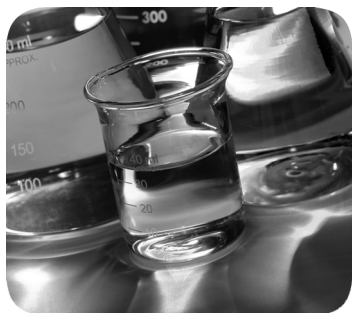


Controladores CompactLogix 5380 y Compact GuardLogix 5380

Números de catálogo 5069-L306ER, 5069-L306ERM, 5069-L310ER, 5069-L310ERM, 5069-L310ER-NSE, 5069-L310ERS2, 5069-L320ER, 5069-L320ERM, 5069-L330ER, 5069-L330ERM, 5069-L340ER, 5069-L340ERM, 5069-L350ERM, 5069-L380ERM, 5069-L3100ERM, 5069-L306ERS2, 5069-L306ERMS2, 5069-L310ERS2, 5069-L310ERMS2, 5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K, 5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K, 5069-L340ERS2, 5069-L340ERMS2, 5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K, 5069-L380ERS2, 5069-L380ERMS2, 5069-L3100ERS2, 5069-L3100ERMS2



Información importante para el usuario

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

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

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

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

Los ejemplos y los diagramas de este manual se incluyen solamente con fines ilustrativos. Debido a las numerosas variables y a los requisitos asociados con cada instalación en particular, Rockwell Automation, Inc. no puede asumir ninguna responsabilidad ni obligación por el uso basado en los ejemplos y diagramas.

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

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

Este manual contiene notas de seguridad en todas las circunstancias en que se estimen necesarias.



ADVERTENCIA: Identifica información acerca de prácticas o circunstancias que pueden causar una explosión en un ambiente peligroso que, a su vez, podría ocasionar lesiones personales o la muerte, daños materiales o pérdidas económicas.



ATENCIÓN: Identifica información acerca de prácticas o circunstancias que pueden producir lesiones personales o la muerte, daños materiales o pérdidas económicas. Estas notas de atención le ayudan a identificar un peligro, a evitarlo y a reconocer las consecuencias.

IMPORTANTE

Identifica información crítica para la correcta aplicación y la comprensión del producto.

Puede haber también etiquetas en el exterior o en el interior del equipo para señalar precauciones específicas.



PELIGRO DE CHOQUE: Puede haber etiquetas en el exterior o en el interior del equipo (por ejemplo, en un variador o un motor) para advertir sobre la posible presencia de voltajes peligrosos.



PELIGRO DE QUEMADURA: Puede haber etiquetas en el exterior o en el interior del equipo (por ejemplo, en un variador o un motor) para advertir sobre superficies que podrían alcanzar temperaturas peligrosas.



PELIGRO DE ARCO ELÉCTRICO: Puede haber etiquetas en el exterior o en el interior del equipo (por ejemplo, en un centro de control de motores) para advertir sobre un posible arco eléctrico. Los arcos eléctricos causan lesiones graves o la muerte. Use el equipo de protección personal (PPE) apropiado. Siga TODOS los requisitos normativos en lo que respecta a las prácticas de trabajo seguras y al equipo de protección personal (PPE).

	Prefacio	11
	Resumen de cambios.....	11
	Descripción general.....	11
	Recursos adicionales.....	12
	 Capítulo 1	
Sistemas y controladores	Requisitos mínimos	15
CompactLogix 5380 y Compact	Compatibilidad entre el firmware del controlador y la	
GuardLogix 5380	aplicación Logix Designer	16
	Sistema CompactLogix 5380.....	17
	Sistema controlador Compact GuardLogix 5380.....	18
	Diseño del sistema.....	20
	Características del controlador	22
	Características admitidas por los controladores Compact	
	GuardLogix 5380 a través de la tarea de seguridad	24
	Encendido del sistema	25
	 Capítulo 2	
Cómo encender los controladores	Dos tipos de alimentación eléctrica	27
CompactLogix 5380	Alimentación MOD.....	29
	Bus de alimentación MOD	29
	Alimentación SA.....	30
	Seguimiento del consumo de corriente del bus de	
	alimentación SA.....	32
	Uso de un distribuidor de potencial de campo 5069-FPD	
	para crear un nuevo bus de alimentación SA.....	34
	Alimentación SA: Notas adicionales.....	35
	 Capítulo 3	
Cómo encender los controladores	Dos tipos de alimentación eléctrica	37
Compact GuardLogix 5380	Alimentación MOD.....	39
	Bus de alimentación MOD	40
	Alimentación SA.....	40
	Seguimiento del consumo de corriente del bus de	
	alimentación SA.....	43
	Uso de un distribuidor de potencial de campo 5069-FPD	
	para crear un nuevo bus de alimentación SA.....	44
	Restricciones al conectar la alimentación SA a un sistema	
	Compact GuardLogix 5380	45
	Alimentación SA: Notas adicionales.....	48

Concepto de seguridad de los controladores Compact GuardLogix 5380

Capítulo 4

Capacidad de seguridad funcional	49
Número de red de seguridad.....	50
Firma de seguridad	51
Diferenciación entre componentes estándar y de seguridad.....	51
Capacidades de flujo de datos del controlador.....	52
Terminología de seguridad	53

Conexión al controlador

Capítulo 5

Configuración de drivers EtherNet/IP y USB en la estación de trabajo	56
Configuración del driver EtherNet/IP en el software RSLinx Classic	57
Configuración de los drivers de dispositivos Ethernet en el software RSLinx Classic.....	59
Configuración del driver de comunicación USB en el software RSLinx Classic	61
Opciones de conexión	63
Conexión de un cable Ethernet	63
Conexión de un cable USB	64
Establecimiento de la dirección IP del controlador	65
Establecimiento de la dirección IP con la herramienta de puesta en marcha BOOTP DHCP EtherNet/IP	67
Inhabilitación de BOOTP/DHCP mediante el uso del software RSLinx Classic.....	69
Uso del servidor DHCP para establecer la dirección IP del controlador	70
Uso del software RSLinx Classic para establecer la dirección IP del controlador	73
Uso de una tarjeta Secure Digital para establecer la dirección IP del controlador	74
Actualización del firmware del controlador	74
Determine el firmware del controlador necesario	75
Obtención del firmware del controlador.....	76
Uso del software ControlFLASH para actualizar el firmware.....	76
Uso de AutoFlash para actualizar el firmware	81

Cómo comenzar a usar el controlador

Capítulo 6

Creación de un proyecto en la aplicación Logix Designer.....	85
Configuración adicional para un controlador Compact GuardLogix.....	88
Asignación del número de red de seguridad (SNN)	88
Copia y pegado de un número de red de seguridad (SNN) del controlador de seguridad.....	93

Entrada en línea con el controlador	95
Uso de RSWho.....	95
Uso de una ruta de comunicación reciente	97
Consideraciones adicionales para entrar en línea con un controlador.....	98
Coincidencia del proyecto con el controlador	98
Coincidencia de la revisión de firmware	99
Consideraciones adicionales para entrar en línea con un controlador Compact GuardLogix.....	100
Firma de seguridad y estado de bloqueo y desbloqueo de seguridad	100
Comprobaciones para la entrada en línea con un controlador GuardLogix.....	101
Descarga al controlador.....	102
Uso de Who Active.....	102
Uso del menú Controller Status	103
Consideraciones adicionales con respecto a la descarga a un controlador Compact GuardLogix.....	104
Carga desde el controlador	105
Uso de Who Active.....	105
Uso del menú Controller Status	106
Consideraciones adicionales con respecto a la carga a un controlador Compact GuardLogix.....	108
Selección del modo de funcionamiento del controlador.....	109
Uso del interruptor de modo para cambiar el modo de funcionamiento	110
Uso de la aplicación Logix Designer para cambiar el modo de funcionamiento.....	111
Cambio de la configuración del controlador	112
Botón de restablecimiento	113
Restablecimiento de etapa 1	114
Restablecimiento de etapa 2	115

Capítulo 7

Uso de la tarjeta Secure Digital

Consideraciones con respecto al almacenamiento y la carga de un proyecto de seguridad.....	120
Almacenamiento en la tarjeta SD	121
Carga desde la tarjeta SD.....	125
Encendido del controlador	125
Acción iniciada por el usuario.....	126
Otras tareas con la tarjeta Secure Digital.....	128

Red EtherNet/IP

Capítulo 8

Funcionalidad de la red EtherNet/IP	130
Software para redes EtherNet/IP	131
Nodos de una red EtherNet/IP	131
Dispositivos incluidos en el conteo de nodos	132
Dispositivos excluidos del conteo de nodos	132
Topologías de red EtherNet/IP	134
Topología de red de anillo a nivel de dispositivos	134
Topología de red lineal	135
Topología de red en estrella	136
Herramientas de Integrated Architecture	136
Velocidades de comunicación de la red EtherNet/IP	137
Interface de socket	139

Capítulo 9

Uso de los modos EtherNet/IP

Niveles de red disponibles	142
Red a nivel de empresa	142
Red a nivel de dispositivo	143
Modos EtherNet/IP	143
Modo de doble IP	143
Modo lineal/DLR	147
Solapamiento de rangos de direcciones IP	149
Configuración de los modos EtherNet/IP	150
Configuración del modo de doble IP en la aplicación	
Logix Designer	150
Configuración del modo de doble IP en el software	
RSLinx Classic	152
Configuración del modo lineal/DLR en la aplicación	
Logix Designer	154
Configuración del modo lineal/DLR en el software	
RSLinx Classic	156
Cambio del modo EtherNet/IP	158
Cambio del modo EtherNet/IP en la aplicación	
Logix Designer	159
Cambio del modo EtherNet/IP en el software	
RSLinx Classic	161
Solicitudes DNS	164
Encaminamiento de solicitudes DNS	164
Servidor SMTP	165
Uso de objetos de socket	165
Instrucciones de envío de mensajes	165
Diferencias de visualización del software para los modos	
EtherNet/IP	166
Dirección IP del controlador y actualizaciones del firmware	168

Administración de comunicaciones del controlador	Capítulo 10	
	Descripción general de la conexión.....	171
	Interacción de comunicación del controlador con datos de control	172
	Producción y consumo de datos (de enclavamiento)	173
	Intervalo solicitado entre paquetes (RPI) de tags de multidifusión	174
	Envío y recepción de mensajes	175
	Determinación de si se dejarán en caché las conexiones de los mensajes	176
Módulos de E/S estándar	Capítulo 11	
	Módulos de E/S locales	177
	Adición de módulos de E/S locales a un proyecto	179
	Codificación electrónica	184
	Módulos de E/S remotos.....	185
	Adición de módulos de E/S remotos a un proyecto	187
	Adición a la configuración de E/S estando en línea	195
	Módulos y dispositivos que se pueden añadir estando en línea	195
	Determinación de cuándo se actualizan los datos	196
	Diagrama de flujo de actualización de datos de entrada.....	196
Diagrama de flujo de actualización de datos de salida.....	197	
Dispositivos de E/S de seguridad	Capítulo 12	
	Adición de dispositivos de E/S de seguridad	199
	Configuración de dispositivos de E/S de seguridad	200
	Uso del traductor de direcciones de red (NAT) con dispositivos CIP Safety	202
	Establecimiento del SNN de un dispositivo de E/S de seguridad	204
	Cambio del SNN de un dispositivo de E/S de seguridad.....	204
	Copia y pegado de un número de red de seguridad (SNN) de dispositivo de E/S de seguridad.....	206
	Límite de tiempo de reacción de la conexión	208
	Firma de dispositivo de E/S de seguridad	209
	Configuración mediante la aplicación Logix Designer.....	209
	Restablecimiento del dispositivo de E/S de seguridad a la condición original	210
	Formato de dirección de dispositivo de E/S.....	211
	Sustitución del dispositivo de E/S de seguridad	212
	Propiedad de la configuración	212
	Reemplazo con “Configure Only When No Safety Signature Exists” habilitado	214
	Reemplazo con “Configure Always” habilitado.....	219

Desarrollo de aplicaciones estándar

Capítulo 13

Elementos de una aplicación de control	221
Tareas	223
Tarea de evento con módulos de E/S Compact 5000	225
Prioridad de las tareas	227
Programas	228
Programas priorizados y no priorizados	229
Rutinas	230
Parámetros y tags locales	231
Parámetros de programa	232
Lenguajes de programación	232
Instrucciones Add-On	233
Propiedades extendidas	234
Acceso al objeto del módulo desde una instrucción Add-On	235
Monitoreo del estado del controlador	236
Monitoreo de las conexiones de E/S	237
Determinación de si la comunicación de E/S ha sobrepasado el tiempo de espera	237
Determinación de si la comunicación de E/S a un módulo de E/S específico sobrepasó el tiempo de espera	238
Gestión automática de fallos de conexión de módulo de E/S	238
Ejemplos de proyectos de controlador	239

Desarrollo de aplicaciones de seguridad

Capítulo 14

Tarea de seguridad	242
Período de la tarea de seguridad	243
Ejecución de la tarea de seguridad	244
Programas de seguridad	244
Rutinas de seguridad	244
Instrucciones Add-On de seguridad	245
Tags de seguridad	245
Tipos de datos válidos	246
Alcance	246
Parámetros de programa	247
Tags de seguridad producidos/consumidos	247
Configuración del SNN para una conexión del controlador de seguridad homólogo	248
Producción de un tag de seguridad	252
Consumo de datos de tag de seguridad	253
Asignación de un tag de seguridad	256
Restricciones	256
Creación de pares de asignación de tags	257
Monitoreo del estado de la asignación de un tag	258
Protección de la aplicación de seguridad	259
Bloqueo de seguridad del controlador Compact GuardLogix 5380	259

Establecimiento de contraseñas para el bloqueo y desbloqueo de seguridad.....	261
Generación de la firma de seguridad.....	262
Restricciones de programación.....	265
Monitoreo del estado de seguridad.....	266
Ver el estado mediante la barra en línea.....	266
Visualización del estado en la ficha Safety.....	268
Monitoreo de las conexiones de seguridad.....	269
Utilización del estado.....	270
Fallos de seguridad.....	272
Fallos de controlador no recuperables.....	272
Fallos de seguridad no recuperables en la aplicación de seguridad.....	272
Fallos recuperables en la aplicación de seguridad.....	273
Visualización de fallos.....	273
Códigos de fallo.....	274
Desarrollo de una rutina de fallo para aplicaciones de seguridad.....	275
Uso de las instrucciones GSV/SSV en una aplicación de seguridad.....	276

Capítulo 15

Desarrollo de aplicaciones de movimiento

Descripción general del control de movimiento.....	278
Programación del control de movimiento.....	279
Obtención de información de los ejes.....	281

Capítulo 16

Resolución de problemas del controlador

Diagnóstico del controlador con Logix Designer.....	283
Símbolo de advertencia en el árbol de configuración de E/S... ..	284
Categorías del cuadro de diálogo I/O Module Properties.....	285
Notificación en el Tag Monitor.....	289
Información de fallo en el cuadro de diálogo Controller Properties.....	289
Diagnóstico de puertos.....	291
Advanced Time Sync.....	293
Diagnóstico de controlador con software basado en Linx.....	296
Páginas web del controlador.....	297
Página web Home.....	298
Página web Tasks.....	299
Páginas web Diagnostics.....	300
Páginas web Ethernet Port.....	301
Páginas web Advanced Diagnostics.....	302
Página web Browse Chassis.....	304
Otros posibles problemas que puede ser necesario resolver.....	305
Tarea continua envía datos de salida a alta velocidad.....	305
Instrucciones de salida inmediata enviadas a alta velocidad ...	305
Movimiento integrado en una red EtherNet/IP con estado de prioridad del tráfico.....	305

Indicadores de estado	Apéndice A
	Pantalla de estado e indicadores. 308
	Mensajes de estado general 309
	Mensajes de estado de Compact GuardLogix 311
	Mensajes de fallo 311
	Mensajes de fallo mayor..... 312
	Códigos de fallo de E/S 314
	Indicadores de estado del controlador 317
	Indicador RUN 317
	Indicador FORCE..... 317
	Indicador SD..... 318
	Indicador OK 318
	Indicadores de estado de EtherNet/IP..... 319
	Indicadores NET A1 y NET A2 319
	Indicadores LINK A1 y LINK A2 319
	Indicadores de estado de alimentación..... 320
	Indicador de alimentación MOD 320
	Indicador de alimentación SA 320
	Monitoreo térmico y comportamiento ante fallo térmico 321
Opciones de seguridad	Apéndice B
	Inhabilitación de un puerto Ethernet 323
	Inhabilitación del puerto Ethernet en la ficha Port Configuration..... 324
	Inhabilitación del puerto Ethernet mediante una instrucción MSG 325
	Inhabilitación de la pantalla de estado de 4 caracteres..... 327
	Inhabilitación de todas las categorías de mensajes..... 328
	Inhabilitación de categorías individuales de mensajes 330
	Inhabilitación de páginas web del controlador 332
Cambio del tipo de controlador	Apéndice C
	Cambio de un controlador estándar a un controlador de seguridad 335
	Cambio de un controlador de seguridad a uno estándar..... 336
	Cambio de los tipos de controlador de seguridad 336
	Índice 337

Resumen de cambios

Este manual contiene información nueva y actualizada según se indica en la siguiente tabla.

Tema	Página
Se añadió información del Compact GuardLogix® 5380 e información de seguridad	Todo el documento
Capítulo 3, Cómo encender los controladores Compact GuardLogix 5380	37
Capítulo 4, Concepto de seguridad de los controladores Compact GuardLogix 5380	49
Capítulo 12, Dispositivos de E/S de seguridad	199
Capítulo 14, Desarrollo de aplicaciones de seguridad	241

Descripción general

Este manual proporciona información sobre cómo diseñar un sistema, hacer funcionar un sistema controlador basado en CompactLogix™ o en Compact GuardLogix y desarrollar aplicaciones.

Usted debe haber recibido la capacitación y tener la experiencia en la creación, operación y mantenimiento de sistemas de seguridad.

Para obtener información sobre los requisitos del nivel de integridad de seguridad (SIL) y del nivel de rendimiento (PL), y los requisitos de las aplicaciones de seguridad, vea el documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#).

Recursos adicionales

Estos documentos contienen información adicional sobre productos relacionados de Rockwell Automation.

Tabla 1 – Recursos adicionales

Recurso	Descripción
Instalación de hardware	Controladores CompactLogix 5380 – Instrucciones de instalación, publicación 5069-IN013
	Controladores Compact GuardLogix 5380 SIL 2 – Instrucciones de instalación, publicación 5069-IN014
	Pautas de cableado y conexión a tierra de automatización industrial para inmunidad de ruido, publicación 1770-4.1
Datos técnicos	Compact 5000 I/O Modules Specifications Technical Data, publicación 5069-TD001
	CompactLogix 5380 and Compact GuardLogix 5380 Controllers Specifications Technical Data, publicación 5069-TD002
Redes	Módulos de comunicación EtherNet/IP en los sistemas de control Logix5000 – Manual del usuario, publicación ENET-UM004
	Guidance for Selecting Cables for EtherNet/IP Networks, publicación ENET-WP007-EN-P
CIP Sync (sincronización de tiempo)	Integrated Architecture and CIP Sync Configuration Application Technique, publicación IA-AT003
Requisitos de las aplicaciones de seguridad	Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación 1756-RM012
Movimiento	Sistema de coordenadas de movimiento – Manual de usuario, publicación MOTION-UM002
	Configuración y puesta en marcha del movimiento integrado en la red EtherNet/IP – Manual del usuario, publicación MOTION-UM003
	Movimiento integrado en la red EtherNet/IP – Manual de referencia, publicación MOTION-RM003
	Logix 5000 Controllers Motion Instructions Reference Manual, publicación MOTION-RM002
Consideraciones de diseño	Logix 5000 Controllers Design Considerations Reference Manual, publicación 1756-RM094
	Ethernet Design Considerations Reference Manual, publicación ENET-RM002
	Replacement Guidelines: Logix 5000 Controllers Reference Manual, publicación 1756-RM100
	CompactLogix System Selection Guide, publicación 1769-SG001
Tareas y procedimientos de programación	Logix 5000 Controllers Common Procedures Programming Manual, publicación 1756-PM001
	Logix 5000 Controllers General Instructions Reference Manual, publicación 1756-RM003
	GuardLogix Safety Application Instruction Set Reference Manual, publicación 1756-RM095
Módulos digitales y de seguridad Compact 5000	Compact 5000 Digital and Safety I/O Modules User Manual, publicación 5000-UM004
	5000 Series Analog I/O Module User Manual, publicación 5000-UM005
	5000 Series High-speed Counter Module User Manual, publicación 5000-UM006

Tabla 1 – Recursos adicionales

Recurso		Descripción
Módulos Guard I/O	Guard I/O DeviceNet Safety Modules User Manual, publicación 1791DS-UM001	Proporciona información sobre cómo usar los módulos de seguridad DeviceNet Guard I/O™, incluyendo los módulos de E/S 1732DS y 1791DS.
	Guard I/O EtherNet/IP Safety Modules User Manual, publicación 1791ES-UM001	Proporciona información sobre cómo usar los módulos de seguridad EtherNet/IP Guard I/O, incluidos los módulos de E/S 1732ES y 1791ES.
	Módulos de seguridad POINT Guard I/O – Manual del usuario, publicación 1734-UM013	Proporciona información sobre cómo usar los módulos POINT Guard I/O™.
Variadores	Servovariadores Kinetix 5500 – Manual del usuario, publicación 2198-UM001	Proporciona información sobre cómo usar un sistema servovariador Kinetix 5500. También incluye los requisitos para utilizar variadores Kinetix 5500 en aplicaciones de seguridad.
	Servovariadores Kinetix 5700 – Manual de usuario, publicación 2198-UM002	Proporciona información sobre cómo usar un sistema servovariador Kinetix® 5700. También incluye los requisitos para utilizar variadores Kinetix 5700 en aplicaciones de seguridad.
	Variador de CA de frecuencia ajustable PowerFlex 527 – Manual del usuario, publicación 520-UM002	Proporciona información sobre cómo usar un variador de CA de frecuencia ajustable de serie 520 PowerFlex®.
Certificaciones de productos	Sitio web de certificaciones de productos, http://www.rockwellautomation.com/global/certification/overview.page	Presenta declaraciones de conformidad, certificados y otros detalles de certificación.

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

Notas:

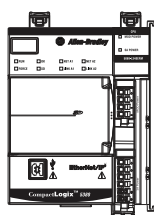
Sistemas y controladores CompactLogix 5380 y Compact GuardLogix 5380

Este capítulo describe las características y funciones asociadas con los controladores CompactLogix® 5380 y Compact GuardLogix® 5380.

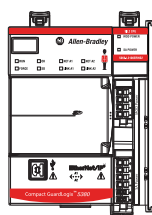
Tema	Página
Requisitos mínimos	15
Sistema CompactLogix 5380	17
Sistema controlador Compact GuardLogix 5380	18
Diseño del sistema	20
Características del controlador	22
Encendido del sistema	25

Requisitos mínimos

CompactLogix



Compact GuardLogix



Los controladores tienen requisitos mínimos.

- Los controladores CompactLogix™ 5380 y Compact GuardLogix® 5380 tienen requisitos de hardware mínimos. Para obtener más información sobre los requisitos de hardware, vea la [Tabla 2 en la página 20](#).
- La revisión de firmware del controlador debe ser compatible con la versión de software utilizada. Para obtener más información, consulte la [página 16](#).
- Software de programación

Sistema	N.º de cat.	Aplicación Studio 5000 Logix Designer ⁽¹⁾
CompactLogix	5069-L320ER, 5069-L340ERM	Versión 28.00.00 y posteriores
CompactLogix	5069-L306ER, 5069-L306ERM, 5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM, 5069-L320ERM, 5069-L330ER, 5069-L330ERM, 5069-L340ER	Versión 29.00.00 y posteriores
CompactLogix	5069-L350ERM, 5069-L380ERM, 5069-L3100ERM	Versión 30.00.00 y posteriores
Compact GuardLogix	5069-L306ERS2, 5069-L306ERMS2, 5069-L310ERS2, 5069-L310ERMS2, 5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K, 5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K, 5069-L340ERS2, 5069-L340ERMS2, 5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K, 5069-L380ERS2, 5069-L380ERMS2, 5069-L3100ERS2, 5069-L3100ERMS2	Versión 31.00.00 y posteriores

(1) Para obtener el software de comunicación basado en Linux y el software ControlFLASH™ compatibles, visite el [Centro de compatibilidad y descarga de productos \(PCDC\)](#).

IMPORTANTE Si para su aplicación se requieren conexiones de seguridad o lógica de seguridad, hay que utilizar un controlador Compact GuardLogix.

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

El envoltente debe tener las debidas propiedades retardadoras de llamas para evitar o minimizar la propagación de llamas, y satisfacer la clasificación de dispersión de llamas de 5VA o estar aprobado para la aplicación si no fuese metálico. El acceso al interior del envoltente solo podrá ser posible mediante el uso de una herramienta.

Para obtener más información sobre clasificaciones de tipos de envoltentes específicos requeridos para cumplir las certificaciones de seguridad de productos, consulte el documento Controladores Compact GuardLogix 5380 – Instrucciones de instalación, publicación [5069-IN014](#).

Residuos de aparatos eléctricos y electrónicos (RAEE)



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

Compatibilidad entre el firmware del controlador y la aplicación Logix Designer

En los sistemas de control Logix 5000™, el firmware del controlador y la aplicación Logix Designer deben tener el mismo nivel de revisión mayor. Por ejemplo, si la revisión del firmware del controlador es la 31.xxx, deberá utilizar la versión 31 de la aplicación Logix Designer.

Hay requisitos mínimos en lo que respecta a la versión de software de las aplicaciones de software que puede utilizar en su sistema.

Las versiones de software compatibles han sido probadas juntas para verificar que funcionan adecuadamente. Las versiones de software no identificadas como compatibles la una con la otra no han sido probadas juntas y no se garantiza su funcionamiento.

Para obtener más información sobre las revisiones de firmware del controlador y los requisitos mínimos de las aplicaciones de software, visite el Centro de compatibilidad y descarga de productos (PCDC) de Rockwell Automation®, disponible en: <http://compatibility.rockwellautomation.com/Pages/home.aspx>

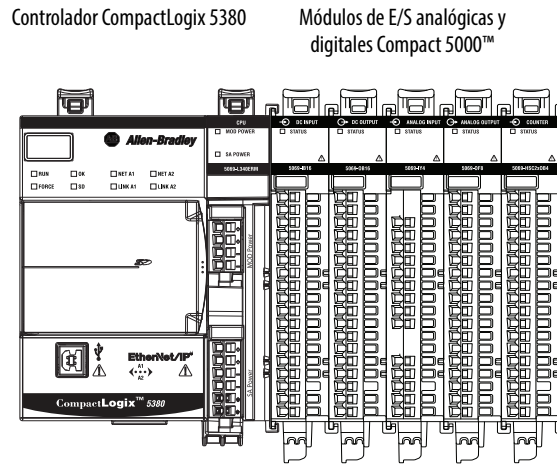
En el PCDC:

- La sección Download tiene el firmware para su controlador.
- La sección Compare tiene información sobre la compatibilidad de software para aplicaciones de software utilizadas en un sistema de control CompactLogix 5380 y Compact GuardLogix 5380.

Sistema CompactLogix 5380

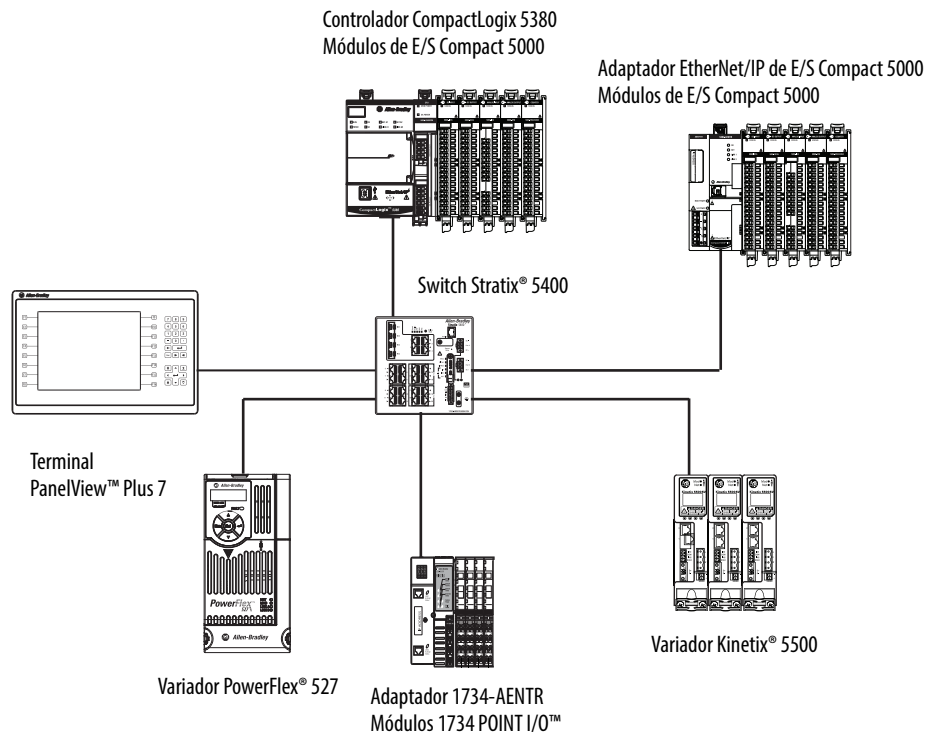
Los sistemas de control CompactLogix 5380 son sistemas para montaje en riel DIN que pueden funcionar en diversas aplicaciones, incluyendo sistemas autónomos que contienen módulos de E/S estándar, tal como se muestra en la [Figura 1](#).

Figura 1 – Controlador CompactLogix 5380 en un sistema autónomo



Los controladores también pueden funcionar en sistemas más complejos con dispositivos conectados al controlador mediante una red EtherNet/IP, tal como se muestra en la [Figura 2](#).

Figura 2 – Controlador CompactLogix 5380 en un sistema más complejo



Sistema controlador Compact GuardLogix 5380

El sistema Compact GuardLogix puede comunicarse con dispositivos de E/S de seguridad a través de CIP Safety mediante una red EtherNet/IP (módulos Guard I/O™, variadores de seguridad integrada, componentes de seguridad integrada).

El uso de un controlador Compact GuardLogix le permite conectarse a E/S estándar a través de tareas estándar y a la vez conectarse a E/S de seguridad mediante la tarea de seguridad.

IMPORTANTE En el caso de la tarea de seguridad, los controladores Compact GuardLogix 5380 admiten solo el diagrama de lógica de escalera.

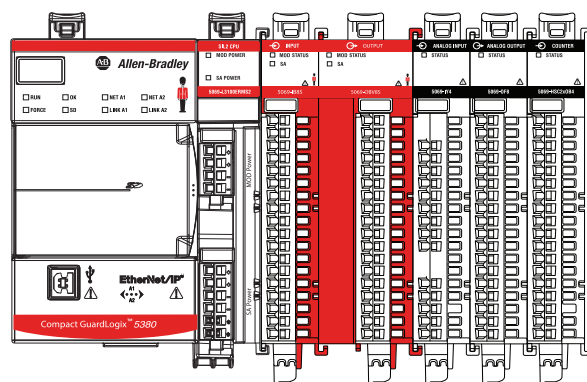
En el caso de tareas estándar, los controladores Compact GuardLogix 5380 admiten:

- Diagrama de lógica de escalera (LD)
- Texto estructurado (ST)
- Diagrama de bloques de funciones (FBD)
- Diagrama de funciones secuenciales (SFC)

Los controladores pueden funcionar en diversas aplicaciones que incluyen sistemas autónomos con módulos de E/S locales, tal como se muestra en la [Figura 3](#).

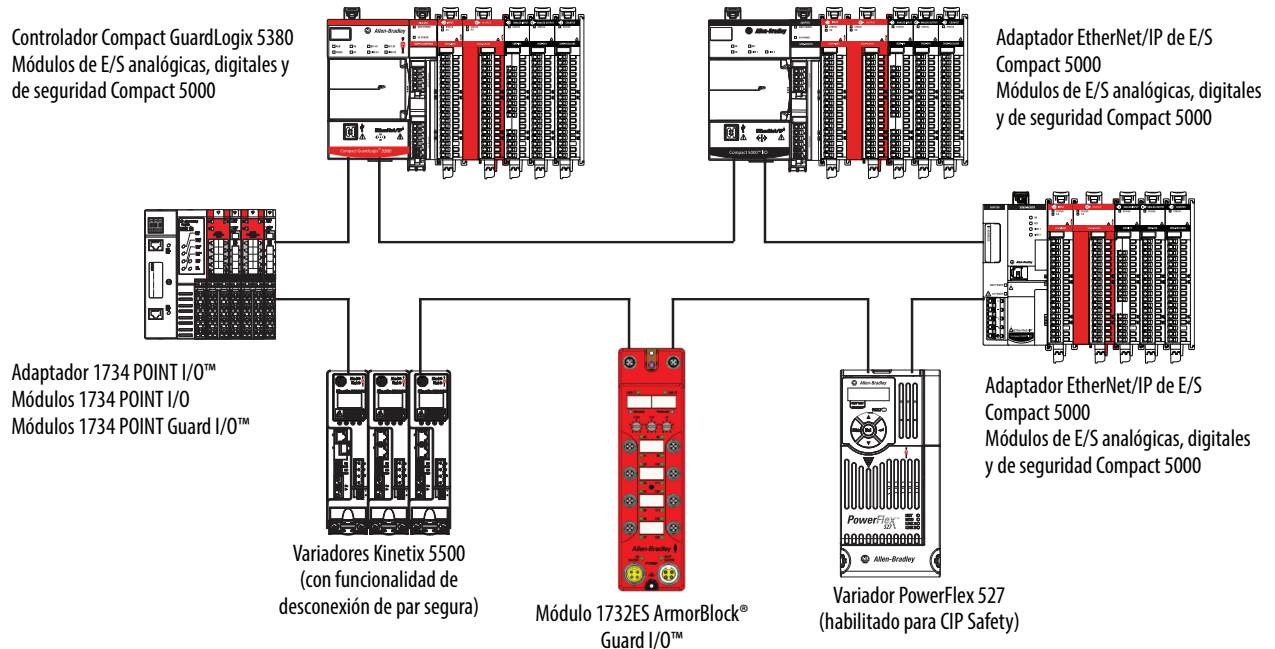
Figura 3 – Controlador Compact GuardLogix 5380 en un sistema autónomo

Controlador Compact GuardLogix 5380 Módulos de E/S analógicas estándar, digitales estándar y digitales de seguridad Compact 5000



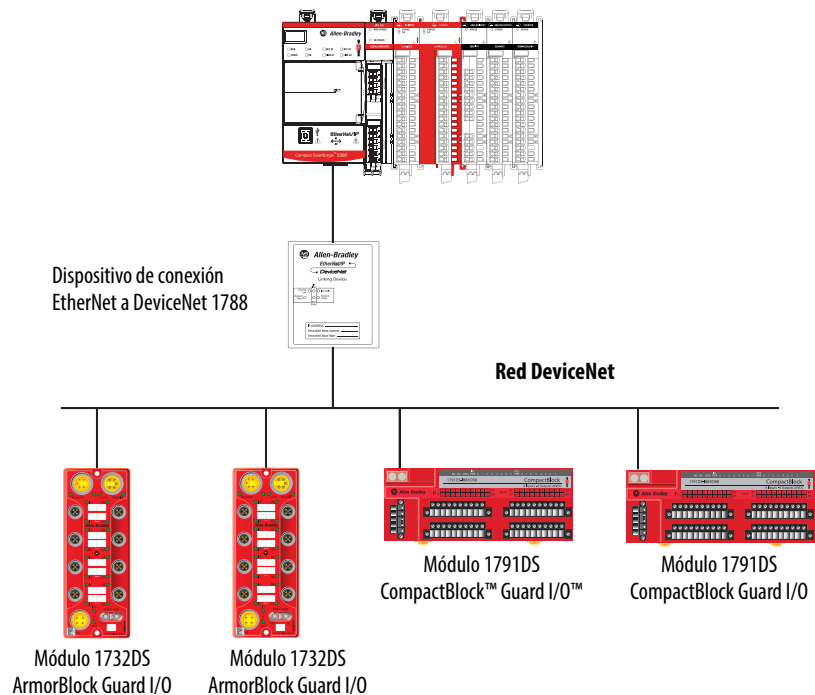
Los controladores también pueden funcionar en sistemas más complejos con dispositivos conectados al controlador mediante una red EtherNet/IP, tal como se muestra en la [Figura 4](#).

Figura 4 – Controlador Compact GuardLogix 5380 en una red EtherNet/IP DLR



Los controladores Compact GuardLogix 5380 pueden comunicarse con dispositivos de seguridad en una red DeviceNet a través de un dispositivo de seguridad mediante un dispositivo de conexión 1788-EN2DN, tal como se muestra en la [Figura 5](#).

Figura 5 – Controlador Compact GuardLogix 5380 conectado a dispositivos en una red DeviceNet



Diseño del sistema

Al diseñar un sistema, hay que determinar qué componentes de sistema necesita su aplicación. La [Tabla 2](#) describe los componentes utilizados comúnmente en los sistemas de control CompactLogix 5380 y Compact GuardLogix 5380.

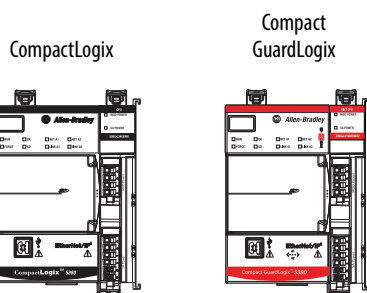


Tabla 2 – Componentes del sistema

Componente	Finalidad	Requerido	Para más información
Riel DIN	Sistema de montaje	Sí	<ul style="list-style-type: none"> Controladores CompactLogix 5380 – Instrucciones de instalación, publicación 5069-IN013 Controladores Compact GuardLogix 5380 – Instrucciones de instalación, publicación 5069-IN014
Tapa de extremo (5069-ECR) IMPORTANTE: La tapa de extremo se envía junto con el controlador.	La tapa de extremo cubre las interconexiones expuestas en el último módulo del sistema. Si no se coloca la tapa de extremo antes de encender el sistema, pueden producirse daños al equipo o lesiones personales por choque eléctrico. IMPORTANTE: La tapa de extremo se instala después de instalar el último módulo en el riel DIN. Este diseño ayuda a evitar que la tapa de extremo se desplace más allá de la posición bloqueada. Si empuja la tapa de extremo más allá de la posición bloqueada o si la inserta al revés, se puede dañar el bus de alimentación MOD y el conector del bus de alimentación SA.	Sí	
Bloques de terminales extraíbles (RTB)	Conectar al controlador estos tipos de alimentación eléctrica: <ul style="list-style-type: none"> Alimentación MOD Alimentación SA 	Sí	
Fuente de alimentación eléctrica externa ⁽¹⁾	Proporciona alimentación eléctrica de módulo (MOD) al sistema	Sí	
Fuente de alimentación eléctrica externa ⁽¹⁾	Proporciona alimentación eléctrica de sensor/ accionador (SA) al sistema	Sí; solo si el sistema requiere alimentación SA. Si el sistema no requiere alimentación SA, no se necesita una fuente de alimentación eléctrica externa.	Encendido del sistema en la página 25
Aplicación Studio 5000 Logix Designer	Configurar el proyecto utilizado para definir la actividad del controlador durante el funcionamiento del sistema	Sí	<ul style="list-style-type: none"> Requisitos mínimos en la página 15 Creación de un proyecto en la aplicación Logix Designer en la página 85
Software de comunicación basado en Linx	Se utiliza para lo siguiente: <ul style="list-style-type: none"> Asignar una dirección IP al controlador Mantener la comunicación a través de la red EtherNet/IP 	Sí	<ul style="list-style-type: none"> Para obtener el software de comunicación basado en Linx compatible, visite el Centro de compatibilidad y descarga de productos (PCDC). Conexión al controlador en la página 55
Software ControlFLASH™	Actualice el firmware del controlador	Sí	<ul style="list-style-type: none"> Para obtener el software ControlFLASH™ compatible, visite el Centro de compatibilidad y descarga de productos (PCDC). Actualización del firmware del controlador en la página 74
Puerto de programación USB	Llevar a cabo tareas que solo requieran una conexión temporal al controlador, por ej., al descargar un proyecto o al actualizar firmware	—	Conexión de un cable USB en la página 64
Puerto Ethernet A1	Conectar a redes a nivel de dispositivo	—	Capítulo 9, Uso de los modos EtherNet/IP en la página 141
Puerto Ethernet A2	Se conecta a estos tipos de redes: <ul style="list-style-type: none"> Red a nivel de empresa Red a nivel de dispositivos 	—	

Tabla 2 – Componentes del sistema

Componente	Finalidad	Requerido	Para más información
Tarjeta Secure Digital (SD) IMPORTANTE: La tarjeta 1784-SD2 se envía junto con el controlador.	Almacenar datos, como el proyecto del controlador y los diagnósticos requeridos por el grupo de asistencia técnica para obtener información si se producen fallos de controlador no recuperables.	Recomendamos dejar instalada la tarjeta SD para que en caso de ocurrir un fallo los datos de diagnóstico se escriban automáticamente en la tarjeta.	Uso de la tarjeta Secure Digital en la página 117
Cables Ethernet	Se utilizan para lo siguiente: <ul style="list-style-type: none"> Obtener acceso al controlador desde la estación de trabajo a través de una red EtherNet/IP para establecer la dirección IP, actualizar el firmware, descargar y cargar proyectos Conectar el controlador a una red EtherNet/IP y llevar a cabo las tareas necesarias para el funcionamiento normal 	Sí.	Conexión de un cable Ethernet en la página 63
Cable USB	Obtener acceso al controlador directamente desde la estación de trabajo para establecer la dirección IP, actualizar el firmware, descargar y cargar proyectos. El puerto USB está concebido solamente para fines de programación local temporal, no para conexión permanente.	Sí. Solo si realiza tareas enumeradas en la columna anterior mediante el puerto USB. También es posible realizar las tareas mediante los puertos Ethernet del controlador.	Conexión de un cable USB en la página 64
Dispositivos de E/S de seguridad integrada en una red EtherNet/IP	Conectados a dispositivos de entrada y salida de seguridad, como por ej., módulos de seguridad de E/S Compact 5000 o la caja de acceso multifuncional Guardmaster®. IMPORTANTE: Los controladores CompactLogix 5380 no pueden utilizar dispositivos de seguridad.	Sí, en el caso de controladores Compact GuardLogix 5380.	Dispositivos de E/S de seguridad en la página 199
Módulos de E/S Compact 5000™	Se utilizan para lo siguiente: <ul style="list-style-type: none"> Módulos de E/S locales estándar que están instalados en el sistema CompactLogix 5380 Módulos de E/S remotos estándar a los cuales se puede acceder a través de una red EtherNet/IP Módulos de E/S locales de seguridad que están instalados en el sistema CompactLogix 5380 Módulos de E/S remotos de seguridad a los cuales se puede acceder a través de una red EtherNet/IP 	Sí	<ul style="list-style-type: none"> Módulos de E/S estándar en la página 177 Dispositivos de E/S de seguridad en la página 199
Dispositivos instalados en una red EtherNet/IP	Depende del tipo de dispositivo. Entre los ejemplos se incluyen: <ul style="list-style-type: none"> Módulos de E/S remotos estándar Módulos de E/S remotos de seguridad Switches Ethernet Dispositivos de control de movimiento, como variadores Dispositivos HMI 	Sí.	<ul style="list-style-type: none"> Módulos de E/S estándar en la página 177 Dispositivos de E/S de seguridad en la página 199 Desarrollo de aplicaciones de movimiento en la página 277

(1) Recomendamos encarecidamente utilizar fuentes de alimentación eléctrica externas independientes para la alimentación MOD y SA, respectivamente.

Características del controlador

La [Tabla 3](#) enumera las características disponibles en los controladores. Las características se describen en el resto del presente manual.

Tabla 3 – Características de controladores CompactLogix 5380 y Compact GuardLogix 5380

Característica	Controladores CompactLogix 5380	Controladores Compact GuardLogix 5380	Valor
Memoria de usuario	5069-L306ER, 5069-L306ERM	5069-L306ERS2, 5069-L306ERMS2	0.6 MB
	5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM	5069-L310ERS, 5069-L310ERMS2	1 MB
	5069-L320ER, 5069-L320ERM	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K	2 MB
	5069-L330ER, 5069-L330ERM	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K	3 MB
	5069-L340ER, 5069-L340ERM	5069-L340ERS2, 5069-L340ERMS2	4 MB
	5069-L350ERM	5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K	5 MB
	5069-L380ERM	5069-L380ERS2, 5069-L380ERMS2	8 MB
	5069-L3100ERM	5069-L3100ERS2, 5069-L3100ERMS2	10 MB
Memoria de seguridad	—	5069-L306ERS2, 5069-L306ERMS2	0.3 MB
	—	5069-L310ERS2, 5069-L310ERMS2	0.5 MB
	—	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K	1 MB
	—	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K	1.5 MB
	—	5069-L340ERS2, 5069-L340ERMS2	2 MB
	—	5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K	2.5 MB
	—	5069-L380ERS2, 5069-L380ERMS2	4 MB
	—	5069-L3100ERS2, 5069-L3100ERMS2	5 MB
Tareas del controlador	<ul style="list-style-type: none"> • 32 tareas • IMPORTANTE: Los controladores Compact GuardLogix 5380 aceptan una tarea de seguridad. La tarea de seguridad se incluye en las 32 tareas disponibles en total con los controladores Compact GuardLogix 5380. Como resultado, los controladores Compact GuardLogix 5380 aceptan 31 tareas estándar. • 1,000 programas/tarea • Tareas de eventos; todos los activadores de eventos 		
Puertos de comunicación	<ul style="list-style-type: none"> • 1 puerto USB, 2.0 velocidad completa, tipo B • 2 puertos EtherNet/IP incorporados, 10 Mbps, 100 Mbps, 1 Gbps 		
Topologías de red EtherNet/IP admitidas	<ul style="list-style-type: none"> • Anillo a nivel de dispositivos (DLR) • Estrella • Lineal 		
Nodos EtherNet/IP admitidos, máx. ⁽¹⁾	5069-L306ER, 5069-L306ERM	5069-L306ERS2, 5069-L306ERMS2	16
	5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM	5069-L310ERS2, 5069-L310ERMS2	24
	5069-L320ER, 5069-L320ERM	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K	40
	5069-L330ER, 5069-L330ERM	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K	60
	5069-L340ER, 5069-L340ERM	5069-L340ERS2, 5069-L340ERMS2	90
	5069-L350ERM	5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K	120
	5069-L380ERM	5069-L380ERS2, 5069-L380ERMS2	150
	5069-L3100ERM	5069-L3100ERS2, 5069-L3100ERMS2	180

Tabla 3 – Características de controladores CompactLogix 5380 y Compact GuardLogix 5380 (continuación)

Característica	Controladores CompactLogix 5380	Controladores Compact GuardLogix 5380	Valor
Modos EtherNet/IP	<ul style="list-style-type: none"> • Modo lineal/DLR • Modo de doble IP: disponible con la aplicación Logix Designer, versión 29.00.00 y posteriores. 		
Ejes de movimiento integrado admitidos IMPORTANTE: No todos los controladores CompactLogix 5380 o Compact GuardLogix 5380 admiten movimiento integrado en una red EtherNet/IP. Solo los controladores con la letra 'M' en el número de catálogo admiten control de movimiento.	5069-L306ERM	5069-L306ERMS2	2
	5069-L310ERM	5069-L310ERMS2	4
	5069-L320ERM	5069-L320ERMS2, 5069-L320ERMS2K	8
	5069-L330ERM	5069-L330ERMS2, 5069-L330ERMS2K	16
	5069-L340ERM	5069-L340ERMS2	20
	5069-L350ERM	5069-L350ERMS2, 5069-L350ERMS2K	24
	5069-L380ERM	5069-L380ERMS2	28
	5069-L3100ERM	5069-L3100ERMS2	32
Módulos de E/S locales, máx.	5069-L306ER, 5069-L306ERM, 5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM	5069-L306ERMS2, 5069-L306ERS2, 5069-L310ERS2, 5069-L310ERMS2	8
	5069-L320ER, 5069-L320ERM	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K	16
	5069-L330ER ⁽²⁾ , 5069-L330ERM ⁽²⁾ , 5069-L340ER, 5069-L340ERM, 5069-L350ERM, 5069-L380ERM, 5069-L3100ERM	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K, 5069-L340ERS2, 5069-L340ERMS2, 5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K, 5069-L380ERS2, 5069-L380ERMS2, 5069-L3100ERS2, 5069-L3100ERMS2	31
Lenguajes de programación	<ul style="list-style-type: none"> • Diagrama de lógica de escalera (LD) • Texto estructurado (ST) • Diagrama de bloques de funciones (FBD) • Diagrama de funciones secuenciales (SFC) 	<ul style="list-style-type: none"> • En el caso de la tarea de seguridad, los controladores Compact GuardLogix admiten solo el diagrama de lógica de escalera. • En el caso de tareas estándar, los controladores Compact GuardLogix admiten: <ul style="list-style-type: none"> – Diagrama de lógica de escalera (LD) – Texto estructurado (ST) – Diagrama de bloques de funciones (FBD) – Diagrama de funciones secuenciales (SFC) 	
Características de controlador admitidas	<ul style="list-style-type: none"> • Control de acceso a datos • Supervisor de firmware • Tarjeta Secure Digital (SD) • Conexiones estándar 	<ul style="list-style-type: none"> • Control de acceso a datos • Supervisor de firmware • Tarjeta Secure Digital (SD) • Conexiones estándar • Conexiones de seguridad 	

(1) Un nodo es un dispositivo EtherNet/IP que se añade directamente a la configuración de E/S y se cuenta al determinar los límites de nodos del controlador. Para obtener más información sobre los modos EtherNet/IP, consulte la [página 131](#).

(2) Al utilizar este controlador con la aplicación Logix Designer, versión 29.00.00, la aplicación limita el número de módulos de E/S locales del proyecto a 16. Para obtener más información, consulte el artículo n.º 942580 de la Knowledgebase de Rockwell Automation®, "5380 CompactLogix controllers limited to 16 local Compact 5000 I/O modules in V29 of Studio 5000". El documento está disponible en <http://www.rockwellautomation.com/knowledgebase>.
Con la aplicación Logix Designer, versión 30.00.00 y posteriores, el controlador admite hasta 31 módulos de E/S locales.

IMPORTANTE Al utilizar un controlador CompactLogix 5380 o Compact GuardLogix 5380, no es necesario configurar un valor para el segmento del tiempo de procesamiento interno del sistema.

Características admitidas por los controladores Compact GuardLogix 5380 a través de la tarea de seguridad

Puede utilizar los controladores Compact GuardLogix 5380 en aplicaciones de seguridad SIL 2/PLd mediante la tarea de seguridad en la aplicación Logix Designer.

En la aplicación Logix Designer, versión 31 y posteriores, la tarea de seguridad admite un subconjunto de características aceptadas en la tarea estándar tal como se enumera en esta tabla.

Característica	Aplicación Studio 5000 Logix Designer, versión 31 y posteriores	
	Tarea de seguridad	Tarea estándar
Instrucciones Add-On	X	X
Alarmas y eventos basados en instrucciones	—	X
Alarmas basadas en tags	—	X
Función de registro del controlador	X	X
Tareas de eventos ⁽¹⁾	—	X
Diagramas de bloques de funciones (FBD)	—	X
Movimiento integrado	X ⁽²⁾	X
Instrucciones de seguridad de variadores	X	—
Diagrama de lógica de escalera (LD)	X	X
Cambio de idioma	X	X
Protección de fuente basada en licencia	—	X
Importación de componentes de programa	—	X
Exportación de componentes de programa	X	X
Rutinas de diagrama de funciones secuenciales (SFC)	—	X
Texto estructurado (ST)	—	X

(1) Aunque la tarea de seguridad no puede ser una tarea de eventos, se pueden activar tareas de eventos estándar mediante el uso de la instrucción de eventos en la tarea de seguridad.

(2) Se restringe al uso de las instrucciones de seguridad de variadores con variadores Kinetix 5700 ERS4.

IMPORTANTE Consideraciones de seguridad

Los controladores Compact GuardLogix 5380 pueden producir tags estándar como unidifusión o multidifusión, pero solo pueden producir tags de seguridad como unidifusión. Los controladores pueden consumir tags de seguridad como unidifusión o multidifusión.

Al configurar un tag de seguridad producido, se permite configurar solo opciones de conexión de unidifusión. Logix Designer no permite configurar opciones de conexión de multidifusión.

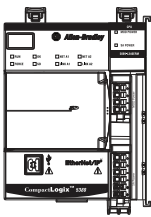
Al configurar un tag consumido, hay que considerar las capacidades del productor:

- Si el productor en el árbol de E/S de este controlador es un controlador GuardLogix 5580 o Compact GuardLogix 5380 y usted está consumiendo un tag de seguridad, hay que configurar el tag consumido para que utilice unidifusión.
- Si el productor en el árbol E/S de este controlador es un controlador GuardLogix 5570, GuardLogix 5560 o Compact GuardLogix 5370, el tag consumido de seguridad se puede configurar como unidifusión o multidifusión. Un controlador GuardLogix 5560 requiere la aplicación Studio 5000 Logix Designer, versión 19.00.00 o posterior, para trabajar con tags de seguridad producidos/consumidos que utilicen unidifusión.

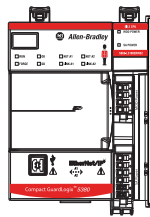
Encendido del sistema

El controlador proporciona alimentación al sistema de la siguiente manera:

CompactLogix



Compact GuardLogix



- Alimentación MOD: Alimentación del lado del sistema que suministra energía al sistema y permite que los módulos transfieran datos y ejecuten la lógica.

La alimentación del lado del sistema se suministra a través del RTB de alimentación MOD.

- Alimentación SA: La alimentación del lado del campo que suministra energía a algunos módulos de E/S Compact 5000 y dispositivos del lado de campo conectados a ellos.

La alimentación del lado del campo se suministra a través del RTB de alimentación SA.

Hay consideraciones y restricciones específicas que debe conocer antes de conectar la alimentación MOD y la alimentación SA a un sistema CompactLogix 5380 o a un sistema Compact GuardLogix 5380.

Para obtener información sobre cómo conectar la alimentación MOD y la alimentación SA a los diferentes sistemas, consulte:

- Cómo encender los controladores CompactLogix 5380 – Capítulo 2 en la [página 27](#)
- Cómo encender los controladores Compact GuardLogix 5380 – Capítulo 3 en la [página 37](#)

Notas:

Cómo encender los controladores CompactLogix 5380

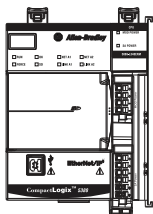
Tema	Página
Dos tipos de alimentación eléctrica	27
Alimentación MOD	29
Alimentación SA	30

Este capítulo describe como encender los controladores CompactLogix™ 5380 estándar.

Para obtener más información sobre cómo encender los controladores Compact GuardLogix® 5380, consulte Capítulo 3, [Cómo encender los controladores Compact GuardLogix 5380 en la página 37](#).

Dos tipos de alimentación eléctrica

CompactLogix



Los controladores CompactLogix 5380 proporcionan alimentación al sistema de la siguiente manera:

- Alimentación MOD: Alimentación del lado del sistema que suministra energía al sistema y permite que los módulos transfieran datos y ejecuten la lógica.

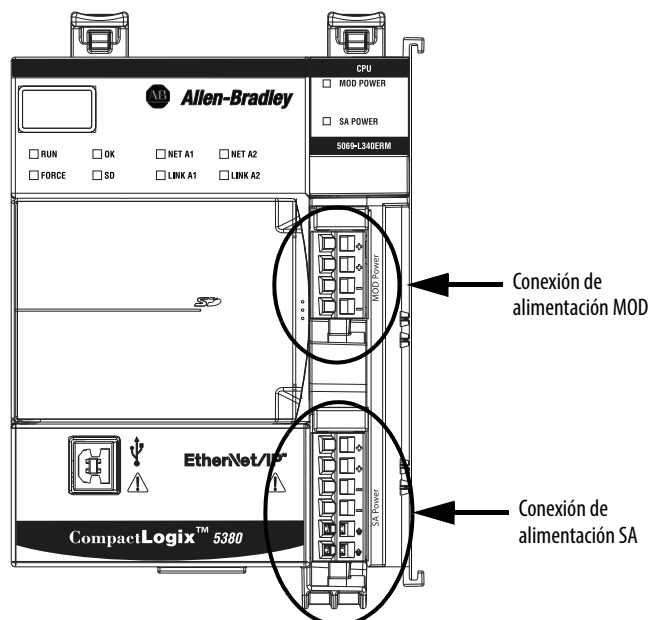
La alimentación del lado del sistema se suministra a través del RTB de alimentación MOD.

- Alimentación SA: Alimentación del lado del campo que suministra energía a algunos módulos de E/S Compact 5000™ y dispositivos del lado de campo conectados a ellos.

La alimentación del lado del campo se suministra a través del RTB de alimentación SA.

Conecte fuentes de alimentación eléctrica externas a los bloques de terminales extraíbles para proporcionar la alimentación MOD y SA. La [Figura 6](#) muestra los bloques de terminales extraíbles en un controlador CompactLogix 5380.

Figura 6 – Bloques de terminales extraíbles de alimentación MOD y SA en un controlador CompactLogix 5380



La alimentación comienza en el controlador y atraviesa los circuitos internos del módulo de E/S Compact 5000 a través de los buses de alimentación eléctrica.

La alimentación MOD atraviesa el bus de alimentación MOD y la alimentación SA atraviesa el bus de alimentación SA. El bus de alimentación MOD y el bus de alimentación SA están aislados entre sí.

IMPORTANTE

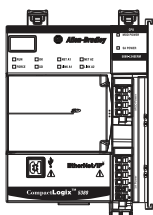
Recomendamos que use fuentes de alimentación eléctrica externas independientes para la alimentación MOD y SA, respectivamente. Esta práctica puede ayudar a evitar consecuencias no previstas que pueden producirse si se usa una sola fuente de alimentación.

Si se usan fuentes de alimentación eléctrica externas independientes, la pérdida de energía de una fuente de alimentación eléctrica externa no afecta la disponibilidad de energía de otra fuente. Por ejemplo, si se utilizan fuentes de alimentación eléctrica externas separadas y se pierde la alimentación SA, sigue estando disponible la alimentación MOD para el controlador CompactLogix 5380 y los módulos de E/S Compact 5000. Como resultado, la transferencia de datos continúa en el sistema.

Para obtener más información sobre cómo conectar la alimentación MOD y la alimentación SA, consulte el documento Controladores CompactLogix 5380 – Instrucciones de instalación, publicación [5069-IN013](#).

Alimentación MOD

CompactLogix



La alimentación MOD es una fuente de alimentación de CC necesaria para el funcionamiento del sistema CompactLogix 5380.

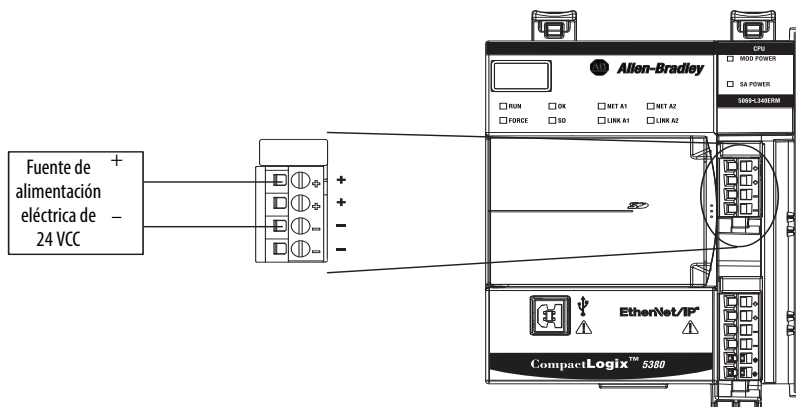
IMPORTANTE Puede utilizar solo alimentación eléctrica de CC en el bus de alimentación MOD. No conecte la alimentación eléctrica de CA al bus de alimentación MOD.

Recuerde lo siguiente:

- Cada módulo del sistema CompactLogix 5380 consume corriente del bus de alimentación MOD y pasa la corriente restante al siguiente módulo.
- La alimentación MOD permite que los módulos de E/S Compact 5000 transfieran datos y que el controlador ejecute lógica.
- Un sistema CompactLogix 5380 utiliza únicamente un bus de alimentación MOD.
- El consumo de corriente total en régimen permanente a través del bus de alimentación MOD no debe superar los 10 A entre 18...32 VCC.
- Le recomendamos que utilice una fuente de alimentación eléctrica externa dimensionada adecuadamente para el consumo total de corriente del bus de alimentación MOD en el sistema.

Debe tener en cuenta los **requisitos de corriente de entrada al momento del arranque** al calcular el consumo total de corriente del bus de alimentación MOD en el sistema.

Figura 7 – La fuente de alimentación eléctrica externa proporciona la alimentación MOD



Bus de alimentación MOD

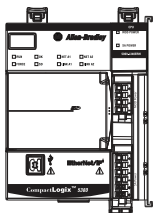
Cuando la fuente de alimentación MOD está encendida, ocurre lo siguiente.

1. El controlador CompactLogix 5380 consume corriente del bus de alimentación MOD y pasa la corriente restante al siguiente módulo.
2. El siguiente módulo consume corriente del bus de alimentación MOD y pasa la corriente restante al siguiente módulo.
3. El proceso continúa hasta que se satisfacen las necesidades de corriente del bus de alimentación MOD de todos los módulos del sistema.

Para obtener más información sobre la corriente que los módulos de E/S Compact 5000 consumen del bus de alimentación MOD, consulte el documento Compact 5000 I/O Modules Specifications Technical Data, publicación [5069-TD001](#).

Alimentación SA

CompactLogix



La alimentación SA proporciona alimentación a los dispositivos conectados a algunos de los módulos de E/S Compact 5000 del sistema CompactLogix 5380. La alimentación SA se conecta al controlador a través de un bloque de terminales extraíble de alimentación SA.

Recuerde lo siguiente:

- Algunos módulos de E/S Compact 5000 consumen corriente del bus de alimentación SA y pasan la corriente restante al siguiente módulo.
- Algunos módulos de E/S Compact 5000 solo pasan la corriente a través del bus de alimentación SA al siguiente módulo.
- Un sistema CompactLogix 5380 puede tener múltiples buses de alimentación SA. El primer bus de alimentación SA comienza en el controlador y atraviesa los módulos de E/S instalados a la derecha del controlador.

Puede utilizar un distribuidor de potencial de campo 5069-FPD para establecer un nuevo bus de alimentación SA. El nuevo bus de alimentación SA está aislado del bus de alimentación SA ubicado a su izquierda en el sistema.

Para obtener más información sobre cómo utilizar un distribuidor potencial de campo 5069-FPD en un sistema CompactLogix 5380, vea la [página 34](#).

- Si la fuente de alimentación SA utiliza voltaje de CC, el consumo de corriente total en régimen permanente a través del bus de alimentación SA no debe superar los 10 A entre 18...32 VCC.
- Le recomendamos que utilice una fuente de alimentación eléctrica externa dimensionada adecuadamente para el consumo total de corriente del bus de alimentación SA en el sistema.

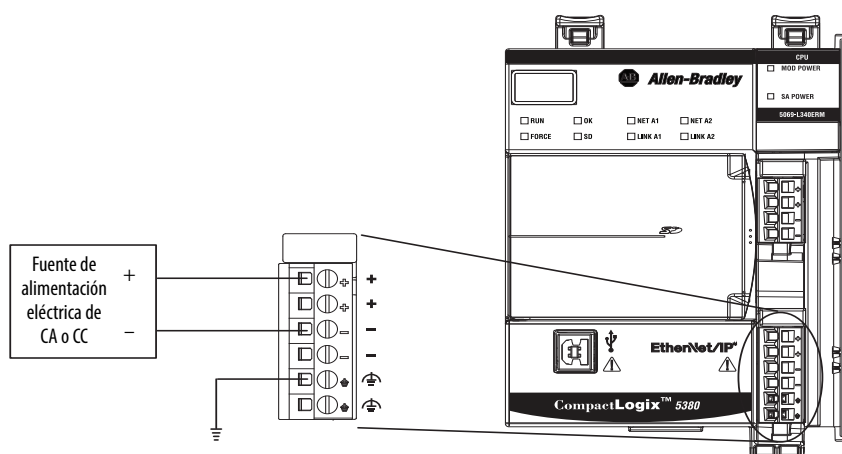
Debe tener en cuenta los **requisitos de corriente de entrada al momento del arranque** al calcular el consumo total de corriente del bus de alimentación SA en el sistema.

- Las conexiones a un bus de alimentación SA emplean un común compartido. Todas las entradas que consumen corriente de un bus de alimentación SA para proporcionar alimentación a dispositivos del lado de campo cuentan con un retorno a través de circuitos al terminal SA en el conector de alimentación SA.

IMPORTANTE Cada bus de alimentación SA tiene un común compartido único de ese bus, ya que los buses de alimentación SA están completamente aislados entre sí.

Es decir, el bus de alimentación SA que el controlador CompactLogix 5380 establece tiene un común compartido. Si utiliza un distribuidor de potencial de campo 5069-FPD para establecer un nuevo bus de alimentación SA en el sistema, ese segundo bus tendrá su propio común compartido para los módulos que consumen corriente del mismo.

Figura 8 – Una fuente de alimentación eléctrica externa proporciona alimentación SA



Cuando la fuente de alimentación SA está encendida, ocurre lo siguiente.

1. El controlador CompactLogix 5380 consume corriente del bus de alimentación SA y pasa la corriente restante al siguiente módulo.

IMPORTANTE El nivel de corriente que el controlador CompactLogix 5380 consume del bus de alimentación SA del controlador es insignificante. Consume 10 mA (alimentación eléctrica de CC), 25 mA (alimentación eléctrica de CA).

2. El siguiente módulo lleva a cabo una de estas tareas.
 - Si el módulo utiliza alimentación SA, el módulo consume corriente del bus de alimentación SA y pasa la corriente restante al siguiente módulo.
 - Si el módulo no utiliza corriente del bus de alimentación SA, el módulo pasa la corriente restante al siguiente módulo.
3. El proceso continúa hasta que se satisfacen todas las necesidades de corriente del bus de alimentación SA de los módulos del bus de alimentación SA.

Si su sistema incluye módulos de CA y CC que requieren alimentación SA, debe utilizar un distribuidor de potencial de campo 5069-FPD para establecer un bus de alimentación SA independiente y separar los tipos de módulos en los buses de alimentación SA aislados.

Para obtener más información sobre la corriente que los módulos de E/S Compact 5000 consumen del bus de alimentación SA, consulte el documento Compact 5000 I/O Modules Specifications Technical Data, publicación [5069-TD001](#).

Seguimiento del consumo de corriente del bus de alimentación SA

Le recomendamos que realice un seguimiento del consumo de corriente del bus de alimentación SA, máx., por módulo y colectivamente, para el sistema CompactLogix 5380.

Debe asegurarse de que los módulos de E/S Compact 5000 instalados en un bus de alimentación SA no consuman más de 10 A. En caso de sobrepasarse los 10 A, debe establecer otro bus de alimentación SA.

Tenga en cuenta lo siguiente con este ejemplo:

- Los valores de este ejemplo corresponden al cálculo para el peor caso posible. Es decir, todos los módulos que consumen corriente del bus de alimentación SA consumen el máximo disponible en el módulo.
- No todos los módulos que aparecen en la [Figura 9](#) utilizan la corriente del bus de alimentación SA. Por ejemplo, los módulos 5069-ARM y 5069-OW4I solo pasan la corriente del bus de alimentación SA al siguiente módulo.

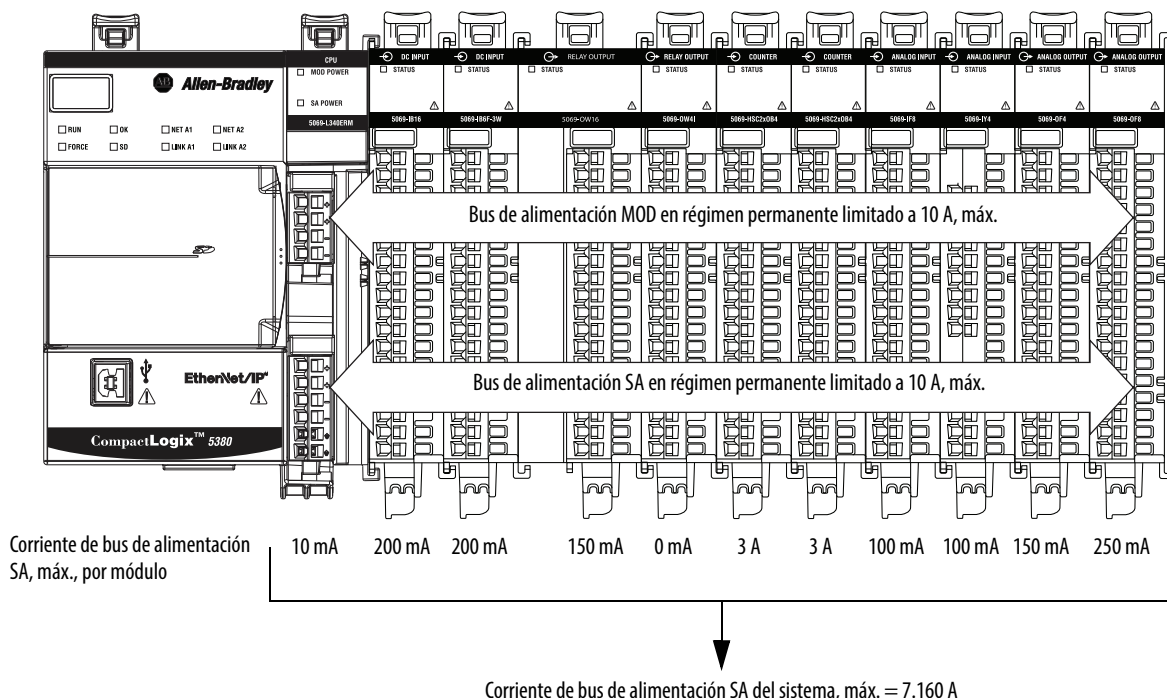
Entre los otros módulos que no utilizan la corriente del bus de alimentación SA, pero no aparecen en el gráfico, se incluyen los módulos 5069-OB16, 5069-OB16F, 5069-OX4I y 5069-SERIAL.

- La corriente máx. del bus de alimentación SA del sistema se calcula cuando cada módulo consume corriente del bus de alimentación SA. El cálculo comienza con el controlador. El consumo de corriente del bus de alimentación SA del controlador utilizado para el cálculo es 10 mA para la alimentación eléctrica de CC

En la [Figura 9](#), después de que el módulo 5069-IB16 en la ranura 1 consuma la corriente del bus de alimentación SA, la corriente máx. del bus de alimentación SA del sistema es 210 mA.

Después de que el módulo 5069-IB16 en la ranura 2 consuma la corriente del bus de alimentación SA, el consumo de corriente del bus de alimentación SA es 410 mA. Este proceso continúa hasta que la corriente máx. del bus de alimentación SA alcanza 7.160 A.

Figura 9 – Sistema CompactLogix 5380 – Cálculo del consumo de corriente del bus de alimentación SA



Uso de un distribuidor de potencial de campo 5069-FPD para crear un nuevo bus de alimentación SA

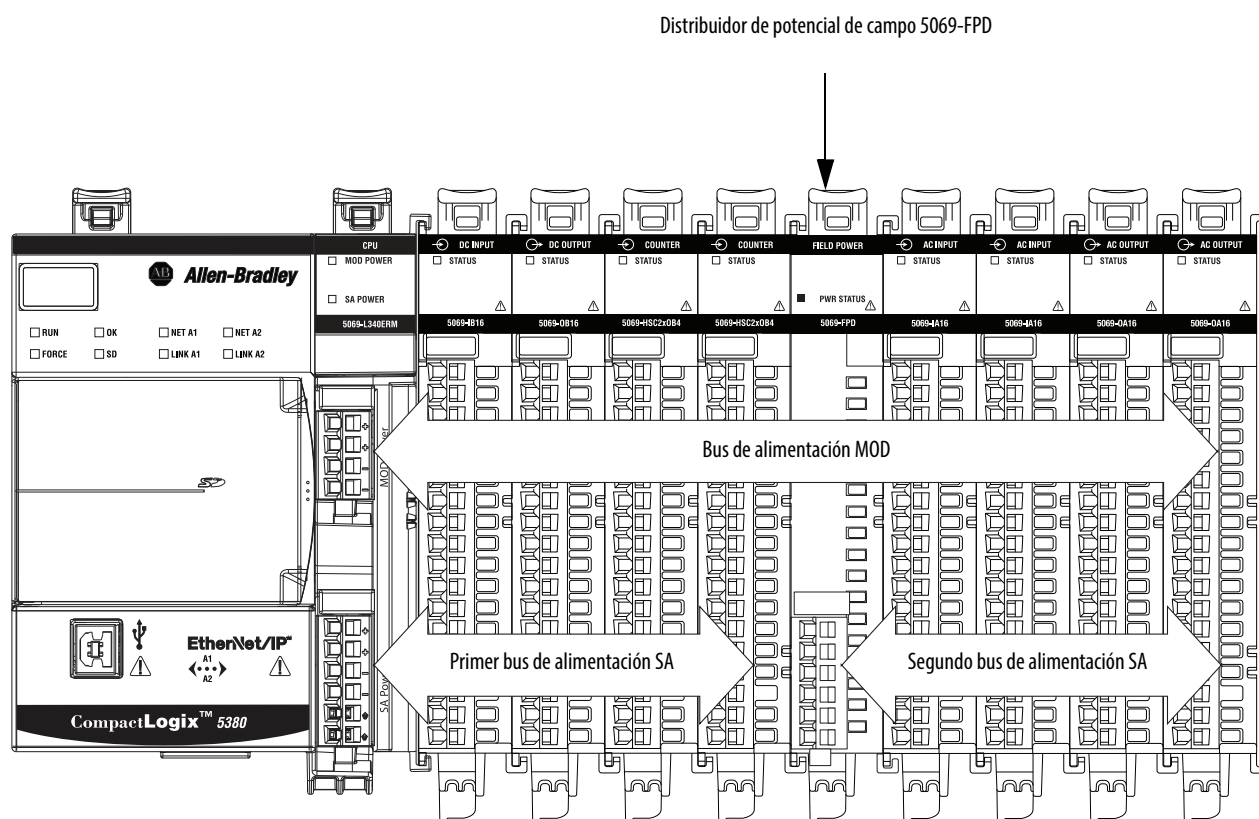
Puede utilizar un distribuidor de potencial de campo 5069-FPD para establecer un nuevo bus de alimentación SA en un sistema CompactLogix 5380.

El distribuidor de potencial de campo impide que la corriente atraviese el bus de alimentación SA ubicado a la izquierda. En dicho punto, el distribuidor de potencial de campo establece un nuevo bus de alimentación SA para los módulos ubicados a la derecha. El nuevo bus de alimentación SA está aislado del bus de alimentación SA ubicado a su izquierda en el sistema.

Puede conectar una fuente de alimentación eléctrica externa de 24 VCC o de 120/240 VCA a un distribuidor de potencial de campo 5069-FPD en un sistema CompactLogix 5380.

La [Figura 10](#) muestra un sistema CompactLogix 5380 que utiliza un distribuidor de potencial de campo 5069-FPD para crear un segundo bus de alimentación SA.

Figura 10 – Sistema CompactLogix 5380 – Creación de un nuevo bus de alimentación SA



Puede instalar múltiples distribuidores de potencial de campo 5069-FPD en el mismo sistema, si es necesario.

Alimentación SA: Notas adicionales

- Otros ejemplos de configuraciones de sistema que utilizan múltiples buses de alimentación SA incluyen:
 - Los módulos del sistema consumen colectivamente más de 10 A de alimentación SA, es decir, la corriente máxima que puede proporcionar un bus de alimentación SA.
 - Los módulos del sistema deben estar aislados dependiendo de los tipos de módulos, como por ejemplo, módulos de E/S digitales y E/S analógicas.
 - Los módulos del sistema están aislados según el tipo de dispositivo del lado de campo al que están conectados.

Por ejemplo, se pueden separar los módulos conectados a dispositivos del lado de campo que utilizan voltaje de CC de los módulos conectados a dispositivos del lado del campo que requieren voltaje de CA.

- La corriente real de un sistema CompactLogix 5380 cambia dependiendo de las condiciones de funcionamiento en un momento dado.

Por ejemplo, el consumo de corriente del bus de alimentación SA en algunos módulos es diferente si todos los canales alimentan a dispositivos de campo o si la mitad de los canales alimentan dispositivos de campo.

- Algunos módulos de E/S Compact 5000 utilizan alimentación del lado del campo pero no la consumen de un bus de alimentación SA. Los módulos reciben alimentación del lado del campo de una fuente de alimentación eléctrica externa conectada directamente al módulo de E/S.

Por ejemplo, los módulos 5069-OB16 y 5069-OB16F utilizan terminales de accionador local (LA) en el RTB del módulo, es decir, los terminales LA+ y LA– de todos los canales del módulo.

En este caso, puede utilizar la misma fuente de alimentación eléctrica externa conectada al RTB de alimentación SA en el controlador a los terminales LA+ y LA–.

IMPORTANTE Debe tener en cuenta el límite de corriente de una fuente de alimentación eléctrica externa si la utiliza para proporcionar alimentación al bloque de terminales extraíble de alimentación SA en el controlador y los terminales LA+ y LA– en un módulo 5069-OB16 o 5069-OB16F.

Notas:

Cómo encender los controladores Compact GuardLogix 5380

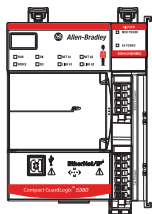
Tema	Página
Dos tipos de alimentación eléctrica	37
Alimentación MOD	39
Alimentación SA	40

Este capítulo describe cómo encender los controladores Compact GuardLogix® 5380.

Para obtener información sobre cómo encender los controladores CompactLogix™ 5380 estándar, vea el Capítulo 2, [Cómo encender los controladores CompactLogix 5380 en la página 27](#).

Dos tipos de alimentación eléctrica

Compact GuardLogix



Los controladores Compact GuardLogix 5380 proporcionan alimentación al sistema de la siguiente manera:

- Alimentación MOD: Alimentación del lado del sistema que suministra energía al sistema y permite que los módulos transfieran datos y ejecuten la lógica.

La alimentación del lado del sistema se suministra a través del RTB de alimentación MOD.

- Alimentación SA: Alimentación del lado del campo que suministra energía a algunos módulos de E/S Compact 5000™ y dispositivos del lado de campo conectados a ellos.

La alimentación del lado del campo se suministra a través del RTB de alimentación SA.

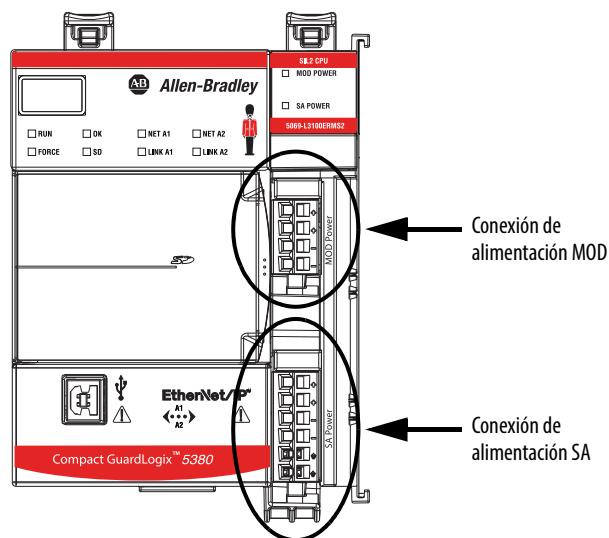
IMPORTANTE

La alimentación MOD y SA debe ser alimentación eléctrica de CC en el lado del controlador. La alimentación eléctrica de CC para los controladores Compact GuardLogix deben proceder de una fuente de alimentación eléctrica con clasificación SELV/PELV.

Si utiliza un voltaje de CA para los módulos de E/S locales, hay que realizar una conexión a través de un módulo distribuidor de potencial de campo 5069-FPD. No se puede conectar un voltaje de CA al controlador.

Conecte fuentes de alimentación eléctrica externas a los bloques de terminales extraíbles para proporcionar la alimentación MOD y SA. La [Figura 11](#) muestra los bloques de terminales extraíbles en un controlador Compact GuardLogix 5380.

Figura 11 – Bloques de terminales extraíbles de alimentación MOD y SA en un controlador Compact GuardLogix 5380



La alimentación comienza en el controlador y atraviesa los circuitos internos del módulo de E/S Compact 5000 a través de los buses de alimentación eléctrica.

La alimentación MOD atraviesa el bus de alimentación MOD y la alimentación SA atraviesa el bus de alimentación SA. El bus de alimentación MOD y el bus de alimentación SA están aislados entre sí.

IMPORTANTE

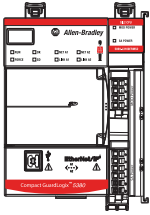
Recomendamos que use fuentes de alimentación eléctrica externas independientes para la alimentación MOD y SA, respectivamente. Esta práctica puede ayudar a evitar consecuencias no previstas que pueden producirse si se usa una sola fuente de alimentación.

Si se usan fuentes de alimentación eléctrica externas independientes, la pérdida de energía de una fuente de alimentación eléctrica externa no afecta la disponibilidad de energía de otra fuente. Por ejemplo, si se utilizan fuentes de alimentación eléctrica externas MOD y SA separadas y se pierde la alimentación SA, sigue estando disponible la alimentación MOD para el controlador Compact GuardLogix 5380 y los módulos de E/S Compact 5000. Como resultado, la transferencia de datos continúa en el sistema.

Para obtener más información sobre cómo conectar la alimentación MOD y la alimentación SA, consulte el documento Controladores Compact GuardLogix 5380 – Instrucciones de instalación, publicación [5069-IN014](#).

Alimentación MOD

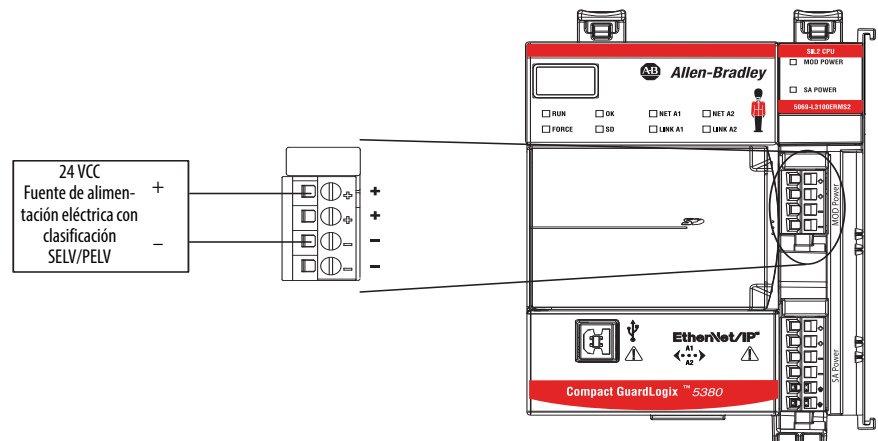
Compact
GuardLogix



La alimentación MOD proviene de una fuente de alimentación de CC necesaria para el funcionamiento del sistema Compact GuardLogix 5380. Recuerde lo siguiente:

- Debe utilizar fuentes de alimentación eléctrica con clasificación SELV/PELV para suministrar alimentación a los controladores Compact GuardLogix 5380.
- Cada módulo del sistema Compact GuardLogix 5380 consume corriente del bus de alimentación MOD y pasa la corriente restante al siguiente módulo.
- La alimentación MOD permite que los módulos de E/S Compact 5000 transfieran datos y que el controlador ejecute lógica.
- Un sistema Compact GuardLogix 5380 utiliza únicamente un bus de alimentación MOD.
- La fuente de alimentación MOD debe limitarse a 5 A, máx., entre 18...32 VCC.
- Le recomendamos que utilice una fuente de alimentación eléctrica externa con clasificación SELV/PELV dimensionada adecuadamente para el consumo total de corriente del bus de alimentación MOD en el sistema. Debe tener en cuenta los **requisitos de corriente de entrada al momento del arranque** al calcular el consumo total de corriente del bus de alimentación MOD en el sistema.

Figura 12 – La fuente de alimentación eléctrica externa proporciona la alimentación MOD



Bus de alimentación MOD

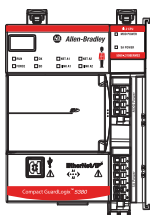
Cuando la fuente de alimentación MOD está encendida, ocurre lo siguiente.

1. El controlador Compact GuardLogix 5380 consume corriente del bus de alimentación MOD y pasa la corriente restante al siguiente módulo.
2. El siguiente módulo consume corriente del bus de alimentación MOD y pasa la corriente restante al siguiente módulo.
3. El proceso continúa hasta que se satisfacen las necesidades de corriente del bus de alimentación MOD de todos los módulos del sistema.

Para obtener más información sobre la corriente que los módulos de E/S Compact 5000 consumen del bus de alimentación MOD, consulte el documento Compact 5000 I/O Modules Specifications Technical Data, publicación [5069-TD001](#).

Alimentación SA

Compact
GuardLogix



La alimentación SA proporciona alimentación a los dispositivos conectados a algunos de los módulos de E/S Compact 5000 del sistema Compact GuardLogix 5380. La alimentación SA se conecta al controlador a través de un bloque de terminales extraíble de alimentación SA.

Recuerde lo siguiente:

IMPORTANTE Se aplican restricciones más específicas al conectar la alimentación SA a un controlador Compact GuardLogix 5380 o a un distribuidor de potencial de campo 5069-FPD.

Para obtener más información, consulte la [página 45](#).

- Debe utilizar fuentes de alimentación eléctrica SELV o PELV para suministrar alimentación a los controladores Compact GuardLogix 5380.
- Si la fuente de alimentación SA usa voltaje de CC, debe limitar la fuente de alimentación SA a 10 A máx. entre 18...32 VCC.
- Algunos módulos de E/S Compact 5000 consumen corriente del bus de alimentación SA y pasan la corriente restante al siguiente módulo.
- Algunos módulos de E/S Compact 5000 solo pasan la corriente a través del bus de alimentación SA al siguiente módulo.
- Si la fuente de alimentación SA es una fuente de alimentación eléctrica de CA, o una fuente de CC sin SELV/PELV, hay que establecer una terminación desde un distribuidor de alimentación eléctrica de campo antes de consumir la alimentación en el bus de alimentación SA.

- Un sistema Compact GuardLogix 5380 puede tener múltiples buses de alimentación SA. El primer bus de alimentación SA comienza en el controlador y atraviesa los módulos de E/S instalados a la derecha del controlador.

Puede utilizar un distribuidor de potencial de campo 5069-FPD para establecer un nuevo bus de alimentación SA. El nuevo bus de alimentación SA está aislado del bus de alimentación SA ubicado a su izquierda en el sistema.

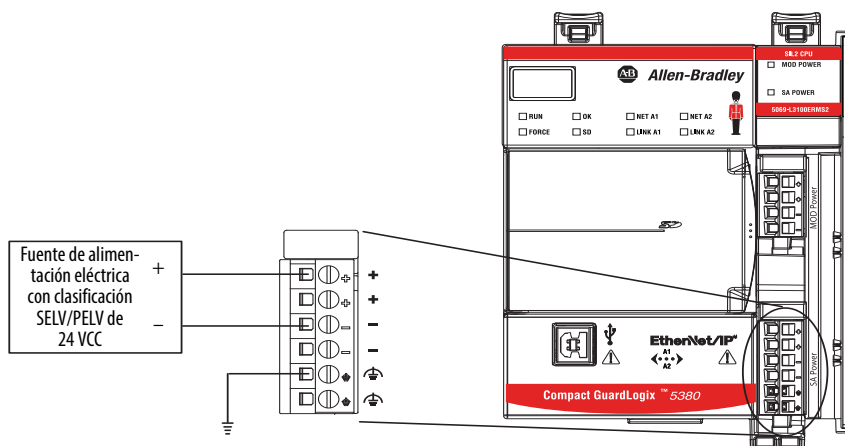
Para obtener más información sobre cómo utilizar un distribuidor de potencial de campo 5069-FPD en un sistema CompactLogix 5380, vea la [página 44](#).

- Le recomendamos que utilice una fuente de alimentación eléctrica externa dimensionada adecuadamente para el consumo total de corriente del bus de alimentación SA en el sistema. Debe tener en cuenta los **requisitos de corriente de entrada al momento del arranque** al calcular el consumo total de corriente del bus de alimentación SA en un bus específico.
- Las conexiones a un bus de alimentación SA emplean un **común compartido**. Todas las entradas que consumen corriente de un bus de alimentación SA para proporcionar alimentación a dispositivos del lado de campo cuentan con un retorno a través de circuitos al terminal SA en el conector de alimentación SA.

IMPORTANTE Cada bus de alimentación SA tiene un común compartido único de ese bus, ya que los buses de alimentación SA están completamente aislados entre sí.

Es decir, el bus de alimentación SA que el controlador establece tiene un común compartido. Si utiliza un distribuidor de potencial de campo 5069-FPD para establecer un nuevo bus de alimentación SA en el sistema, ese segundo bus tendrá su propio común compartido para los módulos que consumen corriente del mismo.

Figura 13 – Una fuente de alimentación eléctrica externa proporciona alimentación SA



Cuando la fuente de alimentación SA está encendida, ocurre lo siguiente.

1. El controlador consume corriente del bus de alimentación SA y pasa la corriente restante al siguiente módulo.

IMPORTANTE	El nivel de corriente que el controlador Compact GuardLogix 5380 consume del bus de alimentación SA del controlador es insignificante. Consume 10 mA.
-------------------	---

2. El siguiente módulo lleva a cabo una de estas tareas.
 - Si el módulo utiliza alimentación SA, el módulo consume corriente del bus de alimentación SA y pasa la corriente restante al siguiente módulo.
 - Si el módulo no utiliza corriente del bus de alimentación SA, el módulo pasa la corriente restante al siguiente módulo.
3. El proceso continúa hasta que se satisfacen todas las necesidades de corriente del bus de alimentación SA de los módulos del bus de alimentación SA.

Para obtener más información sobre la corriente que los módulos de E/S Compact 5000 consumen del bus de alimentación SA, consulte el documento Compact 5000 I/O Modules and EtherNet/IP Adapters Technical Data, publicación [5069-TD001](#).

Seguimiento del consumo de corriente del bus de alimentación SA

Le recomendamos que realice un seguimiento del consumo de corriente del bus de alimentación SA, máx., por módulo y colectivamente, para el sistema Compact GuardLogix 5380. Debe asegurarse de que los módulos de E/S Compact 5000 instalados en un bus de alimentación SA no consuman más de 10 A. En caso de sobrepasarse los 10 A, debe establecer otro bus de alimentación SA.

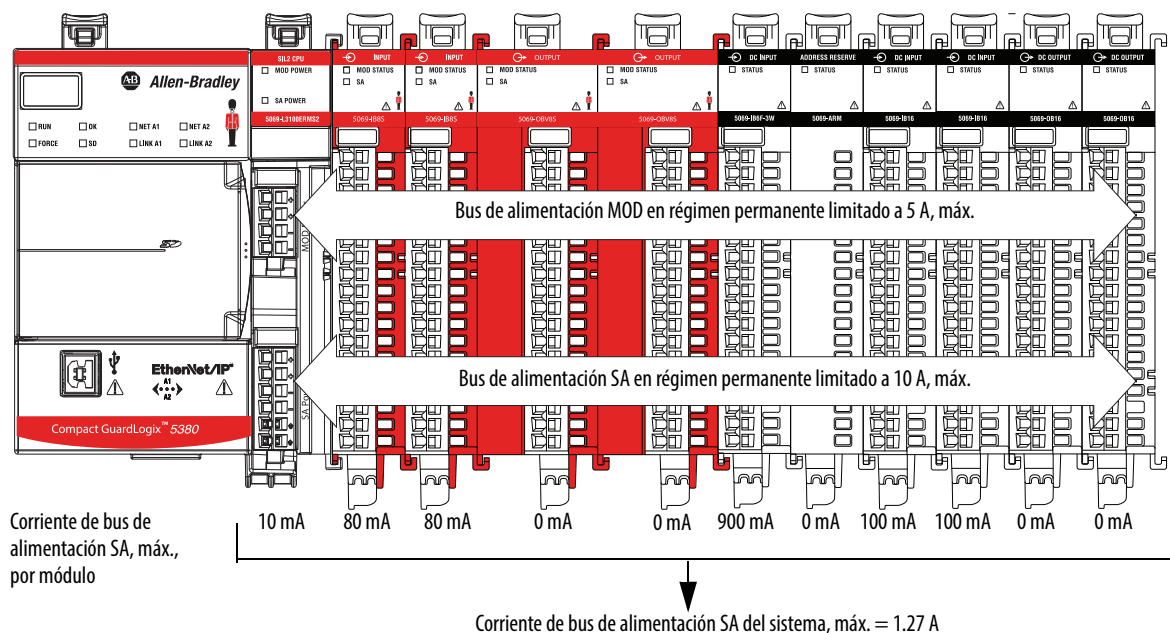
Tenga en cuenta lo siguiente con este ejemplo:

- Los valores de este ejemplo corresponden al cálculo para el peor caso posible. Es decir, todos los módulos que consumen corriente del bus de alimentación SA consumen el máximo disponible en el módulo.
- No todos los módulos que aparecen en la [Figura 14 en la página 43](#) utilizan la corriente del bus de alimentación SA. Por ejemplo, los módulos 5069-OBV8S, 5069-ARM y 5069-OB16 solo pasan la corriente del bus de alimentación SA al siguiente módulo. Entre los otros módulos que no utilizan la corriente del bus de alimentación SA, pero no aparecen en el gráfico, se incluyen los módulos 5069-OB16F y 5069-OX4I.
- La corriente máx. del bus de alimentación SA del sistema se calcula cuando cada módulo consume corriente del bus de alimentación SA. El cálculo comienza con el controlador. El consumo de corriente del bus de alimentación SA del controlador utilizado para el cálculo es 10 mA para la alimentación eléctrica de CC

En la [Figura 14](#), después de que el módulo 5069-IB8S en la ranura 1 consuma la corriente del bus de alimentación SA, la corriente máx. del bus de alimentación SA del sistema será 90 mA.

Después de que el módulo 5069-IB8S en la ranura 2 consuma la corriente del bus de alimentación SA, el consumo de corriente del bus de alimentación SA será 170 mA. Este proceso continúa hasta que la corriente máx. del bus de alimentación SA alcance 1.27 A.

Figura 14 – Sistema Compact GuardLogix 5380 – Cálculo del consumo de corriente del bus de alimentación SA



Uso de un distribuidor de potencial de campo 5069-FPD para crear un nuevo bus de alimentación SA.

IMPORTANTE Si utiliza módulos de relé de E/S Compact 5000 locales o un voltaje de CA para los módulos de E/S Compact 5000 locales, será necesaria una conexión a través de un módulo distribuidor de potencial de campo 5069-FPD. No se puede conectar un voltaje de CA al controlador.

Debe utilizar un distribuidor de potencial de campo 5069-FPD para establecer un nuevo bus de alimentación SA en un sistema Compact GuardLogix 5380.

El distribuidor de potencial de campo impide que la corriente atraviese el bus de alimentación SA ubicado a la izquierda. En dicho punto, el distribuidor de potencial de campo establece un nuevo bus de alimentación SA para los módulos ubicados a la derecha. El nuevo bus de alimentación SA está aislado del bus de alimentación SA ubicado a su izquierda en el sistema.

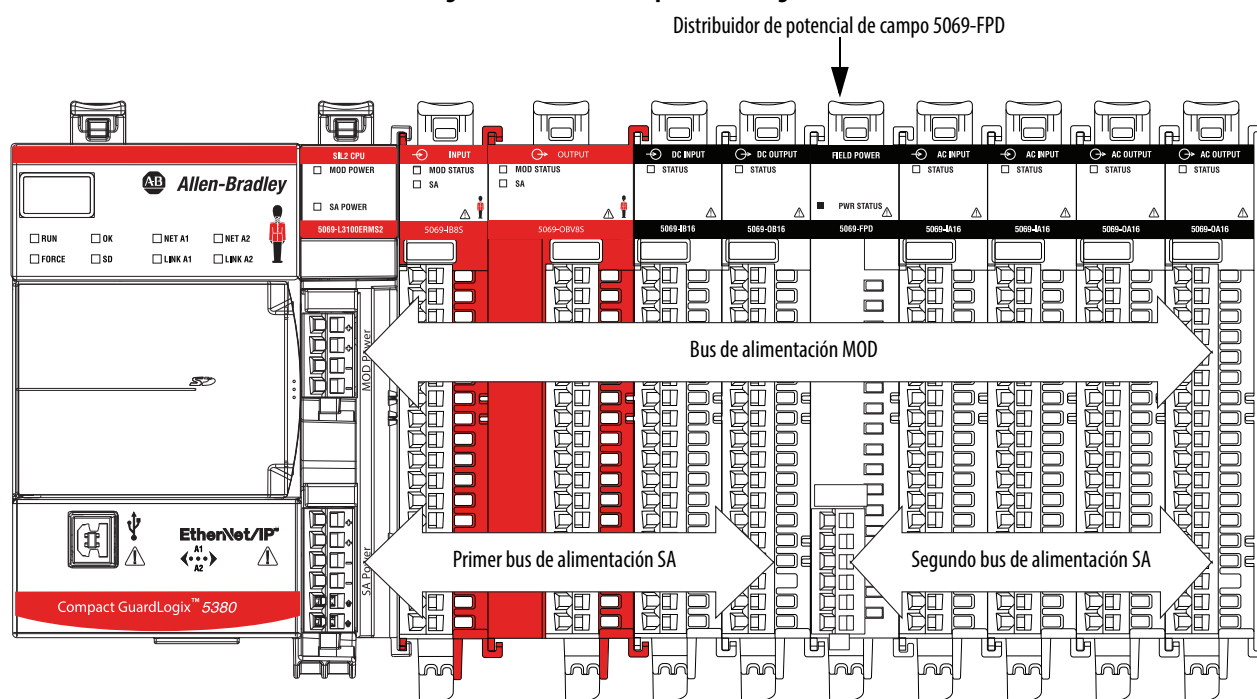
Puede conectar una fuente de alimentación eléctrica externa de 24 VCC o de 120/240 VCA a un distribuidor de potencial de campo 5069-FPD en un sistema Compact GuardLogix 5380.

IMPORTANTE Se aplican algunas restricciones al conectar la alimentación SA a un distribuidor de potencial de campo 5069-FPD.

Para obtener más información, consulte la [página 45](#).

La [Figura 15](#) muestra un sistema Compact GuardLogix 5380 que utiliza un distribuidor de potencial de campo 5069-FPD para crear un segundo bus de alimentación SA.

Figura 15 – Sistema Compact GuardLogix 5380 – Creación de un nuevo bus de alimentación SA



Restricciones al conectar la alimentación SA a un sistema Compact GuardLogix 5380

Recuerde estas restricciones en la [Tabla 4](#) al conectar la alimentación SA a un sistema Compact GuardLogix 5380.

Tabla 4 – Restricciones de alimentación SA – Sistema Compact GuardLogix 5380

Componente al que está conectada la alimentación SA	Restricciones
Controlador Compact GuardLogix 5380	<ul style="list-style-type: none"> • Debe utilizar las fuentes de alimentación eléctrica con clasificación SELV/PELV para suministrar alimentación a los controladores Compact GuardLogix 5380. • Pude conectar solo una fuente de alimentación eléctrica de 24 VCC con clasificación SELV/PELV. • El consumo total de corriente en régimen permanente a través del bus de alimentación SA no debe superar los 10 A máx. entre 0...32 VCC.

Ejemplo de sistema Compact GuardLogix

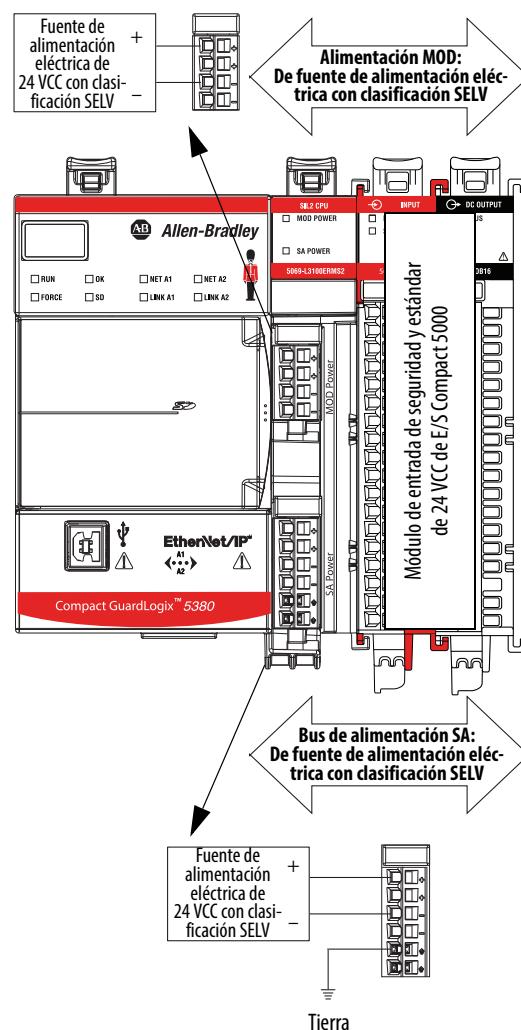


Tabla 4 – Restricciones de alimentación SA – Sistema Compact GuardLogix 5380

Componente al que está conectada la alimentación SA	Restricciones
Distribuidor de potencial de campo 5069-FPD con módulos estándar de E/S Compact 5000 únicamente	<p>Además de las restricciones enumeradas en la página 45, se aplican también estas restricciones:</p> <ul style="list-style-type: none"> Puede utilizar fuentes de alimentación eléctrica sin SELV o PELV solo si los módulos estándar de E/S Compact 5000 se instalan a la derecha del distribuidor de potencial de campo 5069-FPD. Puede conectar una fuente de alimentación eléctrica de 24 VCC o de 120/240 VCA. El ejemplo utiliza una fuente de alimentación eléctrica de 120/240 VCA. <ul style="list-style-type: none"> Si la alimentación SA conectada al distribuidor de potencial de campo 5069-FPD es un voltaje de CC, el consumo total de corriente en régimen permanente a través del bus de alimentación SA no debe superar los 10 A entre 0...32 VCC. Si un sistema Compact GuardLogix 5380 incluye módulos de relé de E/S Compact 5000 (5069-0W4I, 5069-0X4I, 5069-0W16) o módulos de E/S que requieren alimentación SA que es un voltaje de CA, hay que instalar estos módulos a la derecha de un distribuidor de potencial de campo 5069-FPD, tal como se muestra. <p>IMPORTANTE: Este requisito se aplica incluso cuando supone la necesidad de instalar el distribuidor de potencial de campo 5069-FPD justo a la derecha del controlador Compact GuardLogix 5380.</p> <ul style="list-style-type: none"> Si un sistema Compact GuardLogix 5380 incluye módulos estándar de E/S Compact 5000 que utilizan la alimentación SA suministrada por una fuente de alimentación eléctrica sin clasificación SELV/PELV, hay que instalar los módulos de E/S a la derecha de un distribuidor de potencial de campo 5069-FPD. <p>IMPORTANTE: El bus de alimentación SA que el distribuidor de potencial de campo 5069-FPD establece no puede incluir módulos de seguridad de E/S Compact 5000.</p>

Ejemplo de sistema Compact GuardLogix

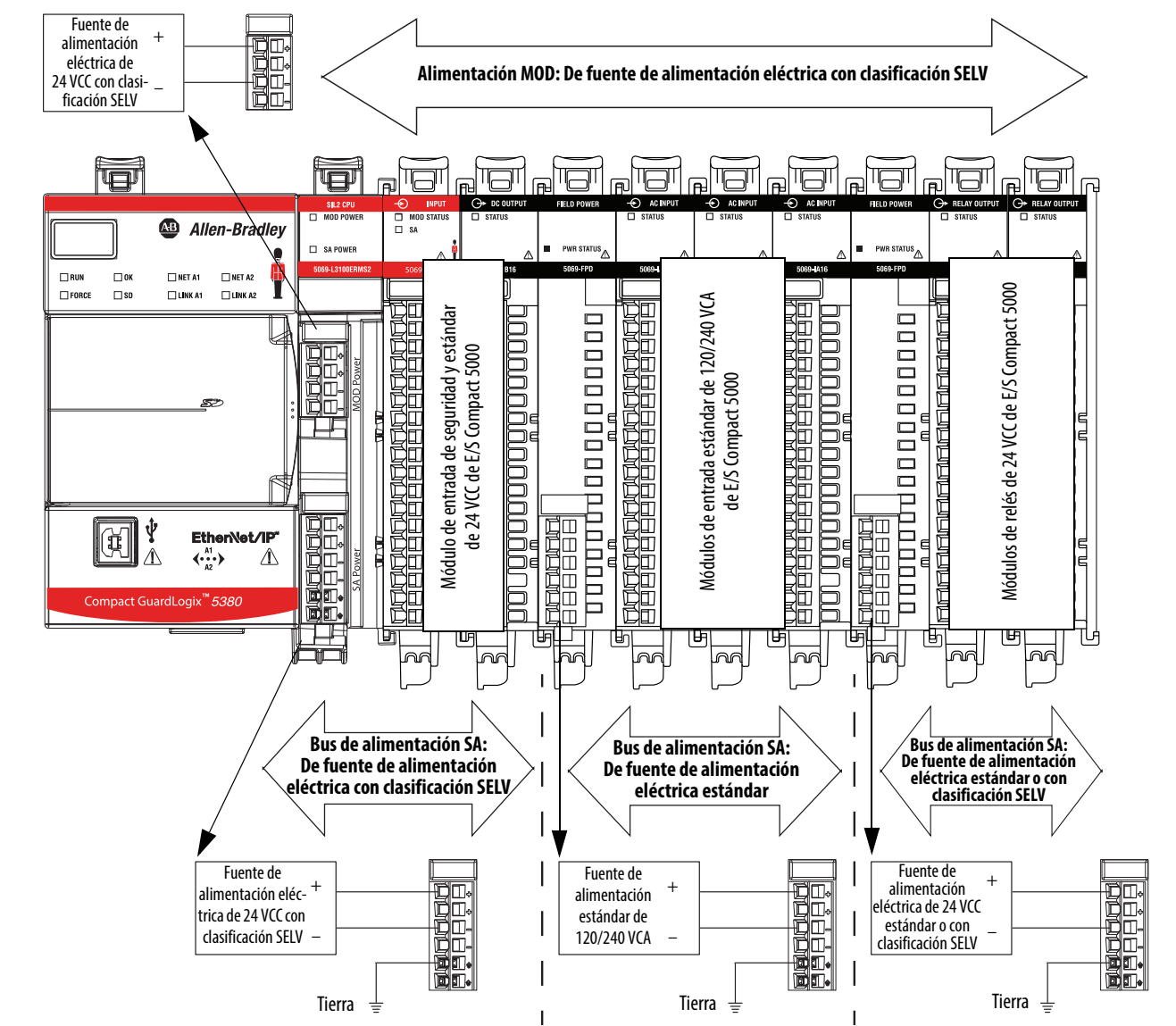
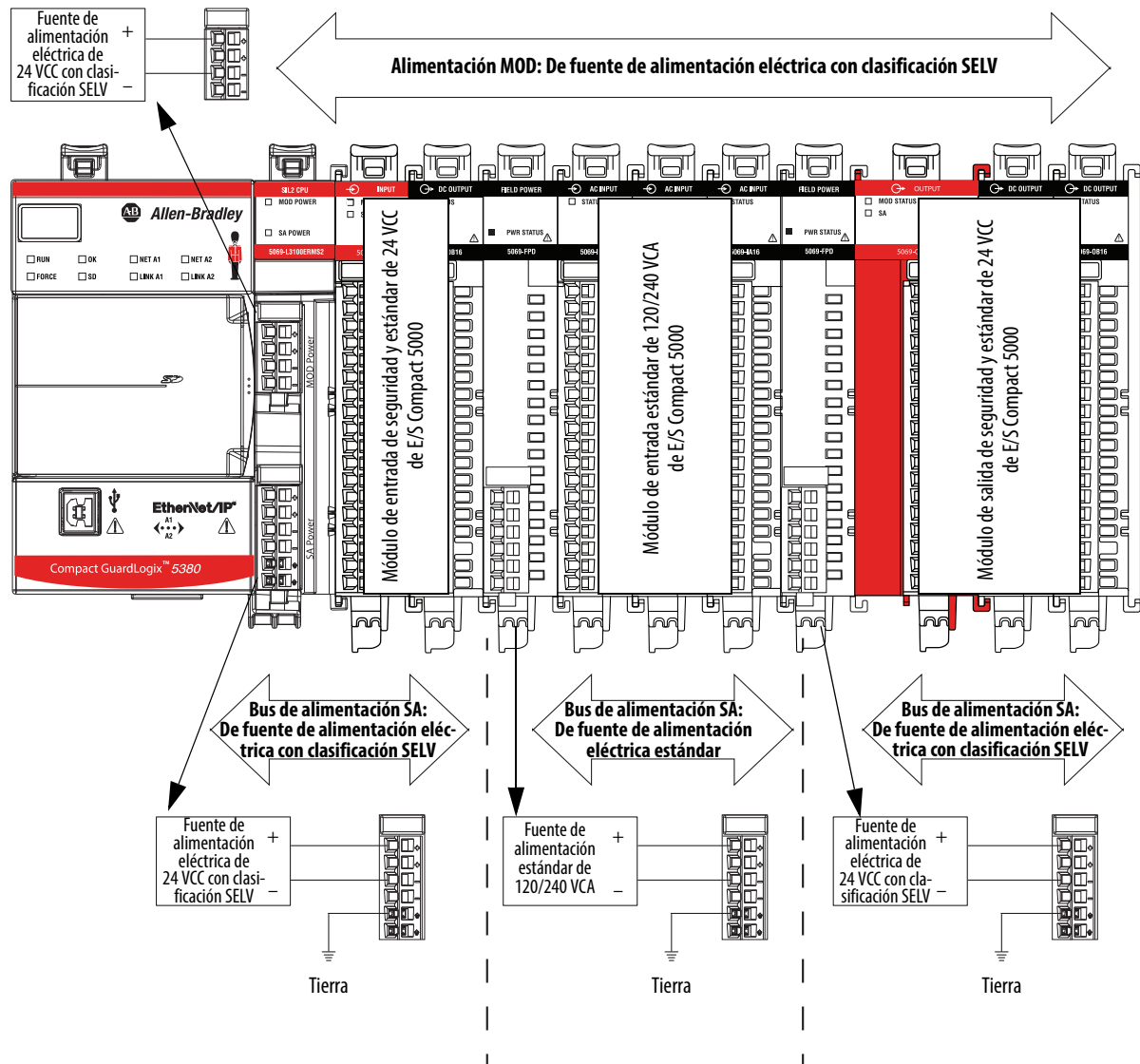


Tabla 4 – Restricciones de alimentación SA – Sistema Compact GuardLogix 5380

Componente al que está conectada la alimentación SA	Restricciones
Distribuidor de potencial de campo 5069-FPD Con módulos de E/S de seguridad y estándar Compact 5000	Además de las restricciones enumeradas en la página 45 y la página 46 , también se aplica esta restricción: <ul style="list-style-type: none"> Debe utilizar fuentes de alimentación eléctrica SELV o PELV para suministrar alimentación SA a los módulos de seguridad de E/S Compact 5000 instalados a la derecha del distribuidor de potencial de campo 5069-FPD.

Ejemplo de sistema Compact GuardLogix



Alimentación SA: Notas adicionales

- Otros ejemplos de configuraciones de sistema que utilizan múltiples buses de alimentación SA incluyen:
 - Los módulos del sistema consumen colectivamente más de 10 A de alimentación SA, es decir, la corriente máxima que puede proporcionar un bus de alimentación SA.
 - Los módulos del sistema deben estar aislados dependiendo de los tipos de módulos, como por ejemplo, módulos de E/S digitales y E/S analógicas.
 - Los módulos del sistema están aislados según el tipo de dispositivo del lado de campo al que están conectados.

Por ejemplo, se pueden separar los módulos conectados a dispositivos del lado de campo que utilizan voltaje de CC de los módulos conectados a dispositivos del lado del campo que requieren voltaje de CA.

- La corriente real de un sistema Compact GuardLogix 5380 cambia dependiendo de las condiciones de funcionamiento en un momento dado.

Por ejemplo, el consumo de corriente del bus de alimentación SA en algunos módulos es diferente si todos los canales alimentan a dispositivos de campo o si la mitad de los canales alimentan dispositivos de campo.

- Algunos módulos de E/S Compact 5000 utilizan alimentación del lado del campo pero no la consumen de un bus de alimentación SA. Los módulos reciben alimentación del lado del campo de una fuente de alimentación eléctrica externa conectada directamente al módulo de E/S.

Por ejemplo, los módulos 5069-OB16, 5069-OB16F y 5069-OBV8S utilizan terminales de accionador local (LA) en el RTB del módulo, es decir, los terminales LA+ y LA– de todos los canales del módulo.

En este caso, puede utilizar la misma fuente de alimentación eléctrica externa conectada al RTB de alimentación SA en el controlador a los terminales LA+ y LA–.

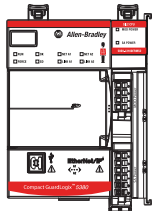
IMPORTANTE Debe tener en cuenta el límite de corriente de una fuente de alimentación eléctrica externa si la utiliza para proporcionar alimentación al bloque de terminales extraíble de alimentación SA del controlador y los terminales LA+ y LA– de un módulo 5069-OB16, 5069-OB16F o 5069-OBV8S. El módulo 5069-OBV8S requiere una fuente de alimentación eléctrica con clasificación SELV/PELV.

Concepto de seguridad de los controladores Compact GuardLogix 5380

Tema	Página
Capacidad de seguridad funcional	49
Número de red de seguridad	50
Firma de seguridad	51
Diferenciación entre componentes estándar y de seguridad	51
Capacidades de flujo de datos del controlador	52
Terminología de seguridad	53

Capacidad de seguridad funcional

Compact GuardLogix



El sistema controlador Compact GuardLogix® 5380 ha sido certificado para uso en aplicaciones de seguridad hasta SIL 2/PLd, inclusive, donde el estado desenergizado es el estado seguro.

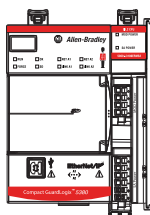
Las aplicaciones de seguridad SIL 2/PLd basadas en controladores Compact GuardLogix 5380 requieren el uso de una firma de seguridad.

En cuanto a los requisitos del sistema de seguridad SIL 2/PLd, incluidos los intervalos de prueba de validación funcionales, el tiempo de reacción del sistema y los cálculos de probabilidad de fallo a demanda/probabilidad de fallo por hora (PFD/PFH), consulte el documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#).

Debe leer, entender y satisfacer estos requisitos antes de operar un sistema de seguridad SIL 2/PLd Compact GuardLogix.

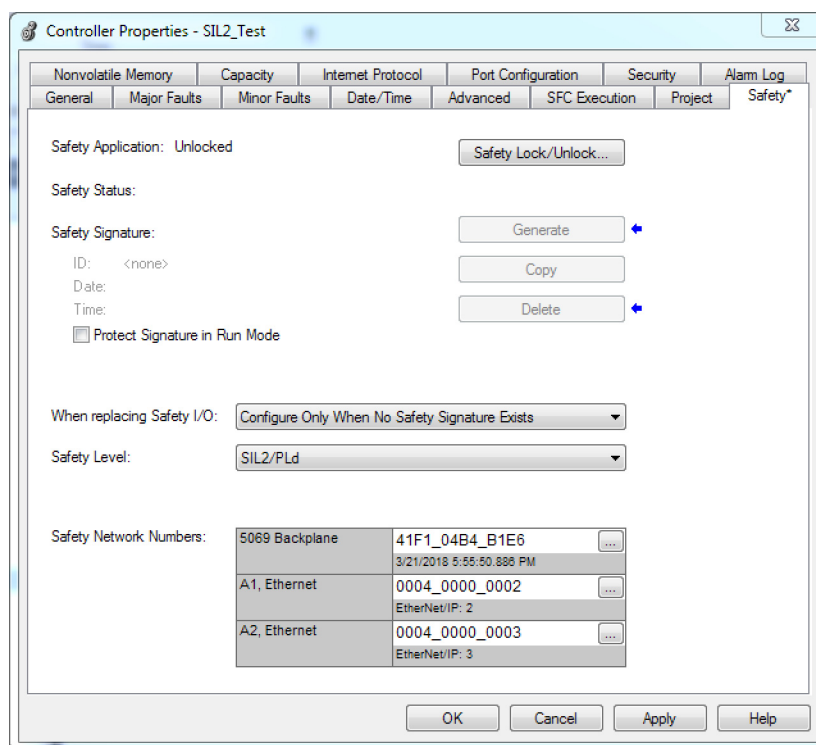
Número de red de seguridad

Compact
GuardLogix



El número de red de seguridad (SNN) identifica de manera única las subredes CIP Safety dentro de una red de seguridad encaminable. La combinación del SNN y la dirección de nodo identifica de manera única cada puerto CIP Safety en cada dispositivo de la red de seguridad encaminable.

La aplicación asigna un SNN a cada subred CIP Safety conectada a un controlador Compact GuardLogix 5380, incluido el backplane. Si hay otros controladores de seguridad Logix conectados a una red Ethernet, asigne el mismo SNN para esta red en cada aplicación de controlador. Esto le permite utilizar la asignación automática de Logix Designer de números de red de seguridad para dispositivos añadidos a la aplicación.

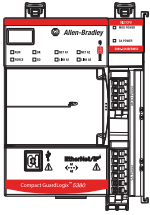


Para obtener una explicación del número de red de seguridad, consulte el documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#).

Para obtener información sobre cómo asignar el SNN, vea [Asignación del número de red de seguridad \(SNN\) en la página 88](#).

Firma de seguridad

Compact
GuardLogix



La firma de de seguridad está compuesta por un número de identificación, la fecha y la hora, información que identifica de manera única la parte de seguridad de un proyecto. Esta firma incluye la lógica, los datos y la configuración de seguridad.

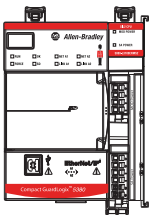
El sistema Compact GuardLogix 5380 utiliza la firma de seguridad para determinar la integridad del proyecto y para que pueda comprobar si se ha descargado el proyecto correcto al controlador receptor. La capacidad de crear, registrar y verificar la firma de seguridad es un aspecto obligatorio del proceso de desarrollo de la aplicación de seguridad.

Una firma de seguridad debe estar presente para funcionar como un controlador de seguridad SIL 2/PLd.

Consulte [Generación de la firma de seguridad en la página 262](#) para obtener más información.

Diferenciación entre componentes estándar y de seguridad

Compact
GuardLogix



Las ranuras de un chasis del sistema Compact GuardLogix 5380 no utilizadas por la función de seguridad se pueden usar para otros módulos de E/S Compact 5000™ certificados de acuerdo a las directivas de bajo voltaje y de compatibilidad electromagnética. Visite <http://www.rockwellautomation.com/rockwellautomation/certification/ce.page> para encontrar el certificado CE para la familia de productos CompactLogix y para determinar qué módulos están certificados.

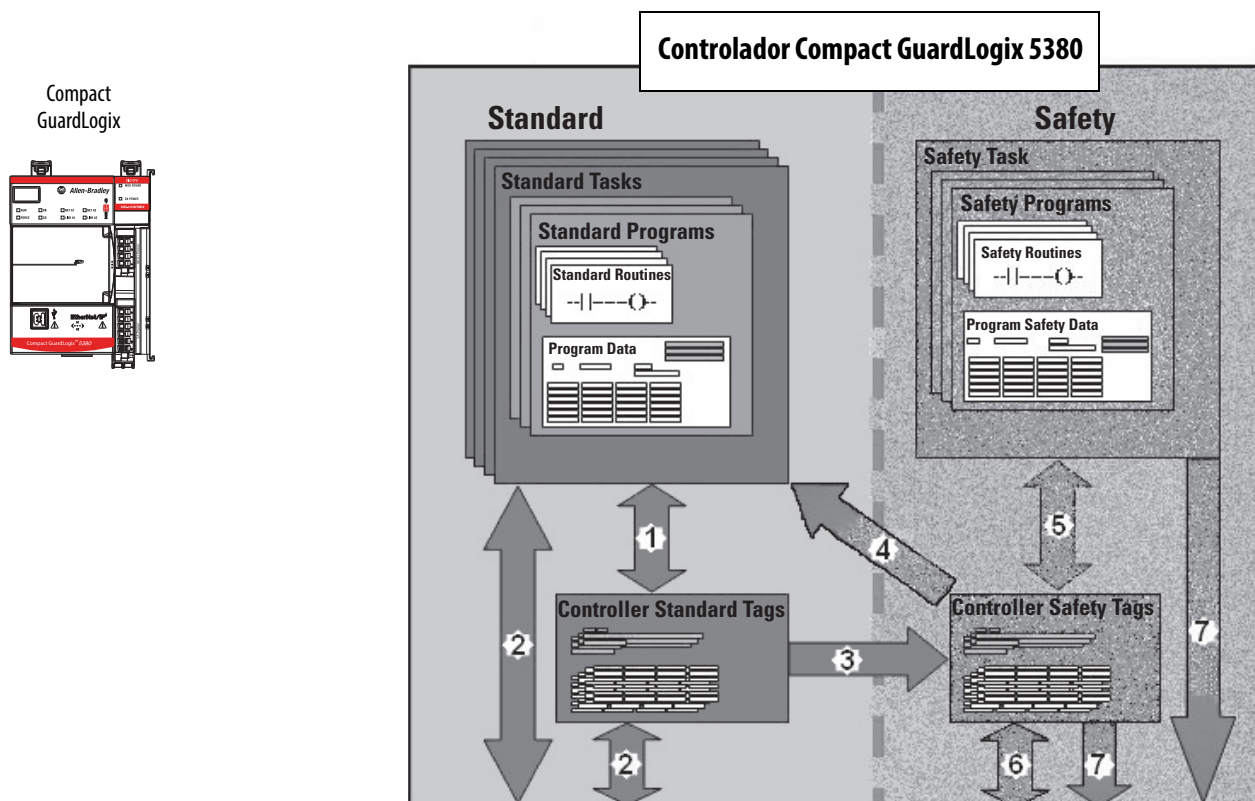
Usted debe crear y documentar una diferenciación clara, lógica y visible entre la parte estándar y la parte de seguridad del proyecto del controlador. Para ayudar a crear esta diferenciación, la aplicación Studio 5000 Logix Designer® cuenta con iconos de identificación de seguridad que identifican la tarea de seguridad, los programas de seguridad, las rutinas de seguridad y los componentes de seguridad.


Además, la aplicación Logix Designer utiliza un atributo de clase de seguridad que se muestra cada vez que se ven en pantalla propiedades de una tarea de seguridad, de un programa de seguridad, de una rutina de seguridad, de un tag de seguridad o de una instrucción Add-On de seguridad.

Capacidades de flujo de datos del controlador

Esta ilustración muestra las capacidades de flujo de datos estándar y de seguridad del controlador Compact GuardLogix 5380.

Figura 16 – Capacidades de flujo de datos



N.º	Descripción
1	Los tags y la lógica estándar se comportan de la misma manera que en un controlador CompactLogix 5380 estándar.
2	Los datos de tags estándar, bajo el control del programa o del controlador, pueden intercambiarse con dispositivos de HMI externos, computadoras personales y otros controladores.
3	Los controladores Compact GuardLogix 5380 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. Esta es la única manera de introducir datos de tags en la tarea de seguridad. La lógica de seguridad en la tarea de seguridad no puede leer ni escribir el tag estándar que es la fuente en la transferencia de datos de asignación de tags; solo puede hacer referencia al destino del tag de seguridad de la asignación. Sin embargo, sí puede leer y escribir dicho tag de seguridad.
	<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> ATENCIÓN: No se deben utilizar los datos de tag asignados para controlar directamente una salida SIL 2/PLd. </div> </div>
4	Los tags de seguridad bajo el control del controlador pueden ser leídos directamente por la lógica estándar.
5	Los tags de seguridad pueden ser leídos o escritos por la lógica de seguridad.
6	Los tags de seguridad se pueden intercambiar entre los controladores de seguridad a través de las redes Ethernet, incluidos los controladores 1756 GuardLogix y 5069 Compact GuardLogix.
7	Los datos de tags de seguridad, bajo el control del programa o del controlador, pueden ser leídos por dispositivos externos tales como dispositivos de HMI, computadoras personales u otros controladores estándar. Los dispositivos no pueden escribir a los tags de seguridad (independientemente de que el controlador esté protegido o no). Una vez que los datos se leen, se consideran datos estándar, no datos SIL 2/PLd.

Terminología de seguridad

En la tabla siguiente se definen los términos utilizados en este manual.

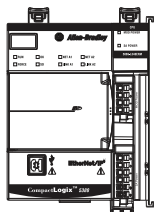
Abreviatura	Término completo	Definición
1oo1	Uno de uno	Identifica la arquitectura del controlador electrónico programable. 1oo1 es un sistema de un solo canal.
1oo2	Uno de dos	Identifica la arquitectura del controlador electrónico programable. 1oo2 es un sistema de dos canales.
CIP Safety	Common Industrial Protocol (protocolo industrial común) – Certificado de seguridad	Versión de CIP con clasificación SIL 2/PLd.
DC	Cobertura del diagnóstico	Relación entre la tasa de fallos detectados y la tasa total de fallos.
PFD	Probabilidad de fallo a demanda	Probabilidad promedio de que un sistema falle al realizar bajo demanda la función para la que está diseñado.
PFH	Probabilidad de fallo por hora	Probabilidad de que un sistema experimente un fallo peligroso por hora.
PL	Nivel de rendimiento	Clasificación de seguridad ISO 13849-1
SIL	Nivel de integridad de seguridad	Un nivel relativo de reducción de riesgo proporcionado por una función de seguridad o para especificar un nivel específico de reducción de riesgo.
SIL CL	Límite de reclamo SIL	El nivel de integridad de seguridad (SIL) máximo que se puede conseguir.
SNN	Número de red de seguridad	Número único que identifica una sección de una red de seguridad.
UNID	ID de nodo única (también conocida como referencia de nodo única)	Esta referencia única es una combinación de un número de red de seguridad (SNN) y la dirección de nodo del propio nodo.

Notas:

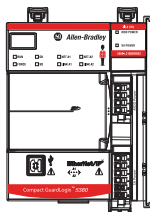
Conexión al controlador

Tema	Página
Configuración de drivers EtherNet/IP y USB en la estación de trabajo	56
Opciones de conexión	63
Establecimiento de la dirección IP del controlador	65
Actualización del firmware del controlador	74

CompactLogix



Compact GuardLogix



Se establece una conexión a un controlador a través de software basado en Linx. Para utilizar el software basado en Linx, hay que utilizar un driver de comunicación que corresponda a las conexiones de cable.

Por ejemplo, antes de poder conectar el controlador con un cable Ethernet, deberá crear un driver EtherNet/IP en el software basado en Linx.

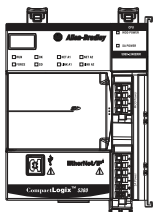
SUGERENCIA Los procedimientos de ejemplo en este capítulo utilizan RSLinx® Classic. En caso de usarse otro software de comunicación basado en Linx, el procedimiento puede variar ligeramente. Consulte la ayuda en línea para su software basado en Linx.

Se necesita un driver de comunicación para llevar a cabo estas tareas:

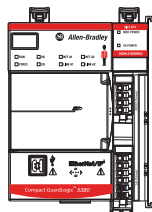
- Cargar y descargar proyectos de aplicación Studio 5000 Logix Designer®
- Actualice el firmware del controlador
- Establecer o cambiar la dirección del controlador
- Recolectar datos del controlador para interfaces electrónicas de operador a través de una red Ethernet
- Conectar RSNetWorx™ para EtherNet/IP a la red Ethernet para el monitoreo en línea del uso de recursos de red.

Configuración de drivers EtherNet/IP y USB en la estación de trabajo

CompactLogix



Compact GuardLogix



Antes de poder conectarse al controlador a través del puerto Ethernet o USB, hay que configurar el driver EtherNet/IP o USB en el software basado en Linux en la estación de trabajo.

Una estación de trabajo en la que se ejecuta la aplicación Studio 5000 Logix Designer puede utilizar estos drivers de comunicación:

- Driver EtherNet/IP:
 - Admite comunicaciones en tiempo de ejecución
 - Requiere que se configuren la estación de trabajo y el controlador
 - Admite la comunicación a través de distancias mayores en comparación con el driver USB
- Driver de dispositivos Ethernet:
 - Permite descargar un proyecto de la aplicación Logix Designer a un controlador que se encuentre en una red Ethernet cuando el controlador no esté conectado directamente a esa red
 - Requiere configurar las direcciones IP que el software debe explorar y, por tanto, los dispositivos con los que se comunica el controlador
- Driver USB:
 - Método adecuado para conectar a un controlador no configurado y configurar el puerto Ethernet
 - Método adecuado para conectar a un controlador cuando se desconoce la configuración del puerto Ethernet
 - Método adecuado para actualizar el firmware del controlador
 - No está concebido para conexiones en tiempo de ejecución; se trata de una conexión de uso únicamente temporal con una distancia de cableado limitada

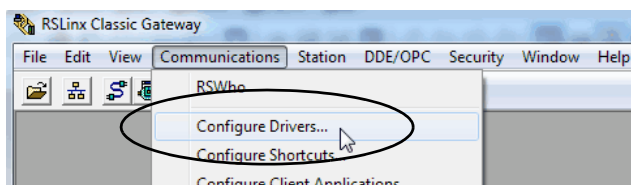
Configuración del driver EtherNet/IP en el software RSLinx Classic

Antes de añadir un driver Ethernet, confirme que se cumplen las siguientes condiciones:

- Se ha conectado debidamente la estación de trabajo a la red EtherNet/IP.
- Se han configurado correctamente la dirección IP y otros parámetros de red en la estación de trabajo.

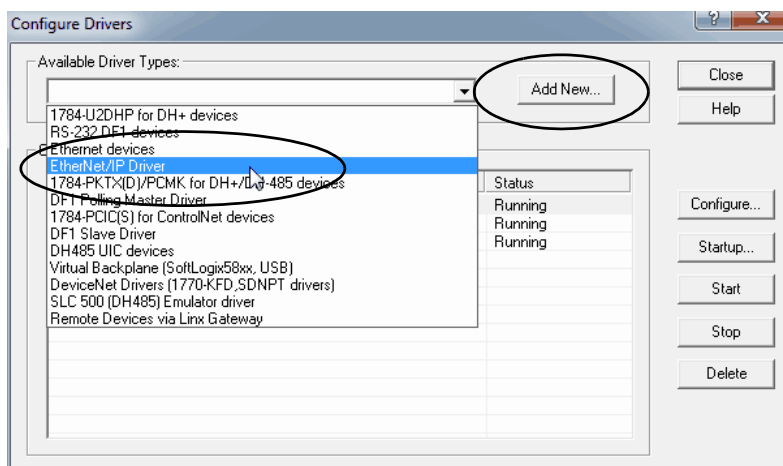
Para configurar el driver EtherNet/IP, siga estos pasos.

1. En el menú desplegable Communications, seleccione Configure Drivers.



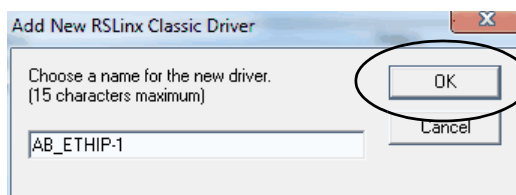
Aparecerá el cuadro de diálogo Configure Drivers.

2. En el menú desplegable Available Driver Types, elija EtherNet/IP Driver.
3. Haga clic en Add New.



Aparecerá el cuadro de diálogo Add New RSLinx Driver.

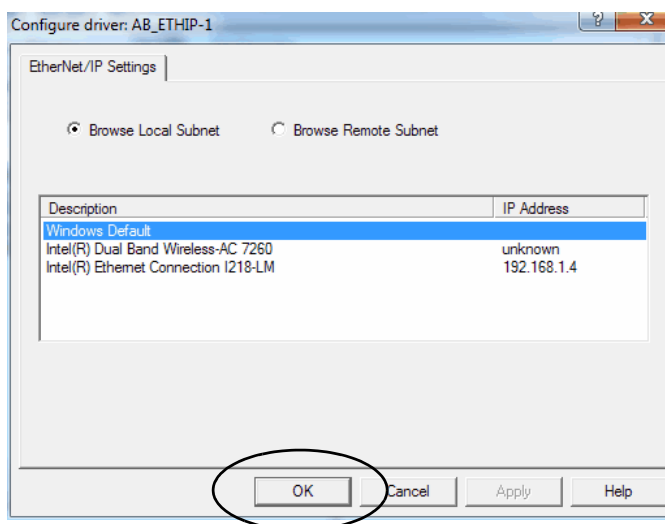
4. Escriba un nuevo nombre o utilice el nombre predeterminado y haga clic en OK.



Aparecerá el cuadro de diálogo Configure driver.

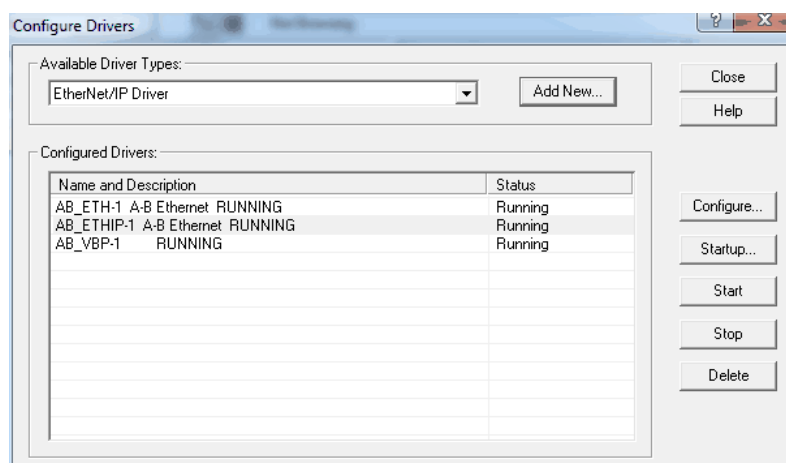
5. Haga clic en Browse Local Subnet.

SUGERENCIA Para ver los dispositivos de otra subred o VLAN desde la estación de trabajo donde se ejecuta el software de comunicación basado en Linx, haga clic en Browse Remote Subnet.



6. Seleccione el driver que desea utilizar.
7. Haga clic en OK para cerrar el cuadro de diálogo.

El nuevo driver estará disponible en el cuadro de diálogo Configure Drivers.



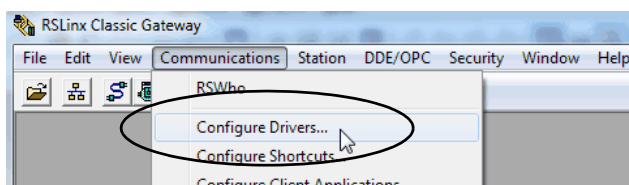
Configuración de los drivers de dispositivos Ethernet en el software RSLinx Classic

Deben cumplirse las siguientes condiciones para configurar un driver de dispositivos Ethernet:

- La estación de trabajo está conectada a una red Ethernet diferente a la del controlador receptor.
- Se han configurado correctamente la dirección IP y otros parámetros de red en la estación de trabajo.

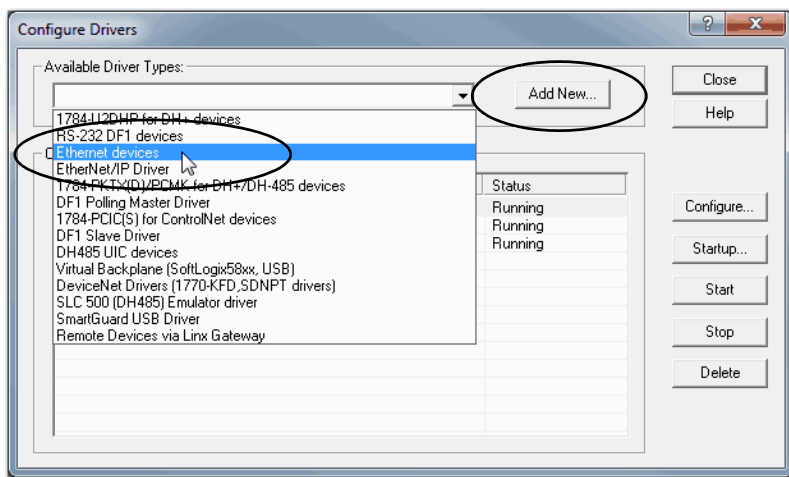
Para configurar el driver de dispositivos Ethernet, siga estos pasos.

1. En el menú desplegable Communications, seleccione Configure Drivers.



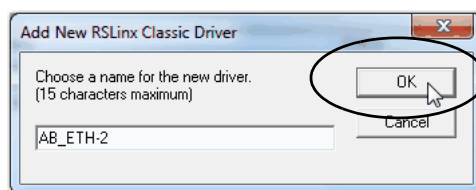
Aparecerá el cuadro de diálogo Configure Drivers.

2. En el menú desplegable Available Driver Types, seleccione Ethernet devices.
3. Haga clic en Add New.



Aparecerá el cuadro de diálogo Add New RSLinx Driver.

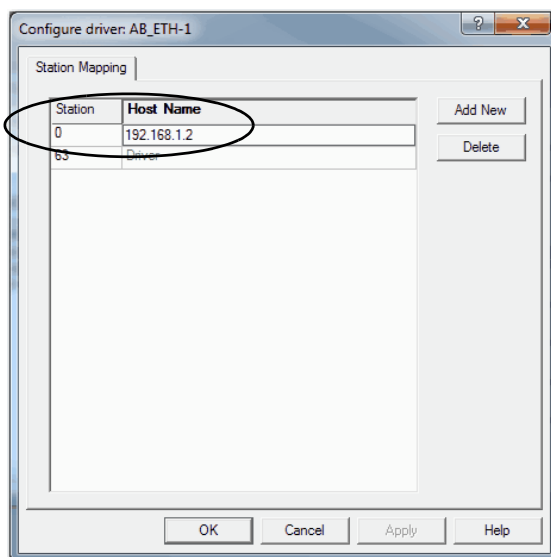
4. Puede utilizar el nombre predeterminado para la nueva unidad, o bien escribir un nuevo nombre y hacer clic en OK.



Aparecerá el cuadro de diálogo Configure driver.

5. En el cuadro de diálogo Configure driver, introduzca un nombre de anfitrión para cada estación que quiera explorar con el software RSLinx Classic.

El nombre de anfitrión es la dirección IP del dispositivo.



6. Haga clic en Add New para añadir estaciones y asigne a cada una un nombre de anfitrión.
7. Una vez que haya terminado de añadir estaciones, haga clic en OK.
8. En el cuadro de diálogo Configure Drivers, haga clic en Close.

Configuración del driver de comunicación USB en el software RSLinx Classic

En el software RSLinx Classic, versión 3.80.00 y posteriores, aparecerá automáticamente un driver USB en el software al conectar al controlador el cable USB de la estación de trabajo.

Tal vez tenga que esperar unos momentos para que el driver USB aparezca en el software RSLinx Classic.

IMPORTANTE Solo aparecerá un driver USB en el software RSLinx Classic cuando se haya conectado un cable USB entre la estación de trabajo y el controlador.

Una vez desconectado el cable, el driver desaparecerá del software RSLinx Classic.

Si utiliza el software RSLinx Classic, versión 3.80.00 y posteriores, y no aparece automáticamente un driver USB, lleve a cabo los siguientes pasos.

1. Confirme que el cable USB está conectado al controlador.

Aparecerá el cuadro de diálogo Found New Hardware Wizard.

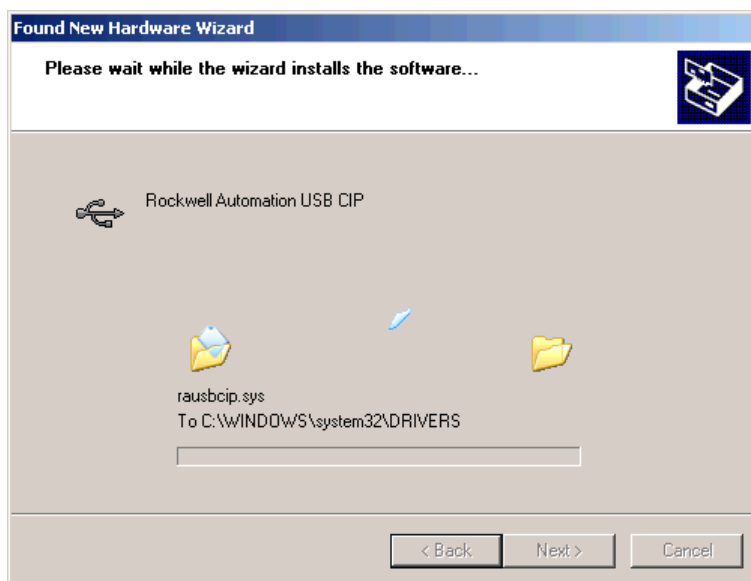
2. Haga clic en cualquiera de las opciones de conexión de Windows Update y haga clic en Next.



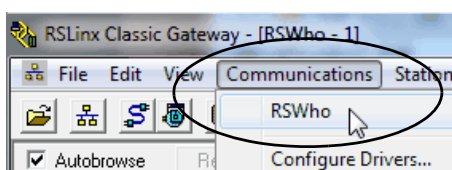
SUGERENCIA Si no encuentra el software para el driver USB y se cancela la instalación, verifique que tiene instalado el software RSLinx Classic, versión 3.80 o una posterior.

3. Haga clic en Install the software automatically (esto es lo recomendado) y haga clic en Next.

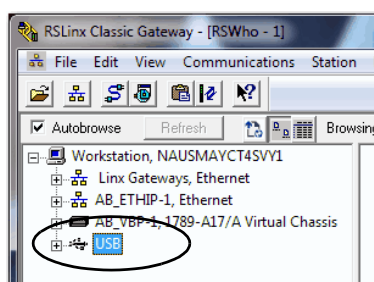
Se instala el software.



4. Haga clic en Finish para configurar el driver USB.
5. En el menú desplegable Communications, seleccione RSWho.

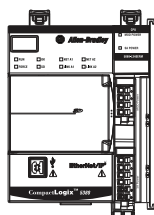


El driver del puerto USB aparece en el organizador de la estación de trabajo RSLink Classic.

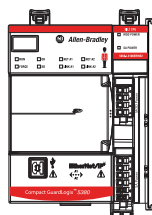


Opciones de conexión

CompactLogix



Compact GuardLogix



Antes de empezar a utilizar el controlador, hay que establecer una conexión al controlador. Asegúrese de que ya haya configurado los drivers de comunicación EtherNet/IP o USB (vea [Configuración de drivers EtherNet/IP y USB en la estación de trabajo en la página 56](#)).

Las opciones de conexión con el controlador incluyen:

- Cable Ethernet a un puerto Ethernet: Los puertos Ethernet del controlador aceptan velocidades de comunicación de 10 Mbps, 100 Mbps y 1 Gbps. Vea [Conexión de un cable Ethernet en la página 63](#).
- Cable USB al puerto USB: El puerto USB del controlador utiliza un receptáculo de tipo B y es compatible con USB 2.0. El puerto funciona a 12 Mbps. Vea [Conexión de un cable USB en la página 64](#).

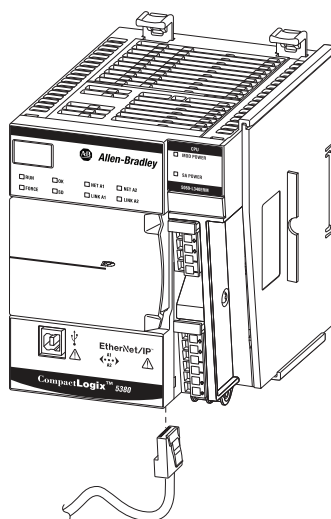
Conexión de un cable Ethernet

El gráfico del ejemplo muestra un controlador CompactLogix™ 5380. Usted realiza la misma tarea para conectar un cable Ethernet a un controlador Compact GuardLogix® 5380.



ADVERTENCIA: Si conecta o desconecta el cable de comunicaciones cuando el módulo o cualquier dispositivo de la red está conectado a la alimentación eléctrica, puede producirse un arco eléctrico. Esto podría causar una explosión en instalaciones ubicadas en zonas peligrosas. Antes de seguir adelante, asegúrese de desconectar la alimentación eléctrica o de verificar que la zona no sea peligrosa.

Si va a conectar el controlador directamente a una red EtherNet/IP, conecte un cable Ethernet CAT 5e o CAT 6 con un conector RJ45 a un puerto Ethernet del controlador.



Para obtener más información sobre cómo elegir el cable adecuado, consulte el documento Guidance for Selecting Cables for EtherNet/IP Networks, publicación [ENET-WP007-EN-P](#).

Conexión de un cable USB

Utilice la conexión USB para actualizar el firmware y descargar programas.

El gráfico del ejemplo muestra un controlador CompactLogix 5380. Usted realiza la misma tarea para conectar un cable Ethernet a un controlador Compact GuardLogix 5380.

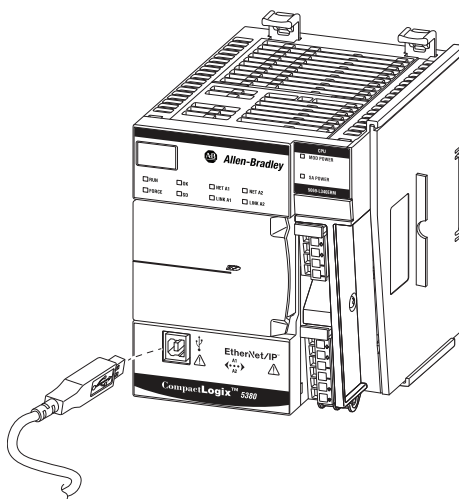


El puerto USB está diseñado solamente para programación local temporal, no para conexión permanente. El cable USB no debe medir más de 3.0 m (9.84 pies) y no debe contener concentradores.



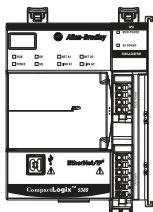
ADVERTENCIA: No use el puerto USB en zonas peligrosas.

Figura 17 – Conexión USB

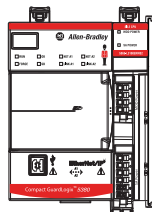


Establecimiento de la dirección IP del controlador

CompactLogix



Compact GuardLogix



Debe establecer la dirección IP de un controlador CompactLogix 5380 o Compact GuardLogix 5380 para que el controlador pueda funcionar en una red EtherNet/IP. Los controladores se envían sin dirección IP.

IMPORTANTE

Esta sección describe de forma general cómo se establece una dirección IP.

El modo EtherNet/IP en el que funciona el controlador afecta los ajustes y el uso de las direcciones IP del controlador. Por ejemplo, si el controlador funciona en modo de doble IP, debe establecer una dirección IP para cada puerto Ethernet del controlador. Es decir, debe llevar a cabo dos veces los pasos que se describen en esta sección; una vez para cada puerto.

Para obtener más información sobre cómo los modos EtherNet/IP afectan la dirección IP del controlador, consulte el Capítulo 9, [Uso de los modos EtherNet/IP en la página 141](#).

Además, las tareas descritas en esta sección muestran un controlador CompactLogix 5380. Usted lleva a cabo el mismo conjunto de tareas para establecer la dirección IP en un controlador Compact GuardLogix 5380.

Cuando el controlador está en su condición original, se cumple lo siguiente respecto a las direcciones IP:

- Los puertos Ethernet incorporados del controlador están configurados para obtener una dirección IP mediante un servidor DHCP.

Si no hay ningún servidor DHCP o el servidor DHCP no está configurado para establecer la dirección IP, deberá establecer manualmente la dirección IP.

- El controlador está configurado para que sea necesario establecer la dirección IP cada vez que se desconecte y se vuelva a conectar la alimentación eléctrica.

Puede configurar el controlador para que no sea preciso establecer una dirección IP cada vez que se desconecte y se vuelva a conectar la alimentación eléctrica.

- El controlador está configurado para utilizar el modo de doble IP. Por lo tanto, hay que establecer una dirección IP única para el puerto A1 y el puerto A2.

Puede utilizar estas herramientas para establecer la dirección IP:

- Herramienta BOOTP-DHCP
- Servidor DHCP
- Software RSLinx® Classic
- Tarjeta SD

Cada herramienta tiene requisitos de conexión para establecer la dirección IP mediante dicha herramienta. Por ejemplo, la computadora debe estar conectada al controlador mediante un cable USB para establecer la dirección IP inicial del controlador con el software o la aplicación RSLinx Classic.

Para funcionar en una red EtherNet/IP, debe definir estos parámetros.

Parámetro de red EtherNet/IP	Descripción
Dirección IP	<p>La dirección IP identifica el módulo de manera única. La dirección IP se expresa en el formato <code>xxx.xxx.xxx.xxx</code> donde cada <code>xxx</code> es un número comprendido entre 000 y 255.</p> <p>Hay varios valores reservados que no puede utilizar como primer octeto de la dirección. Estos números son ejemplos de valores que no puede utilizar:</p> <p>001.xxx.xxx.xxx 127.xxx.xxx.xxx 223 a 255.xxx.xxx.xxx</p> <p>Los valores reservados específicos que no se pueden utilizar cambian según las condiciones de cada aplicación. Los valores anteriores son solo ejemplos de valores reservados.</p>
Máscara de subred	La máscara de subred divide las direcciones IP en una dirección de red y una dirección de anfitrión. Esta define si el controlador intercambia directamente paquetes Ethernet con otro dispositivo o si encamina paquetes a través de la gateway. Este campo se establece de forma predeterminada como 0.0.0.0.
Gateway	Una gateway conecta redes físicas individuales en un sistema de redes. Si un nodo se comunica con otro nodo de otra red, una gateway transfiere los datos entre las dos redes. Este campo se establece de forma predeterminada como 0.0.0.0.

Si utiliza el direccionamiento del sistema de nombres de dominio (DNS) o hace referencia al controlador mediante el nombre del anfitrión en las instrucciones MSG, defina estos parámetros.

Tabla 5 – Parámetros de red EtherNet/IP para direccionamiento DNS

Parámetro de red EtherNet/IP	Descripción
Nombre de anfitrión	<p>Un nombre de anfitrión forma parte de una dirección de texto que identifica el anfitrión de un módulo. La dirección de texto completa de un módulo es <code>host_name.domain_name</code>.</p> <p>Consideraciones de seguridad</p> <ul style="list-style-type: none"> No se permite que las conexiones de seguridad utilicen nombres de anfitrión (esto requiere la búsqueda DNS, la cual no se permite para las E/S de seguridad). Los dispositivos de seguridad en redes EtherNet/IP no presentan el parámetro del nombre de anfitrión. Los dispositivos estándar sí presentan el parámetro del nombre de anfitrión, independientemente de si el proyecto sea de seguridad o estándar. Los controladores Compact GuardLogix 5380 pueden tener conexiones de seguridad o conexiones estándar. Cuando se usan en un proyecto estándar, los controladores GuardLogix 5580 se consideran dispositivos estándar (las únicas conexiones son tags consumidos estándar), por lo que el controlador presenta el parámetro del nombre de anfitrión. Cuando los controladores Compact GuardLogix 5380 se utilizan en un proyecto de seguridad, se supone que son dispositivos de seguridad y el parámetro del nombre de anfitrión no se presenta.
Nombre de dominio	<p>Un nombre de dominio forma parte de una dirección de texto que identifica el dominio en el que se encuentra el módulo. La dirección de texto completa de un módulo es <code>host_name.domain_name</code>. El nombre de dominio tiene un límite de 48 caracteres.</p> <p>Si especifica un servidor DNS, deberá escribir un nombre de dominio. Además, si envía correo electrónico desde el módulo, algunos servidores de retransmisión de correo requieren un nombre de dominio durante el handshake inicial de la sesión SMTP.</p>
Dirección de servidor DNS primario	<p>Una dirección que identifica cualquier servidor DNS que se utilice en la red. Usted debe tener un servidor DNS si ha especificado un nombre de dominio o un nombre de anfitrión en la configuración del módulo. El servidor DNS convierte el nombre de dominio o el nombre de anfitrión en una dirección IP que utiliza la red.</p> <p>Para obtener más información acerca del direccionamiento DNS, consulte la página 72.</p>
Dirección de servidor DNS secundario	

Establecimiento de la dirección IP con la herramienta de puesta en marcha BOOTP DHCP EtherNet/IP

Los controladores están habilitados para DHCP de manera predeterminada.

La herramienta BOOTP-DHCP es una herramienta independiente que puede utilizar para establecer una dirección IP. Cuando se utiliza, la herramienta BOOTP-DHCP establece una dirección IP y otros parámetros del Transport Control Protocol (TCP).

La herramienta BOOTP-DHCP se instala automáticamente al instalar el software RSLinx Classic o la aplicación Logix Designer en una computadora.

Obtenga acceso a la herramienta BOOTP-DHCP desde una de estas ubicaciones:

- Programs > Rockwell Software > BOOTP-DHCP Server

Si no ha instalado el servidor, puede descargarlo e instalarlo desde <http://www.ab.com/networks/ethernet/bootp.html>.

- Directorio Tools del CD de instalación del ambiente Studio 5000®

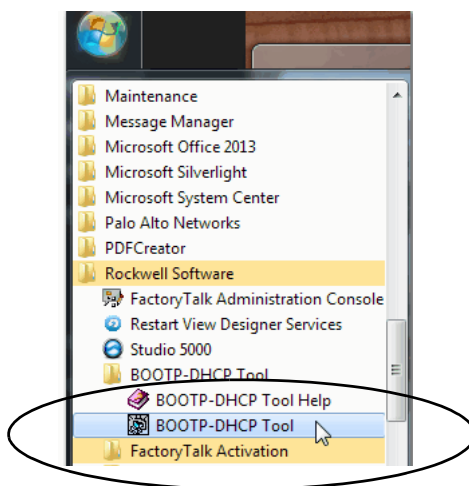
IMPORTANTE Antes de iniciar la herramienta BOOTP-DHCP, asegúrese de tener la dirección de hardware del módulo (MAC).

La dirección MAC se muestra en la pantalla de estado del controlador que está en la parte frontal del controlador. La dirección utiliza un formato similar al siguiente:

00-00-BC-14-55-35

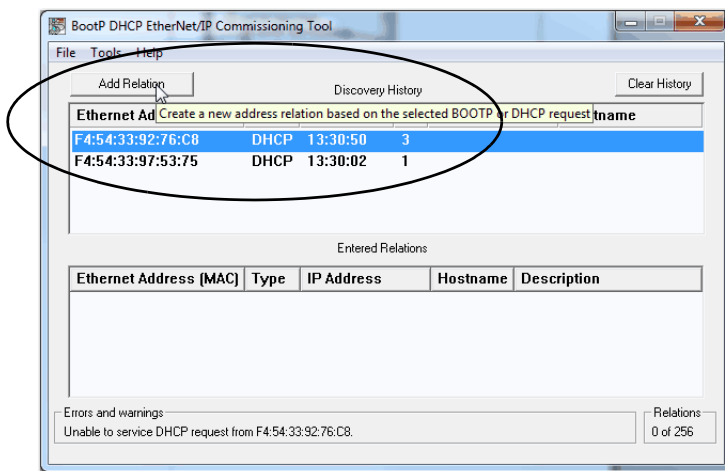
Para establecer la dirección IP con la herramienta BOOTP-DHCP, siga estos pasos.

1. Conecte la estación de trabajo a la red Ethernet donde se encuentra el controlador.
2. Inicie la herramienta BOOTP-DHCP.



La dirección MAC del controlador aparecerá en la ventana Request History.

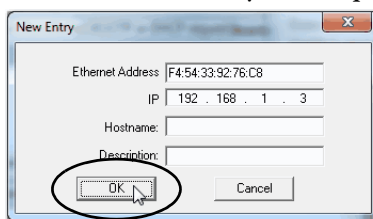
3. Seleccione el controlador adecuado y haga clic en Add to Relation List.



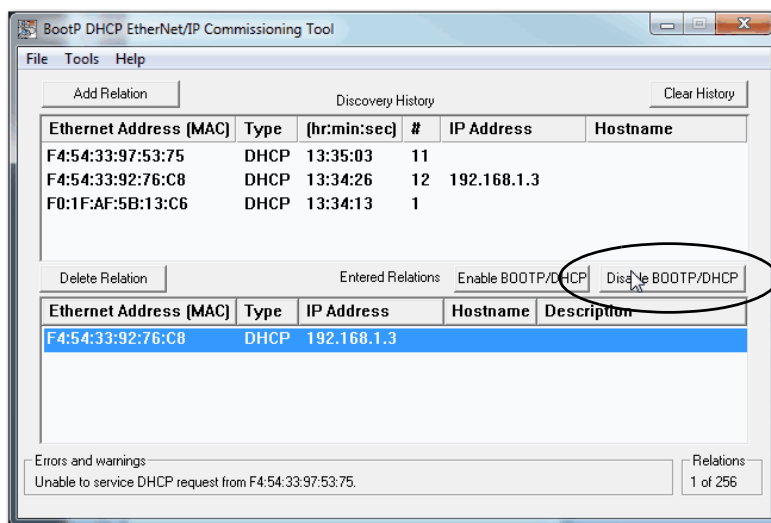
Aparece el cuadro de diálogo New Entry.

4. Escriba la dirección IP, el nombre del anfitrión y la descripción del módulo.

El nombre del anfitrión y la descripción son opcionales.



5. Haga clic en OK.
6. Para asignar esta configuración al módulo, espere a que el módulo aparezca en el panel Relation List y selecciónelo.
7. Haga clic en Disable BOOTP/DHCP.



Ahora el módulo utiliza la configuración asignada y no emite solicitudes BOOTP o DHCP después de desconectarse y volver a conectarse la alimentación eléctrica al controlador.

IMPORTANTE Recuerde lo siguiente:

- Si no hace clic en Disable BOOTP/DHCP, cada vez que apague y encienda el controlador se borrará la configuración de IP actual y el controlador volverá a enviar solicitudes de DHCP.
- Si hace clic en Disable BOOTP/DHCP y no inhabilita BOOTP/DHCP, puede utilizar el software RSLinx Classic para inhabilitar BOOTP/DHCP.

Para obtener más información sobre cómo utilizar el software RSLinx Classic para inhabilitar BOOTP/DHCP, consulte la [página 69](#).

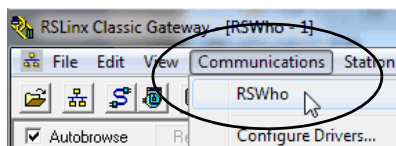
Inhabilitación de BOOTP/DHCP mediante el uso del software RSLinx Classic

Para inhabilitar BOOTP/DHCP mediante el software RSLinx Classic, siga estos pasos.

1. Inicie el software RSLinx Classic.

Tras varios segundos, aparecerá un cuadro de diálogo RSWHo.

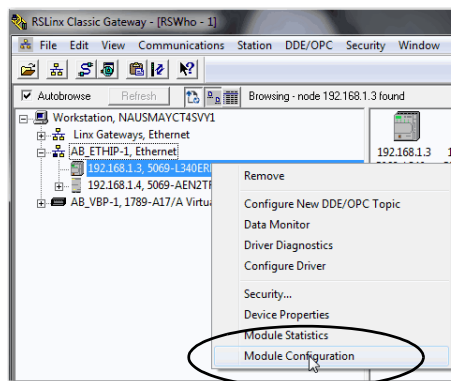
2. Si no aparece ningún cuadro de diálogo RSWHo, elija RSWHo en el menú desplegable Communications.



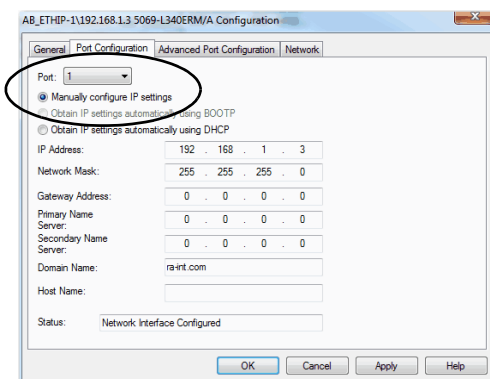
3. Desplácese al controlador.

Puede obtener acceso al controlador mediante el USB o un driver EtherNet/IP.

4. Haga clic con el botón derecho del mouse en el controlador y elija Module Configuration.



5. Haga clic en la ficha Port Configuration.
6. En Network Configuration Type, haga clic en Static para inhabilitar BOOTP/DHCP.



7. Haga clic en OK.

Uso del servidor DHCP para establecer la dirección IP del controlador

Dado que los controladores están habilitados para DHCP cuando se encuentran en su condición original, puede utilizar un servidor DHCP para establecer la dirección IP.

El servidor DHCP asigna automáticamente direcciones IP a las estaciones cliente que se conectan a una red TCP/IP. El DHCP se basa en BOOTP y mantiene cierta compatibilidad con las versiones anteriores.



ATENCIÓN: Puede utilizar un servidor DHCP configurado para asignar siempre la misma dirección IP a dispositivos específicos cuando aparecen en la red EtherNet/IP y solicitan una dirección IP.

Si su sistema **no** utiliza un servidor DHCP que asigne la misma dirección IP a dispositivos específicos, le recomendamos encarecidamente que asigne el controlador a una dirección IP fija. No establezca la dirección IP dinámicamente. Es decir, no utilice la opción Obtain IP settings automatically by using DHCP en el software RSLinx Classic o la aplicación Logix Designer.

Cuando un controlador utiliza la opción Obtain IP settings automatically by using DHCP, la dirección IP de dicho controlador se borra cada vez que se desconecta y vuelve a conectarse a la alimentación eléctrica. Si la misma dirección IP no se asigna automáticamente al controlador mediante un servidor DHCP, cuando solicita una nueva dirección IP, se le puede asignar una nueva dirección IP.

El uso de una nueva dirección IP puede producir consecuencias inesperadas. Por ejemplo, puede existir una condición Duplicate IP Address o el controlador puede experimentar fallos de configuración puesto que la dirección IP es diferente a la almacenada en el proyecto de aplicación Logix Designer.

Ignorar esta precaución puede producir un movimiento no deseado de la máquina o una pérdida del control del proceso.

Detección de direcciones IP duplicadas

El controlador verifica que su dirección IP no coincida con la dirección IP de ningún otro dispositivo de la red cuando realiza cualquiera de las siguientes tareas:

- Conexión del controlador a una red EtherNet/IP.
- Cambio de la dirección IP del controlador.

Si la dirección IP del controlador coincide con la de otro dispositivo de la red, el puerto Ethernet del controlador entra en modo de conflicto. En el modo de conflicto, ocurre lo siguiente:

- El indicador de estado de red (NET) aparece de color rojo fijo.
- La pantalla de 4 caracteres indica el conflicto.

La pantalla muestra: <IP_address_of_this_module> Duplicate IP
<Mac_address_of_duplicate_node_detected>

Por ejemplo: 192.168.1.1 Duplicate IP – 00:00:BC:02:34:B4

Resolución de direcciones IP duplicadas

Cuando dos dispositivos de una red tienen direcciones IP que están en conflicto, la resolución depende de las condiciones en las que se detecte la duplicación. La siguiente tabla describe cómo se resuelven las direcciones IP duplicadas.

Condiciones de detección de direcciones IP duplicadas	Proceso de resolución
<ul style="list-style-type: none"> • Ambos dispositivos admiten la detección de direcciones IP duplicadas. • El segundo dispositivo se añade a la red después de que el primer dispositivo esté funcionando en la red. 	<ol style="list-style-type: none"> 1. El dispositivo que comenzó a funcionar primero utiliza la dirección IP y sigue funcionando sin interrupción. 2. El dispositivo que comenzó a funcionar en segundo lugar detecta la duplicación y entra en modo de conflicto. <p>Para asignar una nueva dirección IP al controlador y salir del modo de conflicto, consulte Establecimiento de la dirección IP con la herramienta de puesta en marcha BOOTP DHCP EtherNet/IP en la página 67.</p>
<ul style="list-style-type: none"> • Ambos dispositivos admiten la detección de direcciones IP duplicadas. • Ambos dispositivos se encendieron aproximadamente al mismo tiempo. 	<p>Ambos dispositivos EtherNet/IP entran en modo de conflicto.</p> <p>Para resolver este conflicto, siga estos pasos:</p> <ol style="list-style-type: none"> a. Asigne una nueva dirección IP al controlador. Para obtener más información, consulte Establecimiento de la dirección IP con la herramienta de puesta en marcha BOOTP DHCP EtherNet/IP en la página 67. b. Desconecte y vuelva a conectar la alimentación eléctrica al otro dispositivo.
Un dispositivo admite la detección de direcciones IP duplicadas y el otro no.	<ol style="list-style-type: none"> 1. Independientemente de qué dispositivo haya obtenido en primer lugar la dirección IP, el dispositivo que no admite la detección de direcciones IP utiliza la dirección IP y sigue funcionando sin interrupción. 2. El dispositivo que admite la detección de direcciones IP duplicadas detecta la duplicación y entra en el modo de conflicto. <p>Para asignar una nueva dirección IP al controlador y salir del modo de conflicto, consulte Establecimiento de la dirección IP con la herramienta de puesta en marcha BOOTP DHCP EtherNet/IP en la página 67.</p>

Direccionamiento DNS

También puede utilizar el direccionamiento DNS para especificar un nombre de anfitrión para un controlador, un nombre de dominio y servidores DNS. El direccionamiento DNS hace posible configurar estructuras de red similares y secuencias de direcciones IP en dominios diferentes.

El direccionamiento DNS solo es necesario si hace referencia al controlador mediante el nombre de anfitrión, como en las descripciones de rutas de las instrucciones MSG.

Para utilizar el direccionamiento DNS, siga estos pasos.

1. Asigne un nombre de anfitrión al controlador.

Un administrador de red puede asignar un nombre de anfitrión. Los nombres de anfitrión válidos deben cumplir la norma IEC-1131-3.

2. Configure los parámetros del controlador.

3. Configure la dirección IP, la máscara de subred, la dirección de la gateway, un nombre de anfitrión para el controlador, nombre de dominio y direcciones del servidor DNS primario/secundario.

En el servidor DNS, el nombre de anfitrión debe coincidir con la dirección IP del controlador.

4. En la aplicación Logix Designer, añada el controlador al árbol de configuración de E/S.

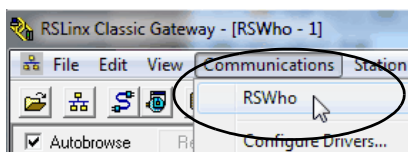
IMPORTANTE Recuerde lo siguiente:

- Si un módulo secundario se encuentra en el mismo dominio que el módulo principal, escriba el nombre de anfitrión. Si el dominio del módulo secundario es diferente del dominio de su módulo principal, escriba el nombre de anfitrión y el nombre de dominio (hostname.domainname)
 - También puede utilizar el direccionamiento DNS en un perfil de módulo en el árbol del controlador de E/S o en una ruta de mensaje. Si el nombre de dominio del módulo de destino es diferente al nombre de dominio del módulo de origen, utilice un nombre de DNS plenamente calificado (hostname.domainname). Por ejemplo, para enviar un mensaje de EN2T1.location1.companyA a EN2T1.location2.companyA, los nombres de anfitrión son idénticos pero los dominios son diferentes. A falta de un nombre de DNS completo, el módulo añade el nombre de dominio predeterminado al nombre de anfitrión especificado.
-

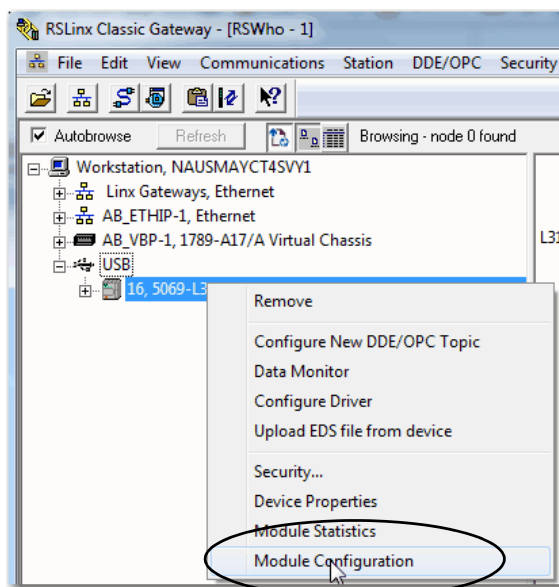
Uso del software RSLinx Classic para establecer la dirección IP del controlador

Siga estos pasos para establecer la dirección IP del controlador mediante el software RSLinx Classic.

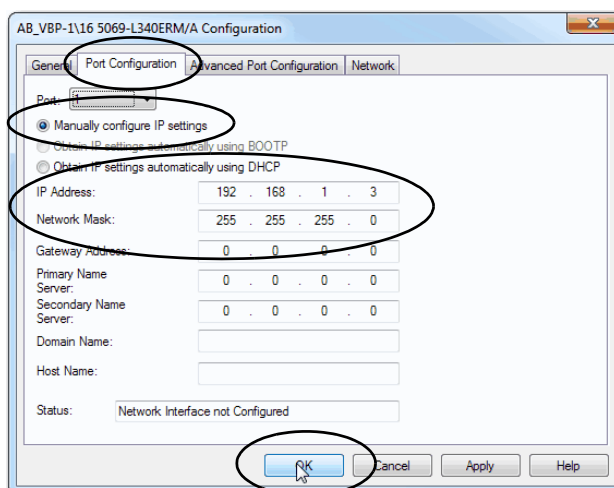
1. Confirme que la computadora está conectada al controlador mediante un cable USB.
2. Inicie el software RSLinx Classic. Tras varios segundos, aparecerá un cuadro de diálogo RSWho.
3. Si no aparece el cuadro de diálogo RSWho, elija RSWho en el menú desplegable Communications.



4. Navegue al controlador mediante el driver USB.
5. Haga clic con el botón derecho del mouse en el controlador y seleccione Module Configuration.



6. En la ficha Port Configuration, haga clic en Manually configure IP settings for the port.
7. Asigne los parámetros de configuración del puerto y haga clic en OK.



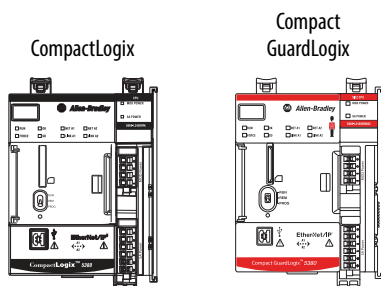
Uso de una tarjeta Secure Digital para establecer la dirección IP del controlador

Puede utilizar una tarjeta SD para establecer la dirección IP del controlador. La tarjeta SD puede establecer la dirección IP cuando se carga un proyecto en el controlador.

Para obtener más información sobre cómo utilizar una tarjeta SD, consulte el Capítulo 7, [Uso de la tarjeta Secure Digital en la página 117](#).

Actualización del firmware del controlador

El controlador se envía con la revisión de firmware 1.xxx instalada. Debe actualizar la revisión del firmware antes de poder utilizarlo en un proyecto de la aplicación Logix Designer.



IMPORTANTE El controlador debe estar en el modo de programación remota o en el modo de programación, y habrá que borrar todos los fallos recuperables mayores para aceptar las actualizaciones.

IMPORTANTE Consideraciones de seguridad

No es posible actualizar un controlador bloqueado por seguridad.

Puede utilizar las siguientes herramientas para actualizar el firmware del controlador:

- Software ControlFLASH™ o ControlFLASH Plus™
- Función AutoFlash de la aplicación Logix Designer

Siga estos pasos para actualizar el firmware del controlador:

- [Determine el firmware del controlador necesario](#)
- [Obtención del firmware del controlador](#)
- [Uso del software ControlFLASH para actualizar el firmware](#)
- [Uso de AutoFlash para actualizar el firmware](#)

IMPORTANTE Esta sección describe de forma general cómo se actualiza el firmware del controlador.

Los cambios del firmware pueden tener efectos diferentes sobre el controlador según las condiciones en que se encontraba el sistema cuando se aplicó el cambio, en especial respecto al modo EtherNet/IP que se utilizaba.

Para obtener más información sobre cómo los cambios en la revisión del firmware del controlador pueden afectar la configuración del controlador en lo que respecta al uso del modo EtherNet/IP, consulte el Capítulo 9, [Uso de los modos EtherNet/IP en la página 141](#).

Determine el firmware del controlador necesario

IMPORTANTE El controlador debe estar en el modo de programación remota o en el modo de programación, y habrá que borrar todos los fallos recuperables mayores para aceptar las actualizaciones.

El nivel de revisión mayor del firmware debe coincidir con el nivel de versión mayor del software. Por ejemplo, si la revisión del firmware del controlador es la 31.xxx, deberá utilizar la versión 31 de la aplicación Logix Designer.

No todos los controladores aceptan las mismas revisiones de firmware mínimas.

Asegúrese de conocer la revisión de firmware apropiada y la versión de software compatible para su controlador antes de obtener y actualizar el firmware.

Descargue el firmware, los archivos asociados (tales como AOP, EDS y DTM) y consulte las notas de la versión del producto en el Centro de compatibilidad y descarga de productos (PCDC) en <http://compatibility.rockwellautomation.com/Pages/home.aspx>.

Obtención del firmware del controlador

Puede obtener el firmware del controlador de las siguientes maneras:

- El firmware viene empaquetado como parte de la instalación de la aplicación Studio 5000 Logix Designer.

IMPORTANTE El firmware que viene empaquetado con la instalación del software es la versión inicial del firmware del controlador. Es posible que se publiquen otras revisiones del firmware.

Recomendamos que visite el PCDC para determinar si están disponibles revisiones posteriores del firmware del controlador. Para obtener más información, consulte la siguiente viñeta.

- Descargue el firmware, los archivos asociados y consulte las notas de la versión del producto desde el PCDC en:

<http://www.rockwellautomation.com/rockwellautomation/support/pcdc.page>

Uso del software ControlFLASH para actualizar el firmware

IMPORTANTE Dependiendo del número de catálogo, la versión de aplicación Logix Designer y la revisión de firmware utilizadas, los controladores CompactLogix 5380 y Compact GuardLogix 5380 tienen requisitos mínimos diferentes de la versión de software ControlFLASH™.

Para determinar la versión de software mínima para su aplicación, visite el PCDC en: <http://www.rockwellautomation.com/rockwellautomation/support/pcdc.page>.

El software ControlFLASH está disponible como:

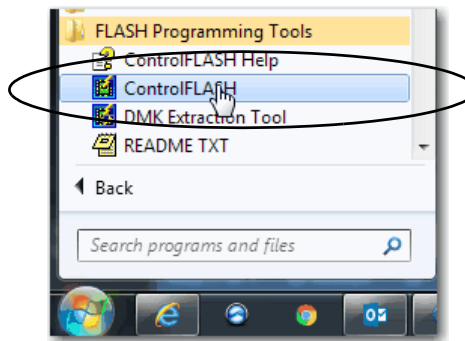
- Parte del proceso de instalación de la aplicación Studio 5000 Logix Designer
- Descarga autónoma del PCDC



ATENCIÓN: Si la tarjeta Secure Digital (SD) está bloqueada y establecida para cargarse durante la puesta en marcha, esta actualización puede ser sobrescrita por el firmware que haya en la tarjeta SD.

Para obtener más información sobre el uso de tarjetas SD, consulte el Capítulo 7, [Uso de la tarjeta Secure Digital en la página 117](#).

1. Compruebe lo siguiente:
 - Se ha establecido una conexión de red.
 - El driver de red ha sido configurado en el software de comunicación basado en Linx.
 - El controlador está en modo de programación o programación remota y se han eliminado todos los fallos mayores recuperables.
2. En el menú Start de Windows, haga clic en FLASH Programming Tools > ControlFLASH.

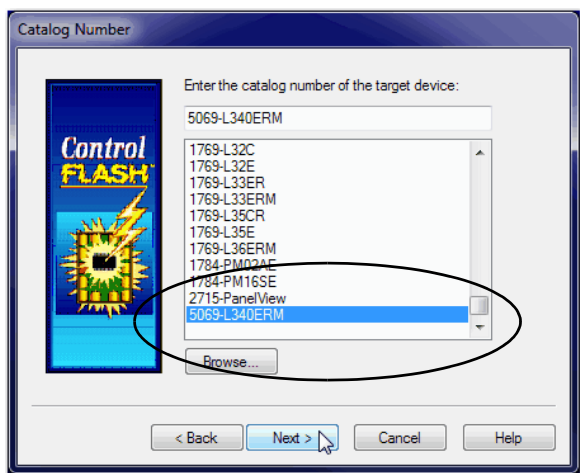


3. Haga clic en Next.

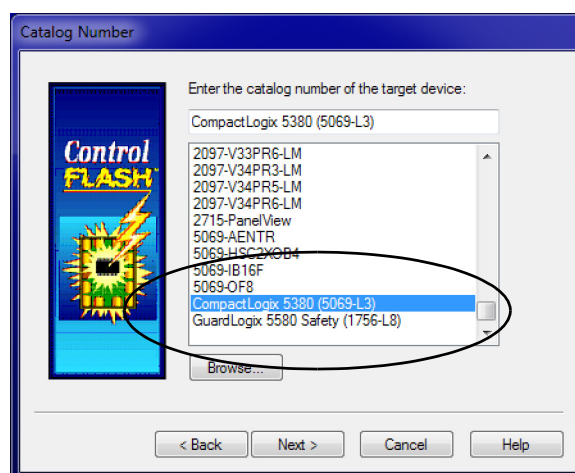


4. Seleccione el controlador y haga clic en Next.

ControlFLASH, versión 15.01.00 y posteriores, tiene un nombre de familia que se aplica a todos los controladores en dicha familia, en vez de números de catálogo individuales de controladores.

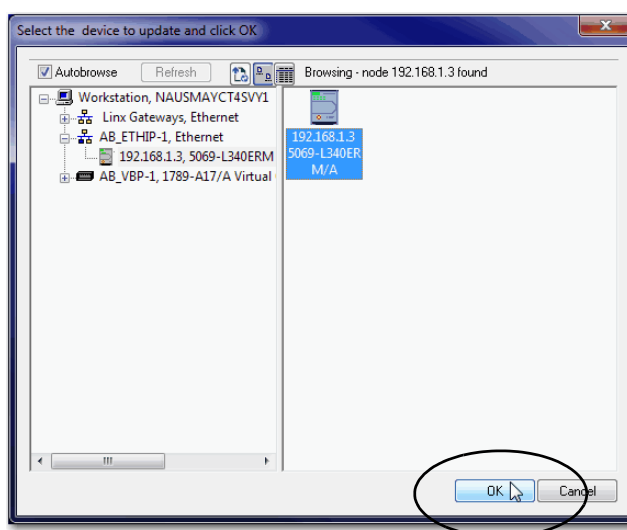


Versión ControlFLASH 14.01.00 y anteriores



ControlFLASH, versión 15.01.00 y posteriores

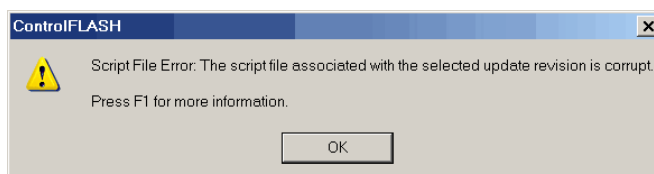
5. Expanda la ruta de comunicación y seleccione el controlador.
6. Haga clic en OK.



7. Seleccione la revisión del firmware y haga clic en Next.

Si la revisión de firmware que necesita no aparece en la lista, seleccione Show all revisions.

SUGERENCIA Si aparece Script File Error después de seleccionar el número de revisión del firmware, tal como se indica, puede haber un problema con los archivos del firmware.

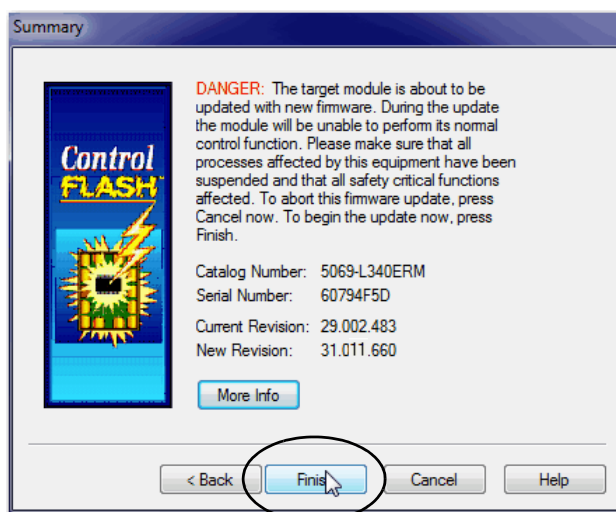


Le recomendamos que utilice la versión más reciente del software ControlFLASH. Si no es así, actualice en primer lugar a la versión más reciente.

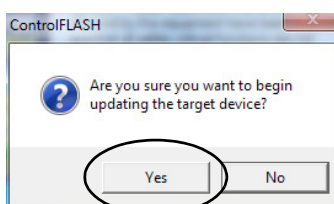
Para resolver el problema, haga lo siguiente:

- Visite <http://www.rockwellautomation.com/support/> y descargue la revisión de firmware a la que desea actualizar. Reemplace la revisión de firmware que instaló previamente por la obtenida del sitio web de asistencia técnica.
- Si la revisión de firmware de reemplazo no resuelve el problema, comuníquese con el grupo de asistencia técnica de Rockwell Automation.

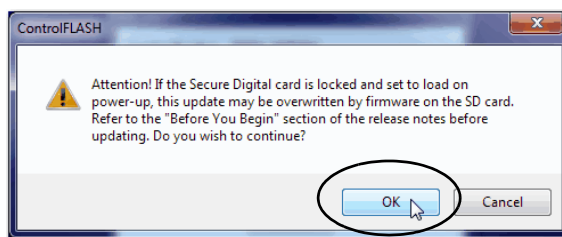
8. En la pantalla Summary, haga clic en Finish.



9. Cuando aparezca un cuadro de diálogo de confirmación, haga clic en Yes.



Antes de que comience la actualización del firmware, aparecerá este cuadro de diálogo. Elija la acción adecuada para su aplicación. En este ejemplo, la actualización continúa al hacer clic en OK.



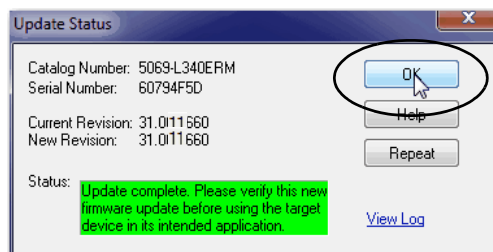
El cuadro de diálogo de progreso indica el progreso de la actualización de firmware. Los controladores indican el progreso en actualizaciones y bloques.

IMPORTANTE Espere a que finalice la actualización del firmware antes de desconectar y volver a conectar la alimentación eléctrica o de interrumpir de cualquier otra manera la actualización.

Si se interrumpe la actualización de firmware, el controlador regresará al firmware de arranque, es decir, a la revisión 1.xxx.

Una vez concluida la actualización, aparece un cuadro de diálogo Update Status para indicar que la actualización ha finalizado.

10. Haga clic en OK.



11. Cierre el software ControlFLASH.

Uso de AutoFlash para actualizar el firmware

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

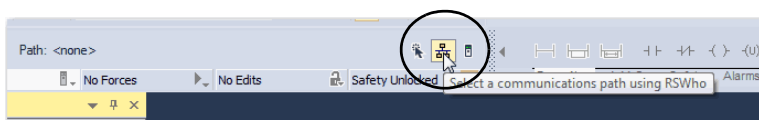


ATENCIÓN: Si la tarjeta Secure Digital está bloqueada y establecida para cargarse durante la puesta en marcha, esta actualización puede ser sobrescrita por el firmware que haya en la tarjeta SD.

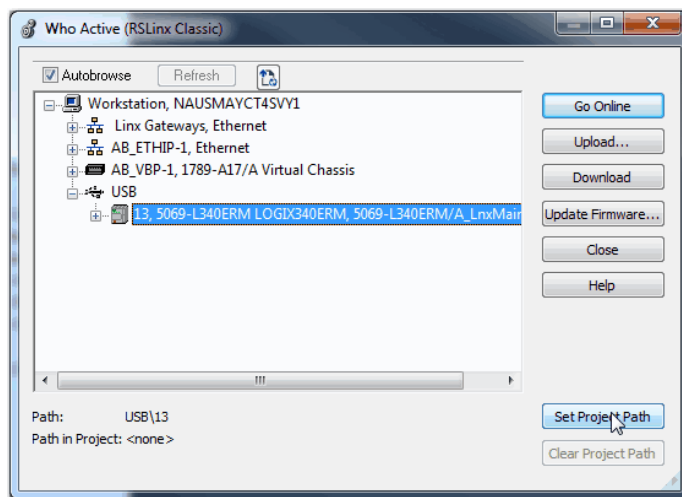
1. Compruebe lo siguiente:
 - Se ha establecido una conexión de red.
 - El driver de red ha sido configurado en el software de comunicación basado en Linx.
 - El controlador está en modo de programación o programación remota y se han eliminado todos los fallos mayores recuperables.
2. Inicie la aplicación Logix Designer y cree un proyecto.

Para obtener más información, consulte [Creación de un proyecto en la aplicación Logix Designer en la página 85](#).

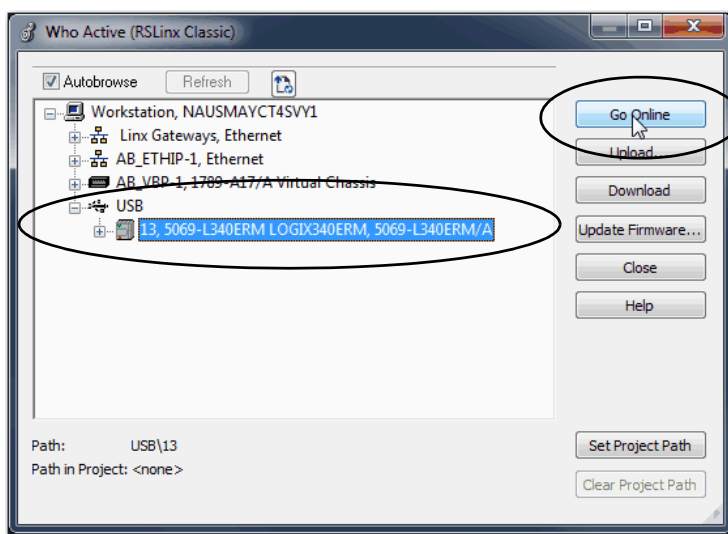
3. En el proyecto, haga clic en RSWho.



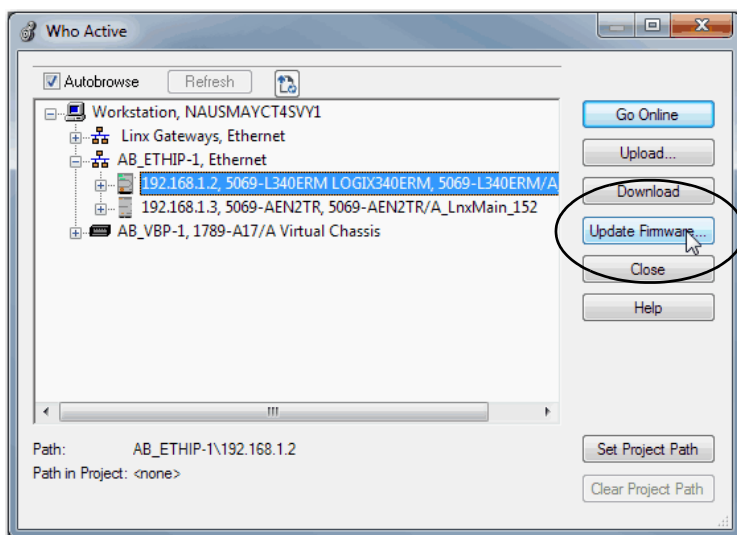
4. Expanda la ruta de comunicación y seleccione el controlador.



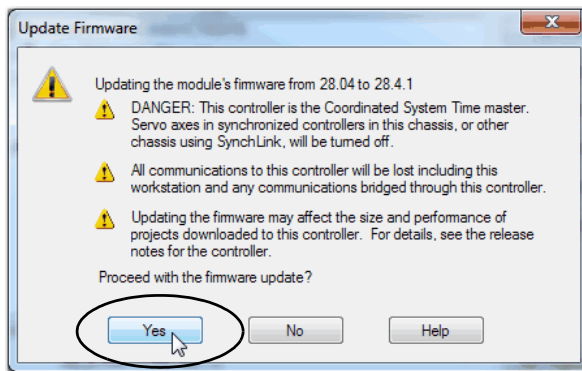
5. Seleccione el controlador y haga clic en Go Online.



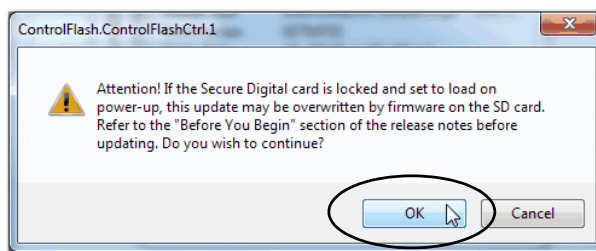
6. En el cuadro de diálogo Who Active, seleccione el controlador que aparece debajo del driver de comunicación que desea utilizar y haga clic en Update Firmware.



7. En el cuadro de diálogo Choose Firmware Revision, abra la ubicación de los archivos del firmware (C:\Program Files (x86)\ControlFlash).
8. Seleccione la revisión del firmware y haga clic en Update.
9. En el cuadro de diálogo de confirmación, haga clic en Yes.



10. En el cuadro de diálogo ControlFlash Attention, haga clic en OK.



El cuadro de diálogo de progreso indica el progreso de la actualización de firmware. Los controladores indican el progreso en actualizaciones y bloques.

IMPORTANTE Espere a que finalice la actualización del firmware antes de desconectar y volver a conectar la alimentación eléctrica o de interrumpir de cualquier otra manera la actualización.

Si se interrumpe la actualización ControlFLASH del controlador, los controladores regresarán al firmware de arranque, es decir, a la revisión 1.xxx.

Una vez concluida la actualización, aparece un cuadro de diálogo Update Status para indicar que la actualización ha finalizado.

11. Haga clic en OK en el cuadro de diálogo Who Active.

Notas:

Cómo comenzar a usar el controlador

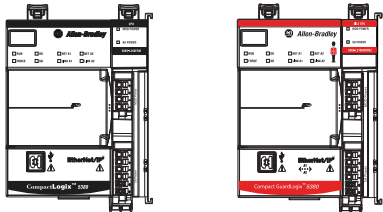
Tema	Página
Creación de un proyecto en la aplicación Logix Designer	85
Configuración adicional para un controlador Compact GuardLogix	88
Entrada en línea con el controlador	95
Descarga al controlador	102
Carga desde el controlador	105
Selección del modo de funcionamiento del controlador	109
Cambio de la configuración del controlador	112
Botón de restablecimiento	113

Creación de un proyecto en la aplicación Logix Designer

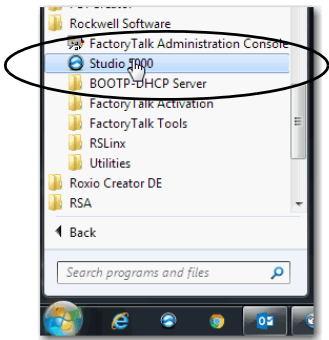
En su condición original, el controlador no cuenta con un proyecto de aplicación Studio 5000 Logix Designer®. Para crear un proyecto en la aplicación Logix Designer, siga estos pasos.

CompactLogix

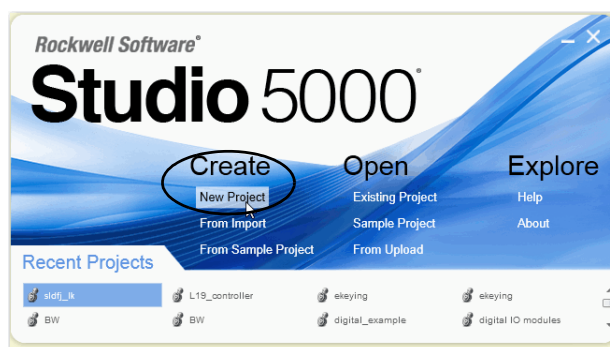
Compact GuardLogix



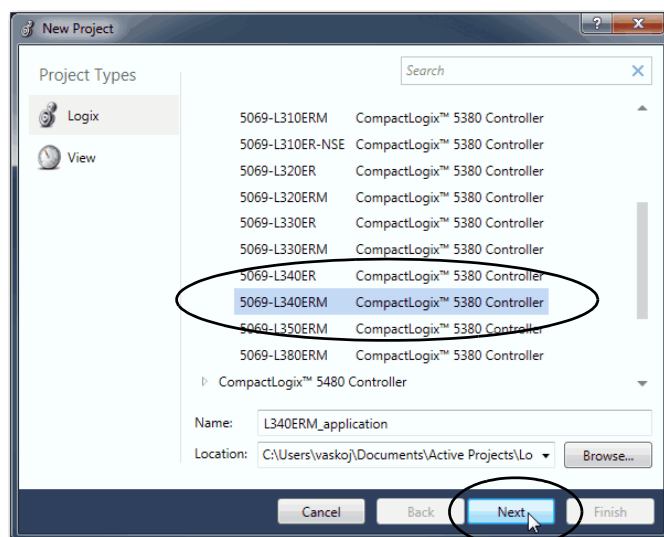
1. Inicie la aplicación. La aplicación Logix Designer forma parte del ambiente Studio 5000®.



2. Haga clic en New Project.



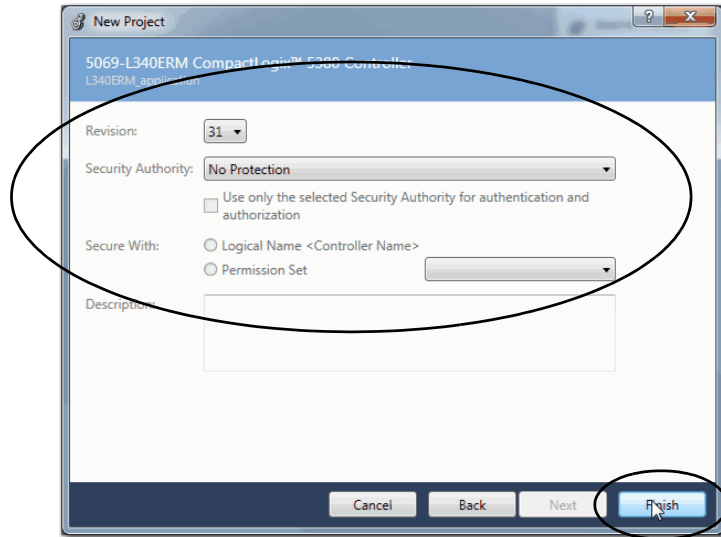
3. En el cuadro de diálogo New Project, siga estos pasos:
- Seleccione el controlador.
 - Indique un nombre para el proyecto.
 - Busque la ubicación donde se creará el archivo del proyecto.
 - Haga clic en Next.



4. Seleccione lo siguiente:

- Revision
- Security Authority (opcional)
- Secure With (solo está disponible si se utiliza Security Authority)

Para obtener más información sobre seguridad, consulte el documento Protección de los controladores Logix5000 – Manual de programación, publicación [1756-PM016](#).

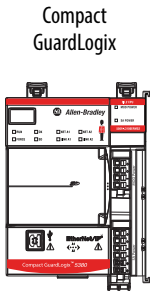


5. Haga clic en Finish.

6. Según el controlador:

- En el caso de un controlador Compact GuardLogix® 5380, continúe con [Configuración adicional para un controlador Compact GuardLogix en la página 88](#).
- En el caso de un controlador CompactLogix™ 5380, continúe con [Entrada en línea con el controlador en la página 95](#).

Configuración adicional para un controlador Compact GuardLogix

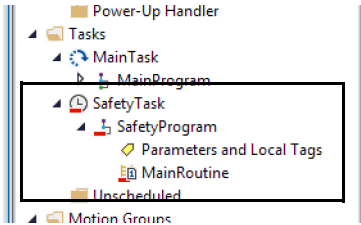


Los controladores Compact GuardLogix 5380 requieren configuración adicional después de crearse el proyecto. Estos temas describen cómo configurar los parámetros adicionales.

Tema	Página
Asignación del número de red de seguridad (SNN)	88
Entrada en línea con el controlador	95

En el caso de un controlador Compact GuardLogix, la aplicación Logix Designer crea una tarea de seguridad y un programa de seguridad. También se crea una rutina de seguridad principal en diagrama de lógica de escalera llamada MainRoutine dentro del programa de seguridad.

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



Asignación del número de red de seguridad (SNN)

Cuando crea proyectos de controlador, la aplicación Studio 5000 Logix Designer genera automáticamente un valor de SNN cuando reconoce una nueva subred que contiene dispositivos CIP Safety:

- Cada puerto compatible con CIP Safety en el controlador tiene asignado un SNN. Los controladores Compact GuardLogix 5380 tienen hasta tres números de red de seguridad: un SNN separado para cada puerto Ethernet, y uno para el backplane.
- Si un puente o un dispositivo adaptador se encuentra en el árbol de E/S y se añade un dispositivo CIP Safety secundario, a la subred creada por el puente o adaptador se le asigna un SNN.

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

- Uno o más puertos del controlador se encuentran en la subred CIP Safety que ya tiene un SNN establecido.
- Se copia un proyecto de seguridad en otra instalación de hardware distinta dentro del mismo sistema CIP Safety encaminable.

Rockwell Automation recomienda cambiar cada SNN al SNN ya establecido para esa subred, si existe. De esta forma, los dispositivos creados más tarde en el proyecto tendrán asignados automáticamente el SNN correcto.

Para obtener información sobre si el controlador o los puertos Ethernet se añaden a subredes existentes, consulte el documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#).

Cada red de seguridad debe tener un número de red de seguridad único. Debe asegurarse de que se asigne un SNN único a cada red CIP Safety que contenga dispositivos de seguridad.

SUGERENCIA Se pueden asignar varios números de red de seguridad a una subred CIP Safety o a un chasis ControlBus™ que contenga varios dispositivos de seguridad. Sin embargo, para simplificar, recomendamos que cada subred CIP Safety tenga solamente un SNN único.

Para obtener una explicación del número de red de seguridad, consulte el documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#).

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.

- [Asignación automática de SNN basado en tiempo en la página 90](#)
- [Asignación manual de SNN en la página 91](#)

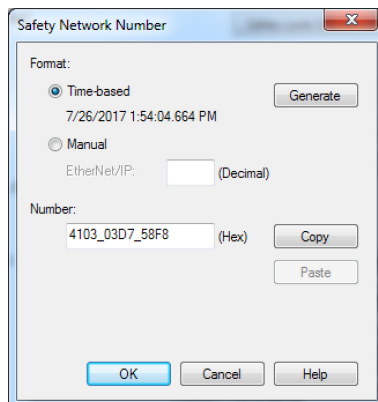
Asignación automática de SNN basado en tiempo

Cuando se crea un nuevo controlador o dispositivo, se asigna automáticamente un SNN basado en tiempo.

- Los dispositivos que se crean directamente bajo el puerto del controlador tienen de forma predeterminada el mismo SNN que ese puerto en el controlador.
- En el caso de dispositivos que no se encuentran directamente bajo un puerto de controlador, las nuevas adiciones subsiguientes de dispositivos de seguridad a la misma red CIP Safety tendrán asignado el mismo SNN definido dentro de la dirección más baja en esa red CIP Safety.

El formato basado en tiempo establece el valor de SNN como la fecha y hora en que se generó el número según la computadora que ejecuta el software de configuración.

Figura 18 – Formato basado en tiempo



Asignación manual de SNN

La asignación manual es útil si diseña su red y coloca los SNN en su diagrama de red. Puede ser más fácil leer los SNN en un diagrama que copiar y pegar los SNN desde múltiples proyectos.

Se requiere asignación manual de SNN si lo siguiente es verdadero:

- Uno o más puertos del controlador se encuentran en la subred CIP Safety que ya tiene un SNN establecido.
- Se copia un proyecto de seguridad en otra instalación de hardware distinta dentro del mismo sistema CIP Safety encaminable.

IMPORTANTE

Si asigna un SNN automáticamente o manualmente, asegúrese de que la expansión del sistema no dé como resultado una duplicación de las combinaciones de SNN y referencias de nodo único.

Aparecerá una advertencia si el proyecto contiene combinaciones duplicadas de SNN y referencias de nodo único. Todavía puede verificar el proyecto, pero Rockwell Automation le recomienda que resuelva las combinaciones duplicadas.

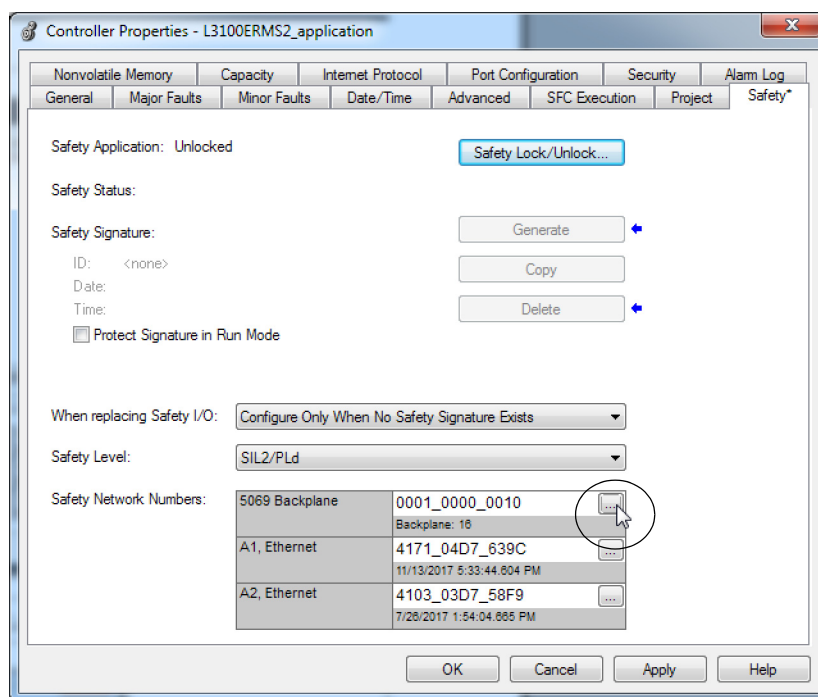
Sin embargo, puede haber dispositivos de seguridad en la red de seguridad encaminable que tengan el mismo SNN y dirección de nodo y no se encuentran en el proyecto. En tal caso, la aplicación Logix Designer desconoce estos dispositivos de seguridad y no aparecerá una advertencia.

Si dos dispositivos diferentes tienen las mismas referencias de nodo, el sistema de seguridad no podrá detectar un paquete recibido por un dispositivo que estaba destinado al otro dispositivo.

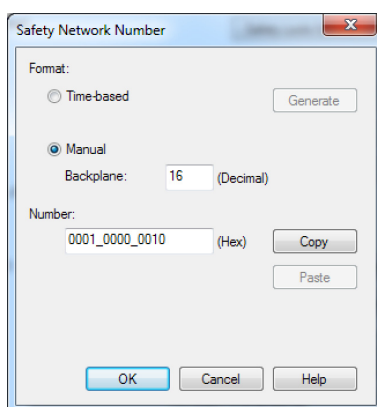
Si hay referencias de nodo único duplicadas, como usuario del sistema, tiene la responsabilidad de demostrar que no se producirá una condición insegura.

Siga estos pasos para cambiar los SNN del controlador a una asignación manual:

1. En la barra de herramientas en línea, haga clic en el icono de Controller Properties.
2. En el cuadro de diálogo Controller Properties, haga clic en la ficha Safety.
3. En la ficha Safety, haga clic en [...] a la derecha del número de red de seguridad del puerto que desea cambiar.



4. En el cuadro de diálogo Safety Network Number, seleccione Manual.
5. Introduzca el SNN como un valor de 1...9999 (decimal).



6. Haga clic en OK.

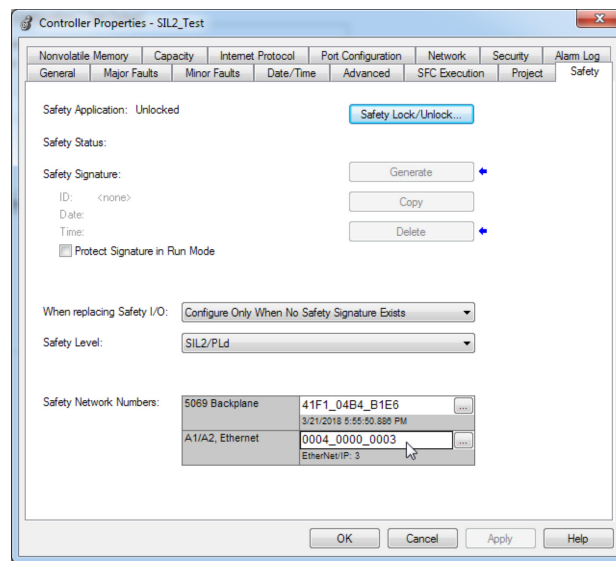
Copia y pegado de un número de red de seguridad (SNN) del controlador de seguridad

Si es necesario aplicar un SNN a otros controladores de seguridad, puede copiar y pegar el SNN. Hay múltiples maneras de copiar y pegar los SNN del controlador de seguridad.


Copia de un SNN del controlador de seguridad

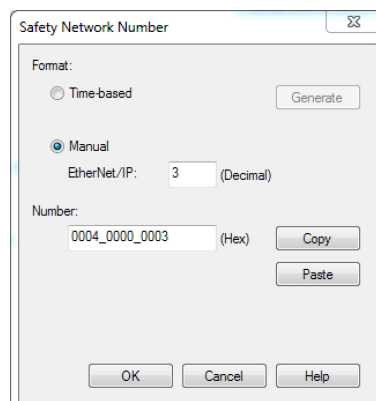
En la ficha Controller Properties Safety:

1. En la ficha Safety, haga clic en el campo SNN que desea copiar.
2. Presione Ctrl-C para copiar el SNN.



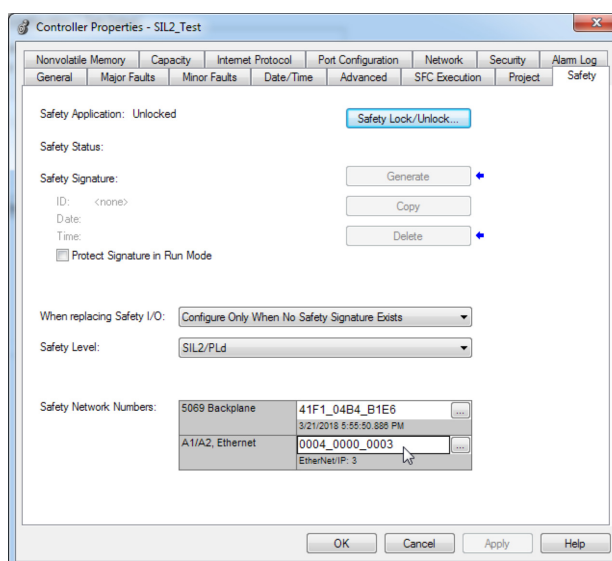
En el cuadro de diálogo Safety Network Number:

1. En el cuadro de diálogo Controller Properties, haga clic en la ficha Safety.
2. Haga clic en  a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.
3. En el cuadro de diálogo Safety Network Number, haga clic en Copy o haga clic en el campo SNN y presione Ctrl-C.

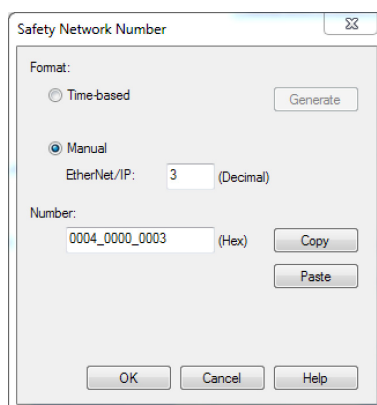


Pegado de un SNN del controlador de seguridad

1. En el cuadro de diálogo Controller Properties, haga clic en la ficha Safety.



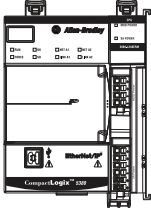
2. Haga clic en ... a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.
3. En el cuadro de diálogo Safety Network Number, haga clic en Paste o haga clic en el campo SNN y presione Ctrl-V.



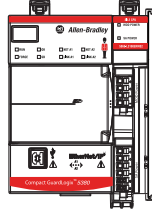
4. Haga clic en OK.
5. En la ficha Controller Properties Safety, haga clic en OK.

Entrada en línea con el controlador

CompactLogix



Compact GuardLogix

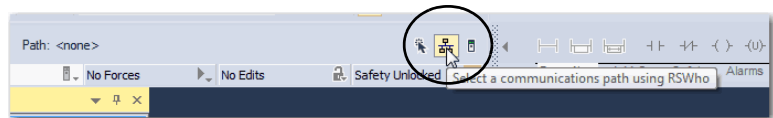


Para entrar en línea con el controlador, primero debe especificar una ruta de comunicación en la aplicación Logix Designer.

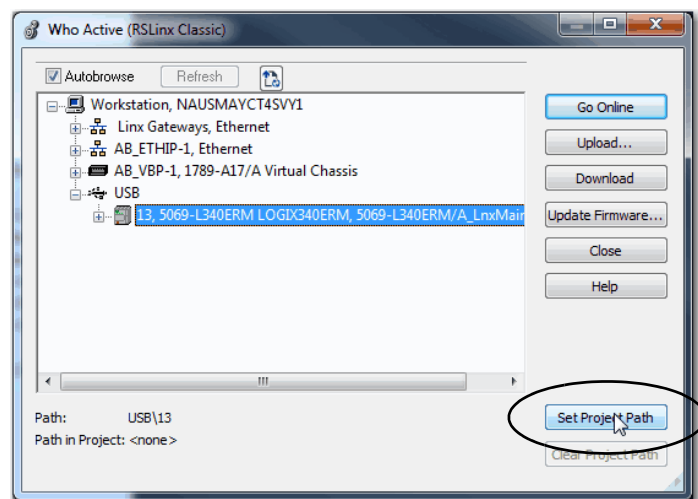
SUGERENCIA En esta sección se ha seleccionado el puerto USB como la ruta de comunicación. También es posible otra ruta a través de los puertos Ethernet incorporados.

Uso de RSWho

1. Abra o cree un proyecto en la aplicación Logix Designer.
2. Haga clic en RSWho en la aplicación.



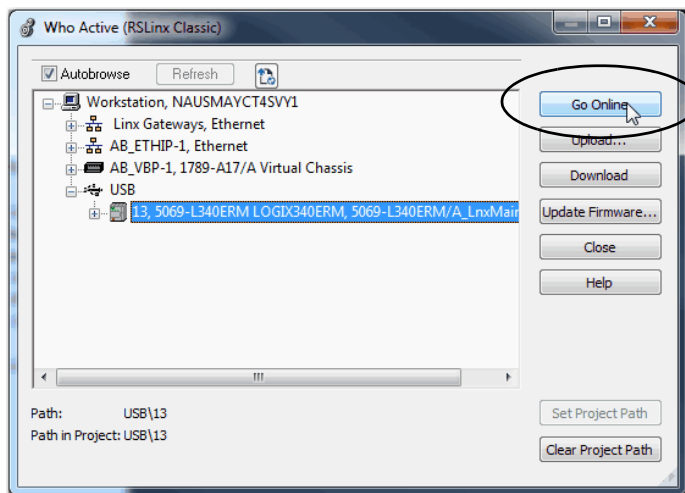
3. Expanda la ruta de comunicación y seleccione el controlador.



4. Si desea guardar la ruta en el archivo de proyecto, haga clic en Set Project Path.

Si almacena la ruta del proyecto en el proyecto, no será necesario elegir la ruta cada vez que entre en línea.

- Después de seleccionar la ruta de comunicación, haga clic en Go Online en el cuadro de diálogo Who Active.



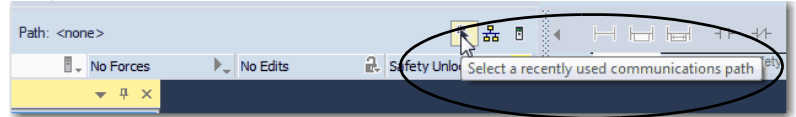
Go Online utiliza el nodo resaltado en el árbol Who Active, independientemente del ajuste de Path in Project. Para obtener más información sobre el cuadro de diálogo Who Active, consulte la ayuda en línea de Logix Designer.

Vea [Consideraciones adicionales para entrar en línea con un controlador en la página 98](#).

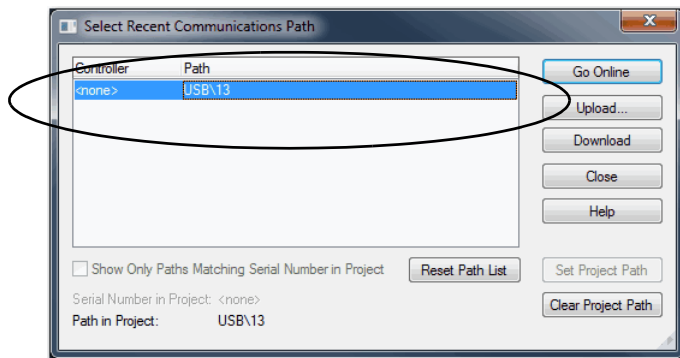
Uso de una ruta de comunicación reciente

También puede seleccionar una ruta de comunicación reciente y entrar en línea o aplicarla al proyecto.

1. Haga clic en el botón Recent Communication Path junto a la barra Path.

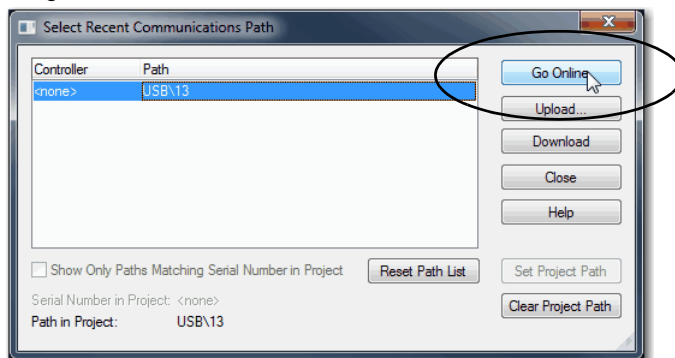


2. Seleccione la ruta en el cuadro de diálogo Select Recent Communications Path.



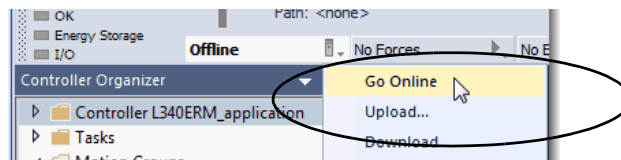
3. Para almacenar la ruta en su proyecto, haga clic en Set Project Path.

4. Haga clic en Go Online.



Para obtener más información sobre el cuadro de diálogo Select Recent Communications Path, consulte la ayuda en línea de Logix Designer.

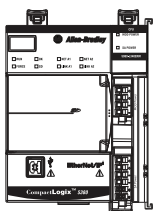
Una vez establecida una ruta de comunicación, puede seleccionar Go Online en el menú Controller Status cuando trabaja con el proyecto.



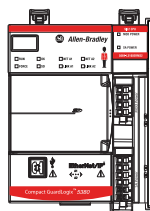
Vea [Consideraciones adicionales para entrar en línea con un controlador en la página 98](#).

Consideraciones adicionales para entrar en línea con un controlador

CompactLogix



Compact GuardLogix



La aplicación Logix Designer 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 se han producido cambios en este.

- 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 se realizaron cambios, puede entrar en línea para monitorear la ejecución del proyecto.

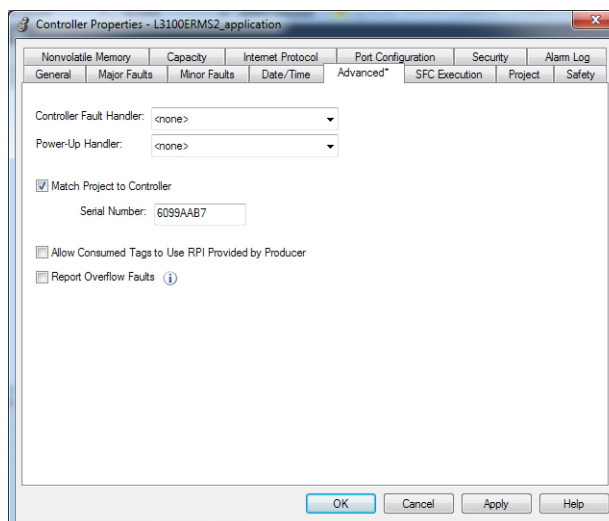
SUGERENCIA Para obtener información sobre la carga de un proyecto, la descarga de un proyecto y los cuadros de diálogo de carga y descarga, consulte la ayuda en línea de Logix Designer.

Hay diversos factores que afectan estos procesos, incluidas la función Match Project to Controller y la función Firmware Revision Match.

En el caso de controladores Compact GuardLogix, las consideraciones adicionales incluyen el estado y los fallos de seguridad, la existencia de una firma de seguridad y el estado de bloqueo/desbloqueo de seguridad del proyecto y controlador. Vea [Consideraciones adicionales para entrar en línea con un controlador Compact GuardLogix en la página 100](#).

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. Esta función se encuentra en la ficha Controller Properties Advanced.



Si la función de coincidencia del proyecto con el controlador está habilitada en el proyecto fuera de línea, la aplicación Logix Designer compara el número de serie del controlador en el proyecto fuera de línea con el del controlador conectado. Si no coinciden, 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

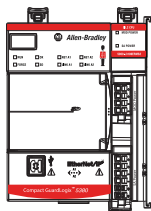
La coincidencia de la revisión de firmware influye en el proceso de descarga. Si la revisión del controlador no coincide con la revisión del proyecto, se le pedirá que actualice el firmware del controlador. La aplicación Logix Designer le permite actualizar el firmware como parte de la secuencia de descarga.

IMPORTANTE	Para actualizar el firmware del controlador, primero deberá instalar un kit de actualización de firmware. El kit de actualización se envía en un DVD suplementario junto con el ambiente Studio 5000®.
-------------------	--

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

Consideraciones adicionales para entrar en línea con un controlador Compact GuardLogix

Compact GuardLogix



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

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

Firma de seguridad y estado de bloqueo y desbloqueo de seguridad

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

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

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

El estado de bloqueo de seguridad siempre se carga con el proyecto, incluso si falta una firma de seguridad.

La existencia de una firma de seguridad y el estado de bloqueo de seguridad del controlador determinan si una descarga puede continuar.

Tabla 6 – Efecto del bloqueo de seguridad y la firma de seguridad en la operación de descarga

Estado de bloqueo de seguridad	Estado de firma de seguridad	Funcionalidad de la descarga
Controlador en desbloqueo de seguridad	La firma de seguridad del proyecto fuera de línea coincide con la firma de seguridad del controlador.	Se descarga la aplicación completa. Los tags de seguridad se reinician con los valores que tenían en el momento en que se creó la firma de seguridad. El estado de bloqueo de seguridad coincide con el estado en el proyecto fuera de línea. No se cambia la firma de seguridad.
	Las firmas de seguridad no coinciden.	Si el controlador tiene una firma 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 de línea.
Controlador en bloqueo de seguridad	Las firmas de seguridad coinciden.	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 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 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 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 de línea.

Comprobaciones para la entrada en línea con un controlador GuardLogix

En el caso de un proyecto de seguridad, la aplicación Logix Designer comprueba lo siguiente:

- ¿Coinciden los números de serie del controlador y el proyecto fuera de línea (si se ha seleccionado Controller Match con el controlador)?
- ¿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 seguridad del controlador y del proyecto fuera de línea?

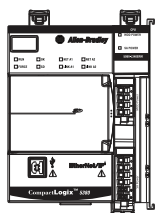
Tabla 7 – Conexión al controlador con un proyecto de seguridad

Si el software indica	Proceda como sigue
No se ha podido establecer una conexión con el controlador. Hay discordancia entre el proyecto fuera de línea y el número de serie del controlador. Es posible que se haya seleccionado un controlador equivocado.	Conéctese al controlador correcto, seleccione otro archivo de proyecto o marque la casilla de selección Update Project Serial Number y seleccione Go Online... para conectarse al controlador y actualizar el número de serie del proyecto, 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.	<p>Elija una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Seleccione Update Firmware. Seleccione la revisión necesaria y haga clic en Update. Haga clic en Yes para confirmar su selección. <p>IMPORTANTE: Se elimina el proyecto en línea.</p> <ul style="list-style-type: none"> • Para conservar el proyecto en línea, cancele el proceso en línea e instale una versión del ambiente Studio 5000® que sea compatible con la revisión de firmware de su controlador.
Debe realizar una carga o una descarga para entrar en línea usando el proyecto abierto.	<p>Elija una de las opciones siguientes:</p> <ul style="list-style-type: none"> • 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 seguridad. La revisión menor de firmware del controlador es incompatible con la firma de seguridad en el proyecto fuera de línea.	<ul style="list-style-type: none"> • Si la revisión menor de firmware es incompatible, a fin de conservar la firma 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 seguridad, haga clic en Download. La firma de seguridad se elimina. <p>IMPORTANTE: El sistema de seguridad requiere revalidación.</p>
No se ha podido establecer una conexión con el controlador. La firma 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.

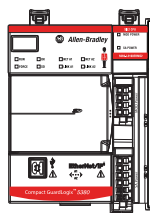
Cuando el controlador y la aplicación Logix Designer están en línea, el estado de bloqueo de seguridad y la firma de seguridad del controlador coinciden con el proyecto del controlador. El controlador sobrescribe el estado de bloqueo de seguridad y la firma de seguridad del proyecto fuera de línea. Si 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.

Descarga al controlador

CompactLogix



Compact GuardLogix



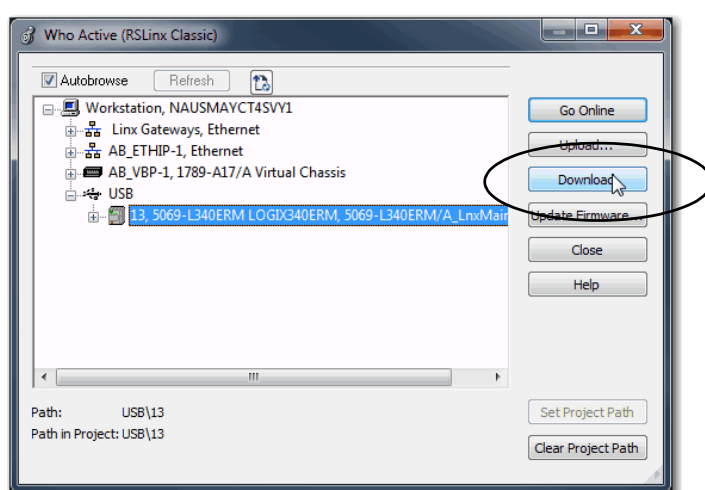
Al descargar un proyecto al controlador, se copia el proyecto de la aplicación Logix Designer al controlador. Puede descargar un proyecto de dos maneras:

- [Uso de Who Active en la página 102](#)
- [Uso del menú Controller Status en la página 103](#)

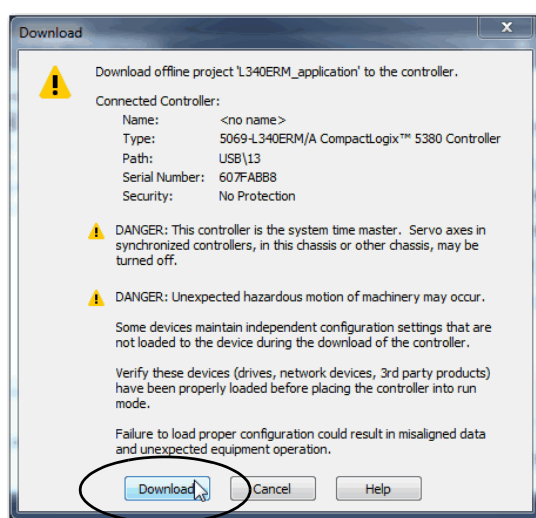
Uso de Who Active

Puede utilizar las funciones del cuadro de diálogo Who Active para descargarlo al controlador tras haber establecido la ruta de comunicación. Siga estos pasos para descargar al controlador.

1. Después de seleccionar la ruta de comunicación, haga clic en Download en el cuadro de diálogo Who Active.



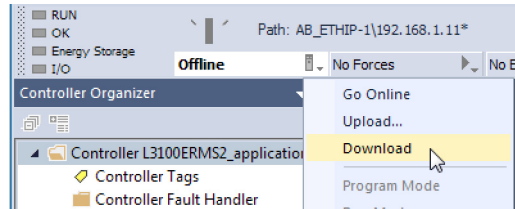
2. Luego de leer las advertencias en el cuadro de diálogo Download, haga clic en Download.



Uso del menú Controller Status

Tras elegir una ruta de comunicación en la aplicación Logix Designer, puede utilizar el menú Controller Status para realizar la descarga al controlador. Para la descarga, elija Download en el menú Controller Status.

Figura 19 – Descarga mediante el menú Controller Status

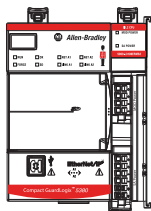


SUGERENCIA

Después de finalizarse la descarga, el nombre del proyecto aparece en la pantalla con desplazamiento de texto de estado.

Consideraciones adicionales con respecto a la descarga a un controlador Compact GuardLogix

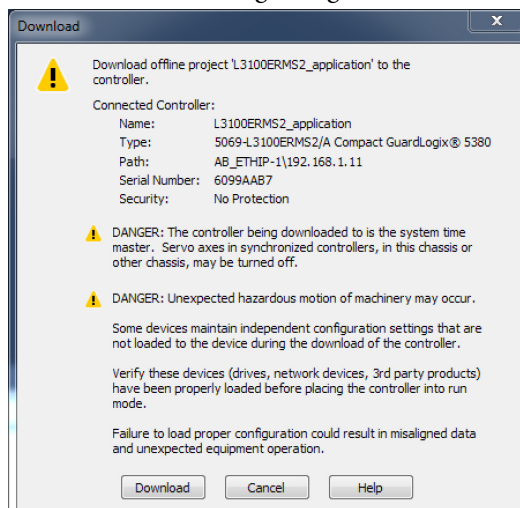
Compact GuardLogix



En el caso de un proyecto de seguridad, la aplicación Logix Designer compara la siguiente información en el proyecto fuera de línea con la del 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 seguridad (si la hay)
- Estado de bloqueo de seguridad

Después de verificarse las comprobaciones, aparece el cuadro de diálogo de confirmación de descarga. Haga clic en Download.



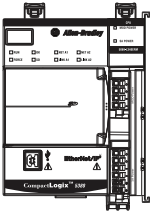
La aplicación Logix Designer muestra los mensajes de estado en el cuadro de diálogo de descarga, la pantalla de progreso y la ventana Errors.

Si el software indica:	Entonces:
No se puede realizar la descarga al controlador. Hay discordancia entre el proyecto fuera de línea y el número de serie del controlador. Es posible que se haya seleccionado un controlador equivocado.	Establezca la conexión al controlador correcto o verifique que este sea el controlador correcto. Si este es el controlador correcto, marque la casilla de selección Update Project Serial Number para permitir que se realice la descarga. El número de serie del proyecto se modifica, 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 su selección.
No se ha podido realizar la descarga al controlador. La firma de seguridad incompatible no se puede eliminar mientras el proyecto esté en bloqueo de seguridad.	<p>Cancele la descarga. Para descargar el proyecto, usted debe poner en desbloqueo de seguridad el proyecto fuera de línea, eliminar la firma de seguridad y descargar el proyecto.</p> <p>IMPORTANTE: El sistema de seguridad requiere revalidación.</p>
No se puede realizar la descarga de modo que se conserve la firma de seguridad. La revisión menor de firmware del controlador es incompatible con la firma de seguridad del proyecto fuera de línea.	<ul style="list-style-type: none"> • Si la revisión menor de firmware es incompatible, a fin de conservar la firma 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 seguridad, haga clic en Download. La firma de seguridad se elimina. <p>IMPORTANTE: El sistema de seguridad requiere revalidación.</p>
No se ha podido realizar la descarga al controlador. El controlador está bloqueado. Las firmas de seguridad del controlador y el proyecto fuera de línea no coinciden.	<p>Seleccione Unlock. Aparece el cuadro de diálogo Safety Unlock for Download. Si la casilla de selección Delete Signature está seleccionada y selecciona Unlock, haga clic en Yes para confirmar la eliminación.</p> <p>IMPORTANTE: El sistema de seguridad requiere revalidación.</p>
Downloading safety signature...	La firma de seguridad está presente en el proyecto fuera de línea y se está descargando.

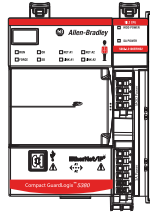
Después de completarse debidamente la descarga, el estado de bloqueo de seguridad y la firma de seguridad del controlador coinciden con el proyecto descargado. Los datos de seguridad se inicializan con los valores que tenían en el momento en que se creó la firma de seguridad.

Carga desde el controlador

CompactLogix



Compact GuardLogix



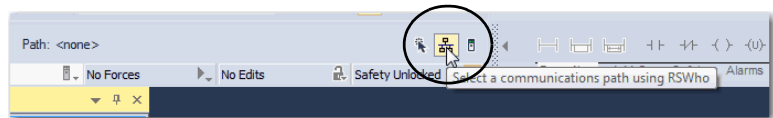
Al cargar un proyecto desde el controlador, se copia el proyecto del controlador a la aplicación Logix Designer. Para cargar un proyecto, utilice uno de los métodos siguientes:

- [Uso de Who Active en la página 105](#)
- [Uso del menú Controller Status en la página 106](#)

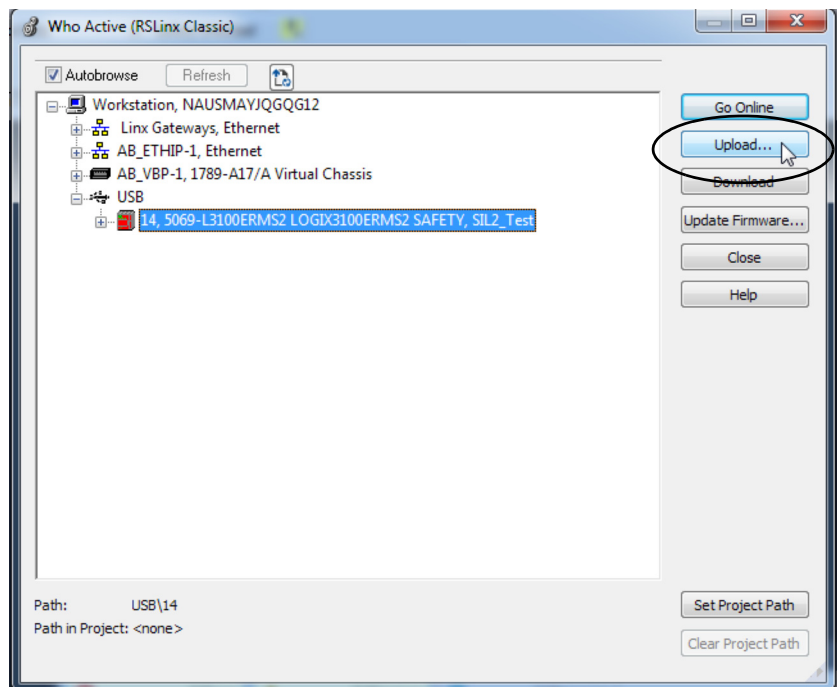
Uso de Who Active

Puede utilizar las funciones del cuadro de diálogo Who Active para realizar la carga desde el controlador tras haber establecido la ruta de comunicación. Siga estos pasos para realizar la carga desde el controlador.

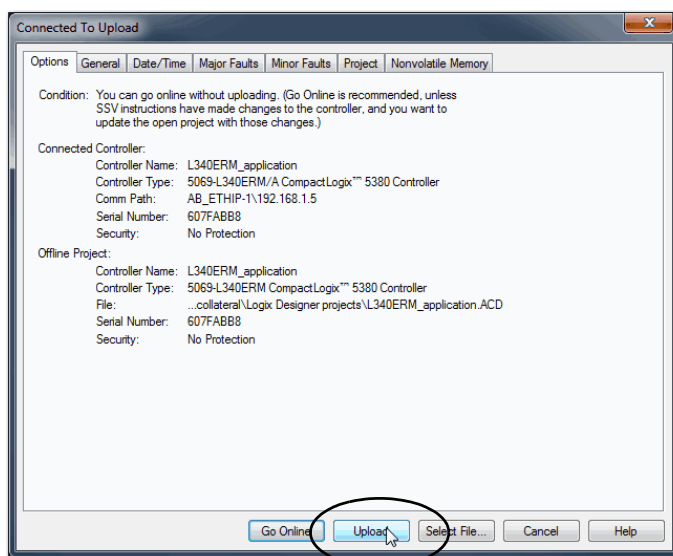
1. En el proyecto de aplicación Logix Designer, haga clic en RSWWho.



2. Expanda la ruta de comunicación y seleccione el controlador.
3. Haga clic en Upload en el cuadro de diálogo Who Active.



4. En el cuadro de diálogo Connected to Upload, compruebe que el proyecto es el que desea cargar.
5. Haga clic en Upload.

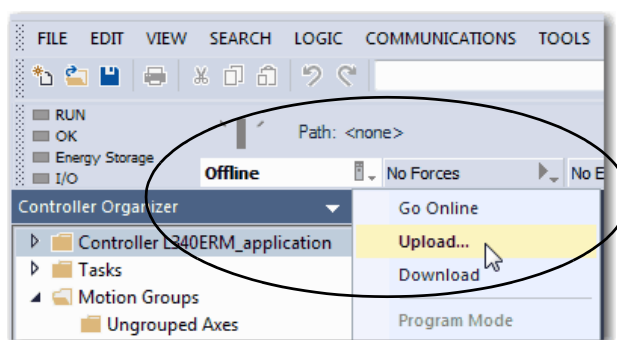


Para obtener más información sobre el cuadro de diálogo Connected To, consulte la ayuda en línea de Logix Designer.

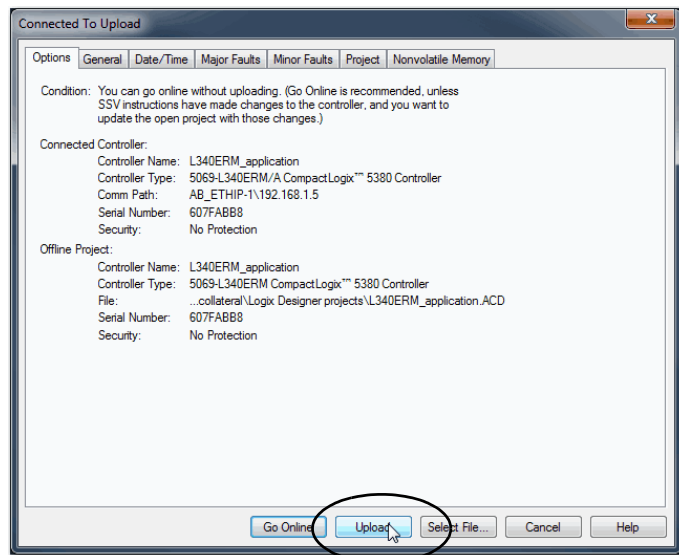
Uso del menú Controller Status

Tras elegir una ruta de comunicación en la aplicación Logix Designer, puede utilizar el menú Controller Status para realizar la carga desde el controlador.

1. En el menú desplegable Controller Status, elija Upload.

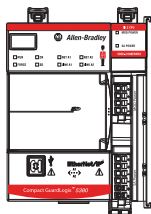


2. En el cuadro de diálogo Connected to Upload, compruebe que el proyecto es el que desea cargar.
3. Haga clic en Upload.



Consideraciones adicionales con respecto a la carga a un controlador Compact GuardLogix

Compact
GuardLogix



En el caso de un proyecto de seguridad, la aplicación Logix Designer compara la siguiente información en el proyecto con la del controlador:

- Número de serie del controlador (si se ha seleccionado la coincidencia del proyecto con el controlador)
- proyecto abierto al proyecto del controlador
- Revisiones mayores y menores del firmware
- Firma de seguridad (si la hay)

IMPORTANTE Se permite una carga independientemente del estado de seguridad y del estado de bloqueo de seguridad del proyecto y del controlador que están fuera de línea. El estado bloqueado sigue el estado del proyecto cargado.

Tabla 8 – Comportamiento de carga

Comportamiento de carga:	Respuesta:
Si se ha habilitado la coincidencia del proyecto con el controlador, la aplicación Logix Designer comprueba si el número de serie del proyecto abierto coincide con el número de serie del controlador.	<ul style="list-style-type: none"> • Establezca la conexión al controlador correcto o verifique que este sea el controlador correcto. • Seleccione un nuevo proyecto para la carga o seleccione otro proyecto distinto mediante Select File. • Si este es el controlador correcto, marque la casilla de selección Update Project Serial Number para permitir que se realice la descarga. El número de serie del proyecto se modifica, de modo que coincida con el número de serie del controlador.
La aplicación Logix Designer comprueba si el proyecto abierto coincide con el proyecto del controlador.	<ul style="list-style-type: none"> • Si los proyectos no coinciden, debe seleccionar un archivo coincidente o cancelar el proceso de carga. • Si los proyectos coinciden, el software comprueba los cambios en el proyecto fuera de línea (abierto).
La aplicación Logix Designer comprueba si hay cambios en el proyecto fuera de línea.	<ul style="list-style-type: none"> • 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. • 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.
Uploading safety signature...	Este mensaje aparece durante la carga solo si una firma de seguridad que coincide con la en el controlador no existe en el proyecto fuera de línea.

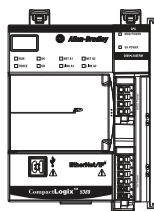
Si selecciona Upload, se cargan las aplicaciones estándar y de seguridad. Si existe una firma de seguridad, también se carga. El estado de bloqueo de seguridad del proyecto refleja el estado original del proyecto en línea (controlador).

SUGERENCIA Antes de la carga, si existe una firma de 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 seguridad, la firma 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 seguridad). Si no desea que estos cambios sean permanentes, no guarde el proyecto fuera de línea después de la carga.

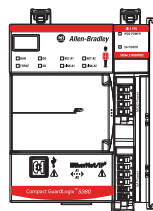
Selección del modo de funcionamiento del controlador

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

CompactLogix



Compact GuardLogix



Posición del interruptor de modo ⁽¹⁾	Modos disponibles del controlador	En este modo puede:	En este modo no puede:	 ATENCIÓN:
RUN	Modo de marcha: el controlador controla de forma activa el proceso o la máquina. No se pueden editar los proyectos en la aplicación Logix Designer en el modo de marcha.	<ul style="list-style-type: none"> Colocar las salidas en el estado que indica la lógica del proyecto Ejecutar (escanear) tareas Enviar mensajes Enviar y recibir datos en respuesta a un mensaje proveniente de otro controlador Producir y consumir tags 	<ul style="list-style-type: none"> Colocar las salidas en el estado configurado para el modo de programación Cambiar el modo del controlador mediante la aplicación Logix Designer Descargar un proyecto Programar una red ControlNet Editar el proyecto en línea 	El modo de marcha solo se utiliza cuando todas las condiciones son seguras.
REM	Modo de marcha remota: este modo es idéntico al modo de marcha, con la única diferencia de que puede editar en línea el proyecto, así como cambiar el modo del controlador mediante la aplicación Logix Designer.	<ul style="list-style-type: none"> Colocar las salidas en el estado que indica la lógica del proyecto Ejecutar (escanear) tareas Cambiar el modo del controlador mediante la aplicación Logix Designer Editar el proyecto en línea Enviar mensajes Enviar y recibir datos en respuesta a un mensaje proveniente de otro controlador Producir y consumir tags 	<ul style="list-style-type: none"> Colocar las salidas en el estado configurado para el modo de programación Descargar un proyecto Programar una red ControlNet 	Puede modificar un archivo de proyecto en línea en modo de marcha remota. Asegúrese de controlar con cuidado las salidas para evitar lesiones al personal y daños a los equipos.
	Modo de programación remota: este modo funciona como el modo de programación, con la única diferencia de que puede cambiar el modo del controlador mediante la aplicación Logix Designer.	<ul style="list-style-type: none"> Colocar las salidas en el estado configurado para el modo de programación Cambiar el modo del controlador mediante la aplicación Logix Designer Descargar un proyecto Programar una red ControlNet Editar el proyecto en línea Enviar y recibir datos en respuesta a un mensaje proveniente de otro controlador Producir y consumir tags 	<ul style="list-style-type: none"> Colocar las salidas en el estado que indica la lógica del proyecto Ejecutar (escanear) tareas 	Las salidas son llevadas al estado del modo de programación, lo que puede ocasionar una situación peligrosa.
	Modo de prueba remota: este modo del controlador ejecuta el código, pero no se controla ninguna E/S. Puede editar en línea el proyecto y cambiar el modo del controlador utilizando la aplicación Logix Designer. Los módulos de salida son llevados a su estado del modo de programación (activado, desactivado o retenido).	<ul style="list-style-type: none"> Colocar las salidas en el estado configurado para el modo de programación Ejecutar (escanear) tareas Cambiar el modo del controlador mediante la aplicación Logix Designer Editar el proyecto en línea Enviar mensajes Enviar y recibir datos en respuesta a un mensaje proveniente de otro controlador Producir y consumir tags 	<ul style="list-style-type: none"> Colocar las salidas en el estado que indica la lógica del proyecto Descargar un proyecto Programar una red ControlNet Enviar mensajes 	
PROG	Modo de programación: este modo del controlador no ejecuta código ni controla E/S, pero están disponibles las operaciones de edición. Los módulos de salida son llevados a su estado del modo de programación (activado, desactivado o retenido). En esta posición, los modos del controlador no se pueden cambiar mediante la aplicación Logix Designer.	<ul style="list-style-type: none"> Colocar las salidas en el estado configurado para el modo de programación Descargar un proyecto Programar una red ControlNet Editar el proyecto en línea Enviar y recibir datos en respuesta a un mensaje proveniente de otro controlador Producir y consumir tags 	<ul style="list-style-type: none"> Colocar las salidas en el estado que indica la lógica del proyecto Ejecutar (escanear) tareas Cambiar el modo del controlador mediante la aplicación Logix Designer Enviar mensajes 	No utilice el modo de programación como paro de emergencia. El modo de programación no es un dispositivo de seguridad. Las salidas son llevadas al estado del modo de programación, lo que puede ocasionar una situación peligrosa.

(1) Al mover la posición del interruptor del modo de marcha al modo remoto el controlador queda en el modo de marcha remota; en cambio, al mover la posición del interruptor de programación al modo remoto en controlador queda en el modo de programación remota. No puede seleccionar el modo de prueba remota usando exclusivamente el interruptor de modo; solo está disponible mediante la aplicación Logix Designer.

Uso del interruptor de modo para cambiar el modo de funcionamiento

Para cambiar el modo de funcionamiento, utilice el interruptor de modo del controlador. El interruptor de modo del controlador ofrece un medio mecánico de mejorar la seguridad del controlador y del sistema de control. Debe accionar físicamente el interruptor de modo del controlador para cambiar el modo de funcionamiento de RUN a REM o a PROG.

Cuando el interruptor de modo del controlador se establece en el modo RUN, se prohíben funciones como la edición en línea, las descargas de programas y las actualizaciones del firmware. Vea [Selección del modo de funcionamiento del controlador en la página 109](#) para ver una lista de características prohibidas.

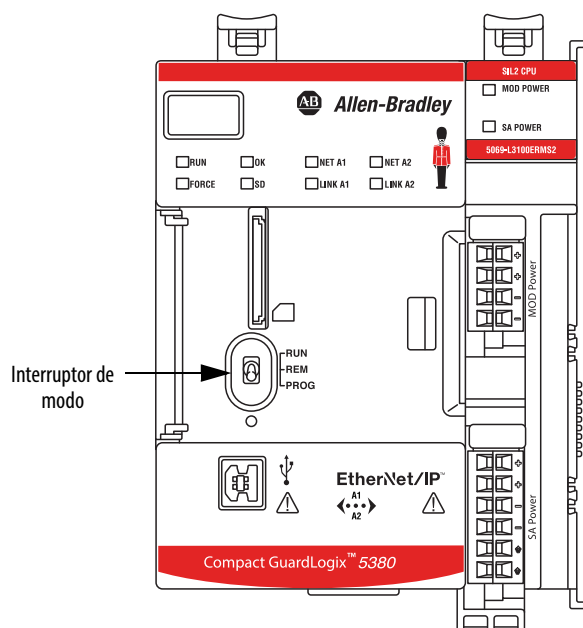
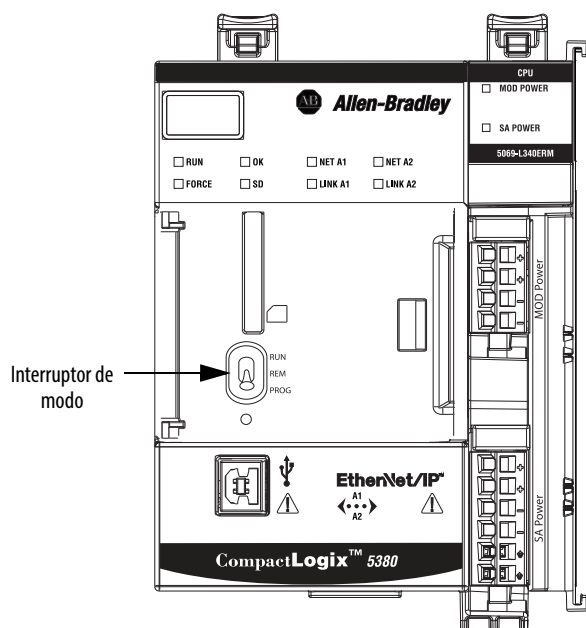
El interruptor de modo puede complementar otros métodos de autorización y autenticación que controlan de manera similar el acceso de los usuarios al controlador, como el servicio FactoryTalk® Security.

IMPORTANTE Durante el tiempo de ejecución, le recomendamos que coloque el interruptor de modo del controlador en el modo RUN. Esto ayuda a evitar el acceso no autorizado al controlador o la posibilidad de manipulación indebida del programa del controlador, configuración o firmware del dispositivo.

Coloque el interruptor de modo en los modos REM o PROG durante la puesta en marcha y el mantenimiento del controlador, y siempre que sea necesario disponer de acceso temporal para cambiar el programa, la configuración o el firmware del producto.

El interruptor de modo ubicado en la parte frontal del controlador se puede utilizar para cambiar el controlador a uno de estos modos:

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



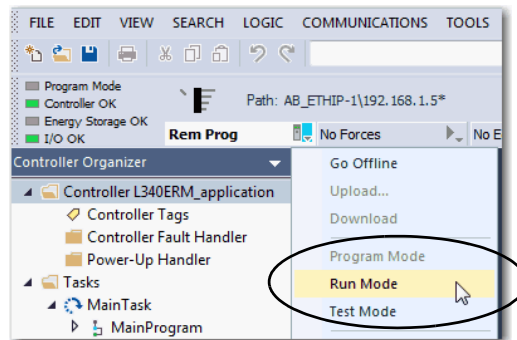
Uso de la aplicación Logix Designer para cambiar el modo de funcionamiento

Cuando está en línea con el controlador y el interruptor de modo del controlador se establece a Remote (REM, en la posición central), puede utilizar Logix Designer para cambiar el modo de funcionamiento.

El menú Controller Status en la esquina superior izquierda de la ventana de la aplicación le permite especificar estos modos de funcionamiento:

- Programación remota
- Marcha remota
- Prueba remota

1. En el menú desplegable Controller Status, seleccione el modo de funcionamiento.

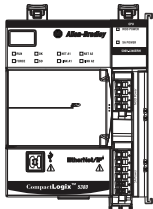


SUGERENCIA

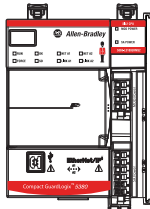
En este ejemplo, el interruptor del modo del controlador está establecido en el modo remoto. Si el interruptor de modo del controlador se establece en modo de marcha o de programación, cambian las opciones del menú.

Cambio de la configuración del controlador

CompactLogix



Compact GuardLogix



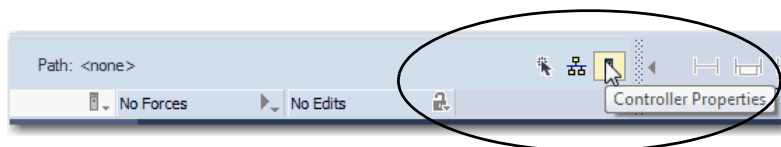
Tras crear el proyecto, puede cambiar algunos parámetros de configuración en el cuadro de diálogo Controller Properties cuando el **controlador está fuera de línea**.

Entre los ejemplos de parámetros configurables que se pueden cambiar fuera de línea, se incluyen los siguientes:

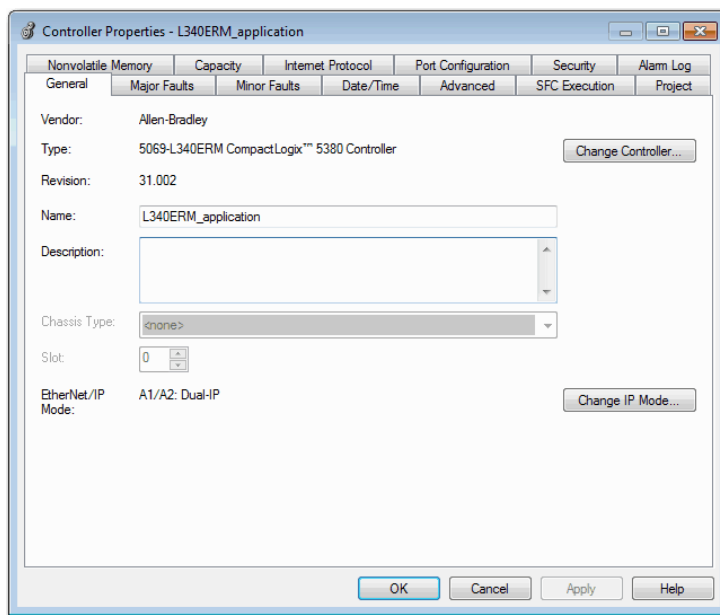
- EtherNet/IP Mode en la ficha General
- Enable Time Synchronization en la ficha Date/Time
- Execution Control en la ficha SFC Execution

Siga estos pasos para cambiar la configuración del controlador mientras el proyecto está fuera de línea:

1. En la barra de herramientas Online, haga clic en el botón Controller Properties.



2. En el cuadro de diálogo Controller Properties, haga clic en la ficha General.



Botón de restablecimiento

Puede restablecer los controladores CompactLogix y Compact GuardLogix utilizando el botón de restablecimiento. El botón de restablecimiento solo se lee durante el encendido o el reinicio. Si presiona el botón de restablecimiento en otro momento, no tendrá ningún efecto.

En el caso de un controlador Compact GuardLogix, el estado de bloqueo de seguridad o la firma de seguridad no le impedirán restablecer el controlador. Puesto que la aplicación se borra del controlador durante un restablecimiento, también se borra el nivel de seguridad del controlador. Al descargar un proyecto de seguridad al controlador, el nivel de seguridad se establece al nivel especificado en el proyecto.

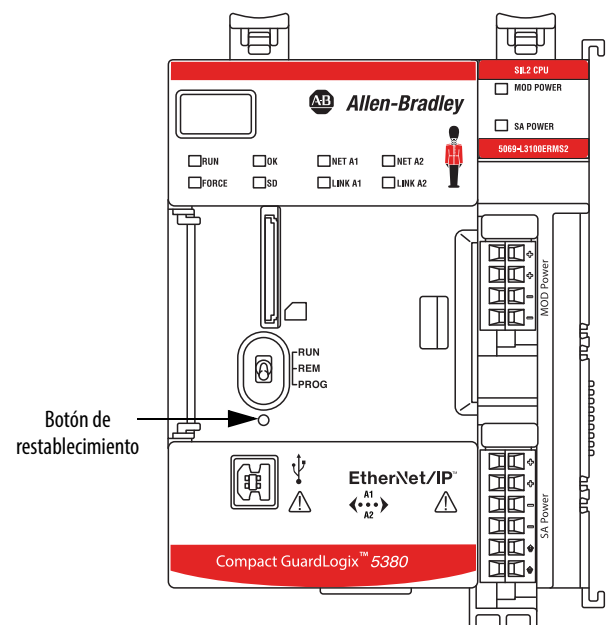
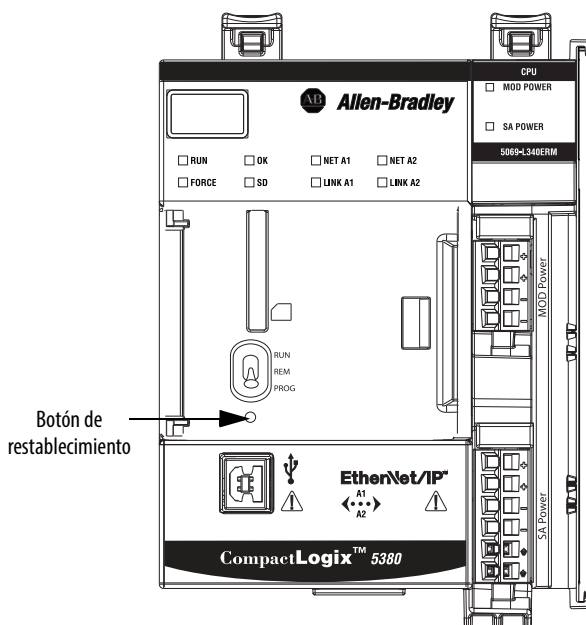
Un controlador tiene dos etapas de restablecimiento:

- Un restablecimiento de etapa 1 borra el programa de aplicación y la memoria, pero conserva la dirección IP, todos los ajustes de red y la revisión del firmware. Solo se produce un restablecimiento de etapa 1 si el controlador contiene una aplicación del usuario. Vea [Restablecimiento de etapa 1 en la página 114](#).
- Un restablecimiento de etapa 2 revierte el controlador a los ajustes originales (incluso el firmware) y borra todos los ajustes de red. Solo se produce un restablecimiento de etapa 2 si el controlador no contiene una aplicación del usuario y el firmware actual del controlador no es una versión 1.x. Vea [Restablecimiento de etapa 2 en la página 115](#).

IMPORTANTE Dado que el estado de habilitación/inhabilitación de los puertos está asociado con el programa de aplicación, el puerto Ethernet queda habilitado después de un restablecimiento de etapa 1 o etapa 2.



ADVERTENCIA: Cuando se presiona el botón de restablecimiento mientras la alimentación eléctrica está conectada, podría producirse un arco eléctrico. Esto podría causar una explosión en instalaciones ubicadas en zonas peligrosas. Antes de seguir adelante, asegúrese de desconectar la alimentación eléctrica o de verificar que la zona no sea peligrosa.



Restablecimiento de etapa 1

IMPORTANTE Solo se produce un restablecimiento de etapa 1 si el controlador contiene una aplicación del usuario.

El restablecimiento de etapa 1 lleva a cabo lo siguiente:

- Borra el programa de aplicación.
- Conserva los ajustes de red del puerto Ethernet incorporado.
- Conserva la información de APR (información de posición de movimiento).
- Conserva todos los parámetros de configuración de PTP (sincronización de hora).
- Conserva la hora de reloj dentro de la capacidad de retención de energía del módulo.
- Crea una entrada con sello de hora en el registro del controlador que indica que se ha producido un evento de restablecimiento de etapa 1.
- Restablece el controlador para comenzar el proceso de puesta en marcha del controlador.
- Evita que el controlador cargue firmware o software desde la tarjeta SD durante este encendido inicial después del restablecimiento, independientemente del ajuste en la tarjeta SD, y sin modificar el contenido de la tarjeta SD (el ajuste de protección de escritura es irrelevante). Una tarjeta SD se recarga (si se configura para hacerlo) cuando se producen situaciones de encendido subsiguientes.
- Habilita el puerto Ethernet, si se inhabilitó anteriormente.

Para realizar un restablecimiento de etapa 1, siga estos pasos. Este proceso supone que hay una tarjeta SD instalada en el controlador.

1. Apague el controlador.
2. Abra la puerta frontal del controlador.
3. Presione y mantenga presionado el botón de restablecimiento, utilice una herramienta pequeña con el diámetro de un sujetapapeles.
4. Mientras mantiene pulsado este botón, encienda el controlador.
5. Siga pulsando el botón de restablecimiento mientras la pantalla de 4 caracteres muestra CLR, 4, 3, 2, 1, Project Cleared.
6. Una vez que aparezca Project Cleared, suelte el botón de restablecimiento.

IMPORTANTE Si suelta el botón de restablecimiento antes de que el mensaje Project Cleared atraviese la pantalla, el controlador continuará con el encendido sin restablecerse.

Tras realizar un restablecimiento de etapa 1, cargue un proyecto de la aplicación Logix Designer en el controlador de una de estas maneras:

- Descargue el proyecto de la aplicación Logix Designer; para obtener más información, consulte [Descarga al controlador en la página 102](#)

- Desconecte y vuelva a conectar la alimentación eléctrica del controlador para cargar un proyecto de la tarjeta SD.

Esta opción solo funciona si el proyecto almacenado en la tarjeta SD se ha configurado para cargar el proyecto durante el encendido.

Restablecimiento de etapa 2

IMPORTANTE Solo se produce un restablecimiento de etapa 2 si el controlador no contiene una aplicación del usuario y el firmware actual del controlador no es una revisión 1.x.

El restablecimiento de etapa 2 lleva a cabo lo siguiente:

- Revierte el módulo a la revisión 1.x del firmware, es decir, la revisión del firmware en su condición original.
- Borra todos los ajustes del usuario, incluidos los ajustes de sincronización de hora y de red.

Si el controlador utiliza la revisión de firmware 29.011 o una posterior, el modo EtherNet/IP se restablece en el modo de doble IP, es decir, el modo predeterminado.

- Restablece el controlador para comenzar el proceso de puesta en marcha del controlador.
- No hay ninguna entrada en el registro del controlador después de un restablecimiento de etapa 2, pero se conservan los registros guardados en la tarjeta SD.

Para realizar un restablecimiento de etapa 2, siga estos pasos. Este proceso supone que hay una tarjeta SD instalada en el controlador.

1. Apague el controlador.
2. Abra la puerta frontal del controlador.
3. Retire la tarjeta SD.
4. Presione y mantenga presionado el botón de restablecimiento, utilice una herramienta pequeña con el diámetro de un sujetapapeles.
5. Mientras mantiene pulsado este botón, encienda el controlador.
6. Siga pulsando el botón de restablecimiento mientras la pantalla de 4 caracteres muestra DFLT, 4, 3, 2, 1, Factory Default.
7. Una vez que aparezca Factory Default, suelte el botón de restablecimiento.
8. En la estación de trabajo, elimine los archivos de la tarjeta SD.
9. Apague el controlador.
10. Reinstale la tarjeta SD.

11. Encienda el controlador.
12. Compruebe que el controlador tiene la revisión de firmware 1.x y que está habilitado para DHCP.

Tras realizar un restablecimiento de etapa 2, debe llevar a cabo las siguientes tareas para volver a utilizar el controlador:

- Configure los puertos Ethernet, establezca el modo EtherNet/IP deseado y establezca la configuración de la dirección IP del controlador.

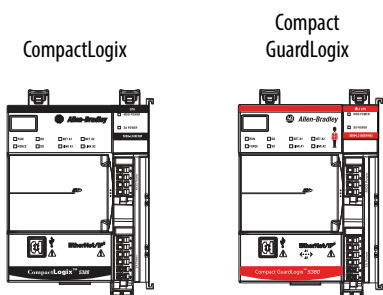
Para obtener más información, consulte [Establecimiento de la dirección IP del controlador en la página 65](#).

- Actualice la revisión del firmware; para obtener más información, consulte [Actualización del firmware del controlador en la página 74](#).
- Descargue un proyecto de la aplicación Logix Designer al controlador de una de las siguientes maneras:
 - Descargue el proyecto desde la aplicación Logix Designer; para obtener más información, consulte [Descarga al controlador en la página 102](#).
 - Desconecte y vuelva a conectar la alimentación eléctrica del controlador para cargar un proyecto de la tarjeta SD.

Esta opción solo funciona si el proyecto almacenado en la tarjeta SD se ha configurado para cargar el proyecto durante el encendido.

Uso de la tarjeta Secure Digital

Tema	Página
Consideraciones con respecto al almacenamiento y la carga de un proyecto de seguridad	120
Almacenamiento en la tarjeta SD	121
Carga desde la tarjeta SD	125
Otras tareas con la tarjeta Secure Digital	128



Los controladores se envían con una tarjeta SD instalada. Recomendamos dejar instalada la tarjeta SD para que en caso de ocurrir un fallo los datos de diagnóstico se escriban automáticamente en la tarjeta. Rockwell Automation puede utilizar los datos para ayudar a investigar la causa del fallo.

Recomendamos el uso de tarjetas SD disponibles de Rockwell Automation:

- Tarjeta 1784-SD2: Tarjeta de 2 GB que se envía con el controlador.
- Tarjeta 1784-SD1: Tarjeta de 1 GB
- CodeMeter CmCard SD, 4 GB, número de catálogo 9509-CMSDCD4 (cuando se habilitan las características de protección de fuente y protección de ejecución basadas en licencia).

Si bien es posible utilizar otras tarjetas SD con el controlador, Rockwell Automation no ha probado el uso de dichas tarjetas con el controlador y podría ocurrir alteración o pérdida de datos.

Las tarjetas SD que no han sido suministradas por Rockwell Automation pueden tener clasificaciones industriales, ambientales y de certificación diferentes a las de las tarjetas que ofrece Rockwell Automation. Es posible que estas tarjetas no puedan resistir los mismos ambientes industriales para los que están preparadas las versiones con clasificación industrial que ofrece Rockwell Automation.

La tarjeta de memoria compatible con su controlador se utiliza para cargar o almacenar el contenido de la memoria del usuario del controlador.

Cuando utiliza la función Store, el proyecto almacenado en la tarjeta SD coincide con el proyecto en la memoria del controlador en ese momento. Los cambios efectuados después de almacenarse el proyecto no se reflejan en el proyecto alojado en la tarjeta SD.

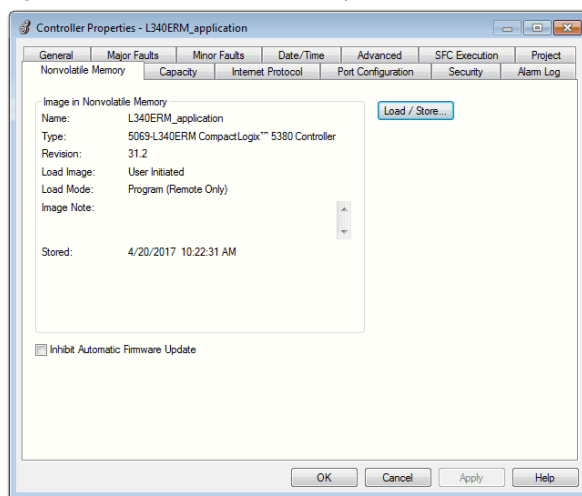
Si hace cambios en el proyecto alojado en la memoria del controlador pero no almacena dichos cambios, sobrescribirá estos la próxima vez que cargue el proyecto desde una tarjeta SD al controlador.

IMPORTANTE No retire la tarjeta SD cuando el controlador lea la tarjeta o escriba en ella. Si retira la tarjeta durante la lectura o escritura, se pueden alterar los datos en la tarjeta o en el controlador.

Además, se puede alterar el firmware del controlador al momento en el que se retira la tarjeta. Deje la tarjeta en el controlador hasta que el indicador de estado SD se ponga verde fijo.

Si se instala una tarjeta SD, 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 seguridad.

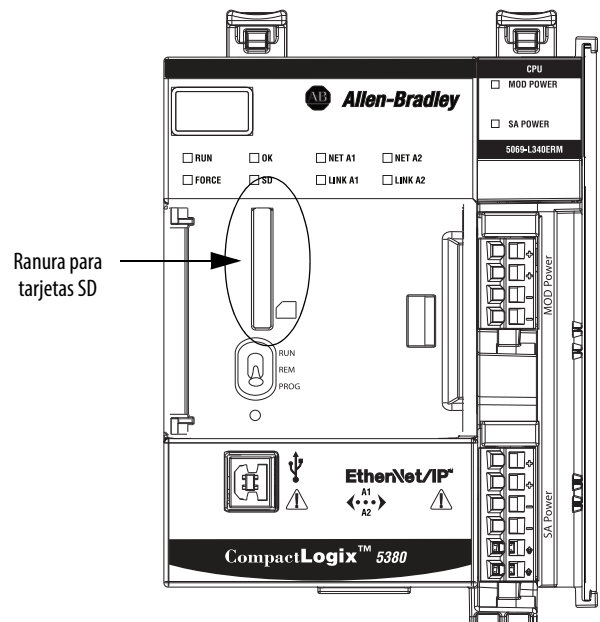
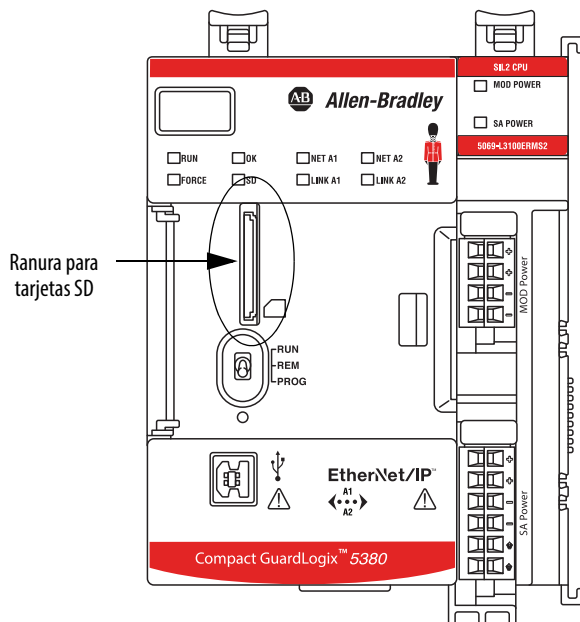
Figura 20 – Ficha Nonvolatile Memory



El proyecto debe estar en línea para poder ver el contenido de la tarjeta SD.

Recuerde lo siguiente:

- Hay una ranura para tarjeta SD en la parte frontal del controlador, detrás de la puerta.



- Si hay una tarjeta instalada y se produce un fallo, los datos de diagnóstico se escribirán automáticamente en la tarjeta. Los datos de diagnóstico ayudan a investigar y corregir la causa de un fallo.
- El controlador detecta la presencia de una tarjeta SD al momento del encendido o si se inserta una tarjeta durante el funcionamiento del controlador.
- La tarjeta SD puede almacenar todos los datos de configuración que se guardan en la memoria no volátil, como por ejemplo, la dirección IP del controlador.
- La tarjeta SD puede almacenar el programa de copia de seguridad.

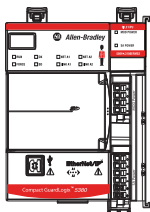
IMPORTANTE Rockwell Automation recomienda que haga una copia de seguridad del programa Studio 5000 Logix Designer® en una tarjeta SD con regularidad.

Si se produce un fallo mayor no recuperable que elimina el programa de la memoria del controlador, es posible restaurar automáticamente en el controlador la copia de seguridad de la tarjeta SD y reanudar rápidamente el funcionamiento normal del controlador.

Para obtener información detallada sobre cómo usar la memoria no volátil, consulte el documento Logix 5000 Controllers Nonvolatile Memory Programming Manual, publicación [1756-PM017](#).

Consideraciones con respecto al almacenamiento y la carga de un proyecto de seguridad

Compact GuardLogix



Solo los controladores Compact GuardLogix® 5380 son compatibles con los proyectos de seguridad. Los controladores CompactLogix™ 5380 no son compatibles con los proyectos de seguridad.

No se puede almacenar un proyecto de seguridad si el estado de seguridad es Safety Task Inoperable. Cuando almacena un proyecto de seguridad, el firmware del controlador también se guarda en la tarjeta SD.

Si no existe un proyecto de aplicación en el controlador, puede guardar solo el firmware del controlador de seguridad.

Si existe una firma 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 almacenan con sus valores actuales
- La firma de seguridad actual se guarda

Cuando almacene un proyecto de aplicación de seguridad en una tarjeta SD, Rockwell Automation recomienda que seleccione Program (Remote Only) como el modo de carga, es decir, el modo al que entra el controlador después de la carga de un proyecto desde la tarjeta SD.

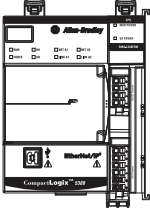
IMPORTANTE Para ayudar a evitar que el firmware almacenado en la tarjeta SD sobrescriba el firmware recién actualizado:

- El proceso de actualización primero comprueba la opción de carga en la tarjeta SD y cambia dicha opción a User Initiated, si procede.
- La actualización de firmware continúa.
- Se restablece el controlador.
- La opción de carga permanece establecida en User Initiated.

Si la tarjeta SD está bloqueada, no se cambia la opción de carga y el firmware almacenado en la tarjeta SD puede sobrescribir el firmware recién actualizado.

Almacenamiento en la tarjeta SD

CompactLogix



Compact GuardLogix

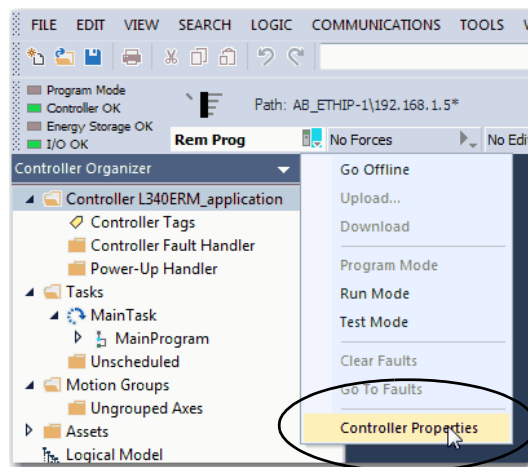


Recomendamos que haga una copia de seguridad de su aplicación Studio 5000 Logix Designer en una tarjeta SD con regularidad.

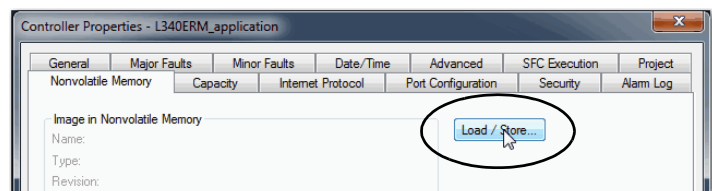
Si se produce un fallo mayor no recuperable que elimina el programa de la memoria del controlador, es posible restaurar automáticamente al controlador la copia de seguridad de la tarjeta SD para reanudar rápidamente el funcionamiento normal del controlador.

Para almacenar un proyecto en la tarjeta SD, siga estos pasos.

1. Asegúrese de que el controlador esté en línea y en modo de programación o en modo de programación remota.
2. En el menú desplegable Controller Status, haga clic en Controller Properties.



3. En la ficha Nonvolatile Memory, haga clic en Load/Store.




SUGERENCIA

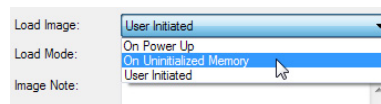
Si Load/Store aparece atenuado (no disponible), compruebe lo siguiente:

- El controlador está en el modo de programación o en el modo de programación remota
- Ha especificado la ruta de comunicación correcta.
- La tarjeta SD está instalada.
- La tarjeta SD está desbloqueada. El estado de bloqueo aparece en la esquina inferior izquierda del cuadro de diálogo Nonvolatile memory/ Load Store.

Si no hay una tarjeta SD instalada, aparece un mensaje en la esquina inferior izquierda de la ficha Nonvolatile Memory para indicar que falta la tarjeta, tal como se muestra aquí.

 Nonvolatile memory not present.

4. Cambie las propiedades de Load Image según los requisitos de su aplicación.



Esta tabla describe las opciones de Load Image.

Tabla 9 – Opciones de imagen de carga

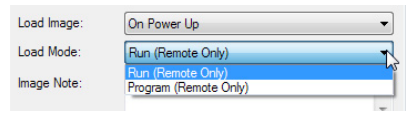
Si desea cargar el proyecto	Seleccione esta opción de imagen de carga	Notas	Consideraciones de seguridad
Siempre que encienda o desconecte y vuelva a conectar la alimentación eléctrica	En el momento del encendido	<ul style="list-style-type: none"> Durante la desconexión y reconexión de la alimentación eléctrica, se pierden todos los cambios en línea, los valores de tags y la programación de la red que no hayan sido almacenados en la memoria no volátil. El controlador carga el proyecto almacenado y el firmware durante el encendido, independientemente del firmware o del proyecto de la aplicación en el controlador. Siempre puede utilizar la aplicación Studio 5000 Logix Designer para cargar el proyecto. 	<ul style="list-style-type: none"> En el caso de una aplicación de seguridad, On Power Up se carga independientemente de si el controlador está o no está en bloqueo de seguridad o si hay una firma de seguridad. Si se configura la aplicación para realizar la carga desde la tarjeta SD al momento de encendido, se sobrescribe la aplicación en el controlador incluso si el controlador está en bloqueo de seguridad.
Cuando no hay un proyecto en el controlador y usted enciende o desconecta y vuelve a conectar la alimentación eléctrica del chasis	En memoria no inicializada	<ul style="list-style-type: none"> Si el proyecto se borró de la memoria, esta opción vuelve a cargar el proyecto en el controlador al momento del encendido. El controlador actualiza el firmware del controlador si es necesario. El proyecto de la aplicación almacenado en la memoria no volátil también se carga, y el controlador entra al modo seleccionado, ya sea programación o marcha. Siempre se puede usar la aplicación Logix Designer para cargar el proyecto. 	<ul style="list-style-type: none"> El controlador también actualiza el firmware en el homólogo de seguridad, si procede.
Solo mediante la aplicación Logix Designer	Iniciado por el usuario	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Puede iniciar una carga, independientemente del estado de seguridad. Puede cargar un proyecto a un controlador en bloqueo de seguridad solo cuando la firma 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 está en bloqueo de seguridad sin una firma 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 seguridad se establecen en los valores contenidos en la memoria no volátil una vez que la carga se ha completado. Si el firmware en el controlador primario coincide con la revisión en la memoria no volátil, el firmware homólogo de seguridad se actualiza, si es necesario, la aplicación almacenada en la memoria no volátil se carga de modo que el estado de seguridad se convierta en Safety Task Operable y el controlador entre al modo de programación.

IMPORTANTE Para ayudar a evitar que el firmware almacenado en la tarjeta SD sobrescriba el firmware recién actualizado:

- El proceso de actualización primero comprueba la opción de carga en la tarjeta SD y cambia dicha opción a User Initiated, si procede.
- La actualización de firmware continúa.
- Se restablece el controlador.
- La opción de carga permanece establecida en User Initiated.

Si la tarjeta SD está bloqueada, no se cambia la opción de carga y el firmware almacenado en la tarjeta SD puede sobrescribir el firmware recién actualizado.

5. Cambie las propiedades de Load Mode según los requisitos de su aplicación.

Si desea que el controlador entre en este modo después de la carga	Seleccione	Elementos del menú
Program	Program (Remote Only)	
Run	Run (Remote Only)	

IMPORTANTE Consideraciones de seguridad

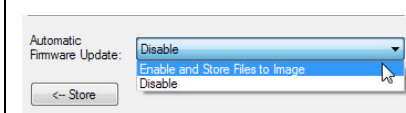
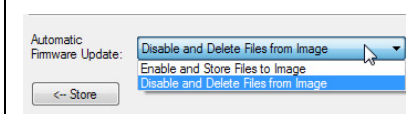
Rockwell Automation recomienda que utilice Program (Remote Only) cuando establezca el modo de carga para un proyecto de la aplicación de seguridad.

6. De acuerdo a sus requisitos de la aplicación, establezca las propiedades de actualización automática de firmware para dispositivos de E/S en el árbol de configuración del controlador. La propiedad Automatic Firmware Update también se conoce como la función Firmware Supervisor.

IMPORTANTE Consideraciones de seguridad

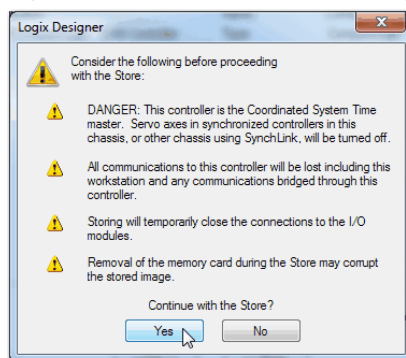
Algunos dispositivos de E/S de seguridad no son compatibles con la función Firmware Supervisor. Por ejemplo, los dispositivos de E/S de seguridad en redes DeviceNet y los módulos POINT Guard I/O™ no son compatibles con la función Firmware Supervisor.

Esta tabla describe las opciones de actualización automática de firmware para los dispositivos de E/S.

Configuración	Descripción	Elementos del menú
Disable	Inhabilita cualquier actualización automática del firmware. Este elemento solo aparece en el menú cuando se guarda en un principio la imagen.	
Enable and Store Files to Image	Habilita las actualizaciones automáticas de firmware en los dispositivos de E/S del árbol de configuración del controlador. Guarda el firmware del dispositivo de E/S y el firmware del controlador en la imagen. Solo los dispositivos de E/S configurados para la codificación exactamente igual participan en el proceso de actualización automática de firmware. ⁽¹⁾	
Inhabilitación y eliminación de archivos de la imagen	Inhabilita las actualizaciones automáticas del firmware para los dispositivos de E/S del árbol de configuración del controlador. Elimina el firmware del dispositivo de E/S de la imagen, pero no elimina el firmware del controlador de la imagen. Este elemento solo aparece en el menú cuando se guarda la imagen después de la primera vez.	

(1) Los dispositivos utilizados con esta opción deben ser compatibles con la revisión de firmware a la cual se actualizan.

7. Haga clic en Store.
8. Haga clic en Yes en el cuadro de diálogo de confirmación que aparecerá.



Si ha habilitado Automatic Firmware Update, aparecerá un cuadro de diálogo para informarle cuáles módulos no se han incluido en la operación Automatic Firmware Update.

IMPORTANTE No retire la tarjeta SD cuando el controlador lea la tarjeta o escriba en ella. Si retira la tarjeta durante la lectura o escritura, se pueden alterar los datos en la tarjeta o en el controlador. Además, se puede alterar el firmware del controlador al momento en el que se retira la tarjeta. Deje la tarjeta en el controlador hasta que el indicador de estado SD se ponga verde fijo.

9. En el cuadro de diálogo Automatic Firmware Update, haga clic en Yes.

El proyecto se guarda en la tarjeta SD, tal como señalan los indicadores de estado del controlador.

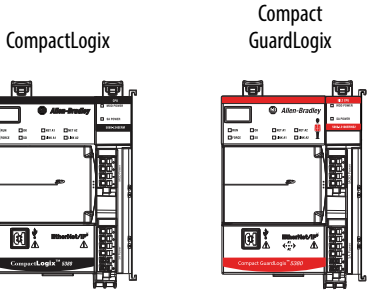
Estas indicaciones muestran el estado de almacenamiento

Mientras la operación de almacenamiento está **en curso**, ocurre lo siguiente:

- El indicador OK parpadea de color verde
 - El indicador SD parpadea de color verde
 - Aparece Saving... Do Not Remove SD Card en la pantalla de estado
 - Un cuadro de diálogo de la aplicación Logix Designer indica que hay una operación de almacenamiento en curso
 - El controlador se restablece
 - Aparece SAVE en la pantalla de estado
- Una vez **concluida** la operación de almacenamiento, ocurre lo siguiente:
- Se restablece el controlador.
-

IMPORTANTE Permita que la operación de almacenamiento concluya sin interrupción. Si interrumpe la operación de almacenamiento, pueden perderse o alterarse los datos.

Carga desde la tarjeta SD



Tras establecer la ruta de comunicación, estar en línea con el controlador y haber cambiado el controlador al modo de programación, puede cargar un proyecto al controlador desde la tarjeta de memoria.

IMPORTANTE

Con la tarjeta SD y nuevos controladores en condición original:

- Si inserta una tarjeta SD con una imagen en un nuevo controlador en condición original (firmware 1.x), durante el encendido el controlador actualiza automáticamente el firmware a la versión de firmware almacenada en la tarjeta SD. Se lleva a cabo la actualización independientemente del ajuste Load Image en la imagen en la tarjeta SD (User Initiated, On Power Up u On Uninitialized Memory).
- Si la imagen fue creada con los ajustes On Power Up u On Uninitialized Memory, el controlador actualiza el firmware y realiza la carga en la aplicación del controlador.

Puede cargar de una tarjeta SD a un controlador de una de estas maneras:

- [Encendido del controlador](#)
- [Acción iniciada por el usuario](#)

SUGERENCIA Siempre se puede usar la aplicación Logix Designer para cargar el proyecto.

Encendido del controlador

Esta tabla muestra qué sucede al momento del encendido cuando la tarjeta SD en el controlador contiene una imagen.

Ajuste de imagen	El controlador está en su condición original (firmware v1.xxx)	Firmware > 1.xxx y la memoria no volátil interna no es válida ⁽²⁾	Firmware > 1.xxx y la memoria no volátil interna es válida ⁽²⁾
User Initiated	Carga únicamente el firmware ⁽¹⁾	No hace nada	No hace nada
On Power Up	Carga el firmware y la aplicación	<ul style="list-style-type: none">• Carga el firmware si hay una discordancia en la revisión• Carga la aplicación	<ul style="list-style-type: none">• Carga el firmware si hay una discordancia en la revisión• Carga la aplicación
On Uninitialized Memory	Carga el firmware y la aplicación ⁽²⁾	<ul style="list-style-type: none">• Carga el firmware si hay una discordancia en la revisión• Carga la aplicación	No hace nada

(1) Indica el cambio de comportamiento entre el CompactLogix 5370 y los controladores más antiguos.

(2) "Valid" incluye la condición No Project.

Acción iniciada por el usuario

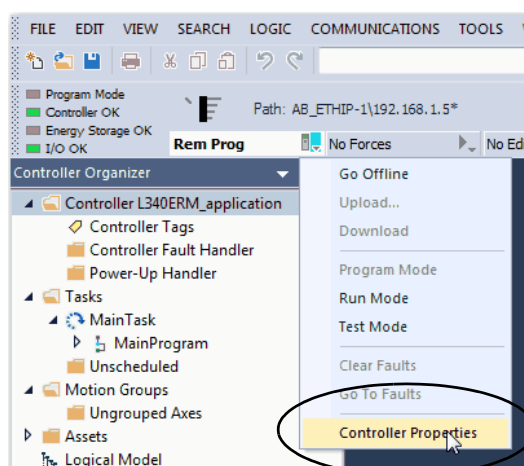
IMPORTANTE En el caso de un controlador en condición original que utiliza la revisión de firmware 1.xx, debe actualizar manualmente el controlador a la revisión de firmware requerida antes de poder cargar un proyecto en el controlador.

Debe hacer lo siguiente antes de poder cargar un proyecto al controlador desde la tarjeta SD cuando el controlador ya está encendido:

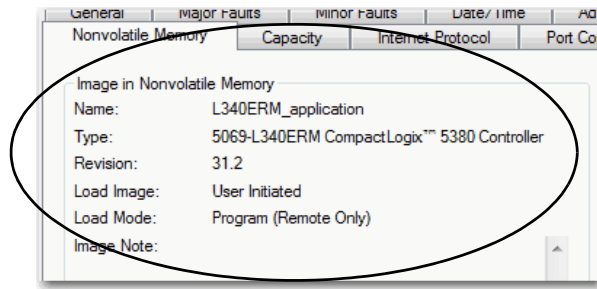
- Asegúrese de que el controlador tenga una revisión de firmware de trabajo.
- Establezca la ruta de comunicación.
- Entre en línea con el controlador.
- Asegúrese de que el controlador esté en modo de programación.

Siga estos pasos para cargar un proyecto al controlador desde la tarjeta SD.

1. En el menú desplegable Controller Status, haga clic en Controller Properties.



2. En la ficha Nonvolatile Memory, compruebe que el proyecto que aparece es el correcto.

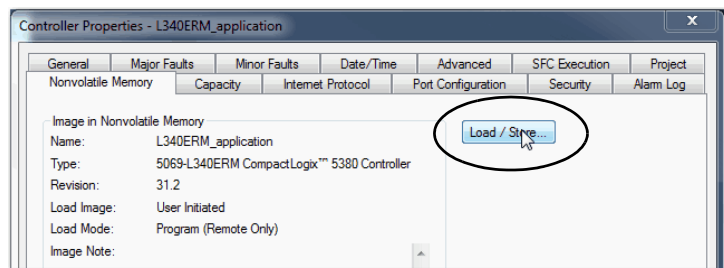


SUGERENCIA Si no hay ningún proyecto almacenado en la tarjeta SD, aparecerá un mensaje en la ficha Nonvolatile Memory para indicar que no hay una imagen (o proyecto) disponible.



Para obtener más información sobre cómo cambiar el proyecto que está disponible para cargarlo desde la memoria no volátil, consulte el documento Logix 5000 Controllers Nonvolatile Memory Programming Manual, publicación [1756-PM017](#).

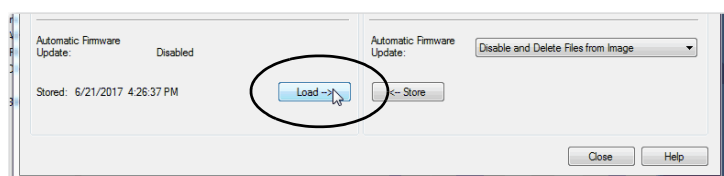
3. Haga clic en Load/Store.



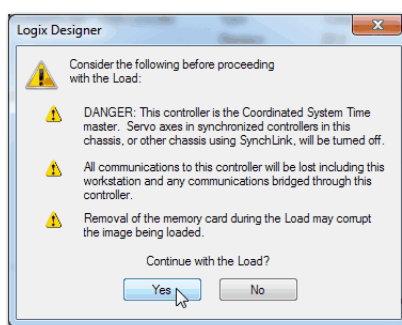
SUGERENCIA Si Load/Store aparece atenuado (no disponible), compruebe lo siguiente:

- Ha especificado la ruta de comunicación correcta y está en línea con el controlador.
- La tarjeta SD está instalada.
- El controlador no está en modo de marcha.

4. Haga clic en Load.



5. Haga clic en Yes en el cuadro de diálogo de confirmación que aparecerá.



Tras hacer clic en Yes, se cargará el proyecto en el controlador tal como informarán los indicadores de estado del controlador.

Estas indicaciones muestran el estado de carga

Mientras la **operación de almacenamiento está en curso**, ocurre lo siguiente:

- El indicador OK está rojo fijo
- El indicador SD parpadea de color verde
- Aparece Saving... Do Not Remove SD Card en la pantalla de estado
- Updating Firmware... Do Not Remove SD Card puede aparecer en la pantalla de estado si el firmware también se está actualizando con la carga
- Un cuadro de diálogo de la aplicación Logix Designer indica que hay una operación de almacenamiento en curso

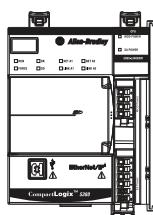
Una vez que la **operación de almacenamiento concluye**, ocurre lo siguiente:

- El controlador se reinicializa.

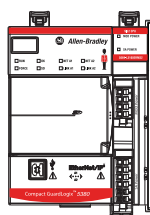
IMPORTANTE Espere a que finalice la operación de carga sin interrupción. Si interrumpe la carga, pueden perderse o alterarse los datos.

Otras tareas con la tarjeta Secure Digital

CompactLogix



Compact GuardLogix



Puede realizar estas tareas con la tarjeta SD:

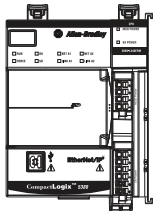
- Cambiar la imagen que se carga de la tarjeta
- Comprobar si se ha completado una carga
- Borrar una imagen de la tarjeta SD
- Almacenar una imagen vacía
- Cambiar los parámetros de la carga
- Leer/escribir datos de la aplicación en la tarjeta
- Ver el estado de bloqueo de seguridad y las firmas de seguridad en la ficha Non-volatile Memory (controladores Compact GuardLogix 5380 únicamente).

Para obtener más información sobre cómo llevar a cabo cualquiera de estas tareas, consulte el documento Logix 5000 Controllers Memory Card Programming Manual, publicación [1756-PM017](#).

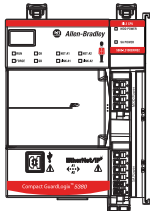
Red EtherNet/IP

Tema	Página
Funcionalidad de la red EtherNet/IP	130
Software para redes EtherNet/IP	131
Nodos de una red EtherNet/IP	131
Topologías de red EtherNet/IP	134
Velocidades de comunicación de la red EtherNet/IP	137
Interface de socket	139

CompactLogix



Compact GuardLogix



Los controladores CompactLogix™ 5380 y Compact GuardLogix® 5380 funcionan en redes EtherNet/IP.

Recuerde que debe configurar el driver en el software RSLinx® Classic antes de que el controlador pueda funcionar en la red EtherNet/IP. Para obtener más información sobre cómo configurar un driver, vea la [página 57](#) y la [página 59](#).

IMPORTANTE Algunos gráficos de ejemplo en este capítulo utilizan los controladores CompactLogix 5380 y algunos utilizan los controladores Compact GuardLogix 5380.

El controlador utilizado se muestra con fines ilustrativos únicamente. Cada ejemplo puede usar los dos tipos de controlador. Por ejemplo, los gráficos mostrados en la sección [Topología de red lineal](#) a partir de la [página 135](#) utilizan los controladores Compact GuardLogix 5380. Puede utilizar los controladores CompactLogix 5380 en los mismos ejemplos.

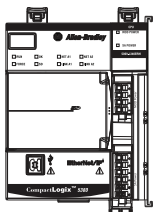
La red EtherNet/IP ofrece un conjunto completo de servicios de control, configuración y recolección de datos mediante la superposición del protocolo industrial común (CIP) sobre los protocolos de Internet estándar, tales como TCP/IP y UDP. Esta combinación de estándares bien aceptados proporciona la capacidad requerida para aceptar intercambio de datos y aplicaciones de control.

Los controladores utilizan las transacciones de interface de socket y la comunicación convencional a través de la red EtherNet/IP para comunicarse con dispositivos Ethernet que no admiten el protocolo de aplicación EtherNet/IP.

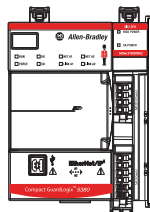
Para obtener más información sobre las transacciones de interface de socket, consulte [Interface de socket en la página 139](#).

Funcionalidad de la red EtherNet/IP

CompactLogix



Compact GuardLogix



Los controladores CompactLogix 5380 y Compact GuardLogix 5380 aceptan la siguiente funcionalidad de red EtherNet/IP:

- Dos puertos de red EtherNet/IP incorporados: Puerto A1 y puerto A2
- Compatibilidad con estos modos EtherNet/IP:
 - Modo de doble IP: disponible con la aplicación Studio 5000 Logix Designer®, versión 29.00.00 y posteriores
 - Modo lineal/DLR
- Compatibilidad con estas topologías de red EtherNet/IP:
 - Anillo a nivel de dispositivos (DLR)
 - Lineal
 - Estrella
- Compatibilidad con las siguientes velocidades de comunicación de la red EtherNet/IP:
 - 10 Mbps
 - 100 Mbps
 - 1 Gbps
- Compatibilidad solo con la comunicación full-duplex

IMPORTANTE Si un dispositivo solo es compatible con half-duplex, habrá que conectarlo a un interruptor para que pueda comunicarse con un controlador CompactLogix 5380 o Compact GuardLogix 5380.

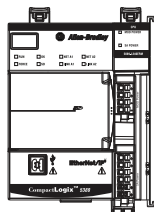
- Compatibilidad con la tecnología CIP Sync basada en la sincronización de hora utilizando el protocolo de tiempo de precisión IEEE-1588
- Detección de direcciones IP duplicadas
- Interface de sockets para comunicarse con dispositivos Ethernet que no admiten el protocolo de aplicación EtherNet/IP
- Compatibilidad con los switches Ethernet estándar de la industria; se recomiendan los switches administrados. Los switches que admiten el protocolo CIP pueden proporcionar un desempeño más predecible.
- CIP Safety a través de una red EtherNet/IP: Controladores Compact GuardLogix 5380 únicamente
- Compatibilidad con mensajes, tags producidos/consumidos, HMI y módulos de E/S distribuidas
- Compatibilidad con movimiento integrado a través de una red EtherNet/IP; no está disponible en todos los controladores CompactLogix 5380 o Compact GuardLogix 5380

Para obtener más información sobre el uso de movimiento integrado a través de una red EtherNet/IP, consulte el Capítulo 15, [Desarrollo de aplicaciones de movimiento en la página 277](#).

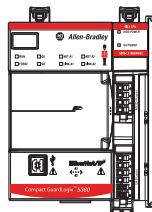
Para obtener más información acerca del diseño de la red, consulte el documento Ethernet Design Considerations Reference Manual, publicación [ENET-RM002](#).

Software para redes EtherNet/IP

CompactLogix



Compact GuardLogix



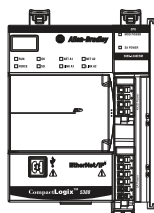
La [Tabla 10](#) indica el software que se utiliza con los módulos y las redes EtherNet/IP.

Tabla 10 – Software para uso con redes EtherNet/IP

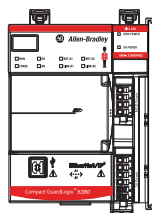
Software	Uso	Necesario u opcional
Aplicación Logix Designer	<ul style="list-style-type: none"> Configurar proyectos CompactLogix. Definir la comunicación EtherNet/IP. 	Requerido
RSLinx® Classic o RSLinx Enterprise	<ul style="list-style-type: none"> Configurar dispositivos de comunicación Proporcionar diagnósticos Establecer comunicación entre dispositivos. 	Requerido
Herramienta de puesta en marcha BOOTP DHCP EtherNet/IP	Asignar direcciones IP al controlador y a los dispositivos de una red EtherNet/IP	Opcional

Nodos de una red EtherNet/IP

CompactLogix



Compact GuardLogix



Al configurar el sistema de control CompactLogix 5380 o Compact GuardLogix 5380, debe tener en cuenta el número de nodos EtherNet/IP incluidos en la sección de configuración de E/S de su proyecto.

La [Tabla 11](#) muestra el número máximo de nodos EtherNet/IP que admiten los controladores.

Tabla 11 – Nodos EtherNet/IP del controlador CompactLogix 5380 y Compact GuardLogix 5380

Controladores CompactLogix 5380	Nodos admitidos, máx.
5069-L306ER, 5069-L306ERM	16
5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM	24
5069-L320ER, 5069-L320ERM	40
5069-L330ER, 5069-L330ERM	50, 60 ⁽¹⁾
5069-L340ER, 5069-L340ERM	55, 90 ⁽¹⁾
5069-L350ERM	60, 120 ⁽¹⁾
5069-L380ERM	70, 150 ⁽¹⁾
5069-L3100ERM	80, 180 ⁽¹⁾
Controladores Compact GuardLogix 5380	Nodos admitidos, máx.
5069-L306ERS2, 5069-L306ERS2	16
5069-L310ERS2, 5069-L310ERS2	24
L320ERS2, 5069-L320ERS2K, 5069-L320ERS2, 5069-L320ERS2K	40
5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERS2, 5069-L330ERS2K	60
5069-L340ERS2, 5069-L340ERS2	90
5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERS2, 5069-L350ERS2K	120
5069-L380ERS2, 5069-L380ERS2	150
5069-L3100ERS2, 5069-L3100ERS2	180

(1) Aplicación Studio 5000 Logix Designer, versión 31 y posteriores

Dispositivos incluidos en el conteo de nodos

Cualquier dispositivo EtherNet/IP que añada a la sección de configuración de E/S se cuenta para el límite de nodos del controlador. A continuación, se indican varios ejemplos de dispositivos que deben incluirse en el conteo:

- Adaptadores de comunicación remotos
- Switches incluidos en la sección de configuración de E/S
- Dispositivos con un puerto EtherNet incorporado, como variadores, módulos de E/S y dispositivos de vínculo
- Controladores remotos cuando se establece una conexión de producir/consumir entre los dos controladores
- Dispositivos HMI incluidos en la sección de configuración de E/S
- Dispositivos de terceros conectados directamente a la red EtherNet/IP

Dispositivos excluidos del conteo de nodos

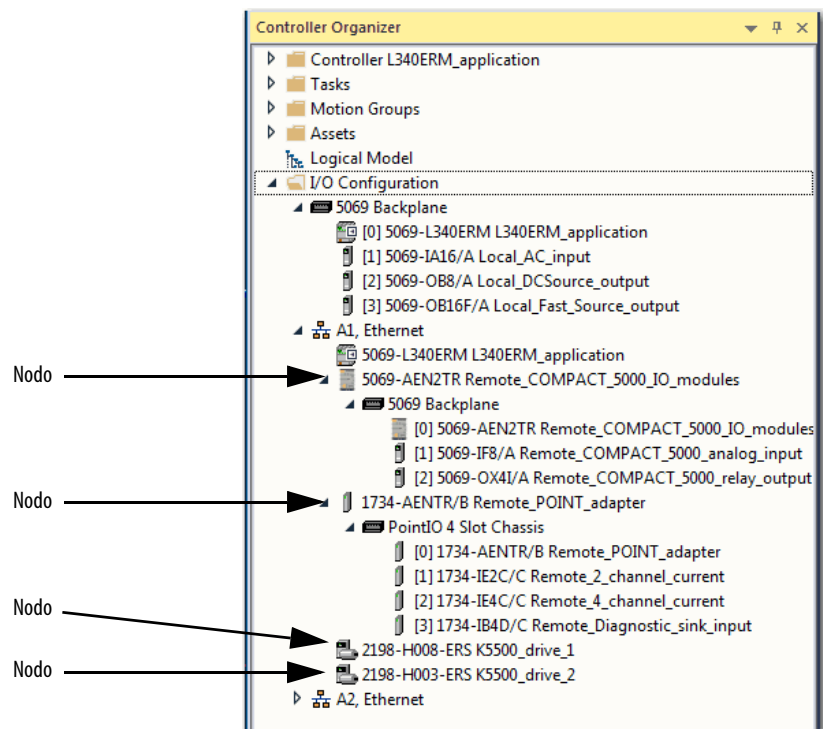
Al calcular la limitación de nodos EtherNet/IP de un controlador, no incluya en el conteo los dispositivos que existen en la red EtherNet/IP pero que no se han añadido a la sección de configuración de E/S.

Los siguientes dispositivos **no se han añadido** a la sección de configuración de E/S y **no se cuentan** para el número de nodos:

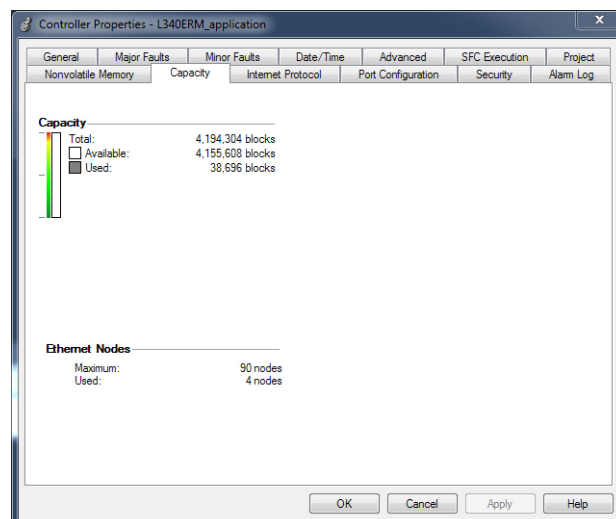
- Computadora
- Interfaces HMI que no se han añadido a la sección de configuración de E/S
- Dispositivos que son el objetivo de instrucciones MSG pero no se han añadido a la sección de configuración de E/S
- Dispositivos Ethernet estándar que se comunican con el controlador mediante una interface de socket

La [Figura 21](#) muestra los nodos de un árbol de E/S.

Figura 21 – Ejemplo de nodos EtherNet/IP

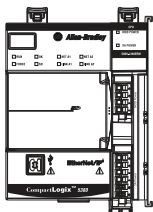


La ficha Capacity en el cuadro de diálogo Controller Properties muestra el número de nodos Ethernet utilizados en un proyecto. El siguiente gráfico corresponde al proyecto que se muestra en la [Figura 21](#).

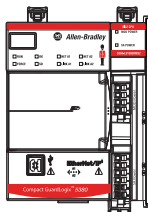


Topologías de red EtherNet/IP

CompactLogix



Compact GuardLogix



Los controladores CompactLogix 5380 y Compact GuardLogix 5380 aceptan estos tipos de red EtherNet/IP:

- [Topología de red de anillo a nivel de dispositivos](#)
- [Topología de red lineal](#)
- [Topología de red en estrella](#)

Algunos ejemplos en esta sección utilizan un controlador CompactLogix 5380 y otros ejemplos utilizan controladores Compact GuardLogix 5380. Esto es para fines ilustrativos solamente. Cualquiera de los dos tipos de controladores puede utilizarse en cada ejemplo.

Topología de red de anillo a nivel de dispositivos

Una topología de red de anillo a nivel de dispositivos (DLR) es una red de anillo con tolerancia a un solo fallo destinada a la interconexión de dispositivos de automatización. Una red DLR utiliza nodos supervisores (activo y de reserva) y nodos de anillo.

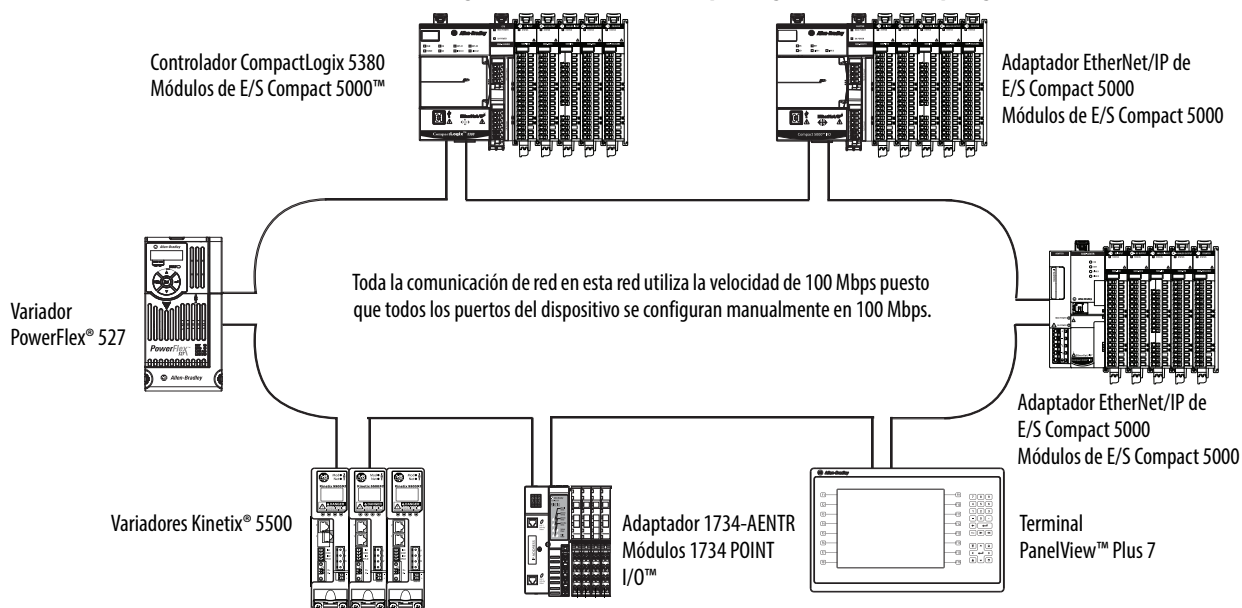
Las topologías de red DLR se convierten automáticamente en topologías de red lineales cuando se detecta un fallo. La conversión a la nueva topología de red mantiene la comunicación de los datos en la red. La condición de fallo normalmente puede detectarse y corregirse con facilidad.

El controlador está típicamente en el modo Linear/DLR cuando se utiliza en una topología DLR. Si el controlador funciona en el modo de doble IP, se debe conectar a una topología DLR mediante una ETAP conectada a un puerto Ethernet del controlador.

IMPORTANTE

Si utiliza un controlador en una red DLR con por lo menos un dispositivo que tenga una velocidad máxima de comunicación de red de 100 Mbps, establezca los puertos del controlador a 100 Mbps. Si hay otros dispositivos en el anillo que aceptan 1 Gbps, todavía debe establecer todos los dispositivos en el anillo a 100 Mbps para contribuir a proporcionar comunicación más confiable.

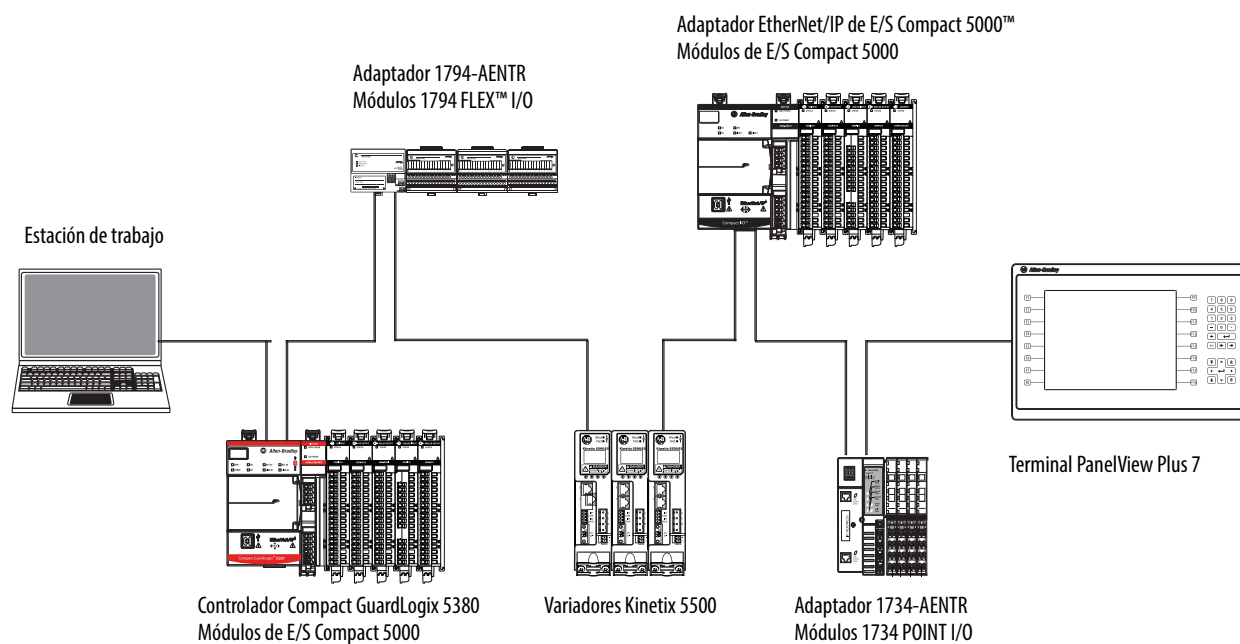
Figura 22 – Controlador CompactLogix 5380 en una topología de red DLR



Topología de red lineal

Una topología de red lineal es una colección de dispositivos conectados en cadena en una red EtherNet/IP. Los dispositivos que se pueden conectar a una topología de red lineal utilizan la tecnología con switch integrado para evitar que sea necesario un switch separado, como ocurre en las topologías de red en estrella.

Figura 23 – Controlador Compact GuardLogix 5380 en una topología de red lineal



Para obtener más información sobre cómo diseñar una red DLR, consulte el documento EtherNet/IP Embedded Switch Technology Application Guide, publicación [ENET-AP005](#).

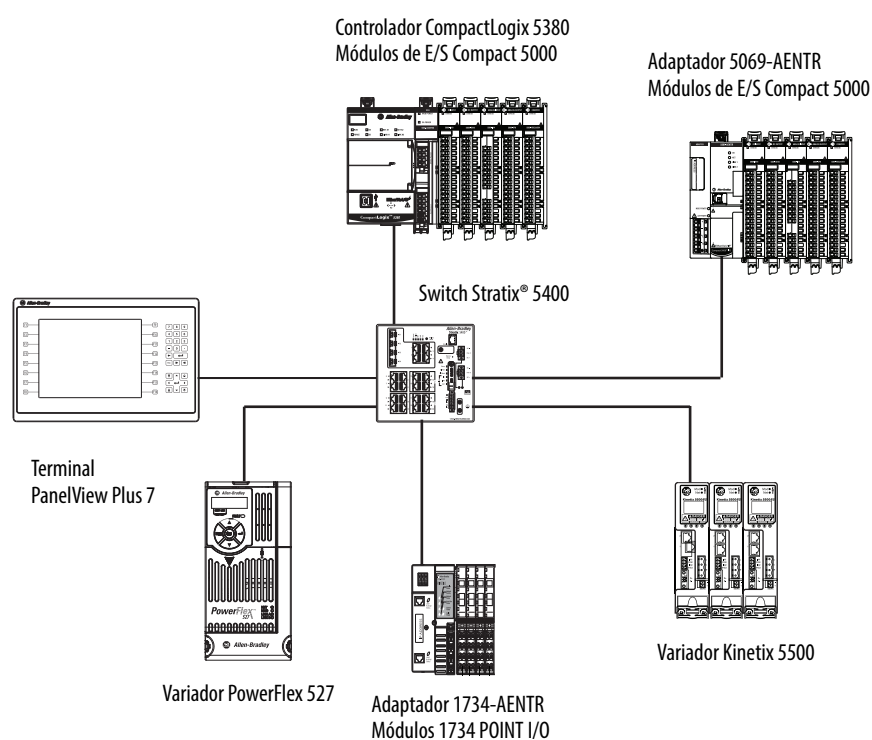
Topología de red en estrella

Una topología de red en estrella es una red EtherNet/IP tradicional que incluye varios dispositivos conectados entre sí mediante un switch Ethernet. El controlador puede funcionar en modo lineal/DLR o de doble IP cuando está conectado a una topología de red en estrella.

Si el controlador funciona en el modo de doble IP, los puertos Ethernet tienen configuraciones IP únicas y se deben conectar a subredes diferentes.

Para obtener más información sobre cómo configurar un controlador que utiliza el modo de doble IP, vea el Capítulo 9, [Uso de los modos EtherNet/IP en la página 141](#).

Figura 24 – Controladores CompactLogix 5380 en una topología de red en estrella



Herramientas de Integrated Architecture

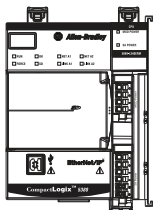
Para obtener más información al diseñar su sistema CompactLogix 5380, consulte la página web de herramientas y recursos de Integrated Architecture®. Por ejemplo, puede consultar los esquemas habituales de configuración con diferentes topologías de red EtherNet/IP.

Puede encontrar la herramienta y los recursos en:

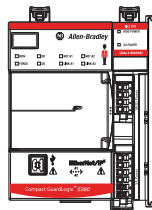
<http://www.rockwellautomation.com/global/products-technologies/integrated-architecture/tools/overview.page>

Velocidades de comunicación de la red EtherNet/IP

CompactLogix



Compact GuardLogix



Los controladores CompactLogix 5380 y Compact GuardLogix 5380 aceptan estas velocidades de comunicación de la red EtherNet/IP:

- 10 Mbps
- 100 Mbps
- 1 Gbps

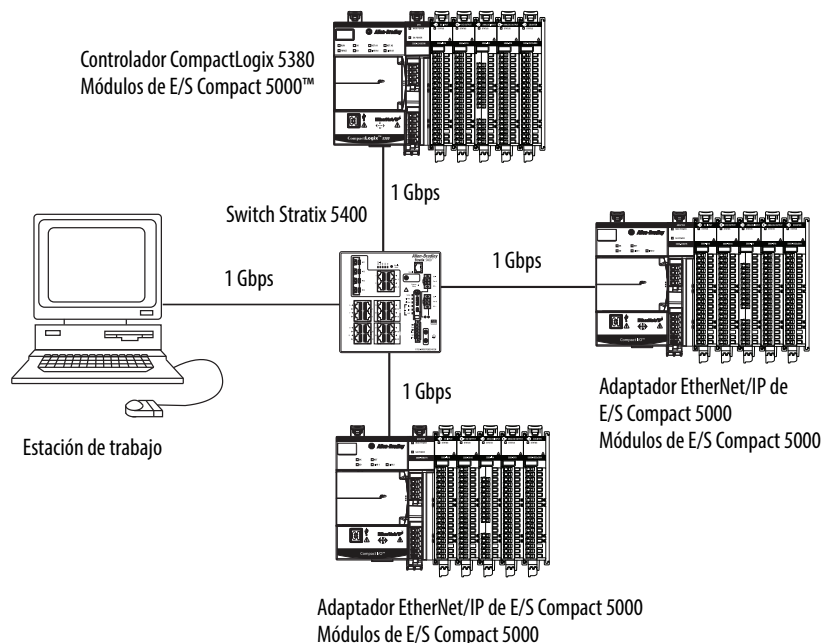
El funcionamiento de la red en un sistema CompactLogix 5380 es óptimo si se utiliza la velocidad de comunicación de red de 1 Gbps. Sin embargo, muchos dispositivos Ethernet no admiten la velocidad de comunicación de red de 1 Gbps, sino una velocidad máxima de 100 Mbps.

La diferencia de las velocidades máximas de comunicación de red afecta el sistema CompactLogix 5380 y, en algunas aplicaciones, le impide utilizar la velocidad de comunicación de red de 1 Gbps en un controlador.

Al diseñar un sistema CompactLogix 5380, si desea utilizar la velocidad de 1 Gbps en el controlador, recuerde lo siguiente:

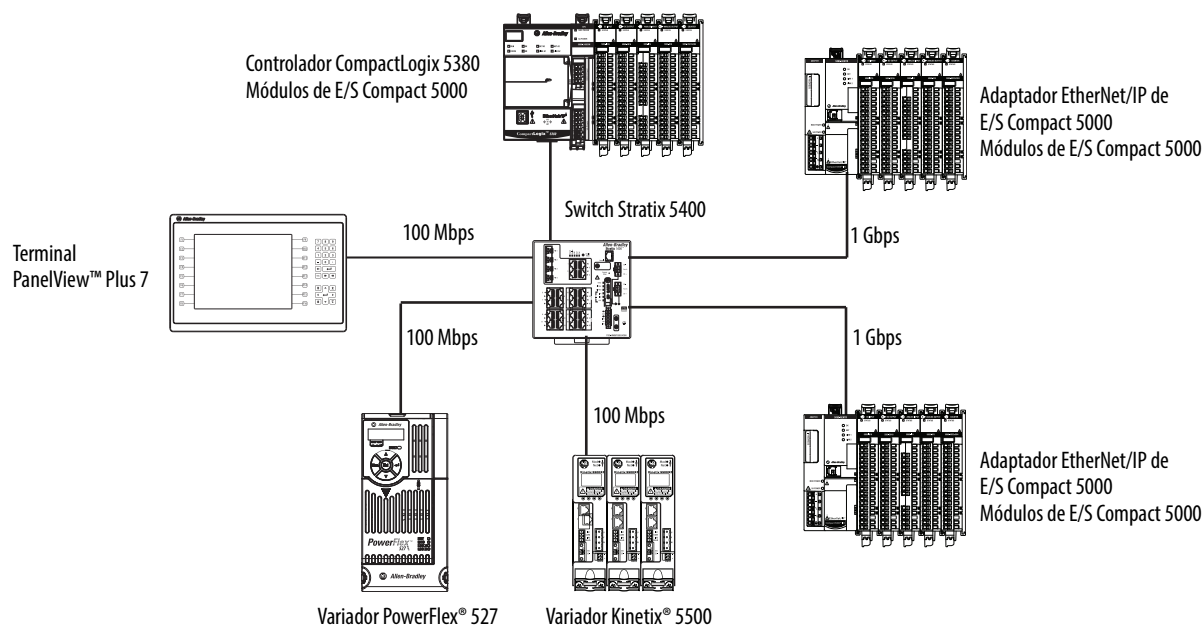
- Puede utilizar la velocidad de comunicación de red de 1 Gbps en los puertos del controlador cuando todos los dispositivos de red aceptan 1 Gbps, como por ejemplo, adaptadores 5069-AEN2TR con módulos de E/S Compact 5000 y un interruptor que acepta velocidades del orden de gigabits.

Cuando utilice la velocidad de comunicación de red de 1 Gbps, configure los puertos del controlador para que utilicen la negociación automática.



- Puede utilizar la velocidad de comunicación de red de 1 Gbps en los puertos del controlador cuando algunos dispositivos de la red admiten una velocidad máxima de comunicación de red de 100 Mbps. No obstante, en este caso, el controlador **debe estar conectado** a estos dispositivos a través de un **switch administrado**.

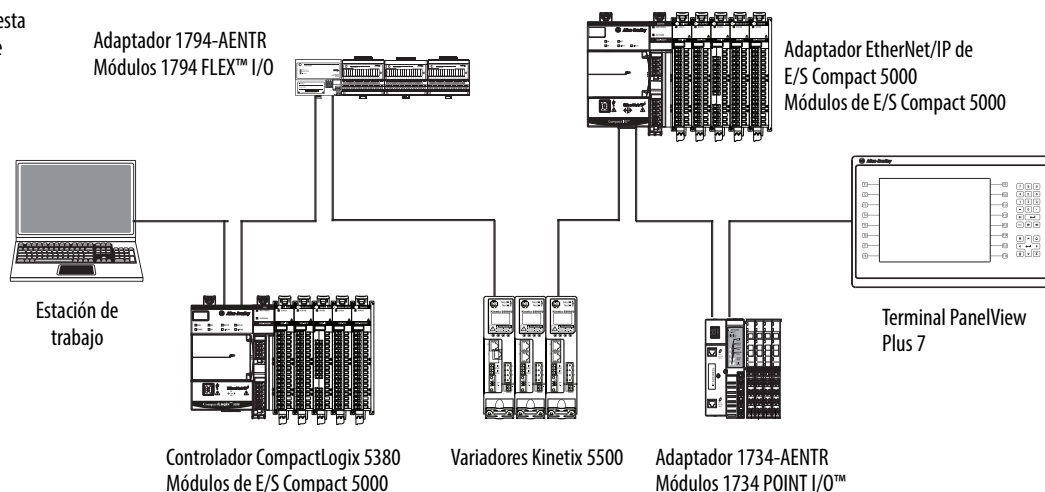
El puerto al que se conecta el controlador debe estar configurado para la negociación automática y la velocidad de comunicación de red de 1 Gbps.



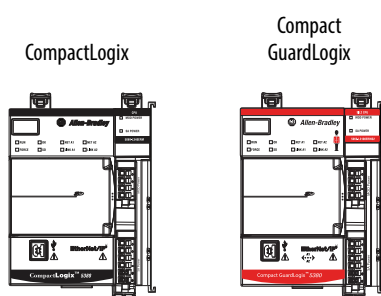
Le recomendamos que no utilice la velocidad de comunicación de red de 1 Gbps en los puertos del controlador si emplea una topología de red lineal o de anillo a nivel de dispositivos y al menos un dispositivo de la red admite la velocidad máxima de comunicación de red de 100 Mbps.

Es decir, no utilice velocidades de comunicación de red diferentes en puertos de dispositivos de la misma red EtherNet/IP sin un switch administrado.

Toda la comunicación de red en esta red se realiza a una velocidad de 100 Mbps.

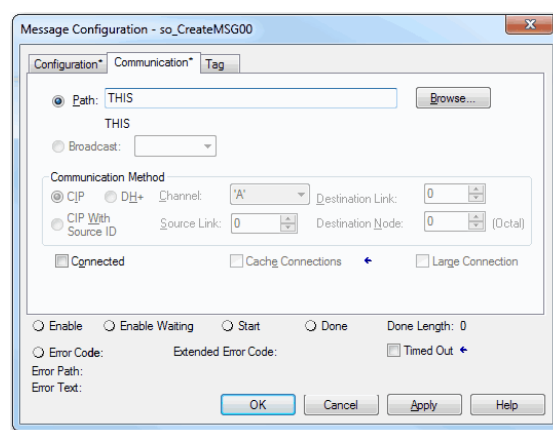
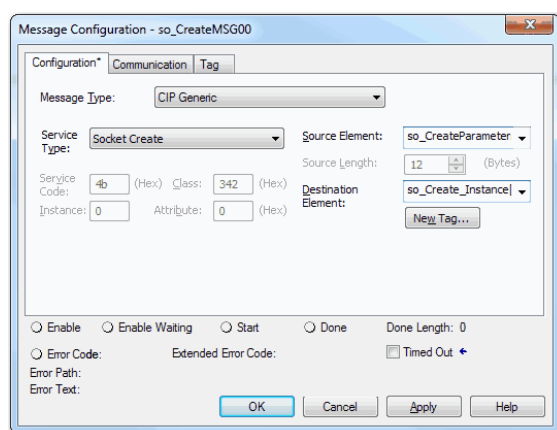


Interface de socket



El controlador puede utilizar interfaces de socket para comunicarse con dispositivos Ethernet que no admiten el protocolo de aplicación EtherNet/IP. La interface de socket se implementa mediante el objeto Socket. El controlador se comunica con el objeto Socket mediante instrucciones MSG.

Debe utilizar instrucciones MSG que configuren y manejen la interface de socket como no conectada y utilicen la ruta Message to Self. Para comunicarse con otro dispositivo, debe entender el protocolo de aplicación del otro dispositivo. A continuación, se muestran ejemplos de pantallas de una instrucción MSG utilizada con una interface de socket.



Los controladores admiten un máximo de 32 ocurrencias de sockets.

IMPORTANTE Considere lo siguiente al utilizar sockets con los controladores:

- La ruta de comunicación constituye una diferencia importante entre los controladores CompactLogix 5380 o Compact GuardLogix 5380 y otros controladores Logix 5000™. Los controladores CompactLogix 5380 no requieren un módulo de comunicación de red EtherNet/IP separado, por ejemplo, un módulo de comunicación 1756-EN2TR. En el caso de los controladores CompactLogix 5380 y Compact GuardLogix 5380, la instrucción MSG se transmite al controlador utilizando la ruta 'THIS'.
- Todos los controladores CompactLogix 5380 y Compact GuardLogix 5380 deben utilizar instrucciones MSG no conectadas para los servidores de sockets. Al configurar un mensaje para un controlador CompactLogix 5380 o Compact GuardLogix 5380, asegúrese de que la casilla de selección Connected en el cuadro de diálogo Message Configuration no esté marcada.
- Cuando el controlador funciona en modo de doble IP y utiliza un objeto de socket, puede utilizar una dirección IP con un tipo de servicio Socket_Create. Para obtener más información, consulte [Uso de objetos de socket en la página 165](#).

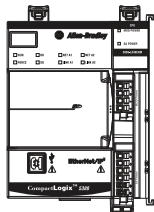
Para obtener más información acerca de la interface de socket, consulte el documento EtherNet/IP Socket Interface Application Technique, publicación [ENET-AT002](#).

Notas:

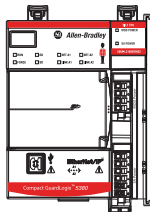
Uso de los modos EtherNet/IP

Tema	Página
Niveles de red disponibles	142
Modos EtherNet/IP	143
Solapamiento de rangos de direcciones IP	149
Configuración de los modos EtherNet/IP	150
Cambio del modo EtherNet/IP	158
Diferencias de visualización del software para los modos EtherNet/IP	166
Dirección IP del controlador y actualizaciones del firmware	168

CompactLogix



Compact GuardLogix



Este capítulo describe los modos EtherNet/IP disponibles con los controladores CompactLogix™ 5380 y Compact GuardLogix® 5380.

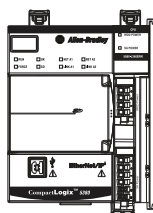
- Doble IP
- Lineal/DLR

Suponemos que cuenta con conocimientos prácticos de ambos modos antes de utilizar un controlador CompactLogix 5380 o Compact GuardLogix 5380. Este capítulo describe tareas específicas de cada aplicación que están relacionadas con los modos EtherNet/IP.

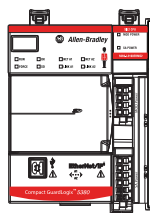
Otros capítulos de esta publicación describen cómo realizar tareas más generales en la aplicación Studio 5000 Logix Designer® y el software RSLinx® Classic software. Si es necesario, lea dichos capítulos para comprender mejor las tareas que se describen en este capítulo.

Niveles de red disponibles

CompactLogix



Compact GuardLogix



Los controladores se pueden conectar a estos niveles de red EtherNet/IP:

- [Red a nivel de empresa](#)
- [Red a nivel de dispositivo](#)

La ventaja de conectarse a niveles de red independientes es que puede segmentar las redes y aislar la comunicación en cada red. Por ejemplo, la comunicación necesaria para que el controlador ejecute una tarea está restringida a la red a nivel de dispositivo.

La segmentación de red y el aislamiento resultante pueden ayudar a mejorar la seguridad de su aplicación. Además, la opción de conectarse a niveles de red independientes lo ayuda a organizar las redes en su aplicación de manera más lógica.

Red a nivel de empresa

Tenga en cuenta lo siguiente al conectarse a las redes a nivel de empresa:

- Puede conectar solo el puerto A1 a una red a nivel de empresa.

IMPORTANTE Cuando establece la dirección IP y la máscara de subred, también establece un rango de direcciones IP para el puerto. Asegúrese de que no se solapen los rangos de direcciones IP establecidos para cada puerto en el controlador. Para obtener más información sobre el solapamiento de los rangos de direcciones IP, vea [Solapamiento de rangos de direcciones IP en la página 149](#).

Al conectar un puerto a una red a nivel de empresa, configura los siguientes parámetros:

- Dirección IP (requerida)
- Máscara de subred, también conocida como máscara de red (requerida)
- Dirección de gateway (opcional)
- Nombre de anfitrión (opcional)
- Nombre de dominio (opcional)
- Dirección de servidor DNS primaria (requerida si el controlador realiza solicitudes DNS)
- Dirección de servidor DNS secundaria (requerida si el controlador realiza solicitudes DNS)

Red a nivel de dispositivo

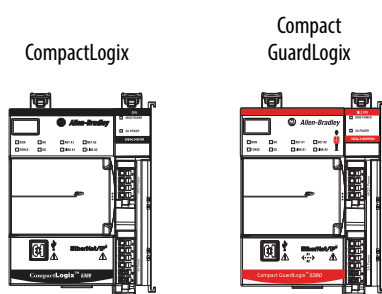
Tenga en cuenta lo siguiente al conectarse a redes a nivel de dispositivo:

- No es necesario conectar el controlador a una red a nivel de empresa para conectarse a redes a nivel de dispositivo.
- Puede conectar el puerto A1, el puerto A2 o los puertos A1 y A2 a redes a nivel de dispositivo.

Al conectar un puerto a una red a nivel de dispositivo, configura los siguientes parámetros:

- Dirección IP (requerida)
- Máscara de subred, también conocida como máscara de red (requerida)
- Dirección de gateway (opcional)
- Nombre de anfitrión (opcional)

Modos EtherNet/IP



Con la aplicación Logix Designer, versión 29 y posteriores, los controladores admiten los siguientes modos EtherNet/IP:

- [Modo de doble IP](#)
- [Modo lineal/DLR](#)

En su condición original, el modo EtherNet/IP del controlador es el de doble IP.

Modo de doble IP

El modo de doble IP le permite conectar los puertos A1 y A2 a redes independientes. En este modo, el puerto A1 puede conectarse a una red a nivel de empresa o a una red a nivel de dispositivo. El puerto A2 solo puede conectarse a una red a nivel de dispositivo.

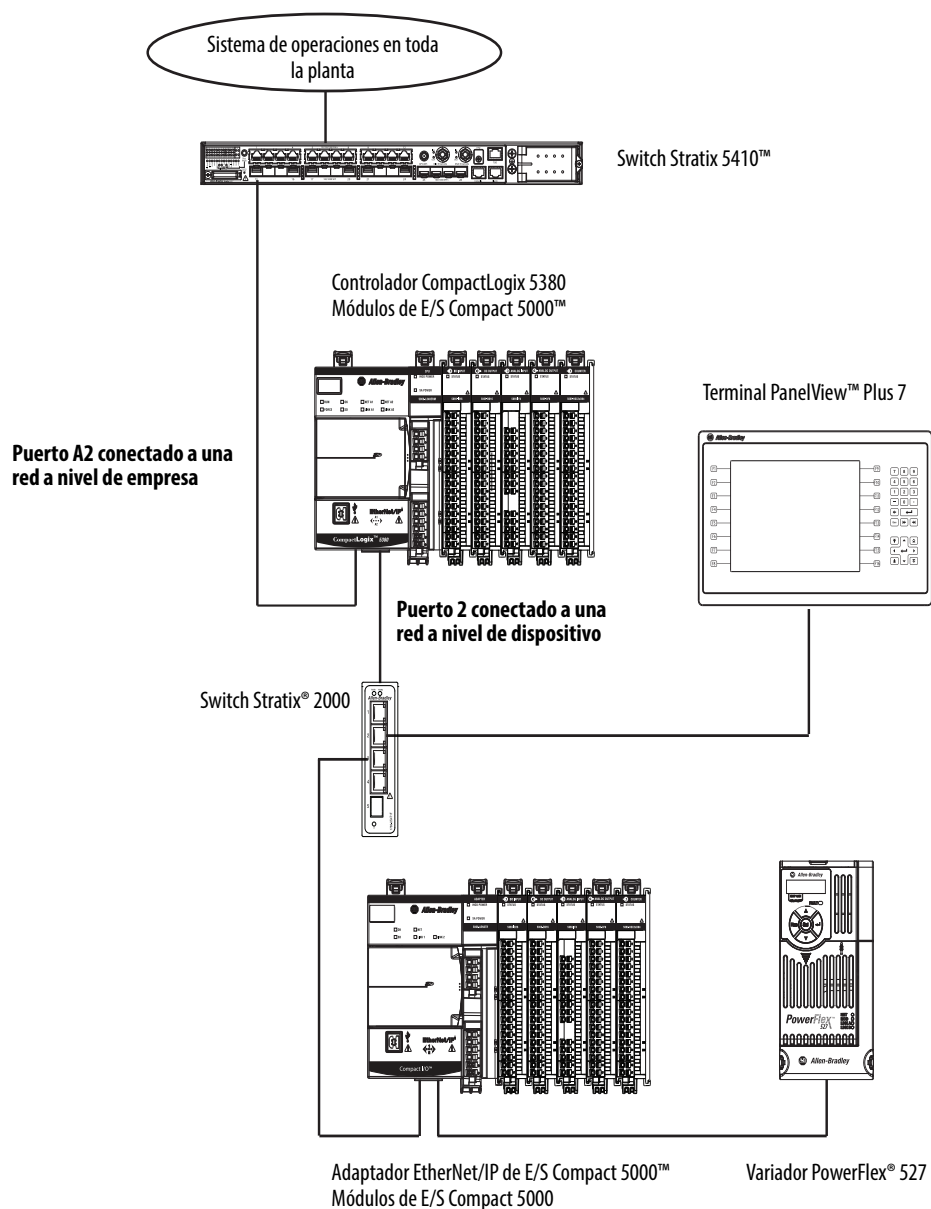
IMPORTANTE El modo de doble IP está disponible por primera vez con la revisión 29.011 y posteriores del firmware del controlador CompactLogix 5380.

En este modo, cada puerto requiere su propia configuración de red. Para obtener más información sobre cómo configurar los puertos Ethernet cuando el controlador utiliza el modo de doble IP, vea [Configuración de los modos EtherNet/IP en la página 150](#).

Hay que evitar el solapamiento de los rangos de direcciones IP al configurar los puertos Ethernet en el modo de doble IP. Para obtener más información, consulte [Solapamiento de rangos de direcciones IP en la página 149](#).

La [Figura 25](#) muestra un controlador CompactLogix 5380 utilizando el modo de doble IP con conexiones a una red a nivel de empresa y a una red a nivel de dispositivo.

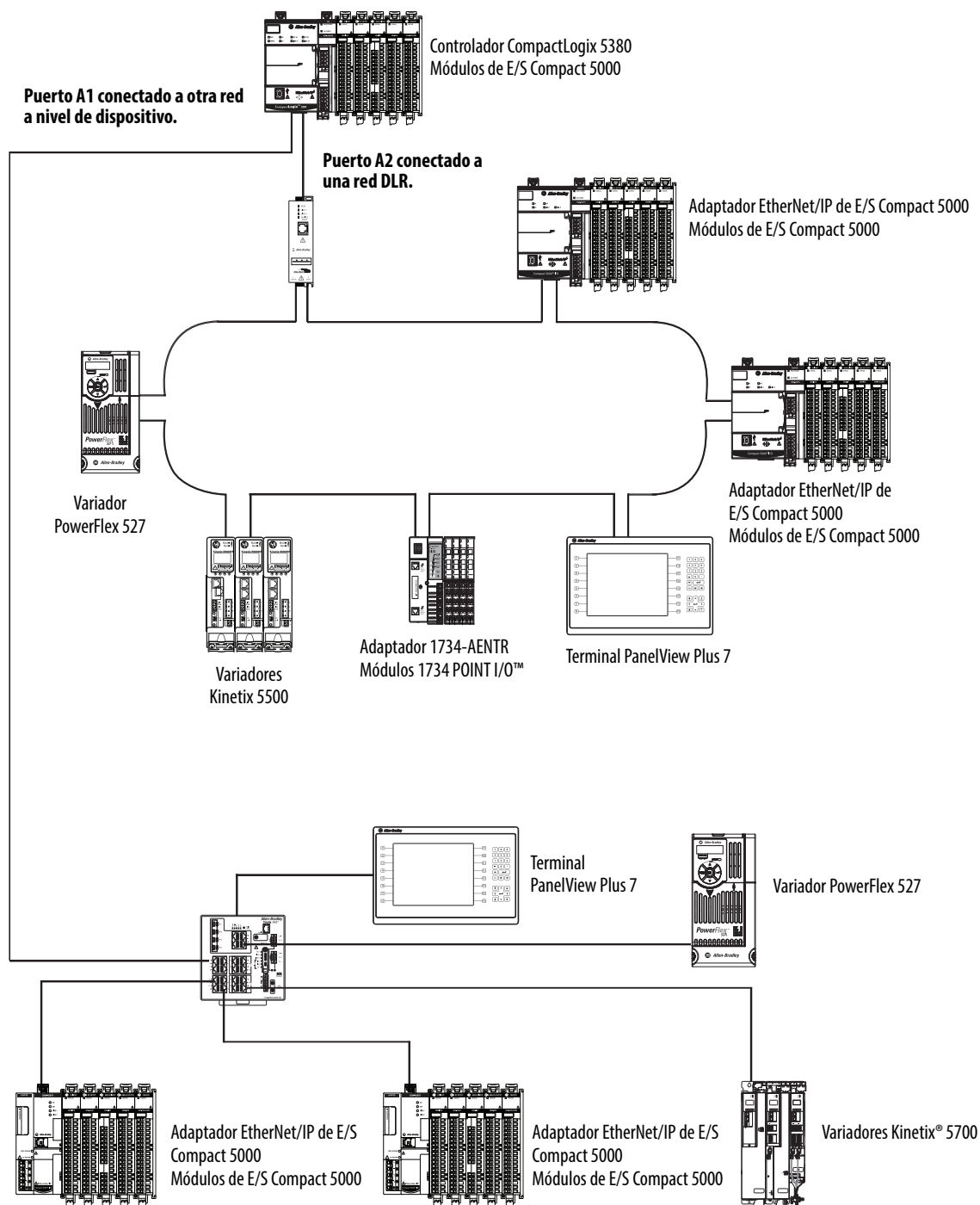
Figura 25 – Controlador CompactLogix 5380 en el modo de doble IP con conexiones de red a nivel de empresa y a nivel de dispositivo



La [Figura 26](#) muestra un controlador CompactLogix 5380 utilizando el modo de doble IP con conexiones a redes independientes a nivel de dispositivo, incluida una red DLR.

Figura 26 – Controlador CompactLogix 5380 en el modo de doble IP con conexiones de red a nivel de dispositivo únicamente

IMPORTANTE Si un controlador utiliza el modo de doble IP, puede conectarse a una topología de red DLR solo a través de una toma 1783 Ethernet, en este caso mediante el puerto A2.



Consideraciones sobre la funcionalidad del controlador en el modo de doble IP

Recuerde las siguientes funciones del controlador cuando utilice el modo de doble IP:

- El controlador no admite estas funciones:
 - Conmutación o encaminamiento TCP entre las dos redes independientes.
 - Conexión en puente CIP de conexiones de E/S (inclusive producción/consumo) entre las dos redes independientes.
- El controlador admite estas funciones:
 - Conexión en puente CIP para conexiones sin E/S como HMI, mensajería o sockets entre las dos redes independientes.
 - Conexión en puente CIP de mensajes CIP no conectados entre las dos redes independientes.

Modo lineal/DLR

Cuando los controladores funcionan en modo lineal/DLR, solo pueden conectarse a una red. Es decir, solo hay una configuración de red. Los dos puertos físicos permiten conectar el controlador a topologías de medios lineales o de anillo a nivel de dispositivos si se desea.

Tras instalar la revisión del firmware 29.011 o una posterior en un controlador, el modo EtherNet/IP se establece automáticamente en el modo de doble IP. Debe cambiar el modo EtherNet/IP para utilizar el modo lineal/DLR.

Para obtener más información sobre cómo cambiar el modo Linear/DLR del controlador, consulte [Cambio del modo EtherNet/IP en la página 158](#).

Figura 27 – Controlador CompactLogix 5380 en el modo lineal/DLR en una red DLR

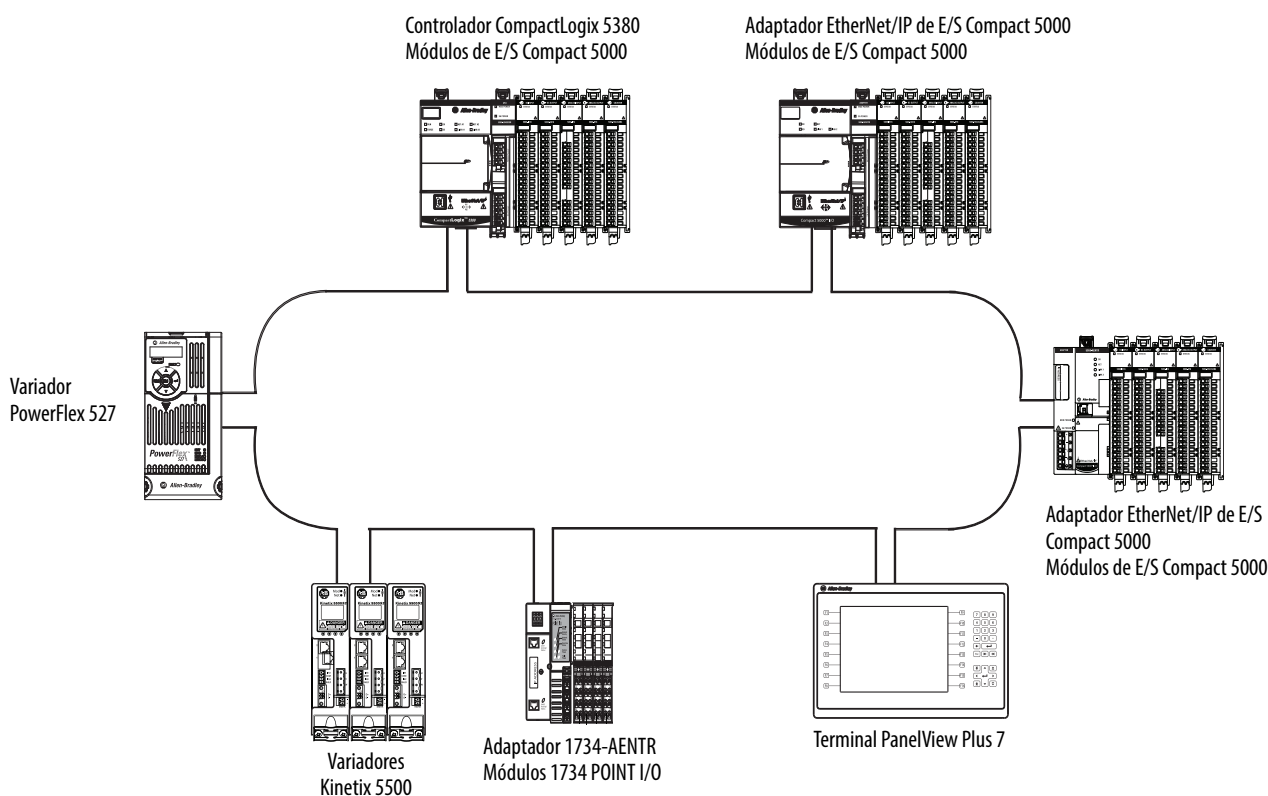


Figura 28 – Controlador Compact GuardLogix 5380 en el modo lineal/DLR en una red lineal

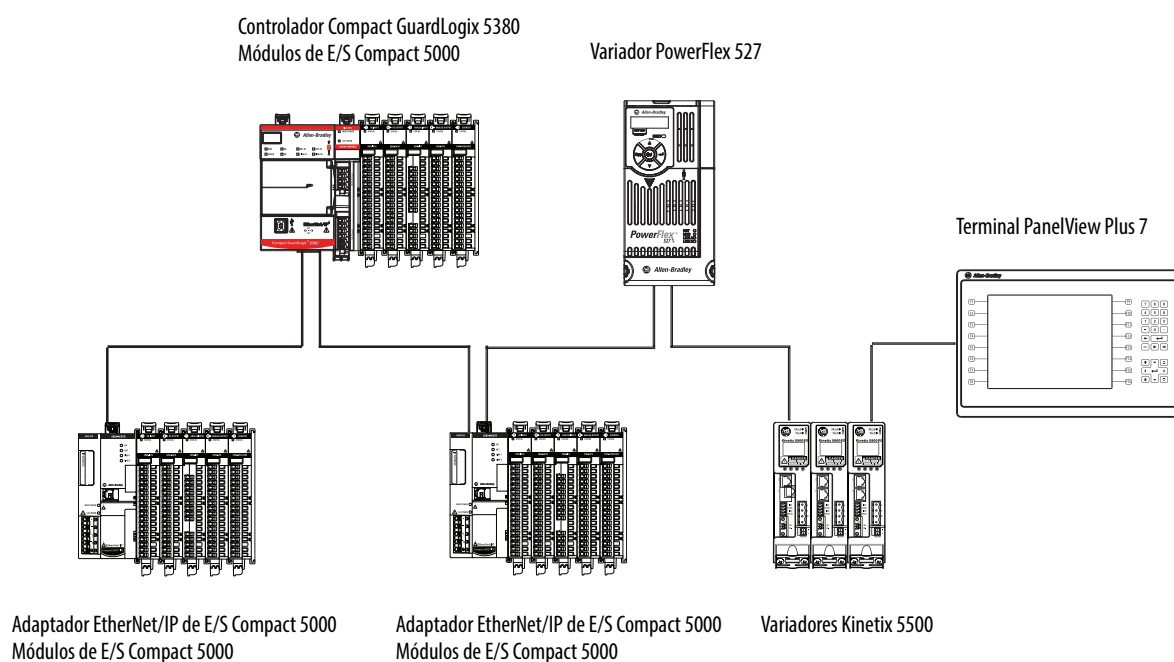
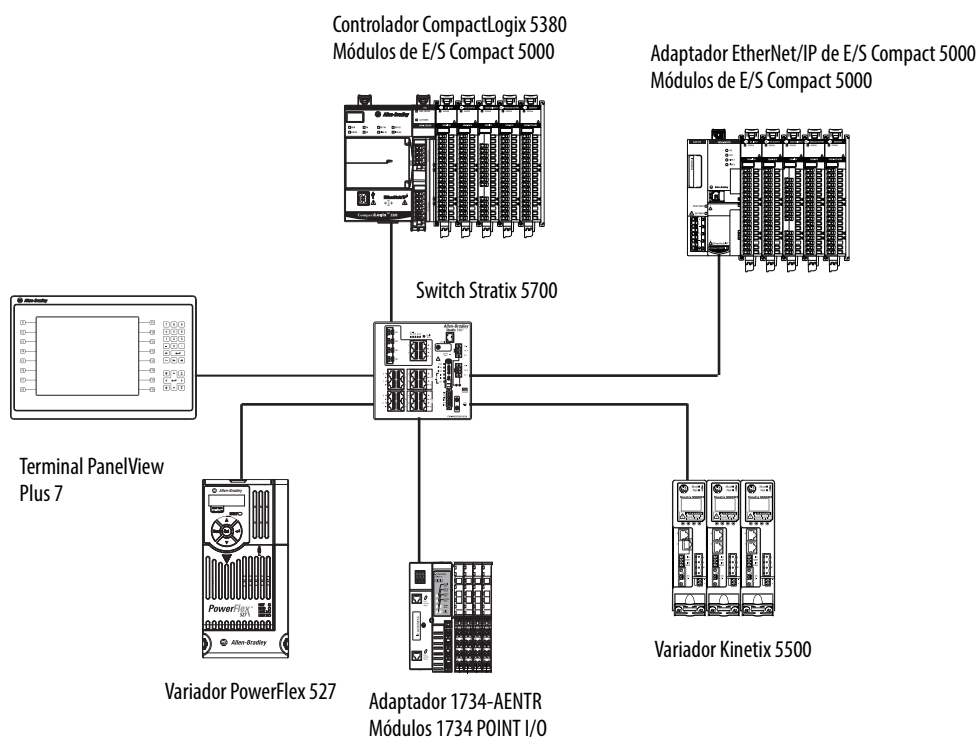
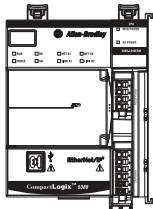


Figura 29 – Controlador CompactLogix 5380 en el modo lineal/DLR en una red en estrella

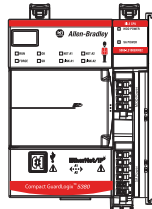


Solapamiento de rangos de direcciones IP

CompactLogix



Compact GuardLogix



IMPORTANTE El solapamiento de rangos de direcciones IP solo se aplica cuando el controlador funciona en modo de doble IP.

Si utiliza el controlador en modo lineal/DLR, puede omitir esta sección y continuar con [Modo lineal/DLR en la página 147](#).

Los valores de dirección IP y máscara de subred asignados a un puerto Ethernet establecen un rango de direcciones IP para el puerto. El valor de la máscara de subred se utiliza para establecer la parte de red de la dirección IP.

El solapamiento de los rangos de direcciones IP se produce cuando alguna dirección IP de un rango también está presente en el otro rango de direcciones IP. Cuando un controlador utiliza el modo de doble IP, las partes de red **no pueden** solaparse entre los puertos Ethernet.

Los siguientes ejemplos describen situaciones en las que los rangos de direcciones IP se solapan o no.

EJEMPLO Los rangos de direcciones IP **no se solapan**

La tabla describe las configuraciones de los puertos A1 y A2 que utilizan rangos de direcciones IP que no se solapan.

Ninguna de las direcciones IP de cualquiera de los rangos de direcciones IP de los puertos existe en el rango de direcciones IP del otro puerto.

Número de puerto	Dirección IP	Máscara de subred/máscara de red	Rango de direcciones IP (de baja a alta)
A1	192.168.1.5	255.255.255.0	192.168.1.1...192.168.1.254
A2	192.168.2.1	255.255.255.0	192.168.2.1...192.168.2.254

EJEMPLO Los rangos de direcciones IP **se solapan**

La tabla describe las configuraciones de los puertos A1 y A2 que utilizan rangos de direcciones IP que se solapan.

Todas las direcciones IP del rango de direcciones IP del puerto A2 están en el rango de direcciones IP del puerto A1.

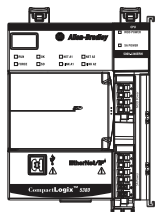
Número de puerto	Dirección IP	Máscara de subred/máscara de red	Rango de direcciones IP (de baja a alta)
A1	192.168.1.5	255.255.252.0	192.168.0.1...192.168.3.254
A2	192.168.2.1	255.255.255.0	192.168.2.1...192.168.2.254

La diferencia entre las configuraciones de puertos de los ejemplos es el valor de la máscara de subred/máscara de red para el puerto A1.

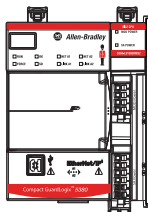
En el primer ejemplo, el valor es 255.255.255.0. En el segundo ejemplo, el valor es 255.255.252.0.

Configuración de los modos EtherNet/IP

CompactLogix



Compact GuardLogix



Puede configurar los modos EtherNet/IP de doble IP y lineal/DLR con estas aplicaciones de software:

- Aplicación Logix Designer, versión 29.00.00 y posteriores
- Software RSLinx® Classic, versión 3.81.00 y posteriores
- En el caso de la aplicación Logix Designer, versión 28.00.00, los controladores 5069-L320ER y 5069-L340ERM solo son compatibles con el modo lineal/DLR.

IMPORTANTE

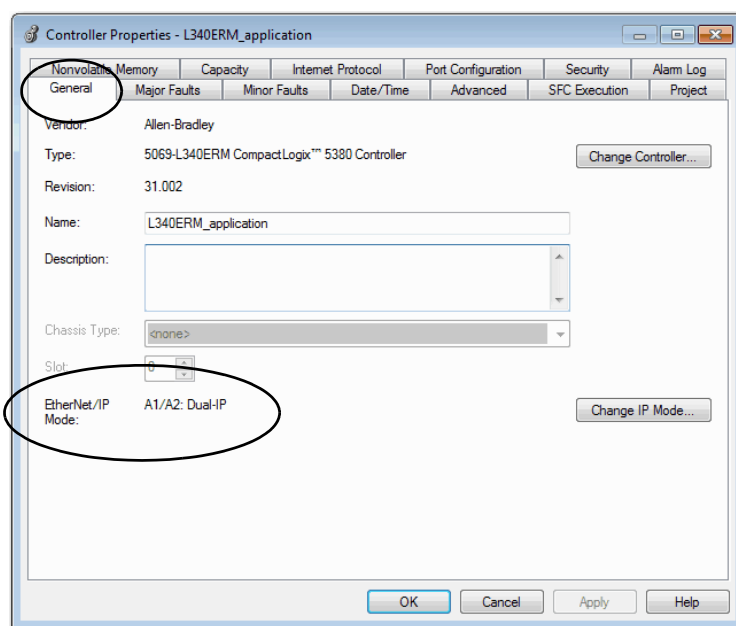
Recuerde que las versiones de software mínimas aplicables varían según el número de catálogo del controlador. Es decir, puede utilizar algunos controladores en versiones mínimas de software más bajas que otros controladores.

Para obtener información sobre cómo determinar cuáles son los requisitos de versión de software mínima para su controlador, vea [Compatibilidad entre el firmware del controlador y la aplicación Logix Designer en la página 16](#).

Las pantallas pueden variar ligeramente en el cuadro de diálogo Controller Properties para los controladores Compact GuardLogix 5380. Por ejemplo, el cuadro de diálogo Controller Properties de Compact GuardLogix 5380 incluye una ficha Safety que no existe en el cuadro de diálogo Controller Properties de CompactLogix 5380.

Configuración del modo de doble IP en la aplicación Logix Designer

En la aplicación Logix Designer, versión 29.00.00 y posteriores, el modo EtherNet/IP es el de doble IP de manera predeterminada y aparece en la ficha General del cuadro de diálogo Controller Properties.



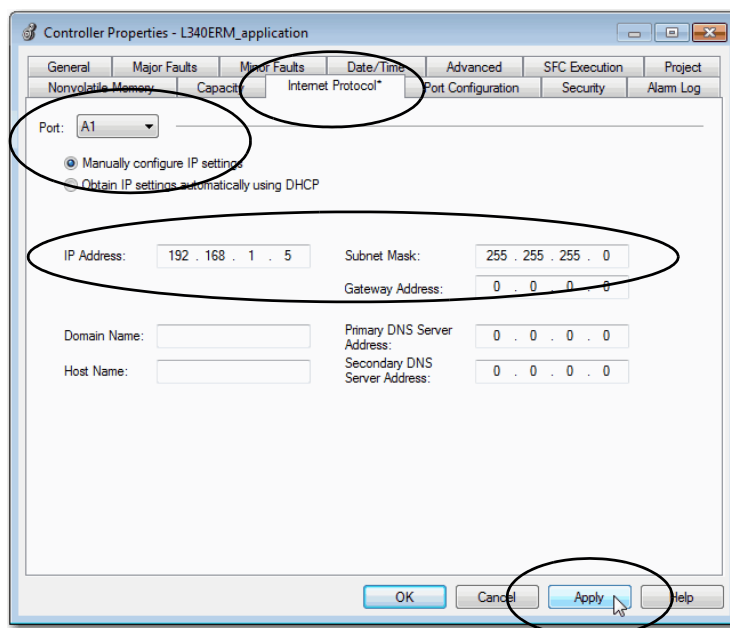
Puede establecer la dirección IP y la máscara de subred en la ficha Internet Protocol.

SUGERENCIA Al establecer la dirección IP y la máscara de subred, le recomendamos que utilice una conexión USB de la estación de trabajo al controlador.

1. Confirme que el proyecto está en línea.
2. Confirme que el controlador se encuentra en uno de estos modos:
 - Modo de programación
 - Modo de programación remota
 - Modo de marcha remota

No puede cambiar la dirección IP ni la máscara de subred si el controlador está en modo de marcha.

3. Haga clic en la ficha Internet Protocol.
4. En el menú desplegable Port, elija A1.
5. Haga clic en Manually configure IP settings.
6. Asigne los valores de dirección IP y máscara de red.
7. Haga clic en Apply.



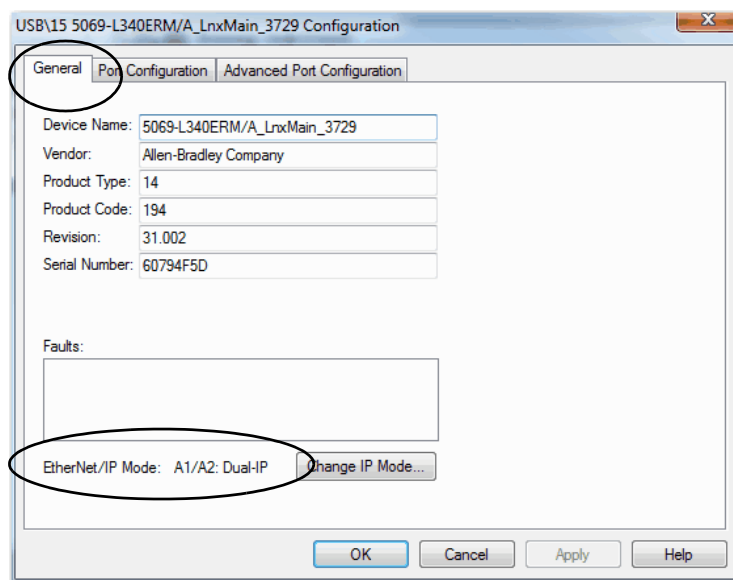
8. Repita los pasos anteriores, comenzando por el [paso 4](#)

En el [paso 4](#), debe elegir A2 en el menú desplegable Port.

Configuración del modo de doble IP en el software RSLinx Classic

En el software RSLinx Classic, el modo IP para el que se ha configurado el controlador aparece en la ficha General del cuadro de diálogo Configuration.

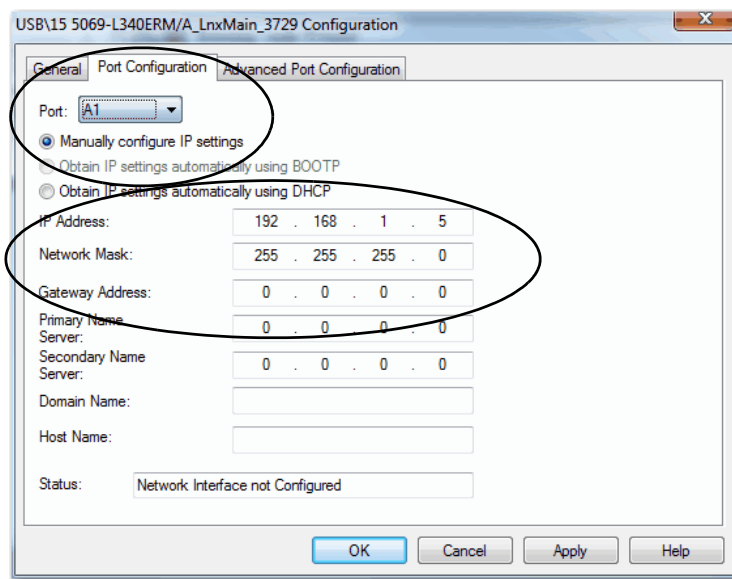
Por ejemplo, este gráfico muestra que el controlador está en el modo de doble IP.



Establezca la dirección IP y la máscara de red en la ficha Port Configuration.

SUGERENCIA Al establecer la dirección IP y la máscara de subred, le recomendamos que utilice una conexión USB de la estación de trabajo al controlador.

1. En el menú desplegable Port, elija A1.
2. Haga clic en Manually configure IP settings.
3. Asigne los valores de dirección IP y máscara de red.
4. Haga clic en Apply.



5. Repita los pasos.

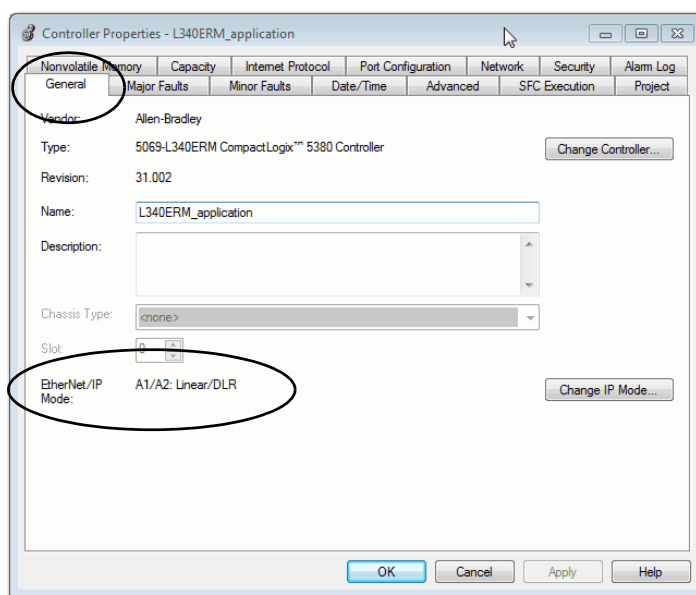
En el [paso 1](#), debe elegir A2 en el menú desplegable Port.

Configuración del modo lineal/DLR en la aplicación Logix Designer

Recuerde: Con la revisión del firmware 29.011 y posteriores, el modo EtherNet/IP es el de doble IP de manera predeterminada. Debe cambiar el modo para utilizar el modo lineal/DLR.

IMPORTANTE Para obtener más información sobre cómo cambiar el modo EtherNet/IP del controlador, consulte [Cambio del modo EtherNet/IP en la página 158](#).

Tras cambiar del modo EtherNet/IP al modo lineal/DLR, aparece una nueva opción de modo en la ficha General del cuadro de diálogo Controller Properties.

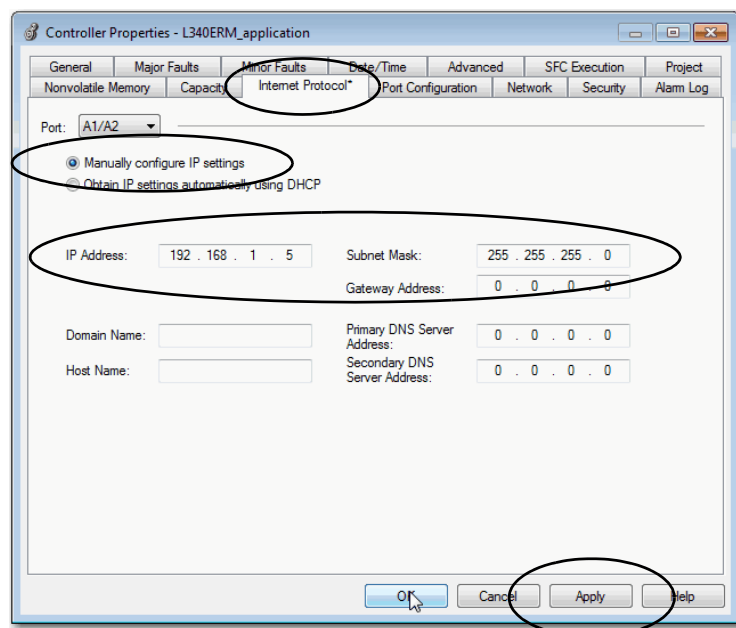


Puede establecer la dirección IP y la máscara de subred en la ficha Internet Protocol.

1. Confirme que el proyecto está en línea y el controlador está en modo de programación, modo de programación remota o modo de marcha remota.

No puede cambiar la dirección IP ni la máscara de subred si el controlador está en modo de marcha.

2. Haga clic en la ficha Internet Protocol.
3. Haga clic en Manually configure IP settings.
4. Asigne los valores de dirección IP y máscara de red.
5. Haga clic en Apply.

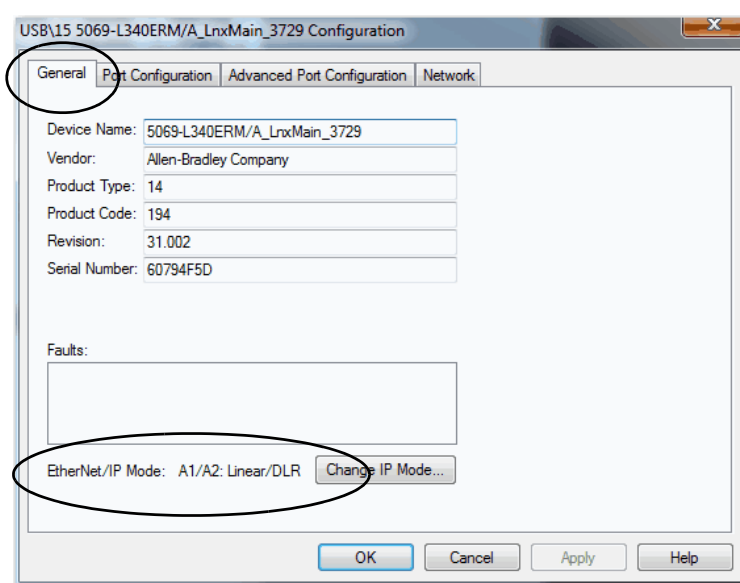


Configuración del modo lineal/DLR en el software RSLinx Classic

Recuerde: Con la revisión del firmware 29.011 y posteriores, el modo EtherNet/IP es el de doble IP de manera predeterminada. Debe cambiar el modo para utilizar el modo lineal/DLR.

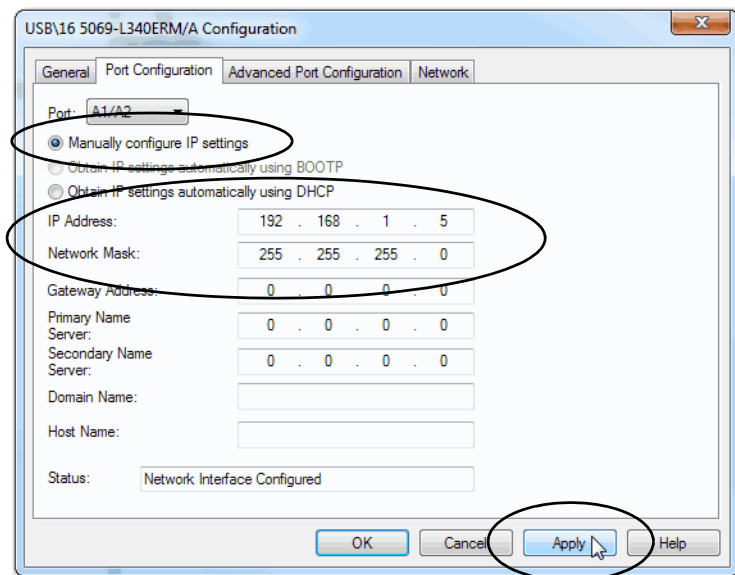
IMPORTANTE Para obtener más información sobre cómo cambiar el modo EtherNet/IP del controlador, consulte [Cambio del modo EtherNet/IP en la página 158](#).

La nueva opción de modo aparece en la ficha General del cuadro de diálogo Controller Properties.



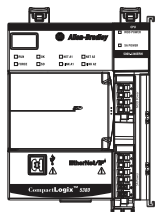
Puede establecer la dirección IP y la máscara de subred en la ficha Internet Protocol.

1. Confirme que el proyecto está en línea.
2. Haga clic en la ficha Port Configuration.
3. Haga clic en Manually configure IP settings.
4. Asigne los valores de dirección IP y máscara de red.
5. Haga clic en Apply.

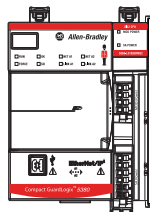


Cambio del modo EtherNet/IP

CompactLogix



Compact GuardLogix



Puede cambiar el modo EtherNet/IP en la aplicación Logix Designer o en el software RSLinx Classic.

IMPORTANTE Recuerde lo siguiente:

- Tenga cuidado al cambiar el modo EtherNet/IP del controlador y considere los posibles efectos del cambio.
- No puede cambiar el modo del controlador EtherNet/IP de doble IP a lineal/DLR cuando esté conectado a través del puerto A1. Debe estar conectado al controlador a través del puerto A2 para cambiar del modo doble IP al modo lineal/DLR.

Los efectos del cambio del modo EtherNet/IP dependen del modo al que se cambie. Asegúrese de que está consciente de ellos antes de cambiar el modo EtherNet/IP.

Tabla 12 – Efecto del cambio del modo EtherNet/IP

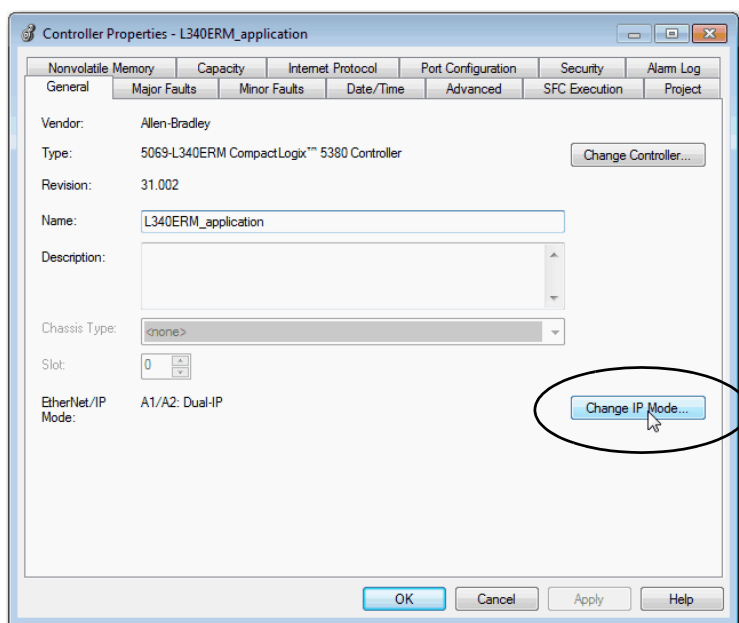
Cambio del modo EtherNet/IP	Efectos
Modo de doble IP a modo lineal/DLR	<ul style="list-style-type: none"> • La dirección IP, la máscara de red y los ajustes predeterminados de gateway del puerto A2 se aplican al puerto A1/A2. • La dirección MAC del puerto A1 se aplica al puerto A1/A2. Este escenario puede darse si se actualiza el firmware del controlador a la revisión 29.011 o una posterior antes de establecer una dirección IP. • Los intentos de cambiar del modo de doble IP al modo lineal/DLR solo tendrán éxito si la sección de configuración de E/S de como mínimo un puerto no contiene módulos. <p>Si las secciones de configuración de E/S de ambos puertos incluyen módulos, no podrá cambiar el modo EtherNet/IP del modo de doble IP al modo lineal/DLR.</p>
Modo lineal/DLR a modo de doble IP	<ul style="list-style-type: none"> • La dirección IP, la máscara de red y los ajustes predeterminados de gateway del puerto A1/A2 se aplican al puerto A2. • Otros ajustes del puerto A1/A2, como por ejemplo, los servidores DNS y el nombre de dominio, se pierden. • La dirección MAC del puerto A1/A2 se aplica al puerto A1. Se aplica una dirección MAC separada al puerto A2. • El puerto A1 está habilitado para DHCP. • La sección de configuración de E/S del proyecto de la aplicación Logix Designer se asigna automáticamente al puerto A1. <p>Puede cambiar la configuración de E/S en el proyecto de la aplicación Logix Designer para asignarlo al puerto A2.</p>

Cambio del modo EtherNet/IP en la aplicación Logix Designer

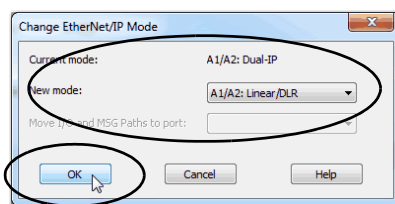
IMPORTANTE Este ejemplo muestra un cambio del modo EtherNet/IP del modo de doble IP al modo lineal/DLR. Las mismas tareas se aplican al cambiar del modo lineal/DLR al modo de doble IP.

Para cambiar el modo EtherNet/IP en la aplicación Logix Designer, siga estos pasos.

1. Confirme que el proyecto está fuera de línea.
2. En la ficha General del cuadro de diálogo Controller Properties, haga clic en Change IP Mode.



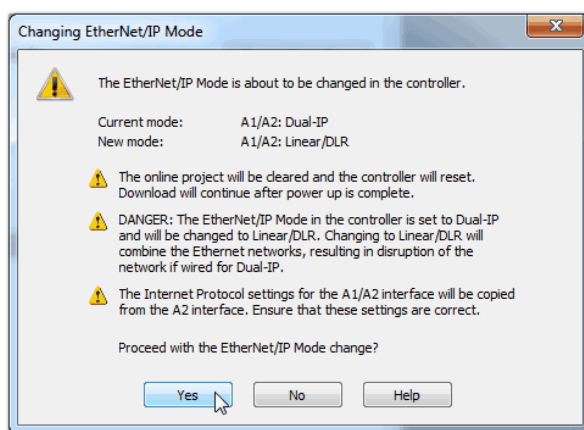
3. En el menú desplegable New mode, elija el nuevo modo y haga clic en OK.



4. Haga clic en OK en el cuadro de diálogo Controller Properties.
5. Guarde el proyecto.
6. Descargue el proyecto actualizado al controlador.
7. Cuando aparezca la siguiente advertencia, léala atentamente.

IMPORTANTE Antes de cambiar el modo EtherNet/IP, asegúrese de que comprende el impacto que tendrá sobre el controlador el cambio de modo.

Para obtener más información sobre los efectos del cambio del modo EtherNet/IP, consulte la [Tabla 12 en la página 158](#).



8. Haga clic en Yes para continuar.

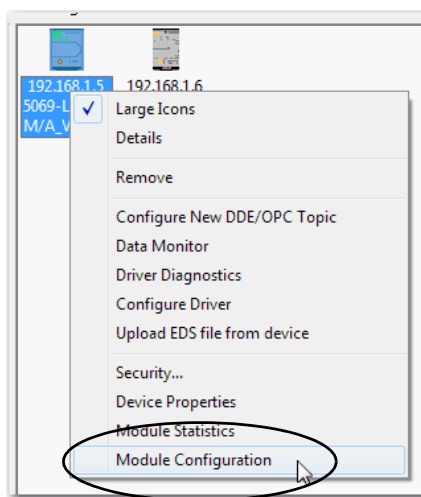
Cambio del modo EtherNet/IP en el software RSLinx Classic

Para cambiar el modo EtherNet/IP en el software RSLinx Classic, siga estos pasos.

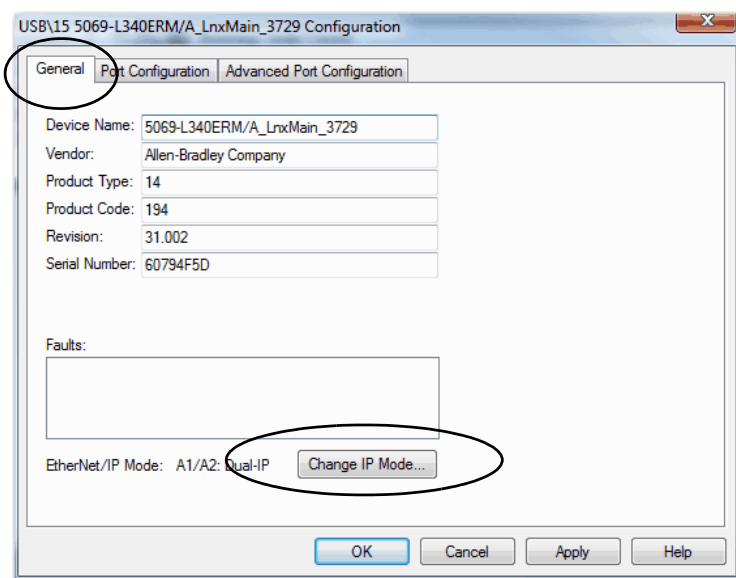
1. Confirme que el controlador está en línea y no hay ningún proyecto en el controlador.
2. Confirme que el controlador se encuentra en uno de estos modos:
 - Modo de programación
 - Modo de programación remota
 - Modo de marcha remota

No puede cambiar la dirección IP ni la máscara de subred si el controlador está en modo de marcha.

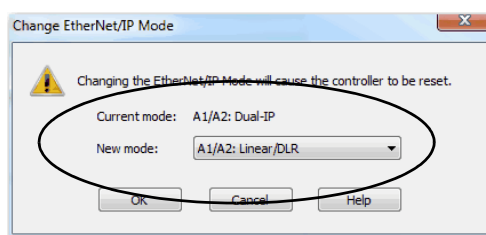
3. Haga clic con el botón derecho del mouse en el controlador y seleccione Module Configuration.



4. En la ficha General del cuadro de diálogo Configuration, haga clic en Change IP Mode.



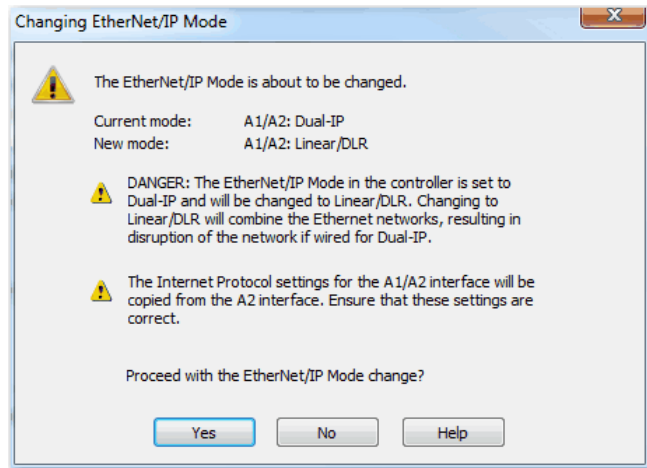
5. En el menú desplegable New mode elija el nuevo modo y haga clic en OK.



6. Cuando aparezca la siguiente advertencia, léala atentamente.

IMPORTANTE Antes de cambiar el modo EtherNet/IP, asegúrese de que comprende el impacto que tendrá sobre el controlador el cambio de modo.

Para obtener más información sobre los efectos del cambio del modo EtherNet/IP, consulte la [Tabla 12 en la página 158](#).



7. Haga clic en Yes para continuar.

Solicitudes DNS

Para calificar la dirección de un módulo, utilice el direccionamiento DNS para especificar el nombre de anfitrión para un módulo, lo cual también implica especificar un nombre de dominio y servidores DNS. El direccionamiento DNS hace posible configurar estructuras de red similares y secuencias de direcciones IP en dominios diferentes.

El direccionamiento DNS solo es necesario si hace referencia al módulo mediante el nombre de anfitrión, como en las descripciones de rutas de las instrucciones MSG.

IMPORTANTE Consideraciones de seguridad

Para obtener información sobre el direccionamiento DNS para los controladores Compact GuardLogix 5380, vea la [Tabla 5](#) – Parámetros de la red EtherNet/IP para el direccionamiento DNS en la [página 66](#).

Para obtener más información sobre el direccionamiento DNS, consulte el documento EtherNet/IP Network Configuration User Manual, publicación [ENET-UM001](#).

Encaminamiento de solicitudes DNS

Las solicitudes DNS se pueden generar desde el puerto A1 o el puerto A2.

Solicitud DNS generada desde el puerto A1

- Si la dirección del servidor DNS se encuentra en la subred local del puerto A1, las solicitudes DNS partirán del puerto A1.
- Si el puerto A2 está habilitado y la dirección del servidor DNS se encuentra en la subred local del puerto A2, las solicitudes DNS partirán del puerto A2.
- Si la dirección del servidor DNS está fuera de todas las subredes locales, las solicitudes DNS partirán del puerto A1 hacia la gateway predeterminada del puerto A1.

Solicitud DNS generada desde el puerto A2

- Si el puerto A1 está habilitado y la dirección del servidor DNS se encuentra en la subred local del puerto A1, las solicitudes DNS partirán del puerto A1.
- Si la dirección del servidor DNS se encuentra en la subred local del puerto A2, las solicitudes DNS partirán del puerto A2.
- Si el puerto A1 está habilitado y la dirección del servidor DNS está fuera de todas las subredes locales, las solicitudes DNS partirán del puerto A1 hacia la gateway predeterminada del puerto A1.
- Si el puerto A1 está inhabilitado y la dirección del servidor DNS está fuera de todas las subredes locales, las solicitudes DNS partirán del puerto A2 hacia la gateway predeterminada del puerto A2.

Servidor SMTP

El servidor SMTP solo está disponible a través del puerto de empresa. Por lo tanto, los correos electrónicos solo se pueden enviar a través del puerto de empresa.

Para obtener más información sobre cómo enviar correos electrónicos a través de un puerto Ethernet, consulte el documento EtherNet/IP Network Configuration User Manual, publicación [ENET-UM001](#).

Uso de objetos de socket

Cuando el controlador funciona en modo de doble IP y utiliza un objeto de socket, puede utilizar una dirección IP con un tipo de servicio Socket_Create. De manera predeterminada, esta dirección IP es INADDR_ANY.

Recuerde lo siguiente:

- Si utiliza INADDR_ANY, la comunicación IP que inicie la instancia del objeto de socket seguirá las mismas reglas de encaminamiento que las reglas de encaminamiento de solicitudes DNS descritas en [Encaminamiento de solicitudes DNS en la página 164](#).
- Si utiliza la dirección IP del puerto A1 en lugar de INADDR_ANY, los paquetes IP solo pueden ir a la subred del puerto A1 o a través de su gateway predeterminada.
- Si utiliza la dirección IP del puerto A2 en lugar de INADDR_ANY, los paquetes IP solo pueden ir a la subred del puerto A2 o a través de su gateway predeterminada.
- Si utiliza una dirección IP diferente de las direcciones IP de los puertos A1 o A2 o INADDR_ANY, se rechazará la solicitud Create_Socket_Service.

Instrucciones de envío de mensajes

Puede enviar instrucciones Message (MSG) a través del puerto de empresa o a través del puerto a nivel de dispositivo. La única diferencia entre las configuraciones de la instrucción MSG es la ruta.

Al configurar una instrucción MSG en un controlador que funciona en modo de doble IP, utilice estas rutas:

- Puerto de empresa (puerto A1) – 3
- Puerto a nivel de dispositivo (puerto A2) – 4

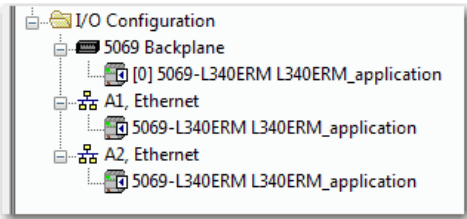
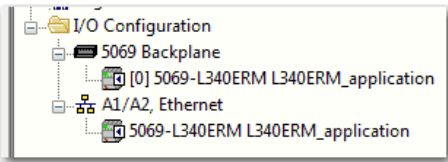
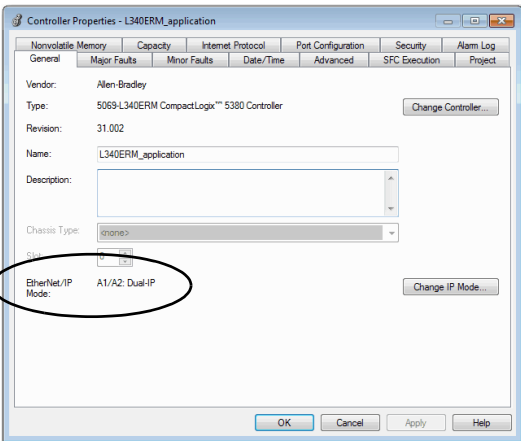
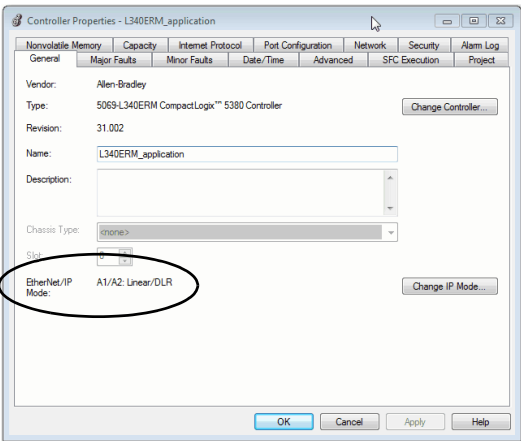
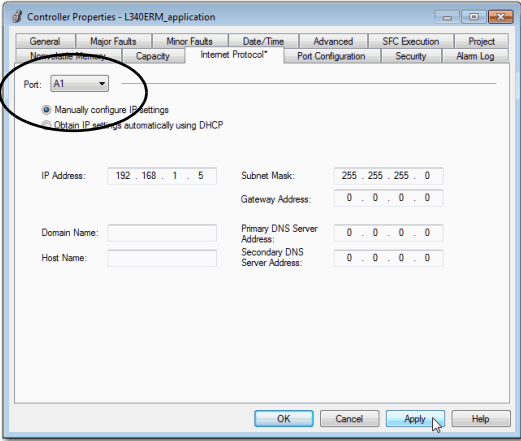
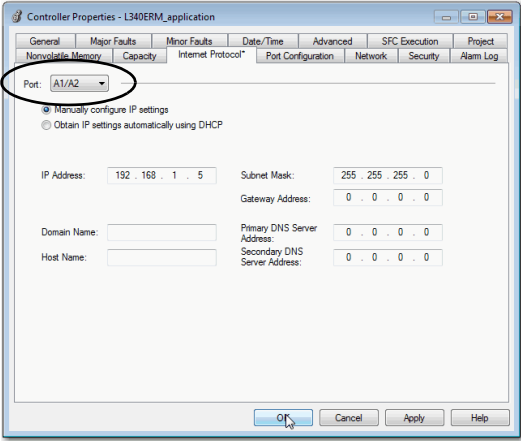
Si el controlador funciona en el modo lineal/DLR, la ruta es 2.

Para obtener más información sobre cómo utilizar las instrucciones MSG, consulte el documento Instrucciones generales de los controladores Logix 5000 – Manual de referencia, publicación [1756-RM003](#).

Diferencias de visualización del software para los modos EtherNet/IP

La [Tabla 13](#) muestra las diferencias en la aplicación Logix Designer cuando el controlador utiliza el modo de doble IP o el modo lineal/DLR.

Tabla 13 – Diferencias de visualización del modo EtherNet/IP en la aplicación Logix Designer

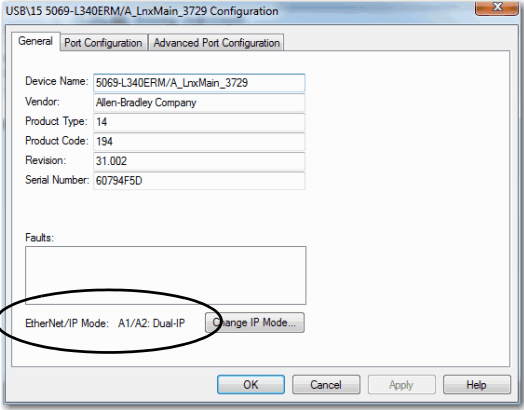
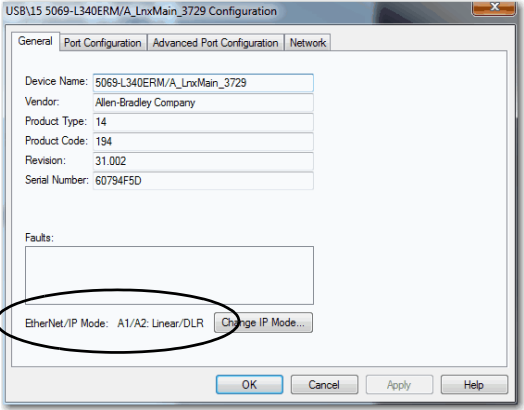
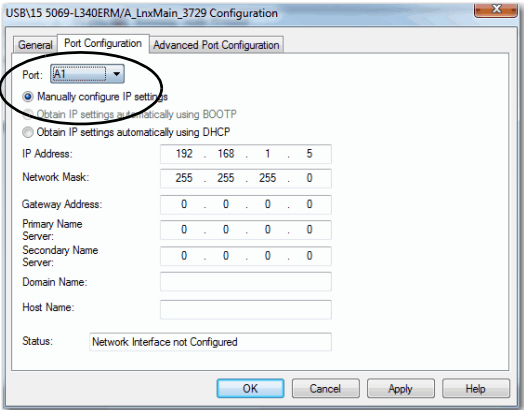
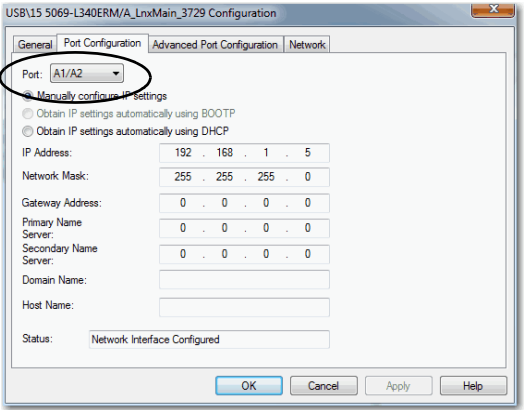
Modo EtherNet/IP		
Sección de la aplicación	Modo de doble IP	Modo lineal/DLR
Árbol de configuración de E/S en Controller Organizer		
Ficha General en el cuadro de diálogo Controller Properties		
Internet Protocol en el cuadro de diálogo Controller Properties		

Si conecta el puerto A1 a una red a nivel de dispositivo, algunos parámetros aparecen como configurables, pero no se usan. Para obtener más información sobre qué parámetros configura para conectar un puerto a una red a nivel de dispositivo, vea [Red a nivel de dispositivo en la página 143](#).

El cuadro de diálogo Controller Properties también proporciona una ficha Network en la aplicación Logix Designer cuando el controlador utiliza el modo lineal/DLR. La ficha Network no está disponible cuando el controlador utiliza el modo de doble IP.

La [Tabla 14](#) muestra las diferencias en el software RSLinx Classic cuando el controlador utiliza el modo de doble IP o el modo lineal/DLR.

Tabla 14 – Diferencias de visualización del modo EtherNet/IP en el software RSLinx Classic

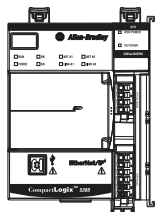
Modo EtherNet/IP		
Sección del software	Modo de doble IP	Modo lineal/DLR
Ficha General		
Ficha Port Configuration		
Si conecta el puerto A1 a una red a nivel de dispositivo, algunos parámetros aparecen como configurables, pero no se usan. Para obtener más información sobre qué parámetros configura para conectar un puerto a una red a nivel de dispositivo, vea Red a nivel de dispositivo en la página 143 .		

El cuadro de diálogo Configuration también proporciona una ficha Network en el software RSLinx Classic cuando el controlador utiliza el modo lineal/DLR. La ficha Network no está disponible cuando el controlador utiliza el modo de doble IP.

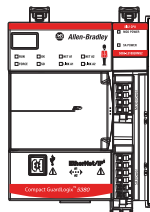
Dirección IP del controlador y actualizaciones del firmware

A fin de funcionar correctamente, los controladores CompactLogix 5380 y Compact GuardLogix 5380 requieren una dirección IP y la revisión de firmware compatible con la versión de Studio 500 Logix Designer que utiliza.

CompactLogix



Compact GuardLogix



IMPORTANTE

Esta sección no se aplica a los controladores Compact GuardLogix 5380 puesto que debe utilizar la revisión de firmware 31.011 y posteriores con dichos controladores.

Las condiciones descritas existen con controladores que utilizan las revisiones de firmware anteriores a la 31.011.

Debe tener en cuenta lo siguiente antes de establecer la dirección IP y actualizar el firmware del controlador:

- Estado del controlador antes de realizar cambios
- Revisión del firmware a la que va a actualizar el controlador
- Orden en el que establece la dirección IP y se actualiza la revisión del firmware

Estado del controlador antes de realizar cambios	Descripción	Revisión de firmware de actualización/cambio	Orden de finalización de las tareas	Resultado al finalizar las tareas en el orden indicado
Condición original	<ul style="list-style-type: none"> • Ninguna dirección IP establecida • Se utilizan direcciones MAC únicas para el puerto A1 y el puerto A2, respectivamente • Cada puerto en el controlador está habilitado para DHCP • Revisión de firmware 1.xxx 	Revisión 29.011 y posteriores	<ol style="list-style-type: none"> 1. Cambie el modo EtherNet/IP del modo de doble IP al modo lineal/DLR. Para obtener más información, consulte Cambio del modo EtherNet/IP en la página 158. 2. Establezca la dirección IP en el puerto A1/A2. 3. Instale el firmware del controlador. 	<ul style="list-style-type: none"> • El modo EtherNet/IP del controlador se establece automáticamente en el modo de doble IP. • La dirección IP, la máscara de red y los ajustes predeterminados de gateway del puerto A1/A2 se aplican al puerto A2. Otros ajustes del puerto A1/A2, como por ejemplo, los servidores DNS y el nombre de dominio, se pierden. • La dirección MAC del puerto A1/A2 se aplica al puerto A1 y una dirección MAC separada se aplica al puerto A2. • Debe establecer la configuración de la dirección IP
			<ol style="list-style-type: none"> 1. Instale el firmware del controlador. 2. Establezca las direcciones IP de los puertos A1 y A2. 	<ul style="list-style-type: none"> • El modo EtherNet/IP del controlador continúa establecido en el modo de doble IP tras instalar el firmware. El modo EtherNet/IP del controlador está establecido en el modo de doble IP cuando se encuentra en su condición original. • Se asigna una dirección MAC única a cada puerto del controlador. • Debe establecer la dirección IP y los parámetros relacionados para el puerto A1 (puerto de empresa) y el puerto A2 (puerto a nivel de dispositivo).
	<ul style="list-style-type: none"> • No se establece ninguna dirección IP • Se utiliza una dirección MAC para el puerto A1/A2 • El puerto A1/A2 está habilitado para DHCP • Revisión de firmware 1.xxx 	Revisión 28.xxx IMPORTANTE: Solo los controladores 5069-L320ER y 5069-L340ERM admiten la revisión 28.xxx.	<ol style="list-style-type: none"> 1. Establezca la dirección IP en el puerto A1/A2. 2. Instale el firmware del controlador. 	<ul style="list-style-type: none"> • El modo EtherNet/IP del controlador se establece automáticamente en el modo lineal/DLR. • Los ajustes de dirección IP del puerto A1/A2 se mantienen iguales.
			<ol style="list-style-type: none"> 1. Instale el firmware del controlador. 2. Establezca la dirección IP en el puerto A1/A2. 	

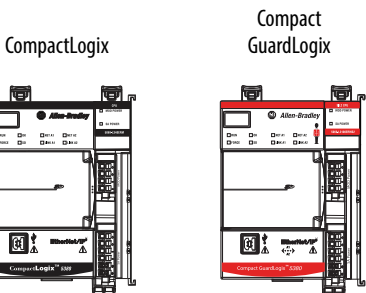
Estado del controlador antes de realizar cambios	Descripción	Revisión de firmware de actualización/cambio	Orden de finalización de las tareas	Resultado al finalizar las tareas en el orden indicado
Funcionamiento	<ul style="list-style-type: none"> Dirección IP establecida en el puerto A1/A2 Se ha instalado la revisión de firmware 28.xxx 	Revisión 29.011 y posteriores	Actualice el firmware del controlador	<ul style="list-style-type: none"> El modo EtherNet/IP cambia al modo de doble IP. La dirección IP, la máscara de red y los ajustes predeterminados de gateway del puerto A1/A2 se aplican al puerto A2. Otros ajustes del puerto A1/A2, como por ejemplo, los servidores DNS y el nombre de dominio, se pierden. La dirección MAC del puerto A1/A2 se aplica al puerto A1. Se aplica una dirección MAC separada al puerto A2. La sección de configuración de E/S del proyecto de la aplicación Logix Designer se asigna automáticamente al puerto A1. Puede cambiar la configuración de E/S en el proyecto de la aplicación Logix Designer para asignarlo al puerto A2. Si es necesario, puede cambiar al modo DLR/lineal tras actualizar la revisión del firmware. Para obtener más información, consulte Cambio del modo EtherNet/IP en la página 158.
	<ul style="list-style-type: none"> El controlador funciona en modo lineal/DLR Dirección IP establecida en el puerto A1/A2 Está instalada la revisión de firmware 29.011 o una posterior 	Realice una actualización retrógrada a la revisión 28.xxx IMPORTANTE: Solo puede realizar esta descarga en los controladores 5069-L320ER y 5069-L340ERM.	Realice una actualización retrógrada del firmware del controlador	<ul style="list-style-type: none"> El modo EtherNet/IP permanece en modo lineal/DLR Los ajustes de dirección IP se mantienen iguales
	<ul style="list-style-type: none"> El controlador funciona en modo de doble IP Las direcciones IP se establecen en los puertos A1 y A2 Está instalada la revisión de firmware 29.011 o una posterior 		Realice una actualización retrógrada del firmware del controlador	<ul style="list-style-type: none"> El modo EtherNet/IP cambia automáticamente del modo de doble IP al modo lineal/DLR Tras realizar el cambio, la configuración del Internet Protocol del puerto A2 se aplica al puerto A1/A2.

Notas:

Administración de comunicaciones del controlador

Tema	Página
Descripción general de la conexión	171
Interacción de comunicación del controlador con datos de control	172
Producción y consumo de datos (de enclavamiento)	173
Envío y recepción de mensajes	175

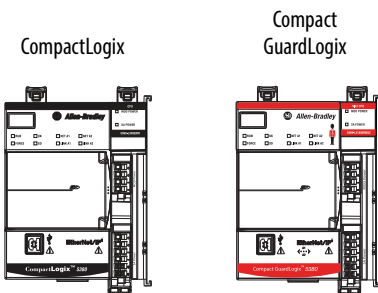
Descripción general de la conexión



Las conexiones se utilizan cuando el sistema cumple estas condiciones:

- Hay módulos de E/S, módulos de comunicación y adaptadores presentes en la configuración de E/S del proyecto del usuario.
- Los tags producidos o consumidos se han configurado en el proyecto del usuario.
- Se ejecutan mensajes conectados en la aplicación del usuario.
- Los dispositivos externos, terminales de programación o terminales HMI se comunican con el controlador.

Interacción de comunicación del controlador con datos de control



El controlador ejecuta la tarea de comunicaciones independientemente del código de la aplicación. El controlador ejecuta las comunicaciones de forma asíncrona con respecto a la aplicación. Por lo tanto, es importante asegurarse de que las comunicaciones que se entregan al controlador estén completas antes de que la aplicación actúe según los nuevos datos que le han entregado. Esto se aplica tanto a los datos que recibe el controlador como a los que envía el controlador.

Por ejemplo, si un dispositivo HMI escribe un bloque grande de datos de recetas en el controlador, el código de la aplicación puede comenzar a actuar según esos datos antes de que se escriban los datos. Esta acción hace que en el espacio de la aplicación esté la mitad de la receta actual y la mitad de la última receta.

Tradicionalmente, los programadores han utilizado lo siguiente para controlar los efectos de las comunicaciones asíncronas:

- Pares UID/UIE
- Transferencia de datos con instrucciones CPS.

Estas opciones dependen del controlador cuando el núcleo principal puede cambiar de tarea. Por lo tanto, la tarea de comunicación no puede cambiar los datos mientras la tarea de control los está utilizando. Dado que el controlador procesa las comunicaciones en un núcleo de CPU independiente, estos métodos ya no son efectivos en todos los casos.

La [Tabla 15](#) indica el comportamiento del controlador.

Tabla 15 – Comportamiento del controlador CompactLogix 5380 y Compact GuardLogix 5380

Construcción de la aplicación	Acceso a tag					
	HMI	MSG	Actualización de E/S	Producir/consumir	Otras tareas del usuario	Planificador de movimiento
UID/UIE	Permite	Permite	Permite	Permite	Bloquea	Permite
CPS	Bloquea	Bloquea	Bloquea	Bloquea	Permite	Permite

Bloquea: Ayuda a impedir que las comunicaciones cambien los valores de los datos de origen durante la ejecución de la aplicación.
 Permite: Las comunicaciones pueden cambiar los valores de los datos de origen durante la ejecución de la aplicación.

Dado que los controladores tienen integridad de datos de 32 bits, esto solo se aplica a estructuras de datos de más de 32 bits. Si la integridad a nivel de palabra es su principal preocupación, la integridad de los datos de 32 bits no afecta su uso de los datos.

Las prácticas recomendadas de programación establecen que deben emplearse dos palabras únicas al principio y al final de los datos. El controlador valida estas palabras para verificar que toda la estructura mantiene la integridad de los datos. Le recomendamos cambiar los datos de handshake y que el código de la aplicación los valide en cada transacción antes de que el código de la aplicación del controlador o el sistema de nivel superior que lee los datos del controlador actúe con base a ellos.

La [Tabla 16](#) muestra dos elementos de datos que se añaden a una estructura para comprobar la integridad de los datos. Es decir, se añaden los datos de inicio y los datos de fin. Le recomendamos que el controlador valide la coincidencia del valor de los datos de inicio y del valor de los datos de fin antes de que el controlador actúe sobre My_Recipe1.

Si los valores de los datos de inicio y de los datos de fin no coinciden, es probable que la comunicación esté todavía rellenando la estructura. Lo mismo puede aplicarse a los sistemas de nivel superior que reciben los datos del controlador.

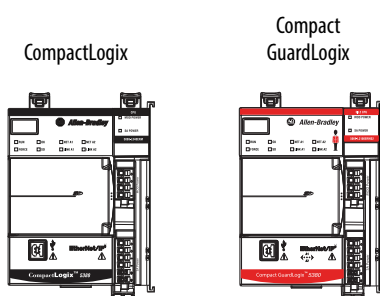
Tabla 16 – Elementos de datos

Estructura	My_Recipe1	My_Recipe2	My_Recipe3
Datos de inicio	101	102	103
Azúcar	3	4	8
Harina	4	3	9
Chocolate	2	2	4
Aceite	6	7	2
Datos de fin	101	102	103

SUGERENCIA

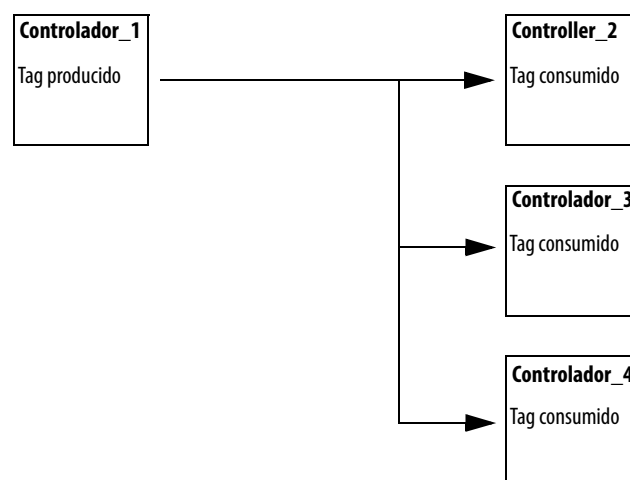
Le recomendamos que lleve a cabo esta prueba en una copia almacenada en búfer de los datos y no en el elemento de datos real en el que el núcleo de comunicación escribe. Si utiliza datos almacenados en búfer, evitará el riesgo de que el núcleo de comunicación cambie los datos después de que se haya superado la prueba de validez de los datos.

Producción y consumo de datos (de enclavamiento)



Los controladores le permiten producir (transmitir) y consumir (recibir) tags bajo el control del controlador. Los controladores CompactLogix™ 5380 y Compact GuardLogix® 5380 producen el mismo tag estándar a través de los puertos Ethernet y el backplane, y los conteos de consumidores se aplican al total de consumidores provenientes de todos los puertos.

Figura 30 – Ejemplo de tags producidos y consumidos



La [Tabla 17](#) describe los tags compartidos por el sistema.

Tabla 17 – Descripciones de los tags producidos y consumidos

Tag	Descripción
Tag producido	Tag que un controlador pone a disposición para que otros controladores lo utilicen. Varios controladores pueden consumir (recibir) simultáneamente los datos. Un tag producido envía sus datos a uno o más tags consumidos (consumidores) sin utilizar lógica.
Tag consumido	Tag que recibe los datos de un tag producido. El tipo de datos del tag consumido debe coincidir con el tipo de datos (incluida cualquier dimensión de la matriz) del tag producido. El RPI del tag consumido determina el período de actualización de los datos.

Para que dos controladores compartan tags producidos o consumidos, estos controladores deben estar conectados a la misma red. No se pueden conectar en puente tags producidos y consumidos a través de dos redes.

Los tags producidos y consumidos usan las conexiones del controlador y los módulos de comunicación empleados.

Los controladores Compact GuardLogix 5380 también pueden utilizar tags de seguridad producidos y consumidos. Para obtener más información sobre cómo utilizarlos, vea [Tags de seguridad producidos/consumidos en la página 247](#).

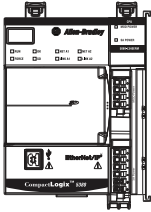
Intervalo solicitado entre paquetes (RPI) de tags de multidifusión

El primer consumidor de un tag producido que use multidifusión en cualquier puerto de comunicaciones establece el valor de RPI correspondiente a dicho puerto. Todos los consumidores subsiguientes que utilicen el mismo puerto deben solicitar el mismo valor de RPI que el primer consumidor; de otra manera, no lograrán conectarse. Los controladores con backplane y puertos de EtherNet pueden producir datos en un valor de RPI independiente en cada puerto.

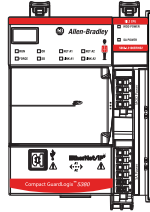
Para obtener más información acerca de los tags producidos/consumidos, consulte el documento Logix 5000 Controllers Produced and Consumed Tags Programming Manual, publicación [1756-PM011](#).

Envío y recepción de mensajes

CompactLogix



Compact GuardLogix



Los mensajes transfieren datos a otros dispositivos, como por ejemplo, a otros controladores o interfaces de operador. La instrucción MSG es una instrucción de salida de un diagrama de lógica de escalera que realiza de manera asíncrona una lectura o escritura de un bloque de datos en otro módulo a través del backplane o una red. El tamaño de la instrucción depende de los tipos de datos y del comando de mensaje que programe.

Los mensajes utilizan recursos de conexión para enviar o recibir datos. Los mensajes pueden dejar la conexión abierta (en caché) o cerrar la conexión cuando el mensaje se termina de transmitir.

Los mensajes pueden ser conectados o no conectados. Los mensajes no conectados dependen de la disponibilidad de búfers no conectados en todos los dispositivos que debe atravesar el mensaje. Los mensajes conectados comienzan con una solicitud para asignar búfers de conexión en todos esos dispositivos, antes de enviar el mensaje propiamente dicho. Si opta por dejar en caché un mensaje conectado, el controlador mantiene la conexión abierta una vez que se ha completado el mensaje. Los mensajes en caché mejoran la eficiencia si tiene previsto enviar el mensaje repetidamente.

Los mensajes conectados utilizan recursos de conexión y son menos eficaces que los mensajes en caché conectados o los mensajes no conectados. Si el mensaje conectado no se deja en caché, los recursos se utilizan temporalmente cada vez que se activa el mensaje. Mientras que un mensaje conectado en caché permanezca en la caché, los recursos permanecerán asignados y no estarán disponibles para otros mensajes. Los mensajes en caché pueden ser expulsados de la caché si la aplicación supera la capacidad de caché del controlador.

Cada mensaje utiliza una conexión del controlador, independientemente del número de dispositivos que se encuentren en la ruta del mensaje.

Tabla 18 – Tipos de mensaje

Tipo de mensaje	Método de comunicación	Mensaje conectado	El mensaje se puede dejar en caché
Tabla de datos CIP de lectura o escritura	–	Configurable	Sí ⁽²⁾
PLC-2 [®] , PLC-3 [®] , PLC-5 [®] o SLC [™] (todos los tipos)	CIP	No	No
	CIP con ID de origen	No	No
	DH+ [™]	Sí	Sí ⁽²⁾
Genérico CIP	–	Opcional ⁽¹⁾	Sí ⁽²⁾
Lectura o escritura de transferencias en bloques	–	Sí	Sí ⁽²⁾

(1) Se pueden conectar mensajes genéricos CIP. Sin embargo, en la mayoría de las aplicaciones recomendamos dejar no conectados los mensajes genéricos CIP.

(2) Le recomendamos que deje en caché los mensajes conectados que se produzcan con una frecuencia superior a una vez cada 60 segundos, si es posible.

Para obtener más información acerca del uso de los mensajes, consulte el documento Logix 5000 Controllers Messages Programming Manual, publicación [1756-PM012](#).

Determinación de si se dejarán en caché las conexiones de los mensajes

Al configurar una instrucción de mensaje, puede dejar en caché la conexión. Utilice la [Tabla 19](#) para decidir si quiere dejar en caché una conexión.

Tabla 19 – Opciones para dejar en caché las conexiones

Si el mensaje se ejecuta	Proceda como sigue
Repetidamente	Deje en caché la conexión. Cuando se deje en caché la conexión, la conexión se mantiene abierta y se optimiza el tiempo de ejecución. Si se abre una conexión cada vez que se ejecuta el mensaje, aumentará el tiempo de ejecución.
Infrecuentemente	No deje en caché la conexión. Si no se deja en caché la conexión, se cerrará la conexión cuando se complete el mensaje. Por lo tanto, la conexión estará disponible para otros usos. Los mensajes no conectados resultan muy útiles para conexiones de mensaje en caché infrecuentes.

SUGERENCIA Las conexiones dejadas en caché transfieren los datos con mayor rapidez que las conexiones no dejadas en caché. El controlador puede dejar en caché un máximo de 256 conexiones.

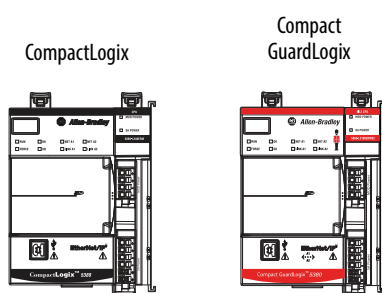
Módulos de E/S estándar

Tema	Página
Módulos de E/S locales	177
Módulos de E/S remotos	185
Adición a la configuración de E/S estando en línea	195
Determinación de cuándo se actualizan los datos	196

Los sistemas CompactLogix™ 5380 y Compact GuardLogix® 5380 admiten las siguientes opciones del módulo de E/S:

- Módulos de E/S locales
- Módulos de E/S remotos

Módulos de E/S locales



El sistema CompactLogix 5380 utiliza los siguientes módulos de E/S Compact 5000™ como módulos de E/S locales. Los módulos se instalan a la derecha del controlador.

El número de módulos de E/S Compact 5000 locales que se pueden instalar en un sistema CompactLogix 5380 depende del controlador que se utilice, hasta un máximo de 31 módulos.

La [Tabla 20](#) indica el número de módulos de E/S locales que admiten los controladores.

Tabla 20 – Módulos de E/S locales en el sistema CompactLogix 5380

Controladores CompactLogix 5380	Controladores Compact GuardLogix 5380	Módulos de E/S locales admitidos, máx.
5069-L306ER, 5069-L306ERM, 5069-L310ER, 5069-L310ERM, 5069-L310ER-NSE	5069-L306ERMS2, 5069-L306ERS2, 5069-L310ERS2, 5069-L310ERMS2	8
5069-L320ER, 5069-L320ERM	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K	16
5069-L330ER ⁽¹⁾ , 5069-L330ERM ⁽¹⁾ , 5069-L340ER, 5069-L340ERM, 5069-L350ERM, 5069-L380ERM, 5069-L3100ERM	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K, 5069-L340ERS2, 5069-L340ERMS2, 5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K, 5069-L380ERS2, 5069-L380ERMS2, 5069-L3100ERS2, 5069-L3100ERMS2	31

(1) Al utilizar este controlador con la aplicación Studio 5000 Logix Designer®, versión 29.00.00, la aplicación limita el número de módulos de E/S locales del proyecto a 16. Para obtener más información, consulte el artículo n.º 942580 de la Knowledgebase de Rockwell Automation®, “5380 CompactLogix controllers limited to 16 local modules in version 29 of Studio 5000®”. El documento está disponible en <http://www.rockwellautomation.com/knowledgebase>.

Con la aplicación Logix Designer, versión 30.00.00 y posteriores, el controlador admite hasta 31 módulos de E/S locales.

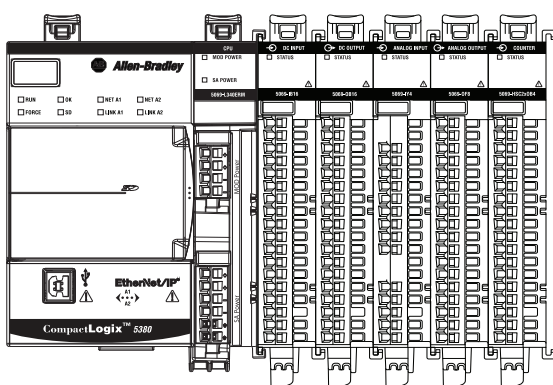
Los siguientes son factores de ejemplo que debe tener en cuenta al decidir cómo utilizar los módulos de E/S locales en un sistema CompactLogix 5380:

- Número de módulos de E/S locales que admite el controlador
- Características disponibles en los diferentes módulos, por ejemplo, una secuencia de eventos por sellos de hora de punto solo en algunos módulos de entradas digitales E/S Compact 5000
- Consumo de energía del módulo de E/S, incluida la alimentación MOD y la alimentación SA

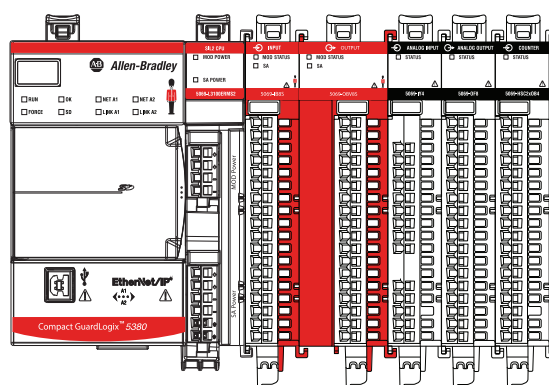
Para obtener más información sobre los módulos de E/S Compact 5000, consulte [Recursos adicionales en la página 12](#).

Figura 31 – Sistemas CompactLogix 5380 y Compact GuardLogix 5380

Controlador CompactLogix 5380 Módulos locales de E/S Compact 5000™



Controlador Compact GuardLogix 5380 Módulos locales de E/S Compact 5000



Adición de módulos de E/S locales a un proyecto

Antes de poder añadir módulos de E/S locales a un proyecto de la aplicación Logix Designer, debe abrir un proyecto existente o crear un proyecto. Para obtener información sobre cómo crear un proyecto, consulte [Creación de un proyecto en la aplicación Logix Designer en la página 85](#).

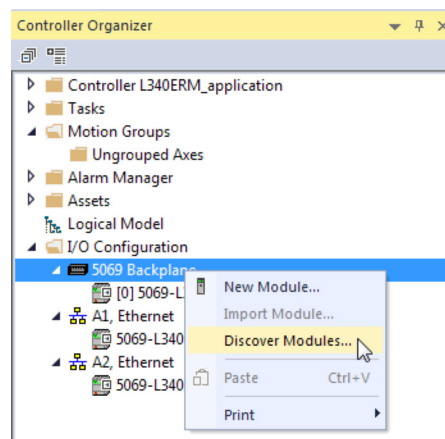
Hay dos métodos para añadir módulos de E/S locales al proyecto:

- [Descubrimiento de módulos](#)
- [Módulo nuevo](#)

Descubrimiento de módulos

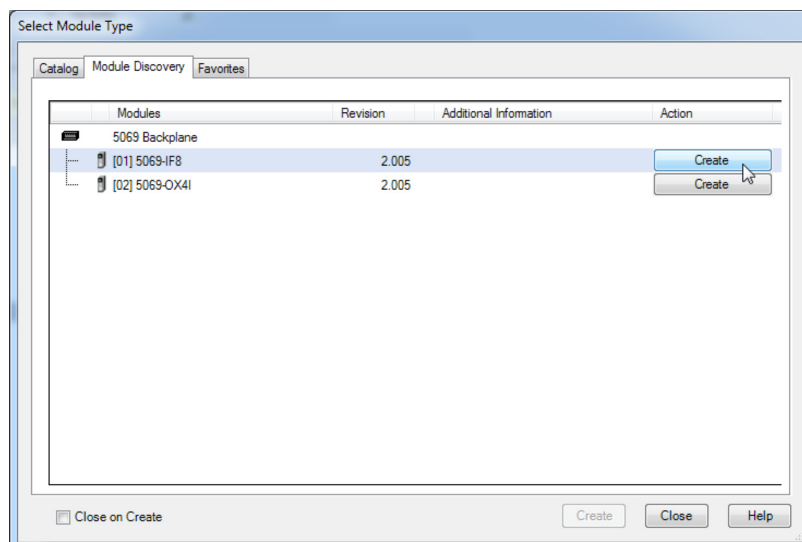
La característica de descubrimiento de módulos es útil cuando los módulos de E/S ya se han instalado y se puede conectar la aplicación Logix Designer al controlador. Para utilizar el descubrimiento de módulos a fin de añadir un módulo de E/S local, siga estos pasos.

1. Entre en línea con la aplicación Logix Designer.
2. Haga clic con el botón derecho del mouse en 5069 Backplane y seleccione Discover Modules.

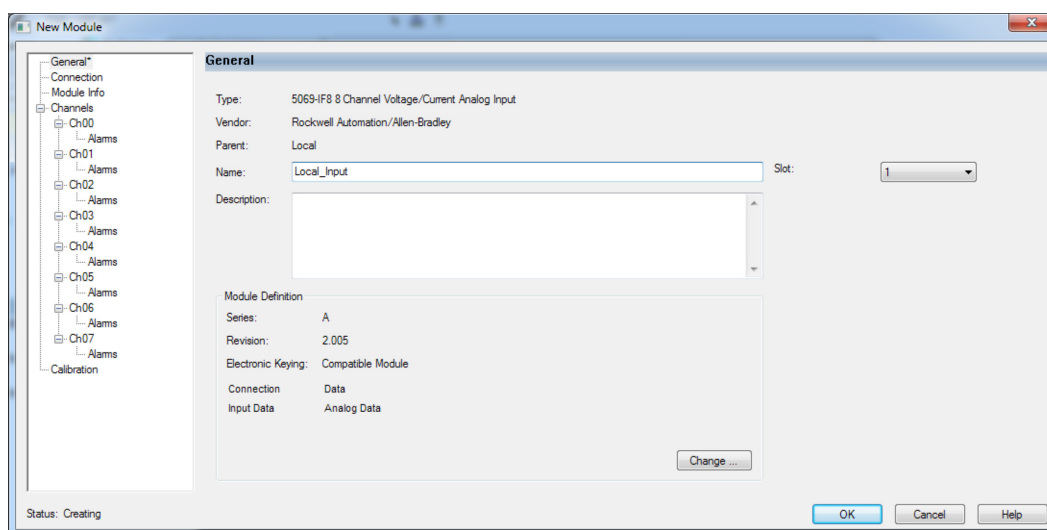


La aplicación Logix Designer detecta automáticamente los módulos disponibles que están instalados en el sistema.

- En la ventana Select Module Type, haga clic en Create para añadir el módulo descubierto a su proyecto.

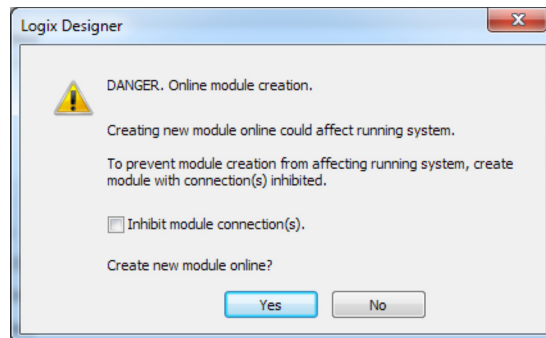


- En la ventana New Module, configure las propiedades del módulo y haga clic en OK.



5. En el cuadro de diálogo de advertencia, haga clic en Yes.

SUGERENCIA Si inhibe la conexión del módulo, debe acordarse de desinhibirla después.



6. Cierre el cuadro de diálogo Select Module Type.

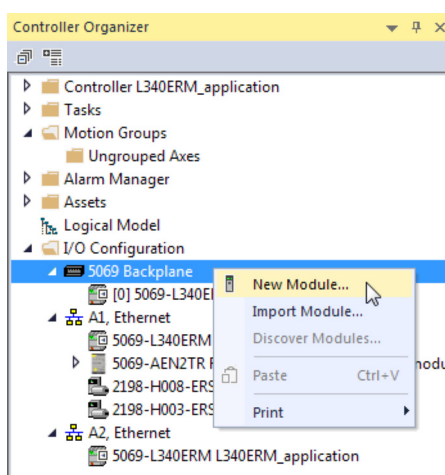
Para añadir módulos de E/S locales adicionales:

- Si desactivó la casilla de selección Close on Create al crear el primer módulo de E/S, repita los pasos [3](#) a [6](#).
- Si no desactivó la casilla de selección Close on Create al crear el primer módulo de E/S, repita los pasos [2](#) a [6](#).

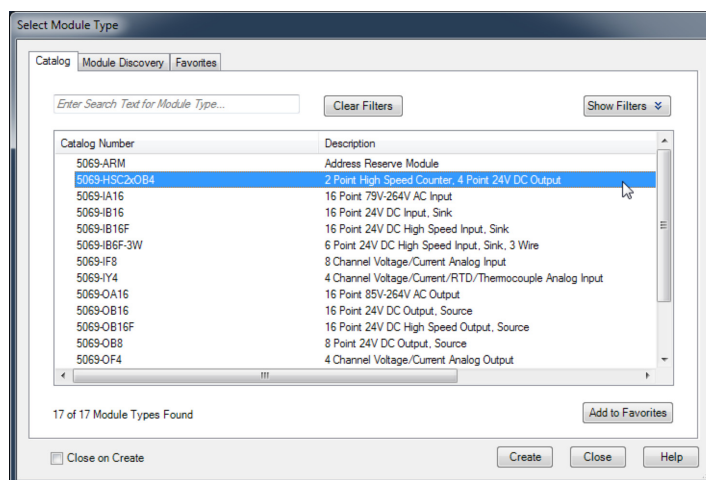
Módulo nuevo

Puede añadir un módulo de E/S estándar fuera de línea o en línea. Si no se han instalado E/S físicas o si no puede conectarse al controlador, este es el método más fácil para añadir E/S. Siga estos pasos para utilizar New Module a fin de añadir un módulo.

1. Haga clic con el botón derecho del mouse en 5069 Bus y elija New Module.



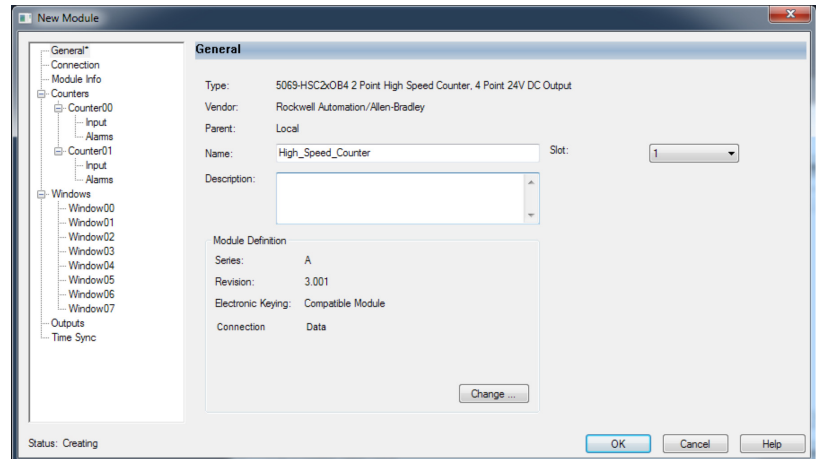
2. Seleccione el módulo y haga clic en Create.



Aparece el cuadro de diálogo New Module.

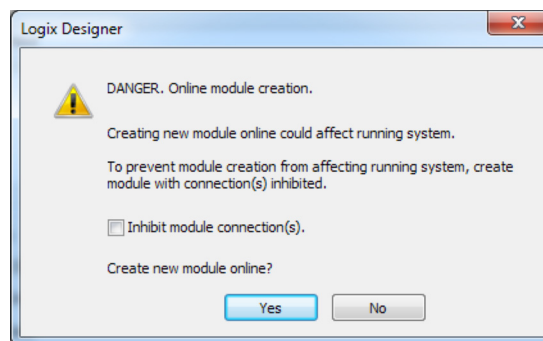
3. En la ficha General, establezca los parámetros Series y Revision.
4. Configure el resto del módulo, si corresponde. Para obtener información acerca de la codificación electrónica, vea [Codificación electrónica en la página 184](#).
5. Una vez completada la configuración, haga clic en OK.

SUGERENCIA Si los valores de los parámetros de serie y revisión no coinciden con los del módulo al que va destinada esta configuración, el proyecto puede experimentar fallos del módulo.



6. Si añade un módulo en línea, haga clic en Yes en el cuadro de diálogo Warning.

SUGERENCIA Si inhibe la conexión del módulo, debe acordarse de desinhibirla después.



7. Cierre el cuadro de diálogo Select Module Type.

Para añadir módulos de E/S locales adicionales:

- Si desactivó la casilla de selección Close on Create al crear el primer módulo de E/S, repita los pasos [2](#) a [3](#).
- Si no desactivó la casilla de selección Close on Create al crear el primer módulo de E/S, repita los pasos [1](#) a [3](#).

Para obtener más información sobre cómo utilizar módulos de E/S locales en un sistema CompactLogix 5380, consulte los recursos que se indican en [Recursos adicionales en la página 12](#).

Codificación electrónica

La codificación electrónica reduce la probabilidad de que se utilice un dispositivo incorrecto en un sistema de control. Para ello, compara el dispositivo definido en el proyecto con el dispositivo instalado. Si falla la codificación, se genera un fallo. Se comparan estos atributos.

Atributo	Descripción
Vendor	El fabricante del dispositivo.
Device Type	El tipo general de producto, por ejemplo, módulo de E/S digitales.
Product Code	Tipo específico de producto. El código de producto corresponde a un número de catálogo.
Major Revision	Número que representa las capacidades funcionales de un dispositivo.
Minor Revision	Número que representa cambios de comportamiento en el dispositivo.

Las siguientes opciones de codificación electrónica están disponibles.

Opción de codificación	Descripción
Compatible Module	Permite que el dispositivo instalado acepte la clave del dispositivo que está definida en el proyecto cuando el dispositivo instalado puede emular el dispositivo definido. Con Compatible Module, normalmente se puede reemplazar un dispositivo por otro que tenga estas características: <ul style="list-style-type: none"> El mismo número de catálogo La misma revisión mayor o una superior La revisión menor según se indica a continuación: <ul style="list-style-type: none"> Si la revisión mayor es la misma, la revisión menor debe ser la misma o una superior. Si la revisión mayor es superior, la revisión menor puede ser cualquier número.
Disable Keying	Indica que los atributos de codificación no se tienen en cuenta al intentar la comunicación con un módulo. Con la opción Disable Keying, puede ocurrir comunicación con un dispositivo diferente al tipo especificado en el proyecto. ATENCIÓN: Sea prudente al utilizar la opción de codificación Disable Keying; si se usa de forma incorrecta, esta opción puede ocasionar lesiones personales o la muerte, daños materiales o pérdidas económicas. Recomendamos encarecidamente que no use la opción Disable Keying. Si utiliza Disable Keying, será plenamente responsable de comprender si el módulo que se va a utilizar puede satisfacer los requisitos funcionales de la aplicación.
Exact Match	Indica que todos los atributos de codificación deben coincidir para establecer la comunicación. Si algún atributo no coincide exactamente, no se produce la comunicación con el dispositivo.

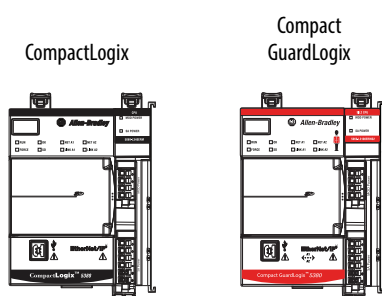
Examine cuidadosamente las implicaciones de cada opción de codificación antes de elegir una.

IMPORTANTE	Al cambiar en línea los parámetros de codificación electrónica, se interrumpen las conexiones con el dispositivo y todos los dispositivos que se conectan a través del dispositivo. Es posible que también se interrumpen las conexiones desde otros controladores. Si se interrumpe una conexión de E/S con un dispositivo, es posible que se pierdan datos.
-------------------	--

Más información

Para obtener información más detallada sobre la codificación electrónica, consulte Electronic Keying in Logix 5000 Control Systems Application Technique, publicación [LOGIX-AT001](#).

Módulos de E/S remotos



Los módulos de E/S remotos no residen en el sistema de control CompactLogix 5380 o Compact GuardLogix 5380. El controlador se conecta a los módulos de E/S mediante una red EtherNet/IP. Los controladores admiten una gran variedad de módulos de E/S remotos. Para lograr el máximo rendimiento, le recomendamos utilizar módulos de E/S Compact 5000 cuando utilice módulos de E/S remotos.

Por ejemplo, los controladores CompactLogix 5380 y Compact GuardLogix 5380 pueden conectarse a las siguientes familias de módulos:

- Familias de módulos de E/S basados en chasis, como los módulos de E/S Compact 5000, 1756 ControlLogix® I/O, 1769 Compact I/O™ o 1746 SLC™ I/O
- Familias de módulos In-Cabinet I/O, como los módulos 1734 POINT I/O™ o 1794 FLEX™ I/O
- Familias de módulos On-Machine™ I/O, como los módulos de E/S 1732E ArmorBlock®

IMPORTANTE

Los siguientes ejemplos de red están destinados únicamente a mostrar módulos de E/S remotos en varias topologías de red. Los ejemplos no abordan las velocidades de comunicación de red entre el controlador y los módulos de E/S.

No obstante, le recomendamos que tenga en cuenta las velocidades de comunicación de red cuando vaya a determinar la mejor manera de incorporar módulos de E/S remotos a su sistema CompactLogix 5380.

Para obtener más información, consulte [Velocidades de comunicación de la red EtherNet/IP en la página 137](#)

Figura 32 – Módulos de E/S remotos en un sistema CompactLogix 5380 en una topología de red DLR

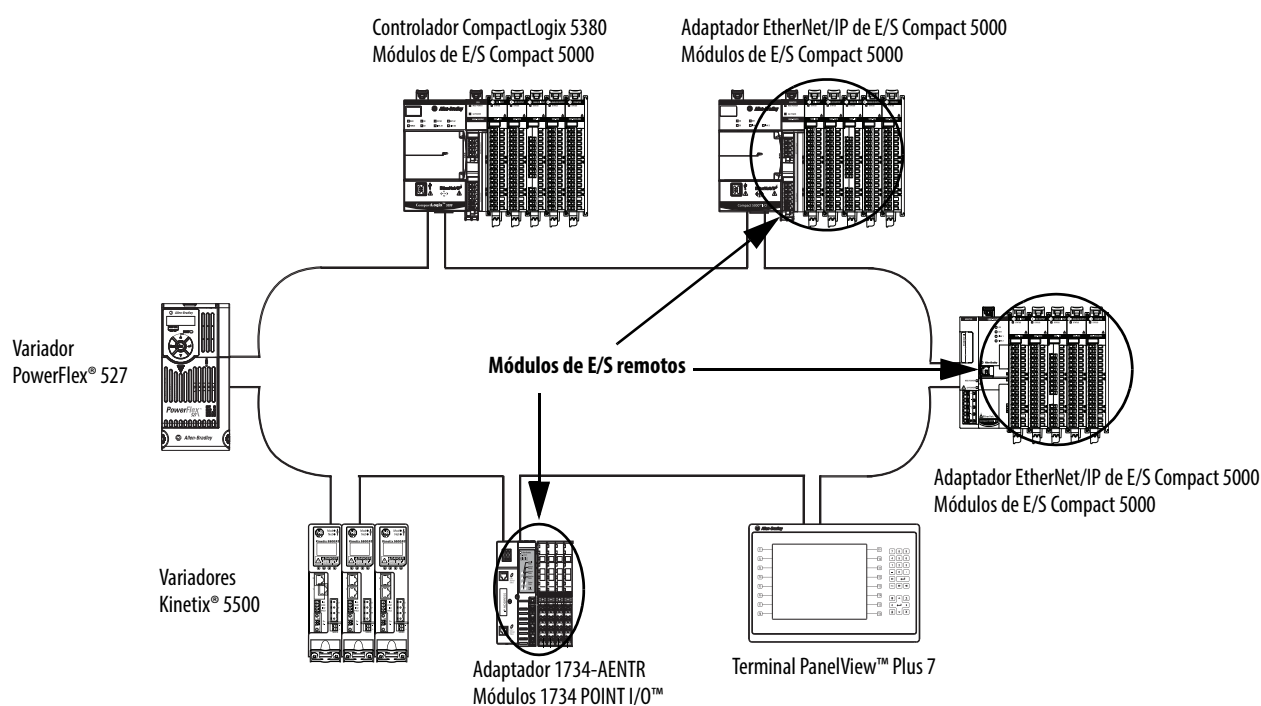


Figura 33 – Módulos de E/S remotos en un sistema CompactLogix 5380 en una topología de red lineal

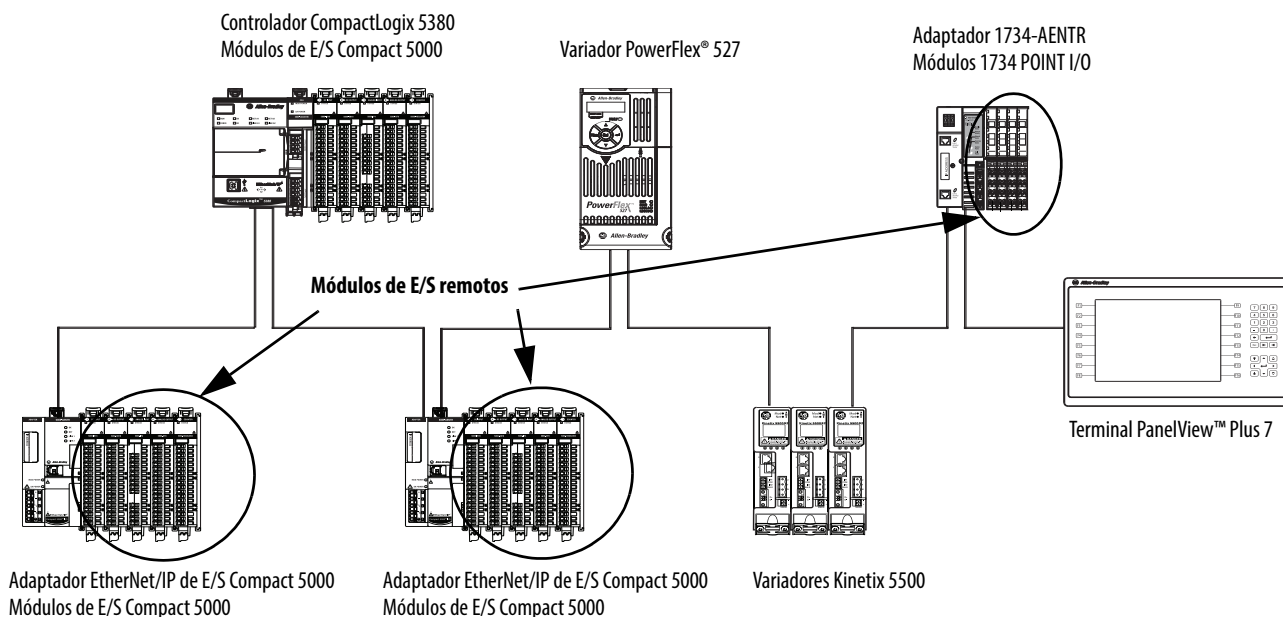
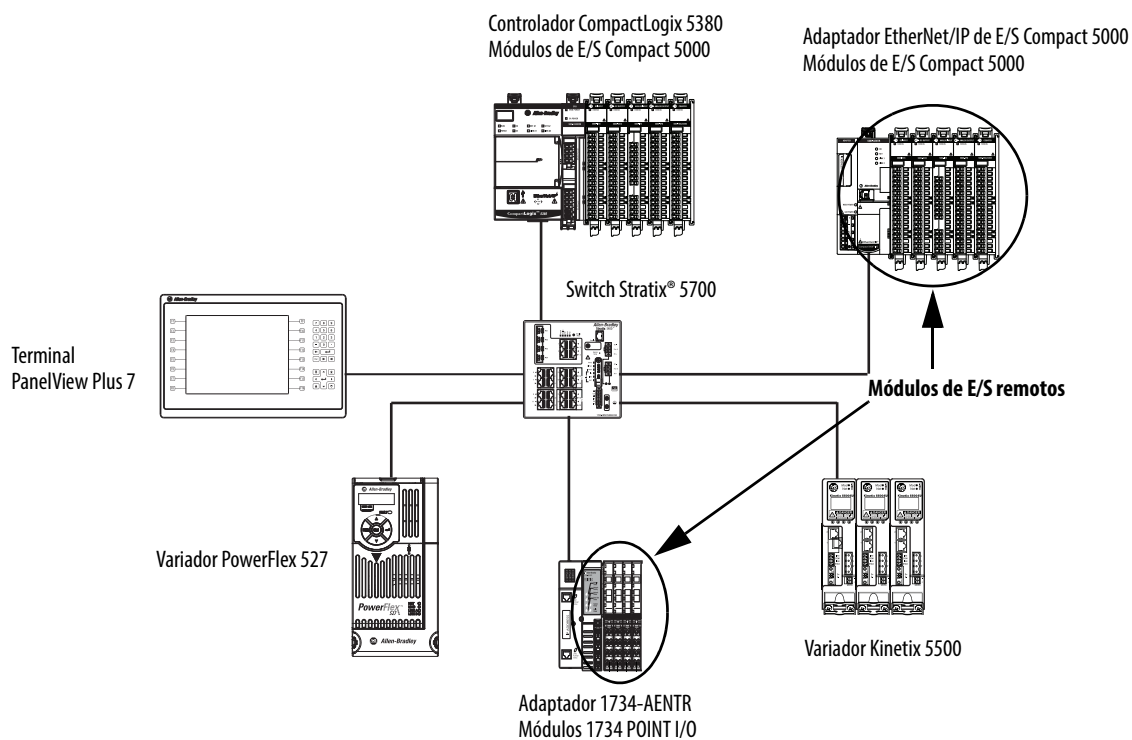


Figura 34 – Módulos de E/S remotos en un sistema CompactLogix 5380 en una topología de red en estrella



Adición de módulos de E/S remotos a un proyecto

Antes de poder añadir módulos de E/S remotos a un proyecto, debe añadir el módulo de comunicación EtherNet/IP que facilita la comunicación entre el controlador y los módulos de E/S remotos.

Hay dos métodos para añadir módulos de E/S remotos al proyecto:

- [Descubrimiento de módulos](#)
- [Módulo nuevo](#)

Descubrimiento de módulos

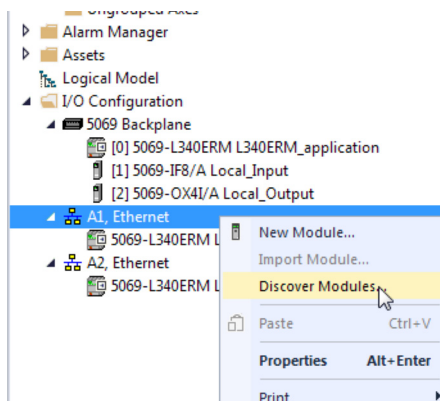
La función de descubrimiento de módulos es útil cuando los módulos de E/S ya se han instalado y están conectados a la red. Cuando se utiliza el descubrimiento de módulos para buscar dispositivos Ethernet, la aplicación Logix Designer realiza la exploración según se haya configurado la exploración de la Ethernet en el software RSLinx® Classic.

- Si se utiliza el driver EtherNet/IP en el software RSLinx Classic, la aplicación Logix Designer detecta automáticamente los módulos de E/S remotos.
- Si se utiliza el driver para dispositivos Ethernet en el software RSLinx Classic, deberá configurar la dirección IP de cada dispositivo Ethernet que quiera que aparezca en el cuadro de diálogo Select Module Type mostrado en la [página 188](#).
- Si se explora el bus Ethernet mediante un router CIP, deberá configurar la dirección IP para cada dispositivo Ethernet que quiera que aparezca en el cuadro de diálogo Select Module Type mostrado en la [página 188](#).

Las tareas que aparecen en esta sección son útiles cuando se utiliza el driver EtherNet/IP en RSWho para explorar la red.

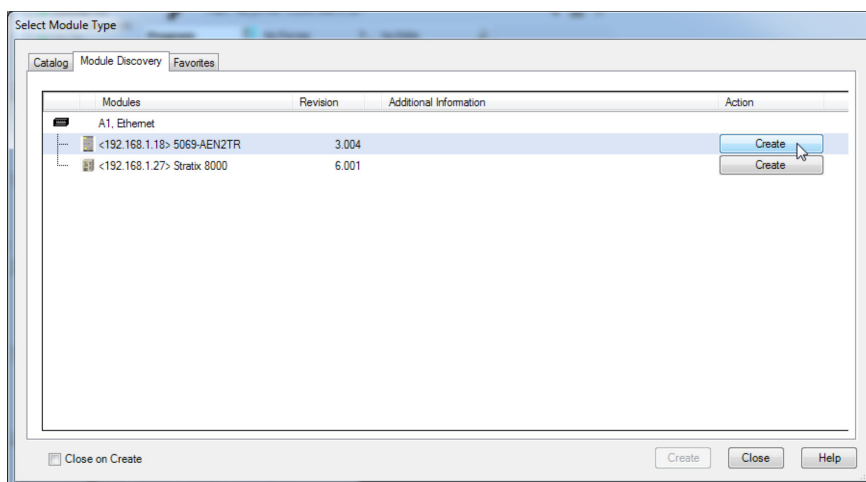
Para utilizar el descubrimiento de módulos a fin de añadir un módulo de E/S remoto, siga estos pasos.

1. Entre en línea con la aplicación Logix Designer.
2. Haga clic con el botón derecho del mouse en Ethernet y seleccione Discover Modules.

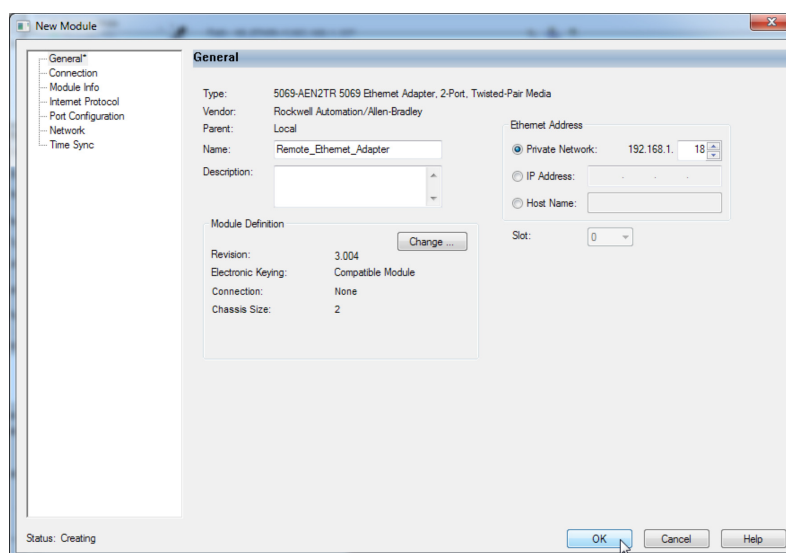


La aplicación Logix Designer detecta automáticamente los módulos disponibles que están instalados en el sistema.

- En la ventana Select Module Type, haga clic en Create para añadir un adaptador descubierto a su proyecto.

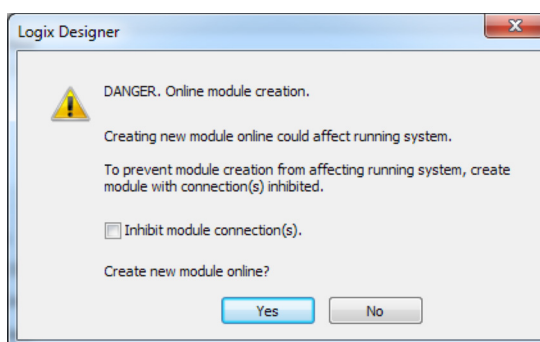


- En la ventana New Module, configure las propiedades del módulo y haga clic en OK.



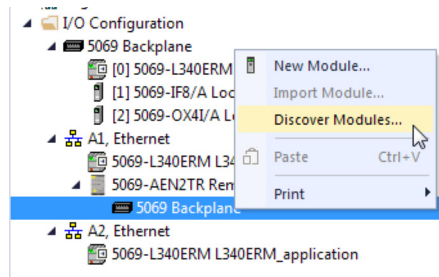
- En el cuadro de diálogo de advertencia, haga clic en Yes.

SUGERENCIA Si inhibe la conexión del módulo, debe acordarse de desinhibirla después.



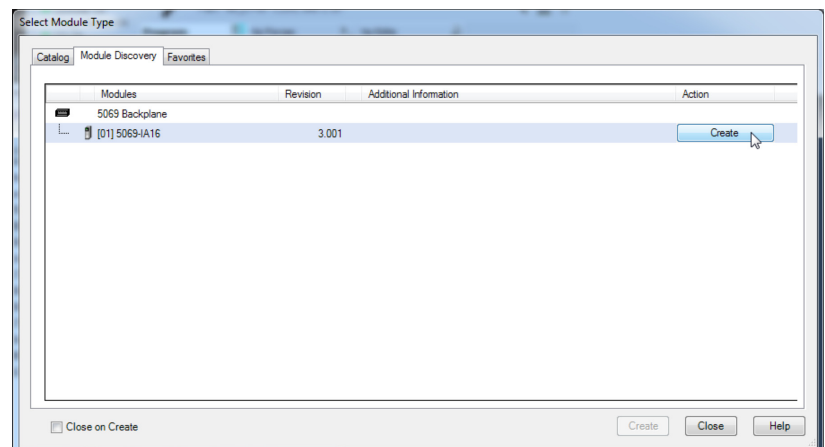
- Cierre el cuadro de diálogo Select Module Type.

7. Haga clic con el botón derecho del mouse en 5069 Backplane y seleccione Discover Modules.

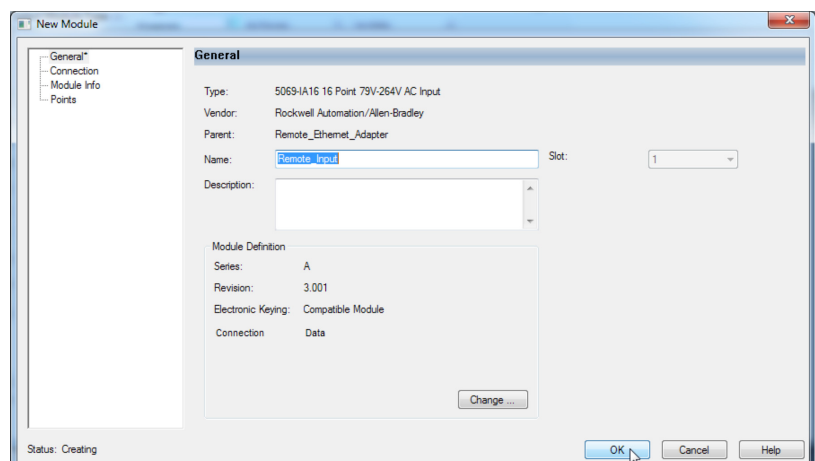


La aplicación Logix Designer detecta automáticamente los módulos disponibles que están instalados en el sistema.

8. En la ventana Select Module Type, haga clic en Create para añadir el módulo descubierto a su proyecto.

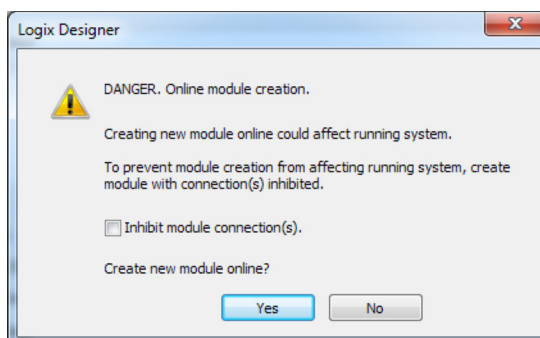


9. En la ventana New Module, configure las propiedades del módulo y haga clic en OK.



10. En el cuadro de diálogo de advertencia, haga clic en Yes.

SUGERENCIA Si inhibe la conexión del módulo, debe acordarse de desinhibirla después.



11. Cierre el cuadro de diálogo Select Module Type.

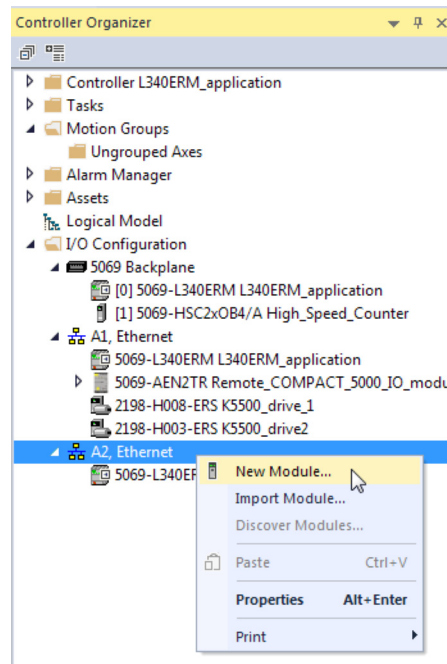
Tras añadir el módulo de E/S remoto, tenga en cuenta lo siguiente:

- Para añadir módulos de E/S remotos a la misma ubicación:
 - Si desactivó la casilla de selección Close on Create al crear el primer módulo de E/S, repita los pasos [8](#) a [11](#).
 - Si no desactivó la casilla de selección Close on Create al crear el primer módulo de E/S, repita los pasos [7](#) a [11](#).
- Para añadir módulos de E/S remotos en otra nueva ubicación remota, repita los pasos [2](#) a [11](#).

Módulo nuevo

Puede añadir un módulo de E/S estándar fuera de línea o en línea. Si no se han instalado E/S físicas o si no puede conectarse al controlador, este es el método más fácil para añadir las E/S. Siga estos pasos para utilizar New Module a fin de añadir un módulo de E/S remoto.

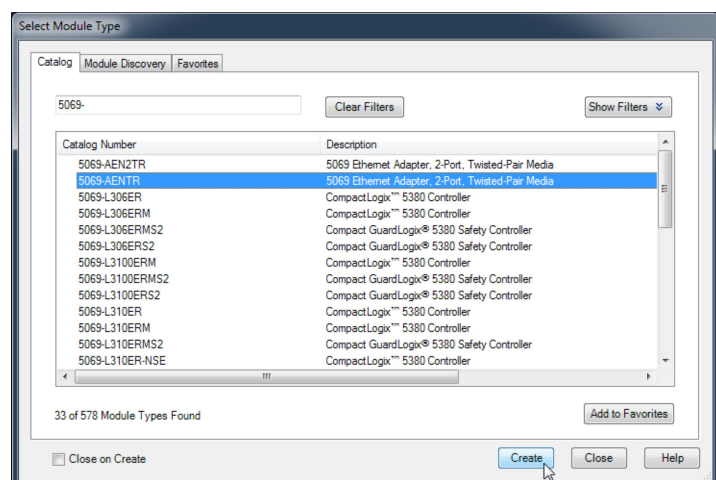
1. Haga clic con el botón derecho del mouse en Ethernet y seleccione New Module.



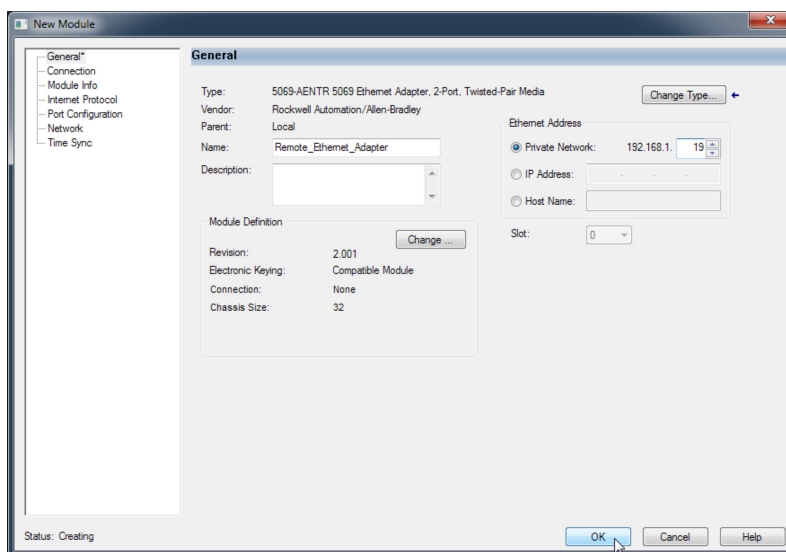
2. Seleccione el adaptador EtherNet/IP y haga clic en Create.

SUGERENCIA Para algunos módulos, es posible que aparezca un cuadro de diálogo Select Major Revision. Si aparece un cuadro de diálogo, elija la revisión mayor del módulo y haga clic en OK.

Recuerde: si los valores de los parámetros de serie y revisión no coinciden con los del módulo al que va destinada esta configuración, el proyecto puede experimentar fallos del módulo.

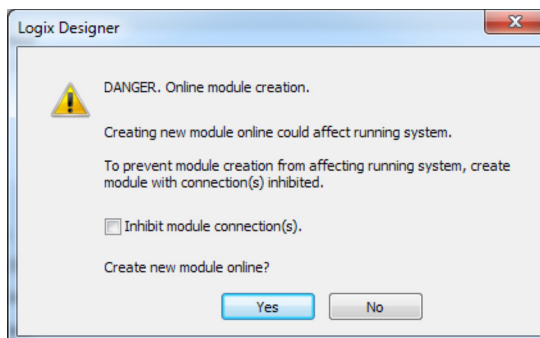


- En la ventana New Module, configure las propiedades del módulo y haga clic en OK.



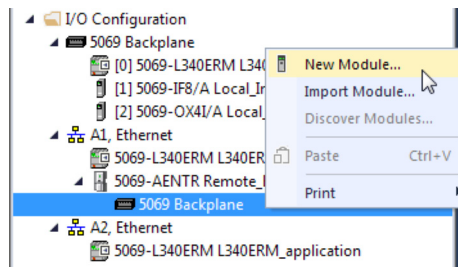
- Si añade un módulo estando en línea, haga clic en Yes en el cuadro de diálogo de advertencia.

SUGERENCIA Si inhibe la conexión del módulo, debe acordarse de desinhibirla después.



- Cierre el cuadro de diálogo Select Module Type.

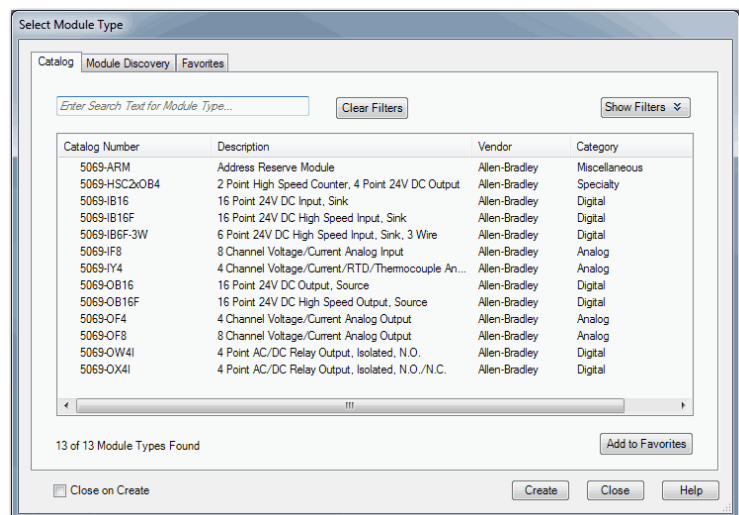
6. Haga clic con el botón derecho del mouse en el módulo de comunicación EtherNet/IP que acaba de añadir o en el backplane y seleccione New Module.



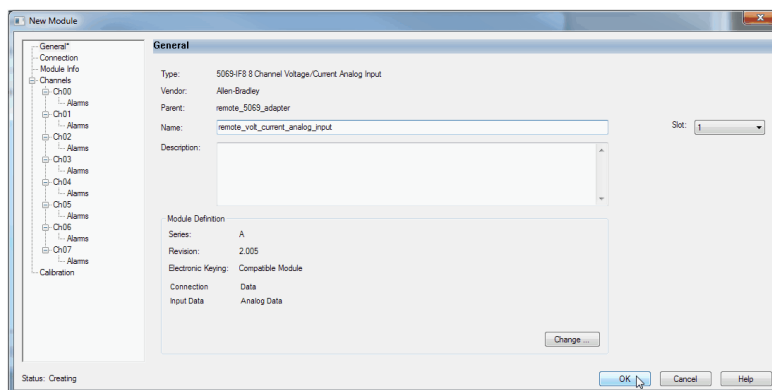
7. Seleccione el módulo de E/S que desea añadir y haga clic en Create.

SUGERENCIA Si debe añadir varios módulos de E/S a la misma ubicación remota, le recomendamos que desmarque la casilla de selección Close on Create antes de hacer clic en Create.

Si se desmarca la casilla de selección Close on Create, cuando termine la configuración de un módulo de E/S aparecerá automáticamente el cuadro de diálogo Select Module Type y podrá saltarse el [paso 6](#).

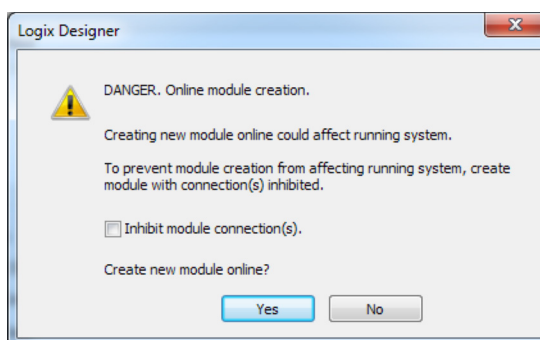


8. Configure el módulo de E/S.
9. En la ventana New Module, configure las propiedades del módulo y haga clic en OK.



10. Si añade un módulo estando en línea, haga clic en Yes en el cuadro de diálogo de advertencia.

SUGERENCIA Si inhibe la conexión del módulo, debe acordarse de desinhibirla después.



11. Cierre el cuadro de diálogo Select Module Type.

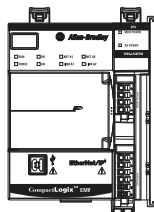
Tras añadir el módulo de E/S remoto, tenga en cuenta lo siguiente:

- Para añadir módulos de E/S remotos a la misma ubicación:
 - Si desactivó la casilla de selección Close on Create al crear el primer módulo de E/S, repita los pasos [7](#) a [8](#).
 - Si no desactivó la casilla de selección Close on Create al crear el primer módulo de E/S, repita los pasos [6](#) a [8](#).
- Para añadir módulos de E/S remotos en otra nueva ubicación remota, repita los pasos [1](#) a [11](#).

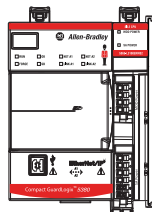
Adición a la configuración de E/S estando en línea

Puede añadir módulos de E/S locales y remotos, así como otros dispositivos a la configuración del controlador mientras el proyecto está en línea.

CompactLogix



Compact GuardLogix



IMPORTANTE

Para añadir módulos de E/S cuando el controlador está en línea, el interruptor de modo del controlador debe estar en las posiciones REM o PROG.

Los módulos de E/S Compact 5000 ya deben haberse instalado en el sistema. No puede instalar los módulos de E/S Compact 5000 mientras el sistema esté encendido.

Los módulos y dispositivos que puede añadir estando en línea dependen de la versión del software que utilice. Las versiones más recientes tienen más módulos y dispositivos que se pueden añadir estando en línea.

Los perfiles Add-On (AOP) para los módulos se publican entre los lanzamientos de las diferentes versiones de la aplicación Logix Designer. Hay casos en los que, después de descargar e instalar el archivo de AOP correspondiente a un módulo, es posible añadir el módulo a un proyecto estando en línea.

Para ver una lista de los archivos de AOP disponibles, visite:

<https://download.rockwellautomation.com/esd/download.aspx?downloadid=addonprofiles>

Para obtener más información sobre cómo añadir a la configuración de E/S estando en línea, consulte el documento Logix 5000 Controllers Design Considerations Reference Manual, publicación [1756-RM094](#).

Módulos y dispositivos que se pueden añadir estando en línea

Puede añadir estos módulos y dispositivos a la configuración de E/S del controlador CompactLogix 5380 o Compact GuardLogix 5380 estando en línea con Logix Designer, versión 28 y posteriores.

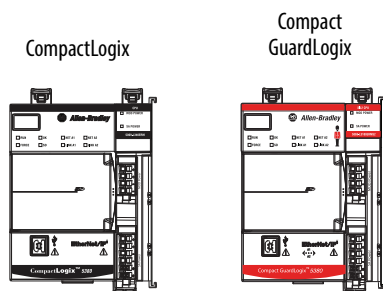
- Módulos de E/S Compact 5000: como módulos de E/S locales o remotos
- Adaptadores EtherNet/IP de E/S Compact 5000
- Módulos EtherNet/IP 1756 ControlLogix
- Módulos 1756 ControlLogix I/O

IMPORTANTE

Estos módulos **no se pueden** añadir cuando está en línea:

- Módulos de movimiento 1756 ControlLogix (1756-M02AE, 1756-HYD02, 1756-M02AS, 1756-M03SE, 1756-M08SE, 1756-M08SEG, 1756-M16SE)
- ControlLogix 1756-RIO
- ControlLogix 1756-SYNCH
- E/S de seguridad

Determinación de cuándo se actualizan los datos



Los controladores CompactLogix 5380 y Compact GuardLogix 5380 actualizan datos de forma asíncrona con la ejecución de lógica. Consulte los siguientes diagramas de flujo para determinar cuándo un controlador, módulo de entrada o puente envía datos:

- [Diagrama de flujo de actualización de datos de entrada](#)
- [Diagrama de flujo de actualización de datos de salida](#)

Diagrama de flujo de actualización de datos de entrada

IMPORTANTE Consideraciones de seguridad

Las entradas estándar Compact GuardLogix se actualizan de la misma manera que las entradas estándar CompactLogix, pero los tags de entrada de seguridad Compact GuardLogix (entradas, consumidos y asignados) se actualizan y se fijan al comienzo de la ejecución de tarea de seguridad. Vea [Ejecución de la tarea de seguridad en la página 244](#).

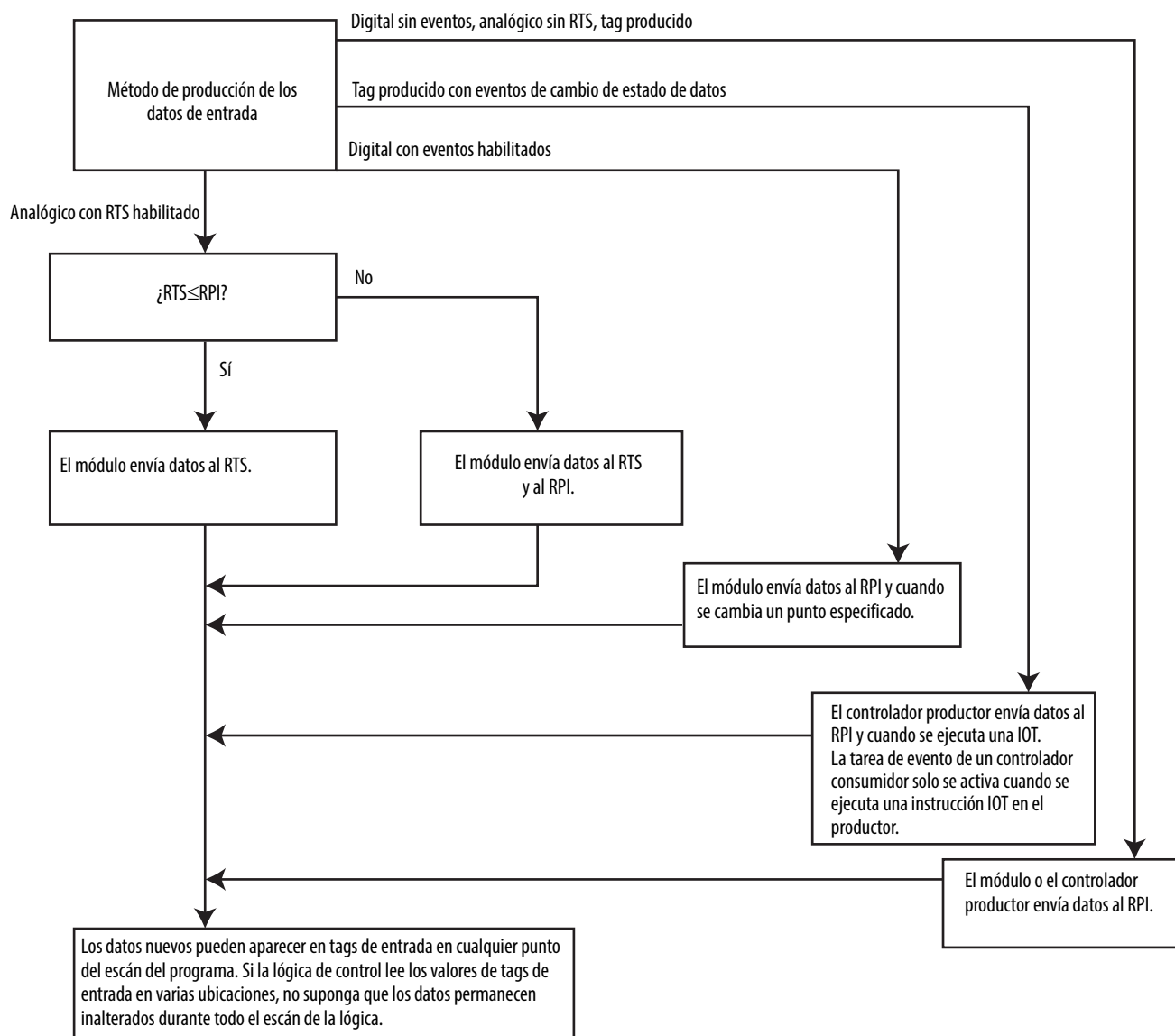
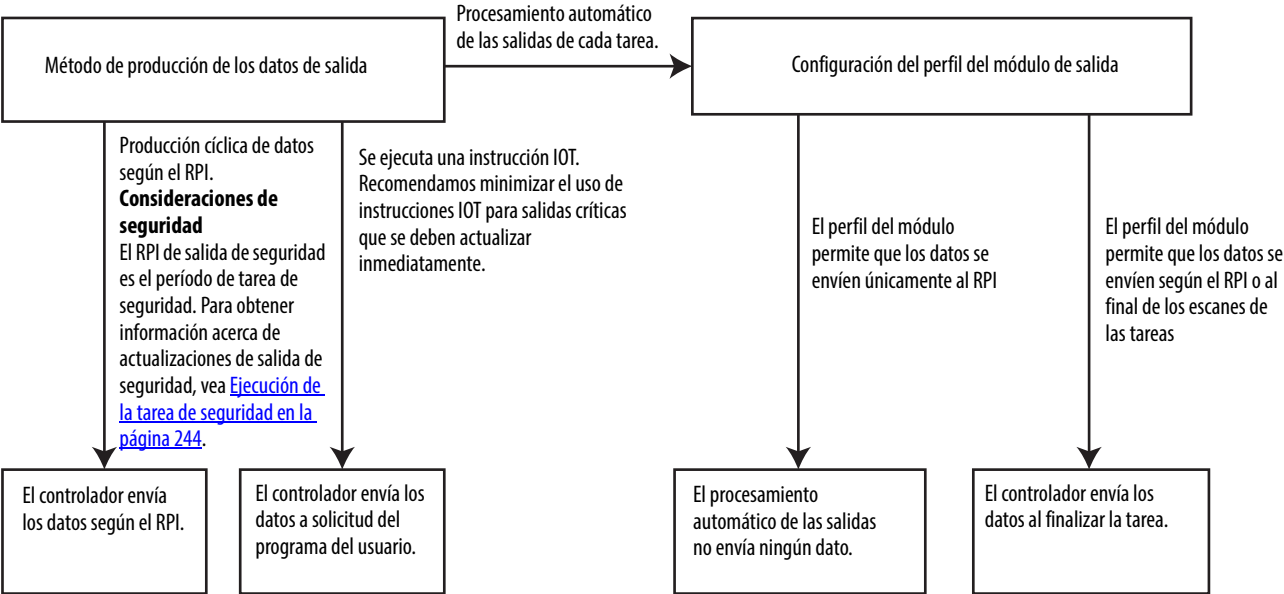


Diagrama de flujo de actualización de datos de salida



Notas:

Dispositivos de E/S de seguridad

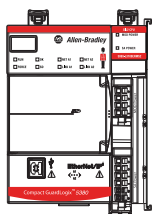
Tema	Página
Adición de dispositivos de E/S de seguridad	199
Configuración de dispositivos de E/S de seguridad	200
Uso del traductor de direcciones de red (NAT) con dispositivos CIP Safety	202
Establecimiento del SNN de un dispositivo de E/S de seguridad	204
Límite de tiempo de reacción de la conexión	208
Firma de dispositivo de E/S de seguridad	209
Formato de dirección de dispositivo de E/S	211
Sustitución del dispositivo de E/S de seguridad	212

Adición de dispositivos de E/S de seguridad

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

- Dirección de nodo para redes DeviceNet

Compact
GuardLogix



IMPORTANTE

Un controlador Compact GuardLogix® 5380 puede acceder a dispositivos en una red DeviceNet solo mediante dispositivos de vínculo, por ejemplo, el dispositivo de conexión 1788-EN2DN.

El controlador puede comunicarse con dispositivos en DeviceNet. Sin embargo, los controladores Compact GuardLogix 5380 normalmente utilizan las redes EtherNet/IP para comunicarse con dispositivos de seguridad.

- Dirección IP para redes EtherNet/IP
- Número de red de seguridad (SNN). Para establecer el SNN, vea la [página 204](#).
- Firma de configuración. Vea [página 209](#) para obtener más información acerca de cuándo se establece automáticamente la firma de configuración y cuándo tiene que establecerla.
- Límite de tiempo de reacción. Vea la [página 208](#) para obtener información sobre cómo establecer el límite de tiempo de reacción.
- La entrada de seguridad, salida y parámetros de prueba completan la configuración del módulo.

IMPORTANTE

- No puede añadir dispositivos de E/S de seguridad estando en línea con el controlador.
- Se pueden configurar los dispositivos de E/S de seguridad a través del controlador Compact GuardLogix 5380 mediante la aplicación Studio 5000 Logix Designer®.
- La función de descubrimiento de módulos no es compatible con los dispositivos de E/S de seguridad.

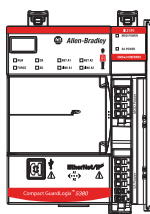
Configuración de dispositivos de E/S de seguridad

Añada el dispositivo de E/S de seguridad en la carpeta I/O Configuration.

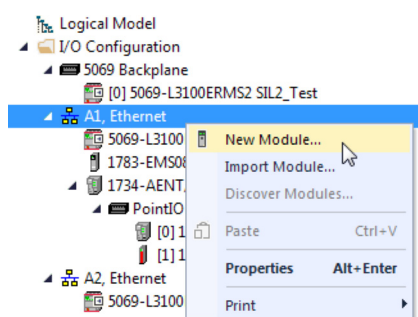
SUGERENCIA

Algunos dispositivos de E/S de seguridad admiten datos estándar y de seguridad. La definición de módulo define los datos disponibles.

Compact GuardLogix



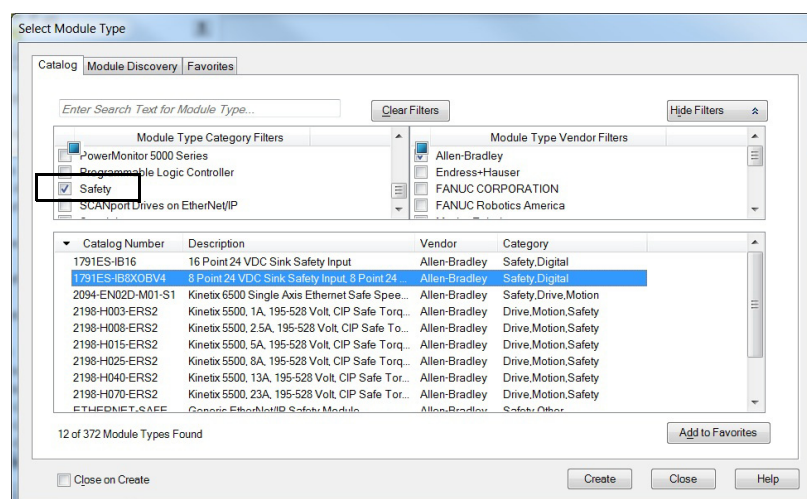
1. Haga clic con el botón derecho del mouse en la red Ethernet y seleccione New Module.



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

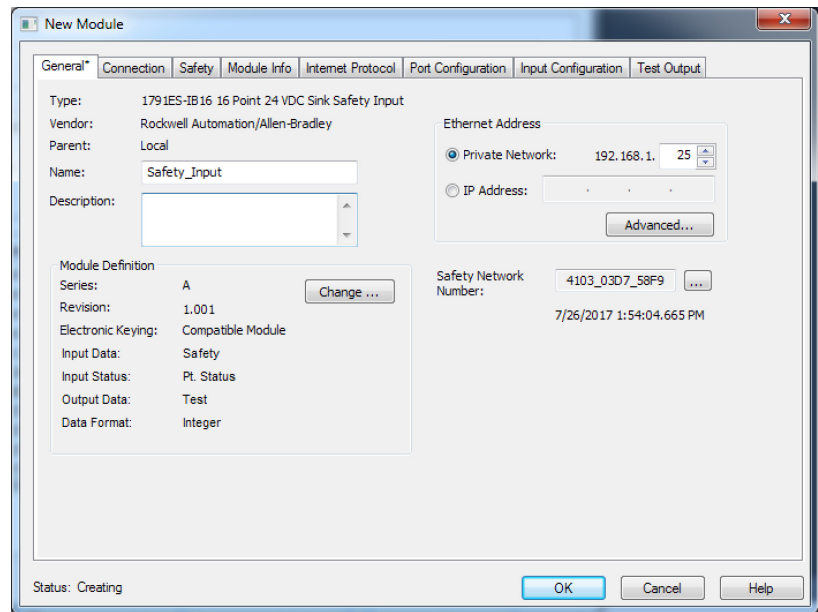
SUGERENCIA

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



3. Haga clic en Create.

4. Escriba un nombre para el nuevo dispositivo.




5. Si es necesario modificar los ajustes de definición del módulo, haga clic en Change.

IMPORTANTE No utilice Disable Keying con los dispositivos de E/S de seguridad. Para obtener más información acerca de la codificación electrónica, vea la [página 184](#).

6. Introduzca la dirección de nodo para las redes DeviceNet o la dirección IP para las redes EtherNet/IP.

Se incluyen solo los números de nodo sin usar en el menú desplegable.

Si su red usa traducción de direcciones de red (NAT), consulte [Uso del traductor de direcciones de red \(NAT\) con dispositivos CIP Safety en la página 202](#).

7. Si es necesario modificar el número de red de seguridad, haga clic en el botón .

Consulte la [página 204](#) para obtener más información.

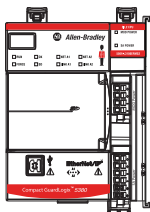
8. Utilice la ficha Safety para establecer el límite de tiempo de reacción de la conexión.

Consulte la [página 208](#) para obtener más información.

9. Para completar la configuración del dispositivo de E/S de seguridad, consulte su documentación del usuario y la ayuda en línea de la aplicación Logix Designer.

Uso del traductor de direcciones de red (NAT) con dispositivos CIP Safety

Compact
GuardLogix



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

Este servicio es útil si tiene que reutilizar las direcciones IP en toda una red. Por ejemplo, la NAT facilita la agrupación de dispositivos en segmentos en varias subredes privadas idénticas a la vez que mantiene las identidades únicas en la subred pública, por ejemplo, en el caso de varias máquinas o líneas idénticas.

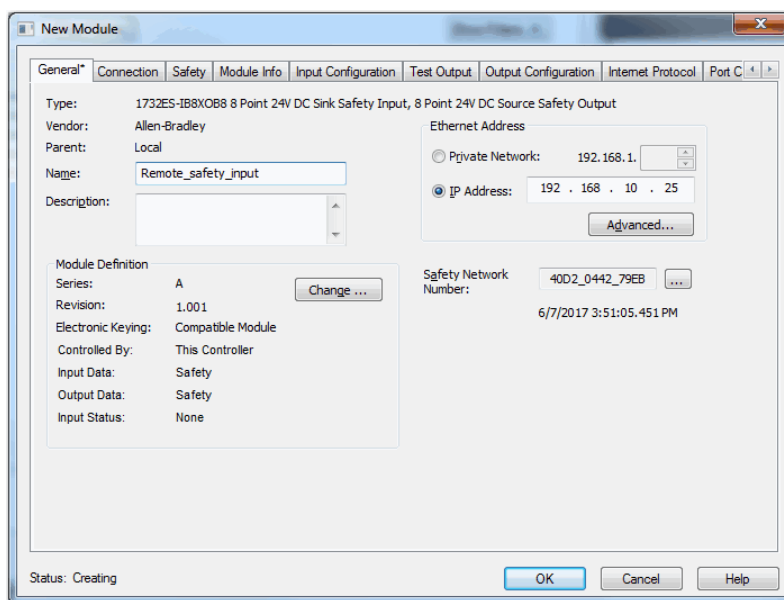
Esta sección se aplica solo a los usuarios de seguridad donde el controlador y los dispositivos con los que se comunica se encuentran en lados separados del router o switch configurado por la NAT.

En el caso de CIP Safety, la dirección IP del dispositivo es parte de la referencia de nodo única que es parte del protocolo. El dispositivo compara la porción de la dirección IP de la referencia de nodo única en los paquetes de seguridad CIP con su propia dirección IP y rechaza los paquetes donde no coincidan. La dirección IP en la referencia de nodo única debe ser la dirección IP traducida por la NAT. El controlador usa la dirección traducida, pero el protocolo CIP Safety requiere la dirección real del dispositivo.

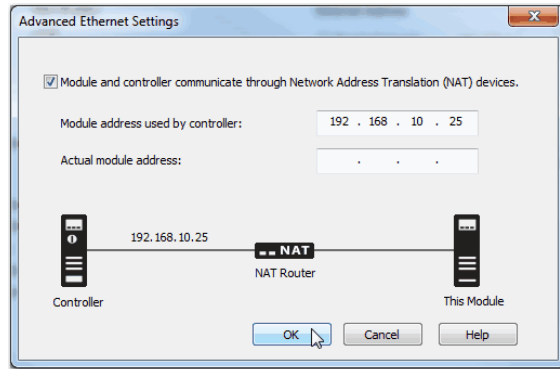
Si utiliza la NAT para comunicarse con un dispositivo CIP Safety, siga estos pasos para establecer la dirección IP.

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

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



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



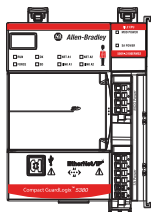
- Marque la casilla de selección para indicar que este módulo y el controlador se comunican a través de dispositivos NAT.
- Escriba la dirección del módulo real.

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

- Haga clic en OK.

Establecimiento del SNN de un dispositivo de E/S de seguridad

Compact
GuardLogix



Un SNN basado en tiempo se asigna automáticamente al añadir el primer dispositivo de E/S de seguridad a la red. Esto no se aplica al backplane del controlador ni a los puertos Ethernet puesto que el controlador se considera como dispositivo en la red.

Al añadirse dispositivos de seguridad subsiguientes a la misma red, se les asigna el mismo SNN definido en la dirección más baja en esa red CIP Safety, o el propio controlador en el caso de puertos conectados al controlador.


Para la mayoría de las aplicaciones, basta con este SNN automático basado en tiempo.

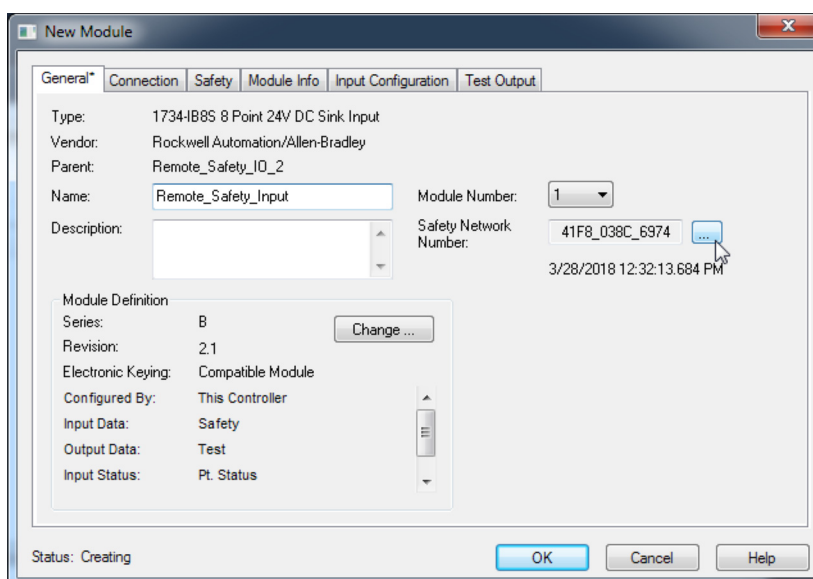
Si la aplicación requiere la asignación manual del SNN de dispositivos de E/S de seguridad, solo habrá que asignar el SNN al primer dispositivo de E/S de seguridad que añada en una red o backplane remoto. Logix Designer asigna el SNN del primer dispositivo a cualquiera de los dispositivos que añade a la misma red remota o al mismo backplane remoto.

Para obtener una explicación del número de red de seguridad (SNN), consulte el documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#).

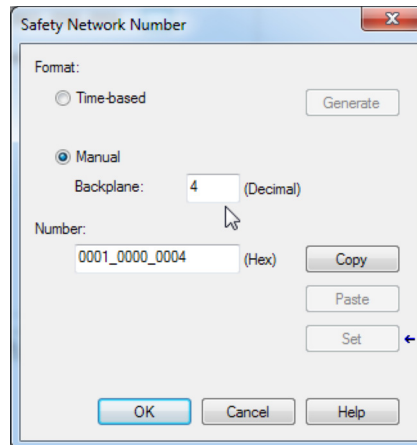
Cambio del SNN de un dispositivo de E/S de seguridad

Siga estos pasos para cambiar el SNN del dispositivo de E/S de seguridad a una asignación manual:

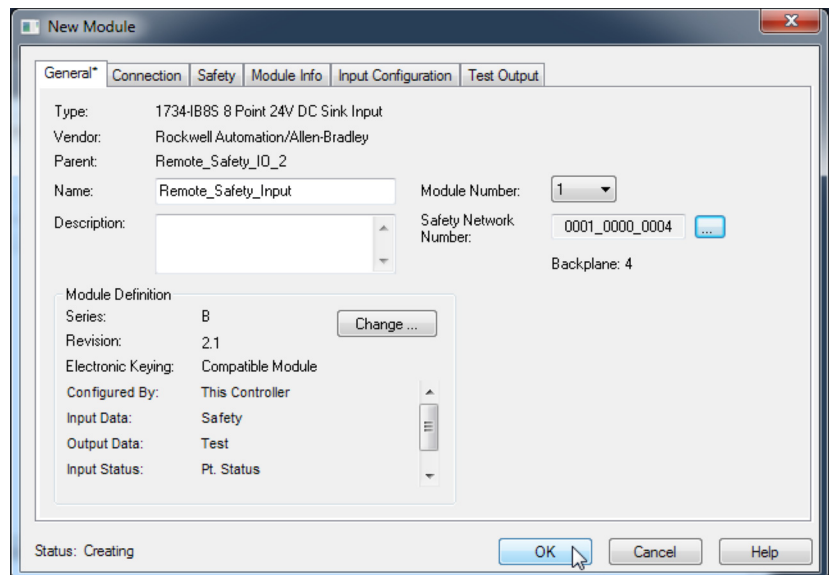
1. Haga clic con el botón derecho del mouse en el módulo de comunicación EtherNet/IP en el árbol I/O Configuration y seleccione New Module.
2. Seleccione el dispositivo de E/S de seguridad y haga clic en Create.
3. En el cuadro de diálogo de configuración New Module, haga clic en  a la derecha del número de red de seguridad.



4. En el cuadro de diálogo Safety Network Number, seleccione Manual
5. Introduzca el SNN como un valor de 1...9999 (decimal).



6. Haga clic en OK.
7. En el cuadro de diálogo de configuración New Module, haga clic en OK.



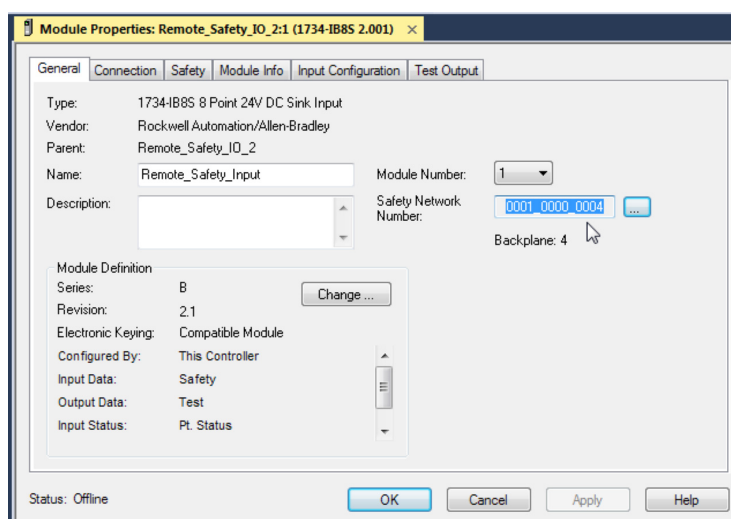
Copia y pegado de un número de red de seguridad (SNN) de dispositivo de E/S de seguridad

Si es necesario aplicar un SNN a otros dispositivos de E/S de seguridad, puede copiar y pegar el SNN. Hay diversas maneras de copiar y pegar los SNN del dispositivo de E/S de seguridad.


Copiado de un SNN del dispositivo de E/S de seguridad

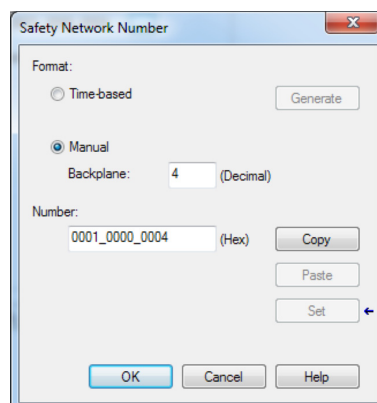
En la ficha Module Properties General:

1. En la ficha General, seleccione y resalte el SNN.
2. Presione Ctrl-C para copiar el SNN.




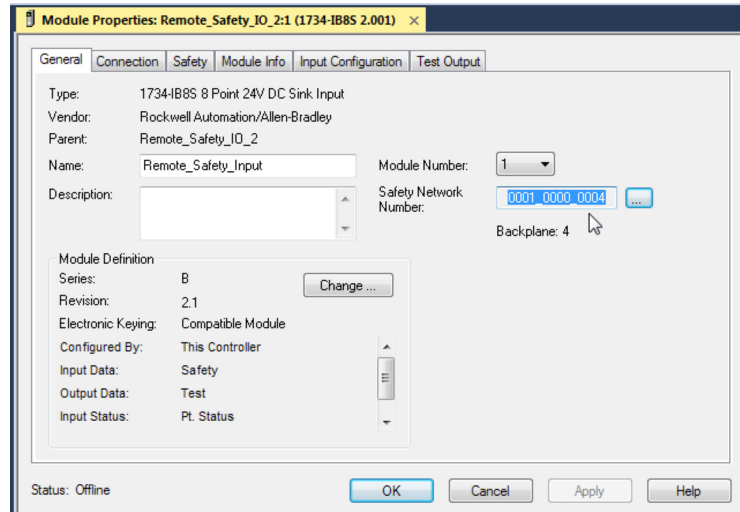
En el cuadro de diálogo Safety Network Number:

1. En la ficha Module Properties General, haga clic en  a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.
2. En el cuadro de diálogo Safety Network Number, haga clic en Copy o haga clic en el campo SNN y presione Ctrl-C.

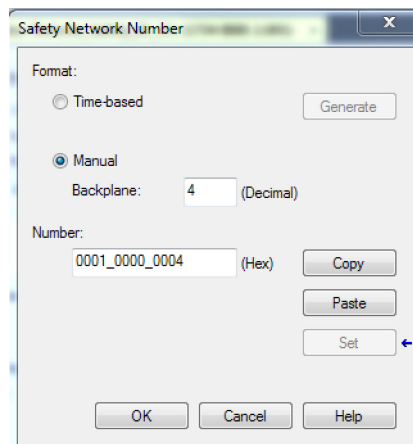


Pegado de un SNN de dispositivo de E/S de seguridad

1. En la ficha Module Properties General, haga clic en  a la derecha del número de red de seguridad para abrir el cuadro de diálogo Safety Network Number.



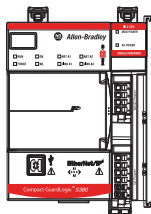
2. En el cuadro de diálogo Safety Network Number, haga clic en Paste o haga clic en el campo SNN y presione Ctrl-V.



Para obtener una explicación del número de red de seguridad, consulte el documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#).

Límite de tiempo de reacción de la conexión

Compact
GuardLogix



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

Valor	Valor predeterminado	Descripción
Requested Packet Interval (RPI)	10 ms (RPI de entrada)	El período con el que los paquetes de entrada y salida se envían al cable (red).
Timeout Multiplier	2	El multiplicador de interrupciones representa el número de reintentos antes de expirar el tiempo de espera.
Network Delay Multiplier	200	El multiplicador de retardo de red compensa los retardos conocidos en el cable. Cuando se producen estos retardos, se puede evitar que expiren los tiempos de espera mediante el uso de este parámetro.

Si ajusta estos valores, también puede ajustar el límite de tiempo de reacción de la conexión. Si no se recibe un paquete válido dentro del CRTL, la conexión de seguridad sobrepasa el tiempo de espera, y los datos de entrada y salida se ponen en el estado seguro (OFF).

IMPORTANTE Los valores predeterminados generan un límite de tiempo de reacción de la conexión de entrada de 40 ms. Si no se editan los valores predeterminados, verifique que este límite de tiempo de reacción de la conexión se utiliza en los cálculos de tiempo de reacción de seguridad.

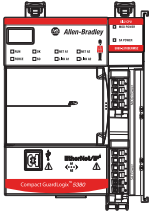
Recomendamos que no reduzca el multiplicador de interrupciones y el multiplicador de retardo de red por debajo del valor predeterminado puesto que esto puede provocar caídas falsas de conexión.

IMPORTANTE En el caso de aplicaciones con bancos grandes de POINT Guard Safety I/O, el límite de tiempo de reacción de la conexión predeterminado puede producir pérdida de conexión con los módulos de E/S de seguridad. En tales casos, puede ser necesario incrementar el valor RPI a partir del valor predeterminado. Asegúrese de que el nuevo límite de tiempo de reacción de la conexión se utilice en los cálculos de tiempo de reacción de seguridad.

Para obtener una explicación de los tiempos de reacción, consulte el documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#).

Firma de dispositivo de E/S de seguridad

Compact
GuardLogix

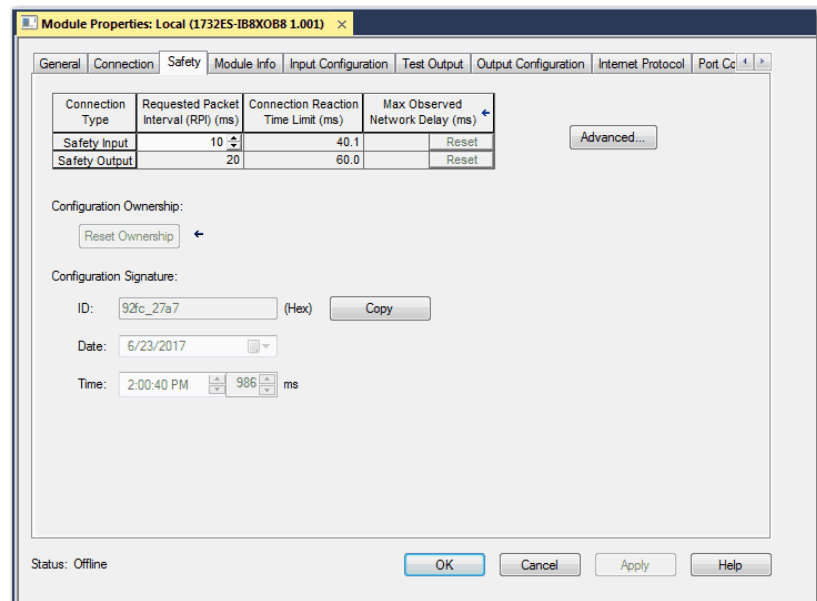


Cada dispositivo de seguridad tiene una firma de configuración única que define la configuración del módulo. La firma de configuración está compuesta por un número de identificación, fecha y hora, y se usa para verificar la configuración del módulo.

Configuración mediante la aplicación Logix Designer

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

Figura 35 – Visualización y copiado de la firma de configuración



Restablecimiento del dispositivo de E/S de seguridad a la condición original

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

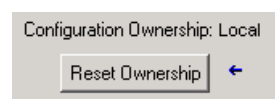
Cuando el proyecto del controlador está en línea, la ficha Safety del cuadro de diálogo Module Properties muestra la propiedad actual de la configuración. Si el proyecto abierto es propietario de la configuración, se muestra Local. Si otro dispositivo es propietario de la configuración, se muestra Remote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

Si la conexión es local, debe inhibir la conexión del dispositivo antes de restablecer la propiedad. 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 seguidamente en OK.

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

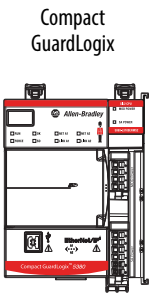
1. Haga clic con el botón derecho del mouse en el módulo y seleccione Properties.
2. Haga clic en la ficha Safety.
3. Haga clic en Reset Ownership.



SUGERENCIA

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

Formato de dirección de dispositivo de E/S



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

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

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

EJEMPLO	Modulename.Type.Member
----------------	------------------------

Tabla 21 – Formato de dirección de dispositivos de E/S de seguridad

Donde	Es	
Modulename	Nombre del dispositivo de E/S de seguridad	
Type	Tipo de datos	Entrada: I Salida: O
Member	Datos específicos provenientes del dispositivo de E/S	
	Módulo solo de entrada	Modulename:I.RunMode ⁽¹⁾ Modulename:I.ConnectionFaulted ⁽¹⁾ Modulename:I.Input Members
	Módulo solo de salida	Modulename:I.RunMode ⁽¹⁾ Modulename:I.ConnectionFaulted ⁽¹⁾ Modulename:O.Output Members
	E/S combinadas	Modulename:I.RunMode ⁽¹⁾ Modulename:I.ConnectionFaulted ⁽¹⁾ Modulename:I.Input Members Modulename:O.Output Members

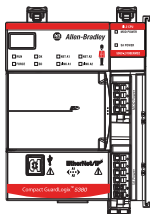
(1) Se requiere este miembro.

Tabla 22 – Más recursos

Recurso	Descripción
Datos de tags y E/S en los controladores Logix 5000 – Manual de programación, publicación 1756-PM004	Proporciona información sobre el direccionamiento de dispositivos de E/S estándar

Sustitución del dispositivo de E/S de seguridad

Compact
GuardLogix



Esta sección proporciona información sobre cómo sustituir los dispositivos de E/S de seguridad conectados a los controladores Compact GuardLogix.

Propiedad de la configuración

Cuando el proyecto del controlador está en línea, la ficha Safety del cuadro de diálogo Module Properties muestra la propiedad actual de la configuración.

- Si el proyecto abierto es propietario de la configuración, se muestra Local.
- Si otro dispositivo es propietario de la configuración, se muestra Remote junto al número de red de seguridad (SNN), y la dirección de nodo o el número de ranura del propietario de la configuración.
- Si falla la lectura del módulo, se muestra Communication error.

Si la conexión es local, debe inhibir la conexión del dispositivo antes de restablecer la propiedad. 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 seguidamente en OK.

Configuración de reemplazo

Se puede usar la aplicación Logix Designer para reemplazar un dispositivo de E/S de seguridad en una red Ethernet.

Para reemplazar un módulo Guard I/O en una red DeviceNet, su selección depende del tipo de módulo.

Tabla 23 – Software

Si está utilizando	Use	Vea
Un dispositivo de E/S de seguridad en una red EtherNet/IP.	La aplicación Logix Designer	Más abajo
Un módulo 1791DS Guard I/O mediante un dispositivo de conexión 1788-EN2DN	Aplicación Logix Designer	Más abajo
Un módulo 1734 POINT Guard I/O™ mediante un dispositivo de conexión 1788-EN2DN y un adaptador 1734-PDN	Software RSNetWorx™ para DeviceNet	Consulte el documento Módulos de seguridad POINT Guard I/O – Manual del usuario, publicación 1734-UM013 .

- Si está confiando en una porción del sistema CIP Safety para mantener el comportamiento SIL 2/PLd durante el reemplazo del dispositivo y las pruebas funcionales, no se puede usar la función Configure Always.

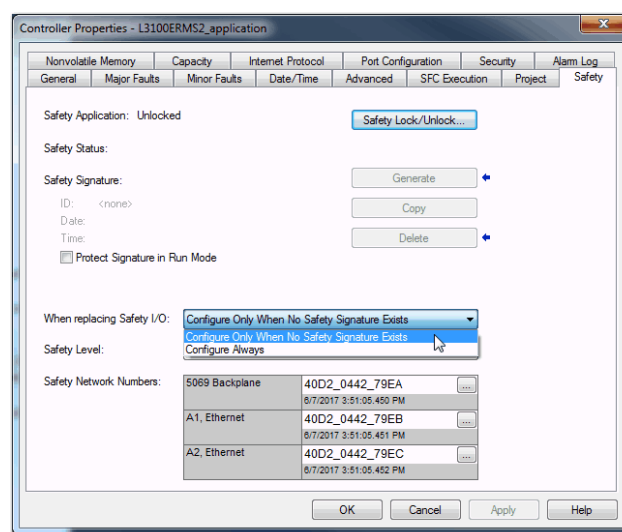
Para obtener más información, consulte [Reemplazo con “Configure Only When No Safety Signature Exists” habilitado en la página 214](#).

- Se puede utilizar la función Configure Always si no se ha confiado a todo el sistema de control CIP Safety encaminable el mantenimiento del SIL 2/PLd durante el reemplazo y la prueba funcional de un dispositivo.

Para obtener más información, consulte [Reemplazo con “Configure Always” habilitado en la página 219](#).

El reemplazo del dispositivo de E/S de seguridad se configura en la ficha Safety del GuardLogixcuadro de diálogo Controller Properties del controlador Compact 5380.

Figura 36 – Reemplazo del dispositivo de E/S de seguridad



Reemplazo con “Configure Only When No Safety Signature Exists” habilitado


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

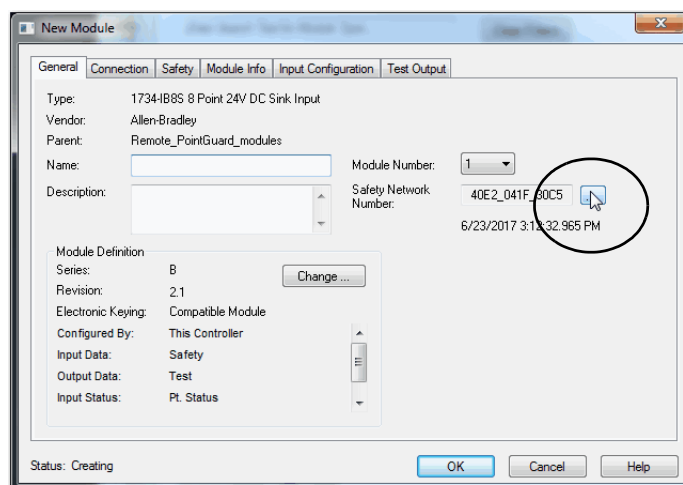
Si el proyecto se configura con la opción como “Configure Only When No Safety Signature Exists”, siga los pasos apropiados indicados en la [Tabla 24](#) para reemplazar un dispositivo de E/S de seguridad basado en su escenario. Tras completar los pasos, el DeviceID coincide con el original y esto hace posible que el controlador de seguridad descargue la configuración de dispositivo apropiada y que restablezca la conexión de seguridad.

Tabla 24 – Sustitución de un módulo

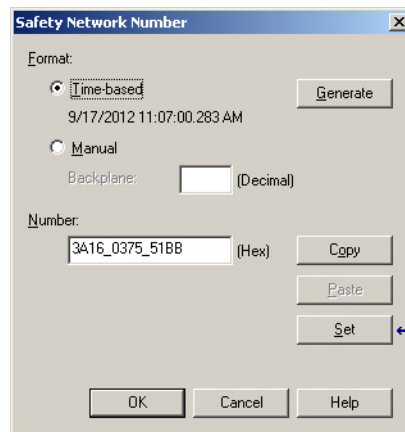
Existe la firma de seguridad Compact GuardLogix	Condición del módulo de repuesto	Acción requerida
No	Sin SNN (condición original)	Ninguna. El dispositivo está listo para ser usado.
Sí o no	El mismo SNN que el de la configuración de tarea de seguridad original	Ninguna. El dispositivo está listo para ser usado.
Sí	Sin SNN (condición original)	Vea Escenario 1 – El dispositivo de repuesto está en su condición original y existe la firma de seguridad en la página 214.
Sí	SNN diferente al de la configuración de tarea de seguridad original	Vea Escenario 2 – El SNN del dispositivo de repuesto es diferente al original y existe la firma de seguridad en la página 216.
No	SNN diferente al de la configuración de tarea de seguridad original	Vea Escenario 3 – El SNN del dispositivo de repuesto es diferente al original y no existe la firma de seguridad en la página 218.

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

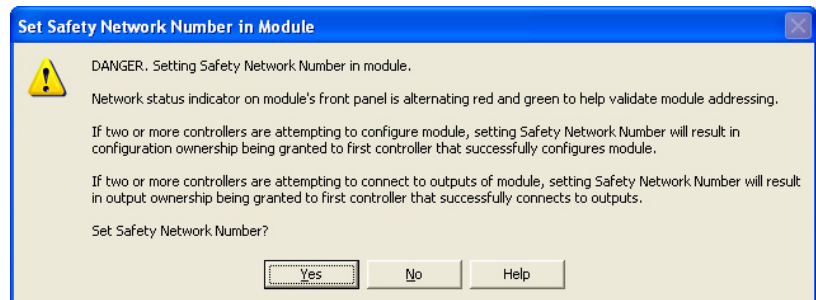
1. Retire el dispositivo de E/S antiguo e instale el nuevo.
2. Haga clic con el botón derecho del mouse en el dispositivo de E/S de seguridad de repuesto y seleccione Properties.
3. Para abrir el cuadro de diálogo Safety Network Number, haga clic en  a la derecha del número de red de seguridad.



4. Haga clic en Set.



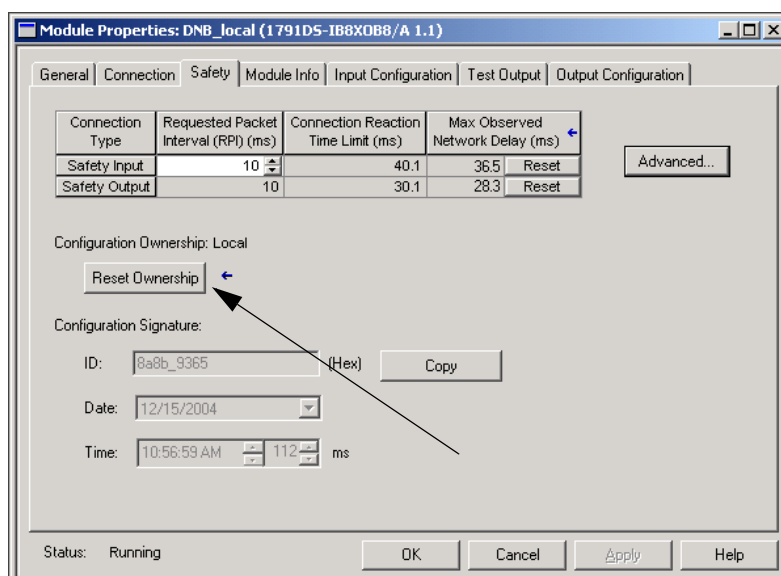
5. Compruebe que el indicador de estado de red (NS) se ilumine alternadamente de colores rojo y verde en el dispositivo correcto antes de hacer clic en Yes en el cuadro de diálogo de confirmación, para establecer el SNN y aceptar el dispositivo de repuesto.



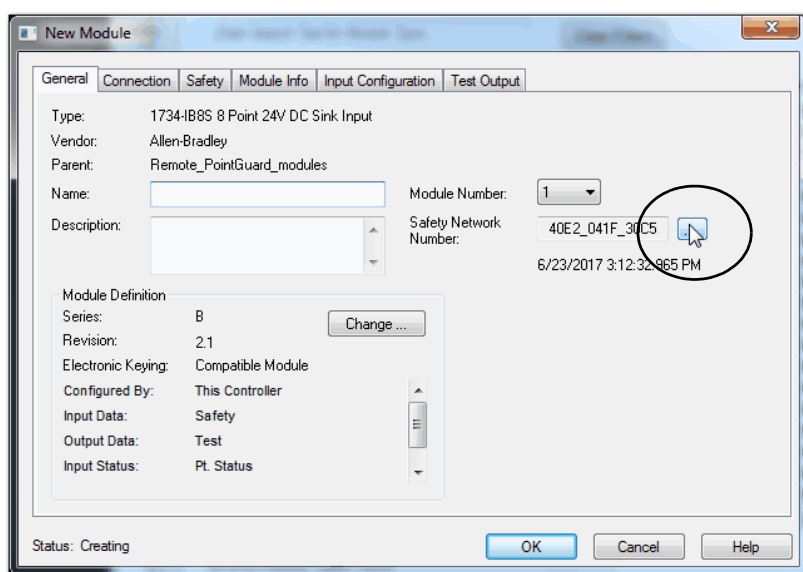
6. Siga los procedimientos establecidos en su empresa para realizar la prueba de funcionamiento del dispositivo de E/S reemplazado y del sistema, y para autorizar el uso del sistema.

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

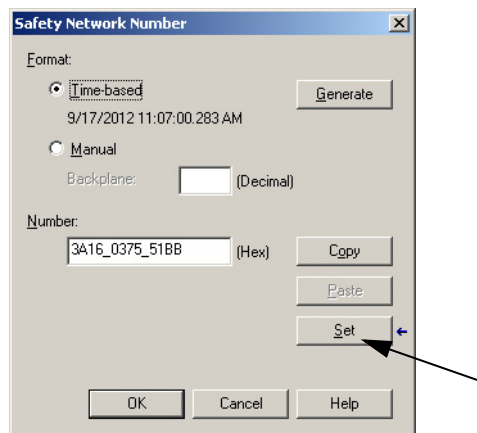
1. Retire el dispositivo de E/S antiguo e instale el nuevo.
2. Haga clic con el botón derecho del mouse en el dispositivo de E/S de seguridad y seleccione Properties.
3. Haga clic en la ficha Safety.
4. Haga clic en Reset Ownership.



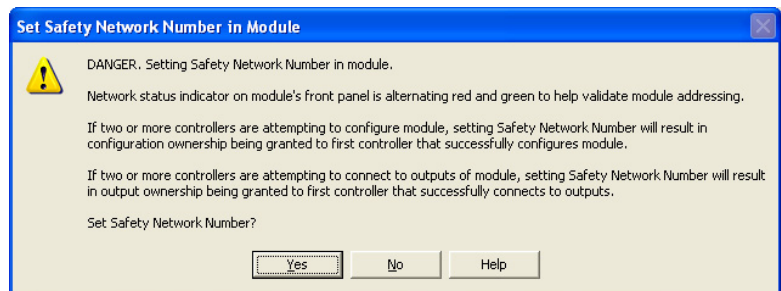
5. Haga clic en OK.
6. Haga clic con el botón derecho del mouse en el dispositivo y seleccione Properties.
7. Para abrir el cuadro de diálogo Safety Network Number, haga clic en ... a la derecha del número de red de seguridad.



8. Haga clic en Set.



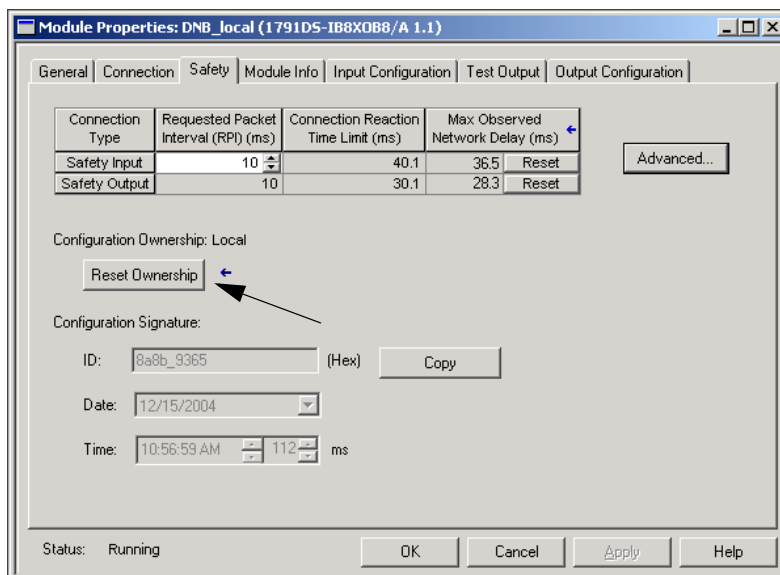
9. Compruebe que el indicador de estado de red (NS) se ilumine alternadamente de colores rojo y verde en el dispositivo correcto antes de hacer clic en Yes en el cuadro de diálogo de confirmación, para establecer el SNN y aceptar el dispositivo de repuesto.



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

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

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



4. Haga clic en Reset Ownership.
5. Haga clic en OK.
6. Siga los procedimientos establecidos en su empresa para realizar la prueba de funcionamiento del dispositivo 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** está comprometido a mantener el comportamiento SIL 2/PLd durante el reemplazo y las pruebas funcionales de un dispositivo.

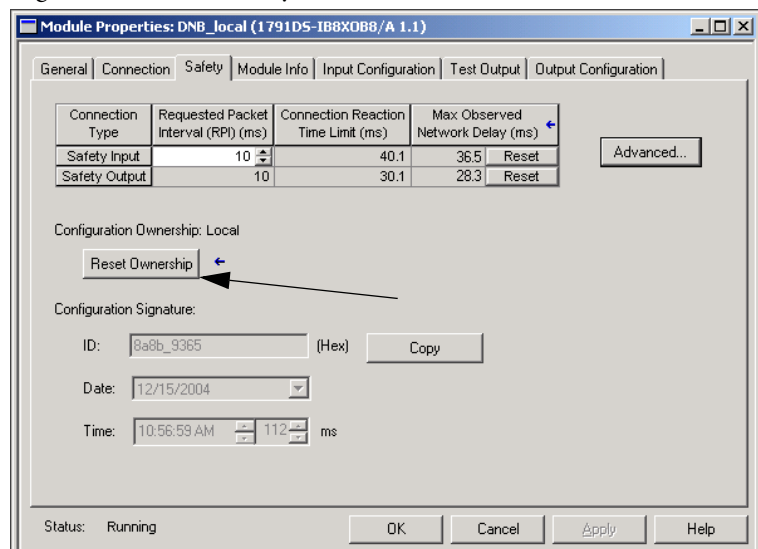
No ponga dispositivos en su condición original en una red CIP Safety si la función Configure Always está habilitada, excepto mientras está siguiendo este procedimiento de reemplazo.

Cuando la función “Configure Always” está habilitada en el proyecto del controlador, el controlador automáticamente verifica y se conecta a un dispositivo de repuesto que cumple todos estos requisitos:

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

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

1. Retire el dispositivo de E/S antiguo e instale el nuevo.
 - a. Si el dispositivo se encuentra en su condición original, vaya al paso 6. No se requiere realizar ninguna acción para que el controlador Compact GuardLogix 5380 asuma la propiedad del dispositivo.
 - b. Si ocurre un error de discordancia de SNN, vaya al siguiente paso para restablecer el dispositivo a su condición original.
2. Haga clic con el botón derecho del mouse en el dispositivo de E/S de seguridad y seleccione Properties.
3. Haga clic en la ficha Safety.



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

Notas:

Desarrollo de aplicaciones estándar

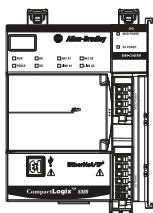
Tema	Página
Elementos de una aplicación de control	221
Tareas	223
Programas	228
Rutinas	230
Parámetros y tags locales	231
Lenguajes de programación	232
Instrucciones Add-On	233
Propiedades extendidas	234
Acceso al objeto del módulo desde una instrucción Add-On	235
Monitoreo del estado del controlador	236
Monitoreo de las conexiones de E/S	237

Elementos de una aplicación de control

Una aplicación de control está compuesta de varios elementos que deben planificarse para que la aplicación se ejecute de forma eficiente. Entre los elementos de la aplicación se incluyen los siguientes:

- Tareas
- Programas
- Rutinas
- Parámetros y tags locales
- Instrucciones Add-On

CompactLogix



Compact GuardLogix

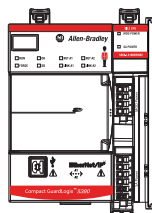
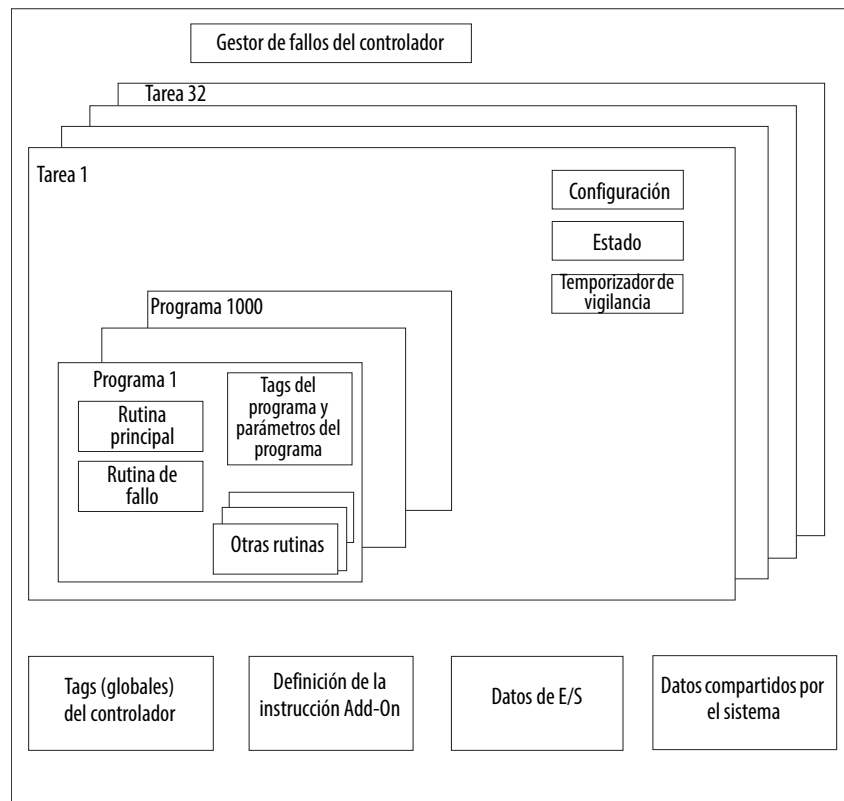


Figura 37 – Elementos de una aplicación de control



Tareas

El controlador le permite utilizar varias tareas para programar y priorizar la ejecución de los programas en función de ciertos criterios. Este procesamiento multitareas asigna el tiempo de procesamiento del controlador a las diferentes operaciones de su aplicación:

- El controlador ejecuta las tareas una por una.
- Una tarea puede interrumpir la ejecución de otra y tomar el control según su prioridad.
- Para cualquier tarea, puede utilizar varios programas. En un momento dado, solo se ejecuta un programa.
- Puede ver las tareas en las vistas del controlador o del Logical Organizer, según sea necesario.

SUGERENCIA Un gran número de tareas puede dificultar el ajuste óptimo del sistema.

Figura 38 – Tarea dentro de una aplicación de control

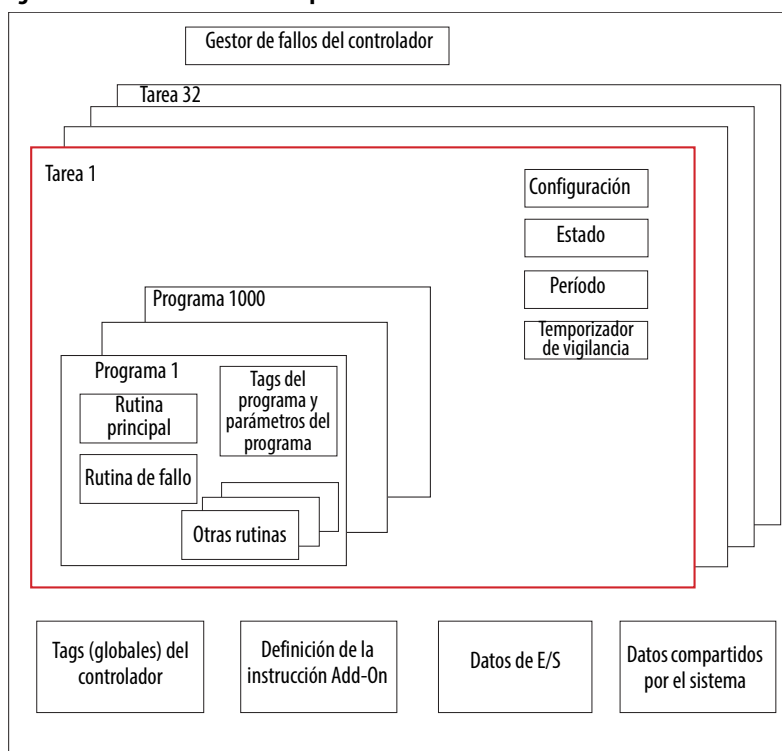
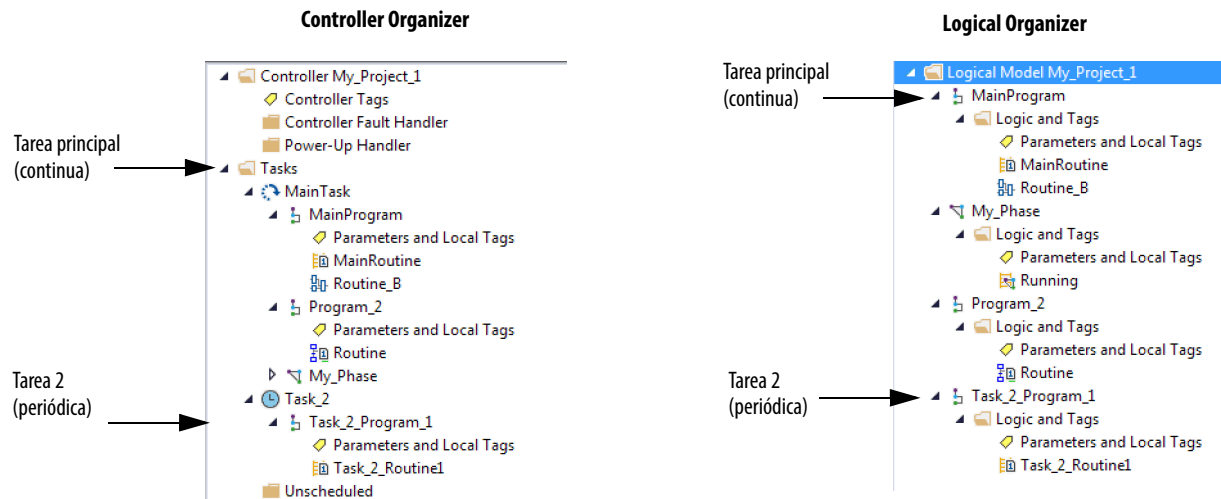
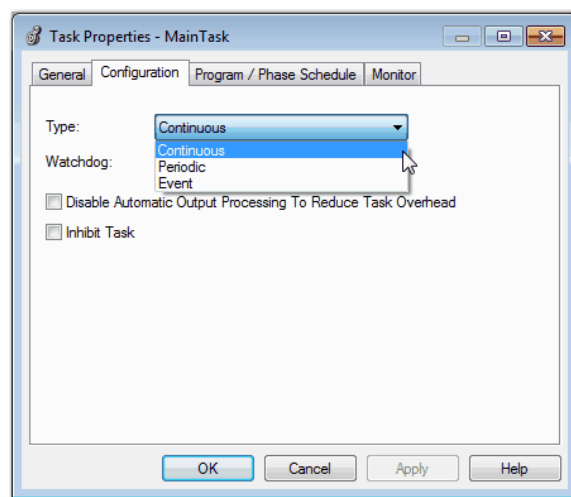


Figura 39 – Tareas



Una tarea ofrece información sobre programación y prioridad para un conjunto de uno o varios programas. Utilice el cuadro de diálogo Task Properties para configurar las tareas como continuas, periódicas o de evento.

Figura 40 – Configuración del tipo de tarea



La [Tabla 25](#) explica los tipos de tareas que puede configurar.

Tabla 25 – Tipos de tareas y frecuencia de ejecución

Tipo de tarea	Ejecución de tarea	Descripción
Continua	Constante	Una tarea continua se ejecuta en segundo plano. Todo el tiempo de CPU que no se haya asignado a otras operaciones (como control de movimiento y otras tareas) se utiliza para ejecutar los programas de la tarea continua. <ul style="list-style-type: none"> La tarea continua se ejecuta constantemente. Cuando la tarea continua realiza un escán completo, se reinicia inmediatamente. Un proyecto no requiere una tarea continua. Si se usa, usted solo utiliza una tarea continua.
Periódica	A un intervalo establecido, como por ejemplo, cada 100 ms	Una tarea periódica desempeña una función a un intervalo. <ul style="list-style-type: none"> Cada vez que transcurre el tiempo correspondiente a la tarea periódica, la tarea interrumpe todas las tareas de menor prioridad, se ejecuta una vez y devuelve el control al punto donde se quedó la tarea anterior. Puede configurar el período de tiempo de 0.1 a 2,000,000.00 ms. El valor predeterminado es 10 ms. También depende del controlador y de la configuración.
Evento	Inmediatamente cuando se produce un evento	Una tarea de evento realiza una función cuando se produce un evento (activador). El activador de una tarea de evento puede ser uno de los siguientes: <ul style="list-style-type: none"> Cambio de estado de los datos de entrada del módulo Activador de tag consumido Instrucción EVENT Activador de eje Activador de evento de movimiento Puede configurar un intervalo de tiempo de espera opcional para los activadores de eventos no detectados. El intervalo de tiempo de espera hace que las tareas de evento se ejecuten incluso en ausencia del activador. Active la casilla de selección Check the Execute Task If No Event Occurs Within <período de tiempo> correspondiente a la tarea.

Los controladores CompactLogix™ 5380 y Compact GuardLogix® 5380 admiten un máximo de 32 tareas. Solo una tarea puede ser continua.

Una tarea puede tener hasta 1,000 programas, cada uno con sus propias rutinas ejecutables y tags bajo el control del programa. Una vez que se dispara (activa) una tarea, se ejecutan los programas asignados a la tarea en el orden en el que se han agrupado. Los programas solo pueden aparecer una vez en el Controller Organizer y varias tareas no pueden compartirlos.

Tarea de evento con módulos de E/S Compact 5000

SUGERENCIA Los módulos de entrada de seguridad de E/S Compact 5000™ no pueden activar eventos.

Algunos módulos de entradas digitales E/S Compact 5000 pueden activar una tarea de evento. Por ejemplo, siga estos pasos para configurar una tarea de evento con un cambio de estado de entrada del módulo 5069-IB16F que activa el evento.

1. Configure el módulo de entrada 5069-IB16F para que active la tarea de evento. Se necesitan las siguientes tareas.
 - a. Utilice el tipo de conexión **Data with Events** en la definición del módulo 5069-IB16F.
 - b. Habilite el evento.
 - c. Seleccione como mínimo un punto en el módulo para que participe en el evento.
 - d. Defina lo que constituye un evento, por ejemplo, un cambio de estado de desactivado a activado.
 - e. Elija qué flanco del evento desencadena el evento. Es decir, el flanco ascendente, el flanco descendente, o ambos pueden activar un evento.

También puede enclavar un evento y habilitar activadores de puntos independientes.

2. Cree una tarea de evento en su proyecto.
3. Configure la tarea de evento.
 - Debe elegir el activador del evento. Por ejemplo, puede elegir Module Input Data State Change como activador.
 - Vincule la tarea al tag de entrada de evento adecuado en el módulo.

Para obtener más información sobre cómo utilizar tareas de evento con los módulos de E/S Compact 5000, consulte el documento Compact 5000 I/O Digital and Safety Module User Manual, publicación [5000-UM004](#).

Para obtener más información sobre cómo utilizar las tareas de evento en general, consulte el documento Logix 5000 Controllers Tasks, Programs, and Routines Programming Manual, publicación [1756-PM005](#).

Prioridad de las tareas

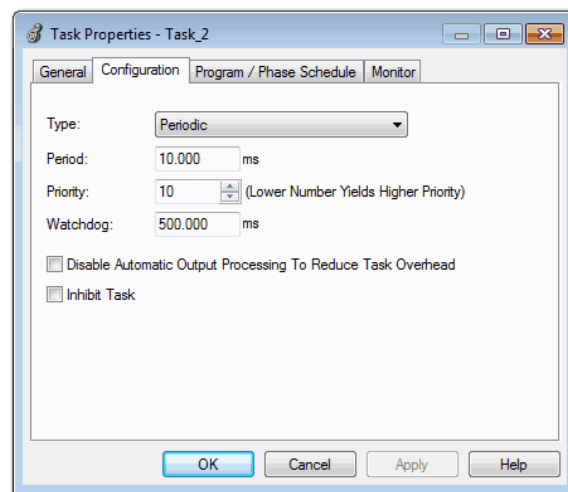
Cada tarea del controlador tiene un nivel de prioridad. El sistema operativo usa el nivel de prioridad para determinar qué tarea se debe ejecutar cuando se activan múltiples tareas. Una tarea de mayor prioridad interrumpe cualquier tarea de menor prioridad. La tarea continua tiene la prioridad más baja y cualquier tarea de evento o periódica la interrumpe.

La tarea continua se ejecuta cuando no se está ejecutando una tarea periódica. Dependiendo de la aplicación, la tarea continua podría ejecutarse con mayor frecuencia que las tareas periódicas o con mucho menos frecuencia. También puede haber una gran variabilidad en la frecuencia a la que se solicita la tarea así como su tiempo de escán (debido al efecto de otras tareas periódicas).

IMPORTANTE Si configura diversas tareas con la misma prioridad, el controlador les asigna intervalos de tiempo, lo cual suboptimiza su aplicación, lo cual no es recomendable.

Las tareas de evento y periódicas pueden configurarse para que se ejecuten desde la prioridad más baja de 15 hasta la prioridad más alta de 1. Utilice el cuadro de diálogo Task Properties para configurar la prioridad de la tarea.

Figura 41 – Configuración de la prioridad de la tarea



Programas

El sistema operativo del controlador es un sistema multitareas que permite la priorización de tareas de conformidad con la norma IEC 61131-3. Este sistema proporciona lo siguiente:

- Programas para agrupar datos y lógica
- Rutinas para encapsular el código ejecutable escrito en un solo lenguaje de programación

Cada programa contiene lo siguiente:

- Tags locales
- Parámetros
- Una rutina principal ejecutable
- Otras rutinas
- Una rutina de fallo opcional

Figura 42 – Programa dentro de una aplicación de control

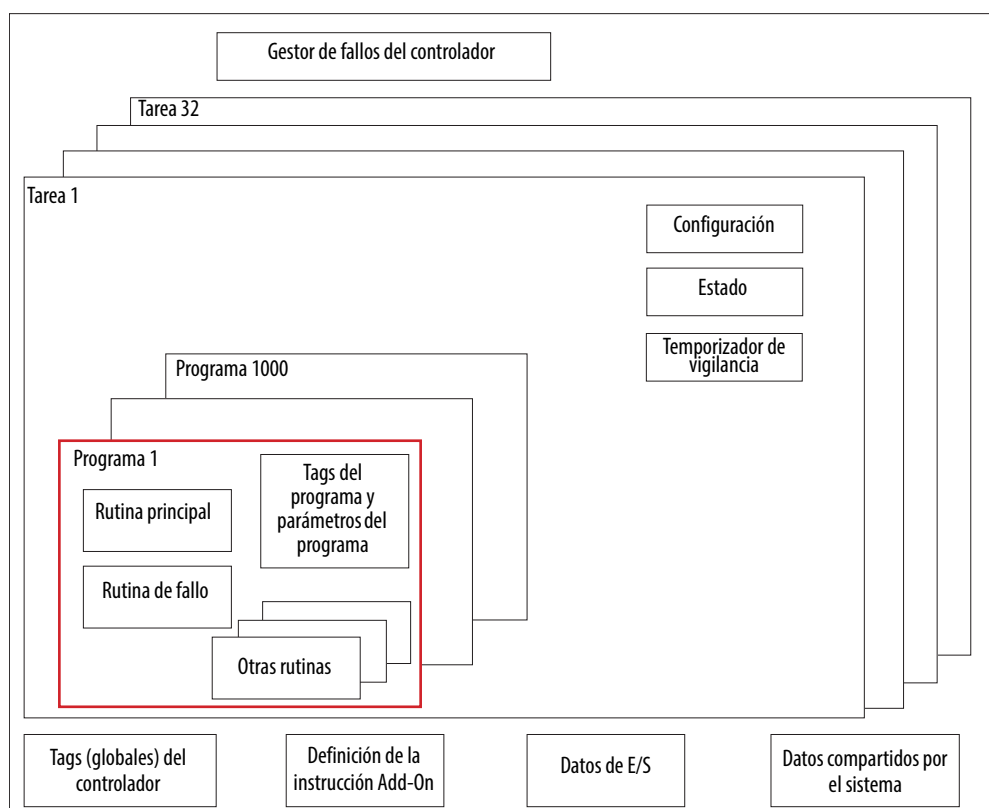
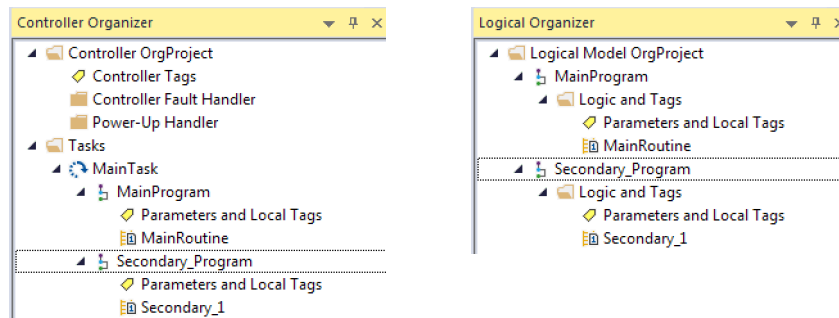


Figura 43 – Programas



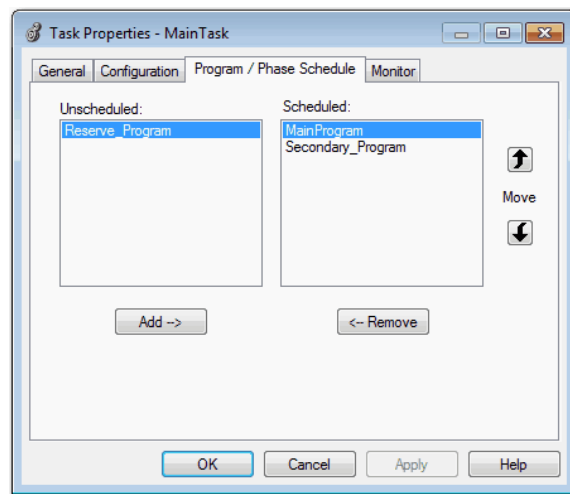
Programas priorizados y no priorizados

Los programas priorizados en una tarea se ejecutan completamente desde el primero hasta el último. Los programas que no están conectados a ninguna tarea aparecen como programas no priorizados.

Los programas no priorizados dentro de una tarea se descargan al controlador con el proyecto completo. El controlador verifica los programas no priorizados, pero no los ejecuta.

Debe priorizar un programa dentro de una tarea antes de que el controlador escanee el programa. Para priorizar un programa no priorizado, use la ficha Program/Phase Schedule del cuadro de diálogo Task Properties.

Figura 44 – Priorización de un programa no priorizado



Rutinas

Una rutina es un conjunto de instrucciones lógicas en un lenguaje de programación, como el diagrama de lógica de escalera. Las rutinas proporcionan el código ejecutable para el proyecto en un controlador.

Cada programa tiene una rutina principal. Esta rutina principal es la primera que se ejecuta cuando el controlador activa la tarea asociada y llama al programa asociado. Use lógica como, por ejemplo, la instrucción Jump to Subroutine (JSR), para llamar a otras rutinas.

También se puede especificar una rutina de fallo de programa opcional. El controlador ejecuta esta rutina si encuentra un fallo en la ejecución de una instrucción dentro de cualquiera de las rutinas en el programa asociado.

Figura 45 – Rutinas de una aplicación de control

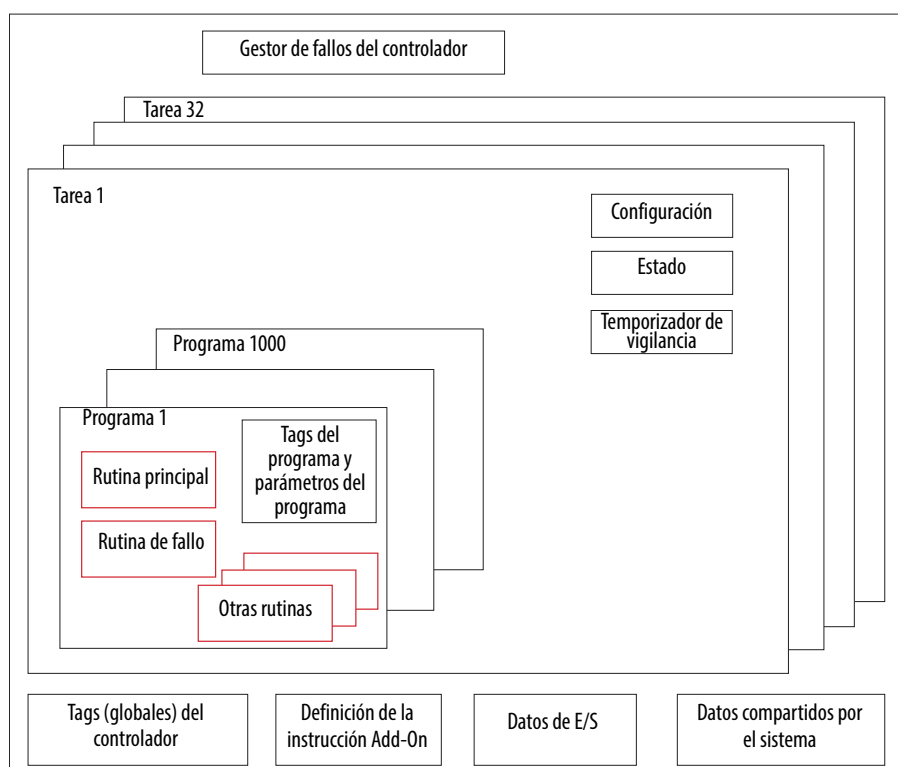
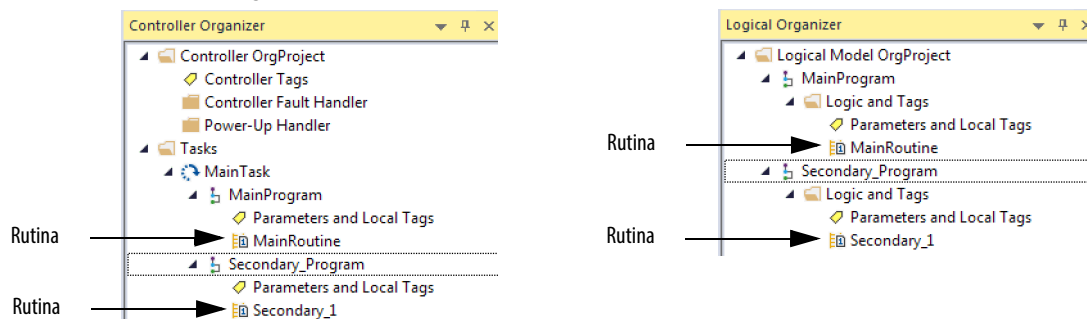


Figura 46 – Rutinas



Parámetros y tags locales

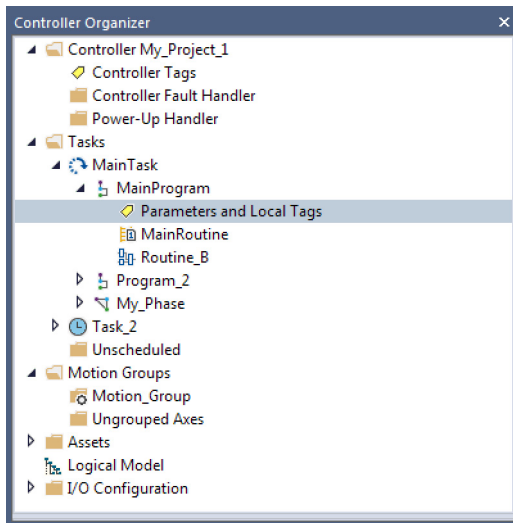
Con un controlador Logix 5000™, se utiliza un tag (nombre alfanumérico) para acceder a los datos (las variables). En los controladores Logix 5000 no hay un formato numérico fijo. El nombre del tag identifica los datos y le permite hacer lo siguiente:

- Organizar los datos para reflejar la maquinaria.
- Documentar la aplicación mientras la desarrolla.

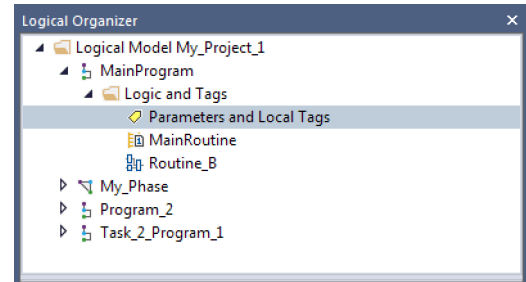
Este ejemplo muestra los tags de datos que se crean dentro del ámbito del programa principal del controlador.

Figura 47 – Ejemplo de tags

Controller Organizer – Parámetros del programa principal y tags locales



Logical Organizer – Parámetros del programa principal y tags locales



Ventana Program Tags – Tags locales y parámetros del programa principal

Scope: MainProgram		Show: All Tags		Y. Enter Name Filter...						
	Name	Usage	Alias For	Base Tag	Data Type	Description	External Access	Constant	Style	
Dispos. de E/S analógicas	north_tank_mix	Local			BOOL		Read/Write	<input type="checkbox"/>	Decimal	
	north_tank_pr...	Local			REAL		Read/Write	<input type="checkbox"/>	Float	
	north_tank_temp	Local			REAL		Read/Write	<input type="checkbox"/>	Float	
Valor entero	[+] one_shots	Local			DINT		Read/Write	<input type="checkbox"/>	Decimal	
	[+] recipe	Local			TANK		Read/Write	<input type="checkbox"/>		
Bit de almacenamiento	[+] recipe_number	Local			DINT		Read/Write	<input type="checkbox"/>	Decimal	
	replace_bit	Local			BOOL		Read/Write	<input type="checkbox"/>	Decimal	
Contador	[+] running_hours	Local			COUNTER		Read/Write	<input type="checkbox"/>		
Temporizador	[+] running_secon...	Local			TIMER		Read/Write	<input type="checkbox"/>		
Disposit. de E/S digitales	start	Local			BOOL		Read/Write	<input type="checkbox"/>	Decimal	
	stop	Local			BOOL		Read/Write	<input type="checkbox"/>	Decimal	
								<input type="checkbox"/>		

Hay varias pautas acerca de cómo crear y configurar parámetros y tags locales para lograr una ejecución óptima de tareas y programas. Para obtener más información, consulte el documento Datos de tags y E/S en los controladores Logix 5000 – Manual de programación, publicación [1756-PM004](#).

Parámetros de programa

Los parámetros de programa definen una interface de datos para programas a fin de facilitar el intercambio de datos. Puede conseguir el intercambio de datos entre programas mediante conexiones predefinidas entre los parámetros o directamente mediante una notación especial.

A diferencia de los tags locales, se puede obtener acceso a todos los parámetros de programa de forma pública fuera del programa. Además, el acceso externo de HMI se puede especificar de modo individual para cada parámetros.

Hay varias pautas acerca de cómo crear y configurar parámetros y tags locales para lograr una ejecución óptima de tareas y programas.

- Datos de tags y E/S en los controladores Logix 5000 – Manual de programación, publicación [1756-PM004](#)
- Logix 5000 Controllers Program Parameters Programming Manual, publicación [1756-PM021](#)
- Logix 5000 Controllers Design Considerations Reference Manual, publicación [1756-RM094](#)

Lenguajes de programación

La aplicación Studio 5000 Logix Designer® admite los siguientes lenguajes de programación.

Lenguaje	Se usa preferentemente en programas con
Diagrama de lógica de escalera (LD)	Ejecución continua o paralela de múltiples operaciones (no secuenciales)
	Operaciones booleanas o basadas en bits
	Operaciones lógicas complejas
	Procesamiento de comunicación y de mensajes
	Enclavamiento de máquinas
	Operaciones que el personal de servicio o mantenimiento deben interpretar para resolver problemas de la máquina o el proceso
	IMPORTANTE: El diagrama de lógica de escalera es el único lenguaje de programación que se puede utilizar con la tarea segura en los controladores Compact GuardLogix 5380.
Diagrama de bloques de funciones (FBD)	Control de variador y de proceso continuo
	Control de lazo
	Cálculos en flujo de circuito
Diagrama de funciones secuenciales (SFC)	Administración de alto nivel de múltiples operaciones
	Secuencia repetitiva de operaciones
	Proceso por lotes
	Control de movimiento que emplea texto estructurado
	Operaciones de máquinas de estados
Texto estructurado (ST)	Operaciones matemáticas complejas
	Procesamiento especializado de lazos de matriz o de tabla
	Manejo de cadenas ASCII o procesamiento de protocolo

Para obtener información sobre la programación en estos lenguajes, consulte el documento Logix 5000 Controllers Common Procedures Programming Manual, publicación [1756-PM001](#).

Instrucciones Add-On

Con la aplicación Logix Designer, es posible diseñar y configurar conjuntos de instrucciones de uso frecuente para mejorar la coherencia de los proyectos. Similares a las instrucciones incorporadas que contienen los controladores Logix 5000, estas instrucciones creadas por el usuario se conocen como instrucciones Add-On.

Las instrucciones Add-On reutilizan algoritmos de control comunes. Gracias a ellas puede hacer lo siguiente:

- Facilitar el mantenimiento creando lógica para una instancia.
- Aplicar protección de fuente para ayudar a proteger la propiedad intelectual.
- Reducir el tiempo de desarrollo de la documentación.

Se pueden usar instrucciones Add-On en varios proyectos. Puede definir sus instrucciones, obtenerlas de otro usuario o copiarlas de otro proyecto. La [Tabla 26](#) explica algunas de las capacidades y ventajas de usar instrucciones Add-On.

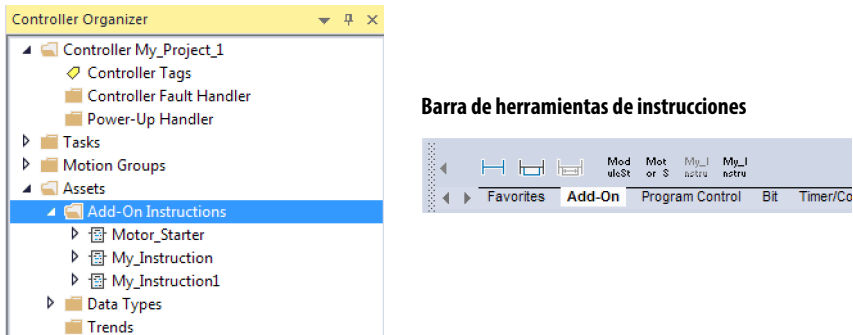
Tabla 26 – Capacidades de las instrucciones Add-On

Capacidad	Descripción
Ahorro de tiempo	Con las instrucciones Add-On, puede combinar la lógica que utiliza con mayor frecuencia en conjuntos de instrucciones reutilizables. Ahorrará tiempo si crea instrucciones para sus proyectos y las comparte con otros. Las instrucciones Add-On aumentan la uniformidad de los proyectos, ya que los algoritmos que se utilizan con frecuencia funcionan siempre de la misma manera, independientemente de quién implemente el proyecto. IMPORTANTE: No se pueden editar AOI en línea. Puede sobrescribir AOI existentes utilizando la función en línea de importación parcial.
Uso de editores estándar	Puede utilizar uno de estos editores para crear instrucciones Add-On: <ul style="list-style-type: none"> • Diagrama de escalera • Diagrama de bloques de funciones • Texto estructurado
Exportación de instrucciones Add-On	Puede exportar instrucciones Add-On a otros proyectos, y copiarlas y pegarlas de un proyecto a otro. Indique para cada instrucción un nombre único y descriptivo para facilitar la gestión y reutilización de su colección de instrucciones Add-On.
Uso de vistas en contexto	Las vistas en contexto le permiten visualizar la lógica de una instrucción para resolver en línea los problemas de las instrucciones Add-On de forma instantánea y simple.
Documentación de la instrucción	Al crear una instrucción, usted introduce información en los campos de descripción. La definición de cada instrucción incluye información sobre la revisión, el historial de cambios y una descripción. El texto de la descripción también se convierte en el tema de ayuda de la instrucción.
Aplicación de protección del código fuente	Al crear instrucciones Add-On, puede especificar que los usuarios dispongan de acceso de solo lectura a sus instrucciones. También puede prohibir el acceso a la lógica interna o a los parámetros locales que utilizan las instrucciones. Esta protección del código fuente le permite impedir cambios no deseados en las instrucciones y contribuye a proteger su propiedad intelectual.

Una vez definidas en un proyecto, las instrucciones Add-On se comportan de manera similar a las instrucciones incorporadas en los controladores Logix 5000.

Con Studio 5000 Logix Designer, versión 31 y posteriores, las instrucciones Add-On aparecen en la carpeta Assets del organizador. Estas aparecen en la barra de herramientas de instrucciones para un fácil acceso, junto con las instrucciones internas.

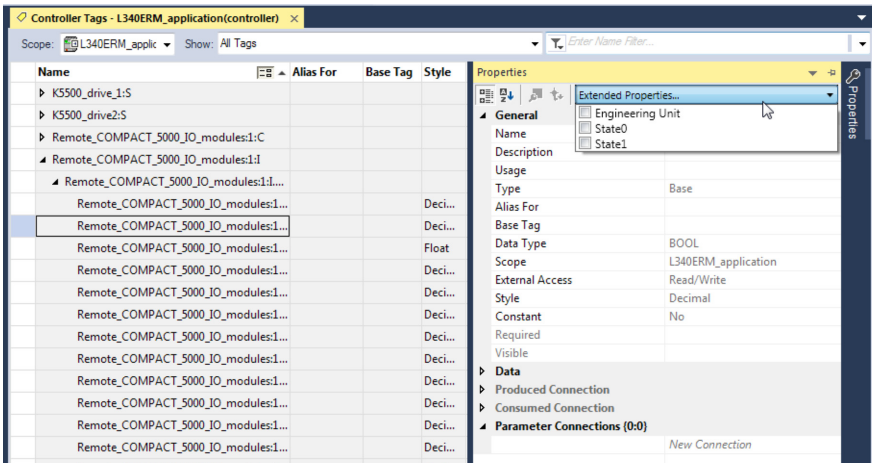
Figura 48 – Instrucciones Add-On (ejemplo de Studio 5000 Logix Designer, versión 31)



Propiedades extendidas

La función de propiedades extendidas le permite definir más información, como límites, unidades de medición o identificadores de estado, para los diferentes componentes del proyecto del controlador.

Componente	Propiedades extendidas
Tag	En el editor de tags, añada propiedades extendidas a un tag.
Tipo de datos definido por el usuario	En el editor de tipos de datos, añada propiedades extendidas a los tipos de datos.
Instrucciones Add-On	En las propiedades asociadas a la definición de la instrucción Add-On, añada propiedades extendidas a las instrucciones Add-On.



El comportamiento de paso “pass-thru” consiste en la capacidad de asignar propiedades extendidas a un nivel mayor de una estructura o instrucción Add-On y tener dicha propiedad extendida automáticamente disponible para todos los miembros. El comportamiento de paso “pass-thru” está disponible para descripciones, identificadores de estado y unidades de medición, y el usuario puede configurarlo.

El comportamiento de paso “pass-thru” se configura en la ficha Project del cuadro de diálogo Controller Properties. Si opta por no mostrar las propiedades de paso “pass-thru”, solo se mostrarán las propiedades extendidas configuradas para un determinado componente.

El comportamiento de paso “pass-thru” **no** está disponible para los límites. Cuando se crea una instancia de un tag, si hay límites asociados con el tipo de datos, se copia la instancia.

Utilice la sintaxis `.@Min` y `.@Max` para definir tags que tengan límites. No hay ninguna indicación en el explorador de tags de que se hayan definido propiedades extendidas de límites para un tag. Si intenta utilizar propiedades extendidas que no se han definido para un tag, los editores muestran una indicación visual y la rutina no se verifica. Los indicadores visuales incluyen:

- Un error de renglón en la lógica de escalera.
- Una X de error de verificación en los diagramas de bloques de funciones.
- El error subrayado en el texto estructurado.

Puede consultar las propiedades extendidas de límites definidas por la sintaxis `.@Min` y `.@Max`. Sin embargo, no es posible escribir en los valores de propiedades extendidas mediante la lógica.

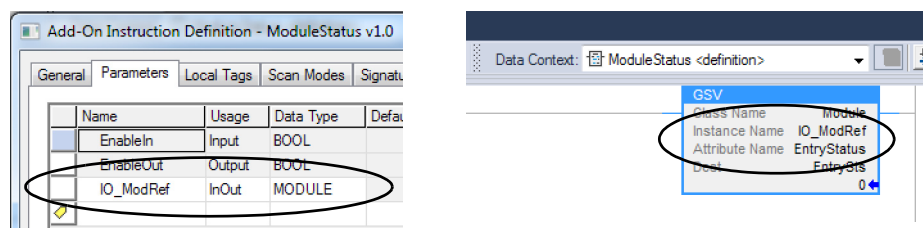
Para obtener más información sobre las propiedades extendidas, consulte el documento Datos de tags y E/S en los controladores Logix 5000 – Manual de programación, publicación [1756-PM004](#).

Acceso al objeto del módulo desde una instrucción Add-On

El objeto MODULE proporciona información de estado acerca de un módulo. Para seleccionar un objeto de módulo concreto, establezca el operando Object Name de la instrucción GSV/SSV en el nombre del módulo. El módulo especificado debe estar presente en la sección I/O Configuration del Controller Organizer y debe tener un nombre de dispositivo.

Puede obtener acceso directamente a un objeto MODULE desde una instrucción Add-On. Anteriormente, podía obtener acceso a los datos del objeto MODULE, pero no desde dentro de una instrucción Add-On.

Debe crear un parámetro Module Reference al definir la instrucción Add-On que desea que tenga acceso a los datos del objeto MODULE. Un parámetro Module Reference es un parámetro InOut del tipo de datos MODULE que apunta al objeto MODULE de un módulo de hardware. Puede utilizar los parámetros de referencia al módulo tanto en la lógica de la instrucción Add-On como en la lógica del programa.



Para obtener más información acerca del parámetro Module Reference, consulte la ayuda en línea de la aplicación Logix Designer y el documento Logix 5000 Controllers Add-On Instructions Programming Manual, publicación [1756-PM010](#).

El objeto MODULE utiliza los siguientes atributos para proporcionar información de estado:

- EntryStatus
- FaultCode
- FaultInfo
- FWSupervisorStatus
- ForceStatus
- Instance
- LEDStatus
- Mode
- Path

Monitoreo del estado del controlador

El controlador usa las instrucciones Get System Value (GSV) y Set System Value (SSV) para obtener y establecer (cambiar) los datos del controlador. El controlador almacena datos de sistema en objetos.

La instrucción GSV recupera la información especificada y la coloca en el destino. La instrucción SSV establece el atributo especificado con datos del origen. Ambas instrucciones están disponibles en la ficha Input/Output de la barra de instrucciones.

Figura 49 – Instrucciones GSV y SSV para monitoreo y establecimiento de atributos

GSV	
Class Name	?
Instance Name	?
Attribute Name	?
Dest	??

SSV	
Class Name	?
Instance Name	?
Attribute Name	?
Source	??

Al añadir una instrucción GSV/SSV al programa, se muestran las clases de objeto, los nombres de objeto y los nombres de atributo de la instrucción. En cuanto a la instrucción GSV, es posible obtener los valores de los atributos disponibles. Para la instrucción SSV, solo se muestran los atributos que es posible establecer.

Algunos tipos de objeto aparecen de forma repetida, por lo que es necesario especificar el nombre de objeto. Por ejemplo, la aplicación puede tener diversas tareas. Cada tarea tiene su propio objeto Task al cual se puede obtener acceso mediante el nombre de la tarea.

Las instrucciones GSV y SSV monitorean y establecen numerosos objetos y atributos. Consulte la ayuda en línea correspondiente a las instrucciones GSV y SSV.


Monitoreo de las conexiones de E/S

Si la comunicación con un dispositivo en la configuración de E/S del controlador no se produce en un período específico de la aplicación, la comunicación sobrepasa el tiempo de espera y el controlador produce advertencias.

El tiempo de espera mínimo, que una vez transcurrido sin comunicación, hace que se sobrepase el tiempo de espera, es 100 ms. El tiempo de espera puede ser mayor en función del RPI de la aplicación. Por ejemplo, si su aplicación utiliza el RPI predeterminado = 20 ms, el tiempo de espera es 160 ms.

Para obtener más información sobre cómo determinar el tiempo para su aplicación, busque el ID de respuesta 38535 en la Knowledgebase de Rockwell Automation®: <http://www.rockwellautomation.com/knowledgebase>.

Cuando se sobrepasa el tiempo de espera, el controlador genera estas advertencias;

- La información de estado de fallo de E/S se desplaza por la pantalla de estado de 4 caracteres del controlador.
- Aparece un icono  sobre la carpeta de configuración de E/S y sobre los dispositivos que han sobrepasado el tiempo de espera.
- Se produce un código de fallo de módulo. Puede consultar el código de fallo de las siguientes maneras:
 - El cuadro de diálogo Module Properties
 - Una instrucción GSV

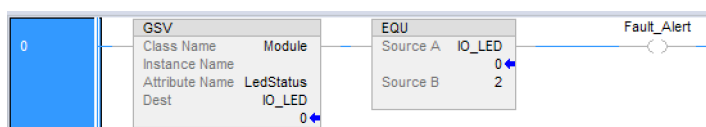
Para obtener más información acerca de los fallos de E/S, consulte el documento Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publicación [1756-PM014](#).

Determinación de si la comunicación de E/S ha sobrepasado el tiempo de espera

Este ejemplo se puede utilizar con los controladores CompactLogix 5380 o Compact GuardLogix 5380 y puede ayudar a determinar si la comunicación del controlador ha sobrepasado el tiempo de espera:

- La instrucción GSV obtiene el estado del indicador de estado I/O (mediante el atributo LEDStatus del objeto Module) y lo almacena en el tag IO_LED.
- El IO_LED es un tag DINT que almacena el estado del indicador de estado de E/S o de la pantalla de estado en la parte frontal del controlador.
- Si IO_LED es igual a 2, se ha perdido como mínimo una conexión de E/S y se establece Fault_Alert.

Figura 50 – Uso de GSV para identificar el tiempo de espera de E/S



IMPORTANTE Consideraciones de seguridad

Cada módulo de E/S de seguridad tiene un estado de conexión en el tag definido por el módulo.

Determinación de si la comunicación de E/S a un módulo de E/S específico sobrepasó el tiempo de espera

Si la comunicación sobrepasa el tiempo de espera con un dispositivo (módulo) en la configuración de E/S del controlador, el controlador produce un código de fallo e información de fallo del módulo. Puede usar las instrucciones GSV para obtener el código de fallo y la información mediante los atributos FaultCode y FaultInfo del objeto Module.

Para obtener información sobre los módulos de E/S de seguridad, vea [Monitoreo de las conexiones de seguridad en la página 269](#).

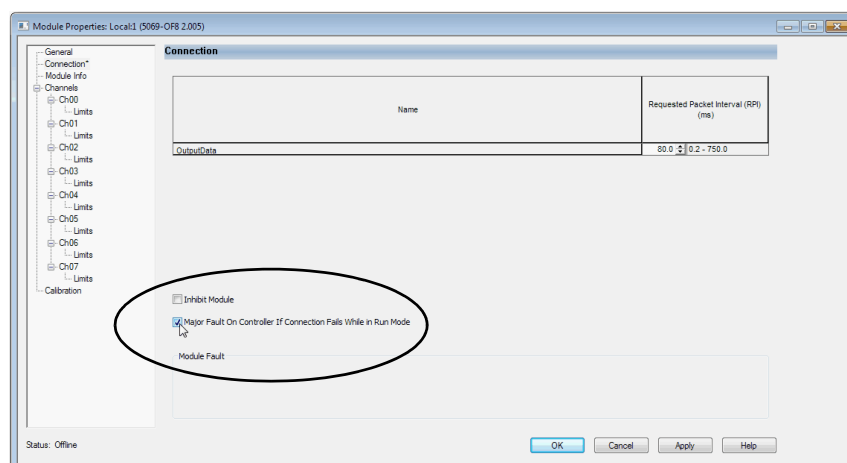
Gestión automática de fallos de conexión de módulo de E/S

Puede utilizar un error de conexión de E/S para hacer que se ejecute el gestor de fallos del controlador. Para ello, establezca la propiedad del módulo que causa un fallo mayor como resultado de un error de conexión de E/S. El fallo mayor causa la ejecución del gestor de fallos del controlador.

IMPORTANTE No puede programar las conexiones del módulo de E/S de seguridad ni las conexiones de producción/consumo de seguridad para causar un fallo mayor en el controlador de manera automática. Vea [Desarrollo de aplicaciones de seguridad en la página 241](#).

Puede ser importante interrumpir el escán del programa normal para gestionar un fallo de conexión de E/S. En este caso, establezca “Major Fault On Controller If Connection Fails While In Run Mode” y coloque la lógica en el gestor de fallos del controlador.

Figura S1 – Fallo de conexión de E/S que causa fallo mayor



Puede configurar la aplicación para que una respuesta a un fallo en la conexión del módulo de E/S pueda esperar hasta el siguiente escán del programa. En este caso, coloque la lógica en una rutina normal y utilice la técnica GSV que se describe en la [página 237](#) para llamar a la lógica.

En primer lugar, desarrolle una rutina en el gestor de fallos del controlador que pueda responder a los fallos de conexión de E/S. A continuación, en el cuadro de diálogo Module Properties del módulo de E/S o un módulo de comunicación primario, marque la casilla Major Fault On Controller If Connection Fails While in Run Mode.

SUGERENCIA La detección de una pérdida de conexión de E/S toma como mínimo 100 milisegundos, incluso cuando se utiliza el gestor de fallos del controlador.

Para obtener más información acerca de cómo programar el gestor de fallos del controlador, consulte el documento Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publicación [1756-PM014](#).

Ejemplos de proyectos de controlador

Logix Designer incluye ejemplos de proyectos que puede copiar y modificar según las necesidades de su aplicación. Para acceder a los ejemplos de proyectos, seleccione Sample Project en la interface Studio 5000®.

Figura 52 – Para abrir los ejemplos de proyectos

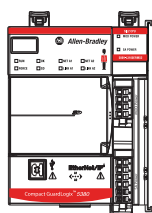


Notas:

Desarrollo de aplicaciones de seguridad

Tema	Página
Tarea de seguridad	242
Programas de seguridad	244
Rutinas de seguridad	244
Tags de seguridad	245
Tags de seguridad producidos/consumidos	247
Asignación de un tag de seguridad	256
Protección de la aplicación de seguridad	259
Generación de la firma de seguridad	262
Restricciones de programación	265
Monitoreo del estado de seguridad	266
Fallos de seguridad	272
Desarrollo de una rutina de fallo para aplicaciones de seguridad	275
Uso de las instrucciones GSV/SSV en una aplicación de seguridad	276

Compact
GuardLogix



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, como por ejemplo, la firma de seguridad y el bloqueo de seguridad.

El documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#), trata los temas siguientes:

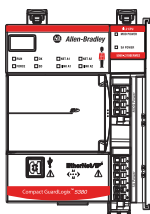
- Pautas y requisitos para desarrollar y poner en marcha las aplicaciones de seguridad SIL 2/PLd, incluyendo el uso de perfiles Add-On
- Creación de una especificación detallada del proyecto
- Escritura, documentación y prueba de la aplicación
- Generación de la firma de seguridad para identificar y ayudar a 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 una revisión independiente de seguridad en caso necesario
- Bloqueo de la aplicación de seguridad
- Cálculo del tiempo de reacción del sistema



ATENCIÓN: La realización de una modificación en línea (de lógica, datos o configuración) puede afectar las funciones de seguridad del sistema si la modificación se efectúa durante la ejecución de la aplicación. Se debe intentar realizar una modificación solo si es absolutamente necesario. Además, si la modificación no se realiza correctamente, puede interrumpir la aplicación. Por lo tanto, cuando se elimina la firma de seguridad para efectuar una edición en línea de la tarea de seguridad, antes de realizar una modificación en línea hay que implementar medidas de seguridad alternativas y estas deben estar presentes durante el período de la actualización.

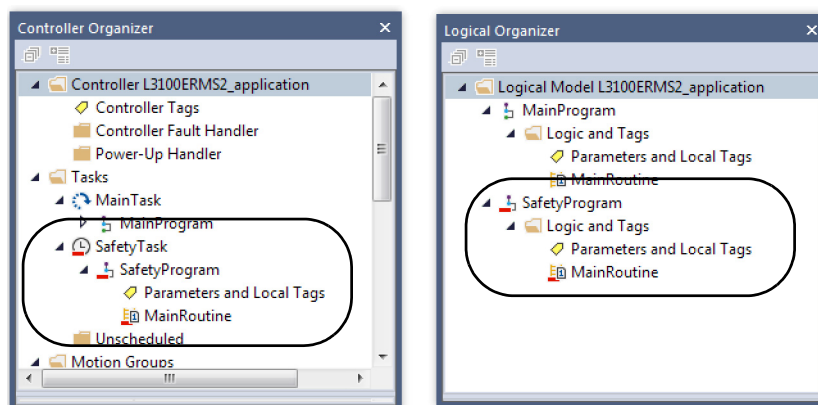
Tarea de seguridad

Compact
GuardLogix



Cuando se crea un proyecto de controlador de seguridad, la aplicación Studio 5000 Logix Designer® crea automáticamente una tarea de seguridad con un programa de seguridad y una rutina (de seguridad) principal.

Figura 53 – Tarea de seguridad en Controller Organizer y Logical Organizer



Dentro de la tarea de seguridad se pueden usar varios programas de seguridad, compuestos a su vez por varias rutinas de seguridad. Los controladores Compact GuardLogix® 5380 admiten una tarea de seguridad. La tarea de seguridad no se puede eliminar.

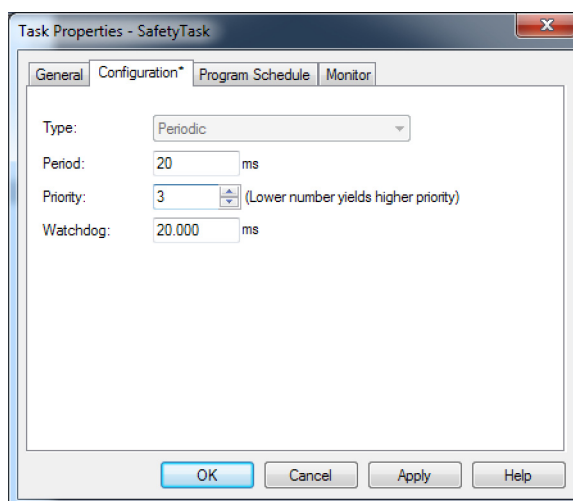
Dentro de la tarea de seguridad no se pueden secuenciar programas estándar ni ejecutar rutinas estándar.

Período de la tarea de seguridad

La tarea de seguridad es una tarea periódica temporizada. Se define la prioridad de la tarea y el tiempo del temporizador de vigilancia en el cuadro de diálogo Task Properties – Safety Task.

Para abrir el cuadro de diálogo, haga clic con el botón derecho del mouse en la tarea de seguridad y elija Properties.

Figura 54 – Configuración del período de la tarea de seguridad



Para obtener el tiempo de ejecución más uniforme de la tarea de seguridad y minimizar los fallos de temporizador de vigilancia de la tarea de seguridad, recomendamos ejecutar la tarea de seguridad como la tarea de usuario con la prioridad más alta.

Debe especificar 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 tiempo transcurrido entre los tiempos de inicio sucesivos para 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.

Para obtener más información sobre cómo calcular el tiempo de reacción del sistema, consulte el documento *Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad*, publicación [1756-RM012](#).

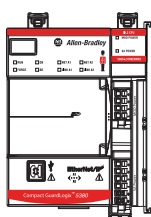
Ejecución de la tarea de seguridad

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

- 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. Para obtener más información acerca de la asignación de tags de seguridad, vea la [página 256](#).
- Los paquetes de salida de seguridad (tags producidos y módulos de salida) se generan al concluirse la ejecución de la tarea de seguridad.
- Cuando el controlador no tiene una firma de seguridad y no está en bloqueo de seguridad, se puede detener la tarea de seguridad hasta se concluya una edición en línea de un elemento de seguridad.

Programas de seguridad

Compact
GuardLogix

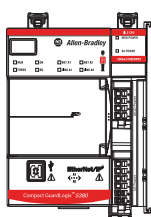


Los programas de seguridad tienen todos los atributos de los programas estándar, salvo que solo se pueden programar en la tarea de seguridad y solo pueden contener componentes de seguridad. Los programas de seguridad solo pueden contener rutinas de seguridad. Una rutina de seguridad debe definirse como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

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

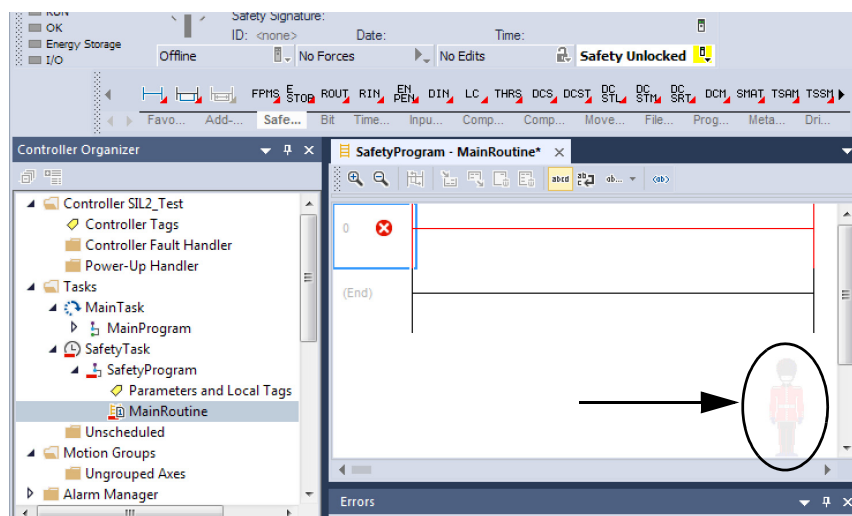
Rutinas de seguridad

Compact
GuardLogix



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

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



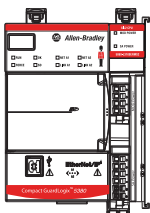
Instrucciones Add-On de seguridad

Puede crear instrucciones Add-On de seguridad para usarlas en aplicaciones de seguridad. Las instrucciones Add-On de seguridad ofrecen una firma de instrucción de seguridad que se puede utilizar en aplicaciones relacionadas con la seguridad en aplicaciones con clasificación hasta SIL 2.

Para obtener más información consulte el documento Logix 5000 Controllers Add On Instructions Programming Manual, publicación [1756-PM010](#).

Tags de seguridad

Compact
GuardLogix



Los tags de seguridad tienen todos los atributos de tags estándar además de los mecanismo certificados para proporcionar integridad de datos SIL 2/PLd.

Al crear un tag, usted asigna las siguientes propiedades.

- Nombre
- Descripción (opcional)
- Tipo de tag
- Tipo de datos
- Alcance
- Class
- Estilo
- Acceso externo
- Si el valor del tag es una constante

IMPORTANTE No puede crear un tag de alias estándar de un tag 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 256](#).

La aplicación Logix Designer puede escribir directamente a tags de seguridad directamente mediante el Tag Monitor cuando el Compact GuardLogix controlador 5380 está en desbloqueo de seguridad, no tiene una firma de seguridad y funciona sin fallos de seguridad.

El controlador no permite escribir en los datos de tag de seguridad desde dispositivos de interface operador-máquina (HMI) externos, ni mediante instrucciones de mensajes de controladores homólogos. Los dispositivos HMI pueden tener acceso de solo lectura a los tags de seguridad (depende del ajuste External Access).

Tipos de datos válidos

El tipo de datos define el tipo de datos que almacena el tag, como bit o número entero.

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 matrices o tipos de datos definidos por el usuario.

Los controladores Logix contienen tipos de datos predefinidos para utilizarse con instrucciones específicas. Los tags de seguridad pueden estar compuestos por lo siguiente:

- Todos los tipos de datos primitivos (por ejemplo, BOOL, SINT, INT, DINT, LINT, REAL)
- Tipos predefinidos que se usan para instrucciones de la aplicación de seguridad
- Tipos de datos definidos por el usuario o matrices compuestos por los dos tipos anteriores

Alcance

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

Los tags de seguridad bajo el control del controlador los pueden leer la lógica estándar o de seguridad, u otros dispositivos de comunicación, pero solo la lógica de seguridad u otro controlador de seguridad pueden escribirlos. Solo las rutinas de seguridad locales proporcionan acceso a los tags de seguridad bajo el control del programa. Estas son rutinas que residen dentro del programa de seguridad.

Al crear tags bajo el control del programa, se especifica automáticamente la clase dependiendo de si creó el tag en un programa estándar o de seguridad. Cuando se crean tags bajo el control del controlador, debe seleccionarse manualmente la clase de tag.

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

- Múltiples programas en el proyecto
- Para producir o consumir datos
- En la asignación de tags de seguridad

Para obtener más información, consulte [Asignación de un tag de seguridad en la página 256](#).

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

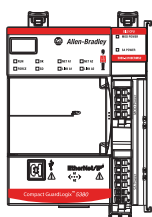
Parámetros de programa

En el caso de parámetros de programa, un parámetro de seguridad no se puede conectar ni ligar a un parámetro estándar o a un tag bajo el control del controlador.

Para obtener más información acerca de los parámetro de programa, vea [Parámetros de programa en la página 232](#).

Tags de seguridad producidos/consumidos

Compact GuardLogix



Para transferir datos de seguridad entre controladores Compact GuardLogix 5380 se utilizan tags de seguridad producidos y consumidos.

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

Tabla 27 – Conexiones producidas y consumidas

Tag	Descripción de la conexión
Producido	<p>Compact GuardLogix Los controladores 5380 pueden producir (enviar) tags de seguridad a otros controladores GuardLogix.</p> <ul style="list-style-type: none"> Compact GuardLogix Los controladores 5380 admiten solo los tags producidos por unidifusión. Compact GuardLogix Los controladores 5380 admiten la producción de un tag con un máximo de 15 consumidores si todos los consumidores se configuran para consumir la unidifusión del tag. El controlador productor utiliza una conexión para cada consumidor.
Consumido	<p>Compact GuardLogix Los controladores 5380 pueden consumir (recibir) tags de seguridad desde otros controladores GuardLogix en estas configuraciones:</p> <ul style="list-style-type: none"> Si tiene un controlador Compact GuardLogix 5380 (el productor) en el árbol de E/S de otro controlador Compact GuardLogix 5380 (el consumidor), el consumidor solo puede consumir un tag desde el productor si el tag es de unidifusión. Si el controlador productor es un controlador GuardLogix 5570, un controlador consumidor Compact GuardLogix 5380 puede consumir tags de multidifusión o unidifusión. 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 un tipos 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 productor Compact GuardLogix 5380.

Para configurar correctamente tags de seguridad producidos y consumidos a fin de intercambiar 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 en esta sección.

Configuración del SNN para una conexión del controlador de seguridad homólogo

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).

La aplicación de seguridad descargada al controlador de seguridad homólogo configura los valores SNN para cada puerto CIP Safety del controlador.

Tabla 28 – SNN y ubicación del controlador

Ubicación del controlador de seguridad homólogo	SNN
Colocado en el chasis local	La aplicación del usuario en el controlador homólogo genera un valor SNN para el puerto de backplane local del controlador.
Colocado en otro chasis	El controlador debe tener un SNN único.

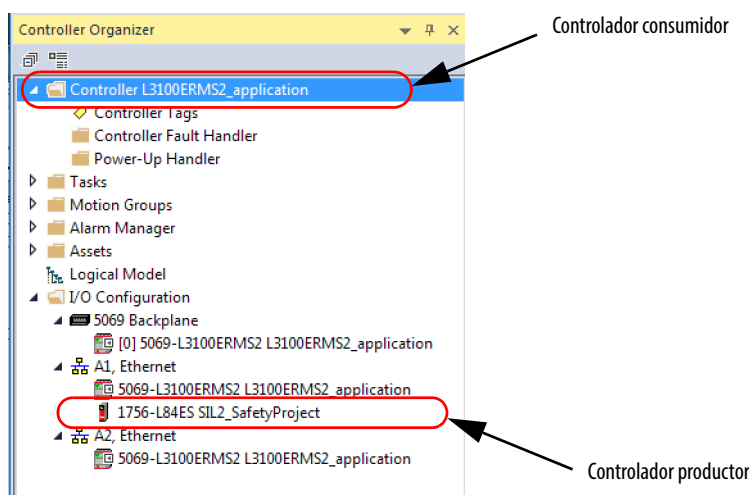
Para obtener una explicación del número de red de seguridad, consulte el documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#).

Ei el SNN automáticamente asignado del controlador productor no coincide con el SNN que el controlador utiliza, puede seguir estos pasos para copiar y pegar el SNN.

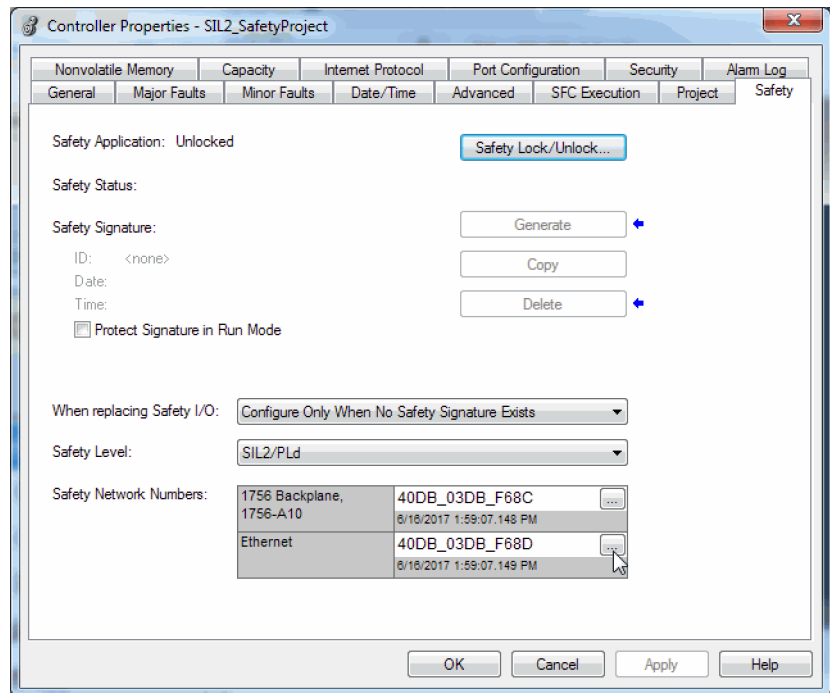
SUGERENCIA Cuando los SNN correctos del controlador se establecen según se describe en [Asignación del número de red de seguridad \(SNN\) en la página 88](#), el SNN correcto se asigna al controlador productor. En tales casos, tiene que llevar a cabo este procedimiento.

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

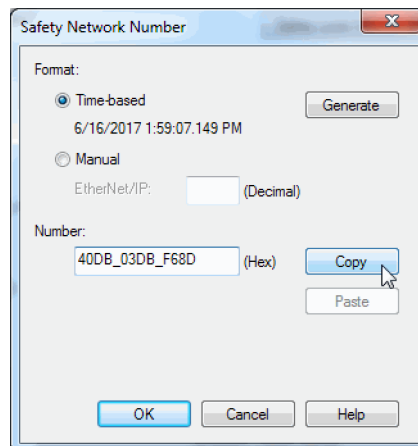
En este ejemplo, una red EtherNet/IP proporciona acceso al controlador productor mediante el puerto Ethernet A1. Establezca el SNN del puerto A1 en el mismo SNN que el SNN del puerto Ethernet de SIL2_SafetyProject.



- En el proyecto del controlador productor, haga clic con el botón derecho del mouse en el controlador productor y seleccione Controller Properties.
- En la ficha Safety, haga clic en [...] al lado del puerto (Ethernet o Backplane) que se comunica con el controlador consumidor. Esto abre el cuadro de diálogo Safety Network Number.

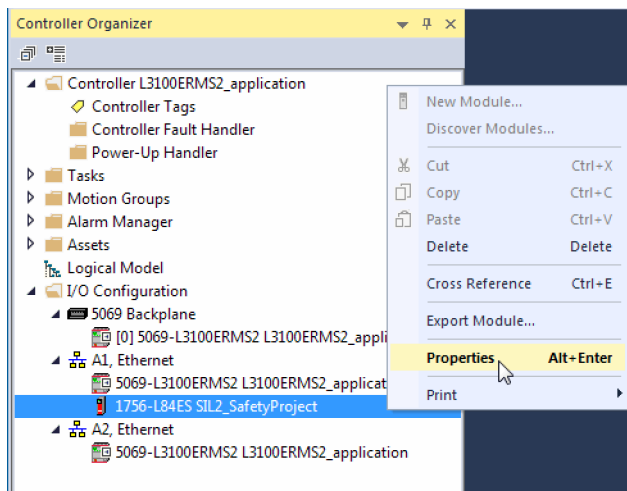



- Copie el SNN del controlador productor.

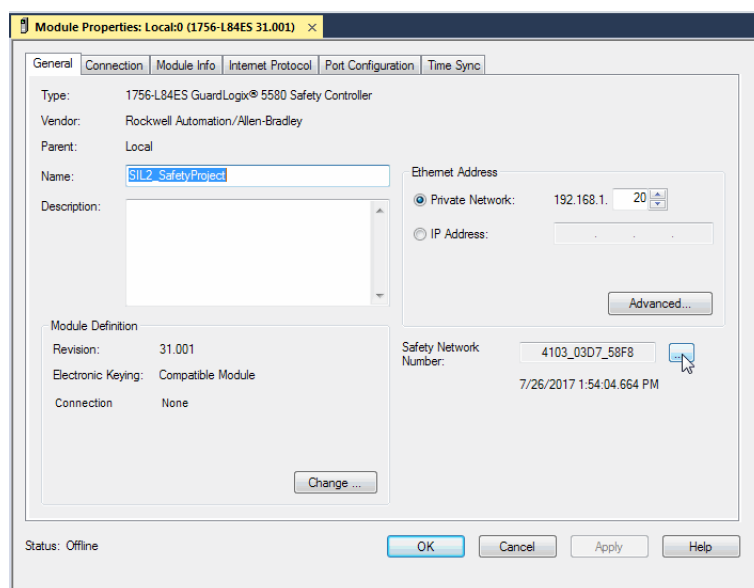


SUGERENCIA También puede copiar el SNN directamente desde la ficha Safety. En la ficha Safety, seleccione la celda con el SNN. Haga clic con el botón derecho del mouse y seleccione Copy (o presione Ctrl-C).

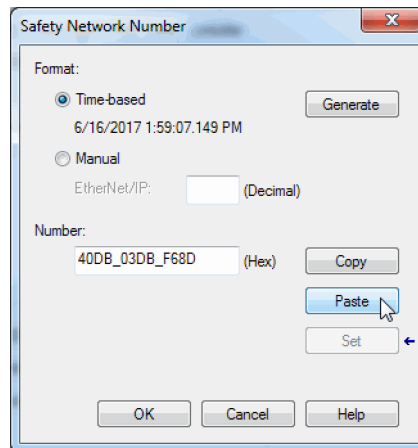
- En el árbol de E/S del proyecto del controlador consumidor, haga clic con el botón derecho del mouse en el módulo que representa el controlador productor y seleccione Properties.



- En la ficha Module Properties General, haga clic en  para abrir el cuadro de diálogo Safety Network Number.

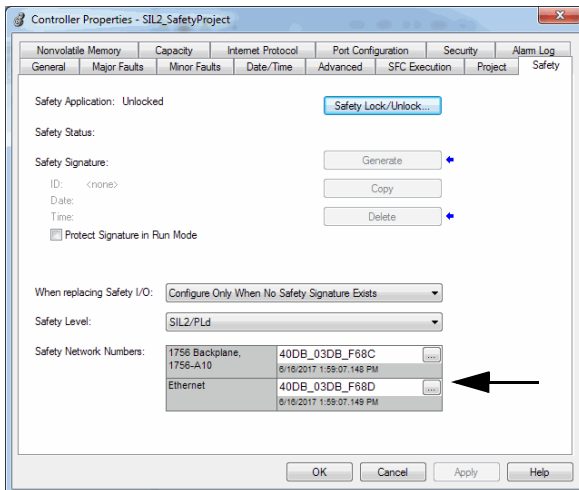


7. Pegue el SNN del controlador productor en el campo SNN y haga clic en OK.

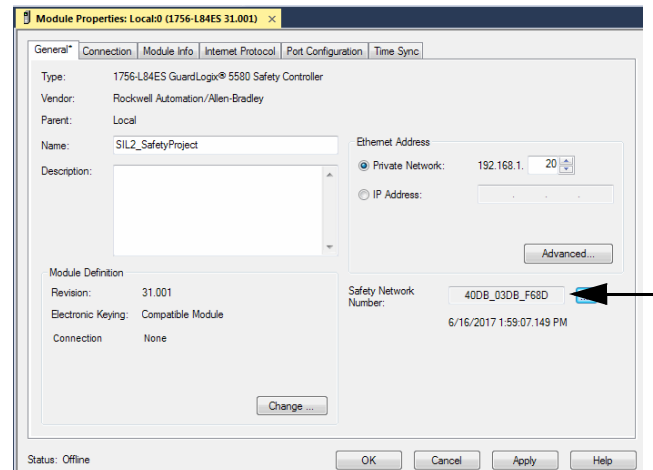


Los números de las redes de seguridad coinciden.

Cuadro de diálogo de propiedades de controlador productor en proyecto productor



Cuadro de diálogo de propiedades de módulo productor en proyecto consumidor



Producción de un tag de seguridad

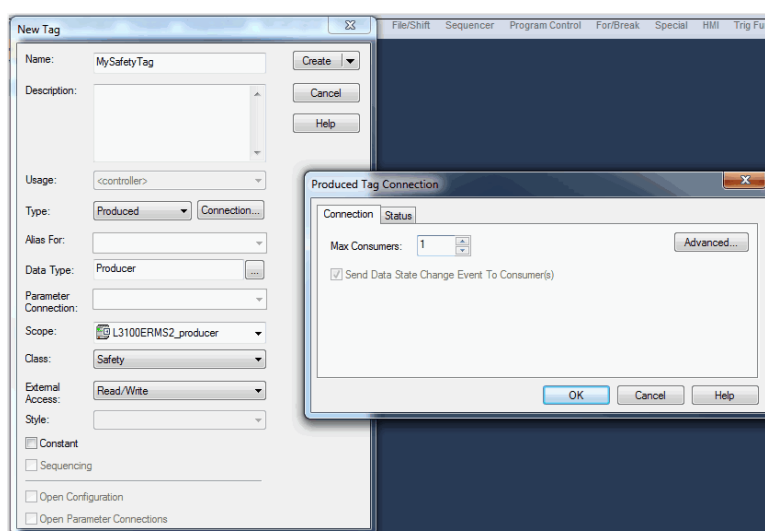
Siga estos pasos para producir un tag de seguridad.

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

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

Para obtener más información acerca del tipo de datos CONNECTION_STATUS, vea Monitoreo de las conexiones de seguridad en la [página 269](#).

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 haya creado en el [paso 1](#).
4. Haga clic en Connection para introducir el límite máx. del número de consumidores (1...15).



5. Haga clic en OK.
6. Haga clic en Create.

Consumo de datos de tag de seguridad

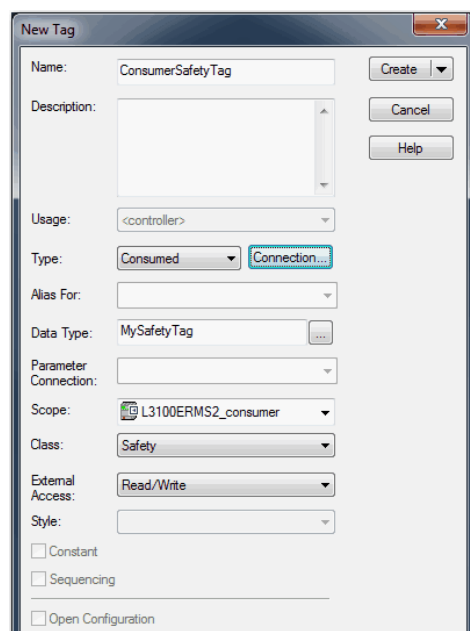
Siga estos pasos para consumir datos producidos por otro controlador.

IMPORTANTE Logix Designer no descarga un proyecto si usted intenta consumir un tag de seguridad desde un controlador remoto que tenga habilitada la inhabilitación de codificación.

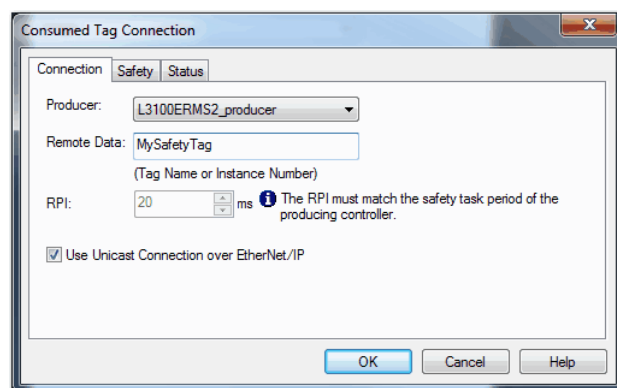
1. En el proyecto del controlador consumidor, cree un tipo de datos definido por el usuario idéntico al creado en el proyecto productor (los nombres de los tipos de datos definidos por el usuario deben coincidir).

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 haya creado en el [paso 1](#).

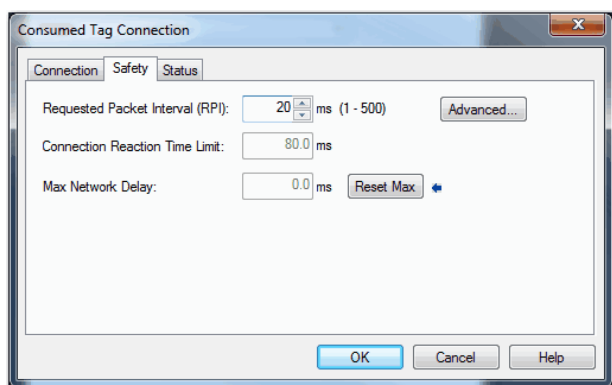


4. Haga clic en Connection para abrir el cuadro de diálogo Consumed Tag Connection.

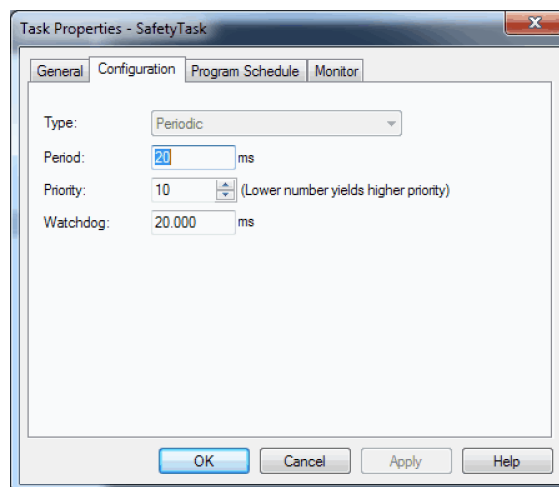


5. En los menús desplegables del productor, elija el controlador que produce los datos.
6. En el campo Remote Data, introduzca el nombre del tag producido.
7. Haga clic en la ficha Safety.
8. En el campo Requested Packet Interval (RPI), introduzca el intervalo solicitado entre paquetes para la conexión en incrementos de 1 ms. El valor predeterminado es 20 ms.
- El RPI especifica el período cuando se actualizan los datos a través de una conexión. El RPI del tag de seguridad consumido debe coincidir con el período de la tarea de seguridad del proyecto de seguridad del productor.

Proyecto consumidor



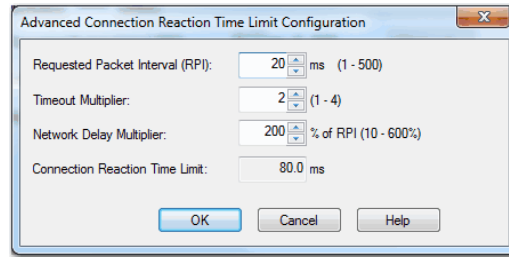
Proyecto productor



- 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 restricciones de temporización simples, puede obtener un límite de tiempo de reacción de la conexión satisfactoria ajustando el período de la tarea de seguridad del controlador productor, lo cual ajusta el RPI.
 - El retardo de red máximo es el retardo de transporte máximo observado desde que se producen los datos hasta el momento en que son recibidos. Si está trabajando en línea, haga clic en Reset Max para restablecer el retardo de red máximo.
9. Si el límite de tiempo de reacción de la conexión es satisfactorio, haga clic en OK.

SUGERENCIA Si un tag consumido de seguridad tiene el código de error: "16#0111 Requested Packet Interval (RPI) out of range", verifique que el RPI del tag consumido coincide con el período de la tarea de seguridad del productor.

10. Si su aplicación tiene requisitos más complejos, haga clic en Advanced en la ficha Safety para acceder a los parámetros de Advanced Connection Reaction Time Limit.



- El multiplicador de interrupciones determina el número de RPI que se debe esperar por un paquete hasta declarar expirado el tiempo de espera de una conexión.
- El multiplicador de retardo de red define el tiempo de transporte de mensaje aplicado 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.

Se puede utilizar el multiplicador de retardo de red para aumentar o reducir el límite de tiempo de reacción de la conexión.



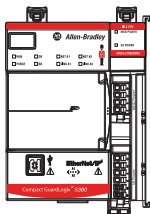
ATENCIÓN: Si usted disminuye el multiplicador de interrupciones o el multiplicador de retardo de red por debajo de los valores predeterminados, se pueden producir falsas pérdidas de conexión de seguridad. Si utiliza redes inalámbricas, podría ser necesario incrementar los valores por encima de los predeterminados.

Tabla 29 – Más recursos

Recurso	Descripción
Límite de tiempo de reacción de la conexión en la página 208	Proporciona información sobre cómo establecer el RPI y entender cómo el retardo máx. de red, el multiplicador de interrupciones y los multiplicadores de retardo de red afectan al tiempo de reacción de la conexión
Monitoreo de las conexiones de seguridad en la página 269	Contiene información acerca del tipo de datos definido previamente CONNECTION_STATUS
Logix 5000 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

Compact
GuardLogix



Una rutina de seguridad puede acceder directamente a los tags estándar. Para poder utilizar datos de un tag estándar dentro de las rutinas de la tarea de seguridad, los controladores Compact GuardLogix 5380 proporcionan una función de asignación de tag de seguridad que permite copiar valores de tag estándar en la memoria de la tarea de seguridad.

Los tags asignados se copian de los tags estándar a sus tags de seguridad correspondientes al comienzo de la tarea de seguridad. Esto puede incrementar el tiempo de escán de la tarea de seguridad.

SUGERENCIA Las rutinas de tarea estándar pueden leer directamente los tags de seguridad.

Restricciones

La asignación de tags de seguridad está sujeta a estas restricciones:

- La pareja formada por el tag de seguridad y el tag estándar deben estar bajo el control del controlador.
- Los tipos de datos de la pareja de tag de seguridad y tag estándar deben coincidir.
- No se admiten tags de alias.
- La asignación debe tener lugar a nivel de todo el tag. Por ejemplo, myTimer.pre no se admite si myTimer es un tag de temporizador (TIMER).
- Una pareja de asignación es un tag estándar asignado a un tag de seguridad.
- No se 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 seguridad.
 - El interruptor de llave se encuentra en la posición de marcha (RUN).
 - Existe un fallo de seguridad no recuperable.

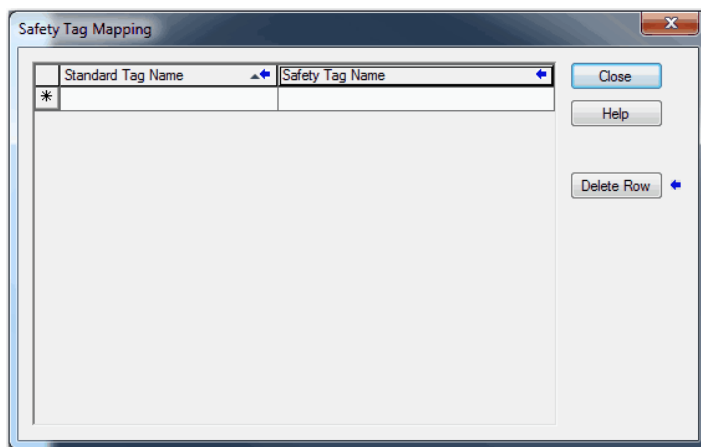


ATENCIÓN: Cuando utilice datos estándar en una rutina de seguridad, debe verificar que los datos se utilicen de manera apropiada. Usar datos estándar en un tag de seguridad no los convierte en datos de seguridad. Usted no debe controlar directamente una salida de seguridad SIL 2/PLD con datos de tag estándar.

Para obtener más información, consulte el documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#).

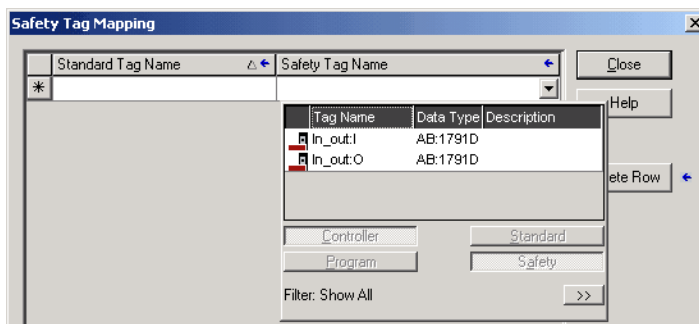
Creación de pares de asignación de tags

1. Para abrir el cuadro de diálogo Safety Tag Mapping, seleccione Map Safety Tags en el menú Logic.



2. Añada 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 de tags filtrados. Si está en la columna Standard Tag Name, el explorador solo muestra los tags estándar bajo el control del controlador. Si está en la columna Safety Tag Name, el explorador muestra los tags de seguridad bajo el control del controlador.







3. Para añadir un nuevo tag a la columna Standard Tag Name o Safety Tag Name:
 - a. Haga clic con el botón derecho del mouse en la celda vacía y seleccione New Tag.
 - b. 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 30 – Iconos de estado de asignación de 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.

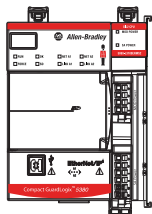
(1) La asignación de tags se comprueba también durante la verificación del proyecto. Si la asignación de un tag no es válida, se produce un error en la verificación del proyecto.

Para obtener más información, vea las restricciones de asignación de tags en la [página 256](#).

Protección de la aplicación de seguridad

Puede ayudar a proteger su programa de aplicación frente a cambios no autorizados generando una firma de seguridad, estableciendo contraseñas y poniendo el controlador en bloqueo de seguridad.

Compact
GuardLogix



Bloqueo de seguridad del controlador Compact GuardLogix 5380



ATENCIÓN: El bloqueo de seguridad por sí solo no satisface los requisitos SIL 2/PLd.

Para ayudar a evitar que se modifiquen los componentes de control relacionados con la seguridad y que se elimine erróneamente la firma de seguridad, puede poner el controlador en bloqueo de seguridad y establecer contraseñas para bloquear y desbloquear el controlador.

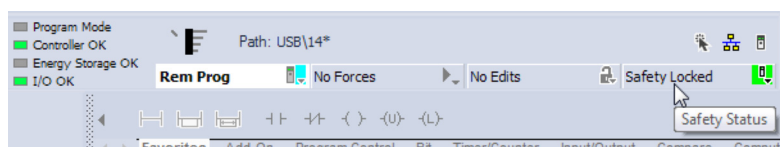
IMPORTANTE Si se configura la aplicación para realizar la carga desde la tarjeta SD al momento de encendido, se sobrescribe la aplicación en el controlador incluso si el controlador está en bloqueo de seguridad.

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 de seguridad, los tags de seguridad, las E/S de seguridad y la firma de seguridad.

Puede modificar todos los componentes estándar cuando el controlador está en bloqueo de seguridad.

SUGERENCIA Hay diversas maneras de ver el estado de bloqueo de seguridad del controlador:

- La pantalla de 4 caracteres en el controlador indica el estado de bloqueo.
- En la aplicación Logix Designer, el texto en el botón Safety Status de la barra en línea indica el estado de bloqueo de seguridad.



- En la bandeja de la aplicación Logix Designer se muestran los iconos siguientes, que indican el estado de bloqueo de seguridad del controlador de seguridad.



= bloqueo de seguridad del controlador



= desbloqueo de seguridad del controlador

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 forzosos de seguridad ni ediciones pendientes de seguridad en línea.

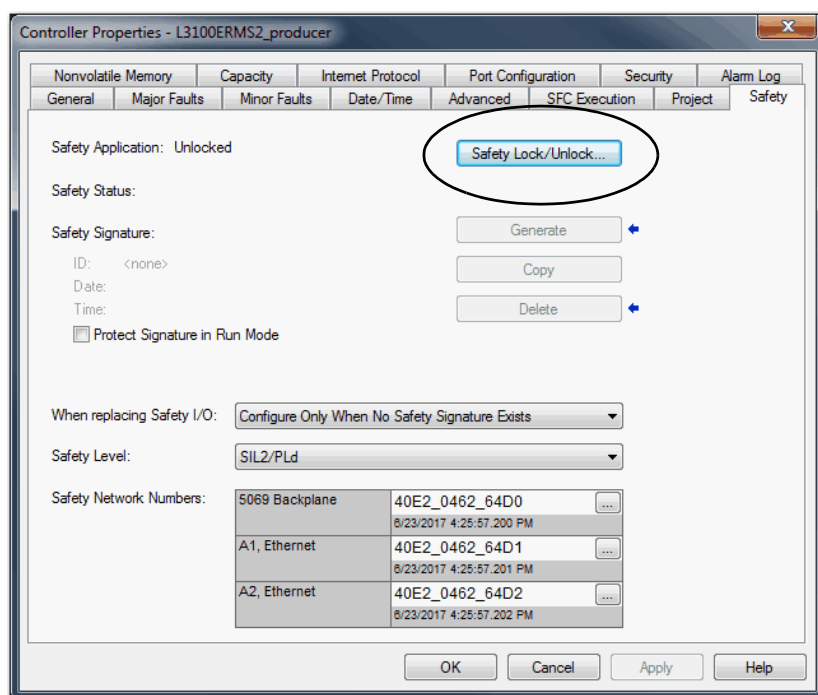
No puede cambiar el estado de bloqueo o desbloqueo de seguridad cuando el interruptor de modo del controlador está en la posición RUN.

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

Para obtener más información sobre como acceder al registro del controlador, consulte el documento Logix 5000 Controllers Controller Information and Status Programming Manual, publicación [1756-PM015](#).

Puede poner el controlador en bloqueo y desbloqueo de seguridad en la ficha Safety del cuadro de diálogo Controller Properties.

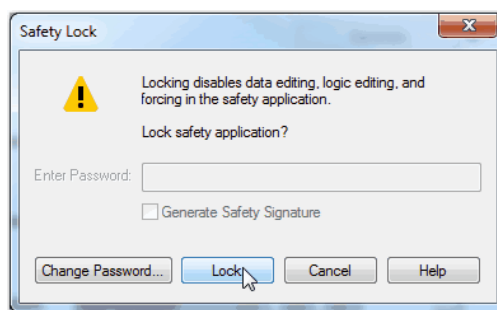
Figura 55 – Bloqueo de seguridad del controlador



SUGERENCIA En la aplicación Logix Designer, puede también seleccionar Tools > Safety > Safety Lock/Unlock.

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

Figura 56 – Bloqueo de seguridad del controlador



También puede establecer o modificar la contraseña en el cuadro de diálogo Safety Lock. Vea [Establecimiento de contraseñas para el bloqueo y desbloqueo de seguridad en la página 261](#).

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

Consulte el documento Logix 5000 Controllers Security Programming Manual, publicación [1756-PM016](#), para obtener información sobre las funciones de protección de Logix Designer.

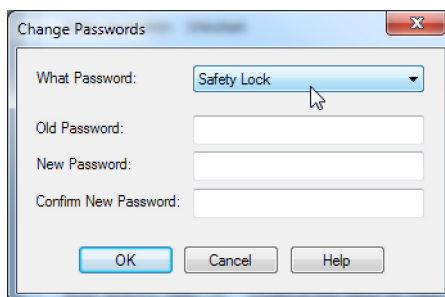
Establecimiento de contraseñas para el bloqueo y desbloqueo de seguridad

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

IMPORTANTE Rockwell Automation no ofrece ningún tipo de servicio de anulación de seguridad o de contraseña. Al configurarse los productos y las contraseñas, Rockwell Automation insta a los clientes a acatar buenas prácticas de seguridad e implementar las disposiciones necesarias para administrar contraseñas.

Siga estos pasos para establecer las contraseñas:

1. En la barra de menú Logix Designer, haga clic en Tools > Safety > Change Passwords.
2. En el menú desplegable What Password, seleccione Safety Lock o Safety Unlock.



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

SUGERENCIA Las contraseñas pueden tener de 1...40 caracteres de longitud, y no hay distinción entre mayúsculas y minúsculas. Pueden utilizarse letras, números y los símbolos siguientes: ' ~ ! @ # \$ % ^ & * () _ + , - = { } [] \ ; ? / . Para eliminar una contraseña existente, introduzca una nueva contraseña con longitud cero.

Generación de la firma de seguridad

IMPORTANTE Para generar una firma, el controlador debe estar en el modo de programación.

Antes de las pruebas de verificación, debe generar la firma de seguridad. Puede generar una firma de seguridad solo cuando existen las siguientes condiciones:

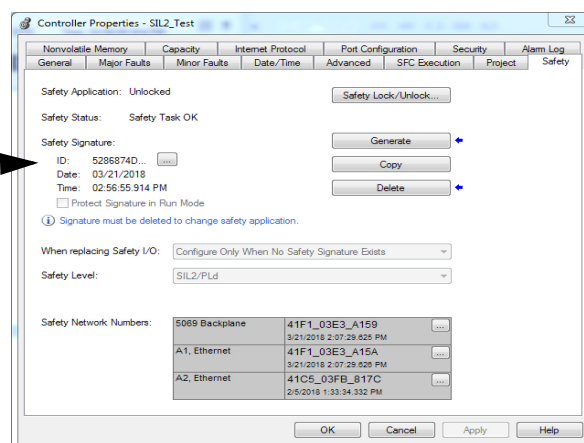
- El proyecto del controlador Compact GuardLogix 5380 con desbloqueo de seguridad está en línea.
- No hay forzados de seguridad, ediciones de seguridad en línea pendientes o fallos de seguridad.
- El estado de seguridad debe ser Safety Task OK.

SUGERENCIA Se puede ver el estado de seguridad con el botón de estado de seguridad en la barra en línea en la ficha Safety del cuadro de diálogo Controller Properties.

Para generar la firma de seguridad desde la ficha Safety del cuadro de diálogo Controller Properties, haga clic en Generate.

Figura 57 – Generación de la firma de seguridad

Con respecto a la firma de seguridad, los controladores Compact GuardLogix 5380 tienen una ID de 32 bytes. Solo los 4 primeros bytes de la ID aparecen en la ficha. Para ver y copiar toda la ID de 32 bytes, haga clic en [...] para abrir el cuadro de diálogo Safety Signature ID.



SUGERENCIA En la aplicación Logix Designer, puede seleccionar Tools > Safety > Generate Signature.

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

SUGERENCIA La creación y eliminación de la firma 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 Logix 5000 Controllers Controller Information and Status Programming Manual, publicación [1756-PM015](#).

Si existe una firma de seguridad, no se permiten estas acciones 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 los módulos de E/S de seguridad o de los controladores productores.
- Manipulación de los datos de seguridad (excepto mediante la lógica de rutina de seguridad).
- Descarga de una nueva aplicación de seguridad solo si el controlador está bloqueado.

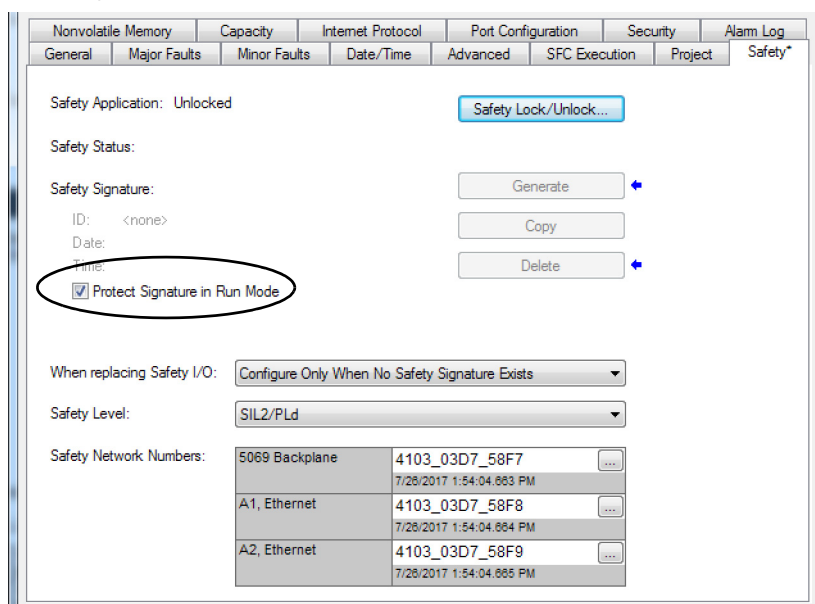
Protección de la firma de seguridad en el modo marcha

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

IMPORTANTE Hay que completar estos pasos antes de crear una firma de seguridad o poner el controlador en bloqueo de seguridad. Una vez que existe una firma de seguridad, la aplicación se pone en bloqueo de seguridad y no se puede editar la casilla de selección Protect Signature in Run Mode.

Siga estos pasos para proteger la firma de seguridad:

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



Copiado de la firma de seguridad

Se puede utilizar el botón Copy para crear un registro de la firma de seguridad y utilizarlo en la documentación, la comparación y la validación del proyecto de seguridad.

Haga clic en Copy para copiar la ID, la fecha y la hora en el portapapeles de Windows.

Eliminación de la firma de seguridad

Haga clic en Delete para eliminar la firma de seguridad. No se puede eliminar la firma de seguridad cuando lo siguiente es verdadero:

- El controlador está en bloqueo de seguridad.
- El controlador está en el modo de marcha cuando el interruptor de modo está en la posición RUN.
- El controlador está en el modo de marcha o marcha remota con la casilla Protect Signature in Run Mode habilitada.



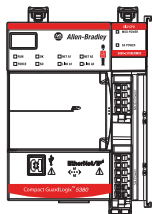
ATENCIÓN: Si elimina y genera una nueva firma de seguridad, debe volver a probar y validar el sistema para cumplir los requisitos SIL 2/PLd.

Sin una firma de seguridad, el controlador no cumple los requisitos SIL2/PLd.

Para obtener más información acerca de los requisitos del nivel de integridad de seguridad (SIL) y nivel de rendimiento (PL), consulte el documento Sistemas controladores GuardLogix 5580 y Compact GuardLogix 5380 – Manual de referencia de seguridad, publicación [1756-RM012](#).

Restricciones de programación

Compact
GuardLogix



La aplicación Logix Designer impone restricciones que limitan la disponibilidad de algunas selecciones y funciones de menú (por ejemplo, cortar, pegar, eliminar, buscar y reemplazar). Estas restricciones ayudan a proteger los componentes de seguridad frente a modificaciones cuando por lo menos una de estas condiciones es verdadera:

- El controlador está en bloqueo de seguridad.
- Existe una firma de seguridad.
- Existen fallos de seguridad.

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

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

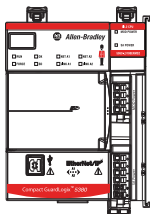
- Crear o modificar objetos de seguridad, incluidos programas de seguridad, rutinas de seguridad, tags de seguridad, instrucciones Add-On de seguridad y dispositivos de E/S de seguridad.
- Aplicar forzados a los tags de seguridad.
- Crear asignaciones nuevas de tag de seguridad.
- Modificar o eliminar 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.
- Crear, modificar o eliminar una conexión de seguridad.

Cuando el controlador está en bloqueo de seguridad, no puede modificar ni eliminar la firma de seguridad.

En el caso de un parámetro de programa, un parámetro de seguridad no se puede conectar ni ligar a un parámetro estándar o un tag bajo el control del controlador.

Monitoreo del estado de seguridad

Compact
GuardLogix



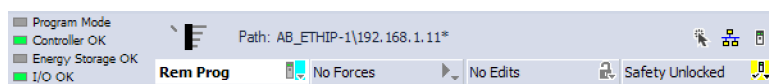
Puede utilizar lo siguiente para monitorear el estado del controlador:

- Barra en línea en la aplicación Logix Designer
- Ficha Safety en el cuadro de diálogo Controller Properties


Ver el 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 forzado, estado de edición en línea y estado de seguridad.

Figura 58 – Botones de estado




Estado del controlador


Si se selecciona el botón Controller Status  como se indicó anteriormente, la barra en línea muestra el modo del controlador (programación remota) y el estado (OK). El indicador Energy Storage OK combina el estado del controlador primario y el homólogo de seguridad.

Si uno o los dos tienen un fallo de almacenamiento de energía, se ilumina el indicador de estado. El indicador de E/S combina el estado de las E/S estándar y de seguridad. Las E/S con el estado de error más significativo se muestra al lado del indicador de estado.

Estado de forzados

El botón Forces Status  indica Forces o No Forces. Cuando se selecciona el botón, la barra en línea muestra si las E/S o los forzados SFC están habilitados, inhabilitados, instalados o no instalados. El menú ForcesStatus contiene comandos para eliminar, habilitar o inhabilitar todos los forzados.

Estado de edición en línea

El botón Online Edit Status  indica si existen o no existen ediciones en la rutina de lógica de escalera en línea o en el diagrama de bloques de funciones. Cuando se selecciona el botón, la barra en línea muestra el estado del controlador. Si otro usuario hace ediciones, esta área muestra una descripción textual de las ediciones.

Estado de seguridad


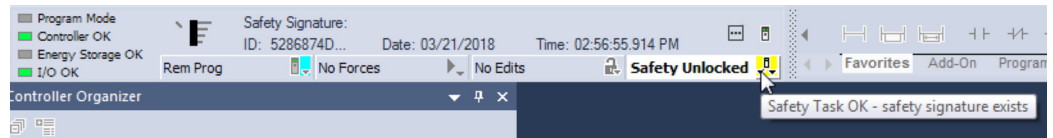
Al hacer clic en el botón Safety Status , la barra en línea muestra la firma de seguridad.

Figura 59 – 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.








Cuando existe una firma de seguridad, el icono incluye una pequeña marca de verificación. 

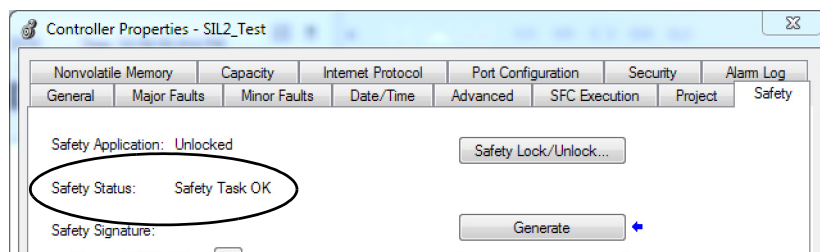
Tabla 31 – Iconos de estado de seguridad en una aplicación SIL 2/PLd, tanto en línea como fuera de línea

Si el estado de seguridad es	Aparece este icono	
Safety Unlocked		El controlador no está en bloqueo de seguridad.
Safety Locked		El controlador está en bloqueo de seguridad.
Safety Faulted		Hay un fallo de seguridad.
Safety Task Inoperable		El controlador no está en bloqueo de seguridad y la tarea de seguridad está inoperativa.
		El controlador está en bloqueo de seguridad y la tarea de seguridad está inoperativa.
		Hay un fallo de seguridad y la tarea de seguridad está inoperativa.

Visualización del estado en la ficha Safety

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

Figura 60 – Estado de seguridad



- Safety task inoperable.
- Safety Task OK.

A excepción de Safety Task OK, las descripciones indican que existen fallos de seguridad no recuperables.

Consulte [Fallos mayores de seguridad \(tipo 14\) en la página 274](#) para obtener los códigos de fallo y las acciones correctivas.

Monitoreo de las conexiones de seguridad

En el caso de tags asociados con datos de seguridad 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 E/S de seguridad tienen un miembro de estado de la conexión llamado SafetyStatus. Los dos tipos de datos contienen dos bits: ConnectionFaulted y RunMode.

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 establece en Faulted (1) por cualquier motivo, los datos de seguridad se restablecen a cero y el valor RunMode se establece en Idle State (0).

El valor RunMode indica si los datos consumidos se están actualizando activamente mediante un dispositivo que se encuentra en modo de marcha (1) o en estado inactivo (en reposo) (0). El estado inactivo 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 de programación o en el modo de prueba. En el caso de las conexiones de E/S de seguridad, RunMode siempre es el inverso del estado ConnectionFaulted. No proporciona datos únicos.

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

Tabla 32 – Estado de la conexión de seguridad

Estado ConnectionFaulted	Estado RunMode	Operación de conexión de seguridad
0 = Válido	1 = Marcha	Los datos se controlan activamente mediante el dispositivo productor. El dispositivo productor se encuentra en el modo de marcha.
0 = Válido	0 = Inactividad	La conexión está activa y el dispositivo productor está en estado inactivo. Los datos de seguridad se ponen en cero. Esto se aplica solo a las conexiones consumidas.
1 = Fallo	0 = Inactividad	La conexión de seguridad presenta un fallo. Se desconoce el estado del dispositivo productor. Los datos de seguridad se ponen en cero y el valor RunMode se establece en Idle State (0).
1 = Fallo	1 = Marcha	Estado no válido.

Si se inhibe un dispositivo, el bit ConnectionFaulted se establece en Faulted (1), mientras que el bit RunMode se establece en Idle (0) en cada una de las conexiones asociadas con el dispositivo. En consecuencia, los datos de seguridad consumidos se ponen en cero.

Utilización del estado

Connection Status(.ConnectionFaulted) es el estado de la conexión de seguridad entre el controlador de seguridad y el módulo de E/S de seguridad. Cuando la conexión funciona correctamente, el bit está LO (0). Cuando la conexión NO funciona correctamente, el bit está HI (1). Cuando el estado de conexión está HI (la conexión no funciona correctamente), todos los otros tags definidos por el módulo están LO y se deben considerar como datos “no válidos”.

El estado de punto está disponible para las entradas de seguridad (.PtxxInputStatus) y las salidas de seguridad (.PtxxOutputStatus). Cuando un tag de estado de punto está en HI (1), indica que el canal individual está funcionando y conectado correctamente, y que la conexión de seguridad entre el controlador de seguridad y el módulo de E/S de seguridad en que reside el canal funciona correctamente.

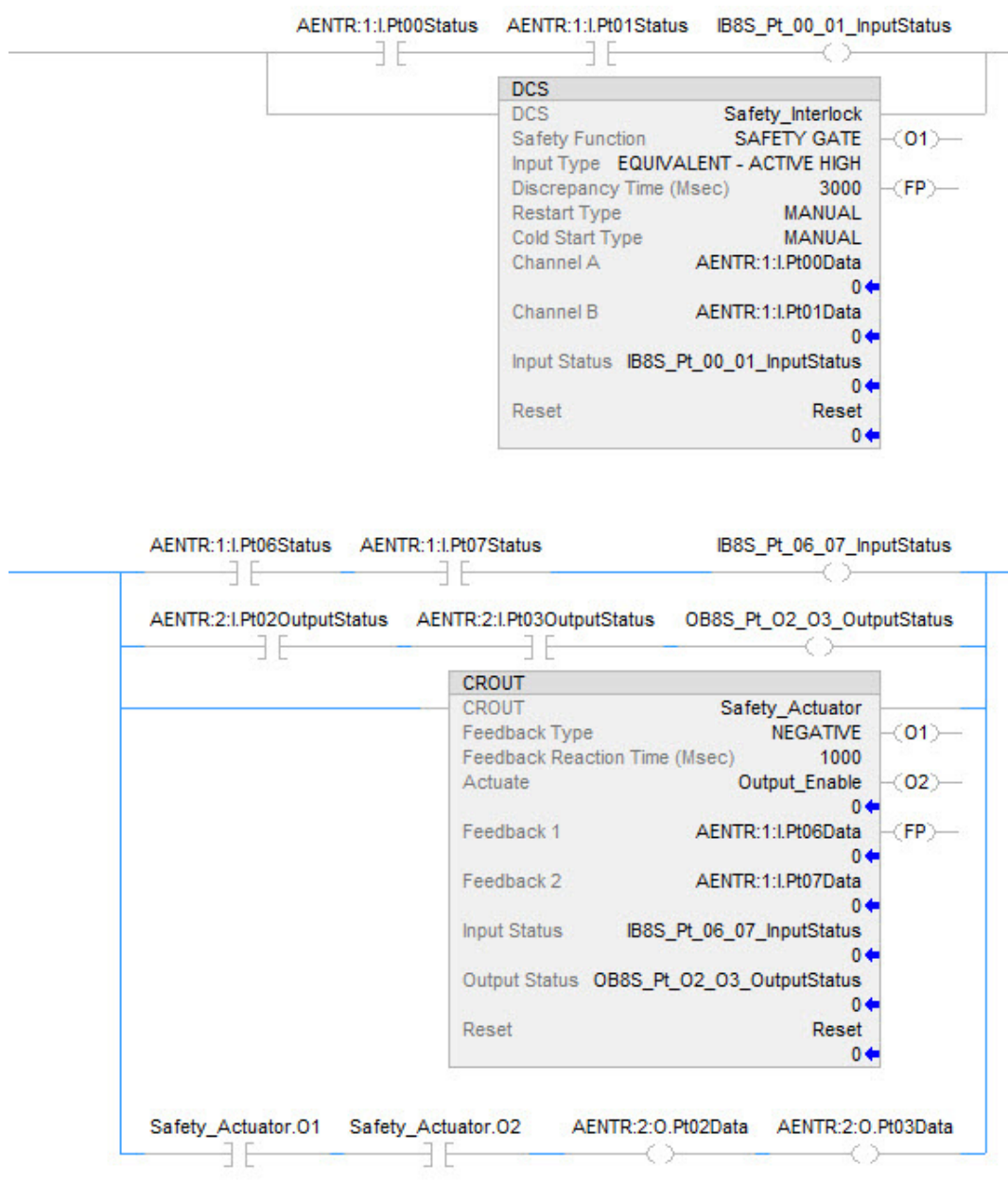
El estado combinado también está disponible para las entradas de seguridad (.CombinedInputStatus) y las salidas de seguridad (.CombinedOutputStatus). Cuando el tag de estado combinado está en HI (1), indica que todos los canales de entrada o salida en el módulo están funcionando y conectados correctamente, y que la conexión de seguridad entre el controlador de seguridad y el módulo de E/S de seguridad en que residen estos canales funciona correctamente.

El uso del estado combinado o el estado de punto depende de la aplicación. El estado de punto proporciona un estado más detallado.

Las instrucciones de seguridad de dos canales tienen monitoreo de estado de E/S de seguridad incorporado. El estado de entrada y el estado de salida son parámetros de las instrucciones de entrada y salida de seguridad. La instrucción DCS (y otras instrucciones de seguridad de dos canales) tiene el estado de entrada para los canales de entrada A y B. La instrucción CROUT tiene el estado de entrada para las retroalimentaciones 1 y 2, y tiene el estado de salida para los canales de salida controlados por las salidas CROUT O1 y O2. Los tags de estado utilizados en estas instrucciones deben estar en HI (1) para que se energicen los tags de salida de la instrucción de seguridad (O1 para las instrucciones de entrada y O1/O2 para CROUT).

Para asegurar la operación adecuada de la instrucción de seguridad, es importante controlar los tags de estado de entrada y estado de salida BEFORE/ ABOVE de la instrucción de seguridad mostrada en la [Figura 61](#).

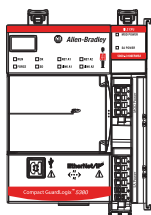
Figura 61 – Ejemplos de instrucciones



El estado de E/S de seguridad se debe interrogar al utilizar instrucciones como XIC y OTE. Esto es responsabilidad del usuario. Debe verificar que el estado del canal de entrada de seguridad está en HI (1) antes de utilizar un canal de entrada de seguridad como enclavamiento. Debe verificar que el estado del canal de salida de seguridad está en HI (1) antes de energizar un canal de salida de seguridad.

Fallos de seguridad

Compact
GuardLogix



Los fallos en el sistema Compact GuardLogix 5380 pueden ser:

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

Fallos de controlador no recuperables

Los fallos del controlador no recuperables se producen cuando falla el diagnóstico interno del controlador. Si se produce un fallo del controlador no recuperable, se detienen la ejecución de la tarea estándar y de seguridad, y se interrumpen las conexiones de salida. Los dispositivos de E/S responden ante la pérdida de datos de salida cambiando al estado de seguridad. Para la recuperación es necesario que se vuelva a descargar el programa de aplicación.

Si se produce un fallo, los datos de diagnóstico se escriben automáticamente en la tarjeta SD. Rockwell Automation puede utilizar los datos para ayudar a investigar la causa del fallo. Comuníquese con el grupo de asistencia técnica.

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 de temporizador de vigilancia de seguridad y la asociación de control se incluyen en esta categoría.

Cuando la tarea de seguridad encuentra un fallo de seguridad no recuperable, también se registra un fallo recuperable mayor estándar y el controlador ejecuta el gestor de fallos del controlador, si lo hay. Si el gestor de fallos del controlador gestiona este fallo, las tareas estándar siguen ejecutándose aunque la tarea de seguridad permanezca en el estado de fallo.



ATENCIÓN: Si anula un fallo de seguridad, no se borra dicho fallo. Si anula un fallo de seguridad, tiene la responsabilidad de demostrar que la operación de su sistema sigue siendo segura.

Deberá proporcionar prueba a la agencia certificadora de que su sistema puede seguir funcionando de manera segura tras la anulación de un fallo de seguridad.

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

- Si utiliza el botón Clear Majors o el ítem de menú Clear en Logix Designer para borrar el fallo, la aplicación estándar deberá seguir ejecutándose mientras se recupere la aplicación de seguridad desde la copia dinámica.

- Si utiliza el método de interruptor de modo (gire el interruptor de modo a Program y de regreso a Run), se recupera la aplicación de seguridad desde la copia dinámica, pero la aplicación estándar sale momentáneamente del modo marcha.

Fallos recuperables en la aplicación de seguridad

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

Cuando se borra un fallo recuperable como parte de la programación, la tarea de seguridad continúa sin interrupción.

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

Si no se maneja el fallo de seguridad recuperable, también se registra un fallo recuperable mayor estándar y el controlador ejecuta el gestor de fallos del controlador, si lo hay. Si el gestor de fallos del controlador gestiona este fallo, las tareas estándar siguen ejecutándose aunque la tarea de seguridad permanezca en el estado de fallo.

La ocurrencia de fallos recuperables es un indicio de que el código de aplicación no se está protegiendo frente a valores o condiciones de datos no válidos. Considere modificar la aplicación para eliminar estos fallos, y así no tener que enfrentarlos durante el tiempo de ejecución.



ATENCIÓN: Si anula un fallo de seguridad, no se borra dicho fallo. Si anula un fallo de seguridad, tiene la responsabilidad de demostrar que la operación de su sistema sigue siendo segura.

Deberá proporcionar prueba a la agencia certificadora de que su sistema puede seguir funcionando de manera segura tras la anulación de un fallo de seguridad.

Visualización de fallos

El cuadro de diálogo Recent Faults en 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 en controlador también muestra los códigos de fallo con un mensaje breve. Vea [Indicadores de estado en la página 307](#).

Códigos de fallo

La [Tabla 33](#) muestra los códigos de fallo específicos de los controladores Compact GuardLogix 5380. El tipo y el código corresponden al tipo y código que aparecen en la ficha Major Faults del cuadro de diálogo Controller Properties, así como en el objeto PROGRAM, atributo MAJORFAULTRECORD (o MINORFAULTRECORD).

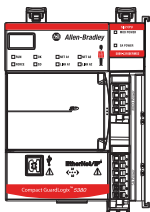
Tabla 33 – Fallos mayores de seguridad (tipo 14)

Código	Causa	Estado	Acción correctiva
01	Expiró el temporizador de vigilancia de tarea. 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 o hay una tarea de mayor prioridad que impide que concluya esta tarea.	Nonrecoverable	Borre el fallo. Si existe una firma de seguridad, la memoria de seguridad se reinicializa y la tarea de seguridad empieza a ejecutarse. Si no existe una firma de seguridad, deberá volver a descargar el programa de modo que se pueda ejecutar la tarea de seguridad.
02	Hay un error en una rutina de la tarea de seguridad.	Recoverable	Corrija el error en la lógica del programa de usuario.
07	La tarea de seguridad está inoperativa. Se produce este fallo cuando la lógica de seguridad no es válida.	Nonrecoverable	Borre el fallo. Si existe una firma 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 seguridad, se debe descargar de nuevo el programa para que la tarea de seguridad pueda ejecutarse.

El documento Logix 5000 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 para aplicaciones de seguridad

Compact
GuardLogix



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.

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



ATENCIÓN: Deberá proporcionar prueba a la agencia certificadora de que su sistema puede seguir funcionando de manera segura tras la anulación de un fallo de seguridad.

La ocurrencia de fallos recuperables es un indicio de que el código de aplicación no se está protegiendo frente a valores o condiciones de datos no válidos. Considere modificar la aplicación para eliminar estos fallos, y así no tener que enfrentarlos durante el tiempo de ejecución.

El controlador acepta dos niveles para manejar fallos mayores en una aplicación de seguridad:

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

Ambas rutinas pueden utilizar las instrucciones GSV y SSV, como se describe en la [página 276](#).

Cada programa de seguridad 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 del programa no borra el fallo o si no existe una rutina de fallo del programa, se desactivan los fallos de la tarea de seguridad.

Cuando falla la tarea de seguridad, también se registra un fallo recuperable mayor estándar y el controlador ejecuta el gestor de fallos del controlador, si lo hay. Si el gestor de fallos del controlador gestiona este fallo, las tareas estándar siguen ejecutándose aunque la tarea de seguridad permanezca en el estado de fallo.

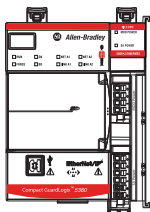
El gestor de fallos del controlador es un componente opcional que se ejecuta cuando la rutina de fallo de programa no puede borrar el fallo o cuando este no existe.

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

El documento Logix 5000 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 en una aplicación de seguridad

Compact
GuardLogix



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

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



ATENCIÓN: Utilice la instrucción SSV con cuidado. Los cambios en los objetos pueden provocar la operación inesperada del controlador o lesiones al personal.

Acceso a los atributos de FaultRecord

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

Tabla 34 – 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 u 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)

Captura de información de fallo

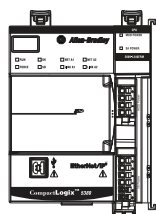
Los atributos SafetyStatus y SafetyTaskFaultRecord pueden captar información acerca de fallos no recuperables. Use una instrucción GSV en el gestor de fallos del controlador para captar y almacenar información de fallos. La instrucción GSV puede usarse en una tarea estándar junto con una rutina de gestor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

Para obtener más información acerca del uso de las instrucciones GSV y SSV en aplicaciones de seguridad, consulte el capítulo Instrucciones de entrada/salida en el documento Instrucciones generales de los controladores Logix 5000 – Manual de referencia, publicación [1756-RM003](#).

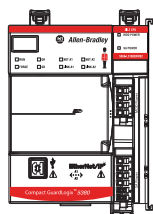
Desarrollo de aplicaciones de movimiento

Tema	Página
Descripción general del control de movimiento	278
Obtención de información de los ejes	281
Programación del control de movimiento	279

CompactLogix



Compact GuardLogix



Algunos controladores CompactLogix™ 5380 y Compact GuardLogix™ 5380 admiten movimiento integrado a través de una red EtherNet/IP en interfaces de movimiento integrado y digitales.

- Los controladores admiten estos números de ejes de movimiento integrado:

Controladores CompactLogix 5380		Controladores Compact GuardLogix 5380	
5069-L306ERM	2	5069-L306ERMS2	2
5069-L310ERM	4	5069-L310ERMS2	4
5069-L320ERM	8	5069-L320ERMS2, 5069-L320ERMS2K	8
5069-L330ERM	16	5069-L330ERMS2, 5069-L330ERMS2K	16
5069-L340ERM	20	5069-L340ERMS2	20
5069-L350ERM	24	5069-L350ERMS2, 5069-L350ERMS2K	24
5069-L380ERM	28	5069-L380ERMS2	28
5069-L3100ERM	32	5069-L3100ERMS2	32

- Las interfaces de variadores digitales incluyen variadores conectados a EtherNet/IP.
- El movimiento integrado a través de una red EtherNet/IP acepta algunos variadores Kinetix® y algunos variadores PowerFlex®. Por ejemplo, Kinetix 5700 y PowerFlex 755.
- Todos los controladores CompactLogix 5380 y Compact GuardLogix 5380 admiten control de motores de un solo eje con variadores de frecuencia variable PowerFlex a través de una red EtherNet/IP.

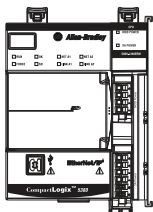
Esta funcionalidad está disponible en los controladores CompactLogix 5380 y Compact GuardLogix 5380 que no admiten otros aspectos del movimiento integrado a través de una red EtherNet/IP.

Para obtener más información, consulte:

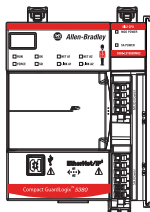
- Configuración y puesta en marcha del movimiento integrado en la red Ethernet/IP – Manual del usuario, publicación [MOTION-UM003](#).
- Movimiento integrado en la red EtherNet/IP – Manual de referencia, publicación [MOTION-RM003](#).

Descripción general del control de movimiento

CompactLogix



Compact GuardLogix



Los controladores admiten hasta 256 ejes de movimiento integrado. Los 256 ejes pueden ser cualquier combinación de ejes CIP, virtuales y consumidos. Puede añadir todos los ejes a un grupo de movimiento y puede asignar cualquier combinación de ejes a programas de actualización de ejes diferentes. Puede asociar ejes de movimiento integrado a cualquier variador adecuado.

Los controladores no admiten movimiento analógico o SERCOS.

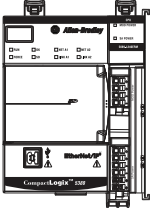
El proceso de configuración varía según la selección de aplicación y variador. Los siguientes son pasos generales para configurar una aplicación de movimiento.

1. Cree un proyecto de controlador.
2. Seleccione el tipo de variador.
3. Cree los tags de eje en caso necesario.
4. Configure el variador.
5. Cree ejes en caso necesario.

Programación del control de movimiento

El controlador proporciona un conjunto de instrucciones de control de movimiento para los ejes:

CompactLogix



Compact GuardLogix



- El controlador utiliza estas instrucciones de la misma manera que el resto de las instrucciones Logix 5000™.
- Cada instrucción de movimiento funciona en uno o varios ejes.
- Puede utilizar instrucciones de control de movimiento en estos lenguajes de programación:
 - Diagrama de lógica de escalera (LD)
 - Texto estructurado (ST)
 - Diagrama de funciones secuenciales (SFC)
- Cada instrucción de movimiento necesita un tag de control de movimiento. El tag utiliza un tipo de datos `MOTION_INSTRUCTION` y almacena el estado de la información de la instrucción.

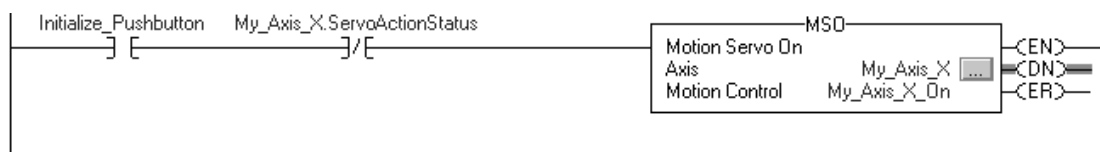
Para obtener más información, consulte el documento Logix 5000 Controller Motion Instructions Reference Manual, publicación [MOTION-RM002](#).



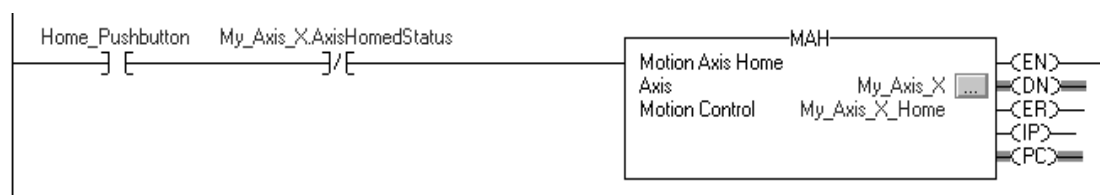
ATENCIÓN: Utilice cada tag de control de movimiento en solo una instrucción de movimiento. Puede producirse una operación inesperada si reutiliza el mismo tag de control de movimiento en otras instrucciones de movimiento o si escribe en cualquiera de los elementos del tag de control de movimiento.

En este ejemplo, veremos un simple diagrama de lógica de escalera que regresa un eje a la posición inicial, lo impulsa y lo mueve.

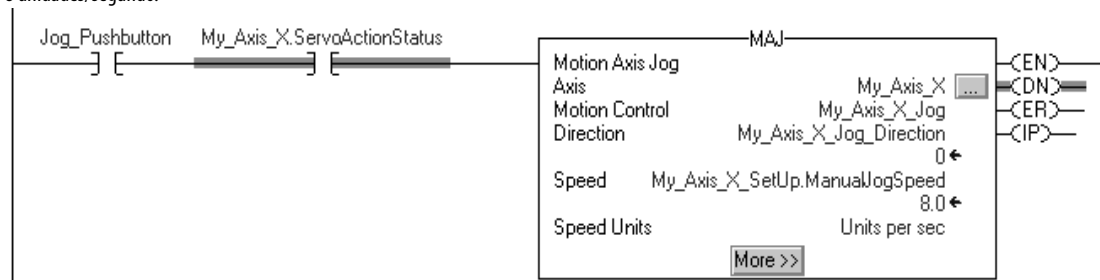
Si Initialize_Pushbutton = activado y el eje = desactivado (My_Axis_X.ServoActionStatus = desactivado), la instrucción MSO activa el eje.



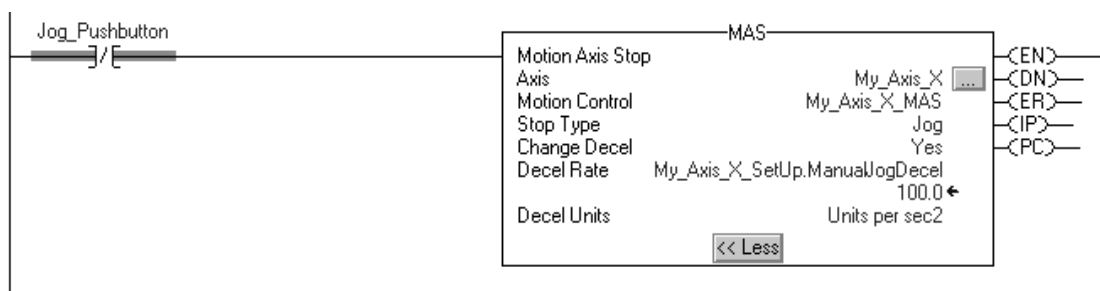
Si Home_Pushbutton = activado y el eje no ha regresado a la posición inicial (My_Axis_X.AxisHomedStatus = desactivado), la instrucción MAH regresa el eje a la posición inicial.



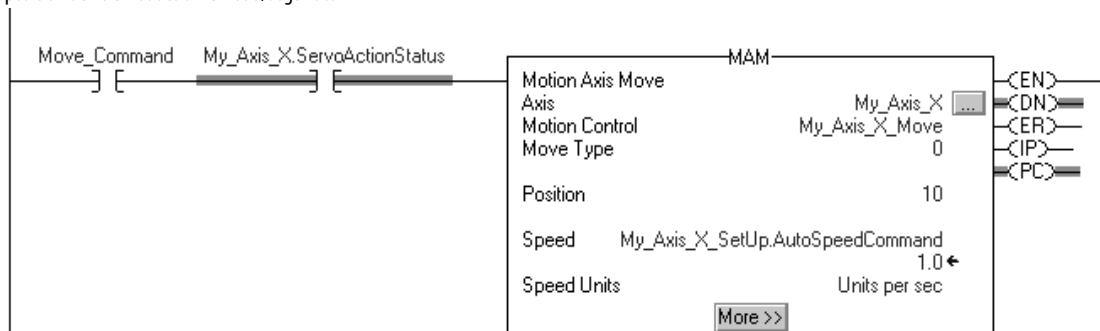
Si Jog_Pushbutton = activado y el eje = activado (My_Axis_X.ServoActionStatus = activado), la instrucción MAJ impulsa el eje hacia adelante a 8 unidades/segundo.



Si Jog_Pushbutton = desactivado, la instrucción MAS detiene el eje a 100 unidades/segundo². Asegúrese de que Change Decel esté en Yes. De no hacerlo, el eje se desacelera a su velocidad máxima.



Si Move_Command = activado y el eje = activado (My_Axis_X.ServoActionStatus = activado), la instrucción MAM mueve el eje. El eje se mueve a la posición de 10 unidades a 1 unidad/segundo.



Obtención de información de los ejes

Puede obtener información de los ejes mediante estos métodos:

- Haga doble clic en el eje para abrir el cuadro de diálogo Axis Properties.
- Utilice una instrucción Get System Value (GSV) o Set System Value (SSV) para leer o cambiar la configuración en tiempo de ejecución.
- Consulte la sección de ventana Quick View para ver el estado y los fallos de un eje.
- Utilice un tag de eje para conocer el estado y los fallos.

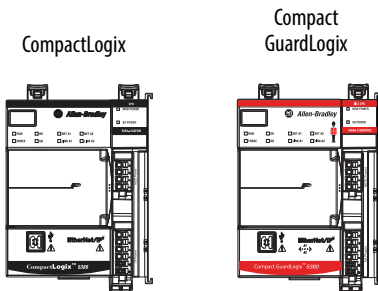
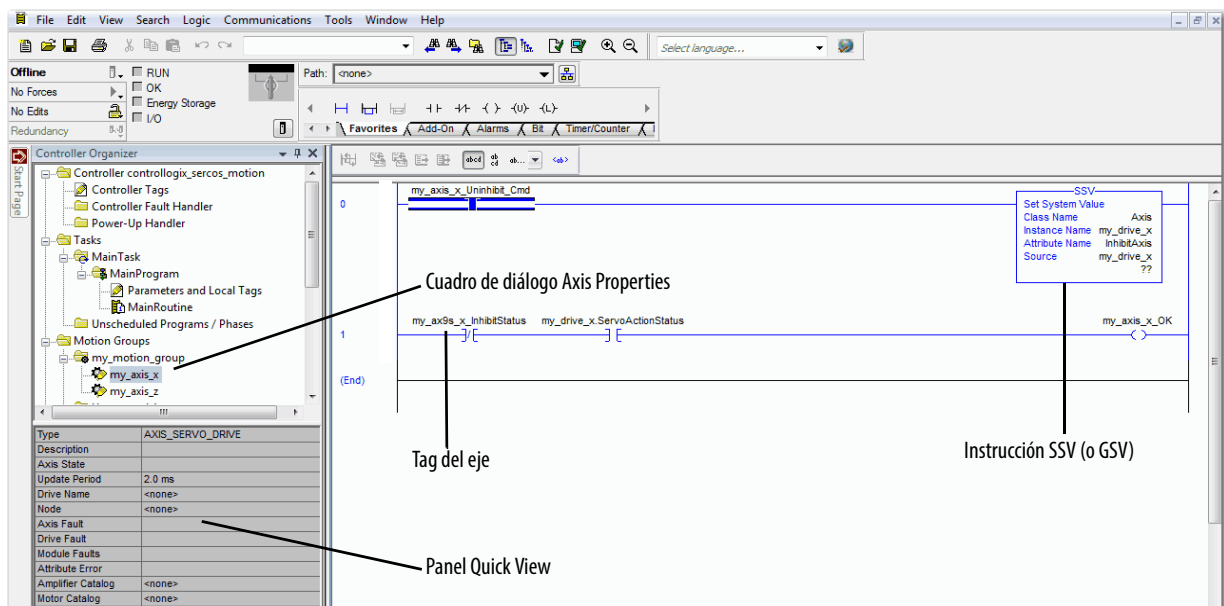


Figura 62 – Obtención de información de los ejes



Notas:

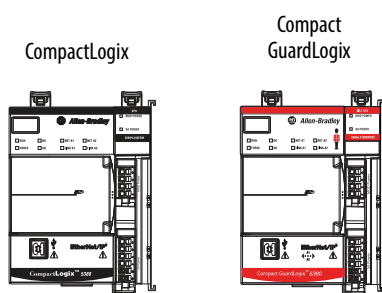
Resolución de problemas del controlador

Tema	Página
Diagnóstico del controlador con Logix Designer	283
Diagnóstico de controlador con software basado en Linx	296
Páginas web del controlador	297
Otros posibles problemas que puede ser necesario resolver	305

Este capítulo describe cómo resolver problemas del controlador si se produce cualquier incidente durante el funcionamiento normal.

Puede utilizar los mensajes en la pantalla de 4 caracteres para resolver problemas del controlador. Para obtener más información, vea el Apéndice A, [Indicadores de estado en la página 307](#).

Diagnóstico del controlador con Logix Designer



Puede utilizar Controller Properties en la aplicación Studio 5000 Logix Designer® para ver las condiciones de fallo de las maneras siguientes:

- [Símbolo de advertencia en el árbol de configuración de E/S](#)
- [Categorías del cuadro de diálogo I/O Module Properties](#)
- [Notificación en el Tag Monitor](#)
- [Información de fallo en el cuadro de diálogo Controller Properties](#)
- [Diagnóstico de puertos](#)
- [Advanced Time Sync](#)

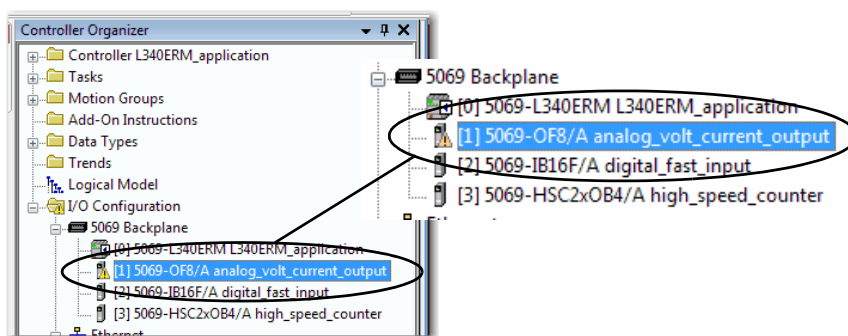
Símbolo de advertencia en el árbol de configuración de E/S

IMPORTANTE Consideraciones de seguridad

No puede configurar las conexiones de seguridad para que presenten automáticamente un fallo de controlador.

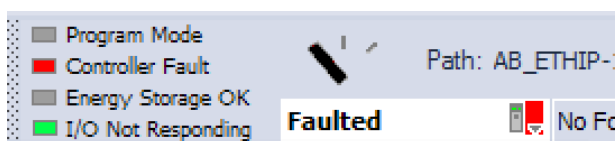
Aparece un símbolo de advertencia en el Controller Organizer al lado del módulo de E/S. Esto ocurre cuando hay fallos u otras condiciones en el módulo de E/S, o si la conexión al módulo de E/S falla en el modo de marcha.

Figura 63 – Símbolo de advertencia en el módulo de E/S



Las condiciones posibles son las siguientes:

- Cuando el módulo de E/S está configurado para que se produzca un fallo mayor en el controlador y se produce un fallo en el módulo de E/S, puede ocurrir lo siguiente:
 - El estado del controlador indica Faulted.
 - El estado del controlador muestra Controller Fault y está rojo fijo.
 - El estado del módulo de E/S muestra I/O Not Responding y parpadea de color verde.

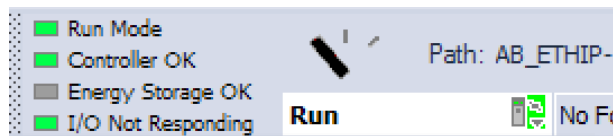


IMPORTANTE Las descripciones de la aplicación Logix Designer pueden cambiar dependiendo del modo y el estado del controlador.

IMPORTANTE Consideraciones de seguridad

No puede configurar las conexiones de seguridad para que presenten automáticamente un fallo de controlador.

- Cuando el módulo de E/S no está configurado para que se produzca un fallo mayor en el controlador y se produce un fallo en el módulo de E/S, ocurre lo siguiente:
 - El estado del controlador muestra el estado actual, por ejemplo, Rem Run.
 - El estado del controlador muestra Controller OK y está verde fijo.
 - El estado del módulo de E/S muestra I/O Not Responding y parpadea de color verde.



Categorías del cuadro de diálogo I/O Module Properties

El cuadro de diálogo Module Properties de los módulos de E/S incluye varias categorías. Puede utilizar algunas de las categorías para resolver los problemas del controlador.

IMPORTANTE El número y el tipo de categorías cambian según el tipo de módulo de E/S.

A continuación, puede ver varios ejemplos de maneras de utilizar las categorías del cuadro de diálogo Module Properties para resolver los problemas de un controlador:

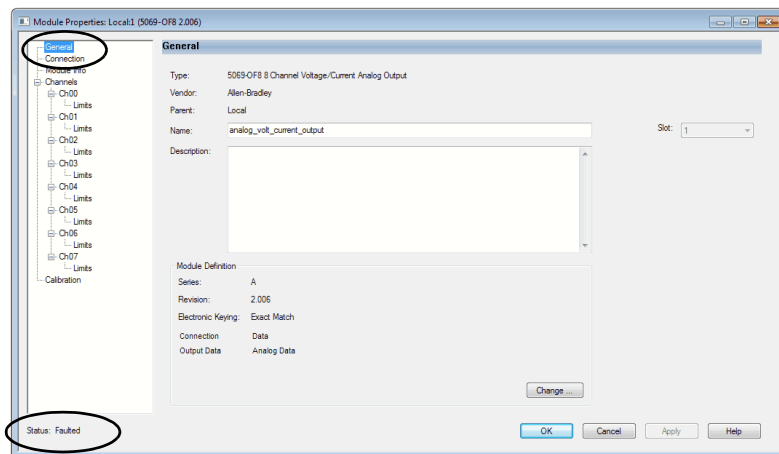
- [Estado de módulo en la categoría General](#)
- [Descripciones de fallo del módulo en la categoría Connection](#)
- [Descripción de los fallos del módulo en la categoría Module Info](#)
- [Opción Diagnostics en la categoría Module Info](#)

Las categorías que se describen en esta sección muestran el estado del módulo. Cuando hay un fallo, aparece el texto **Status: Faulted** en la línea de estado del módulo tal como se muestra en la [Figura 64](#).

Estado de módulo en la categoría General

La categoría General muestra el estado del módulo.

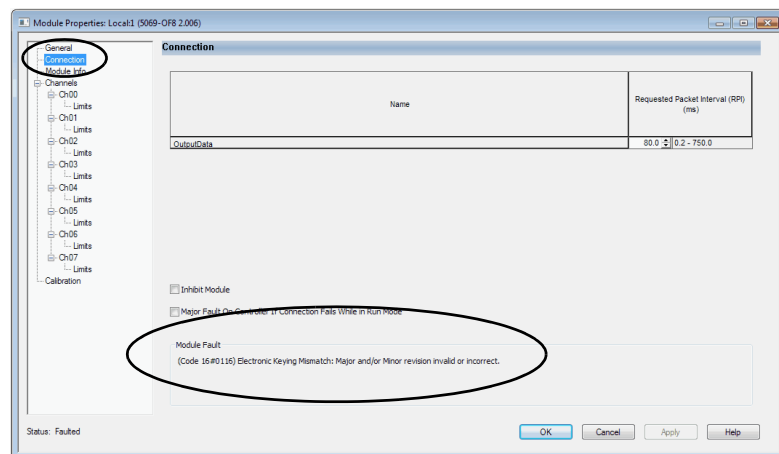
Figura 64 – Estado del módulo en línea de mensaje de fallo



Descripciones de fallo del módulo en la categoría Connection

La categoría Connection muestra una descripción del fallo del módulo que incluye un código de error asociado con el tipo concreto de fallo.

Figura 65 – Descripción del fallo con código de error



Descripción de los fallos del módulo en la categoría Module Info

Al hacer clic en la categoría Module Info, un cuadro de diálogo muestra la descripción del fallo del módulo y el correspondiente código de fallo. Haga clic en OK para consultar la categoría Module Info.

SUGERENCIA

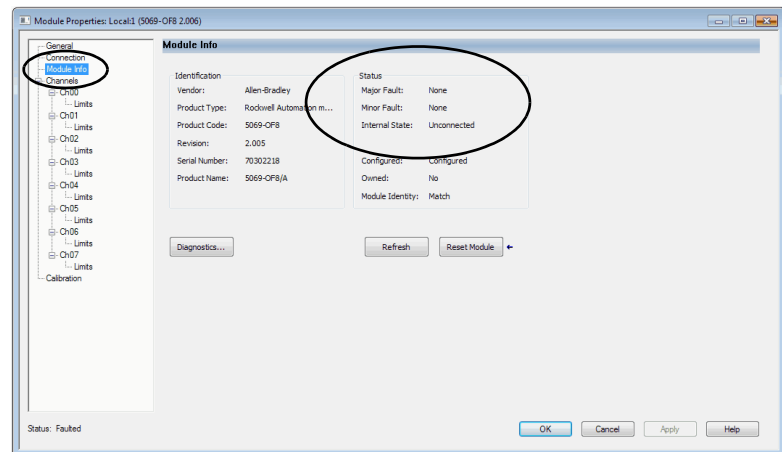
La ficha Module Info requiere que se haya establecido correctamente la comunicación para ayudar a solucionar eficazmente un fallo. Tenga en cuenta lo siguiente:

- Si la comunicación con el módulo de E/S es correcta pero el módulo presenta un fallo, le recomendamos que utilice la categoría Module Info para resolver el fallo.
- Si la comunicación con el módulo de E/S presenta un fallo, le recomendamos que utilice la categoría Connection para resolver el fallo.

En la categoría Module Info, la sección Status muestra los siguientes datos acerca del módulo de E/S:

- Fallos mayores y menores
- Estado interno

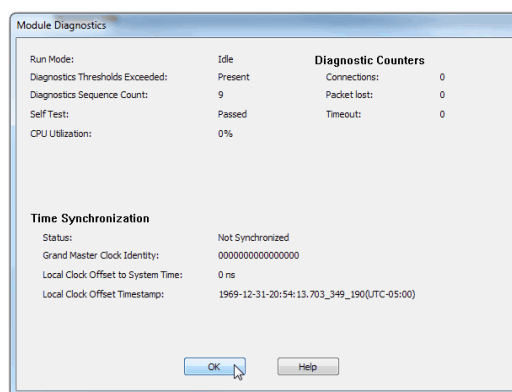
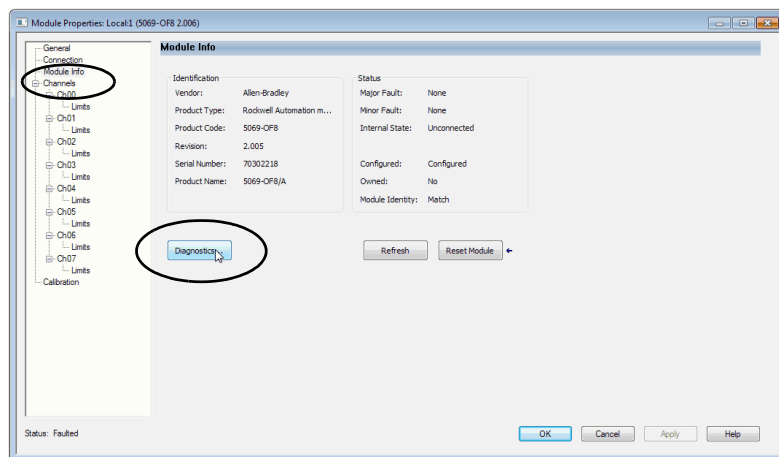
Figura 66 – Información sobre fallos mayores y menores



Opción Diagnostics en la categoría Module Info

Puede acceder al diagnóstico de un módulo mediante la categoría Module Info. Haga clic en Diagnostics para abrir el cuadro de diálogo Module Diagnostics.

Figura 67 – Module Diagnostics



Notificación en el Tag Monitor

Los fallos generales y de diagnóstico del módulo aparecen en el Tag Monitor del proyecto de la aplicación Logix Designer.

El campo Value indica un fallo con el número 1.

Name	Value	Force Mask	Style	Data Type
Local:1:C	{...}	{...}		AB:5000_AO8:C:0
Local:1:1	{...}	{...}		AB:5000_AO8:I:0
Local:1:1.RunMode	0		Decimal	BOOL
Local:1:1.ConnectionFaulted	1		Decimal	BOOL
Local:1:1.DiagnosticActive	1		Decimal	BOOL
Local:1:1.DiagnosticSequenceCount	9		Decimal	SINT
Local:1:1.Ch00	{...}	{...}		CHANNEL_AO_D...
Local:1:1.Ch00.Fault	1		Decimal	BOOL
Local:1:1.Ch00.Unloadain	0		Decimal	BOOL

Información de fallo en el cuadro de diálogo Controller Properties

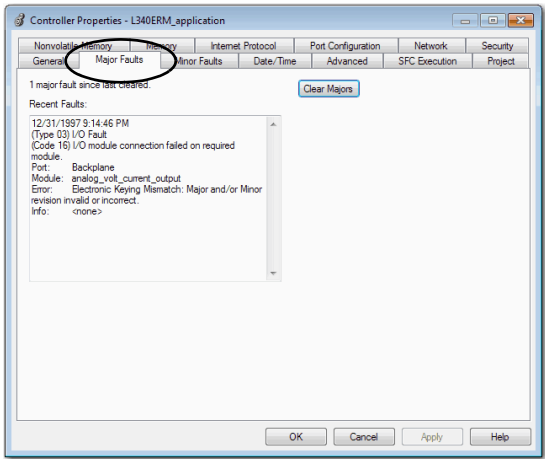
Puede utilizar estas fichas del cuadro de diálogo Controller Properties para resolver los problemas del controlador:

- [Major Faults](#)
- [Minor Faults](#)
- [Network](#)

Major Faults

Puede monitorear la información acerca de los fallos mayores y también borrarlos mediante la ficha Major Faults.

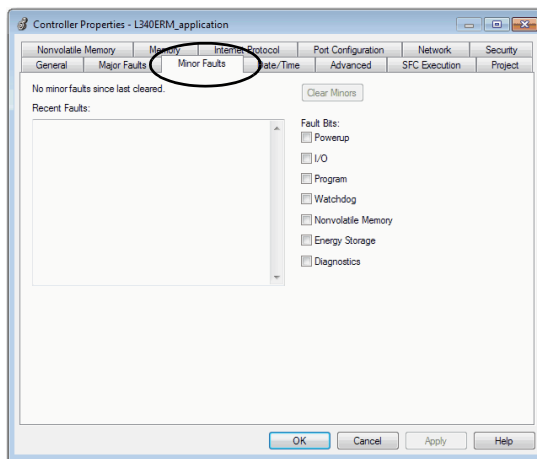
Figura 68 – Ficha Major Faults en el cuadro de diálogo Controller Properties



Minor Faults

Puede monitorear la información acerca de los fallos menores y también borrarlos mediante la ficha Minor Faults.

Figura 69 – Ficha Minor Faults en el cuadro de diálogo Controller Properties

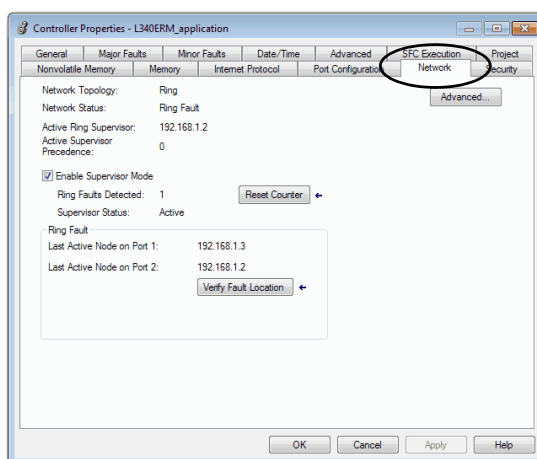


Network

Normalmente, la ficha Network se utiliza para monitorear los fallos que se producen cuando el controlador se utiliza en una red DLR.

IMPORTANTE La ficha Network no está disponible cuando el controlador funciona en modo de doble IP.-

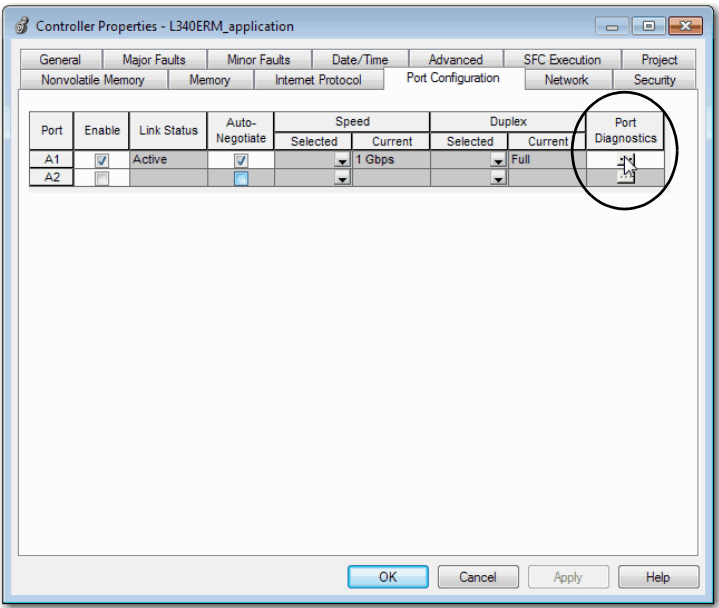
Figura 70 – Ficha Network Tab en el cuadro de diálogo Controller Properties



Diagnóstico de puertos

Cuando el proyecto está en línea, puede ver el estado de los puertos Ethernet incorporados en el controlador.

- 1. Acceda a las propiedades del controlador.
- 2. Haga clic en la ficha Port Configuration.
- 3. En la ficha Port Configuration, haga clic en el botón Port Diagnostics correspondiente a un puerto activo.



La página Port Diagnostics muestra la información sobre el puerto. Consulte la [Tabla 35 en la página 292](#) para leer las descripciones de los parámetros.

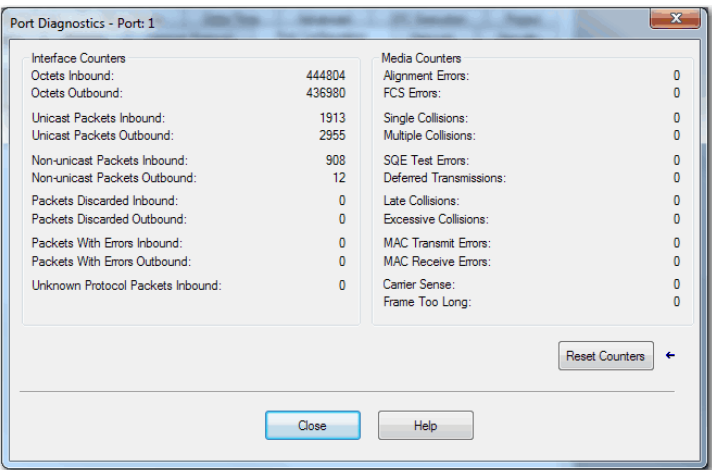


Tabla 35 – Parámetros de diagnóstico de los puertos – Logix Designer

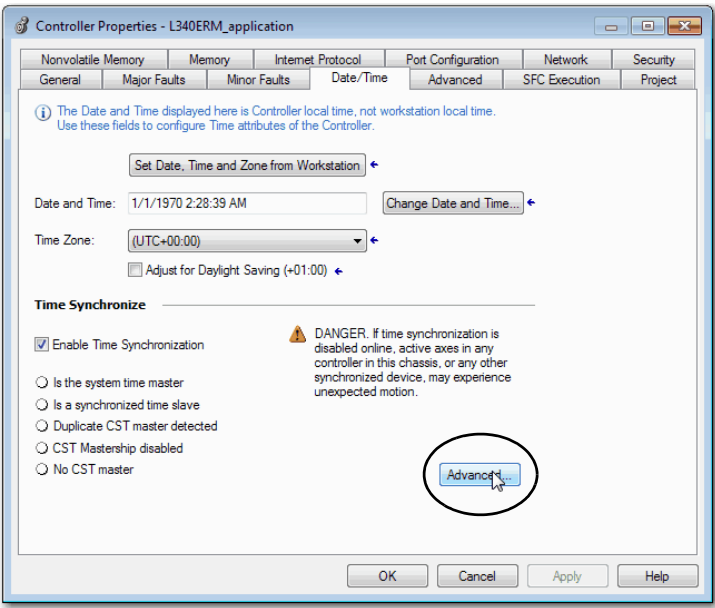
Parámetro	Descripción
Interface Counters	Los valores de Interface Counters no tienen valor cuando no puede comunicarse desde el puerto.
Octets Inbound	Muestra el número de octetos que se reciben por la interface.
Octets Outbound	Muestra el número de octetos que se transmiten por la interface.
Unicast Packets Inbound	Muestra el número de paquetes de unidifusión que se reciben por la interface.
Unicast Packets Outbound	Muestra el número de paquetes de unidifusión que se transmiten por la interface.
Non-unicast Packets Inbound	Muestra el número de paquetes no de unidifusión que se reciben por la interface.
Non-unicast Packets Outbound	Muestra el número de paquetes no de unidifusión que se transmiten por la interface.
Packets Discarded Inbound	Muestra el número de paquetes entrantes que se reciben por la interface pero se descartan.
Packets Discarded Outbound	Muestra el número de paquetes salientes que se transmiten por la interface pero se descartan.
Packets With Errors Inbound	Muestra el número de paquetes entrantes que contienen errores (no se incluyen los paquetes entrantes descartados).
Packets With Errors Outbound	Muestra el número de paquetes salientes que contienen errores (no se incluyen los paquetes salientes descartados).
Unknown Protocol Packets Inbound	Muestra el número de paquetes entrantes con un protocolo desconocido.
Media Counters	Los contadores de medios no tienen ningún valor cuando usted está fuera de línea, o cuando está en línea y se produce un error de comunicación.
Alignment Errors	Muestra el número de tramas recibidas cuya longitud no es un número entero de octetos.
FCS Errors	Muestra el número de tramas recibidas que no pasan la comprobación FCS.
Single Collisions	Muestra el número de tramas correctamente transmitidas que han experimentado exactamente una colisión.
Multiple Collisions	Muestra el número de tramas transmitidas correctamente que han experimentado varias colisiones.
SQE Test Errors	Muestra el número de veces que se ha generado un mensaje de error de prueba SQE.
Deferred Transmissions	Muestra el número de tramas para las que se ha retrasado el primer intento de transmisión porque el medio estaba ocupado.
Late Collisions	Muestra el número de veces que se ha detectado una colisión después de 512 tiempos de bit en la transmisión de un paquete.
Excessive Collisions	Muestra el número de tramas cuya transmisión ha fallado por un exceso de colisiones.
MAC Transmit Errors	Muestra el número de tramas en las que falló la transmisión debido a un error de transmisión de subcapa MAC interna.
MAC Receive Errors	Muestra el número de tramas en las que falló la recepción por una interface debido a un error de recepción de subcapa MAC interna.
Carrier Sense	Muestra el número de veces que la condición de detección de portadora se perdió o nunca se logró al intentar transmitir una trama.
Frame Too Long	Muestra el número de tramas recibidas que han superado el tamaño de trama máximo permitido.
Reset Counters	Haga clic en Reset Counter para poner a cero los valores de los contadores de medios e interfaces del módulo, y actualizar los valores del cuadro de diálogo. Reset Counter aparece atenuado cuando está: <ul style="list-style-type: none"> fuera de línea en línea y se ha producido un error de comunicación

Advanced Time Sync

El cuadro de diálogo Advanced Time Sync muestra información relacionada con la sincronización de hora CIP Sync.

IMPORTANTE La información solo aparece si el proyecto está en línea y está habilitada la sincronización de hora en la ficha Date/Time. Además, cuando el controlador funciona en modo de doble IP, la ficha Advanced Time Sync proporciona los datos correspondientes a cada puerto.

1. En la ficha Date/Time, haga clic en el botón Advanced.



Se abre el cuadro de diálogo Advanced Time Sync. Consulte la [Tabla 36 en la página 294](#) para leer las descripciones de los parámetros.

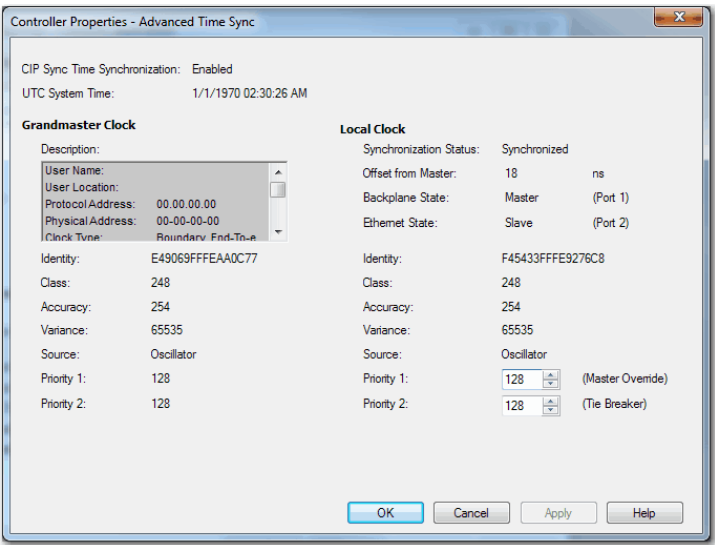


Tabla 36 – Parámetros Time Sync

Reloj Grandmaster	
Description	<p>Muestra información sobre el reloj Grandmaster. El proveedor del dispositivo Grandmaster controla esta información. Se especifica la siguiente información:</p> <ul style="list-style-type: none"> • Nombre del usuario • Ubicación del usuario • Dirección del protocolo • Dirección física • Tipo de reloj • Nombre del fabricante • Modelo • Número de serie • Revisión de hardware • Revisión de firmware • Versión de software • Identidad del perfil • Protocolo físico • Protocolo de red • Número de puerto <p>Utilice la barra de desplazamiento vertical para ver los datos.</p>
Identity	Muestra el identificador único del reloj Grandmaster. El formato depende del protocolo de red. La red Ethernet codifica la dirección MAC en el identificador.
Class	Muestra una medida de la calidad del reloj Grandmaster. Los valores están dentro del rango de 0 . . . 255 correspondiendo el cero al mejor reloj.
Accuracy	Indica la exactitud absoluta esperada del reloj Grandmaster relativa al tiempo PTP. La exactitud se especifica mediante una escala graduada que empieza en 25 ns y termina en más de 10 segundos o desconocido. Cuanto menor sea el valor de exactitud, mejor será el reloj.
Variance	Muestra la medida de las propiedades de estabilidad inherente del reloj Grandmaster. El valor se expresa en unidades de registro escaladas de offset. Cuanto menor sea la varianza, mejor será el reloj.
Source	<p>Muestra la fuente horaria del reloj Grandmaster. Los valores disponibles son:</p> <ul style="list-style-type: none"> • Atomic Clock • GPS • Radio • PTP • NTP • HAND set • Other • Oscillator
Priority 1/Priority 2	Muestra la prioridad relativa del reloj Grandmaster respecto a otros relojes del sistema. El intervalo de los valores de prioridad está comprendido entre 0 y 255. La prioridad más alta es cero. El valor predeterminado para ambos ajustes es 128.

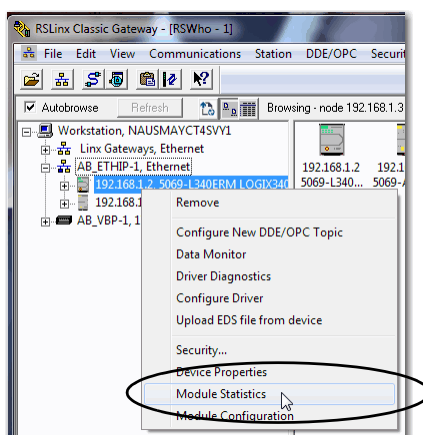
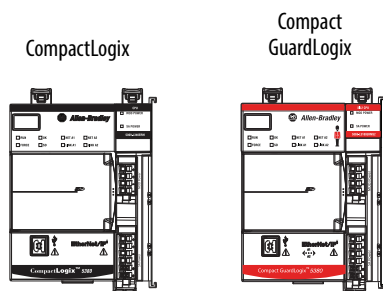
Tabla 36 – Parámetros Time Sync (continuación)

Reloj local	
Synchronization Status	Indica si el reloj local está sincronizado o no con el reloj Grandmaster de referencia. Un reloj está sincronizado si tiene un puerto en el estado esclavo y recibe actualizaciones del reloj maestro.
Offset to Master	Muestra la magnitud de la desviación entre el reloj local y el reloj Grandmaster, en nanosegundos.
Backplane State	Muestra el estado actual del backplane. Los valores disponibles son los siguientes: <ul style="list-style-type: none"> • Initializing • Faulty • Disabled • Listening • PreMaster • Master • Passive • Uncalibrating • Slave • None
Ethernet State	Muestra el estado del puerto Ethernet. Los valores disponibles son los siguientes: <ul style="list-style-type: none"> • Initializing • Faulty • Disabled • Listening • PreMaster • Master • Passive • Uncalibrating • Slave • None <p>IMPORTANTE: Cuando el controlador funciona en modo de doble IP, este atributo proporciona datos para cada puerto del controlador. Los campos aparecen de la siguiente manera:</p> <ul style="list-style-type: none"> • A1, estado de Ethernet • A2, estado de Ethernet
Identity	Muestra el identificador único para el reloj local. El formato depende del protocolo de red. La red Ethernet codifica la dirección MAC en el identificador.
Class	Muestra una medida de calidad del reloj local. Los valores están dentro del rango de 0...255, correspondiendo el cero al mejor reloj.
Accuracy	Indica la exactitud absoluta esperada del reloj local relativa al tiempo de sincronización del PTP. La exactitud se especifica mediante una escala graduada que empieza en 25 ns y termina en más de 10 segundos o desconocido. Cuanto menor sea el valor de exactitud, mejor será el reloj.
Variance	Muestra la medida de las propiedades de estabilidad inherente del reloj local. El valor se expresa en unidades de registro escaladas de offset. Cuanto menor sea la varianza, mejor será el reloj.
Source	Muestra la fuente horaria del reloj local. Los valores disponibles son: <ul style="list-style-type: none"> • Atomic Clock • GPS • Terrestrial Radio • PTP • NTP • HAND set • Other • Oscillator

Diagnóstico de controlador con software basado en Linx

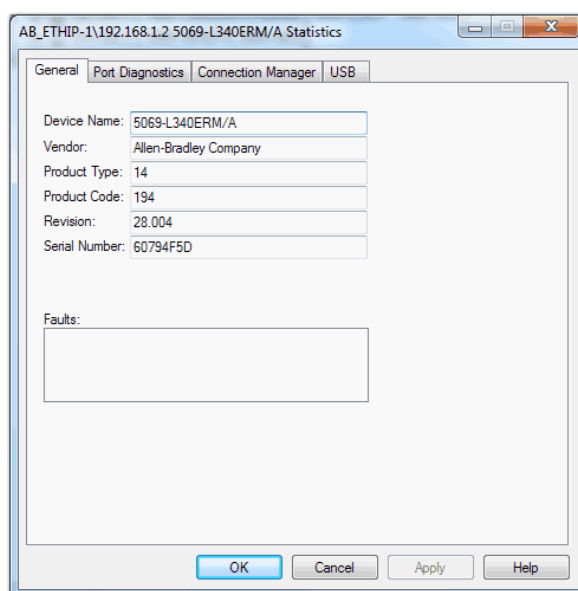
También puede ver información de diagnóstico en el software basado en Linx.

1. Utilice el botón RSWWho para navegar.
2. Desplácese hasta la red Ethernet.
3. Haga clic con el botón derecho del mouse en el controlador y elija Module Statistics.



El cuadro de diálogo Module Statistics proporciona la siguiente información:

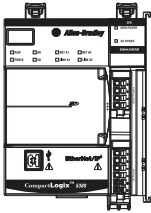
- La ficha General muestra información sobre el dispositivo y cualquier fallo que haya en el controlador.
- La ficha Port Diagnostics muestra la información sobre el puerto Ethernet.
- La ficha Connection Manager muestra la información sobre las solicitudes de conexión.
- La ficha USB muestra la información sobre el puerto USB.



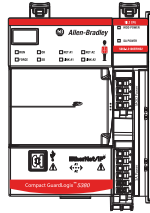
Páginas web del controlador

El controlador ofrece páginas web de diagnóstico que realizan un seguimiento del funcionamiento del controlador, la red y el backplane.

CompactLogix



Compact GuardLogix



Para consultar las páginas web de diagnóstico, siga estos pasos.

1. Abra su navegador web.
2. En el campo Address, escriba la dirección IP del controlador y presione Enter.
3. Para acceder a la información que necesita, utilice los vínculos en la barra de navegación izquierda.

IMPORTANTE

Las páginas web del controlador varían ligeramente en función del modo EtherNet/IP que se utilice. Las páginas web tienen un aspecto diferente y suministran datos distintos.

Por ejemplo, tenga en cuenta lo siguiente:

- Cuando el controlador funciona en modo lineal/DLR, la barra de navegación de la izquierda muestra una carpeta Ethernet Port A1/A2 con tres fichas.

Hay una página web Ethernet Port para ambos puertos y las páginas web del controlador proporcionan un conjunto de datos Ethernet.

- Cuando el controlador funciona en modo de doble IP, la barra de navegación de la izquierda muestra una carpeta Ethernet Port A1 y una carpeta Ethernet Port A2. Cada carpeta tiene tres fichas.

Hay una página web Ethernet Port para cada puerto y las páginas web del controlador proporcionan un conjunto de datos Ethernet para el puerto A1 y otro conjunto de datos Ethernet para el puerto A2.

Página web Home

La página web Home proporciona información de dispositivo y estado del controlador.

Modo lineal/DLR

The screenshot shows the Rockwell Automation web interface for a device named 'SIL2_Test'. The left sidebar is expanded to show 'Ethernet Port A1/A2'. The main content area displays the following information:

General Information	
Device Name	5069-L3100ERMS2/A_RelR31_724
Project Name	SIL2_Test
Device Description	
Device Location	
Product Revision	31.011
Firmware Version Date	Mar 8 2018, 04:49:46
Serial Number	6099AAB7
Uptime	00h:03m:26s
Port A1/A2 Ethernet Address (MAC)	F4:54:33:9B:20:86
Port A1/A2 IP Address	192.168.1.11

Controller Status	
Keyswitch Position	Remote
Controller Mode	Program
Change Detection Audit Value	16#E58B_9D12_32CB_5788
I/O Forces	Disabled - None Installed
SFC Forces	Disabled - None Installed

Seconds Between Refresh: 0 Disable Refresh with 0.

Copyright © 2017 Rockwell Automation, Inc. All Rights Reserved.

Modo de doble IP

The screenshot shows the Rockwell Automation web interface for a device named 'SIL2_Test' in Dual IP mode. The left sidebar is expanded to show 'Ethernet Port A1' and 'Ethernet Port A2'. The main content area displays the following information:

General Information	
Device Name	5069-L3100ERMS2/A_RelR31_724
Project Name	SIL2_Test
Device Description	
Device Location	
Product Revision	31.011
Firmware Version Date	Mar 8 2018, 04:49:46
Serial Number	6099AAB7
Uptime	00h:03m:52s
Port A1 Ethernet Address (MAC)	F4:54:33:9B:20:86
Port A1 IP Address	192.168.1.11
Port A2 Ethernet Address (MAC)	F4:54:33:9B:20:87
Port A2 IP Address	192.168.2.12

Controller Status	
Keyswitch Position	Remote
Controller Mode	Program
Change Detection Audit Value	16#AEE7_7600_D871_47C9
I/O Forces	Disabled - None Installed
SFC Forces	Disabled - None Installed

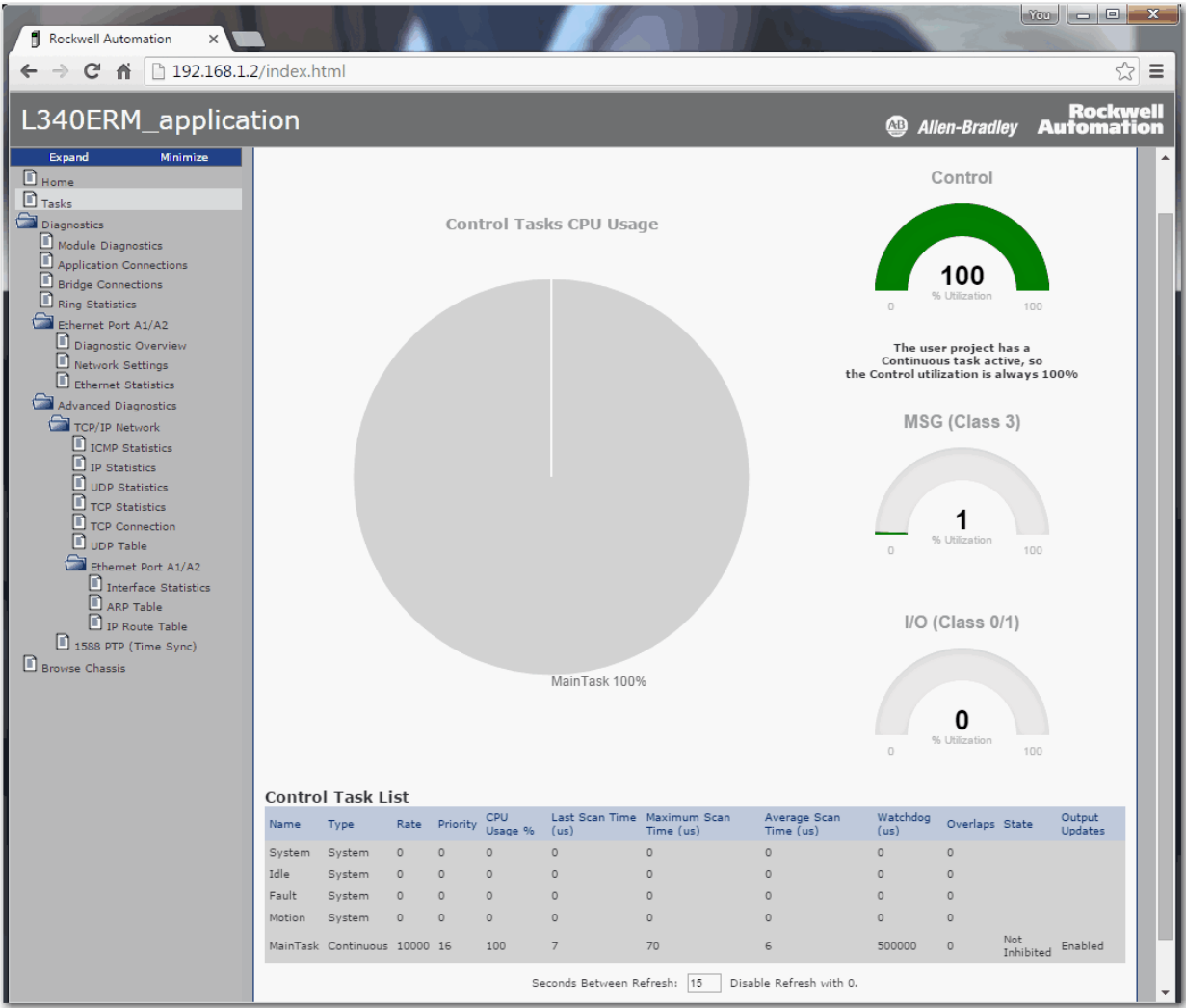
Seconds Between Refresh: 0 Disable Refresh with 0.

Copyright © 2017 Rockwell Automation, Inc. All Rights Reserved.

Página web Tasks

En la página web Tasks, el gráfico circular muestra el porcentaje de la CPU del núcleo de control consumido por las tareas que se ejecutan en dicho núcleo. Los indicadores muestran el uso de la CPU de los núcleos de control y comunicaciones.

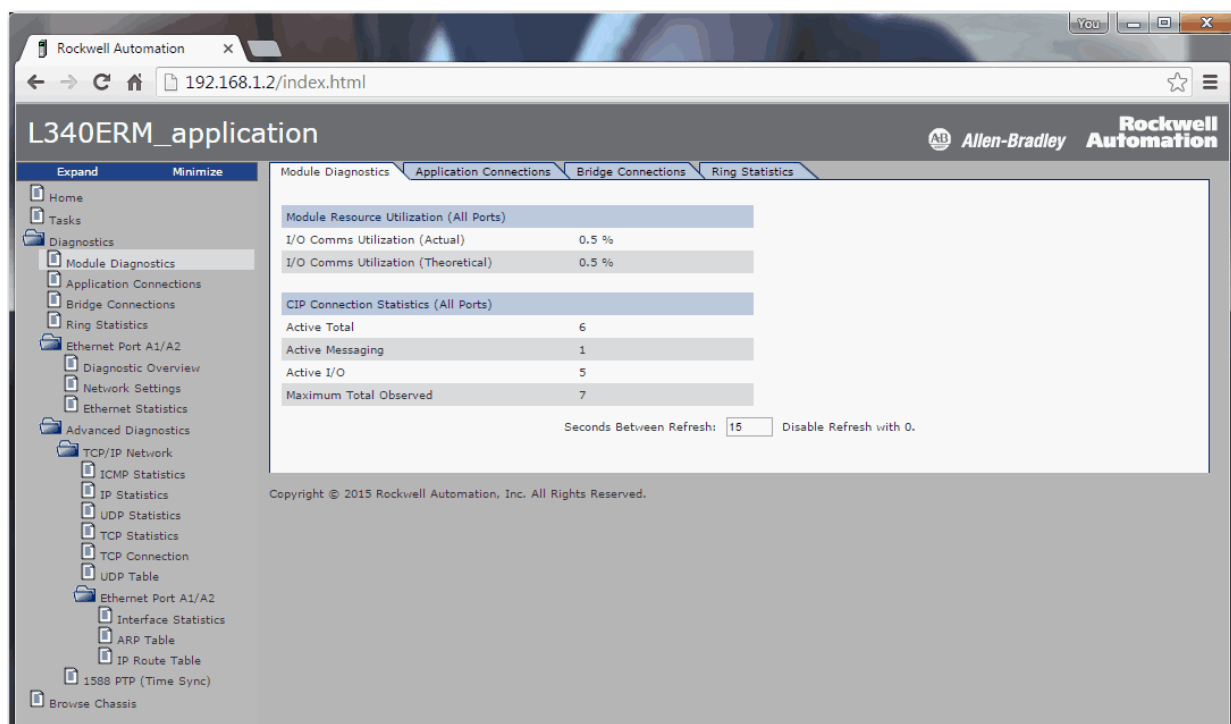
La tabla muestra las tareas que se ejecutan en el núcleo de control (todas las tareas del sistema se resumen como una sola tarea).



Páginas web Diagnostics

Las páginas web Diagnostics utilizan varias fichas para mostrar información acerca de lo siguiente:

- Module Diagnostics
- Application Connections
- Bridge Connections
- Ring Statistics

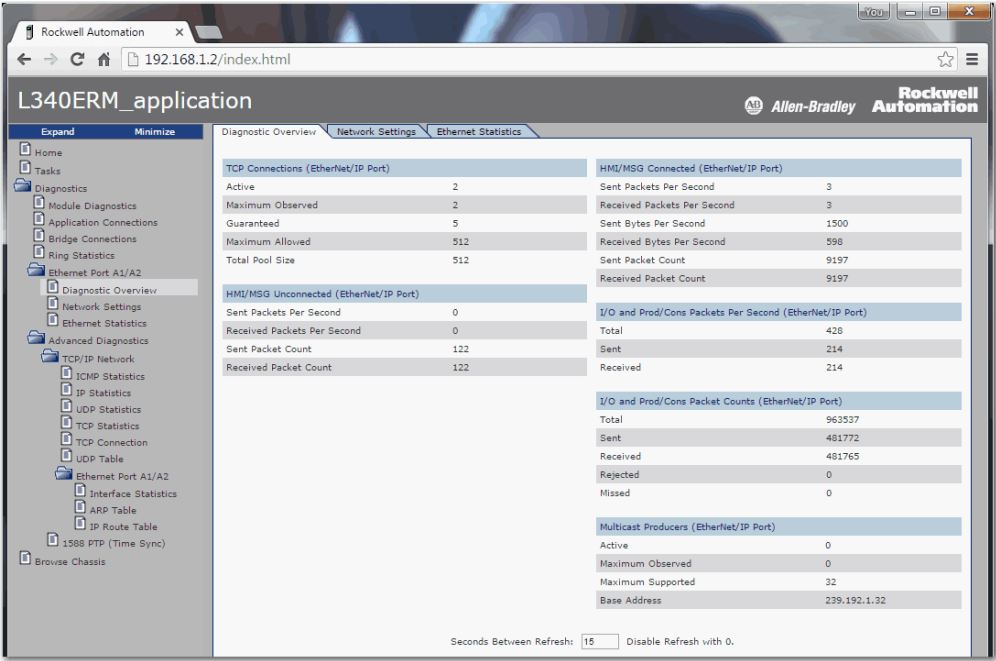


Páginas web Ethernet Port

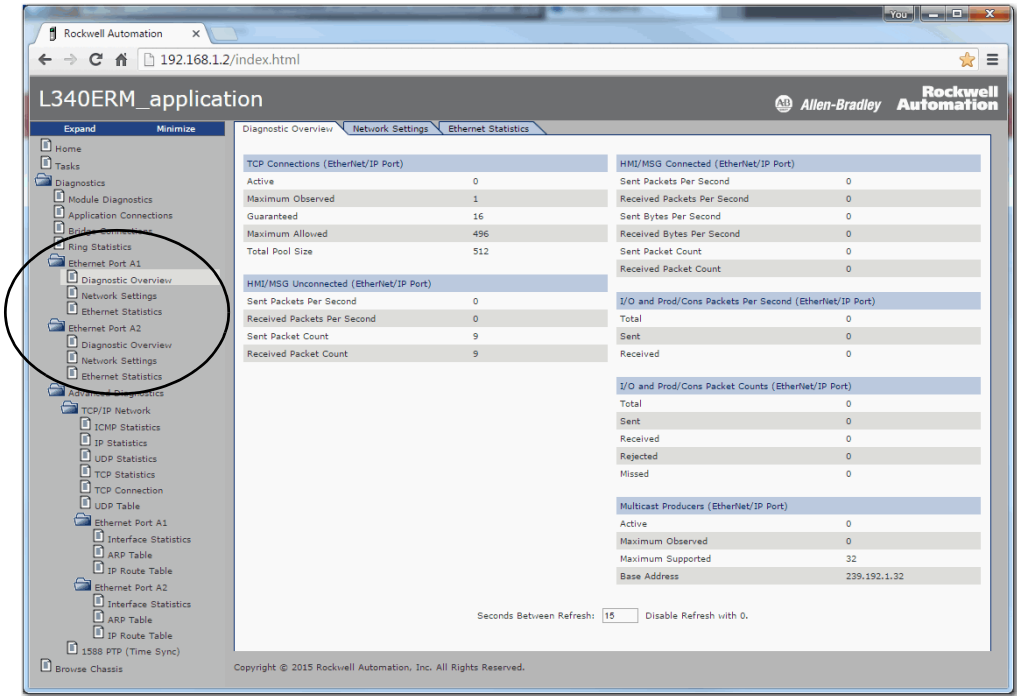
Las páginas web Ethernet Port utilizan varias fichas para mostrar información acerca de lo siguiente:

- Diagnostic Overview
- Network Settings
- Ethernet Statistics

Modo lineal/DLR



Modo de doble IP



Páginas web Advanced Diagnostics

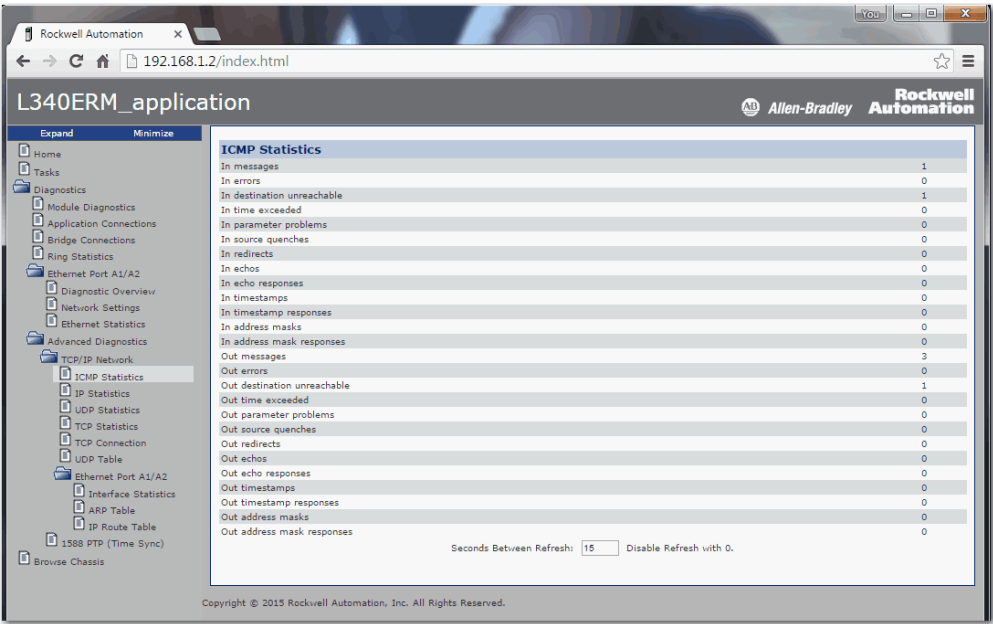
Las páginas web Advanced Diagnostics proporcionan información acerca de lo siguiente:

- TCP/IP Network – Ofrece información sobre lo siguiente:
 - ICMP Statistics
 - IP Statistics
 - UDP Statistics
 - TCP Statistics
 - TCP Connection
 - UDP Table
- Ethernet Port A1/A2 – Ofrece información acerca de lo siguiente:
 - Interface Statistics
 - ARP Table
 - IP Route Table

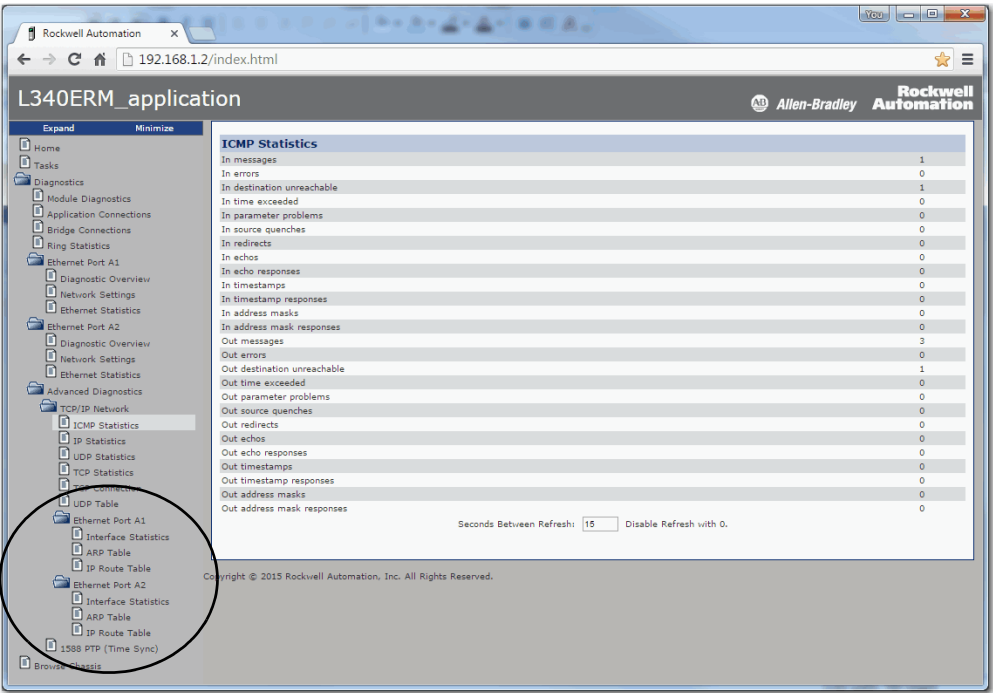
IMPORTANTE	Esta información se indica por separado y es única para cada puerto cuando el controlador funciona en modo de doble IP.
-------------------	---

- 1588 PTP (Time Sync)

Modo lineal/DLR

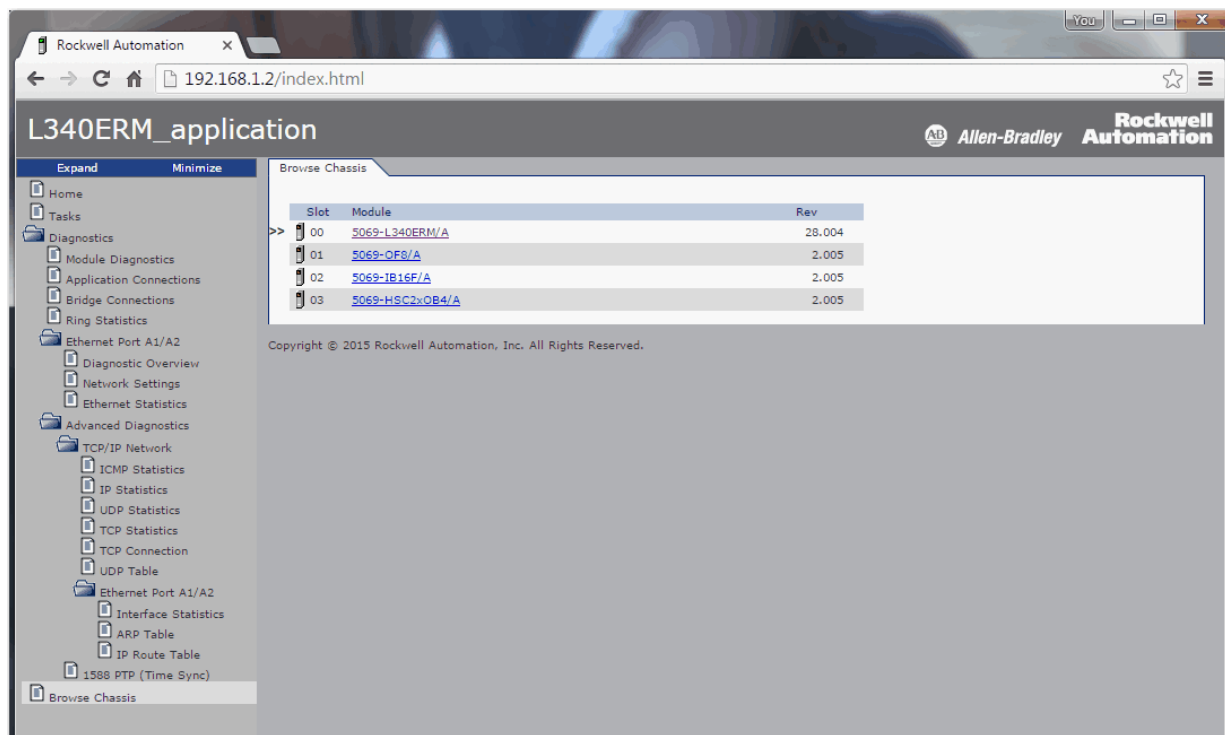


Modo de doble IP



Página web Browse Chassis

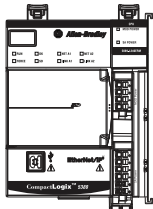
La ficha Browse Chassis proporciona información acerca de los dispositivos del sistema. Puede hacer clic en el vínculo correspondiente a cada número de catálogo para consultar más información sobre ese dispositivo.



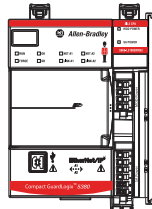
Otros posibles problemas que puede ser necesario resolver

El controlador puede experimentar otros problemas que se deben resolver.

CompactLogix



Compact GuardLogix



Tarea continua envía datos de salida a alta velocidad

Una tarea continua de ejecución libre puede seguir enviando salidas a una velocidad alta. Si la tarea continua se ejecuta repetidamente con un tiempo de ejecución de tarea corto y los datos producidos o la salida local cambian, es posible que el controlador produzca datos con una rapidez mayor a la rapidez con que los módulos receptores pueden reaccionar. Le recomendamos que escriba debidamente el programa para evitar esta situación.

Instrucciones de salida inmediata enviadas a alta velocidad

Los controladores CompactLogix™ 5380 y Compact GuardLogix® 5380 pueden enviar instrucciones Immediate Output (IOT) a una rapidez mayor a la rapidez con que los módulos de E/S pueden reaccionar. Le recomendamos que programe las instrucciones IOT para que se envíen a una velocidad adecuada para el módulo de E/S y los correspondientes dispositivos físicos.

Movimiento integrado en una red EtherNet/IP con estado de prioridad del tráfico

Si utiliza un switch administrado Stratix® para cambiar la velocidad de comunicación de la red de 1 Gbps a 100 Mbps, es posible que el sistema no pueda dar mayor prioridad al movimiento integrado en una comunicación de red EtherNet/IP que a la comunicación de E/S estándar.

Para obtener más información sobre cuándo utilizar un switch administrado Stratix para cambiar la velocidad de comunicación de la red de 1 Gbps a 100 Mbps, consulte la [página 137](#).

Para obtener más información acerca de los switches administrados en general, consulte la sección sobre la red EtherNet/IP del directorio de productos que encontrará en esta dirección: <http://ab.rockwellautomation.com/networks-and-communications/ethernet-ip-network>.

Notas:

Indicadores de estado

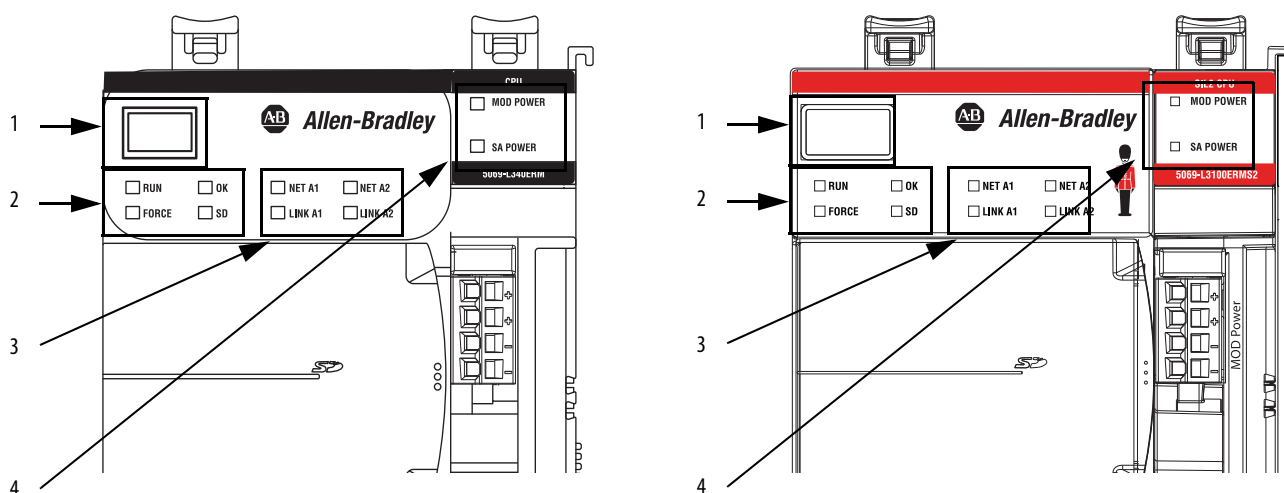
Los controladores CompactLogix™ 5380 y Compact GuardLogix™ 5380 tienen una pantalla de estado de cuatro caracteres con desplazamiento, indicadores de estado del controlador, indicadores de estado de red EtherNet/IP e indicadores de alimentación.

Tema	Página
Pantalla de estado e indicadores	308
Mensajes de estado general	309
Mensajes de estado de Compact GuardLogix	311
Mensajes de fallo	311
Mensajes de fallo mayor	312
Códigos de fallo de E/S	314
Indicadores de estado del controlador	317
Indicadores de estado de EtherNet/IP	319
Indicadores de estado de alimentación	320
Monitoreo térmico y comportamiento ante fallo térmico	321

Pantalla de estado e indicadores

La [Figura 71](#) muestra la pantalla de estado e indicadores de los controladores CompactLogix 5380 y Compact GuardLogix 5380.

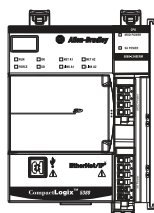
Figura 71 – Pantalla de estado e indicadores



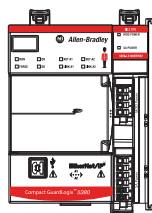
Ítem	Descripción
1	Pantalla de estado de 4 caracteres con desplazamiento, consulte la página 309
2	Indicadores de estado del controlador, consulte la página 317
3	Indicadores de estado de EtherNet/IP, consulte la página 319
4	Indicadores de estado de la alimentación, consulte la página 320

Mensajes de estado general

CompactLogix



Compact GuardLogix



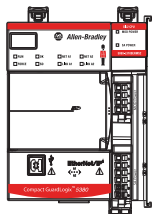
Los mensajes con desplazamiento descritos en esta tabla se muestran normalmente al momento del encendido, de la desactivación y cuando el controlador está funcionando para mostrar el estado del controlador.

Mensaje	Interpretación
No se indica ningún mensaje	El controlador está apagado. Verifique el indicador de estado MOD POWER para determinar si la alimentación eléctrica del sistema está conectada. Verifique el indicador OK para determinar si el controlador está encendido y determinar el estado del controlador.
TEST	El controlador está efectuando las pruebas de encendido.
CHRG	El circuito de almacenamiento de energía incorporado se está cargando.
PASS	Las pruebas de encendido han concluido correctamente.
Saving... Do Not Remove SD Card	El controlador se dispone a guardar una imagen en la tarjeta SD.
SAVE	Se está guardando un proyecto en la tarjeta SD. Para obtener más información, consulte Indicador SD en la página 318 . Espere a que finalice la operación de almacenamiento antes de: <ul style="list-style-type: none"> Retirar la tarjeta SD. Desconectar la alimentación eléctrica. IMPORTANTE: No retire la tarjeta SD mientras el controlador está guardando datos en la tarjeta SD. Espere a que finalice la operación de almacenamiento sin interrupciones. Si interrumpe la operación de almacenamiento, pueden perderse o alterarse los datos.
Uno de los siguientes: <ul style="list-style-type: none"> CARGA Loading... Do Not Remove SD Card 	Se está guardando un proyecto en la tarjeta SD. Para obtener más información, consulte Indicador SD en la página 318 . Espere a que finalice la operación de carga antes de hacer lo siguiente: <ul style="list-style-type: none"> Retirar la tarjeta SD Desconectar la alimentación eléctrica IMPORTANTE: No retire la tarjeta SD mientras el controlador está cargando datos de la tarjeta SD. Espere a que finalice la operación de carga sin interrupciones. Si interrumpe la carga, pueden perderse o alterarse los datos.
UPDT	Se está realizando una actualización de firmware desde la tarjeta SD al momento del encendido. Para obtener más información, consulte Indicador SD en la página 318 . Si no desea que el firmware se actualice al momento del encendido, cambie la propiedad Load Image del controlador.
Rev XX.xxx	Las revisiones mayor y menor del firmware del controlador.
5069-L3xxx	El número de catálogo y de serie del controlador.
Link Down	Este mensaje aparece cuando un puerto Ethernet no tiene conexión de red. El mensaje se desplaza constantemente en la pantalla durante el funcionamiento. IMPORTANTE: Cuando el controlador funciona en modo de doble IP, esta información se proporciona para cada vínculo, es decir, el vínculo A1 y el vínculo A2. El nombre del vínculo aparece antes de la información.
Link Disabled	Este mensaje aparece cuando ha inhabilitado un puerto Ethernet. El mensaje se desplaza constantemente en la pantalla durante el funcionamiento. IMPORTANTE: Cuando el controlador funciona en modo de doble IP, esta información se proporciona para cada vínculo, es decir, el vínculo A1 y el vínculo A2. El nombre del vínculo aparece antes de la información.
DHCP-00:00:XX:XX:XX:XX	Este mensaje aparece cuando el controlador está establecido para DHCP, pero no se ha configurado en una red. El mensaje muestra la dirección MAC del controlador. El mensaje atraviesa continuamente la pantalla durante el funcionamiento si no se ha establecido ninguna dirección IP. IMPORTANTE: Cuando el controlador funciona en modo de doble IP, esta información se proporciona para el puerto A1 y el puerto A2. El nombre del puerto aparece antes de la información.
Ethernet Port Rate/Duplex State	La velocidad del puerto y el estado dúplex actuales cuando un puerto Ethernet tiene una conexión. El mensaje se desplaza constantemente en la pantalla durante el funcionamiento. IMPORTANTE: Cuando el controlador funciona en modo de doble IP, esta información se proporciona para cada vínculo, es decir, el vínculo A1 y el vínculo A2. El nombre del vínculo aparece antes de la información.
IP Address	Dirección IP del controlador. Aparece al momento del encendido y se desplaza continuamente durante el funcionamiento. Si no se ha establecido todavía la dirección IP, aparece la dirección MAC. IMPORTANTE: Cuando el controlador funciona en modo de doble IP, esta información se proporciona para el puerto A1 y el puerto A2. El nombre del puerto aparece antes de la información.

Mensaje	Interpretación
Duplicate IP – 00:00:XX:XX:XX:XX	Este mensaje aparece cuando el controlador detecta un dispositivo con la misma dirección IP en la red. El mensaje indica la dirección MAC del dispositivo que tiene la dirección IP duplicada. El mensaje se desplaza constantemente en la pantalla durante el funcionamiento. IMPORTANTE: Cuando el controlador funciona en modo de doble IP, esta información se proporciona para el puerto A1 y el puerto A2. El nombre del puerto aparece antes de la información.
DHCP-Address Lost	El controlador se comunicó con el servidor DHCP para renovar la dirección IP. El servidor no ha respondido o no ha renovado la dirección IP. El controlador sigue funcionando, pero sin ninguna conectividad Ethernet en este puerto. IMPORTANTE: Cuando el controlador funciona en modo de doble IP, esta información se proporciona para el puerto A1 y el puerto A2. El nombre del puerto aparece antes de la información.
IP Address/Mask/Gateway/DNS Invalid	El servidor DHCP ha respondido con una combinación no utilizable. IMPORTANTE: Cuando el controlador funciona en modo de doble IP, esta información se proporciona para el puerto A1 y el puerto A2. El nombre del puerto aparece antes de la información.
IP Address Invalid	La dirección IP utilizada en la configuración del puerto no es válida. IMPORTANTE: Cuando el controlador funciona en modo de doble IP, esta información se proporciona para el puerto A1 y el puerto A2. El nombre del puerto aparece antes de la información.
Mask Invalid	La máscara de subred/red utilizada en la configuración del puerto no es válida. IMPORTANTE: Cuando el controlador funciona en modo de doble IP, esta información se proporciona para el puerto A1 y el puerto A2. El nombre del puerto aparece antes de la información.
Gateway Invalid	La dirección de gateway utilizada en la configuración de la IP del puerto no es válida. IMPORTANTE: Cuando el controlador funciona en modo de doble IP, esta información se proporciona para el puerto A1 y el puerto A2. El nombre del puerto aparece antes de la información.
DNS Invalid	El DNS utilizado en la configuración de la IP del puerto no es válido.
No Project	No hay ningún proyecto cargado en el controlador. Para cargar un proyecto: <ul style="list-style-type: none">• Utilice la aplicación Studio 5000 Logix Designer® para descargar el proyecto al controlador• Utilice una tarjeta SD para cargar un proyecto en el controlador
Project Name	El nombre del proyecto que se ha cargado al controlador.
BUSY	Los módulos de E/S asociados al controlador todavía no están totalmente encendidos. Espere a que terminen el encendido y la autoprueba de los módulos de E/S.
Corrupt Certificate Received	El certificado de seguridad asociado al firmware está alterado. Visite http://www.rockwellautomation.com/support/ y descargue la revisión de firmware a la que desea actualizar. Reemplace la revisión de firmware que instaló previamente por la obtenida del sitio web de asistencia técnica.
Corrupt Image Received	El archivo de firmware está alterado. Visite http://www.rockwellautomation.com/support/ y descargue la revisión de firmware a la que desea actualizar. Reemplace la revisión de firmware que instaló previamente por la obtenida del sitio web de asistencia técnica.
Backup Energy HW Failure – Save Project	Se produjo un fallo del circuito de almacenamiento incorporado y el controlador no podrá guardar el programa en caso de que falle la alimentación eléctrica. Si ve este mensaje, guarde su programa en la tarjeta SD antes de desconectar la alimentación eléctrica y reemplazar el controlador.
Backup Energy Low – Save Project	El circuito de almacenamiento incorporado no tiene suficiente energía para que el controlador pueda guardar el programa en caso de que falle la alimentación eléctrica. Si ve este mensaje, guarde su programa en la tarjeta SD antes de desconectar la alimentación eléctrica y reemplazar el controlador.
Flash in Progress	Hay una actualización de firmware en curso que se ha iniciado mediante las utilidades ControlFLASH™ o AutoFlash. Espere a que finalice la actualización del firmware sin interrupción.
Firmware Installation Required	El controlador está usando firmware de arranque, es decir, la revisión 1.xxx, y requiere una actualización del firmware.
SD Card Locked	Hay una tarjeta SD instalada que está bloqueada.
Download in Progress	Hay una descarga activa en curso
Aborting Download	Se está anulando una descarga activa. Esto se puede deber a una cancelación iniciada por el usuario, un fallo de descarga o una pérdida de conexión.

Mensajes de estado de Compact GuardLogix

Compact GuardLogix



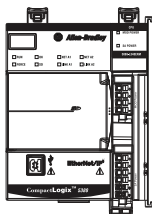
La pantalla del controlador Compact GuardLogix 5380 puede mostrar los siguientes mensajes con desplazamiento.

Tabla 37 – Mensajes de estado de seguridad

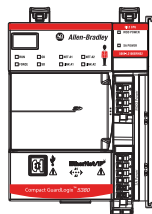
Mensaje	Interpretación
No Safety Signature	La tarea de seguridad está en el modo de marcha sin una firma de seguridad. Genere una firma de seguridad.
Safety Task Inoperable	La lógica de seguridad no es válida. Por ejemplo, expiró un temporizador (watchdog) o la memoria está alterada.
Safety Unlocked	El controlador está en el modo de marcha con una firma de seguridad, pero no está en bloqueo de seguridad. Ponga el controlador en bloqueo de seguridad.

Mensajes de fallo

CompactLogix



Compact GuardLogix



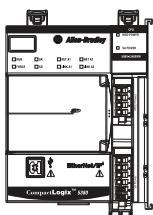
Si el controlador muestra un fallo, pueden aparecer estos mensajes en la pantalla de estado.

Tabla 38 – Mensajes de fallo

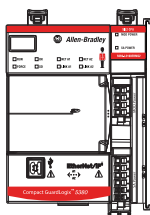
Mensaje	Interpretación
Major Fault TXX:CXX message	Se detectó un fallo mayor de tipo XX y código XX. Por ejemplo, si la pantalla de estado indica MajorFault T04:C42 Invalid JMP Target, se programa una instrucción JMP para que salte a una instrucción LBL no válida. Para obtener información detallada acerca de los fallos mayores recuperables, consulte el documento Logix 5000™ Major, Minor, and I/O Fault Codes Programming Manual, publicación 1756-PM014 .
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. Para obtener información detallada acerca de cada código de fallo de E/S, consulte el documento Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publicación 1756-PM014 .
I/O Fault ModuleName #XXXX message	Ocurrió un fallo de E/S en un módulo en un chasis remoto. El nombre del módulo que ha fallado 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. Para obtener información detallada acerca de cada código de fallo de E/S, consulte el documento Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publicación 1756-PM014 .
I/O Fault ModuleParent:X #XXXX message	Ocurrió un fallo de E/S en un módulo en un chasis remoto. Se indica el nombre del primario del módulo porque no se ha configurado ningún nombre de módulo en el árbol de configuración de E/S de la aplicación Logix Designer. Además, se indica el código de fallo con una breve descripción del fallo. Tome la acción correctiva correspondiente al tipo de fallo indicado. Para obtener información detallada acerca de cada código de fallo de E/S, consulte el documento Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publicación 1756-PM014 .
X/I/O Faults	Hay fallos de E/S presentes y X = el número de fallos de E/S presentes. Si hay varios 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 mensaje de fallo de E/S indica el siguiente fallo reportado. Tome la acción correctiva correspondiente al tipo de fallo indicado. Para obtener información detallada acerca de cada código de fallo de E/S, consulte el documento Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publicación 1756-PM014 .

Mensajes de fallo mayor

CompactLogix



Compact GuardLogix



El mensaje Major Fault *TXX:CXX message* en la pantalla de estado del controlador indica fallos mayores. La [Tabla 39](#) indica los tipos de fallos, los códigos y los mensajes asociados, tal como aparecen en la pantalla de estado.

Para leer las descripciones detalladas y métodos de recuperación sugeridos para los fallos mayores, consulte el documento Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publicación [1756-PM014](#).

Tabla 39 – Mensajes de estado de fallo mayor

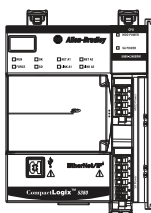
Tipo	Código	Mensaje
1	1	Run Mode Powerup
1	60	Nonrecoverable
1	61	Nonrecoverable – Diagnostics Saved on SD Card
3	16	I/O Connection Failure
3	20	Chassis Failure
3	21	
3	23	Connection Failure
4	16	Unknown Instruction
4	20	Invalid Array Subscript
4	21	Control Structure LEN o POS < 0
4	31	Invalid JSR Parameter
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	

Tabla 39 – Mensajes de estado de fallo mayor (continuación)

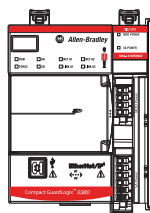
Tipo	Código	Mensaje
6	1	Task Watchdog Expired
7	40	Save Failure
7	41	Bad Restore Type
7	42	Bad Restore Revision
7	43	Bad Restore Checksum
7	44	Failed to Restore Processor Memory
8	1	Mode switch Change Ignored
11	1	Positive Overtravel Limit Exceeded
11	2	Negative Overtravel Limit Exceeded
11	3	Position Error Tolerance Exceeded
11	4	Encoder Channel Connection Fault
11	5	Encoder Noise Event Detected
11	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	14	Inactive Drive Enable Input Detected
11	15	Drive Phase Loss Detected
11	16	DriveGuard® Fault
11	32	Motion Task Overlap Fault
11	33	CST Reference Loss Detected
14	1	Safety Task Watchdog Expired
14	2	Error In Routine of Safety Task
14	7	Safety Task Inoperable
18	1	CIP Motion Initialization Fault
18	2	CIP Motion Initialization Fault Mfg
18	3	CIP Motion Axis Fault
18	4	CIP Motion Axis Fault Mfg
18	5	CIP Motion Fault
18	6	CIP Module Fault
18	7	Motion Group Fault
18	8	CIP Motion Configuration Fault
18	9	CIP Motion APR Fault
18	10	CIP Motion APR Fault Mfg
18	128	CIP Motion Guard Fault

Códigos de fallo de E/S

CompactLogix



Compact GuardLogix



El controlador indica los fallos de E/S 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 que tiene un fallo. La manera en que se indica la ubicación depende de su configuración de E/S y de las propiedades del módulo especificadas en la aplicación Studio 5000 Logix Designer®.

La última parte del formato, #XXXX *message*, puede usarse para diagnosticar el tipo de fallo de E/S y las posibles acciones correctivas. Para obtener información detallada acerca de cada código de fallo de E/S, consulte el documento Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publicación [1756-PM014](#).

Tabla 40 – 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

Tabla 40 – Mensajes de fallo de E/S (continuación)

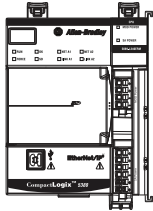
Código	Mensaje
#0111	RPI Out of Range
#0113	Out of Connections
#0114	Wrong Module
#0115	Wrong Device Type
#0116	Wrong Revision
#0117	Invalid Connection Point
#0118	Invalid Configuration Format
#0119	Module Not Owned
#011A	Out of Connection Resources
#0203	Connection Timeout
#0204	Unconnected Message Timeout
#0205	Invalid Parameter
#0206	Message Too Large
#0301	No Buffer Memory
#0302	Bandwidth Not Available
#0303	No Bridge Available
#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
#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
#FD0A	Axis Attribute Reject
#FD1F	Safety I/O
#FD20	No Safety Task
#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

Tabla 40 – Mensajes de fallo de E/S (continuación)

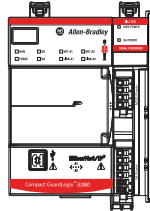
Código	Mensaje
#FE07	Invalid Output Connection
#FE08	Invalid Output Data Pointer
#FE09	Invalid Output Data Size
#FE0A	Invalid Output Force Pointer
#FE0B	Invalid Symbol String
#FE0C	Invalid Scheduled Personal Computer Instance
#FE0D	Invalid Symbol Instance
#FE0E	Module Firmware Updating
#FE0F	Invalid 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

Indicadores de estado del controlador

CompactLogix



Compact GuardLogix



Los indicadores de estado del controlador muestran el estado del controlador.

IMPORTANTE Consideraciones de seguridad

Los indicadores de estado no son indicadores confiables de las funciones de seguridad. Úselos solo para diagnóstico general durante la puesta en marcha o la resolución de problemas. No intente utilizar los indicadores de estado para determinar el estado de operación.

Indicador RUN

El indicador RUN muestra el modo actual del controlador.

Para cambiar el modo del controlador, puede utilizar el interruptor de modo ubicado en la parte frontal de controlador o el menú Controller Status de la aplicación Logix Designer.

Tabla 41 – Indicador RUN

Estado	Descripción
Off	El controlador está en el modo de programación o en el modo de prueba.
Verde fijo	El controlador está en el modo de marcha.

Indicador FORCE

El indicador Force muestra si hay forzados de E/S habilitados en el controlador.

Tabla 42 – Indicador FORCE

Estado	Descripción
Off	No hay tags que contengan valores de forzados de E/S.
Amarillo fijo	Los forzados de E/S están habilitados. Si hay valores de forzados de E/S, están activos. IMPORTANTE: Tome precauciones al cambiar los valores de forzados. En este estado, los cambios surten efecto de manera inmediata.
Amarillo parpadeante	Hay forzados de E/S en la aplicación, pero no están activos porque no se han habilitado los forzados de E/S. IMPORTANTE: Tome precauciones al habilitar los forzados de E/S. Todos los valores de forzados de E/S existentes surten efecto de forma inmediata.

Indicador SD

El indicador SD muestra si se está utilizando la tarjeta SD.

Tabla 43 – Indicador SD

Estado	Descripción
Off	No hay ninguna actividad que involucre a la tarjeta SD.
Verde parpadeante	El controlador está leyendo la tarjeta SD o escribiendo en ella. IMPORTANTE: No retire la tarjeta SD mientras el controlador está leyendo o escribiendo.
Verde fijo	Espere a que finalice la operación de lectura/escritura sin interrupciones. Si interrumpe la lectura/escritura, pueden perderse o alterarse los datos.
Rojo parpadeante	Se ha presentado una de las siguientes situaciones: <ul style="list-style-type: none"> La tarjeta SD no tiene un sistema de archivos válido. La tarjeta SD estaba consumiendo una corriente excesiva y se ha desconectado la alimentación de la tarjeta.
Rojo fijo	El controlador no reconoce la tarjeta SD.

Indicador OK

El indicador OK muestra el estado del controlador.

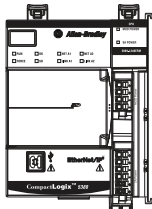
Tabla 44 – Indicador OK

Estado	Descripción
Off	No hay alimentación eléctrica aplicada.
Rojo parpadeante	Se ha presentado una de las siguientes situaciones: <ul style="list-style-type: none"> El controlador necesita una actualización de firmware. Normalmente, el controlador se encuentra en su estado original cuando se requiere una actualización del firmware. Si se necesita una actualización del firmware, la pantalla de 4 caracteres indica Firmware Installation Required. Para obtener más información sobre cómo actualizar el firmware, consulte Carga desde el controlador en la página 105. Hay una actualización de firmware en curso. Si hay una actualización de firmware en curso, la pantalla de 4 caracteres indica Flash in Progress. Para obtener más información sobre cómo actualizar el firmware, consulte Carga desde el controlador en la página 105. El controlador presenta un fallo mayor. El fallo puede ser recuperable o no. Si el fallo no es recuperable, el programa se ha borrado de la memoria del controlador. Si se ha producido un fallo, la pantalla de 4 caracteres muestra información acerca del fallo, por ejemplo, el tipo y el código. Para obtener información detallada acerca de los fallos mayores, consulte la siguiente información: <ul style="list-style-type: none"> Las descripciones de fallo en Mensajes de estado general que comienzan en la página 309. Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publicación 1756-PM014. Se detienen todas las tareas de usuario estándar y de seguridad.
Rojo fijo	Uno de los siguientes: <ul style="list-style-type: none"> El controlador está realizando los diagnósticos de encendido. El controlador está agotando su energía almacenada residual al haber fallado la alimentación eléctrica. El controlador está encendido pero está inoperativo. El controlador está cargando un proyecto en la memoria no volátil. El controlador está experimentando un fallo de preservación del hardware causado por una alta temperatura interna del módulo. En esta situación, solo el indicador de estado recibe alimentación eléctrica. Cuando el controlador se enfríe y alcance una temperatura aceptable, se aplicará toda la alimentación eléctrica.
Verde fijo	El controlador está funcionando normalmente.

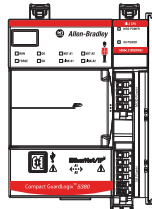
Indicadores de estado de EtherNet/IP

Los indicadores de EtherNet/IP muestran el estado de los puertos Ethernet del controlador y la actividad de comunicación de red.

CompactLogix



Compact GuardLogix



Indicadores NET A1 y NET A2

Los indicadores NET A1 y NET A2 muestran el estado del puerto Ethernet.

Tabla 45 – Indicadores NET A1 y NET A2

Estado	Descripción
Off	Uno de los siguientes: <ul style="list-style-type: none"> El controlador no está configurado o no tiene una dirección IP. El puerto está inhabilitado desde el punto de vista de administración. El modo EtherNet/IP es el modo lineal/DLR. En este caso, el indicador NET A2 está apagado. El indicador NET A1 permanece encendido.
Verde parpadeante	El controlador tiene una dirección IP pero no se ha establecido ninguna conexión activa.
Verde fijo	El controlador tiene una dirección IP y al menos una conexión activa establecida.
Rojo fijo	Dirección IP duplicada o configuración no válida.

Indicadores LINK A1 y LINK A2

Los indicadores LINK A1 y LINK A2 muestran el estado de los vínculos EtherNet/IP.

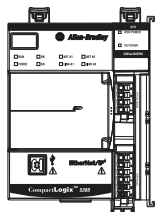
Tabla 46 – Indicadores LINK A1 y LINK A2

Estado	Descripción
Off	El vínculo está inactivo. Existe una o varias de estas condiciones: <ul style="list-style-type: none"> Los cables Ethernet no están correctamente conectados en ambos extremos. Es decir, los cables no están conectados debidamente al puerto Ethernet del controlador y al dispositivo conectado. No hay ningún vínculo en el puerto. Por ejemplo, el dispositivo conectado no está encendido. El puerto está inhabilitado desde el punto de vista de administración. Solo LINK A2: <ul style="list-style-type: none"> El controlador es el supervisor de anillo activo de una red DLR y el anillo no está roto. Este es el funcionamiento normal. El controlador es el supervisor de anillo activo de una red DLR y ha detectado un fallo de anillo rápido.
Verde parpadeante	Se dan todas estas condiciones: <ul style="list-style-type: none"> El puerto está habilitado. Hay un vínculo. Es decir, el cable está debidamente conectado a un puerto Ethernet habilitado del controlador y a otro dispositivo. Hay actividad en el puerto.
Verde fijo	Se dan todas estas condiciones: <ul style="list-style-type: none"> El puerto está habilitado. Hay un vínculo. Es decir, el cable está debidamente conectado a un puerto Ethernet habilitado del controlador y a otro dispositivo. No hay actividad en el puerto.

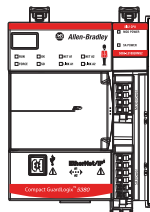
Indicadores de estado de alimentación

Los indicadores de estado de alimentación muestran el estado de la alimentación de módulo y la alimentación de sensor/accionador, denominadas alimentación MOD y alimentación SA, respectivamente.

CompactLogix



Compact GuardLogix



Indicador de alimentación MOD

La [Tabla 47](#) describe el indicador de alimentación MOD en los controladores CompactLogix 5380 y Compact GuardLogix 5380.

Tabla 47 – Indicador de alimentación MOD

Estado	Descripción
Off	No hay alimentación de módulo presente
Verde fijo	Hay alimentación de módulo presente ⁽¹⁾

(1) Aunque es poco probable, es posible que haya suficiente alimentación de módulo para que el indicador se ponga verde fijo, pero que la alimentación eléctrica no sea válida. La alimentación válida es de 18...32 VCC para que funcione un sistema CompactLogix 5380. Si el sistema no se enciende y funciona correctamente, es posible que la alimentación de módulo no sea válida.

Si la alimentación de módulo no es válida, le recomendamos que compruebe que la fuente de alimentación eléctrica externa funciona correctamente, se ha dimensionado correctamente para su aplicación y todo el cableado es correcto.

Indicador de alimentación SA

La [Tabla 48](#) describe el indicador de alimentación SA en los controladores CompactLogix 5380 y Compact GuardLogix 5380.

Tabla 48 – Indicador de alimentación SA

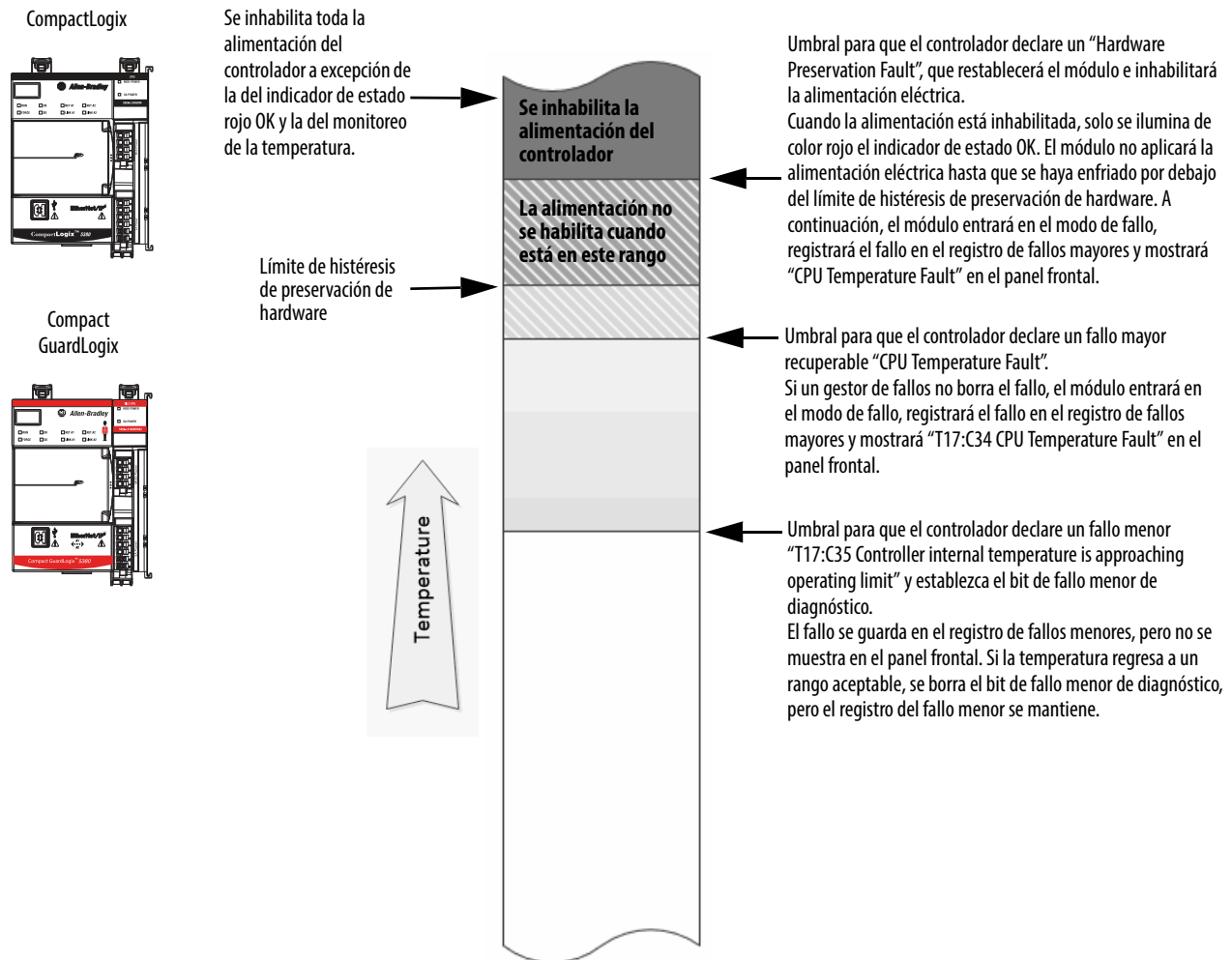
Estado	Descripción
Off	Uno de los siguientes: <ul style="list-style-type: none"> La alimentación de accionador de sensor no está presente Se desconoce el estado de la alimentación de accionador de sensor
Verde fijo	La alimentación de accionador de sensor está presente ⁽¹⁾

(1) Aunque es poco probable, es posible que haya suficiente alimentación de sensor/accionador para que el indicador se ponga verde fijo, pero que la alimentación eléctrica no sea válida. La alimentación válida es de 18...32 VCC en aplicaciones que requieren voltaje de CC, y de 18...240 VCA en aplicaciones que requieren voltaje de CA.

Si la alimentación de sensor/accionador no es válida, le recomendamos que compruebe que la fuente de alimentación eléctrica externa funciona correctamente, que se ha dimensionado debidamente para su aplicación y que todo el cableado está correcto.

Monitoreo térmico y comportamiento ante fallo térmico

Los controladores monitorean las temperaturas internas del módulo. Tal como se muestra a continuación, el controlador toma medidas según se incrementa la temperatura.



IMPORTANTE Si sigue los límites de temperatura ambiente (de entrada) recomendados y tiene en cuenta el espacio libre requerido alrededor del sistema, es poco probable que el controlador alcance la temperatura de advertencia inicial (fallo menor).

Para obtener más información acerca de las especificaciones del controlador CompactLogix 5380 y Compact GuardLogix 5380, consulte el documento CompactLogix 5380 and Compact GuardLogix 5380 Controller Specifications Technical Data, publicación [5069-TD002](#).

IMPORTANTE La presencia de cualquier advertencia de temperatura indica que es necesario tomar medidas para reducir la temperatura ambiente del módulo.

Puede encontrar instrucciones acerca de cómo utilizar el diagrama de lógica de escalera para comprobar un fallo menor en el documento Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publicación [1756-PM014](#).

Puede utilizar una instrucción GSV para leer el atributo MinorFaultBits del nombre de clase FaultLog. Si el bit de fallo menor de diagnóstico (bit 17) está establecido, es posible que haya un fallo menor de temperatura. Consulte la ficha Minor Faults del cuadro de diálogo Controller Properties de Logix Designer para determinar si el fallo menor es una advertencia de temperatura.

Notas:

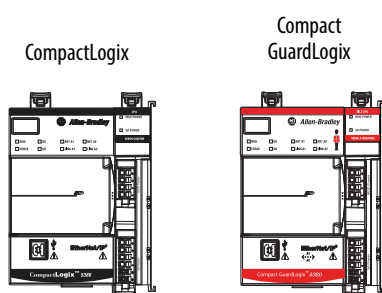
Opciones de seguridad

Tema	Página
Inhabilitación de un puerto Ethernet	323
Inhabilitación de la pantalla de estado de 4 caracteres	327
Inhabilitación de páginas web del controlador	332

Para mejorar la seguridad, puede inhabilitar la funcionalidad en su controlador.

Inhabilitación de un puerto Ethernet

Puede inhabilitar los puertos Ethernet del controlador con la aplicación Studio 5000 Logix Designer®, versión 28.00.00 y posteriores.



IMPORTANTE

Recuerde lo siguiente:

- Cuando se utiliza la aplicación Logix Designer, versión 29.00.00 y posteriores, puede inhabilitar cualquiera de los puertos Ethernet si el controlador utiliza el modo de doble IP o el modo lineal/DLR.
- Una vez inhabilitado un puerto Ethernet, se perderán todas las conexiones que se hayan establecido a través de dicho puerto.
- No se pueden inhabilitar los puertos Ethernet si el controlador está en modo de marcha o si los ajustes FactoryTalk® Security rechazan esta opción de edición.

Los puertos Ethernet regresarán al ajuste predeterminado después de que ocurra lo siguiente en el controlador:

- Restablecimiento de etapa 1
- Restablecimiento de etapa 2
- Se descarga un nuevo proyecto; en este caso, se aplican los ajustes del nuevo proyecto.
- Se borra un programa del controlador; a continuación se presentan varios ejemplos de situaciones en las que se borra el programa del controlador:
 - Ocurre un fallo mayor no recuperable.
 - Ocurre una actualización de firmware.

Debe volver a configurar los ajustes para inhabilitar un puerto Ethernet después de que el puerto se revierta a sus ajustes predeterminados.

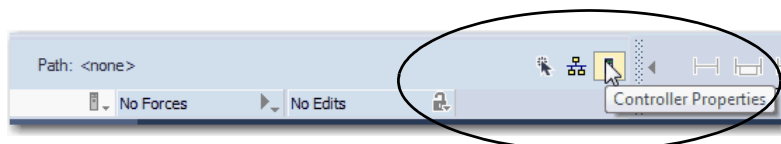
Hay dos métodos para inhabilitar el puerto Ethernet:

- [Inhabilitación del puerto Ethernet en la ficha Port Configuration en la página 324](#)
- [Inhabilitación del puerto Ethernet mediante una instrucción MSG en la página 325](#)

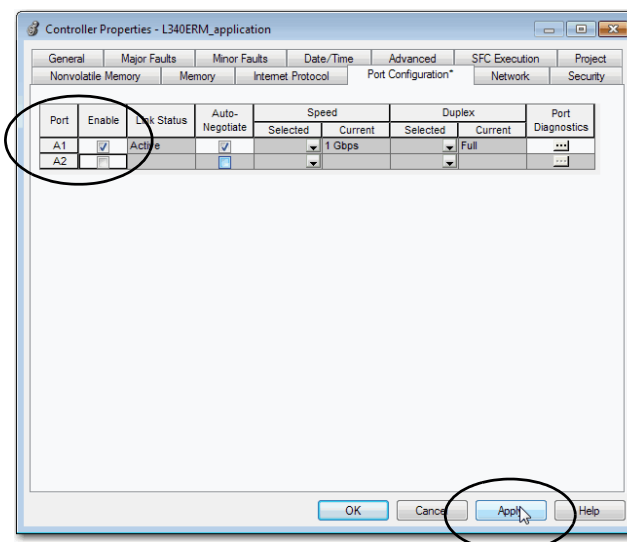
Inhabilitación del puerto Ethernet en la ficha Port Configuration

Puede inhabilitar el puerto Ethernet incorporado en el controlador. Este método retiene el ajuste en el proyecto, de manera que se inhabilita el puerto Ethernet cada vez que usted descarga el proyecto al controlador.

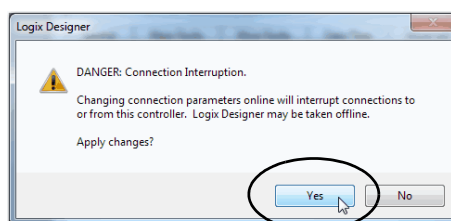
1. En la barra de herramientas Online, haga clic en el botón Controller Properties.



2. En el cuadro de diálogo Controller Properties, haga clic en la ficha Port Configuration.
3. En la ficha Port Configuration, desmarque la casilla de selección Enable correspondiente al puerto que desea inhabilitar y haga clic en Apply.



4. Si está en línea al hacer este cambio, haga clic en Yes en el cuadro de diálogo Alert.



- El cambio surtirá efecto inmediatamente.
 - Si está fuera de línea, el cambio surtirá efecto cuando descargue el programa al controlador.
5. En la ficha Port Configuration, haga clic en OK.

Inhabilitación del puerto Ethernet mediante una instrucción MSG

Puede utilizar un MSG genérico CIP con una ruta de THIS para ejecutar esta opción. No puede utilizar esta instrucción MSG para inhabilitar el puerto Ethernet en un controlador diferente.

1. Añada una instrucción MSG a su programa.

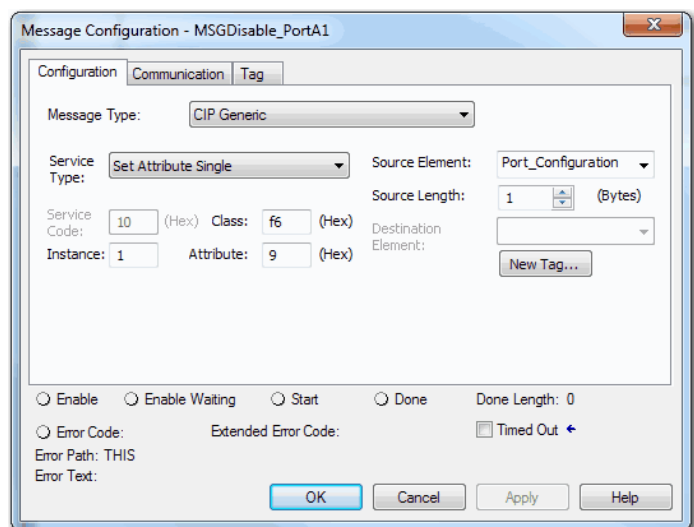
Este mensaje se debe ejecutar solo una vez; no es necesario que se ejecute con cada escán del programa.

IMPORTANTE No puede añadir una instrucción MSG a su programa si el controlador está en modo de marcha o si los ajustes de seguridad de FactoryTalk rechazan esta opción de edición.

2. Configure la ficha Configuration del cuadro de diálogo Message Configuration según se indica a continuación:

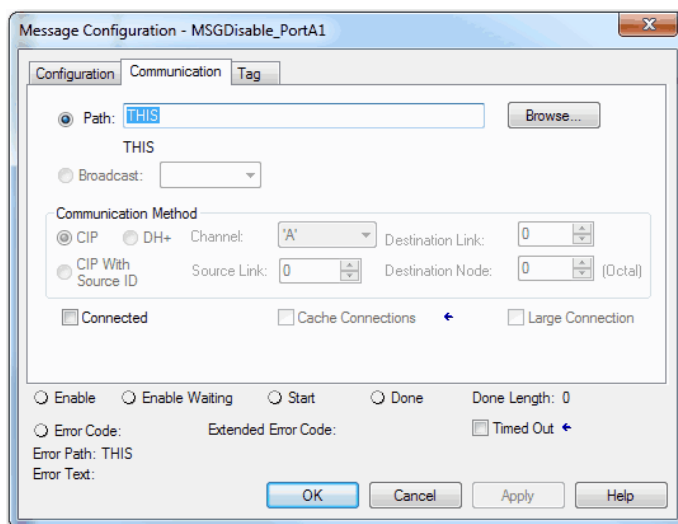
IMPORTANTE Los valores indicados a continuación se almacenan en la memoria NVS de tal forma que no es necesario ejecutar la instrucción MSG cada vez que se enciende el controlador.

- Message Type: CIP Generic
 - Service Type: Set Attribute Single
 - Instance: 1 para inhabilitar el puerto A1; 2 para inhabilitar el puerto A2
 - Class: f6
 - Attribute: 9
 - Source Element: tag del controlador del tipo de datos SINT
- En este ejemplo, el tag del controlador tiene el nombre Port_Configuration.
- Source Length: 1



- Configure la ficha Communication para utilizar una ruta THIS.

IMPORTANTE Los mensajes a THIS deben ser mensajes desconectados.



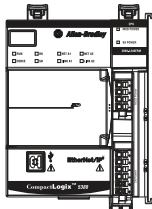
- Antes de habilitar la instrucción MSG, asegúrese de que el valor del tag Source Element es 2.

IMPORTANTE Puede volver a habilitar un puerto Ethernet después de que se haya inhabilitado.

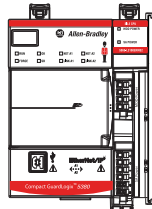
Para volver a habilitarlo, siga los pasos que se describen en esta sección. No obstante, antes de habilitar las instrucciones MSG, asegúrese de que el valor del tag Source Element es 1.

Inhabilitación de la pantalla de estado de 4 caracteres

CompactLogix



Compact GuardLogix



Con la aplicación Studio 5000 Logix Designer, versión 29.00.00 y posteriores, puede inhabilitar ciertas categorías de mensajes en la pantalla de estado de 4 caracteres:

- [Inhabilitación de todas las categorías de mensajes en la página 328](#)
- [Inhabilitación de categorías individuales de mensajes en la página 330](#)

Utiliza un MSG genérico CIP para ejecutar cada opción.

IMPORTANTE Estos mensajes del sistema siempre aparecen en pantalla y no se pueden inhabilitar:

- Mensajes de encendido (TEST, PASS, CHRG)
 - Mensaje de número de catálogo
 - Mensaje de revisión de firmware
 - Mensajes de fallos mayores/críticos
-

La pantalla de estado de 4 caracteres se revierte al ajuste predeterminado después de que ocurre una de estas acciones en el controlador:

- Restablecimiento de etapa 1
- Restablecimiento de etapa 2
- Se descarga un nuevo proyecto; en este caso, se aplican los ajustes del nuevo proyecto.
- Se borra un programa del controlador: a continuación, se presentan varios ejemplos de situaciones en las que se borra el programa:
 - Ocurre un fallo mayor no recuperable.
 - Ocurre una actualización de firmware.

Debe volver a configurar los ajustes para inhabilitar un puerto Ethernet después de que el puerto se revierta a sus ajustes predeterminados.

Inhabilitación de todas las categorías de mensajes

Al inhabilitar por completo la pantalla de 4 caracteres, se deja de mostrar la siguiente información:

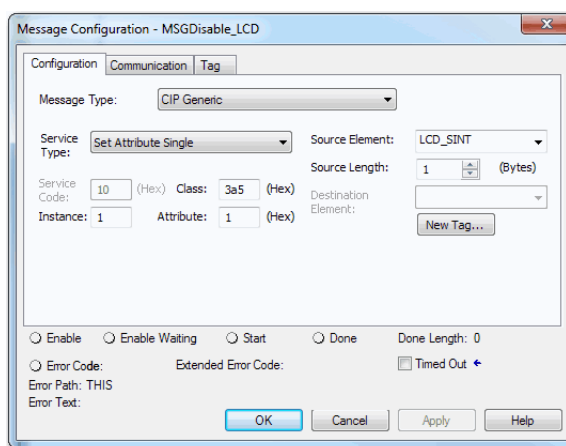
- Nombre del proyecto
- Estado del vínculo
- Estado del puerto
- Dirección IP

Siga estos pasos.

1. Añada una instrucción MSG a su programa.

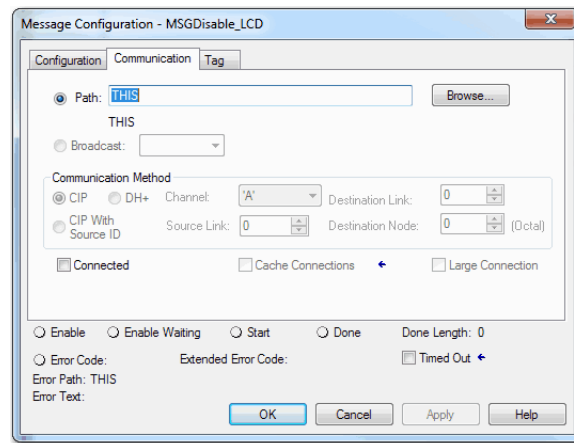
IMPORTANTE No puede añadir una instrucción MSG a su programa si el controlador está en modo de marcha o si los ajustes de seguridad de FactoryTalk rechazan esta opción de edición.

2. Configure la ficha Configuration del cuadro de diálogo Message Configuration según se indica a continuación:
 - Message Type: CIP Generic
 - Service Type: Set Attribute Single
 - Instance: 1
 - Class: 3a5
 - Attribute: 1
 - Source Element: tag del controlador del tipo de datos SINT
En este ejemplo, el tag del controlador tiene el nombre LCD_SINT.
 - Source Length: 1



- Configure la ficha Communication para utilizar una ruta THIS.

IMPORTANTE Los mensajes a THIS deben ser mensajes desconectados.



- Antes de habilitar la instrucción MSG, asegúrese de que el valor del tag Source Element sea 1.

IMPORTANTE Puede volver a habilitar la pantalla de 4 caracteres después de inhabilitarla.

Para volver a habilitar la pantalla de 4 caracteres, siga los pasos que se describen en esta sección. No obstante, antes de habilitar las instrucciones MSG, asegúrese de que el valor del tag Source Element sea 0.

Inhabilitación de categorías individuales de mensajes

Puede inhabilitar un subconjunto de la información que se muestra en el controlador. Puede inhabilitar los subconjuntos siguientes:

- Nombre del proyecto y estado del vínculo
- Estado del puerto y dirección IP

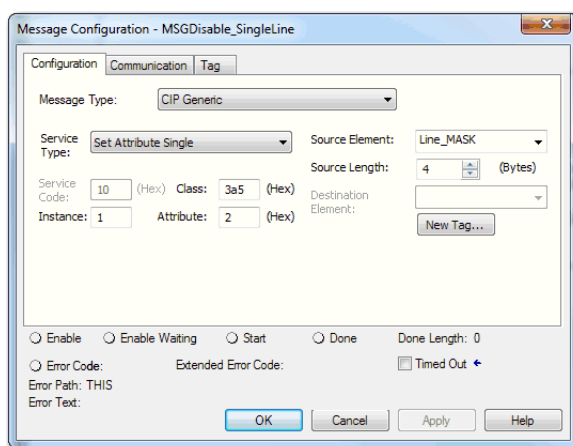
Siga estos pasos.

1. Añada una instrucción MSG a su programa.

Este mensaje se debe ejecutar solo una vez; no es necesario que se ejecute con cada escán del programa.

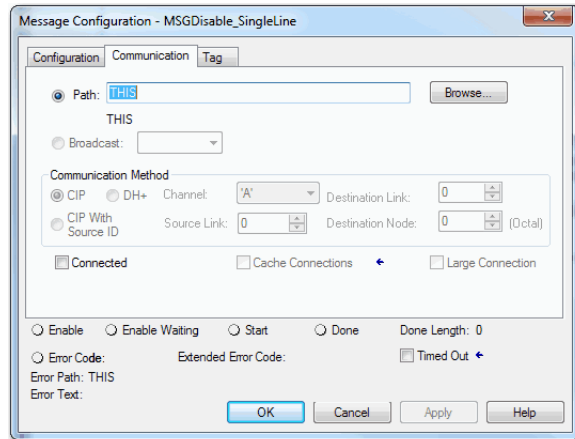
IMPORTANTE No puede añadir una instrucción MSG a su programa si el controlador está en modo de marcha o si los ajustes de seguridad de FactoryTalk rechazan esta opción de edición.

2. Configure la ficha Configuration del cuadro de diálogo Message Configuration según se indica a continuación:
 - Message Type: CIP Generic
 - Service Type: Set Attribute Single
 - Instance: 1
 - Class: 3a5
 - Attribute: 2
 - Source Element: tag del controlador del tipo de datos DINT. En este ejemplo, el tag del controlador tiene el nombre Line_MASK.
 - Source Length: 4



3. Configure la ficha Communication para utilizar una ruta THIS.

IMPORTANTE Los mensajes a THIS deben ser mensajes desconectados.

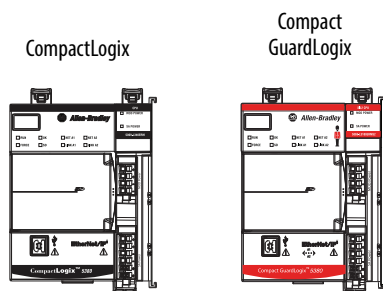


4. Antes de habilitar la instrucción MSG, establezca los bits del tag Source Element en los siguientes valores, según la información que quiera inhabilitar:
- Nombre del proyecto y estado del vínculo:
bit 0 de Source Element = 1
 - Estado del puerto y dirección IP:
bit 1 de Source Element = 1

IMPORTANTE Puede volver a habilitar los subconjuntos de información en la pantalla de 4 caracteres después de inhabilitarlos.

Para volver a habilitarlos, siga los pasos que se describen en esta sección. No obstante, antes de habilitar las instrucciones MSG, asegúrese de que el bit adecuado del valor del tag Source Element sea 0.

Inhabilitación de páginas web del controlador



Puede inhabilitar las páginas web del controlador con la aplicación Studio 5000 Logix Designer®, versión 28.00.00 y posteriores.

Utiliza un MSG genérico CIP para ejecutar esta opción.

Las páginas web del controlador regresarán al ajuste predeterminado después de que ocurra lo siguiente en el controlador:

- Restablecimiento de etapa 1
- Restablecimiento de etapa 2
- Se descarga un nuevo proyecto; en este caso, se aplican los ajustes del nuevo proyecto.
- Se borra un programa del controlador; a continuación se presentan varios ejemplos de situaciones en las que se borra el programa del controlador:
 - Ocurre un fallo mayor no recuperable.
 - Ocurre una actualización de firmware.

Debe volver a configurar los ajustes para inhabilitar las páginas web del controlador después de revertirse a sus ajustes predeterminados.

1. Añada una instrucción MSG a su programa.

IMPORTANTE No puede añadir una instrucción MSG a su programa si el controlador está en modo de marcha o si los ajustes de seguridad de FactoryTalk rechazan esta opción de edición.

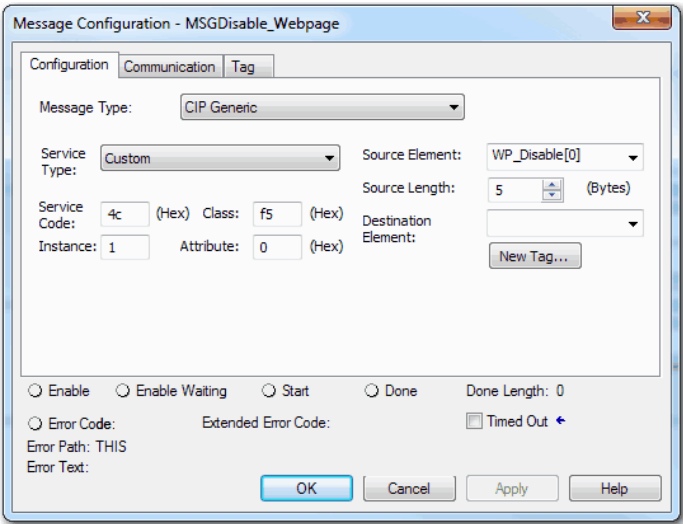
2. Configure la ficha Configuration del cuadro de diálogo Message Configuration según se indica a continuación:
 - Message Type: CIP Generic
 - Service Type: Custom
 - Service Code: 4c
 - Instance: 1
 - Class: f5
 - Attribute: 0
 - Source Element: tag del controlador del tipo de datos SINT[5].

En este ejemplo, el tag del controlador tiene el nombre WP_Disable y debe coincidir con este gráfico.

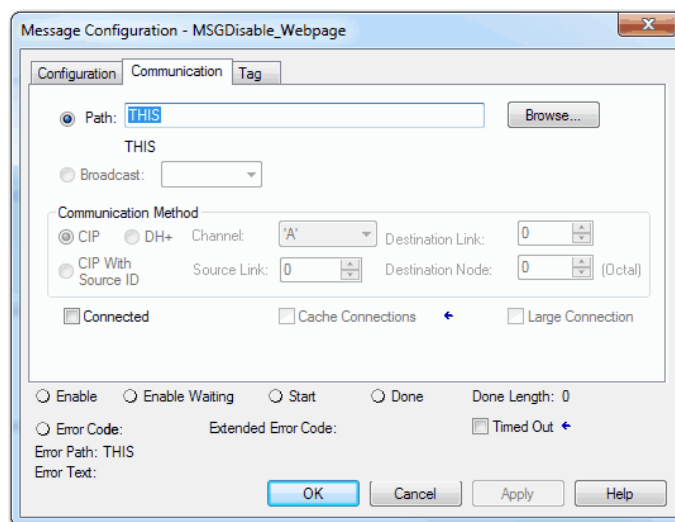
IMPORTANTE El tag Source Element en su proyecto de la aplicación Logix Designer debe coincidir con los valores que se muestran en el gráfico. Si utiliza valores diferentes de los mostrados, no se inhabilitarán las páginas web del controlador.

WP_Disable	{...}	{...}	Hex	SINT[5]
WP_Disable[0]	16#00		Hex	SINT
WP_Disable[1]	16#50		Hex	SINT
WP_Disable[2]	16#00		Hex	SINT
WP_Disable[3]	16#06		Hex	SINT
WP_Disable[4]	16#00		Hex	SINT

– Source Length: 5



3. Configure la ficha Communication para utilizar una ruta THIS.



4. Antes de habilitar la instrucción MSG, tenga en cuenta lo siguiente:

- Para inhabilitar la página web del controlador, el último elemento de la matriz SINT del Source Element debe ser 0.

▲ WP_Disable	{...}	{...}	Hex	SINT[5]
▶ WP_Disable[0]	16#00		Hex	SINT
▶ WP_Disable[1]	16#50		Hex	SINT
▶ WP_Disable[2]	16#00		Hex	SINT
▶ WP_Disable[3]	16#06		Hex	SINT
▶ WP_Disable[4]	16#00		Hex	SINT

- Para habilitar la página web del controlador, el último elemento de la matriz SINT del Source Element debe ser 1.

▲ WP_Disable	{...}	{...}	Hex	SINT[5]
▶ WP_Disable[0]	16#00		Hex	SINT
▶ WP_Disable[1]	16#50		Hex	SINT
▶ WP_Disable[2]	16#00		Hex	SINT
▶ WP_Disable[3]	16#06		Hex	SINT
▶ WP_Disable[4]	16#01		Hex	SINT

Cambio del tipo de controlador

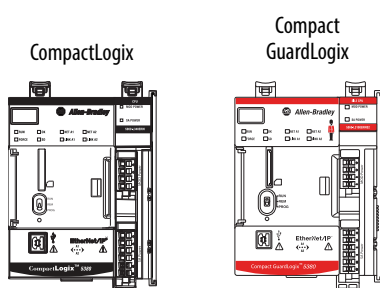
Tema	Página
Cambio de un controlador estándar a un controlador de seguridad	335
Cambio de un controlador de seguridad a uno estándar	336
Cambio de los tipos de controlador de seguridad	336

Los controladores de seguridad tienen requisitos especiales y no son compatibles con determinadas características estándar. Es necesario entender el comportamiento del sistema al cambiar el tipo de controlador (de controlador estándar a controlador de seguridad, o viceversa) en su proyecto del controlador.

El cambio del tipo de controlador afecta los siguientes aspectos:

- Funciones compatibles
- Configuración física del proyecto
- Propiedades del controlador
- Componentes del proyecto tales como tareas, programas, rutinas y tags
- Instrucciones Add-On de seguridad

Cambio de un controlador estándar a un controlador de seguridad



Puede cambiar de un controlador CompactLogix™ 5380 a un controlador Compact GuardLogix® 5380 en las aplicaciones de seguridad SIL 2/PLd.

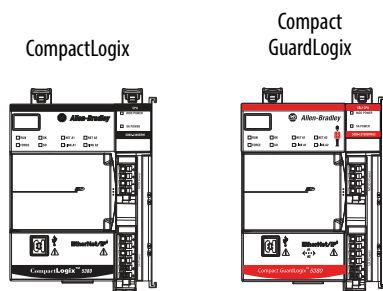
Una vez confirmado el cambio de un proyecto de controlador estándar a un proyecto de controlador de seguridad, se crean componentes de seguridad a fin de cumplir los requisitos mínimos de un controlador de seguridad:

- 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.

SUGERENCIA Si su proyecto ya contiene 32 tareas y usted intenta cambiar de un controlador estándar a un controlador de seguridad, no se convierte el proyecto y permanece con el controlador estándar.

- Se crean componentes de seguridad (la tarea de seguridad, el programa de seguridad, etc.).
- Se genera un número de red de seguridad (SNN) basado en tiempo para el chasis local.
- También se genera un número de red de seguridad (SNN) basado en tiempo para cada puerto EtherNet/IP incorporado.
- Toda función del controlador estándar que no sea compatible con el controlador de seguridad, como por ejemplo, redundancia, se retira del cuadro de diálogo Controller Properties (si aparece en dicho cuadro).

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:

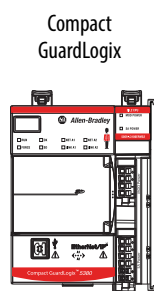
- Los dispositivos de E/S de seguridad y sus tags se eliminan.
- Los programas, las rutinas y la tarea de seguridad se cambian a programas, a rutinas y a una tarea estándar.
- Todos los tags de seguridad, salvo los tags de consumo de seguridad, se cambian por tags estándar. Los tags de consumo de seguridad se eliminan.
- Las asignaciones de tags de seguridad se eliminan.
- Los números de red de seguridad (SNN) se eliminan.
- 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 de seguridad homólogos no se eliminan, aunque no les queden conexiones.

- Las instrucciones pueden todavía referenciar a módulos eliminados y pueden producir errores de verificación.
- Los tags consumidos se eliminan cuando se elimina el módulo productor.
- A raíz de los cambios en el sistema antes descritos, no se verifican las instrucciones específicas de seguridad ni los tags de E/S de seguridad.

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 los tipos de controlador de seguridad



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

Si cambia de un controlador de seguridad con una aplicación SIL 3/PL_e a un controlador Compact GuardLogix 5380, la aplicación se cambia a SIL 2/PL_d.

Los números de red de seguridad también se conservan durante el cambio a un controlador Compact GuardLogix 5380.

A

- acceso externo** 245
- actualización de datos**
 - datos de E/S 196
- actualizar**
 - determinar frecuencia 196
- actualizar firmware**
 - AutoFlash 81
- actualizar firmware del controlador** 74...83
- almacenar**
 - en tarjeta de memoria 121
- almacene un proyecto** 120
- añadir módulos de E/S estando en línea** 195
- aplicación**
 - elementos 221
- aplicación Logix Designer** 131
 - añadir módulos de E/S estando en línea 195
 - añadir módulos de E/S locales a un proyecto 179...183
 - añadir módulos de E/S remotos a un proyecto 187...194
 - cambiar el modo EtherNet/IP 159
 - cambiar modo de funcionamiento del controlador 111
 - cargar proyecto 105
 - configurar el modo de doble IP 150
 - configurar el modo lineal/DLR 154
 - desarrollar aplicaciones 221
 - desarrollar aplicaciones de movimiento 277...281
 - descargar proyecto 102
 - diagnóstico 283...295
 - entrar en línea 95
 - establecer ruta de comunicación 95
 - instrucciones Add-On 233
 - instrucciones de movimiento 279
 - lenguajes de programación 232
 - obtener información de eje de movimiento 281
 - parámetros 231
 - programas 228
 - resolver problemas con categoría Connection 286
 - resolver problemas con categoría General 286
 - resolver problemas con categoría Module Info 287
 - resolver problemas con cuadro de diálogo Advanced Time Sync 293
 - resolver problemas con cuadro de diálogo de propiedades del módulo de E/S 285...288
 - resolver problemas con cuadro de diálogo Ethernet Port Diagnostics 291
 - rutina 230
 - rutinas 230
 - tags 231
 - tareas continuas 225
 - tareas de eventos 225
 - tareas de un proyecto 223
 - tareas periódicas 225

archivo de script

error 79

AutoFlash

actualizar 81

B

- barra en línea** 266
- bit ConnectionFaulted** 269
- bit RunMode** 269
- bloquear comunicación** 172
- bloqueo**
 - Consulte bloqueo de seguridad
- bloqueo de seguridad** 259
 - contraseña 260
 - controlador 260
 - efecto en la carga 100
 - icono 259
- borrar**
 - fallos 272
- botón de restablecimiento** 113
 - restablecimiento de etapa 1 114
 - restablecimiento de etapa 2 115

C

- cambio de controladores** 336
- cargar**
 - desde tarjeta de memoria 125...128
 - efecto de coincidencia de controlador 98
 - efecto de la firma de tarea de seguridad 100
 - efecto del bloqueo de seguridad 100
 - proyecto 105
- cargar un proyecto**
 - al encender 122
 - cuando se altera la memoria 122
 - iniciado por el usuario 122
- certificado de seguridad**
 - error 79
- CIP Safety** 219
- CIP Safety I/O**
 - dirección de nodo 199
 - firma de configuración 209
- codificación electrónica**
 - acerca de 184
- códigos de fallo** 314...316
 - fallos de seguridad mayores 274
 - pantalla de estado 273
 - utilizar instrucción GSV para obtener 238
- códigos de fallo de E/S**
 - en pantalla de estado de 4 caracteres 314...316
- CompactLogix 5380**
 - sistema de diseño 20
- comunicación**
 - bloquear 172
 - con dispositivos EtherNet/IP mediante interface de socket 139
 - permitir 172

- condición original** 214
 - restablecimiento de módulo 210
 - conexión**
 - estado 269
 - configuración de propiedad** 210
 - configurar**
 - movimiento 278
 - servidor DHCP 70
 - configurar siempre** 219
 - CONNECTION_STATUS** 247, 269
 - consumir datos** 173
 - consumir datos de tag** 253
 - contraseña**
 - establecer 261
 - controlador**
 - cambio de tipo 335...??
 - cargar proyecto 105
 - coincidencia 98
 - comportamiento 172
 - descargar proyecto 102
 - desigualdad de número de serie 104
 - discordancia de números de serie 101
 - entrar en línea 95
 - establecer ruta de comunicación 95
 - gestor de fallos 275
 - modos disponibles 109
 - número de serie 98
 - registro
 - bloqueo, desbloqueo de seguridad 260
 - firma de seguridad 262
 - sistema de diseño con 20
 - tipo de cambio ??...336
 - controlador de seguridad homólogo**
 - intercambio de datos 247
 - SNN 248
 - ubicación 248
 - copiar**
 - firma de seguridad 264
- ## D
- datos de control** 172
 - datos estándar en una rutina de seguridad** 256
 - desbloquea controlador** 260
 - desbloqueo de seguridad**
 - controlador 260
 - icono 259
 - descargar**
 - efecto de coincidencia de controlador 98
 - efecto de coincidencia de revisión de firmware 99
 - efecto del estado de seguridad 100
 - proyecto 102
 - diagnóstico**
 - con Logix Designer 283...295
 - con software RSLinx Classic 296
 - dirección de nodo** 199
 - dirección de red**
 - direccionamiento DNS 72
 - dirección IP duplicada**
 - detección 71
 - resolución 71
 - direccionamiento DNS** 66, 72
 - parámetros de red EtherNet/IP 66
 - direcciones IP**
 - definición 66
 - detección de direcciones duplicadas 71
 - modo de doble IP 143
 - solapamiento de rangos de direcciones IP 149
 - modo lineal/DLR 147
 - resolución de direcciones duplicadas 71
 - servidor DHCP 70
 - diseño**
 - sistema 20
 - drivers**
 - software RSLinx Classic 57...58, 59...60
- ## E
- E/S**
 - determinar actualización de los datos 196
 - E/S CIP Safety**
 - añadir 199
 - edición** 263
 - efecto del bloqueo de seguridad en la descarga** 100
 - eje**
 - obtener información 281
 - ejes**
 - consumidos 278
 - virtuales 278
 - elementos**
 - aplicación de control 221
 - eliminar**
 - firma de seguridad 264
 - en línea**
 - entrar 95
 - enviar mensajes** 175
 - error**
 - archivo de script 79
 - establecer dirección de red IP**
 - servidor BOOTP/DHCP 67...69
 - estado**
 - mensajes 311
 - estado de la red**
 - indicador 215, 217
 - estado de seguridad**
 - botón 262, 267
 - efecto en la descarga 100
 - firma de seguridad 262
 - ver 100, 266, 268
 - estado del controlador**
 - pantalla de estado de 4 caracteres
 - códigos de fallo de E/S 314...316
 - mensajes de estado general 309
 - mensajes de fallo 311

F**fallo**

- borrar 272
- conservación de hardware 321
- controlador no recuperable 272
- recuperable 273, 321
- seguridad no recuperable 268, 272
- temperatura de cpu 321

fallo de controlador no recuperable 272**fallo de seguridad no recuperable 268, 272**

- restablecer la tarea de seguridad 272

fallo recuperable 273

- borrar 273

fallos de seguridad mayores 274**FBD**

- uso 232

ficha major faults 273, 274**ficha minor faults 274****ficha safety 268**

- ver estado de seguridad 100, 268

ficha seguridad 260, 262

- bloqueo de seguridad 260
- controlador de bloqueo de seguridad 260
- desbloquear 260
- generar firma de seguridad 262
- módulo de repuesto 213

firma de configuración

- componentes 209
- copiar 209
- definición 209

firma de seguridad

- almacenamiento de un proyecto 120
- copiar 264
- descripción 51
- eliminar 264
- firma de configuración 209
- generar 262
- operaciones restringidas 263
- restricciones 265
- ver 267

firma de tarea de seguridad

- efecto en la carga 100
- efecto en la descarga 100

firmware

- actualizar con AutoFlash 81
- actualizar con ControlFLASH 76
- actualizar firmware del controlador 74...83
- certificado de seguridad, error 79
- necesario 75
- obtener 76

firmware del controlador

- actualizar con AutoFlash 81
- actualizar con ControlFLASH 76
- obtener 76

forzado 263**G****gateway 66****gestor de fallos**

- ejecutar en fallo del módulo de E/S 238

H**handshake 172****I****indicador de alimentación MOD 320****indicador de alimentación SA 320****indicador de estado FORCE 317****indicador de estado OK 318****indicador de estado RUN 317****indicador de estado SD 318****indicadores de estado**

- estado del controlador 317
- indicador de alimentación MOD 320
- indicador de alimentación SA 320
- indicador FORCE 317
- indicador OK 318
- indicador RUN 317
- indicador SD 318
- indicadores de estado de alimentación 320
- indicadores de estado de EtherNet/IP 319
- indicadores LINK A1 y LINK A2 319
- indicadores NET A1 y NET A2 319

indicadores de estado de alimentación 320

- indicador de alimentación MOD 320
- indicador de alimentación SA 320

indicadores de estado de EtherNet/IP 319

- indicadores LINK A1 y LINK A2 319
- indicadores NET A1 y NET A2 319

indicadores de estado del controlador 317

- indicador FORCE 317
- indicador OK 318
- indicador RUN 317
- indicador SD 318

indicadores de estado LINK A1 y LINK A2 319**indicadores de estado NET A1 y NET A2 319****inhabilitar**

- páginas web del controlador 332...334
- pantalla de 4 caracteres 328...329
- puerto Ethernet 323...326
- subconjunto de la información de la pantalla de 4 caracteres 330...331

inhabilitar los puertos Ethernet 116**instrucción GSV**

- monitorear una conexión 237
- utilizar para obtener códigos de fallo 238

instrucciones

- movimiento 279

instrucciones Add-On 233, 336**interface de socket 139****interruptor de modo**

- cambiar modo de funcionamiento del controlador 110
- posición 109

intervalo solicitado entre paquetes 247

- tag consumido 254

L**lenguajes de programación 232**

FBD 232
 lógica de escalera 232
 SFC 232
 texto estructurado 232

límite de tiempo de reacción

CIP Safety I/O 208

límite de tiempo de reacción de la conexión 208, 254**lógica de escalera**

uso 232

M**MajorFaultRecord 276****máscara de subred 66****memoria no volátil**

ficha 118

mensaje

acerca de 175

mensajes

estado de seguridad 311

mensajes de estado

en pantalla de estado de 4 caracteres 309

mensajes de fallo

en pantalla de estado de 4 caracteres 311

modo de doble IP 143

solapamiento de rangos de direcciones IP 149

modo de funcionamiento del controlador

cambiar con aplicación Logix Designer 111

cambiar con interruptor de modo 110

modo EtherNet/IP

cambiar 158...163

cambiar mediante el software RSLinx Classic 161

cambiar mediante la aplicación Logix Designer 159

configurar 150...157

configurar el modo de doble IP mediante el software RSLinx Classic 152

configurar el modo de doble IP mediante la aplicación Logix Designer 150

configurar el modo lineal/DLR mediante el software RSLinx Classic 156

configurar el modo lineal/DLR mediante la aplicación Logix Designer 154

modo de doble IP 143

solapamiento de rangos de direcciones IP 149

modo lineal/DLR 147

modo lineal/DLR 147**módulo**

propiedades

ficha de configuración 210

módulos 1732 ArmorBlock Guard I/O 185**módulos 1732D ArmorBlock I/O 185****módulos 1734 POINT I/O 185****módulos 1746 SLC I/O 185****módulos 1756 ControlLogix I/O 185****módulos 1769 Compact I/O 185****módulos 1794 FLEX I/O 185****módulos Compact 5000 177****módulos Compact I/O 5069 185****módulos de E/S**

acerca de los módulos de E/S locales 177

acerca de los módulos de E/S remotos 185

añadir estando en línea 195

añadir módulos de E/S locales al proyecto de la aplicación Logix Designer 179...183

añadir módulos de E/S remotos al proyecto de la aplicación Logix Designer 187...194

en una topología de red de anillo a nivel de dispositivos 185

en una topología de red en estrella 186

en una topología de red lineal 186

error de conexión 238

locales

ejemplo 178

remotos

ejemplo 185

módulos de E/S locales

acerca de 177

añadir a un proyecto de la aplicación Logix Designer 179...183

ejemplo 178

módulos de E/S remotos

1732 ArmorBlock Guard I/O 185

1732D ArmorBlock I/O 185

1734 POINT I/O 185

1746 SLC I/O 185

1756 ControlLogix I/O 185

1769 Compact I/O 185

1794 FLEX I/O 185

acerca de 185

añadir a un proyecto de la aplicación Logix Designer 187...194

Compact I/O 5069 185

ejemplo 185

monitorear conexiones de E/S 237**monitoreo térmico 321****movimiento**

acerca de 278

instrucciones 279

obtener información de eje 281

programa 279

multiplicador de interrupciones 255**multiplicador de retardo de red 255****N****nivel de rendimiento 49****nodos de una red EtherNet/IP 131****nombre de anfitrión 66****nombre de dominio 66**

número de red de seguridad

- asignación automática 90
- asignación manual 91
- basado en tiempo 90
- copiar 93, 206
- descripción 88
- establecer 204
- gestión 89
- pegar 93, 206

número de serie 98**O****obtener**

- información de eje 281

obtener firmware 76**optimizar el rendimiento de la red EtherNet/IP 137****P****página web Advanced Diagnostics**

- usar para resolver problemas 302

página web Browse Chassis

- usar para resolver problemas 304

página web Diagnostics

- usar para resolver problemas 300

página web Ethernet Port A1/A2

- usar para resolver problemas 301

página web Home

- usar para resolver problemas 298

página web Tasks

- usar para resolver problemas 299

páginas web del controlador

- inhabilitar 332...334
- resolver problemas con página web Advanced Diagnostics 302
- resolver problemas con página web Browse Chassis 304
- resolver problemas con página web Diagnostics 300
- resolver problemas con página web Ethernet Port A1/A2 301
- resolver problemas con página web Home 298
- resolver problemas con página web Tasks 299
- usar para resolver problemas 297...304

pantalla de 4 caracteres

- desactivar un subconjunto de la información en pantalla 330...331
- inhabilitar 328...329

pantalla de estado de 4 caracteres

- códigos de fallo de E/S 314...316
- mensajes de estado general 309
- mensajes de fallo 311

paquete de actualización de firmware 99**parámetros**

- del proyecto 231

parámetros de la red

- direccionamiento DNS 66
- direcciones IP 66
- gateway 66
- máscara de subred 66
- nombre de anfitrión 66
- nombre de dominio 66

período de tarea de seguridad 243, 247**permitir comunicación 172****producir datos 173****producir un tag 252****producir/consumir datos 173****programación 263****programas**

- del proyecto 228
- no priorizados 229
- priorizados 229

programas de seguridad 244**programas no priorizados 229****programas priorizados 229****propiedad**

- restablecer 210

propietario de la configuración

- identificación 210
- restablecer 210
- restablecimiento 212

protección de la aplicación de**seguridad 259...264**

- firma de seguridad 262
- seguridad 261

protección del modo marcha 264**proteger la aplicación de seguridad**

- bloqueo de seguridad 259

proteger la firma en el modo marcha 263**proyecto**

- cargar 105
- descargar 102
- elementos 221
- entrar en línea 95
- programas 228
- rutinas 230
- tareas 223

proyecto para coincidencia de controlador 98**proyectos**

- instrucciones Add-On 233
- lenguajes de programación 232
- parámetros 231
- tags 231

puertos Ethernet

- inhabilitar 116, 323...326
- modo de doble IP 143
- modo lineal/DLR 147

R

- recibir mensajes** 175
- red EtherNet/IP**
 - comunicación mediante interface de socket 139
 - driver de comunicación en el software RSLinx Classic 57...58, 59...60
 - nodos 131
 - optimizar el rendimiento de la red 137
 - parámetros para direccionamiento DNS 66
 - topología de red de anillo a nivel de dispositivos 134
 - topología de red en estrella 136
 - topología de red lineal 135
 - topologías 134...136
 - velocidades de comunicación de la red 137
- reemplazar**
 - módulo Guard I/O 213...219
- resolver problemas**
 - con categoría Connection en aplicación Logix Designer 286
 - con categoría General en aplicación Logix Designer 286
 - con categoría Module Info en aplicación Logix Designer 287
 - con cuadro de diálogo Advanced Time Sync de aplicación Logix Designer 293
 - con cuadro de diálogo de propiedades de módulo de E/S en aplicación Logix Designer 285...288
 - con cuadro de diálogo Ethernet Port Diagnostics en aplicación Logix Designer 291
 - con página web Advanced Diagnostics 302
 - con página web Browse Chassis 304
 - con página web Diagnostics 300
 - con página web Ethernet Port A1/A2 301
 - con página web Home 298
 - con página web Tasks 299
 - con páginas web del controlador 297...304
- restablecer**
 - propiedad 210
- restablecimiento de etapa 1** 114
- restablecimiento de etapa 2** 115
- restablecimiento de módulo** 210, 212
- restablecimiento del controlador**
 - etapa 1 114
 - etapa 2 115
- restricciones**
 - asignación de un tag de seguridad 256
 - cuando existe una firma de seguridad 263
 - programación 265
 - software 265
- restricciones de programación** 265
- retardo de red máximo observado**
 - restablecimiento 254
- revisión de firmware**
 - coincidencia 99
 - desigualdad 104
 - discordancia 101
- RSWho**
 - establecer ruta de comunicación 95
- ruta**
 - establecer 95

ruta de comunicación

- establecer 95
- rutina de fallo de programa** 275
- rutina de seguridad** 244
 - utilizar datos estándar 256
- rutinas** 230
 - del proyecto 230

S

- SafetyTaskFaultRecord** 276
- seguridad**
 - inhabilitar la pantalla de 4
 - caracteres 328...329
 - inhabilitar las páginas web del controlador 332...334
 - inhabilitar un puerto Ethernet 323...326
 - inhabilitar un subconjunto de la información de la pantalla de 4
 - caracteres 330...331
- sercos** 278
- servidor BOOTP/DHCP** 131
 - configuración de dirección de red IP 67...69
- SFC**
 - uso 232
- software**
 - añadir módulos de E/S estando en línea 195
 - añadir módulos de E/S locales a un proyecto de Logix Designer 179...183
 - añadir módulos de E/S remotos a un proyecto de Logix Designer 187...194
 - aplicación Logix Designer 131
 - cambiar el modo EtherNet/IP 159
 - cambiar modo de funcionamiento del controlador 111
 - cargar proyecto 105
 - configurar el modo de doble IP 150
 - configurar el modo lineal/DLR 154
 - desarrollar aplicaciones 221
 - desarrollar aplicaciones de movimiento 277...281
 - descargar proyecto 102
 - descripción general del movimiento 278
 - diagnóstico 283...295
 - establecer ruta de comunicación 95
 - instrucciones Add-On 233
 - instrucciones de movimiento 279
 - lenguajes de programación 232
 - obtener información de eje de movimiento 281
 - parámetros del proyecto 231
 - programas del proyecto 228
 - resolver problemas con categoría Connection 286
 - resolver problemas con categoría General 286
 - resolver problemas con categoría Module Info 287
 - resolver problemas con cuadro de diálogo Advanced Time Sync 293

- resolver problemas con cuadro de diálogo de propiedades del módulo de E/S 285...288
 - resolver problemas con cuadro de diálogo Ethernet Port Diagnostics 291
 - rutinas del proyecto 230
 - tags del proyecto 231
 - tareas 223
 - tareas continuas 225
 - tareas de eventos 225
 - tareas periódicas 225
 - cambiar el modo EtherNet/IP 158...163
 - configurar el modo EtherNet/IP 150...157
 - entrar en línea 95
 - restricciones 265
 - RSLink Classic 131
 - cambiar el modo EtherNet/IP 161
 - configurar el modo de doble IP 152
 - configurar el modo lineal/DLR 156
 - diagnóstico 296
 - driver de dispositivos Ethernet 59...60
 - driver EtherNet/IP 57...58
 - driver USB 61
 - software ControlFLASH** 76, 99
 - software RSLink Classic** 131
 - cambiar el modo EtherNet/IP 161
 - configurar el modo de doble IP 152
 - configurar el modo lineal/DLR 156
 - diagnóstico 296
 - driver de dispositivos Ethernet 59...60
 - driver EtherNet/IP 57...58
 - driver USB 61
 - software RSLogix 5000**
 - restricciones 265
 - solapamiento de rangos de direcciones IP** 149
 - sustituir**
 - configurar siempre habilitado 219
 - configure only... habilitado 214
- T**
- tag consumido** 247
- tag producido** 247
- tags**
 - acceso externo 245
 - alcance 246
 - asignar nombre 211
 - consumir 173
 - datos de seguridad producidos/consumidos 247
 - del proyecto 231
 - E/S de seguridad 247
 - producir 173
 - tipo de datos 246
- tags de seguridad**
 - asignación 256...258
 - bajo el control del controlador 246
 - descripción 245
- tarea continua** 225
- tarea de seguridad** 242
 - ejecución 244
 - prioridad 243
 - temporizador de vigilancia 243
- tareas**
 - continuas 225
 - en proyecto de la aplicación Logix Designer 223
 - eventos 225
 - periódicas 225
 - prioridad 227
- tareas de eventos** 225
- tareas del controlador** 223
- tareas periódicas** 225
- tarjeta de memoria**
 - cargar proyecto desde tarjeta 125...128
 - guardar proyecto en la tarjeta 121
 - otras tareas 128
- tarjeta SD**
 - almacenar en 121
 - cargar desde 125...128
 - otras tareas 128
- tarjetas 1784-SD1 y 1784-SD2**
 - almacenar en 121
 - cargar desde 125...128
 - otras tareas 128
- temperatura**
 - advertencia 321
 - límite 321
- temporizador de vigilancia** 243
- texto estructurado**
 - uso 232
- tiempo de reacción** 243
- tiempos de escán**
 - restablecer 265
- tipos de datos**
 - CONNECTION_STATUS 247
- topología de red de anillo a nivel de dispositivos** 134, 185
- topología de red en estrella** 136, 186
- topología de red lineal** 135, 186
- topologías**
 - anillo a nivel de dispositivos 134
 - disponibles en una red EtherNet/IP 134...136
 - estrella 136
 - lineal 135
- traductor de direcciones de red (NAT)**
 - establecer la dirección IP 202
- U**
- USB**
 - driver de comunicación en el software RSLink Classic 61
- utilizar instrucción GSV para obtener códigos de fallo** 238
- V**
- velocidades de comunicación de la red**
 - en una red EtherNet/IP 137
- ver**
 - estado de seguridad 100

Notas:

Servicio de asistencia técnica de Rockwell Automation

Utilice los siguientes recursos para obtener acceso a la información de asistencia técnica.

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

Comentarios sobre la documentación

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

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

Allen-Bradley, ArmorBlock, COMPACT 5000, Compact I/O, CompactLogix, ControlBus, ControlFLASH, ControlFLASH Plus, ControlLogix, DriveGuard, FactoryTalk, FLEX I/O, Guard I/O, Guardmaster, GuardLogix, Integrated Architecture, Kinetix, Logix 5000, On-Machine, PanelView, POINT I/O, POINT Guard I/O, PowerFlex, Rockwell Automation, Rockwell Software, RSLinx, RSNetWorx, SLC, Stratix y Studio 5000 Logix Designer son marcas comerciales de Rockwell Automation, Inc.

CIP, CIP Motion, CIP Safety, CIP Sync, ControlNet, DeviceNet y EtherNet/IP son marcas comerciales de ODVA, Inc.

Las marcas comerciales que no pertenecen a Rockwell Automation son propiedad de sus respectivas empresas.

www.rockwellautomation.com

Oficinas corporativas de soluciones de potencia, control e información

Américas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel.: (1) 414.382.2000, Fax: (1) 414.382.4444

Europa/Medio Oriente/África: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Bélgica, Tel.: (32) 2 663 0600, Fax: (32) 2 663 0640

Asia-Pacífico: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel.: (852) 2887 4788, Fax: (852) 2508 1846

Argentina: Rockwell Automation S.A., Av. Leandro N. Alem 1050, Piso 5, Ciudad Autónoma de Buenos Aires, Tel.: (54) 11.5554.4040, www.rockwellautomation.com.ar

Chile: Rockwell Automation Chile S.A., Av. Presidente Riesco 5435, Piso 15, Las Condes, Santiago, Tel.: (56) 2.290.0700, www.rockwellautomation.com.cl

Colombia: Rockwell Automation S.A., Edif. North Point, Carrera 7 N 156-78 Piso 19, PBX: (57) 1.649.9600, www.rockwellautomation.com.co

España: Rockwell Automation S.A., C/ Josep Pla, 101-105, Barcelona, España 08019, Tel.: 34 902 309 330, www.rockwellautomation.es

México: Rockwell Automation de S.A. de C.V., Av. Santa Fe 481, Piso 3 Col. Cruz Manca, Deleg. Cuajimalpa, Ciudad de México C.P. 05349, Tel. 52 (55) 5246-2000, www.rockwellautomation.com.mx

Perú: Rockwell Automation S.A., Av. Victor Andrés Belaunde N 147, Torre 12, Of.102, San Isidro Lima, Perú, Tel.: (511) 211-4900, www.rockwellautomation.com.pe

Puerto Rico: Rockwell Automation, Inc., Calle 1, Metro Office #6, Suite 304, Metro Office Park, Guaynabo, Puerto Rico 00968, Tel.: (1) 787.300.6200, www.rockwellautomation.com.pr

Venezuela: Rockwell Automation S.A., Edif. Allen-Bradley, Av. González Rincones, Zona Industrial La Trinidad, Caracas 1080, Tel.: (58) 212.949.0611, www.rockwellautomation.com.ve