcionamiento normal.

**fallo recuperable** Fallo que, cuando se maneja adecuadamente mediante la implementación de mecanismos de manejo de fallos proporcionados por el controlador, no fuerza la terminación de la ejecución de la lógica del usuario.

**firma de configuración** Número que identifica de manera única la configuración de un dispositivo. La firma de configuración está compuesta de un número de identificación o ID, una fecha y una hora.

**firma de instrucción** La firma de instrucción está compuesta por un número de identificación y un sello de fecha/hora que identifica el contenido de la definición de la instrucción Add-On en un momento dado.

**firma de instrucción de seguridad** La firma de instrucción de seguridad es un número de identificación que identifica las características de ejecución de la instrucción Add-On de seguridad. La firma se utiliza para verificar la integridad de la instrucción Add-On de seguridad durante las descargas al controlador.

**firma de seguridad** Valor calculado por el firmware que representa de forma única la lógica y la configuración del sistema de seguridad. Se utiliza para verificar la integridad del programa de aplicación de seguridad durante las descargas al controlador.

**fracción de fallos seguros (SFF)** La suma de fallos de seguridad más la suma de fallos detectados peligrosos, divididas entre la suma de todos los fallos.

**frecuencia promedio de un fallo peligroso (PFH)** Probabilidad de que un sistema experimente un fallo peligroso por hora.

**GSV (obtener valor del sistema)** Instrucción de la aplicación del usuario que obtiene información especificada sobre el estado del controlador y la pone en un tag de destino.

**homólogo de seguridad** Procesador en un controlador con dos procesadores que interactúa con el controlador primario para realizar funciones relacionadas con la seguridad en un sistema SIL 3.

**instrucción Add-On** Instrucción que usted crea como adición al conjunto de instrucciones Logix. Una vez definida, una instrucción Add-On puede usarse como cualquier otra instrucción Logix, en varios proyectos. Una instrucción Add-On se compone de parámetros, tags locales, rutina lógica y rutinas de modo de escán opcionales.

**instrucción Add-On de seguridad** Instrucción Add-On que puede usar instrucciones de aplicaciones de seguridad. Además de la firma de instrucción usada para instrucciones Add-On de gran integridad, las instrucciones Add-On de seguridad cuentan con una firma de instrucción de seguridad SIL 2 o SIL 3 para uso en funciones relacionadas con la seguridad.

**instrucciones de aplicaciones de seguridad** Son instrucciones de seguridad que proporcionan la funcionalidad relacionada con la seguridad. Han recibido la certificación SIL 2 o SIL 3 para ser usadas en rutinas de seguridad.

**intervalo solicitado entre paquetes (RPI)** Frecuencia con la que la aplicación de origen requiere la transmisión de datos procedentes de la aplicación de destino.

**lambda (λ)** Designación de una tasa de fallos.

**límite de reclamación SIL (SILCL)** SIL máximo que se puede reclamar para un subsistema SRECS en relación con las restricciones arquitectónicas y la integridad de seguridad sistemática. (según la norma IEC 62061)

**MT (tiempo de misión)** Intervalo de tiempo durante el que el dispositivo mantiene los valores de PFD, PFH y λ indicados antes de que sea necesario sustituirlo.

**multiplicador de interrupciones** Este valor determina el número de mensajes que se pueden perder antes de declarar un error de conexión. Consulte también multiplicador de retardo de red.

**multiplicador de retardo de red** Este valor representa el tiempo de transporte de un mensaje a través de la red de comunicación. Consulte también fallo no detectado.

**nivel de integridad de seguridad (SIL)** Nivel relativo de reducción del riesgo proporcionado por una función de seguridad o utilizado para especificar un nivel objetivo de reducción del riesgo.

**nivel de rendimiento (PL)** Nivel discreto que se utiliza en la norma EN ISO 13849-1 para especificar la capacidad de las partes relacionadas con la seguridad de los sistemas de control de llevar a cabo una función de seguridad en las condiciones previsibles.

**norma europea (EN)** Estándar oficial europeo.

**número de red de seguridad (SNN)** Identifica de forma única una red entre todas las redes del sistema de seguridad. Usted es responsable de asignar un número único a cada red de seguridad o subred de seguridad que haya dentro de un sistema. El número de red de seguridad es parte del identificador único de nodo (UNID).

**período de la tarea de seguridad** Período en que se ejecuta la tarea de seguridad.

**probabilidad de fallo peligroso a demanda (PFD)** Probabilidad promedio de un fallo peligroso a demanda.

**probabilidad de fallo peligroso por hora (PFH)** Frecuencia promedio de un fallo peligroso por hora.

**programa de seguridad** Un programa de seguridad que tiene todos los atributos de un programa estándar, con la excepción de que se puede priorizar solo en una tarea de seguridad. El programa de seguridad consta de cero o más rutinas de seguridad. No puede contener rutinas estándar ni tags estándar.

**protocolo de seguridad** Método de comunicación en red diseñado y certificado para el transporte de datos con gran integridad.

**rutina** Conjunto de instrucciones lógicas en un lenguaje de programación como, por ejemplo, diagrama de lógica de escalera. Las rutinas proporcionan código ejecutable para el proyecto de un controlador. Cada programa tiene una rutina principal. También se pueden especificar rutinas opcionales.

**rutina de seguridad** Una rutina de seguridad que tiene todos los atributos de una rutina estándar, con la excepción de que es válida solo en un programa de seguridad y que consta de una o más instrucciones apropiadas para aplicaciones de seguridad. (Consulte el Apéndice A en la página 71 para obtener una lista de instrucciones de aplicación de seguridad y de instrucciones Logix estándar que pueden usarse en la lógica de la rutina de seguridad).

**SSV (establecer valor del sistema)** Instrucción de la aplicación del usuario que define los datos del sistema controlador.

**superposición** Sucede cuando una tarea (periódica o de evento) se activa sin que la misma haya terminado de ejecutarse tras la activación anterior.

**tags de seguridad** Un tag de seguridad tiene todos los atributos de un tag estándar, con excepción de que el controlador GuardLogix proporciona mecanismos con certificación SIL 2 o SIL 3 para ayudar a proteger la integridad de los datos asociados. Pueden estar cubiertos por el programa o cubiertos por el controlador.

**tarea** Mecanismo de priorización para ejecutar un programa. Una tarea proporciona la información de priorización y secuenciamiento para uno o más programas que se ejecutan con base en un criterio determinado. Una vez que se activa una tarea, todos los programas asignados (programados) a la tarea se ejecutan en el orden en el cual se muestran en el organizador del controlador.

**tarea de seguridad** Una tarea de seguridad tiene todos los atributos de una tarea estándar, con la excepción de que es válida solo en un controlador GuardLogix y de que solamente puede priorizar programas de seguridad. Puede existir una sola tarea de seguridad en un controlador GuardLogix. La tarea de seguridad tiene que ser una tarea periódica/temporizada.

**tarea periódica** Tarea que el sistema operativo activa con un período repetitivo. Cuando expira el tiempo, la tarea se activa y se ejecutan sus programas. Los datos y las salidas que los programas de la tarea establecen conservan sus valores hasta la siguiente ejecución de la tarea o hasta que otra tarea los manipule. Las tareas periódicas siempre interrumpen la tarea continua.

**temporizador de vigilancia de la tarea de seguridad** Tiempo máximo permitido desde el inicio de la ejecución de la tarea de seguridad hasta que la misma se completa. Al expirar el temporizador de vigilancia de la tarea de seguridad se activa un fallo de seguridad no recuperable.

**tiempo de reacción de la tarea de seguridad** Suma del período de la tarea de seguridad más el periodo del temporizador de vigilancia de la tarea de seguridad. Este tiempo representa el retardo en el peor de los casos, desde el momento en que ocurre cualquier cambio de entrada presentado al controlador GuardLogix, hasta el momento en que la salida procesada está disponible para la conexión productora.

**tiempo de reacción del sistema** El tiempo transcurrido, en el peor de los casos, desde que se produce un evento relacionado con la seguridad como entrada al sistema o como fallo dentro del sistema, hasta el momento en que el sistema queda en estado seguro. El tiempo de reacción del sistema incluye los tiempos de reacción del sensor y el accionador, los tiempos de reacción de entrada y salida (incluyendo los retardos de conexión de red) y el tiempo de reacción del controlador.

**tolerancia a fallos de hardware** La HFT es igual a *n*, donde *n*+1 fallos pueden ocasionar la pérdida de la función de seguridad. Una HFT de 1 indica que hacen falta 2 fallos antes de que se pierda la seguridad.

## Notas:

## E



## F

## G



## H



## I



## L



## M



## N

## O



## P



## R



## S

## T



## U



## V

## Notas:

## Servicio de asistencia técnica de Rockwell Automation

Utilice los siguientes recursos para consultar la información de asistencia.

| | | |
|---|---|---|
| **Centro de asistencia técnica** | Artículos de Knowledgebase, vídeos con tutoriales, preguntas frecuentes, chat, foros de usuarios y actualizaciones de notificación de productos. | https://rockwellautomation.custhelp.com/ |
| **Números de teléfono de asistencia técnica local** | Busque el número de teléfono correspondiente a su país. | http://www.rockwellautomation.com/global/support/get-support-now.page |
| **Códigos de llamada directa** | Busque el código de llamada directa para su producto. Utilice el código para dirigir su llamada directamente a un ingeniero de asistencia técnica. | http://www.rockwellautomation.com/global/support/direct-dial.page |
| **Literature Library** | Instrucciones de instalación, manuales, folletos y datos técnicos. | http://www.rockwellautomation.com/global/literature-library/overview.page |
| **Centro de compatibilidad y descarga de productos (PCDC)** | Obtenga ayuda para determinar cómo interactúan los productos, comprobar las características y capacidades, y buscar el firmware asociado. | http://www.rockwellautomation.com/global/support/pcdc.page |

## Comentarios sobre la documentación

Sus comentarios nos ayudarán a atender mejor sus necesidades de documentación. Si tiene alguna sugerencia sobre cómo mejorar este documento, rellene el formulario How Are We Doing? en http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.

Rockwell Automation mantiene información medioambiental actualizada sobre sus productos en su sitio web en http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.



**www.rockwellautomation.com**

**Oficinas corporativas de soluciones de potencia, control e información**

Américas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europa/Medio Oriente/África: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Bélgica, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia-Pacífico: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Argentina: Rockwell Automation S.A., Av. Leandro N. Alem 1050, Piso 5, Ciudad Autónoma de Buenos Aires, Tel.: (54) 11.5554.4040, www.rockwellautomation.com.ar
Chile: Rockwell Automation Chile S.A., Av. Presidente Riesco 5435, Piso 15, Las Condes, Santiago, Tel.: (56) 2.290.0700, www.rockwellautomation.com.cl
Colombia: Rockwell Automation S.A., Edf. North Point, Carrera 7 N 156-78 Piso 19, PBX: (57) 1.649.9600, www.rockwellautomation.com.co
España: Rockwell Automation S.A., C/ Josep Plà, 101-105, Barcelona, España 08019, Tel.: 34 902 309 330, www.rockwellautomation.es
México: Rockwell Automation de S.A. de C.V., Av. Santa Fe 481, Piso 3 Col. Cruz Manca, Deleg, Cuajimalpa, Ciudad de México C.P. 05349, Tel. 52 (55) 5246-2000, www.rockwellautomation.com.mx
Perú: Rockwell Automation S.A., Av. Victor Andrés Belaunde N 147, Torre 12, Of.102, San Isidro Lima, Perú, Tel.: (511) 211-4900, www.rockwellautomation.com.pe
Puerto Rico: Rockwell Automation, Inc., Calle 1, Metro Office #6, Suite 304, Metro Office Park, Guaynabo, Puerto Rico 00968, Tel.: (1) 787.300.6200, www.rockwellautomation.com.pr
Venezuela: Rockwell Automation S.A., Edf. Allen-Bradley, Av. González Rincones, Zona Industrial La Trinidad, Caracas 1080, Tel.: (58) 212.949.0611, www.rockwellautomation.com.ve

Publicación 1756-RM012B-ES-P - Abril 2018