Manual del usuario

Allen-Bradley

Controladores GuardLogix

Números de catálogo 1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP, 1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP, 1756-L73SXT, 1756-L7SPXT

Información importante para el usuario

Las características de funcionamiento de los equipos de estado sólido son distintas de las de los equipos electromecánicos. El documento Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls (publicación SGI-1.1 disponible en la oficina local de ventas de Rockwell Automation o en línea en http://www.rockwellautomation.com/literature/) describe algunas diferencias importantes entre equipo de estado sólido y dispositivos electromecánicos cableados. Debido a esta diferencia, y también a la gran diversidad de usos de los equipos de estado sólido, todos los responsables de aplicar este equipo deben asegurarse de la idoneidad de cada una de las aplicaciones concebidas para estos equipos.

Rockwell Automation, Inc. no se responsabiliza bajo ningún concepto de los daños indirectos o consecuentes derivados del uso o de la aplicación de este equipo.

Los ejemplos y los diagramas incluidos en el manual son meramente ilustrativos. Debido a las múltiples variables y los requisitos asociados con cualquier instalación en particular, Rockwell Automation, Inc. no se puede responsabilizar de los resultados obtenidos por el uso real que se haga en función de los ejemplos y los diagramas.

Rockwell Automation, Inc. no asume ningún derecho de patente con respecto al uso de la información, los circuitos, el equipo o el software que se describen 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 todas las circunstancias en que se estimen necesarias.

	**ADVERTENCIA:** Identifica la información acerca de prácticas o circunstancias que pueden provocar una explosión en un ambiente peligroso, a raíz de la cual pueden producirse lesiones personales o la muerte, daños materiales o pérdidas económicas.
	**ATENCIÓN:** Identifica la información acerca de prácticas o circunstancias que pueden provocar lesiones personales o la muerte, daños materiales o pérdidas económicas. Los mensajes de Atención le ayudan a identificar los peligros y a reconocer las consecuencias.
	**PELIGRO DE CHOQUE:** Puede haber etiquetas en el exterior o en el interior del equipo (por ejemplo, en un variador o en un motor) para advertir sobre la posible presencia de voltajes peligrosos.
	**PELIGRO DE QUEMADURA:** En el equipo o dentro del mismo puede haber etiquetas (por ejemplo, en un variador o en un motor) a fin de advertir acerca de superficies que pueden llegar a alcanzar temperaturas peligrosas.
IMPORTANTE	Identifica la información crucial para comprender y aplicar debidamente el producto.

A continuación se resumen los cambios efectuados en este manual desde su última publicación.

Tema	Páginas
Información acerca de los controladores 1756-L71S	11, 18, 21, 27, 47
Guía para instalar el módulo de almacenamiento de energía	46

Notas:

Prefacio

Capítulo 1

Descripción general del sistema

Capítulo 2

Instalación del controlador

Capítulo 3

Configuración del controlador

Capítulo 4

Comunicación a través de redes

Capítulo 5

Cómo añadir, configurar, monitorear y reemplazar 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

Mantenimiento de la batería

Apéndice C

Cambio del tipo de controlador en proyectos RSLogix 5000

Apéndice D

Historial de cambios

Índice

Notas:

Tema	Página
Información sobre los controladores 1756 GuardLogix	11
Explicación de la terminología	12
Recursos adicionales	13

Este manual constituye una guía para utilizar los controladores GuardLogix™. Describe los procedimientos específicos de GuardLogix que se utilizan para configurar, operar y resolver problemas del controlador.

Utilice este manual si es responsable de diseñar, instalar, programar o resolver problemas de sistemas de control que utilicen controladores GuardLogix.

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 crear, operar y dar mantenimiento a sistemas de seguridad.

Para obtener información detallada sobre temas relacionados como la programación del controlador GuardLogix, los requisitos SIL 3/PLe o información sobre los componentes Logix estándar, vea la lista de Recursos adicionales en la página 13.

Información sobre los controladores 1756 GuardLogix

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

Tabla 1 – Diferencias entre los controladores 1756-L7*x*S y 1756-L6*x*S

Característica	**1756-L7*x*S** (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT)	**1756-L6*x*S** (1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP)
Compatibilidad con reloj y copia de seguridad usada para retención de memoria al momento del encendido	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
Indicadores de estado	Pantalla de estado desplazable y cuatro indicadores LED de estado	Indicadores LED de estado

Los controladores ControlLogix para ambientes difíciles, números de catálogo 1756-L73SXT y 1756-L7SPXT, proporcionan la misma funcionalidad que los controladores 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 extremas 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 extremas.

Explicación de la terminología

La siguiente tabla define los términos utilizados en este manual.

Tabla 2 – Términos y definiciones

Abreviatura	Significado de las siglas	Definición
1oo2	One Out of Two (uno de dos)	Se refiere al diseño del comportamiento de un sistema de seguridad con varios procesadores.
CIP	Common Industrial Protocol (protocolo industrial común)	Protocolo de comunicación diseñado para aplicaciones industriales de automatización.
CIP Safety	Common Industrial Protocol (protocolo industrial común) – Certificado de seguridad	Versión de CIP con clasificación SIL 3/PLe
DC	diagnostic coverage (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	Se usa para compatibilidad con reloj y copia de seguridad para retención de memoria al momento del encendido en los controladores 1756-L7xS y 1756-L73SXT.
GSV	Get System Value (obtener valor del sistema)	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.
PFD	Probability of Failure on Demand (probabilidad de fallo a demanda)	Probabilidad media de un sistema de fallar al realizar bajo demanda la función para la que está diseñado.
PFH	Probability of Failure per Hour (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	Velocidad esperada medida en tiempo para 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 (establecer valor del sistema)	Una instrucción que establece datos del sistema controlador.
–	Standard (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.

Recursos adicionales

Los documentos que se indican a continuación incluyen información adicional sobre productos de Rockwell Automation relacionados.

Tabla 3 – Publicaciones relacionadas con los controladores y sistemas GuardLogix

Para obtener más información acerca de	Consulte este recurso	Descripción
Requisitos de las aplicaciones (seguridad)	Sistemas controladores GuardLogix, publicación 1756-RM093	Contiene los requisitos detallados para obtener y mantener un SIL 3/PLe con el sistema controlador GuardLogix.
Baterías	Pautas para el tratamiento de baterías de litio, publicación AG-5.4	Proporciona información acerca del almacenamiento manipulación, transporte y desecho de las baterías de litio.
	Programmable Controllers Battery Reference, http://www.ab.com/programmablecontrol/batteries.html	Proporciona Hojas de datos sobre seguridad de materiales (MSDS) para baterías de reemplazo individuales.
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.
Diseño y selección	Logix5000 Controllers Design Considerations Reference Manual, publicación 1756-RM094	Proporciona a los usuarios avanzados las pautas para la optimización del sistema así como información sobre el sistema como orientación para las selecciones relacionadas al diseño del sistema.
	ControlLogix Selection Guide, publicación 1756-SG001	Proporciona un proceso de selección de alto nivel para componentes del sistema ControlLogix®, información crítica sobre las especificaciones para tomar las decisiones iniciales y vínculos a información completa sobre las especificaciones.
Guard I/O	Guard I/O DeviceNet Safety Modules User Manual, 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.
	POINT Guard I/O Safety Modules User Manual, publicación 1734-UM013	Proporciona información sobre cómo instalar, configurar y usar los módulos POINT Guard I/O™.
Instalación del hardware	ControlLogix Chassis and Power Supplies Installation Instructions, 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 la conexión a tierra y el cableado de 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 seguridad GuardLogix.
	Logix5000 Controllers General Instructions Reference Manual, 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.
	CIP Motion Configuration and Startup User Manual, publicación MOTION-UM003	Detalla cómo configurar un control de movimiento integrado en un sistema de aplicación de redes EtherNet/IP.
	CIP Motion 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 para configurar y programar un controlador Logix5000 para usar fases de equipos.

Tabla 3 – Publicaciones relacionadas con los controladores y sistemas GuardLogix

Para obtener más información acerca de	Consulte este recurso	Descripción
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 de escalera, rutinas de prueba, creación de instrucciones Add-On, datos de estado del controlador, manejo de fallos, importación y exportación de componentes del proyecto y más.
	Logix5000 Controllers Execution Time and Memory Use Reference Manual, publicación 1756-RM087	Ayuda a calcular el uso de memoria y el tiempo de ejecución de la lógica programada y ayuda a seleccionar entre diferentes opciones de programación.
Redundancia	ControlLogix Redundancy System User Manual, publicación 1756-UM523	Sirve de guía para el diseño, el desarrollo y la implementación de un sistema de redundancia ControlLogix estándar.
	ControlLogix Enhanced Redundancy System User Manual, publicación 1756-UM535	Sirve de guía para el diseño, el desarrollo y la implementación de un sistema de redundancia ControlLogix con características mejoradas.

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

Descripción general del sistema

Requisitos de las aplicaciones de seguridad

El controlador GuardLogix está certificado para ser usado en aplicaciones de seguridad hasta el nivel de integridad de seguridad (SIL) 3 y el nivel de rendimiento (e), en los 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 fallo (PFD y PFH), los ajustes del tiempo de reacción del sistema, y las pruebas de verificación de funcionamiento que cumplen con los criterios de SIL 3/PLe.

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 PFD/PFH, consulte el documento Sistemas controladores GuardLogix, publicación 1756-RM093. Se recomienda leer, comprender y completar estos requisitos antes de utilizar un sistema de seguridad SIL 3, PLe GuardLogix.

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

Consulte el documento Sistemas controladores GuardLogix, publicación 1756-RM093, para obtener detalles.

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 CIP Safety 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 53.

Firma de la tarea de seguridad

La firma de la tarea de seguridad está compuesta por un número de identificación, la fecha y la hora, información esta que identifica de forma única la parte de seguridad de un proyecto. Esto 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 creación, la grabación y la comprobación de 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 106 para obtener más información.

Diferenciación entre componentes estándar y de seguridad

Las ranuras del chasis de un sistema GuardLogix no utilizadas por la función de seguridad pueden ser ocupadas por otros módulos ControlLogix certificados según las directivas de compatibilidad electromagnética (EMC) y de bajo voltaje. Visite http://ab.com/certification/ce 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 parte estándar y la parte de seguridad de la aplicación. Para ayudar a crear esta diferenciación, el software de programación RSLogix 5000 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, el software RSLogix 5000 utiliza un atributo de clase de seguridad que se muestra cada vez que se ven en pantalla propiedades de una tarea de seguridad, un programa de seguridad, una rutina de seguridad, 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 HMI externos, ni mediante instrucciones de mensajes de otros controladores homólogos. El software RSLogix 5000 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 documento ControlLogix Controllers User Manual, publicación 1756-UM001, contiene información acerca de la utilización de dispositivos ControlLogix en aplicaciones estándar (que no sean de seguridad).

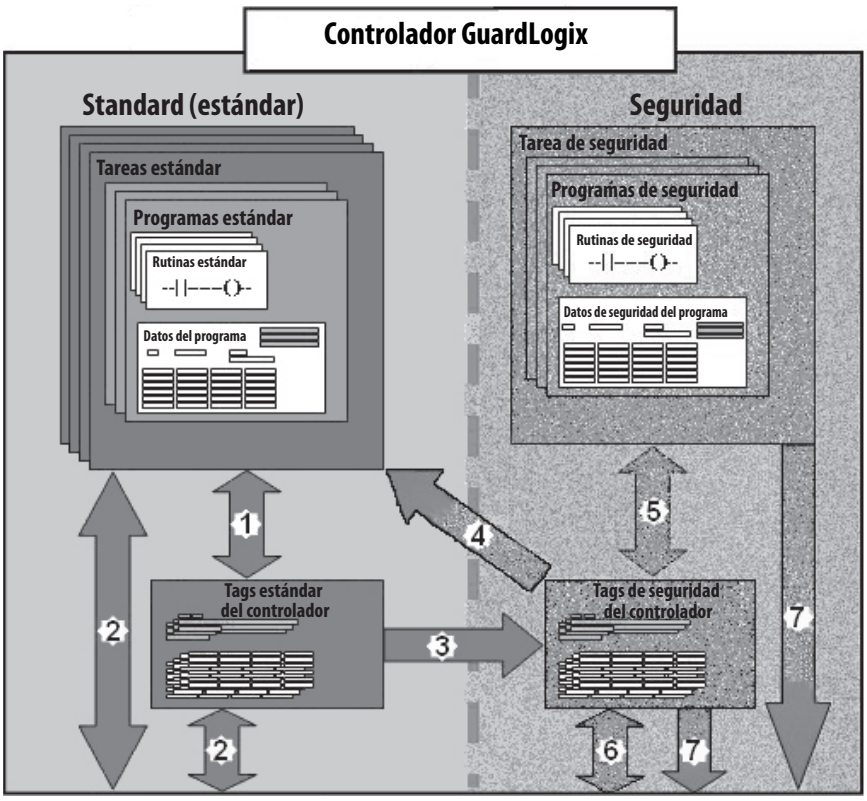
Dispositivos de HMI

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



Núm.	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, restringidos al programa o al 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 restringidos al 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 mediante las redes Ethernet o ControlNet, incluso los controladores GuardLogix 1756 y 1768.	
7	Los datos de tags de seguridad, restringidos al programa o al 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 consta de un controlador primario y un homólogo de seguridad que funcionan juntos en una arquitectura 1oo2. La Tabla 4 lista 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-L61S, 1756-L62S, 1756-L63S	1756-LSP
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

Núm. de cat.	Memoria de usuario (capacidad de RAM)	
	Tareas y componentes estándar	Tareas y componentes de seguridad
1756-L61S	2 MB	1 MB
1756-L62S	4 MB	1 MB
1756-L63S	8 MB	3.75 MB
1756-L71S	2 MB	1 MB
1756-L72S	4 MB	2 MB
1756-L73S,1756-L73SXT	8 MB	4 MB

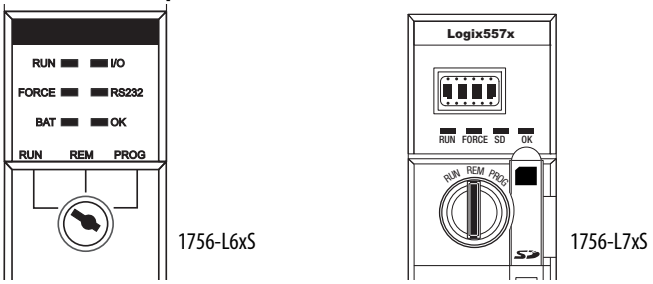
En el software RSLogix 5000, versión 18 o posteriores, el controlador GuardLogix es compatible con actualizaciones del sistema operativo o almacenamiento y recuperación de programas de usuario mediante una tarjeta de memoria. Sin embargo, en las versiones 16 y 17 del software RSLogix 5000, usted solo podía ver el contenido de una tarjeta de memoria si ésta estaba instalada en el controlador primario. Antes de la versión 16, las tarjetas de memoria no eran compatibles.

Consulte el Capítulo 8, Almacenamiento y carga de proyectos usando la memoria no volátil, para obtener más información.

Un conmutador 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
- PROG (Programa)
- REM (Remoto): este modo es habilitado por software, y 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 listadas en la página 28 son adecuadas para uso en las aplicaciones SIL 3. Para utilizar las fuentes de alimentación eléctrica en el nivel SIL 3 no se necesita configuración ni cableado adicionales.

Selección de los módulos Safety I/O

Los dispositivos de entrada y salida de seguridad pueden conectarse a CIP Safety I/O en redes DeviceNet o EtherNet/IP, lo que le permite al sistema controlador GuardLogix controlar los dispositivos de salida mediante comunicación DeviceNet o EtherNet/IP.

Para obtener la información más actualizada sobre números de catálogo de CIP Safety I/O, series certificadas y revisiones de firmware, visite http://www.ab.com/certification/safety.

Selección de las redes de comunicación

El controlador GuardLogix es compatible con comunicaciones que le permiten:

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

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

Tabla 6 – Módulos de comunicación

Para hacer 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	ENET-IN002
Controladores en la red ControlNet	1756-CN2, 1756-CN2R 1756-CN2RXT	CNET-IN005

El controlador GuardLogix puede conectarse al software de programación RSLogix 5000 mediante una conexión en serie o USB, un módulo EtherNet o un módulo ControlNet.

Los controladores 1756-L6xS tienen un puerto serial. Los controladores 1756-L7xS tienen un puerto USB.

Consulte Recursos adicionales en la página 13 para obtener más información sobre el uso de los módulos de comunicación de red.

Requisitos de programación

El software RSLogix 5000 es la herramienta de programación para aplicaciones del controlador GuardLogix.

Use la Tabla 7 para conocer las versiones mínimas de software que puede usar con los controladores GuardLogix. El software RSLogix 5000, versión 15, no es compatible con el nivel de integridad de seguridad (SIL) 3.

Tabla 7 – Versiones de software

Núm. de cat.	Versión de software RSLogix 5000(1)	Versión de software RSLinx® Classic Software(1)
1756-L61S, 1756-L62S	14	Cualquier versión
1756-L63S	16	
1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT	20	2.59

(1) Esta versión o posterior.

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 programados bajo la tarea de seguridad son compatibles solamente con lógica de escalera.

Tabla 8 – Características compatibles con el software RSLogix 5000, versión

Característica	Versión 14		Versión 16		Versión 17		Versión 18		Versión 19		Versión 20	
	Tarea de seguridad	Tarea estándar	Tarea de seguridad	Tarea estándar	Tarea de seguridad	Tarea estándar	Tarea de seguridad	Tarea estándar	Tarea de seguridad	Tarea estándar	Tarea de seguridad	Tarea estándar
Instrucciones adicionales				X		X	X	X	X	X	X	X
Alarmas y eventos				X		X		X		X		X
Función de registro del controlador					X	X	X	X	X	X	X	X
Control de acceso a datos							X	X	X	X	X	X
Rutinas de fase de equipo				X		X		X		X		X
Tareas de eventos				X		X		X		X		X
Firmware Supervisor				X		X	X	X	X	X	X	X
Diagramas de bloques de func. (FBD)				X		X		X		X		X
Movimiento integrado				X		X		X		X		X
Lógica de escalera	X	X	X	X	X	X	X	X	X	X	X	X
Cambio de idioma					X	X	X	X	X	X	X	X
Tarjeta de memoria							X	X	X	X	X	X
Importación y exportación en línea de componentes del programa						X		X		X		X
Rutinas de diagrama de función secuencial (SFC)				X		X		X		X		X
Texto estructurado				X		X		X		X		X
Conexiones unidifusión para tags de seguridad producidos y consumidos									X	X	X	X
Conexiones unidifusión para módulos de E/S de seguridad en redes EtherNet/IP											X	X

Para obtener información acerca del uso de estas funciones, consulte el documento Logix5000 Controllers Common Procedures Programming Manual, publicación 1756-PM001, las publicaciones listadas en la sección Recursos adicionales en la página 13 y la ayuda en línea del software RSLogix 5000.

Notas:

Instalación del controlador

Precauciones

Lea y siga estas precauciones durante el uso del producto.

Información del entorno y del envolvente

ATENCIÓN: Este equipo está diseñado para ser usado en ambientes industriales de Grado de Contaminación 2, en aplicaciones con sobrevoltaje de Categoría II (según se estipula en IEC 60664-1), a alturas de hasta 2000 m (6562 pies) sin reducción del régimen nominal.

Este equipo se considera equipo industrial del Grupo 1, Clase A según la publicación 11 de la IEC/CISPR. Si no se observan las normas de precaución adecuadas, pueden producirse problemas con la compatibilidad electromagnética en entornos residenciales y de otro tipo, debido a perturbaciones conducidas y radiadas.

Este equipo se suministra como equipo de tipo abierto. Debe montarse en un envolvente debidamente diseñado para las condiciones ambientales especificadas que se darán y adecuadamente diseñado para prevenir lesiones personales debidas a la exposición a piezas energizadas. El envolvente debe tener propiedades retardadoras de llama, para evitar o minimizar la propagación de llamas y respetar la clasificación de dispersión de la llama de 5 VA o tener aprobación para la aplicación si no fuese metálico. Solo se debe poder acceder al interior del envolvente mediante el uso de una herramienta. En las secciones posteriores de esta publicación puede haber información adicional relativa a las clasificaciones de tipo de envolvente que se necesitan para cumplir con los requisitos de determinadas certificaciones de seguridad del producto.

Además de esta publicación consulte:

- Pautas de cableado y conexión a tierra de equipos de automatización industrial, publicación 1770-4.1, para obtener información adicional sobre requisitos de instalación
- Normas NEMA 250 e IEC 60529, según sea el caso, para obtener 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 debe conocer los requisitos de seguridad en la aplicación del sistema y tener experiencia 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 activa se puede producir un arco eléctrico. Esto podría provocar una explosión en zonas peligrosas.

Asegúrese de desconectar la alimentación eléctrica y de constatar que la zona no sea peligrosa antes de seguir adelante.La recurrencia de arcos eléctricos puede provocar desgaste excesivo en el módulo y en su conector de acoplamiento. Los contactos desgastados pueden ofrecer resistencia eléctrica que puede afectar el funcionamiento del módulo.

Aprobación norteamericana para uso en zonas peligrosas

The following information applies when operating this equipment in hazardous locations:	**Informations sur l'utilisation de cet équipement en environnements dangereux:**
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.	Les produits marqués « CL I, DIV 2, GP A, B, C, D » ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.
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.	**AVERTISSEMENT:** RISQUE D'EXPLOSION • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles.

Cuando este equipo se utiliza en lugares peligrosos, debe tenerse en cuenta la siguiente información:

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 uno de los productos se suministra con distintivos en la placa de datos técnicos del fabricante, que indican el código de temperatura de 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 equipo en su sistema están sujetas a investigación por parte de la autoridad local con la debida jurisdicción al momento de la instalación.

ADVERTENCIA: PELIGRO DE EXPLOSIÓN

- No desconecte el equipo, a menos que se haya desactivado la alimentación eléctrica o que esté seguro que la zona no es peligrosa.
- No desconecte las conexiones a este equipo, a menos que se haya desactivado la alimentación eléctrica o que esté seguro que la zona no es peligrosa. Ajuste 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 considerada no peligrosa.

Aprobación legal europea para ubicación en zonas peligrosas

Lo siguiente aplica cuando el producto tiene la marca Ex.

Este equipo fue diseñado para ser utilizado en atmósferas potencialmente explosivas, tal como lo define la Directiva 94/9/CE de la Unión Europea. Cumple con los Requisitos Esenciales de Seguridad y Salud en relación al diseño y a la fabricación de equipos de Categoría 3 para uso en atmósferas potencialmente explosivas Zona 2, disponibles en el anexo II de esta directiva.

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

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

ADVERTENCIA:

- El equipo se debe instalar en un recinto que cuente al menos con un grado de protección IP54 al utilizarse en ambientes de zona 2.
- Este equipo se debe utilizar dentro de las clasificaciones establecidas por Rockwell Automation.
- Este equipo debe usarse sólo con backplanes de Rockwell Automation con certificación ATEX.
- Ajuste bien las conexiones externas de empalme con este equipo mediante tornillos, seguros deslizantes, conectores roscados u otros medios proporcionados con este producto.
- No desconecte el equipo, a menos que se haya desactivado la alimentación eléctrica o que esté seguro que la zona no es peligrosa.

Evite una descarga electrostática

ATENCIÓN: Este equipo es sensible a las descargas electrostáticas, las cuales pueden causar daños internos y afectar el funcionamiento normal. Siga las siguientes pautas al usar este equipo:

- Toque un objeto que esté conectado a tierra para descargar el potencial electrostático de su cuerpo.
- Use una muñequera conductiva aprobada.
- No toque los conectores ni los pines de las tarjetas de componentes.
- No toque los componentes de circuitos dentro del equipo.
- Utilice una estación de trabajo a prueba de cargas electrostáticas, siempre que sea posible.
- Cuando no vaya a usar el equipo, guárdelo en un paquete adecuado con protección contra descargas electrostáticas.

Asegúrese de tener todos los componentes

Antes de comenzar, asegúrese de tener todos los componentes necesarios.

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

Controladores 1756-L6xS

Una llave 1747-KY y la batería 1756-BA2 se incluyen con el controlador 1756-L6xS, mientras que el homólogo de seguridad 1756-LSP se envía con la batería 1756-BA2.

Si desea conectar un dispositivo al puerto en serie del controlador (por ejemplo, conectar una computadora al controlador), use un cable en serie 1756-CP3.

Para la memoria no volátil, puede usar una tarjeta 1784-CF128 CompactFlash con controladores 1756-L6xS GuardLogix, revisión de firmware 18 y posteriores.

Controladores 1756-L7xS

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

Núm. de 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 1784-SD1 Secure Digital (SD), 1 GB • Llave 1747-KY
1756-L7SP	Homólogo de seguridad	• Módulo de almacenamiento de energía (ESM) 1756-SPESMNSE
1756-L73SXT	Controlador primario para temperatura extrema	• 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	Entonces use esta pieza
Memoria no volátil	1784-SD1 (1 GB) o 1784-SD2 (2 GB)
Que el ESM instalado descargue su energía almacenada residual 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 sin alimentación eléctrica de respaldo WallClockTime. Además, puede usar este ESM con un controlador 1756-L73S (8 MB) o uno con menor memoria solamente.
ESM que protege el controlador evitando la conexión USB y el uso de 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 del EMS, consulte la sección Calcule la asistencia técnica de WallClocktime del ESM en la página 123.

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

(3) Para el controlador primario de temperaturas extremas y el homólogo de seguridad 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.

Núm. de 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.

Núm. de 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.

Conecte la batería (controladores 1756-L6xS únicamente)

Los controladores 1756-L6xS y el homólogo de seguridad 1756-LSP tienen una batería de litio cuyo reemplazo podría ser necesario durante la vida útil del producto.

ADVERTENCIA: Cada vez que conecte o que desconecte la batería puede producirse un arco eléctrico. Esto podría provocar una explosión en zonas peligrosas. Asegúrese de desconectar la alimentación eléctrica y de constatar que la zona no sea peligrosa antes de seguir adelante.

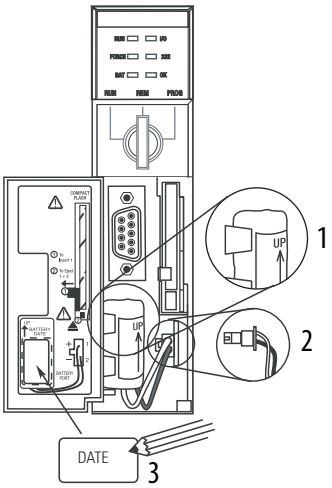
Para obtener información de seguridad sobre el manejo de las baterías de litio, incluido el manejo y desecho de baterías con fugas, consulte el documento Pautas para el tratamiento de baterías de litio, publicación AG 5-4.

Para mantener la memoria del controlador mientras el este no tiene alimentación eléctrica, conecte una batería. Siga el procedimiento tanto para el controlador 1756-L6*x*S como para el homólogo de seguridad 1756-LSP.

IMPORTANTE Conecte solo una batería 1756-BA2 al controlador. Si conecta una batería diferente, puede dañar el controlador.

Siga estos pasos para instalar una batería 1756-BA2 nueva.

1. Coloque la batería como se muestra.
2. Conecte la batería:
   + Rojo
   - Negro
3. Anote la fecha de instalación de la batería en la etiqueta de la batería, y adhiera la etiqueta en la parte interior de la puerta del controlador.



Vea el Apéndice B para obtener información sobre el mantenimiento de la batería.

Instale el controlador en el chasis

Puede instalar o retirar un controlador mientras el chasis recibe alimentación y el sistema está en funcionamiento.

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.

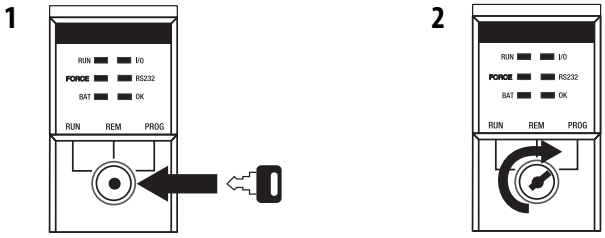
Asegúrese de desconectar la alimentación eléctrica y de constatar que la zona no sea peligrosa antes de seguir adelante. La recurrencia de arcos eléctricos puede provocar desgaste excesivo en el módulo y en su conector de acoplamiento. Los contactos desgastados pueden crear resistencia eléctrica, la cual puede afectar el funcionamiento del módulo.

IMPORTANTE En el caso de los controladores 1756-L7xS y los homólogos de seguridad 1756-L7SP, ESM comienza a cargarse cuando ocurre uno de los siguientes:

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

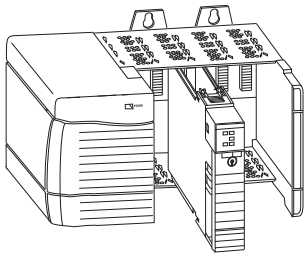
Cuando se conecta la alimentación eléctrica, el ESM se carga por hasta dos minutos según lo indicado por CHRG o ESM Charging en la pantalla de estado.

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



El homólogo de seguridad no tiene un interruptor de llave.

3. Alinee la tarjeta de circuito con las guías superior e inferior en el chasis.



4. Inserte el controlador en el chasis.

   El controlador está completamente instalado cuando se encuentra al 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 descritos anteriormente para instalar el homólogo de seguridad.

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

Insertar o retirar 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 zonas peligrosas. Asegúrese de desconectar la alimentación eléctrica y de constatar que la zona no sea peligrosa antes de seguir adelante.

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, si conecta o desconecta la alimentación eléctrica o si se produce un fallo, la tarjeta podría cargar un sistema operativo o un proyecto diferente en el controlador.

Los controladores 1756-L7xS utilizan tarjetas Secure Digital (SD). Vea la página 31.

El controlador 1756-L6xS utiliza tarjetas CompactFlash (CF). Vea la página 33.

Tarjeta Secure Digital (controladores 1756-L7xS)

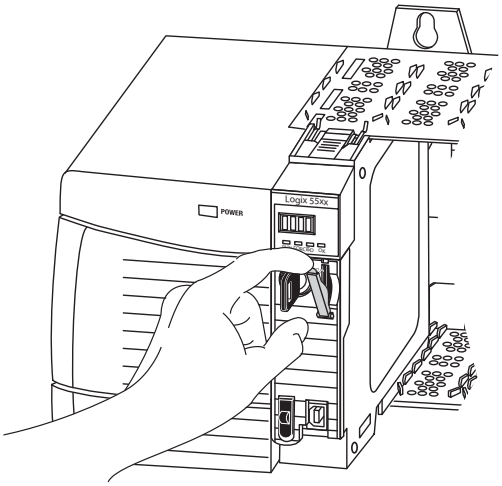
El controlador 1756-L7*x*S se envía con una tarjeta SD instalada. Recomendamos que deje una tarjeta SD instalada.

Retire la tarjeta SD

Si desea extraer la tarjeta SD del controlador 1756-L7*x*S, siga estos pasos.

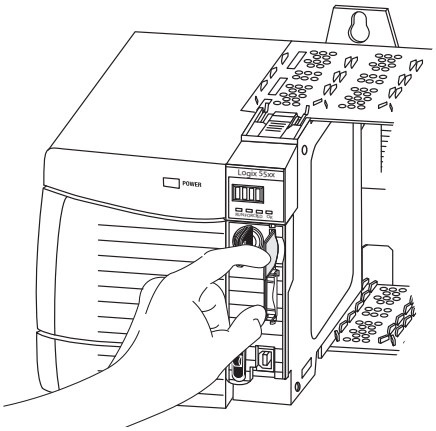
IMPORTANTE Verifique que el indicador de estado de la tarjeta SD esté apagado y que la tarjeta no esté en uso antes de retirarla.

1. Coloque el interruptor de llave en la posición PROG.
2. Abra la puerta para acceder a la tarjeta SD.



32015-M

3. Presione y suelte la tarjeta SD para expulsarla.



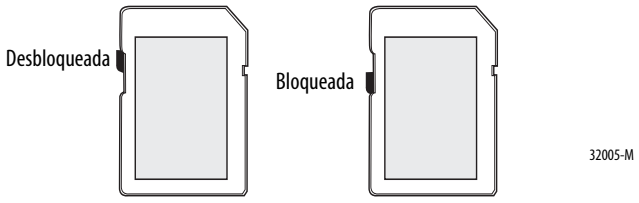
32004-M

4. Retire la tarjeta SD y cierre la puerta.

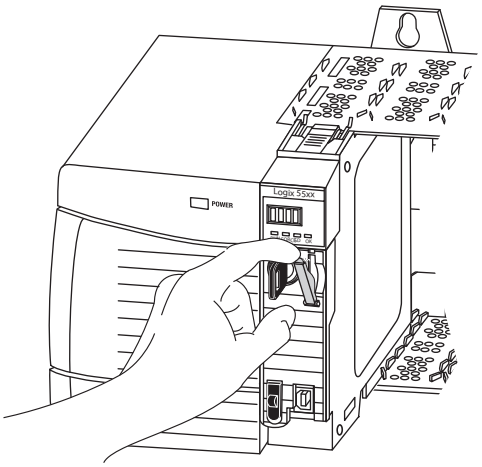
Instale la tarjeta SD

Siga estos pasos para instalar la tarjeta SD en los controladores 1756-L7*x*S.

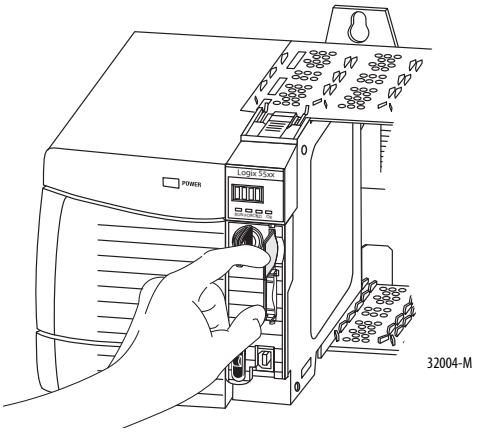
1. Verifique que la tarjeta SD esté bloqueada o desbloqueada, según su preferencia.



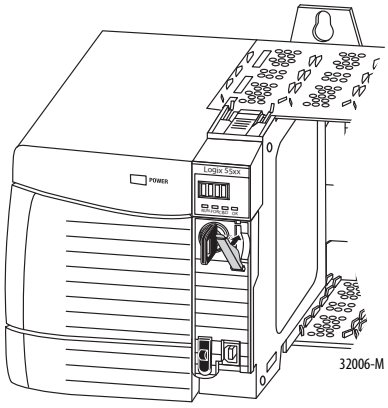
2. Abra la puerta de la tarjeta SD.



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.



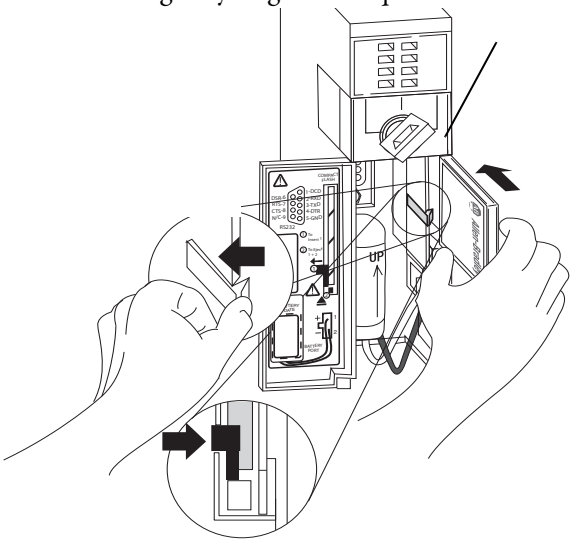
Tarjeta CompactFlash (controladores 1756-L6xS)

Los controladores 1756-L6xS no se envían con tarjetas CompactFlash instaladas.

Instale una tarjeta CF

Siga estos pasos para insertar la tarjeta de memoria.

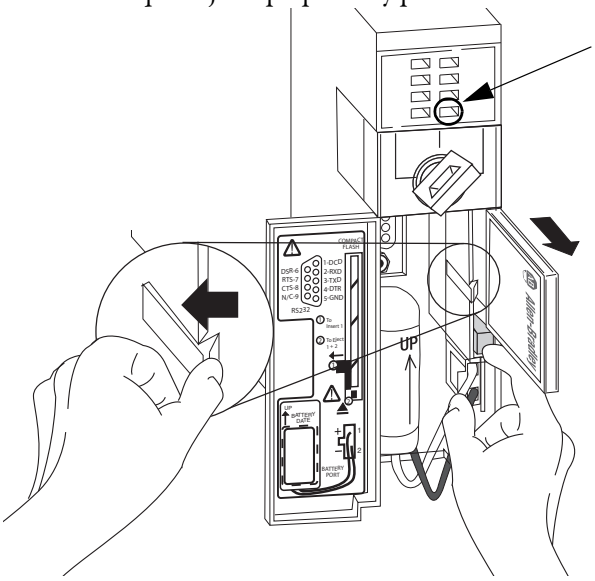
1. Coloque el interruptor de llave en la posición PROG.
2. Abra la puerta del controlador.
3. Coloque el seguro hacia la izquierda.
4. Inserte la tarjeta de memoria con el logotipo de A-B orientado hacia la izquierda.
5. Suelte el seguro y asegúrese de que se deslice sobre la tarjeta de memoria.



Retire una tarjeta CF

Siga estos pasos para retirar la tarjeta de memoria.

1. Si el indicador de estado OK se ilumina de color verde y parpadea, espere hasta que deje de parpadear y permanezca de color verde.



2. Abra la puerta del controlador.
3. Coloque y mantenga el seguro hacia la izquierda.
4. Presione el botón de expulsión y retire la tarjeta.
5. Suelte el seguro.

Haga las conexiones de comunicación

Los controladores 1756-L7xS tienen un puerto USB. Vea Conecte al puerto serial del controlador 1756-L7xS.

Los controladores 1756-L6xS tienen un puerto serial. Vea Conecte al puerto serial del controlador 1756-L6xS en la página 37.

Conecte al puerto serial del controlador 1756-L7xS

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

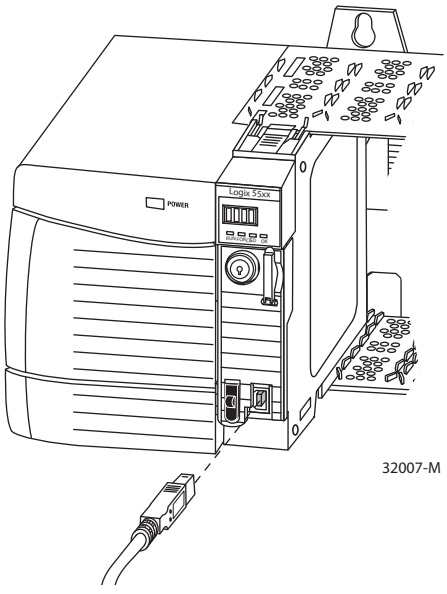
Para usar el puerto USB del controlador usted debe tener el software RSLinx, versión 2.59 o posterior, instalado en su estación de trabajo. Use un cable USB para conectar su estación de trabajo al puerto USB. Con esta conexión es posible actualizar el firmware y descargar programas al controlador directamente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

ATENCIÓN: El puerto USB está diseñado para programación local temporal solamente, no para una conexión permanente.

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

ADVERTENCIA: No use el puerto USB en zonas peligrosas.

Figura 3 – Conexión USB



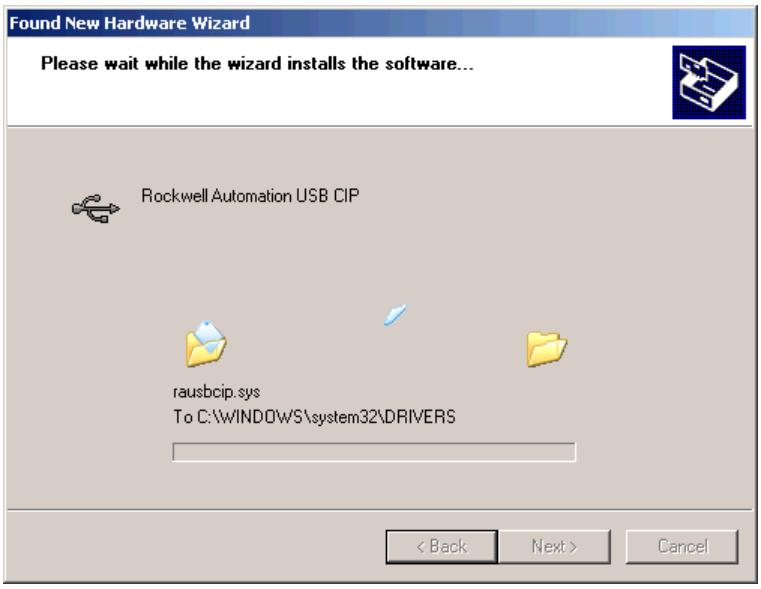
Para configurar el software RSLinx para usar un puerto USB, primero debe configurar un driver USB. Para configurar un driver USB, realice este procedimiento.

1. Conecte su controlador y estación de trabajo usando 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 Se no 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 (esto es lo recomendado) y haga clic en Next.

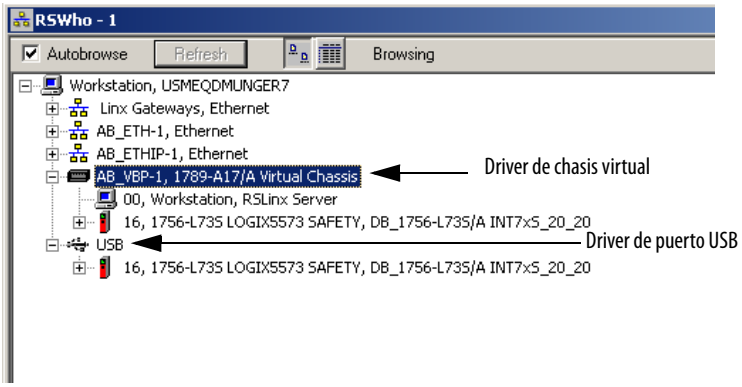
   Se instala el software.



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

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

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



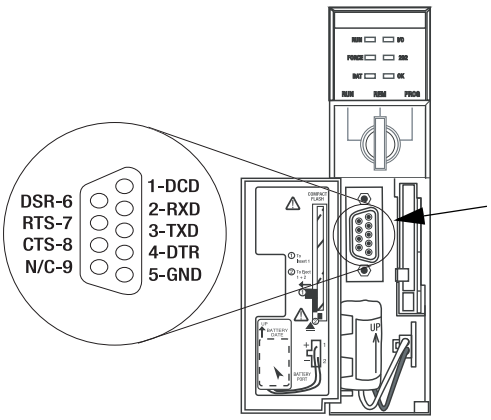
Conecte al puerto serial del controlador 1756-L6xS

ADVERTENCIA: Si conecta o desconecta el cable en serie con la alimentación eléctrica conectada a este módulo o el dispositivo en serie en el otro extremo del cable, puede ocurrir un arco eléctrico. Esto podría provocar una explosión en zonas peligrosas.

Antes de continuar, asegúrese de que la alimentación eléctrica esté desconectada o de que la zona no sea peligrosa.

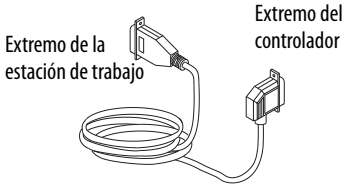
Use el puerto serial del controlador 1756-L6*x*S para la comunicación RS-232.

Figura 4 – Puerto serial



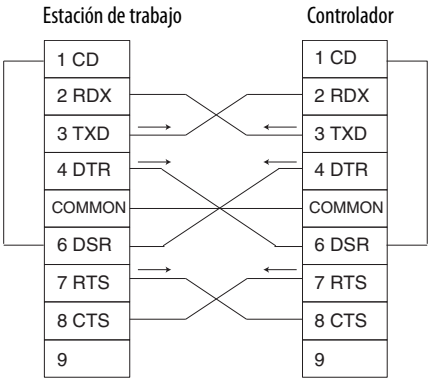
Para conectar una estación de trabajo al puerto serial, use uno de los siguientes cables:

- Cable en serie 1756-CP3
- Cable 1747-CP3 de la familia de productos SLC (si usa este cable, quizás no cierre la puerta del controlador).



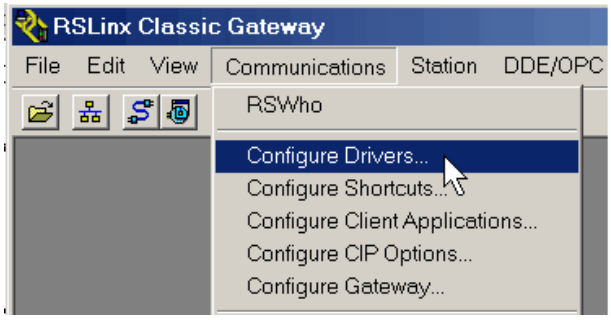
Si va a preparar su propio cable serial, siga estas pautas.

- No debe medir más de 15.2 m (50 pies).
- Cablee los conectores como se muestra a continuación.
- Conecte el blindaje a ambos conectores.

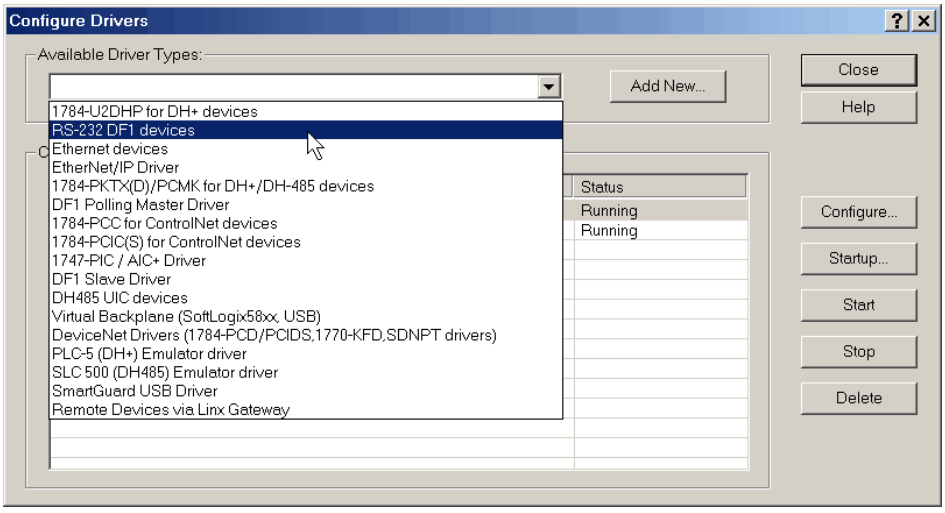


Siga estos pasos para usar el software RSLinx para configurar el driver del dispositivo RS-232 DF1 para comunicaciones en serie.

1. En el software RSLinx, desde el menú Communications, seleccione Configure Drivers.

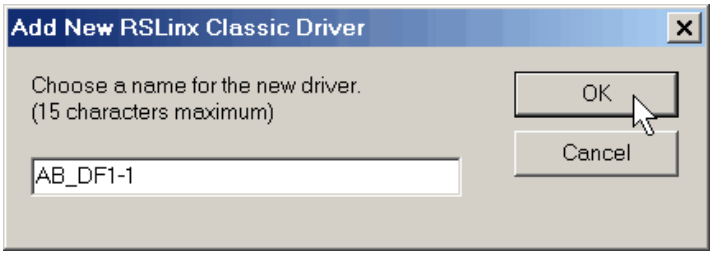


Aparece el cuadro de diálogo Configure Drivers.

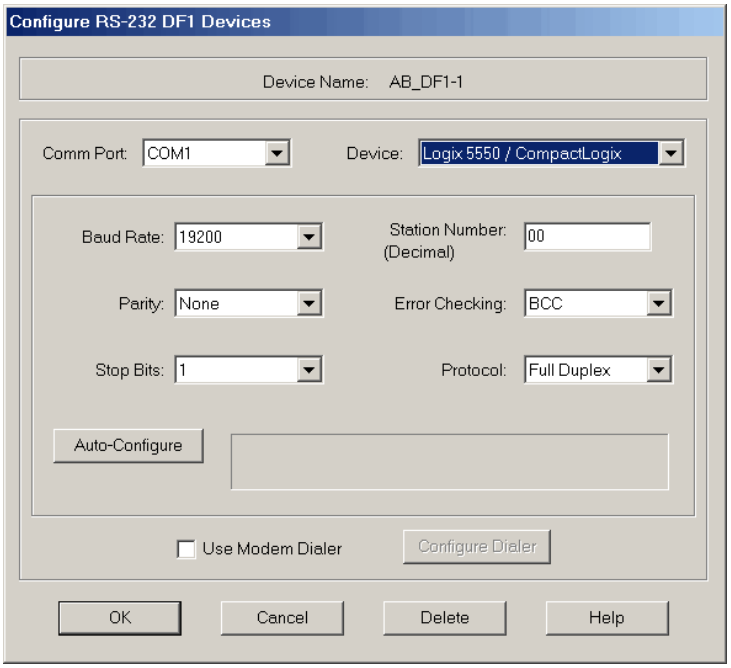


2. En la lista desplegable Available Driver Types, seleccione el driver del dispositivo RS-232 DF1.
3. Haga clic en Add New.

Aparece el cuadro de diálogo Add New RSLinx Driver.



4. Escriba el nombre del driver y haga clic en OK.
5. Especifique los parámetros de configuración del puerto en serie.
   a. En el menú desplegable Comm Port seleccione el puerto serie (en la estación de trabajo) al que está conectado el cable.
   b. En el menú desplegable Device, seleccione Logix 5550/CompactLogix.
   c. Haga clic en Auto-Configure.



6. Si la auto-configuración se realiza correctamente, haga clic en OK.

   Si la auto-configuración no se realiza correctamente, verifique que se haya seleccionado el puerto de comunicación correcto.
7. Haga clic en Close.

Actualización del controlador

Los controladores se envían sin firmware. El firmware del controlador se suministra en paquete con el software de programación RSLogix 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/.

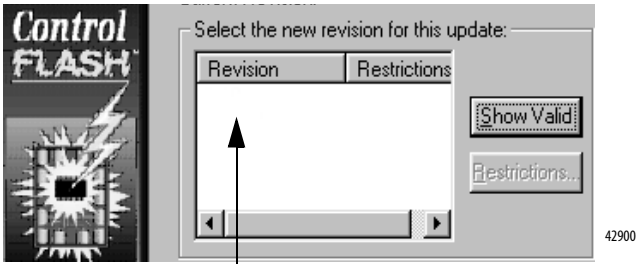
Puede actualizar su firmware usando el software ControlFLASH™, que se incluye con el software RSLogix 5000 software, o usando la función AutoFlash del software RSLogix 5000.

Uso del software ControlFLASH para actualizar el firmware

Con el software ControlFlash, versión 8 (software RSLogix 5000, versión 18 o posterior), el homólogo de seguridad se actualiza automáticamente cuando se actualiza el controlador.

IMPORTANTE	En los controladores 1756-L7xS, 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 a continuación 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 al que desea actualizar el controlador y haga clic en Next.
8. Para empezar a actualizar el controlador, haga clic en Finish y, a continuación, en Yes.

   Cuando el controlador esté actualizado, 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 lo contrario se interrumpirá la actualización.

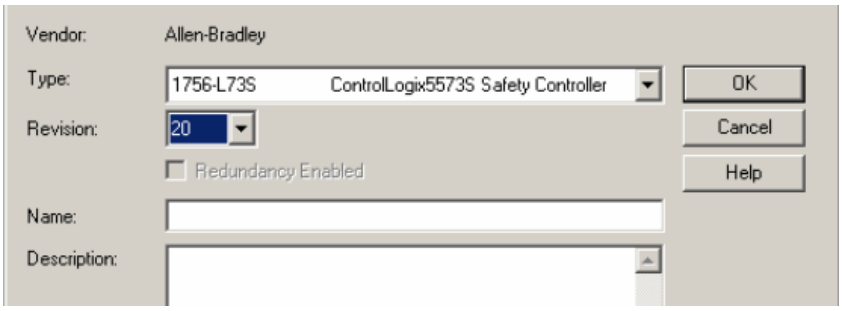
SUGERENCIA	Si se interrumpe la actualización ControlFLASH del controlador, el controlador 1756-L7*x*S revierte a inicializar el firmware, o sea el firmware revisión 1.*xxx*.

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

Cómo usar AutoFlash para actualizar el firmware

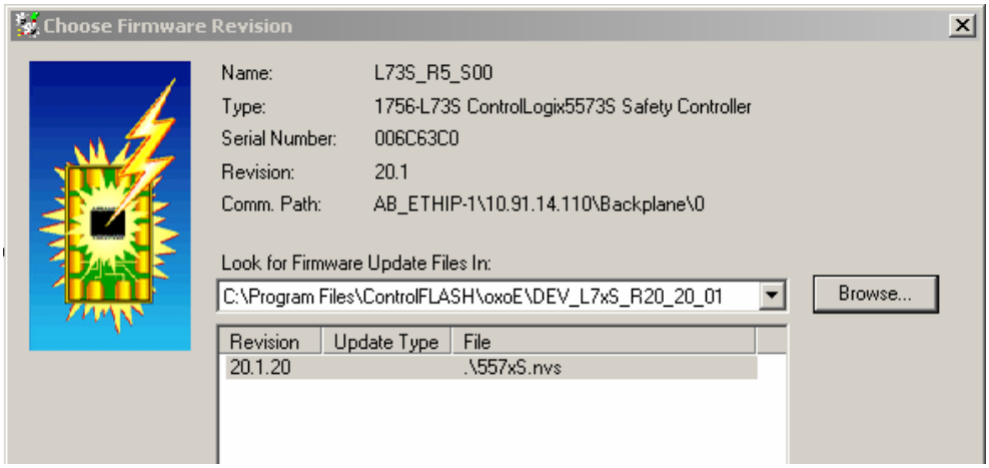
Para actualizar su firmware de su controlador con la función AutoFlash del software RSLogix 5000, realice estos pasos.

1. Verifique que esté hecha la conexión de red apropiada y que su driver de red esté configurado en el software RSLinx.
2. Use el software de programación RSLogix 5000 para crear un proyecto del controlador en la versión que usted necesita.



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

4. Seleccione su controlador y haga clic en Update Firmware.
5. Seleccione la revisión de firmware a la cual va a actualizar el sistema.



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 realizar otras tareas en el software RSLogix 5000.

Cómo seleccionar el modo de funcionamiento del controlador

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

Tabla 9 – Modos de funcionamiento del controlador

Si desea	Seleccione uno de estos modos				
	Run	Remoto			PROG (Programa)
		Run	Test	PROG (Programa)	
Colocar las salidas en el estado que indica la lógica del proyecto	X	X			
Colocar las salidas al estado configurado para el modo de programación			X	X	X
Ejecutar (escanear) tareas	X	X	X		
Cambiar el modo del controlador a través del software		X	X	X	
Descargar un proyecto		X	X	X	X
Programar una red ControlNet				X	X
Editar el proyecto 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

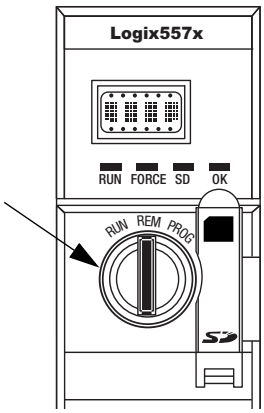
Use el interruptor de llave para cambiar el modo de operación

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

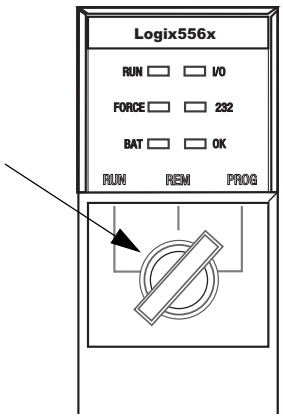
- Programación (PROG)
- Remoto (REM)
- Marcha (RUN)

Figura 5 – Interruptor de llave del controlador

1756-L7*x*S



1756-L6*x*S



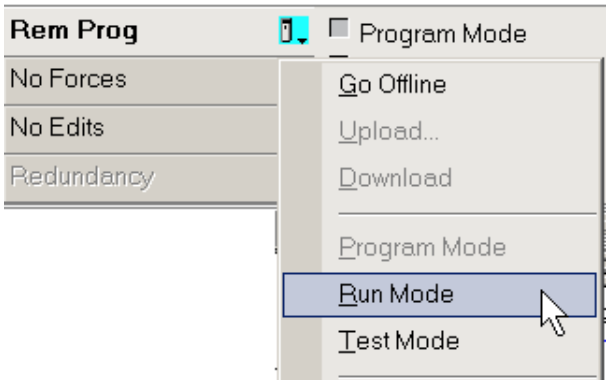
Use el software RSLogix 5000 para cambiar el modo de operación

Dependiendo del modo del controlador especificado mediante el interruptor de llave, puede cambiar el modo de operación del controlador mediante el software RSLogix 5000.

Cuando está en línea con el controlador y el interruptor de llave del controlador está establecido en Remoto (REM o la posición central), puede usar el menú Controller Status situado en la esquina superior izquierda de la ventana del software RSLogix 5000 para especificar estos modos de operación:

- Programación remota
- Marcha remota
- Prueba remota

Figura 6 – Modo de operación mediante el software RSLogix 5000



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 los modos de marcha o programación, cambiarán las opciones de menú.

Desinstale el módulo de almacenamiento de energía (ESM)

Los controladores 1756-L7xS se envían con un ESM instalado.

Controlador	Núm. de cat. de ESM instalado
Controlador 1756-L7xS	1756-ESMCAP
Controlador para temperatura extrema 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 interrumpa la alimentación eléctrica de los controladores 1756-L7*x*S, ya sea porque se desconectó la alimentación eléctrica del chasis o porque se retiró el controlador de un chasis activado, no retire el ESM inmediatamente.

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

- Use el módulo 1756-ESMNSE si su aplicación requieren que el ESM instalado descargue su energía almacenada residual 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 de un controlador 1756-L7xS.

IMPORTANTE Antes de retirar un ESM, haga los ajustes necesarios en el programa considerando los cambios potenciales al atributo WallClockTime.

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

ADVERTENCIA: Si su aplicación requiere que el ESM descargue su energía almacenada residual a un nivel de 40 µJ o menos antes de transportarlo a su aplicación o fuera de ella, use solo 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 luego se apaga.

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

   No existe indicación visual de cuándo han transcurrido los 20 minutos. **Es necesario dar seguimiento a dicho período de tiempo**.

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

Asegúrese de desconectar la alimentación eléctrica y de constatar que la zona no sea peligrosa antes de seguir adelante. La recurrencia de arcos eléctricos puede provocar desgaste excesivo en el módulo y en su conector de acoplamiento.

1. Retire la llave del interruptor de llave.

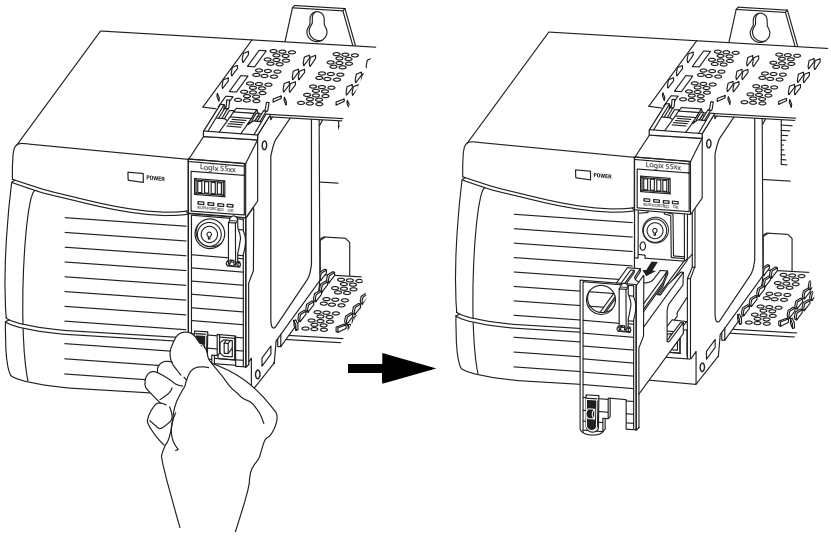
IMPORTANTE El siguiente paso depende de cuál de las siguientes condiciones aplica a su aplicación:

- Si va a retirar el ESM de un controlador 1756-L7*x*S(XT) activado, vaya al paso 2.
- Si está retirando el ESM de un controlador 1756-L7*x*S(XT) que no está activado, ya sea porque se desconectó la alimentación eléctrica del chasis o porque se retiró el controlador de un chasis activado, **no retire** el ESM inmediatamente.

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

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

2. Use su pulgar para presionar hacia abajo el dispositivo de liberación negro y jale el ESM separándolo del controlador.



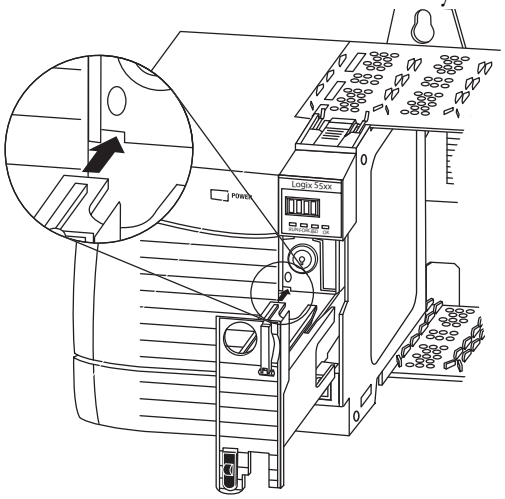
Instale el módulo de almacenamiento de energía (ESM)

Tabla 10 – Módulos de almacenamiento de energía compatibles

Núm. de cat.	ESM compatibles
1756-L7xS	1756-ESMCAP, 1756-ESMNSE, 1756-ESMNRM
1756-L7xSXT	1756-ESMCAPXT, 1756-ESMNSEXT, 1756-ESMNRMXT
1756-L7SP	1756-SPESMNSE, 1756-SPESMNRM
1756-L7SPXT	1756-SPESMNSEXT, 1756-SPESMNRMXT

Para instalar un SMS, realice 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 un daño potencial al producto al insertar el ESM, alinee el ESM en la pista 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, puede tardar hasta 15 segundos para 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 esté totalmente cargado vea la pantalla y confirme que los mensajes 'CHRG' o 'ESM Charging' no estén presentes.

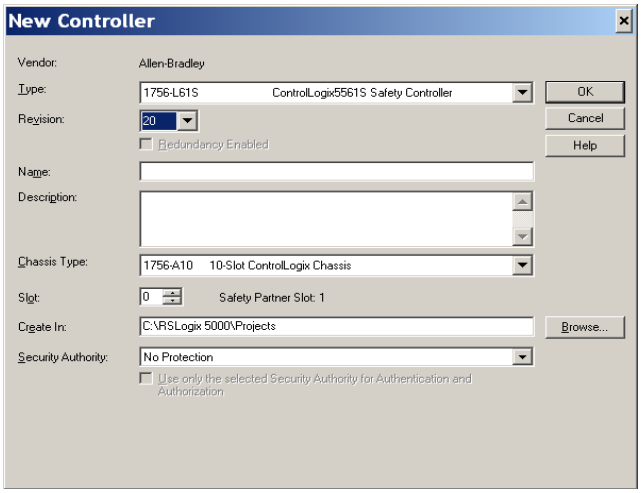
SUGERENCIA Verifique los atributos del objeto WallClockTime después de instalar un ESM para verificar que la hora del controlador sea la correcta.

Configuración del controlador

Creación de un proyecto de controlador

A fin de configurar y programar su controlador, utilice el software RSLogix 5000 para crear y administrar un proyecto de controlador.

1. Para crear un nuevo proyecto en el software RSLogix 5000, haga clic en el botón New de la barra de herramientas principal.
2. En el menú desplegable Type, seleccione un controlador GuardLogix:
   - Controlador 1756-L61S ControlLogix5561S
   - Controlador 1756-L62S ControlLogix5562S
   - Controlador 1756-L63S ControlLogix5563S
   - Controlador 1756-L71S ControlLogix5571S
   - Controlador 1756-L72S ControlLogix5572S
   - Controlador 1756-L73S ControlLogix5573S



3. Introduzca la más reciente revisión de firmware del controlador.
4. Escriba un nombre para el controlador.

   Al crear un proyecto, el proyecto recibe el mismo nombre que el controlador. Sin embargo, usted puede cambiar de nombre al proyecto o al controlador.

5. Seleccione el tamaño del chasis.
6. Introduzca el número de ranura del controlador.

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

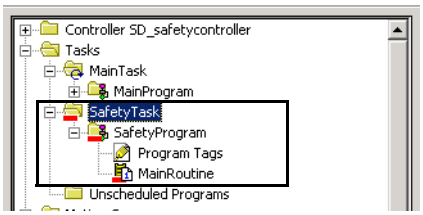
   Si selecciona un número de ranura para el controlador primario que no admite la ubicación del homólogo de seguridad justo a la derecha del controlador primario, se le pedirá que introduzca un número válido de ranura.
7. Especifique la carpeta en la que se debe almacenar el proyecto del controlador de seguridad.
8. En RSLogix 5000, versión 20 o posterior, seleccione una opción de Security Authority.

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

El software RSLogix 5000 crea automáticamente 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 7 – Tarea de seguridad en el organizador del controlador



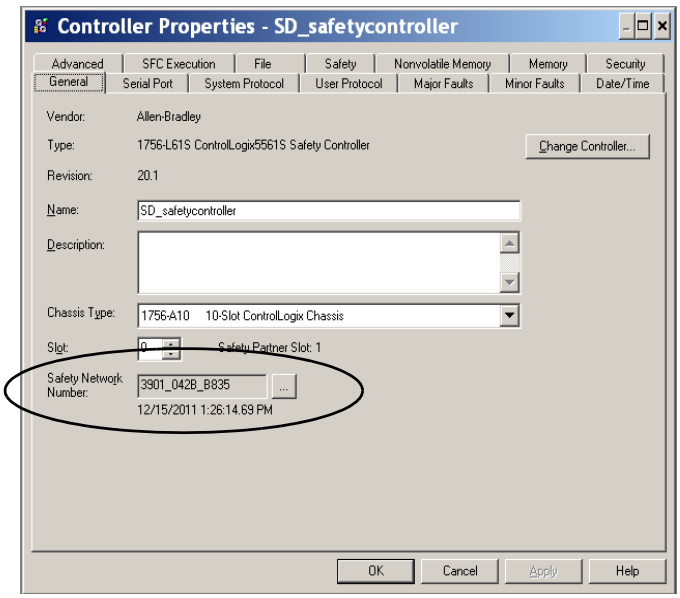
Una barra roja debajo del icono de la carpeta distingue los programas y las rutinas de seguridad de los componentes estándar del proyecto en el organizador del controlador RSLogix 5000.

Cuando se crea un nuevo proyecto de seguridad, el software RSLogix 5000 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 conveniente introducir un SNN específico.

Figura 8 – Número de red de seguridad



SUGERENCIA

Puede utilizar el cuadro de diálogo Controller Properties para cambiar de un controlador estándar a otro de seguridad y viceversa; para ello, haga clic en Change Controller. Sin embargo, esto afecta considerablemente los proyectos estándar y de seguridad.

Vea el Apéndice C, Cambio del tipo de controlador en proyectos RSLogix 5000, 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.

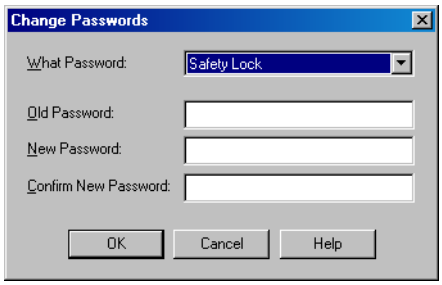
Establecimiento de contraseñas para bloqueo y desbloqueo de seguridad

El bloqueo de seguridad del controlador ayuda a proteger los componentes de control de seguridad frente a una posible modificación. Esto solo afecta a los componentes de seguridad como la tarea de seguridad, los programas de seguridad, las rutinas de seguridad y los tags de seguridad. No afecta a 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. Seleccione Tools > Safety > Change Password.
2. En el menú desplegable What Password, seleccione Safety Lock o Safety Unlock.

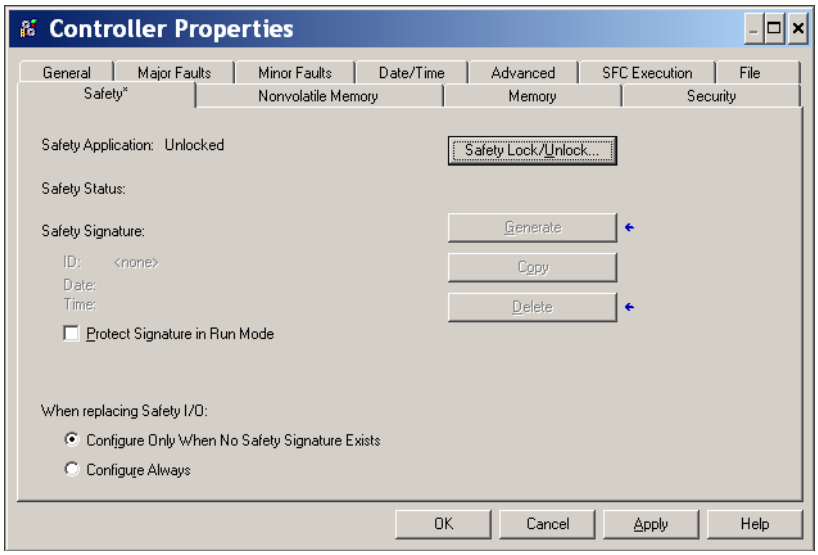


3. Escriba la contraseña anterior, si existe.
4. Escriba y confirme la nueva contraseña.
5. Haga clic en OK.

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

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

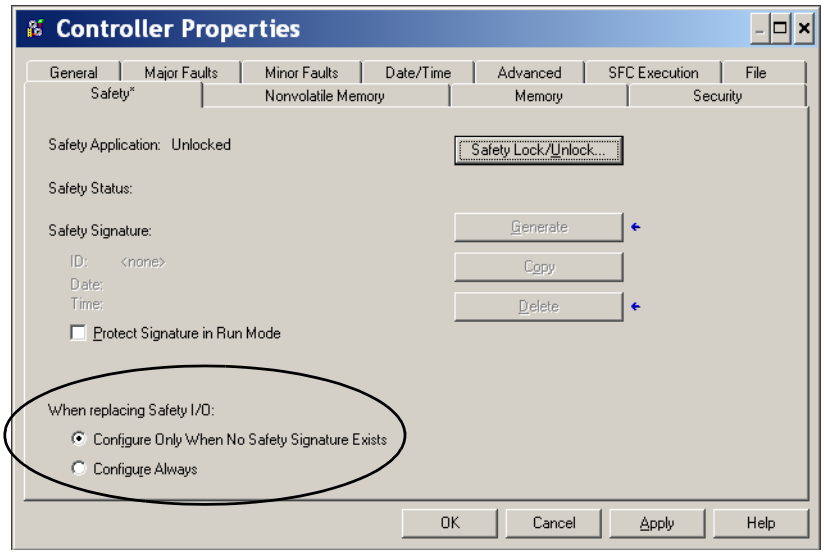
Usted puede evitar la generación o eliminación de la firma de la tarea de seguridad mientras el controlador está en el modo marcha o marcha remota, independientemente de que la aplicación de seguridad esté bloqueada o desbloqueada, seleccionando Protect Signature in Run Mode en la ficha Safety del cuadro de diálogo Controller Properties.



Reemplazo de un módulo de E/S

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

Figura 9 – Opciones de reemplazo de módulos de E/S



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

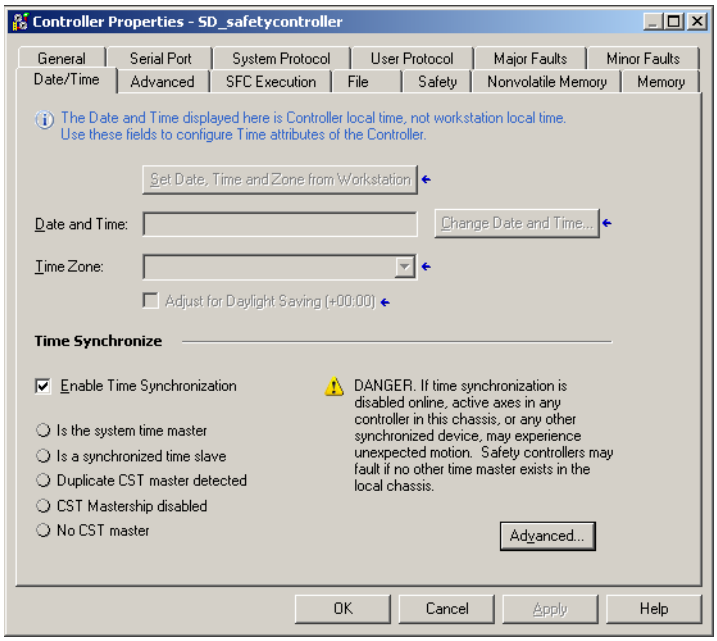
Vea el Capítulo 5, Cómo añadir, configurar, monitorear y reemplazar CIP Safety I/O para obtener más información.

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). Para permitir que el controlador se convierta en el maestro de la hora coordinada del sistema, habilite Time Synchronization en la ficha Date/Time del cuadro de diálogo Controller Properties. La opción Time Synchronization proporciona un mecanismo estándar para sincronizar los relojes en una red de dispositivos distribuidos.

(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 la tarea de seguridad en la página 16 y Generación de una firma de tarea de seguridad en la página 106 para obtener más información.

Figura 10 – 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 restringidos al controlador.

Para obtener detalles sobre cómo configurar los controladores de seguridad homólogos y cómo producir y consumir tags de seguridad, consulte Tags de seguridad producidos/consumidos en la página 97.

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 permite el encaminamiento de mensajes CIP Safety desde y hacia dispositivos CIP Safety a través de puentes, conmutadores y encaminadores.

Para mantener un alto grado de integridad durante el encaminamiento a través de puentes, conmutadores y encaminadores 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

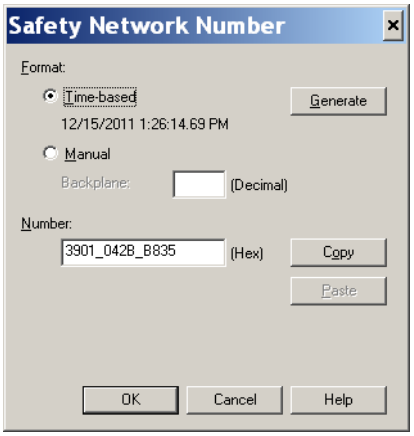
SUGERENCIA Se pueden asignar varios números de red de seguridad a una subred CIP Safety o a un chasis ControlBus que contenga más de un dispositivo de seguridad. **No obstante, para simplificar las cosas, recomendamos que cada subred CIP Safety tenga un solo SNN único.**

El SNN puede ser asignado por el software (basado en tiempo) o por el usuario (manual). Estos dos formatos de 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 generado representa la fecha y la hora en que se generó el número según la computadora personal en la que se ejecuta el software de configuración.

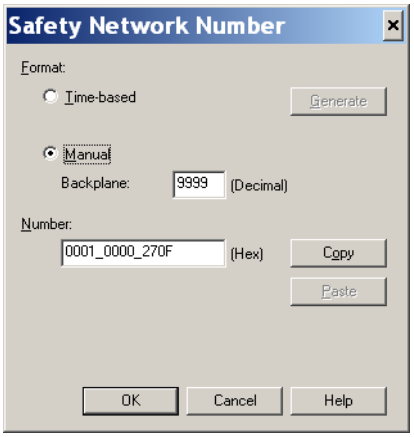
Figura 11 – Formato basado en tiempo



Número de red de seguridad manual

Si se selecciona el formato manual, el SNN es un número introducido, de 1...9999 decimal.

Figura 12 – Entrada manual



Asignación del número de red de seguridad (SNN)

Se puede permitir que el software RSLogix 5000 asigne automáticamente un SNN, o usted puede asignar el SNN manualmente.

Asignación automática

Cuando se crea un nuevo controlador o módulo, se le asigna automáticamente un SNN basado en tiempo mediante el software de configuración. A los módulos 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 caso de que los usuarios deseen administrar y asignar el SNN de manera lógica, de acuerdo a su aplicación específica.

Vea Cambio del número de red de seguridad (SNN) en la página 55.

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.

Automático vs. manual

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

- 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.

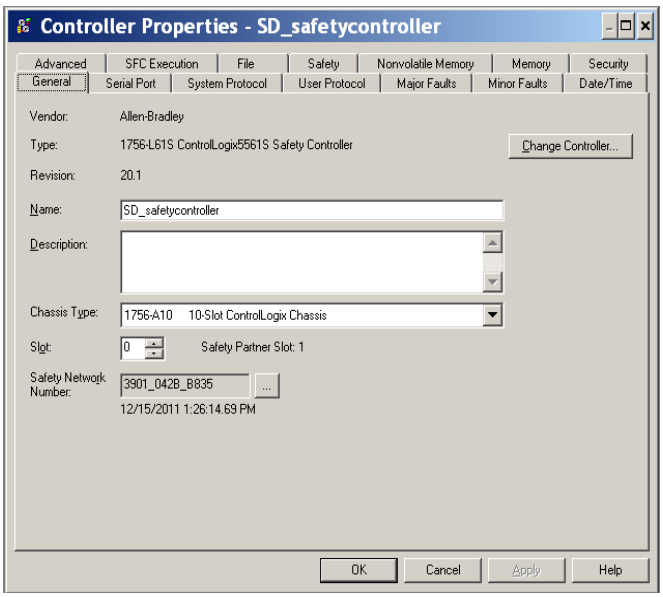
Cambio del número de red de seguridad (SNN)

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

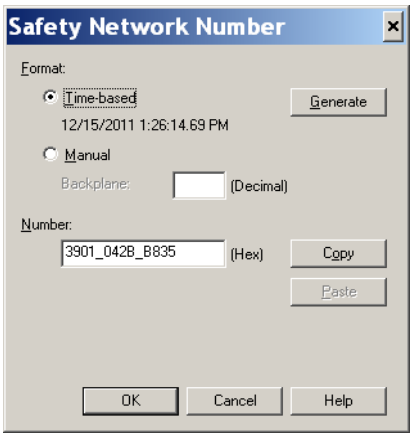
- Desbloquear el proyecto si está en bloqueo de seguridad;
  Vea Bloqueo de seguridad del controlador en la página 105.
- Eliminar la firma de tarea seguridad, si la hay.
  Vea Elimine la firma de tarea de seguridad en la página 108.

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 luego en Generate.



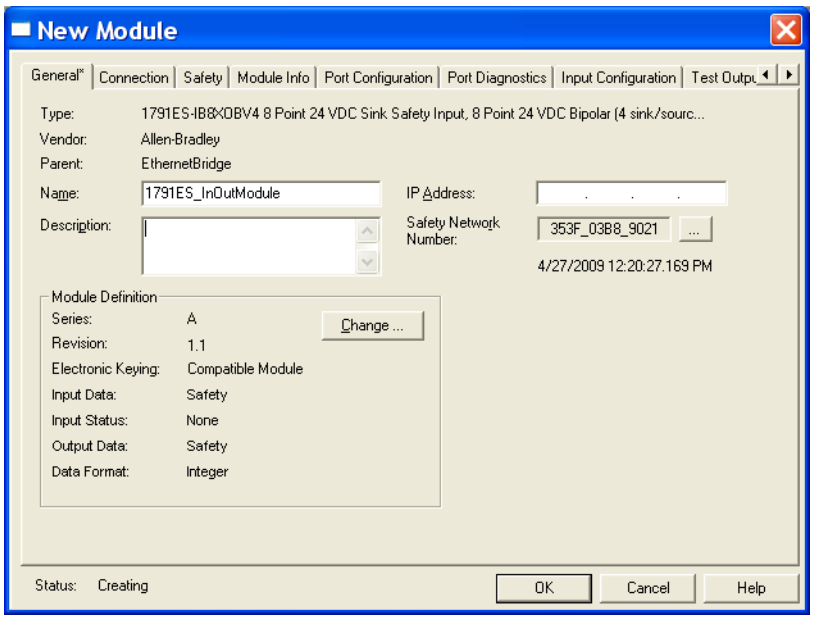
4. Haga clic en OK.

Cambio del número de red de seguridad (SNN) de módulos Safety I/O 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 módulos Safety I/O disponibles a través del módulo de comunicación EtherNet/IP.

3. Haga doble clic en el primer módulo Safety I/O para ver la ficha General.

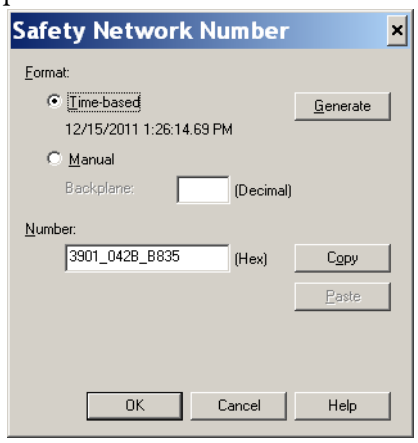


4. Haga clic en ... a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.
5. Seleccione Time-based y haga clic en Generate para generar un nuevo SNN para esa red EtherNet/IP.
6. Haga clic en OK.
7. Haga clic en Copy para copiar el nuevo SNN en el portapapeles de Windows.
8. Abra la ficha General del cuadro de diálogo Module Properties del siguiente módulo Safety I/O 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 módulos Safety I/O bajo ese módulo de comunicación EtherNet/IP.
13. Repita los pasos 2...10 para los módulos de comunicación de red restantes bajo el árbol I/O Configuration.

Copia y colocación de un número de red de seguridad (SNN)

Si la configuración del módulo está en posesión de otro controlador, es posible que deba copiar el SNN del propietario de la configuración y colocarlo en el árbol I/O Configuration.

1. En la herramienta de configuración del 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 módulo 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, incluyendo control de módulo Safety I/O, seleccione 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 lista los módulos y sus principales funciones.

Tabla 12 – Módulos y capacidades de comunicación EtherNet/IP

Módulo	Características
1756-ENBT	• Conectar controladores a módulo 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 demandantes. • 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 entornos extremos con temperaturas de –25…70 °C (–13…158 °F).
1756-EN2TR	• Realizar las mismas funciones que un módulo 1756-EN2T. • Aceptar comunicación en una topología de anillo para una red con topología de anillo tolerante a fallo único a nivel de dispositivo (DLR).
1756-EN3TR	• Realizar las mismas funciones que el módulo 1756-EN2TR. • Tres 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 RJ45, cable doble trenzado, sin blindaje, categoría 5
- Compatibilidad con operación half/full duplex, 10 M o 100 M
- Funcionamiento con interruptores estándar
- No requieren programación de red
- No requieren tablas de encaminamiento

Estos productos de software están disponibles para las redes EtherNet/IP.

Tabla 13 – Software para módulos EtherNet/IP

Software	Propósito	Requerido
Software de programación RSLogix 5000	Este software se requiere para configurar el proyecto del controlador y para definir la comunicación EtherNet/IP.	Sí
Utilidad BOOTP/DHCP	Esta utilidad viene con el software RSLogix 5000. Se puede usar esta utilidad para asignar direcciones IP a dispositivos en una red EtherNet/IP.	No
Software RsNetWorx™ para EtherNet/IP	Se puede usar este software para configurar dispositivos EtherNet/IP por direcciones IP y/o nombres de anfitriones.	No
Software RSLinx	Se puede usar este software para configurar dispositivos, establecer comunicación entre dispositivos y proporcionar diagnósticos.	Sí

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 mediante 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 se necesita.

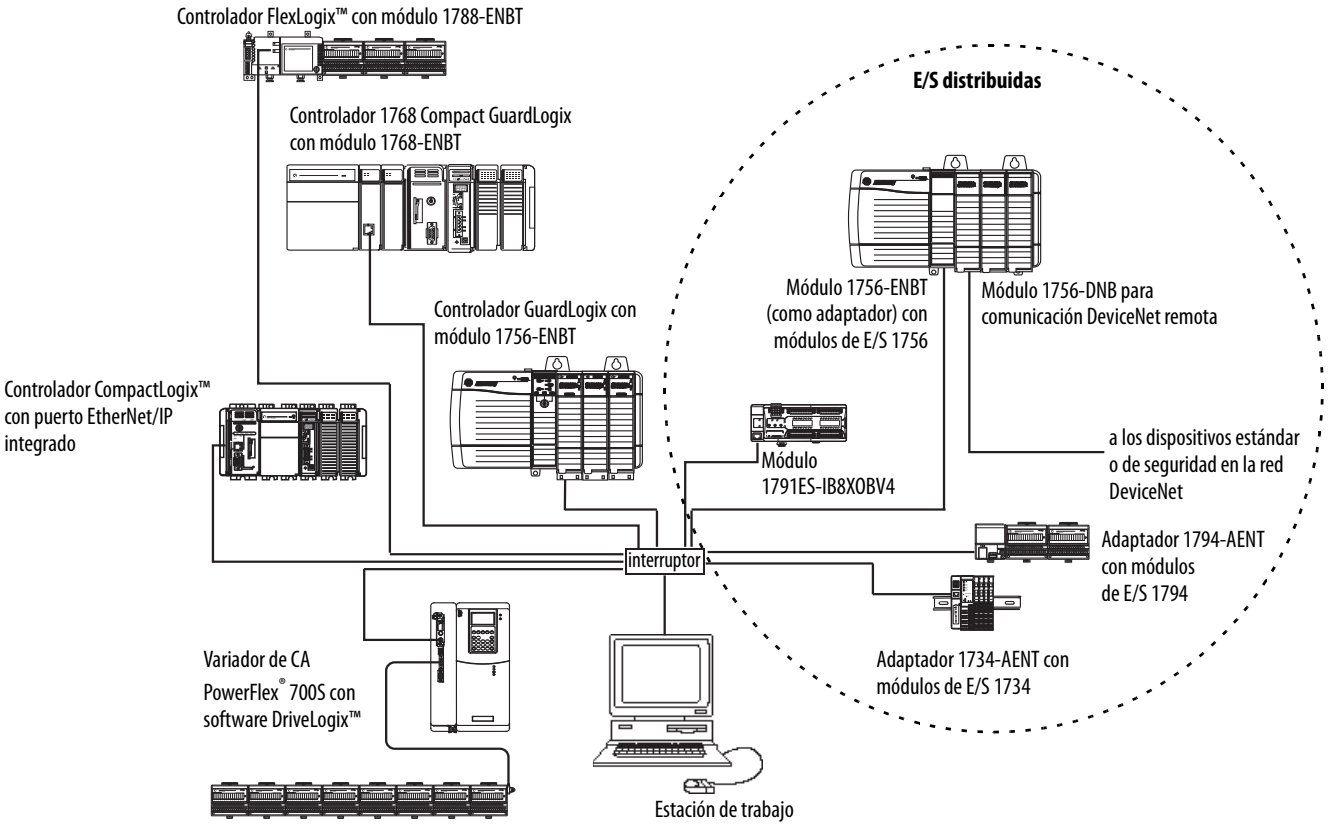
Los módulos de comunicación EtherNet/IP admiten 128 conexiones del protocolo industrial común (CIP) mediante una red EtherNet/IP.

Ejemplo de comunicación EtherNet/IP

Este ejemplo ilustra lo siguiente:

- 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 computadora personal puede cargar/descargar proyectos a los controladores;
- la computadora personal puede configurar dispositivos en la red EtherNet/IP.

Figura 13 – Ejemplo de comunicación EtherNet/IP

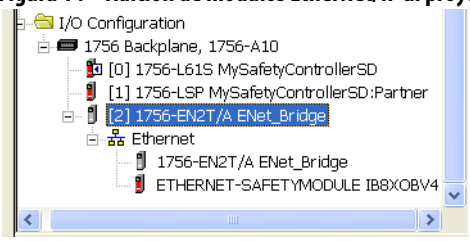


Conexiones EtherNet/IP para módulos CIP Safety I/O

Los módulos CIP Safety I/O en las redes EtherNet/IP se agregan al proyecto debajo del módulo de comunicación EtherNet/IP, como se describe en el Capítulo 5, Cómo añadir, configurar, monitorear y reemplazar CIP Safety I/O. Cuando se añade un módulo CIP Safety I/O, el software RSLogix 5000 crea automáticamente tags de datos de seguridad restringidos al controlador para ese módulo.

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

Figura 14 – Adición de módulos EtherNet/IP al proyecto



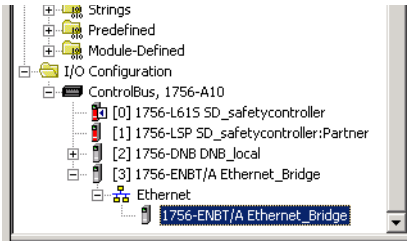
Conexiones EtherNet/IP estándar

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
IP Address	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
Subnet Mask	El direccionamiento de subred es una extensión del esquema de dirección IP que le permite a un sitio utilizar una sola 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 parte de identificación de red personalizada y una parte 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. Utilice el software RSLogix 5000 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 módulos de E/S estándar; • requiere un adaptador para E/S distribuidas en 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 entornos extremos con temperaturas de –25…70 °C (–13…158 °F)	1756-CN2RXT

Estos productos de software están disponibles para las redes ControlNet.

Tabla 15 – Software para módulos ControlNet

Software	Propósito	Requerido
Software de programación RSLogix 5000	Este software se requiere para configurar el proyecto GuardLogix y para definir la comunicación ControlNet.	Sí
Software RSNetWorx para ControlNet	Este software se necesita para configurar la red ControlNet, definir el tiempo de actualización de la red (NUT) y programar la red ControlNet.	Sí
Software RSLinx	Se puede usar este software para configurar dispositivos, establecer comunicación entre dispositivos y 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 es 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.

La conexiones ControlNet pueden ser programadas o sin programar.

Tabla 16 – Conexiones ControlNet

Tipo de conexión	Descripción
Programada (único para la red ControlNet)	Las conexiones programadas son únicas para la comunicación ControlNet. Las conexiones programadas le permiten enviar y recibir datos repetidamente a un intervalo predeterminado, el cual es el intervalo solicitado entre paquetes (RPI). Por ejemplo, una conexión a un módulo 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 RSNetWorx para el software ControlNet a fin de habilitar las conexiones programadas y establecer el tiempo de actualización (NUT). Al programar una conexión se reserva el ancho de banda de la red para administrar específicamente la conexión.
No programada	Las conexiones no programadas son transferencias de mensajes entre controladores activadas 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 se necesita. 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 configure no 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.

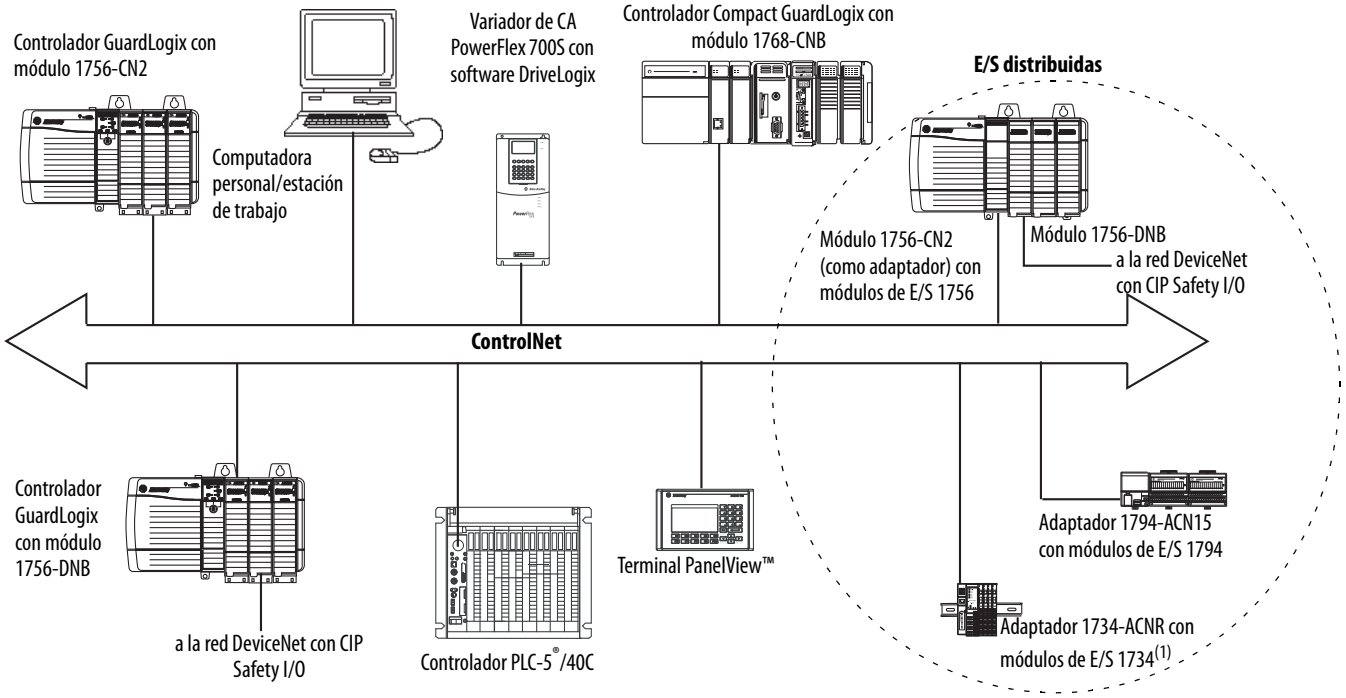
Ejemplo de comunicación ControlNet

Este ejemplo ilustra lo siguiente:

- los controladores GuardLogix pueden producir y consumir tags estándar o de seguridad entre sí;
- los controladores GuardLogix pueden iniciar instrucciones MSG que envían/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 15 – 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 módulos de E/S distribuidas a través de una red ControlNet, añada un puente ControlNet, un adaptador ControlNet y módulos de E/S a la carpeta I/O Configuration del controlador.

Comunicación DeviceNet

Para comunicarse e intercambiar datos con módulos CIP Safety I/O 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 de software se usan con las redes DeviceNet y el módulo 1756-DNB.

Tabla 17 – Software para uso con redes DeviceNet

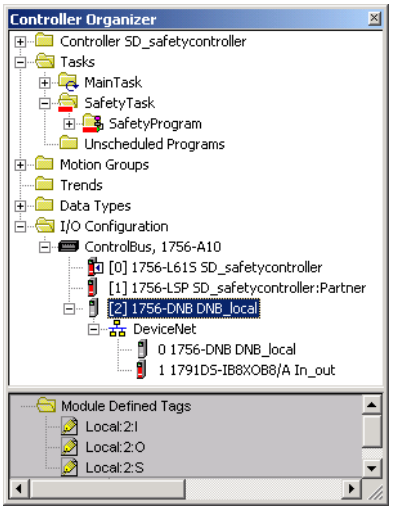
Software	Se usa para	Requerido/opcional
RSLogix 5000	• Configurar proyectos ControlLogix. • Definir la comunicación DeviceNet.	Requerido
RSNetWorx™ para DeviceNet	• Configurar dispositivos DeviceNet • Definir la lista de escán para esos dispositivos	
RSLinx Classic o RSLinx Enterprise	• Configurar dispositivos de comunicación • Proporcionar diagnósticos • Establecer comunicación entre dispositivos	

Conexiones DeviceNet para módulos CIP Safety I/O

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

Los módulos CIP Safety I/O en las redes DeviceNet se agregan al proyecto debajo del módulo 1756-DNB, como se describe en el Capítulo 5, Cómo añadir, configurar, monitorear y reemplazar CIP Safety I/O. Cuando se añade un módulo CIP Safety I/O, el software RSLogix 5000 crea automáticamente tags de datos de seguridad restringidos al controlador para ese módulo.

Figura 16 – Módulo DeviceNet en el controlador en el árbol de configuración de E/S



Conexiones DeviceNet estándar

Si utiliza E/S DeviceNet estándar con su controlador GuardLogix, tiene que reservar 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, el software RSLogix 5000 crea automáticamente un conjunto de tags estándar para los datos de entrada, salida y estado de la red.

Comunicaciones en serie

Para utilizar el controlador GuardLogix en una red en serie, se necesita lo siguiente:

- Una estación de trabajo con un puerto en serie
- El software RSLinx para configurar el driver de comunicación en serie
- El software RSLogix 5000 para configurar el puerto serial del controlador

Para que el controlador se pueda comunicar con una estación de trabajo o con otro dispositivo a través de la red en serie, debe seguir estos pasos.

1. Configurar el driver de comunicaciones serie para la estación de trabajo.
2. Configurar el puerto serial del controlador.

Tabla 18 – Modos de comunicaciones en serie

Utilice este modo	Si desea
DF1 punto a punto	Comunicación entre el controlador y otro dispositivo compatible con el protocolo DF1. Este es el modo predeterminado del sistema. Este modo suele utilizarse para programar el controlador a través de su puerto en serie.
DF1 maestro	Controlar la interrogación secuencial y la transmisión de mensajes entre los nodos maestros y esclavos. La red de maestros/esclavos incluye un controlador configurado como nodo maestro y un máximo de 254 nodos esclavos. Los nodos esclavos se vinculan mediante módems o drivers en línea. Una red de maestros/esclavos puede tener números de nodo de 0…254. Cada uno de los nodos debe tener una dirección de nodo única. Además, debe haber como mínimo 2 nodos para definir el vínculo como red (los dos nodos son 1 estación maestra y 1 estación esclava).
DF1 esclavo	Un controlador que funciona como estación esclava en una red de comunicaciones en serie maestro/esclavo. Cuando haya múltiples estaciones esclavas en la red, vincule las estaciones esclavas a la estación maestra usando módems o drivers en línea. Si solo tiene una estación esclava en la red, no necesita un módem para conectar la estación esclava a la maestra. Puede configurar los parámetros de control para que no haya handshaking. Se pueden conectar 2…255 nodos a un vínculo. En el modo DF1 esclavo, un controlador utiliza el protocolo DF1 Half-duplex. Un nodo se designa como maestro y controla el acceso al vínculo. Todos los demás nodos serán estaciones esclavas y deben esperar a que el nodo maestro les conceda permiso antes de transmitir datos.
DH-485	Comunicación con otra red de paso de testigo de múltiples maestros de dispositivos DH-485, que permita programación y transmisión de mensajes entre homólogos.

Recursos adicionales

Recurso	Descripción
EtherNet/IP Modules in Logix5000 Control Systems User Manual, publicación ENET-UM001	Contiene información detallada sobre cómo configurar y usar los módulos de comunicación EtherNet/IP en un sistema de control Logix5000
ControlNet Modules in Logix5000 Control Systems User Manual, publicación CNET-UM001	Contiene información detallada sobre cómo configurar y usar los módulos de comunicación ControlNet en un sistema de control Logix5000
DeviceNet Modules in Logix5000 Control Systems User Manual, publicación DNET-UM004	Contiene información detallada sobre cómo configurar y usar el módulo 1756-DNB en un sistema de control Logix5000.

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

Para obtener más información sobre la instalación, la configuración y la operación de los módulos de CIP Safety I/O, consulte las siguientes recursos:

- Guard I/O DeviceNet Safety Modules User Manual, publicación 1791DS-UM001
- Guard I/O EtherNet/IP Safety Modules User Manual, publicación 1791ES-UM001
- POINT Guard I/O™ Safety Modules Installation and User Manual, publicación 1734-UM013
- Ayuda en línea del software RSLogix 5000

Adición de módulos CIP Safety I/O

Cuando se añade un módulo 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 módulo CIP Safety I/O no se puede establecer en redes DeviceNet mediante el software RSLogix 5000. Las direcciones de nodo de los módulos se establecen mediante los conmutadores giratorios de los módulos.

- Dirección IP para redes EtherNet/IP

  Para establecer la dirección IP, usted puede ajustar los interruptores giratorios del módulo, usar el software DHCP disponible a través de Rockwell Automation, o recuperar la dirección predeterminada de la memoria no volátil.

- Número de red de seguridad (SNN)

  Vea la página 71 para obtener información sobre cómo establecer el SNN.

- Firma de configuración

  Consulte la página 75 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 71 para obtener información sobre cómo establecer el límite del tiempo de reacción.

- Entrada de seguridad, salida y parámetros de prueba

Puede configurar los módulos CIP Safety I/O a través del controlador GuardLogix usando el software RSLogix 5000.

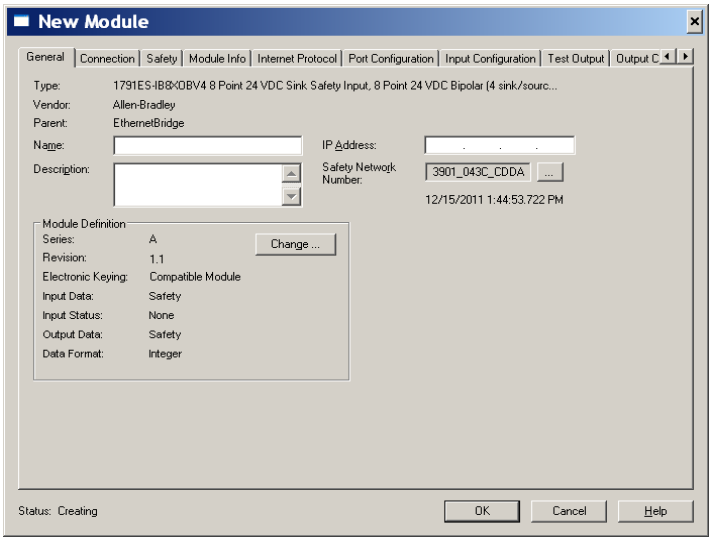
SUGERENCIA Los módulos Safety I/O admiten datos estándar y de seguridad. La configuración del módulo define los datos que están disponibles.

Configuración de módulos CIP Safety I/O mediante el software RSLogix 5000

Añada el módulo CIP Safety I/O al módulo de comunicación bajo la carpeta I/O Configuration del proyecto RSLogix 5000.

SUGERENCIA No se puede añadir ni eliminar un módulo CIP Safety I/O mientras se está en línea.

1. Haga clic con el botón derecho del mouse en la red apropiada y seleccione New Module.
2. Expanda la categoría Safety y seleccione un módulo CIP Safety I/O.
3. Especifique las propiedades del módulo.



   a. Modifique los ajustes de definición del módulo en caso necesario; para ello, haga clic en el botón Change.
   b. Escriba un nombre para el nuevo módulo.
   c. Introduzca la dirección de nodo o la dirección IP del módulo en su red de conexión.

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

d. Modifique el número de red de seguridad (SNN) en caso necesario; para ello, haga clic en el botón ....

   Consulte la página 71 para obtener más información.

e. Establezca los parámetros de configuración del módulo en las fichas Input Configuration, Test Output y Output Configuration.

   Consulte la ayuda en línea de RSLogix 5000 para obtener más información acerca de la configuración del módulo CIP Safety I/O.

f. Establezca el límite de tiempo de reacción de la conexión en la ficha Safety.

   Consulte la página 71 para obtener más información.

Cómo establecer el número de red de seguridad (SNN)

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

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

Vea Asignación del número de red de seguridad (SNN) en la página 55.

Uso de conexiones unidifusión en las redes EtherNet/IP

En el software RSLogix 5000, versión 20 o posterior, usted puede configurar módulos de E/S EtherNet/IP para usar conexiones unidifusión. Las conexiones 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 unidifusión, seleccione la ficha Connection y seleccione Use Unicast Connection over Ethernet/IP.

Establecimiento del límite de tiempo de reacción de la conexión

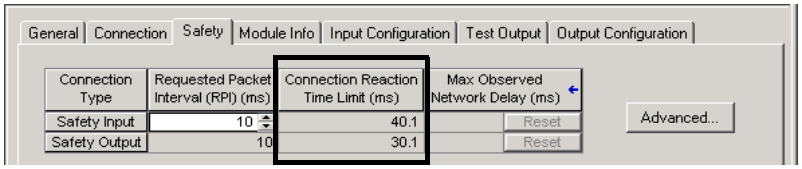
El límite de tiempo de reacción de la conexión corresponde a la longevidad máxima de los paquetes de seguridad en la conexión asociada. Si la longevidad de los datos utilizados por el dispositivo consumidor supera el límite de tiempo de reacción de la conexión, se produce un fallo de conexión. El límite 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 17 – Límite de tiempo de reacción de la conexión



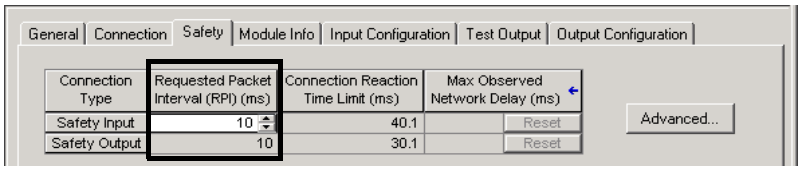
Especifique el intervalo solicitado entre paquetes (RPI)

El RPI especifica el período durante el cual 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 el software RSLogix 5000.

Figura 18 – 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 90 para obtener más información acerca del período de la tarea de seguridad.

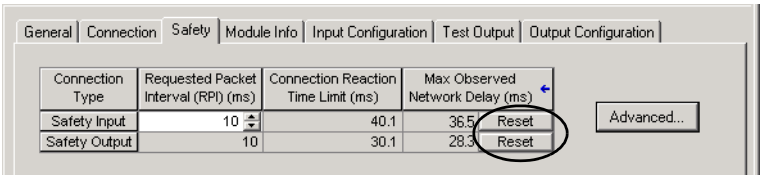
Para aplicaciones típicas, generalmente es suficiente el intervalo solicitado entre paquetes predeterminado. Para requisitos más complejos, utilice el botón Advanced para modificar los parámetros del límite de tiempo de reacción de la conexión tal y como se describe en la página 73.

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, puede restablecer el retardo de red máximo observado; para ello, haga clic en Reset.

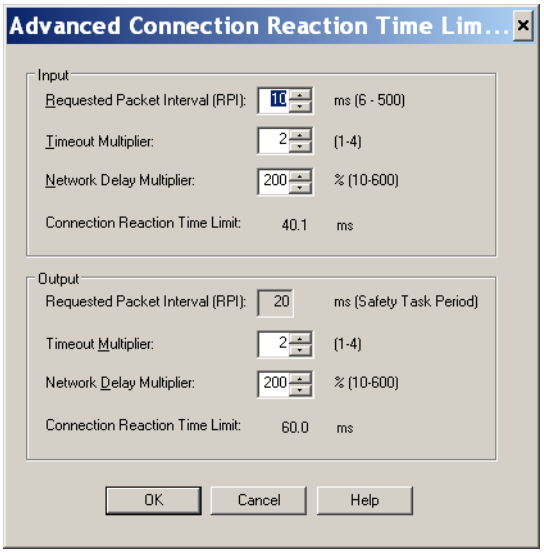
Figura 19 – Restablecimiento del retardo de red máximo observado



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

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

Figura 20 – Configuración avanzada



Multiplicador de interrupciones

El valor de Timeout Multiplier determina el número de RPI que se debe esperar por un paquete hasta declarar terminado 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 RPI (2 x RPI).

Multiplicador de retardo de red

El valor de Network Delay Multiplier 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 el recorrido inverso de confirmación. 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 den 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 ejecuta 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 en ejecución 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 19 – Recursos adicionales

Recurso	Descripción
GuardLogix Controllers Systems Safety Reference Manual, publicación 1756-RM093	Proporciona información acerca del cálculo de los tiempos de reacción.
Guard I/O DeviceNet Safety Modules User Manual, publicación 1791DS-UM001	
Guard I/O EtherNet/IP Safety Modules User Manual, publicación 1791ES-UM001	

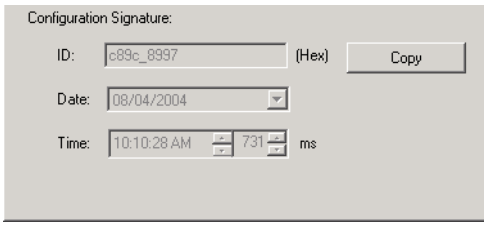
Explicación de la firma de configuración

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 el software RSLogix 5000

Si el módulo de E/S se configura mediante el software RSLogix 5000, 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 21 – Vea y copia la firma de configuración



Propietario de configuración diferente (conexión de solo recepción)

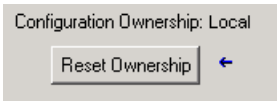
Cuando la configuración del módulo de E/S está en posesión de otro controlador, usted debe copiar la firma de configuración del módulo del proyecto de su propietario y pegarla en la ficha Safety del cuadro de diálogo Module Properties.

SUGERENCIA Si el módulo está configurado solamente para entradas, usted puede copiar y pegar la firma de configuración. Si el módulo 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 módulo Safety I/O

Si el software RSLogix 5000 está en línea, la ficha Safety del cuadro de diálogo Module Properties muestra la posesión actual de la configuración. Si el proyecto abierto posee 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 módulo.

Cuando se trabaja en línea, se puede restablecer el módulo a la configuración que tenía al sacarlo de la caja; para ello, haga clic en Reset Ownership.



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 Safety I/O

Cuando se añade un módulo a la carpeta de configuración de E/S, el software RSLogix 5000 crea automáticamente tags restringidos al controlador para el módulo.

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 módulo de E/S. El nombre del tag se basa en el nombre del módulo en el sistema.

La dirección de dispositivo CIP Safety I/O tiene este formato:

Modulename:Type.Member

Tabla 20 – Formato de dirección de módulo CIP Safety I/O

Donde	Es	
Modulename	El nombre del módulo CIP Safety I/O	
Tipo	Tipo de datos	
	Entrada: I	
	Salida: O	
Member	Datos específicos del módulo 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

Tabla 21 – Recursos adicionales

Recurso	Descripción
Capítulo 9, Monitoreo de estado y manejo de fallos	Contiene información acerca del monitoreo de datos de tags de seguridad
Logix5000 Controllers I/O and Tag Data Programming Manual, publicación 1756-PM004	Proporciona información sobre cómo direccionar módulos de E/S estándar

Monitoreo del estado del módulo Safety I/O

Puede monitorear el estado del módulo Safety I/O mediante los mensajes explícitos o mediante los indicadores de estado de los módulos de E/S.

Las siguientes publicaciones contienen información sobre la resolución de problemas del módulo de E/S:

- Guard I/O DeviceNet Safety Modules User Manual, publicación 1791DS-UM001
- Guard I/O EtherNet/IP Modules User Manual, publicación 1791ES-UM001
- POINT Guard I/O Safety Modules Installation and User Manual, publicación 1734-UM013

Tabla 22 – Operación del indicador de estado

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	Funcionamiento en condiciones normales		
	Verde parpadeante	El dispositivo está inactivo.		
	Rojo parpadeante	Hay un fallo recuperable.	Está presente un fallo recuperable, o una actualización de firmware está en curso.	
	Rojo fijo	Hay un fallo irrecuperable.		
	Rojo/verde parpadeante	Autopruebas en curso	Hay autopruebas en curso o el módulo no está correctamente 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	Se sobrepasó el tiempo de espera de comunicación.	Se sobrepasó el tiempo de espera de comunicación o una actualización de firmware está en curso.	
	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 aplicable
Puntos de entrada (INx)	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 (Ox)	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 (Tx)	Apagado	No aplicable	La salida está desactivada.	No aplicable
	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.	El software RSLogix 5000 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 el dispositivo se configuró para el software RSLogix 5000.		
IN PWR	Verde apagado	No hay alimentación eléctrica de entrada.		No aplicable
	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 aplicable		Sin alimentación eléctrica
	Verde fijo			El voltaje de alimentación está dentro de especificaciones.
	Amarillo fijo			El voltaje de alimentación está fuera de especificaciones.

Restablecimiento de un módulo a la condición original

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

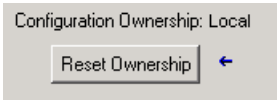
Si el software RSLogix 5000 está en línea, la ficha Safety del cuadro de diálogo Module Properties muestra la posesión actual de la configuración. Si el proyecto abierto posee la configuración, se visualiza Local. Si la configuración está en posesión de otro dispositivo, aparece Remote junto al número 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 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. Seleccione Inhibit Connection.
4. Haga clic en Apply y luego 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.



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.

Cómo reemplazar un módulo mediante el software RSLogix 5000

Puede usar el software RSLogix 5000 para reemplazar un módulo Guard I/O en una red Ethernet. Para reemplazar un módulo Guard I/O en una red DeviceNet, su selección de software depende del tipo del módulo.

Tabla 23 – Software

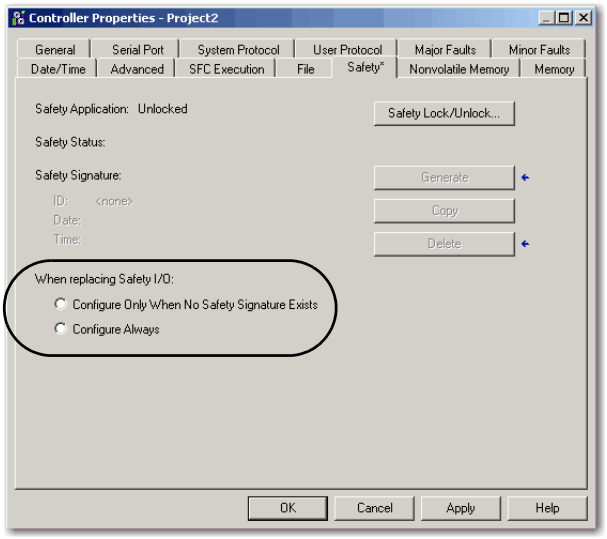
Si está usando un	Use	Consulte
Módulo 1791DS Guard I/O con un adaptador 1756-DNB	software RSLogix 5000	a continuación
Módulo 1734 POINT Guard I/O con un adaptador 1734-PDN	Software RSNetWorx para DeviceNet	Reemplazo de un módulo POINT Guard I/O usando el software RSNetWorx para DeviceNet en la página 86

Si está confiando en una porción del sistema CIP Safety para mantener el comportamiento SIL 3 durante el reemplazo del módulo y las pruebas funcionales, no puede usar la función Configure Always. Vaya a Remplazo con 'Configure Only When No Safety Signature Exists' habilitado en la página 80.

Puede utilizar la función Configure Always si no se ha confiado a todo el sistema de control CIP Safety enrutable el mantenimiento del SIL 3/PLe durante el reemplazo y la prueba de funcionamiento de un módulo. Vaya a Reemplazo con 'Configure Always' habilitado en la página 84.

El reemplazo de módulo se configura en la ficha Safety del controlador GuardLogix.

Figura 22 – Reemplazo del módulo Safety I/O



Remplazo con 'Configure Only When No Safety Signature Exists' habilitado

Cuando se reemplaza un módulo, la configuración se descargará desde el controlador de seguridad si el DeviceID del nuevo módulo 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.

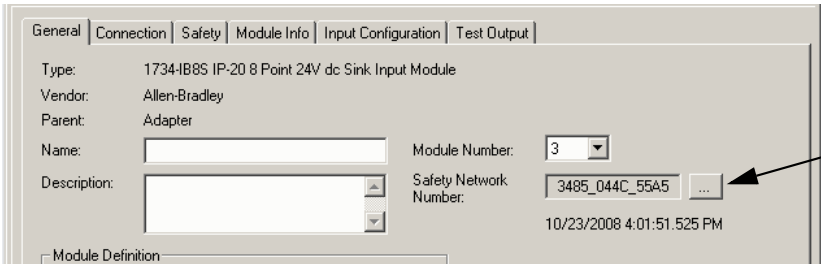
Si el proyecto se configura con la opción 'Configure Only When No Safety Signature Exists', siga los pasos apropiados indicados en la Tabla 24 para reemplazar un módulo POINT Guard I/O basado en su escenario. Una vez que haya realizado los pasos correctamente, el DeviceID coincidirá con en el original, habilitando al controlador de seguridad para descargar la configuración de módulo apropiada y restablecer la conexión de seguridad.

Tabla 24 – Cómo reemplazar un módulo

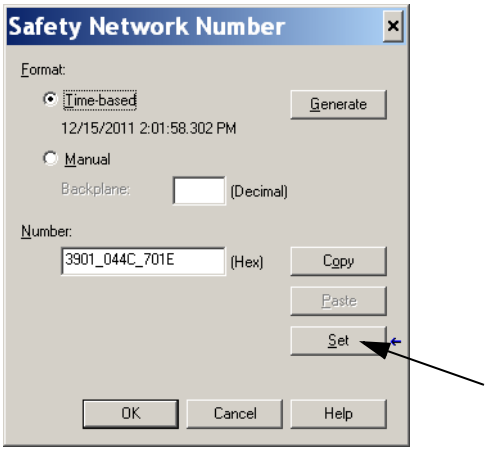
Existe la firma de seguridad GuardLogix	Condición del módulo de repuesto	Acción requerida
No	Sin SNN (condición original)	Ninguna. El módulo está listo para uso.
Sí o No	El mismo SNN que el de la configuración de tarea de seguridad original	Ninguna. El módulo está listo para uso.
Sí	Sin SNN (condición original)	Vea Escenario 1 – El módulo de repuesto está en su condición original y existe la firma de seguridad en la página 81.
Sí	SNN diferente al de la configuración de tarea de seguridad original	Vea Escenario 2 – El SNN del módulo de repuesto es diferente al del original y existe la firma de seguridad en la página 82.
No		Vea Escenario 3 – El SNN del módulo de repuesto es diferente al del original y no existe la firma de seguridad en la página 84.

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

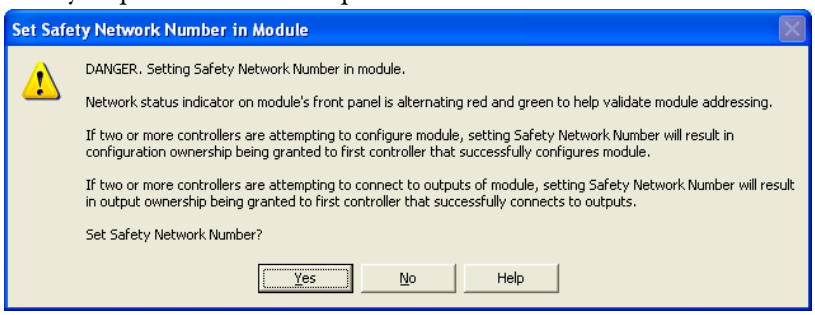
1. Retire el módulo de E/S antiguo e instale el nuevo.
2. Haga clic con el botón derecho del mouse en el módulo POINT Guard I/O de repuesto y seleccione Properties.
3. Haga clic en ... a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.



4. Haga clic en Set.



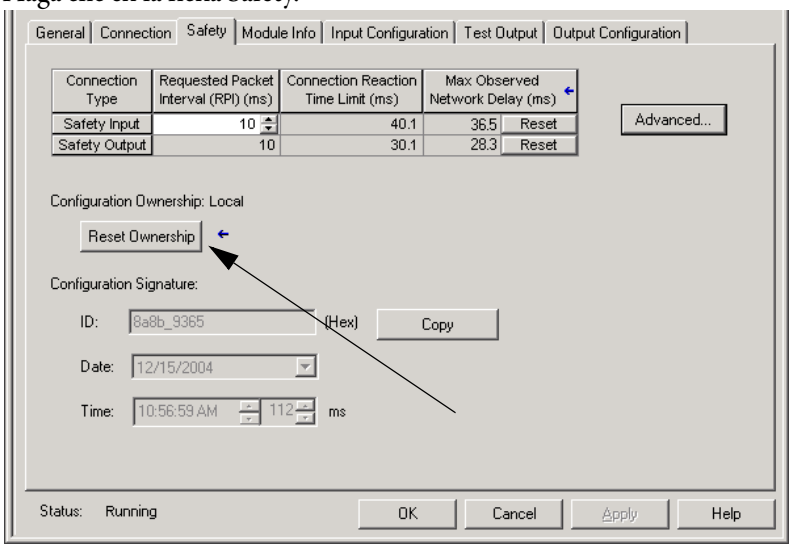
5. Compruebe que el indicador de estado de red (NS) se ilumine alternadamente de colores rojo a verde en el módulo correcto antes de hacer clic en Yes en el cuadro de diálogo de confirmación, para establecer el SNN y aceptar el módulo de repuesto.



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

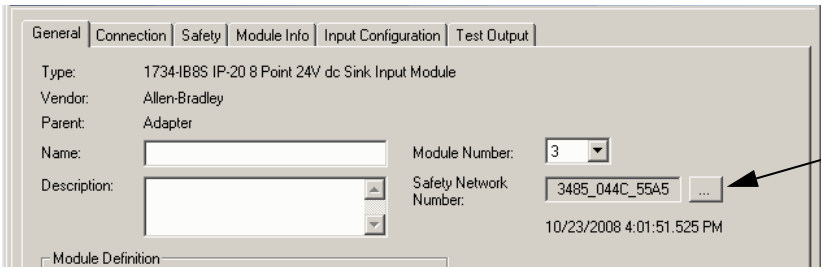
Escenario 2 – El SNN del módulo de repuesto es diferente al del original y existe la firma de seguridad

1. Retire el módulo de E/S antiguo e instale el nuevo.
2. Haga clic con el botón derecho del mouse en su módulo POINT Guard I/O y seleccione Properties.
3. Haga clic en la ficha Safety.

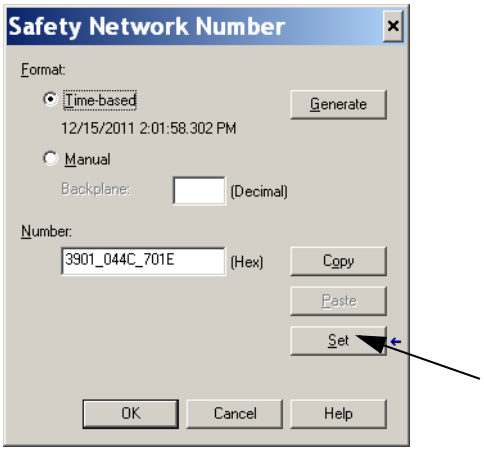


4. Haga clic en Reset Ownership.
5. Haga clic en OK.
6. Haga clic con el botón derecho del mouse en su controlador y seleccione Properties.

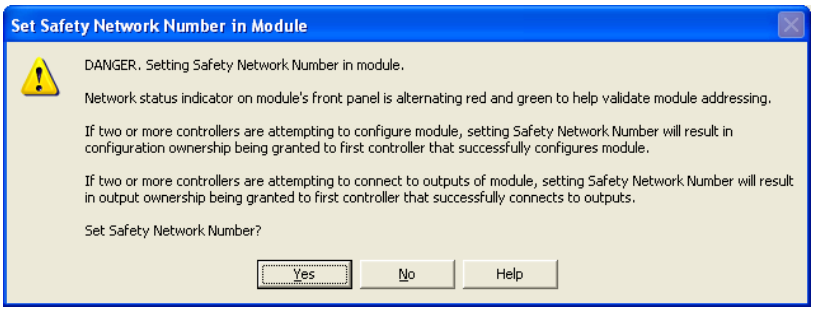
7. Haga clic en ... a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.



8. Haga clic en Set.



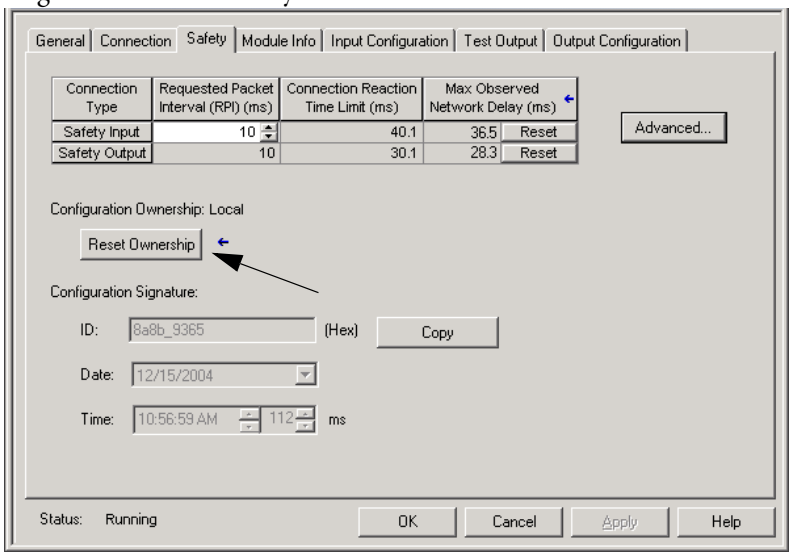
9. Compruebe que el indicador de estado de red (NS) se ilumine alternadamente de colores rojo a verde en el módulo correcto antes de hacer clic en Yes en el cuadro de diálogo de confirmación, para establecer el SNN y aceptar el módulo de repuesto.



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

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

1. Retire el módulo de E/S antiguo e instale el nuevo.
2. Haga clic con el botón derecho del mouse en su módulo POINT Guard I/O 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 en su empresa para realizar la prueba de funcionamiento del módulo de E/S reemplazado y del sistema, y para 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 la prueba funcional de un módulo.

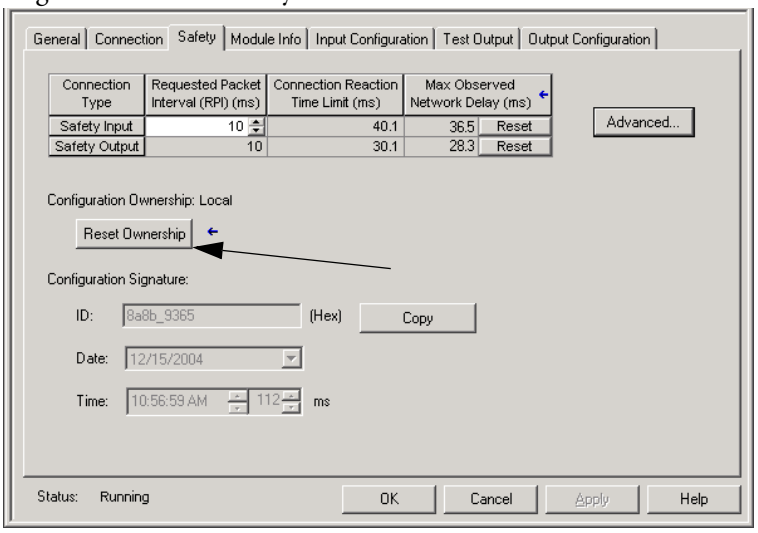
No ponga módulos en su condición original en una red CIP Safety si la función Configure Always está habilitada, excepto mientras está siguiendo este procedimiento de reemplazo.

Si la función 'Configure Always' está habilitada en el software RSLogix 5000, el controlador automáticamente verifica y se conecta a un módulo de reemplazo que cumple con todos los requisitos siguientes:

- El controlador tiene datos de configuración para un módulo compatible en esa dirección de red.
- El módulo 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 módulo POINT Guard I/O.

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



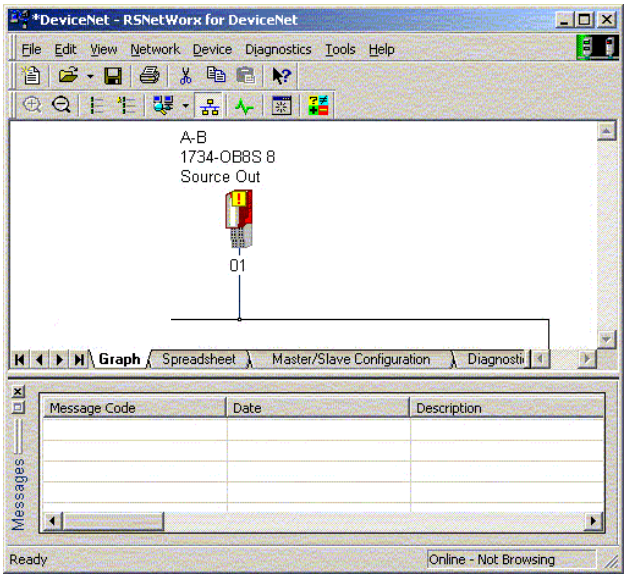
4. Haga clic en Reset Ownership.
5. Haga clic en OK.
6. Siga los procedimientos establecidos en su empresa para realizar la prueba de funcionamiento del módulo de E/S reemplazado y del sistema, y para autorizar el uso del sistema.

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

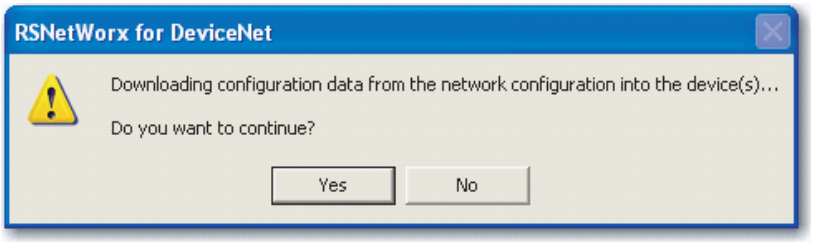
Siga estos pasos para reemplazar un módulo POINT Guard I/O cuando el módulo y el controlador están en una red DeviceNet.

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

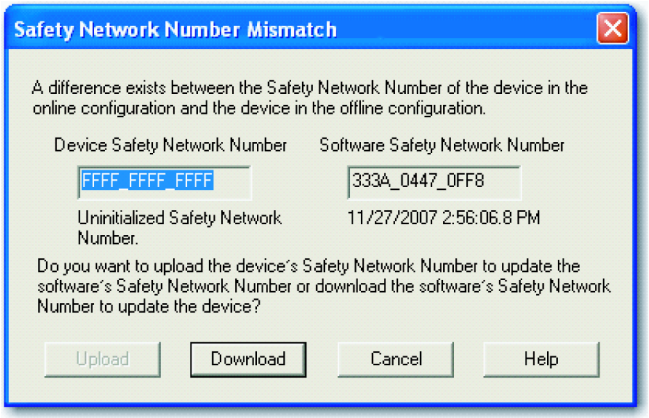
   Si el módulo de repuesto está en su condición original o tiene un SNN que no coincide con el del módulo original, el módulo aparecerá con un signo de exclamación.



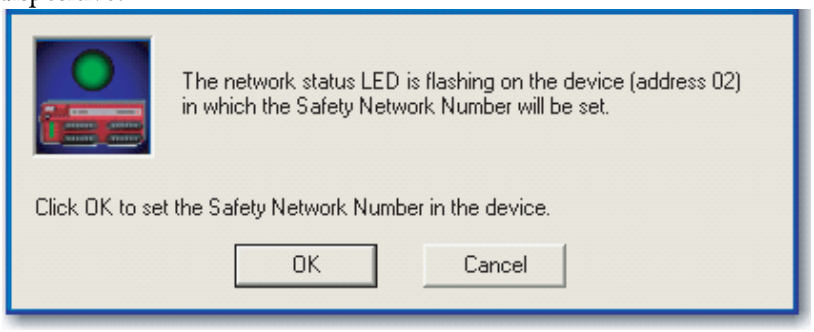
3. Haga clic con el botón derecho del mouse en el módulo y seleccione Download to Device.



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.

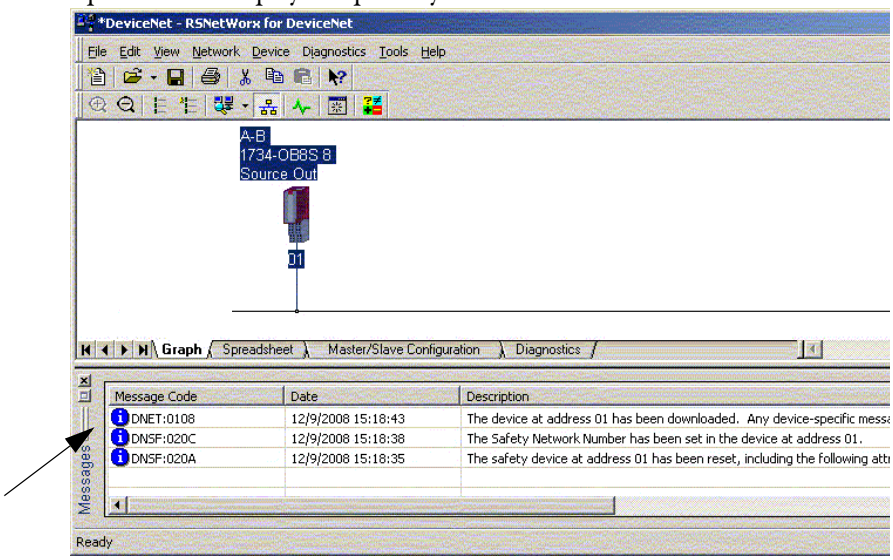


6. Verifique que el indicador LED de estado de la red (NS) esté parpadeando en el módulo correcto y haga clic en OK para establecer el SNN en dicho dispositivo.



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

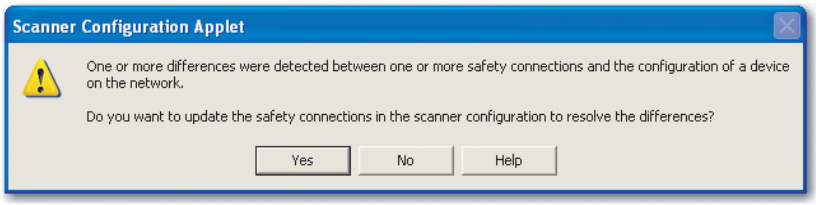
Una vez que la descarga se realice exitosamente, la vista del proyecto principal muestra este mensaje: 'The device at address *xx* has been downloaded. Any device-specific messages related to the download operation are displayed separately.'



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 marcha para descargar al módulo de repuesto.

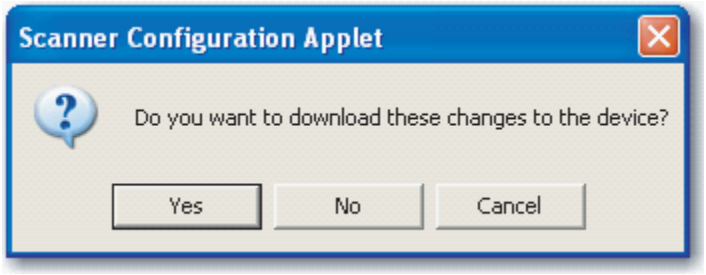
Si descarga esta configuración a una configuración temporal, coloque el módulo en la red y este se conecta automáticamente al controlador.

Si la configuración descargada al módulo no fuera la del archivo DNT original, la firma de configuración no coincidirá con la del original. Aun 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 cual no se hace 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, primero debe revalidar 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 SmartGuard.

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

9. Siga los procedimientos establecidos en 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, la firma de la 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 GuardLogix Controller Systems Safety Reference Manual, publicación 1756-RM093.

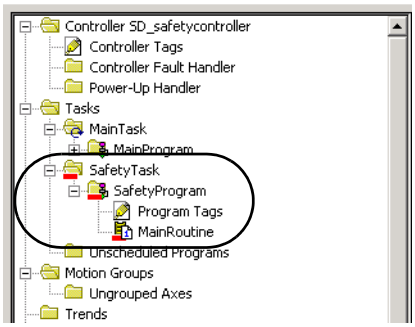
En el manual de referencia de seguridad se tratan los temas siguientes:

- Creación de una especificación detallada del proyecto
- Escritura, documentación y pruebas de la aplicación
- Generación de la firma de la 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

Tarea de seguridad

Cuando se crea un proyecto de controlador de seguridad, el software RSLogix 5000 crea automáticamente una tarea de seguridad con un programa de seguridad y una rutina (de seguridad) principal.

Figura 23 – Tarea de seguridad en el organizador del controlador



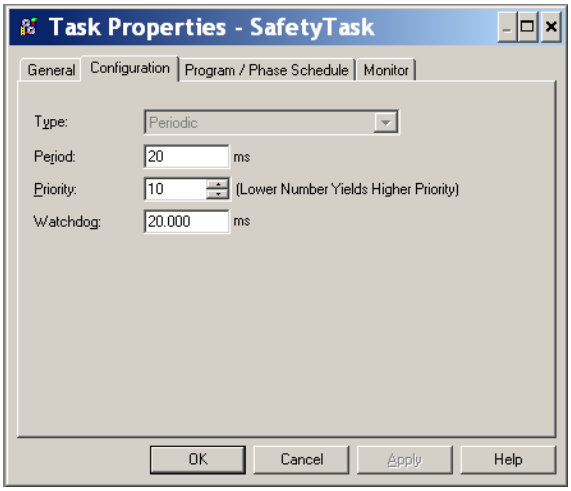
Dentro de la tarea de seguridad se pueden usar varios programas de seguridad, compuestos a su vez por varias rutinas de seguridad. El controlador GuardLogix acepta una tarea de seguridad. La tarea de seguridad no se puede eliminar.

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 selecciona la prioridad de la tarea y el tiempo del temporizador de control (watchdog) 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 a continuación seleccione Properties.

Figura 24 – Configuración del período de la tarea de seguridad



La tarea de seguridad debe tener alta prioridad. Especifique el período de la tarea de seguridad (en ms) y el temporizador de vigilancia 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 termina.

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 disparar. 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, publicación 1756-RM093, 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 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 102 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

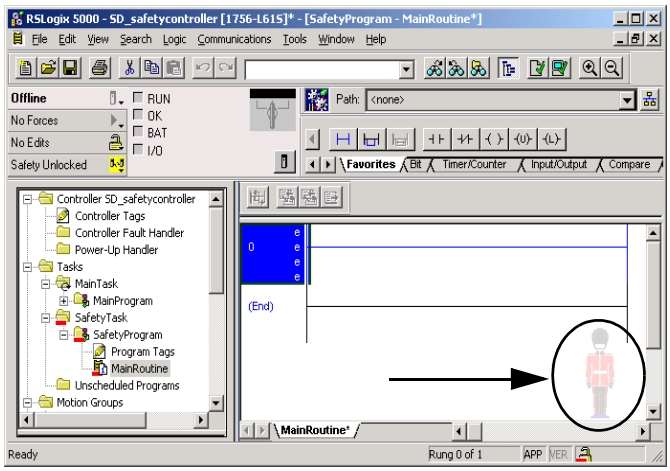
Los programas de seguridad tienen todos los atributos de los programas estándar, salvo que solo se pueden programar en una tarea de seguridad y solo pueden contener componentes de seguridad. Los programas de seguridad solo pueden contener rutinas de seguridad, una de las cuales debe definirse como la rutina principal; también se puede definir otra rutina 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 como parte de un programa de seguridad. Actualmente, sólo el diagrama de lógica de escalera es compatible con las rutinas de seguridad.

SUGERENCIA El software RSLogix 5000 utiliza una imagen semitransparente para diferenciar 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 y además mecanismos certificados para proporcionar el nivel de integridad de datos SIL 3.

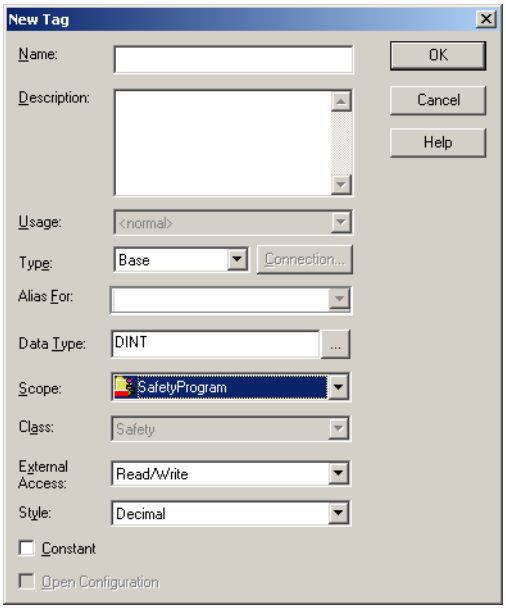
Al crear un tag, usted asigna las siguientes propiedades.

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

También puede especificar si un valor de tag debe ser 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 seleccione New Tag.

Figura 25 – Cómo crear un nuevo tag



Tipo de tag

La Tabla 25 define los cuatro tipos de tags: base, alias, producido y consumido.

Tabla 25 – Cuatro tipos de tags

Tipo de tag	Descripción
Base	Estos tags almacenan valores utilizados por la lógica dentro del proyecto.
Alias	Tag que hace referencia a otro tag. Un tag de alias puede hacer referencia a otro tag alias o a un tag base. Un tag 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:** En las aplicaciones de seguridad está prohibido establecer relaciones de alias entre tags estándar y tags de seguridad. En lugar de ello, los tags estándar pueden asignarse a tags de seguridad mediante la función de asignación a tags de seguridad. Vea Asignación de un tag de seguridad en la página 102.
Producidos	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 ninguna lógica. Los datos de tag producido se envían al RPI del tag consumidor.
Consumidos	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 al que se actualizan los datos.

Tipo de datos

El tipo de datos define el tipo de datos que el tag almacena, como bit, número entero, valor con punto flotante (coma flotante) o cadena.

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.

Solo 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	PHASE
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

Los tipos de datos REAL son válidos en proyectos del controlador 1756-L7xS, pero no son válidos en proyectos de los controladores 1756-L6xS o 1768-L4xS.

IMPORTANTE Esta restricción incluye los tipos de datos definidos por el usuario que contengan tipos de datos predefinidos.

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 ser restringidos al controlador o restringidos al programa de seguridad.

Tags bajo el control del controlador

Cuando los tags de seguridad son restringidos al controlador, todos los programas pueden tener acceso a los datos de seguridad. Los tags deben ser restringidos al controlador si se usan en los siguientes:

- En más de un programa del proyecto
- Para producir o consumir datos
- Para comunicarse con un terminal PanelView/HMI
- En la asignación de un tag de seguridad
  Consulte la sección Asignación de un tag de seguridad en la página 102 para obtener más información.

Los tags de seguridad restringidos al controlador pueden ser leídos pero no escritos por rutinas estándar.

IMPORTANTE	Los tags de seguridad restringidos al 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 Safety I/O y a datos de seguridad producidos o consumidos deben ser tags de seguridad restringidos al 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 del 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 127	Proporciona más información acerca del miembro CONNECTION_STATUS.
Logix5000 Controllers I/O and Tag Data Programming Manual, publicación 1756-PM004	Proporciona instrucciones para crear tipos de datos definidos por el usuario.

Tags restringidos al programa

Cuando los tags son restringidos al programa, los datos se aíslan de los otros programas. Los nombres de tags restringidos al programa se pueden volver a utilizar en otros programas.

Los tags de seguridad restringidos al programa de seguridad solo pueden ser leídos o escritos mediante una rutina de seguridad restringida en el 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 restringidos al 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 restringidos al controlador, debe seleccionarse manualmente la clase de tag.

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.

El software RSLogix 5000 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 el software RSLogix 5000 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 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 unidifusión en la versión 19 y posteriores del software RSLogix 5000.

Tabla 29 – Conexiones de tags producidos y consumidos

Tag	Descripción de la conexión
Producidos	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.
Consumidos	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.

Configure los números de redes de seguridad de los controladores de seguridad homólogos

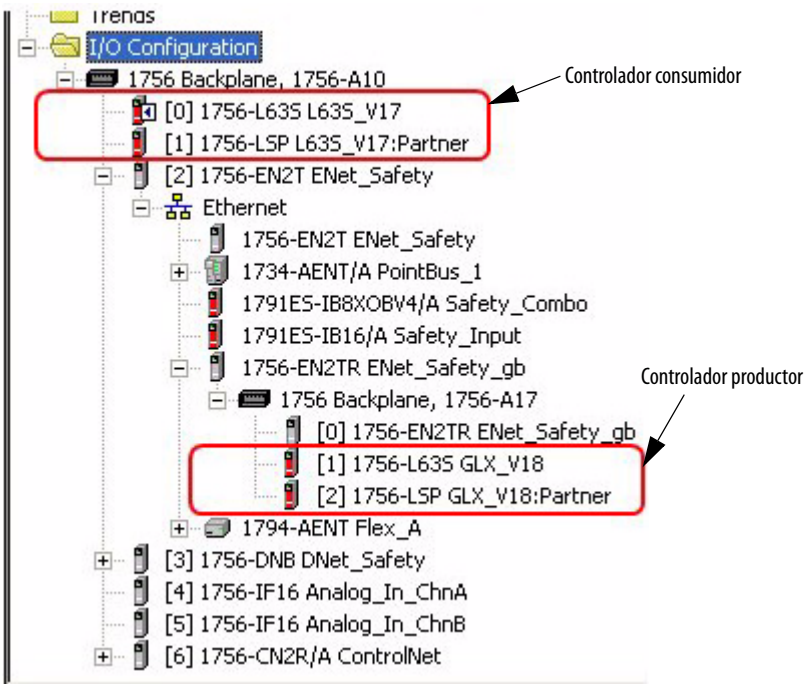
El controlador de seguridad homólogo está sujeto a los mismos requisitos de configuración que el controlador de seguridad local. El controlador de seguridad homólogo también debe tener un número de red de seguridad (SNN). El SNN del controlador de seguridad homólogo depende de su ubicación en el sistema.

Tabla 30 – SNN y ubicación del controlador

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

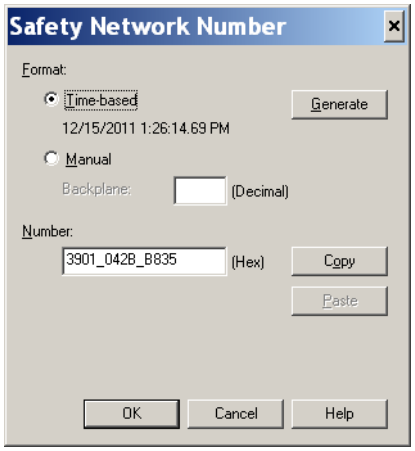
Siga estos pasos para copiar y pegar el SNN.

1. Añada el controlador productor al árbol I/O del controlador consumidor.



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

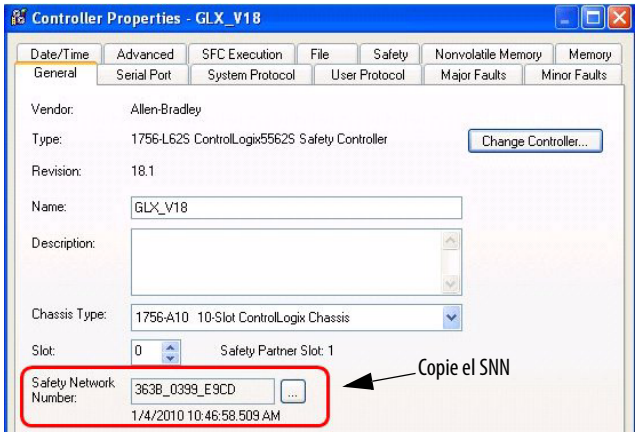
SUGERENCIA Un SNN se puede copiar y pegar mediante los botones del cuadro de diálogo Safety Network Number. Abra los cuadros de diálogo Safety Network Number correspondientes; para ello haga clic en ... a la derecha de los campos de SNN en los cuadros de diálogo de propiedades.



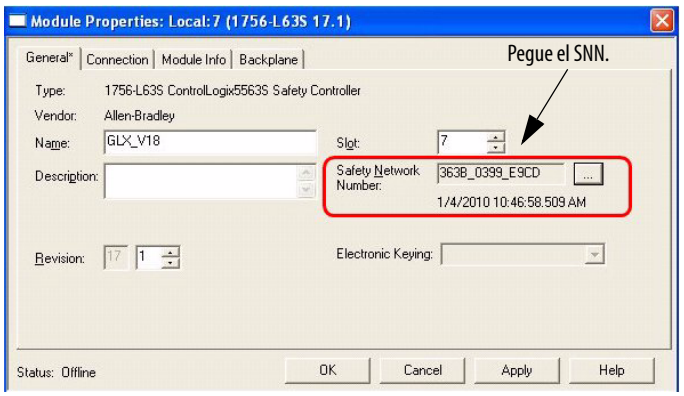
4. En el proyecto del controlador consumidor, haga clic con el botón derecho del mouse en el controlador productor y seleccione Module Properties.

5. Pegue el SNN del controlador productor en el campo SNN.

Cuadro de diálogo Controller Properties del módulo productor en el proyecto productor



Cuadro de diálogo Module Properties en el proyecto consumidor



Producción de un tag de seguridad

Siga este procedimiento para producir un tag de seguridad.

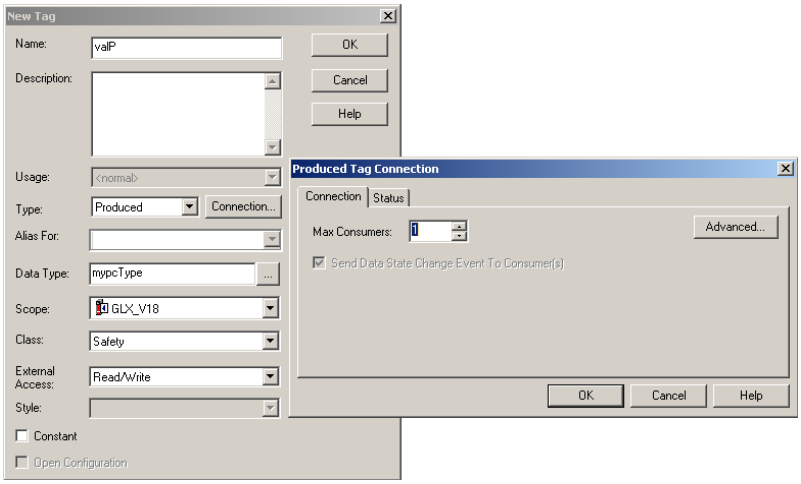
1. En el proyecto del controlador productor, cree un tipo de datos tipo de datos definido por el usuario que defina la estructura de los datos que se van a producir.

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

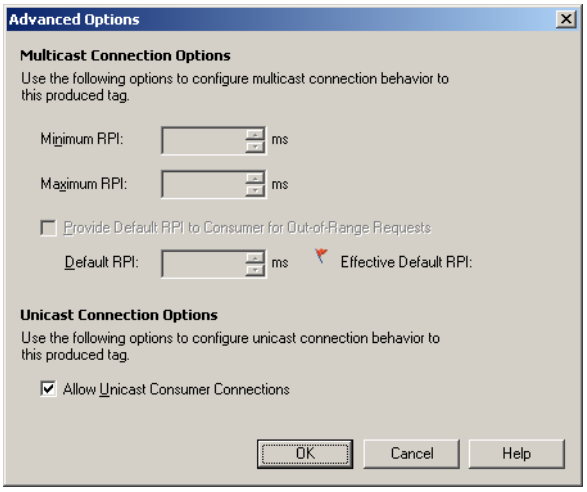
2. Haga clic con el botón derecho del mouse en Controller Tags y seleccione New Tag.

3. En la opción Type seleccione Produced, en la opción 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 borrando la marca de verificación de 'Allow Unicast Consumer Connections'.



6. Haga clic en OK.

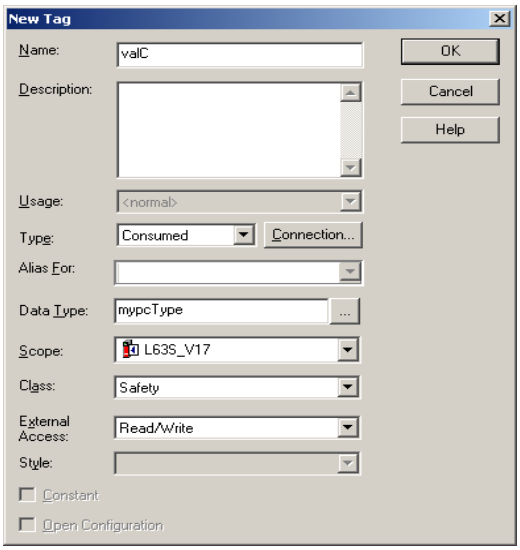
Consumo de datos de tag de seguridad

Siga estos pasos para consumir datos producidos por otro controlador.

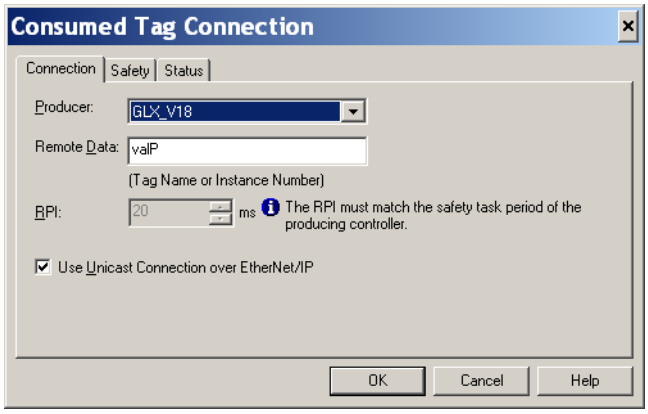
1. En el proyecto del controlador consumidor, cree un tipo de datos definido por el usuario idéntico al creado en el proyecto del productor.

   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 la opción Type seleccione Consumed, en la opción Class seleccione Safety, y en Data Type seleccione el tipo de datos definido por el usuario que creó en el paso 1.



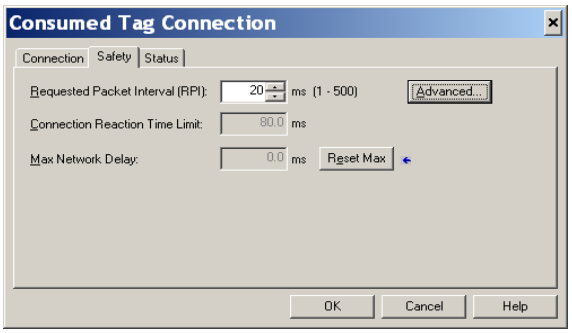
4. Haga clic en Connection para abrir el cuadro de diálogo Consumed Tag Connection.



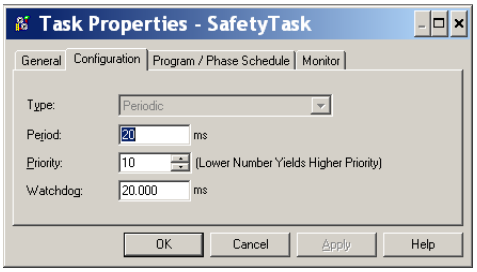
5. Seleccione el controlador que produce los datos.
6. Introduzca el nombre del tag producido.
7. Haga clic en la ficha Safety.
8. Introduzca el intervalo solicitado entre paquetes (RPI) para la conexión en incrementos de 1 ms.

   El valor predeterminado es 20 ms.

Proyecto del consumidor



Proyecto del productor

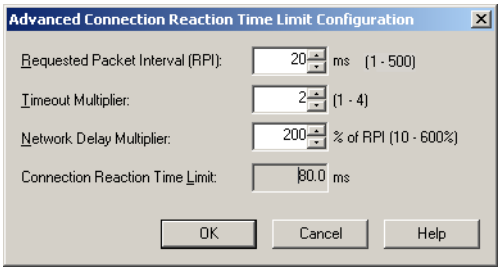


El RPI especifica el período durante el cual se actualizan los datos a través de una conexión. El RPI del tag de seguridad consumido debe coincidir con el período de la tarea de seguridad del proyecto de seguridad del productor.

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, puede restablecer el retardo de red máximo; para ello, haga clic Reset Max.

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 valor de Timeout Multiplier determina el número de RPI que se debe esperar por un paquete hasta declarar terminado el tiempo de espera de una conexión.

El valor de Network Delay Multiplier 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 – Recursos adicionales

Recurso	Descripción
Páginas 71…75	Proporciona más información sobre cómo seleccionar el RPI y cómo el retardo máximo de red, el multiplicador del tiempo de espera 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 restringidos al 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:

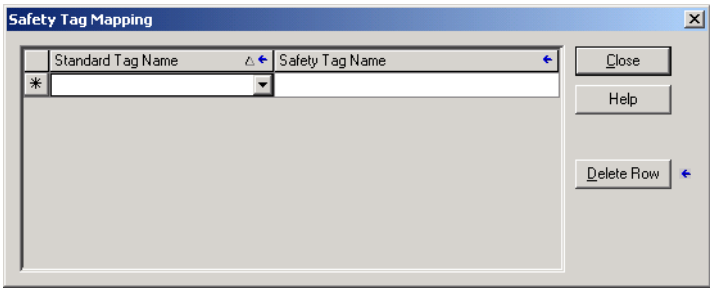
- La pareja formada por el tag de seguridad y el tag estándar debe ser restringida al controlador.
- Los tipos de datos de la pareja de tag de seguridad y tag estándar deben coincidir.
- No se admiten tags de alias.
- La asignación debe tener lugar a nivel de todo el tag. Por ejemplo, myTimer.pre no 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 lo siguiente es cierto:
  - 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, usted será el responsable de proporcionar una forma confiable de garantizar 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 GuardLogix Controller Systems Safety Reference Manual, publicación 1756-RM093, para obtener más información.

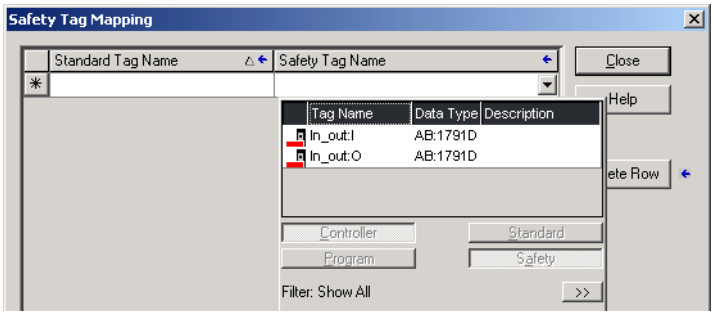
Creación de pares de asignación de tags

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 del 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 restringidos al controlador. Si está en la columna Safety Tag Name, el explorador muestra los tags de seguridad restringidos al 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, y 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 enfocada 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 103.

Protección de las aplicaciones de seguridad

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

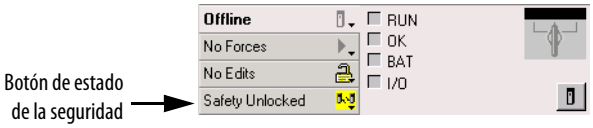
Bloqueo de seguridad del controlador

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, los programas de seguridad, las rutinas de seguridad, las instrucciones Add-On, los tags de seguridad, las E/S de seguridad y la firma de tarea de seguridad.

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

- Programación o edición en línea/fuera de línea (inclusive instrucciones Add-On)
- 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 con 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.

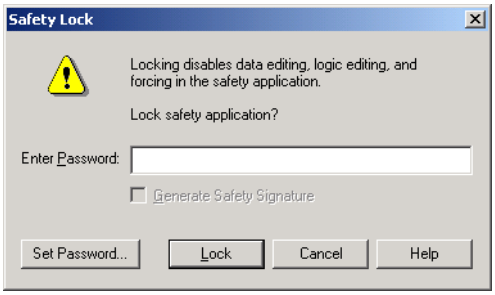
El estado de bloqueo o desbloqueo de seguridad no se puede cambiar cuando el conmutador de llave se encuentra en la posición de marcha (RUN).

SUGERENCIA Las acciones de bloqueo de seguridad o desbloqueo 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 26 – Bloqueo de seguridad del controlador



Si ha establecido una contraseña para la función de bloqueo de seguridad, escríbala 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 49.

La función de bloqueo de seguridad descrita en esta sección y las medidas de seguridad estándar de RSLogix se pueden usar en las aplicaciones del controlador GuardLogix.

Consulte el documento Logix5000 Controllers Security Programming Manual, publicación 1756-PM016, para obtener información acerca de las funciones de seguridad de RSLogix 5000.

Generación de una firma de tarea de seguridad

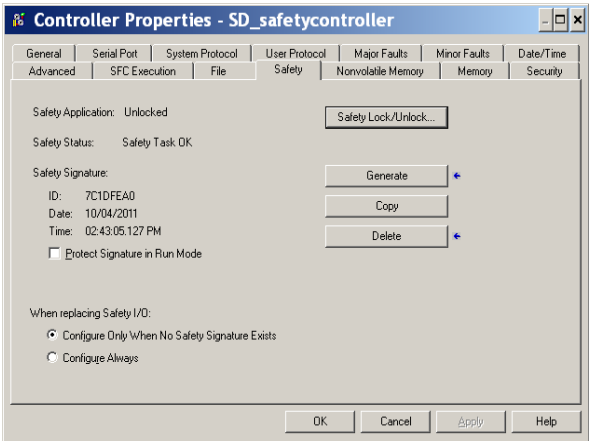
Antes de las pruebas de verificación, usted debe generar la firma de tarea de seguridad. Solo podrá generar la firma de tarea de seguridad si está en línea con el controlador GuardLogix en desbloqueo de seguridad, en el modo de programación, sin forzados de seguridad y sin ediciones de seguridad en línea 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 126) o en la ficha Safety del cuadro de diálogo Controller Properties, como se muestra en la página 107.

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

Figura 27 – Ficha safety



Si existe una firma anterior, se le pide que la sobrescriba.

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 parte 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 los controladores productores
- Manejo de datos de seguridad (salvo con la lógica de rutina de seguridad)

Copia de 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 el identificador, la fecha y la hora en el portapapeles de Windows.

Elimine la firma de tarea de seguridad

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

- El controlador está en bloqueo de seguridad.
- El controlador está en el modo de marcha cuando el interruptor de llave está en la posición de 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, publicación 1756-RM093, para obtener más información sobre los requisitos de SIL 3/PLe.

Restricciones del software

El software de programación 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 lo siguiente es verdadero:

- El controlador está en bloqueo de seguridad.
- Existe una firma de tarea de seguridad.
- Existen fallos de seguridad.
- El estado de la 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 módulos Safety I/O.

  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
En serie	Cable 1756-CP3 o 1747-CP3	Conecte al puerto serial del controlador 1756-L6xS en la página 37
USB	Cable USB 2.0	Conecte al puerto serial del controlador 1756-L7xS en la página 35
EtherNet/IP	Módulo EtherNet/IP en una ranura abierta en el mismo chasis que el controlador	Conexión del dispositivo EtherNet/IP y la computadora en la página 110
DeviceNet	Módulo 1756-DNB en una ranura abierta en el mismo chasis que el controlador	Conecte el módulo de comunicación ControlNet o escáner DeviceNet y su computadora en la página 110
ControlNet	Módulo 1756-CN2 en una ranura abierta en el mismo chasis que el controlador	

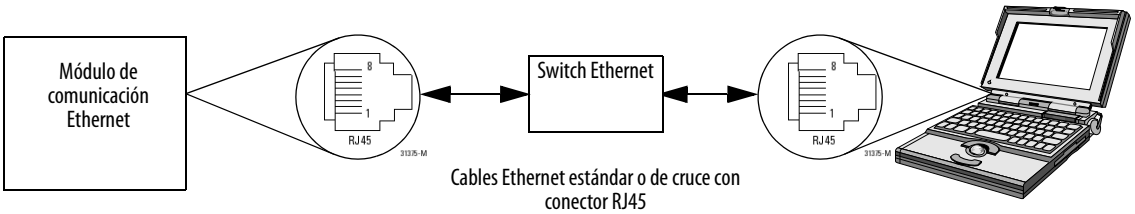
Conexión del dispositivo EtherNet/IP y la computadora

ADVERTENCIA: Si conecta o desconecta el cable de comunicación con la alimentación eléctrica conectada a este módulo o a cualquier otro dispositivo de la red, puede producirse un arco eléctrico. Esto podría provocar una explosión en zonas peligrosas.

Asegúrese de desconectar la alimentación eléctrica y de constatar que la zona no sea peligrosa antes de seguir adelante.

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

Figura 28 – Conexiones Ethernet



Conecte el módulo de comunicación ControlNet o escáner DeviceNet y su computadora

Para acceder a la red ControlNet o DeviceNet , puede hacer uno de los siguientes:

- 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

El software RSLogix 5000 determina si usted puede entrar en línea con un controlador receptor, 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 al controlador. Si se modificó un proyecto, se le pide que realice una carga o una descarga. Si no 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, 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 afecta los procesos de descarga, carga y entrada en línea de los proyectos, tanto estándar como de seguridad.

Si la función de coincidencia del proyecto con el controlador está habilitada en el proyecto fuera de línea, el software RSLogix 5000 compara el número de serie del controlador en el proyecto fuera de línea con el del controlador conectado. Si no coinciden, usted debe 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 receptor.

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. El software RSLogix 5000 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 software RSLogix 5000.

SUGERENCIA	También puede actualizar el firmware seleccionando ControlFLASH™ en el Menú Tools del software RSLogix 5000.

Estado/fallos de seguridad

Se permite cargar la lógica de programa y entrar en línea independientemente del estado de seguridad. El estado de seguridad y los fallos solamente 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, ¿coincide la firma de tarea de seguridad del proyecto fuera de línea 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 del 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 el proyecto completo se descarga. El estado de bloqueo de seguridad coincide con el estado en el proyecto fuera del 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 primero debe desbloquear el controlador para permitir que proceda la descarga.
	Las firmas de la tarea de seguridad no coinciden.	En primer lugar debe poner el controlador en desbloqueo de seguridad, de modo que se pueda continuar con la descarga. Si el controlador tiene una firma de tarea de seguridad, esta se elimina automáticamente y el proyecto completo se descarga. El estado de bloqueo de seguridad coincide con el estado en el proyecto fuera del línea.

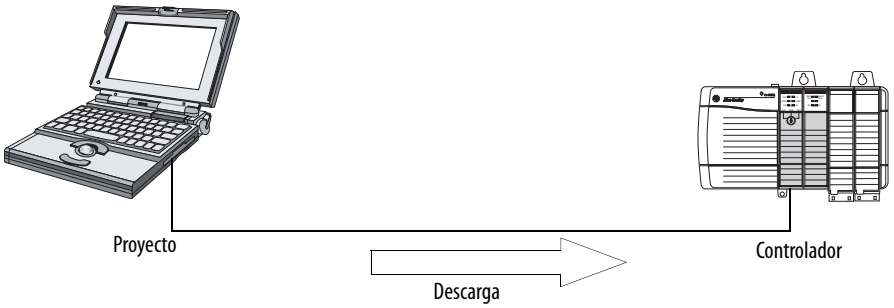
IMPORTANTE Durante una descarga a un controlador con desbloqueo de seguridad, si el firmware en el controlador es diferente al del proyecto fuera de línea, prosiga de una de las siguientes maneras:

- 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 usted actualiza el proyecto, la firma de la tarea de seguridad se elimina y el sistema requiere revalidación.

Descarga

Siga estos pasos para transferir el proyecto de su computadora a su controlador.



1. Mueva el interruptor de llave del controlador a la posición REM.
2. Abra el proyecto de RSLogix 5000 que desee descargar.
3. Defina la ruta de acceso al controlador.
   a. Haga clic en Who Active  .
   b. Seleccione el controlador.
      Para ver el desglose de un nivel, haga clic en el signo +. Si ya se ha seleccionado un controlador, compruebe que sea el correcto.
4. Haga clic en Download.

   El software 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 la seguridad
   - Firma de la tarea de seguridad (si la hay)
   - Estado de bloqueo de seguridad

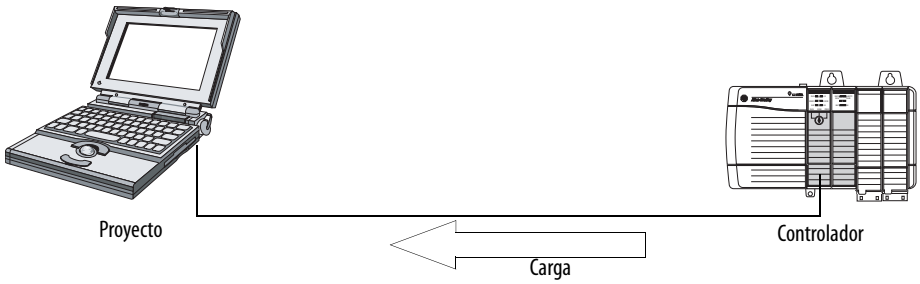
5. Siga las indicaciones de esta tabla para completar la descarga según la respuesta del software.

Si el software indica	Haga lo siguiente
Descarga al controlador.	Seleccione Download. El proyecto se descarga al controlador y el software RSLogix 5000 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, seleccione el cuadro de verificación Update Project Serial Number para permitir que se realice la descarga. El número de serie del proyecto se modifica, de modo 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 la selección.
No se ha podido 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 ha podido 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 la selección.
No se ha podido 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 ha podido 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 la 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 de modo 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 la tarea de seguridad se elimina. **IMPORTANTE:** El sistema de seguridad requiere revalidación.
No se ha podido realizar la descarga al controlador. El controlador está bloqueado. Las firmas de tareas de seguridad del controlador y el proyecto fuera de línea no coinciden.	Seleccione Unlock. Aparece el cuadro de diálogo Safety Unlock for Download. Si se ha seleccionado la casilla de verificación Delete Signature y selecciona Unlock, debe seleccionar 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 su computadora.



1. Defina la ruta de acceso al controlador.
   a. Haga clic en Who Active  .
   b. Seleccione el controlador.
   Para ver el desglose de un nivel, haga clic en el signo +. Si ya se ha seleccionado un controlador, compruebe 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, el software RSLogix 5000 comprueba si el número de serie del proyecto abierto coincide con el número de serie del controlador.

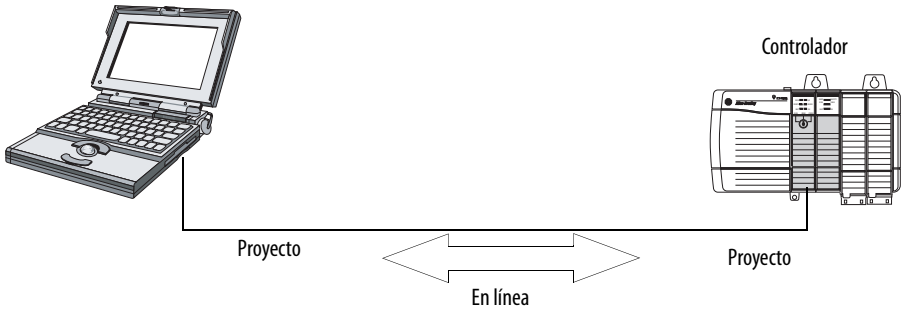
   Si los números de serie de controlador no coinciden, puede realizar una de las siguientes acciones:
   - Cancelar la carga y conectarse a un controlador que sí coincida. Seguidamente, iniciar de nuevo el procedimiento de carga.
   - Seleccionar un nuevo proyecto para la carga o seleccionar otro proyecto distinto mediante Select File.
   - Actualizar el número de serie del proyecto, de modo que coincida con el controlador; para ello, marque la casilla de verificación Update Project Serial Number y seleccione Upload.
5. El software comprueba si el proyecto abierto coincide con el proyecto del controlador.
   a. Si los proyectos no coinciden, debe seleccionar un archivo coincidente o cancelar el proceso de carga.
   b. Si los proyectos coinciden, el software comprueba los cambios en el proyecto fuera de línea (abierto).
6. El software 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 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 ver el desglose de un nivel, haga clic en el signo +. Si ya se ha seleccionado un controlador, compruebe que sea el correcto.
2. Haga clic en Go Online.

   El software comprueba lo siguiente:
   - ¿Coinciden los números de serie del controlador y el 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 – Establecimiento de la 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 verificación Update Project Serial Number … y seleccione Go Online … para conectarse al controlador y actualizar el número de serie del proyecto, de modo 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 la selección. **IMPORTANTE:** Se elimina el proyecto en línea. • Para conservar el proyecto en línea, cancele el proceso en línea e instale una versión del software RSLogix 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 cargar el proyecto fuera de línea. • Download para descargar 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 del proyecto fuera de línea.	• Si la revisión menor de firmware es incompatible, a fin de conservar la firma de la tarea de seguridad actualice la revisión de firmware del controlador de modo 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 la 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 la entrada en línea. Debe poner el proyecto fuera de línea en desbloqueo de seguridad antes de intentar entrar en línea.

Cuando el controlador y el software RSLogix 5000 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 de la entrada en línea.

Notas:

Almacenamiento y carga de proyectos usando la memoria no volátil

Uso de tarjetas de memoria para memoria no volátil

Los controladores GuardLogix, revisión 18 o posterior aceptan una tarjeta de memoria para 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 mediante el software RSLogix 5000

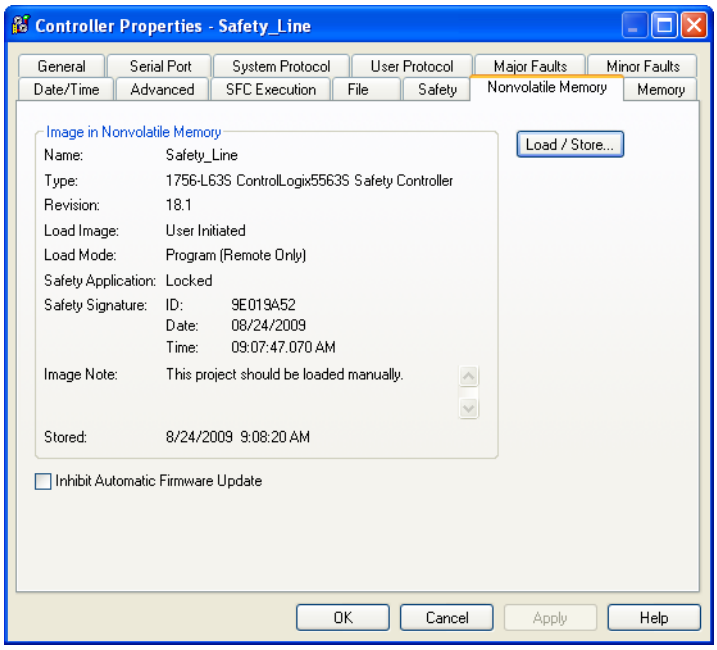
IMPORTANTE La memoria no volátil guarda el contenido de la memoria de usuario al momento en que usted guarda el proyecto:

- 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 al cargar 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 datos de sincronización 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 del indicador de estado OK de color verde. Esto podría contaminar los datos de la tarjeta o del controlador, así como 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 29 – 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 ninguna aplicación en el controlador, se puede guardar solo el firmware del controlador de seguridad únicamente si existe una asociación válida. Una carga de firmware solamente 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 la tarea de seguridad actual se guarda.

Cuando se almacena 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 debe entrar el controlador después de la carga.

Carga de un proyecto de seguridad

Solo se puede iniciar una carga de la memoria no volátil, si lo siguiente es verdadero:

- 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	Entonces seleccione esta opción de imagen de carga	Notas
Siempre que encienda o 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 los cronogramas de 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 de la 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 el software RSLogix 5000 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 puede borrarse de la memoria. Cuando se restaura la alimentación eléctrica, esta opción de carga vuelve a cargar el proyecto al controlador. • El controlador actualiza el firmware en el controlador primario o en el homólogo de seguridad, si es necesario. La aplicación almacenada en la memoria no volátil también se carga, y el controlador entra al modo seleccionado, ya sea programación o marcha. • Siempre se puede usar el software RSLogix 5000 para cargar el proyecto.
Sólo mediante el software RSLogix 5000	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. • Solo está permitido cargar un proyecto a un controlador con bloqueo de seguridad cuando la firma de la 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 programa o 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.

Use módulos de almacenamiento de energía (controladores 1756-L7xS solamente)

Puede usar los ESMs ControlLogix para ejecutar cualquiera de las siguientes tareas:

- Proporcionar alimentación eléctrica a los controladores 1756-L7xS para guardar el programa en la memoria de almacenamiento no volátil (NVS) incorporada en el controlador después de desconectar la alimentación eléctrica del chasis o después de retirar el controlador de un chasis activado.

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 en el controlador 1756-L7*x*S. Para obtener más información consulte Borre el programa de la memoria NVS incorporada

La tabla siguiente describe los ESMs.

Tabla 37 – Módulos de almacenamiento de energía

Núm. de cat.	Descripción
1756-ESMCAP(XT)	ESM basado en condensador Los controladores 1756-L7*x*S vienen con este ESM instalado.
1756-ESMNSE(XT)	ESM basado en condensador sin alimentación eléctrica de respaldo WallClockTime Use este ESM si su aplicación requieren que el ESM instalado descargue su energía almacenada residual a un nivel de 200 µJ o menos antes de transportarlo a su aplicación o fuera de ella. Además, puede usar este ESM con un controlador 1756-L73S (8 MB) o uno con menor memoria solamente.
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 su aplicación requieren que el ESM instalado descargue su energía almacenada residual a un nivel de 200 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

Guarde el programa en la memoria NVS incorporada

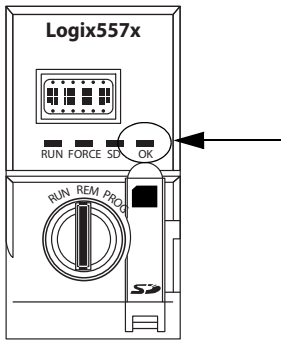
Siga estos pasos para guardar el programa en la memoria NVS cuando se interrumpa la alimentación eléctrica del controlador.

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 activado.

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

Figura 30 – 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 que el indicador de estado OK cambie de rojo fijo a apagado.

Borre el programa de la memoria NVS incorporada

Si su aplicación lo permite, siga estos pasos para borrar el programa de la memoria NVS incorporada en el controlador 1756-L7*x*S.

1. Extraiga el ESM del controlador.

2. Desconecte la alimentación eléctrica del controlador desconectando la alimentación eléctrica del chasis mientras el controlador está instalado en el chasis, o retirando el controlador de un chasis activado.

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.

Calcule la asistencia técnica de WallClocktime del ESM

El ESM ofrece asistencia técnica para el mantenimiento del atributo WallClockTime del controlador cuando se desconecta la alimentación eléctrica. Use esta tabla para calcular el tiempo de retención del ESM basado en la temperatura del controlador y el ESM instalado.

Tabla 38 – Temperatura vs. tiempo de retención

	Tiempo de retención (en días)		
Temperatura	**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 de firmware con la función Firmware Supervisor

A partir de la versión 18 del software RSLogix 5000, se puede usar la función Firmware Supervisor para administrar el 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 programa o marcha.
- La codificación electrónica debe estar configurada para Exact Match.
- El kit de firmware para el dispositivo receptor debe residir en la tarjeta de memoria del controlador.
- El dispositivo debe aceptar actualizaciones de firmware mediante la utilidad ControlFLASH.

La función Firmware Supervisor acepta productos de E/S distribuidos no modulares que se colocan directamente en la red sin un adaptador, entre ellos los módulos CIP Safety I/O en las redes EtherNet/IP. Los módulos CIP Safety I/O en las 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.

El software RSLogix 5000 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

Vea 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 31 – 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 alguno de ellos o los dos presentan un fallo de batería, el indicador de estado se ilumina.El indicador LED I/O 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 32 – 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	
Safety Task Inoperable	
Partner Missing (falta el homólogo) Partner Unavailable (el homólogo no está disponible) Hardware Incompatible (hardware incompatible) Firmware Incompatible (firmware incompatible)	
Offline (fuera de línea)	

Los iconos aparecen en color verde cuando el controlador está en bloqueo de seguridad, en color amarillo cuando el controlador está en desbloqueo de seguridad, y en 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 conexiones

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

Todas las conexiones

Si la comunicación con un dispositivo en la configuración de E/S del controlador tarda más de 100 ms, se sobrepasa el tiempo de espera y el controlador muestra las advertencias siguientes:

- El indicador de E/S ubicado en la parte frontal del controlador parpadea en 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 módulo, al cual puede acceder mediante la ficha Connections del cuadro de diálogo Module Properties del módulo 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 la 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.

Vea Conexiones de seguridad.

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 de salida, los tags de Safety I/O tienen un miembro de estado de la 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 Marcha (1) o en estado de inactividad (en reposo) (0). El estado de inactividad se indica si la conexión está cerrada, si la tarea de seguridad presenta un fallo, o si el controlador remoto o el dispositivo se encuentran en el modo Programa o en el modo 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 Marcha.
0 = Inactividad	0 = Válido	La conexión está activa y el dispositivo productor está en estado de inactividad. 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 de inactividad (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

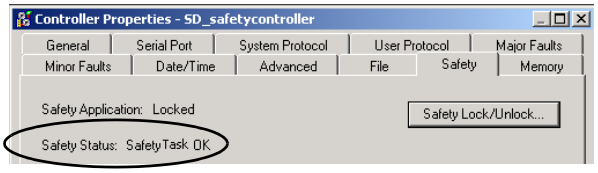
Los controladores Logix, incluso los controladores GuardLogix aceptan palabras clave de estado que se pueden utilizar en la lógica para monitorear determinados eventos.

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 la 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 33 – Estado de la tarea de seguridad



Estas son las opciones posibles del estado de seguridad:

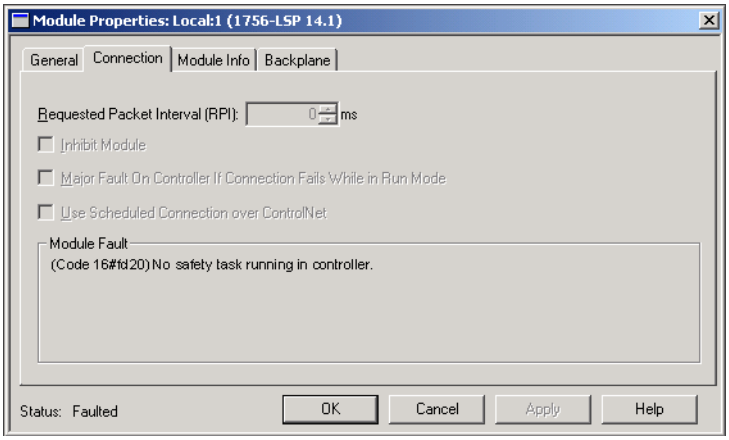
- Safety partner is missing or unavailable.
- Safety partner hardware is incompatible with primary controller.
- Safety partner firmware is incompatible with the primary controller.
- Safety task inoperable.
- Safety task OK.

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

Consulte Fallos de seguridad mayores (Tipo 14) en la página 130 para obtener información sobre los códigos de fallo y las acciones correctivas.

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

Figura 34 – 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 módulos CIP Safety I/O entra 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 control (watchdog) 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 administrador de fallos del controlador, la aplicación estándar sigue ejecutándose.

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

Debe demostrar a su organismo certificador que al dejar seguir funcionando una parte del sistema, el funcionamiento sigue siendo seguro.

Si existe una firma de tarea de seguridad, solo tiene que borrar el fallo para que la tarea de seguridad se pueda ejecutar. 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 o no detener la ejecución de la tarea de seguridad, en función de si el fallo es manejado por el administrador de fallos del programa en la aplicación de seguridad.

Si se borra un fallo recuperable como parte de la programación, la tarea de seguridad puede continuar 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 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 desbloquear el controlador y eliminar la firma de tarea de seguridad antes de poder editar la aplicación de seguridad.

Visualización de fallos

El cuadro 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 de los controladores 1756-L7xS también muestra códigos de fallo con un mensaje de estado breve, como se describe en la página 137.

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 de seguridad mayores (Tipo 14)

Código	Causa	Estado	Acción correctiva
01	Se sobrepasó el tiempo del temporizador de control (watchdog) 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 mediante la firma 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 poder ejecutar la tarea de seguridad. 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 es no válida, por ejemplo existe una desigualdad de lógica entre el controlador primario y el homólogo de seguridad, se sobrepasó el tiempo permitido del temporizador de vigilancia o se alteró 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 poder ejecutar la tarea de seguridad.
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.

Se produce un fallo menor recuperable tipo (10), código 11, cuando no está presente o necesita reemplazarse la batería del homólogo de seguridad 1756-LSP.

Vea el Apéndice B para obtener información sobre el reemplazo de la batería.

El documento Logix5000 Controllers Major and Minor Faults Programming Manual, publicación 1756-PM014, incluye descripciones de los códigos de fallo comunes a todos 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 función de su aplicación, tal vez no convenga que todos los fallos de seguridad desactiven todo el sistema. En esos casos, puede utilizar una rutina de fallo para borrar un fallo concreto y dejar que la parte de control estándar del sistema siga funcionando, o bien configurar algunas salidas para que permanezcan activadas.

ATENCIÓN: Debe demostrar a su organismo certificador que al dejar seguir funcionando una parte del sistema, el funcionamiento sigue siendo seguro.

El controlador admite dos niveles de manejo de fallos mayores:

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

Ambas rutinas pueden utilizar las instrucciones GSV y SSV, como se describe en la página 132.

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 administrador de fallos del controlador (si lo hay).

Administrador de fallos del controlador

El administrador 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.

Solo se puede crear un programa para el administrador 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 las 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 muestra solo 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 módulo Safety I/O.

Para los objetos de seguridad, la Tabla 42 muestra para cuáles atributos puede obtener valores usando la instrucción GSV, y cuáles atributos 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 evento de este objeto de tarea. Los valores válidos son 0…31.	✓		✓	
	MaximumInterval	DINT[2]	Intervalo de tiempo máximo entre ejecuciones sucesivas de esta tarea.			✓	✓
	MaximumScanTime	DINT	Tiempo de ejecución registrado máximo (ms) para esta tarea.			✓	✓
	MinimumInterval	DINT[2]	Intervalo de tiempo mínimo entre ejecuciones sucesivas de esta tarea.			✓	✓
	Priority	INT	Prioridad relativa de esta tarea en comparación con otras tareas; los valores válidos son 0…15.	✓		✓	
	Rate	DINT	Período de la tarea (en ms) o valor de sobrepaso del tiempo de espera para la tarea (en ms).	✓		✓	
	Watchdog	DINT	Límite de tiempo (en ms) para ejecutar todos los programas asociados con esta tarea.	✓		✓	
Programa de seguridad	Instance	DINT	Proporciona el número de evento del objeto de programa.	✓		✓	
	MajorFaultRecord[1]	DINT[11]	Registra los fallos mayores para este programa.	✓	✓	✓	
	MaximumScanTime	DINT	Tiempo de ejecución registrado máximo (ms) para este programa.			✓	✓
Rutina de seguridad	Instance	DINT	Proporciona el número de evento de este objeto de rutina. Los valores válidos son 0…65,535.	✓			

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
Controlador de seguridad	SafetyLocked	SINT	Indica si el controlador está en bloqueo o en desbloqueo de seguridad.	✓		✓	
	SafetyStatus[2]	INT	Especifica el estado de la seguridad como: • Safety task OK. (1000000000000000) • Safety task inoperable. (1000000000000001) • Partner missing. (0000000000000000) • Partner unavailable. (0000000000000001) • Hardware incompatible. (0000000000000010) • Firmware incompatible. (0000000000000011)			✓	
	SafetySignatureExists	SINT	Indica si está presente una firma de tarea de seguridad.	✓		✓	
	SafetySignatureID	DINT	Número de identificación de 32 bits.			✓	
	SafetySignature	String[3]	Número de identificación de 32 bits.			✓	
	SafetyTaskFaultRecord[1][2]	DINT[11]	Registra los fallos de la tarea de seguridad.			✓	
AOI (seguridad)	LastEditDate	LINT	Sello de fecha y hora de la última edición a una definición de instrucción Add-On.			✓	
	SignatureID	DINT	Número de identificación.			✓	
	SafetySignatureID	DINT	Número de identificación de 32 bits.			✓	

(1) Vea Acceso a los atributos de FaultRecord en la página 133 para obtener información sobre cómo obtener acceso a este atributo.
(2) Vea Captura de información de fallo en la página 134 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 los atributos de 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 de 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
Tipo	INT	Decimal	Tipo de fallo (programa, E/S y otro)
Código	INT	Decimal	Código único para este fallo (depende del tipo de fallo)
Info	DINT[8]	Hexadecimal	Información específica del fallo (depende del tipo de fallo y código)

Para obtener más información sobre el uso de las instrucciones GSV y SSV, consulte el capítulo sobre instrucciones de entrada/salida del documento Logix5000 Controllers General Instructions Reference Manual, 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 administrador 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 administrador de fallos del controlador que borra el fallo y permite que las tareas estándar continúen ejecutándose.

Indicadores de estado

Indicadores de estado del controlador 1756-L6xS

Los indicadores LED de estado muestran el estado del controlador primario y del homólogo de seguridad.

Tabla 44 – Descripción de los indicadores de estado del 1756-L6xS

Indicador	Estado	Descripción del controlador primario	Descripción del homólogo de seguridad
RUN	Apagado	No hay ninguna tarea de usuario en ejecución. El controlador se encuentra en el modo PROG (Programa).	No corresponde
	Verde	El controlador se encuentra en el modo RUN (Marcha).	No corresponde
SAFE RUN	Apagado	No corresponde	La tarea de seguridad del usuario o las salidas de seguridad están inhabilitadas. El controlador se encuentra en el modo PROG (Programa) o en el modo de prueba, o bien la tarea de seguridad presenta un fallo.
	Verde	No corresponde	La tarea de seguridad del usuario y las salidas de seguridad están habilitadas. La aplicación de seguridad se está ejecutando. La firma de la tarea de seguridad está presente.
	Verde parpadeante	No corresponde	La tarea de seguridad del usuario y las salidas de seguridad están habilitadas. La aplicación de seguridad se está ejecutando. La firma de la tarea de seguridad no está presente.
FORCE	Apagado	No hay forzados estándar ni de seguridad habilitados en el controlador.	No corresponde
	Ámbar	Se han habilitado forzados estándar y/o de seguridad.	No corresponde
	Ámbar parpadeante	Se ha forzado el encendido o el apagado de una o más direcciones de E/S, estándar y/o de seguridad, pero no se han habilitado forzados.	No corresponde
BAT	Apagado	La batería es suficiente para la memoria.	La batería es suficiente para la memoria.
	Rojo	La batería no es suficiente para la memoria.	La batería no es suficiente para la memoria.
OK	Apagado	No hay alimentación eléctrica aplicada.	No hay alimentación eléctrica aplicada.
	Verde	El controlador está funcionando y no presenta fallos.	El homólogo de seguridad está funcionando y no presenta fallos.
	Rojo parpadeante	Fallo no recuperable o recuperable no manejado en el administrador de fallos. Todas las tareas del usuario, estándar y de seguridad, se detienen.	No corresponde
	Rojo	Fallo de encendido o fallo de controlador no recuperable.	Fallo de encendido o fallo de controlador no recuperable.

Tabla 44 – Descripción de los indicadores de estado del 1756-L6xS

Indicador	Estado	Descripción del controlador primario	Descripción del homólogo de seguridad
I/O[1]	Apagado	Sin actividad; no se ha configurado ninguna E/S.	No corresponde
	Verde	El controlador se está comunicando con todos los dispositivos de E/S configurados, tanto estándar como de seguridad.	No corresponde
	Verde parpadeante	Uno o más dispositivos de E/S no responden.	No corresponde
	Rojo parpadeante	El controlador no se está comunicando con E/S configuradas.	No corresponde
RS232	Apagado	Sin actividad	No corresponde
	Verde	Se están recibiendo o transmitiendo datos.	No corresponde
SAFETY TASK	Apagado	No corresponde	No se ha establecido una asociación. Falta el controlador primario, no está funcionando correctamente o la revisión de firmware es incompatible con la del homólogo de seguridad.
	Verde	No corresponde	El estado del controlador de seguridad es "OK". La hora coordinada del sistema (CST) está sincronizada y se han establecido las conexiones de E/S de seguridad.
	Verde parpadeante	No corresponde	El estado del controlador de seguridad es "OK". La hora coordinada del sistema (CST) no está sincronizada en el controlador primario o en el homólogo de seguridad.
	Rojo	No corresponde	Se perdió la asociación y no se ha establecido una asociación nueva. Falta el controlador primario, no está funcionando correctamente o la revisión de firmware es incompatible con la del homólogo de seguridad.
	Rojo parpadeante	No corresponde	No se puede ejecutar la tarea de seguridad.

(1) Las E/S incluyen tags producidos/consumidos provenientes de otros controladores.

Indicadores de estado de los controladores 1756-L7xS

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

Tabla 45 – Descripción de los indicadores de estado del controlador primario 1756-L7xS

Indicador	Estado	Descripción
RUN	Apagado	No hay ninguna tarea de usuario en ejecución. El controlador se encuentra en el modo PROG (Programa).
	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 estará efectivo inmediatamente.**
	Ámbar parpadeante	Se ha forzado el encendido o el apagado de una o más direcciones de E/S, estándar y/o de seguridad, 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 se hacen efectivos.**
SD	Apagado	No hay actividad con la tarjeta de memoria.
	Verde parpadeante	El controlador está leyendo la tarjeta de memoria o escribiendo a esta. No retire la tarjeta de memoria mientras el controlador está 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.

Tabla 45 – Descripción de los indicadores de estado del controlador primario 1756-L7xS

Indicador	Estado	Descripción
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 administrador 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 de 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 activado, pero no está operativo. • El controlador está cargando un proyecto en la memoria no volátil.

El homólogo de seguridad 1756-L7SP tiene un indicador de estado OK.

Tabla 46 – 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 1756-L7xS

La pantalla de estado del controlador 1756-L7*x*S desplaza 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 la seguridad

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

Tabla 47 – Pantalla de estado de la 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, ocurrió una desigualdad entre el controlador primario y el homólogo de seguridad, se sobrepasó el tiempo de espera del temporizador de control (watchdog) o se alteró la memoria.
Safety Unlocked	El controlador está en el modo marcha con una firma de seguridad, pero no tiene bloqueo de seguridad.

Mensajes de estado general

Los mensajes descritos en la Tabla 48 generalmente aparecen al momento del encendido, al momento de la desactivación y mientras el controlador está en marcha. Estos mensajes indican el estado del controlador y del ESM.

Tabla 48 – Pantalla de estado general

Mensaje	Interpretación
No hay 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 activado y determine el estado del controlador.
TEST	El controlador está realizando las pruebas del momento del encendido.
PASS	Las pruebas del momento del encendido se realizaron correctamente.
SAVE	Se está guardando un proyecto en la tarjeta SD durante la desactivación. También puede ver el indicador SD (vea la página 136) para obtener información de estado adicional. Deje que concluya la operación de guardar antes de retirar la tarjeta SD o desconectar la alimentación eléctrica.
LOAD	Se está cargando un proyecto desde la tarjeta SD al momento del encendido del controlador. También puede ver el indicador SD (vea la página 136) para obtener información de estado adicional. Deje que la carga concluya 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 al momento del encendido. También puede ver el indicador SD (vea la página 136) para obtener información de estado adicional. Si no desea que el firmware se actualice al 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 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 el software RSLogix 5000 para descargar el proyecto al controlador, o use una tarjeta SD para cargar un proyecto en el controlador.
Project Name	El nombre del proyecto cargado actualmente en el controlador. El nombre indicado se basa en el nombre del proyecto especificado en el software RSLogix 5000.
BUSY	Los módulos de E/S asociados con el controlador todavía no están totalmente activados. Permita tiempo para la activación y autoprueba del módulo de E/S.
Corrupt Certificate Received	El certificado de protección asociado con el firmware está alterado. 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 con la obtenida del sitio web de asistencia técnica.
Corrupt Image Received	El archivo de firmware está alterado. 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 con la obtenida del sitio web de asistencia técnica.
ESM Not Present	Un ESM no está presente y el controlador no puede guardar la aplicación al momento del apagado. Inserte un ESM compatible y, si está usando 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 con un ESM compatible.
ESM Hardware Failure	Se produjo un fallo del ESM y el controlador no puede guardar el programa en el caso de una desactivación. 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 para que guarde el programa en caso de una desactivación. 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	Una actualización de firmware iniciada mediante las utilidades ControlFLASH o AutoFlash está en curso. Permita que la actualización de firmware concluya sin interrupción.
Firmware Installation Required	El controlador está usando firmware de inicio (es decir la revisión 1.*xxx*) y requiere una actualización de firmware. Actualice el firmware del controlador.
SD Card Locked	Hay una tarjeta SD bloqueada instalada.

Mensajes de fallo

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

Tabla 49 – Mensajes de fallo(1)

Mensaje	Interpretación
Major Fault T*XX*:C*XX message*	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, entonces se programa una instrucción JMP para que salte a una instrucción LBL no válida.
I/O Fault Local:*X #XXXX message*	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 descripción breve. Por ejemplo, I/O Fault Local:3 #0107 Connection Not Found indica que una conexión al módulo de E/S locales en la ranura tres no está abierta. Tome la acción correctiva correspondiente al tipo de fallo indicado.
I/O Fault *ModuleName #XXXX message*	Ocurrió un fallo de E/S en un módulo en un chasis remoto. El nombre del módulo con fallo, como se configura en el árbol I/O Configuration del software RSLogix 5000, 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 una conexión al módulo llamado 'My_Module' no está abierta. Tome la acción correctiva correspondiente al tipo de fallo indicado.
I/O Fault *ModuleParent:X #XXXX message*	Ocurrió un fallo de E/S en un módulo en un chasis remoto. El nombre del primario del módulo se indica porque ningún nombre de módulo está configurado en el árbol I/O Configuration del software RSLogix 5000. 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 una conexión a un módulo en la ranura 3 del chasis con el módulo de comunicación llamado 'My_CNet' no está abierta. 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, se reduce el número de fallos indicado y el siguiente fallo reportado es 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 message* en la pantalla de estado del controlador. En la Tabla 50 en la página 140 se listan los 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 50 – 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	Keyswitch 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 fallos 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 message*
- I/O Fault *ModuleName #XXXX message*
- I/O Fault *ModuleParent*:*X #XXXX message*

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 el software RSLogix 5000.

La última parte del formato, #XXXX message, puede usarse para diagnosticar el tipo de fallo de E/S y las acciones correctivas potenciales. 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 51 – 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 Settable
#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	Timeout Multiplier
#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
–	

Mantenimiento de la batería

Los controladores primarios GuardLogix 1756-L6xS y los homólogos de seguridad 1756-LSP contienen una batería de litio cuyo reemplazo podría ser necesario. Los controladores GuardLogix 1756-L7xS y los homólogos de seguridad 1756-L7SP no tienen batería.

Vida útil estimada de la batería

La vida útil de la batería depende de la temperatura del chasis, de la magnitud del proyecto y de la frecuencia con que se desconecta y se vuelve a conectar la alimentación eléctrica al controlador. La vida útil de la batería no depende de si el controlador está encendido o no.

Antes de que el indicador LED BAT se encienda

Utilice esta tabla para calcular el tiempo en el peor de los casos, antes de que el indicador BAT se encienda de color rojo.

Tabla 52 – Cálculo aproximado del indicador de la batería (en el peor de los casos)

Temperatura 2.54 cm (1 pulg.) Debajo del chasis	Desconexiones y reconexiones de la alimentación eléctrica al día	Magnitud del proyecto			
		1 MB	2 MB	4 MB	8 MB
0…40 °C (32…104 °F)	3	3 años	3 años	26 meses	20 meses
	2 o menos	3 años	3 años	3 años	31 meses
41…45 °C (105…113 °F)	3	2 años	2 años	2 años	20 meses
	2 o menos	2 años	2 años	2 años	2 años
46…50 °C (114…122 °F)	3 o menos	16 meses	16 meses	16 meses	16 meses
51…55 °C (123…131 °F)	3 o menos	11 meses	11 meses	11 meses	11 meses
56…60 °C (132…140 °F)	3 o menos	8 meses	8 meses	8 meses	8 meses

EJEMPLO En las siguientes condiciones, la batería dura como mínimo 20 meses antes de que el indicador LED BAT se encienda de color rojo.

- La máxima temperatura a 2.54 cm (1 pulg.) debajo del chasis es 45 °C (113 °F)
- La alimentación eléctrica se desconecta y reconecta tres veces al día.
- El controlador contiene un proyecto de 8 MB

Después de que el indicador LED BAT se enciende

IMPORTANTE Si el indicador BAT se enciende por primera vez mientras se está suministrando alimentación eléctrica al controlador, la vida útil de la batería será menor a lo que indica la Tabla 53. La batería siempre tiene una pequeña fuga constante. Es posible que parte de la vida útil de la batería se haya consumido mientras el controlador estaba apagado y, por tanto, no pudo encenderse el indicador BAT.

Tabla 53 – Vida útil de la batería después de que el indicador BAT se enciende de color rojo (en el peor de los casos)

Temperatura, máx. 25.4 mm (1 pulg.) Debajo del chasis	Desconexiones y reconexiones de la alimentación eléctrica	Magnitud del proyecto			
		1 MB	2 MB	4 MB	8 MB
0…20 °C (0…68 °F)	3 al día	26 semanas	18 semanas	12 semanas	9 semanas
	1 al día	26 semanas	26 semanas	26 semanas	22 semanas
	1 al mes	26 semanas	26 semanas	26 semanas	26 semanas
21…40 °C (70…104 °F)	3 al día	18 semanas	14 semanas	10 semanas	8 semanas
	1 al día	24 semanas	21 semanas	18 semanas	16 semanas
	1 al mes	26 semanas	26 semanas	26 semanas	26 semanas
41…45 °C (106…113 °F)	3 al día	12 semanas	10 semanas	7 semanas	6 semanas
	1 al día	15 semanas	14 semanas	12 semanas	11 semanas
	1 al mes	17 semanas	17 semanas	17 semanas	17 semanas
46…50 °C (115…122 °F)	3 al día	10 semanas	8 semanas	6 semanas	6 semanas
	1 al día	12 semanas	11 semanas	10 semanas	9 semanas
	1 al mes	12 semanas	12 semanas	12 semanas	12 semanas
51…55 °C (124…131 °F)	3 al día	7 semanas	6 semanas	5 semanas	4 semanas
	1 al día	8 semanas	8 semanas	7 semanas	7 semanas
	1 al mes	8 semanas	8 semanas	8 semanas	8 semanas
56…60 °C (133…140 °F)	3 al día	5 semanas	5 semanas	4 semanas	4 semanas
	1 al día	6 semanas	6 semanas	5 semanas	5 semanas
	1 al mes	6 semanas	6 semanas	6 semanas	6 semanas

Cuándo reemplazar la batería

Cuando la batería está descargada aproximadamente en un 95%, el controlador lo advierte del modo siguiente:

- El indicador BAT ubicado en la parte frontal del controlador se enciende (rojo fijo).
- Ocurre un fallo menor (tipo 10, código 10 para el controlador).

ATENCIÓN: Para evitar fugas químicas potencialmente peligrosas de la batería, reemplace la batería según el cronograma siguiente, incluso si el indicador BAT está apagado.

Tabla 54 – Cronograma de reemplazo de la batería

Si la temperatura a 2.54 cm (1 pulg.) debajo del chasis es	Reemplace la batería cada
-25…35 °C (-13…95 °F)	No es necesario reemplazar
36…40 °C (96.8…104 °F)	3 años
41…45 °C (105.8…113 °F)	2 años
46…50 °C (114.8…122 °F)	16 meses
51…55 °C (123.8…131 °F)	11 meses
56…70 °C (132.8…158 °F)	8 meses

IMPORTANTE Puesto que el controlador GuardLogix es un controlador 1oo2 (con dos procesadores), recomendamos encarecidamente reemplazar las baterías de ambos controladores simultáneamente.

Reemplazo de la batería

Este controlador tiene una batería de litio que debe reemplazarse durante la vida útil del producto. Usted debe seguir precauciones específicas al tocar o desechar la batería.

ATENCIÓN: El controlador utiliza una batería de litio que contiene productos químicos potencialmente peligrosos.

Antes de tocar o de desechar una batería, revise el documento Pautas para el tratamiento de baterías de litio, publicación AG-5.4.

ADVERTENCIA: Cada vez que conecte o que desconecte la batería puede producirse un arco eléctrico. Esto podría provocar una explosión en zonas peligrosas. Asegúrese de desconectar la alimentación eléctrica y de constatar que la zona no sea peligrosa antes de seguir adelante.

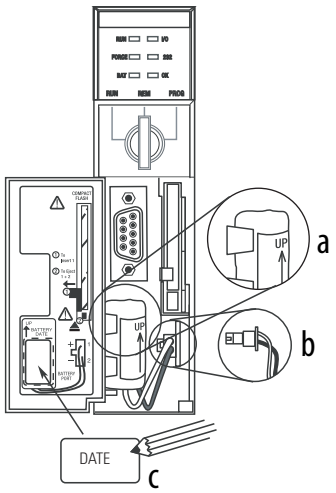
IMPORTANTE Si retira la batería y posteriormente se produce una interrupción de la alimentación eléctrica, se perderá el proyecto que se encuentre en el controlador.

Siga este procedimiento para reemplazar la batería.

1. Encienda la alimentación eléctrica del chasis.
2. ¿Presenta la batería señales de fuga o de daño?

Si la respuesta es	Haga lo siguiente
Sí	Antes de tocar la batería, revise el documento Pautas para el tratamiento de baterías de litio, publicación AG-5.4
No	Vaya al paso siguiente.

3. Retire la batería anterior.
4. Instale una batería 1756-BA2 nueva.
   a. Coloque la batería como se muestra.
   b. Conecte la batería:
      + Rojo
      - Negro
   c. Anote la fecha de instalación de la batería en la etiqueta de la batería, y adhiera la etiqueta en la parte interior de la puerta del controlador.



ATENCIÓN: Instale exclusivamente una batería 1756-BA2. Si instala una batería diferente podría provocar daños al controlador.

5. Determine si está apagado el indicador LED BAT ubicado en la parte frontal del controlador.

Si la respuesta es	Haga lo siguiente
Sí	Vaya al paso siguiente.
No	1. Compruebe que la batería esté bien conectada al controlador. 2. Si el indicador BAT sigue encendido, instale otra batería 1756-BA2. 3. Si después de instalar otra batería en el paso 2 el indicador BAT sigue encendido, comuníquese con el representante o con el distribuidor local de Rockwell Automation.

6. Deseche la batería anterior de conformidad con los reglamentos locales.

ADVERTENCIA: No incinere ni deseche las baterías de litio en el basurero colectivo. Las baterías podrían explotar o abrirse repentinamente. Observe todos los reglamentos locales relativos al desecho de estos materiales. Se le considerará responsable legalmente de los peligros provocados durante el desecho de la batería.

ATENCIÓN: Este producto contiene una batería de litio sellada que quizás deba ser reemplazada durante la vida útil del producto.

Al final de su vida útil, la batería de este producto no debe desecharse en la basura municipal general.

La recolección y el reciclaje de las baterías ayudan a proteger el medio ambiente y contribuyen a la conservación de recursos naturales en la medida que se recuperan valiosos materiales.

Almacenamiento de baterías de reemplazo

ATENCIÓN: Una batería puede producir fugas de productos químicos potencialmente peligrosos si se almacena incorrectamente. Almacene las baterías en un entorno fresco y seco. Recomendamos una temperatura de 25 °C (77 °F) con una humedad relativa de 40…60%. Puede almacenar las baterías un máximo de 30 días a temperaturas entre -45…85 °C (-49…185 °F), por ejemplo, durante el transporte. Para evitar posibles fugas, no almacene las baterías a más de 60 °C (140 °F) durante más de 30 días.

Recursos adicionales

Consulte el documento Pautas para el tratamiento de baterías de litio, publicación AG-5.4, Para obtener información acerca de cómo manejar, almacenar y desechar las baterías de litio.

Notas:

Cambio del tipo de controlador en proyectos RSLogix 5000

Dado que los controladores de seguridad tienen requisitos especiales y no son compatibles con ciertas funciones estándar, usted debe 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 RSLogix 5000. El cambio del tipo de controlador afecta los siguientes aspectos:

- Funciones compatibles
- Configuración física del proyecto, es decir, el homólogo de seguridad y las E/S de seguridad
- Propiedades del controlador
- Componentes del proyecto tales como tareas, programas, rutinas y tags
- Instrucciones Add-On de seguridad.

Cambio de un controlador estándar a uno de seguridad

Para cambiar adecuadamente el tipo de controlador de un controlador estándar a un controlador de seguridad, la ranura del chasis ubicada 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 (es decir, 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, 1756-LSP, se elimina del chasis de E/S.
- Los módulos Safety I/O y sus tags se eliminan.
- Los programas, las rutinas y la tarea de seguridad se cambian a programas, a rutinas y a una tarea estándar.
- Todos los tags de seguridad, salvo los tags de consumo de seguridad, se cambian por 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 no disponibles en el controlador de seguridad, las nuevas características aparecen en el cuadro de diálogo Controller Properties.

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

- Las instrucciones podrían seguir haciendo referencia a módulos eliminados y producirán errores de verificación.
- Los tags consumidos se eliminan cuando se elimina el módulo productor.
- A raíz de los cambios en el sistema antes descritos, las instrucciones específicas de seguridad y los tags de E/S de seguridad no verificarán.

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

Cambio de un controlador 1756 GuardLogix a un controlador 1768 Compact GuardLogix o viceversa

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

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

- El homólogo de seguridad se crea en la ranura x (ranura primaria + 1) al cambiar a un controlador 1756 GuardLogix.
- 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 1756 GuardLogix aceptan 100 programas de seguridad en la tarea de seguridad, mientras que los controladores 1768 Compact GuardLogix aceptan 32.

Cambio de un controlador 1756-L7xS a un controlador 1756-L6xS o 1768-L4xS

Las instrucciones de valor con punto flotante (coma flotante), tales como FAL, FLL, FSC, SIZE, CMP, SWPB y CPT son compatibles en los controladores 1756-L7xS pero no en los controladores 1756-L6xS y 1768-L4xS. Si su programa de seguridad contiene estas instrucciones, ocurrirán errores de verificación al cambiar de un controlador 1756-L7xS a un controlador 1756-L6xS o 1768-L4xS.

Recursos adicionales

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

Notas:

Historial de cambios

Debido a las nuevas funciones en los controladores, módulos, aplicaciones y el software RSLogix 5000, este manual se ha revisado para incluir información actualizada. Este apéndice resume brevemente los cambios hechos con respecto a cada revisión previa de este manual.

Consulte este apéndice si necesita determinar los cambios hechos en múltiples revisiones. Esto puede ser especialmente útil si usted está decidiendo actualizar su hardware o software basado en información añadida en revisiones anteriores de este manual.

1756-UM020H-EN-P Abril de 2012

Lista corregida de fuentes de alimentación eléctrica compatibles.

1756-UM020G-EN-P, Febrero de 2012

- Se añadió información sobre los controladores 1756-L7xS y 1756-L73SXT
- Se actualizó lista de recursos adicionales
- Se añadió un capítulo sobre cómo instalar el controlador
- Se añadió información sobre cómo usar las conexiones unidifusión para módulos de E/S de seguridad en redes EtherNet/IP
- Se añadió información sobre la instalación
- Se añadió información sobre protección en el modo marcha para la firma de tarea de seguridad
- Se actualizaron los procedimientos de reemplazo de E/S para incluir diversos escenarios de reemplazo
- Se actualizó el valor máximo del intervalo solicitado entre paquetes
- Se añadieron los tipos de datos DCA_INPUT y DCAF_INPUT a la lista de tipos válidos para los tags de seguridad
- Se reestructuró la información sobre los tags de seguridad producidos y consumidos y la configuración de los controladores de seguridad homólogos, de modo que toda la información aparezca junta en el Capítulo 6.
- Se añadió información sobre el impacto de una tarjeta SD bloqueada en una actualización de firmware.
- Se añadió información sobre cómo usar el módulo de almacenamiento de energía (ESM) para memoria no volátil
- Se movieron las tablas de descripción de indicadores de estado a un apéndice y se añadió información sobre la resolución de problemas

- Se actualizó la información sobre cuándo reemplazar la batería en los controladores 1756-L6xS
- Se añadió información sobre cambio a un controlador 1756-L7*x*S
- Se añadió el apéndice de Historial de cambios

1756-UM020F-EN-P, Agosto de 2010

- Los controladores GuardLogix son compatibles con RSLogix 5000, versión 19
- El tipo de conexión predeterminado para los tags de seguridad producidos y consumidos es unidifusión

1756-UM020E-EN-P, Enero de 2010

- Se añadieron instrucciones Add-On de alta integridad y de seguridad a la lista de funciones compatibles con RSLogix 5000
- Habilitación de sincronización de hora
- Se actualizaron los ejemplos de cambio del número de red de seguridad (SNN) de módulos Safety I/O en la red CIP Safety para mostrar los módulos de E/S de seguridad EtherNet/IP
- Se aclaró la información sobre el direccionamiento Ethernet
- Conexiones ControlNet para módulos de E/S distribuidas
- Definición de un tag como constante
- Establecimiento del nivel de acceso externo para datos de tags
- Procedimientos actualizados para producir y consumir tags de seguridad
- Restricción para asignación de tags de valor constante
- Tabla actualizada de respuestas de software durante la descarga
- Capacidad de acceso a GSV/SSV para objeto de seguridad AOI
- Almacenamiento y carga de proyectos usando la memoria no volátil
- Información actualizada sobre desecho de la batería
- Cambio de un controlador 1756 GuardLogix a un controlador 1768 Compact GuardLogix o viceversa

1756-UM020D-EN-P, Julio de 2008

- Se actualizó la tabla Recursos adicionales para incluir nuevos manuales
- Información acerca del controlador 1756-L63S
- Información general sobre programación usando el software RSLogix 5000, versión 17, inclusive mejoras y versiones de software compatibles
- Uso del módulo 1756-EN2T en un sistema basado en GuardLogix
- Información sobre los módulos de seguridad Guard I/O EtherNet/IP
- Se actualizó la lista de tipos de datos válidos para tags de seguridad
- Las acciones de bloqueo y desbloqueo de seguridad quedan registradas
- La creación y eliminación de la firma de seguridad quedan registradas
- El proceso de descarga ahora incluye la verificación del maestro de hora coordinada del sistema (CST)
- Se actualizó la descripción del código de fallo por tarea de seguridad inoperativa
- Se accede al valor de firma de seguridad mediante la instrucción GSV

- Se accede a información sobre tipo de datos para atributos mediante las instrucciones GSV y SSV
- Acceso a la información de fallo mediante la instrucción GSV
- Se actualizó la información sobre homologación
- Se actualizó la información sobre cómo calcular la vida útil de la batería
- Se actualizó la información sobre desecho apropiado de la batería

1756-UM020C-EN-P, Diciembre de 2006

- Descripción de las Capacidades de flujo de datos de un controlador GuardLogix
- El controlador no es compatible con actualizaciones del sistema operativo mediante CompactFlash
- La tarea de seguridad no es compatible con las instrucciones add-on ni con el software FactoryTalk® Alarms and Events
- El RPI máximo para las conexiones de seguridad cambió de 500 ms a 100 ms
- La lista de tipos de datos no válidos para los programas de seguridad se reemplazó por una lista de tipos de datos válidos
- Descripción revisada de las conexiones de tags producidos y consumidos
- Descripción revisada del efecto de la función de bloqueo de seguridad y la firma de seguridad en la operación de descarga
- Se añadió la homologación UL NRGF
- Se añadieron los valores de probabilidad de fallo a demanda (PFD) y probabilidad de fallo por hora (PFH) a las especificaciones del controlador

1756-UM020B-EN-P, Octubre de 2005

El software de programación RSLogix 5000, versión 14.01 y posteriores, ya no compara series de hardware entre el homólogo de seguridad y el controlador primario, ni entre el controlador y la firma de seguridad en el proyecto.

1756-UM020A-EN-P, Enero de 2005

Versión inicial.

Números

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X

Servicio de asistencia técnica de Rockwell Automation

Rockwell Automation proporciona información técnica en la Internet para ayudarle a utilizar sus productos. En http://www.rockwellautomation.com/support/, puede encontrar manuales técnicos, respuestas a preguntas formuladas con frecuencia, notas técnicas y de aplicación, ejemplos de códigos y vínculos a paquetes de servicio de software, además de la función MySupport que puede personalizar para aprovechar al máximo estas herramientas.

Con el fin de brindarle un nivel adicional de asistencia técnica por teléfono para la instalación, la configuración y la resolución de problemas, ofrecemos los programas de asistencia técnica TechConnect^{SM}. Para obtener más información, comuníquese con el distribuidor regional o con el representante de Rockwell Automation, o visite http://www.rockwellautomation.com/support/.

Asistencia para la instalación

Si se presenta un problema durante las 24 horas posteriores a la instalación, revise la información proporcionada en este manual. También puede llamar a un número especial de asistencia técnica para obtener ayuda inicial para la puesta en servicio del producto.

Estados Unidos o Canadá	1.440.646.3434
Fuera de los Estados Unidos o Canadá	Utilice el buscador mundial en http://www.rockwellautomation.com/support/americas/phone_en.html, o comuníquese con su representante local de Rockwell Automation.

Devolución de productos nuevos

Rockwell Automation prueba todos sus productos para asegurarse de que estén en perfecto estado de funcionamiento cuando salen de la fábrica. Sin embargo, si su producto no funciona y debe 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 en lo que respecta al proceso de devolución.

Comentarios sobre la documentación

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

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 Ciérulos 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-UM020I-ES-P – Agosto 2012