Manual del usuario

Allen-Bradley

Controladores GuardLogix 5570

Números de catálogo 1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP, 1756-L73SXT, 1756-L7SPXT, 1756-L72EROMS

Studio 5000 Automation Engineering & Design Environment

Traducción de las Instrucciones originales

Información importante para el usuario

Lea este documento y los documentos enumerados en la sección de recursos adicionales sobre la instalación, configuración y operación de este equipo antes de instalar, configurar, operar o realizar el mantenimiento de este producto. Los usuarios deberán familiarizarse con las instrucciones de instalación y cableado, y con los requisitos de todos los códigos, leyes y normas aplicables.

Las actividades que incluyan instalación, ajustes, puesta en servicio, uso, montaje, desmontaje y mantenimiento deberán ser realizadas por personal debidamente capacitado de conformidad con el código de prácticas aplicable.

Si este equipo se utiliza de una forma diferente a la indicada por el fabricante, la protección proporcionada por el equipo puede verse afectada.

En ningún caso Rockwell Automation, Inc. responderá ni será responsable de los daños indirectos o consecuentes que resulten del uso o la aplicación de este equipo.

Los ejemplos y los diagramas que aparecen en este manual se incluyen únicamente con fines ilustrativos. 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 en aplicaciones reales basado en los ejemplos y los diagramas.

Rockwell Automation, Inc. no asume ninguna obligación de patente por el 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 por escrito 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 provocar una explosión en un ambiente peligroso, la cual podría ocasionar lesiones personales o la muerte, daños materiales o pérdidas económicas.
	**ATENCIÓN:** Identifica información sobre las prácticas o circunstancias que pueden ocasionar lesiones personales o la muerte, daños materiales o pérdidas económicas. Los mensajes de Atención le ayudan a identificar un peligro, a evitar un peligro y a reconocer las consecuencias.
IMPORTANTE	Identifica información esencial para usar el producto y comprender su funcionamiento.

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) a fin de advertir sobre superficies que podrían alcanzar temperaturas peligrosas.
	**PELIGRO DE ARCO ELÉCTRICO:** Puede haber etiquetas sobre el equipo o dentro del mismo (por ejemplo, en un centro de control de motores) para alertar sobre la posibilidad de que se produzca un arco eléctrico. Un arco eléctrico puede provocar lesiones graves o la muerte. Lleve un equipo de protección personal (PPE) adecuado. Siga TODOS los requisitos reglamentarios en torno a las prácticas de trabajo seguras y al equipo de protección personal (PPE).

Este manual contiene información nueva y actualizada.

Información nueva y actualizada

Esta tabla contiene los cambios realizados en esta revisión.

Tema	Página
Se cambió el título de la sección, de Más recursos a Para obtener más información.	11
Se cambió la descripción de la columna de recursos, de Servovariadores Kinetix® a Variadores.	12
Se añadieron los documentos Kinetix 5700 Servo Drives User Manual y PowerFlex® 527 Adjustable Frequency AC Drive User Manual al material de recursos de variadores.	12
Se eliminó la información de las versiones anteriores de la tabla Características compatibles.	19
Se cambió el título de la columna, de Versión 24 a Versiones 24 y posteriores.	19
Se añadió una oración introductoria y la Figura 10.	48
Se añadió contenido de asignación de SNN a la tabla Importante.	49
Se revisó la Figura 14 para incluir los variadores PowerFlex 527 y Kinetix 5700.	56
Se añadieron los variadores Kinetix 5700 y PowerFlex 527 a la información de dirección de variadores.	73
Se revisó el título de la tabla 20 y la información de la tabla para incluir más variadores.	73
Se añadieron los variadores Kinetix 5700 y PowerFlex 527 a la referencia para obtener información adicional.	74

Notas:

Capítulo 3

Configuración del controlador

Capítulo 4

Comunicación a través de redes

Capítulo 5

Cómo añadir, configurar, monitorear y reemplazar dispositivos CIP Safety I/O

Capítulo 6

Desarrollo de aplicaciones de seguridad

Capítulo 7

Entrada en línea con el controlador

Capítulo 8

Almacenamiento y carga de proyectos usando la memoria no volátil

Capítulo 9

Monitoreo de estado y manejo de fallos

Apéndice A

Indicadores de estado

Apéndice B

Cambio del tipo de controlador

Índice

Este manual constituye una guía para los casos en que se usa un controlador GuardLogix® 5570 en una aplicación Studio 5000 Logix Designer™. En él se describen los procedimientos específicos de GuardLogix que se utilizan para configurar, operar y resolver problemas del controlador.

Utilice este manual si es responsable del diseño, instalación, programación o resolución de problemas de sistemas de control con controladores GuardLogix 5570.

Debe tener conocimientos básicos sobre circuitos eléctricos y estar familiarizado con la lógica de relés. Además, debe haber recibido la formación adecuada y tener la experiencia necesaria en la creación, operación y mantenimiento de sistemas de seguridad.

Para obtener información detallada sobre temas relacionados con el controlador GuardLogix, los requisitos de nivel de integridad de seguridad (SIL) 3 y nivel de rendimiento (e) (SIL 3/PLe), o información sobre los componentes Logix estándar, consulte la lista de Para obtener más información en la página 11.

Información sobre los controladores GuardLogix

Hay dos líneas de controladores 1756 GuardLogix disponibles. Estos controladores comparten muchas características, pero también tienen algunas diferencias. La Tabla 1 proporciona una breve descripción de estas diferencias.

Tabla 1 – Diferencias entre los controladores GuardLogix 5570 y GuardLogix 5560

Característica	**Controladores GuardLogix 5570** (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT)	**Controladores GuardLogix 5560** (1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP)
Alimentación del reloj y respaldo que se usa para retener los datos en la memoria mientras la unidad está apagada	Módulo de almacenamiento de energía (ESM)	Batería
Puertos de comunicación (incorporados)	USB	En serie
Conexiones, controlador	500	250
Memoria, no volátil	Tarjeta Secure Digital (SD)	Tarjeta CompactFlash (CF)
Indicadores de estado	Pantalla de estado desplazable e indicadores de estado	Indicadores de estado
Herramienta de programación	Ambiente Studio 5000, versión 21 o posterior Software RSLogix™ 5000, versión 20 o posterior	Software RSLogix 5000, versión 14 Software RSLogix 5000, versión 16 o posterior
Manual del usuario	• Ambiente Studio 5000: este manual • Software RSLogix 5000: 1756-UM020	1756-UM020
Manual de referencia de seguridad	• Ambiente Studio 5000: 1756-RM099 • Software RSLogix 5000: 1756-RM093	1756-RM093

Controladores para ambientes difíciles

Los controladores ControlLogix para ambientes difíciles, números de catálogo 1756-L73SXT y 1756-L7SPXT, proporcionan la misma funcionalidad que el controlador 1756-L73S, pero están diseñados para soportar temperaturas de –25...70 °C (–13...158 °F).

IMPORTANTE	Los componentes del sistema Logix-XT están clasificados para condiciones ambientales difíciles solo cuando se usan correctamente con otros componentes del sistema Logix-XT. El uso de componentes Logix-XT con componentes del sistema Logix tradicional anula las clasificaciones para condiciones ambientales difíciles.

Controladores Armor GuardLogix

El controlador Armor™ GuardLogix (número de catálogo 1756-L72EROMS) combina un controlador GuardLogix 1756-L72S y un homólogo de seguridad con dos canales de comunicación EtherNet/IP™ compatibles con DLR en un envolvente con calificación IP67 para montaje en una máquina. Para obtener más información acerca del controlador Armor GuardLogix, consulte las instrucciones de instalación del controlador Armor GuardLogix, publicación 1756-IN060.

Ambiente Studio 5000

Studio 5000 Automation Engineering & Design Environment™ combina los elementos de ingeniería y diseño en un ambiente común. El primer elemento es la aplicación Studio 5000 Logix Designer. Logix Designer es el nuevo nombre de marca asignado a la aplicación de software RSLogix 5000, y continuará siendo el producto para programar los controladores Logix5000™ en soluciones discretas, de procesos, de lotes, de control de movimiento, de seguridad y basadas en variadores.

El ambiente Studio 5000 constituye la base para las futuras herramientas y capacidades de diseño de ingeniería de Rockwell Automation®. El ambiente Studio 5000 es el lugar donde los ingenieros de diseño desarrollan todos los elementos de sus sistemas de control.

Terminología

La siguiente tabla define los términos utilizados en este manual.

Tabla 2 – Términos y definiciones

Abreviatura	Significado de las siglas	Definición
1oo2	Uno de dos	Se refiere al diseño del comportamiento de un sistema de seguridad con varios procesadores.
CIP	Protocolo industrial común	Protocolo de comunicación diseñado para aplicaciones industriales de automatización.
CIP Safety	Protocolo industrial común – Certificado para seguridad	Versión de CIP con clasificación SIL 3/PLe.
DC	Cobertura del diagnóstico	Relación entre la tasa de fallos detectados y la tasa total de fallos.
EN	Normativa europea	Estándar oficial europeo.
ESM	Módulo de almacenamiento de energía	Usado para alimentación del reloj y respaldo para retener los datos en la memoria mientras los controladores GuardLogix 5570 están apagados.
GSV	Get System Value	Una instrucción que obtiene información sobre el estado del controlador especificado y la pone en un tag de destino.
—	Multidifusión	La transmisión de información de un transmisor a múltiples receptores.
NAT	Traducción de direcciones de red	La traducción de una dirección de protocolo de Internet (IP) a otra dirección IP de una red diferente.
PFD	Probabilidad de fallo a demanda	Probabilidad promedio de que un sistema no realice la función a demanda para la que está diseñado.
PFH	Probabilidad de fallo por hora	Probabilidad de que un sistema experimente un fallo peligroso por hora.
PL	Nivel de rendimiento	Clasificación de seguridad ISO 13849-1.
RPI	Intervalo solicitado entre paquetes	El período de tiempo esperado de producción de datos durante la comunicación a través de una red.
SNN	Número de red de seguridad	Número único que identifica una sección de una red de seguridad .
SSV	Set System Value	Una instrucción que establece datos en el sistema controlador.
—	Estándar	Objeto, tarea, tag, programa o componente en su proyecto que no es un ítem relacionado con la seguridad.
—	Unidifusión	La transmisión de información de un transmisor a un receptor.

Para obtener más información

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

Tabla 3 – Publicaciones relacionadas con los controladores y sistemas GuardLogix

Recurso		Descripción
Requisitos de las aplicaciones de seguridad	Sistemas controladores GuardLogix 5570 – Manual de referencia de seguridad, publicación 1756-RM099	Contiene los requisitos detallados para obtener y mantener SIL 3/PLe con el sistema controlador GuardLogix.5570 usando la aplicación Studio 5000 Logix Designer.
	Sistemas controladores GuardLogix – Manual de referencia de seguridad, publicación 1756-RM093	Contiene los requisitos detallados para obtener y mantener SIL 3/PLe con el sistema controlador GuardLogix 5560 o 5570 usando el software RSLogix 5000.
CIP Sync (sincronización de tiempo)	Integrated Architecture® and CIP Sync Configuration Application Technique, publicación IA-AT003	Proporciona información detallada y completa sobre cómo aplicar la tecnología CIP Sync para sincronizar relojes en un sistema de control Logix.
Módulos Guard I/O™	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.
	Guard I/O EtherNet/IP Safety Modules User Manual, publicación 1791ES-UM001	Proporciona información sobre cómo usar los módulos de seguridad Guard I/O EtherNet/IP.
	Módulos de seguridad POINT Guard I/O™ – Manual del usuario, publicación 1734-UM013	Proporciona información sobre cómo instalar, configurar y usar los módulos POINT Guard I/O.
	Controlador Armor GuardLogix – Instrucciones de instalación, publicación 1756-IN060	Proporciona información sobre cómo instalar y usar los controladores Armor GuardLogix.

Tabla 3 – Publicaciones relacionadas con los controladores y sistemas GuardLogix (continuación)

Recurso		Descripción
Variadores	Servovariadores Kinetix 5500 – Manual del usuario, publicación 2198-UM001	Proporciona información sobre cómo instalar, configurar, poner en marcha y resolver los problemas de un sistema de servovariadores Kinetix 5500. También incluye los requisitos para utilizar variadores Kinetix 5500 en aplicaciones de seguridad.
	Manual del usuario de los servovariadores Kinetix 5700, publicación 2198-UM002	Proporciona información sobre cómo instalar, configurar, poner en marcha y resolver los problemas de un sistema de servovariadores Kinetix 5700. También incluye los requisitos para utilizar variadores Kinetix 5700 en aplicaciones de seguridad.
	PowerFlex 527 Adjustable Frequency AC Drive User Manual, publicación 520-UM002	Proporciona información sobre cómo instalar, poner en marcha y resolver los problemas del variador de CA de frecuencia ajustable PowerFlex serie 520.
Instalación del hardware	Chasis y fuente de alimentación eléctrica ControlLogix® – Instrucciones de instalación, publicación 1756-IN005	Describe cómo instalar y conectar a tierra el chasis y las fuentes de alimentación eléctrica ControlLogix.
	Pautas de cableado y conexión a tierra de equipos de automatización industrial, publicación 1770-4.1	Proporciona información detallada sobre cómo conectar a tierra y cablear los controladores programables.
Instrucciones (programación)	GuardLogix Safety Application Instruction Set Reference Manual, publicación 1756-RM095	Proporciona información acerca del conjunto de instrucciones de las aplicaciones de GuardLogix Safety.
	Instrucciones generales de los controladores Logix5000 – Manual de referencia, publicación 1756-RM003	Proporciona a los programadores detalles acerca de cada instrucción disponible para un controlador Logix5000.
	Logix5000 Controllers Motion Instructions Reference Manual, publicación MOTION-RM002	Proporciona a los programadores detalles acerca de las instrucciones de control de movimiento que se encuentran disponibles para un controlador Logix5000.
Movimiento	Sercos Motion Configuration and Startup User Manual, publicación MOTION-UM001	Detalla cómo configurar un sistema de aplicación de movimiento SERCOS.
	Motion Coordinated Systems User Manual, publicación MOTION-UM002	Detalla cómo crear y configurar un sistema de aplicación de movimiento coordinado.
	Configuración y puesta en marcha del movimiento integrado en la red EtherNet/IP – Manual del usuario, publicación MOTION-UM003	Detalla cómo configurar un control de movimiento integrado en un sistema de aplicación de redes EtherNet/IP.
	Integrated Motion on the EtherNet/IP Network Reference Manual, publicación MOTION-RM003	Información detallada sobre modos de control de ejes y atributos para movimiento integrado en redes EtherNet/IP.
Redes (ControlNet™, DeviceNet, EtherNet/IP)	EtherNet/IP Modules in Logix5000 Control Systems User Manual, publicación ENET-UM001	Describe cómo configurar y operar módulos EtherNet/IP en un sistema de control Logix5000.
	ControlNet Modules in Logix5000 Control Systems User Manual, publicación CNET-UM001	Describe cómo configurar y operar módulos ControlNet en un sistema de control Logix5000.
	DeviceNet Modules in Logix5000 Control Systems User Manual, publicación DNET-UM004	Describe cómo configurar y operar módulos DeviceNet en un sistema de control Logix5000.
PhaseManager™	PhaseManager User Manual, publicación LOGIX-UM001	Proporciona pasos, guía y ejemplos sobre cómo configurar y programar un controlador Logix5000 para usar fases de equipos.
Tareas y procedimientos de programación	Logix5000 Controllers Common Procedures Programming Manual, publicación 1756-PM001	Proporciona acceso al conjunto de manuales de programación de los controladores Logix5000, los cuales incluyen temas de administración de archivos de proyecto, organización de tags, programación de lógica, rutinas de prueba, manejo de fallos y más.
	Logix5000 Controllers Execution Time and Memory Use Reference Manual, publicación 1756-RM087	Proporciona ayuda sobre cómo calcular el uso de memoria y el tiempo de ejecución de la lógica programada, y cómo seleccionar las diferentes opciones de programación.

Puede ver o descargar publicaciones en http://www.rockwellautomation.com/literature. Para solicitar copias impresas de la documentación técnica, comuníquese con el distribuidor de Allen-Bradley® o representante de ventas de Rockwell Automation correspondiente a su localidad.

Descripción general del sistema

Requisitos de las aplicaciones de seguridad

El sistema controlador GuardLogix 5570 está certificado para uso en aplicaciones de seguridad hasta el límite de declaración de nivel de integridad de seguridad (SIL CL) 3 y el nivel de rendimiento (e), en las que el estado de seguridad es el estado desenergizado. Entre los requisitos de las aplicaciones de seguridad se incluyen la evaluación de la probabilidad de tasas de fallo, como:

- Probabilidad de fallo a demanda (PFD)
- Probabilidad de fallo por hora (PFH)
- Ajustes del tiempo de reacción del sistema
- Pruebas de verificación de funcionamiento que cumplen con los criterios de SIL 3/PLe.

Las aplicaciones de seguridad SIL 3/PLe basadas en GuardLogix requieren que use como mínimo un número de red de seguridad (SNN) y una firma de tarea de seguridad. Ambos repercuten en la configuración del controlador y de E/S, y en las comunicaciones de red.

En cuanto a los requisitos del sistema de seguridad SIL 3 y PLe, incluidos los intervalos de prueba de validación, el tiempo de reacción del sistema y los cálculos de probabilidad de fallo a demanda/probabilidad de fallo por hora, consulte el manual de referencia de seguridad de los sistemas controladores GuardLogix 5570, publicación 1756-RM099. Es necesario leer, comprender y completar estos requisitos antes de utilizar un sistema de seguridad SIL 3, PLe GuardLogix.

Número de red de seguridad

El número de red de seguridad (SNN) debe ser un número único que identifique las subredes de seguridad. Cada subred de seguridad que el controlador usa para la comunicación de seguridad debe tener un SNN único. Cada dispositivo de E/S de seguridad también debe configurarse con el SNN de la subred de seguridad. El SNN se puede asignar manual o automáticamente.

Para obtener información sobre cómo asignar el SNN, vea Administración del número de red de seguridad (SNN) en la página 47.

Firma de tarea de seguridad

La firma de tarea de seguridad está compuesta por un número de identificación, la fecha y la hora, información esta que identifica de forma única la porción de seguridad de un proyecto. Esta firma incluye la configuración, los datos y la lógica de seguridad. El sistema GuardLogix utiliza la firma de tarea de seguridad para determinar la integridad del proyecto y para permitirle comprobar si se ha descargado el proyecto correcto al controlador de destino. La capacidad de crear, grabar y comprobar la firma de tarea de seguridad es una parte obligatoria del proceso de desarrollo de aplicaciones de seguridad.

Vea Generación de una firma de tarea de seguridad en la página 102 para obtener más información.

Diferenciacióntre componentes estándar y de seguridad

Las ranuras del chasis de un sistema GuardLogix que no utiliza la función de seguridad pueden ser ocupadas por otros módulos ControlLogix certificados según las directivas de compatibilidad electromagnética (EMC) y de bajo voltaje. Vea http://www.rockwellautomation.com/rockwellautomation/certification/ce.page para encontrar la certificación CE de la familia de productos ControlLogix de control programable y determinar qué módulos están certificados.

Usted debe crear y documentar una diferenciación clara, lógica y visible entre la porción estándar y la porción de seguridad del proyecto del controlador. Como parte de esta diferenciación, la aplicación Logix Designer cuenta con iconos de identificación de seguridad que identifican la tarea de seguridad, los programas de seguridad, las rutinas de seguridad y los componentes de seguridad. Además, la aplicación Logix Designer utiliza un atributo de clase de seguridad que se muestra cada vez que se ven en pantalla propiedades de una tarea de seguridad, de programas de seguridad, de una rutina de seguridad, de un tag de seguridad o de la instrucción Add-On de seguridad.

El controlador no permite escribir en los datos de tag de seguridad desde dispositivos de interface operador-máquina (HMI) externos, ni mediante instrucciones de mensajes de otros controladores homólogos. La aplicación Logix Designer puede escribir tags de seguridad cuando el controlador GuardLogix está en desbloqueo de seguridad, no tiene firma de tarea de seguridad y se encuentra en funcionamiento sin fallos de seguridad.

El manual del usuario de los controladores ControlLogix, publicación 1756-UM001, contiene información acerca de la utilización de dispositivos ControlLogix en aplicaciones estándar (no de seguridad).

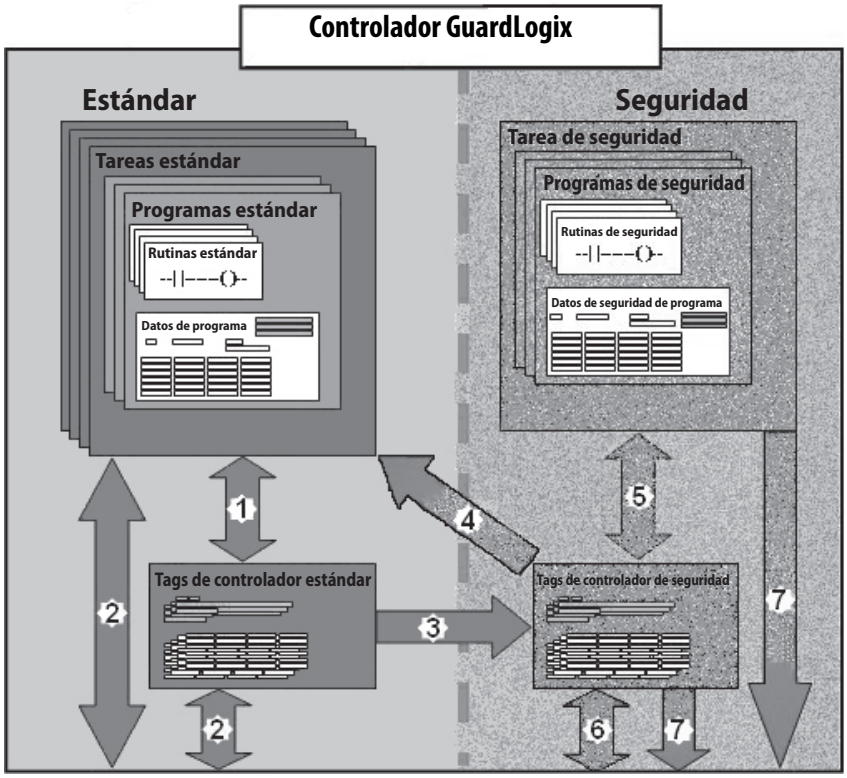
Dispositivos de HMI

Con los controladores GuardLogix se pueden utilizar dispositivos de interface de operador máquina (HMI). Los dispositivos de HMI pueden obtener acceso a tags estándar igual que cualquier otro controlador estándar. Sin embargo, los dispositivos de HMI no pueden escribir en tags de seguridad; los tags de seguridad son de solo lectura para los dispositivos de HMI.

Capacidades de flujo de datos del controlador

Esta ilustración explica las capacidades de flujo de datos estándar y de seguridad del controlador GuardLogix.

Figura 1 – Capacidades de flujo de datos



Nº	Descripción
1	La lógica y los tags estándar se comportan de la misma manera que en la plataforma Logix estándar.
2	Los datos de tags estándar, bajo el control del programa o del controlador, pueden intercambiarse con dispositivos de HMI externos, computadoras personales y otros controladores.
3	Los controladores GuardLogix son controladores integrados con la capacidad de mover (asignar) datos de tags estándar a tags de seguridad para uso dentro de la tarea de seguridad.
	ATENCIÓN: Estos datos no deben usarse para controlar directamente una salida SIL 3/PLe.
4	Los tags de seguridad bajo el control del controlador pueden ser leídos directamente por la lógica estándar.
5	Los tags de seguridad pueden ser leídos o escritos por la lógica de seguridad.
6	Los tags de seguridad pueden intercambiarse entre controladores de seguridad a través de redes Ethernet o ControlNet, incluso los controladores GuardLogix 1756 y 1768.
7	Los datos de tags de seguridad, bajo el control del programa o del controlador, pueden ser leídos por dispositivos externos tales como dispositivos de HMI, computadoras personales u otros controladores estándar.
	IMPORTANTE Una vez que los datos se leen, se consideran datos estándar, no datos SIL 3/PLe.

Selección del hardware del sistema

El sistema GuardLogix es compatible con aplicaciones de seguridad SIL 3 y PLe. El controlador GuardLogix se compone de un controlador primario y un homólogo de seguridad que funcionan juntos en una arquitectura 1oo2. La Tabla 4 indica los números de catálogo de los controladores primarios y los homólogos de seguridad.

El homólogo de seguridad debe instalarse en la ranura que se encuentra justo a la derecha del controlador primario. Las revisiones mayores y menores de firmware del controlador primario y del homólogo de seguridad deben coincidir exactamente para poder establecer la asociación de control necesaria para aplicaciones de seguridad.

Tabla 4 – Números de catálogo del controlador primario y el correspondiente homólogo de seguridad

Controlador primario	Homólogo de seguridad
1756-L71S, 1756-L72S, 1756-L73S	1756-L7SP
1756-L73SXT	1756-L7SPXT

Controlador primario

El controlador primario es el procesador que realiza funciones 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. Las funciones estándar incluyen las siguientes:

- Control de E/S
- Lógica
- Temporización
- Conteo
- Generación de informes
- Comunicación
- Cálculos aritméticos
- Manejo de archivos de datos

El controlador primario consta de un procesador central, interface de E/S y memoria.

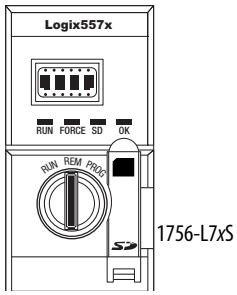
Tabla 5 – Capacidad de memoria

Nº cat.	Memoria de usuario (capacidad de RAM)	
	Componentes y tareas estándar	Componentes y tareas de seguridad
1756-L71S	2 MB	1 MB
1756-L72S	4 MB	2 MB
1756-L73S,1756-L73SXT	8 MB	4 MB

Un interruptor de llave de tres posiciones situado en la parte frontal del controlador primario gobierna los modos de funcionamiento del controlador. Se pueden seleccionar los modos siguientes:

- RUN
- PROGram
- REMote: este modo habilitado por software puede ser Program (programa), Run (marcha) o Test (prueba).

Figura 2 – Posiciones del interruptor de llave



Homólogo de seguridad

El homólogo de seguridad es un coprocesador que proporciona un segundo canal aislado (redundancia) para las funciones relacionadas con la seguridad en el sistema.

El homólogo de seguridad no tiene interruptor de llave ni puerto de comunicación. Su configuración y su operación son controladas por el controlador primario.

Chasis

El chasis ControlLogix proporciona las conexiones físicas entre los módulos y el controlador GuardLogix.

Fuente de alimentación eléctrica

Las fuentes de alimentación eléctrica ControlLogix indicadas en la página 25 son adecuadas para uso en aplicaciones SIL 3. Para utilizar las fuentes de alimentación eléctrica en el nivel SIL 3 no se necesita configuración ni cableado adicionales.

Selección del dispositivo de E/S de seguridad

Los dispositivos de entrada y salida de seguridad, como sensores y accionadores, pueden conectarse a E/S de seguridad en redes DeviceNet o EtherNet/IP. Esta conexión permite a un sistema controlador GuardLogix controlar dispositivos de salida a través de comunicación DeviceNet o EtherNet/IP.

Para obtener la información más actualizada sobre números de catálogo de E/S de seguridad, series certificadas y revisiones de firmware disponibles, consulte los certificados de seguridad en http://www.rockwellautomation.com/rockwellautomation/certification/safety.page.

Selección de las redes de comunicación

El controlador GuardLogix es compatible con comunicaciones que le permiten:

- Distribuir y controlar E/S de seguridad a través de redes DeviceNet o EtherNet/IP
- Distribuir y controlar E/S de seguridad remotas a través de redes DeviceNet, EtherNet/IP o ControlNet
- Producir y consumir datos de tags de seguridad entre controladores GuardLogix 1756 y 1768 distribuidos por todas las redes EtherNet/IP o ControlNet, o dentro del mismo chasis ControlLogix
- Distribuir y controlar E/S estándar a través de redes Ethernet, ControlNet o DeviceNet

Use estos módulos de comunicación para proporcionar una interface entre controladores GuardLogix y dispositivos de redes.

Tabla 6 – Módulos de comunicación

Para servir de interface entre	Use este módulo	Consulte estas instrucciones de instalación
El controlador GuardLogix y los dispositivos DeviceNet	1756-DNB	DNET-IN001
El controlador GuardLogix y los dispositivos EtherNet/IP	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR 1756-EN3TR 1756-EN2TXT 1756-EN2TRXT	ENET-IN002
Controladores en la red ControlNet	1756-CN2 1756-CN2R 1756-CN2RXT	CNET-IN005

El controlador GuardLogix puede conectarse a la aplicación Logix Designer mediante un puerto USB, un módulo Ethernet o un módulo ControlNet.

Consulte Para obtener más información en la página 11 para obtener más información sobre los módulos de comunicación de redes.

Requisitos de programación

Use la Tabla 7 para identificar la herramienta de programación y las versiones que se utilizan con los controladores GuardLogix 5570.

Tabla 7 – Versiones de software

Nº cat.	Ambiente Studio 5000	Versión de software RSLogix 5000(1)	Versión de software RSLinx® Classic
1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT	21 o posterior	20 o posterior	2.59 o posterior

(1) Para obtener información sobre cómo usar un controlador GuardLogix con el software RSLogix 5000, consulte el manual del usuario de los controladores GuardLogix, publicación 1756-UM020, y el documento GuardLogix Controller Systems Safety Reference Manual, publicación 1756-RM093.

Las rutinas de seguridad incluyen instrucciones de seguridad, las cuales constituyen un subconjunto del conjunto de instrucciones de lógica de escalera estándar, y de las instrucciones de las aplicaciones de seguridad. Los programas que se han programado bajo la tarea de seguridad son compatibles solamente con lógica de escalera.

Tabla 8 – Características compatibles

Característica	Aplicación Studio 5000 Logix Designer Versiones 24 y posteriores	
	Tarea de seguridad	Tarea estándar
Instrucciones Add-On	X	X
Alarmas y eventos		
Registro del controlador	X	
Control de acceso a datos		
Rutinas de fase de equipo		
Tareas de eventos		
Supervisor de firmware	X	
Diagramas de bloques de funciones (FBD)		
Movimiento integrado		
Lógica de escalera	X	
Cambio de idioma		
Tarjeta de memoria		
Traducción de direcciones de redes (NAT)		
Importación y exportación en línea de componentes del programa		
Conexiones de seguridad y estándar	X	
Rutinas de diagrama de funciones secuenciales (SFC)		
Texto estructurado		
Conexiones de unidifusión para tags de seguridad producidos y consumidos	X	
Conexiones de unidifusión para dispositivos de E/S de seguridad en redes EtherNet/IP		

Para obtener información acerca de cómo usar estas características, consulte el documento Logix5000 Controllers Common Procedures Programming Manual, publicación 1756-PM001, las publicaciones listadas en la sección Para obtener más información en la página 11 y la ayuda en línea.

Notas:

Instalación del controlador

Precauciones

Lea y tome estas precauciones durante el uso del producto.

Información sobre el ambiente y el envolvente

ATENCIÓN: Este equipo se ha diseñado para uso en un ambiente industrial con un grado de contaminación 2, en aplicaciones de sobrevoltajes de categoría II (según se define en la norma IEC 60664-1), a altitudes de hasta 2000 m (6562 pies) sin reducción del régimen nominal.

Este equipo no se ha diseñado para uso en ambientes residenciales y es posible que no ofrezca la protección adecuada para servicios de radiocomunicación en estos ambientes.

Este equipo se suministra como equipo de tipo abierto. Debe montarse dentro de un envolvente diseñado adecuadamente para las condiciones ambientales específicas y para ayudar a evitar lesiones ocasionadas por el acceso a piezas energizadas. El envolvente debe tener las propiedades retardadoras de llama adecuadas para ayudar a evitar o a minimizar la propagación de llamas, y así cumplir con una clasificación de dispersión de llamas de 5VA, V o estar aprobado para la aplicación si no fuese metálico. El interior del envolvente debe ser accesible solo por medio de una herramienta. Las secciones posteriores de esta publicación pueden contener información adicional respecto a las especificaciones sobre tipos de envolvente requeridas para cumplir con determinadas certificaciones de seguridad de productos.

Además de esta publicación, consulte las publicaciones siguientes para obtener más información:

- Pautas de cableado y conexión a tierra de equipos de automatización industrial, publicación 1770-4.1, para obtener información sobre requisitos de instalación adicionales.
- Normas NEMA 250 e IEC 60529, según correspondan, en lo que respecta a las explicaciones sobre los grados de protección que brindan los envolventes

Sistemas electrónicos programables (PES)

ATENCIÓN: El personal responsable de la aplicación de los sistemas electrónicos programables (PES) relacionados con la seguridad deben conocer los requisitos de seguridad en la aplicación del sistema y haber recibido capacitación en el uso del sistema.

Desconexión y reconexión con la alimentación conectada (RIUP)

ADVERTENCIA: Al introducir o retirar el módulo cuando la alimentación del backplane está conectada se puede producir un arco eléctrico. Esto podría provocar una explosión en zonas peligrosas.

Antes de seguir adelante, asegúrese de desconectar la alimentación eléctrica o de verificar que la zona no sea peligrosa. La recurrencia de arcos eléctricos puede provocar desgaste excesivo en los contactos tanto del módulo como del conector de acoplamiento. Los contactos desgastados podrían ofrecer resistencia eléctrica lo cual puede afectar el funcionamiento del módulo.

Aprobación legal norteamericana para uso en zonas peligrosas

The following information applies when operating this equipment in hazardous locations.	**La siguiente información se aplica cuando este equipo se pone en funcionamiento en zonas peligrosas:**
Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	Los productos con las marcas "CL I, DIV 2, GP A, B, C, D" son adecuados para uso exclusivamente en zonas peligrosas Clase I, División 2, Grupos A, B, C, D, así como en zonas no peligrosas. Cada producto se suministra con marcas en la placa del fabricante que indican el código de temperatura para zonas peligrosas. Si se combinan productos en un sistema, se puede utilizar el código de temperatura más desfavorable (número "T" más bajo) para facilitar la determinación del código de temperatura general del sistema. Las combinaciones de equipos en el sistema están sujetas a investigación por parte de la autoridad local con jurisdicción en el momento de instalación.
WARNING: EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**ADVERTENCIA:** PELIGRO DE EXPLOSIÓN • No desconecte el equipo a menos de que se haya desconectado la alimentación eléctrica o se sepa que la zona no peligrosa. • No desconecte las conexiones a este equipo a menos de que se haya desconectado la alimentación eléctrica o la zona se considere no peligrosa. Sujete bien las conexiones externas de empalme con este equipo mediante tornillos, seguros deslizantes, conectores roscados u otros medios proporcionados con este producto. • La sustitución de componentes podría afectar la idoneidad para la Clase I, División 2. • Si el producto contiene baterías, estas solo deben cambiarse en una zona que se sepa no es peligrosa.

Aprobación legal europea para ubicación en zonas peligrosas

Los siguientes puntos se aplican cuando el producto tiene la marca Ex.

Este equipo se ha diseñado para su uso en atmósferas potencialmente explosivas, de acuerdo con la Directiva 94/9/EC de la Unión Europea, y cumple los requisitos esenciales de salud y seguridad relativos al diseño y construcción de equipos de Categoría 3 aptos para su uso en atmósferas potencialmente explosivas de Zona 2, según se establece en el anexo II de esta directiva.

La conformidad con los requisitos esenciales de salud y seguridad está garantizada mediante la conformidad con EN 60079-15 y EN 60079-0.

ATENCIÓN: Este equipo no es resistente a la luz solar ni a otras fuentes de radiación UV.

ADVERTENCIA: Siga estas pautas para montar y utilizar el equipo:

- Este equipo se debe montar en un envolvente con certificación ATEX y clasificación de protección contra ingreso IP54 como mínimo (según se define en IEC60529) y debe utilizarse en un ambiente con un grado de contaminación 2 como máximo (según se define en IEC 60664-1) cuando se incorpore en ambientes de Zona 2. El envolvente debe utilizar una cubierta o puerta desmontable mediante herramientas.
- Debe utilizarse dentro de las clasificaciones establecidas por Rockwell Automation.
- Debe usarse solo con backplanes de Rockwell Automation con certificación ATEX.
- No lo desconecte, a menos que se haya desconectado la alimentación eléctrica o que esté seguro que la zona no es peligrosa.

Tome las medidas para evitar que el voltaje nominal exceda perturbaciones transientes mayores al 140% del voltaje nominal al utilizarse en ambientes de Zona 2.

Sujete bien las conexiones externas de empalme con este equipo mediante tornillos, seguros deslizantes, conectores roscados u otros medios proporcionados con este equipo.

Prevención de descargas electroestáticas

ATENCIÓN: Este equipo es sensible a las descargas electrostáticas, lo que puede provocar daños internos y alterar el funcionamiento normal. Siga estas pautas al manipular el equipo:

- Toque un objeto que esté conectado a tierra para descargar el potencial electrostático de su cuerpo.
- Use una muñequera de puesta a tierra aprobada.
- No toque los conectores ni los pines de las tarjetas de componentes.
- No toque los componentes del circuito dentro del equipo.
- Utilice una estación de trabajo con protección contra estática, si está disponible.
- Cuando no vaya a usarlo, guarde el equipo en un envoltorio adecuado con protección contra descargas electrostáticas.

Asegúrese de que tiene todos los componentes

Antes de comenzar, asegúrese de que tiene todos los componentes necesarios.

IMPORTANTE Deberá usar un controlador primario **y** un homólogo de seguridad para cumplir con las especificaciones SIL 3/PLe.

Estas piezas se incluyen con el controlador primario y el homólogo de seguridad.

Nº cat.	Descripción	Se envía con
1756-L71S 1756-L72S 1756-L73S	Controlador primario	• Módulo de almacenamiento de energía (ESM) basado en condensador 1756-ESMCAP • Tarjeta de memoria SD 1784-SD, 1 GB • Llave 1747-KY
1756-L7SP	Homólogo de seguridad	• Módulo de almacenamiento de energía (ESM) 1756-SPESMNSE
1756-L73SXT	Controlador primario para temperaturas extremas	• Módulo de almacenamiento de energía (ESM) basado en condensador 1756-ESMCAPXT • Llave 1747-KY
1756-L7SPXT	Homólogo de seguridad para temperaturas extremas	• Módulo de almacenamiento de energía (ESM) basado en condensador 1756-SPESMNSEXT

Puede usarse el siguiente equipo opcional.

Si la aplicación requiere	Use esta pieza
Memoria no volátil	1784-SD1 (1 GB) o 1784-SD2 (2 GB)
Que el ESM instalado descargue su energía residual almacenada a 200 µJ o menos antes de transportarlo a su aplicación o fuera de ella(1)	1756-ESMNSE para el controlador primario 1756-SPESMNSE para el homólogo de seguridad(2) Este ESM no tiene alimentación eléctrica de respaldo WallClockTime. Además, solo puede usar este ESM con un controlador 1756-L73S (8 MB) o uno con menor memoria.
ESM que protege el controlador evitando el uso del puerto USB y la tarjeta SD(1)	1756-ESMNRM para el controlador primario 1756-SPESMNRM para el homólogo de seguridad(3) Este ESM proporciona a su aplicación un mayor grado de protección.

(1) Para obtener información acerca del tiempo de retención de los EMS, consulte la sección Cálculo del apoyo de ESM de WallClockTime en la página 118.

(2) Para el controlador primario de temperaturas extremas y el homólogo de seguridad use el 1756-ESMNSEXT y el 1756-SPESMNSEXT, respectivamente.

(3) Si se necesita usar el controlador primario y el homólogo de seguridad para temperaturas extremas, use el 1756-ESMNRMXT y el 1756-SPESMNRMXT, respectivamente.

Instalación de un chasis y una fuente de alimentación eléctrica

Antes de instalar un controlador, necesita instalar un chasis y una fuente de alimentación eléctrica.

1. Instale un chasis ControlLogix según las instrucciones de instalación correspondientes.

Nº cat.	Ranuras disponibles	Serie	Consulte estas instrucciones de instalación
1756-A4	4	B	1756-IN005
1756-A7	7		
1756-A10	10		
1756-A13	13		
1756-A17	17		
1756-A4LXT	4	B	
1756-A5XT	5	B	
1756-A7XT	7	B	
1756-A7LXT	7	B	

Los controladores para ambientes difíciles (XT) requieren un chasis XT.

2. Instale una fuente de alimentación eléctrica ControlLogix según las instrucciones de instalación correspondientes.

Nº cat.	Descripción	Serie	Consulte estas instrucciones de instalación
1756-PA72	Fuente de alimentación eléctrica, CA	C	1756-IN005
1756-PB72	Fuente de alimentación eléctrica, CC		
1756-PA75	Fuente de alimentación eléctrica, CA	B	
1756-PB75	Fuente de alimentación eléctrica, CC		
1756-PAXT	Fuente de alimentación eléctrica XT, CA	B	
1756-PBXT	Fuente de alimentación eléctrica XT, CC		

Los controladores para ambientes difíciles (XT) requieren una fuente de alimentación eléctrica XT.

Instale el controlador en el chasis

Puede instalar o retirar un controlador con alimentación aplicada y el sistema en funcionamiento.

ADVERTENCIA: Al introducir o retirar el módulo con la alimentación del backplane conectada se puede producir un arco eléctrico. Esto podría provocar una explosión en zonas peligrosas.

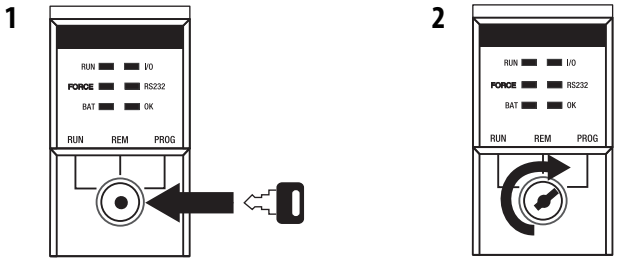
Antes de seguir adelante, asegúrese de desconectar la alimentación eléctrica o de verificar que la zona no sea peligrosa. La recurrencia de arcos eléctricos puede provocar desgaste excesivo en los contactos tanto del módulo como del conector de acoplamiento. Los contactos desgastados pueden ofrecer resistencia eléctrica lo cual puede afectar el funcionamiento del módulo.

IMPORTANTE El ESM comienza a cargarse cuando se da alguna de las siguientes condiciones:

- El controlador y el ESM están instalados en un chasis energizado.
- Está conectada la alimentación eléctrica al chasis que contiene un controlador con el ESM instalado.
- Está instalado un ESM en un controlador energizado.

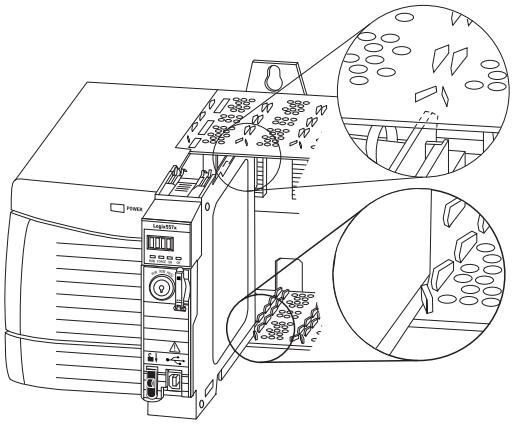
Cuando se conecta la alimentación eléctrica, el ESM se carga durante un máximo de dos minutos, lo cual se indica en la pantalla de estado mediante CHRG o ESM Charging.

1. Inserte la llave en el controlador primario.
2. Gire la llave hasta la posición PROG.



El homólogo de seguridad no tiene interruptor de llave.

3. Alinee la tarjeta de circuitos con las guías inferior y superior del chasis.



4. Inserte el controlador en el chasis.

   El controlador está completamente instalado cuando se encuentra a ras con la fuente de alimentación eléctrica u otros módulos instalados, y los seguros superior e inferior están enganchados.

IMPORTANTE Debe instalar el homólogo de seguridad en la ranura que se encuentra justo a la derecha del controlador primario. Siga los pasos 3 y 4 antes descritos para instalar el homólogo de seguridad.

Después de insertar el controlador en el chasis, consulte el Capítulo 9 para obtener información sobre cómo interpretar los indicadores de estado en el controlador primario y en el homólogo de seguridad.

Inserción o extracción de una tarjeta de memoria

ADVERTENCIA: Cuando se inserta o se retira la tarjeta de memoria con la alimentación eléctrica conectada, puede producirse un arco eléctrico. Esto podría provocar una explosión en instalaciones ubicadas en zonas peligrosas. Antes de seguir adelante, asegúrese de desconectar la alimentación eléctrica o de verificar que la zona no sea peligrosa.

ATENCIÓN: Si **no** conoce con exactitud el contenido de la tarjeta de memoria, **antes** de instalar la tarjeta, mueva el interruptor de llave del controlador a la posición PROG. Según el contenido de la tarjeta, al desconectar y volver a conectar la alimentación eléctrica o al producise un fallo la tarjeta podría cargar un sistema operativo o un proyecto diferente en el controlador.

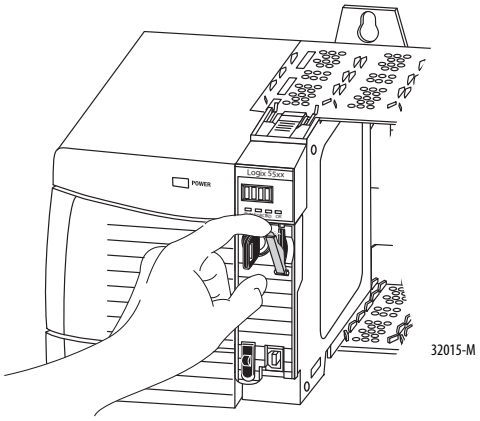
El controlador se envía con una tarjeta SD instalada. Recomendamos que deje una tarjeta SD instalada.

Extracción de la tarjeta SD

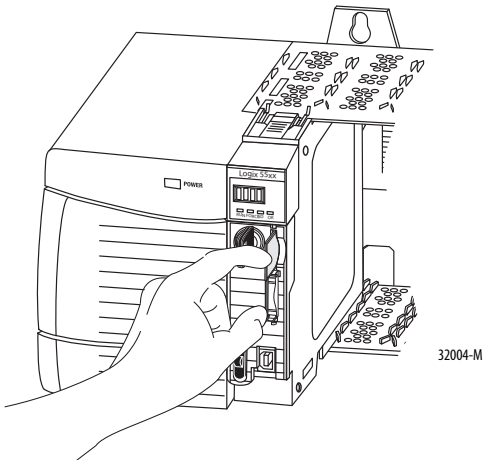
Siga estos pasos para retirar la tarjeta SD.

IMPORTANTE Verifique que el indicador de estado de la tarjeta SD esté apagado y que la tarjeta no esté en uso antes de sacarla.

1. Gire el interruptor de llave hasta la posición PROG.
2. Abra la puerta para obtener acceso a la tarjeta SD.



3. Presione y suelte la tarjeta SD para expulsarla.

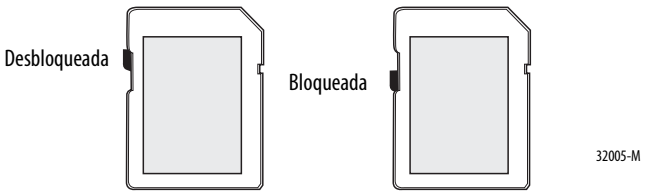


4. Retire la tarjeta SD y cierre la puerta.

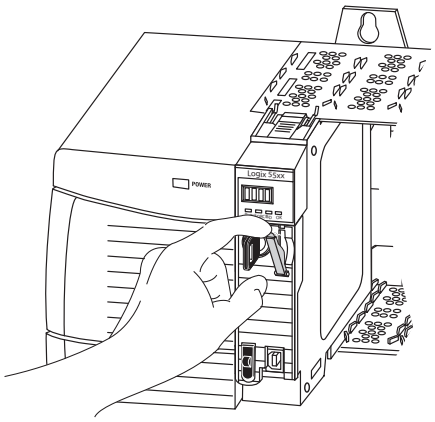
Instale la tarjeta SD

Siga estos pasos para instalar la tarjeta SD.

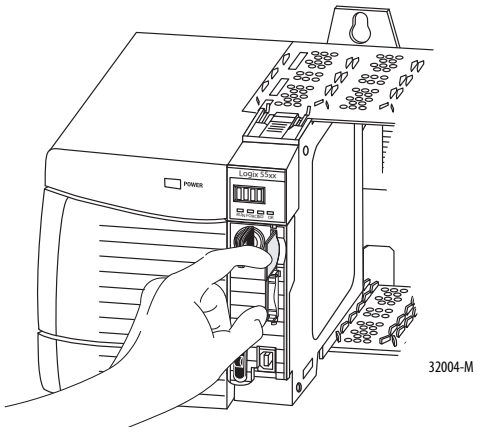
1. Verifique que la tarjeta SD esté bloqueada o desbloqueada, según su preferencia.



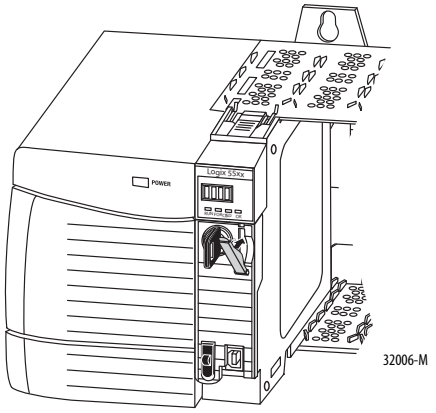
2. Abra la puerta de la tarjeta SD.



3. Inserte la tarjeta SD en la ranura para tarjeta SD.
4. Presione suavemente la tarjeta hasta que encaje en su lugar.



5. Cierre la puerta de la tarjeta SD.



Establecimiento de las conexiones de comunicación

El controlador tiene un puerto USB que utiliza un receptáculo tipo B. La conexión es compatible con USB 2.0-y opera a 12 M.

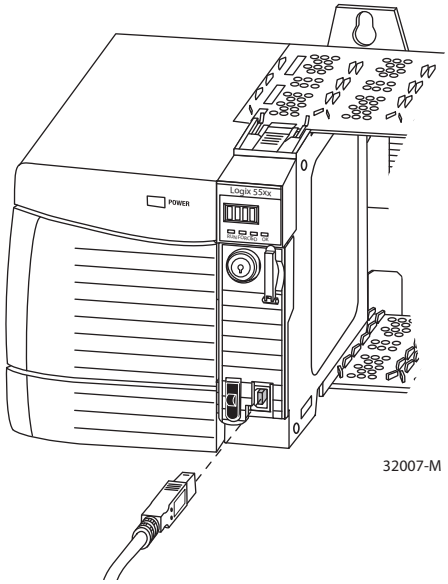
Para usar el puerto USB del controlador, debe tener instalado en su estación de trabajo el software RSLinx, versión 2.59 o posterior. Use un cable USB para conectar su estación de trabajo al puerto USB. Con esta conexión es posible actualizar el firmware y descargar programas al controlador directamente desde su estación de trabajo.

ATENCIÓN: Utilice el puerto USB para fines de programación local temporal. No utilice el puerto USB como una conexión permanente.

El cable USB no debe medir más de 3.0 m (9.84 pies) y no debe contener concentradores.

ADVERTENCIA: No utilice el puerto USB en zonas peligrosas.

Figura 3 – Puerto USB



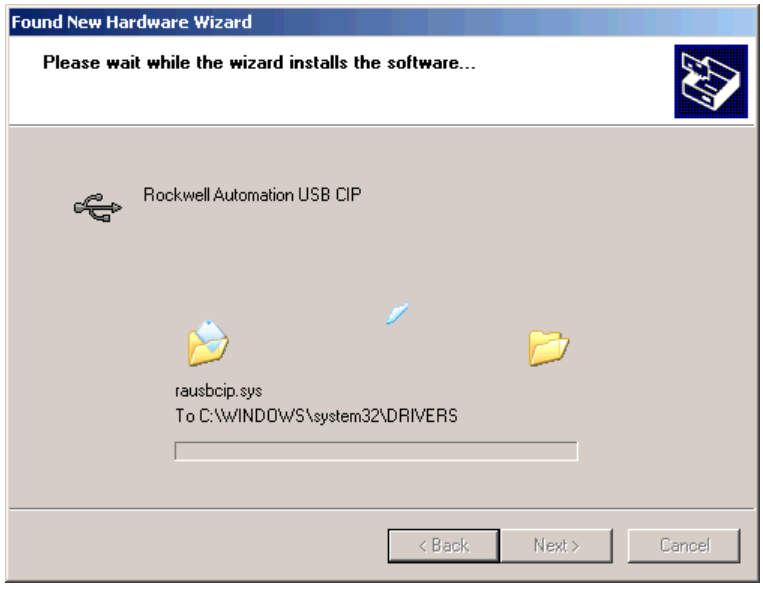
Para configurar el software RSLinx a fin de usar un puerto USB, primero debe configurar un driver USB. Para configurar un driver USB, realice este procedimiento.

1. Conecte el controlador y la estación de trabajo mediante un cable USB.
2. En el cuadro de diálogo Found New Hardware Wizard, haga clic en cualquiera de las opciones de conexión de Windows Update y haga clic en Next.

SUGERENCIA Si no se encuentra el software para el driver USB y se cancela la instalación, verifique que tiene instalado el software RSLinx Classic, versión 2.59 o posterior.

3. Haga clic en Install the software automatically (Recommended) y haga clic en Next.

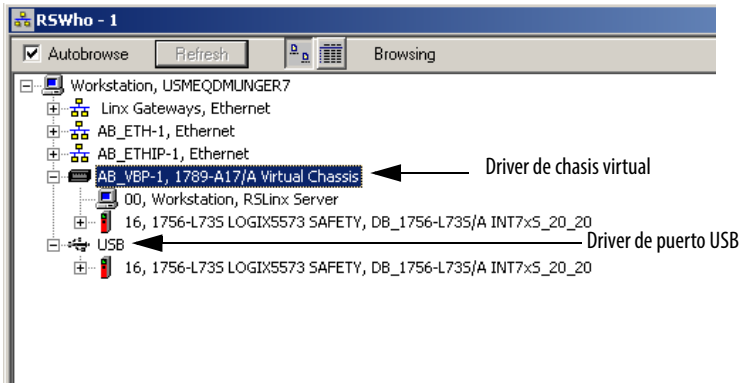
   Se instala el software.



4. Haga clic en Finish para configurar su driver USB.

5. Para ir al controlador en el software RSLinx, haga clic en RSWho

En el organizador de la estación de trabajo RSLinx, el controlador aparece bajo dos drivers diferentes: un chasis virtual y el puerto USB. Puede usar cualquiera de los dos drivers para navegar hasta el controlador.



Actualización del controlador

Los controladores se envían sin firmware. El firmware del controlador se incluye con el ambiente Studio 5000. Además, el firmware del controlador también está disponible para descarga en el sitio web de asistencia técnica de Rockwell Automation en: http://www.rockwellautomation.com/support/.

Puede actualizar el firmware usando ya sea el software ControlFLASH™ o bien la función AutoFlash de la aplicación Logix Designer.

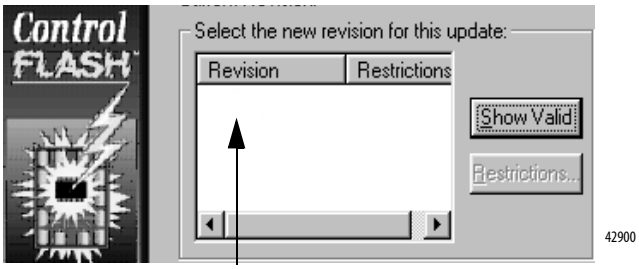
Uso del software ControlFLASH para actualizar el firmware

El homólogo de seguridad se actualiza automáticamente cuando se actualiza el controlador primario.

IMPORTANTE	Si la tarjeta SD está bloqueada y la opción Load Image del proyecto se establece en On Power Up, el firmware del controlador no se actualiza como resultado de estos pasos. En su lugar se cargan el firmware y los proyectos almacenados previamente.

1. Verifique que esté hecha la conexión de red apropiada y que el driver de red esté configurado en el software RSLinx.
2. Inicie el software ControlFLASH.
3. Seleccione Next.
4. Seleccione el número de catálogo del controlador y haga clic en Next.
5. Expanda la red hasta que vea el controlador.

6. Seleccione el controlador y haga clic en Next.



7. Seleccione el nivel de revisión de la actualización del controlador y, a continuación, haga clic en Next.
8. Para empezar a actualizar el controlador, haga clic en Finish y, a continuación, en Yes.

   Después de actualizar el controlador, el cuadro de diálogo de estado mostrará "Update complete".

IMPORTANTE	Permita que el firmware se actualice completamente antes de desconectar y volver a conectar la alimentación eléctrica; de no hacerlo se interrumpirá la actualización.

SUGERENCIA	Si se interrumpe la actualización ControlFLASH del controlador, el controlador regresa al firmware con que arrancó, o sea el firmware revisión 1.*xxx*.

9. Haga clic en OK.
10. Cierre el software ControlFLASH.

Uso de AutoFlash para actualizar el firmware

Para actualizar el firmware del controlador con la función AutoFlash, realice estos pasos.

1. Verifique que esté hecha la conexión de red apropiada y que el driver de red esté configurado en el software RSLinx.
2. Use la aplicación Logix Designer para crear un proyecto de controlador en la versión que usted necesita.

3. Haga clic en RSWho para especificar la ruta del controlador.

4. Seleccione el controlador y haga clic en Update Firmware.
5. Seleccione la revisión de firmware que desea.
6. Haga clic en Update.
7. Haga clic en Yes.

Permita que la actualización de firmware concluya sin interrupción. Al concluir la actualización de firmware, se abre el cuadro de diálogo Who Active. Puede completar otras tareas en la aplicación Logix Designer.

Selección del modo de operación del controlador

Use esta tabla como referencia al determinar el modo de operación del controlador.

Tabla 9 – Modos de operación del controlador

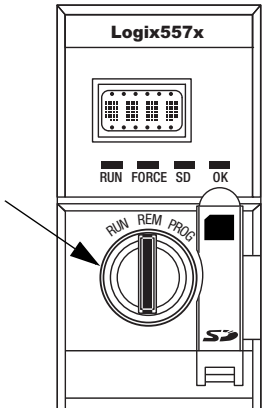
Si desea	Seleccione uno de estos modos				
	Run	Remote			Program
		Run	Test	Program	
Colocar las salidas en el estado dictado por la lógica del proyecto	X	X			
Colocar las salidas en el estado configurado para el modo de programación (Program)			X	X	X
Ejecutar (escanear) tareas	X	X	X		
Cambiar el modo del controlador por software		X	X	X	
Descargar un proyecto		X	X	X	X
Programar una red ControlNet				X	X
Editar el proyecto mientras está en línea		X	X	X	X
Enviar mensajes	X	X	X		
Enviar y recibir datos en respuesta a un mensaje de otro controlador	X	X	X	X	X
Producir y consumir tags	X	X	X	X	X

Utilizar el interruptor de llave para cambiar el modo de operación

El interruptor de llave situado en la parte frontal del controlador puede usarse para cambiar el controlador a uno de estos modos:

- Programación (PROG)
- Remoto (REM)
- Marcha (RUN)

Figura 4 – Interruptor de llave del controlador



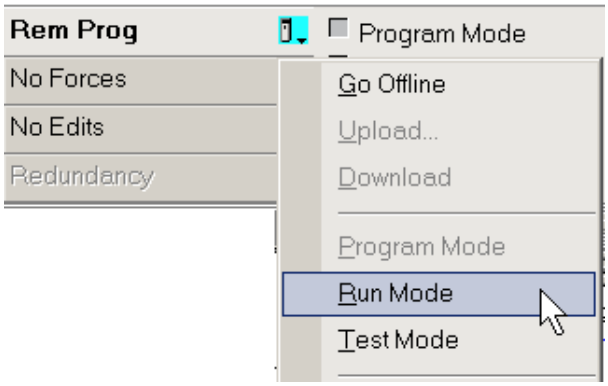
Uso de la aplicación Logix Designer para cambiar el modo de operación

Dependiendo del modo del controlador haya especificado mediante el interruptor de llave, puede cambiar el modo de operación del controlador mediante la aplicación Logix Designer.

Una vez que usted se ponga en línea con el controlador y el interruptor de llave del controlador se establezca en Remoto (REM o la posición central), puede usar el menú Controller Status situado en la esquina superior izquierda de la ventana de la aplicación Logix Designer para especificar estos modos de operación:

- Programación remota
- Marcha remota
- Prueba remota

Figura 5 – Modo de operación mediante la aplicación Logix Designer



SUGERENCIA En este ejemplo, el interruptor de llave del controlador está establecido en el modo remoto. Si el interruptor de llave del controlador se establece en el modo de marcha o el modo de programación, cambiarán las opciones del menú.

Desinstalación de un módulo de almacenamiento de energía (ESM)

Los controladores se envían con un ESM instalado.

Controlador	Nº de cat. de ESM instalado
Controlador 1756-L7xS	1756-ESMCAP
Controlador para temperaturas extremas 1756-L7xSXT	1756-ESMCAPXT
Homólogo de seguridad 1756-L7SP	1756-SPESMNSE
Homólogo de seguridad para temperaturas extremas 1756-L7SPXT	1756-SPESMNSEXT

Considere estos puntos antes de retirar el ESM:

- Cuando se interrumpe la alimentación eléctrica del controlador, ya sea porque se desconectó la alimentación eléctrica del chasis, o bien porque se retiró el controlador de un chasis energizado, no retire el ESM inmediatamente.

  Espere hasta que el indicador de estado OK del controlador cambie de verde a rojo fijo y posteriormente a apagado (OFF) antes de retirar el ESM.

- Use el módulo 1756-ESMNSE si la aplicación requiere que el ESM instalado descargue su energía residual almacenada a un nivel de 40 µJ o menos antes de transportarlo a su aplicación o fuera de ella.
- Una vez instalado, no podrá desinstalar el módulo 1756-ESMNRM del controlador.

IMPORTANTE Antes de retirar un ESM, haga los ajustes necesarios en el programa a fin de prepararlo para posibles cambios en el atributo WallClockTime.

Siga estos pasos para retirar un módulo 1756-ESMCAP(XT), 1756-ESMNSE(XT) o 1756-SPESMNSE(XT).

ADVERTENCIA: Si su aplicación requiere que el ESM descargue su energía residual almacenada a un nivel de 40 µJ o menos antes de transportarlo a su aplicación o fuera de ella, deberá utilizar el módulo 1756-ESMNSE(XT) para el controlador primario y el 1756-SPESMNSE(XT) para el homólogo de seguridad. En este caso, realice estos pasos antes de retirar el ESM.

a. Desconecte la alimentación eléctrica del chasis.

   Después de desconectar la alimentación eléctrica del chasis, el indicador de estado OK del controlador cambia de verde a rojo fijo y seguidamente se apaga.

b. Espere **por lo menos 20 minutos** para que la energía residual almacenada se reduzca a 40 µJ o menos antes de retirar el ESM.

   No existe indicación visual de cuándo han transcurrido los 20 minutos. **Deberá medir por su cuenta ese período de tiempo**.

ADVERTENCIA: Al introducir o retirar el módulo de almacenamiento de energía con alimentación del backplane conectada se puede producir un arco eléctrico. Esto podría provocar una explosión en instalaciones ubicadas en zonas peligrosas.

Antes de seguir adelante, asegúrese de desconectar la alimentación eléctrica o de verificar que la zona no sea peligrosa. La recurrencia de arcos eléctricos puede provocar desgaste excesivo en los contactos tanto del módulo como del conector de acoplamiento.

1. Retire la llave del interruptor de llave.

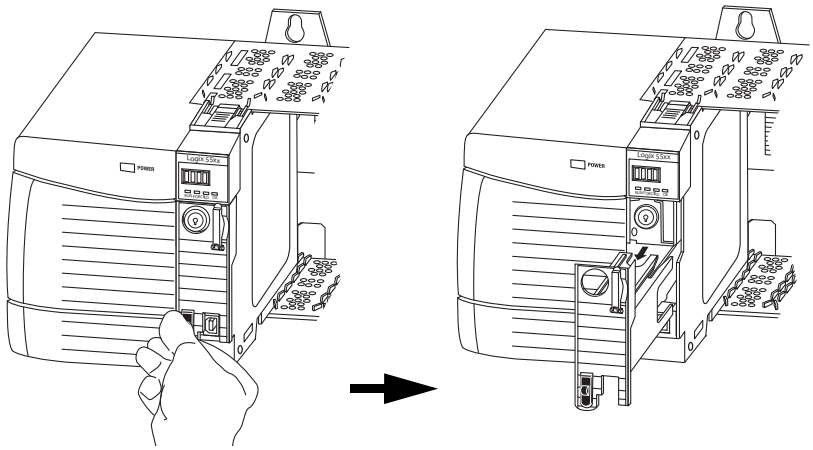
IMPORTANTE El siguiente paso depende de las condiciones que correspondan a su aplicación:

- Si va a retirar el ESM de un controlador energizado, vaya al paso 2.
- Si está retirando el ESM de un controlador que no está energizado, ya sea porque se desconectó la alimentación eléctrica del chasis o porque se retiró el controlador de un chasis energizado, **no retire** el ESM inmediatamente.

  Espere hasta que el indicador de estado OK del controlador cambie de verde a rojo fijo y posteriormente se apague antes de retirar el ESM.

  Cuando se apague el indicador de estado OK, vaya al paso 2.

2. Use el dedo pulgar para presionar hacia abajo el dispositivo de liberación negro y tire del ESM para separarlo del controlador.



Instalación de un módulo de almacenamiento de energía (ESM)

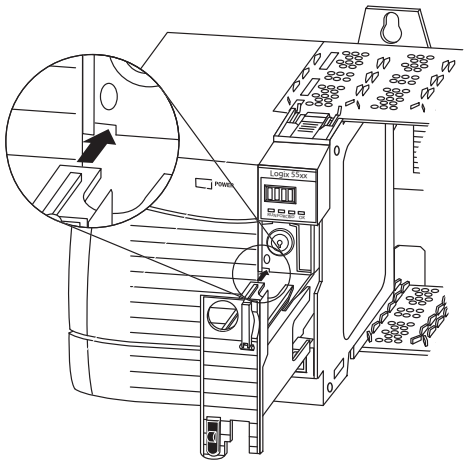
La Tabla 10 indica los ESM y los controladores GuardLogix compatibles.

Tabla 10 – Módulos de almacenamiento de energía compatibles

Nº cat.	ESM compatibles
1756-L7*x*S	1756-ESMCAP, 1756-ESMNSE, 1756-ESMNRM
1756-L7*x*SXT	1756-ESMCAPXT, 1756-ESMNSEXT, 1756-ESMNRMXT
1756-L7SP	1756-SPESMNSE, 1756-SPESMNRM
1756-L7SPXT	1756-SPESMNSEXT, 1756-SPESMNRMXT

Para instalar un ESM, siga estos pasos. Siga los mismos pasos para el homólogo de seguridad.

1. Alinee las ranuras de machihembrado del ESM y del controlador.



2. Deslice el ESM en el chasis hasta que encaje en su lugar.

ATENCIÓN: Para evitar posibles daños en el producto al insertar el ESM, alinee el ESM en la guía y deslícelo suavemente hacia adelante hasta que el ESM encaje en su lugar.

El ESM comienza a cargarse después de la instalación. El estado de carga es indicado por uno de estos mensajes de estado:

- ESM Charging
- CHRG

Después de instalar el ESM, pueden transcurrir hasta 15 segundos antes de que aparezcan los mensajes de estado de carga.

IMPORTANTE	Deje que el ESM termine de cargarse antes de desconectar la alimentación eléctrica del controlador. Para verificar que el ESM está totalmente cargado, examine la pantalla y confirme que los mensajes "CHRG" o "ESM Charging" no están presentes.
SUGERENCIA	Verifique los atributos del objeto WallClockTime después de instalar un ESM para verificar que la hora del controlador sea la correcta.

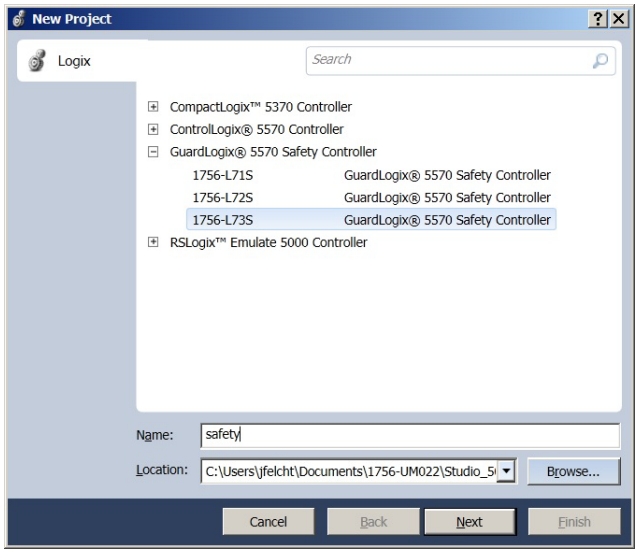
Notas:

Configuración del controlador

Creación de un proyecto de controlador

A fin de configurar y programar su controlador, utilice la aplicación Logix Designer para crear y administrar un proyecto de controlador.

1. Haga clic en el botón New  de la barra de herramientas principal para crear un proyecto.
2. Haga doble clic en GuardLogix 5570 Safety Controller para expandir la lista de opciones de controladores.
3. Elija un controlador GuardLogix:
   - 1756-L71S Controlador de seguridad GuardLogix 5570
   - 1756-L72S Controlador de seguridad GuardLogix 5570
   - 1756-L73S Controlador de seguridad GuardLogix 5570

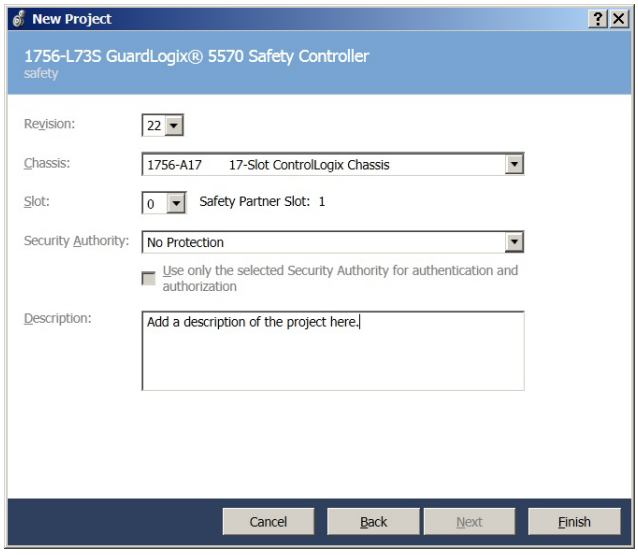


4. En el campo Name, escriba el nombre del proyecto.
5. Haga clic en Browse para especificar la carpeta en la que se almacenará el proyecto de controlador de seguridad.
6. Haga clic en Next.

7. En el menú desplegable Revision, elija la revisión mayor del firmware del controlador.
8. En el menú desplegable Chassis, seleccione el tamaño del chasis.
9. En el menú desplegable Slot, elija la ranura para el homólogo de seguridad.

   El cuadro de diálogo New Project indica la ubicación de la ranura del homólogo de seguridad, basada en el número de ranura especificado para el controlador primario.

   Si selecciona un número de ranura para el controlador primario que no admite la ubicación del homólogo de seguridad justo a la derecha del controlador primario, se le pedirá que introduzca un número válido de ranura.



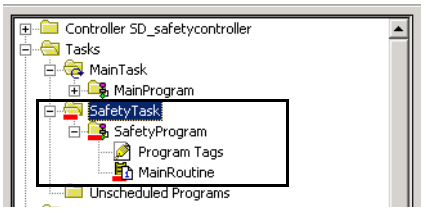
10. En el menú desplegable Security Authority, elija una opción de autoridad de seguridad.

    Para obtener información detallada sobre seguridad, consulte el documento Logix5000 Controllers Security Programming Manual, publicación 1756-PM016.

11. Marque la casilla que hay debajo de Security Authority si desea utilizar la protección seleccionada para autenticación y autorización.
12. En el campo Description, introduzca la descripción del proyecto.
13. Haga clic en Finish.

La aplicación Logix Designer crea una tarea de seguridad y un programa de seguridad. También se crea una rutina de seguridad de lógica de escalera principal llamada MainRoutine dentro del programa de seguridad.

Figura 6 – Tarea de seguridad en el Controller Organizer



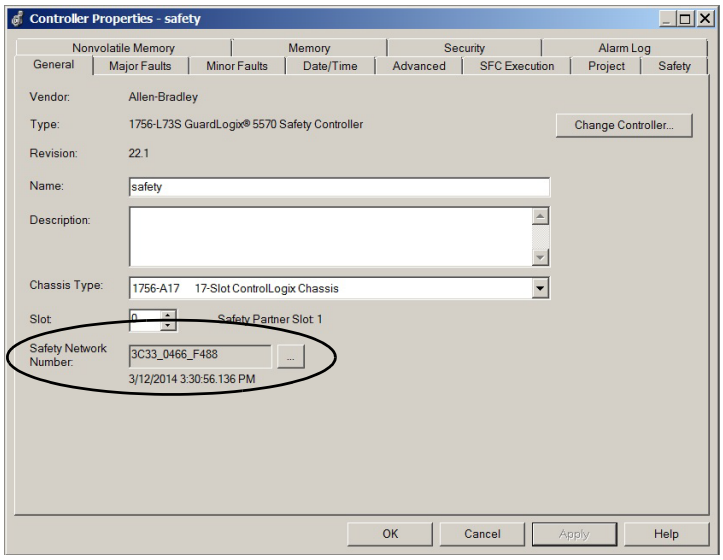
Una barra roja debajo del icono de la carpeta distingue los programas y las rutinas de seguridad de los componentes del proyecto estándar en el Controller Organizer.

Cuando se crea un nuevo proyecto de seguridad, la aplicación Logix Designer también crea automáticamente un número de red de seguridad (SNN) basado en tiempo.

Este SNN define el backplane del chasis local como una subred de seguridad. Se puede ver y modificar en la ficha General del cuadro de diálogo Controller Properties.

En la mayoría de las aplicaciones, basta con este SNN automático, basado en tiempo. Sin embargo, hay casos en los que es necesario especificar un SNN específico.

Figura 7 – Número de red de seguridad



SUGERENCIA Puede utilizar el cuadro de diálogo Controller Properties para cambiar de un controlador estándar a uno de seguridad (o de seguridad a estándar). Para ello, haga clic en el botón Change Controller. Sin embargo, esto afecta considerablemente los proyectos estándar y de seguridad.

Vea el Apéndice B, Cambio del tipo de controlador, si desea información detallada acerca de las repercusiones del cambio de controladores.

Tabla 11 – Recursos adicionales

Recurso	Descripción
Capítulo 6, Desarrollo de aplicaciones de seguridad	Contiene más información acerca de la tarea de seguridad, los programas de seguridad y las rutinas de seguridad.
Capítulo 4, Comunicación a través de redes	Proporciona más información sobre la administración del SNN.

Codificación electrónica

La codificación electrónica reduce la posibilidad de que se utilice un dispositivo incorrecto en un sistema de control. Compara el dispositivo definido en el proyecto con el dispositivo instalado. Si falla la codificación, se genera un fallo. Los atributos que se comparan son los siguientes.

Atributo	Descripción
Proveedor	Fabricante del dispositivo.
Tipo de dispositivo	Tipo general del producto, por ejemplo, módulo de E/S digitales.
Código de producto	Tipo específico de producto. El código de producto corresponde a un número de catálogo.
Revisión mayor	Número que representa las capacidades funcionales de un dispositivo.
Revisión menor	Número que representa cambios de comportamiento en el dispositivo.

Están disponibles las siguientes opciones de codificación electrónica.

Opción de codificación	Descripción
Compatible Module	Permite que el dispositivo instalado acepte la clave del dispositivo definido en el proyecto cuando el dispositivo instalado puede emular el dispositivo definido. Con Compatible Module, normalmente se puede reemplazar un dispositivo por otro que tenga las siguientes características: • Número de catálogo igual • Revisión mayor igual o superior • Revisión menor como se indica a continuación: – Si la revisión mayor es la misma, la revisión menor debe ser la misma o superior. – Si la revisión mayor es superior, la revisión menor puede ser cualquier número.
Exact Match	Indica que todos los atributos de codificación deben coincidir para establecer la comunicación. Si algún atributo no coincide exactamente, no se produce la comunicación con el dispositivo. Exact Match es necesario si está usando Firmware Manager.

Examine cuidadosamente las implicaciones de cada opción de codificación antes de elegir una.

IMPORTANTE Si se cambian en línea los parámetros de codificación electrónica, se interrumpen las conexiones con el dispositivo y todos los dispositivos que se conectan a través del dispositivo. Es posible que también se interrumpan las conexiones desde otros controladores.

Si se interrumpe una conexión de E/S con un dispositivo, es posible que se pierdan datos.

Más información

Para obtener información más detallada sobre la codificación electrónica, consulte Electronic Keying in Logix5000 Control Systems Application Technique, publicación LOGIX-AT001.

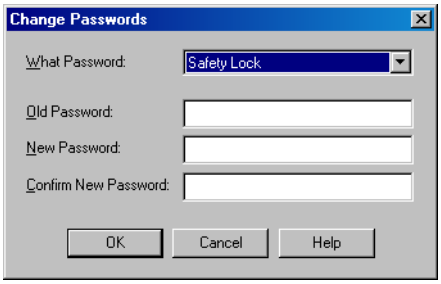
Establecimiento de contraseñas para bloqueo y desbloqueo de seguridad

El bloqueo de seguridad del controlador ayuda a proteger los componentes de control de seguridad frente a una posible modificación. Esto solo afecta los componentes de seguridad como la tarea de seguridad, los programas de seguridad, las rutinas de seguridad y los tags de seguridad. No afecta los componentes estándar. Usted puede establecer un bloqueo o desbloqueo de seguridad, ya sea en línea o fuera de línea.

La función de bloqueo y desbloqueo de seguridad utiliza dos contraseñas distintas. Las contraseñas son opcionales.

Siga estos pasos para establecer las contraseñas:

1. Haga clic en Tools > Safety > Change Passwords.
2. En el menú desplegable What Password, seleccione Safety Lock o Safety Unlock.



3. Escriba la contraseña anterior, si existe.
4. Escriba y confirme la nueva contraseña.
5. Haga clic en OK.

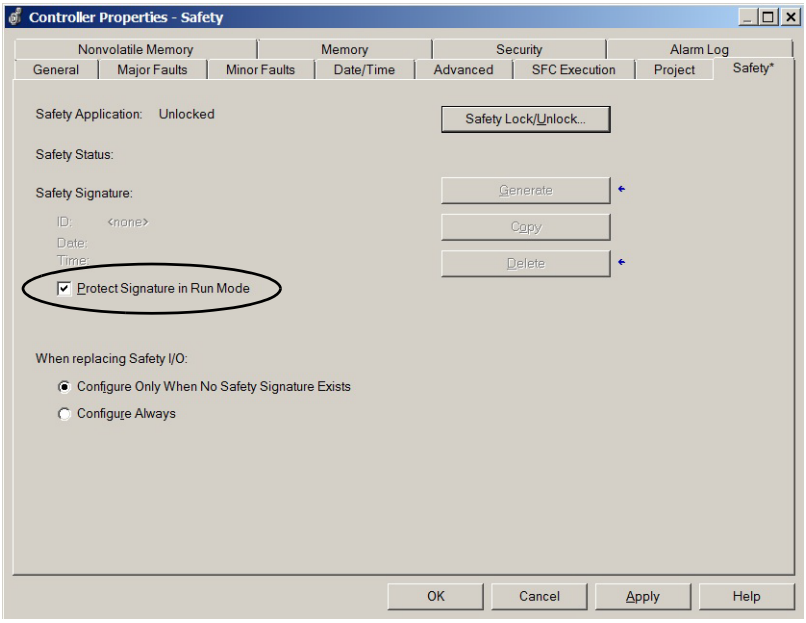
   Las contraseñas pueden tener de 1...40 caracteres de longitud, y no hay distinción entre mayúsculas y minúsculas.- Puede utilizar letras, números y los siguientes símbolos
   : ‘ ~ ! @ # $ % ^ & * ( ) _ + , - = { } | [ ] \ : ; ? / .

Protección de la firma de tarea de seguridad en el modo marcha

Puede evitar que se genere o elimine la firma de tarea de seguridad mientras el controlador está en el modo marcha o en el modo de marcha remota, independientemente de que la aplicación de seguridad esté bloqueada o desbloqueada.

Siga estos pasos para proteger la firma de tarea de seguridad:

1. Abra el cuadro de diálogo Controller Properties.
2. Haga clic en la ficha Safety.
3. Marque Protect Signature in Run Mode.
4. Haga clic en OK.



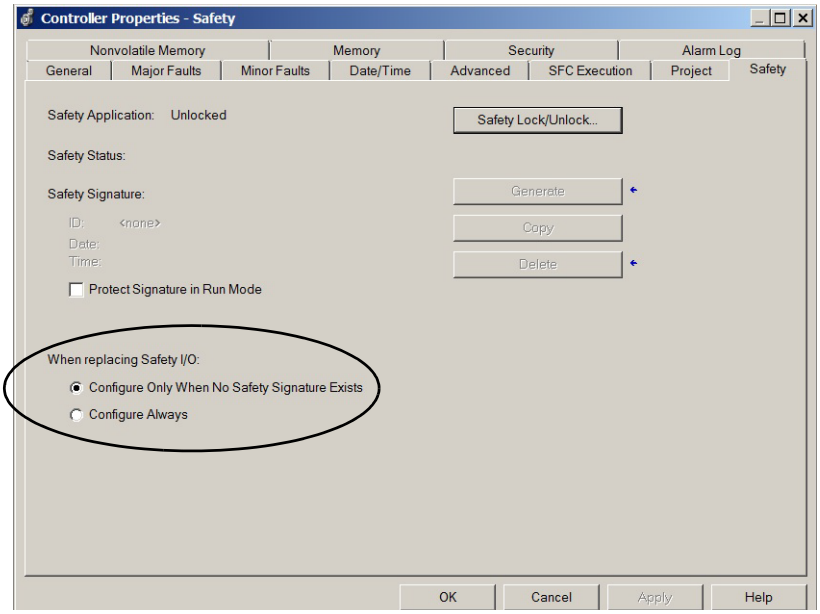
Reemplazo de un dispositivo de E/S

La ficha Safety del cuadro de diálogo Controller Properties le permite definir cómo debe comportarse el controlador durante el reemplazo de un dispositivo de E/S en el sistema. Esta opción determina si el controlador establece el número de red de seguridad (SNN) de un dispositivo de E/S al que se ha conectado y tiene datos de configuración en caso de que exista una firma[1] de tarea de seguridad.

Siga estos pasos para configurar cómo se comporta el controlador ante el reemplazo de un dispositivo de E/S en el sistema.

1. Abra el cuadro de diálogo Controller Properties.
2. Haga clic en la ficha Safety.
3. Seleccione la opción de configuración que desea que utilice el controlador al reemplazar E/S de seguridad.
4. Haga clic en OK.

Figura 8 – Opciones de reemplazo de dispositivos de E/S



ATENCIÓN: Habilite la función Configure Always solo si no se ha confiado a todo el sistema de control CIP Safety encaminable el mantenimiento del SIL 3 durante el reemplazo y las pruebas de funcionamiento de un dispositivo.

Vea el Capítulo 5, Cómo añadir, configurar, monitorear y reemplazar dispositivos CIP Safety I/O para obtener más información.

(1) La firma de tarea de seguridad es un número que se utiliza para identificar de forma inequívoca la lógica, los datos y la configuración del proyecto, lo que le permite proteger el nivel de integridad de seguridad (SIL) del sistema. Consulte las secciones Firma de tarea de seguridad en la página 14 y Generación de una firma de tarea de seguridad en la página 102 para obtener más información.

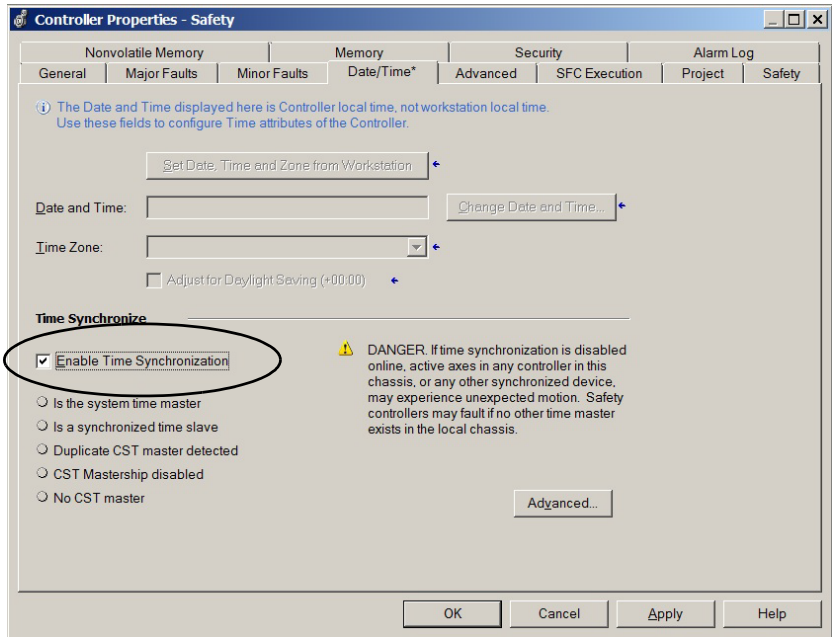
Habilitación de sincronización de hora

En un sistema de controlador GuardLogix, un dispositivo en el chasis local debe ser designado maestro de hora coordinada del sistema (CST). La sincronización de hora proporciona un mecanismo estándar para sincronizar los relojes de una red de dispositivos distribuidos.

Siga estos pasos para configurar el controlador a fin de que sea el maestro de CST.

1. Abra el cuadro de diálogo Controller Properties.
2. Haga clic en la ficha Date/Time.
3. Marque Enable Time Synchronization.
4. Haga clic en OK.

Figura 9 – Ficha Date/Time



Para obtener más información sobre la sincronización de hora, consulte el documento Integrated Architecture and CIP Sync Configuration Application Solution, publicación IA-AT003.

Configuración de un controlador de seguridad homólogo

Puede añadir un controlador de seguridad homólogo a la carpeta de configuración de E/S del proyecto de seguridad, a fin de permitir el consumo de tags estándar o de seguridad. Para compartir datos de seguridad entre controladores homólogos, se producen y se consumen tags de seguridad bajo el control del controlador.

Para obtener detalles sobre cómo configurar los controladores de seguridad homólogos, y sobre cómo producir y consumir tags de seguridad, consulte Tags de seguridad producidos/consumidos en la página 92.

Comunicación a través de redes

La red de seguridad

El protocolo CIP Safety es un protocolo de seguridad de nodo final a nodo final que proporciona el encaminamiento de mensajes CIP Safety desde y hacia dispositivos de E/S de seguridad a través de puentes, switches y routers.

Para mantener un alto grado de integridad durante el encaminamiento a través de puentes, switches y routers estándar, cada uno de los nodos finales dentro de un sistema de control CIP Safety debe tener una referencia única. Esta referencia única es una combinación de un número de red de seguridad (SNN) y la dirección de nodo del dispositivo de red.

Administración del número de red de seguridad (SNN)

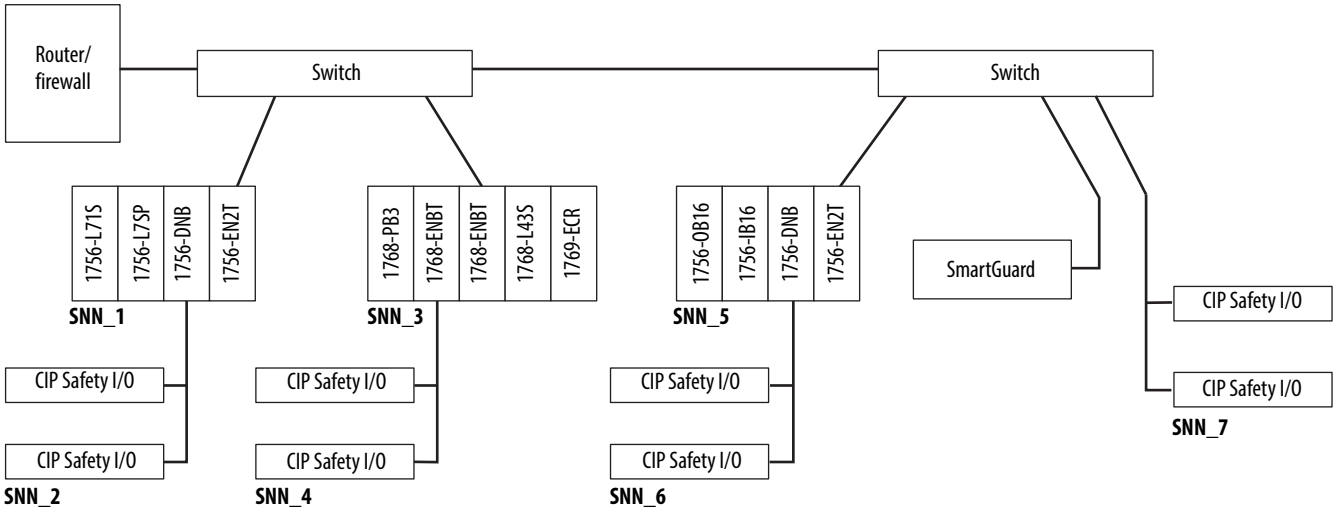
El SNN asignado a dispositivos de seguridad en un segmento de red debe ser único. Es necesario asegurarse de que un SNN único se asigne a los siguientes:

- Cada red CIP Safety que contenga dispositivos de seguridad
- Cada chasis que contenga uno o más controladores GuardLogix

SUGERENCIA Se pueden asignar varios números de red de seguridad a una subred CIP Safety o a un chasis ControlBus que contenga más de un dispositivo de seguridad. No obstante, para simplificar las cosas, recomendamos que cada subred CIP Safety tenga solo un SNN único.

Figura 10 muestra un sistema CIP Safety con siete subredes diferentes y un SNN único en cada subred.

Figura 10 – Ejemplo de CIP Safety con más de un SNN

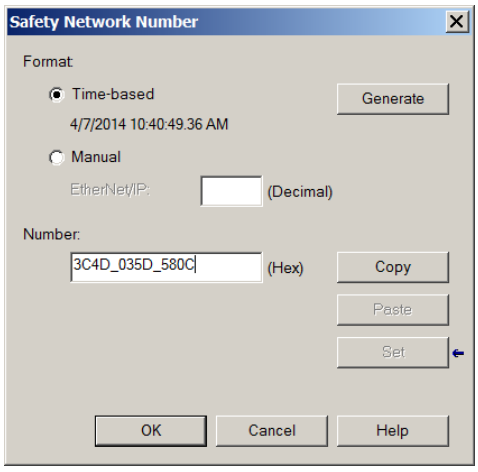


El SNN puede ser asignado por el software (basado en tiempo) o por el usuario (manual). Estos dos formatos del SNN se describen en las secciones siguientes.

Número de red de seguridad basado en tiempo

Si se selecciona el formato basado en tiempo, el valor de SNN es la fecha y la hora en que se generó el número, según la computadora en la que se ejecuta el software de configuración.

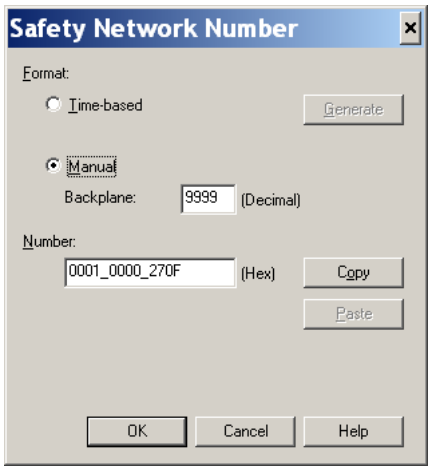
Figura 11 – Formato basado en tiempo



Número de red de seguridad manual

Si se selecciona el formato manual, el SNN se especifica como valores de 1...9999 decimal.

Figura 12 – Entrada manual



Asignación del número de red de seguridad (SNN)

Usted puede permitir que la aplicación Logix Designer asigne automáticamente un SNN, o puede asignar el SNN manualmente.

Asignación automática

Cuando se crea un nuevo controlador o dispositivo, se le asigna automáticamente un SNN basado en tiempo. A los dispositivos de seguridad añadidos posteriormente a la misma red CIP Safety se les asigna el mismo SNN, definido dentro de la dirección de nodo más baja en la red CIP Safety.

Asignación manual

La opción manual se ha previsto para sistemas CIP Safety encaminables con un número reducido de subredes y redes de interconexión, en los que quiera administrar y asignar el SNN de manera lógica según su aplicación específica.

Consulte Cambio del número de red de seguridad (SNN) en la página 50.

IMPORTANTE	Si asigna un SNN manualmente, asegúrese de que la expansión del sistema no dé como resultado una duplicación de las combinaciones de SNN y direcciones de nodo. En Logix Designer, versión 24, se producirá un error de verificación si el proyecto contiene combinaciones de SNN y dirección de nodo duplicadas. En Logix Designer, versión 26, aparecerá una advertencia si el proyecto contiene combinaciones de SNN y direcciones de nodo duplicadas. Si lo prefiere, puede verificar el proyecto, pero Rockwell Automation recomienda eliminar las combinaciones duplicadas.

Automático frente a manual

A los usuarios típicos les basta con la asignación automática de un SNN. Sin embargo, se requiere un manejo manual del SNN si se cumple lo siguiente:

- se utilizan tags de seguridad consumidos;
- el proyecto consume datos de entrada de seguridad provenientes de un módulo cuya configuración está en posesión de otro dispositivo;
- se copia un proyecto de seguridad en otra instalación de hardware distinta dentro del mismo sistema CIP Safety encaminable.

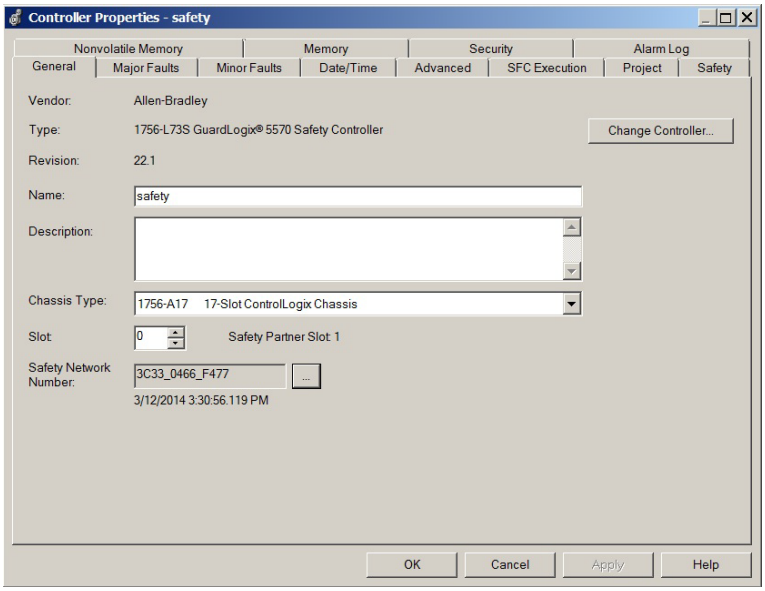
Cambio del número de red de seguridad (SNN)

Antes de cambiar el SNN, es necesario hacer lo siguiente:

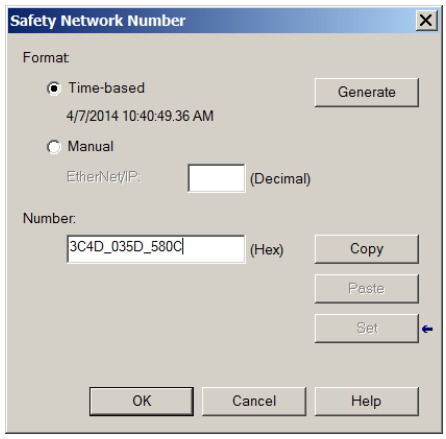
- Desbloquear el proyecto si está en bloqueo de seguridad;
  Consulte Bloqueo de seguridad del controlador en la página 101.
- Eliminar la firma de tarea de seguridad, si la hay.
  Consulte Eliminación de la firma de tarea de seguridad en la página 103.

Cambio del número de red de seguridad (SNN) del controlador

1. En el Controller Organizer, haga clic con el botón derecho del mouse en el controlador y seleccione Properties.
2. En la ficha General del cuadro de diálogo Controller Properties, haga clic en ... ubicado a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.



3. Haga clic en Time-based y, a continuación, en Generate.

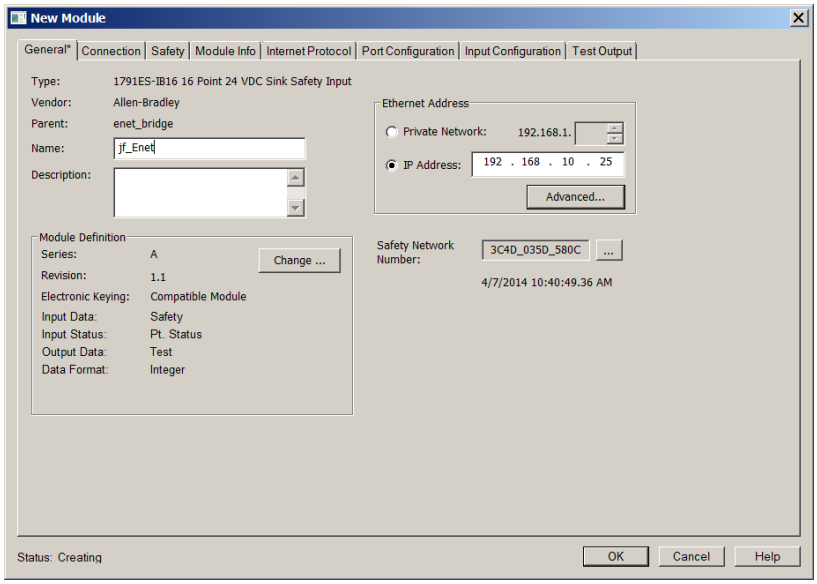


4. Haga clic en OK.

Cambio del número de red de seguridad (SNN) de dispositivos de E/S de seguridad en la red CIP Safety

En este ejemplo se utiliza una red EtherNet/IP.

1. Busque el primer módulo de comunicación EtherNet/IP en el árbol de configuración de E/S.
2. Expanda los dispositivos de E/S de seguridad disponibles a través del módulo de comunicación EtherNet/IP.
3. Haga doble clic en el primer dispositivo de E/S de seguridad para ver la ficha General.



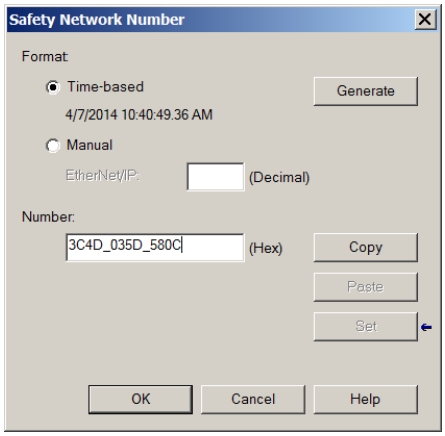
4. Haga clic en ... a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.
5. Seleccione Time-based y haga clic en Generate para generar un nuevo SNN para esa red EtherNet/IP.
6. Haga clic en OK.
7. Haga clic en Copy para copiar el nuevo SNN en el portapapeles de Windows.

8. Abra la ficha General del cuadro de diálogo Module Properties del siguiente dispositivo de E/S de seguridad bajo ese módulo EtherNet/IP.
9. Haga clic en ... a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.
10. Seleccione Time-based y haga clic en Paste para pegar el SNN de esa red EtherNet/IP en ese dispositivo.
11. Haga clic en OK.
12. Repita los pasos 8...10 con los demás dispositivos de E/S de seguridad bajo ese módulo de comunicación EtherNet/IP.
13. Repita los pasos 2...10 para los módulos de comunicación de red restantes bajo el árbol de configuración de E/S.

Copiado y pegado de un número de red de seguridad (SNN)

Si la configuración del módulo está en posesión de otro controlador, puede copiar el SNN del propietario de la configuración y pegarlo en el módulo del árbol de configuración de E/S.

1. En la herramienta de configuración de software del propietario de la configuración del módulo, abra el cuadro de diálogo Safety Network Number correspondiente al módulo.



2. Haga clic en Copy.
3. Haga clic en la ficha General del cuadro de diálogo Module Properties del dispositivo de E/S en el árbol de configuración de E/S del proyecto del controlador consumidor.
   Este controlador consumidor no es el propietario de la configuración.
4. Haga clic en ... a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.
5. Haga clic en Paste.
6. Haga clic en OK.

Comunicación EtherNet/IP

Para la comunicación de red EtherNet/IP en un sistema GuardLogix, usted tiene varias opciones de módulos. Para la comunicación CIP Safety, incluido el control de dispositivos de E/S de seguridad, elija cualquiera de los módulos mostrados en la Tabla 12, excepto el módulo 1756-EWEB, que no es compatible con la comunicación CIP Safety.

La Tabla 12 indica los módulos y sus principales características.

Tabla 12 – Módulos y capacidades de comunicación EtherNet/IP

Módulo	Características
1756-ENBT	• Conectar controladores a dispositivos de E/S (requiere un adaptador para E/S distribuidas). • Comunicarse con otros dispositivos EtherNet/IP (mensajes). • Servir como ruta para compartir datos entre controladores Logix5000 (producir/consumir). • Conectar en puente nodos EtherNet/IP para encaminar mensajes a dispositivos en otras redes.
1756-EN2T	• Realizar las mismas funciones que un módulo 1756-ENBT, con el doble de capacidad para aplicaciones más exigentes. • Proporcionar una conexión de configuración temporal mediante el puerto USB. • Configurar direcciones IP rápidamente usando interruptores giratorios.
1756-EN2F	• Realizar las mismas funciones que un módulo 1756-EN2T. • Conectar el medio físico de fibra mediante un conector de fibra LC en el módulo.
1756-EN2TXT	• Realizar las mismas funciones que un módulo 1756-EN2T. • Operar en ambientes difíciles con temperaturas de –25…70 °C (–13…158 °F).
1756-EN2TR	• Realizar las mismas funciones que un módulo 1756-EN2T. • Permitir la comunicación en una topología de anillo en una red con topología de anillo tolerante a fallo único a nivel de dispositivo (DLR).
1756-EN2TRXT	• Realizar las mismas funciones que un módulo 1756-EN2T. • Permitir la comunicación en una topología de anillo en una red con topología de anillo tolerante a fallo único a nivel de dispositivo (DLR). • Operar en ambientes difíciles con temperaturas de –25…70 °C (–13…158 °F).
1756-EN3TR	• Realizar las mismas funciones que el módulo 1756-EN2TR. • Dos puertos para conexión DLR.
1756-EWEB	• Proporcionar páginas web personalizables para acceso externo a información del controlador. • Proporcionar acceso remoto a tags de un controlador ControlLogix local mediante un explorador de Internet. • Comunicarse con otros dispositivos EtherNet/IP (mensajes). • Conectar en puente nodos EtherNet/IP para encaminar mensajes a dispositivos en otras redes. • Aceptar dispositivos Ethernet que no están basados en EtherNet/IP con una interface de socket. Este módulo no ofrece compatibilidad con E/S ni con tags producidos/consumidos, y no es compatible con comunicación CIP Safety.

Los módulos de comunicación EtherNet/IP ofrecen las siguientes funciones:

- Admiten transmisión de mensajes, tags producidos/consumidos, HMI y E/S distribuidas
- Mensajes encapsulados dentro del protocolo TCP/UDP/IP estándar
- Una capa de aplicación común con las redes ControlNet y DeviceNet
- Interconexión mediante cable de pares trenzados sin blindaje categoría 5 con conectores RJ45
- Compatibilidad con operación half/full duplex, 10 M o 100 M
- Funcionamiento con switches estándar
- No requieren programación de red
- No requieren tablas de encaminamiento

Estos productos están disponibles para las redes EtherNet/IP.

Tabla 13 – Producto para módulos EtherNet/IP

Producto	Se usa para	Requerido
Ambiente Studio 5000	• Configurar el proyecto del controlador • Definir la comunicación EtherNet/IP	Sí
Utilidad BOOTP/DHCP(1)	Asignar direcciones IP a dispositivos en una red EtherNet/IP	No
Software RSNetWorx™ para EtherNet/IP	Configurar dispositivos EtherNet/IP mediante direcciones IP y/o nombres de anfitrión	No
Software RSLinx	• Configurar dispositivos • Establecer comunicación entre dispositivos • Proporcionar diagnósticos	Sí

(1) Esta utilidad viene con el ambiente Studio 5000.

Producción y consumo de datos a través de una red EtherNet/IP

El controlador permite producir (enviar) y consumir (recibir) tags a través de una red EtherNet/IP. Los tags producidos y consumidos requieren conexiones. El número total de tags que se pueden producir o consumir está limitado por el número de conexiones disponibles.

Conexiones por la red EtherNet/IP

El número de conexiones que utiliza el controlador de seguridad se determina indirectamente al configurarlo para que se comunique con otros dispositivos en el sistema. Las conexiones son asignaciones de recursos que proporcionan comunicación más confiable entre dispositivos, en comparación con los mensajes no conectados (instrucciones de mensajes).

Las conexiones EtherNet/IP son conexiones no programadas. Una conexión no programada es activada por el intervalo solicitado entre paquetes (RPI) para control de E/S o el programa (tal como una instrucción MSG). La transmisión de mensajes no programada le permite enviar y recibir datos cuando es necesario.

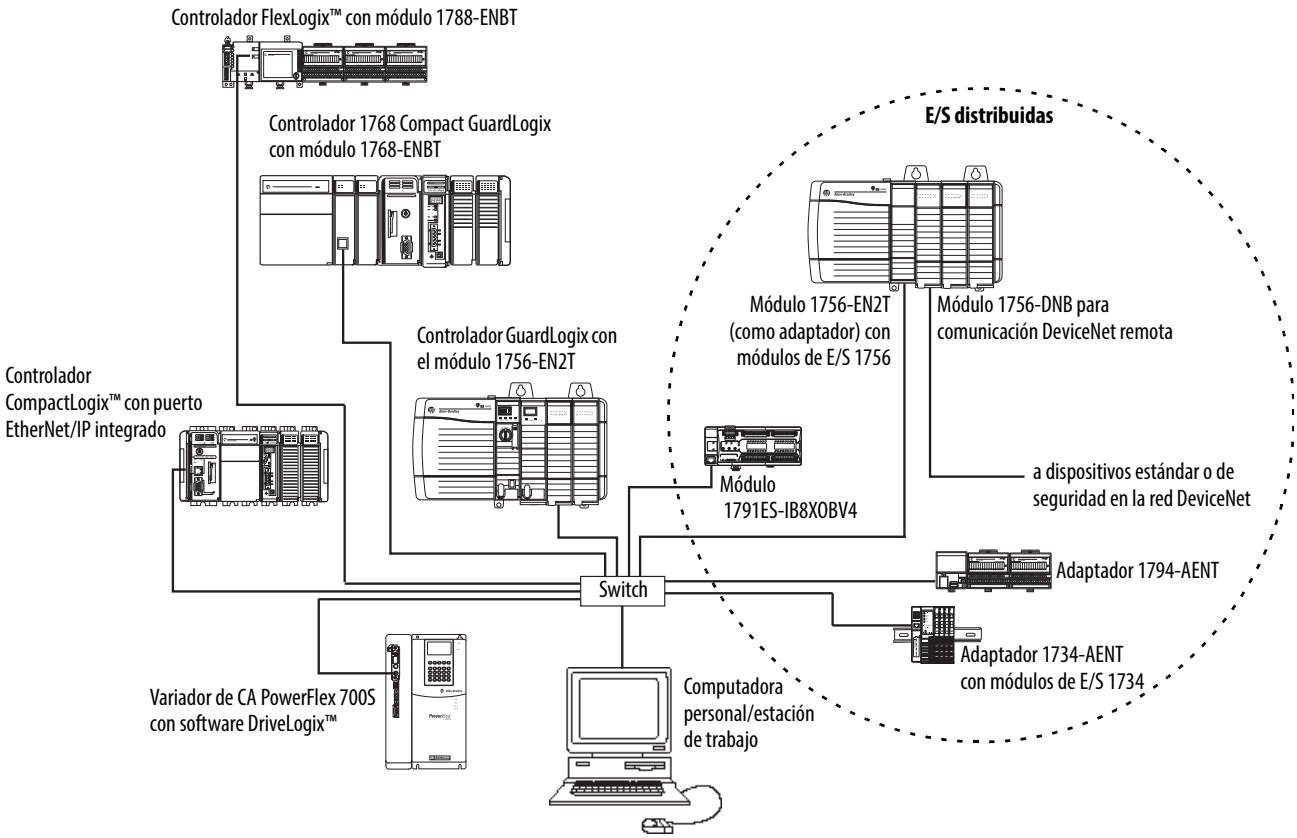
Los módulos de comunicación EtherNet/IP admiten 128 conexiones del protocolo industrial común (CIP) a través de una red EtherNet/IP.

Ejemplos de comunicación EtherNet/IP

La Figura 13 ilustra las siguientes funciones de comunicación:

- Los controladores pueden producir y consumir tags estándar o de seguridad entre sí.
- Los controladores pueden iniciar instrucciones MSG que envían o reciben datos estándar o configuran dispositivos.(1)
- El módulo de comunicación EtherNet/IP se usa como puente, dejando que el controlador de seguridad produzca y consuma datos estándar y de seguridad.
- La estación de trabajo puede cargar/descargar proyectos a los controladores.
- La estación de trabajo puede configurar dispositivos en la red EtherNet/IP.

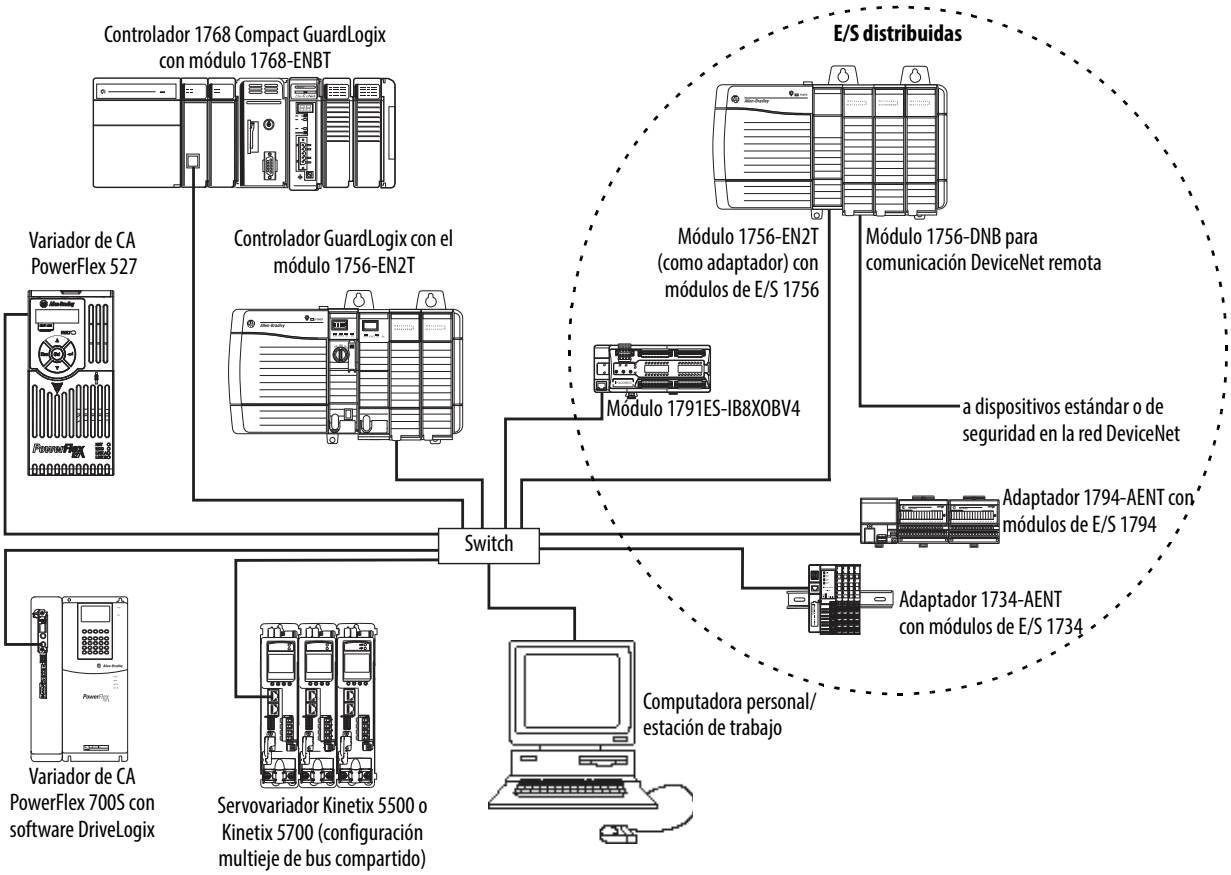
Figura 13 – Ejemplo de comunicación EtherNet/IP



(1) Los controladores GuardLogix no aceptan instrucciones MSG para datos de seguridad.

En la aplicación Logix Designer, versión 24 y posterior, el controlador admite una conexión estándar y de seguridad mediante una única conexión.

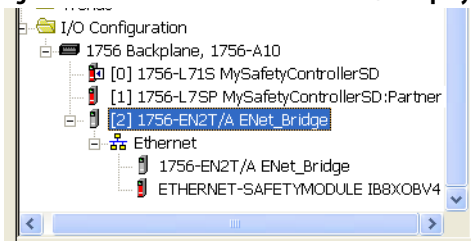
Figura 14 – Ejemplo de comunicación EtherNet/IP con conexión estándar y de seguridad



Conexiones EtherNet/IP para dispositivos de E/S de seguridad

Los dispositivos de E/S de seguridad en las redes EtherNet/IP se añaden al proyecto debajo del módulo de comunicación EtherNet/IP, como se describe en Adición de dispositivos de E/S de seguridad en la página 63. Al añadir un dispositivo de E/S de seguridad, la aplicación Logix Designer crea automáticamente tags de datos de seguridad bajo el control del controlador para ese dispositivo.

Figura 15 – Adición de módulos EtherNet/IP al proyecto



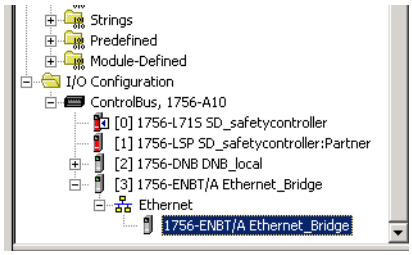
Conexiones EtherNet/IP estándar

Para usar un módulo EtherNet/IP estándar con el controlador de seguridad, añada el módulo al proyecto del controlador de seguridad y descargue el proyecto al controlador GuardLogix.

1. Para configurar el módulo, defina la dirección IP, la máscara de subred y el gateway.

Parámetro de EtherNet/IP	Descripción
Dirección IP	La dirección IP identifica el módulo de forma única. La dirección IP tiene el formato *xxx.xxx.xxx.xxx.* donde cada xxx es un número entre 0 y 255. Sin embargo, hay algunos valores que no se pueden usar como primer octeto en la dirección: • 000.*xxx.xxx.xxx* • 127.*xxx.xxx.xxx* • 223…255.*xxx.xxx.xxx*
Máscara de subred	El direccionamiento de subred es una extensión del esquema de dirección IP que permite a un sitio utilizar una identificación de red para varias redes físicas. El encaminamiento fuera del sitio prosigue mediante la división de la dirección IP en una identificación de red y una identificación de anfitrión a través de la clase. Dentro de un sitio, la máscara de subred se utiliza para volver a dividir la dirección IP en una porción de identificación de red personalizada y una porción de identificación de anfitrión. Este campo se define de forma predeterminada como 0.0.0.0. Si se cambia la máscara de subred de un módulo ya configurado, debe desconectar y volver a conectar la alimentación eléctrica para que el cambio surta efecto.
Gateway	Un gateway conecta redes físicas individuales en un sistema de redes. Si un nodo tiene que comunicarse con otro nodo en otra red, un gateway transfiere los datos entre las dos redes. Este campo se define de forma predeterminada como 0.0.0.0.

2. Después de instalar un módulo EtherNet/IP físicamente y establecer su dirección IP, añada el módulo al Controller Organizer en el proyecto del controlador GuardLogix.



3. Use la aplicación Logix Designer para descargar el proyecto.

Comunicación ControlNet

Para comunicación ControlNet, seleccione un módulo 1756-CNB o 1756-CNBR para comunicación estándar o un módulo 1756-CN2, 1756-CN2R o 1756-CN2RXT para comunicación de seguridad.

Tabla 14 – Módulos ControlNet

Si su aplicación	Seleccione
• Controla dispositivos de E/S estándar • Requiere un adaptador para E/S distribuidas por vínculos ControlNet • Se comunica con otros dispositivos ControlNet (mensajes) • Comparte datos estándar con otros controladores Logix5000 (productor/consumidor) • Conecta en puente vínculos ControlNet para encaminar mensajes a dispositivos en otras redes	1756-CNB
• Realiza las mismas funciones que un módulo 1756-CNB • También acepta medios físicos ControlNet redundantes	1756-CNBR
• Realiza las mismas funciones aceptadas por el módulo 1756-CNB con mayor rendimiento • Admite comunicación CIP Safety	1756-CN2
• Realiza las mismas funciones que un módulo 1756-CN2 • También acepta medios físicos ControlNet redundantes	1756-CN2R
• Realiza las mismas funciones que un módulo 1756-CN2R • Opera en ambientes difíciles con temperaturas de –25…70 °C (–13…158 °F)	1756-CN2RXT

Estos productos están disponibles para las redes ControlNet.

Tabla 15 – Productos para módulos ControlNet

Producto	Se usa para	Requerido
Ambiente Studio 5000	• Configurar el proyecto GuardLogix • Definir la comunicación ControlNet	Sí
Software RSNetWorx para ControlNet	• Configurar la red ControlNet • Definir el tiempo de actualización de la red (NUT) • Programar la red ControlNet	Sí
Software RSLinx	• Configurar dispositivos • Establecer comunicación entre dispositivos • Proporcionar diagnósticos	Sí

Los módulos de comunicación ControlNet ofrecen lo siguiente:

- Compatibilidad con mensajería, tags estándar y de seguridad producidos/consumidos, y E/S distribuidas
- Admiten el uso de repetidores coaxiales y de fibra para aislamiento y mayor alcance.

Producción y consumo de datos a través de una red ControlNet

El controlador GuardLogix permite producir (enviar) y consumir (recibir) tags a través de redes ControlNet. El número total de tags que pueden ser producidos o consumidos está limitado por el número de conexiones disponibles en el controlador GuardLogix.

Conexiones mediante la red ControlNet

El número de conexiones que utiliza el controlador está determinado por la manera en que usted configura el controlador para que se comunique con otros dispositivos en el sistema. Las conexiones son asignaciones de recursos que proporcionan una comunicación más confiable entre dispositivos en comparación con los mensajes no conectados.

Las conexiones ControlNet pueden ser programadas o sin programar.

Tabla 16 – Conexiones ControlNet

Tipo de conexión	Descripción
Programada (única para la red ControlNet)	La conexión programada es única para la comunicación ControlNet. La conexión programada le permite enviar y recibir datos repetidamente a un intervalo predeterminado, el cual es el intervalo solicitado entre paquetes (RPI). Por ejemplo, una conexión a un dispositivo de E/S es una conexión programada porque recibe datos repetidamente desde el módulo a un intervalo especificado. Otras conexiones programadas incluyen conexiones a: • Dispositivos de comunicación • Tags producidos/consumidos En una red ControlNet, se debe usar el software RSNetWorx para ControlNet a fin de habilitar las conexiones programadas y establecer un tiempo de actualización de red (NUT). Al programar una conexión se reserva el ancho de banda de la red para administrar específicamente la conexión.
No programada	La conexión no programada es una transferencia de mensajes entre controladores activada por el intervalo solicitado entre paquetes (RPI) o el programa (tal como una instrucción MSG). La transmisión de mensajes no programada le permite enviar y recibir datos cuando es necesario. Las conexiones no programadas usan el resto del ancho de banda de la red después de que se asignan las conexiones programadas. Las conexiones producidas/consumidas de seguridad son conexiones no programadas.

Los módulos de comunicación 1756-CNB and 1756-CNBR admiten 64 conexiones CIP a través de una red ControlNet. Sin embargo, recomendamos que usted no configure más de 48 conexiones a fin de mantener un rendimiento óptimo.

El módulo 1756-CN2 admite 128 conexiones CIP a través de la red ControlNet.

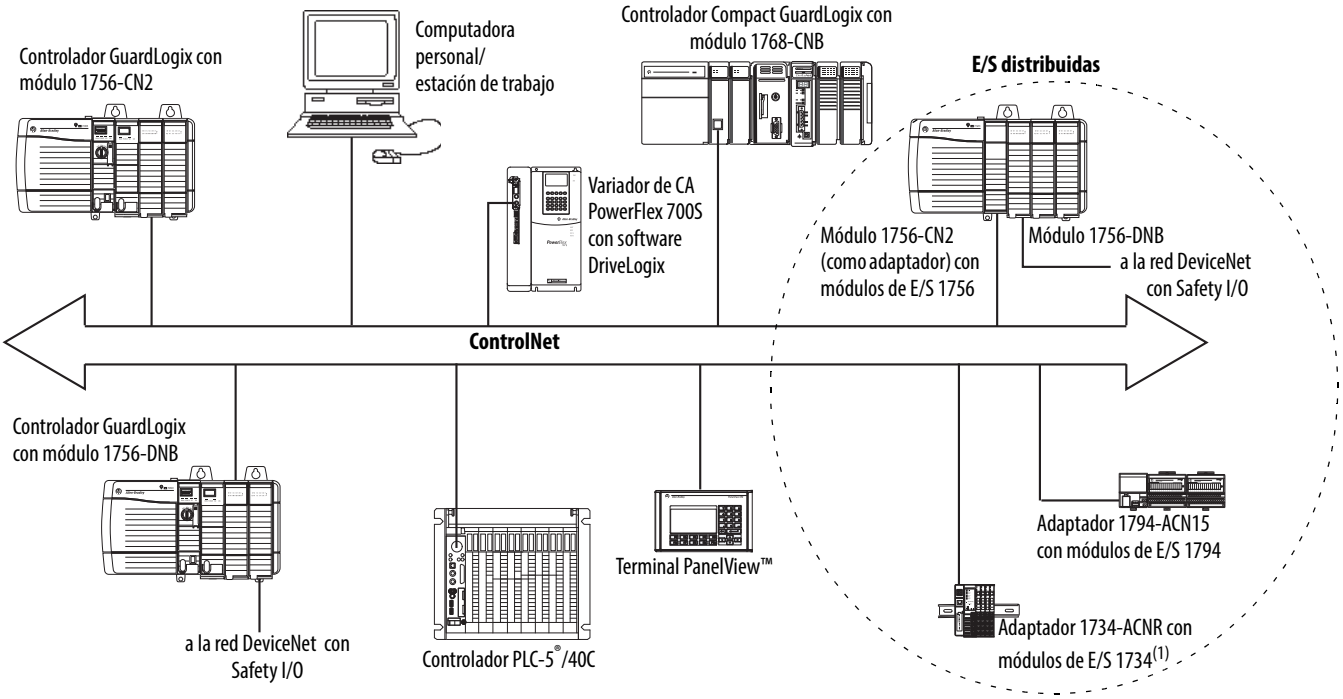
Ejemplo de comunicación ControlNet

Este ejemplo ilustra lo siguiente:

- Los controladores GuardLogix pueden producir y consumir tags estándar o de seguridad entre sí.
- GuardLogix Los controladores pueden iniciar instrucciones MSG que envían o reciben datos estándar o configuran dispositivos.(1)
- El módulo 1756-CN2 puede usarse como puente, dejando que el controlador GuardLogix produzca y consuma datos estándar y de seguridad hacia y desde dispositivos de E/S.
- La computadora personal puede cargar/descargar proyectos a los controladores.
- La computadora personal puede configurar dispositivos en la red ControlNet, y puede configurar la misma red.

(1) Los controladores GuardLogix no aceptan instrucciones MSG para datos de seguridad.

Figura 16 – Ejemplo de comunicación ControlNet



(1) El adaptador 1734-ACN no acepta módulos POINT Guard Safety I/O.

Conexiones ControlNet para E/S distribuidas

Para comunicarse con los dispositivos de E/S distribuidas a través de una red ControlNet, añada un puente ControlNet, un adaptador ControlNet y dispositivos de E/S a la carpeta I/O Configuration del controlador.

Comunicación DeviceNet

Para comunicarse e intercambiar datos con dispositivos de E/S de seguridad en redes DeviceNet, necesita un módulo 1756-DNB en el chasis local.

Para obtener información acerca de cómo instalar el módulo 1756-DNB, consulte el documento ControlLogix DeviceNet Scanner Module Installation Instructions, publicación 1756-IN566.

El módulo 1756-DNB permite la comunicación con dispositivos DeviceNet Safety y dispositivos DeviceNet estándar. Se pueden usar ambos tipos.

Estos productos se usan con las redes DeviceNet y el módulo 1756-DNB.

Tabla 17 – Productos para uso con redes DeviceNet

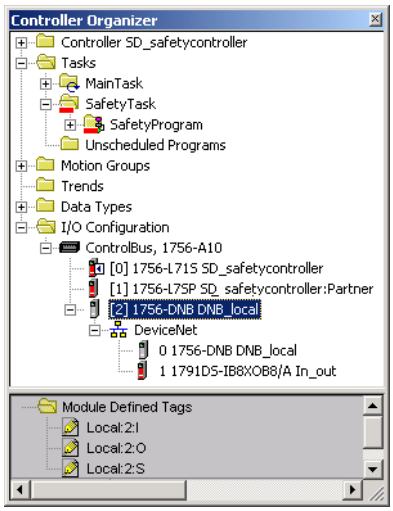
Producto	Se usa para	Requerido
Ambiente Studio 5000	• Configurar proyectos ControlLogix. • Definir la comunicación DeviceNet	Sí
Software RSNetWorx para DeviceNet	• Configurar dispositivos DeviceNet • Definir la lista de escán de esos dispositivos	Sí
Software RSLinx Classic o RSLinx Enterprise	• Configurar dispositivos de comunicación • Proporcionar diagnósticos • Establecer comunicación entre dispositivos	Sí

Conexiones DeviceNet para dispositivos de E/S de seguridad

Para obtener acceso a los dispositivos de E/S de seguridad en redes DeviceNet, añada un 1756-DNB al árbol de configuración de E/S del proyecto del controlador GuardLogix.

Los dispositivos de E/S de seguridad en las redes DeviceNet se añaden al proyecto debajo del módulo 1756-DNB, como se describe en el Capítulo 5, Cómo añadir, configurar, monitorear y reemplazar dispositivos CIP Safety I/O. Al añadir un dispositivo de E/S de seguridad, la aplicación Logix Designer crea automáticamente tags de datos de seguridad bajo el control del controlador para ese dispositivo.

Figura 17 – Módulo DeviceNet en el controlador en el árbol de configuración de E/S



Conexiones DeviceNet estándar

Si utiliza DeviceNet I/O estándar con el controlador GuardLogix, tiene que asignar dos conexiones por cada módulo 1756-DNB. Una conexión es para la configuración y el estado del módulo, y la otra es una conexión optimizada para rack, para los datos DeviceNet I/O.

Para utilizar el módulo 1756-DNB a fin de obtener acceso a datos estándar a través de la red DeviceNet, debe utilizar el software RSNetWorx para DeviceNet a fin de:

- crear un archivo de configuración para la red;
- configurar cada uno de los dispositivos estándar en la red;
- configurar el 1756-DNB;
- añadir los dispositivos de E/S estándar a la lista de escán del 1756-DNB.

Cuando se añade el módulo 1756-DNB a la configuración de E/S del controlador, la aplicación Logix Designer crea automáticamente un conjunto de tags estándar para los datos de entrada, salida y estado de la red.

Notas:

Cómo añadir, configurar, monitorear y reemplazar dispositivos CIP Safety I/O

Para obtener más información sobre la instalación, configuración y operación de los dispositivos de E/S de seguridad, consulte Para obtener más información en la página 11.

Adición de dispositivos de E/S de seguridad

Al añadir un dispositivo de E/S de seguridad al sistema, se debe definir una configuración específica para el mismo que incluya lo siguiente:

- Dirección de nodo para redes DeviceNet

  La dirección de nodo de un dispositivo de E/S de seguridad no se puede establecer en redes DeviceNet mediante la aplicación Logix Designer. Las direcciones de nodo se establecen mediante los interruptores giratorios de los dispositivos.

- Dirección IP para redes EtherNet/IP

  Para establecer la dirección IP, puede ajustar los interruptores giratorios del dispositivo, usar el software DHCP (disponible a través de Rockwell Automation), usar la aplicación Logix Designer o recuperar la dirección predeterminada de la memoria no volátil.

- Número de red de seguridad (SNN)

  Vea la página 67 para obtener información sobre cómo establecer el SNN.

- Firma de configuración

  Consulte la página 71 para obtener más información acerca de cuándo se establece automáticamente la firma de configuración y cuándo tiene que ser establecida por el usuario.
- Límite de tiempo de reacción

  Vea la página 67 para obtener información sobre cómo establecer el límite del tiempo de reacción.
- La entrada de seguridad, salida y parámetros de prueba completan la configuración del módulo.

Puede configurar los dispositivos de E/S de seguridad a través del controlador GuardLogix mediante la aplicación Logix Designer.

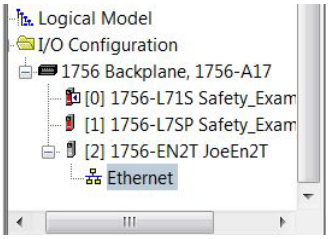
SUGERENCIA Los dispositivos de E/S de seguridad admiten datos estándar y de seguridad. La configuración del dispositivo define los datos que están disponibles.

Configuración de dispositivos de E/S de seguridad

Añada el dispositivo de E/S de seguridad al módulo de comunicación bajo la carpeta I/O Configuration del proyecto del controlador.

SUGERENCIA No se puede añadir ni eliminar un dispositivo de E/S de seguridad mientras se está en línea.

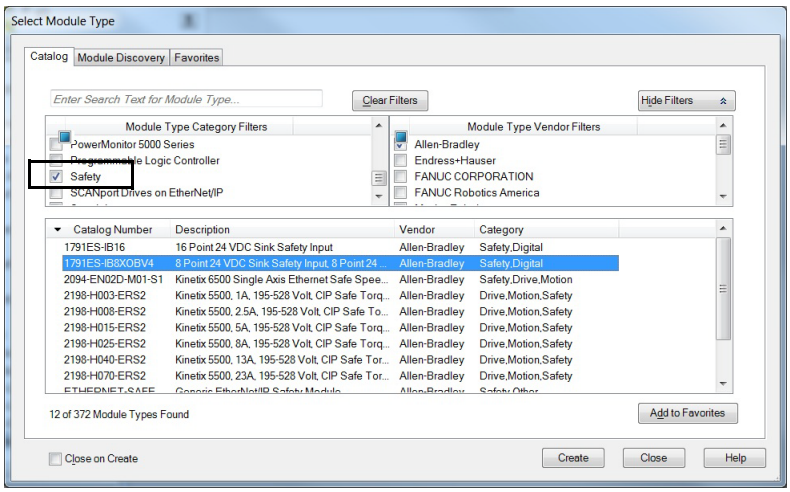
1. Haga clic con el botón derecho del mouse en la red DeviceNet o Ethernet y elija New Module.



En este ejemplo se utiliza una red Ethernet.

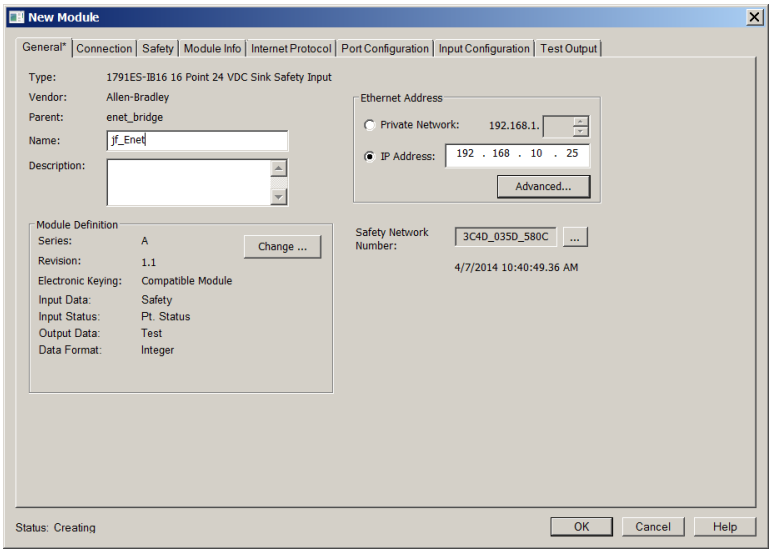
2. En la ficha Catalog, elija el dispositivo de E/S de seguridad.

SUGERENCIA Utilice los filtros para reducir la lista de los módulos entre los que puede elegir.



3. Haga clic en Create.

4. Escriba un nombre para el nuevo dispositivo.



5. En caso de que sea necesario modificar los ajustes de definición del módulo, haga clic en Change.
6. Introduzca la dirección de nodo para redes DeviceNet o la dirección IP para redes EtherNet/IP.

   En el menú desplegable solo aparecen números de nodo no utilizados.

   Si su red usa traductor de direcciones de red (NAT), consulte Definición de la dirección IP utilizando el traductor de direcciones de red (NAT) en la página 65.
7. Para modificar el número de red de seguridad, haga clic en el botón ... (si es necesario).

   Consulte la página 67 para obtener más información.
8. Establezca el límite de tiempo de reacción de la conexión en la ficha Safety.

   Consulte la página 67 para obtener más información.
9. Para completar la configuración del dispositivo de E/S de seguridad, consulte la documentación del usuario y la ayuda en línea de la aplicación Logix Designer.

Definición de la dirección IP utilizando el traductor de direcciones de red (NAT)

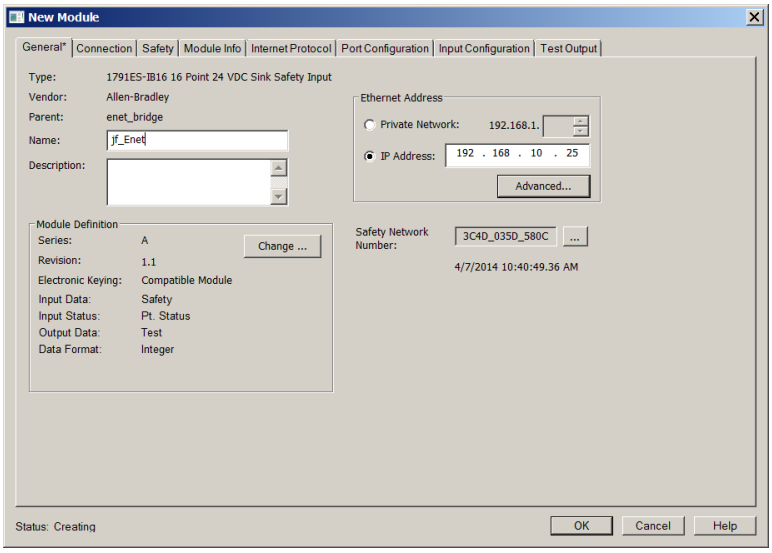
NAT traduce una dirección IP a otra dirección IP mediante un switch o router configurado para NAT. El router o switch traduce las direcciones de origen y destino dentro de los paquetes de datos a medida que el tráfico atraviesa las subredes.

Este servicio es útil si necesita volver a utilizar direcciones IP a lo largo de una red. Por ejemplo, con NAT es posible segmentar los dispositivos en varias subredes privadas idénticas manteniendo identidades únicas en la subred pública.

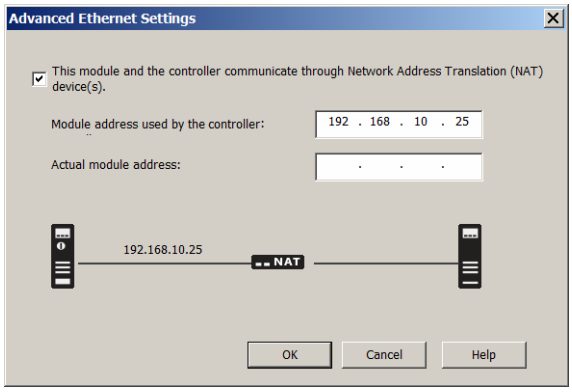
Si usa NAT, siga estos pasos para definir la dirección IP.

1. En el campo IP Address, introduzca la dirección IP que utilizará el controlador.

   Esta suele ser la dirección IP de la red pública cuando se utiliza NAT.



2. Haga clic en Advanced para abrir el cuadro de diálogo Advanced Ethernet Settings.



3. Marque la casilla de selección para indicar que este módulo y el controlador se comunican a través de dispositivos NAT.
4. Escriba la dirección del módulo real.

SUGERENCIA Si ha configurado la dirección IP mediante los interruptores giratorios, esta es la dirección que se define en el dispositivo. Alternativamente, la dirección del módulo real es la misma dirección que aparece en la ficha Internet Protocol del dispositivo.

5. Haga clic en OK.

El controlador usa la dirección traducida, pero el protocolo CIP Safety requiere la dirección real del dispositivo.

Establecimiento del número de red de seguridad (SNN)

La asignación de un SNN basado en tiempo es automática cuando se añaden nuevos dispositivos de E/S de seguridad. A los dispositivos de seguridad añadidos posteriormente a la misma red se les asigna el mismo SNN, definido dentro de la dirección más baja en esa red CIP Safety.

En la mayoría de las aplicaciones, basta con el SNN basado en tiempo automático. Sin embargo, hay casos en los que se debe modificar un SNN.

Consulte Asignación del número de red de seguridad (SNN) en la página 49.

Uso de conexiones de unidifusión en las redes EtherNet/IP

Las conexiones de unidifusión son conexiones punto a punto entre un nodo de origen y un nodo de destino. No tiene que introducir un rango de RPI mínimo o máximo ni un valor predeterminado para este tipo de conexión.

Para configurar las conexiones de unidifusión, seleccione la ficha Connection y marque Use Unicast Connection over EtherNet/IP.

Establecimiento del límite de tiempo de reacción de la conexión

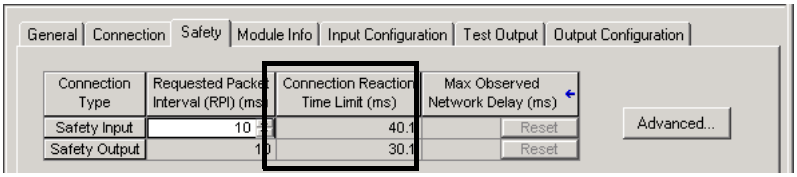
El límite de tiempo de reacción de la conexión corresponde a la longevidad máxima de los paquetes de seguridad en la conexión asociada. Si la longevidad de los datos utilizados por el dispositivo consumidor supera el límite de tiempo de reacción de la conexión, se produce un fallo de conexión. El límite de tiempo de reacción de la conexión se calcula mediante las ecuaciones siguientes:

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 18 – Límite de tiempo de reacción de la conexión



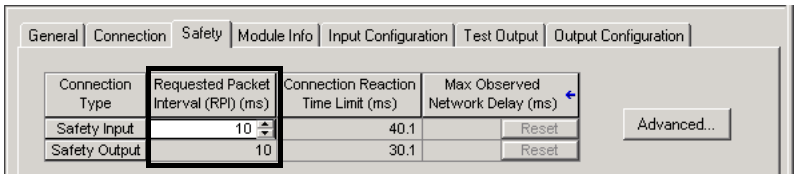
Especificación del intervalo solicitado entre paquetes (RPI)

El RPI especifica el período cuando 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 intervalo solicitado entre paquetes se introduce en incrementos de 1 ms, con un rango de 1...100 ms. El valor predeterminado es 10 ms.

El límite de tiempo de reacción de la conexión se ajusta inmediatamente cuando se cambia el RPI mediante la aplicación Logix Designer.

Figura 19 – 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.

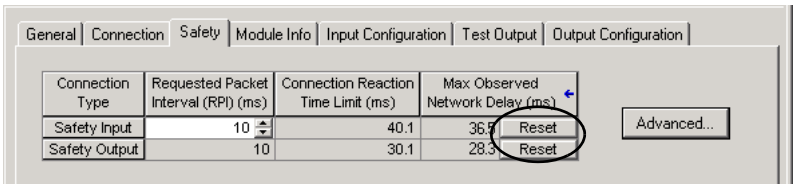
Consulte Especificación del período de la tarea de seguridad en la página 86 para obtener más información acerca del período de la tarea de seguridad.

Para aplicaciones típicas, generalmente es suficiente el intervalo solicitado entre paquetes predeterminado. 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 69.

Visualización del retardo de red máximo observado

Cuando el controlador GuardLogix recibe un paquete de seguridad, el software registra el retardo de red máximo observado. Para entradas de seguridad, el retardo de red máximo observado muestra el retardo de ida y vuelta desde el módulo de entrada hasta el controlador, y el recorrido inverso de confirmación al módulo de entrada. Para salidas de seguridad, este muestra el retardo de ida y vuelta del controlador al módulo de salida, y el recorrido inverso de confirmación al controlador. 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 20 – Restablecimiento del retardo de red máximo observado

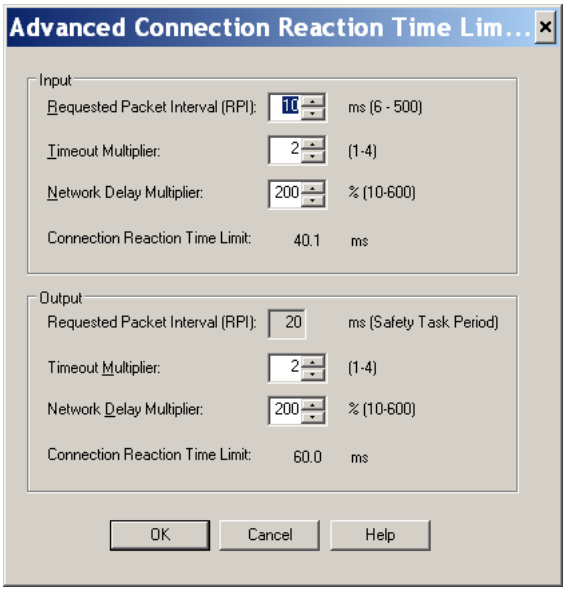


IMPORTANTE El tiempo de retardo de red máximo real del productor al consumidor es menor que el valor que se muestra en el campo Maximum Network Delay de la ficha Safety. En general, el retardo máximo real del mensaje es aproximadamente la mitad del valor del retardo de red máximo que se indica.

Establecimiento de los parámetros avanzados de límite de tiempo de reacción de la conexión

Configure los parámetros de conexión, tales como el multiplicador de interrupciones y multiplicador de retardo de red en el cuadro de diálogo Advanced Connection Reaction Time Limit.

Figura 21 – Configuración avanzada



Multiplicador de interrupciones

El multiplicador de interrupciones determina el número de RPI que se debe esperar por un paquete hasta declarar expirado el tiempo de espera de una conexión. Equivale al número de mensajes que pueden perderse antes de que se declare un error de conexión.

Por ejemplo, un multiplicador de interrupciones de 1 indica que deben recibirse mensajes durante cada intervalo RPI. Un multiplicador de interrupciones de 2 indica que se puede perder 1 mensaje siempre que se reciba como mínimo 1 mensaje en 2 veces el RPI (2 x RPI).

Multiplicador de retardo de red

El multiplicador de retardo de red define el tiempo de transporte de mensaje impuesto por el protocolo CIP Safety. El multiplicador de retardo de red especifica el retardo de ida y vuelta desde el productor hasta el consumidor, y la confirmación que se envía por el recorrido inverso. Se puede utilizar el multiplicador de retardo de red para reducir o incrementar el límite de tiempo de reacción de la conexión cuando el tiempo de transporte de mensaje impuesto sea considerablemente mayor o menor que el RPI. Por ejemplo, ajustar el multiplicador de retardo de red puede resultar útil cuando el RPI de una conexión de salida es igual a un período de tarea de seguridad prolongado.

En los casos en los que el RPI de entrada o de salida es relativamente lento o rápido en comparación con el tiempo de retardo de mensaje impuesto, se puede realizar un ajuste aproximado al multiplicador de retardo de red mediante uno de los dos métodos.

Método 1: Utilice la relación entre el RPI de entrada y el período de la tarea de seguridad. Utilice este método solo cuando se cumplan todas las condiciones siguientes:

- Si la ruta o el retardo es aproximadamente igual a la ruta o al retardo de salida.
- El RPI de entrada se ha configurado de modo que el tiempo de transporte de mensaje de entrada real sea menor que el RPI de entrada.
- El período de la tarea de seguridad es lento en comparación con el RPI de entrada.

Si se dan estas condiciones, el multiplicador de retardo de red de salida se puede ajustar de forma aproximada de la forma siguiente:

Multiplicador de retardo de red de entrada x [RPI de entrada ÷ período de la tarea de seguridad]

EJEMPLO **Cálculo aproximado del multiplicador de retardo de red de salida**

Si:

RPI de entrada = 10 ms
Multiplicador de retardo de red de entrada = 200%
Período de la tarea de seguridad = 20 ms

Por consiguiente, el multiplicador de retardo de red de salida es igual a:

200% x [10 ÷ 20] = 100%

Método 2: Utilice el retardo de red máximo observado. Si el sistema se hace funcionar durante un período prolongado en las peores condiciones de carga, el multiplicador de retardo de red se puede establecer a partir del retardo de red máximo observado. Este método se puede utilizar en una conexión de entrada o de salida. Si el sistema ha estado funcionando durante un período prolongado en las peores condiciones de carga, registre el retardo de red máximo observado.

El multiplicador de retardo de red se puede calcular de forma aproximada mediante la ecuación siguiente:

[Retardo de red máximo observado + Factor_de_margen] ÷ RPI

EJEMPLO **Cálculo del multiplicador de retardo de red a partir del retardo de red máximo observado**

Si:

RPI = 50 ms
Retardo de red máximo observado = 20 ms
Factor_de_margen = 10

Por tanto, el multiplicador de retardo de red es igual a:

[20 + 10] ÷ 50 = 60%

Tabla 18 – Más información

Recurso	Descripción
Sistemas controladores GuardLogix 5570 – Manual de referencia de seguridad, publicación 1756-RM099	Proporciona información acerca del cálculo de los tiempos de reacción.
Módulos de seguridad Guard I/O DeviceNet – Manual del usuario, publicación 1791DS-UM001	
Módulos de seguridad Guard I/O DeviceNet – Manual del usuario, publicación 1791ES-UM001	

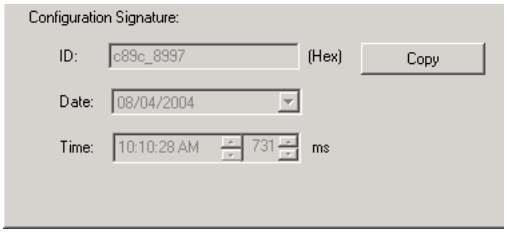
Explicación de la firma de configuración

Cada dispositivo de seguridad tiene una firma de configuración única que define la configuración del módulo. La firma de configuración está compuesta por un número de identificación, fecha y hora, y se usa para verificar la configuración de un módulo.

Configuración mediante la aplicación Logix Designer

Si el dispositivo de E/S se configura mediante la aplicación Logix Designer, la firma de configuración se genera automáticamente. Se puede ver y copiar la firma de configuración mediante la ficha Safety en el cuadro de diálogo Module Properties.

Figura 22 – Visualización y copia de la firma de configuración



Propietario de configuración diferente (conexión de solo recepción)

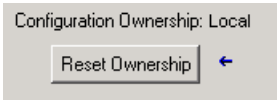
Cuando la configuración del dispositivo de E/S está en posesión de otro controlador, es necesario copiar la firma de configuración del módulo del proyecto de su propietario y pegarla en la ficha Safety del cuadro de diálogo Module Properties.

SUGERENCIA Si el dispositivo solamente está configurado para entradas, usted puede copiar y pegar la firma de configuración. Si el dispositivo tiene salidas de seguridad, estas están en posesión del controlador propietario de la configuración, y el cuadro de texto Configuration Signature no está disponible.

Restablecimiento de la propiedad del dispositivo de E/S de seguridad

Cuando el proyecto del controlador está en línea, la ficha Safety del cuadro de diálogo Module Properties muestra la posesión actual de la configuración. Si el proyecto abierto está en posesión de la configuración, se visualiza Local. Si la configuración está en posesión de otro dispositivo, aparece Remote junto al número de red de seguridad (SNN) y la dirección de nodo o el número de ranura del propietario de la configuración. Aparece Communication error cuando falla la lectura del dispositivo.

Cuando se trabaja en línea, haga clic en Reset Ownership para restablecer el dispositivo a su configuración original.



SUGERENCIA No se puede restablecer la propiedad cuando hay ediciones pendientes de las propiedades de los módulos, cuando existe una firma de tarea de seguridad o cuando está en bloqueo de seguridad.

Direccionamiento de datos de E/S de seguridad

Al añadir un dispositivo a la carpeta de configuración de E/S, la aplicación Logix Designer crea automáticamente tags bajo el control del controlador para el dispositivo.

La información de E/S se presenta como un conjunto de tags. Cada tag utiliza una estructura de datos, según el tipo y las funciones del dispositivo de E/S. El nombre del tag se basa en el nombre del dispositivo en el sistema.

Formato de dirección de módulos de E/S de seguridad

La dirección de un módulo de E/S de seguridad sigue este ejemplo.

EJEMPLO Modulename:Type.Member

Tabla 19 – Formato de dirección de dispositivos de E/S de seguridad

Donde	Es	
Modulename	Nombre del dispositivo de E/S de seguridad	
Type	Tipo de datos	Entrada: I Salida: O
Member	Datos específicos del dispositivo de E/S	
	Módulo solo de entrada	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members
	Módulo solo de salida	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:O.Output Members
	E/S combinadas	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members Modulename:O.Output Members

Formato de dirección de variadores Kinetix 5500, Kinetix 5700 y PowerFlex 527

La dirección de los variadores Kinetix 5500, Kinetix 5700 y PowerFlex 527 sigue este ejemplo.

EJEMPLO Drivename:Type.Member

Tabla 20 – Formato de dirección de dispositivos de E/S de seguridad de variador

Donde	Es	
Drivename	Nombre del variador Kinetix o PowerFlex	
Type	Tipo de datos	Entrada: SI Salida: SO
Member	Datos específicos del dispositivo de E/S	
	Módulo solo de entrada	Drivename:SI.ConnectionStatus Drivename:SI.RunMode Drivename:SI.ConnectionFaulted Drivename:SI.Status Drivename:SI.TorqueDisabled Drivename:SI.SafetyFault Drivename:SI.ResetRequired
	Módulo solo de salida	Drivename:SO.Command Drivename:SO.SafeTorqueOff Drivename:SO.Reset

Tabla 21 – Más recursos

Recurso	Descripción
Capítulo 9, Monitoreo de estado y manejo de fallos	Contiene información acerca del monitoreo de datos de tags de seguridad
Datos de tags y E/S en los controladores Logix5000 – Manual de programación, publicación 1756-PM004	Proporciona información sobre cómo direccionar dispositivos de E/S estándar

Monitoreo del estado de módulo de E/S de seguridad

Puede monitorear el estado del dispositivo de E/S de seguridad mediante mensajes explícitos o mediante los indicadores de estado de los módulos de E/S. Consulte los manuales de Guard I/O indicados en Para obtener más información en la página 11 para obtener información sobre la resolución de problemas de los módulos de E/S.

Tabla 22 – Funcionamiento de los indicadores de estado de los módulos Guard I/O

Indicador	Estado	Descripción		
		Módulos Guard I/O DeviceNet	**Módulos Guard I/O EtherNet/IP**	**Módulos POINT Guard I/O**
Estado de módulo (MS)	Apagado	Sin alimentación eléctrica		
	Verde fijo	Funcionando en condiciones normales.		
	Verde parpadeante	El dispositivo está inactivo.		
	Rojo parpadeante	Hay un fallo recuperable.	Hay un fallo recuperable o está en curso una actualización de firmware.	
	Rojo fijo	Hay un fallo irrecuperable.		
	Rojo/verde parpadeante	Autopruebas en curso.	Hay autopruebas en curso o el módulo no está debidamente configurado. Vea el indicador de estado de la red para obtener más información.	
Estado de red (NS)	Apagado	El dispositivo no está en línea o no está conectado a la alimentación eléctrica.		
	Verde fijo	El dispositivo está en línea; hay conexiones establecidas.		
	Verde parpadeante	El dispositivo está en línea; no hay conexiones establecidas.		
	Rojo parpadeante	Expiró el tiempo de espera de comunicación.	Expiró el tiempo de espera de comunicación o está en curso una actualización de firmware.	
	Rojo fijo	Fallo de comunicación. El dispositivo ha detectado un error que ha impedido la comunicación en red.		
	Rojo/verde parpadeante	El dispositivo se encuentra en estado de fallo de comunicación o se está estableciendo el número de red de seguridad (SNN).	Autoprueba en curso	No se aplica.
Puntos de entrada (IN*x*)	Apagado	La entrada de seguridad está desactivada.		
	Amarillo fijo	La entrada de seguridad está activada.		
	Rojo fijo	Se ha producido un error en el circuito de entrada.		
	Rojo parpadeante	Al seleccionar la operación de doble canal, se ha producido un error en el circuito de entrada del homólogo.		
Puntos de salida (O*x*)	Apagado	La salida de seguridad está desactivada.		
	Amarillo fijo	La salida de seguridad está activada.		
	Rojo fijo	Se ha producido un error en el circuito de salida.		
	Rojo parpadeante	Al seleccionar la operación de doble canal, se ha producido un error en el circuito de salida del homólogo.		
Puntos de salida de prueba (T*x*)	Apagado	No se aplica.	La salida está desactivada.	No se aplica.
	Amarillo fijo		La salida está activada.	
	Rojo fijo		Se ha producido un error en el circuito de salida.	
LOCK	Amarillo fijo	La configuración del dispositivo está bloqueada.	La aplicación Logix Designer no es compatible con esta función.	
	Amarillo parpadeante	La configuración del dispositivo es válida, pero el dispositivo no está bloqueado.		
	Amarillo apagado	No válido; no hay datos de configuración o se configuró el dispositivo.		
IN PWR	Verde apagado	No hay alimentación eléctrica de entrada.		No se aplica.
	Verde fijo	El voltaje de alimentación de entrada está dentro de especificaciones.		
	Amarillo fijo	El voltaje de alimentación de entrada está fuera de especificaciones.		
OUT PWR	Verde apagado	No hay alimentación de salida.		
	Verde fijo	El voltaje de alimentación de salida está dentro de especificaciones.		
	Amarillo fijo	El voltaje de alimentación de salida está fuera de especificaciones.		
PWR	Verde apagado	No se aplica.		Sin alimentación eléctrica
	Verde fijo			El voltaje de alimentación está dentro de especificaciones.
	Amarillo fijo			El voltaje de alimentación está fuera de especificaciones.

Consulte la página 11 para obtener más información sobre los indicadores de estado de los variadores Kinetix 5500, Kinetix 5700 y PowerFlex 527.

Restablecimiento de un módulo a la condición original

Si anteriormente se usó un módulo Guard I/O, restablezca el módulo a su condición original para borrar la configuración existente antes de instalarlo en una red de seguridad.

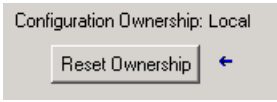
Cuando el proyecto del controlador está en línea, la ficha Safety del cuadro de diálogo Module Properties muestra la posesión actual de la configuración. Si el proyecto abierto está en posesión de la configuración, aparece Local. Si la configuración está en posesión de otro dispositivo, aparece Remote junto al número de red de seguridad (SNN) y la dirección de nodo o el número de ranura del propietario de la configuración. Aparece Communication error cuando falla la lectura del módulo.

Si la conexión es Local, debe inhibir la conexión del módulo antes de restablecer la posesión. Siga estos pasos para inhibir el módulo.

1. Haga clic con el botón derecho del mouse en el módulo y seleccione Properties.
2. Haga clic en la ficha Connection.
3. Marque Inhibit Connection.
4. Haga clic en Apply y, a continuación, en OK.

Siga estos pasos para restablecer el módulo a su configuración original cuando esté en línea.

1. Haga clic con el botón derecho del mouse en el módulo y seleccione Properties.
2. Haga clic en la ficha Safety.
3. Haga clic en Reset Ownership.



Reemplazo de un dispositivo mediante la aplicación Logix Designer

Puede usar la aplicación Logix Designer para reemplazar un dispositivo de E/S de seguridad en una red Ethernet. Para reemplazar un módulo Guard I/O en una red DeviceNet, su selección depende del tipo del módulo.

Tabla 23 – Software

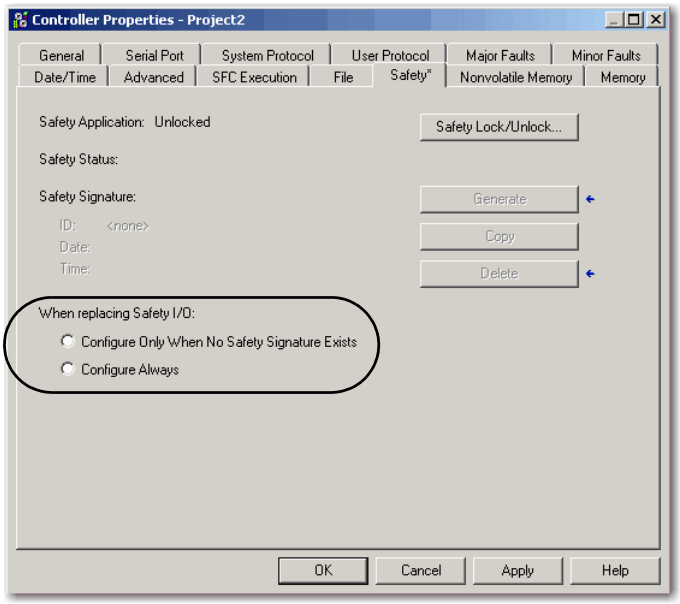
Si está usando un	Use	Consulte
Módulo 1791DS Guard I/O con adaptador 1756-DNB	La aplicación Logix Designer	A continuación
Módulo 1734 POINT Guard I/O con un adaptador 1734-PDN	Software RSNetWorx para DeviceNet	Reemplazo de un módulo POINT Guard I/O usando el software RSNetWorx para DeviceNet en la página 81

Si está confiando en una porción del sistema CIP Safety para mantener el comportamiento SIL 3 durante el reemplazo del dispositivo y las pruebas de funcionamiento, no se puede usar la función Configure Always. Vaya a Reemplazo con “Configure Only When No Safety Signature Exists” habilitado en la página 76.

Si no se ha confiado a todo el sistema de control CIP Safety encaminable el mantenimiento del SIL 3/PLe durante el reemplazo y la prueba de funcionamiento de un dispositivo, se puede utilizar la función Configure Always. Vaya a Reemplazo con "Configure Always" habilitado en la página 80.

El reemplazo del dispositivo de E/S de seguridad se configura en la ficha Safety del controlador GuardLogix.

Figura 23 – Reemplazo de dispositivo de E/S de seguridad



Reemplazo con "Configure Only When No Safety Signature Exists" habilitado

Cuando se reemplaza un dispositivo de E/S de seguridad, la configuración se descarga desde el controlador de seguridad si el DeviceID del nuevo dispositivo coincide con el del original. DeviceID es una combinación de dirección de nodo/IP y el número de red de seguridad (SNN) y se actualiza cada vez que se establece el SNN.

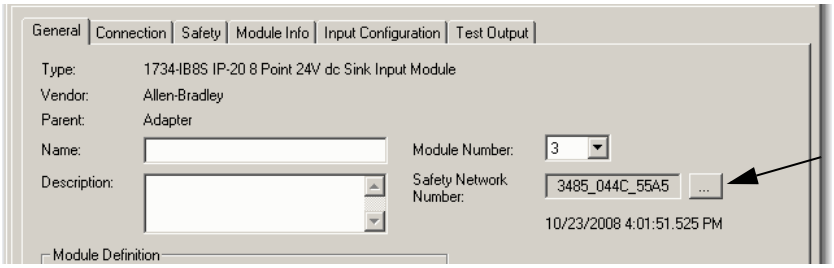
Si el proyecto se configura con la opción "Configure Only When No Safety Signature Exists", siga los pasos apropiados indicados en la Tabla 24 para reemplazar un dispositivo de E/S de seguridad basado en su escenario. Una vez que haya realizado correctamente los pasos, el DeviceID coincide con el original y habilita el controlador de seguridad para descargar la configuración de dispositivo apropiada y restablecer la conexión de seguridad.

Tabla 24 – Reemplazo de un módulo

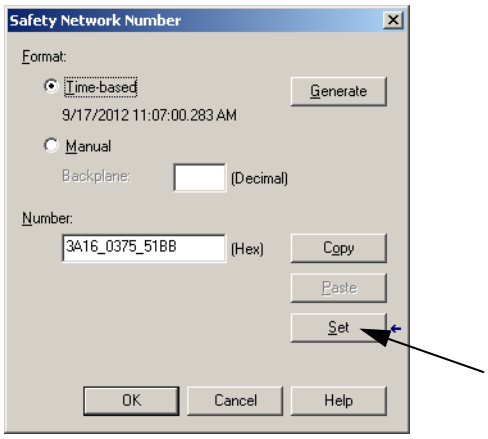
Existe la firma de seguridad GuardLogix	Condición del módulo de repuesto	Acción requerida
No	Sin SNN (condición original)	Ninguna. El dispositivo está listo para usar.
Sí o No	El mismo SNN que el de la configuración de tarea de seguridad original	Ninguna. El dispositivo está listo para usar.
Sí	Sin SNN (condición original)	Vea Escenario 1 – El módulo de repuesto está en su condición original y existe la firma de seguridad en la página 77.
Sí	SNN diferente al de la configuración de tarea de seguridad original	Vea Escenario 2 – El SNN del dispositivo de repuesto es diferente al del original y existe la firma de seguridad en la página 78.
No		Vea Escenario 3 – El SNN del dispositivo de repuesto es diferente al del original y no existe ninguna firma de seguridad en la página 79.

Escenario 1 – El módulo de repuesto está en su condición original y existe la firma de seguridad

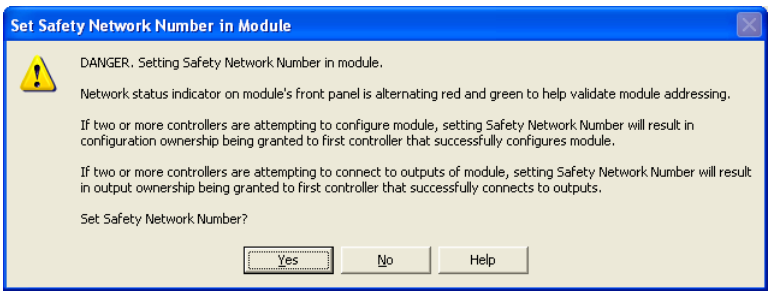
1. Retire el dispositivo de E/S antiguo e instale el nuevo.
2. Haga clic con el botón derecho del mouse en el dispositivo de E/S de seguridad de repuesto y seleccione Properties.
3. Haga clic en ... a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.



4. Haga clic en Set.



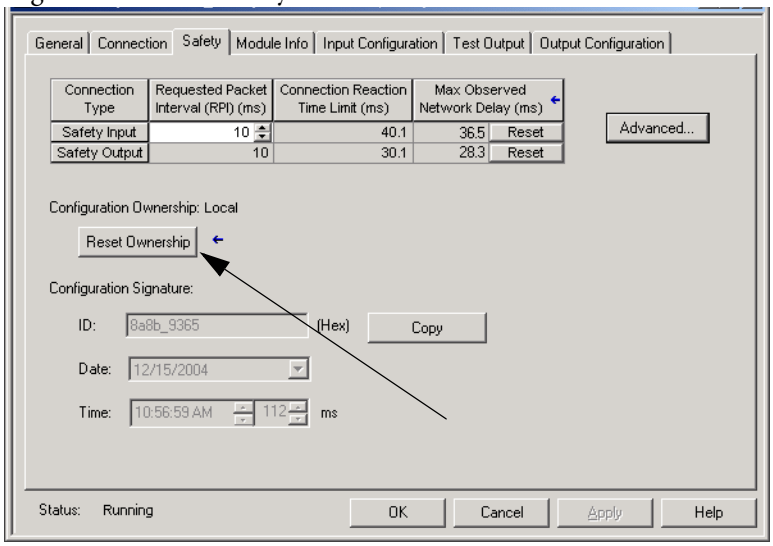
5. Compruebe que el indicador de estado de red (NS) se ilumine alternadamente de colores rojo a verde en el dispositivo correcto antes de hacer clic en Yes en el cuadro de diálogo de confirmación, para establecer el SNN y aceptar el dispositivo de repuesto.



6. Siga los procedimientos establecidos por su empresa para realizar la prueba funcional del dispositivo de E/S y el sistema reemplazados y autorizar el uso del sistema.

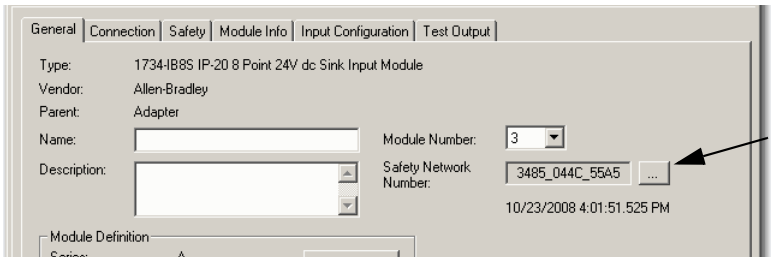
Escenario 2 – El SNN del dispositivo de repuesto es diferente al del original y existe la firma de seguridad

1. Retire el dispositivo de E/S antiguo e instale el nuevo.
2. Haga clic con el botón derecho del mouse en el dispositivo de E/S de seguridad y seleccione Properties.
3. Haga clic en la ficha Safety.

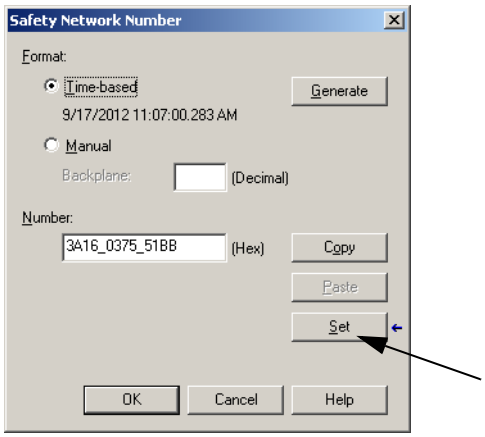


4. Haga clic en Reset Ownership.
5. Haga clic en OK.
6. Haga clic con el botón derecho del mouse en el dispositivo y seleccione Properties.

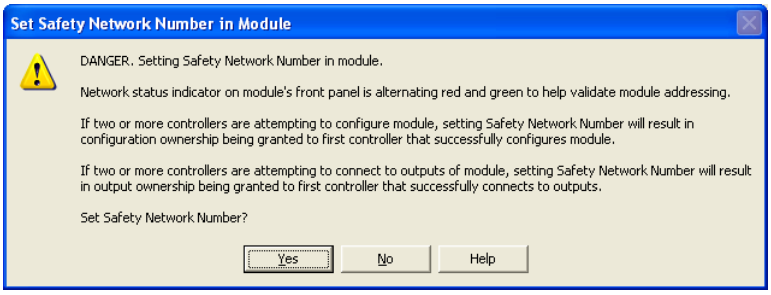
7. Haga clic en ... a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.



8. Haga clic en Set.



9. Compruebe que el indicador de estado de red (NS) se ilumine alternadamente de colores rojo a verde en el dispositivo correcto antes de hacer clic en Yes en el cuadro de diálogo de confirmación, para establecer el SNN y aceptar el dispositivo de repuesto.

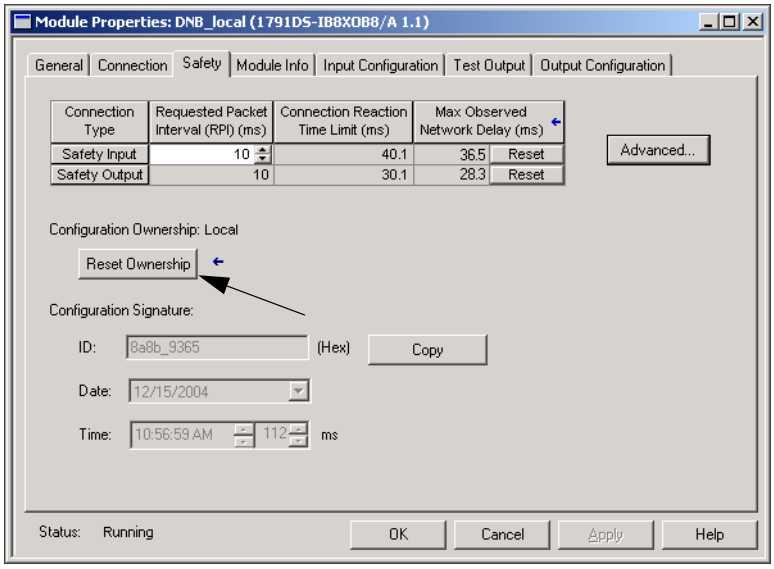


10. Siga los procedimientos establecidos por su empresa para realizar la prueba de funcionamiento del dispositivo de E/S y el sistema reemplazados y autorizar el uso del sistema.

Escenario 3 – El SNN del dispositivo de repuesto es diferente al del original y no existe ninguna firma de seguridad

1. Retire el dispositivo de E/S antiguo e instale el nuevo.
2. Haga clic con el botón derecho del mouse en el dispositivo de E/S de seguridad y seleccione Properties.

3. Haga clic en la ficha Safety.



4. Haga clic en Reset Ownership.
5. Haga clic en OK.
6. Siga los procedimientos establecidos por su empresa para realizar la prueba de funcionamiento del dispositivo de E/S y el sistema reemplazados y autorizar el uso del sistema.

Reemplazo con "Configure Always" habilitado

ATENCIÓN: Habilite la función "Configure Always" solo si todo el sistema de control CIP Safety **no** se usa para mantener el comportamiento SIL 3 durante el reemplazo y las pruebas de funcionamiento de un dispositivo.

No ponga dispositivos en su condición original en una red CIP Safety cuando la función Configure Always está habilitada, excepto mientras está siguiendo este procedimiento de reemplazo.

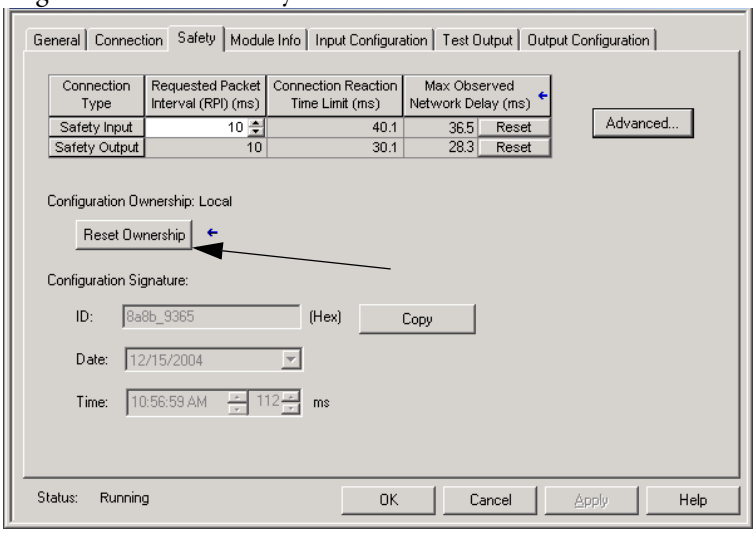
Si la función "Configure Always" está habilitada en el proyecto del controlador, el controlador automáticamente verifica y se conecta a un dispositivo de repuesto que cumple con todos los requisitos siguientes:

- El controlador tiene datos de configuración para un dispositivo compatible en esa dirección de red.
- El dispositivo se encuentra en su condición original o tiene un SNN que coincide con la configuración.

Si el proyecto está configurado para usar la opción "Configure Always", siga los pasos apropiados para reemplazar un dispositivo de E/S de seguridad.

1. Retire el dispositivo de E/S antiguo e instale el nuevo.
   a. Si el dispositivo se encuentra en su condición original, vaya al paso 6. No se requiere realizar ninguna acción para que el controlador GuardLogix tome posesión del dispositivo.
   b. Si ocurre una desigualdad de SNN, vaya al siguiente paso para restablecer el dispositivo a su condición original.
2. Haga clic con el botón derecho del mouse en el dispositivo de E/S de seguridad y seleccione Properties.

3. Haga clic en la ficha Safety.



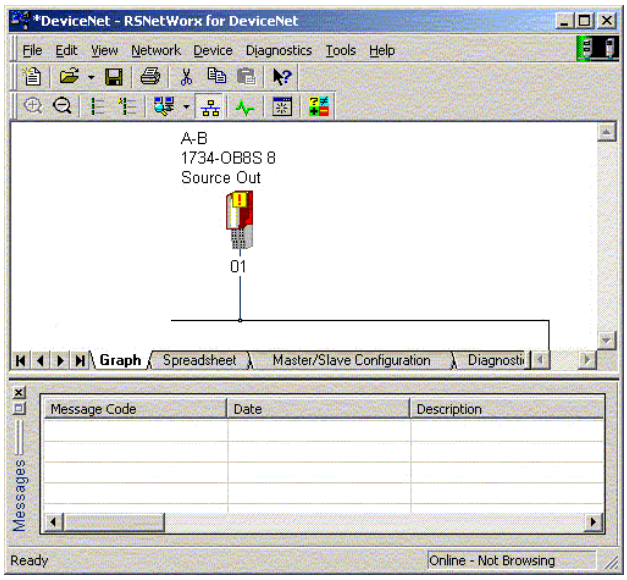
4. Haga clic en Reset Ownership.
5. Haga clic en OK.
6. Siga los procedimientos establecidos por su empresa para realizar la prueba de funcionamiento del dispositivo de E/S y el sistema reemplazados y autorizar el uso del sistema.

Reemplazo de un módulo POINT Guard I/O usando el software RSNetWorx para DeviceNet

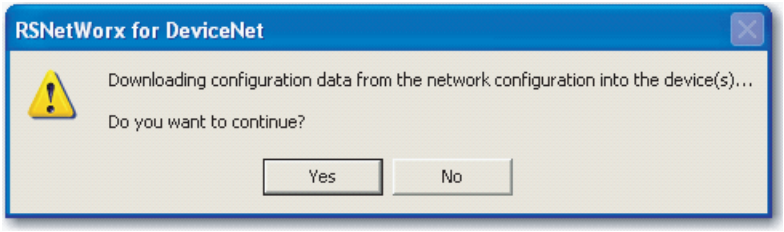
Siga estos pasos para reemplazar un módulo POINT Guard I/O cuando el módulo y el controlador están en una red DeviceNet.

1. Reemplace el módulo y use el mismo número de nodo que el del módulo original.
2. En el software RSNetWorx para DeviceNet, abra el proyecto.

   Si el módulo de repuesto está en su condición original o tiene un SNN que no coincide con el del módulo original, el módulo aparecerá con un signo de exclamación.

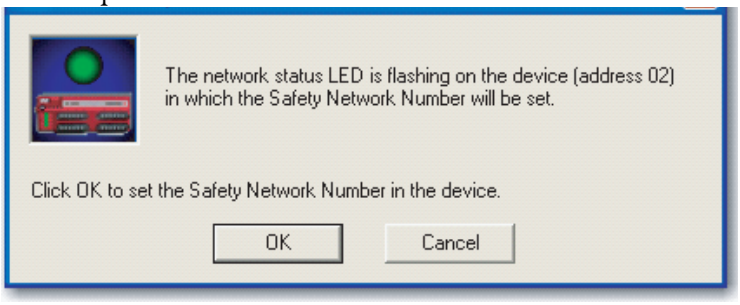


3. Haga clic con el botón derecho del mouse en el módulo y elija Download to Device.



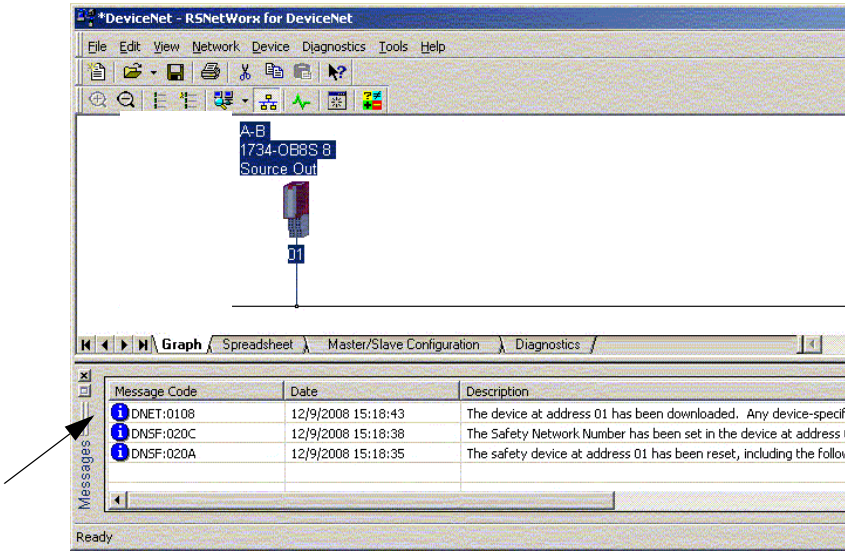
4. Haga clic en Yes para confirmar.
5. Haga clic en Download en el cuadro de diálogo Safety Network Number Mismatch para establecer el SNN en el módulo de repuesto.

6. Verifique que el indicador de estado de la red (NS) esté parpadeando en el módulo correcto y haga clic en OK para establecer el SNN en dicho dispositivo.



El software RSNetWorx para DeviceNet confirma que el SNN está establecido.

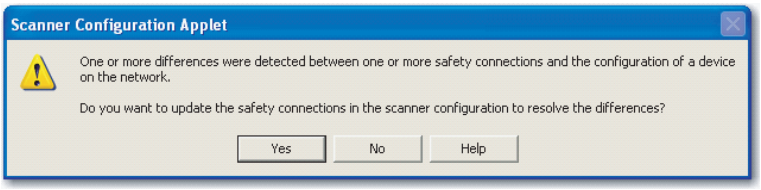
Una vez que la descarga se realiza exitosamente, la vista del proyecto principal muestra este mensaje: "The device at address *xx* has been downloaded. Any device-specific messages related to the download operation are displayed separately."



Suponiendo que esta es la configuración correcta proveniente del archivo DNT original, el SNN y la firma de configuración ahora coinciden con los del original. Si ya está conectado con el controlador, está hecha la conexión. El controlador no necesita ponerse fuera del modo de marcha para descargar al módulo de repuesto.

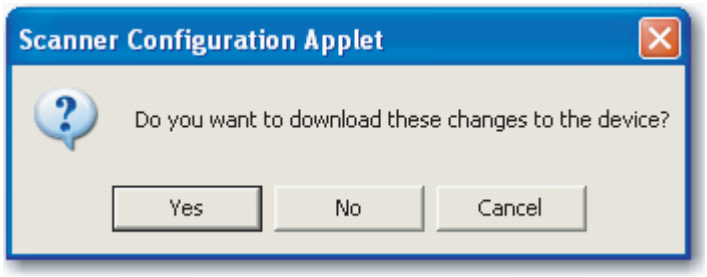
Si descarga esta configuración a una configuración temporal, coloque el módulo en la red y este se conecta automáticamente al controlador.

Si la configuración descargada al módulo no es la del archivo DNT original, la firma de configuración no coincidirá con la del original. Incluso si vuelve a crear los mismos parámetros en un nuevo archivo DNT, las porciones de tiempo y datos de la firma serán diferentes, por lo que no se hará la conexión al controlador. Si esto ocurre, haga clic en la ficha Safety Connection del controlador que le indicó que la firma de configuración es diferente, lo que ofrece la opción de igualar la nueva firma de configuración. Sin embargo, revalide primero el sistema de seguridad porque este no está usando el archivo DNT original.



7. Haga clic en Yes.

   Esto hace que el controlador salga del modo marcha y le indica que descargue los cambios.



8. Haga clic en Yes para descargar la nueva configuración de conexión al controlador.

   Cuando haya concluido la descarga, coloque el controlador nuevamente en el modo de marcha y se establecerá la conexión al módulo de repuesto.

9. Siga los procedimientos establecidos por su empresa para realizar la prueba de funcionamiento del módulo de E/S reemplazado y del sistema, y para autorizar el uso del sistema.

Desarrollo de aplicaciones de seguridad

Este capítulo explica los componentes que conforman un proyecto de seguridad y proporciona información sobre el uso de funciones que ayudan a proteger la integridad de la aplicación de seguridad, por ejemplo, como la firma de tarea de seguridad y el enclavamiento de seguridad.

En cuanto a las pautas y a los requisitos para el desarrollo y la puesta en marcha de aplicaciones de seguridad SIL 3 y PLe, consulte el documento Sistemas controladores GuardLogix 5570 – Manual de referencia de seguridad, publicación 1756-RM099.

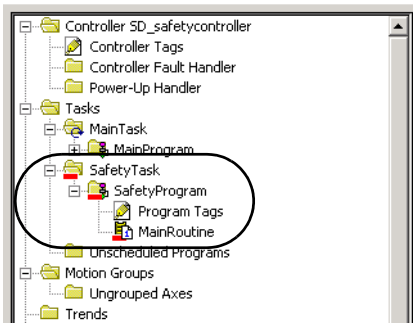
En el manual de referencia de seguridad se tratan los temas siguientes:

- Creación de una especificación detallada del proyecto
- Escritura, documentación y pruebas de la aplicación
- Generación de la firma de tarea de seguridad para identificar y proteger el proyecto
- Confirmación del proyecto mediante la impresión o la visualización del proyecto cargado y comparación manual de las configuraciones, los datos de seguridad y la lógica del programa de seguridad
- Comprobación del proyecto con casos de prueba, simulaciones, pruebas de verificación de funcionamiento y la revisión independiente de seguridad en caso necesario
- Bloqueo de la aplicación de seguridad
- Cálculo del tiempo de reacción del sistema

La tarea de seguridad

Cuando se crea un proyecto de controlador de seguridad, la aplicación Logix Designer crea automáticamente una tarea de seguridad con un programa de seguridad y una rutina (de seguridad) principal.

Figura 24 – Tarea de seguridad en el Controller Organizer



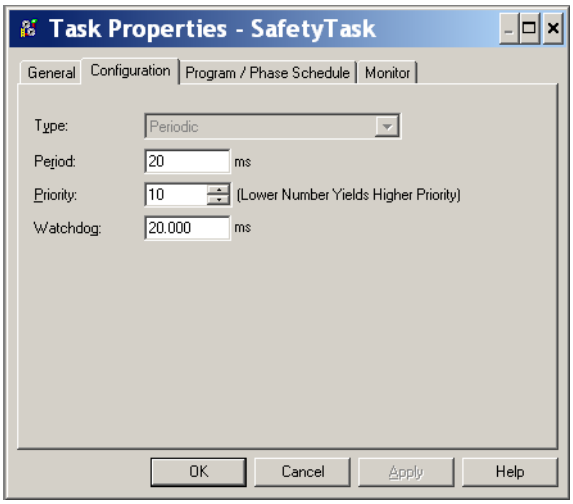
Dentro de la tarea de seguridad se pueden usar varios programas de seguridad, compuestos a su vez por varias rutinas de seguridad. El controlador GuardLogix acepta una tarea de seguridad. La tarea de seguridad no se puede eliminar.

Dentro de la tarea de seguridad no se pueden secuenciar programas estándar ni ejecutar rutinas estándar.

Especificación del período de la tarea de seguridad

La tarea de seguridad es una tarea periódica temporizada. Usted establece la prioridad de la tarea y el tiempo del temporizador de vigilancia en el cuadro de diálogo Task Properties - Safety Task. Para abrir el cuadro de diálogo, haga clic con el botón derecho del mouse en la tarea de seguridad y elija Properties.

Figura 25 – Configuración del período de la tarea de seguridad



La tarea de seguridad es de alta prioridad. Especifique el período de la tarea de seguridad (en ms) y el temporizador de vigilancia (watchdog) de la tarea de seguridad (en ms). El período de la tarea de seguridad es el período con el que se ejecuta la tarea de seguridad. El temporizador de vigilancia de la tarea de seguridad es el tiempo máximo que puede transcurrir desde que se inicia la ejecución de la tarea de seguridad hasta que se completa.

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 terminar la ejecución de la lógica antes de volverse a activar. Si se sobrepasa el tiempo de espera del temporizador de vigilancia de la tarea de seguridad, se genera un fallo de seguridad no recuperable en el controlador de seguridad.

El período de la tarea de seguridad afecta directamente el tiempo de reacción del sistema.

El documento Sistemas controladores GuardLogix 5570 – Manual de referencia de seguridad, publicación 1756-RM099, proporciona información detallada sobre cómo calcular el tiempo de reacción del sistema.

Ejecución de la tarea de seguridad

La tarea de seguridad se ejecuta del mismo modo que la tarea periódica estándar, salvo por las excepciones siguientes:

- La tarea de seguridad no comienza a ejecutarse mientras el controlador primario y el homólogo de seguridad no hayan establecido su asociación de control. (Las tareas estándar empiezan a ejecutarse en cuanto el controlador pasa al modo de marcha).
- Todos los tags de entrada de seguridad (entradas, consumidos y asignados) se actualizan y se congelan cuando se empieza a ejecutar la tarea de seguridad.

  Consulte la página 98 si desea información acerca de la asignación de tags de seguridad.
- Los valores de tags de salida de seguridad (salida y producidos) se actualizan cuando finaliza la ejecución de la tarea de seguridad.

Programas de seguridad

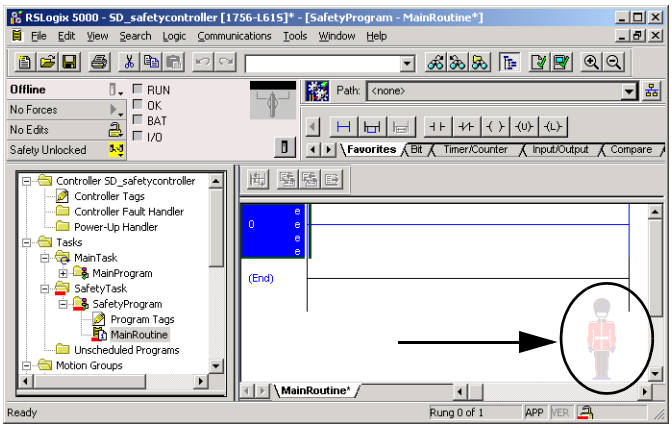
Los programas de seguridad tienen todos los atributos de los programas estándar, salvo que solo se pueden programar en la tarea de seguridad y solo pueden contener componentes de seguridad. Los programas de seguridad solo pueden contener rutinas de seguridad. Una rutina de seguridad debe definirse como la rutina principal y otra rutina de seguridad se puede definir como rutina de fallo.

Los programas de seguridad no pueden contener rutinas estándar ni tags estándar.

Rutinas de seguridad

Las rutinas de seguridad tienen todos los atributos de las rutinas estándar, salvo que solo pueden existir en un programa de seguridad. Actualmente, solo el diagrama de lógica de escalera es compatible con las rutinas de seguridad.

SUGERENCIA Una imagen semitransparente distingue visualmente una rutina de seguridad de una rutina estándar.



Tags de seguridad

Un tag es un área de la memoria del controlador donde se almacenan datos. Los tags son un mecanismo básico para asignar memoria, hacer referencia a datos de la lógica y monitorear datos. Los tags de seguridad tienen todos los atributos de los tags estándar, además de mecanismos certificados para proporcionar el nivel de integridad de datos SIL 3.

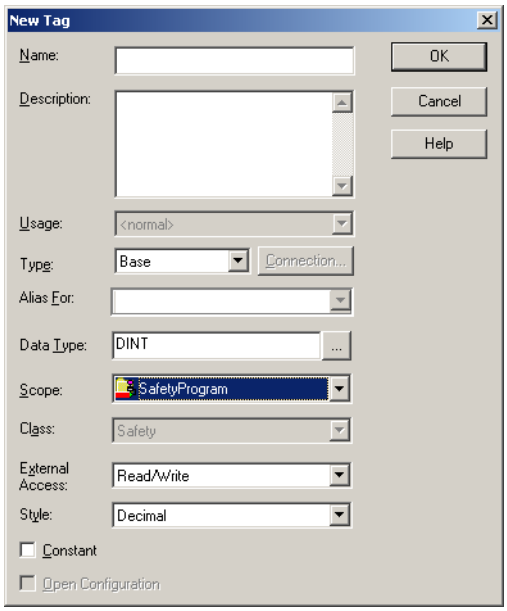
Al crear un tag, usted asigna las siguientes propiedades.

- Nombre
- Descripción (opcional)
- Tipo de tag
- Tipo de datos
- Alcance
- Clase
- Estilo
- Acceso externo

También puede especificar si un valor de tag es una constante.

Para crear un tag de seguridad, abra el cuadro de diálogo New Tag; para ello haga clic con el botón derecho del mouse en Controller Tags o Program Tags y, a continuación, elija New Tag.

Figura 26 – Creación de un nuevo tag



Tipo de tag

La Tabla 25 define los cuatro tipos de tags.

Tabla 25 – Cuatro tipos de tags

Tipo de tag	Descripción
Tag de base	Estos tags almacenan valores utilizados por la lógica dentro del proyecto.
Tag de alias	Tag que hace referencia a otro tag. Un tag de alias puede hacer referencia a otro tag de alias o a un tag de base. Un tag de alias puede hacer referencia además a otro tag mediante una referencia a un miembro de una estructura, a un elemento de matriz o a un bit dentro de un tag o un miembro. **IMPORTANTE:** No utilice tags de alias entre tags estándar y tags de seguridad en aplicaciones de seguridad. En lugar de ello, los tags estándar pueden asignarse a tags de seguridad mediante la función de asignación a tags de seguridad. Consulte Asignación de un tag de seguridad en la página 98.
Tag producido	Tag que un controlador pone a disposición para que otros controladores lo utilicen. Como máximo 15 controladores pueden consumir (recibir) simultáneamente los datos. Un tag producido envía sus datos a uno o más tags consumidores sin utilizar lógica. Los datos de tags producidos se envían al RPI del tag consumidor.
Tag consumido	Tag que recibe los datos de un tag producido. El tipo de datos del tag consumido debe coincidir con el tipo de datos del tag producido. El intervalo solicitado entre paquetes (RPI) del tag consumido determina el período cuando se actualizan los datos.

Tipo de datos

El tipo de datos define el tipo de datos que el tag almacena, como bits o números enteros.

Los tipos de datos se pueden combinar para formar estructuras. Una estructura proporciona un tipo de datos único que coincide con una necesidad específica. Dentro de una estructura, cada tipo de datos individuales se conoce como miembro. Al igual que los tags, los miembros tienen un nombre y un tipo de datos. Usted puede crear sus propias estructuras, como tipos de datos definidos por el usuario.

Los controladores Logix contienen tipos de datos predefinidos que deben utilizarse con instrucciones específicas.

Se permiten estos tipos de datos para los tags de seguridad.

Tabla 26 – Tipos de datos válidos para tags de seguridad

AUX_VALVE_CONTROL	DCI_STOP_TEST_MUTE	MANUAL_VALVE_CONTROL
BOOL	DINT	MUTING_FOUR_SENSOR_BIDIR
CAM_PROFILE	DIVERSE_INPUT	MUTING_TWO_SENSOR_ASYM
CAMSHAFT_MONITOR	EIGHT_POS_MODE_SELECTOR	MUTING_TWO_SENSOR_SYM
CB_CONTINUOUS_MODE	EMERGENCY_STOP	MOTION_INSTRUCTION
CB_CRANKSHAFT_POS_MONITOR	ENABLE_PENDANT	FASE
CB_INCH_MODE	EXT_ROUTINE_CONTROL	PHASE_INSTRUCTION
CB_SINGLE_STROKE_MODE	EXT_ROUTINE_PARAMETERS	REDUNDANT_INPUT
CONFIGURABLE_ROUT	FBD_BIT_FIELD_DISTRIBUTE	REDUNDANT_OUTPUT
CONNECTION_STATUS	FBD_CONVERT	SAFETY_MAT
CONTROL	FBD_COUNTER	SERIAL_PORT_CONTROL
COUNTER	FBD_LOGICAL	SFC_ACTION
DCA_INPUT	FBD_MASK_EQUAL	SFC_STEP
DCAF_INPUT	FBD_MASKED_MOVE	SFC_STOP
DCI_MONITOR	FBD_TIMER	SINT
DCI_START	FIVE_POS_MODE_SELECTOR	STRING
DCI_STOP	INT	THRS_ENHANCED
DCI_STOP_TEST	LIGHT_CURTAIN	TIMER
DCI_STOP_TEST_LOCK	MAIN_VALVE_CONTROL	TWO_HAND_RUN_STATION

Alcance

El alcance de un tag determina dónde se puede obtener acceso a los datos del tag. Cuando se crea un tag, se define como tag de controlador (datos globales) o tag de programa para un programa estándar o de seguridad específico (datos locales). Los tags de seguridad pueden estar bajo el control del controlador o bajo el control del programa de seguridad.

Tags bajo el control del controlador

Cuando los tags de seguridad están bajo el control del controlador, todos los programas tienen acceso a los datos de seguridad. Los tags deben estar bajo el control del controlador si se usan de las siguientes maneras:

- En más de un programa en el proyecto
- Para producir o consumir datos
- Para comunicarse con un terminal PanelView™
- En la asignación de un tag de seguridad

  Vea Asignación de un tag de seguridad en la página 98 para obtener más información.

Los tags de seguridad bajo el control del controlador pueden ser leídos, pero no escritos, por rutinas estándar.

IMPORTANTE	Los tags de seguridad bajo el control del controlador pueden ser leídos por cualquier rutina estándar. La velocidad de actualización de los tags de seguridad se basa en el período de la tarea de seguridad.

Los tags asociados a E/S de seguridad y a datos de seguridad producidos o consumidos deben ser tags de seguridad bajo el control del controlador. En el caso de los tags de seguridad producidos o consumidos, es necesario crear un tipo de datos definido por el usuario con el primer miembro de la estructura de tag reservado para el estado de la conexión. Este miembro es un tipo de datos predefinido llamado CONNECTION_STATUS.

Tabla 27 – Recursos adicionales

Recurso	Descripción
Conexiones de seguridad en la página 121	Proporciona más información acerca del miembro CONNECTION_STATUS.
Datos de tags y E/S en los controladores Logix5000 – Manual de programación, publicación 1756-PM004	Proporciona instrucciones para crear tipos de datos definidos por el usuario.

Tags bajo el control del programa

Cuando los tags están bajo el control del programa, los datos se aíslan de los otros programas. Los nombres de tags bajo el control del programa se pueden reutilizar entre programas.

Los tags de seguridad bajo el control del programa de seguridad solo pueden ser leídos o escritos mediante una rutina de seguridad bajo el control del mismo programa de seguridad.

Clase

Los tags se pueden clasificar como tags estándar o de seguridad. Los tags clasificados como tags de seguridad deben tener un tipo de datos permitido para tags de seguridad.

Cuando se crean tags bajo el control del programa, la clase se especifica automáticamente en función de si el tag fue creado en un programa estándar o en un programa de seguridad.

Cuando se crean tags bajo el control del controlador, debe seleccionarse manualmente la clase de tags.

Valor constante

Cuando usted designa un tag como valor constante, este no puede ser modificado por la lógica del controlador ni por una aplicación externa tal como una interface operador-máquina (HMI). Los tags de valor constante no pueden forzarse.

La aplicación Logix Designer puede modificar tags estándar constantes y tags de seguridad siempre que no esté presente una firma de tarea de seguridad. Los tags de seguridad no pueden modificarse si está presente una firma de tarea de seguridad.

Acceso externo

El acceso externo define el nivel de acceso permitido para dispositivos externos, tales como una interface operador-máquina, para ver o modificar valores de tags. El acceso mediante la aplicación Logix Designer no se ve afectado por este ajuste. El valor predeterminado es lectura/escritura.

Tabla 28 – Niveles de acceso externo

Ajuste de acceso externo	Descripción
None	Los tags no son accesibles desde el exterior del controlador.
Read Only	Los tags pueden examinarse o leerse, pero no escribirse desde fuera del controlador.
Read/Write	Los tags estándar pueden examinarse, leerse y escribirse hacia/desde fuera del controlador.

En el caso de los tags de alias, el tipo de acceso externo es igual al tipo configurado para el tag receptor base.

Tags de seguridad producidos/consumidos

Para transferir datos de seguridad entre controladores GuardLogix se utilizan tags de seguridad producidos y consumidos. Los tags producidos y consumidos requieren conexiones. El tipo de conexión predeterminado para los tags producidos y consumidos es el de unidifusión.

Tabla 29 – Conexiones de tags producidos y consumidos

Tag	Descripción de la conexión
Producido	Un controlador GuardLogix puede producir (enviar) tags de seguridad a otros controladores 1756 o 1768 GuardLogix. El controlador productor utiliza una sola conexión para cada consumidor.
Consumido	Los controladores GuardLogix pueden consumir (recibir) tags de seguridad de otros controladores 1756 o 1768 GuardLogix. Cada tag consumido consume una conexión.

Los tags de seguridad producidos y consumidos están sujetos a las restricciones siguientes:

- solo se pueden compartir tags de seguridad bajo el control del controlador;
- los tags de seguridad producidos y consumidos están limitados a 128 bytes;
- los pares de tags producidos y consumidos deben ser del mismo tipo de datos definido por el usuario;
- el primer miembro del tipo de datos definido por el usuario debe ser el tipo de datos CONNECTION_STATUS predefinido;
- el intervalo solicitado entre paquetes (RPI) del tag de seguridad consumido debe coincidir con el período de la tarea de seguridad del controlador GuardLogix productor.

Para configurar correctamente tags de seguridad producidos y consumidos para compartir datos entre controladores de seguridad homólogos, debe configurar correctamente los controladores de seguridad homólogos, producir un tag de seguridad y consumir un tag de seguridad, como se describe a continuación.

Configuración de los números de red de seguridad de los controladores de seguridad homólogos

El controlador de seguridad homólogo está sujeto a los mismos requisitos de configuración que el controlador de seguridad local. El controlador de seguridad homólogo también debe tener un número de red de seguridad (SNN). El SNN del controlador de seguridad homólogo depende de su ubicación en el sistema.

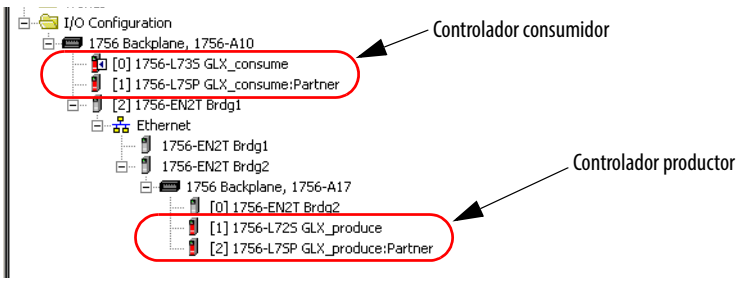
Tabla 30 – SNN y ubicación del controlador

Ubicación del controlador de seguridad homólogo	SNN
Ubicado en el chasis local	Los controladores GuardLogix de un chasis común tienen el mismo SNN.
Ubicado en otro chasis	El controlador debe tener un SNN único.

Siga estos pasos para copiar y pegar el SNN.

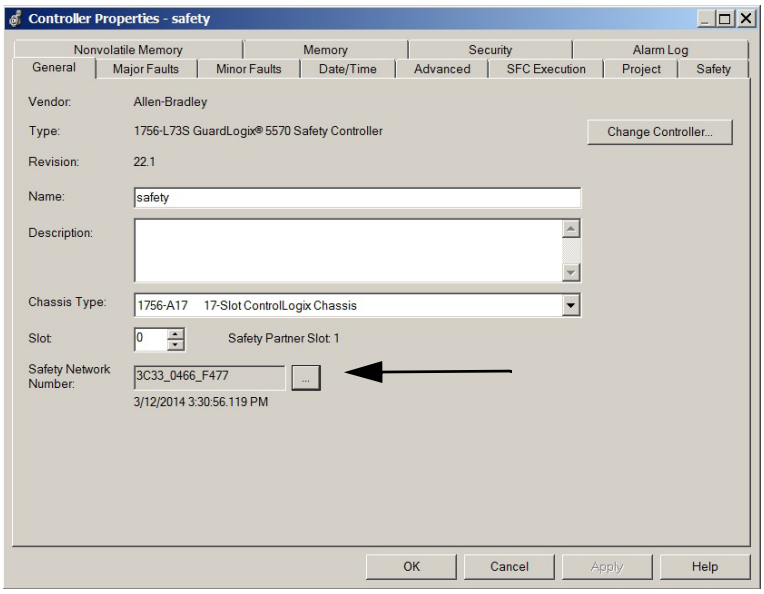
1. Añada el controlador productor al árbol de E/S del controlador consumidor.

SUGERENCIA El mismo controlador productor no debe aparecer más de una vez en el árbol de E/S del controlador o se producirá un error de verificación.

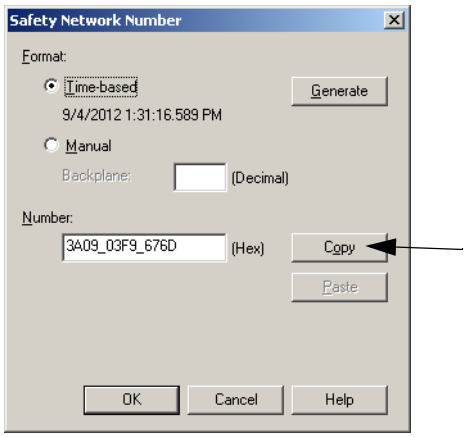


2. En el proyecto del controlador productor, haga clic con el botón derecho del mouse en el controlador productor y seleccione Controller Properties.

3. Haga clic en ... para abrir el cuadro de diálogo Safety Network Number.



4. Copie el SNN del controlador productor.



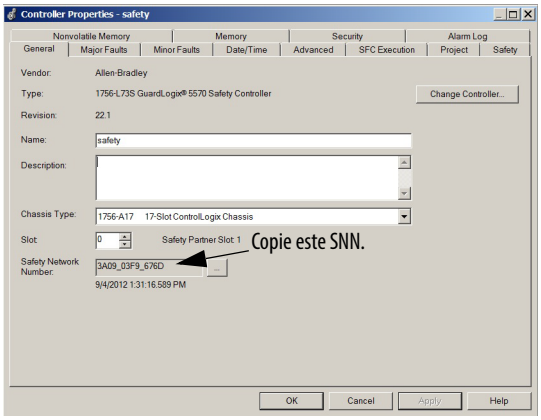
5. En el proyecto del controlador consumidor, haga clic con el botón derecho del mouse en el controlador productor y seleccione Module Properties.

6. Haga clic en ... para abrir el cuadro de diálogo Safety Network Number.

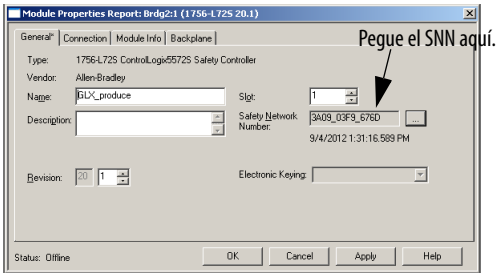
7. Pegue el SNN del controlador productor en el campo SNN y haga clic en OK.

   Los números de red de seguridad coinciden.

Cuadro de diálogo Producer Controller Properties del módulo



Cuadro de diálogo Module Properties en el proyecto consumidor



Producción de un tag de seguridad

Siga este procedimiento para producir un tag de seguridad.

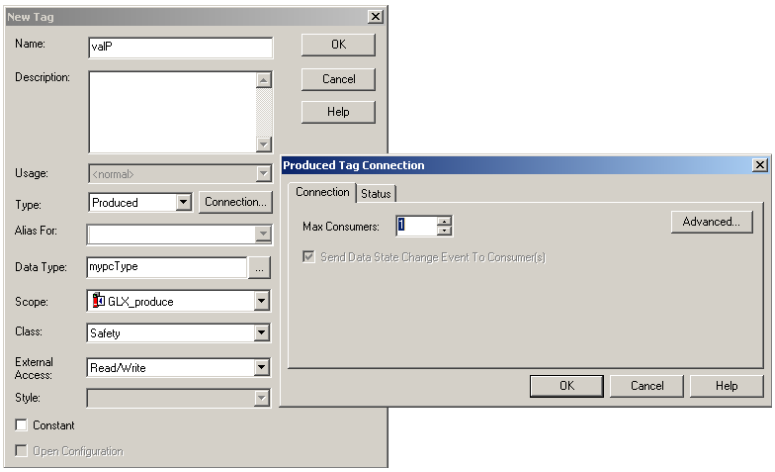
1. En el proyecto de controladores productor, cree un tipo de datos definido por el usuario que defina la estructura de los datos que se van a producir.

   Asegúrese de que el primer miembro de datos sea del tipo de datos CONNECTION_STATUS.

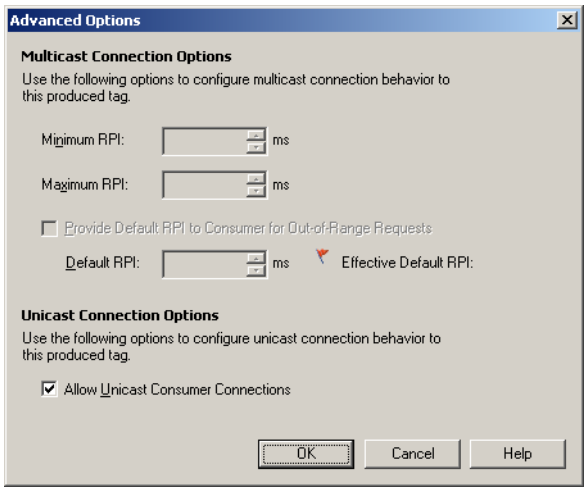
2. Haga clic con el botón derecho del mouse en Controller Tags y seleccione New Tag.

3. En Type seleccione Produced, en Class seleccione Safety, y en Data Type seleccione el tipo de datos definido por el usuario que creó en el paso 1.

4. Haga clic en Connection e introduzca el número de consumidores.



5. Haga clic en Advanced si desea cambiar el tipo de conexión desmarcando “Allow Unicast Consumer Connections”.



6. Haga clic en OK.

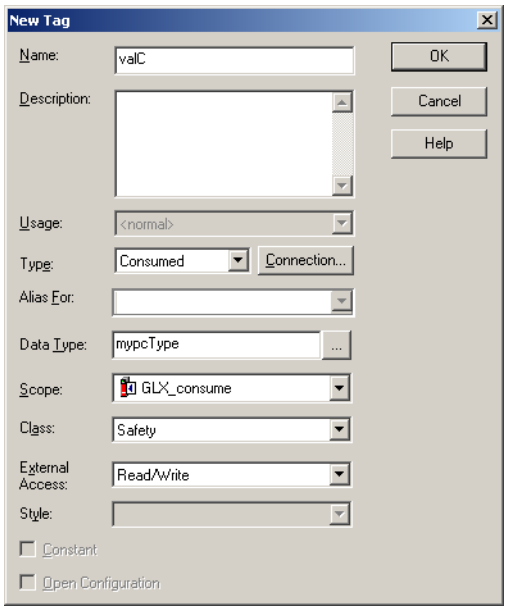
Consumo de datos de tag de seguridad

Siga estos pasos para consumir datos producidos por otro controlador.

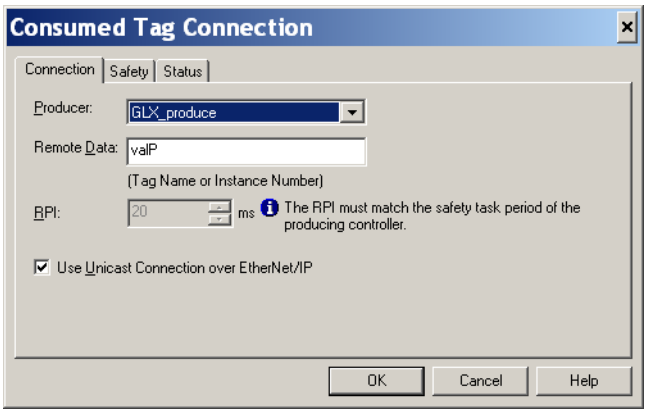
1. En el proyecto del controlador consumidor, cree un tipo de datos definido por el usuario idéntico al creado en el proyecto productor.

   SUGERENCIA El tipo de datos definido por el usuario puede copiarse desde el proyecto productor y pegarse en el proyecto consumidor.

2. Haga clic con el botón derecho del mouse en Controller Tags y seleccione New Tag.
3. En Type seleccione Consumed, en Class seleccione Safety y en Data Type seleccione el tipo de datos definido por el usuario que creó en el paso 1.



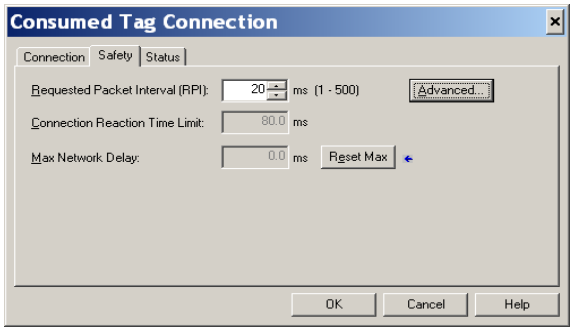
4. Haga clic en Connection para abrir el cuadro de diálogo Consumed Tag Connection.



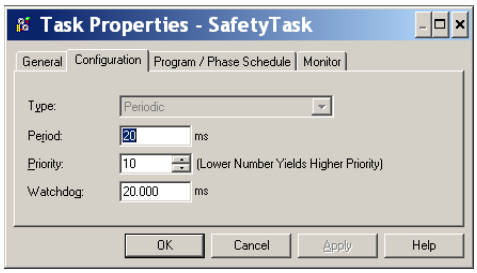
5. En los menús desplegables del productor, elija el controlador que produce los datos.
6. En el campo Remote Data, introduzca el nombre del tag producido.
7. Haga clic en la ficha Safety.
8. En el campo Requested Packet Interval (RPI), introduzca el intervalo solicitado entre paquetes para la conexión en incrementos de 1 ms.

   El valor predeterminado es 20 ms.

Proyecto del consumidor



Proyecto del productor

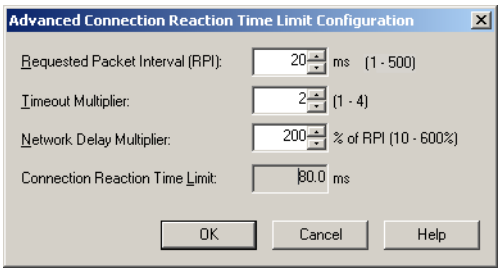


El RPI especifica el período cuando se actualizan los datos a través de una conexión. El RPI del tag de seguridad consumido debe coincidir con el período de la tarea de seguridad del proyecto de seguridad del productor.

El límite de tiempo de reacción de la conexión corresponde a la longevidad máxima de los paquetes de seguridad en la conexión asociada. En el caso de las restricciones de temporización simples, para conseguir un límite de tiempo de reacción de la conexión aceptable se puede ajustar el RPI.

El retardo de red máximo es el retardo de transporte máximo observado desde que se producen los datos hasta que son recibidos. Si está trabajando en línea, haga clic en Reset Max para restablecer el retardo de red máximo.

9. Si valor de Connection Reaction Time Limit es aceptable, haga clic en OK; o para requisitos más complejos, haga clic en Advanced para establecer los parámetros para Advanced Connection Reaction Time Limit.



El multiplicador de interrupciones determina el número de RPI que se debe esperar por un paquete hasta declarar expirado el tiempo de espera de una conexión.

El multiplicador de retardo de red define el tiempo de transporte de mensaje impuesto por el protocolo CIP Safety. El multiplicador de retardo de red especifica el retardo de ida y vuelta, del productor al consumidor y del consumidor al productor. Puede utilizar el multiplicador de retardo de red para aumentar o reducir el límite de tiempo de reacción de la conexión.

Tabla 31 – Más recursos

Recurso	Descripción
Páginas 67…69	Proporciona más información sobre cómo establecer el RPI y cómo el retardo de red máximo, el multiplicador de interrupciones y los multiplicadores de retardo de red afectan el tiempo de reacción de la conexión.
Capítulo 9	Contiene información acerca del tipo de datos predefinido CONNECTION_STATUS.
Logix5000 Controllers Produced and Consumed Tags Programming Manual, publicación 1756-PM011	Proporciona información detallada sobre cómo usar tags de seguridad producidos y consumidos

Asignación de un tag de seguridad

Una rutina de seguridad no puede obtener acceso directamente a los tags estándar bajo el control del controlador. Para poder utilizar datos de un tag estándar dentro de las rutinas de la tarea de seguridad, los controladores GuardLogix proporcionan una función de asignación de tag de seguridad que permite copiar valores de tag estándar en la memoria de la tarea de seguridad.

Restricciones

La asignación de un tag de seguridad está sujeta a estas restricciones:

- La pareja formada por el tag de seguridad y el tag estándar debe estar bajo el control del controlador.
- Los tipos de datos de la pareja de tag de seguridad y tag estándar deben coincidir.
- No se admiten tags de alias.

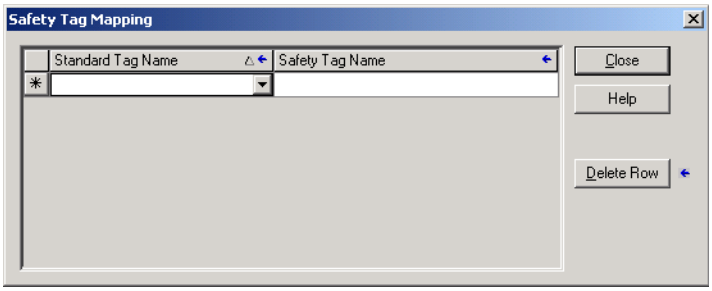
- La asignación debe tener lugar a nivel de todo el tag. Por ejemplo, myTimer.pre no se admite si myTimer es un tag de temporizador (TIMER).
- Una pareja de asignación es un tag estándar asignado a un tag de seguridad.
- Usted no puede asignar un tag estándar a un tag de seguridad designado como constante.
- La asignación de un tag no se puede modificar si se cumple lo siguiente:
  - el proyecto está en bloqueo de seguridad;
  - existe una firma de tarea de seguridad;
  - el interruptor de llave se encuentra en la posición de marcha (RUN);
  - existe un fallo de seguridad no recuperable;
  - existe una asociación no válida entre el controlador primario y el homólogo de seguridad.

ATENCIÓN: Cuando utilice datos estándar en una rutina de seguridad, debe verificar que los datos se utilicen de manera apropiada. Usar datos estándar en un tag de seguridad no los convierte en datos de seguridad. Usted no debe controlar directamente una salida de seguridad SIL 3/PLe con datos de tag estándar.

Consulte el documento Sistemas controladores GuardLogix 5570 – Manual de referencia de seguridad, publicación 1756-RM099, para obtener más información.

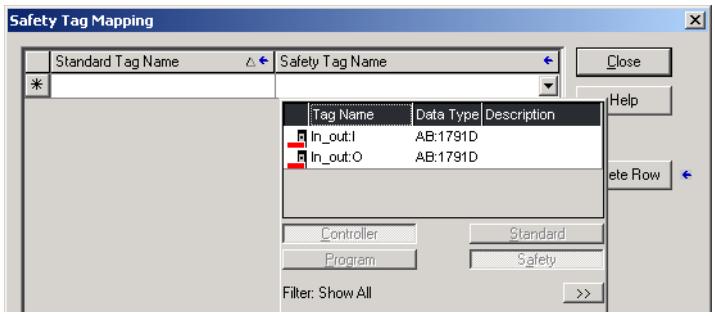
Creación de pares de asignación de tags

1. Seleccione Map Safety Tags en el menú Logic para abrir el cuadro de diálogo Safety Tag Mapping.



2. Agregue un tag existente a la columna Standard Tag Name o Safety Tag Name; para ello escriba el nombre del tag en la celda o seleccione un tag en el menú desplegable.

Haga clic en la flecha para visualizar un cuadro de diálogo de explorador con los tags filtrados. Si está en la columna Standard Tag Name, el explorador solo muestra los tags estándar bajo el control del controlador. Si está en la columna Safety Tag Name, el explorador muestra los tags de seguridad bajo el control del controlador.



3. Añada un nuevo tag en la columna Standard Tag Name o Safety Tag Name; para ello haga clic con el botón derecho del mouse en la celda vacía, seleccione New Tag y escriba el nombre del tag en la celda.
4. Haga clic con el botón derecho del mouse en la celda y seleccione New tagname, donde tagname es el texto que introdujo en la celda.

Monitoreo del estado de la asignación de un tag

La columna en el extremo izquierdo del cuadro de diálogo Safety Tag Mapping indica el estado de la pareja asignada.

Tabla 32 – Iconos del estado de la asignación de un tag

Contenido de la celda	Descripción
Vacía	La asignación de tag es válida.
	Cuando se trabaja fuera de línea, el icono X indica que la asignación de tag no es válida. Puede desplazarse a otra fila o cerrar el cuadro de diálogo Safety Tag Mapping.(1) Cuando se trabaja en línea, si una asignación de tag no es válida, aparece un mensaje de error que explica el motivo. Si hay un error de asignación de tag, no podrá desplazarse a otra fila ni cerrar el cuadro de diálogo Safety Tag Mapping.
	Indica la fila sobre la cual recae el enfoque en ese momento.
	Representa la fila de creación de un nuevo tag asignado.
	Representa una edición pendiente.

(1) La asignación de tags se comprueba además durante la verificación del proyecto. Si la asignación de un tag no es válida, se produce un error en la verificación del proyecto.

Para obtener más información, vea las restricciones de asignación de tags en la página 98.

Protección de las aplicaciones de seguridad

Usted puede proteger su programa de aplicación frente a cambios no autorizados mediante un bloqueo de seguridad del controlador, o generando y registrando la firma de tarea de seguridad.

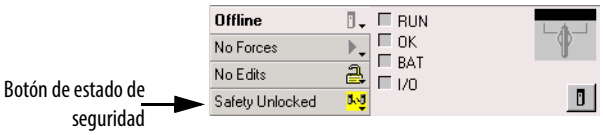
Bloqueo de seguridad del controlador

El controlador GuardLogix puede estar en bloqueo de seguridad a fin de proteger los componentes de control relacionados con la seguridad frente a posibles modificaciones. La función de bloqueo de seguridad solo es aplicable a componentes de seguridad como la tarea de seguridad, programas de seguridad, rutinas de seguridad, instrucciones Add-On de seguridad, tags de seguridad, E/S de seguridad y la firma de tarea de seguridad.

Las acciones siguientes no están permitidas en la porción de seguridad de la aplicación cuando el controlador está en bloqueo de seguridad:

- Programación o edición en línea/fuera de línea (inclusive instrucciones Add-On de seguridad)
- Forzado de E/S de seguridad
- Cambio del estado de inhibición de las E/S de seguridad o las conexiones producidas
- Manejo de datos de seguridad (salvo por la lógica de rutina de seguridad)
- Generación o eliminación de la firma de tarea de seguridad

SUGERENCIA El texto del botón de estado de seguridad de la barra de conexión en línea indica el estado de bloqueo de seguridad.



Además, en la bandeja de la aplicación se muestran los iconos siguientes, que indican el estado de bloqueo de seguridad del controlador de seguridad.

-  = controlador en bloqueo de seguridad
-  = controlador en desbloqueo de seguridad

Usted puede aplicar un bloqueo de seguridad al proyecto del controlador independientemente de si trabaja en línea o fuera de línea, e independientemente de si tiene o no la fuente original del programa. Sin embargo, no puede haber forzados de seguridad ni ediciones pendientes de seguridad en línea.

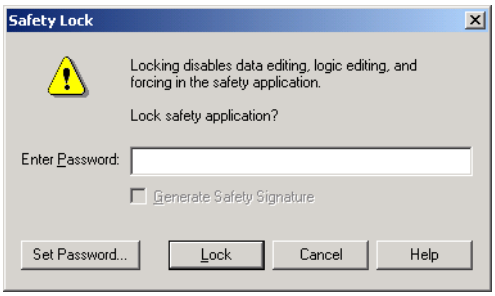
El estado de bloqueo o desbloqueo de seguridad no se puede cambiar cuando el interruptor de llave se encuentra en la posición de marcha (RUN).

SUGERENCIA Las acciones de bloqueo o desbloqueo de seguridad se registran en el registro del controlador.

Para obtener más información acerca de cómo obtener acceso al registro del controlador, consulte el documento Logix5000 Controllers Controller Information and Status Programming Manual, publicación 1756-PM015.

Puede bloquear o desbloquear la seguridad del controlador desde la ficha Safety del cuadro de diálogo Controller Properties o seleccionando Tools>Safety>Safety Lock/Unlock.

Figura 27 – Bloqueo de seguridad del controlador



Si ha establecido una contraseña para la función de bloqueo de seguridad, debe escribirla en el campo Enter Password. Si no, haga clic en Lock.

También puede establecer o modificar la contraseña en el cuadro de diálogo Safety Lock. Vea la página 43.

La función de bloqueo de seguridad descrita en esta sección y las medidas de seguridad estándar de la aplicación Logix Designer son aplicables a los proyectos del controlador GuardLogix.

Consulte el documento Protección de los controladores Logix5000 – Manual de programación, publicación 1756-PM016, para obtener información sobre las funciones de protección de Logix Designer.

Generación de una firma de tarea de seguridad

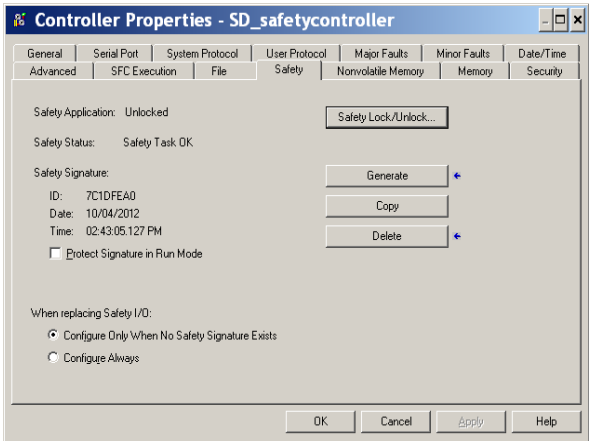
Antes de las pruebas de verificación, usted debe generar la firma de tarea de seguridad. Solo podrá generar la firma de tarea de seguridad si está en línea con el controlador GuardLogix en desbloqueo de seguridad, en el modo de programación, sin forzados de seguridad y sin ediciones de seguridad en línea pendientes, ni fallos de seguridad. El estado de seguridad debe ser Safety Task OK.

Además, no podrá generar una firma de tarea de seguridad si el controlador está en el modo marcha con la protección de modo marcha habilitada.

SUGERENCIA Puede ver el estado de seguridad con el botón de estado de seguridad en la barra de la conexión en línea (consulte la página 120) o en la ficha Safety del cuadro de diálogo Controller Properties, como se muestra en la página 103.

Haga clic en Generate para generar la firma de tarea de seguridad desde la ficha Safety del cuadro de diálogo Controller Properties. También puede seleccionar Tools>Safety>Generate Signature.

Figura 28 – Ficha Safety



Si existe una firma anterior, se le preguntará si desea sobrescribirla.

SUGERENCIA La creación y eliminación de la firma de tarea de seguridad se registra en el registro del controlador.

Para obtener más información acerca de cómo obtener acceso al registro del controlador, consulte el documento Logix5000 Controllers Controller Information and Status Programming Manual, publicación 1756-PM015.

Si existe una firma de tarea de seguridad, no se permiten las acciones siguientes en la porción de seguridad de la aplicación:

- Programación o edición en línea/fuera de línea (inclusive instrucciones Add-On de seguridad)
- Forzado de E/S de seguridad
- Cambio del estado de inhibición de las E/S de seguridad o de los controladores productores
- Manejo de datos de seguridad (salvo con la lógica de rutina de seguridad)

Copiar la firma de tarea de seguridad

Puede utilizar el botón Copy para crear un registro de la firma de tarea de seguridad y utilizarlo en la documentación, la comparación y la validación del proyecto de seguridad. Haga clic en Copy para copiar los componentes de identificación, fecha y hora en el portapapeles de Windows.

Eliminación de la firma de tarea de seguridad

Haga clic en Delete para eliminar la firma de tarea de seguridad. La firma de tarea de seguridad no puede eliminarse cuando se cumple lo siguiente:

- El controlador está en bloqueo de seguridad.
- El controlador está en el modo de marcha cuando el interruptor de llave está en la posición RUN.

- El controlador está en el modo de marcha o marcha remota con protección del modo marcha habilitada.

ATENCIÓN: Si elimina la firma de tarea de seguridad, debe volver a probar y revalidar su sistema para mantener la clasificación SIL 3/PLe.

Consulte el documento Sistemas controladores GuardLogix 5570 – Manual de referencia de seguridad, publicación 1756-RM099, para obtener más información sobre los requisitos de SIL 3/PLe.

Restricciones de programación

La aplicación Logix Designer impone restricciones que limitan la disponibilidad de algunos ítems y funciones de menú (p. ej., cortar, pegar, eliminar, buscar y reemplazar) a fin de proteger los componentes de seguridad frente a posibles modificaciones cuando se cumple lo siguiente:

- El controlador está en bloqueo de seguridad.
- Existe una firma de tarea de seguridad.
- Existen fallos de seguridad.
- El estado de seguridad es el siguiente:
  - Partner missing
  - Partner unavailable
  - Hardware incompatible
  - Firmware incompatible

Si se da alguna de las condiciones anteriores, no es posible hacer lo siguiente:

- Crear ni modificar objetos de seguridad, incluidos programas de seguridad, rutinas de seguridad, tags de seguridad, instrucciones Add-On de seguridad y dispositivos de E/S de seguridad.

  IMPORTANTE Los tiempos de escán de la tarea de seguridad y otros programas de seguridad se pueden restablecer cuando se trabaja en línea.

- Aplicar forzados a los tags de seguridad.
- Crear asignaciones nuevas de tag de seguridad.
- Modificar o eliminar asignaciones de tags.
- Modificar o eliminar tipos de datos definidos por el usuario que estén utilizando los tags de seguridad.
- Modificar el nombre de controlador, la descripción, el tipo de chasis, la ranura y el número de red de seguridad.
- Modificar o eliminar la firma de tarea de seguridad cuando exista un bloqueo de seguridad.

Entrada en línea con el controlador

Conexión del controlador a la red

Si todavía no lo ha hecho, conecte el controlador a la red.

Tabla 33 – Conexiones de comunicación

Para este tipo de conexión	Use	Consulte
USB	Cable USB 2.0	Establecimiento de las conexiones de comunicación en la página 29
EtherNet/IP	Dispositivo EtherNet/IP en una ranura abierta en el mismo chasis que el controlador	Conexión del dispositivo EtherNet/IP y la computadora en la página 105
DeviceNet	Módulo 1756-DNB en una ranura abierta en el mismo chasis que el controlador	Conexión del módulo de comunicación ControlNet o escáner DeviceNet y su computadora en la página 106
ControlNet	Módulo 1756-CN2 en una ranura abierta en el mismo chasis que el controlador	

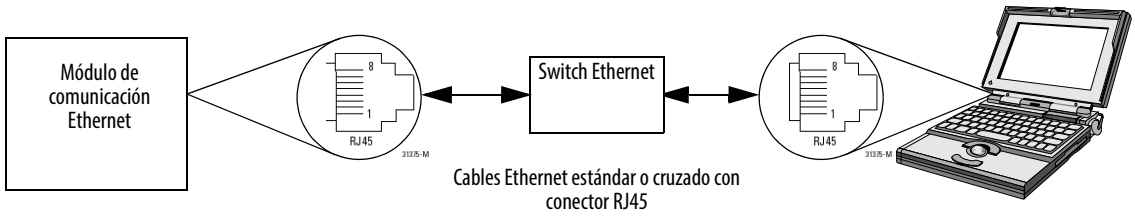
Conexión del dispositivo EtherNet/IP y la computadora

ADVERTENCIA: Si conecta o desconecta el cable de comunicación con la alimentación aplicada a este módulo o a cualquier dispositivo de la red, se puede producir un arco eléctrico. Esto podría provocar una explosión en instalaciones ubicadas en zonas peligrosas.

Antes de seguir adelante, asegúrese de desconectar la alimentación eléctrica o de verificar que la zona no sea peligrosa.

Conecte el dispositivo EtherNet/IP y la computadora mediante un cable Ethernet.

Figura 29 – Conexiones Ethernet



Conexión del módulo de comunicación ControlNet o escáner DeviceNet y su computadora

Para obtener acceso a la red ControlNet o DeviceNet, puede realizar una de las siguientes acciones:

- Conectarse directamente a la red.
- Conectarse a una red serie o EtherNet/IP, y navegar (establecer un puente) hasta la red que desee. Para ello no hace falta ninguna programación adicional.

Configuración de un driver EtherNet/IP, ControlNet o DeviceNet

Para obtener información sobre cómo configurar un driver, consulte la publicación correspondiente.

- EtherNet/IP Modules in Logix5000 Control Systems, publicación ENET-UM001
- ControlNet Modules in Logix5000 Control Systems User Manual, publicación CNET-UM001
- DeviceNet Modules in Logix5000 Control Systems, publicación DNET-UM004

Factores que influyen en la entrada en línea

La aplicación Logix Designer determina si usted puede entrar en línea con un controlador de destino, lo cual depende de si el proyecto fuera de línea es nuevo o si ha sido modificado. Si el proyecto es nuevo, primero debe descargar el proyecto en el controlador. Si se modificó el proyecto, se le pide que realice una carga o una descarga. Si no se realizaron cambios, puede entrar en línea para monitorear la ejecución del proyecto.

Hay una serie de factores que influyen en estos procesos, entre ellos la función de coincidencia del proyecto con el controlador Project to Controller Match, el estado de seguridad y los fallos, la existencia de una firma de tarea de seguridad, y el estado de bloqueo o desbloqueo de seguridad del proyecto y del controlador.

Coincidencia del proyecto con el controlador

La función de coincidencia del proyecto con el controlador Project to Controller Match afecta los procesos de descarga, la carga y la entrada en línea de los proyectos, tanto estándar como de seguridad.

Si la función Project to Controller Match está habilitada en el proyecto fuera de línea, la aplicación Logix Designer compara el número de serie del controlador en el proyecto fuera de línea con el del controlador conectado. Si no coinciden, usted deberá cancelar la carga/descarga, conectarse al controlador correcto o confirmar que está conectado al controlador correcto, lo cual actualiza el número de serie en el proyecto para que coincida con el controlador de destino.

Coincidencia de la revisión de firmware

La coincidencia de la revisión de firmware influye en el proceso de descarga. Si la revisión del controlador no coincide con la revisión del proyecto, se le pide que actualice el firmware del controlador. La aplicación Logix Designer le permite actualizar el firmware como parte de la secuencia de descarga.

IMPORTANTE	Para actualizar el firmware del controlador, antes deberá instalar un paquete de actualización de firmware. El paquete de actualización se envía en un CD suplementario junto con el ambiente Studio 5000.

SUGERENCIA	También puede actualizar el firmware seleccionando ControlFLASH en el menú Tools de la aplicación Logix Designer.

Estado/fallos de seguridad

Se permite cargar la lógica de programa y entrar en línea independientemente del estado de seguridad. El estado y los fallos de seguridad solo afectan el proceso de descarga.

Puede ver el estado de seguridad mediante la ficha Safety del cuadro de diálogo Controller Properties.

Firma de tarea de seguridad y estado de bloqueo y desbloqueo de seguridad

La existencia de una firma de tarea de seguridad y el estado de bloqueo o desbloqueo de seguridad del controlador afectan los procesos de carga y descarga.

Durante la carga

Si el controlador tiene una firma de tarea de seguridad, la firma de tarea de seguridad y el estado de bloqueo de tarea de seguridad se cargan con el proyecto. Por ejemplo, si el proyecto en el controlador está en desbloqueo de seguridad, el proyecto fuera de línea permanece en desbloqueo de seguridad después de la carga aunque estuviera bloqueado antes de la carga.

Después de una carga, la firma de tarea de seguridad del proyecto fuera de línea coincide con la firma de tarea de seguridad del controlador.

Durante la descarga

La existencia de una firma de tarea de seguridad y el estado de bloqueo de seguridad del controlador determinan si se puede realizar una descarga o no.

Tabla 34 – Efecto del bloqueo de seguridad y la firma de tarea de seguridad en la operación de descarga

Estado de bloqueo de seguridad	Estado de la firma de tarea de seguridad	Funcionalidad de la descarga
Controlador en desbloqueo de seguridad	La firma de tarea de seguridad del proyecto fuera de línea coincide con la firma de tarea de seguridad del controlador.	Se descargan todos los componentes del proyecto estándar. Los tags de seguridad se reinicializan con los valores que tenían en el momento en que se creó la firma de tarea de seguridad. La tarea de seguridad no se ha descargado. El estado de bloqueo de seguridad coincide con el estado en el proyecto fuera de línea.
	Las firmas de la tarea de seguridad no coinciden.	Si el controlador tiene una firma de tarea de seguridad, esta se elimina automáticamente y se descarga el proyecto completo. El estado de bloqueo de seguridad coincide con el estado en el proyecto fuera de línea.
Controlador en bloqueo de seguridad	Coinciden las firmas de tarea de seguridad.	Si el proyecto fuera de línea y el controlador tienen bloqueo de seguridad, todos los componentes del proyecto estándar se descargan y la tarea de seguridad se reinicializa con los mismos valores que tenía cuando se creó la firma de tarea de seguridad. Si el proyecto fuera de línea no está en bloqueo de seguridad pero el controlador sí lo está, la descarga se bloquea y usted deberá desbloquear primero el controlador para permitir que se realice la descarga.
	Las firmas de la tarea de seguridad no coinciden.	En primer lugar debe poner el controlador en desbloqueo de seguridad para que se pueda realizar la descarga. Si el controlador tiene una firma de tarea de seguridad, esta se elimina automáticamente y se descarga el proyecto completo. El estado de bloqueo de seguridad coincide con el estado en el proyecto fuera de línea.

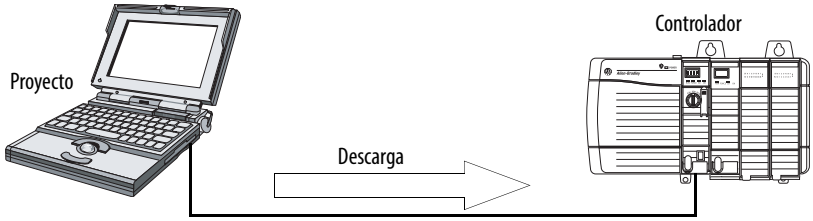
IMPORTANTE Durante una descarga a un controlador con desbloqueo de seguridad, si el firmware en el controlador es diferente al del proyecto fuera de línea, prosiga de una de las siguientes maneras:

- Realice una actualización del controlador, de modo que coincida con el proyecto fuera de línea. Una vez que concluye la actualización, se descarga todo el proyecto.
- Actualice el proyecto a la versión del controlador.

Si actualiza el proyecto, la firma de tarea de seguridad se elimina y el sistema requerirá revalidación.

Descarga

Siga estos pasos para transferir el proyecto de la computadora al controlador.



1. Mueva el interruptor de llave del controlador a la posición REM.
2. Abra el proyecto del controlador que desea descargar.
3. Defina la ruta de acceso al controlador.
   a. Haga clic en Who Active  .
   b. Seleccione el controlador.
   Para abrir un nivel, haga clic en el signo +. Si ya se ha seleccionado un controlador, asegúrese de que sea el correcto.
4. Haga clic en Download.

La aplicación Logix Designer compara la siguiente información en el proyecto fuera de línea y el controlador:

- número de serie del controlador (si se ha seleccionado la coincidencia del proyecto con el controlador)
- revisiones mayores y menores del firmware
- estado de seguridad
- firma de tarea de seguridad (si la hay)
- estado de bloqueo de seguridad

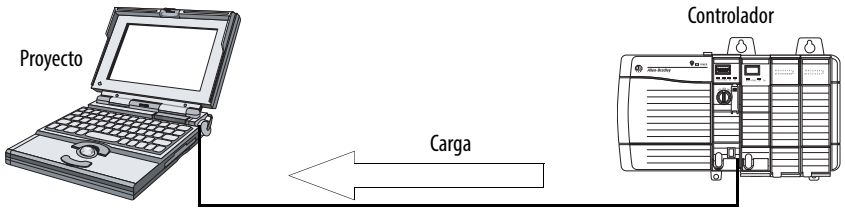
5. Siga las indicaciones que aparecen en esta tabla para completar la descarga según la respuesta de la aplicación Logix Designer.

Si el software indica	Haga lo siguiente
Descarga al controlador.	Seleccione Download. Se descarga el proyecto en el controlador y entra en línea.
No se puede realizar la descarga al controlador. No hay coincidencia entre el proyecto fuera de línea y el número de serie del controlador. Es posible que se haya seleccionado un controlador equivocado.	Establezca la conexión al controlador correcto o verifique que este sea el controlador correcto. Si este es el controlador correcto, marque la casilla de selección Update Project Serial Number para permitir que se realice la descarga. El número de serie del proyecto se modifica para que coincida con el número de serie del controlador.
No se puede realizar la descarga al controlador. La revisión mayor del proyecto fuera de línea y el firmware del controlador no son compatibles.	Seleccione Update Firmware. Seleccione la revisión necesaria y haga clic en Update. Haga clic en Yes para confirmar su selección.
No se puede realizar la descarga al controlador. Falta el homólogo de seguridad o no está disponible.	Cancele el proceso de descarga. Instale un homólogo de seguridad compatible antes de intentar realizar una descarga.
No se puede realizar la descarga al controlador. La revisión de firmware del homólogo de seguridad es incompatible con el controlador primario.	Actualice la revisión de firmware del homólogo de seguridad. Seleccione Update Firmware. Seleccione la revisión necesaria y haga clic en Update. Haga clic en Yes para confirmar su selección.
No se puede realizar la descarga al controlador. La asociación de seguridad no se ha establecido.	Cancele este proceso de descarga e intente realizar una nueva descarga.
No se puede realizar la descarga al controlador. La firma de tarea de seguridad incompatible no se puede eliminar mientras el proyecto esté en bloqueo de seguridad.	Cancele la descarga. Para descargar el proyecto, usted debe poner en desbloqueo de seguridad el proyecto fuera de línea, eliminar la firma de tarea de seguridad y descargar el proyecto. **IMPORTANTE:** El sistema de seguridad requiere revalidación.
No se puede realizar la descarga de modo que se conserve la firma de tarea de seguridad. La revisión menor de firmware del controlador es incompatible con la firma de tarea de seguridad del proyecto fuera de línea.	• Si la revisión menor de firmware es incompatible, a fin de conservar la firma de tarea de seguridad actualice la revisión del firmware en el controlador para que coincida exactamente con el proyecto fuera de línea. A continuación, descargue el proyecto fuera de línea. • Para continuar con la descarga a pesar de la incompatibilidad de la firma de tarea de seguridad, haga clic en Download. La firma de tarea de seguridad se elimina. **IMPORTANTE:** El sistema de seguridad requiere revalidación.
No se puede realizar la descarga al controlador. El controlador está bloqueado. Las firmas de tarea de seguridad del controlador y del proyecto fuera de línea no coinciden.	Seleccione Unlock. Aparece el cuadro de diálogo Safety Unlock for Download. Si se ha marcado la casilla de selección Delete Signature y elige Unlock, haga clic en Yes para confirmar la eliminación.
Se produce un fallo de seguridad no recuperable en el controlador de seguridad. No existe un maestro de hora coordinada del sistema (CST) designado.	Seleccione Enable Time Synchronization y haga clic en Download para seguir adelante.

Después de una descarga satisfactoria, el estado de bloqueo de seguridad y la firma de tarea de seguridad del controlador coinciden con el proyecto descargado. Los datos de seguridad se inicializan con los valores que tenían en el momento en que se creó la firma de tarea de seguridad.

Carga

Siga estos pasos para transferir un proyecto del controlador a la computadora.



1. Defina la ruta de acceso al controlador.
   a. Haga clic en Who Active  .
   b. Seleccione el controlador.
   Para expandir un nivel, haga clic en el signo +. Si ya se ha seleccionado un controlador, asegúrese de que sea el correcto.
2. Haga clic en Upload.
3. Si el archivo del proyecto no existe, seleccione File>Select>Yes.
4. Si el archivo de proyecto existe, selecciónelo.

   Si se ha habilitado la coincidencia del proyecto con el controlador, la aplicación Logix Designer comprueba si el número de serie del proyecto abierto coincide con el número de serie del controlador.

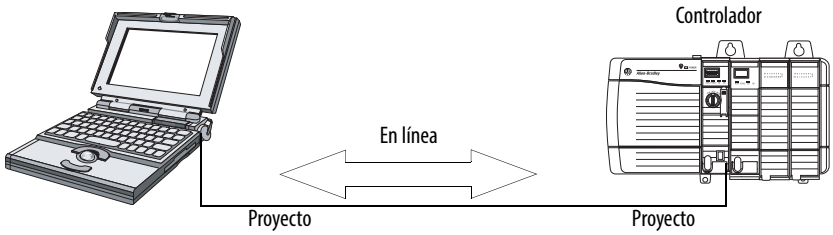
   Si los números de serie de controlador no coinciden, puede realizar una de las siguientes acciones:
   - Cancelar la carga y conectarse a un controlador que coincida. Seguidamente, iniciar de nuevo el procedimiento de carga.
   - Seleccionar un nuevo proyecto para la carga o seleccionar otro proyecto distinto mediante Select File.
   - Actualizar el número de serie del proyecto para que coincida con el controlador; para ello, marque la casilla de selección Update Project Serial Number y seleccione Upload.
5. La aplicación Logix Designer comprueba si el proyecto abierto coincide con el proyecto del controlador.
   a. Si los proyectos no coinciden, debe seleccionar un archivo que coincida o cancelar el proceso de carga.
   b. Si los proyectos coinciden, el software comprueba los cambios en el proyecto fuera de línea (abierto).
6. La aplicación Logix Designer verifica si hay cambios en el proyecto fuera de línea.
   a. Si no se han realizado cambios en el proyecto fuera de línea, puede entrar en línea sin realizar la carga. Haga clic en Go Online.
   b. Si se han realizado cambios en el proyecto abierto que no están presentes en el controlador, puede elegir entre cargar el proyecto, cancelar la carga o seleccionar otro archivo.

Si selecciona Upload, se cargan las aplicaciones estándar y de seguridad. Si existe una firma de tarea de seguridad, también se carga. El estado de bloqueo de seguridad del proyecto refleja el estado original del proyecto en línea (controlador).

SUGERENCIA Antes de la carga, si existe una firma de tarea de seguridad fuera de línea, o si el proyecto fuera de línea está en bloqueo de seguridad pero el controlador está en desbloqueo de seguridad o no tiene firma de tarea de seguridad, la firma de tarea de seguridad fuera de línea y el estado de bloqueo de seguridad son reemplazados por los valores en línea (en desbloqueo de seguridad sin firma de tarea de seguridad). Si no desea que estos cambios sean permanentes, no guarde el proyecto fuera de línea después de la carga.

Entrada en línea

Siga estos pasos para entrar en línea y monitorear un proyecto que el controlador esté ejecutando.



1. Defina la ruta de acceso al controlador.
   a. Haga clic en Who Active  .
   b. Seleccione el controlador.
   Para expandir un nivel, haga clic en el signo +. Si ya se ha seleccionado un controlador, asegúrese de que sea el correcto.
2. Haga clic en Go Online.

   La aplicación Logix Designer verifica lo siguiente:
   - ¿Coinciden los números de serie del controlador y del proyecto fuera de línea (si se ha seleccionado Project to Controller Match)?
   - ¿Contiene el proyecto fuera de línea cambios que no están presentes en el proyecto del controlador?
   - ¿Coinciden las revisiones de firmware del controlador y del proyecto fuera de línea?
   - ¿Están en bloqueo de seguridad el controlador o el proyecto fuera de línea?
   - ¿Son compatibles las firmas de tarea de seguridad del controlador y del proyecto fuera de línea?
3. Siga las instrucciones descritas en la tabla para conectarse al controlador.

Tabla 35 – Conexión al controlador

Si el software indica	Haga lo siguiente
No se ha podido establecer una conexión con el controlador. No hay coincidencia entre el proyecto fuera de línea y el número de serie del controlador. Es posible que se haya seleccionado un controlador equivocado.	Conéctese al controlador correcto, seleccione otro archivo de proyecto o marque la casilla de selección Update Project Serial Number y seleccione Go Online… para conectarse al controlador y actualizar el número de serie del proyecto fuera de línea para que coincida con el controlador.
No se ha podido establecer una conexión con el controlador. La revisión del proyecto fuera de línea y el firmware del controlador no son compatibles.	Elija una de las opciones siguientes: • Seleccione Update Firmware. Seleccione la revisión necesaria y haga clic en Update. Haga clic en Yes para confirmar su selección. **IMPORTANTE:** Se elimina el proyecto en línea. • Para conservar el proyecto en línea, cancele el proceso en línea e instale una versión del ambiente Studio 5000 que sea compatible con la revisión de firmware del controlador.
Debe realizar una carga o una descarga para entrar en línea usando el proyecto abierto.	Elija una de las opciones siguientes: • Upload para actualizar el proyecto fuera de línea. • Download para actualizar el proyecto del controlador. • Choose File para seleccionar otro proyecto fuera de línea.
No se puede establecer una conexión de modo que se conserve la firma de tarea de seguridad. La revisión menor de firmware del controlador es incompatible con la firma de tarea de seguridad en el proyecto fuera de línea.	• Si la revisión menor de firmware es incompatible, a fin de conservar la firma de tarea de seguridad actualice la revisión de firmware del controlador para que coincida exactamente con el proyecto fuera de línea. Seguidamente entre en línea con el controlador. • Para continuar con la descarga a pesar de la incompatibilidad de la firma de tarea de seguridad, haga clic en Download. La firma de tarea de seguridad se elimina. **IMPORTANTE:** El sistema de seguridad requiere revalidación.
No se ha podido establecer una conexión con el controlador. La firma de tarea de seguridad incompatible no se puede eliminar mientras el proyecto esté en bloqueo de seguridad.	Cancele el proceso de entrada en línea. Debe poner el proyecto fuera de línea en desbloqueo de seguridad antes de intentar entrar en línea.

Cuando el controlador y la aplicación Logix Designer están en línea, el estado de bloqueo de seguridad y la firma de tarea de seguridad del controlador coinciden con el proyecto del controlador. El controlador sobrescribe el estado de bloqueo de seguridad y la firma de tarea de seguridad del proyecto fuera de línea. Si no desea que los cambios en el proyecto fuera de línea sean permanentes, no guarde el archivo de proyecto después del proceso de entrada en línea.

Almacenamiento y carga de proyectos usando la memoria no volátil

Uso de tarjetas de memoria para memoria no volátil

Los controladores GuardLogix 5570 aceptan una tarjeta de memoria para uso como memoria no volátil. La memoria no volátil le permite mantener una copia de su proyecto en el controlador. El controlador no necesita alimentación eléctrica ni una batería para mantener esta copia.

El proyecto almacenado se puede cargar de la memoria no volátil a la memoria de usuario del controlador:

- En cada activación
- Cuando no hay un proyecto en el controlador y este último se enciende
- En cualquier momento utilizando la aplicación Logix Designer

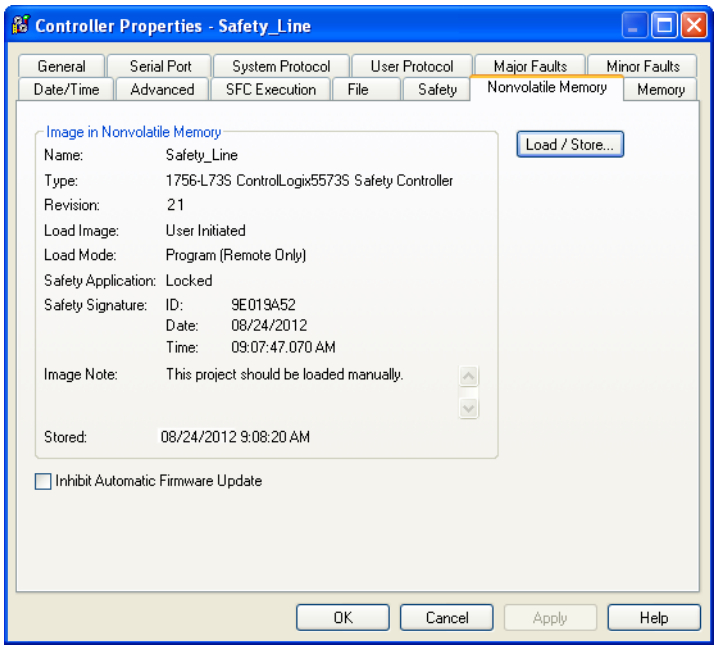
IMPORTANTE La memoria no volátil guarda el contenido de la memoria de usuario al momento en que usted guarda el proyecto:

- Los cambios realizados después de guardar el proyecto no se reflejan en la memoria no volátil.
- Si usted hace cambios al proyecto pero no guarda los cambios, los perderá cuando cargue el proyecto desde la memoria no volátil. Si esto ocurre, tendrá que cargar o descargar el proyecto para ponerse en línea.
- Si desea guardar cambios como, por ejemplo, ediciones en línea, valores de tags o la programación de la red ControlNet, vuelva a guardar el proyecto después de hacer los cambios.

ATENCIÓN: No extraiga la tarjeta de memoria mientras el controlador esté leyendo o escribiendo en la tarjeta, según lo indicado por el parpadeo de color verde del indicador de estado OK. Esto podría contaminar los datos de la tarjeta o del controlador, así como contaminar el firmware más reciente del controlador. Deje la tarjeta en el controlador hasta que el indicador de estado OK se encienda de color verde fijo.

Si se instala una tarjeta de memoria, usted podrá ver el contenido de la tarjeta en la ficha Nonvolatile Memory del cuadro de diálogo Controller Properties. Si se almacena una aplicación de seguridad en la tarjeta, aparecen el estado de bloqueo de seguridad y la firma de tarea de seguridad.

Figura 30 – Ficha Nonvolatile Memory



Para obtener información detallada sobre cómo usar la memoria no volátil, consulte el documento Logix5000 Controllers Nonvolatile Memory Programming Manual, publicación 1756-PM017.

Almacenamiento de un proyecto de seguridad

No se puede almacenar un proyecto de seguridad si el estado de la tarea de seguridad es “Safety Task Inoperable”. Cuando usted guarda un proyecto de seguridad, el firmware del controlador primario y del homólogo de seguridad se guardan en la tarjeta de memoria.

Si no existe un proyecto de aplicación en el controlador, únicamente se puede guardar el firmware del controlador de seguridad si existe una asociación válida. Una carga de solo firmware no borra una condición “Safety Task Inoperable”.

Si existe una firma de tarea de seguridad cuando usted almacena un proyecto, ocurre lo siguiente:

- los tags de seguridad se almacenan con el valor que tenían en el momento en que se creó inicialmente la firma de seguridad;
- los tags estándar se actualizan;
- la firma de tarea de seguridad actual se guarda.

Cuando almacene un proyecto de aplicación de seguridad en una tarjeta de memoria, recomendamos que seleccione Program (Remote Only) como modo de carga; es decir, el modo en que entra el controlador después de la carga.

Carga de un proyecto de seguridad

Puede iniciar una carga desde memoria no volátil cuando se cumple lo siguiente:

- El tipo de controlador especificado por el proyecto almacenado en la memoria no volátil coincide con el tipo del controlador.
- Las revisiones mayor y menor del proyecto alojadas en la memoria no volátil coinciden con las revisiones mayor y menor del controlador.
- Su controlador no está en el modo de marcha.

Existen varias opciones respecto a cuándo (en qué condiciones) cargar un proyecto en la memoria de usuario del controlador.

Tabla 36 – Opciones para cargar un proyecto

Si desea cargar el proyecto	Seleccione esta opción de imagen de carga	Notas
Siempre que encienda o que desconecte y vuelva a conectar la alimentación eléctrica	On Power Up	• Durante la desconexión y reconexión de la alimentación eléctrica, se pierden todos los cambios en línea, los valores de tags y la programación de la red que no hayan sido almacenados en la memoria no volátil. • El controlador carga el proyecto almacenado y el firmware durante cada puesta en marcha, independientemente del firmware o el proyecto de aplicación en el controlador. La carga ocurre independientemente de que el controlador esté en bloqueo de seguridad o tenga una firma de tarea de seguridad. • Siempre se puede usar la aplicación Logix Designer para cargar el proyecto.
Cuando no hay un proyecto en el controlador y usted enciende o desconecta y vuelve a conectar la alimentación al chasis	On Corrupt Memory	• Por ejemplo, si la batería se descarga y se desconecta la alimentación eléctrica del controlador, el proyecto se borra de la memoria. Cuando se restaura la alimentación eléctrica, esta opción de carga vuelve a cargar el proyecto en el controlador. • El controlador actualiza el firmware en el controlador primario o en el homólogo de seguridad, si es necesario. El proyecto de aplicación almacenado en la memoria no volátil también se carga, y el controlador entra al modo seleccionado, ya sea de programación o de marcha. • Siempre se puede usar la aplicación Logix Designer para cargar el proyecto.
Solo a través de la aplicación Logix Designer	User Initiated	• Si el tipo de controlador así como las revisiones mayores y menores del proyecto en la memoria no volátil coinciden con el tipo de controlador y con las revisiones mayores y menores del controlador, se puede iniciar una carga, independientemente del estado de la tarea de seguridad. • Puede cargar un proyecto a un controlador con bloqueo de seguridad cuando la firma de tarea de seguridad del proyecto almacenado en la memoria no volátil coincide con el proyecto en el controlador. • Si las firmas no coinciden o el controlador tiene bloqueo de seguridad sin una firma de tarea de seguridad, se le pedirá que primero desbloquee el controlador. **IMPORTANTE:** Cuando se desbloquea el controlador y se inicia una carga desde la memoria no volátil, el estado de bloqueo de seguridad, las contraseñas y la firma de tarea de seguridad se establecen en los valores contenidos en la memoria no volátil una vez que la carga se haya completado. • Si el firmware en el controlador primario coincide con la revisión en la memoria no volátil, el firmware del homólogo de seguridad se actualiza (si es necesario), la aplicación almacenada en la memoria no volátil se carga de modo que el estado Safety Task se convierta en Safety Task Operable, y el controlador entra al modo seleccionado, ya sea de programación o de marcha.

IMPORTANTE Antes de usar el software ControlFLASH, asegúrese de que la tarjeta SD esté desbloqueada si el sistema está establecido para la opción de carga On Power Up. De lo contrario, los datos actualizados pueden ser sobrescritos por el firmware en la tarjeta de memoria.

Uso de módulos de almacenamiento de energía

Puede usar los ESM GuardLogix para ejecutar cualquiera de las siguientes tareas:

- Proporcionar alimentación eléctrica al controlador para guardar el programa en la memoria de almacenamiento no volátil (NVS) después de desconectar la alimentación eléctrica del chasis o después de retirar el controlador de un chasis energizado.

IMPORTANTE	Cuando usted usa un ESM para guardar el programa en la memoria NVS incorporada **no** se guarda el programa en la tarjeta SD instalada en el controlador.

- Borre el programa de la memoria NVS incorporada del controlador. Para obtener más información consulte Borrado del programa de la memoria NVS incorporada

La tabla siguiente describe los ESM.

Tabla 37 – Módulos de almacenamiento de energía

Nº cat.	Descripción
1756-ESMCAP(XT)	ESM basado en condensador Los controladores se envían con este ESM instalado.
1756-ESMNSE(XT)	ESM basado en condensador sin alimentación eléctrica de respaldo WallClockTime Use este ESM si su aplicación requiere que el ESM instalado descargue su energía residual almacenada a un nivel de 40 µJ o menos antes de transportarlo a su aplicación o fuera de ella. Además, solamente puede usar este ESM con un controlador 1756-L73S (8 MB) o uno con menos memoria.
1756-ESMNRM(XT)	ESM basado en condensador seguro (no extraíble) Este ESM proporciona a su aplicación un mayor grado de protección al evitar el acceso físico al conector USB y a la tarjeta SD.
1756-SPESMNSE(XT)	ESM basado en condensador sin alimentación eléctrica de respaldo WallClockTime para el homólogo de seguridad Use este ESM si la aplicación requiere que el ESM instalado descargue su energía residual almacenada a un nivel de 40 µJ o menos antes de transportarlo a su aplicación o fuera de ella. El homólogo de seguridad para temperaturas extremas 1756-L7SPXT se envía con el 1756-SPESMNSEXT instalado.
1756-SPESMNRM(XT)	ESM basado en condensador seguro (no extraíble) para el homólogo de seguridad

Almacenamiento del programa en la memoria NVS incorporada

Siga estos pasos para guardar el programa en la memoria NVS cuando se interrumpa la alimentación eléctrica del controlador.

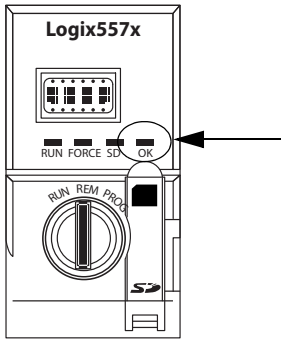
1. Desconecte la alimentación eléctrica del controlador.

   Puede desconectar la alimentación eléctrica de cualquiera de estas maneras:

   - Desconecte la alimentación del chasis mientras el controlador está instalado en el chasis.
   - Retire el controlador de un chasis energizado.

Inmediatamente después de que se desenergiza el controlador, el indicador de estado OK se enciende de color rojo fijo y permanece así el tiempo suficiente para guardar el programa.

Figura 31 – Indicador de estado OK.



2. Deje el ESM en el controlador hasta que el indicador de estado OK se apague.

3. Si es necesario, retire el ESM del controlador después de que el indicador de estado OK cambie de rojo fijo a apagado.

Borrado del programa de la memoria NVS incorporada

Si su aplicación le permite borrar programas, siga estos pasos para borrar el programa de la memoria NVS incorporada en el controlador.

1. Extraiga el ESM del controlador.

2. Desconecte la alimentación eléctrica del controlador; para ello desconecte la alimentación eléctrica del chasis mientras el controlador está instalado en el chasis o retire el controlador de un chasis energizado.

3. Reinstale el ESM en el controlador.

4. Restaure la alimentación eléctrica del controlador.
   a. Si el controlador ya está instalado en el chasis, conecte nuevamente la alimentación eléctrica del chasis.
   b. Si el controlador no está instalado en el chasis, reinstale el controlador en el chasis y conecte nuevamente la alimentación eléctrica del chasis.

Cálculo del apoyo de ESM de WallClockTime

El ESM ofrece apoyo para el mantenimiento del atributo WallClockTime del controlador cuando no está aplicada la alimentación eléctrica. Use esta tabla para calcular el tiempo de retención del ESM según la temperatura del controlador y el ESM instalado.

Tabla 38 – Temperatura vs. tiempo de retención

Temperatura	Tiempo de retención (en días)		
	1756-ESMCAP(XT)	1756-ESMNRM(XT) 1756-SPESMNRM(XT)	1756-ESMNSE(XT) 1756-SPESMNSE(XT)
20 °C (68 °F)	12	12	0
40 °C (104 °F)	10	10	0
60 °C (140 °F)	7	7	0

Administración del firmware con la función Firmware Supervisor

Puede usar la función Firmware Supervisor para administrar firmware en los controladores. La función Firmware Supervisor permite a los controladores realizar automáticamente la actualización de los dispositivos.

- Puede actualizar los módulos locales y remotos en los modos de programación o de marcha.
- La codificación electrónica debe estar configurada para Exact Match.
- El paquete de firmware para el dispositivo objetivo debe residir en la tarjeta de memoria del controlador.
- El dispositivo debe aceptar actualizaciones de firmware mediante el software ControlFLASH.

La función Firmware Supervisor acepta productos de E/S distribuidas no modulares que se colocan directamente en la red sin un adaptador, entre ellos dispositivos de E/S de seguridad en redes EtherNet/IP. Los dispositivos de E/S de seguridad en redes DeviceNet y los módulos POINT Guard I/O actualmente no son compatibles.

Siga estos pasos para habilitar la función Firmware Supervisor.

1. En el cuadro de diálogo Controller Properties, haga clic en la ficha Nonvolatile Memory.
2. Haga clic en Load/Store.
3. En el menú desplegable Automatic Firmware Updates, seleccione Enable and Store Files to Image.

La aplicación Logix Designer mueve los kits de firmware de su computadora a la tarjeta de memoria del controlador para ser usados por la función Firmware Supervisor.

SUGERENCIA Si usted inhabilita la función Firmware Supervisor, solo inhabilita las actualizaciones de la función Firmware Supervisor. Esto no incluye actualizaciones de firmware del controlador que ocurren cuando la imagen del controlador vuelve a cargarse desde la tarjeta de memoria.

Monitoreo de estado y manejo de fallos

Consulte el Apéndice A, Indicadores de estado para obtener información sobre cómo interpretar los indicadores de estado y los mensajes en pantalla del controlador.

Visualización de estado mediante la barra en línea

La barra en línea muestra información acerca del proyecto y del controlador, incluido el estado del controlador, estado de forzados, estado de edición en línea y estado de seguridad.

Figura 32 – Botones de estado

Si se selecciona el botón de estado del controlador como se indicó anteriormente, la barra en línea muestra el modo del controlador (RUN) y el estado (OK). El indicador BAT combina el estado del controlador primario y el del homólogo de seguridad. Si uno de ellos o ambos presentan un fallo de batería, el indicador de estado se ilumina. El indicador de E/S combina el estado de las E/S estándar y las E/S de seguridad, y se comporta como indicador de estado del controlador. Las E/S con el estado de error más importante aparecen junto al indicador de estado.

Si se selecciona el botón Safety Status como se muestra a continuación, la barra en línea muestra la firma de tarea de seguridad.

Figura 33 – Visualización en línea de firma de seguridad

El botón Safety Status indica si el controlador está en bloqueo o desbloqueo de seguridad, o si hay un fallo. Además, muestra un icono que indica el estado de seguridad.

Tabla 39 – Icono de estado de seguridad

Si el estado de seguridad es	Aparece este icono
Safety Task OK (la tarea de seguridad funciona bien)	
Safety task inoperable (la tarea de seguridad no funciona)	
Partner Missing (falta el homólogo) Partner Unavailable (homólogo no disponible) Hardware Incompatible (hardware incompatible) Firmware Incompatible (firmware incompatible)	
Offline (fuera de línea)	

Los iconos aparecen de color verde cuando el controlador está en bloqueo de seguridad, de color amarillo cuando el controlador está en desbloqueo de seguridad, y de color rojo cuando hay un fallo de seguridad. Si existe una firma de tarea de seguridad, el icono incluye una pequeña marca de comprobación. 

Monitoreo de las conexiones

Usted puede monitorear el estado de las conexiones estándar y de seguridad.

Todas las conexiones

Si no ocurre comunicación con un dispositivo en la configuración de E/S del controlador por más de 100 ms, se sobrepasa el tiempo de espera por la comunicación y el controlador muestra las advertencias siguientes:

- El indicador de E/S ubicado en la parte frontal del controlador parpadea de color verde.
- Aparece un símbolo de alerta ⚠ sobre la carpeta I/O Configuration y sobre el dispositivo que ha sobrepasado el tiempo de espera.
- Se produce un fallo del dispositivo, al que puede obtener acceso mediante la ficha Connections del cuadro de diálogo Module Properties del dispositivo o mediante la instrucción GSV.

ATENCIÓN: Las conexiones de E/S de seguridad y de productor/consumidor no se pueden configurar de modo que se presente automáticamente un fallo de controlador cuando se pierda una conexión. Por lo tanto, es necesario monitorear los fallos de conexión para asegurarse de que el sistema de seguridad mantenga la integridad SIL 3/PLe.

Consulte Conexiones de seguridad en la página 121.

Conexiones de seguridad

En el caso de los tags asociados con los datos de seguridad producidos o consumidos, se puede monitorear el estado de las conexiones de seguridad mediante el miembro CONNECTION_STATUS. Para monitorear las conexiones de entrada y salida, los tags de Safety I/O tienen un miembro de estado de conexión llamado SafetyStatus. Los dos tipos de datos contienen dos bits: RunMode y ConnectionFaulted.

El valor RunMode indica si los datos consumidos se están actualizando activamente mediante un dispositivo que se encuentra en el modo de marcha (1) o en estado inactivo (0). El estado inactivo se indica si la conexión está cerrada, si la tarea de seguridad presenta un fallo, o si el dispositivo o el controlador remoto se encuentran en el modo de programación o en el modo de prueba.

El valor ConnectionFaulted indica si la conexión de seguridad entre el productor de seguridad y el consumidor de seguridad es válida (0) o presenta un fallo (1). Si ConnectionFaulted se pone en fallo (1) a consecuencia de una pérdida de conexión física, los datos de seguridad se ponen en cero.

En la tabla siguiente se describen las combinaciones de los estados RunMode y ConnectionFaulted.

Tabla 40 – Estado de la conexión de seguridad

Estado RunMode	Estado ConnectionFaulted	Operación de conexión de seguridad
1 = Marcha	0 = Válido	Los datos se controlan activamente mediante el dispositivo productor. El dispositivo productor se encuentra en el modo de marcha.
0 = Inactividad	0 = Válido	La conexión está activa y el dispositivo productor está en estado inactivo. Los datos de seguridad se ponen en cero.
0 = Inactividad	1 = Con fallo	Fallo en la conexión de seguridad. Se desconoce el estado del dispositivo productor. Los datos de seguridad se ponen en cero.
1 = Marcha	1 = Con fallo	Estado no válido.

Si se inhibe un módulo, el bit ConnectionFaulted se pone en fallo (1), mientras que el bit RunMode se pone en estado inactivo (0) en cada una de las conexiones asociadas con el módulo. En consecuencia, los datos de seguridad consumidos se ponen en cero.

Monitoreo de los indicadores de estado

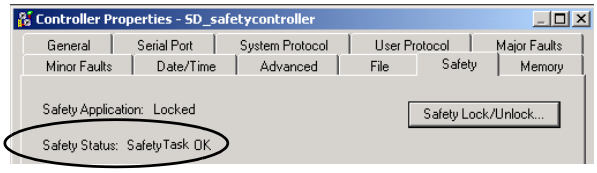
Los controladores Logix, incluso los controladores GuardLogix, aceptan palabras clave de estado que se pueden utilizar en la lógica para monitorear determinados eventos.

Para obtener más información acerca de cómo usar estas palabras clave, consulte el documento Logix5000 Controllers Controller Information and Status Programming Manual, publicación 1756-PM015.

Monitoreo del estado de seguridad

Vea la información de estado de seguridad en el botón de estado de seguridad en la barra de la conexión en línea y en la ficha Safety del cuadro de diálogo Controller Properties.

Figura 34 – Estado de la tarea de seguridad



Estas son las opciones posibles del estado de seguridad:

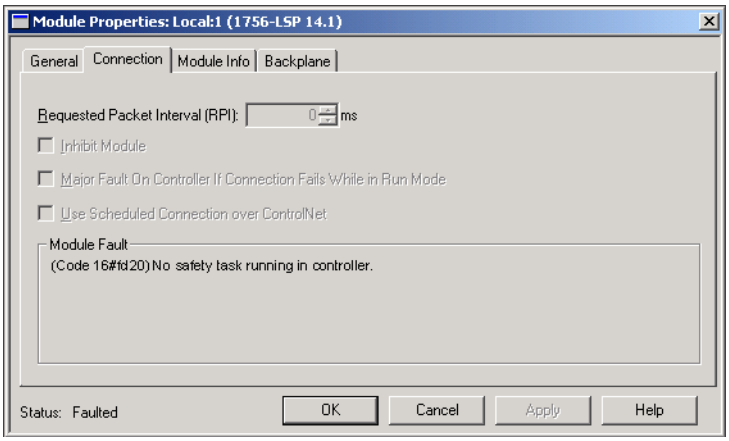
- Safety partner is missing or unavailable.
- Safety partner hardware is incompatible with primary controller.
- Safety partner firmware is incompatible with the primary controller.
- Safety task inoperable.
- Safety Task OK.

Con excepción de Safety task OK, las descripciones indican que hay un fallo de seguridad no recuperable.

Consulte Fallos mayores de seguridad (tipo 14) en la página 124 para obtener información sobre los códigos de fallo y las acciones correctivas.

El estado del homólogo de seguridad se puede ver en la ficha Connections del cuadro de diálogo Module Properties.

Figura 35 – Estado del homólogo de seguridad



Fallos del controlador

Los fallos en el sistema GuardLogix pueden ser fallos de controlador no recuperables, fallos de seguridad no recuperables en la aplicación de seguridad o fallos de seguridad recuperables en la aplicación de seguridad.

Fallos de controlador no recuperables

Se producen cuando falla el diagnóstico interno del controlador. Si se produce un fallo de controlador no recuperable, se interrumpe la ejecución de la tarea de seguridad y los dispositivos de E/S de seguridad entran en 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.

Si la tarea de seguridad encuentra un fallo de seguridad no recuperable que se elimina conforme a la programación en el gestor de fallos del controlador, la aplicación estándar sigue ejecutándose.

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

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

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

Fallos recuperables en la aplicación de seguridad

Si se produce un fallo recuperable en la aplicación de seguridad, es posible que el sistema pueda detener la ejecución de la tarea de seguridad, dependiendo de si el fallo es manejado por el gestor de fallos del programa en la aplicación de seguridad.

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 tipo 14, código 2. La ejecución del programa 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 el estado de seguridad y el productor de tags consumidos de seguridad ordena a los consumidores ponerlos también en estado de seguridad.

Los fallos recuperables le permiten editar la aplicación estándar y de seguridad según corresponda para corregir la causa del fallo. Sin embargo, si existe una firma de tarea de seguridad o si el controlador está en bloqueo de seguridad, debe primero desbloquear el controlador y eliminar la firma de tarea de seguridad antes de poder editar la aplicación 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 códigos de fallo con un mensaje de estado breve, como se describe en la página 127.

Códigos de fallo

La Tabla 41 muestra los códigos de fallo específicos de los controladores GuardLogix. 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 41 – Fallos mayores de seguridad (tipo 14)

Code	Causa	Estado	Acción correctiva
01	Se sobrepasó el tiempo del temporizador de vigilancia de tareas. La tarea del usuario no se ha completado en el período especificado. Un error en el programa ha provocado un lazo infinito, el programa es demasiado complejo para ejecutarse con la rapidez especificada, hay una tarea de mayor prioridad que impide que concluya esta tarea o se ha eliminado el homólogo de seguridad.	No recuperable	Borre el fallo. Si existe una firma de tarea de seguridad, la memoria de seguridad se reinicializa y la tarea de seguridad empieza a ejecutarse. Si no existe una firma de tarea de seguridad, debe volver a descargar el programa para que la tarea de seguridad pueda ejecutarse. Vuelva a insertar el homólogo de seguridad si fue retirado.
02	Hay un error en una rutina de la tarea de seguridad.	Recuperable	Corrija el error en la lógica del programa de usuario.
03	Falta el homólogo de seguridad.	No recuperable	Instale un homólogo de seguridad compatible.
04	El homólogo de seguridad no está disponible.	No recuperable	Instale un homólogo de seguridad compatible.
05	El hardware del homólogo de seguridad es incompatible.	No recuperable	Instale un homólogo de seguridad compatible.
06	El firmware del homólogo de seguridad es incompatible.	No recuperable	Actualice el homólogo de seguridad de modo que las revisiones mayores y menores de firmware coincidan con el controlador primario.
07	No se puede ejecutar la tarea de seguridad. Este fallo ocurre cuando la lógica de seguridad no es válida, por ejemplo, existe una desigualdad en la lógica entre el controlador primario y el homólogo de seguridad, se sobrepasó el tiempo permitido del temporizador de vigilancia o se contaminó la memoria.	No recuperable	Borre el fallo. Si existe una firma de tarea de seguridad, la memoria de seguridad se reinicializa mediante la firma de tarea de seguridad y la tarea de seguridad empieza a ejecutarse. Si no existe una firma de tarea de seguridad, debe volver a descargar el programa para que la tarea de seguridad pueda ejecutarse.
08	No se ha encontrado la hora coordinada del sistema (CST).	No recuperable	Borre el fallo. Configure un dispositivo para que sea el CST maestro.
09	Fallo de controlador no recuperable del homólogo de seguridad.	No recuperable	Borre el fallo y descargue el programa. Si el problema persiste, reemplace el homólogo de seguridad.

El documento Logix5000 Controllers Major and Minor Faults Programming Manual, publicación 1756-PM014, incluye descripciones de los códigos de fallo comunes a los controladores Logix.

Desarrollo de una rutina de fallo

Si se produce una condición de fallo suficientemente grave como para que el controlador se desactive, el controlador genera un fallo mayor y detiene la ejecución de la lógica.

En algunas aplicaciones no es conveniente que todos los fallos de seguridad desactiven todo el sistema. En esos casos, utilice una rutina de fallo para borrar un fallo determinado y dejar que la parte de control estándar del sistema siga funcionando, o configure algunas salidas para que permanezcan activadas.

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

El controlador admite dos niveles de manejo de fallos mayores:

- Rutina de fallo de programa
- Gestor de fallos del controlador

Ambas rutinas pueden utilizar las instrucciones GSV y SSV, como se describe en la página 125.

Rutina de fallo de programa

Cada programa puede tener su propia rutina de fallo. El controlador ejecuta la rutina de fallo de programa cuando falla una instrucción. Si la rutina de fallo de programa no borra el fallo, o si no existe una rutina de fallo de programa, el controlador ejecuta el gestor de fallos del controlador (si lo hay).

Gestor de fallos del controlador

El gestor de fallos del controlador es un componente opcional que se ejecuta cuando la rutina de fallo de programa no puede borrar el fallo o cuando este no existe.

Puede crear un programa para el gestor de fallos del controlador. Después de crear el programa, debe configurar una rutina como rutina principal.

El documento Logix5000 Controllers Major and Minor Faults Programming Manual, publicación 1756-PM014, proporciona información detallada acerca de cómo crear y probar una rutina de fallo.

Uso de instrucciones GSV/SSV

Los controladores Logix almacenan datos del sistema en objetos y no en archivos de estado. Se pueden utilizar las instrucciones Get System Value (GSV) y Set System Value (SSV) para recuperar y establecer datos del controlador.

La instrucción GSV recupera la información especificada y la coloca en el destino especificado. La instrucción SSV cambia el atributo especificado por datos procedentes de la fuente de la instrucción. Si introduce una instrucción GSV o SSV, el software de programación muestra las clases de objeto, los nombres de objeto y los nombres de atributo para cada instrucción.

En el caso de las tareas estándar, se puede utilizar la instrucción GSV a fin de obtener valores para los atributos disponibles. Si utiliza una instrucción SSV, el software solo muestra los atributos que usted puede establecer.

En el caso de la tarea de seguridad, las instrucciones GSV y SSV están más restringidas. Observe que las instrucciones SSV en las tareas de seguridad y estándar no pueden establecer el bit 0 (fallo mayor ante error) en el atributo de modo de un dispositivo de E/S de seguridad.

Para los objetos de seguridad, la Tabla 42 muestra los atributos cuyos valores puede obtener usando la instrucción GSV y los atributos que puede establecer usando la instrucción SSV, en las tareas de seguridad y estándar.

ATENCIÓN: Utilice las instrucciones GSV/SSV con precaución. Los cambios en los objetos pueden provocar la operación inesperada del controlador o lesiones al personal.

Tabla 42 – Accesibilidad a GSV/SSV

Objeto de seguridad	Nombre del atributo	Tipo de datos	Descripción del atributo	Accesible desde la tarea de seguridad		Accesible desde las tareas estándar	
				GSV	SSV	GSV[4]	SSV
Tarea de seguridad	Instance	DINT	Proporciona el número de instancia de este objeto de tarea. Los valores válidos son 0…31.	X		X	
	MaximumInterval	DINT[2]	Intervalo de tiempo máximo entre ejecuciones sucesivas de esta tarea.			X	X
	MaximumScanTime	DINT	Tiempo de ejecución registrado máximo (ms) para esta tarea.			X	X
	MinimumInterval	DINT[2]	Intervalo de tiempo mínimo entre ejecuciones sucesivas de esta tarea.			X	X
	Priority	INT	Prioridad relativa de esta tarea en comparación con otras tareas; Los valores válidos son 0…15.	X		X	
	Rate	DINT	Período de la tarea (en ms) o valor de sobrepaso del tiempo de espera para la tarea (en ms).	X		X	
	Watchdog	DINT	Límite de tiempo (en ms) para ejecutar todos los programas asociados con esta tarea.	X		X	
Programa de seguridad	Instance	DINT	Proporciona el número de instancia del objeto de programa.	X		X	
	MajorFaultRecord[1]	DINT[11]	Registra los fallos mayores para este programa.	X	X	X	
	MaximumScanTime	DINT	Tiempo máximo de ejecución registrado (ms) para este programa.			X	X
Rutina de seguridad	Instance	DINT	Proporciona el número de instancia de este objeto de rutina. Los valores válidos son 0…65,535.	X			
Controlador de seguridad	SafetyLocked	SINT	Indica si el controlador está en bloqueo o en desbloqueo de seguridad.	X		X	
	SafetyStatus[2]	INT	Especifica el estado de seguridad como: • Safety task OK. (1000000000000000) • Safety task inoperable. (1000000000000001) • Partner missing. (0000000000000000) • Partner unavailable. (0000000000000001) • Hardware incompatible. (0000000000000010) • Firmware incompatible. (0000000000000011)			X	
	SafetySignatureExists	SINT	Indica si está presente la firma de tarea de seguridad.	X		X	
	SafetySignatureID	DINT	Número de identificación de 32 bits.			X	
	SafetySignature	String[3]	Número de identificación de 32 bits.			X	
	SafetyTaskFaultRecord[1][2]	DINT[11]	Registra los fallos de la tarea de seguridad.			X	
AOI (seguridad)	LastEditDate	LINT	Sello de fecha y hora de la última edición a una definición de instrucción Add-On.			X	
	SignatureID	DINT	Número de identificación.			X	
	SafetySignatureID	DINT	Número de identificación de 32 bits.			X	

(1) Vea Acceso a atributos FaultRecord en la página 127 para obtener información sobre cómo obtener acceso a este atributo.

(2) Vea Captura de información de fallo en la página 127 para obtener información sobre cómo obtener acceso a este atributo.

(3) Longitud = 37.

(4) Desde la tarea estándar, la accesibilidad de GSV de los atributos de objeto de seguridad es la misma que para los atributos de objeto estándar.

Acceso a atributos FaultRecord

Cree una estructura definida por el usuario para simplificar el acceso a los atributos MajorFaultRecord y SafetyTaskFaultRecord.

Tabla 43 – Parámetros para obtener acceso a los atributos FaultRecord

Nombre	Tipo de datos	Estilo	Descripción
TimeLow	DINT	Decimal	Los 32 bits inferiores del valor de sello de hora del fallo
TimeHigh	DINT	Decimal	Los 32 bits superiores del valor de sello de hora del fallo
Type	INT	Decimal	Tipo de fallo (programa, E/S u otro)
Code	INT	Decimal	Código único para este fallo (depende del tipo de fallo)
Info	DINT[8]	Hexadecimal	Información específica del fallo (depende del tipo y código de fallo)

Para obtener más información sobre el uso de las instrucciones GSV y SSV, consulte el capítulo sobre instrucciones de entrada/salida del documento Instrucciones generales de loscontroladores Logix5000 – Manual de referencia, publicación 1756-RM003.

Captura de información de fallo

Los atributos SafetyStatus y SafetyTaskFaultRecord pueden captar información acerca de fallos no recuperables. Use una instrucción GSV en el gestor de fallos del controlador para captar y almacenar información de fallos. La instrucción GSV puede usarse en una tarea estándar junto con una rutina de gestor de fallos del controlador que borra el fallo y permite que las tareas estándar continúen ejecutándose.

Notas:

Indicadores de estado

Indicadores de estado de los controladores

El estado del controlador primario se muestra mediante cuatro indicadores de estado.

Tabla 44 – Descripciones de los indicadores de estado del controlador primario

Indicador	Estado	Descripción
RUN	Apagado	No hay tareas de usuario en ejecución. El controlador se encuentra en el modo PROG (programación).
	Verde	El controlador se encuentra en el modo RUN (marcha).
FORCE	Apagado	No hay forzados estándar ni de seguridad habilitados en el controlador.
	Ámbar	Se han habilitado forzados estándar y/o de seguridad. **Tome medidas de precaución al instalar (agregar) un forzado. Si instala un forzado, este entrará en vigor inmediatamente.**
	Ámbar parpadeante	Una o más direcciones de E/S, estándar y/o de seguridad, se han forzado a un estado activado o desactivado, pero no se han habilitado forzados. **Tome precauciones al habilitar forzados de E/S. Si activa forzados de E/S, todos los forzados de E/S existentes también entran en vigor.**
SD	Apagado	No hay actividad con la tarjeta de memoria.
	Verde parpadeante	El controlador está leyendo la tarjeta de memoria o escribiendo en esta. No retire la tarjeta de memoria mientras el controlador esté leyendo o escribiendo.
	Verde	
	Rojo parpadeante	La tarjeta de memoria no tiene un sistema de archivos válido.
	Rojo	El controlador no reconoce la tarjeta de memoria.
OK	Apagado	No hay alimentación eléctrica aplicada.
	Verde	El controlador está funcionando y no presenta fallos.
	Rojo parpadeante	• Fallo no recuperable o recuperable no manejado en el gestor de fallos. Todas las tareas del usuario, estándar y de seguridad, se detienen. • Si el controlador es nuevo, recién adquirido, requiere una actualización de firmware. La pantalla de estado indica Firmware Installation Required.
	Rojo	• El controlador está realizando los diagnósticos en el momento del encendido. • Ocurrió un fallo mayor no recuperable y el programa se borró de la memoria. • La carga del condensador en el módulo de almacenamiento de energía (ESM) se descarga al apagar el sistema. • El controlador está energizado, pero no está operativo. • El controlador está cargando un proyecto en la memoria no volátil.

El homólogo de seguridad tiene un indicador de estado OK.

Tabla 45 – Indicador de estado 1756-L7SP

Indicador	Estado	Descripción
OK	Apagado	No hay alimentación eléctrica aplicada.
	Verde	El homólogo de seguridad está funcionando y no presenta fallos.
	Rojo	Fallo de encendido o fallo de controlador no recuperable.

Pantalla de estado del controlador

La pantalla de estado del controlador presenta mensajes que proporcionan información acerca de la revisión de firmware del controlador, el estado del módulo de almacenamiento de energía (ESM), el estado del proyecto y los fallos mayores.

Mensajes de estado de seguridad

La pantalla del controlador primario puede mostrar los siguientes mensajes. El homólogo de seguridad muestra 'L7SP'.

Tabla 46 – Pantalla de estado de seguridad

Mensaje	Interpretación
No Safety Signature	La tarea de seguridad está en el modo marcha sin una firma de tarea de seguridad.
Safety Partner Missing	Falta el homólogo de seguridad o no está disponible.
Hardware Incompatible	El hardware del homólogo de seguridad y el del controlador primario son incompatibles.
Firmware Incompatible	Los niveles de revisión de firmware del homólogo de seguridad y del controlador primario son incompatibles.
No CST Master	No se ha encontrado el maestro de la hora coordinada del sistema (CST).
Safety Task Inoperable	La lógica de seguridad no es válida. Por ejemplo, se presentó una desigualdad entre el controlador primario y el homólogo de seguridad, se sobrepasó el tiempo de espera del temporizador de vigilancia o se contaminó la memoria.
Safety Unlocked	El controlador está en modo de marcha con una firma de seguridad, pero no está en bloqueo de seguridad.

Mensajes de estado general

Los mensajes descritos en la Tabla 47 generalmente aparecen al momento del encendido, al momento del apagado y mientras el controlador está en funcionamiento. Estos mensajes indican el estado del controlador y del ESM.

Tabla 47 – Pantalla de estado general

Mensaje	Interpretación
No aparece ningún mensaje	El controlador está apagado o se ha producido un fallo mayor no recuperable (MNRF). Examine el indicador OK para determinar si el controlador está energizado y determine el estado del controlador.
TEST	El controlador está realizando las pruebas en el momento del encendido.
PASS	Las pruebas en el momento del encendido se realizaron correctamente.
SAVE	Se está guardando un proyecto en la tarjeta SD en el momento del apagado. También puede ver el indicador SD (vea la página 129) para obtener información de estado adicional. Espere a que concluya la operación de guardar antes de retirar la tarjeta SD o de desconectar la alimentación eléctrica.
LOAD	Se está cargando un proyecto desde la tarjeta SD en el momento del encendido del controlador. También puede ver el indicador SD (vea la página 129) para obtener información de estado adicional. Espere a que concluya la carga antes de retirar la tarjeta SD, retirar el módulo ESM o desconectar la alimentación eléctrica.
UPDT	Se está realizando una actualización de firmware desde la tarjeta SD en el momento del encendido. También puede ver el indicador SD (vea la página 129) para obtener información de estado adicional. Si no desea que el firmware se actualice en el momento del encendido, cambie la propiedad Load Image del controlador.
CHRG	El ESM basado en condensador se está cargando.
1756-L7*x*/*X*	El número de catálogo y la serie del controlador.
Rev *XX.xxx*	La revisión mayor y menor del firmware del controlador.
No Project	No hay un proyecto cargado en el controlador. Para cargar un proyecto, use la aplicación Logix Designer para descargar el proyecto al controlador, o use una tarjeta SD para cargar un proyecto en el controlador.
Nombre del proyecto	El nombre del proyecto cargado actualmente en el controlador. El nombre indicado se basa en el nombre del proyecto especificado en la aplicación Logix Designer.
BUSY	Los dispositivos de E/S asociados con el controlador todavía no están totalmente energizados. Espere un tiempo para el encendido y la autoprueba del dispositivo de E/S.
Corrupt Certificate Received	El certificado de protección asociado con el firmware está contaminado. Vaya a http://www.rockwellautomation.com/support/ y descargue la revisión de firmware a la que desea actualizar el sistema. Reemplace la revisión de firmware que instaló previamente por la obtenida en el sitio web de asistencia técnica.
Corrupt Image Received	El archivo de firmware está contaminado. Vaya a http://www.rockwellautomation.com/support/ y descargue la revisión de firmware a la que desea actualizar el sistema. Reemplace la revisión de firmware que instaló previamente por la obtenida en el sitio web de asistencia técnica.
ESM Not Present	No está presente un ESM y el controlador no puede guardar la aplicación en el momento del apagado. Inserte un ESM compatible y, si se utiliza un ESM basado en condensador, no desconecte la alimentación eléctrica hasta que el ESM esté cargado.
ESM Incompatible	El ESM es incompatible con el tamaño de memoria del controlador. Reemplace el ESM incompatible por un ESM compatible.
ESM Hardware Failure	Se produjo un fallo del ESM y el controlador no puede guardar el programa en el caso de que se apague. Reemplace el ESM antes de desconectar la alimentación eléctrica del controlador para que se guarde el programa del controlador.
ESM Energy Low	El ESM basado en condensador no tiene suficiente energía para habilitar el controlador a fin de guardar el programa en caso de que se apague. Reemplace el ESM.
ESM Charging	El ESM basado en condensador se está cargando. No desconecte la alimentación eléctrica hasta que haya concluido la carga.
Flash in Progress	Se está realizando una actualización de firmware iniciada mediante el software ControlFLASH o AutoFlash. Deje que la actualización de firmware concluya sin interrupción.
Firmware Installation Required	El controlador está usando firmware de inicialización (es decir la revisión 1.*xxx*) y requiere una actualización de firmware. Actualice el firmware del controlador.
SD Card Locked	Está instalada una tarjeta SD bloqueada.

Mensajes de fallo

Si el controlador entró en fallo, estos mensajes pueden aparecer en la pantalla de estado.

Tabla 48 – Mensajes de fallo(1)

Mensaje	Interpretación
Major Fault T*XX*:C*XX mensaje*	Se detectó un fallo mayor del tipo *XX* y código *XX*. Por ejemplo, si la pantalla de estado indica Major Fault T04:C42 Invalid JMP Target, significa que se ha programado una instrucción JMP para que salte a una instrucción LBL no válida.
I/O Fault Local:*X #XXXX mensaje*	Ocurrió un fallo de E/S en un módulo en el chasis local. Se indican el número de ranura y el código de fallo, junto con una breve descripción. Por ejemplo, I/O Fault Local:3 #0107 Connection Not Found indica que no está abierta una conexión al módulo de E/S local en la ranura tres. Tome la acción correctiva correspondiente al tipo de fallo indicado.
I/O Fault *ModuleName #XXXX mensaje*	Ocurrió un fallo de E/S en un módulo en un chasis remoto. El nombre del módulo con fallo, como se encuentre configurado en el árbol de configuración de E/S de la aplicación Logix Designer, se indica junto con el código de fallo y una breve descripción del fallo. Por ejemplo, I/O Fault My_Module #0107 Connection Not Found indica que no está abierta una conexión al módulo llamado "My_Module". Tome la acción correctiva correspondiente al tipo de fallo indicado.
I/O Fault *ModuleParent:X #XXXX mensaje*	Ocurrió un fallo de E/S en un módulo en un chasis remoto. El nombre del primario del módulo se indica porque no está configurado ningún nombre de módulo en el árbol I/O Configuration de la aplicación Logix Designer. Además, se indica el código de fallo con una breve descripción del fallo. Por ejemplo, I/O Fault My_CNet:3 #0107 Connection Not Found indica que no está abierta una conexión a un módulo en la ranura 3 del chasis con el módulo de comunicación llamado My_CNet. Tome la acción correctiva correspondiente al tipo de fallo indicado.
X I/O Faults	Hay fallos de E/S presentes y *X* = el número de fallos de E/S presentes. En el caso de múltiples fallos de E/S, el controlador indica el primer fallo reportado. A medida que se resuelve cada fallo de E/S, el número de fallos indicados se reduce y el siguiente fallo reportado aparece indicado por el mensaje I/O Fault. Tome la acción correctiva correspondiente al tipo de fallo indicado.

(1) Para obtener detalles acerca de los códigos de fallo de E/S, consulte el documento Logix5000 Major, Minor, and I/O Fault Codes Programming Manual, publicación 1756-PM014.

Mensajes de fallo mayor recuperable

Los fallos mayores recuperables se indican mediante Major Fault T*XX*:C*XX mensaje* en la pantalla de estado del controlador. En la Tabla 49 en la página 133 se indican tipos de fallo específicos y los mensajes asociados tal como se muestran en la pantalla de estado.

Para obtener descripciones detalladas y métodos de recuperación sugeridos para los fallos mayores recuperables, consulte el documento Logix5000 Major, Minor, and I/O Fault Codes Programming Manual, publicación 1756-PM014.

Tabla 49 – Mensajes de estado de fallo mayor recuperable

Tipo	Código	Mensaje
1	1	Run Mode Powerup
1	60	Non-recoverable
1	61	Non-recoverable – Diagnostics Saved
1	62	Non-recoverable – Program Saved
3	16	I/O Connection Failure
3	20	Chassis Failure
3	21	
3	23	Connection Failure
4	16	Unknown Instruction
4	20	Invalid Array Subscript
4	21	Control Structure LEN or POS < 0
4	31	Invalid JSR Parameter
4	34	Timer Failure
4	42	Invalid JMP Target
4	82	SFC Jump Back Failure
4	83	Value Out of Range
4	84	Stack Overflow
4	89	Invalid Target Step
4	90	Invalid Instruction
4	91	Invalid Context
4	92	Invalid Action
4	990	Definido por el usuario
4	991	
4	992	
4	993	
4	994	
4	995	
4	996	
4	997	
4	998	
4	999	
6	1	Task Watchdog Expired
7	40	Save Failure

Tipo	Código	Mensaje
7	41	Bad Restore Type
7	42	Bad Restore Revision
7	43	Bad Restore Checksum
8	1	key switch Change Ignored
11	1	Positive Overtravel Limit Exceeded
11	2	Negative Overtravel Limit Exceeded
11	3	Position Error Tolerance Exceeded
11	4	Encoder Channel Connection Fault
11	5	Encoder Noise Event Detected
11	6	SERCOS Drive Fault
11	7	Synchronous Connection Fault
11	8	Servo Module Fault
11	9	Asynchronous Connection Fault
11	10	Motor Fault
11	11	Motor Thermal Fault
11	12	Drive Thermal Fault
11	13	SERCOS Communications Fault
11	14	Inactive Drive Enable Input Detected
11	15	Drive Phase Loss Detected
11	16	Drive Guard Fault
11	32	Motion Task Overlap Fault
11	33	CST Reference Loss Detected
18	1	CIP Motion Initialization Fault
18	2	CIP Motion Initialization Fault Mfg
18	3	CIP Motion Axis Fault
18	4	CIP Motion Axis Fault Mfg
18	5	CIP Motion Fault
18	6	CIP Module Fault
18	7	Motion Group Fault
18	8	CIP Motion Configuration Fault
18	9	CIP Motion APR Fault
18	10	CIP Motion APR Fault Mfg
18	128	CIP Motion Guard Fault

Códigos de fallo de E/S

Los fallos de E/S indicados por el controlador se indican en la pantalla de estado en uno de estos formatos:

- I/O Fault Local:*X #XXXX mensaje*
- I/O Fault *ModuleName #XXXX mensaje*
- I/O Fault *ModuleParent*:*X #XXXX mensaje*

La primera parte del formato se usa para indicar la ubicación del módulo con fallo. La manera en que se indica la ubicación depende de su configuración de E/S y de las propiedades del módulo especificadas en la aplicación Logix Designer.

La última parte del formato, #XXXX mensaje, puede usarse para diagnosticar el tipo de fallo de E/S y las posibles acciones correctivas. Para obtener detalles acerca de cada código de fallo de E/S, consulte el documento Logix5000 Major, Minor, and I/O Fault Codes Programming Manual, publicación 1756-PM014.

Tabla 50 – Mensajes de fallo de E/S

Código	Mensaje
#0001	Connection Failure
#0002	Insufficient Resource
#0003	Invalid Value
#0004	IOI Syntax
#0005	Destination Unknown
#0006	Partial Data Transferred
#0007	Connection Lost
#0008	Service Unsupported
#0009	Invalid Attribute Value
#000A	Attribute List Error
#000B	State Already Exists
#000C	Object Mode Conflict
#000D	Object Already Exists
#000E	Attribute Not Setable
#000F	Permission Denied
#0010	Device State Conflict
#0011	Reply Too Large
#0012	Fragment Primitive
#0013	Insufficient Command Data
#0014	Attribute Not Supported
#0015	Data Too Large
#0100	Connection In Use
#0103	Transport Not Supported
#0106	Ownership Conflict
#0107	Connection Not Found
#0108	Invalid Connection Type
#0109	Invalid Connection Size
#0110	Module Not Configured
#0111	RPI Out of Range
#0113	Out of Connections
#0114	Wrong Module

Código	Mensaje
#0115	Wrong Device Type
#0116	Wrong Revision
#0117	Invalid Connection Point
#0118	Invalid Configuration Format
#0119	Module Not Owned
#011A	Out of Connection Resources
#0203	Connection Timeout
#0204	Unconnected Message Timeout
#0205	Invalid Parameter
#0206	Message Too Large
#0301	No Buffer Memory
#0302	Bandwidth Not Available
#0303	No Bridge Available
#0304	ControlNet Schedule Error
#0305	Signature Mismatch
#0306	CCM Not Available
#0311	Invalid Port
#0312	Invalid Link Address
#0315	Invalid Segment Type
#0317	Connection Not Scheduled
#0318	Invalid Link Address
#0319	No Secondary Resources Available
#031E	No Available Resources
#031F	No Available Resources
#0800	Network Link Offline
#0801	Incompatible Multicast RPI
#0802	Invld Safety Conn Size
#0803	Invld Safety Conn Format
#0804	Invld Time Correct Conn Format
#0805	Invld Ping Intrvl EPI Multiplier
#0806	Time Coord Msg Min Multiplier

Mensajes de fallo de E/S (continuación)

Código	Mensaje
#0807	Time Expectation Multiplier
#0808	Multiplicador de interrupciones
#0809	Invld Max Consumer Number
#080A	Invld CPCRC
#080B	Time Correction Conn ID Invld
#080C	Safety Cfg Signature Mismatch
#080D	Safety Netwk Num Not Set OutOfBx
#080E	Safety Netwk Number Mismatch
#080F	Cfg Operation Not Allowed
#0814	Data Type Mismatch
#FD01	Bad Backplane EEPROM
#FD02	No Error Code
#FD03	Missing Required Connection
#FD04	No CST Master
#FD05	Axis or GRP Not Assigned
#FD06	SERCOS Transition Fault
#FD07	SERCOS Init Ring Fault
#FD08	SERCOS Comm Fault
#FD09	SERCOS Init Node Fault
#FD0A	Axis Attribute Reject
#FD1F	Safety Data Fault
#FD20	No Safety Task Running
#FD21	Invld Safety Conn Parameter
#FE01	Invalid Connection Type
#FE02	Invalid Update Rate
#FE03	Invalid Input Connection
#FE04	Invalid Input Data Pointer
#FE05	Invalid Input Data Size
#FE06	Invalid Input Force Pointer
#FE07	Invalid Output Connection

Código	Mensaje
#FE08	Invalid Output Data Pointer
#FE09	Invalid Output Data Size
#FE0A	Invalid Output Force Pointer
#FE0B	Invalid Symbol String
#FE0C	Invalid Scheduled P/C Instance
#FE0D	Invalid Symbol Instance
#FE0E	Module Firmware Updating
#FE0F	Invalid Firmware File Revision
#FE10	Firmware File Not Found
#FE11	Firmware File Invalid
#FE12	Automatic Firmware Update Failed
#FE13	Update Failed - Active Connection
#FE14	Searching Firmware File
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
—	

Notas:

Cambio del tipo de controlador

Dado que los controladores de seguridad tienen requisitos especiales y no son compatibles con ciertas funciones estándar, usted deberá conocer cómo se comporta el sistema cuando se cambia el tipo de controlador de tipo estándar a tipo de seguridad o viceversa en el proyecto del controlador. El cambio del tipo de controlador afecta los siguientes aspectos:

- Funciones compatibles
- Configuración física del proyecto (homólogo de seguridad y E/S de seguridad)
- Propiedades del controlador
- Componentes del proyecto tales como tareas, programas, rutinas y tags
- Instrucciones Add-On de seguridad

IMPORTANTE Los controladores GuardLogix 5560 y los controladores 1768 Compact GuardLogix® no son compatibles con Studio 5000 versión 21 o posteriores.

Cambio de un controlador estándar a uno de seguridad

Para cambiar el tipo de controlador adecuadamente, de un controlador estándar a un controlador de seguridad, la ranura del chasis ubicada justo a la derecha del controlador primario de seguridad debe estar disponible para el homólogo de seguridad.

Una vez confirmado el cambio de un proyecto de controlador estándar a un proyecto de controlador de seguridad, se crean componentes de seguridad a fin de cumplir con los requisitos mínimos de un controlador de seguridad:

- La tarea de seguridad solo se crea si no se ha alcanzado el número máximo de tareas descargables. La tarea de seguridad se inicializa con sus valores predeterminados.
- Se crean componentes de seguridad (la tarea de seguridad, el programa de seguridad, etc.).
- Se genera un número de red de seguridad (SNN) basado en tiempo para el chasis local.
- Cualquier función del controlador estándar que no sea compatible con el controlador de seguridad, por ejemplo, redundancia, se retira del cuadro de diálogo Controller Properties (si existía).

Cambio de un controlador de seguridad a uno estándar

Una vez confirmado el cambio de un proyecto de controlador de seguridad a controlador estándar, algunos componentes se cambian y otros se eliminan, como se describe a continuación:

- El homólogo de seguridad se elimina del chasis de E/S.
- Los dispositivos de E/S de seguridad y sus tags se eliminan.
- La tarea, los programas y las rutinas de seguridad se cambian a tarea, programas y rutinas estándar.
- Todos los tags de seguridad, salvo los tags de consumo de seguridad, se cambian a tags estándar. Los tags de consumo de seguridad se eliminan.
- Las asignaciones de tags de seguridad se eliminan.
- El número de red de seguridad (SNN) se elimina.
- Las contraseñas de bloqueo y desbloqueo de seguridad se eliminan.
- Si el controlador estándar es compatible con funciones que no estaban disponibles en el controlador de seguridad, esas nuevas funciones aparecen visibles en el cuadro de diálogo Controller Properties.

  SUGERENCIA Los controladores de seguridad homólogos no se eliminan, aunque no queden conexiones.

- Las instrucciones pueden seguir haciendo referencia a módulos que fueron eliminados y pueden producir errores de verificación.
- Los tags consumidos se eliminan cuando se elimina el módulo productor.
- Como resultado de los cambios en el sistema antes mencionados, las instrucciones específicas de seguridad y los tags de E/S de seguridad no se verifican.

Si el proyecto del controlador de seguridad contiene instrucciones Add-On de seguridad, debe eliminarlas del proyecto o cambiar su clase a estándar antes de cambiar el tipo de controlador.

Cambio de tipos de controlador de seguridad

IMPORTANTE Los controladores 1768 Compact GuardLogix y los controladores GuardLogix 5560 no son compatibles con la aplicación Logix Designer, versión 21.

Cuando se cambia de un tipo de controlador de seguridad a otro, las clases de tags, las rutinas y los programas no cambian. Los dispositivos de E/S que ya no son compatibles con el controlador de destino se eliminan.

La representación del homólogo de seguridad se actualiza para que aparezca apropiada para el controlador de destino:

- El homólogo de seguridad se crea en la ranura *x* (ranura primaria + 1) al cambiar de un controlador 1768 Compact GuardLogix a un controlador GuardLogix 5570.

- Al cambiar a un controlador 1768 Compact GuardLogix, el homólogo de seguridad se retira puesto que es interno al controlador Compact GuardLogix.

SUGERENCIA Los controladores 5570 GuardLogix aceptan 100 programas de seguridad en la tarea de seguridad, mientras que los controladores 1768 Compact GuardLogix aceptan 32.

Las instrucciones de punto flotante, tales como FAL, FLL, FSC, SIZE, CMP, SWPB y CPT, son compatibles en los controladores GuardLogix 5570, pero no en los controladores GuardLogix 5560 y 1768 Compact GuardLogix. Si su programa de seguridad contiene estas instrucciones, se pueden producir errores de verificación al cambiar de un controlador GuardLogix 5570 a un controlador GuardLogix 5560 o 1768 Compact GuardLogix.

Más recursos

Consulte el documento Logix5000 Controllers Add-On Instructions Programming Manual, publicación 1756-PM010 para obtener más información sobre las instrucciones Add-on.

Notas:

Números

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X

Notas:

Servicio de asistencia técnica de Rockwell Automation

Rockwell Automation proporciona información técnica a través de Internet para ayudarle a utilizar sus productos. En http://www.rockwellautomation.com/support encontrará notas técnicas y de aplicación, ejemplos de códigos y vínculos a Service Packs de software. También puede visitar nuestro centro de asistencia técnica en https://rockwellautomation.custhelp.com/, donde encontrará actualizaciones de software, información técnica, chat y foros de asistencia técnica, respuestas a preguntas frecuentes, y podrá registrarse a fin de recibir actualizaciones de notificación de productos.

Además, ofrecemos varios programas de asistencia técnica para instalación, configuración y resolución de problemas. Para obtener más información, comuníquese con el distribuidor o representante de Rockwell Automation correspondiente a su localidad, o visite http://www.rockwellautomation.com/services/online-phone.

Asistencia para la instalación

Si se le presenta algún problema durante las primeras 24 horas posteriores a la instalación, revise la información incluida en este manual. También puede comunicarse con el servicio de asistencia técnica al cliente para obtener ayuda inicial con la puesta en marcha del producto.

Estados Unidos o Canadá	1.440.646.3434
Fuera de los Estados Unidos o Canadá	Use el Worldwide Locator en http://www.rockwellautomation.com/rockwellautomation/support/overview.page o comuníquese con el representante de Rockwell Automation.

Devolución de productos nuevos

Rockwell Automation prueba todos sus productos antes de que salgan de la fábrica, para ayudar a garantizar su perfecto funcionamiento. No obstante, si su producto no funciona correctamente y necesita devolverlo, siga estos procedimientos.

Estados Unidos	Comuníquese con el distribuidor. Deberá proporcionar al distribuidor un número de caso de asistencia técnica al cliente (llame al número de teléfono anterior para obtener uno) a fin de completar el proceso de devolución.
Fuera de los Estados Unidos	Comuníquese con el representante local de Rockwell Automation para obtener información sobre el procedimiento de devolución.

Comentarios sobre la documentación

Sus comentarios nos ayudarán a atender mejor sus necesidades de documentación. Si tiene alguna sugerencia sobre cómo mejorar este documento, llene este formulario, publicación RA-DU002, disponible en http://www.rockwellautomation.com/literature/.

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., Alem 1050, 5º Piso, CP 1001AAS, Capital Federal, Buenos Aires, Tel.: (54) 11.5554.4000, Fax: (54) 11.5554.4040, www.rockwellautomation.com.ar
Chile: Rockwell Automation Chile S.A., Luis Thayer Ojeda 166, Piso 6, Providencia, Santiago, Tel.: (56) 2.290.0700, Fax: (56) 2.290.0707, www.rockwellautomation.cl
Colombia: Rockwell Automation S.A., Edf. North Point, Carrera 7 N° 156 – 78 Piso 18, PBX: (57) 1.649.96.00 Fax: (57)649.96.15, www.rockwellautomation.com.co
España: Rockwell Automation S.A., C/ Josep Plà, 101-105, 08019 Barcelona, Tel.: (34) 932.959.000, Fax: (34) 932.959.001, www.rockwellautomation.es
México: Rockwell Automation S.A. de C.V., Bosques de Cierulos Nº 160, Col. Bosques de Las Lomas, C.P. 11700 México, D.F., Tel.: (52) 55.5246.2000, Fax: (52) 55.5251.1169, 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) 441.59.00, Fax: (511) 222.29.87, 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, Fax: (1) 787.706.3939, 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, Fax: (58) 212.943.3955, www.rockwellautomation.com.ve

Publicación 1756-UM022C-ES-P - Mayo 2015