Manual do usuário

Tradução de instruções originais

Controladores Compact GuardLogix 5370

Códigos de catálogo 1769-L30ERMS, 1769-L33ERMS, 1769-L33ERMOS, 1769-L36ERMS, 1769-L36ERMOS, 1769-L37ERMOS

Informações importantes do usuário

Leia este documento e os documentos listados na seção recursos adicionais sobre a instalação, configuração e operação deste equipamento antes de instalar, configurar, operar ou fazer a manutenção deste produto. É necessário que os usuários se familiarizem com instruções de instalação e fiação, além de requisitos de todos os códigos aplicáveis, lei e normas.

Atividades incluindo a instalação, os ajustes, colocando em serviço, utilização, montagem, desmontagem e manutenção devem ser realizadas por pessoal adequadamente treinado em conformidade com o código aplicável de práticas.

Se este equipamento for usado de uma maneira não especificada pelo fabricante, a proteção fornecida pelos equipamentos pode ser prejudicada.

Em nenhum caso a Rockwell Automation, Inc. será responsável por danos indiretos ou resultantes do uso ou da aplicação deste equipamento.

Os exemplos e diagramas contidos neste manual destinam-se unicamente a fins ilustrativos. A Rockwell Automation, Inc. não se responsabiliza pelo uso real com base nos exemplos e diagramas, devido a variações e requisitos diversos associados a qualquer instalação específica.

Nenhuma responsabilidade de patente será considerada pela Rockwell Automation, Inc. em relação ao uso de informações, circuitos, equipamentos ou softwares descritos neste manual.

É proibida a reprodução do conteúdo contido neste manual, integral ou parcial, sem permissão escrita da Rockwell Automation, Inc.

Ao longo do manual, sempre que necessário, serão usadas notas para alertá-lo sobre tópicos relacionados à segurança.

	**ADVERTÊNCIA:** Identifica informações sobre práticas ou circunstâncias que podem causar um explosão em uma área classificada, o que poderia levar a ferimentos pessoais ou morte, dano à propriedade ou perda econômica.
	**ATENÇÃO:** Identifica informações sobre práticas ou circunstâncias que podem levar a ferimentos pessoais ou morte, prejuízos a propriedades ou perda econômica. A atenção ajuda a identificar e evitar um risco e reconhecer a consequência.
IMPORTANTE	Identifica informações que são críticas para a aplicação bem sucedida e o entendimento do produto.

As etiquetas também podem estar sobre ou dentro do equipamento para fornecer precauções específicas.

	**PERIGO DE CHOQUE:** As etiquetas podem estar no equipamento ou dentro dele, por exemplo, um inversor ou um motor, para alertar as pessoas que pode estar presente uma tensão perigosa.
	**PERIGO DE QUEIMADURA:** As etiquetas podem estar no equipamento ou dentro dele, por exemplo, um inversor ou um motor, para alertar as pessoas que superfícies podem atingir temperaturas perigosas.
	**PERIGO DE ARCO ELÉTRICO:** As etiquetas podem estar sobre ou dentro do equipamento, por exemplo, um centro de controle de motores, para alertar as pessoas de potencial arco elétrico. Arco elétrico causará grave lesão ou morte. Vista o equipamento protetivo pessoal (PPE). Siga TODAS as especificações de regulamentação para as práticas de trabalho seguro e equipamento protetivo pessoal (PPE).

Capítulo 4

Configurar o controlador

Capítulo 5

Comunique-se pelas redes

Capítulo 6

Adicionar e configurar módulos de E/S padrão

Capítulo 7

Adição, configuração, monitoração e substituição de dispositivos de E/S de segurança CIP

Capítulo 8

Elementos de uma aplicação de controle

Capítulo 9

Desenvolver aplicações de segurança

Capítulo 10

Desenvolver Movimento Integrado em uma aplicação de rede EtherNet/IP

Capítulo 11

Comunicação com o Controlador

Capítulo 12

Monitorar o Status e Controlar Falhas

Capítulo 13

Guardar e carregar programas com um cartão Secure Digital

Esta publicação contém informações novas e atualizadas conforme indicado na tabela a seguir.

Tópico	Página
Incluídos os códigos de catálogo 1769-L33ERMOS, 1769-L36ERMOS e 1769-L37ERMOS.	Ao longo
Incluída a publicação Armor Compact GuardLogix na tabela 2.	12
Incluídos os três parágrafos introdutórios no Capítulo 1.	15
Incluída a nota de rodapé 'Disponível na versão do firmware 30' sobre o código de catálogo 1769-L37ERMOS.	15, 19, 20, 25, 55, 71, 75, 81, 163
Relocado o parágrafo introdutório na seção Sistema de controle Compact GuardLogix 5370 para a primeira página do Capítulo 1.	19
Feitas as seguintes mudanças na Tabela 1: • Incluída a linha 1769-ERMOS • Incluídas informações sobre a fonte de alimentação embutida • Atualizada a descrição do botão de reset • Incluídas as notas de rodapé 1 e 2	19
Incluídas linhas para novos códigos de catálogo e nós Ethernet correspondentes na Tabela 7.	71
Incluído conteúdo no parágrafo introdutório na subseção Versão do firmware compatível.	168
Incluída nota de rodapé na tabela na seção Download.	171

Observações:

Este manual descreve as tarefas necessárias para instalar, configurar, programar e operar um controlador CompactLogix 5370. Este manual é destinado a engenheiros de automação e desenvolvedores de sistemas de controle.

Os controladores CompactLogix 5370 são projetados para oferecer soluções em aplicações de pequeno e médio porte.

Terminologia

A tabela a seguir define os termos usados neste manual.

Abreviação	Termo completo	Definição
1oo2	Um de dois	Refere-se ao projeto comportamental de um sistema de segurança de multicontroladores.
CIP	Protocolo Industrial Comum	Protocolo de comunicação criado para aplicações de automação industrial.
Segurança CIP	Protocolo Industrial Comum – Certificado de Segurança	SIL 3/PLe versão classificada de CIP.
DC	Abrangência do diagnóstico	A relação de taxa de falha detectada no total.
DLR	Anel de nível de dispositivo	Um protocolo de comunicação que permite dispositivos multiportas EtherNet/IP operarem em topologia de anel.
EN	Norma Europeia	Norma europeia oficial.
GSV	Obter valor do sistema (GSV)	Uma instrução que recupera informações de status de controlador especificadas e as posiciona no tag de destino.
–	Multicast	A transmissão de informações de um emissor para vários receptores.
NAT	Conversão de endereço de rede	A conversão de um endereço Internet Protocol (IP) para um endereço IP diferente em outra rede.
PFD	Probabilidade de falha na demanda	Probabilidade média de um sistema falhar ao executar sua função de projeto quando solicitado.
PFH	Probabilidade de falha por hora	A probabilidade que um sistema tem de uma falha perigosa ocorrer por hora.
PL	Nível de desempenho	Classificação de segurança ISO 13849-1.
RPI	Intervalo do pacote requisitado	É a taxa esperada no tempo de produção de dados ao se comunicar em uma rede.
SNN	Número da rede de segurança	Número exclusivo que identifica uma seção de uma rede de segurança.
SSV	Set System Value (Definir Valor do Sistema)	Uma instrução que configura os dados do sistema do controlador.
–	Padrão	Um objeto, uma tarefa, um tag, um programa ou componente no seu projeto que não é um item relacionado à segurança.
–	Unicast	A transmissão de informações de um emissor para um receptor.

Recursos adicionais

Esses documentos contêm mais informações sobre produtos relacionados da Rockwell Automation.

Recurso	Descrição
Manual de referência de segurança dos sistemas de controle GuardLogix 5570 e Compact GuardLogix 5370, publicação1756-RM099	Oferece informações sobre requisitos de aplicativos de segurança para o controlador GuardLogix 5570 e Compact GuardLogix 5370 nos projetos com Studio 5000 Logix Designer.
Instruções de instalação dos controladores Armor Compact GuardLogix, publicação 1769-IN022	Fornece informações sobre como instalar, montar e conectar controladores Armor Compact GuardLogix a uma rede.
Manual do usuário do módulo scanner DeviceNet 1769-SDN, publicação 1769-UM009	Descreve como usar o módulo scanner 1769-SDN com controladores Compact GuardLogix.
Manual do usuário do módulo contador de alta velocidade Compact, publicação 1769-UM006	Descreve a operação de contador de alta velocidade para módulo unitário 1769-HSC quando usado com controladores Compact GuardLogix.
Instruções de instalação do módulo Scanner DeviceNet Compact I/O™, publicação1769-IN060	Descreve como instalar módulos Compact I/O.
Instruções de instalação de fontes de alimentação de expansão Compact I/O, publicação 1769-IN028	Descreve como fazer a fiação da fonte de alimentação Compact I/O 1769.
Instruções de instalação dos módulos Compact I/O, publicação 1769-IN088	Descreve como instalar módulos Compact I/O 1769 com qualquer controlador Compact GuardLogix.
Dados técnicos das especificações dos controladores CompactLogix™, publicação 1769-TD005	Formece especificações do controlador GuardLogix para todos os controladores Compact GuardLogix.
Guia de seleção do sistema CompactLogix, publicação 1769-SG001	Descreve informações sobre produtos usados em um sistema de controle CompactLogix para auxiliá-lo a projetar uma solução de controle.
Manual de referência sobre considerações de design de Ethernet, publicação ENET-RM002	Descreve os seguintes conceitos que você deve considerar ao projetar um sistema de controle que inclua uma rede EtherNet/IP: • visão geral EtherNet/IP • infraestrutura Ethernet • protocolo EtherNet/IP
Guia de aplicação da tecnologia de comutador incorporado a EtherNet/IP, publicação ENET-AP005	Descreve como usar a topologia de rede DLR.
Técnica de aplicação de interface de soquete EtherNet/IP, publicação ENET-AT002	Descreve as aplicações da interface de soquete.
Manual de referência de instruções do tempo de execução e uso de memória do controlador Logix5000™, publicação 1756-RM087	Explica como estimar o uso da a memória e o tempo de execução de logica programada, e como selecionar de diferentes opções de programação.
Técnica de aplicação de configuração CIP Sync e Arquitetura integrada®, publicação IA-AT003	Descreve tecnologia CIP Sync e como sincronizar relógios no sistema de Integrated Architecture™ Rockwell Automation.
Manual do usuário de configuração e inicialização de movimento integrado na rede EtherNet/IP, publicação MOTION-UM003	Descreve como configurar um Movimento Integrado por meio de aplicação de movimento EtherNet/IP e inicializar essa solução de movimento em um sistema de controle Logix5000.
Manual do usuário dos Servo-Drives Kinetix® 5500, publicação 2198-UM001	Fornece informações sobre como instalar, configurar, inicializar e fazer a localização de falhas para o sistema servo-drives Kinetix 5500. Também inclui requisitos para uso de inversores Kinetix 5500 em aplicações de segurança.
Manual do usuário dos Servo-Drives Kinetix 5700, publicação 2198-UM002	Fornece informações sobre como instalar, configurar, inicializar e fazer a localização de falhas para o sistema servo-drives Kinetix 5700. Também inclui requisitos para uso de inversores Kinetix 5700 em aplicações de segurança.
Manual de programação de procedimentos comuns aos controladores Logix5000, publicação 1756-PM001	Guia todos os níveis de usuário no desenvolvimento de projetos para controladores Logix5000 e fornece links para guias individuais com informações sobre tópicos como importação/exportação, mensagens, segurança e programação em diferentes linguagens.
Manual de referência sobre considerações de design dos controladores Logix5000, publicação 1756-RM094	Proporciona aos usuários avançados diretrizes para otimização e informações para escolhas do projeto do sistema.
Manual de referência de instruções dos controladores Logix, publicação 1756-RM009	Fornece informação sobre a definição de instrução Logix5000 que inclui instruções gerais, de movimento e de processo.
Manual de referência de instruções de movimento dos controladores Logix5000, publicação MOTION-RM002	Detalhes sobre como programar os controladores para aplicações de movimento.
Manual de programação de cartões de memória não volátil dos controladores Logix5000, publicação 1756-PM017	Explica a energização do controlador e situações de memória corrupta.
Manual de referência do conjunto de instruções de inversores/controles de processo de controladores Logix5000, publicação 1756-RM006	Detalhes sobre como programar o controlador para aplicações sequenciais.

Recurso	Descrição
Manual do usuário da unidade CA de frequência ajustável PowerFlex® 527, publicação 520-UM002	Fornece informações sobre como instalar, inicializar e fazer a localização de falhas no drive CS de frequência ajustável da série PowerFlex 520.
Orientação sobre fiação de automação industrial e aterramento, publicação 1770-4.1	Fornece orientações gerais para instalar um sistema industrial Rockwell Automation®.
Site de certificação de produto, http://www.rockwellautomation.com/global/certification/overview.page	Fornece declarações de conformidade, certificados, e outros detalhes de certificação.

Você pode visualizar ou descarregar publicações em http://www.rockwellautomation.com/global/literature-library/overview.page.

Para solicitar cópias impressas da documentação técnica, entre em contato com o distribuidor local Allen-Bradley ou o representante de vendas da Rockwell Automation local.

Observações:

Características gerais do sistema

Os controladores Compact GuardLogix® 5370 oferecem controle, comunicação e elementos de E/S de tecnologia de ponta, em um pacote de controle distribuído. Esta família de produtos inclui os seguintes controladores Compact GuardLogix:

- 1769-L30ERMS
- 1769-L33ERMS
- 1769-L33ERMOS
- 1769-L36ERMS
- 1769-L36ERMOS
- 1769-L37ERMOS(1)

O controlador Armor™ Compact GuardLogix (1769-L33ERMOS, 1769-L36ERMOS ou 1769-L37ERMOS(1)) combina um controlador Compact GuardLogix com uma fonte de alimentação em um gabinete classificado IP67 para montar em uma máquina. Para obter informações sobre como instalar o controlador Armor Compact GuardLogix, consulte Armor Compact GuardLogix Controllers Installation Instructions, publicação 1769-IN022.

Para uma descrição completa dos componentes e funcionalidade do sistema de controle CompactLogix 5370, consulte Tabela 1 e Tabela 2, respectivamente.

(1) Disponível na versão do firmware 30.

Requisitos da aplicação de segurança

O controlador Compact GuardLogix 5370 é certificado para uso em aplicações de segurança até e inclusive o nível de integridade de segurança (SIL) 3 e o nível de desempenho (PL)e, em que o estado desenergizado é o estado seguro. As especificações para a aplicação de segurança incluem a avaliação de probabilidade de taxas de falha (PFD e PFH), as configurações de tempo de reação do sistema e os testes de verificação de funcionamento que atendem critérios SIL 3/PLe.

Para as especificações do sistema de segurança SIL 3 e PLe, inclusive os intervalos de teste de validação de funcionamento, tempo de reação do sistema e cálculos PFD/PFH, consulte o Manual de referência de segurança dos sistemas de controladores GuardLogix 5570 e GuardLogix 5370, publicação 1756-RM099. É preciso ler, entender e satisfazer esses requisitos antes de operar um sistema de segurança SIL 3, PLe.

As aplicações de segurança SIL 3/PLe baseadas no requerem o uso de pelo menos um SNN (número da rede de segurança) e uma Assinatura de tarefa de segurança. Elas afetam a configuração do controlador e da E/S, bem como a comunicação de rede.

Para obter mais informações, consulte o Manual de referência de segurança dos sistemas de controladores GuardLogix 5570 e Compact GuardLogix 5370, publicação1756-RM099.

Número da rede de segurança

O SNN precisa ser um número exclusivo que identifique sub-redes de segurança. Cada subrede de segurança que o controlador usa para comunicação de segurança deve possuir um SNN único. Cada dispositivo de Segurança CIP deve também ser configurado com o SNN de subrede de segurança. O SNN pode ser atribuído automática ou manualmente.

Para obter informações sobre a atribuição do número da rede de segurança (SNN), consulte Gerenciamento do número da rede de segurança (SNN) na página 64.

Assinatura de tarefa de segurança

A assinatura da tarefa de segurança é composta por um número de identificação, data e hora que identificam exclusivamente a parte de segurança de um projeto. Isto inclui a lógica, dados e configuração de segurança. O sistema utiliza a assinatura da tarefa de segurança para determinar a integridade do projeto e para que seja possível verificar se fez-se download do projeto correto no controlador desejado. Criar, registrar e verificar a assinatura da tarefa de segurança é um item obrigatório do processo de criação de uma aplicação de segurança.

Consulte Gerar uma assinatura de tarefa de segurança na página 158 para obter mais informações.

Diferença entre componentes padrão e de segurança

Os slots no backplane Compact GuardLogix não utilizados pela função de segurança podem ser populados por outros módulos CompactLogix certificados para Baixa Tensão e Diretivas EMC.

Veja as certificações do produto em http://www.rockwellautomation.com/global/certification/overview.page para encontrar a certificação CE para a família de produtos de controle programável – CompactLogix e determinar quais módulos são certificados.

É necessário criar e documentar uma diferença clara, lógica e visível entre as partes padrão e de segurança do projeto do controlador. Para ajudar na criação dessa distinção, a aplicação Logix Designer fornece ícones de identificação de segurança para indicar a tarefa de segurança, programas, rotinas e componentes de segurança. Além disso, a aplicação Logix Designer utiliza um atributo de classe de segurança que é visível sempre que a tarefa, os programas, a rotina ou as propriedades das instruções adicionais de segurança forem exibidas.

O controlador não permite gravar dados de tags de segurança em dispositivos de IHM externos ou por meio de instruções de mensagem de controladores peer. A aplicação Logix Designer pode gravar os tags de segurança quando o controlador estiver desbloqueado por segurança, não tiver uma assinatura de tarefa de segurança e estiver operando sem falhas de segurança.

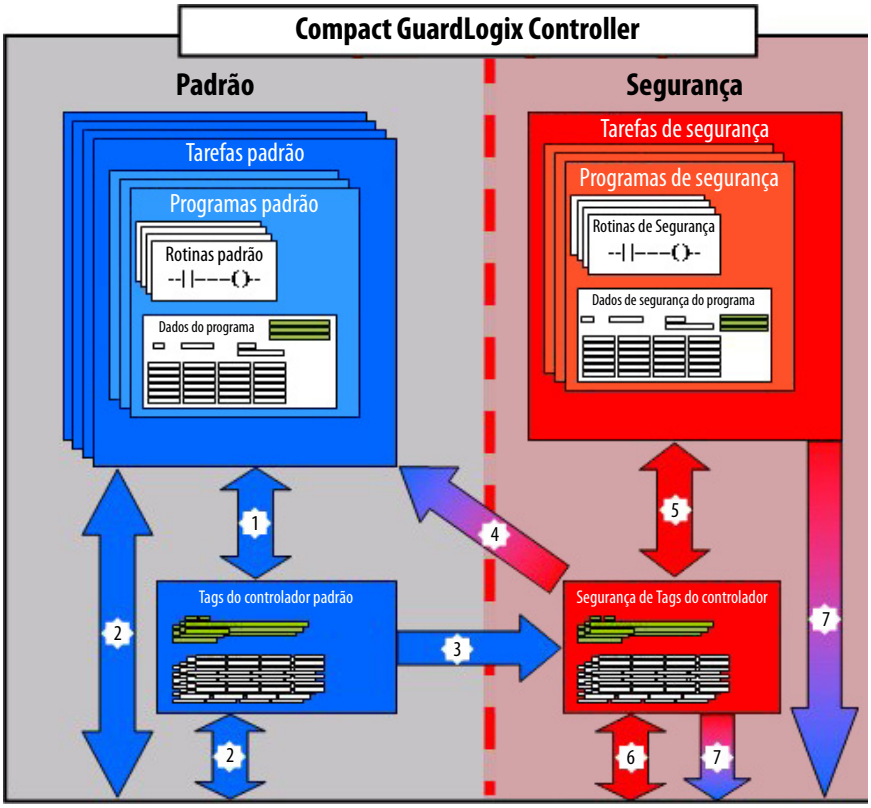
Dispositivos HMI

Os dispositivos de IHM podem ser usados com controladores Compact GuardLogix. Os dispositivos de IHM podem acessar tags padrão da mesma forma que qualquer controlador padrão. No entanto, os dispositivos de IHM não podem gravar em tags de segurança, pois elas são somente leitura para os dispositivos de IHM.

Recursos de fluxo de dados do controlador

Figura 1 explica os recursos de fluxo de dados padrão e de segurança do Compact GuardLogix controlador.

Figura 1 – Recursos de fluxo de dados



Núm.	Descrição	
1	Os tags padrões e lógicos comportam-se da mesma forma que na plataforma Logix padrão.	
2	Os dados dos tags padrão, do programa ou do controlador, podem ser compartilhados com dispositivos de IHM externos, microcomputadores e outros controladores.	
3	Compact GuardLogix os controladores são controladores integrados com a habilidade de mover (mapear) dados do tag padrão dentro dos tags de segurança para uso na tarefa de segurança.	
		**ATENÇÃO:** Estes dados não devem ser usados para controlar diretamente uma saída SIL 3/PLe.
4	Os tags de segurança do controlador podem ser lidos diretamente por uma lógica padrão.	
5	Os tags de segurança podem ser lidos ou escritos pela lógica de segurança.	
6	Tags de segurança podem ser trocadas entre controladores de segurança em uma rede Ethernet, incluindo os controladores GuardLogix 5570 e Compact GuardLogix 5370.	
7	Os dados de tag de segurança do programa ou do controlador podem ser lidos por dispositivos externos, como dispositivos de IHM, microcomputadores e outros controladores padrão.	
	IMPORTANTE	Uma vez que estes dados são lidos, eles são considerados dados padrão e não dados SIL 3/PLe.

Sistema de controle Compact GuardLogix 5370

Tabela 1 descreve os componentes usados em um sistema de controle Compact GuardLogix 5370 típico.

Tabela 1 – Componentes do sistema

Componente do Sistema	Descrição
Controller	Um dos controladores documentados nesta publicação
Fonte de alimentação	Uma das seguintes fontes de alimentação 1769 Compact I/O: • 1769-PA2 • 1769-PB2(2) • 1769-PA4 • 1769-PB4
Componentes das redes de comunicação	Quaisquer dos seguintes: • Rede EtherNet/IP via portas de rede EtherNet/IP incorporadas (comunicação de segurança e padrão) • Rede DeviceNet via módulo 1769-SDN (apenas para comunicação padrão)(3) • Conexão USB para programação e upgrades de firmware apenas
Software	• Aplicativo Logix Designer, versão 28.00.00 ou posterior • Software RSLinx® Classic, versão 3.80.*xx* ou posterior • Software RSNetWorx™ para DeviceNet, versão 25.00.00 ou posterior
Cartão Secure Digital (SD) para Memória Externa Não Volátil	• Cartão 1784-SD1 – Sai de fábrica com o controlador Compact GuardLogix 5370 e oferece 1 GB de memória • Cartão 1784-SD2 – Disponível para compra em separado e oferece 2 GB de memória
Módulos de E/S(1)	• Módulos de expansão locais – Módulos 1769 Compact I/O • E/S distribuída – Linhas múltiplas de produto de módulos de E/S em redes DeviceNet e EtherNet/IP
Botão Reiniciar	Se pressionado e mantido assim quando o controlador é ligado, este botão limpa o programa do usuário da memória interna do controlador e do parceiro de segurança interno.

(1) Sistemas de controle Armor Compact GuardLogix não suportam E/S dentro de seus gabinetes classificados IP67. Para obter E/S, você deve se conectar via EtherNet/IP a E/S distribuídas.
(2) Sistemas de controle Armor Compact GuardLogix têm esta fonte de alimentação dentro de seus gabinetes classificados IP67.
(3) Para comunicação de segurança, é necessário um módulo de ponte que vá do Ethernet ao DeviceNet, ver página 100.

Funcionalidade do Controlador

Tabela 2 descreve a funcionalidade disponível com controladores Compact GuardLogix 5370.

Tabela 2 – Funcionalidade de Controlador CompactLogix 5370

Nº. Núm.	Tarefas de Controlador Suportadas	Programas suportados por tarefa	Solução de Armazenamento de Energia Interna	Suporte a Topologia de Rede EtherNet/IP	Faixa de distância da fonte de alimentação	Tamanho de Memória de Usuário On-board		Suporte local dos Módulos Compact I/O	Eixos de movimento
						Padrão	Segurança		
1769-L30ERMS	32(2)	100	Sim – Eliminando a necessidade de uma bateria	Suporta as seguintes topologias: • Anel em nível de equipamento (DLR) • linear • Estrela tradicional	4	1	0.5	Até 8	4
1769-L33ERMS						2	1	Até 16	8
1769-L33ERMOS								–	
1769-L36ERMS						3	1.5	Até 30	16
1769-L36ERMOS								–	
1769-L37ERMOS(1)									

(1) Disponível na versão do firmware 30.
(2) Inclui uma tarefa de segurança.

Requisito de programação

Use Tabela 3 para identificar a ferramenta de programação e as versões para o uso com seus Compact GuardLogix controladores 5370.

Tabela 3 – Versões de software

Nº. Núm.	Ambiente Studio 5000®	Versão de software RSLinx Classic
1769-L30ERMS 1769-L33ERMS 1769-L33ERMOS 1769-L36ERMS 1769-L36ERMOS 1769-L37ERMOS(1)	28.00.00 ou posterior	3.80 ou posterior

(1) Disponível na versão do firmware 30.

As rotinas de segurança incluem instruções de segurança que são um subconjunto do conjunto de instruções de lógica ladder padrão e das instruções de aplicação de segurança. Programas agendados de acordo com a tarefa de segurança são compatíveis somente com a lógica ladder.

Tabela 4 – Recursos suportados

Recurso	Aplicação Studio 5000 Logix Designer	
	Tarefa de segurança	Tarefa padrão
Alarmes e eventos		X
Armazenamento no controlador	X	
Cartão de memória		
Conexões unicast para módulos de E/S de segurança em redes EtherNet/IP		
Conexões unicast para tags de segurança produzidos e consumidos		
Conversão de endereço de rede (NAT)		
Dados de controle de acesso		
Exportação e importação on-line de componentes de programação		
FBD (Diagramas de Blocos de Funções)		
Instruções adicionais	X	
Lógica ladder		
Movimento Integrado		
Rotinas de Fase de Equipamento		
Rotinas SFC (Controle Seqüencial de Funções)		
Segurança e conexões padrão	X	
Supervisor de firmware		
Tarefas de Evento		
Texto estruturado		
Troca de idiomas	X	

Para obter mais informações sobre como usar estes recursos, consulte o Manual de Programação de Procedimentos Comuns dos Controladores Logix5000™, publicação 1756-PM001 as publicações listadas em Recursos adicionais na página 12, e a ajuda online.

Instale o controlador

Precauções

ATENÇÃO: Ambiente e gabinete

Este equipamento foi projetado para utilização em ambientes industriais de Grau de Poluição 2, em aplicações de sobretensão de Categoria II (conforme definido na publicação IEC 60664-1), em altitudes de até 2000 metros (6562 pés), sem redução de capacidade.

Este equipamento é fornecimento como um equipamento do "tipo aberto". Ele deve ser montado junto a um gabinete que seja adequadamente projetado para essas condições ambientais específicas que estarão presentes e devidamente projetado para evitar ferimentos pessoais resultantes da acessibilidade à partes sob tensão. O gabinete deve ter propriedades à prova de fogo para impedir ou minimizar as chamas, de acordo com a classificação de 5 VA, ou ser aprovado para a aplicação se não for metálico. O interior do gabinete deve ser acessível somente pelo uso de uma ferramenta. Seções subsequentes desta publicação podem conter informações adicionais com relação aos graus de proteção do gabinete específicos que são necessários para atender determinadas certificações de segurança do produto.

Além desta publicação, consulte:

- Industrial Automation Wiring and Grounding Guidelines, publicação 1770-4.1, para obter especificações adicionais de instalação
- As normas NEMA 250 e IEC 60529, conforme aplicável, para obter explicações sobre os graus de proteção de diversos tipos de gabinetes

Aprovação Norte-Americana para Uso em Áreas Classificadas

The following information applies when operating this equipment in hazardous locations.	As informações a seguir destinam-se à operação deste equipamento em áreas classificadas.
Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local authority having jurisdiction at the time of installation.	Os produtos identificados "CL I, DIV 2, GP A, B, C, D" são adequados para uso em áreas classificadas Classe I Divisão 2 Grupos A, B, C, D, e áreas não classificadas apenas. Cada produto é fornecido com indicações na placa de identificação informando o código de temperatura da área classificada. Ao combinar produtos dentro de um sistema, o código de temperatura mais adversa (número "T" mais inferior) pode ser usado para ajudar a determinar o código de temperatura geral do sistema. As combinações de equipamentos em seu sistema estão sujeitas à fiscalização pela autoridade local competente no momento da instalação.
WARNING: EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**ADVERTÊNCIA:** RISCO DE EXPLOSÃO • Não desconecte o equipamento a menos que não haja energia ou a área não apresente risco. • Não remova conexões deste equipamento a menos que não haja energia ou a área não apresente risco. Fixe as conexões externas relativas a este equipamento usando parafusos, travas corrediças, conectores rosqueados ou outros meios fornecidos com este produto. • A substituição de componentes pode prejudicar a adequação com a Classe I, Divisão 2. • Este produto contém baterias que devem ser trocadas em uma área conhecida por não ser classificada.

Aprovação de áreas classificadas europeias

O seguinte se aplica a produtos marcados com  II 3 G. Tais módulos:

- São equipamentos do Grupo II, equipamentos Categoria 3 e em conformidade com as Especificações de Segurança e Saúde Essenciais relacionadas ao projeto e construção de tais equipamentos, dadas no Anexo II da Diretiva 94/9/EC. Consulte a declaração de conformidade EC em http://www.rockwellautomation.com/global/certification/overview.page para detalhes. O tipo de proteção usada é "Ex nA IIC T5 Gc" de acordo com EN60079-15. O código de temperatura específico está marcado no produto.
- Foram projetadas para o uso em áreas nas quais atmosferas explosivas causadas por gases, vapores, umidade, ar ou misturas de poeira são difíceis de ocorrer, ou passíveis de ocorrer ocasionalmente e por pouco tempo. Tais localizações correspondem à classificação de zona 2, de acordo com as diretrizes ATEX 1999/92/EC.
- Podem ter códigos de catálogo que terminam em 'K' para indicar revestimento isolante.
- Em conformidade com os padrões EN60079-0:2002+A11:2013, EN 60079-15:2010, número de certificado de referência DEMKO 15ATEX1388X

ADVERTÊNCIA: Condições especiais para o uso seguro:

- Este equipamento deve ser instalado em um gabinete certificado ATEX com uma taxa de proteção de entrada mínima de IP54 (conforme definido em IEC60529) e usado em um ambiente não acima de Grau de Poluição 2 (conforme definido em IEC/EN 60664-1) quando aplicado em ambientes de Zona 2. O gabinete deve utilizar uma porta ou tampa removível por ferramenta.
- Este equipamento deve ser usado dentro das suas taxas de especificação definidas pela Rockwell Automation.
- Deverão ser tomadas medidas para prevenir que a tensão nominal seja excedida por distúrbios transientes de mais de 140% da tensão nominal quando aplicados em ambientes de Zona 2.
- Este equipamento deve ser usado apenas com backplanes da Rockwell Automation com certificação ATEX.
- Fixe as conexões externas relativas a este equipamento usando parafusos, travas corrediças, conectores rosqueados ou outros meios fornecidos com este produto.
- Não desconecte o equipamento a menos que não haja energia ou a área não apresente risco.

Peças do Controlador Compact GuardLogix 5370

Estes números de peça estão inclusos na caixa quando você pedir o seu controlador:

- Controlador – Número de catálogo específico varia por ordem
- 1784-SD1 cartão Secure Digital (SD) com 1 GB de memória para armazenamento

  Um cartão SD 1784-SD2 com 2 GB de memória para armazenamento, ou dois cartões SD 1784-SD1 adicionais, também estão disponíveis caso você precise de memória adicional.

IMPORTANTE	A expectativa de vida de mídia flash é altamente dependente do número de ciclo de gravações que são realizados. Mídia não volátil utiliza uma técnica de nivelamento de utilização, ou tecnologia para prolongamento do tempo de serviço, mas deve-se evitar gravações frequentes. Evitar gravações frequentes quando carregar os dados Recomendamos que você grave dados em um buffer na memória do seu controlador e limite o número de gravações dos dados na mídia removível.

Instalar o Cartão Secure Digital (SD)

O controlador CompactLogix 5370 é enviado da fábrica com o cartão 1784-SD1 SD instalado.

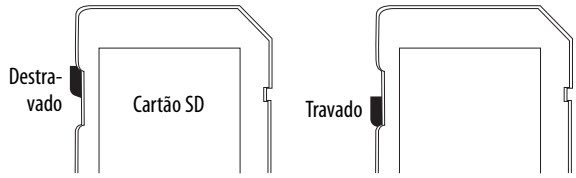
Complete estas etapas para reinstalar um cartão SD removível no controlador ou um novo cartão SD no controlador.

Recomenda-se deixar o cartão SD no controlador, mesmo quando ele não for usado. Se o controlador sofrer uma falha grave irrecuperável, informações sobre falhas adicionais são salvas no cartão.

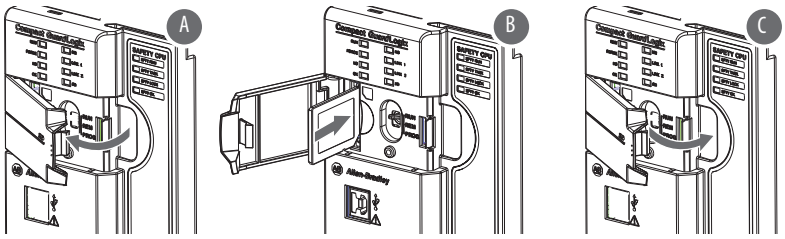
ADVERTÊNCIA: Ao inserir ou remover o cartão SD enquanto a alimentação estiver ligada, um arco elétrico pode ocorrer. Isto pode causar uma explosão em instalações reconhecidas como área classificada.

Antes de continuar, certifique-se de que não haja energia ou que a área não apresenta risco

1. Verifique se o cartão SD está travado ou destravado de acordo com a sua preferência. Considere isso ao decidir como travar o cartão antes da instalação:
   – Se o cartão está destravado, o controlador pode gravar dados nele ou ler dados a partir dele.



2. Abra a porta para o cartão SD (A).



3. Insira o cartão SD no slot do cartão SD.

   Você pode instalar o cartão SD em uma orientação apenas. O canto em relevo deve ficar no topo. Um logo de orientação está impresso no cartão.

   Se você sentir resistência ao inserir o cartão SD, puxe-o para fora e mude a orientação.

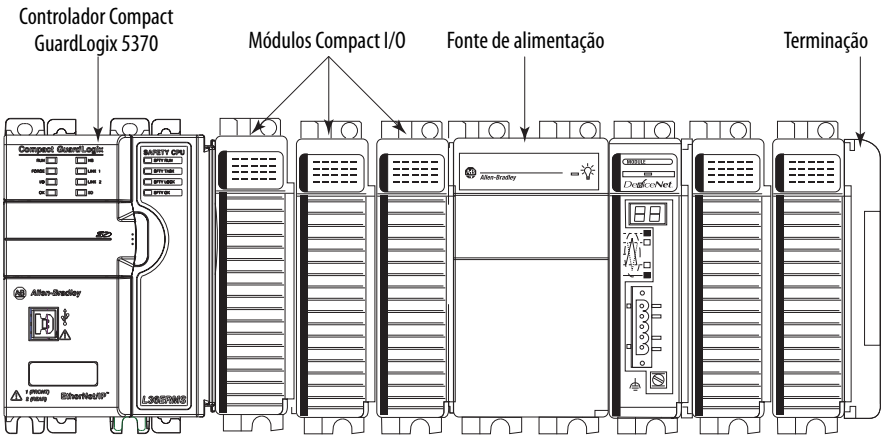
4. Pressione gentilmente o cartão até que clique no lugar (B).
5. Feche a porta do cartão SD (C).

Recomendamos que você mantenha a porta do cartão SD fechada durante a operação normal do sistema. Para obter mais informações sobre o cartão SD, consulte Capítulo 13.

Planejar o sistema

Quando você planejar o seu sistema controlador Compact GuardLogix 5370, considere o seguinte:

- O controlador é o equipamento mais para a esquerda no banco local.
- Apenas um controlador pode ser usado em um CompactBus 1769 local. O controlador suporta o banco local e até dois bancos mais.
- O controlador tem uma faixa de distância da fonte de alimentação de quatro. Esta classificação significa que o controlador deve estar dentro de quatro slots da fonte de alimentação. Você pode instalar até três módulos entre a fonte de alimentação e o controlador, como mostrado no gráfico a seguir.



- Os controladores são compatíveis com os vários módulos de expansão local em múltiplos bancos de E/S.

Nº. Núm.	Módulos de expansão local compatíveis, máx.
1769-L30ERMS	8
1769-L33ERMS	16
1769-L33ERMOS	–
1769-L36ERMS	30
1769-L36ERMOS 1769-L37ERMOS(1)	–

(1) Disponível na versão do firmware 30.

- Cada banco de E/S requer a sua própria fonte de alimentação.
- Você precisa eliminar o final do último banco em um sistema de controle CompactLogix 5370 Você pode usar como terminal um banco à direita ou à esquerda de outro banco, dependendo do design de seu sistema.

  Uma terminação 1769-EC*x* é necessária para terminar o final do último banco no sistema de controle.

  Por exemplo, se um sistema de controle CompactLogix 5370 usa um banco único, você precisa usar uma terminação direita 1769-ECR para eliminar a terminação direita do banco.

  Consulte Posicionamento físico de módulos de E/S na página 89 para especificações relacionadas aos módulos de expansão locais Compact I/O.

Para exemplos de sistemas de controle Compact GuardLogix 5370 que usam um banco ou múltiplos bancos, consulte Montar o sistema na página 27.

ATENÇÃO: Os sistemas de controlador CompactLogix 5370 não suportam remoção e inserção sob alimentação (RIUP). Estes eventos ocorrem quando o Sistema Controlador Compact GuardLogix 5370 está sob energia:

- Qualquer interrupção na conexão entre a fonte de alimentação e o controlador, por exemplo, removendo a fonte de alimentação, controlador, ou um módulo de E/S, pode sujeitar os circuitos lógicos a condições transientes acima dos limites normais de projeto e podem resultar em danos aos componentes do sistema ou comportamento inesperado.
- Remover uma terminação final ou um módulo de E/S causa uma falha no controlador e pode resultar também em dano aos componentes do sistema.

Montar o sistema

Você pode engatar um módulo Compact I/O™ adjacente ou fonte de alimentação Compact I/O 1769 a um controlador CompactLogix 5370 antes ou depois da montagem. Para instruções de montagem, consulte Dimensões do sistema na página 29 ou Monte o controlador em um Painel na página 30.

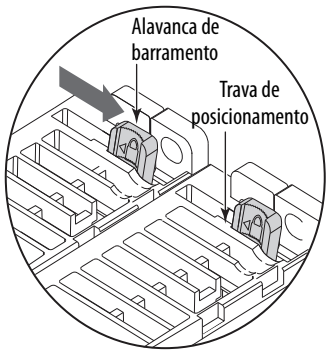
ATENÇÃO: Não remova ou substitua este módulo enquanto a alimentação estiver aplicada. Interrupção do backplane pode resultar em operação ou movimento da máquina não intencionais.

ADVERTÊNCIA: Desenergize antes de remover ou inserir este módulo. Se você inserir ou remover o módulo enquanto a alimentação estiver ligada, um arco elétrico pode ocorrer. Isto pode causar uma explosão em instalações reconhecidas como área classificada.

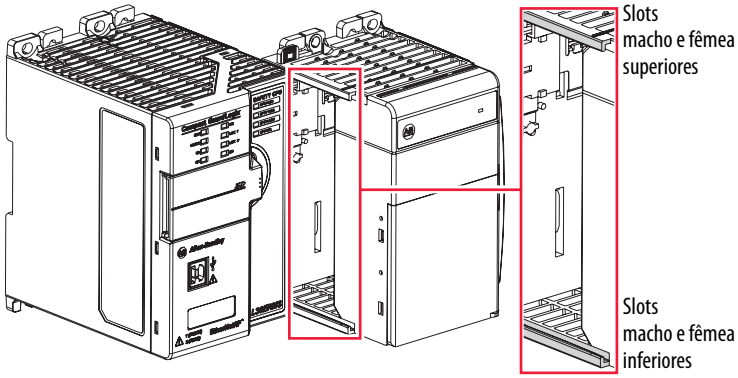
Antes de continuar, certifique-se de que não haja energia ou que a área não apresenta risco

Complete estes passos para instalar o controlador. Este exemplo descreve como montar uma fonte de alimentação Compact I/O 1769 ao controlador.

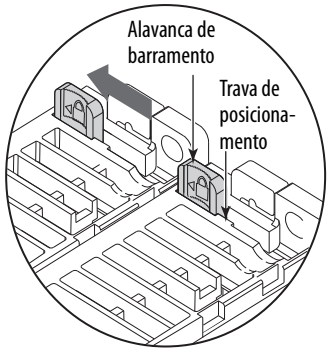
1. Verifique se a alimentação está desligada.
2. Use os seus dedos ou uma chave de fenda pequena para empurrar a alavanca do barramento da fonte de alimentação 1769 Compact I/O para trás levemente para limpar a trava de posicionamento.
3. Mova a alavanca de barramento para a direita da aba de posicionamento de modo a ficar na posição destravada.



4. Use os slots macho e fêmea superior e inferior para firmar o controlador e a fonte de alimentação juntos.



5. Mova a fonte de alimentação para trás ao longo dos slots macho e fêmea até que os conectores do barramento estejam alinhados uns com os outros.
6. Use os seus dedos ou uma chave de fenda para empurrar a alavanca do barramento da fonte de alimentação para trás levemente para limpar a trava de posicionamento.



7. Mova alavanca de barramento da fonte de alimentação para a esquerda da guia de posicionamento até que se ouça um clique, certifique-se de que está travada.
8. Caso seu sistema não utilize módulos de expansão local, use os slots macho e fêmea descritos anteriormente para engatar uma terminação Compact I/O 1769 no último módulo do sistema.

IMPORTANTE	É necessário instalar uma terminação na lateral direita do sistema do CompactLogix 5370 na extremidade do controlador ou na extremidade de qualquer módulo de expansão local que possa estar instalado no controlador.

9. Faça o cabeamento da fonte de alimentação 1769 Compact I/O de acordo com as orientações nas instruções de instalação de fontes de alimentação na expansão Compact I/O, publicação 1769-IN028.

   Se você estiver usando módulos de expansão locais, consulte Módulos de Expansão Locais na página 81.

Montar o sistema

ATENÇÃO: Este produto destina-se a ser montado em uma superfície bem aterrada como uma chapa de metal. Conexões adicionais de aterramento das presilhas de montagem ou do trilho DIN da fonte de alimentação (se usado) não são necessárias, a menos que a superfície de montagem não possa ser aterrada.

Consulte Orientações de Fiação e Aterramento para Automação industrial, Publicação Rockwell Automation 1770-4.1, para informações adicionais.

Você pode montar um sistema controlador Compact GuardLogix 5370 em um painel ou em um Barramento DIN.

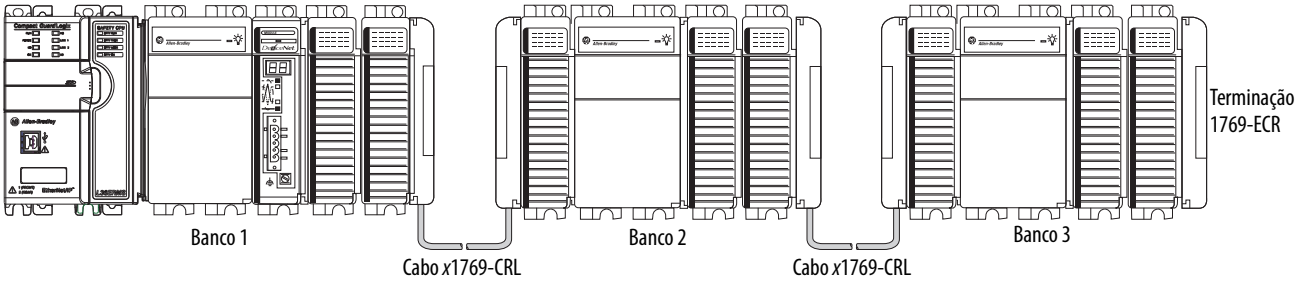
ATENÇÃO: Durante a montagem em trilho DIN ou em painel de todos os equipamentos, certifique-se de que detritos (como lascas de metal ou pedaços de fio) sejam impedidos de cair no controlador. Detritos que caiam no controlador podem causar dano enquanto o controlador estiver energizado.

Um sistema de controle CompactLogix 5370 precisa ser montado de modo que os módulos estejam na horizontal, um em relação do outro. Se você separar módulos em bancos múltiplos, os bancos podem ser verticais ou horizontais um em relação ao outro.

Figura 2 mostra exemplos de sistemas com módulos de expansão locais incluídos.

Figura 2 – Exemplo de bancos e configurações de sistema

Orientação Horizontal



Orientações verticais

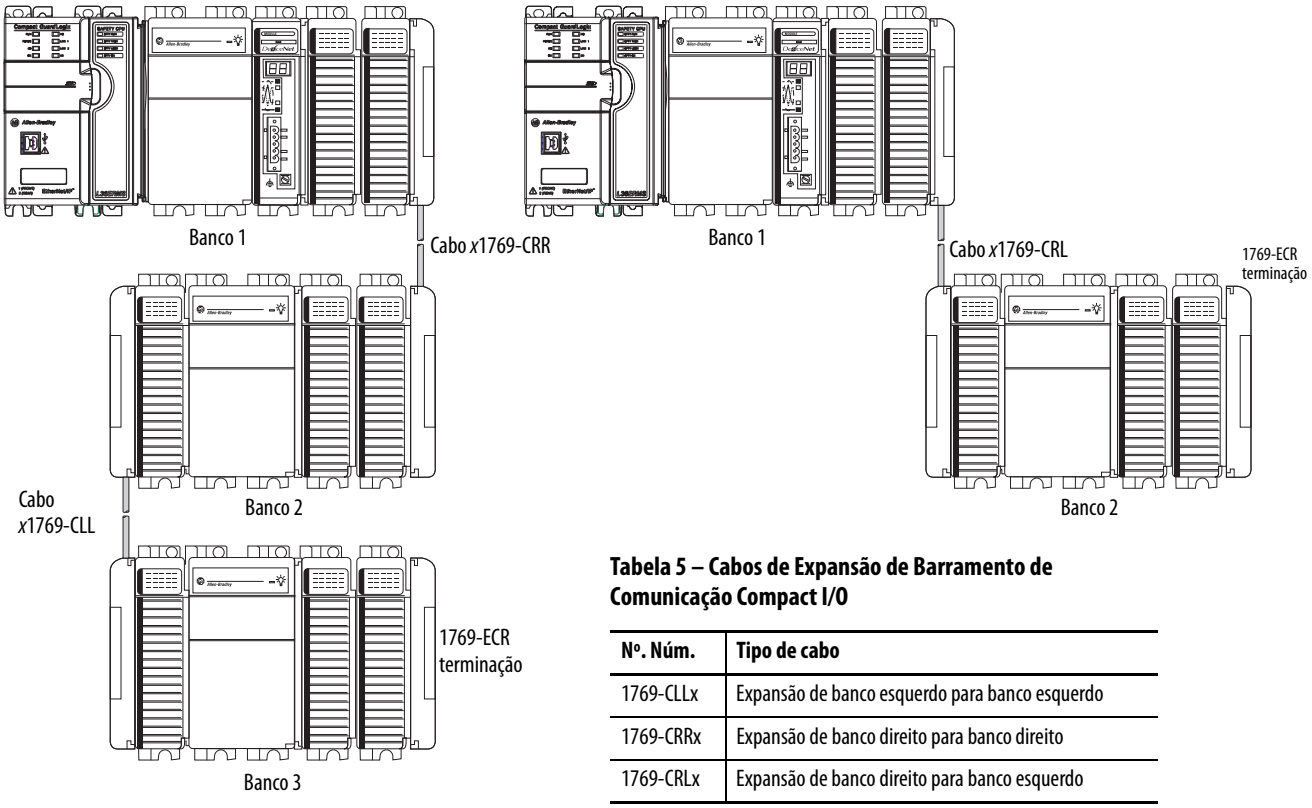


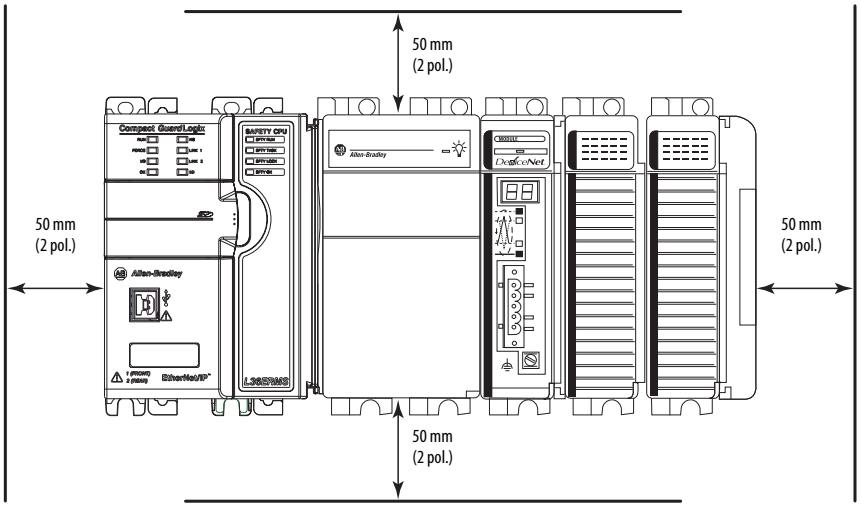
Tabela 5 – Cabos de Expansão de Barramento de Comunicação Compact I/O

Nº. Núm.	Tipo de cabo
1769-CLLx	Expansão de banco esquerdo para banco esquerdo
1769-CRRx	Expansão de banco direito para banco direito
1769-CRLx	Expansão de banco direito para banco esquerdo

Para obter mais informações sobre estes cabos, consulte as Instruções de Instalação de Cabos de Expansão de Barramento de Comunicação 1769 Compact I/O, publicação 1769-IN014.

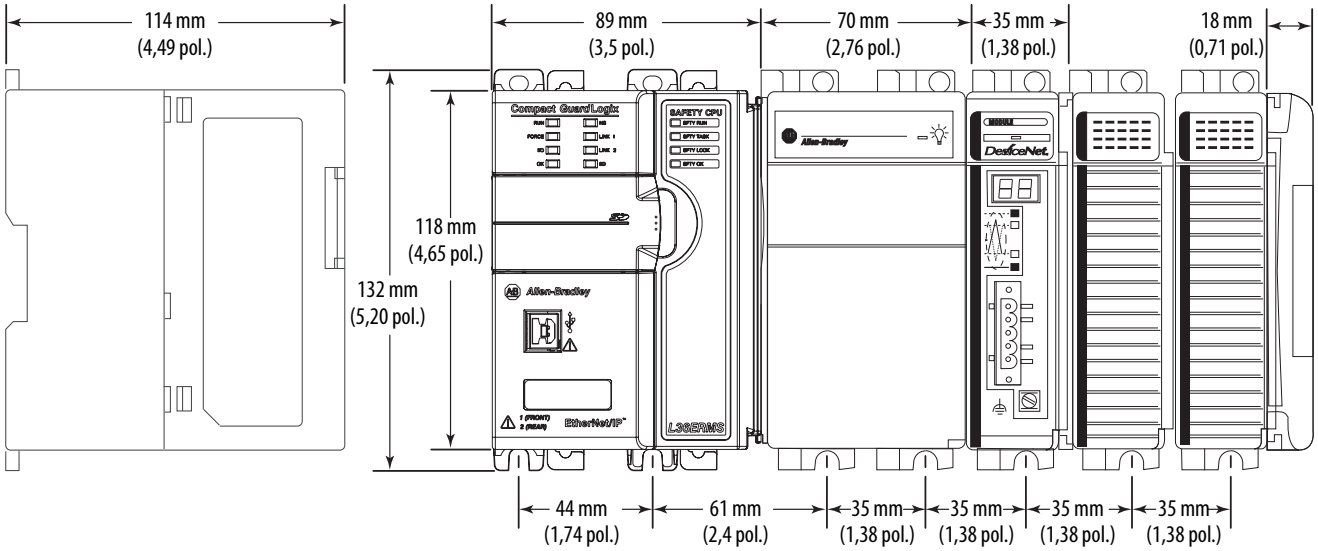
Espaçamento Mínimo

Mantenha o espaçamento de paredes do gabinete, condutores e equipamentos adjacentes. Permita 50 mm (2 pol.) de espaço em todos os lados, como mostrado. Isso fornece ventilação e isolamento elétrico.



Dimensões do sistema

Este gráfico mostra as dimensões do sistema.



Monte o controlador em um Painel

Use dois parafusos com cabeça em forma trapezoidal M4 ou #8 para montar o controlador. Os parafusos de fixação são necessários em todos os módulos. Use este procedimento para usar os módulos montados como padrão para fazer furos no painel.

IMPORTANTE Devido a uma tolerância de furo de montagem para módulo, é importante seguir estes procedimentos.

1. Em uma superfície de trabalho limpa, monte no máximo três módulos.
2. Usando os módulos montados como um gabarito, marque cuidadosamente o centro de todos os furos de montagem do módulo no painel.
3. Retorne os módulos montados à superfície de trabalho limpa, incluindo qualquer módulo montado previamente.
4. Perfure e faça a rosca dos furos de montagem para o parafuso M4 ou #8 recomendado.
5. Coloque os módulos de volta no painel e verifique o devido alinhamento do furo.

   DICA Quando o módulo está montado no painel, a placa de aterramento (onde você instala os parafusos de montagem) aterra-se ao módulo.
6. Use os parafusos de fixação para prender os módulos ao painel.

   DICA Se você está montando mais módulos, monte apenas o último deste grupo e coloque os outros de lado. Isto reduz o tempo de remontagem quando você está perfurando e rosqueando o próximo grupo de módulos.
7. Repita os passos 1 a 6 para quaisquer módulos faltantes.

Monte o controlador em um trilho DIN

Você pode montar o controlador GuardLogix 5370 nos seguintes trilhos DIN:

- EN 50 022 – 35 x 7,5 mm (1,38 x 0,30 pol.)
- EN 50 022 – 35 x 15 mm (1,38 x 0,59 pol.)

ATENÇÃO: Este controlador está aterrado ao rack através do trilho DIN. Use um trilho DIN de aço cromado amarelo revestido de zinco para garantir o aterramento adequado. O uso de trilho DIN de outros materiais (por exemplo, alumínio ou plástico) que possam corroer, oxidar ou sejam maus condutores pode resultar em aterramento incorreto ou intermitente. Fixe o trilho DIN à superfície de montagem a cada 200 mm (7,8 pol.) aproximadamente e use postes adequadamente.

1. Antes de montar o controlador num trilho DIN, feche as travas do trilho DIN.
2. Pressione a área de montagem do trilho DIN do controlador contra o trilho DIN.

   As travas momentaneamente abrem e travam-se no lugar.

Conecte Energia ao Sistema de Controle

A maneira que você conecta a energia no sistema de controlador Compact GuardLogix 5370 é baseada na fonte de alimentação Compact I/O 1769 que seu aplicativo usa. Para obter mais informações sobre a conexão de energia ao seu sistema, consulte as Instruções de instalação de fontes de alimentação de expansão Compact I/O, publicação 1769-IN028.

Conecte ao Controlador via um Cabo USB

O controlador GuardLogix 5370 tem uma porta USB que usa um receptáculo Tipo B. A porta é compatível com USB 2.0 e opera a 12 Mbps.

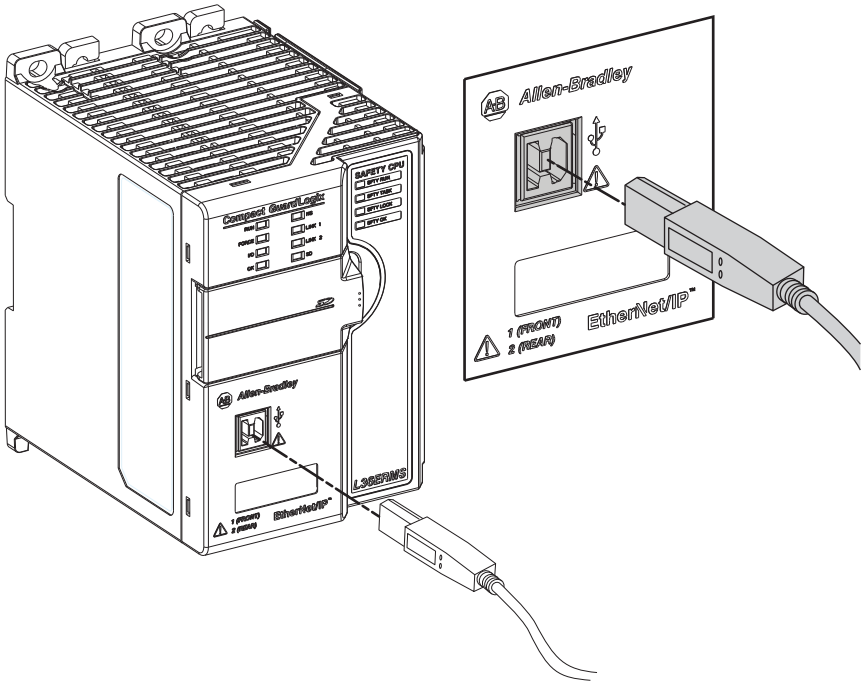
Use um cabo USB para conectar o seu computador à porta USB. Com esta conexão, você pode fazer upgrade de firmware e fazer download de programas para o controlador diretamente do seu computador.

ATENÇÃO: A porta USB destina-se apenas a fins de programação local temporária e não para conexão permanente.

O cabo USB não deve exceder 3,0 m (9,84 pés) e não pode conter hubs.

ADVERTÊNCIA: Não use a porta USB em áreas classificadas.

Plugue o cabo USB no controlador CompactLogix 5370 como mostrado.



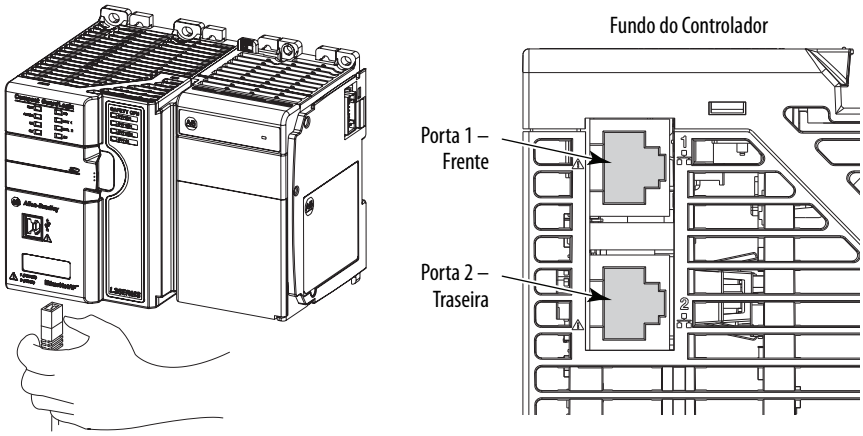
Conecte o Controlador a Uma Rede EtherNet/IP

ADVERTÊNCIA: Se você conectar o cabo de comunicação com alimentação aplicada a este módulo ou a qualquer equipamento na rede, um arco elétrico pode ocorrer. Isto pode causar uma explosão em instalações reconhecidas como área classificada.

Antes de continuar, certifique-se de que não haja energia ou que a área não apresenta risco

Conecte o conector RJ45 do cabo Ethernet a uma das portas Ethernet no controlador. As portas estão no fundo do controlador.

ATENÇÃO: Não plugue um cabo de rede DH-485 ou um cabo NAP numa porta Ethernet. Comportamento indesejável ou dano à porta pode acontecer.



IMPORTANTE Este exemplo mostra como conectar o controlador à rede por uma porta. Dependendo da sua aplicação de topologia de rede, você pode conectar ambas as portas do controlador à rede EtherNet/IP.

Para mais informações sobre topologias de rede EtherNet/IP, consulte Comunicação de Rede EtherNet/IP na página 70.

Conectando a Diferentes Topologias de Rede EtherNet/IP

Os controladores CompactLogix 5370 têm tecnologia de chave incorporada e duas portas EtherNet/IP que permitem que você os use em diversas topologias de rede EtherNet/IP:

- Topologia de rede de anel em nível de equipamento – Ambas as portas no controlador estão conectadas à rede com especificações sobre como as conexões são feitas.
- Topologia de rede linear – Ambas as portas no controlador estão conectadas à rede com requerimentos sobre como as conexões são feitas.
- Topologia de rede em estrela – Uma porta no controlador está conectada à rede.

Para obter mais informações, consulte Comunicação de Rede EtherNet/IP na página 70.

Completar a configuração do controlador

Para concluir as tarefas descritas neste capítulo, é necessário que o software descrito na tabela a seguir esteja instalado em seu computador.

- RSLinx® Classic
- Ambiente Studio 5000®
- Servidor BOOTP-DHCP (instalado com RSLinx Classic)
- Software ControlFLASH™ (instalado junto com o ambiente Studio 5000)

Controladores CompactLogix® 5370 requerem um endereço de rede de Protocolo de Internet (IP) para operarem em uma rede EtherNet/IP.

Defina o endereço IP

O endereço IP identifica exclusivamente o controlador. O endereço IP está na forma *xxx.xxx.xxx.xxx* onde cada *xxx* é um número de 000 a 254 com algumas exceções para valores reservados. Estes números são **exemplos** de valores reservados que você não pode usar:

- 000.*xxx.xxx.xxx*
- 127.*xxx.xxx.xxx*
- 224 a 255.*xxx.xxx.xxx*

Alguns outros valores específicos são reservados com base em uma frequência aplicação a aplicação.

Você pode completar uma dessas tarefas dependentes das condições do sistema.

- **Defina** o endereço IP para um controlador que já esteja com um endereço IP atribuído a ele.
- Mude o endereço IP para um controlador que já esteja com um endereço IP atribuído a ele.

IMPORTANTE	Os controladores Compact GuardLogix 5370 têm duas portas de EtherNet/IP para se conectar a uma rede EtherNet/IP; você não pode instalar nenhuma porta adicional nestes controladores. As portas carregam o mesmo tráfego de rede como parte da chave incorporada do controlador. Porém, o controlador usa apenas um endereço IP.

Você deve configurar um endereço IP de controlador CompactLogix 5370 quando o controlador é energizado pela primeira vez, ou seja, ao montar o controlador pela primeira vez. Você não é requerido a configurar um endereço IP cada vez que a alimentação for enviada ao controlador.

É possível utilizar estas ferramentas para **definir** o endereço IP em um controlador CompactLogix 5370:

- protocolo Servidor Bootstrap (BOOTP)
- servidor de Protocolo de Configuração de Host Dinâmico (DHCP)
- software RSLinx Classic
- Logix Designer
- cartão SD

Use o servidor BOOTP para configurar o endereço IP

Protocolo Bootstrap (BOOTP) é um protocolo que permite ao controlador comunicar-se com um servidor BOOTP. O servidor também pode ser usado para atribuir um endereço IP. É possível utilizar um servidor BOOTP para definir o endereço IP em um controlador CompactLogix 5370.

Considere estes pontos ao usar o servidor BOOTP:

- O servidor BOOTP está instalado automaticamente quando você instala software RSLogix 5000 ou RSLinx Classic no seu computador. O servidor BOOTP configura um endereço IP e outros parâmetros de Protocolo de Controle de Transmissão (TCP).
- Um controlador enviado da fábrica sem um endereço IP e BOOTP habilitado.
- Esta seção descreve como usar um servidor BOOTP/DHCP Rockwell Automation. Se você usa um servidor BOOTP/DHCP diferente, contate o seu administrador de rede para verificar que você esteja usando-o corretamente.
- Para usar o servidor BOOTP, o seu computador e o controlador devem estar conectados à mesma rede EtherNet/IP.
- Se o controlador estiver com o BOOTP desabilitado, você não pode usar o servidor BOOTP para configurar o endereço IP.

Há duas condições nas quais os controladores Compact GuardLogix 5370 usam servidores BOOTP para configurar o endereço IP do controlador:

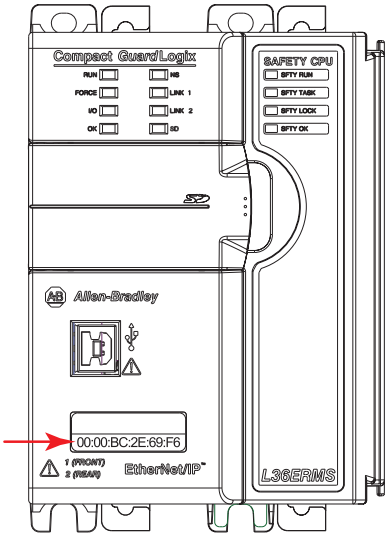
- **Energização inicial** – Porque o controlador CompactLogix 5370 sai de fábrica com o BOOTP habilitado, quando ele é energizado pela primeira vez, o controlador envia um requisito para um endereço IP na rede EtherNet/IP. Você pode usar o servidor BOOTP para configurar o endereço IP, como descrito posteriormente nesta seção.
- **Energização após a operação do controlador ter começado** – Quando a tensão de comando é passada após a operação ter começado, o servidor BOOTP/DHCP configura o endereço IP se cada uma destas condições existir:
  - Controlador estiver com BOOTP habilitado – Você configura o endereço IP manualmente com o servidor BOOTP.
  - Controlador está com DHCP habilitado – O endereço IP é configurado automaticamente via o servidor DHCP.

Acesse o utilitário BOOTP/DHCP de um destes locais:

- Início>Programas>Software Rockwell >Servidor BOOTP-DHCP

  Se você não instalou o utilitário, pode fazer download dele e instalá-lo de http://www.ab.com/networks/ethernet/bootp.html.
- Diretório Ferramentas no CD de instalação do software de programação

IMPORTANTE Antes de iniciar o utilitário BOOTP/DHCP, certifique-se de que você tenha o endereço de hardware (MAC) do controlador.
O endereço de hardware está na frente do controlador e usa um endereço em formato similar ao seguinte:
00:00:BC:2E:69:F6



Use o servidor DHCP para configurar o endereço IP

O Servidor de Protocolo de Configuração de Host Dinâmico (DHCP) atribui automaticamente endereços IP a estações de clientes conectadas a uma rede TCP/IP. O DHCP é baseado em BOOTP e mantém alguma compatibilidade retroativa. A principal diferença é que BOOTP permite configuração manual (estática), enquanto DHCP permite tanto alocação estática quanto dinâmica dos endereços de rede e configurações a controladores recém-anexados.

Seja cuidadoso ao usar o servidor DHCP para configurar um controlador. Um cliente BOOTP, como os Controladores CompactLogix pode começar de um servidor DHCP apenas se o servidor DHCP for especificamente escrito para também lidar com solicitações BOOTP. Isto é específico do servidor DHCP usado. Consulte o seu administrador de sistema para ver se um servidor DHCP suporta comandos BOOTP e alocação de IP manual.

ATENÇÃO: Atribui um endereço de rede fixo aos Controladores Compact GuardLogix 5370. O endereço IP deste controlador não deve ser fornecido dinamicamente.

A inobservância dessa precaução pode resultar em movimento involuntário da máquina ou perda de controle do processo.

Se você usa o servidor BOOTP ou DHCP da Rockwell Automation em uma subrede com uplink onde um servidor DHCP exista, um controlador pode pegar um endereço do servidor da empresa antes que o utilitário Rockwell Automation perceba o controlador. Desconectar-se do link superior para definir o endereço e configurar o controlador para reter seu endereço estático antes de se reconectar ao link superior, se necessário.

Use o software RSLinx Classic para configurar o endereço IP

É possível utilizar o software RSLinx para definir o endereço IP em um controlador CompactLogix 5370.

IMPORTANTE Esta seção explica como atribuir um endereço IP a um controlador Compact GuardLogix que ainda não possui um.

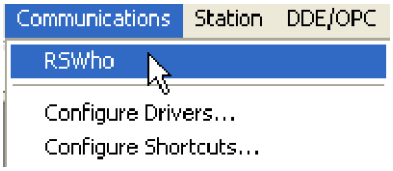
Para atribuir um endereço IP a um controlador Compact GuardLogix via software RSLinx, é necessário estar conectado ao seu controlador através da porta USB.

Completar estas etapas para definir o endereço IP do controlador com software RSLinx.

IMPORTANTE Estes passos mostram um controlador 1769-L36ERMS. Os mesmos passos aplicam-se também a outros controladores CompactLogix 5370 com pequenas variações nas telas.

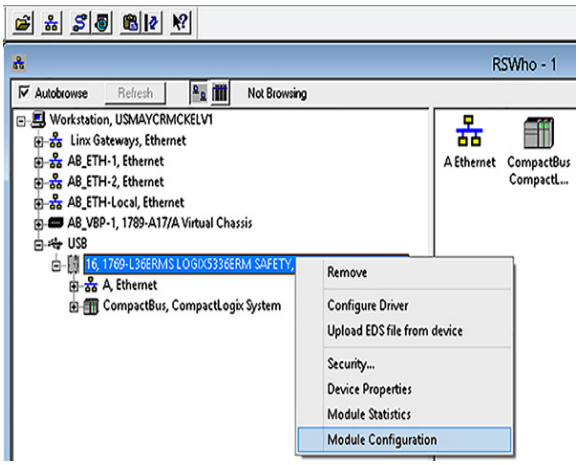
1. Certifique-se de que um cabo USB esteja conectado ao seu computador e ao controlador.
2. Inicie o software RSLinx.

   Após vários segundos, caixa de diálogo RSWho é exibida.
3. Se a caixa de diálogo RSWho não aparecer, a partir do menu Comunicações, escolha RSWho.



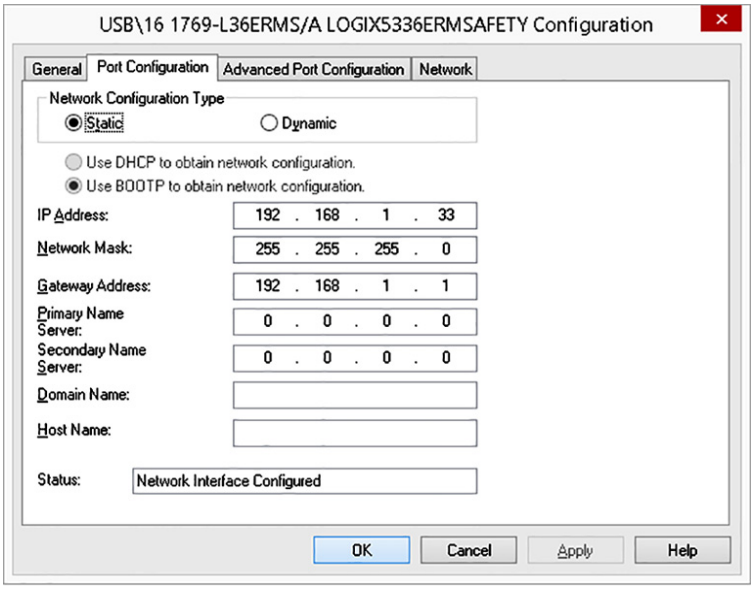
A caixa de diálogo RSWho aparece e inclui o driver USB.

4. Clique com o botão direito do módulo EtherNet/IP e escolha Configuração do Módulo.



A caixa de diálogo Configuração de Módulo aparecerá.

5. Clique na guia configuração da Porta.



6. Para Tipo de configuração de rede, clique em Estático para atribuir permanentemente essa configuração à porta

IMPORTANTE	Se você clicar em Dinâmico, ao desligar e ligar novamente, o controlador limpa a configuração IP atual e volta a enviar solicitações BOOTP.

7. Digite o novo endereço de IP e a máscara de rede
8. Clique em OK.

Como com todas as mudanças de configuração, se desejado, certifique-se de que você esteja usando o cartão SD de um modo que não sobrescreva o endereço IP no próximo ciclo de alimentação do controlador.

Para obter mais informações sobre o uso do cartão SD, consulte Capítulo 13.

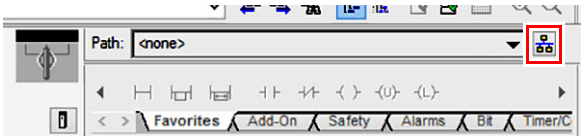
Use o ambiente Studio 5000 para configurar o endereço IP

É possível utilizar o aplicativo Logix Designer para definir o endereço IP em um controlador CompactLogix 5370. Para configurar o endereço IP através da aplicação, é necessário estar conectado ao seu controlador através da porta USB.

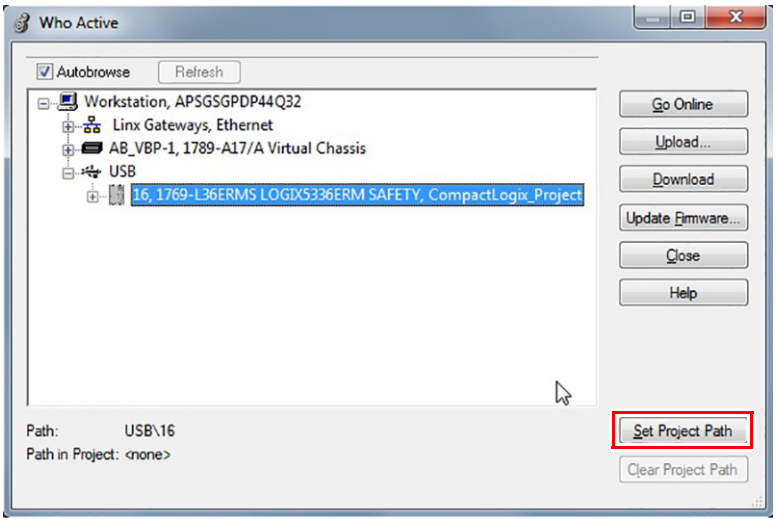
Completar estas etapas para definir o endereço IP do controlador.

IMPORTANTE	Estes passos mostram um controlador 1769-L36ERMS. Os mesmos passos aplicam-se a outros controladores CompactLogix 5370 com pequenas variações nas telas.

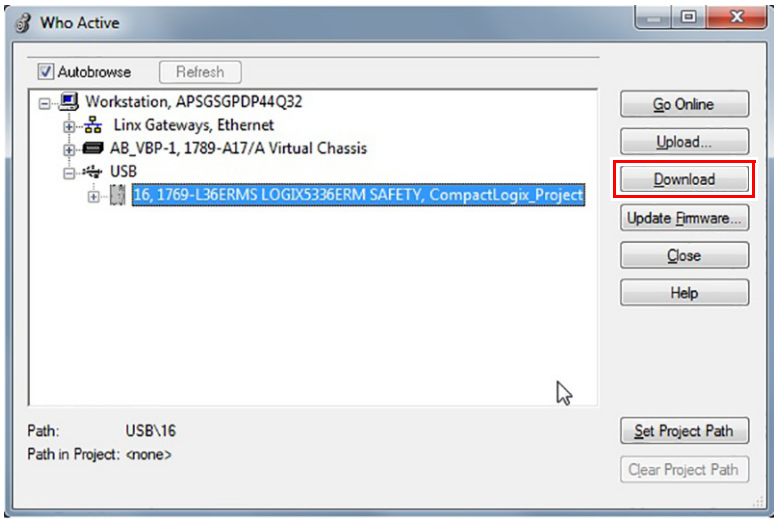
1. Inicie o aplicativo Logix Designer.
2. Clique em RSWho para especificar o caminho do controlador.



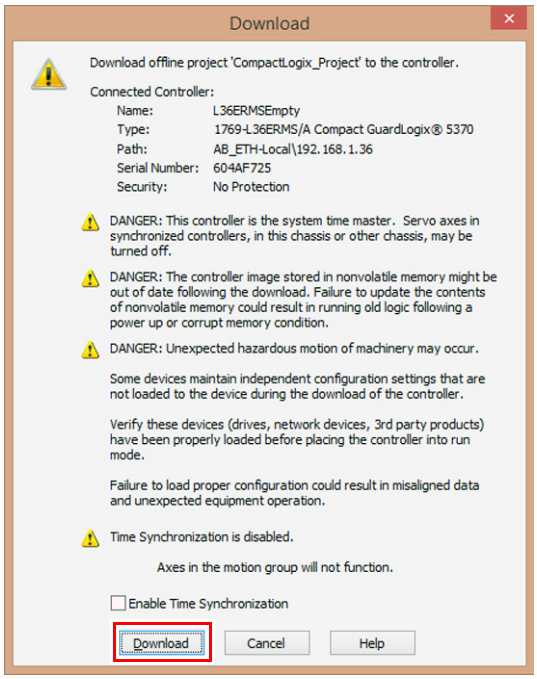
   A caixa de diálogo RSWho é exibida.
3. Navegue na rede USB e selecione o controlador Compact GuardLogix.
4. Clique em Definir caminho do projeto.



5. Clique em Download.

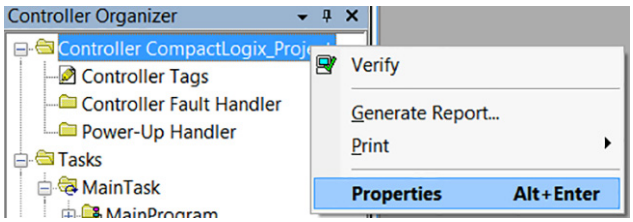


6. Clique em Download novamente.



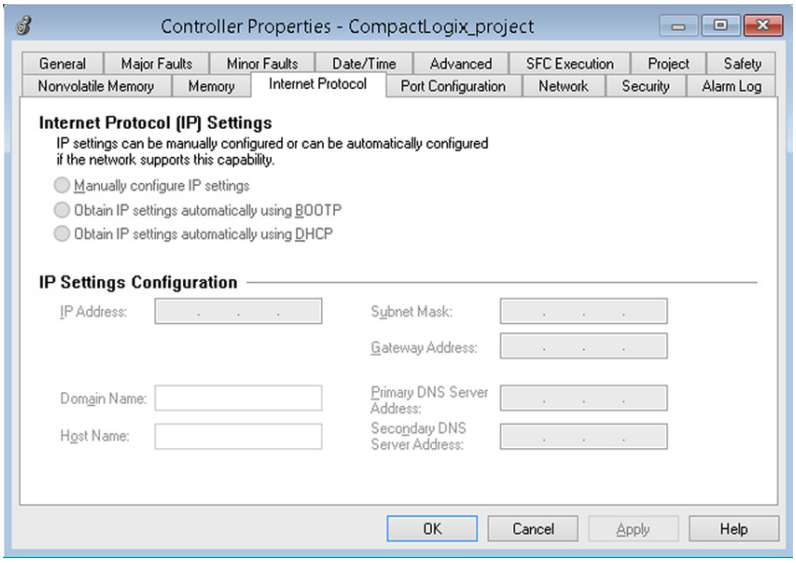
O novo projeto é baixado para o controlador e o projeto entra online, em programa remoto ou modo de programa.

7. Com o botão direito, clique no nome do controlador e escolha Propriedades.

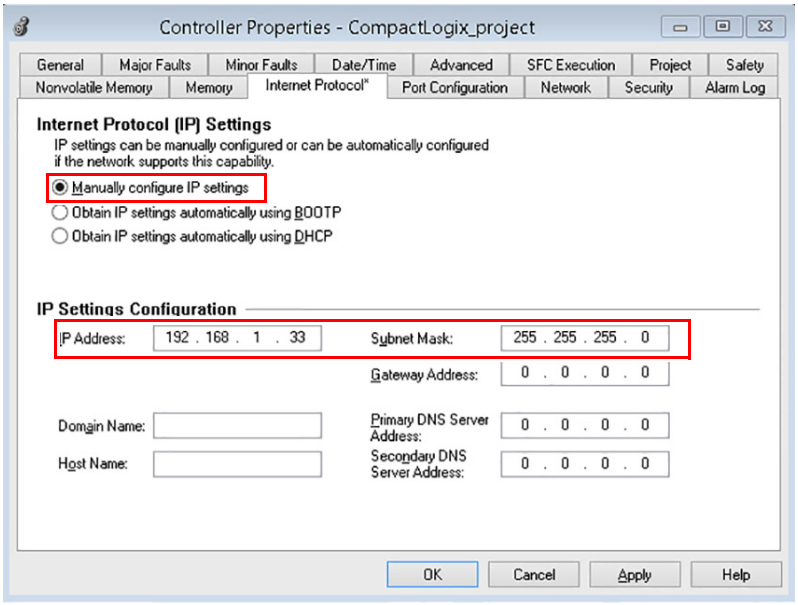


8. Na caixa de diálogo Propriedades do Controlador, clique na guia Protocolo Internet.

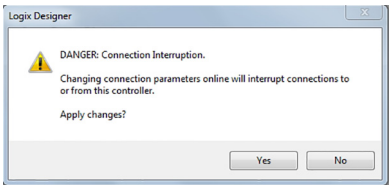
   Os valores de configuração de parâmetro de IP mostram que o controlador não tem endereço IP associado.



9. Clique e Manualmente configure os ajustes de IP.
10. Insira o endereço IP desejado e outras informações de configuração e clique em OK.



11. Quando perguntado para confirmar a configuração do endereço IP, diga Sim.



O controlador agora usa o endereço IP recém-configurado.

Use o servidor cartão SD para configurar o endereço IP

É possível utilizar um cartão SD para definir o endereço IP em um controlador CompactLogix 5370. Usar o cartão SD para carregar endereço IP elimina a necessidade para um software completar esta tarefa.

IMPORTANTE

A configuração do endereço IP de um cartão SD não requer software durante o processo de energização. Entretanto, é necessário ter gravado o projeto anteriormente no cartão SD.

O endereço IP do Controlador Compact GuardLogix 5370 é automaticamente configurado quando se inicia a alimentação, desde que você tenha um endereço IP configurado, guardado o programa em um controlador e definido o cartão SD no parâmetro de carregamento de imagem definido no início da alimentação.

A opção para configurar um endereço IP de controlador CompactLogix 5370 através de um cartão SD na energização é apenas uma parte do processo de carregar um projeto inteiro para o controlador a partir do cartão SD.

Use esta opção cuidadosamente. Por exemplo, o cartão SD pode conter um endereço IP desejável como parte de um projeto indesejável, por exemplo, um projeto mais antigo que o projeto atualmente usado no controlador.

É possível utilizar um cartão SD para definir o endereço IP em um controlador CompactLogix 5370:

- Um projeto deve ser armazenado no cartão SD.
- O projeto que está guardado no cartão SD está configurado com o parâmetro Carregar Imagem definido para durante a inicialização.

Especificações adicionais aplicam-se para projetos de segurança. Consulte Capítulo 13 e o Manual de referência de segurança dos controladores GuardLogix 5570 e Compact GuardLogix 5370, publicação1756-RM099.

Mudar o endereço IP

É possível mudar o endereço IP em um controlador CompactLogix 5370 depois de ter começado a operação do sistema. Neste caso, mude o endereço IP para um controlador que já esteja com um endereço IP atribuído a ele, mas você deve alterar este endereço IP.

Você pode usar estas ferramentas para mudar um endereço IP de controlador:

- software RSLinx Classic
- aplicação Studio 5000 Logix Designer
- cartão SD

IMPORTANTE	Você **não pode** usar nenhuma destas ferramentas para **mudar** um endereço IP de controlador: • Protocolo Servidor Bootstrap (BOOTP) • Servidor de Protocolo de Configuração de Host Dinâmico (DHCP)

Considere estes fatores ao determinar como mudar um endereço IP de controlador:

- Isolamento de rede de, ou integrando-se a, rede da planta/empresa
- Tamanho da rede – Para redes grandes, isoladas, pode ser mais fácil e seguro usar um servidor BOOTP/DHCP do que um RSLogix 5000 ou software RSLinx Classic. Um servidor BOOTP/DHCP limita a possibilidade de atribuir endereços IP duplos.

  Porém, Você pode usar o servidor BOOTP/DHCP apenas para **configurar** o endereço IP do controlador e não para mudá-lo. Se você decidir mudar o endereço IP do controlador e quiser usar um servidor BOOTP/DHCP para limitar a possibilidade de atribuir endereços IP duplos, você precisa primeiro limpar o endereço IP.

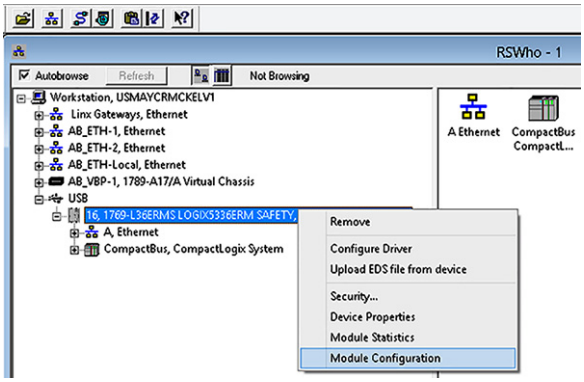
  Após limpar o endereço IP, use os passos descritos em Use o servidor BOOTP para configurar o endereço IP na página 34 ou Use o servidor DHCP para configurar o endereço IP na página 35 para configurar o endereço IP do controlador.
- Políticas da empresa e procedimentos relativos à instalação e manutenção da rede do chão de fábrica
- Nível de envolvimento por pessoal de TI em instalação e manutenção de rede de chão de fábrica
- Tipo de treinamento oferecido para controlar engenheiros e pessoal de manutenção

Mudar o endereço IP com o software RSLinx

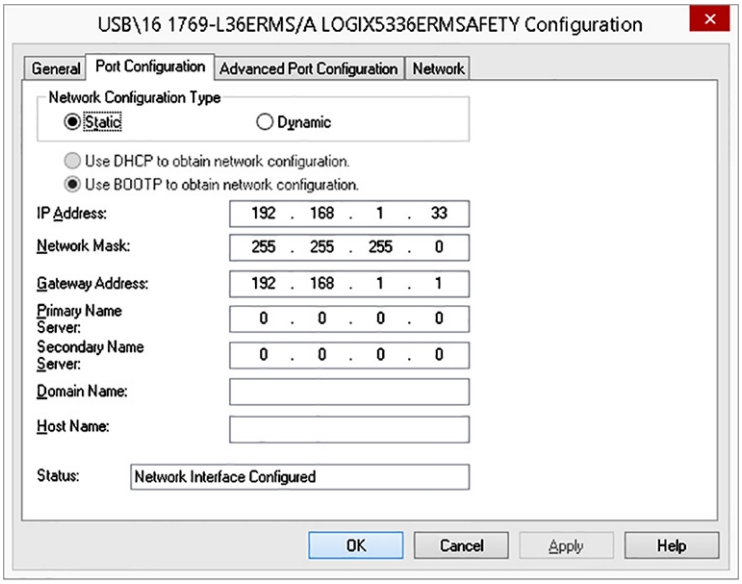
Completar estas etapas para mudar o endereço IP do controlador.

IMPORTANTE Estes passos mostram um controlador 1769-L36ERMS. Os mesmos passos aplicam-se a outros controladores CompactLogix 5370 com pequenas variações nas telas.

1. Certifique-se de que um cabo USB esteja conectado ao seu computador e ao controlador.
2. No organizador do controlador, clique com o botão direito do mouse no controlador e escolha Configuração do Módulo.



3. Clique na guia Configuração da porta.



O controlador tem um endereço IP válido e Tipo de Configuração de Rede.

4. Digite o novo endereço de IP e a máscara de rede.
5. Para Tipo de configuração de rede, clique em Estático para atribuir permanentemente essa configuração à porta.

IMPORTANTE Se você clicar em Dinâmico, ao desligar e ligar novamente, o controlador limpa a configuração IP atual e volta a enviar solicitações BOOTP.

6. Clique em OK.

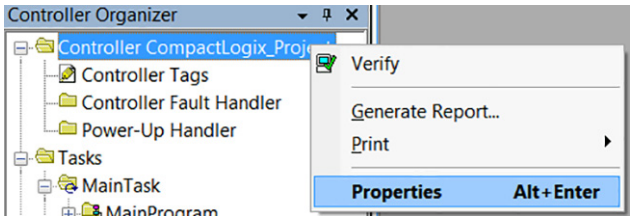
Mudar o endereço IP com o software Logix Designer

É possível mudar o endereço IP em um controlador Compact GuardLogix 5370 via aplicativo Logix Designer com uma conexão USB ou EtherNet/IP.

Completar estas etapas para mudar o endereço IP do controlador.

IMPORTANTE Estes passos mostram um controlador 1769-L36ERMS. Os mesmos passos aplicam-se a outros controladores CompactLogix 5370 com pequenas variações nas telas.

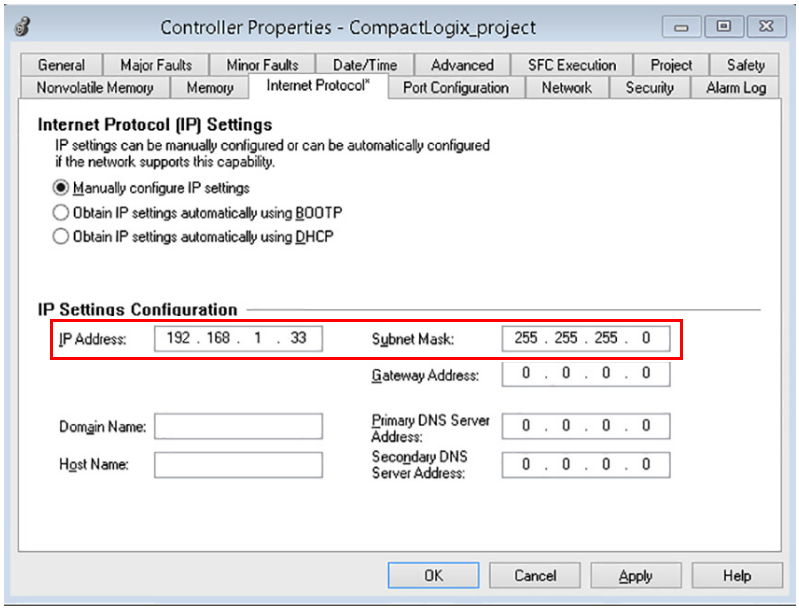
1. Verifique que o seu computador esteja conectado ao controlador.
2. Verifique se o projeto está on-line.
3. Com o botão direito, clique no nome do controlador e escolha Propriedades.



DICA Você poderia também clicar com o botão direito no nó Ethernet na seção configuração de E/S e escolher Propriedades.

A caixa de diálogo Propriedades do controlador aparece na guia Protocolo de Internet.

4. Mudar o endereço IP para o controlador.
5. Faça outras mudanças onde necessário.



6. Clique em OK.

Mudar o endereço IP com um cartão SD

É possível utilizar um cartão SD para alterar o endereço IP em um controlador Compact GuardLogix 5370 quando se reinicia. Usar o cartão SD para carregar endereço IP elimina a necessidade para um software completar esta tarefa.

IMPORTANTE	A configuração do endereço IP de um cartão SD não requer software durante o processo de energização. Entretanto, é necessário ter gravado o projeto anteriormente no cartão SD.

É possível utilizar um cartão SD para alterar o endereço IP em um controlador CompactLogix 5370:

- Há um projeto armazenado no cartão SD.
- O projeto que está armazenado no cartão SD inclui outro endereço IP para o controlador Compact GuardLogix 5370 que não o endereço IP atualmente usado no controlador físico que leva o cartão SD.
- O projeto que está guardado no cartão SD está configurado com o parâmetro Carregar Imagem definido para durante a inicialização.
- Alimentação é fornecida ao controlador com o cartão SD instalado.

Especificações adicionais aplicam-se para projetos de segurança. Consulte Capítulo 13 e o Manual de referência de segurança dos controladores GuardLogix 5570 e Compact GuardLogix 5370, publicação 1756-RM099.

Carregar o firmware do controlador

Você precisa descarregar o firmware atual antes de usar o controlador Compact GuardLogix 5370.

IMPORTANTE	Não interrompa um upgrade de firmware enquanto estiver em processo. A interrupção da atualização do firmware pode fazer com que a revisão controlador Compact GuardLogix reverta-se ao seu nível de revisão padrão, ou seja, 1.-*xxx*.

Para carregar firmware, você pode usar qualquer um dos seguintes:

- Software ControlFlash que é instalado com o aplicativo Logix Designer
- AutoFlash que roda pela aplicação quando você faz download de um projeto e o controlador não tem a revisão de firmware compatível
- Cartão SD (códigos de catálogo 1784-SD1 ou 1784-SD2) com imagem já armazenada no cartão

Se você usa utilitários ControlFLASH ou AutoFlash, você precisa de uma conexão de rede EtherNet/IP ou USB ao controlador.

IMPORTANTE A revisão de firmware do controlador que foi carregada através do software ControlFLASH ou da opção AutoFlash pode ser substituída depois de ciclos de alimentação futuros se existirem as condições descritas em Usar o cartão Secure Digital para carregar firmware na página 52.

O firmware está disponível com o aplicativo ou você pode fazer o download no site de suporte do Centro de download e compatibilidade do produto Rockwell Automation (PCDC) em http://www.rockwellautomation.com/global/support/pcdc.page.

Usar o software ControlFLASH para carregar firmware

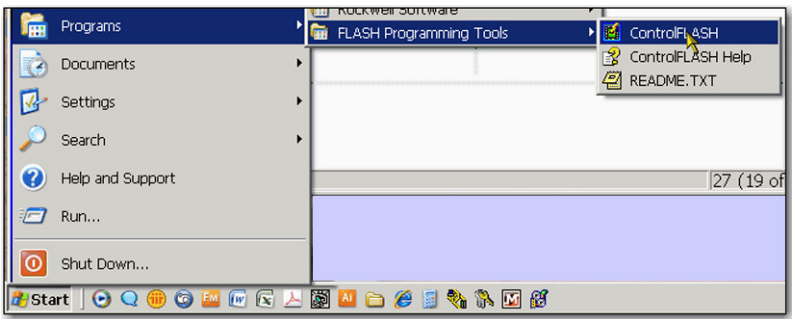
Usar o software ControlFLASH para carregar firmware através de uma conexão USB ou de conexão de rede EtherNet/IP. Recomendamos o seguinte quando você carregar firmware por meio do utilitário ControlFLASH:

- Use uma conexão USB para carregar o firmware.
- Se um estiver instalado no controlador, remova o cartão SD.

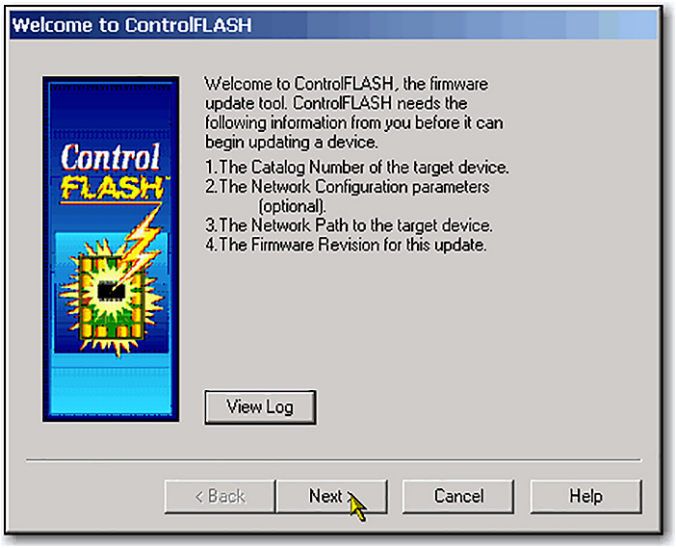
Complete estas etapas para usar o utilitário ControlFLASH para carregar firmware.

IMPORTANTE Estes passos mostram um controlador 1769-L36ERMS. Os mesmos passos aplicam-se também a outros controladores CompactLogix 5370 com pequenas variações nas telas.

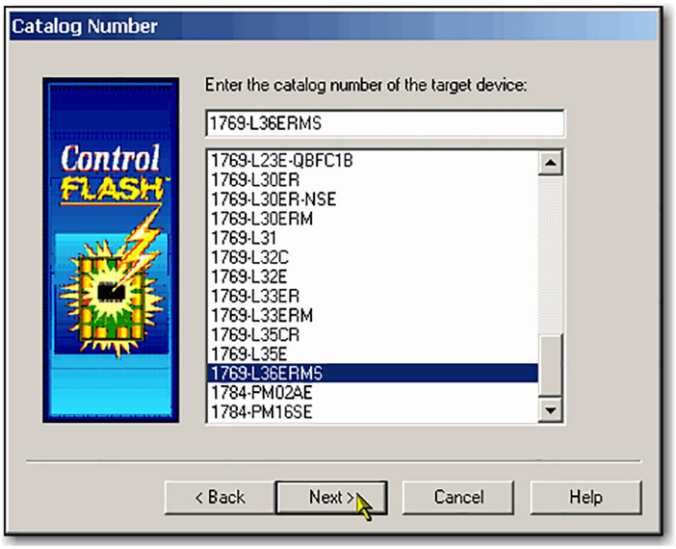
1. Verifique que uma conexão exista entre o seu computador e o controlador CompactLogix 5370.
2. Escolha Início>Programas>Ferramentas de programação FLASH>ControlFLASH.



3. Quando a caixa de diálogo Bem-vindo aparecer, clique em Próximo.

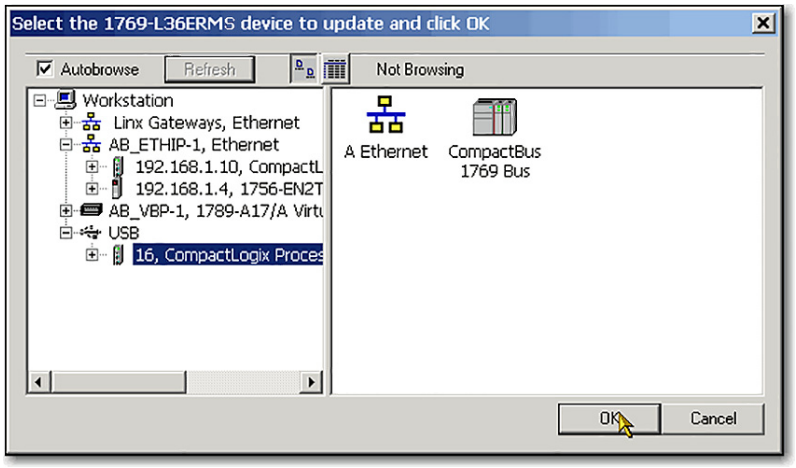


4. Escolha o código de catálogo de controlador apropriado e clique em Próximo.

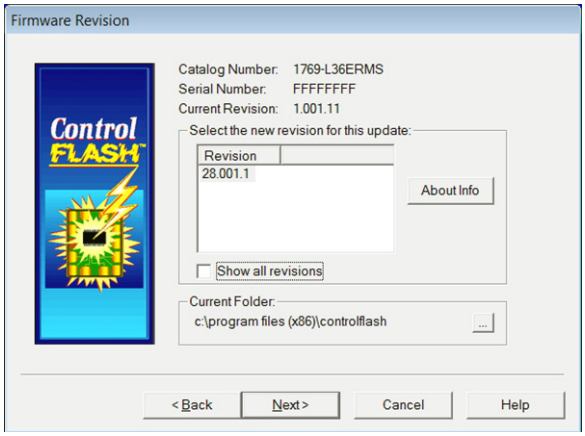


5. Expanda a rede até que você veja o controlador.

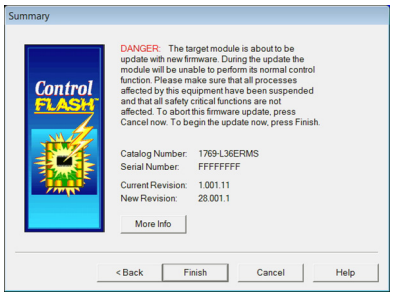
6. Escolha o controlador na primeira instância em que aparece, conforme mostrado abaixo, e clique em OK.

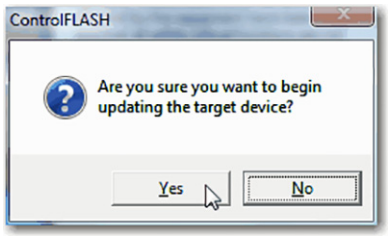


7. Escolha o nível de revisão para o qual você quer atualizar o controlador e clique em Próximo.

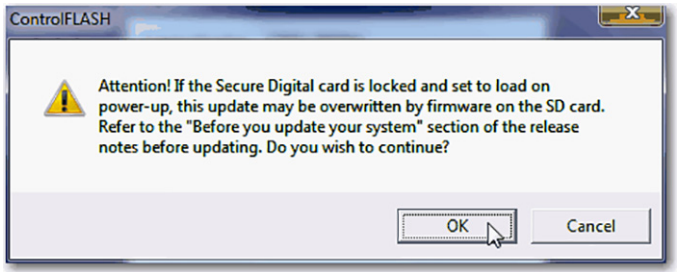


8. Para iniciar a atualização do controlador, clique em Terminar e então clique em Sim.

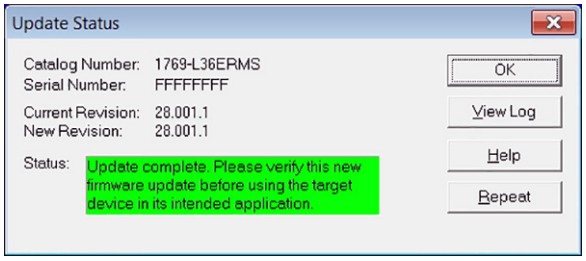




Antes que o upgrade de firmware comece, você vê a seguinte caixa de diálogo. Toma a ação apropriada para a sua aplicação. Neste exemplo, o upgrade continua quando você clica em OK.



Após o controlador ter sido atualizado, a caixa de diálogo de status exibe a mensagem Atualização completa.



9. Clique em OK.
10. Para fechar o software ControlFLASH, clique em Cancelar e depois em Sim.

Usar o utilitário AutoFlash para carregar firmware

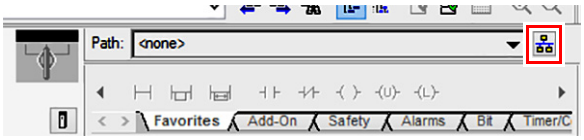
Usar o utilitário AutoFlash para carregar firmware através de uma conexão USB ou de rede EtherNet/IP.

Deixe a atualização ser concluída sem interrupções. Caso uma atualização de firmware que esteja em curso seja interrompida, você será alertado de que um erro ocorreu. Neste caso, desligue e ligue a alimentação ao controlador. O nível de revisão de firmware volta ao nível de revisão 1.*xxx* e você pode começar o processo de upgrade novamente.

Complete estas etapas para usar o utilitário AutoFlash para carregar firmware.

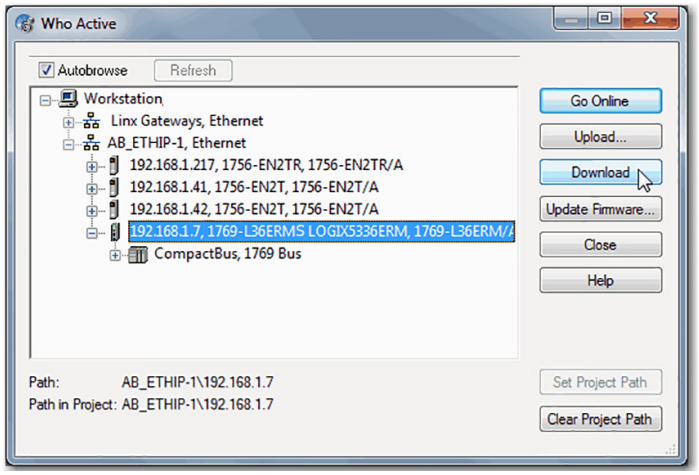
IMPORTANTE Estes passos mostram um controlador 1769-L36ERMS. Os mesmos passos aplicam-se também a outros controladores CompactLogix 5370 com pequenas variações nas telas.

1. Certifique-se de que a conexão de rede apropriada tenha sido feita e o seu driver de rede esteja configurado em software RSLinx Classic.
2. Criação de um projeto do controlador.
3. Clique em RSWho para especificar o caminho do controlador.



A caixa de diálogo RSWho é exibida.

4. Navegue na rede Ethernet e selecione o controlador Compact GuardLogix.

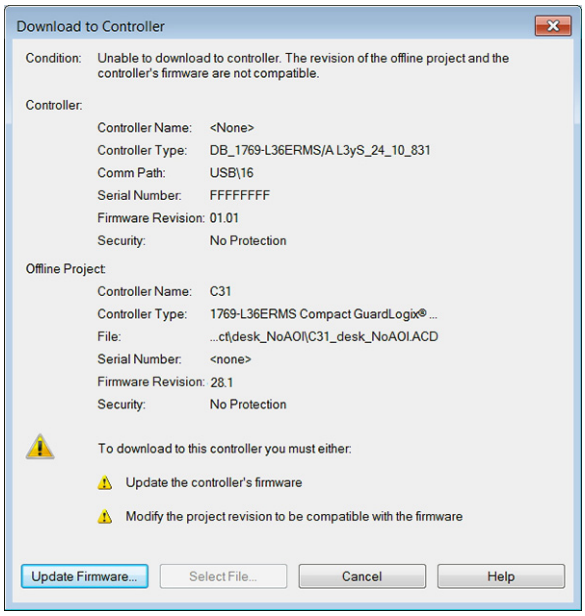


5. Clique em Download.

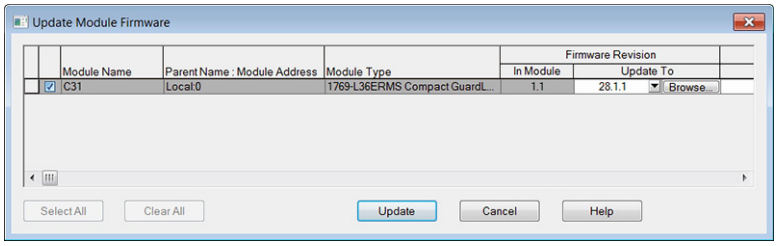
DICA Você pode clicar em Atualizar Firmware ao invés de em Download para completar este processo. Se fizer isso, pule para passo 6.

Uma caixa de diálogo aparece indicando que a revisão do projeto e a revisão do firmware do controlador são diferentes.

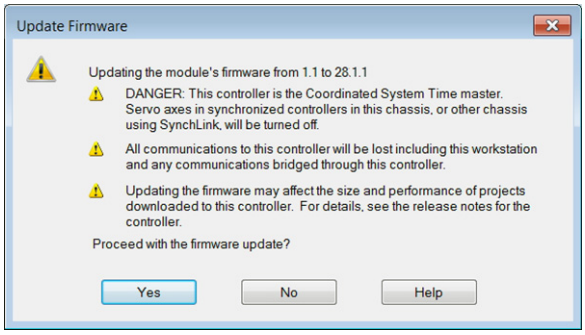
6. Clique em Atualizar Firmware.



7. Use a caixa de seleção e o menu para escolher o seu controlador e revisão de firmware.
8. Clique em Atualizar.



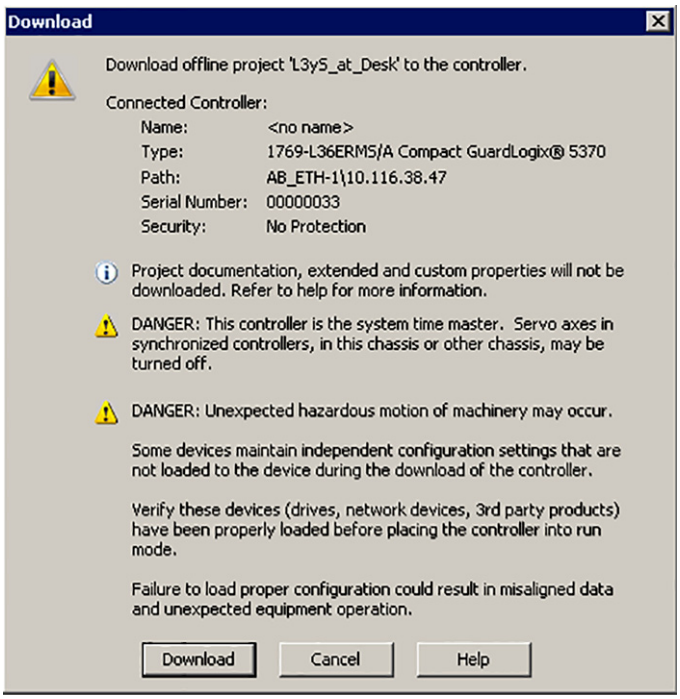
9. Quando a caixa de diálogo Atualizar firmware aparecer, clique em Sim.



Antes de iniciar a atualização do firmware, pode ser que você seja avisado sobre a ausência do cartão SD do seu controlador. Toma a ação apropriada, geralmente clique OK.

O upgrade de firmware começa.

10. Quando a atualização do firmware estiver completa, a caixa de diálogo Quem está Ativo se abre. Neste exemplo, o projeto é baixado para o controlador quando você clica em Download.



Usar o cartão Secure Digital para carregar firmware

É possível utilizar um cartão SD para carregar o firmware em um controlador Compact GuardLogix 5370. Usar o cartão SD para carregar firmware elimina a necessidade para um software completar esta tarefa.

IMPORTANTE	Um carão SD instalado faz a atualização automática do firmware do controlador Compact GuardLogix 5370 se o cartão SD estiver configurado com o parâmetro de carregar imagem ajustado para o fazer no início da alimentação.

Sua aplicação exige o seguinte para carregar o firmware de um cartão SD na energização:

- É necessário ter gravado o projeto no cartão SD antes do ciclo de energia.
- A revisão do firmware no projeto armazenado no cartão SD é diferente da revisão do firmware no controlador CompactLogix 5370.

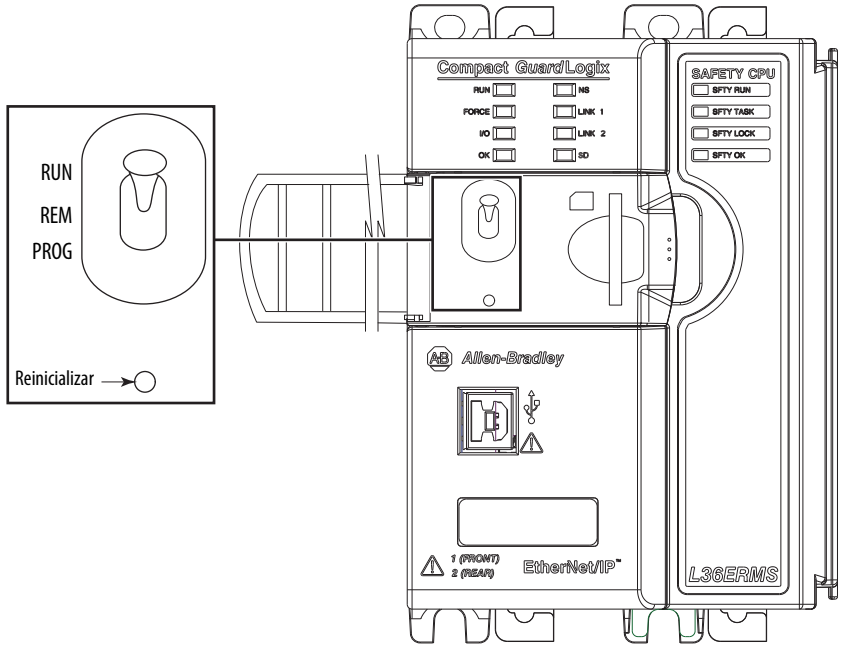
Especificações adicionais aplicam-se para projetos de segurança. Consulte Capítulo 13 e o Manual de referência de segurança dos controladores GuardLogix 5570 e Compact GuardLogix 5370, publicação1756-RM099.

Selecione o modo de operação do controlador

ADVERTÊNCIA: Quando você muda configurações de chave enquanto a energia está ligada, uma arco elétrico pode ocorrer. Isto pode causar uma explosão em instalações reconhecidas como área classificada.

Antes de continuar, certifique-se de que não haja energia ou que a área não apresenta risco

O seguinte gráfico mostra o comutador de modo do Controlador Compact GuardLogix 5370. Usar o comutador de modo no controlador para definir o modo de operação.



IMPORTANTE Restrições aplicam-se para projetos de segurança. Consulte Capítulo 9, Desenvolver aplicações de segurança e o Manual de referência de segurança dos sistemas de controladores GuardLogix 5570 e Compact GuardLogix 5370, publicação 1756-RM099 para informações detalhadas sobre restrições de programação.

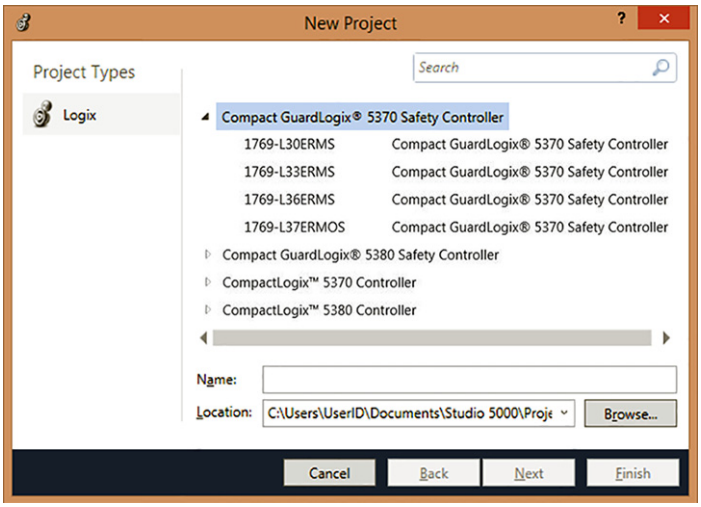
Posição da Chave de Modo	Descrição	
Run	Você pode realizar estas tarefas: • Carregar projetos. • Executar o programa e habilitar saídas. Você não pode realizar estas tarefas: • Atualizar o firmware do controlador. • Criar ou apagar tarefas, programas, ou rotinas. • Criar ou apagar tags ou editar online. • Importar um programa para o controlador. • Alterar a configuração da porta do controlador, configuração de porta avançada, ou ajustes de configuração de rede. • Mudar parâmetros de configuração do controlador diretamente configurados para operação em uma topologia da rede de anel em nível de equipamento (DLR).	
Prog	Você pode realizar estas tarefas: • Atualizar o firmware do controlador. • Desabilitar saídas. • Fazer upload/download de projetos. • Criar, modificar e apagar tarefas, programas, ou rotinas. • Alterar a configuração da porta do controlador, configuração de porta avançada, ou ajustes de configuração de rede. Você não pode realizar estas tarefas: • Usar o controlador para executar (fazer uma varredura de) tarefas.	
Rem	Você pode realizar estas tarefas: • Fazer upload/download de projetos. • Alterar a configuração da porta do controlador, configuração de porta avançada, ou ajustes de configuração de rede. • Alterar entre Programa remoto, Teste remoto e modos de Operação remota através da aplicação.	
	Operação Remota	• O controlador executa (faz uma varredura de) tarefas. • Habilita saídas. • Edição online.
	Programa Remoto	• Atualizar o firmware do controlador. • Desabilitar saídas. • Criar, modificar e apagar tarefas, programas, ou rotinas. • Baixa projetos. • Edição online. • O controlador não executa (faz uma varredura de) tarefas.
	Teste Remoto	• Executa tarefas com saídas desabilitadas. • Edição online.

Configurar o controlador

Criar um projeto do controlador

Para configurar e programar seu controlador, siga estas etapas para criar e gerenciar um projeto para o controlador com o aplicativo Logix Designer.

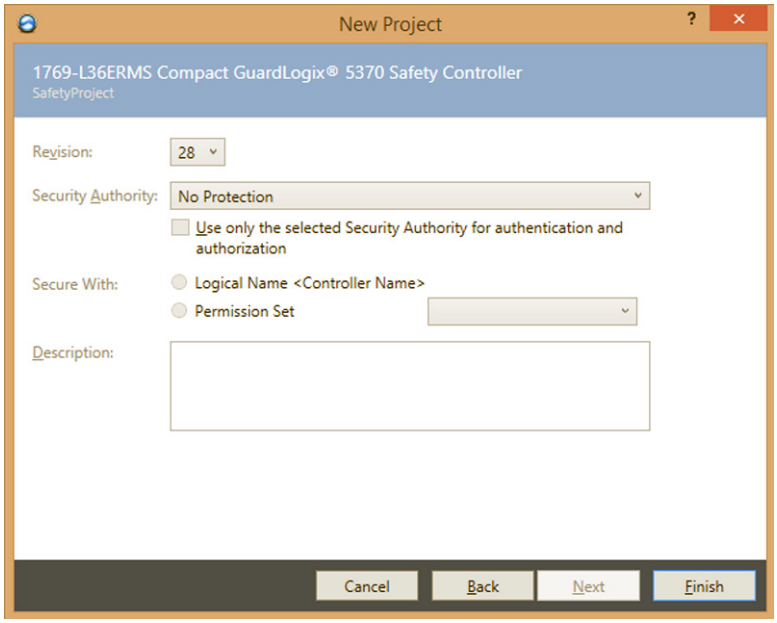
1. Clique no botão Novo na barra de ferramentas principal para criar um projeto.
2. Clique duas vezes no controlador de segurança GuardLogix® 5370 para expandir a lista de opções de controlador.
3. Escolher um Controlador Compact GuardLogix 5370:
   - 1769-L30ERMS
   - 1769-L33ERMS
   - 1769-L36ERMS
   - 1769-L37ERMOS(1)



4. No campo nome, digite o nome do projeto.

(1) Disponível na versão do firmware 30.

5. Clique em Procurar para especificar a pasta para armazenar o projeto do controlador de segurança.
6. Clique em Próximo.
7. No menu de revisão, escolha a revisão principal de firmware para o controlador.



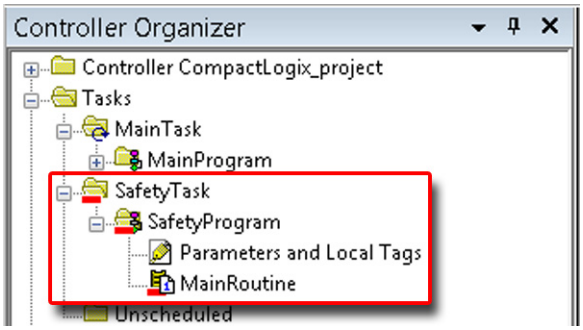
8. No menu autoridade de segurança, escolha uma opção de autoridade de segurança.

   Para obter informações detalhadas sobre segurança, consulte o Manual de programação de segurança dos controladores Logix5000™, publicação 1756-PM016.

9. Marque a caixa abaixo de autoridade de segurança se você deseja usar a proteção selecionada para autenticação e autorização.
10. No campo Descrição, digite uma descrição do projeto.
11. Clique em Terminar.

A aplicação Logix Designer cria automaticamente uma tarefa de segurança e um programa de segurança. Uma rotina de segurança de lógica ladder denominada MainRoutine também é criada no programa de segurança.

Figura 3 – Tarefa de segurança no organizador do controlador



Uma barra vermelha abaixo do ícone diferencia os programas e as rotinas de segurança dos componentes-padrão do projeto no organizador do controlador.

Quando um novo projeto de segurança é criado, a aplicação Logix Designer também cria automaticamente um número da rede de segurança (SNN) baseado na hora.

Este SNN define a EtherNet/IP no qual o controlador reside como uma subrede de segurança. Pode-se ver e modificar na guia Geral na caixa de diálogo Propriedades do controlador.

Na maioria das aplicações, o SNN automático baseado na hora é suficiente. No entanto, existem casos quando é necessário inserir um SNN específico.

Figura 4 – Número da rede de segurança

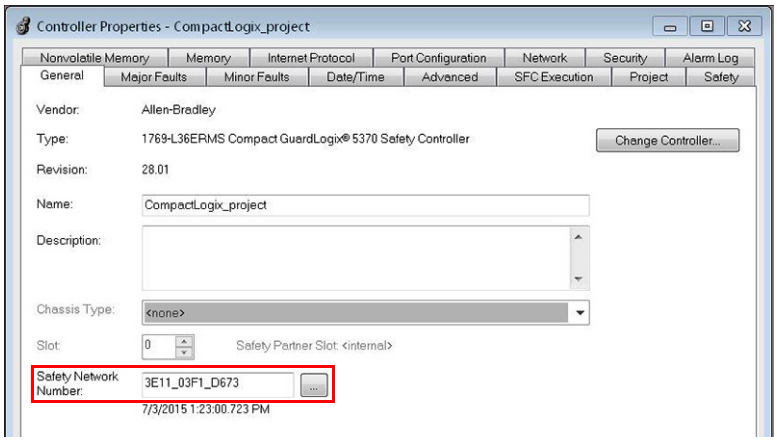


Tabela 6 – Recursos adicionais

Recurso	Descrição
Capítulo 9, Desenvolver aplicações de segurança	Contém mais informações sobre a tarefa, os programas e as rotinas de segurança
Capítulo 5, Comunique-se pelas redes	Fornece mais informações sobre como gerenciar o SNN

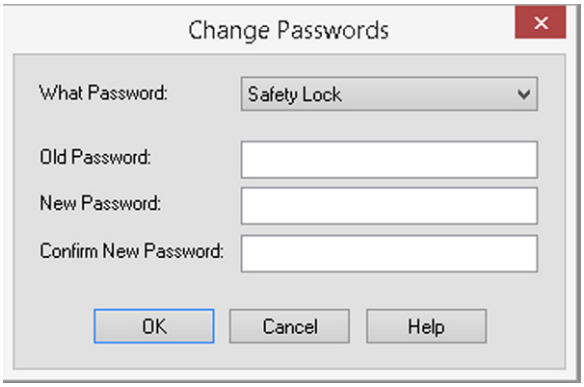
Definir senhas para trava de segurança e desbloqueio

Você pode bloquear o controlador para ajudar a proteger contra modificações as componentes do controle de segurança. Somente componentes de segurança, como a tarefa de segurança, programas, rotinas e tags de segurança são afetados. Componentes padrão não são afetados. É possível bloquear ou desbloquear a segurança do projeto do controlador quando estiver on-line ou off-line.

A função de bloqueio e desbloqueio de segurança utiliza duas senhas distintas, que são opcionais.

Siga estas etapas para configurar as senhas:

1. Clique em Ferramentas > Segurança > Alterar senhas.
2. No menu Qual Senha, escolha Trava de segurança ou Desbloqueio de segurança.



3. Digite a senha antiga, se houver uma.
4. Digite e confirme a nova senha.
5. Clique em OK.

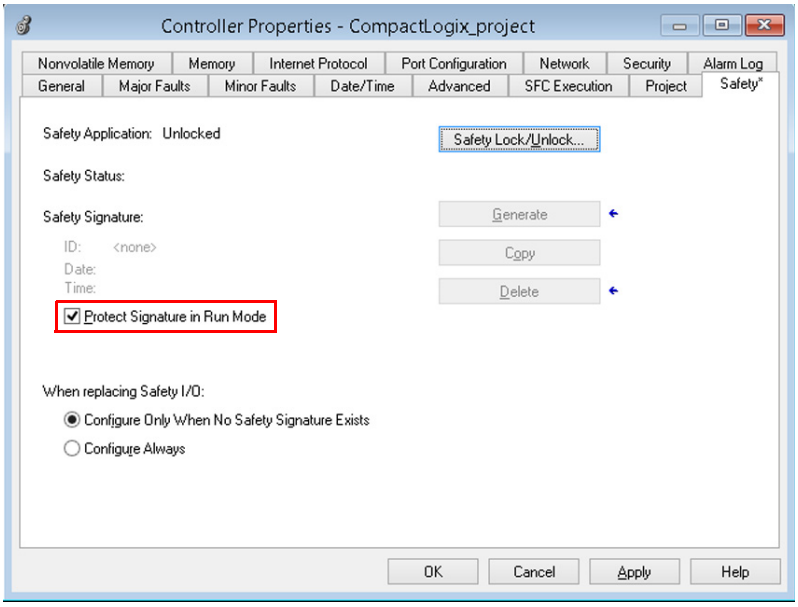
   As senhas podem conter de 1 a 40 caracteres e não diferenciam maiúsculas e minúsculas. As letras, os números e os símbolos a seguir podem ser usados: ‘ ~ ! @ # $ % ^ & * ( ) _ + , – = { } | [ ] \ : ; ? /.

Proteger a assinatura da tarefa de segurança no modo de operação

Você pode impedir que a assinatura de tarefa de segurança seja gerada ou excluída enquanto o controlador está no modo de operação ou modo de operação remoto, independentemente se a aplicação de segurança está bloqueada ou desbloqueada.

Siga estas etapas para proteger a assinatura de tarefa de segurança:

1. Abra a caixa de diálogo Propriedades do Controlador.
2. Clique na guia Segurança.
3. Verificar Proteger a assinatura em modo de operação.
4. Clique em OK.



Codificação eletrônica

O chaveamento eletrônico reduz a possibilidade de que você use o dispositivo incorreto em um sistema de controle. Ele compara o dispositivo definido em seu projeto para o dispositivo instalado. Se o chaveamento falhar, ocorre uma falha. Esses atributos são comparados.

Atributo	Descrição
Fornecedor	Fabricante do dispositivo.
Tipo de dispositivo	O tipo geral do produto, por exemplo, módulo de E/S digital.
Código de produto	O tipo específico do produto. Código do produto é mapeado para um número de catálogo.
Revisão principal	Um número que representa as capacidades funcionais de um dispositivo.
Revisão secundária	Um número que representa mudanças de comportamento no dispositivo.

As seguintes opções de chaveamento eletrônico estão disponíveis.

Opção de codificação	Descrição
Módulo compatível	Permite que o dispositivo instalado aceite a chave do dispositivo que é definido no projeto quando o dispositivo instalado pode emular o dispositivo definido. Com o módulo compatível, você pode geralmente substituir um dispositivo por outro dispositivo que tenha as seguintes características: • Mesmo número de catálogo • Revisão principal igual ou superior • Revisão secundária da seguinte forma: – Se a revisão principal é igual, a revisão secundária deve ser a mesma ou superior. – Se a revisão principal for maior, a revisão secundária pode ser qualquer número.
Correspondência exata	Indica que todos os atributos de codificação devem combinar para estabelecer comunicação. Se qualquer atributo não corresponder precisamente, a comunicação com o dispositivo não ocorre. A correspondência exata é necessária se você está usando o Firmware do Manager.

Com cuidado, considere as consequências de cada opção de codificação quando selecionar uma.

IMPORTANTE A alteração online de parâmetros de chaveamento eletrônico interrompe conexões com o dispositivo e todos os dispositivos que estão conectados por meio dele. Conexões de outros controladores também podem ser interrompidas.

Se uma conexão de E/S para um dispositivo for interrompida, o resultado pode ser uma perda de dados.

Para obter informações mais detalhadas sobre codificação eletrônica, consulte Codificação Eletrônica na Técnica de aplicação de sistemas de controle Logix5000, publicação LOGIX-AT001.

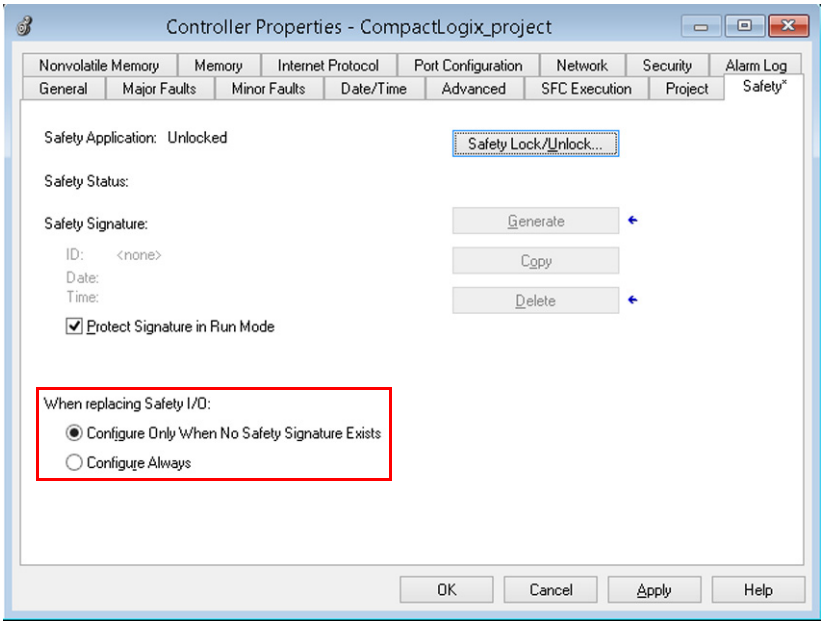
Opções de substituição do dispositivo de E/S

A guia Segurança da caixa de diálogo Propriedades do controlador lhe permite definir como o controlador lida com a substituição de um dispositivo de E/S do sistema. Essa opção determina se o controlador ajusta o número de rede de segurança (SNN) de um dispositivo de E/S ao qual ele esteja conectado e tenha dados de configuração, para quando uma assinatura de tarefa de segurança(1) existir.

Siga estas etapas para configurar como o controlador lida com a substituição de um dispositivo de E/S do sistema.

1. Abra a caixa de diálogo Propriedades do Controlador.
2. Clique na guia Segurança.
3. Selecione a opção configurar para o controlador para usar quando substituir a E/S de segurança.
4. Clique em OK.

Figura 5 – Opções de substituição do dispositivo de E/S



ATENÇÃO: Habilite a funcionalidade Configurar Sempre somente se o sistema de controle de segurança CIP inteiro roteável não precisar manter o SIL 3 durante a substituição e o teste de funcionamento de um dispositivo.

Para obter mais informações, consulte Capítulo 5, Comunique-se pelas redes na página 63.

(1) A assinatura da tarefa de segurança é um número usado exclusivamente para identificar a lógica, os dados e a configuração de cada projeto, protegendo assim o nível de integridade de segurança do sistema (SIL). Consulte Assinatura de tarefa de segurança na página 16 e Gerar uma assinatura de tarefa de segurança na página 158 para obter mais informações.

Habilitar a sincronização de tempo

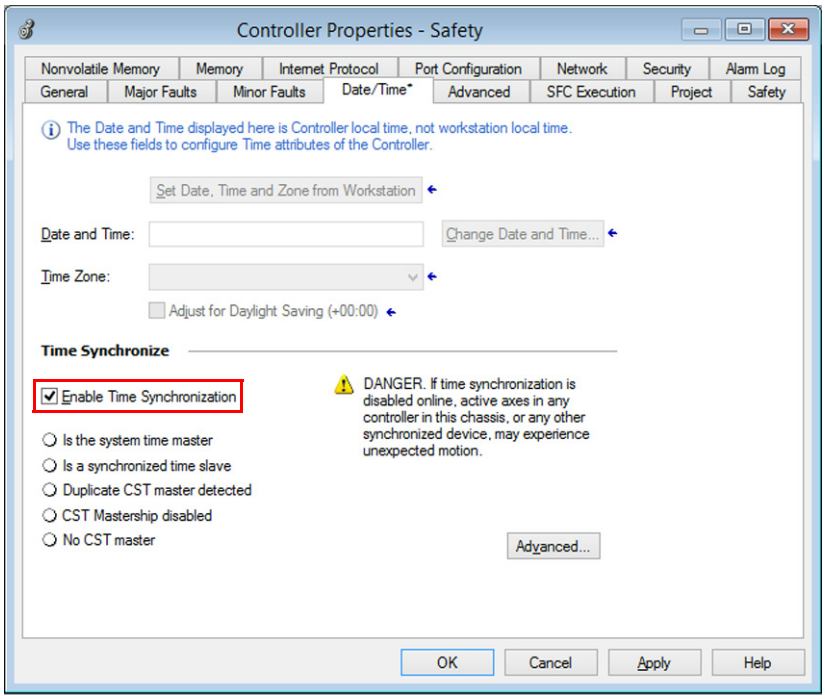
Em um sistema do controlador Compact GuardLogix 5370, um controlador deve ser designado como o mestre para o tempo de sistema coordenado (CST). A opção Sincronização de tempo oferece um mecanismo padrão para sincronizar relógios em uma rede de dispositivos distribuídos.

IMPORTANTE A sincronização de tempo é necessária para aplicativos de movimento.

Siga estas etapas para configurar o controlador para se tornar o mestre CST.

1. Abra a caixa de diálogo Propriedades do Controlador.
2. Clique na guia data/hora.
3. Marque Habilitar a sincronização de tempo
4. Clique em OK.

Figura 6 – Guia Date/Time



Configurar um controlador de segurança de peer

É possível adicionar um controlador de segurança de peer à pasta Configuração de E/S de seu projeto de segurança para permitir que as tags padrão ou de segurança sejam consumidas. Para compartilhar dados de segurança entre controladores peer, você produz e consome tags de segurança com escopo no controlador.

Para obter detalhes sobre a configuração dos controladores de segurança de peer e a produção e o consumo de tags de segurança, consulte Tags de segurança produzidas/consumidas na página 146.

Comunique-se pelas redes

Todos os controladores CompactLogix® 5370 suportam estas tarefas por meio de uma rede EtherNet/IP:

- Controles distribuídos de E/S para ambas conexões de segurança e padrão.
- Envio/recebimento de mensagens para/de outros equipamentos na mesma rede ou outra rede
- Produzir/consumir (interbloquear) dados entre controladores.
- Interface de soquete

Todos os controladores CompactLogix® 5370 suportam estas tarefas por meio de uma rede EtherNet/IP:

- Controles distribuídos de E/S apenas para conexões padrão.
- Envio de mensagens para equipamentos na mesma rede: o controlador não pode receber mensagens de outros equipamentos na rede.

Todos os controladores CompactLogix 5370 também suportam conexões temporárias a partir do seu computador por meio de uma conexão USB.

Rede de Segurança

O protocolo CIP Safety é um protocolo de segurança de nó final a nó final que permite o roteamento de mensagens CIP Safety de e para dispositivos CIP Safety por meio de pontes, chaves e dispositivos de roteamento.

Para manter a alta integridade durante o roteamento por pontes, chaves ou dispositivos de roteamento padrões, cada nó final dentro de um sistema de controle CIP Safety roteável precisa apresentar uma referência exclusiva. Essa referência é a combinação de um SNN (Safety Network Number, número da rede de segurança) com o Endereço de Nó do dispositivo de rede.

Gerenciamento do número da rede de segurança (SNN)

O SNN atribuído aos dispositivos de segurança em um segmento de rede precisa ser exclusivo. Você deve certificar-se de que apenas um SNN esteja indicado para cada rede CIP Safety que contenha dispositivos de segurança.

O SNN atribuído aos dispositivos de segurança em um segmento de rede precisa ser exclusivo. Você deve certificar-se de que apenas um SNN esteja indicado para cada rede CIP Safety que contenha dispositivos de segurança.

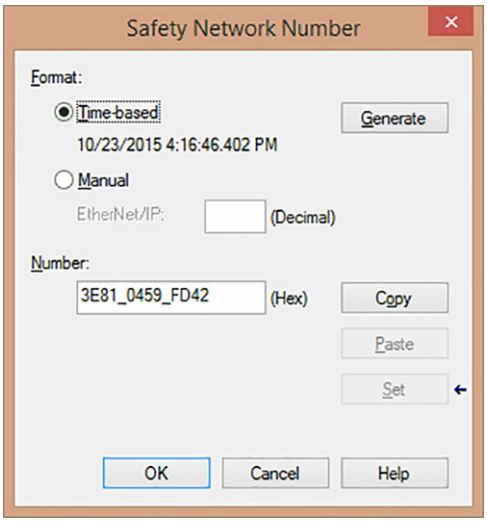
DICA Vários números de rede de segurança podem ser atribuídos a uma sub-rede CIP Safety ou a um rack ControlBus™ contendo vários dispositivos de segurança.

O SNN pode ser atribuído ao software (baseado em tempo) ou atribuído ao usuário (manual). Os dois formatos de SNN serão descritos nas próximas seções.

SNN com base na hora

Se o formato com base na hora for selecionado, o valor do SNN gerado representará a data e hora nas quais o número foi gerado, de acordo com o microcomputador que executa o software de configuração.

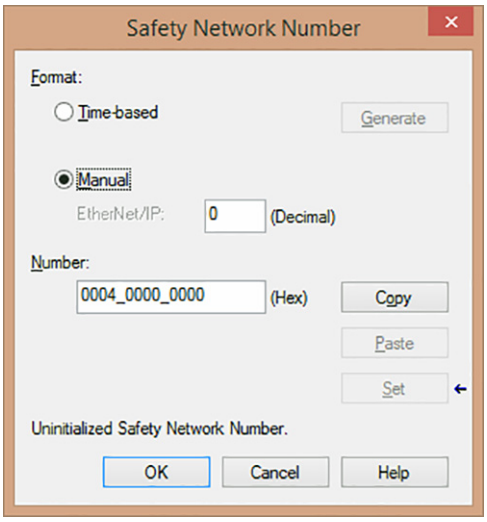
Figura 7 – Formato com base na hora



SNN manual

Se o formato manual for selecionado, o SNN será representado pelos valores inseridos de 1 a 9999 decimal.

Figura 8 – Formato SNN com base manual



Atribuição do número da rede de segurança (SNN)

Você pode permitir que a aplicação Logix Designer atribua automaticamente um SNN ou você pode atribuir o SNN manualmente.

Atribuição automática

Quando um novo controlador ou módulo é criado, um SNN baseado na hora é atribuído automaticamente pelo software de configuração. As adições subsequentes do novo módulo de segurança à mesma rede CIP Safety são atribuídas ao mesmo SNN definido no endereço mais inferior da rede CIP Safety.

Atribuição manual

A opção manual destina-se a sistemas CIP Safety roteáveis nos quais o número de sub-redes da rede e redes de interconexão é pequeno e aos quais os usuários podem querer gerenciar e atribuir o SNN de forma lógica de acordo com a aplicação específica.

Consulte Alteração do número da rede de segurança (SNN) na página 66.

IMPORTANTE	Se um SNN for atribuído de forma manual, certifique-se de que a expansão do sistema não resultará em duplicação de combinações de SNN e endereço de nó. Um erro de verificação ocorre se seu projeto contém SNN e combinações de endereço do nó duplicados. Você ainda pode verificar o projeto, mas a Rockwell Automation recomenda que você resolva as combinações duplicadas.

Automático vs. manual

Para usuários comuns, a atribuição automática de um SNN é suficiente. Todavia, a manipulação manual do SNN é necessária se o seguinte for verdade:

- São utilizados tags consumidas de segurança.
- O projeto consome dados de entrada de segurança de um módulo cuja configuração pertence a outro dispositivo.
- Um projeto de segurança é copiado em uma instalação de hardware diferente dentro do mesmo sistema CIP Safety roteável.

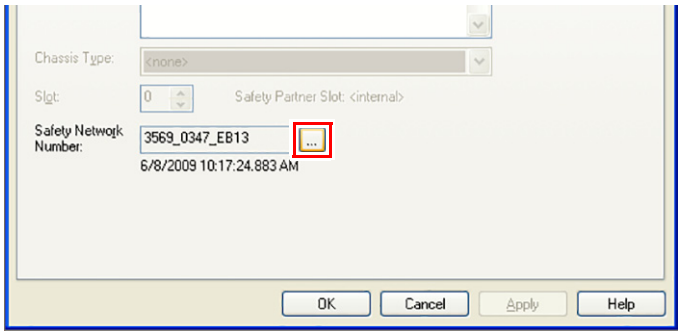
Alteração do número da rede de segurança (SNN)

Antes de mudar o SNN, é necessário fazer o seguinte:

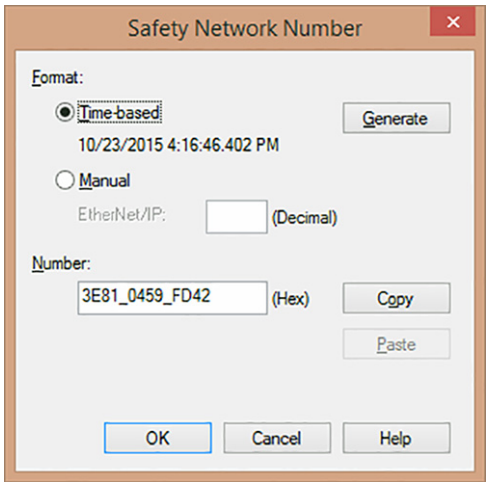
- Se o projeto está com trava de segurança, então é necessário destravá-lo. Consulte Bloqueando o controlador com trava de segurança na página 156.
- Se existe uma assinatura de tarefa de segurança, então é necessário excluí-la.
  Consulte Excluir a assinatura da tarefa de segurança na página 159.

Mudar o endereço SNN do controlador

1. No organizador do controlador, clique com o botão direito do mouse no controlador e escolha Propriedades.
2. Na guia General da caixa de diálogo Propriedades do Controlador, clique ... à direita de número da rede de segurança para abrir a caixa de diálogo Número da rede de Segurança.



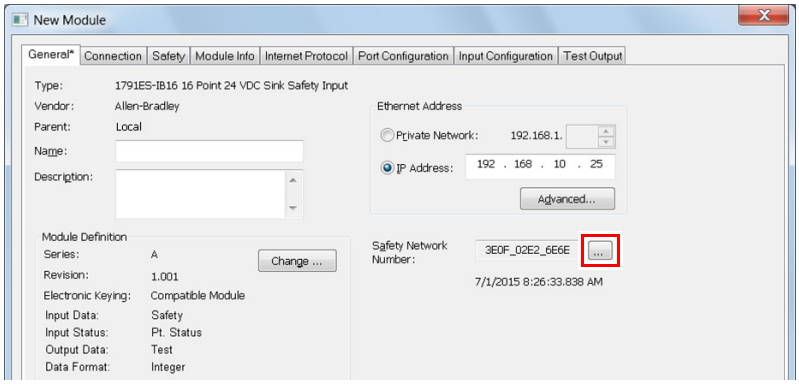
3. Clique em Baseado no tempo e em Gerar.



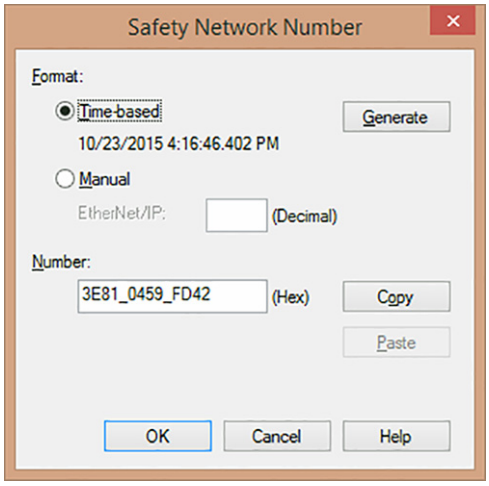
4. Clique em OK.

Altere SNN dos módulos de E/S de segurança nas redes CIP Safety

1. No organizador do controlador, fazer duplo clique no primeiro módulo de E/S de segurança na rede Ethernet para ver a guia Geral.
2. Clique em ... à direita do número da rede de segurança para abrir a caixa de diálogo Número da rede de Segurança.



3. Escolha Baseado no tempo e clique em GeneraGerarcriar um novo SNN referente à rede EtherNet/IP.

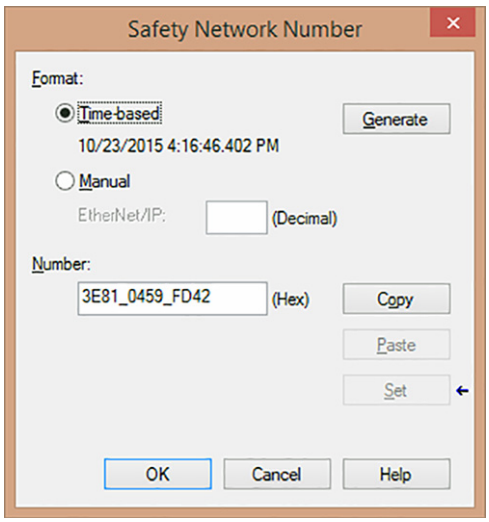


4. Clique em OK.
5. Clique em Copiar para copiar o novo SNN para a área de transferência do Windows.
6. Abra a guia Geral da caixa de diálogo Propriedades do Módulo do próximo módulo de E/S de segurança no módulo EtherNet/IP.
7. Clique em ... à direita do número da rede de segurança para abrir a caixa de diálogo Número da rede de Segurança.
8. Escolha Baseado no tempo e clique em Colar para colar o SNN da rede EtherNet/IP neste dispositivo.
9. Clique em OK.
10. Repita as etapas 6 a 8 para os módulos de segurança de E/S remanescentes sob o módulo de comunicação EtherNet/IP.
11. Repita as etapas 2 a 8 para quaisquer módulos de comunicação de rede remanescentes sob a árvore de Configuração E/S.

Copiar e Colar um SNN

Se a configuração do módulo pertencer a um controlador diferente, será necessário copiar e colar o SNN do proprietário da configuração no módulo na sua árvore de configuração E/S.

1. Na ferramenta de configuração de software do proprietário da configuração do módulo, abra a caixa de diálogo Número da Rede de Segurança do módulo.
2. Clique em Copiar.



3. Clique na guia General da caixa de diálogo Propriedades do Módulo do módulo de E/S na árvore Configuração de E/S do projeto do controlador consumidor.
   O controlador consumidor não é o proprietário da configuração.
4. Clique em ... à direita do número da rede de segurança para abrir a caixa de diálogo Número da rede de Segurança.
5. Clique em Paste.
6. Clique em OK.

Comunicação de Rede EtherNet/IP

A rede EtherNet/IP oferece um conjunto completo de serviços de controle, configuração e coleta de dados através de camadas do Protocolo Industrial Comum (CIP) através dos protocolos internet padrões, como TCP/IP e UDP. Esta combinação dos padrões mais aceitos oferece a capacidade necessária suportar troca de dados de informação e aplicações de controle.

Controladores CompactLogix 5370 usam interfaces de soquete e comunicação convencional sobre a rede Ethernet/IP para comunicação com equipamentos Ethernet que não suportam o protocolo de aplicação EtherNet/IP.

Para mais informações sobre transações de interface de soquete, consulte Interface de soquete na página 75.

Software disponível

O software listado na seguinte tabela é usado com um controlador CompactLogix 5370 em uma rede EtherNet/IP.

Software	Versão Requerida	Funções	Necessário
Studio 5000® ambiente	28.00.00 ou posterior	• Configura o projeto CompactLogix™ • Define a comunicação EtherNet/IP • Muda o endereço IP para equipamentos na rede, incluindo o controlador CompactLogix 5370.	Sim
RSLinx® Classic	3.80 ou posterior	• Atribui ou mude endereços IP para equipamentos em uma rede EtherNet/IP. • Configura os dispositivos de comunicação. • Fornece diagnósticos. • Estabelece comunicação entre os dispositivos.	
BOOTP/DHCP utilitário	A maioria das versões atuais está instalada com instalação de software RSLinx Classic	Atribui endereços IP a dispositivos em uma rede EtherNet/IP	Não

Funcionalidade EtherNet/IP

Os controladores CompactLogix 5370 oferecem esta funcionalidade de rede EtherNet/IP:

- Portas de rede EtherNet/IP incorporadas duplas
- Suporte às seguintes topologias de Rede EtherNet/IP:
  - topologia de Rede de Anel em Nível de Equipamento
  - topologia de rede linear
  - topologia da rede de estrela
- Suporte para protocolo de segurança CIP
- Suporte a Movimento Integrado por uma rede EtherNet/IP
- Interface de soquete para comunicação com equipamentos Ethernet que não suportam o protocolo de aplicação EtherNet/IP

- Detecção de endereço IP duplicado
- Comunicação unicast e multicast
- Suportam envio de mensagem, tags produzidos/consumidos, IHM e E/S distribuída
- Interface via cabos de par trançado RJ45
- suportam operação de transmissão half/full-duplex de 10 Mbps ou de 100 Mbps.
- Suportam chaves-padrão.
- Não requerem sequenciamento de rede
- Não requerem tabelas de roteamento

Nós em uma Rede EtherNet/IP

Ao configurar o seu sistema de controle CompactLogix 5370, é necessário contar com o número de nós Ethernet a serem incluídos na seção Configuração de E/S do seu projeto. Controladores CompactLogix 5370 têm limites no número de nós que eles suportam na seção de configuração de E/S.

Tabela 7 – Orientações de Nó Ethernet de Controlador Compact GuardLogix 5370

Nº. Núm.	Nós Ethernet Suportados
1769-L30ERMS	16
1769-L33ERMS 1769-L33ERMOS	32
1769-L36ERMS 1769-L36ERMOS	48
1769-L37ERMOS(1)	64

(1) Disponível na versão do firmware 30.

IMPORTANTE Enquanto os controladores CompactLogix 5370 oferecem a opção de usar contagem de nó Ethernet para efetivamente e eficientemente projetar um sistema de controle, os controladores não têm limites de conexão em uma rede EtherNet/IP.

Para mais informações sobre como projetar uso de rede EtherNet/IP no seu sistema de controle CompactLogix 5370, consulte estes recursos:

- A Ferramenta de Capacidade EtherNet/IP disponível em http://www.rockwellautomation.com/global/products-technologies/integrated-architecture/tools/overview.page.
  A Ferramenta de Capacidade EtherNet/IP lhe ajuda no layout inicial da sua rede EtherNet/IP.
- Manual de referência sobre considerações de design de Ethernet, publicação ENET-RM002.

Equipamentos Excluídos da Contagem de Nós

Ao considerar a limitação de nós Ethernet de um controlador CompactLogix 5370, você não conta dispositivos Ethernet que existam na rede EtherNet/IP mas não estejam adicionados à seção Configuração de E/S do projeto.

Os seguintes dispositivos não são adicionados à seção Configuração de E/S do seu projeto e não são contados entre o número total de nós:

- Computador
- Equipamentos IHM que não são incluídos na seção de configuração de E/S, por exemplo, terminais PanelView™ Plus
- Instrução MS
- Dispositivos com os quais os controladores Compact GuardLogix 5370 usam uma Interface de soquete para se comunicar.

  Por exemplo, os seguintes equipamentos requerem comunicação via uma interface de soquete:
  - Equipamento Modbus TCP/IP
  - Scanners de código de barras

Topologias de Rede EtherNet/IP

Os controladores CompactLogix® 5370 suportam tipos de rede EtherNet/IP:

- Topologia de Rede de Anel em Nível de Equipamento (DLR)
- Topologia de rede linear
- Topologia da rede de estrela

Cada uma destas topologias de rede EtherNet/IP suporta aplicações que usam Movimento Integrado por meio de uma rede EtherNet/IP, se requerido.

Topologia de Rede de Anel em Nível de Equipamento (DLR)

Uma topologia da rede DLR é uma rede em anel com tolerância para falha única destinada à interconexão de equipamentos de automação. Uma rede DLR é composta de nós Supervisor (Ativo e Backup) e de Anel.

Topologias de rede DLR automaticamente convertem-se a topologias de rede lineares quando uma falha é detectada. A conversão a uma nova topologia de rede mantém a comunicação de dados na rede. A condição de falha é tipicamente facilmente detectada e corrigida.

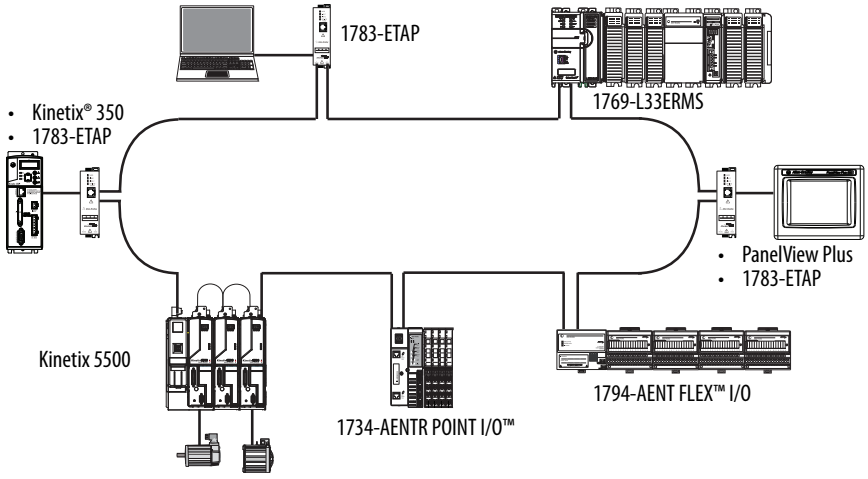
Controladores Compact GuardLogix 5370 conectam-se diretamente a uma topologia de rede DLR, ou seja, sem requerer um grampo 1783-ETAP para conectar-se à rede. Os controladores podem funcionar em qualquer um dos papéis em uma topologia da rede DLR, ou seja, nó supervisor ativo, nó supervisor de backup ou nó de anel.

IMPORTANTE	Os gráficos de topologia mostrados nesta seção são exemplos de aplicações que usam apenas topologias de rede DLR. Recomendamos que você tome cuidado ao considerar projetar uma aplicação que inclua conexão de uma topologia DLR com uma topologia de rede linear ou em estrela.

Para obter mais informações sobre como usar uma topologia de rede DLR, consulte o Guia de aplicação de tecnologia de comutação integrada EtherNet/IP, publicação ENET-AP005.

Figura 9 mostra um exemplo de sistema de controle 1769-L33ERMS usando uma topologia de rede DLR.

Figura 9 – Exemplo de sistema de controle 1769-L33ERMS usando uma topologia de rede DLR

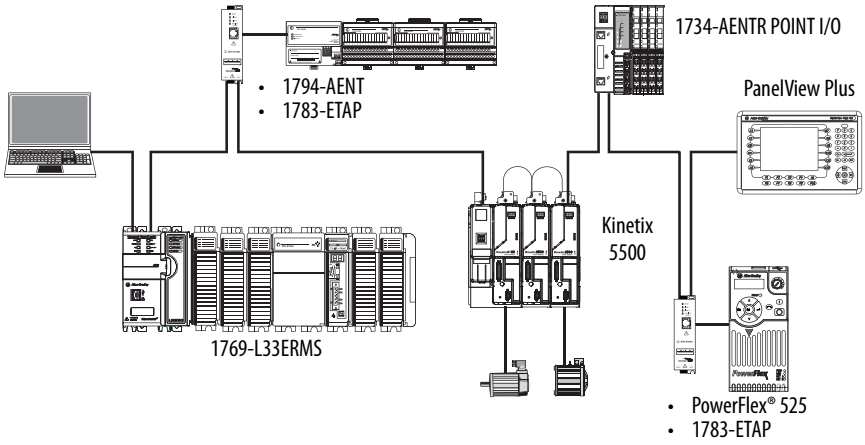


Topologia de rede linear

Uma topologia de rede linear é uma coleção de equipamentos que são conectados em formato de ligação em cadeia por uma rede EtherNet/IP. Equipamentos capazes de conectarem-se em uma topologia de rede linear usam tecnologia de chave incorporada para eliminar qualquer necessidade para uma chave separada, como requerido em topologias de rede de Estrela.

Figura 10 mostra um exemplo de sistema de controle 1769-L33ERMS usando uma topologia de rede linear.

Figura 10 – Exemplo de sistema de controle 1769-L33ERMS usando uma topologia de rede linear

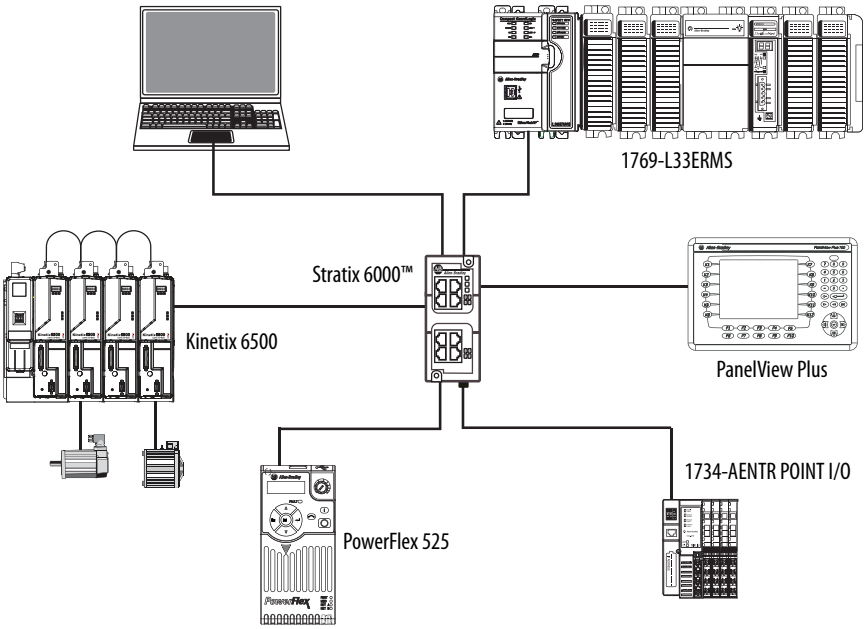


Topologia da rede de estrela

Uma topologia de rede de estrela é uma rede EtherNet/IP tradicional que inclui múltiplos equipamentos conectados um ao outro por meio de um comutador Ethernet.

Figura 11 mostra um exemplo de sistema de controle 1769-L33ERMS usando uma topologia de rede de estrela.

Figura 11 – Exemplo de sistema de controle 1769-L33ERMS usando uma topologia de rede de estrela



Conexões de Rede EtherNet/IP

Controladores CompactLogix 5370usam conexões para gerenciar a comunicação na rede EtherNet/IP Uma conexão é um mecanismo de comunicação ponto a ponto usado para transferir dados entre um transmissor e um receptor. Conexões podem ser lógicas ou físicas.

Você determina de forma indireta o número de conexões que o controlador usa ao configurar o controlador para comunicar-se com outros equipamentos no sistema. As conexões são alocações de recursos que fornecem comunicação mais confiáveis entre os equipamentos se comparados às mensagens não conectadas.

Todas as conexões EtherNet/IP são não programáveis. Uma conexão não programável é uma transferência de mensagem entre os dispositivos que é disparada pelo intervalo do pacote requisitado (RPI) ou pelo programa, como uma instrução MSG. O envio de mensagem não agendada permite enviar e receber dados quando necessário.

Tabela 8 – Especificações de porta de rede EtherNet/IP de controlador Compact GuardLogix 5370

Nº. Núm.	As conexões			Mensagens Desconectadas CIP (backplane + Ethernet)	Capacidade de Taxa de Pacote (pacotes/segundo)[2]		Suporte SNMP (senha requerida)	Suporte de Mídia	Tags produzidos/consumidos	
	Controller	TCP	CIP		E/S	IHM/MSG			Número de Tags Multicast, máx.[3]	Unicast Disponí-vel
1769-L30ERMS	256	120	256	256	6000 a 500 bytes/ pacote	400 mensagens/ s a 20% fatia de com. no tempo	Sim	Par Trançado	• 32 tags produzidos em multicast • 128 tags produzidas em unicast	Sim
1769-L33ERMS										
1769-L33ERMOS										
1769-L36ERMS										
1769-L36ERMOS										
1769-L37ERMOS[1]										

(1) Disponível na versão do firmware 30.

(2) Capacidade de taxa de pacote total = Tag produzida de E/S, máx + HMI/MSG, taxa de pacote máxima varia dependendo do tamanho do pacote. Para especificações mais detalhadas, consulte a seção de capacidade do arquivo EDS para o código de catálogo específico.

(3) Estes são os números máximos de conexões de E/S CIP.

Interface de soquete

O controlador CompactLogix 5370 pode usar interfaces de soquete para comunicação com equipamentos Ethernet que não suportam o protocolo de aplicação EtherNet/IP.

Exemplos de equipamentos que não suportam o protocolo de aplicação EtherNet/IP mas podem ser usados em uma aplicação de controlador CompactLogix 5370 incluem os seguintes:

- Equipamento Modbus TCP/IP
- Scanners de código de barras
- Leitores RFID

A interface de soquete é implementada por meio do Objeto Soquete. Controladores CompactLogix 5370 comunicam-se com o Objeto de Soquete por meio das instruções MSG. Todos os controladores CompactLogix 5370 devem utilizar instruções MS desconectadas com interfaces de soquete.

Para mais informações sobre interface de soquete, consulte o seguinte:

- Manual do usuário dos Controladores CompactLogix 5370, publicação 1769-UM021
- Técnica de Aplicação de Interface de Soquete EtherNet/IP, publicaçãoENET-AT002

Conexões de Qualidade de Serviço (QoS) e de Módulo de E/S

Controlador Compact GuardLogix 5370 suportam a tecnologia Quality of Service (QoS) A QoS permite que o controlador dê prioridade ao tráfego de rede EtherNet/IP. Por padrão, os controladores CompactLogix 5370 ficam com QoS habilitado. O QoS pode ser desabilitado configurando uma instrução de mensagem no aplicativo Logix Designer.

Alguns equipamentos EtherNet/IP não suportam tecnologia QoS a menos que o firmware do equipamento seja atualizado para um nível de revisão mínimo exigido do firmware. Por exemplo, o módulo de comunicação ControlLogix 1756-ENBT precisa usar a revisão de firmware 4.005 ou posterior para suportar tecnologia QoS.

Para certificar-se de que a comunicação entre controladores CompactLogix 5370 e módulos de E/S é mantida, verifique que os equipamentos EtherNet/IP usem a revisão de firmware mínima requerida pelo produto para suportar tecnologia QoS.

Para obter mais informações sobre o seguinte, veja a Nota Técnica 66325 da Base de Conhecimentos da Rockwell Automation® (disponível em https://rockwellautomation.custhelp.com/):

- Níveis mínimos de revisão de firmware dos dispositivos EtherNet/IP para suportarem tecnologia QoS
- Habilitar/Desabilitar QoS

Comunicação de Rede DeviceNet

Os controladores CompactLogix 5370 comunicam-se com outros dispositivos por meio de uma rede DeviceNet através de um módulo scanner DeviceNet 1769-SDN Compact I/O. A rede DeviceNet usa o protocolo industrial comum (CIP) para fornecer os recursos de controle, conexão e aquisição de dados para os dispositivos industriais.

IMPORTANTE	Controladores Compact GuardLogix suportam conexões padrão com a rede DeviceNet. Redes de segurança CIP sobre DeviceNet não são suportadas.

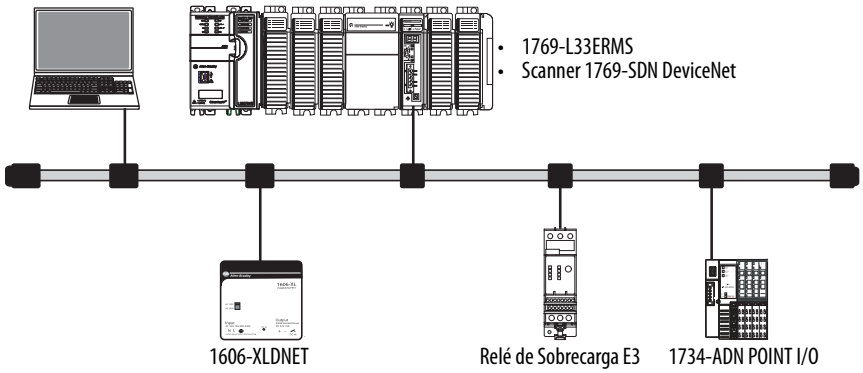
Software disponível

As aplicações de software listadas nesta tabela são necessárias ao usar um controlador CompactLogix 5370 em uma rede DeviceNet.

Software	Versão Requerida	Funções
Studio 5000 ambiente	28.00.00 ou posterior	Configura o projeto CompactLogix
RSLinx Classic	3.80 ou posterior	• Configura os dispositivos de comunicação. • Fornece diagnósticos. • Estabelece comunicação entre os dispositivos.
RSNetWorx™ para DeviceNet	25.00.00 ou posterior se usada com as versões de ambiente Studio 5000 acima	• Configura equipamentos DeviceNet • Define a lista de varredura para a rede DeviceNet

Figura 12 mostra um exemplo de sistema de controle 1769-L33ERMS usando uma rede DeviceNet.

Figura 12 – Exemplo de sistema de controle 1769-L33ERMS usando uma rede DeviceNet



Scanner DeviceNet Compact I/O 1769-SDN

Conecte um controlador CompactLogix 5370 a uma rede DeviceNet por meio de um módulo scanner DeviceNet 1769-SDN Compact I/O para **comunicação** padrão.

IMPORTANTE	A segurança CIF não é suportada em uma rede DeviceNet com scanner 1769-SDN. Os módulos de E/S de segurança DeviceNet não podem ser conectados a um sistema controlador Compact GuardLogix 5370 através de um scanner 1769-SDN

Considerações

Antes de instalar o módulo scanner, considere o seguinte:

- Você pode conectar o módulo scanner a um controlador, fonte de energia ou módulo de E/S adjacente.
- Você precisa considerar estas duas exigências em conjunto:
  - Classificação de distância da fonte de alimentação; consulte página 78
  - Capacidade de corrente em sistemas de controle Compact GuardLogix; consulte página 80
- O módulo scanner, como um mestre, pode gerenciar até 63 nós de E/S escravos.
- Outro mestre DeviceNet pode ser proprietário de um scanner que é simultaneamente um mestre e um escravo.

Recursos do scanner

O scanner tem a seguinte funcionalidade:

- suporta mensagem a equipamentos, não de controlador a controlador
- suporta rede de nível de controle a rede em nível de equipamento para programação, configuração, controle ou coleta de dados
- compartilha uma camada de aplicação comum com redes EtherNet/IP
- oferece diagnósticos para melhor aquisição de dados e detecção de falhas.

Classificação de distância da fonte de alimentação

Sistemas de controle CompactLogix 5370 permitem que você instale scanners 1769-SDN como módulos de expansão local. O módulo scanner 1769-SDN possui uma faixa de distância da fonte de alimentação que deve ser considerada antes de sua instalação.

A faixa de distância da fonte de alimentação é o número de slots de distância da fonte de alimentação a qual um módulo scanner 1769-SDN pode ser instalado. O módulo scanner 1769-SDN tem uma faixa de distância da fonte de alimentação de quatro. Portanto, seu sistema de controle CompactLogix 5370 pode incluir até 3 módulos entre o módulo scanner 1769-SDN e a fonte de alimentação.

Os sistemas de controlador CompactLogix 5370 não possuem módulos de E/S incorporados. Comece a contar os slots de expansão local com o primeiro módulo Compact I/O instalado próximo à fonte de alimentação quando for determinar o local de instalação de um scanner 1769-SDN e atender à faixa de distância da fonte de alimentação.

Em sistemas de controle do CompactLogix 5370, é possível instalar módulos scanner 1769-SDN à esquerda ou direita da fonte de alimentação. É possível também utilizar bancos adicionais ou locais nos sistemas de controle CompactLogix 5370, cada um permitindo a inclusão de um módulo scanner 1769-SDN.

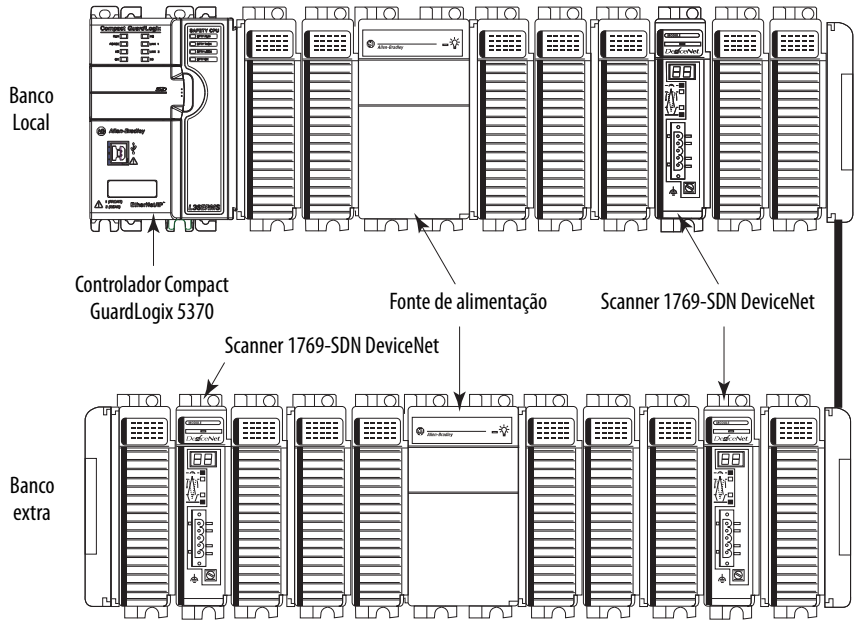
No banco local, o controlador deve ser o dispositivo localizado à extrema esquerda no sistema e é possível instalar no máximo três módulos entre o controlador e a fonte de alimentação. Portanto, quaisquer módulos scanner 1769-SDN que sejam instalados à esquerda da fonte de alimentação no banco local estão em um slot que atende às especificações de faixa de distância da fonte de alimentação.

Os sistemas do Controlador Compact GuardLogix 5370 também suportam o uso de bancos extra para os módulos de expansão local do sistema. Cada banco adicional exige uma fonte de alimentação Compact I/O1769. O banco pode ser projetado com módulos de expansão local em qualquer lado da fonte de alimentação.

Neste caso, é necessário instalar o módulo 1769-SDN com não mais de três módulos Compact I/O entre o scanner e a alimentação, independente se os módulos estão instalados à esquerda ou direita da fonte de alimentação.

Figura 13 na página 79 mostra os scanners 1769-SDN que estão instalados em um sistema de controle 1769-L36ERMS que estão de acordo com a classificação de distância da fonte de alimentação do módulo.

Figura 13 – Exemplo de classificação de distância da fonte de alimentação para um scanner 1769-SDN



Capacidade de corrente em sistemas de controle Compact GuardLogix 5370

Em um banco adicional ou local, os módulos instalados em ambos os lados da fonte de alimentação não podem consumir mais corrente do que a fonte de alimentação pode fornecer. Esta exigência parcialmente dita a colocação de módulos no banco.

Por exemplo, se um banco usa uma fonte de alimentação Compact I/O 1769-PA2, cada lado do banco tem uma capacidade atual de 1 A em 5 Vcc e 0,4 A em 24 Vcc. Como o scanner 1769-SDN tem uma corrente de consumo de 440 mA a 5 Vcc e 0 mA a 24 Vcc, só se pode instalar até dois scanners em cada lado da fonte de alimentação no banco, neste caso.

Para obter mais informações sobre capacidade de corrente máxima da fonte de alimentação 1769 Compact I/O e cálculos que você pode usar para projetar os módulos usados em bancos locais ou adicionais, consulte Calcule o consumo de energia do sistema na página 87.

Adicionar e configurar módulos de E/S padrão

Selecione módulos de E/S

Sistemas de controle Compact GuardLogix® 5370 oferecem estas opções de módulos de E/S padrão:

- Módulos de Expansão Locais
- Módulos de E/S Distribuída padrão por meio de uma Rede EtherNet/IP
- Módulos de E/S Distribuída em uma Rede DeviceNet

Módulos de Expansão Locais

Sistemas de controlador CompactLogix 5370 suportam o uso de módulos Compact I/O™ como módulos de expansão local juntamente com o backplane do CompactBus.

Considere o seguinte ao usar módulos de expansão locais:

- Os controladores suportam este tanto de módulos Compact I/O através de no máximo três bancos de E/S, ou seja, o banco local e dois bancos adicionais.

Nº. Núm.	Módulos de expansão local compatíveis, máx.
1769-L30ERMS	8
1769-L33ERMS	16
1769-L33ERMOS	–
1769-L36ERMS	30
1769-L36ERMOS 1769-L37ERMOS(1)	–

(1) Disponível na versão do firmware 30.

- Quando possível, use módulos Compact I/O específicos para atender às especificações de aplicação únicas.
- Considere o uso de um sistema de fiação 1492 para cada módulo de E/S como uma alternativa ao borne que vêm com o módulo.
- Use módulos PanelConnect™ 1492 e cabos se você estiver conectando módulos de entrada a sensores.

Instalar módulos de expansão local

Siga estes passos para adicionar um módulo Compact I/O ao seu sistema de controle CompactLogix 5370 e configurá-lo.

1. Prenda os módulos de E/S ou de comunicação Compact 1769 conforme descrito nestas publicações:
   - Instruções de instalação dos Módulos Compact I/O, publicação 1769-IN088
   - Instruções de instalação do módulo Scanner Compact I/O DeviceNet, publicação 1769-IN060
2. Se o seu sistema usa um banco local apenas, siga estes passos.
   a. Use os slots macho e fêmea para engatar uma terminação Compact I/O 1769-ECR no último módulo do sistema.
   b. Mova a alavanca do terminador do barramento terminal totalmente para a esquerda até clicar para travar o terminador do barramento terminal.
3. Se o seu sistema usa bancos adicionais, siga estes passos.
   a. Instale um cabo de expansão de barramento de comunicação Compact I/O 1769-CR*x* no lado direito do banco local.
   b. Conecte o cabo 1769-CR*x* adequado ao banco adicional se necessário.

      Ou seja, como você conecta o primeiro banco adicional – do lado direito ou esquerdo do banco, determina o cabo de expansão que é instalado no terminal do banco local. Consulte página 91 para exemplos de como conectar um banco local a bancos adicionais.
   c. Complete a instalação dos bancos restantes no seu sistema.

IMPORTANTE	Certifique-se de que você instale uma terminação no final do último banco no seu sistema.

Figura 2 na página 28 mostra exemplos de sistemas com módulos de expansão locais incluídos.

Cabear os módulos de expansão local

Faça a fiação de cada módulo Compact I/O usado como um módulo de expansão local de acordo com a documentação técnica daquele módulo.

Módulos de E/S Distribuída padrão por meio de uma Rede EtherNet/IP

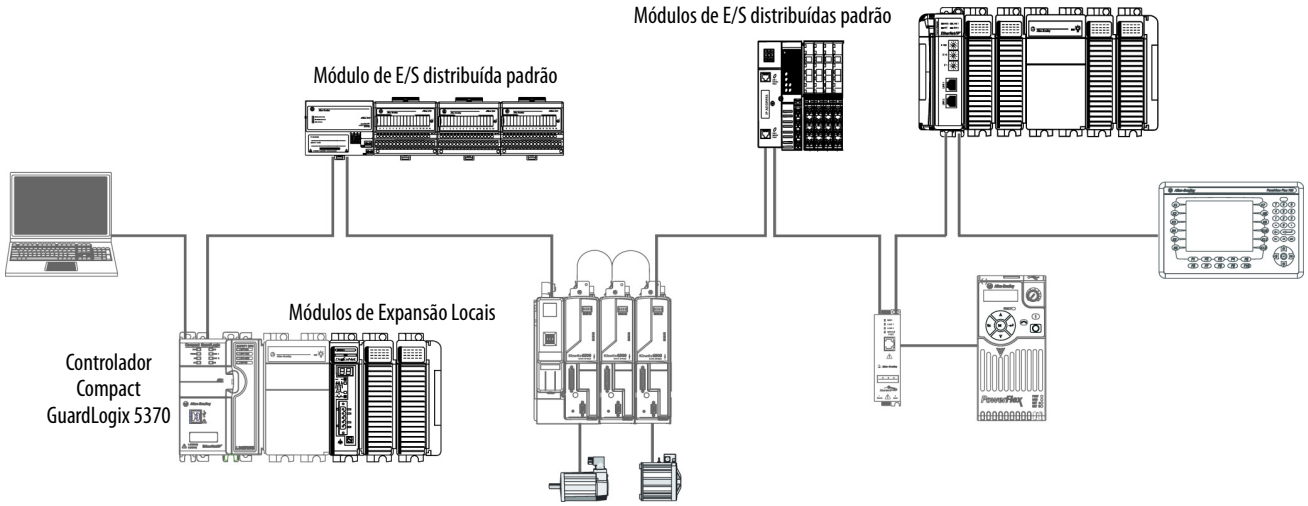
Você pode incluir módulos de E/S distribuída por meio de uma rede EtherNet/IP no seu sistema de controle CompactLogix 5370. Considere o seguinte ao usar módulos de E/S distribuída por meio de uma Rede EtherNet/IP:

- Cada adaptador EtherNet/IP remoto incluso no sistema precisa ser contado entre o número máximo de nós EtherNet/IP do controlador.

  Para obter mais informações sobre o número máximo de nós EtherNet/IP, consulte Nós em uma Rede EtherNet/IP na página 71.
- Os ajustes de parâmetro configuráveis de RPI variam dependendo de quais módulos de E/S distribuída são usados no sistema.

Figura 14 a seguir mostra um exemplo de sistema de controle 1769-L33ERMS que usa módulos de expansão locais e módulos de E/S distribuídos padrão por meio de uma rede EtherNet/IP.

Figura 14 – Exemplo do sistema de controle 1769-L33ERMS com módulos em uma rede EtherNet/IP



Módulos de E/S Distribuída em uma Rede DeviceNet

Você pode incluir módulos de E/S distribuída por meio de uma rede DeviceNet no seu sistema de controle CompactLogix 5370.

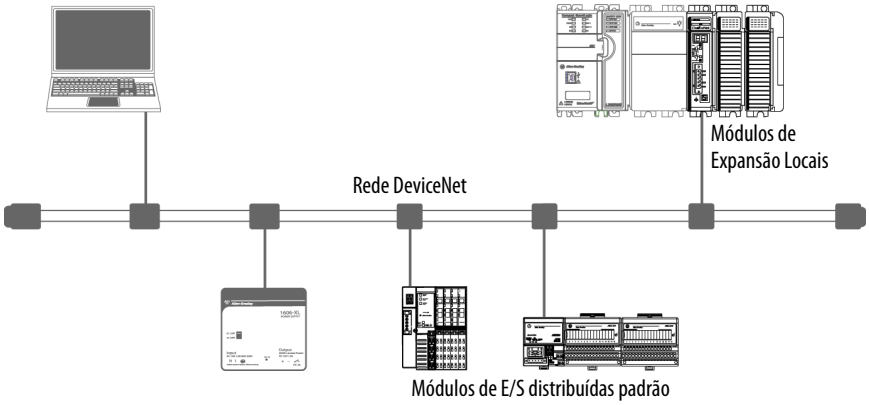
IMPORTANTE	A segurança CIF não é suportada no DeviceNet com módulo 1769-SDN. Os módulos de E/S de segurança DeviceNet não podem ser conectados a um sistema Compact GuardLogix através de um módulo 1769-SDN

Considere o seguinte ao usar módulos de E/S distribuída por meio de uma Rede DeviceNet:

- Ambiente Studio 5000® – Consulte Configure Módulos de E/S Distribuída por meio de uma Rede EtherNet/IP na página 96 para obter mais informações.
- Software RSNetWorx™ para DeviceNet – Para obter mais informações, consulte Comunicação de Rede DeviceNet na página 76.
- Para obter informações sobre como adicionar módulos de E/S distribuída ao seu sistema de controle Compact GuardLogix 5370, consulte Configure Módulos de E/S Distribuída por uma Rede DeviceNet na página 98.

Figura 15 mostra um exemplo de sistema de controle 1769-L33ERMS que usa módulos de expansão locais e módulos de E/S distribuídos padrão por meio de uma rede DeviceNet.

Figura 15 – Exemplo do sistema de controle 1769-L33ERMS com módulos em uma rede DeviceNet



Valide o Layout de E/S padrão

Após você ter selecionado os seus módulos de E/S, você precisa validar o sistema que você quer projetar. Considere estes pontos ao validar o posicionamento de layout de E/S:

- Estimar o intervalo do pacote requisitado
- Falhas de módulo relacionadas a estimativas de RPI
- Calcule o consumo de energia do sistema
- Faixa de distância da fonte de alimentação
- Posicionamento físico dos módulos de E/S

Estimar o intervalo do pacote requisitado

O intervalo do pacote requisitado (RPI) define a frequência em que o controlador envia dados para os módulos de E/S e recebe dados dos mesmos. Você define uma taxa de RPI para cada módulo de E/S do seu sistema.

Os controladores CompactLogix 5370 sempre tentam varrer um módulo de E/S na taxa RPI configurada. Para módulos de E/S individuais, uma falha de advertência ocorre se houver ao menos um módulo de E/S que não possa ser alimentado dentro do seu tempo de RPI.

Os parâmetros de configuração específicos para um sistema determinam o impacto nas taxas RPI reais. Estes fatores de configuração podem ter impacto na frequência de varrimento efetiva para qualquer módulo individual:

- Taxas às quis as taxas RPI são ajustadas para outros módulos Compact I/O
- Número de outros módulos Compact I/O no sistema
- Tipos de outros módulos Compact I/O no sistema
- Prioridades de tarefa de usuário nas aplicações

Tabela 9 – Orientações do Intervalo do Pacote Requisitado

Tipo do Módulo	Orientações[1]
Todos digitais	As seguintes orientações se aplicam: • 1 a 2 módulos podem ser varridos em 0,5 ms. • 3 a 4 módulos podem ser varridos em 1 ms. • 5 a 30 módulos podem ser varridos em 2 ms.
Mistura de digital e analógico ou todos analógicos	As seguintes orientações se aplicam: • 1 a 2 módulos podem ser varridos em 0,5 ms. • 3 a 4 módulos podem ser varridos em 1 ms. • 5 a 13 módulos podem ser varridos em 2ms. • 14 a 30 módulos podem ser varridos em 3 ms.
Especialidade	As seguintes condições se aplicam: • Para cada módulo 1769-SDN no sistema, aumente o RPI de cada outro módulo em 2 ms. • Para cada módulo 1769-HSC no sistema, aumente o RPI de cada outro módulo em 1 ms. • Para cada módulo 1769-ASCII no sistema, aumente o RPI de cada outro módulo em 1 ms. • Para cada módulo 1769-SM2 no sistema, aumente o RPI de cada outro módulo em 2 ms.

(1) As orientações nesta tabela não é um fator nos seguintes itens, que afetam o carregamento da CPU do controlador Compact GuardLogix 5370:

- Cronometragem RPI de E/S não afeta a tarefa de prioridade. Tarefas eventuais e periódicas têm maior prioridade que tarefas de usuário e de E/S.
- IOT (Instrução de saída imediata)
- Mensagem
- Navegação CompactBus como o acesso de rede DeviceNet através do 1769-SDN com conexão Ethernet ou USB Compact GuardLogix 5370

As diretrizes do módulo RPI podem exigir ajustes (aumentar 1 ms ou mais) se o aplicativo controlador Compact GuardLogix 5370 incluir um ou mais dos listados nesta tabela. Monitorar falhas menores no controlador para determinas se ocorreram sobreposições do módulo RPI.

Você pode configurar as taxas RPI de módulos Compact I/O individuais mais altas que as taxas listadas em Tabela 9. O RPI mostra quão rapidamente módulos podem sofrer varredura, e não o quão rapidamente uma aplicação pode usar os dados. O RPI é assíncrono à varredura do programa. Outros fatores, como duração da execução do programa, afetam o tráfego de E/S.

Falha de módulo relacionada a estimativas de RPI

Ao seguir as orientações descritas na Tabela 9, a maioria dos sistemas de controle Compact GuardLogix 5370 opera como esperado. Alguns sistemas que seguem as orientações podem apresentar uma falha secundária de sobreposição de módulo RPI descrita em Tabela 10.

Tabela 10 – Falha de sobreposição de RPI do módulo

Nome	Informações sobre a falha	Condição Em Que a Falha Ocorre
Sobre-posição de RPI do Módulo	Falha de E/S (Tipo 03) (Código 94) Sobreposição do RPI do módulo detectado Slot do Módulo = *x*, onde *x* é o número de slot do módulo de E/S na seção de configuração de E/S	Esta falha é iniciada quando a atualização da RPI atua de um módulo de E/S sobrepõe-se com a atualização anterior de RPI. A guia Falhas secundárias na caixa de diálogo Propriedades do Controlador indica qual RPI do módulo está sobrepondo. Se múltiplos módulos de E/S sofrerem a falha, a aplicação indica que a falha ocorreu no primeiro destes módulos de E/S. Tipicamente, é um módulo de E/S com grandes tamanhos de vetor de Entrada/Saída. Exemplos de módulos que usam grandes tamanhos de vetor de Entrada/Saída incluem módulos 1769-SDN e 1769-HSC. Nestes casos, recomendamos que você ajuste o RPI do módulo para remover a falha. Uma vez a falha tendo sido eliminada do primeiro módulo de E/S, o aplicativo indica o próximo módulo que esta com a falha. Este padrão continua até a falha ser eliminada de todos os módulos de E/S afetados. Para evitar esta falha, configure a taxa RPI dos módulos de E/S para valores numéricos mais altos. Recomendamos a utilização de um valor RPI que não seja um múltiplo comum de outros valores RPI de módulos, como 2,5 ms, 5,5 ms ou 7 ms • Recomendamos que você não coloque em operação sistemas de controle CompactLogix 5370 com falhas de Sobreposição de RPI de Módulo. • Um sistema que experiencie muitas falhas de Sobreposição de RPI de Módulo pode não operar corretamente porque dados de E/S não são amostrados na taxa esperada, determinada pelas configurações de RPI. • Quando se faz download do projeto ou um valor de RPI de módulo de E/S é ajustado, espera-se que uma falha de advertência ocorra. Falhas sob estas condições são transitórias. Limpe a falha e espere para que esta reapareça antes de ajustar o valor RPI ou as prioridades de tarefa.

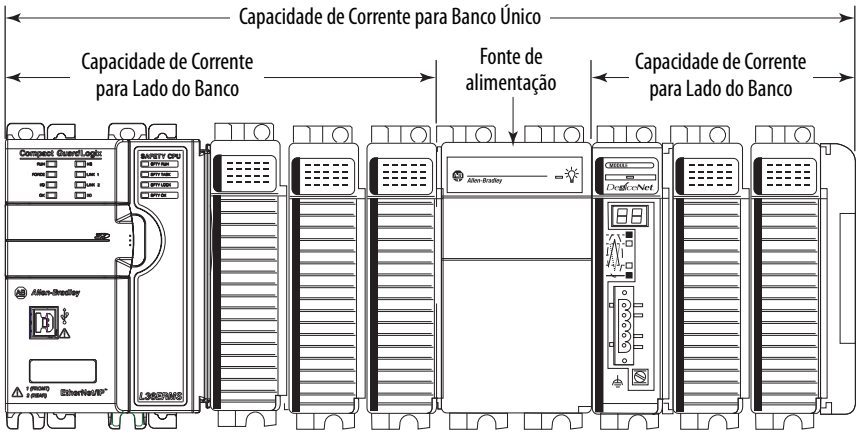
Calcule o consumo de energia do sistema

As fontes de energia Compact I/O 1769 fornecem energia a bancos locais e adicionais CompactLogix. A alimentação fornecida é medida em capacidade de corrente.

Considere estes pontos quando projetar seus bancos do sistema controlador Compact GuardLogix 5370:

- Fontes de energia Compact I/O 1769 têm dois requisitos máximos de capacidade de corrente que afetam como você projeta e configura um banco único.

  Estes a seguir são os requisitos de capacidade de corrente máxima:
  - Capacidade de corrente máxima para um banco único
  - Capacidade de corrente máxima para cada lado da fonte de alimentação



- Os requisitos de capacidade máxima de corrente variam de acordo com a fonte de alimentação usada no banco.

Cat. da fonte de alimentação Núm.	Capacidade de Corrente, máx. para Banco Único	Capacidade de Corrente, máx. para Cada Lado do Banco[1]
1769-PA2	2 A a 5 Vcc e 0,8 A a 24 Vcc	1 A a 5 Vcc e 0,4 A a 24 Vcc
1769-PB2		
1769-PA4	4 A a 5Vcc e 2 A a 24 Vcc	2 A a 5Vcc e 1 A a 24 Vcc
1769-PB4		

(1) Especificações para bancos com equipamentos em ambos os lados esquerdo e direito da fonte de alimentação.

Calcule o Consumo de Energia em um Banco Adicional

IMPORTANTE Um banco requer controladores Compact GuardLogix 5370 para poder residir no slot mais à esquerda. No mínimo, você precisa calcular o consumo de energia do controlador do lado esquerdo da fonte de alimentação.

Se existirem módulos adicionais no lado esquerdo da fonte de alimentação, você precisa calcular o consumo de energia para esses módulos também.

Se existirem módulos adicionais instalados à direita da fonte de alimentação, você precisa calcular o consumo de energia para esse lado separadamente.

Use esta tabela para calcular o consumo de energia em um banco.

Tabela 11 – Cálculo de Consumo de Energia de Módulo para um Banco Local

Lado da Fonte de Energia	Cat. do dispositivo Núm.	Número de módulos[3]	Especificações de Corrente do Módulo		Corrente Calculada = (Número de Módulos) x (Especificações de Corrente do Módulo)	
			a 5 Vcc (em mA)	a 24 Vcc (em mA)	a 5 Vcc (em mA)	a 24 Vcc (em mA)
Esquerda – Exigido	1769-L30ERMS 1769-L33ERMS 1769-L36ERMS	1	500	225	500	225
Esquerda – Opcional	Específicas de Módulo de E/S	Até 3	Específicas do Módulo	Específicas do Módulo		
	Corrente total necessária[2]:					
Direita	Específicas de Módulo de E/S **IMPORTANTE**: Insira uma sequência separada neste cálculo para cada módulo de E/S.	Até 8	Específicas do Módulo	Específicas do Módulo		
	Corrente total necessária[2]:					
Corrente total requerida para banco único se forem instalados módulos em ambos os lados da fonte de alimentação[1]:						

(1) Este número não pode exceder a capacidade de corrente da fonte de alimentação para o banco.

(2) Este número não pode exceder a capacidade de corrente da fonte de alimentação para este lado do banco.

(3) No banco local, você pode instalar no máximo três módulos à esquerda da fonte de alimentação porque os controladores CompactLogix 5370 possuem uma faixa de distância da fonte de alimentação de quatro é necessário que estejam dentro de quatro slots da fonte de alimentação Compact I/O. Do lado direito da fonte de alimentação no banco local e em ambos os lados da fonte de alimentação em bancos adicionais, é possível instalar até oito módulos se as faixas de distância para os módulos validarem o projeto do sistema.

Calcule o Consumo de Energia em um Banco Adicional

IMPORTANTE Em bancos adicionais, você pode instalar módulos de E/S para o lado esquerdo, direito, ou ambos os lados da fonte de alimentação.

O projeto do sistema determina como usar a tabela abaixo.

Use Tabela 12 para calcular o consumo de energia em um banco adicional.

Tabela 12 – Cálculo de consumo de energia de módulo para um banco adicional

Lado da Fonte de Energia	Cat. do dispositivo Núm.	Número de módulos[3]	Especificações de Corrente do Módulo		Corrente Calculada = (Número de Módulos) x (Especificações de Corrente do Módulo)	
			a 5 Vcc (em mA)	a 24 Vcc (em mA)	a 5 Vcc (em mA)	a 24 Vcc (em mA)
Esquerda – Opcional em um banco adicional	Módulos de E/S **IMPORTANTE**: Insira uma sequência separada neste cálculo para cada módulo de E/S.	Até 8	Específicas do Módulo	Específicas do Módulo		
	Corrente total necessária[2]:					
Direita – Opcional em um banco único	Módulos de E/S **IMPORTANTE**: Insira uma sequência separada para cada módulo de E/S.	Até 8	Específicas do Módulo	Específicas do Módulo		
	Corrente total necessária[2]:					
Corrente total requerida para banco se forem instalados módulos em ambos os lados da fonte de alimentação[1]:						

(1) Este número não pode exceder a capacidade de corrente da fonte de alimentação para o banco.
(2) Este número não pode exceder a capacidade de corrente da fonte de alimentação para este lado do banco.
(3) É possível instalar até oito módulos em bancos adicionais se as faixas de distância da fonte de alimentação para os módulos validarem o projeto do sistema.

Posicionamento físico de módulos de E/S

Dependendo do código de catálogo do controlador, controladores CompactLogix 5370 suportam entre 8 e 30 módulos de E/S. Para obter mais informações sobre códigos de catálogo, consulte Módulos de Expansão Locais na página 81.

Considere estes fatores ao determinar o posicionamento físico dos módulos de E/S:

- Você pode instalar módulos de E/S em bancos locais e adicionais.
- Você pode instalar módulos de E/S à esquerda e à direita da fonte de alimentação.
- Quando um sistema exige vários bancos, você pode instalar os bancos adicionais horizontalmente ou verticalmente, como mostrado em Figura 2 na página 28.
- Cada módulo de E/S também tem uma faixa de distância de fonte de alimentação e corrente de consumo máxima específicas. Consideradas em conjunto, faixas de distância e correntes de consumo determinam onde os módulos de E/S podem ser posicionados em um banco e qual configuração de módulos pode ser instalada no banco.

  Para obter mais informações sobre classificações de distância da fonte de alimentação, consulte Classificação de distância da fonte de alimentação na página 91. Para obter mais informações sobre consumo de energia do sistema, consulte Calcule o consumo de energia do sistema na página 87.

Banco Local

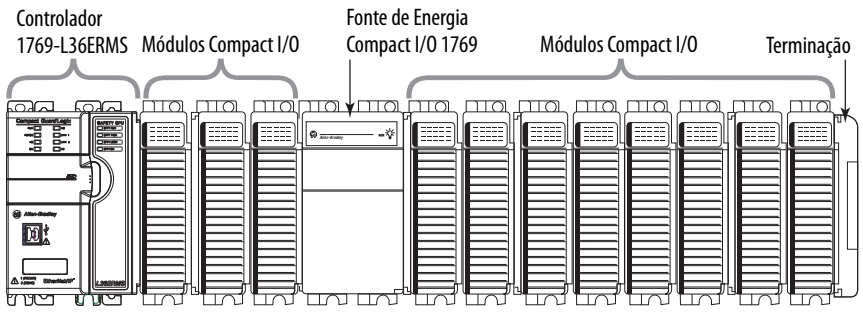
Para validar o projeto de banco local, confirme que o projeto atenda estas especificações:

- O controlador é o equipamento mais para a esquerda no banco local.
- Não mais do que três módulos estão instalados entre o controlador e o lado esquerdo da fonte de alimentação.
- Não mais do que oito módulos estão instalados para a direita da fonte de alimentação.
- O consumo de energia dos módulos em cada lado da donte de alimentação não excede a capacidade da fonte naquele lado.
- O consumo de energia total por todos os módulos no banco não excede a capacidade da fonte de alimentação para o banco todo.
- Módulos estão instalados de modo que as especificações de faixa de distância e consumo de energia do sistema são atendidas.

  Por exemplo, o módulo scanner 1769-SDN tem uma faixa de distância da fonte de alimentação de quatro. Se o projeto inclui a instalação de um scanner 1769-SDN com mais do que três módulos entre ele e a fonte de alimentação, o design é inválido.

IMPORTANTE	Com relação a faixas de distância da fonte de alimentação, se você instalar um módulo que viole sua especificação de faixa de distância, o sistema pode parecer operar normalmente por um período de tempo, mas pode experienciar problemas operacionais ao longo do tempo, como falhas de E/S.

O gráfico de exemplo abaixo mostra um banco local.



Bancosadicionais

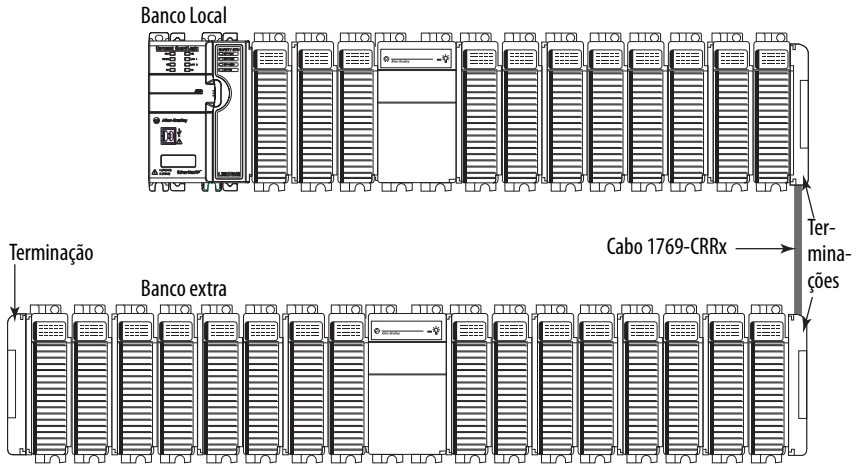
Se a sua aplicação pedir doze ou mais módulos de E/S, no mínimo, você deve instalar os módulos em bancos múltiplos adicionais. As condições de cada aplicação determinam o número de bancos adicionais.

Uma vez que o projeto do banco local tenha sido validado, você precisa validar o projeto para quaisquer bancos adicionais. Para validar projetos de bancos adicionais, confirme que o projeto atenda estas especificações:

- Cabos de expansão de barramento de comunicação Compact I/O sejam usados apropriadamente.

  DICA Cabos de expansão Compact I/O tenham as mesmas dimensões que as terminações independentemente de se elas serão instaladas no lado direito ou esquerdo do barramento de comunicação.

- Não mais do que oito módulos estejam instalados para qualquer lado da fonte de alimentação.
- O consumo de energia dos módulos em cada lado da donte de alimentação não excede a capacidade da fonte naquele lado.
- Módulos estão instalados de modo que as especificações de faixa de distância são atendidas.
- As terminações estão devidamente instaladas, como mostrado no seguinte gráfico.



Classificação de distância da fonte de alimentação

Os sistemas de controlador CompactLogix 5370 não possuem módulos de E/S incorporados. Comece a contar os slots de expansão local com o primeiro módulo Compact I/O instalado próximo à fonte de alimentação quando for determinar o local de instalação de um módulo Compact I/O e atender à faixa de distância da fonte de alimentação.

Em sistemas de controle do CompactLogix 5370, é possível instalar módulos Compact I/O à esquerda ou direita da fonte de alimentação. É possível também utilizar bancos adicionais ou locais nos sistemas de controle CompactLogix 5370, cada um permitindo a inclusão dos módulos Compact I/O.

Banco Local

No banco local, o controlador deve ser o dispositivo localizado à extrema esquerda no sistema e é possível instalar no máximo três módulos entre o controlador e a fonte de alimentação. Portanto, quaisquer módulos Compact I/O que sejam instalados à esquerda da fonte de alimentação no banco local estão em um slot que atende às especificações de faixa de distância da fonte de alimentação.

Bancos adicionais

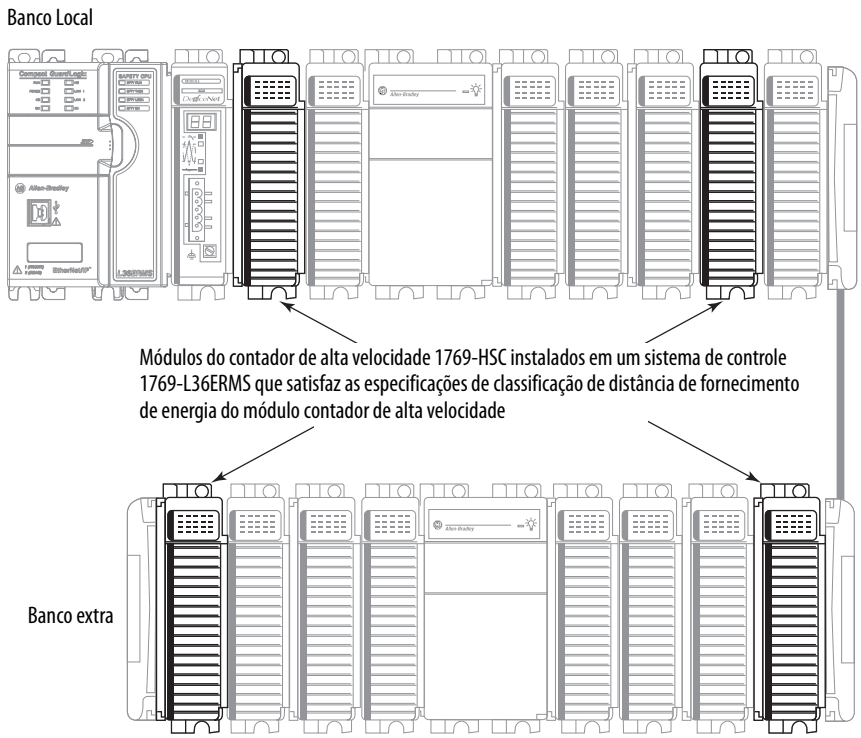
Os sistemas do Controlador Compact GuardLogix 5370 também suportam o uso de bancos extra para os módulos de expansão local do sistema. Cada banco adicional exige uma fonte de alimentação Compact I/O 1769. O banco pode ser projetado com módulos de expansão local em qualquer lado da fonte de alimentação.

A maioria dos módulos Compact I/O possui valores de faixa de distância da fonte de alimentação que permitem sua instalação em qualquer slot em ambos os lados da fonte de alimentação em bancos adicionais. Alguns módulos Compact I/O têm classificações de distância da fonte de alimentação que afetam o local em que podem ser instalados no sistema de controle Compact GuardLogix 5370.

Por exemplo, os módulos do contador de alta velocidade 1769-ASCII Compact ASCII e 1769-HSC Compact possuem uma faixa de distância de quatro. Esses módulos podem ser instalados nos slots de 1 a 3 dos módulos de expansão local.

Neste caso, é necessário instalar o módulo 1769-ASCII e o módulo do contador de alta velocidade 1769-HSC com não mais de três módulos Compact I/O entre o módulo e a alimentação, independente se os módulos estão instalados à esquerda ou direita da fonte de alimentação.

Este gráfico mostra os módulos do contador de alta velocidade 1769-HSC que são instalados em um sistema de controle 1769-L36ERMS que está de acordo com a faixa de distância da fonte de alimentação do módulo.

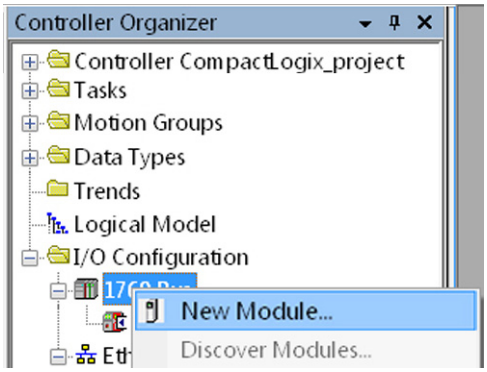


Para obter mais informações sobre a classificação de distância da fonte de alimentação para um módulo Compact I/O, consulte o guia de Seleção CompactLogix™, publicação 1769-SG001.

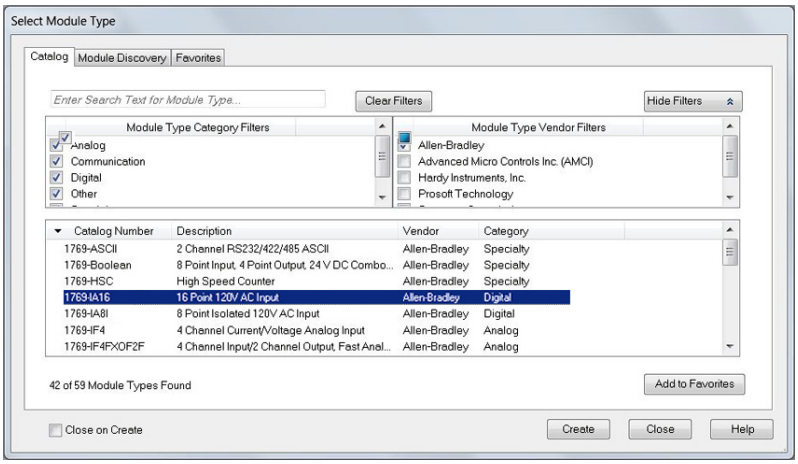
Configurar E/S padrão

Siga estes passos para adicionar um módulo Compact I/O ao seu sistema de controle CompactLogix 5370 e configurá-lo.

1. No Organizador do Controlador, selecione e clique com o botão direito no barramento 1769-AENT em Configuração de E/S, e então escolha Novo Módulo.

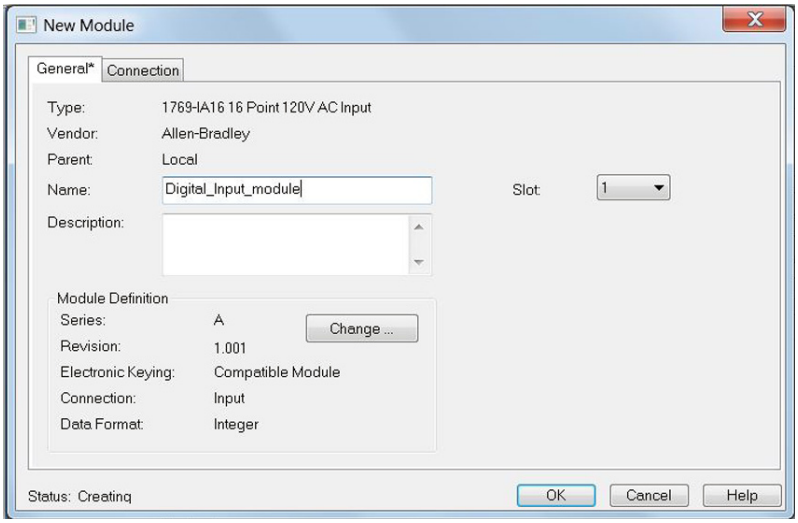


2. Selecione o módulo de E/S desejado e clique em Criar.



A caixa de diálogo Novo Módulo aparecerá.

3. Configure o novo módulo de E/S como necessário e clique em OK.



Parâmetros de Configuração Comuns

Enquanto as opções de configuração variam de módulo para módulo, existem algumas opções comuns que você configura tipicamente ao usar módulos Compact I/O em um sistema de controle Compact GuardLogix 5370, como descrito na Tabela 13.

Tabela 13 – Parâmetros de configuração comuns

Opção de configuração	Descrição
Intervalo do pacote requisitado (RPI)	O RPI especifica o intervalo em que os dados são transmitidos ou recebidos por uma conexão. Para módulos de E/S Locais Compact 1769, dados são transmitidos ao controlador de acordo com o RPI. Quando varridos no barramento local ou por meio de uma rede EtherNet/IP, módulos de entrada sofrem varredura de acordo com o RPI especificado na configuração do módulo. Tipicamente, você configura um RPI em milissegundos (ms). Para módulos de E/S, a faixa é de 0,5 a 750 ms. Ao serem varridos por uma rede DeviceNet, módulos de entrada distribuídas sofrem varredura na taxa suportada pelo módulo adaptador DeviceNet conectando os módulos de entrada à rede. Por exemplo, a taxa de varredura para POINT I/O™ 1734 distribuídos por DeviceNet pode ocorrer apenas tão rapidamente quanto o adaptador DeviceNet 1734-ADN puder transmitir os dados.
Definição do módulo	Conjunto de parâmetros de configuração que afetam a transmissão de dados entre o controlador e o módulo de E/S. Os parâmetros incluem o seguinte: • Séries – Séries de hardware do módulo. • Revisão – Níveis de revisão de firmware principal e secundário usados no módulo. • Codificação eletrônica – Consulte LOGIX-AT001 para informações sobre codificação eletrônica. • Conexão – Tipo de conexão entre o controlador gravando a configuração e o módulo de E/S, como Output. • Formato de dados – Tipo dos dados transferidos entre o controlador e o módulo de E/S, e quais tags são gerados quando a configuração é concluída.
Falha de Módulo no Controlador Se a Conexão Falha Enquanto no Modo de Operação	Esta opção determina como o controlador é afetado se a conexão a um módulo de E/S falhar durante o modo de operação. Você pode configurar o projeto para que uma falha de conexão cause uma falha grave no controlador, ou não. A configuração padrão é para esta opção estar habilitada, ou seja, se a conexão a um módulo de E/S falhar no modo de Operação, uma falha grava ocorrerá no controlador.

Conexões de E/S

Um sistema Logix5000™ usa conexões para transmitir dados de E/S, como descrito em Tabela 14.

Tabela 14 – Conexões de Módulo de E/S

Conexão	Descrição
Direta	Uma conexão direta é um link de transferência de dados em tempo real entre o controlador e um módulo de E/S. O controlador mantém e monitora a conexão. Qualquer quebra na conexão, como uma falha de módulo, faz com que o controlador configure bits de status de falha na área de dados associada ao módulo. Tipicamente, módulos de E/S analógicos, módulos de E/S de diagnóstico, e módulos especializados requerem conexões de tipo direto.
Otimizadas para rack	Para módulos de E/S digitais, você pode selecionar comunicação otimizada para rack. Esta opção é usada com módulos de E/S distribuída e a seleção de conexão com Otimização para Rack é feita ao configurar o adaptador remoto. Por exemplo, se você quiser usar uma conexão otimizada para rack com módulos de E/S digital em um sistema POINT I/O 1734 remoto, você configura o módulo 1734-AENT(R) para usar um tipo de conexão de otOptimizadinhoRack. Uma conexão otimizada para rack consolida uso de conexão entre o controlador e todos os módulos de E/S digital em um rack remoto ou em um trilho DIN único. Ao invés de ter conexões individuais, diretas a cada módulo de E/S, existe uma conexão para todo o rack (ou trilho DIN).

Configure Módulos de E/S Distribuída por meio de uma Rede EtherNet/IP

O seu sistema de controle CompactLogix 5370 pode usar módulos de E/S distribuído por meio de uma rede EtherNet/IP.

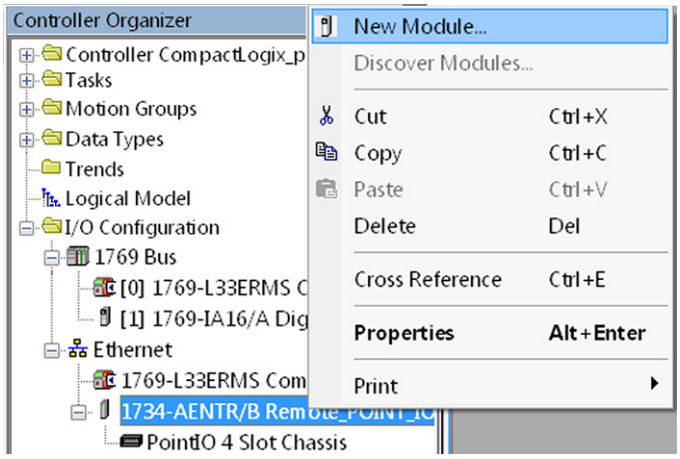
IMPORTANTE Ao acrescentar módulos de E/S distribuída, lembre-se de contar o adaptador Ethernet remoto para manter dentro da limitação do número máximo de nós de rede EtherNet/IP para o seu controlador específico.

Os módulos de E/S remota conectados ao controlador por meio do adaptador Ethernet não são contados para o limite máximo de nós Ethernet para o controlador.

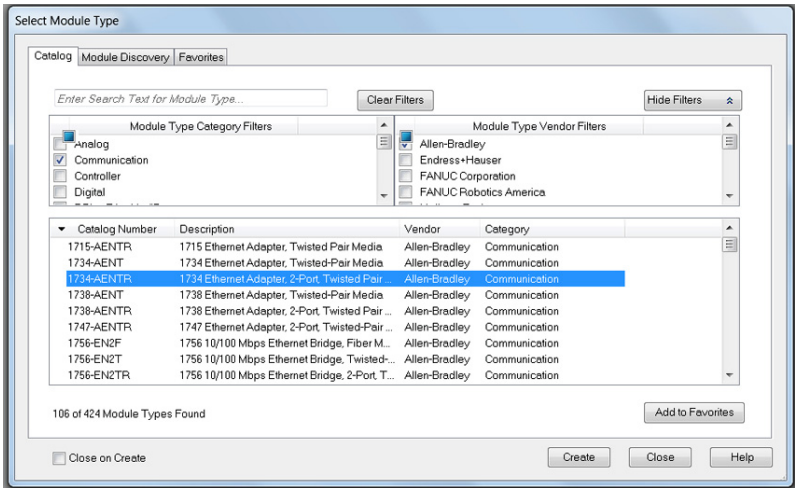
Para obter mais informações sobre limitações de nós, consulte Nós em uma Rede EtherNet/IP na página 71.

Complete estas etapas para configurar módulos de E/S distribuídos por meio de uma rede EtherNet/IP.

1. No Organizador do Controlador, selecione e clique com o botão direito em 1734-AENT em Ethernet, e então escolha Novo Módulo.

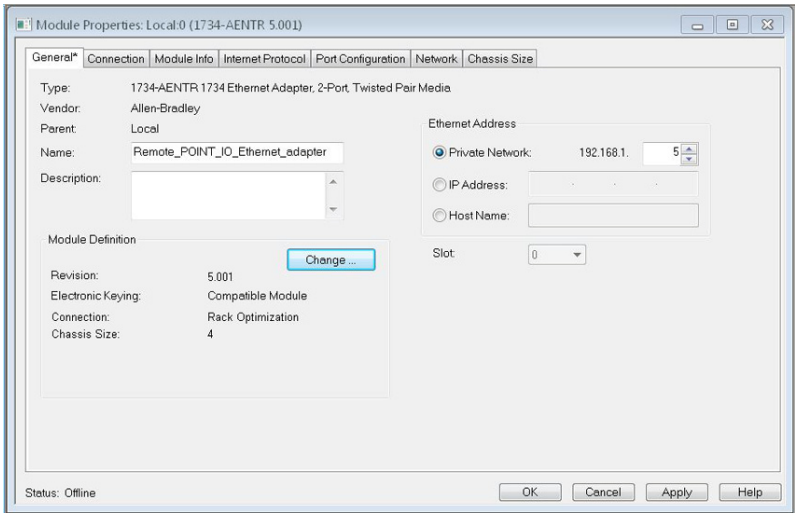


2. Selecione o adaptador Ethernet desejado e clique em Criar.

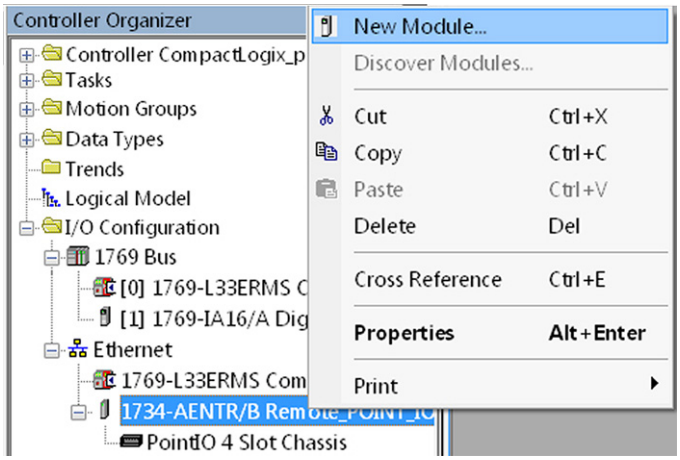


A caixa de diálogo Novo Módulo aparecerá.

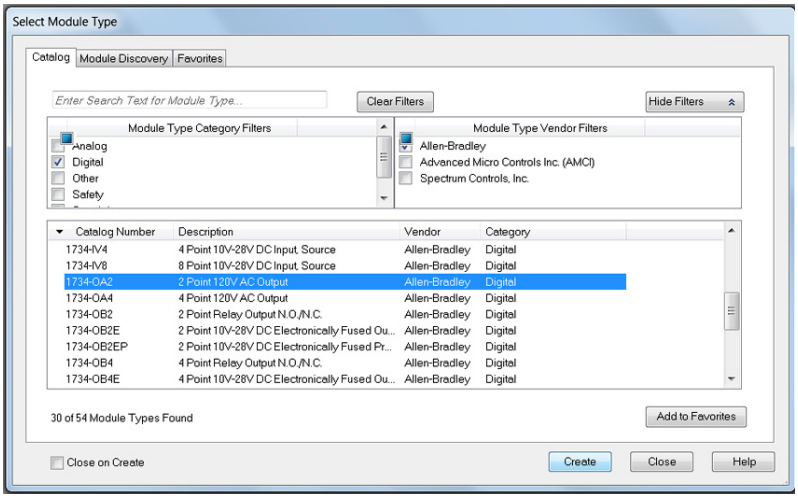
3. Configure o novo adaptador Ethernet como necessário e clique em OK.



4. No Organizador do Controlador, clique com o botão direito na pasta Tarefas e escolha Nova Tarefa.

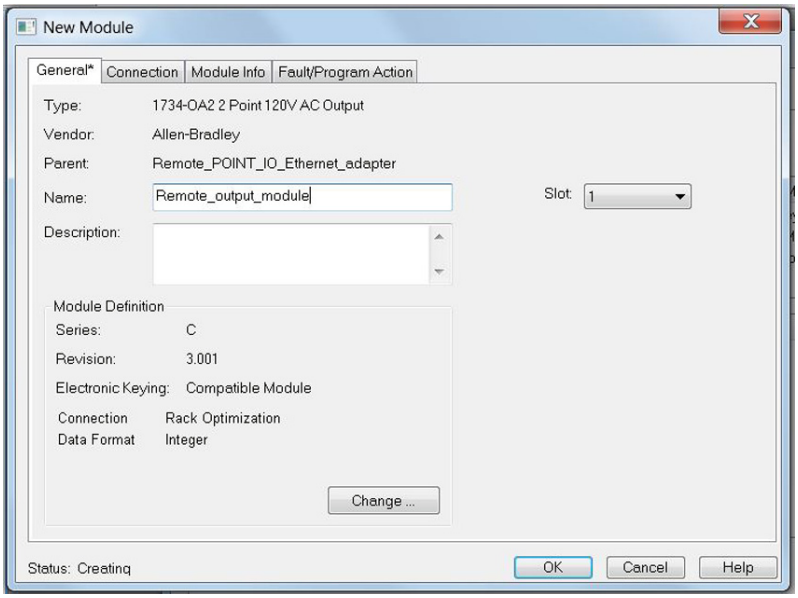


5. Selecione o módulo de E/S desejado e clique em Criar.



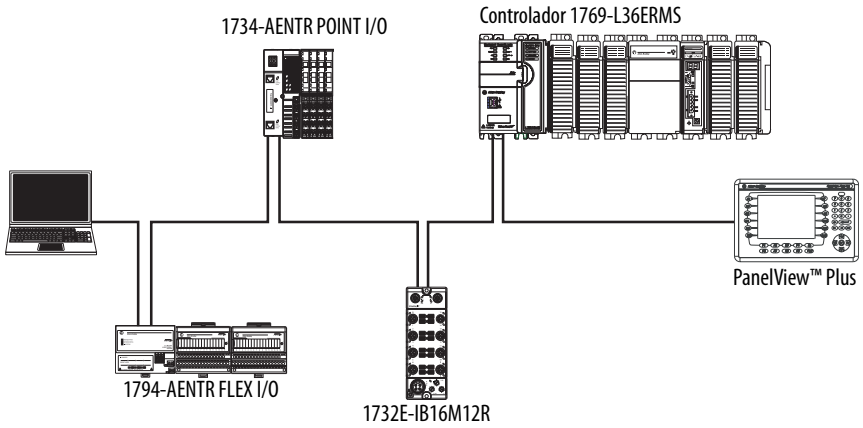
A caixa de diálogo Novo Módulo aparecerá.

6. Configure o novo módulo de E/S como necessário e clique em OK.



7. Repita estas etapas para adicionar todos os módulos desejados de E/S distribuída.

O gráfico a seguir é um exemplo de um sistema de controle 1769-L36ERMS que usa módulos de E/S distribuída por meio de uma rede EtherNet/IP.



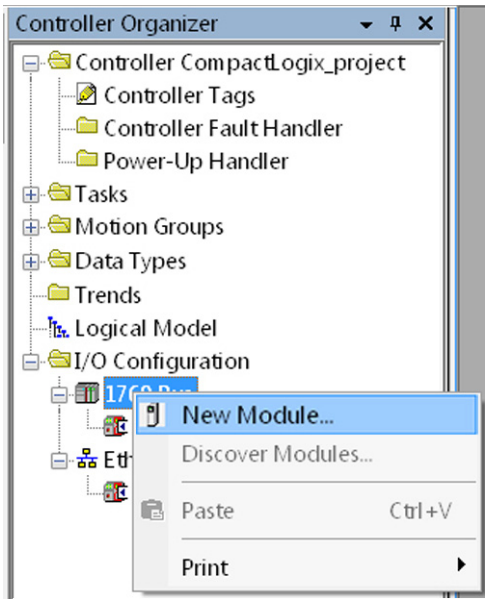
Configure Módulos de E/S Distribuída por uma Rede DeviceNet

O seu sistema de controle CompactLogix 5370 pode usar módulos de E/S distribuído por meio de uma rede DeviceNet.

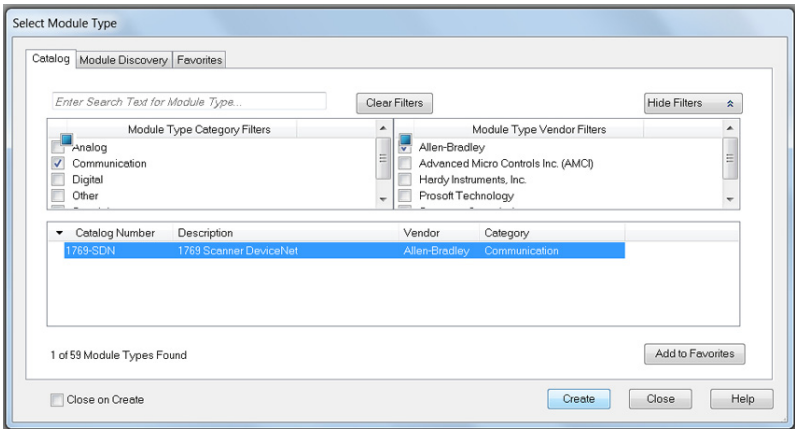
Complete estas etapas para configurar módulos de E/S distribuídos por meio de uma rede DeviceNet.

1. Se você não tiver feito isso ainda, instale um módulo scanner DeviceNet Compact I/O 1769-SDN no banco local do seu sistema de controle CompactLogix 5370.

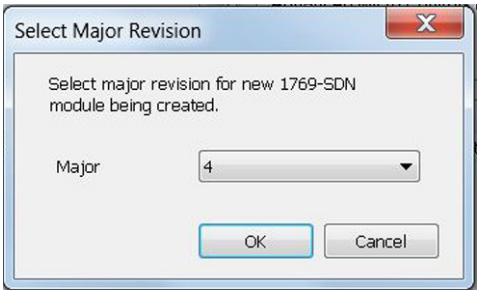
2. No Organizador do Controlador, selecione e clique com o botão direito no barramento 1769-AENT em Configuração de E/S, e então escolha Novo Módulo.



3. Selecione o módulo scanner 1769-SDN e clique em Criar.

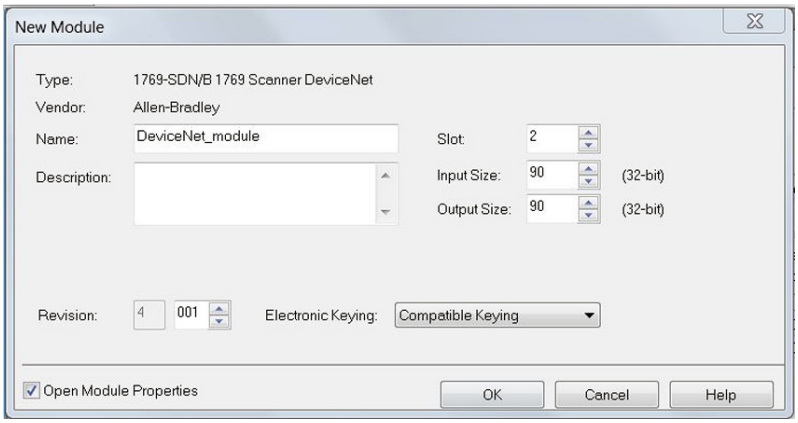


4. Escolha uma Revisão Principal e clique em OK.



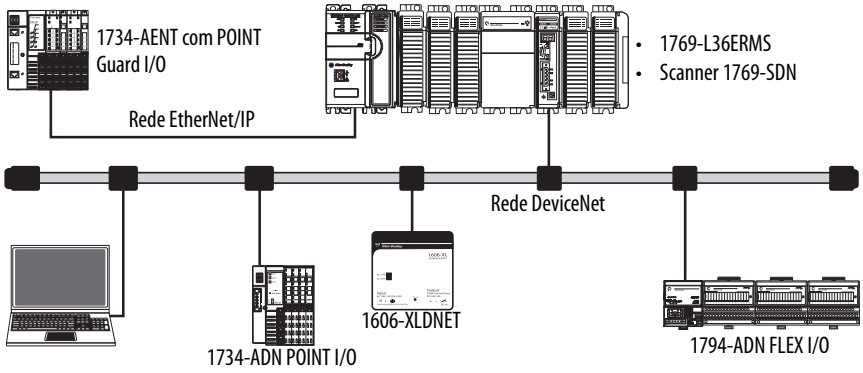
A caixa de diálogo Novo Módulo aparecerá.

5. Configure o novo scanner 1769-SDN como necessário e clique em OK.



6. Use software RSNetWorx™ para DeviceNet para definir a lista de varredura no módulo scanner 1769-SDN para comunicar dados entre os equipamentos e o controlador, por meio do módulo scanner.

O gráfico a seguir é um exemplo de sistema de controle 1769-L36ERMS que usa módulos de E/S distribuída padrão em uma rede DeviceNet.

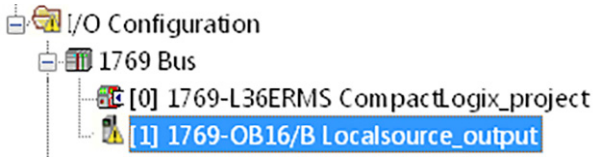


Monitorar os módulos de E/S padrão

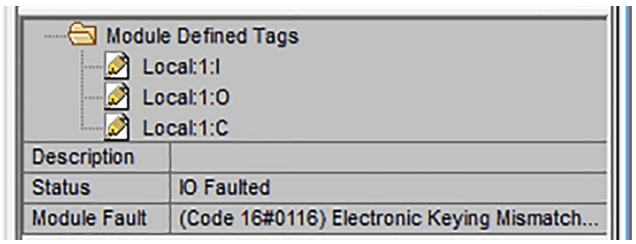
Com controladores CompactLogix 5370, você pode monitorar módulos de E/S dos seguintes modos:

- Painel de Visualização Rápida (QuickView™ Pane) no organizador do controlador
- Guia Conexão na caixa de diálogo Propriedades do Módulo
- Programando a lógica para monitorar dados de falha para que você possa tomar as ações apropriadas

Quando uma falha ocorre em um módulo de E/S, um triângulo amarelo na aparência do módulo no organizador do controlador alerta a falha.

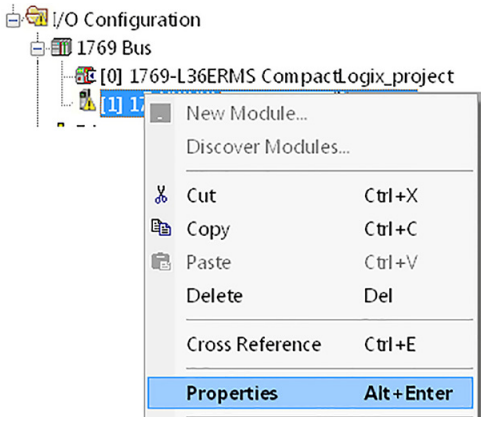


O seguinte gráfico mostra o painel de visualização rápida, que indica o tipo de falha.



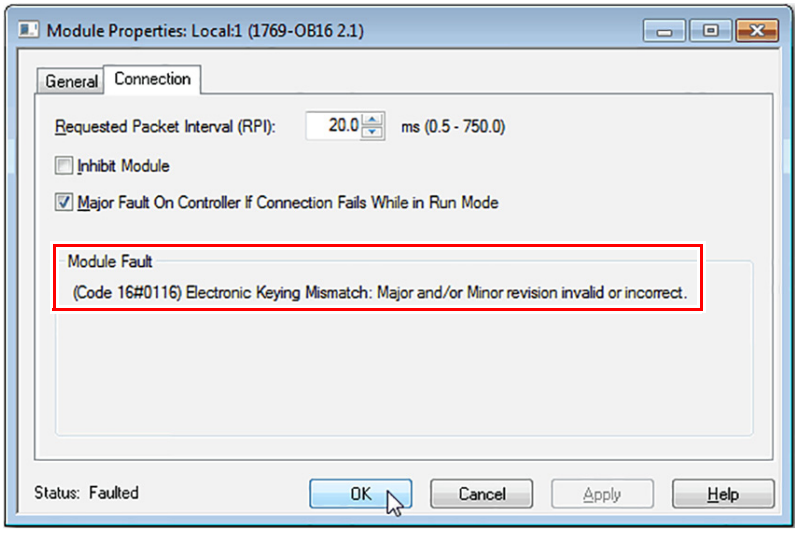
Para visualizar a descrição da falha na guia Conexão na caixa de diálogo Propriedades do Módulo, siga esses passos.

1. No Organizador do Controlador, selecione e clique com o botão direito no módulo em falha em Configuração de E/S, e então escolha propriedades.



2. Na caixa de diálogo Propriedades do Módulo, selecione a guia Conexão.

   Na seção Falha no módulo, use a descrição da falha para diagnosticar o problema.



3. Clique em OK para fechar a caixa de diálogo e corrigir o problema.

Detecção de terminação e falhas de módulo

Detecção de terminação é realizada por meio do último módulo em um Barramento 1769. Se esse módulo experienciar uma falha que o impeça de comunicar-se com o Barramento 1769, os eventos a seguir ocorrem:

- Detecção de terminação falha
- Falhas do controlador

Adição, configuração, monitoração e substituição de dispositivos de E/S de segurança CIP

Adicionar dispositivos de E/S de segurança

Quando você adicionar um dispositivo de E/S de segurança para o sistema, você deve definir a configuração para o dispositivo, inclusive o seguinte:

- Endereço de IP para redes EtherNet/IP

  Para ajustar o endereço IP, você pode ajustar as chaves rotativas no dispositivo; usar o software DHCP (disponível na Rockwell Automation); usar a aplicação do Logix Designer; ou recuperar o endereço padrão da memória não volátil.
- Número da rede de segurança (SNN); consulte página 106 para informações sobre a configuração do SNN
- Assinatura de configuração; consulte página 110 para obter informações sobre quando a assinatura de configuração é definida automaticamente e quando é necessário defini-la
- Limite do tempo de reação; consulte página 107 para informações sobre configuração do limite do tempo de reação
- Parâmetros de teste, e entrada e saída de segurança completam a configuração do módulo

Você pode configurar dispositivos de E/S de segurança através do controlador Compact GuardLogix® usando o aplicativo Logix Designer.

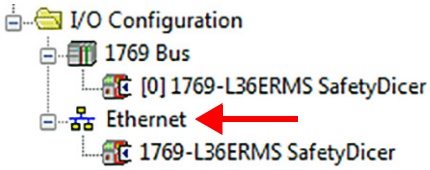
DICA Os dispositivos de E/S de segurança são compatíveis com os dados padrão e de segurança. A configuração do dispositivo define quais dados estão disponíveis.

Configurar dispositivos de E/S de segurança

Adicione o dispositivo de E/S de segurança ao módulo de comunicação na pasta Configuração de E/S do projeto do controlador.

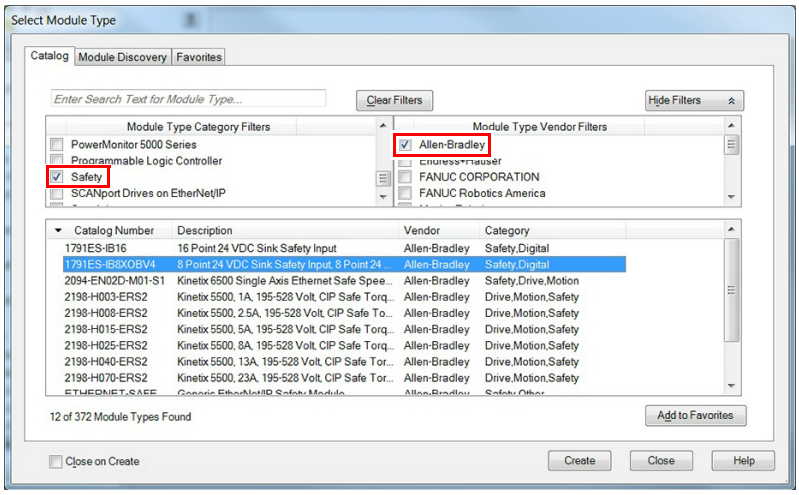
DICA Não é possível adicionar ou excluir um dispositivo de E/S de segurança enquanto online.

1. Clique com o botão direito na rede Ethernet e selecione Novo módulo.

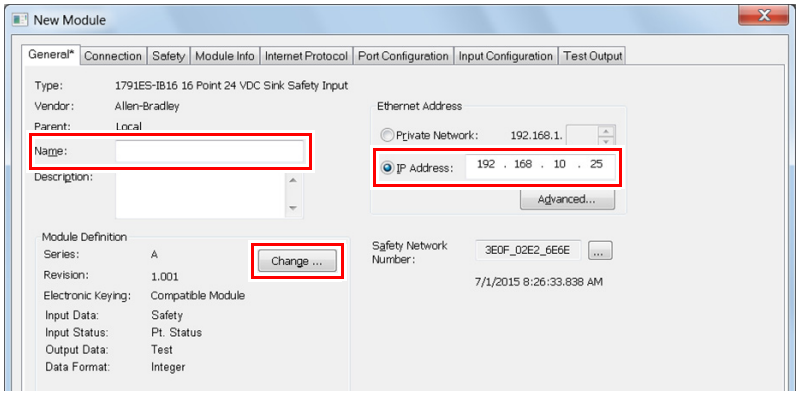


2. Na guia de catálogo, selecione o dispositivo de E/S de segurança.

DICA Use os filtros para reduzir a lista de módulos para escolher.



3. Clique em criar.
4. Digite um nome para o novo dispositivo.
5. Para modificar as configurações de definição de módulo, clique em alterar (se necessário).
6. Introduza o endereço de IP para redes EtherNet/IP.



Se sua rede usa a conversão de endereço de rede (NAT), consulte Configure o endereço IP por meio da conversão de endereços de rede (NAT) na página 105.

7. Para modificar o número de rede de segurança, clique no botão ... (se necessário).

   Consulte página 106 para obter detalhes.

8. Para definir o Limite do tempo de reação de conexão, acesse a guia Segurança.

   Consulte página 107 para obter detalhes.

9. Para concluir a configuração do dispositivo de E/S de segurança, consulte a ajuda online da aplicação do Logix Designer e a sua documentação do usuário.

Configure o endereço IP por meio da conversão de endereços de rede (NAT)

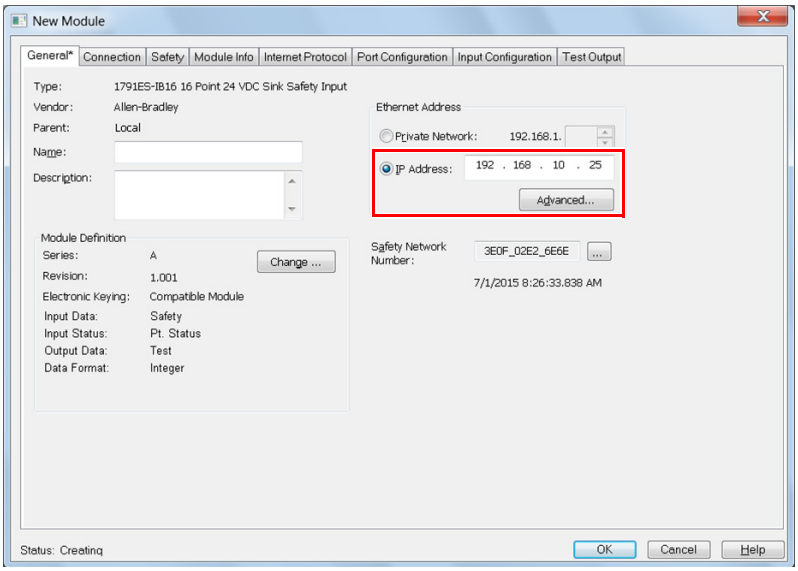
NAT converte um endereço IP para outro endereço IP através de um comutador ou um roteador NAT configurado. O comutador ou roteador converte os endereços de fonte e destino dentro de pacotes de dados à medida que o tráfego passa entre sub-redes.

Este serviço é útil se você precisa reutilizar os endereços IP ao longo de uma rede. Por exemplo, NAT torna possível para os dispositivos serem segmentados em várias sub-redes particulares idênticas mantendo identidades únicas na sub-rede pública.

Se você está usando NAT, siga estas etapas para ajustar o endereço IP.

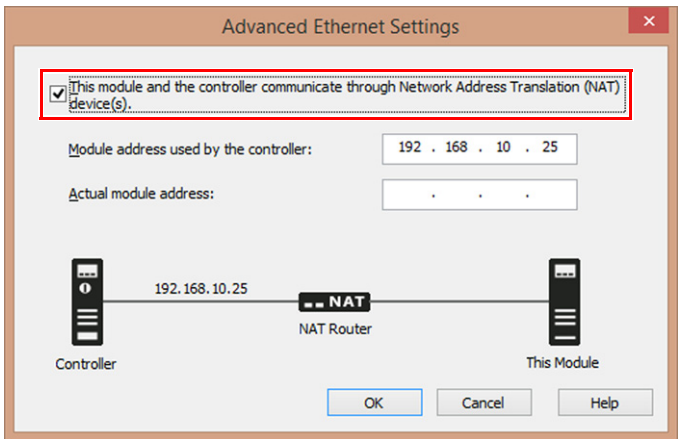
1. No campo endereço IP, digite o endereço IP que o controlador usará.

   Esse geralmente é o endereço IP na rede pública quando usando NAT.



2. Clique em avançado para abrir a caixa de diálogo Configurações avançadas de Ethernet.

3. Marque a caixa de seleção para indicar que este módulo e o controlador comunicam através de dispositivos NAT.



4. Digite o endereço do módulo real.

DICA Se você tiver configurado o endereço IP usando as chaves rotativas, esse é o endereço que é definido no dispositivo. Como alternativa, o endereço do módulo real é o mesmo endereço mostrado na guia de protocolo de Internet do dispositivo.

5. Clique em OK.

O controlador usa o endereço convertido, mas protocolo de segurança CIP exige o endereço real do dispositivo.

Definir o número da rede de segurança (SNN)

A atribuição de um SNN é automática quando novos dispositivos de E/S de segurança são adicionados. As adições subsequentes do dispositivo de segurança à mesma rede são atribuídas ao mesmo SNN definido no endereço mais inferior da rede CIP Safety.

Na maioria das aplicações, o SNN automático baseado na hora é suficiente. Porém, há casos nos quais é necessária a manipulação de um SNN.

Consulte Atribuição do número da rede de segurança (SNN) na página 65.

Conexões Unicast em redes EtherNet/IP

As conexões Unicast são conexões ponto a ponto entre uma fonte e um nó de destino. Não é preciso inserir uma faixa RPI mínima ou máxima ou valor-padrão para este tipo de conexão.

Para configurar as conexões unicast, escolha a guia Conexão e selecione Use Conexão Unicast sobre Ethernet/IP.

Definir o limite de tempo de reação de conexão

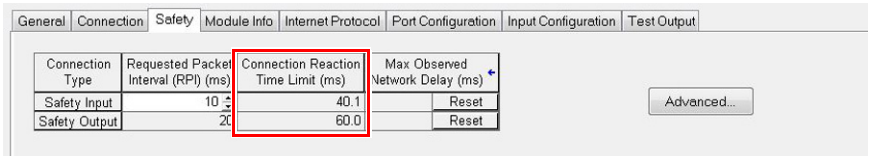
O limite de tempo de reação de conexão é a idade máxima dos pacotes de segurança na conexão associada. Se o período dos dados usado pelo dispositivo em consumo exceder o limite de tempo de reação da conexão, ocorrerá uma falha de conexão. Esse Limite é determinado pelas seguintes equações:

Limite de tempo de reação da conexão de entrada =
entrada RPI x [multiplicador de tempo limite + multiplicador de atraso da rede]

Limite de tempo de reação da conexão de entrada =
período de tarefa de segurança x [Multiplicador de tempo limite + Multiplicador de atraso da rede – 1]

O limite de tempo de reação de conexão é exibido na guia Segurança da caixa de diálogo Propriedades do Módulo.

Figura 16 – Limite do tempo de reação de conexão



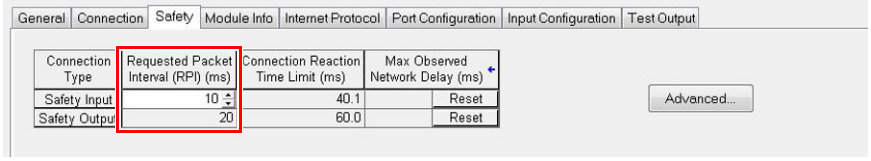
Especificar oIntervalo do pacote requisitado (RPI)

A RPI especifica o período que os dados são atualizados através de uma conexão. Por exemplo, um módulo de entrada produz dados no RPI atribuído.

Para conexões de entrada de segurança, é possível definir o RPI na guia Segurança da caixa de diálogo Propriedades do módulo. O RPI é inserido em incrementos de 1 ms, com um intervalo de 1 a 100 ms. O padrão é 10 ms.

O limite de tempo de reação da conexão é ajustado imediatamente quando o RPI é alterado por meio da aplicação Logix Designer.

Figura 17 – intervalo do pacote requisitado



Para conexões de saída de segurança, o RPI é fixado no período da tarefa de segurança. Se o limite de reação do tempo de conexão correspondente não for satisfatório, você pode ajustar o período da tarefa de segurança na caixa de diálogo Propriedades de tarefa de segurança.

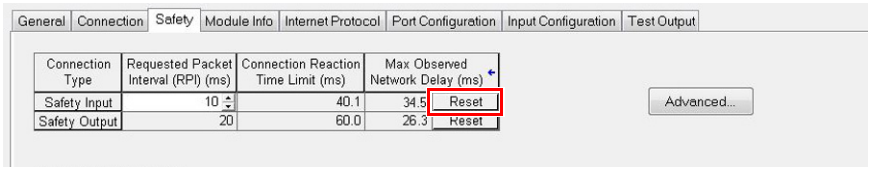
Consulte Especificação do período da tarefa de segurança na página 140 para obter mais informações sobre o período da tarefa de segurança.

Para aplicações normais, o RPI padrão é normalmente suficiente. Para requisitos mais complexos, use o botão Avançado para modificar os parâmetros do limite de tempo de reação de conexão, conforme descrito na página 108.

Ver o atraso máximo de rede observado

Quando o controlador Compact GuardLogix recebe um pacote de segurança, o software registra o atraso de rede máximo observado. Para entradas de segurança, o atraso máximo de rede observado mostra o atraso completo do módulo de entrada ao controlador e reconhece o módulo de entrada. Para saídas de segurança, ele mostra o atraso completo do controlador para o módulo de saída e o reconhecimento do controlador. O atraso máximo de rede observado é exibido na guia Safety da caixa de diálogo Module Propriedades. Quando online, clique em Reinicializar para reiniciar o atraso de rede máximo observado.

Figura 18 – Reiniciar o Atraso máximo de rede observado

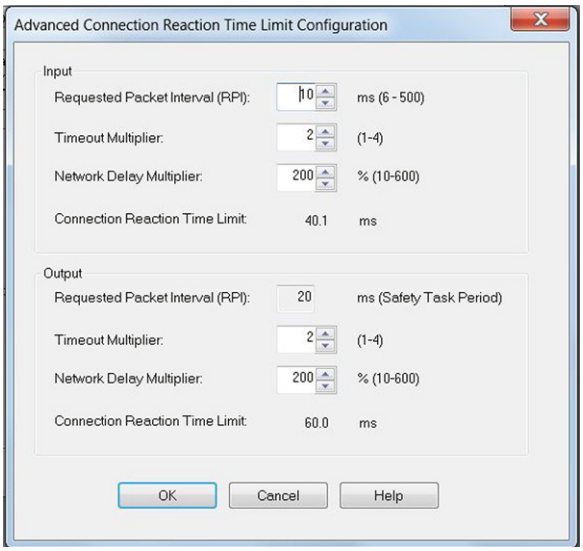


IMPORTANTE O atraso de rede máximo real do produtor para o consumidor é inferior ao valor exibido no campo atraso de rede máximo na guia segurança. Em geral, o atraso real máximo da mensagem é aproximadamente metade do valor de atraso de rede máximo que é exibido.

Definir os parâmetros do limite de tempo de reação de conexão avançado

Configure os parâmetros de conexão como o multiplicador de tempo-limite e multiplicador de atraso de rede na caixa de diálogo Limite do tempo de reação de conexão avançado.

Figura 19 – Configuração avançada



Multiplicador de tempo-limite

O campo Multiplicador de Tempo Limite determina o número de RPIs a aguardar por um pacote antes de declarar o tempo-limite de conexão. Isto é traduzido no número de mensagens perdidas antes da confirmação de um erro de conexão.

Por exemplo, o multiplicador de tempo-limite 1 indica que as mensagens precisam ser recebidas durante cada intervalo RPI. O Multiplicador de Tempo-limite 2 indica que uma mensagem pode ser perdida contanto que, pelo menos, uma seja recebida em duas vezes no RPI (2 x RPI).

Multiplicador de atraso de rede

O campo Multiplicador de atraso de rede define o tempo de transporte da mensagem imposto pelo protocolo de segurança CIP. Esse multiplicador especifica o atraso do desarme completo do produtor ao consumidor e o conhecimento de volta ao produtor. Você pode usar o Multiplicador de atraso de rede para reduzir ou aumentar o Limite do tempo de reação de conexão em casos onde o tempo de transporte de mensagens reforçadas é significantemente menor ou maior que o RPI. Por exemplo, ajustar o multiplicador de atraso de rede pode ser útil quando o RPI de uma conexão de saída é o mesmo que o de um período da tarefa de segurança

Quando os RPIs de entrada ou de saída forem relativamente lentos ou rápidos se comparados ao tempo de atraso da mensagem imposto, o multiplicador de atraso de rede pode ser aproximado por meio de um dos dois métodos.

Método 1: Use a razão entre o RPI de entrada e o período da tarefa de segurança. Utilize este método somente quando todas as seguintes condições se aplicarem:

- se o caminho ou atraso for quase igual ao caminho ou atraso de saída.
- o RPI de entrada for configurado de forma que o tempo de transporte da mensagem de entrada real seja inferior ao RPI de entrada.
- o período da tarefa de segurança for lento em relação ao RPI de entrada.

  Nessas condições, o Multiplicador de Atraso da Rede de Saída pode ser estimado da seguinte forma:

  Multiplicador de atraso da rede de entrada x [entrada RPI ÷ período da tarefa de segurança]

EXEMPLO	**Cálculo aproximado do multiplicador de atraso da rede de saída**
	Se: Entrada RPI = 10 ms Multiplicador de atraso da rede de entrada = 200% Período da tarefa de segurança = 20 ms Portanto, o multiplicador de atraso da rede de saída será igual: 200% x [10 ÷ 20] = 100%

Método 2: Use o atraso máximo de rede observado. Se o sistema for executado por muito tempo em condições problemáticas de carregamento, o campo Multiplicador de atraso de rede poderá ser definido de acordo com Atraso Máximo Observado na Rede. Este método pode ser usado em uma conexão de entrada ou saída. Após o sistema ser executado por muito tempo em condições adversas de carregamento, registre o Atraso Máximo Observado na Rede.

O campo Multiplicador de atraso de rede pode apresentar um valor aproximado de acordo com a seguinte equação:

[Atraso máximo de rede observado + Margin_Factor] ÷ RPI

EXEMPLO **Calcule o multiplicador de atraso máximo de rede observado a partir do atraso de rede observado**

Se:
RPI = 50 ms
Atraso máximo observado na rede = 20 ms
Margin_Factor = 10

Portanto, multiplicador de atraso da rede será igual a:
[20 + 10] ÷ 50 = 60%

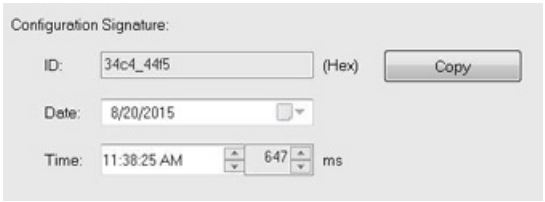
Entender a assinatura de configuração

Cada dispositivo de segurança tem uma assinatura de configuração única que define a configuração do módulo. A assinatura de configuração é composta de um número de ID, data e hora e é utilizada para verificar a configuração do módulo.

Configuração por meio da aplicação Logix Designer

Quando o módulo de E/S é configurado por meio da aplicação Logix Designer, a assinatura de configuração é gerada automaticamente. É possível visualizar e copiar a assinatura de configuração na aba de Segurança na caixa de diálogo Propriedades do módulo.

Figura 20 – Visualize e copie a assinatura de configuração



Proprietário de configuração diferente (conexão em modo de escuta)

Quando a configuração do dispositivo de E/S é propriedade de outro controlador, é necessário copiar a assinatura de configuração do módulo do projeto do seu proprietário e colá-la na guia Segurança da caixa de diálogo Propriedades do Módulo.

DICA Se o dispositivo é configurado para entradas apenas, é possível copiar e colar a assinatura de configuração. Se o dispositivo tiver saídas de segurança, elas são controladas pelo controlador que possui a configuração e a caixa de texto da assinatura de configuração não está disponível.

Reinicializar a propriedade do dispositivo de E/S de segurança

Quando o projeto do controlador está online, a guia Segurança da caixa de diálogo Propriedades do Módulo exibe a atual propriedade de configuração. Quando a configuração pertence ao projeto aberto, Local é exibido. Quando a configuração pertence a um segundo dispositivo, Remoto é exibido, com o número da rede de segurança (SNN) e o endereço de nó ou o número de slot do controlador da configuração. A mensagem de erro de comunicação é exibida quando a leitura do dispositivo falha.

Quando estiver on-line, clique em Reinicializar propriedade para reiniciar o dispositivo na sua configuração original.

DICA Não é possível reinicializar a propriedade quando houver edições pendentes nas propriedades do módulo, quando houver uma assinatura de tarefa de segurança ou quando estiver com bloqueio de segurança.

Endereço de dados de E/S de segurança

Quando você adiciona um dispositivo à pasta de configuração de E/S, a aplicação Logix Designer cria automaticamente tags de escopo do controlador para o dispositivo.

As informações de E/S são apresentadas como um conjunto de tags. Cada tag utiliza uma estrutura de dados, de acordo com o tipo e as funções do dispositivo de E/S. O nome de uma tag é baseado no nome do dispositivo no sistema.

Formato do endereço dos módulos de E/S de segurança

Um módulo de E/S de segurança este exemplo

EXEMPLO Modulename:Type.Member

Tabela 15 – Formato de endereço de dispositivo de E/S de segurança

Onde	É	
Modulename	O nome do dispositivo de E/S de segurança	
Tipo	Tipo de dados	Entrada: E Saída: S
Membro	Dados específicos do dispositivo de E/S	
	Módulo somente de Entrada	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members
	Módulo somente de Saída	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:O.Output Members
	Combinação de E/S	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members Modulename:O.Output Members

Formato de endereço de unidade Kinetix 5500, Kinetix 5700 e PowerFlex 527

Um endereço de unidade Kinetix® 5500, Kinetix 5700, e PowerFlex® 527 segue este exemplo.

EXEMPLO	DriveName:Type.member

Tabela 16 – Formato de endereço de dispositivo de E/S de segurança de inversor

Onde	**É**	
DriveName	O nome da unidade Kinetix ou PowerFlex	
Tipo	Tipo de dados.	Entrada: SI Saída: SO
Membro	Dados específicos do dispositivo de E/S	
	Módulo somente de Entrada	Drivename:SI.ConnectionStatus Drivename:SI.RunMode Drivename:SI.ConnectionFaulted Drivename:SI.Status Drivename:SI.TorqueDisabled Drivename:SI.SafetyFault Drivename:SI.ResetRequired
	Módulo somente de Saída	Drivename:SO.Command Drivename:SO.SafeTorqueOff Drivename:SO.Reset

Tabela 17 – Mais recursos

Recurso	**Descrição**
Capítulo 9, Desenvolver aplicações de segurança	Contém informações sobre como monitorar dados de tags de segurança
Manual dos controladores de E/S Logix5000 e de Programação de Dados de Tag, publicação 1756-PM004	Fornece informações sobre o endereçamento de dispositivos de E/S padrão

Monitorar o status do dispositivo de E/S de segurança

É possível monitorar o status do dispositivo de E/S de segurança por mensagem explícita ou por indicadores de status nos dispositivos de E/S.

Estas publicações fornecem informações sobre localização de falhas no módulo de E/S:

- Manual do usuário dos módulos de segurança Guard I/O™ EtherNet/IP, publicação 1791ES-UM001
- Manual do usuário e de instalação dos módulos de segurança POINT Guard I/O™, publicação 1734-UM013
- Manual do usuário dos servo-drives Kinetix 5500, publicação 2198-UM001
- Manual do usuário dos servo-drives Kinetix 5700, publicação 2198-UM002
- Manual do usuário da unidade CA de frequência ajustável PowerFlex 527, Publicação 520-UM002

Reinicializar o dispositivo de E/S de segurança para sua condição original

Se um módulo Guard I/O foi usado anteriormente, exclua a configuração existente antes de instalá-lo em uma rede de segurança reiniciando o módulo para a sua condição "original".

Quando o projeto do controlador está online, a guia Segurança da caixa de diálogo Propriedades do Módulo exibe a propriedade de configuração atual. Quando a configuração pertence ao projeto aberto, Local é exibido. Quando a configuração pertence a um segundo dispositivo, Remoto é exibido, com o número da rede de segurança (SNN) e o endereço de nó ou o número de slot do controlador da configuração. A mensagem de erro de comunicação é exibida quando a leitura do módulo falha.

Se a conexão for local, deve-se inibir a conexão do módulo antes de reiniciar a propriedade. Siga estes passos para inibir o dispositivo.

1. No organizador do controlador, clique com o botão direito do mouse no controlador e escolha Propriedades.
2. Clique na guia Conexão.
3. Marque Inibir conexão.
4. Clique em Aplicar e então OK.

Siga estas etapas para reiniciar o módulo até a sua configuração original quando estiver on-line.

1. No organizador do controlador, clique com o botão direito do mouse no controlador e escolha Propriedades.
2. Clique na guia Segurança.
3. Clique em Reinicializar Propriedade.

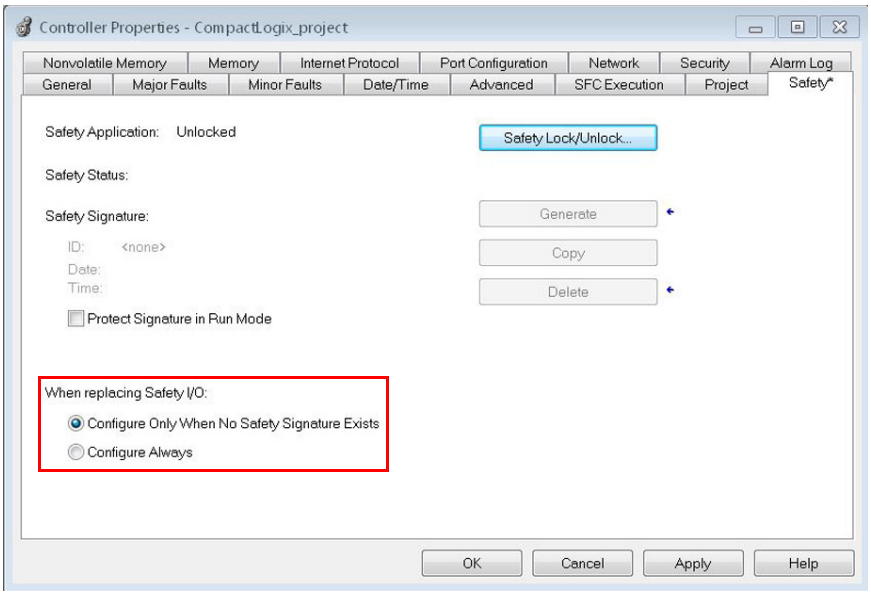
Substituir um dispositivo de E/S de segurança

Pode-se usar a aplicação Logix Designer para substituir um dispositivo Guard I/O em uma rede Ethernet. Se você estiver considerando uma parte do sistema de segurança CIP para manter o comportamento SIL 3 durante a substituição e o teste funcional de um dispositivo, a função Configurar Sempre não pode ser usada. Vá para Substituição com "Configurar somente quando não existir assinatura de segurança" habilitada na página 114.

Se o sistema de controle CIP Safety inteiro roteável não precisar manter o SIL 3/PLe durante a substituição e o teste de funcionamento de um módulo, a função Configurar Sempre poderá ser usada. Vá para Substituição com "Configurar Sempre" habilitada na página 118.

A substituição do dispositivo de segurança de E/S é configurada na Guia de segurança do controlador Compact GuardLogix.

Figura 21 – Substituição de dispositivo de E/S de segurança



Substituição com "Configurar somente quando não existir assinatura de segurança" habilitada

Quando um dispositivo de E/S de segurança é substituído, é feito o download da configuração a partir do controlador de segurança se o DeviceID do dispositivo novo combina com os originais. O DeviceID é uma combinação do endereço IP/do nó e o Número de Rede de Segurança (SNN) e é atualizado sempre que o SNN for ajustado.

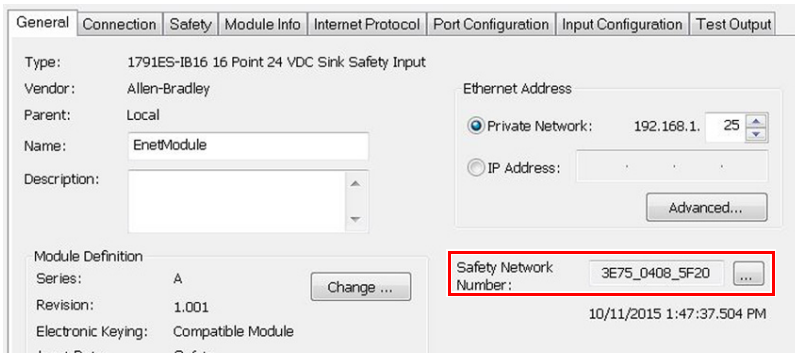
Se o projeto estiver configurado para 'configurar somente quando não existir assinatura de segurança', siga as etapas apropriadas em Tabela 18 para substituir um dispositivo de E/S de segurança com base em seu cenário. Uma vez que você completou as etapas corretamente, o DeviceID irá combinar com o original, habilitando o controlador de segurança para fazer download da configuração de dispositivo adequada e restabelecer a conexão de segurança.

Tabela 18 – Substituir um módulo

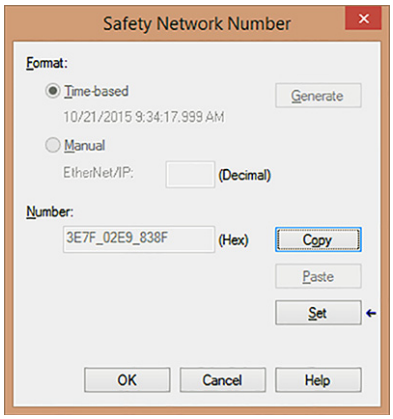
Existe assinatura de segurança Compact GuardLogix	Condição de substituição de módulo	Ação necessária
Não	Sem SNN (fora da caixa)	Nenhuma O dispositivo está pronto para o uso.
Sim ou não	O mesmo SNN conforme a configuração de tarefa de segurança original	Nenhuma O dispositivo está pronto para o uso.
Sim	Sem SNN (fora da caixa)	Consulte Situação 1 – O dispositivo de substituição está Original e a assinatura de segurança existe na página 115.
Sim	SNN diferente da configuração de tarefa de segurança original	Consulte Situação 2 – O SNN do dispositivo de substituição é diferente do original e a assinatura de segurança existe na página 116.
Não		Consulte Situação 3 – O SNN do dispositivo de substituição é diferente do original e a assinatura de segurança não existe na página 118.

Situação 1 – O dispositivo de substituição está Original e a assinatura de segurança existe

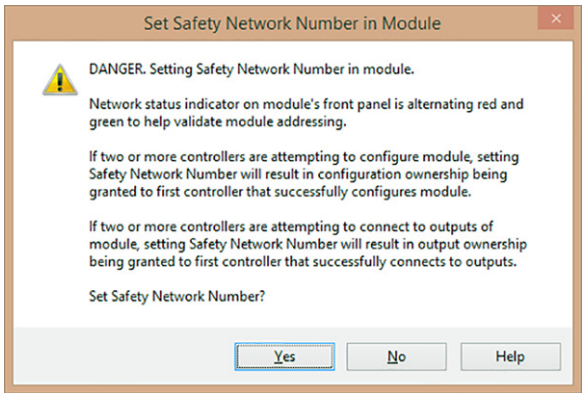
1. Remoção do dispositivo de E/S antigo e instalação de um novo dispositivo.
2. Clique com o botão direito no dispositivo de E/S de segurança de substituição e escolha Propriedades.
3. Clique em ... à direita do número da rede de segurança para abrir a caixa de diálogo Número da rede de segurança.



4. Clique em Configurar.



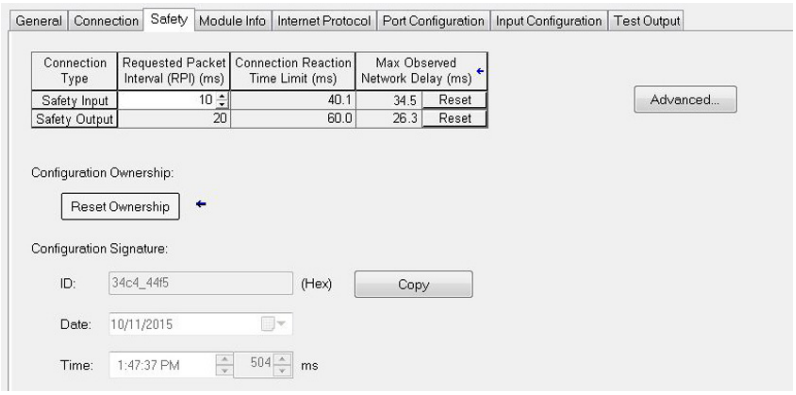
5. Verifique que o indicador de status de rede (NS) esteja alternando vermelho/verde no dispositivo correto antes de clicar em Sim na caixa de diálogo de confirmação para ajustar o SNN e aceitar o dispositivo de substituição.



6. Siga os procedimentos descritos pela empresa para testar a funcionalidade do dispositivo e sistema de E/S substituído e autorizar o sistema para uso.

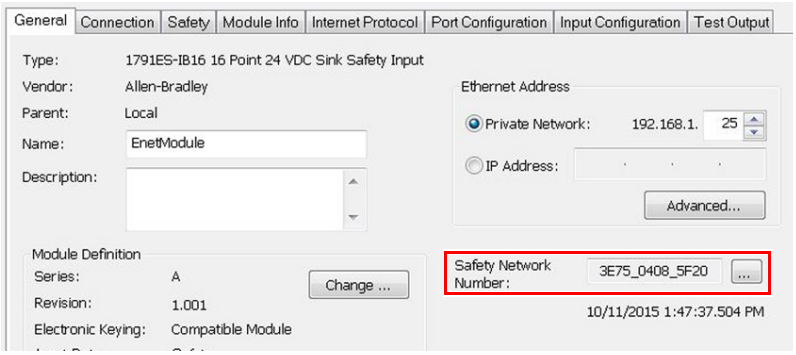
Situação 2 – O SNN do dispositivo de substituição é diferente do original e a assinatura de segurança existe

1. Remoção do dispositivo de E/S antigo e instalação de um novo dispositivo.
2. Clique com o botão direito em seu dispositivo de E/S de segurança e escolha Propriedades.
3. Clique na guia Segurança.

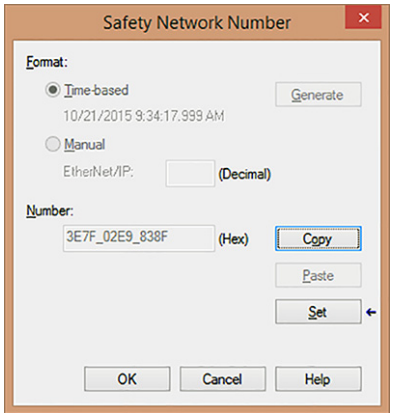


4. Clique em Reinicializar Propriedade.
5. Clique em OK.
6. Com o botão direito no dispositivo e escolha Propriedades.

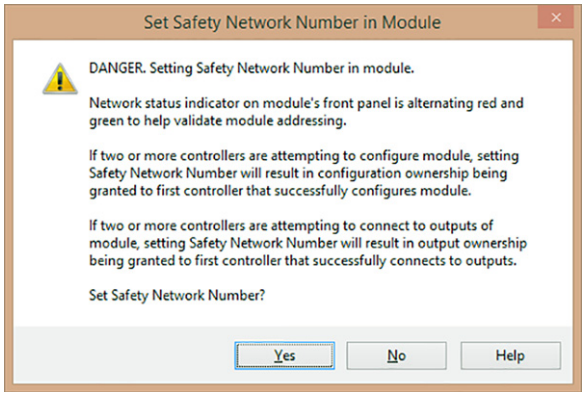
7. Clique em ... à direita do número da rede de segurança para abrir a caixa de diálogo Número da rede de segurança.



8. Clique em Set.



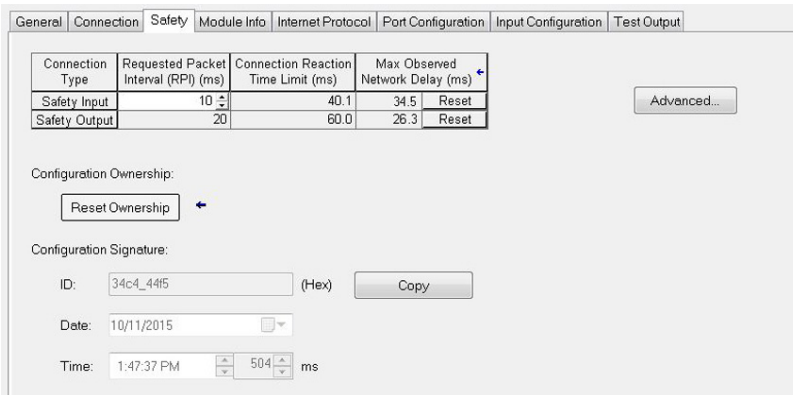
9. Verifique que o indicador de status de rede (NS) está alternando vermelho/verde no dispositivo correto antes de clicar em Sim na caixa de diálogo de confirmação para ajustar o SNN e aceitar o dispositivo de substituição.



10. Siga os procedimentos descritos pela empresa para testar a funcionalidade do dispositivo e sistema de E/S substituído e autorizar o sistema para uso.

Situação 3 – O SNN do dispositivo de substituição é diferente do original e a assinatura de segurança não existe

1. Remoção do dispositivo de E/S antigo e instalação de um novo dispositivo.
2. Clique com o botão direito em seu dispositivo de E/S de segurança e escolha Propriedades.
3. Clique na guia Segurança.



4. Clique em Reinicializar Propriedade.
5. Clique em OK.
6. Siga os procedimentos descritos pela empresa para testar a funcionalidade do dispositivo e sistema de E/S substituído e autorizar o sistema para uso.

Substituição com "Configurar Sempre" habilitada

ATENÇÃO: Habilite a funcionalidade 'Configurar Sempre' somente se o sistema de controle de segurança CIP inteiro roteável **não** precisar manter o comportamento SIL 3 durante a substituição e o teste de funcionamento de um dispositivo.

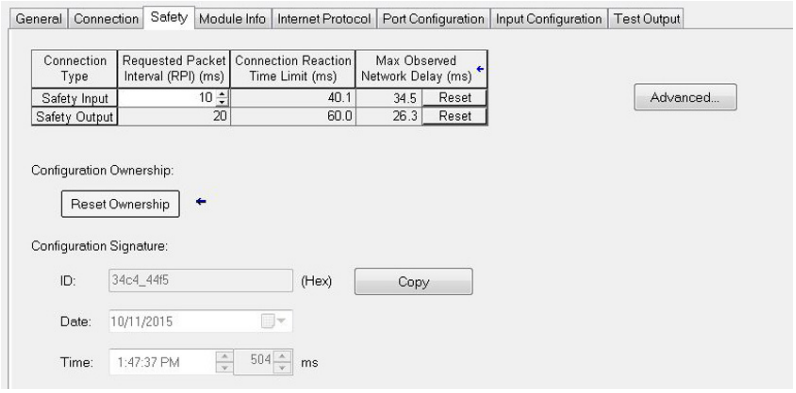
Não coloque módulos que estiverem na condição pronto para uso em uma rede de segurança CIP quando a função Configurar Sempre estiver habilitada, exceto ao seguir esse procedimento de substituição.

Quando a função "Configurar Sempre" estiver habilitada no projeto do controlador, o controlador verificará automaticamente e se conectará a um dispositivo de substituição que atenda a todas as especificações a seguir:

- O controlador tem dados de configuração de um dispositivo compatível no endereço de rede.
- O dispositivo está na condição pronto para uso ou tem um SNN que combina com a configuração.

Se o projeto for configurado para “Configurar Sempre”, siga as etapas apropriadas para substituir um dispositivo de E/S de segurança.

1. Remoção do dispositivo de E/S antigo e instalação de um novo dispositivo.
   a. Se o dispositivo estiver na condição original, vá para a etapa 6. Nenhuma ação é necessária para que o controlador Compact GuardLogix tome a propriedade do dispositivo.
   b. Se um erro de combinação SNN ocorrer, vá para a próxima etapa para reiniciar o módulo para a condição pronto para uso.
2. Clique com o botão direito em seu dispositivo de E/S de segurança e escolha Propriedades.
3. Clique na guia Segurança.



4. Clique em Reinicializar Propriedade.
5. Clique em OK.
6. Siga os procedimentos descritos pela empresa para testar funcionalmente o dispositivo e sistema de E/S substituído e autorizar o sistema para uso.

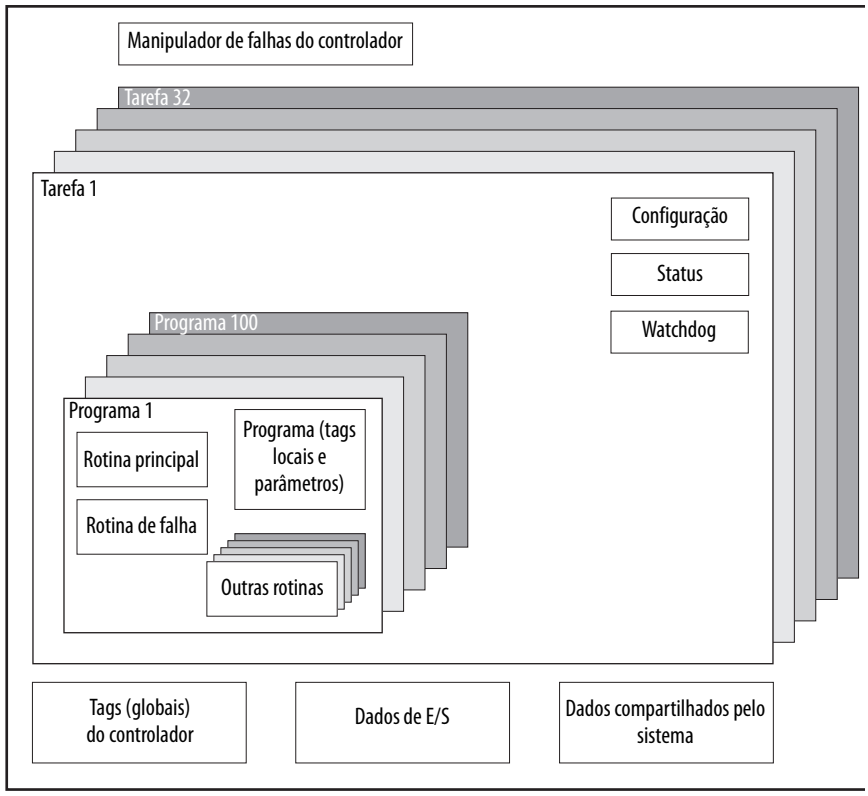
Observações:

Elementos de uma aplicação de controle

Uma aplicação de controle consiste em vários elementos que exigem planejamento para execução eficiente da aplicação. Elementos de aplicação incluem o seguinte:

- Tarefas
- Programas
- Rotinas
- Parâmetros e tags locais

Figura 22 – Aplicação de controles



Tarefas

Um controlador Logix5000™ permite que você use várias tarefas para programar e priorizar a execução de seus programas com base em critérios. Estas multitarefas alocam o tempo de processamento do controlador entre as diferentes operações de sua aplicação:

- O controlador executa somente uma tarefa por vez.
- Uma tarefa pode interromper outra execução e assumir o controle.
- Em qualquer tarefa, múltiplos programas podem ser usados. Entretanto, somente um programa pode ser executado por vez.
- Você pode exibir tarefas nas visualizações do controlador ou do organizador lógico, conforme a necessidade.

Figura 23 – Tarefa em uma aplicação de controle

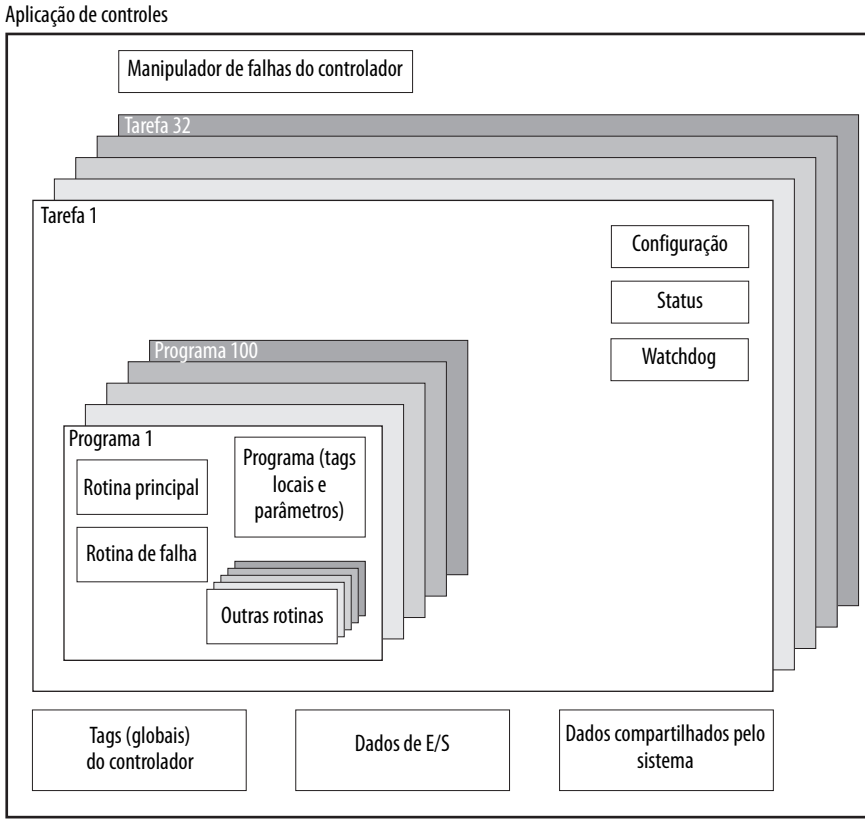
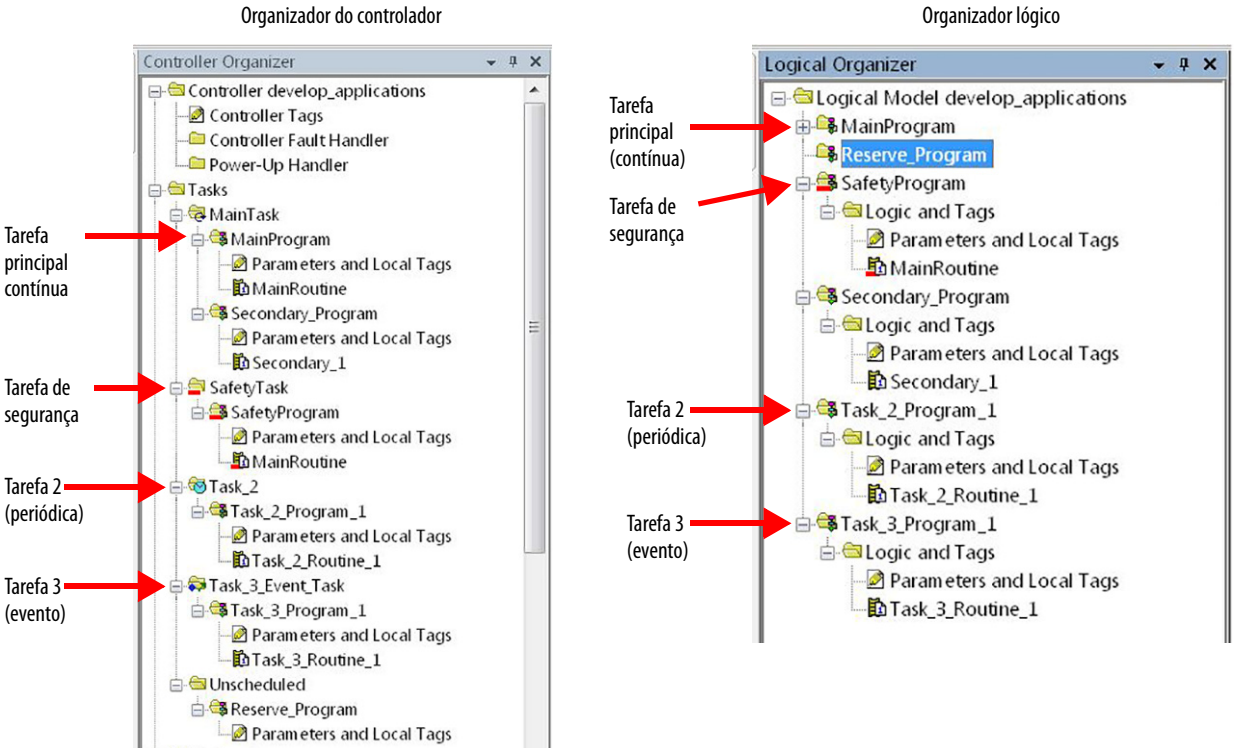
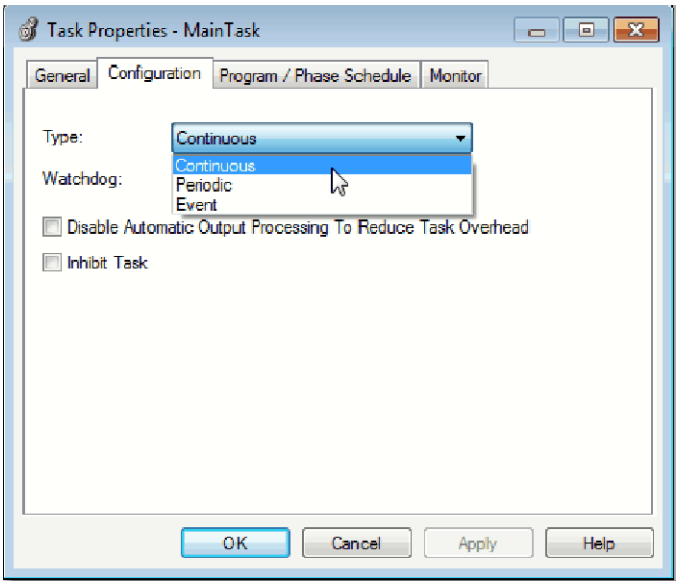


Figura 24 – Tarefas em aplicação



Uma tarefa proporciona agendamento e informações de prioridade para um conjunto de um ou mais programas. Configurar tarefas como contínuas, periódica, ou evento utilizando a caixa de diálogo Propriedades da Tarefa.

Figura 25 – Configuração do tipo de tarefa



Esta tabela explica os tipos de tarefas que você pode configurar.

Tabela 19 – Tipos de tarefa e frequência de execução

Tipo de tarefa	Execução da tarefa	Descrição
Contínuo	Sempre	A tarefa contínua opera no plano de fundo. Qualquer tempo da CPU não alocado para outras operações (como movimento, comunicação e outras tarefas) é usado para executar os programas na tarefa contínua. • A tarefa contínua é executada constantemente. Quando a tarefa contínua completa uma varredura total, ela reinicia imediatamente. • Um projeto não precisa de uma tarefa contínua. Se usado, pode haver apenas uma tarefa contínua.
Periódica	• Em um intervalo estabelecido, por exemplo, a cada 100 ms • Tempos múltiplos na varredura da sua outra lógica	Uma tarefa periódica realiza uma função em um intervalo específico. • Sempre que o tempo da tarefa periódica expirar, a tarefa interrompe todas as tarefas de prioridade mais baixa, executa uma vez e devolve o controle de onde a tarefa anterior parou. • Você pode configurar o período de 0,1 a 2.000.000,00 ms. O padrão é 10 ms. Ele também depende da configuração e do controlador. • O desempenho de uma tarefa periódica depende do tipo do controlador Logix5000 e da lógica na tarefa. • A tarefa periódica processa os dados de E/S dos controladores CompactLogix, FlexLogix, DriveLogix e SoftLogix com as seguintes considerações: – Para controladores CompactLogix, FlexLogix e DriveLogix, opera na prioridade 6 – Para controladores SoftLogix, opera em Windows prioridade 16 (Inativo) – As tarefas de maior prioridade têm preferência sobre a tarefa de E/S e podem ter um impacto no processamento – Executa no RPI mais rápido que você programou para o sistema. – Executa o tempo que leva para varrer os módulos de E/S configurados.
Evento	Imediatamente quando um evento ocorre	Uma tarefa de evento realiza uma função apenas quando um evento (acionamento) ocorre. O disparo para a tarefa de evento pode ser o seguinte: • Um disparo de tag consumido • Uma instrução de EVENTO • Um disparo de eixo • Um disparo de evento de movimento • Mudança de Estado dos Dados de Entrada do Módulo

O controlador CompactLogix 5370 suporta até 32 tarefas, somente uma das quais pode ser contínua.

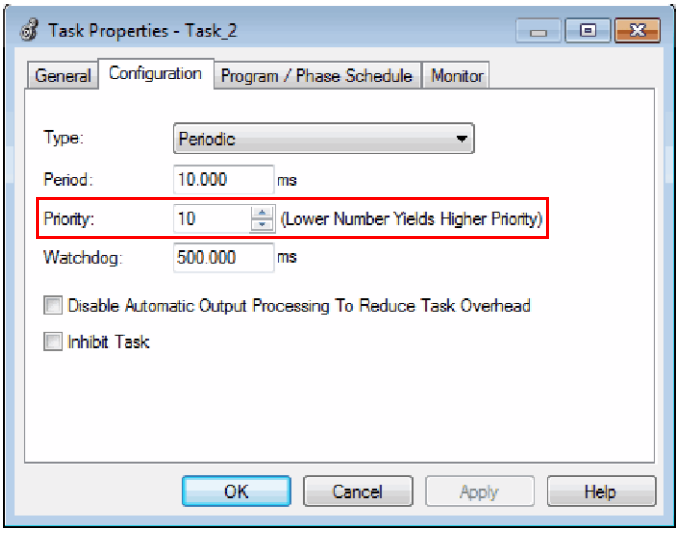
Uma tarefa pode ter até 100 Programas separados por tarefa, cada um com suas próprias rotinas executáveis e tags com escopo de programa. Uma vez que uma tarefa é acionada (ativada), todos os programas atribuídos à tarefa executam na sequência em que foram agrupados. As Tarefas Múltiplas não podem compartilhar Programas e Programas aparecem apenas uma vez no Organizador do controlador.

Prioridade de tarefa

Cada tarefa no controlador tem um nível de prioridade. O sistema operacional usa o nível de prioridade para determinar qual tarefa executar quando diversas tarefas são disparadas. Uma tarefa com prioridade mais alta interrompe qualquer uma com prioridade mais baixa. Uma tarefa de evento periódica interrompe uma tarefa contínua, que tem prioridade mais baixa.

É possível configurar tarefas periódicas para executar a partir da prioridade mais baixa de 15 até a prioridade mais alta de 1. Configure a prioridade de tarefas utilizando a caixa de diálogo Propriedades da Tarefa.

Figura 26 – Defina a prioridade da tarefa.



Programas

O sistema operacional do controlador é um sistema multitarefas preventivo que está em conformidade com a IEC 1131-3. Esse sistema oferece o seguinte:

- programas para agrupar dados e lógica
- rotinas para encapsular códigos executáveis gravados em uma linguagem de programação

Cada programa contém o seguinte:

- tags locais
- parâmetros
- uma rotina principal executável
- outras rotinas
- uma rotina de falha opcional

Figura 27 – Programa em uma aplicação de controle

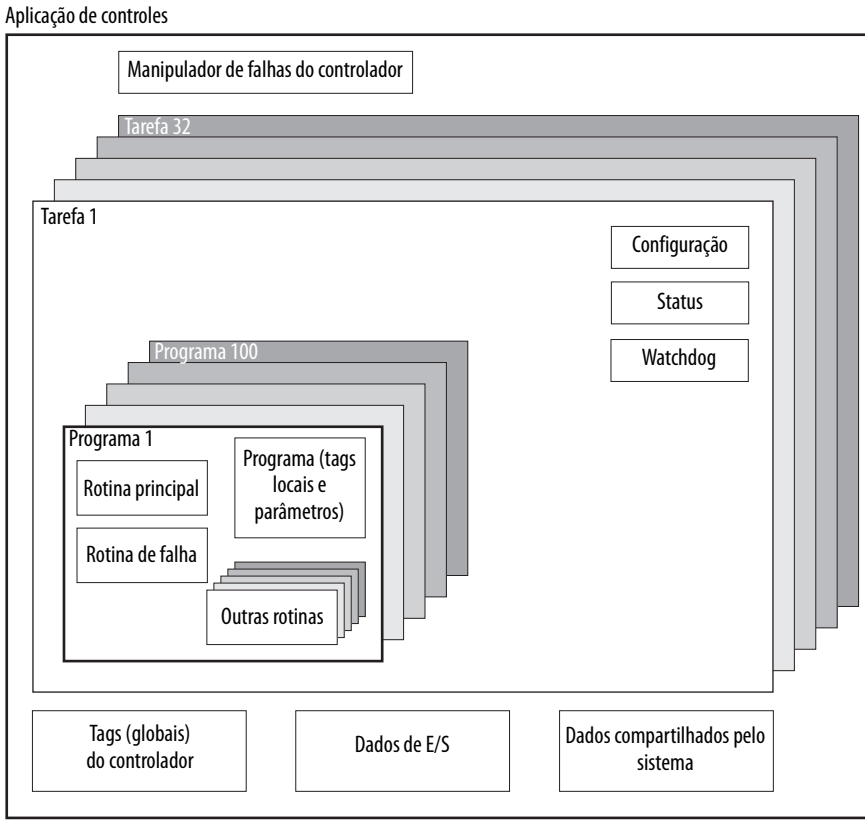
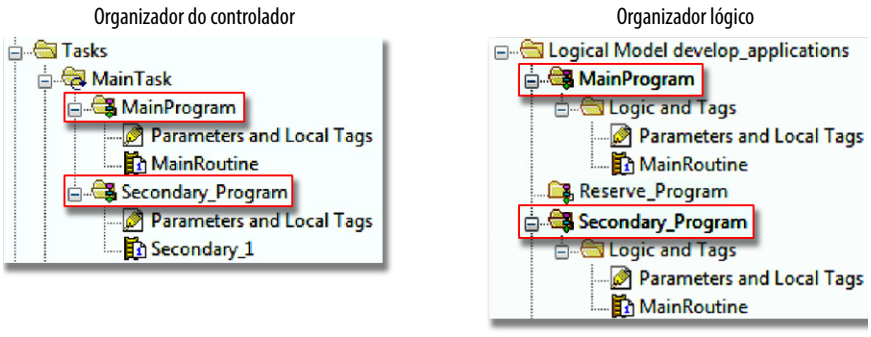


Figura 28 – Programas em aplicação



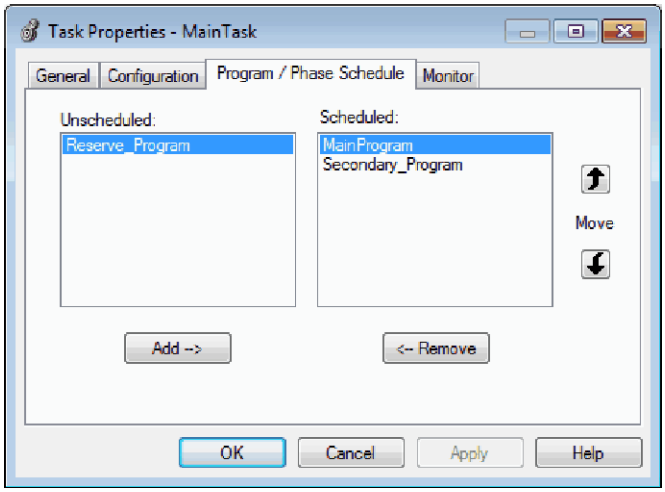
Programas programáveis e não programáveis

Os programas programáveis em uma tarefa são executados até sua conclusão começando do primeiro ao último. Os programas que não estão anexados a nenhuma tarefa aparecem como programas não programáveis.

Os não programáveis em uma tarefa são baixados ao controlador juntamente com todo o projeto. O controlador verifica os programas não programáveis mas não os executa.

É necessário agendar um programa em uma tarefa antes que o controlador possa fazer uma varredura no programa. Para agendar um programa não programável, use a guia Agendamento de Programa/Fase da caixa de diálogo Propriedades da Tarefa.

Figura 29 – Agendando um programa não programável



Rotinas

Uma rotina é um conjunto de instruções lógicas em uma linguagem de programação, como diagrama ladder (lógica ladder). As rotinas fornecem um código executável para o projeto em um controlador.

Cada programa tem uma rotina principal. Esta é a primeira rotina a ser executada quando o controlador dispara a tarefa associada e chama o programa associado. Use lógica, como a instrução Avançar para Subrotina (JSR), para chamar outras rotinas.

Também é possível especificar uma rotina de falha de programa opcional. O controlador executa esta rotina se encontrar uma falha de execução-instrução em qualquer uma das rotinas no programa associado.

Figura 30 – Rotinas em uma aplicação de controle

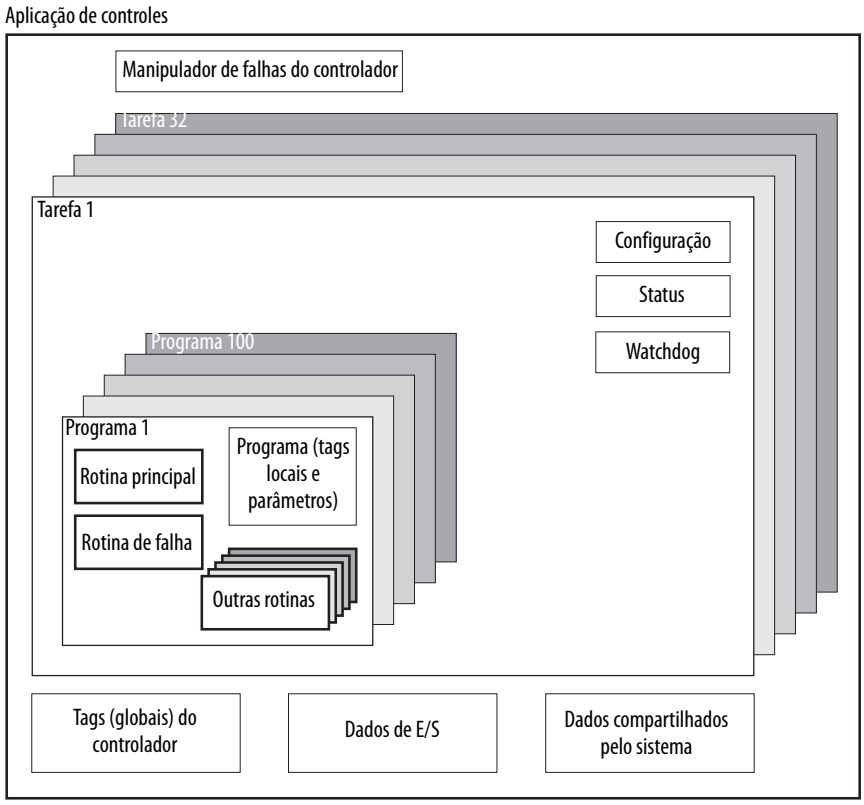
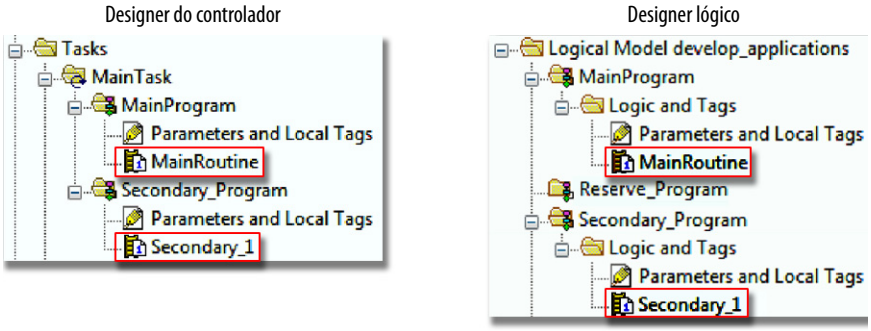


Figura 31 – Rotinas em aplicação



Tags

Com um controlador Logix5000, usa-se uma tag (nome alfanumérico) para endereçar os dados (variáveis). Nos controladores Logix5000, não há formato numérico fixo. Por exemplo, conforme mostrado abaixo, é possível utilizar o nome de tag **north_tank_mix** em vez de um formato numérico, como N7:0.0.

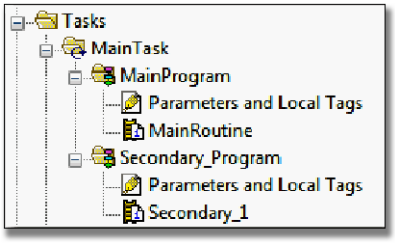
O próprio nome do tag identifica os dados. A tag permite que você faça o seguinte:

- Organize seus dados para refletir suas máquinas
- Documente sua aplicação conforme seu desenvolvimento.

Figura 32 mostra as tags de dados criadas dentro do escopo do Programa Principal do controlador.

Figura 32 – Exemplo de tags

Organizador do controlador – Parâmetros do programa principal e tags locais



Janela de tags do programa – principais tags do programa

Scope: MainProgram Show: All Tags Enter Name Filter...

Name	Usage	Alias For	Base Tag	Data Type	Description	External Access	Constant	Style
north_tank_mix	Local			BOOL		Read/Write		Decimal
north_tank_pr...	Local			REAL		Read/Write		Float
north_tank_temp	Local			REAL		Read/Write		Float
one_shots	Local			DINT		Read/Write		Decimal
recipe	Local			TANK		Read/Write		
recipe_number	Local			DINT		Read/Write		Decimal
replace_bit	Local			BOOL		Read/Write		Decimal
running_hours	Local			COUNTER		Read/Write		
running_secon...	Local			TIMER		Read/Write		
start	Local			BOOL		Read/Write		Decimal
stop	Local			BOOL		Read/Write		Decimal

Dispositivo de E/S analógico
Valor inteiro
Bit de armazenamento
Counter
Timer
Dispositivo de E/S digital

Há várias orientações para criação e configuração de parâmetros e tags locais para tarefas ideias e execução do programa. Para obter mais informações, consulte o Manual de programação de dados de tag de E/S e de controladores Logix5000, publicação 1756-PM004.

Propriedades estendidas

O recurso de propriedades estendidas permite que você defina informações adicionais, como limites, unidades de engenharia ou identificadores de estado para vários componentes dentro de seu projeto do controlador.

Componente	Propriedades estendidas
Tag	No Editor de tag, adicione propriedades estendidas para um tag.
Tipo definido pelo usuário	No Editor de tipo de dados, adicione propriedades estendidas aos tipos de dados.
Instruções adicionais	Nas propriedades associadas com a definição da Instrução Adicional, adicione as propriedade estendidas às instruções Adicionais.

O comportamento pass-through é a habilidade de atribuir propriedades estendidas a um nível superior de uma estrutura ou Instrução Adicionais e disponibilizar aquela propriedade estendida automaticamente para todos os membros. O comportamento de passagem está disponível para descrições, identificadores de estado e unidades de engenharia, além de poder ser configurado. Configure o comportamento de passagem na guia Projeto da caixa de diálogo Propriedades do Controlador. Se você optar por não mostras as propriedades de passagem, somente as propriedades estendidas que forem configuradas para um determinado componente serão exibidos.

O comportamento de passagem **não** está disponível para limites. Quando um exemplo de um tag é criado, se os limites estiverem associados ao tipo de dados, o exemplo é copiado.

Você precisa saber quais tags têm limites associados a eles, pois não há nenhuma indicação no navegador de tags de que as propriedades estendidas estão definidas por uma tag. Se, entretanto, você tentar utilizar propriedades estendias que não tenham sido definidas para um tag, os editores exibem uma indicação visual e a rotina não verifica.

Acessar as propriedades estendidas na lógica

Você pode acessar os limites definidos nas tags usando a sintaxe .@Min e .@Max:

- Não é possível gravar em valores de propriedades estendidas na lógica.
- Para usar as propriedades de tag estendida em uma Instrução Adicionais, você deve passá-las para dentro das Instruções como entradas de operandos.
- Os aliases das tags que tiveram as propriedades estendidas não podem acessar as propriedades estendidas na lógica.
- Os limites podem ser configurados para parâmetros de entrada e saída nas Instruções Adicionais. Entretanto, os limites não podem ser definidos em um parâmetro InOut de uma Instrução Adicional.
- Os limites não podem ser acessados dentro da lógica de instrução Adicionais. Os limites são somente para uso em aplicações IHM.

Se um tag vetor estiver utilizando um endereçamento indireto para acessar limites na lógica, as seguintes condições se aplicam:

- Caso uma tag do vetor tenha os limites configurados, as propriedades estendidas são aplicadas a qualquer elemento do vetor que não tenha aquela propriedade estendida específica explicitamente configurada. Por exemplo, se o tag do vetor MyArray tiver Max configurado em 100, qualquer elemento do vetor que não tiver Max configurado herda o valor de 100 quando for usado na lógica. Porém, você não poderá visualizar que este valor herdado do MyArray está configurado nas propriedades do tag.
- Pelo menos um elemento do vetor deve ter um limite configurado para a lógica do vetor referenciada indiretamente a verificar. Por exemplo, se MyArray[x].@Max estiver sendo usado na lógica, pelo menos, um elemento do vetor MyArray[] deve ter a propriedade estendida Max configurada se Max não é configurado por MyArray.
- Um valor padrão do tipo de dados é usado nas seguintes circunstâncias:
  - O vetor é acessado programaticamente com referência indireta.
  - O tag vetor não possui a propriedade estendida configurada.
  - Um membro de um vetor não possui a propriedade estendida configurada.

  Por exemplo, para um vetor do tipo SINT, quando o limite máx. é chamado na lógica para um membro, use o valor de 127.

Se um elemento do vetor for acessado diretamente, o elemento deve estar com a propriedade estendida definida. Se não, a verificação falha.

Linguagens de programação

O controlador Control GuardLogix 5370 suporta estas linguagens de programação, tanto on-line quanto off-line.

Tabela 20 – Linguagens de Programação do Controlador Compact GuardLogix

Linguagem	É melhor utilizada em programas com
Lógica ladder a relé	Execução contínua ou paralela de múltiplas operações (fora de sequência)
	Operações boolianas ou baseadas em bits
	Operações lógicas complexas
	Processamento de comunicação e mensagem
	Intertravamento de máquinas
	Operações que a equipe de serviço ou manutenção pode ter que interpretar para localizar falhas da máquina ou do processo
Diagrama de blocos de funções(1)	Controle de inversor e processo contínuo
	Controle de malha
	Cálculos de vazão
Controle Sequencial de Funções (SFC)(1)	Gestão de alto nível de operações múltiplas
	Sequência repetitiva de operações
	Processo por batelada
	Controle de posicionamento usando texto estruturado
	Operações de uma máquina de estado
Texto estruturado(1)	Operações matemáticas complexas
	Processamento de malha de tabela ou vetor especializado
	Processamento de protocolo ou manuseio de grupo ASCII

(1) Somente com programas padrão.

Para obter informações sobre programação nessas linguagens, consulte o Manual de programação de procedimentos comuns dos controladores Logix5000, publicação 1756-PM001.

Instruções add-on

É possível projetar e configurar conjuntos de instruções comumente utilizadas para aumentar a consistência do projeto. Similares às instruções incorporadas contidas nos controladores Logix5000, essas instruções que você cria são chamadas de instruções adicionais. As instruções adicionais reutilizam algoritmos de controle comum. Com elas, você pode fazer o seguinte:

- Facilitar a manutenção ao animar a lógica para uma instância.
- Proteger a propriedade intelectual com a Proteção da fonte.
- Tempo de desenvolvimento de documentação reduzido.

É possível usar instruções adicionais em múltiplos projetos. É possível definir suas instruções, obtê-las de outras pessoas ou copiá-las de outro projeto.

Tabela 21 explica alguns dos recursos e das vantagens de usar as instruções add-on.

Tabela 21 – Capacidades das instruções add-on

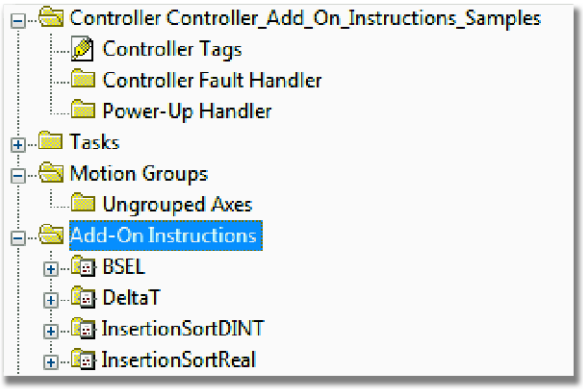
Capacidade	Descrição
Economize tempo	Com instruções adicionais, é possível combinar sua lógica mais comumente usada em conjuntos de instruções reutilizáveis. Você economiza tempo quando cria instruções para seus projetos e então as compartilha com outras. As instruções Adicionais aumentam a consistência do projeto porque todos os algoritmos comumente utilizados funcionam da mesma maneira, independente de quem implementa o projeto.
Use editores-padrão	Você cria instruções Adicionais utilizando um dos três editores: • Lógica ladder a relé • Diagrama de blocos de funções(1) • Texto estruturado(1) Uma vez criadas as instruções, é possível utilizá-las em qualquer editor.
Exporte instruções adicionais	Você pode exportar instruções adicionais para outros projetos, além de copiá-las e colá-las de um projeto para outro. Dê a cada instrução um nome unívoco para que não corra o risco de substituir acidentalmente uma outra instrução de mesmo nome.
Use visualizações de contexto	As visualizações de contexto permitem que você visualize a lógica de uma instrução para localização de falhas on-line instantânea e simplificada de suas instruções adicionais. Cada instrução contém uma revisão, um histórico de alterações e uma página de ajuda autogerada.
Crie ajuda personalizada	Quando você cria uma instrução, você insere informações nos campos de descrição em caixas de diálogo, informações que tornam-se o que é conhecido como Ajuda personalizada. A Ajuda personalizada facilita a obtenção de ajuda necessária na implementação das instruções.
Aplique a proteção da fonte	Como o criador das instruções adicionais, você pode limitar os usuários de suas instruções para acesso somente leitura ou barrar o acesso à lógica interna ou aos parâmetros locais usados pelas instruções. Esta proteção de fonte permite que você impeça alterações indesejadas às suas instruções, protegendo a propriedade intelectual.

(1) Somente com programas padrão.

Uma vez definidas em um projeto, as instruções adicionais se comportam de modo similar às instruções incorporadas nos controladores Logix5000. Elas aparecem na barra de ferramentas de instruções para fácil acesso, da mesma forma que as instruções.

Figura 33 – Instruções adicionais

Organizador do controlador



Barra de ferramentas instruções

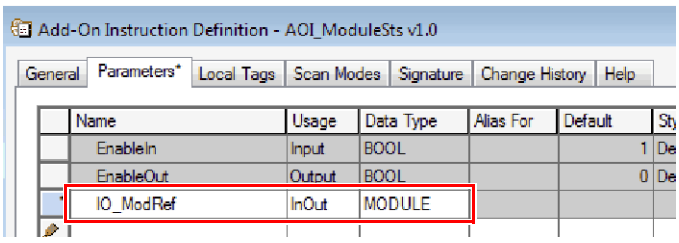
Acesse o objeto do módulo

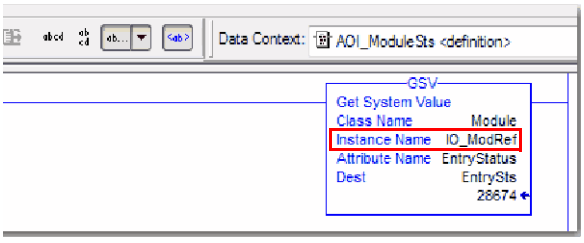
O objeto MODULE fornece informações de status sobre um módulo. Para selecionar um objeto de módulo em particular, defina o operando Nome do Objeto da instrução GSV/SSV para o nome do módulo. O módulo especificado deve estar presente na seção I/O Configuração do organizador do controlador e deve ter um nome de dispositivo.

Criar a Instrução Adicional

Com a aplicação Logix Designer, versão e posterior, você pode acessar um objeto MODULE diretamente a partir da instrução adicional. Anteriormente, você podia acessar os dados do objeto MODULE mas não a partir da Instrução Adicional.

Você deve criar um parâmetro Referência de Módulo ao definir a instrução adicional para acessar os dados do objeto MODULE. Um parâmetro de Módulo de Referência é um parâmetro InOut do tipo de dados do MODULE que aponta para o objeto MODULE de um módulo de hardware. Você pode usar os parâmetros de referência do módulo tanto na lógica da instrução adicional como na lógica do programa.





Para obter mais informações sobre o parâmetro referência de módulo, consulte o Manual de programação de instruções add-on para controladores Logix5000, publicação 1756-PM010 e a ajuda on-line para a aplicação Logix Designer.

O objeto MODULE usa os atributos a seguir para fornecer informações de status:

- EntryStatus
- FaultCode
- FaultInfo
- FWSupervisorStatus
- ForceStatus
- Instância
- LEDStatus
- Modo
- Caminho

O Caminho do atributo está disponível com o aplicativo Logix Designer, que fornece um caminho de comunicação com o módulo.

Para obter mais informações sobre os atributos disponíveis no objeto MODULE, consulte o Manual de referência de instruções dos controladores Logix, publicação 1756-RM009.

Quando você adiciona uma instrução GSV/SSV ao programa, são exibidas as classes de objeto, os nomes de objetos e os nomes de atributo para cada instrução. Para tarefas padrão, é possível usar a instrução GSV para obter os valores dos atributos disponíveis. Para a instrução SSV, somente são exibidos aqueles atributos cujas definições são permitidas.

Alguns tipos de objetos aparecem repetidamente, pois você pode precisar especificar o nome do objeto. Por exemplo, pode haver diversas tarefas na sua aplicação. Cada tarefa tem seu próprio objeto Tarefa que você acessa pelo nome da tarefa.

Há vários objetos e atributos os quais é possível utilizar as instruções GSV e SSV para monitorar e definir o sistema. Para obter mais informações sobre as instruções GSV, SSV, objetos e atributos, consulte o Manual de referência de instruções gerais dos controladores Logix, publicação 1756-RM009, e Usar instruções GSV/SSV na página 182.

Fatia de tempo de atraso do sistema

O controlador Compact GuardLogix 5370 comunica-se com outros dispositivos a uma taxa especificada (programável) ou quando há tempo de processamento disponível para realizar análise da comunicação.

O período de tempo de atraso do sistema especifica a porcentagem de tempo que um controlador dedica a serviço de comunicação. Se tiver uma tarefa contínua, a fatia de tempo do diretório do sistema na guia Avançado da caixa de diálogo propriedades do Controlador especifica a relação comunicação de serviço/tarefa contínua. Porém, se não houver tarefa contínua, a fatia de tempo de atraso não tem efeito.

A tabela mostra a relação entre a tarefa contínua e a comunicação de serviço em vários períodos de tempo de atraso do sistema.

Tabela 22 – Relação entre tarefa contínua e comunicação de serviço

Fatia deste momento	A tarefa contínua está em operação	A comunicação de serviço ocorre por até
10%	9 ms	1 ms
20%	4 ms	1 ms
25%	3 ms	1 ms
33%	2 ms	1 ms
50%	1 ms	1 ms
66%	1 ms	2 ms
75%	1 ms	3 ms
80%	1 ms	4 ms
90%	1 ms	9 ms

Conforme mostrado em Tabela 22, se a fatia de tempo de atraso do sistema for menor ou igual a 50%, a duração permanecerá fixa em 1 ms. O mesmo se aplica para 66% e superior, exceto quando há vários intervalos de 1 ms. Por exemplo, a 66% há dois intervalos de 1 ms de tempo consecutivo e a 90% há nove intervalos de 1 ms de tempo consecutivo.

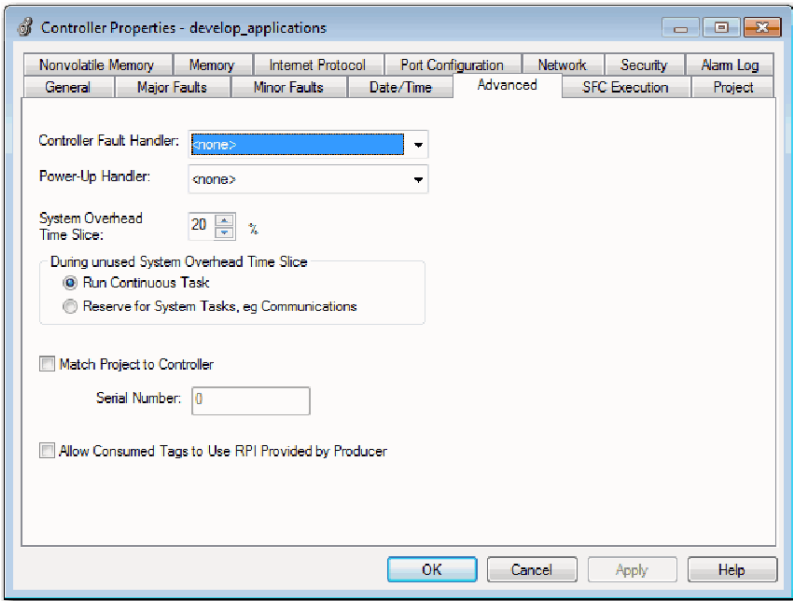
Configurar a fatia de tempo do diretório do sistema

Para configurar a fatia de tempo de atraso do sistema, siga este procedimento.

1. No organizador do controlador, clique com o botão direito do mouse no controlador e escolha Propriedades.

   A caixa de diálogo Propriedades do Controlador aparece.

2. Clique na guia Avançado.
3. Insira um valor numérico na caixa Fatia de Tempo do Diretório do Sistema.
4. Use Executar Tarefa Contínua (padrão) ou Reservar para Tarefas do Sistema.
   - Clique em executar Tarefa Contínua quando não houver comunicação ou tarefas de fundo a processar; o controlador retorna imediatamente à tarefa contínua.
   - Clique em Reservar para Tarefa do Sistema para alocar toda a fatia de tempo de 1 ms se o controlador tiver tarefas de fundo ou comunicação para executar antes de retornar à tarefa contínua. Isto permite que você simule uma carga de comunicação no controlador durante projeto e programação antes que IHMs, mensagens controlador a controlador, e assim por diante, sejam ajustadas.
5. Clique em OK.



Observações:

Desenvolver aplicações de segurança

Este capítulo explica os componentes que formam um projeto de segurança e oferece informações sobre o uso de recursos que ajudam a proteger a integridade da aplicação de segurança, como assinatura de tarefa de segurança e o bloqueio de segurança.

Para obter orientações e especificações para o desenvolvimento e comissionamento de aplicações de segurança SIL 3 e PLe, consulte o Manual de referência de segurança dos sistemas de controle GuardLogix® 5570 e Compact GuardLogix® 5370, publicação 1756-RM099.

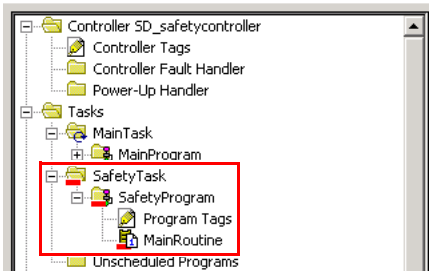
Esse manual de referência de segurança abrange o seguinte:

- Criar uma especificação de projeto detalhada
- Gravar, documentar e testar o aplicativo
- Gera a assinatura de tarefa de segurança para identificar e proteger o projeto
- A confirmação do projeto por meio da impressão ou exibição do projeto carregado e da comparação manual das configurações, dados de segurança e lógica do programa de segurança
- A verificação do projeto por meio de casos de teste, simulações, testes de verificação funcional e uma revisão de segurança independente, se necessária
- Bloquear o aplicativo de segurança
- Calcular o tempo de reação do sistema

A tarefa de segurança

Quando se cria um projeto de controlador de segurança, a aplicação Logix Designer cria automaticamente uma tarefa de segurança com um programa de segurança e uma rotina (de segurança) principal.

Figura 34 – Tarefa de segurança no organizador do controlador



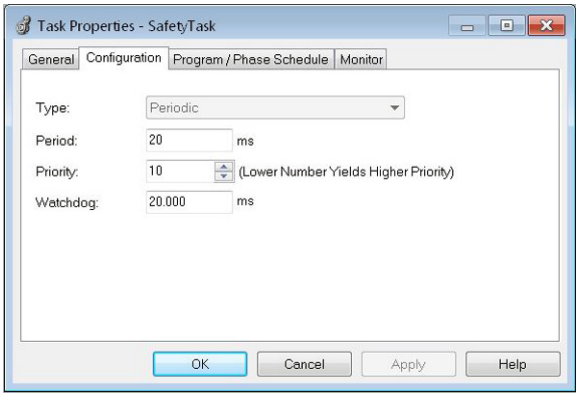
Na tarefa de segurança, você pode usar vários programas de segurança, compostos por várias rotinas de segurança. O controlador GuardLogix suporta uma tarefa de segurança. A tarefa de segurança não pode ser removida.

Não é possível agendar programas padrão ou executar rotinas padrão na tarefa de segurança.

Especificação do período da tarefa de segurança

A tarefa de segurança é uma tarefa periódica. Você seleciona a prioridade da tarefa e o tempo de watchdog na caixa de diálogo Propriedades da tarefa – Tarefa de Segurança. Abra a caixa de diálogo, clique com o botão direito na tarefa de segurança e escolha Propriedades.

Figura 35 – Configuração do período da tarefa de segurança



A tarefa de segurança é uma prioridade alta. O período (em ms) e o watchdog (em ms) da tarefa de segurança precisam ser especificados. O período da tarefa de segurança é o período no qual a tarefa de segurança é executada. O watchdog é o tempo máximo permitido do início da execução da tarefa de segurança até o término.

O período da tarefa de segurança está limitado a um máximo de 500 ms e não pode ser modificado on-line. Certifique-se de que a tarefa de segurança tenha tempo suficiente para a execução da lógica antes de ser disparada novamente. Se ocorrer um tempo-limite do watchdog da tarefa de segurança, será gerada uma falha de segurança irrecuperável no controlador de segurança.

O período da tarefa de segurança afeta diretamente o tempo de reação do sistema.

O Manual de referência de segurança dos sistemas de controle GuardLogix 5570 e Compact GuardLogix 5370, publicação 1756-RM099, fornece informações detalhadas sobre como calcular o tempo de reação.

Execução da Tarefa de Segurança

A tarefa de segurança é executada da mesma forma que uma tarefa periódica padrão, com as seguintes exceções:

- A tarefa de segurança não começa a execução até que os controladores primário e o parceiro de segurança estabeleçam uma parceria de controle. (As tarefas padrão serão executadas assim que o controlador passar para o modo de operação)
- Todos os tags de entrada de segurança (entradas, consumidos e mapeados) são atualizados e congelados no início da execução da tarefa de segurança.

  Consulte a página 154 para obter informações sobre o mapeamento de tags de segurança.
- Os valores do tag de saída de segurança (saída e produzida) são atualizados na conclusão da execução da tarefa de segurança.

Programas de segurança

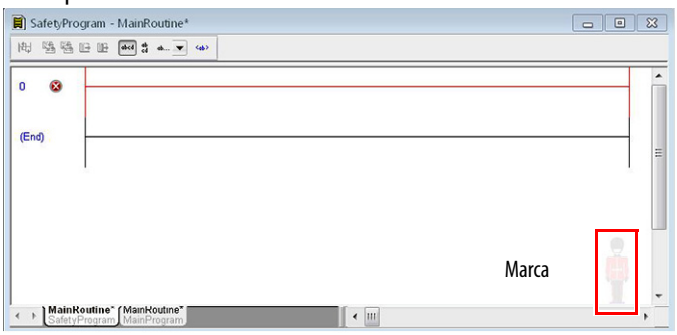
Os programas de segurança apresentam todos os atributos de programas padrão, porém eles só podem ser programados na tarefa de segurança e podem conter somente componentes de segurança. Programas de segurança apenas podem conter rotinas de segurança. Uma rotina de segurança deve ser considerada a rotina principal, e outra rotina de segurança pode ser considerada a rotina de falha.

Eles não podem conter rotinas padrão ou tags de segurança.

Rotinas de segurança

As rotinas de segurança apresentam todos os atributos de rotinas-padrão, mas podem existir apenas em um programa de segurança. Neste momento, somente o diagrama de lógica ladder é suportado para rotinas de segurança.

DICA O recurso de marca d´água distingue visualmente uma rotina de segurança de uma rotina-padrão.



Tags de segurança

Uma tag é uma área da memória do controlador onde os dados são armazenados. Os tags são o mecanismo básico de alocação de memória, a referência de dados da lógica e o monitoramento de dados. As tags de segurança apresentam todos os atributos de tags padrão com a adição de mecanismos certificados para oferecer a integridade de dados SIL 3.

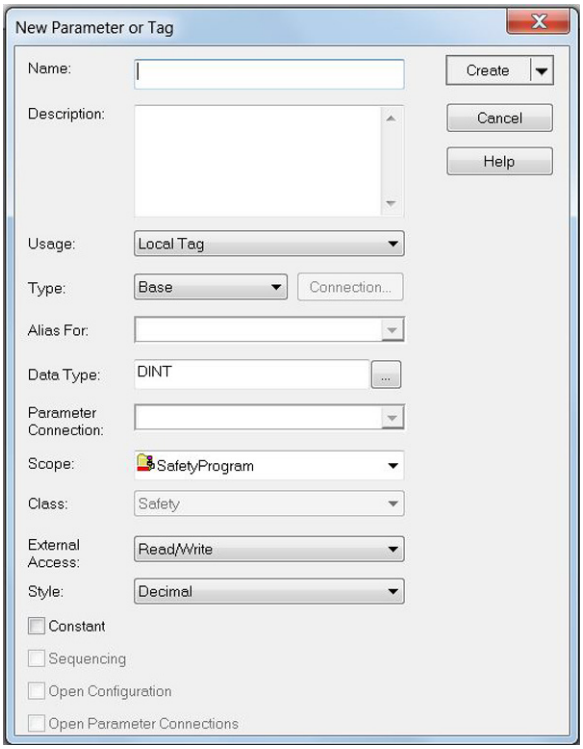
Quando um tag é criado, você atribui as propriedades a seguir:

- Nome
- Descrição (opcional)
- Tipo de tag
- Tipo de dados
- Escopo
- Classe
- Estilo
- Acesso externo

Você também pode especificar se o valor da tag é uma constante.

Para criar uma tag de segurança, abra a caixa de diálogo Nova Tag clicando com o botão direito nas Tags do Controlador ou nas Tags do Programa e escolha Nova Tag.

Figura 36 – Criando um novo tag



Tipo de tag

Tabela 23 define os quatro tipos de tags.

Tabela 23 – Quatro tipos de tag

Tipo de tag	Descrição
Tag de base	Estes tags armazenam valores para uso pela lógica dentro do projeto.
Tag de alias	Um tag relacionado a outro. Um tag sinônimo pode se relacionar a outro semelhante ou a um tag de base. Da mesma forma, pode-se referir a um componente de outro tag relacionando-se a um membro de uma estrutura, a um elemento de vetor ou a um bit em um tag ou membro. **IMPORTANTE:** Não use tags do alias entre tags padrão e de segurança em aplicações de segurança. Em vez disso, os tags padrão podem ser mapeados para tags de segurança usando um mapeamento de tags de segurança. Consulte Mapeamento de tags de segurança na página 154.
Tag produzida	Um tag disponibilizado pelo controlador para uso por outros controladores. No máximo 15 controladores podem consumir (receber) simultaneamente os dados. Um tag produzido envia dados a um ou mais tags em consumo sem usar a lógica. Os dados da tag produzida são enviados no RPI da tag em consumo.
Tag consumida	Um tag que recebe os dados de um tag produzido. O tipo de dados do tag consumido precisa corresponder ao tipo de dados do tag produzido. O Intervalo do Pacote Requisitado (RPI) da tag consumida determina o período de atualização dos dados.

Tipo de dados

O tipo de dados define o tipo de dados que a tag armazena, como um bit ou um número inteiro.

Os tipos de dados podem ser combinados para formar estruturas. Uma estrutura oferece um tipo de dado único que atende a uma necessidade específica. Nessa estrutura, cada tipo de dados é denominado um membro. Como os tags, os membros têm um nome e um tipo de dados. Você pode criar suas próprias estruturas, como tipos de dados definidos pelo usuário.

Os controladores Logix apresentam tipos de dados predefinidos para uso em instruções específicas.

Esses tipos de dados são permitidos para tags de segurança.

Tabela 24 – Tipos de dados válidos para tags de segurança

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

Escopo

O escopo de um tag determina o local de acesso possível a dados do tag. Quando você cria um tag, define-o como um tag do controlador (dados globais) ou um tag de programa para uma segurança específica ou um programa padrão (dados locais). Os tags de segurança podem ser do controlador ou do programa de segurança.

Tags com escopo no controlador

Quando as tags são com escopo no controlador, todos os programas têm acesso aos dados de segurança. Os tags precisarão ter escopo no controlador se forem usados no seguinte:

- Mais de um programa no projeto
- Para produzir ou consumir dados
- Para se comunicar com um terminal PanelView ™
- Em mapeamento de tags de segurança

  Consulte Mapeamento de tags de segurança na página 154 para obter mais informações.

É possível fazer a leitura de tags de segurança com escopo no controlador, mas elas não podem ser gravadas por rotinas-padrão.

IMPORTANTE	Os tags de segurança do controlador são lidos por qualquer rotina padrão. A taxa de atualização do tag de segurança está baseada no período de tarefa de segurança.

Tags associadas a E/S de segurança e dados de segurança produzidos ou consumidos precisam ser tags de segurança com escopo no controlador. Para tags de segurança produzidos/consumidos, é necessário criar um tipo de dados definido pelo usuário com o primeiro membro da estrutura do tag reservada para o status da conexão. Esse membro é um tipo de dados predefinido denominado CONNECTION_STATUS.

Tabela 25 – Recurso adicional

Recurso	Descrição
Manual dos controladores de E/S Logix5000™ e de programação de dados de tag, publicação 1756-PM004	Fornece instruções para a criação de tipos de dados definidos pelo usuário

Tags com escopo no programa

Quando as tags são com escopo no programa, os dados são isolados de outros programas. A reutilização de nomes de tags do programa é permitida entre programas.

As tags de segurança com escopo no programa de segurança podem ser lidas ou gravadas somente por meio de uma rotina de segurança com escopo no mesmo programa de segurança.

Classe

As tags de segurança podem ser classificadas como padrão ou de segurança. Os tags classificados como tags de segurança devem ter um tipo de dados permitido para esses tags.

Quando você cria tags do programa, a classe é automaticamente especificada, dependendo se o tag foi criado em um programa padrão ou de segurança.

Quando criar tags do controlador, você deve selecionar a classe do tag manualmente.

Valor constante

Ao designar uma tag como um valor constante, não é possível modificá-la pela lógica no controlador ou por uma aplicação externa, como um IHM. Tags de valor constante não podem ser forçadas.

A aplicação Logix Designer pode modificar os tags padrão constantes e os tags de segurança desde que uma assinatura de tarefa de segurança não esteja presente. As tags de segurança não podem ser modificadas se uma assinatura da tarefa de segurança estiver presente.

Acesso externo

O acesso externo define o nível de acesso permitido para dispositivos externos, como um IHM, para ver ou modificar os valores das tags. O acesso pela aplicação Logix Designer não é afetado por este ajuste de parâmetro. O valor padrão é ler/escrever.

Tabela 26 – Níveis de acesso externo

Configuração do acesso externo	Descrição
Nenhuma	Os tags não são acessíveis a partir de fora do controlador.
Somente leitura	Os tags podem ser navegados ou lidos, mas não gravados de fora do controlador.
Leitura/escrita	Os tags padrão podem ser navegados, lidos ou gravados de fora do controlador.

Para tags iguais, o tipo de acesso externo é igual ao tipo configurado para o tag alvo de base.

Tags de segurança produzidas/consumidas

Para compartilhar dados de segurança entre controladores Compact GuardLogix, você utiliza tags de segurança produzidas e consumidas. Tags produzidas e consumidas necessitam de conexões. O tipo de conexão-padrão para tags produzidas e consumidas é unicast.

Tabela 27 – Conexões produzidas e consumidas

Tag	Descrição da conexão
Produzida	Um GuardLogix ou um controlador Compact GuardLogix pode produzir (enviar) tags de segurança a outros GuardLogix ou a controladores GuardLogix. O controlador produtor utiliza um única conexão para cada consumidor.
Consumida	GuardLogix ou um controlador Compact GuardLogix pode consumir (receber) tags de segurança a outros GuardLogix ou a controladores GuardLogix. Cada tag consumido utiliza uma conexão.

Os tags de segurança produzidos e consumidos estão sujeitos às restrições a seguir:

- Somente os tags de segurança com escopo no controlador podem ser compartilhados.
- Os tags de segurança produzidos e consumidos estão limitados a 128 bytes.
- Os pares de tags produzidos/consumidos precisam apresentar o mesmo tipo de dados definido pelo usuário.

- O primeiro membro do tipo de dados definido pelo usuário precisa ser o tipo predefinido de dados CONNECTION_STATUS.
- O RPI da tag de segurança consumida precisa ser compatível com o período da tarefa de segurança do controlador GuardLogix produtor.

Para configurar adequadamente as tags de segurança produzidas e consumidas para compartilhar dados entre controladores de segurança peer, deve-se configurar adequadamente os controladores de segurança peer, produzir uma tag de segurança e consumir uma tag de segurança, conforme descrito abaixo.

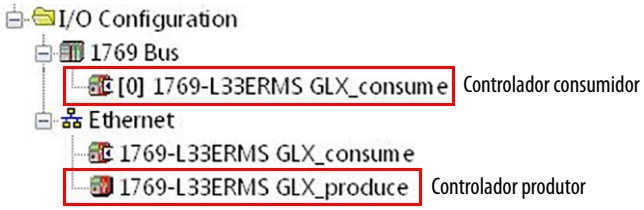
Configure os números da rede de segurança dos controladores de segurança peer

O controlador de segurança peer está sujeito às mesmas especificações de configuração que o controlador de segurança local. O controlador de segurança peer também deve ter um número de rede de segurança (SNN).

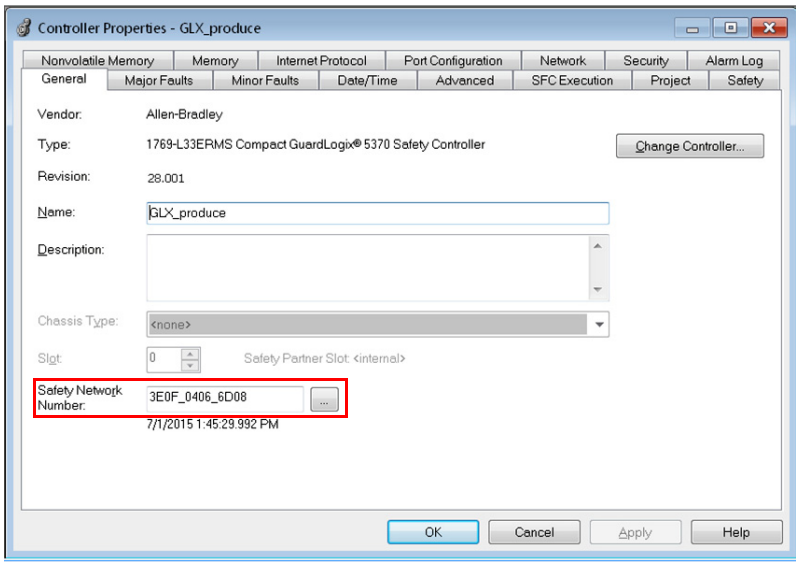
Siga estas etapas para copiar e colar o SNN.

1. Adicione o controlador produtor à árvore de E/S do controlador consumidor.

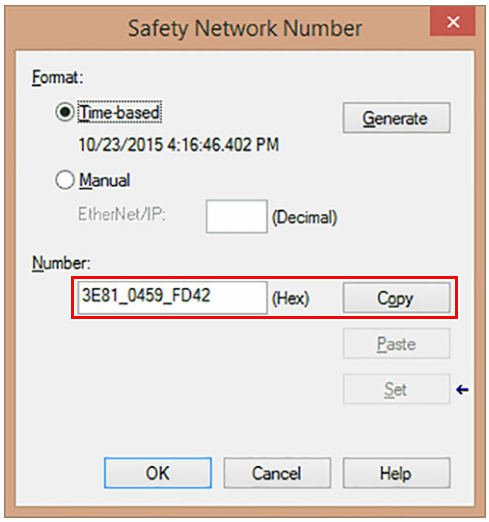
   DICA O mesmo controlador de produção não deve aparecer mais do que uma vez na árvore de E/S do seu controlador ou um erro de verificação ocorre.



2. No projeto do controlador produtor, clique com o botão direito do mouse no controlador produtor e escolha Propriedades do Controlador.
3. Clique em ... para abrir a caixa de diálogo Número da rede de segurança.

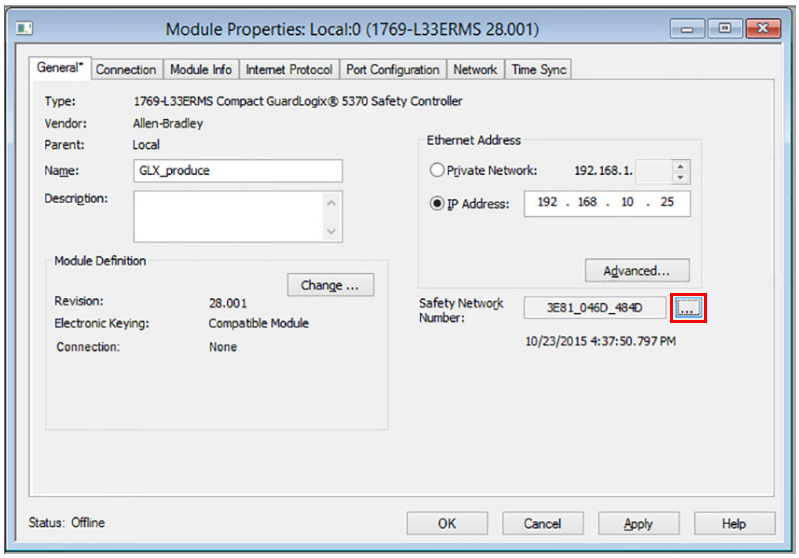


4. Clique em Copiar para copiar o controlador produtor do SNN.

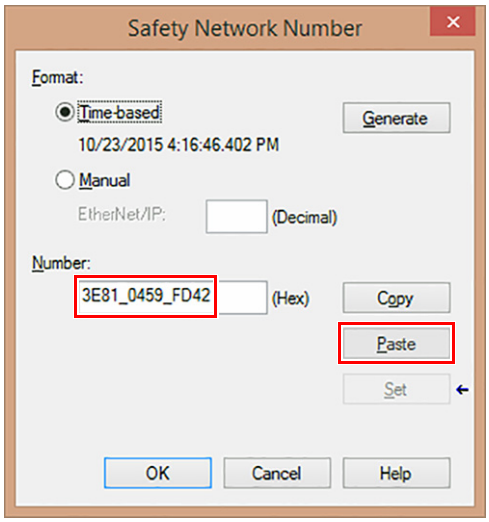


5. No projeto do controlador consumidor, clique com o botão direito do mouse no controlador produtor e escolha Propriedades do Módulo.

6. Clique em ... para abrir a caixa de diálogo Número da rede de segurança.

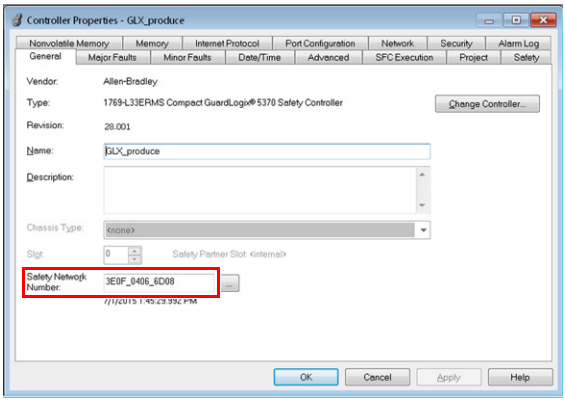


7. Cole o SNN do controlador produtor no campo SNN e clique em OK.

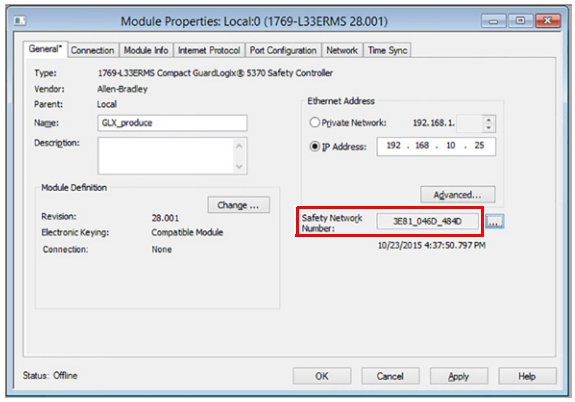


Os números da rede de segurança combinam.

Caixa de diálogo Propriedades do controlador no projeto produtor



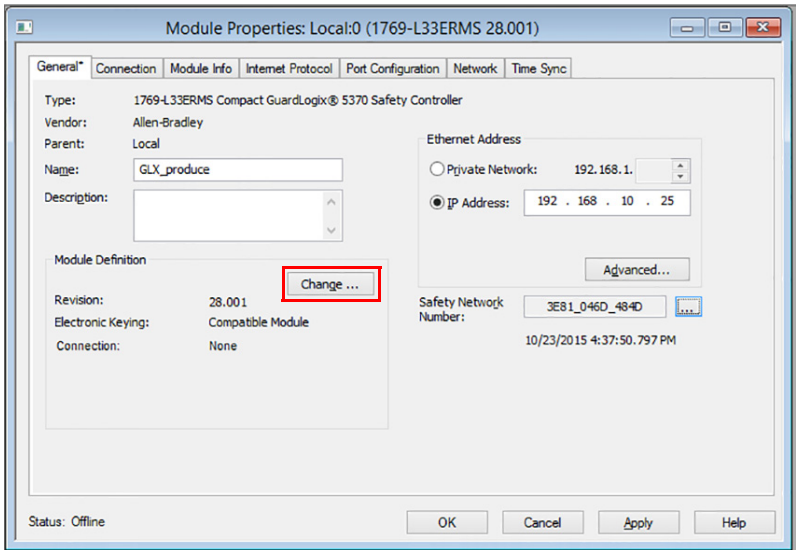
Caixa de diálogo Propriedades do Módulo no projeto do consumidor



Alterar a codificação eletrônica

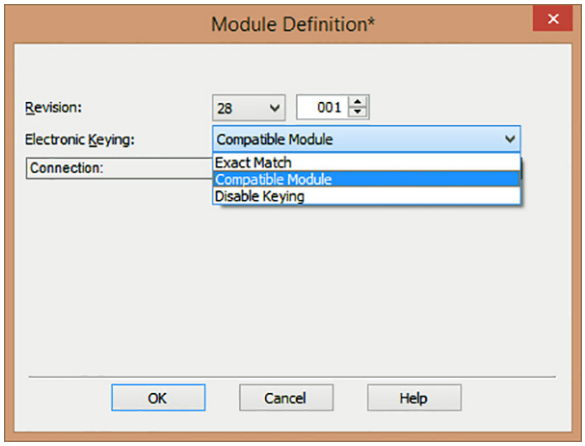
Para alterar a codificação eletrônica, siga estas etapas.

1. No projeto do controlador consumidor, clique com o botão direito do mouse no controlador produtor e escolha Propriedades do Módulo.
2. Clique em Alterar na área Definição do módulo.



Aparece a caixa de diálogo Definição do módulo.

3. A partir do menu suspenso Codificação eletrônica, escolha o que for apropriado para sua aplicação.



IMPORTANTE Se você estiver consumindo tags de segurança, então é preciso escolher entre Correspondência exata ou Módulo compatível a partir do menu suspenso.

Escolha a desabilitação do chaveamento apenas quando as tags padrão forem consumidas.

4. Clique em OK para fechar a caixa de diálogo Definição do módulo e corrigir o problema.
5. Clique em OK para fechar a caixa de diálogo Propriedades dos Módulos

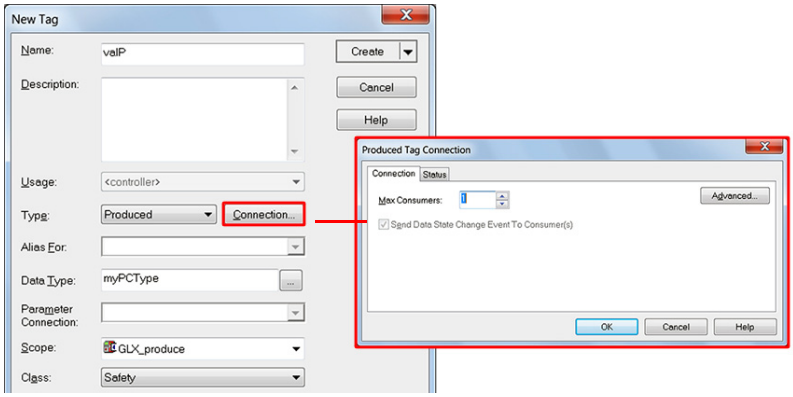
Produzir uma tag de segurança

Siga este procedimento para produzir uma tag de segurança.

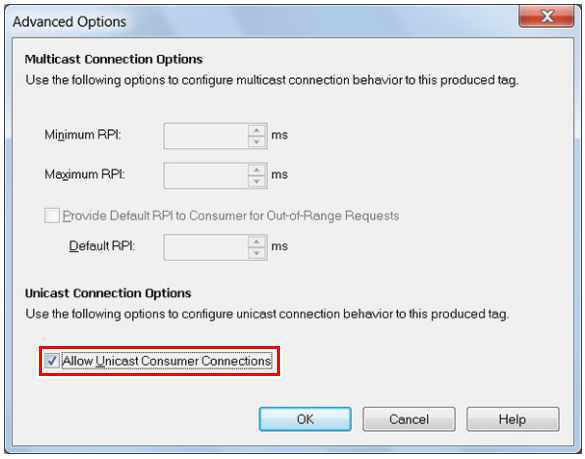
1. No projeto dos controladores de produção, crie um tipo de dados definido pelo usuário escolhendo a estrutura dos dados a serem produzidos.

   Certifique-se de que o primeiro membro dos dados é o tipo CONNECTION_STATUS.

2. Com o botão direito, clique em Tags do controlador e escolha Nova Tag.
3. Defina o tipo como Produzido, a classe como Segurança e o tipo de dados como o tipo definido pelo usuário que foi criado na etapa 1.
4. Clique em Conexão e insira o número de consumidores.



5. Clique em Avançado se quiser mudar o tipo de conexão ao tirar a seleção de “Permitir conexões Unicast do consumidor”.



6. Clique em OK.

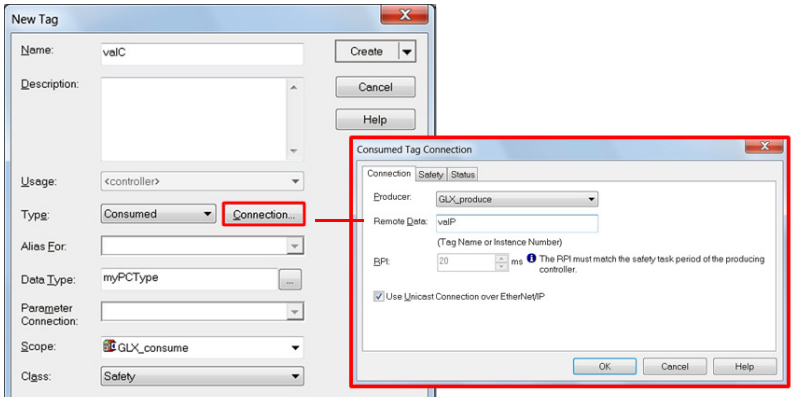
Consumir dados de tags de segurança

Siga estas etapas para consumir os dados produzidos por outro controlador.

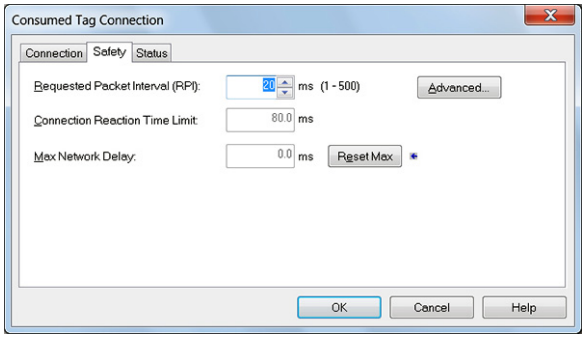
1. No projeto do controlador consumidor, crie um tipo de dado definido pelo usuário idêntico ao criado no projeto do produtor.

   DICA Esse tipo pode ser copiado do projeto produtor e colado no projeto consumidor.

2. Com o botão direito, clique em Tags do controlador e escolha Nova Tag.
3. Defina o tipo como Consumida, a classe como Segurança e o tipo de dados como o tipo definido pelo usuário que foi criado na etapa 1.
4. Clique em Conexão para abrir a caixa de diálogo conexão de tag consumido.



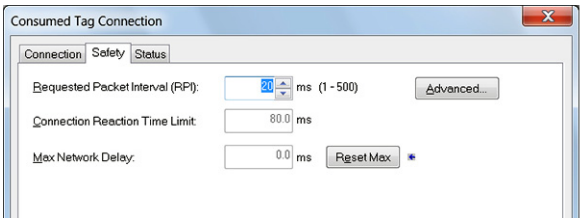
5. No menu suspenso produtor, selecione o controlador que produz os dados.
6. No campo de dados remoto, digite o nome da tag produzida.
7. Clique na guia Segurança.



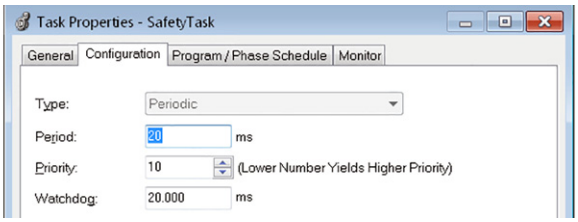
8. No campo intervalo do pacote requisitado (RPI), digite o RPI para a conexão em incrementos de 1 ms. O padrão é 20 ms.

   A RPI especifica o período quando os dados atualizam através de uma conexão. O RPI do tag de segurança consumido precisa ser compatível com o período da tarefa de segurança do projeto produtor de segurança.

Projeto Consumidor



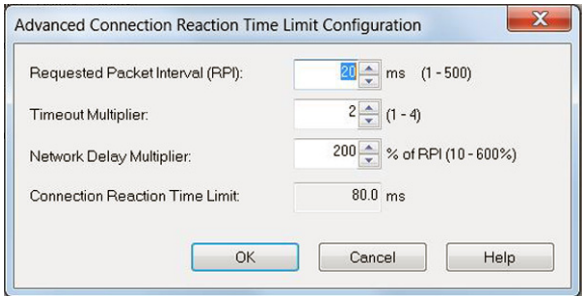
Projeto Produtor



O limite de tempo de reação da conexão é a idade máxima dos pacotes de segurança na conexão associada. Para limitações de tempo simples, você pode atingir um limite de tempo de reação de conexão aceitável ajustando o RPI.

Atraso máximo de rede é o atraso máximo de transporte observado desde o momento de produção dos dados até o momento no qual são recebidos. Quando online, clique em Reiniciar Máx para reiniciar o atraso de rede Máx.

9. Se o limite do tempo de reação da conexão for aceitável, clique em OK; ou, para especificações mais complexas, clique em Avançado para definir os parâmetros avançados do limite de tempo de reação da conexão.



O campo Multiplicador de tempo-limite determina o número de RPIs para aguardar um pacote antes de declarar o tempo-limite de conexão.

O campo Multiplicador de atraso de rede define o tempo de transporte da mensagem imposto pelo protocolo de segurança CIP. Esse campo especifica o atraso do ciclo completo do produtor até o consumidor e de volta ao produtor. Você pode usar o campo Multiplicador de atraso de rede para aumentar ou diminuir o Limite do tempo de reação de conexão.

Tabela 28 – Recursos adicionais

Recurso	Descrição
Estimate Requested Packet Interval na página 85 e Module Fault Related to RPI Estimates na página 86	Fornece mais informações sobre a configuração do RPI e entendimento sobre a Max. Atraso de rede; Multiplicador de tempo-limite e Multiplicadores de atraso de rede afetam o tempo de reação de conexão
Manual de programação de tags consumidas e produzidas dos controladores Logix5000™, publicação 1756-PM011	Fornece informações detalhadas sobre como usar tags de segurança produzidos e consumidos

Mapeamento de tags de segurança

Os tags padrão com escopo controlado não podem ser acessados diretamente por uma rotina de segurança. Para permitir que os dados padrão da tag sejam usados em rotinas de tarefa de segurança, os controladores GuardLogix oferecem um recurso de mapeamento de tag de segurança que permite que os valores padrão de tag sejam copiados na memória da tarefa de segurança.

Restrições

O mapeamento de tags de segurança está sujeito às seguintes restrições:

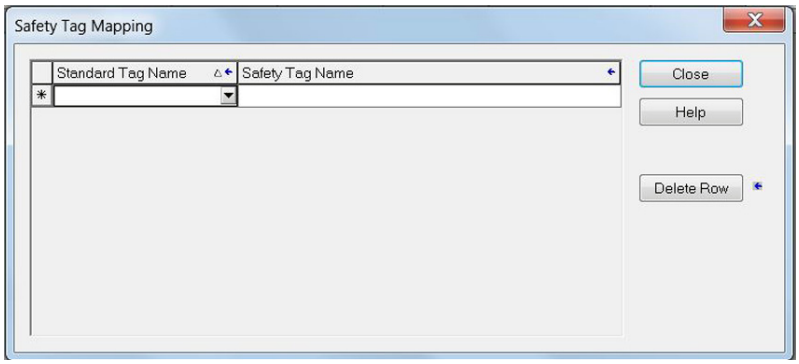
- o par de tags de segurança e padrão precisa ser do controlador.
- os tipos de dados do par de tags de segurança e padrão devem corresponder.
- não são permitidos tags alias.
- o mapeamento precisa ocorrer no nível do tag inteiro. Por exemplo, myTimer.pre não será permitido se myTimer for um tag TIMER.
- um par de mapeamento é um tag padrão mapeado em um tag de segurança.
- não é possível mapear uma tag padrão em uma tag de segurança que foi designada como uma constante.
- o mapeamento de tags não pode ser modificado quando o seguinte for verdade:
  - o projeto está com bloqueio de segurança.
  - uma assinatura de tarefa de segurança existir.
  - a chave seletora está na posição RUN.
  - existir uma falha de segurança irrecuperável.
  - existir uma parceria inválida entre o controlador principal e o parceiro de segurança.

ATENÇÃO: Quando usar dados padrão em uma rotina de segurança, você deve verificar que os dados são usados de forma adequada. O uso de dados padrão em um tag de segurança não os torna dados de segurança. Não é possível controlar diretamente uma saída de segurança SIL 3/PLe com dados de tag padrão.

Consulte o Manual de referência de segurança dos sistemas de sistemas de controle GuardLogix 5570 e Compact GuardLogix 5370, publicação 1756-RM099, para mais informações.

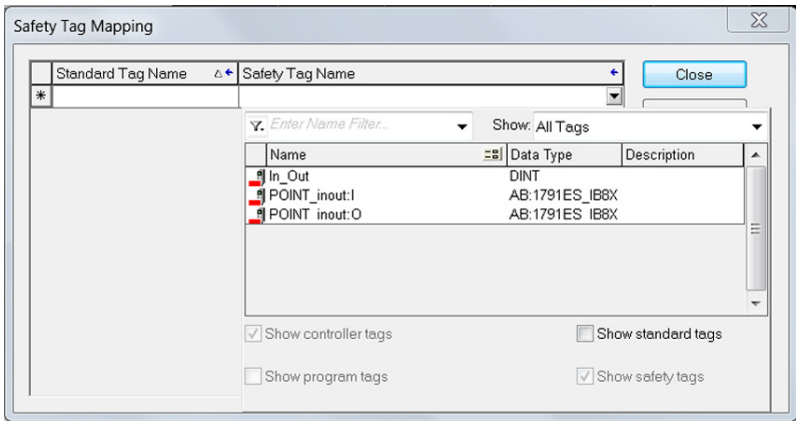
Criar pares para mapeamento de tags

1. Escolha Tags de segurança de mapeamento no menu Logic para abrir a caixa de diálogo Mapeamento de tags de segurança



2. Adicione um tag existente à coluna Nome de tag padrão ou Nome de tag de segurança digitando o nome do tag na célula ou escolhendo um tag do menu.

   Clique na seta para exibir uma caixa de diálogo do navegador de tags filtrados. Se você estiver na coluna Standard Tag Name, o navegador exibirá somente tags padrão do controlador. Se você estiver na coluna Safety Tag Name, o navegador exibirá tags de segurança do controlador.



3. Adicione um novo tag na coluna Nome de tag padrão ou Nome de tag de segurança clicando com o botão direito do mouse na célula vazia e selecionado Nova Tag e digitando o nome da tag na célula.
4. Clique com o botão direito do mouse na célula e escolha Nova tagname, onde tagname é o texto inserido na célula.

Monitorar o status de mapeamento de tags

A coluna à esquerda da caixa de diálogo Mapeamento de tags de segurança indica o status do par mapeado.

Tabela 29 – Ícones de status de mapeamento de tags

Conteúdo da célula	Descrição
Vazia	O mapeamento de tag é válido.
	Quando off-line, o ícone X indica que o mapeamento do tag é inválido. Você pode mudar para outra sequência ou fechar a caixa de diálogo mpeamento de tag de segurança.(1) Quando on-line, um mapeamento de tags inválido resulta em uma mensagem informando o motivo do mapeamento inválido. Você não pode mudar para uma sequência diferente ou fechar a caixa diálogo Mapeamento de tags de segurança se ocorrer um erro de mapeamento de tags.
	Indica a sequência atualmente em enfoque.
	Representa a sequência Criar nova tag mapeada.
	Representa uma edição pendente.

(1) O mapeamento de tags também é analisado durante a verificação do projeto. O mapeamento inválido de tags resulta em um erro de verificação do projeto.

Para obter mais informações, consulte as restrições de mapeamento de tag na página 154.

Proteção de aplicações de segurança

É possível proteger o programa aplicativo de mudanças não autorizadas por meio do bloqueio de segurança no controlador e gerando e gravando a assinatura de tarefa de segurança.

Bloqueando o controlador com trava de segurança

O controlador GuardLogix pode ter uma trava de segurança para proteger os componentes de controle relacionados à segurança de modificações. O recurso de trava de segurança se aplica apenas a componentes de segurança, tais como tarefa de segurança, programas de segurança, rotinas de segurança, instruções adicionais, tags de segurança, E/S de segurança e assinatura de tarefa de segurança.

Quando o controlador estiver protegido, as seguintes ações não serão permitidas na parte de segurança da aplicação:

- edição e programação on-line/off-line (inclusive Instruções Adicionais de segurança)
- forçar a E/S de segurança
- mudando o estado de inibição da E/S de segurança ou as conexões produzidas
- manipulação de dados de segurança (exceto pela lógica de rotina de segurança)
- criação ou remoção da assinatura de tarefa de segurança

DICA O texto do botão de status de segurança da barra on-line indica o status da trava de segurança.

A bandeja da aplicação também exibe os seguintes ícones para indicar o status de trava de segurança do controlador de segurança:

- = Controlador protegido
- = Controlador Desprotegido

É possível bloquear por segurança o projeto do controlador, independentemente do estado on-line ou off-line da fonte original do programa. No entanto, nenhuma imposição de segurança ou edição de segurança online pendente pode existir.

Os status bloqueado por segurança e desbloqueado por segurança não podem ser alterados quando a chave seletora está na posição RUN.

DICA As ações de trava ou desbloqueio de segurança são armazenadas no registro do controlador.

Para mais informações sobre acesso ao log do controlador, consulte o Manual de programação de status e informações de controlador dos controladores Logix5000™, publicação 1756-PM015.

Você pode travar e destravar por segurança o controlador na guia segurança da caixa de diálogo Propriedades do controlador ou selecionando Ferramentas>Segurança> travar/destravar segurança.

Figura 37 – Bloqueando o controlador com trava de segurança

Se configurar uma senha para a função de trava de segurança, você deve digitá-la no campo Inserir Senha. Caso contrário, clique em Bloquear.

Você também pode configurar ou mudar a senha na caixa de diálogo Trava de Segurança Consulte Definir senhas para trava de segurança e desbloqueio na página 58.

O recurso de trava de segurança, descrito nesta seção, e as medidas-padrão de segurança na aplicação Logix Designer são aplicáveis a projetos do controlador GuardLogix.

Consulte o Manual de programação de segurança dos controladores Logix5000, publicação 1756-PM016, para obter informações sobre os recursos de segurança do Logix Designer.

Gerar uma assinatura de tarefa de segurança

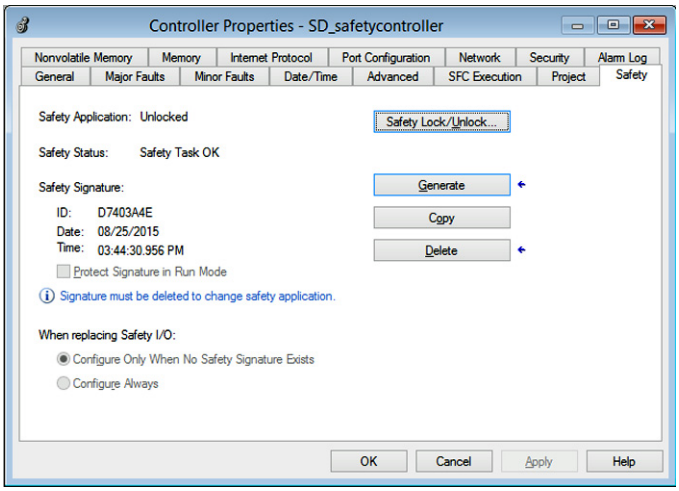
Antes do teste de verificação, deve ser gerada a assinatura de tarefa de segurança. Você pode criá-la somente quando o controlador GuardLogix on-line, no modo programa, desprotegido e sem imposições de segurança, edições de segurança on-line pendentes ou falhas de segurança. O status de segurança deve ser Tarefa de segurança OK.

Além disso, você não pode gerar uma assinatura de tarefa de segurança se o controlador estiver no modo de operação com a proteção do modo de operação habilitada.

DICA Você pode visualizar o status de segurança por meio do botão de status de segurança na barra on-line (consulte a página 157) ou na guia segurança da caixa de diálogo propriedades do controlador, conforme exibido em Figura 38.

Clique em Gerar para gerar uma assinatura de tarefa de segurança a partir da guia Segurança na caixa de diálogo Propriedades do controlador. Você também pode escolher Ferramentas>Segurança>Gerar assinatura.

Figura 38 – Guia Segurança



Se já existir uma assinatura, será necessário sobrescrevê-la.

DICA A criação e a exclusão da assinatura da tarefa de segurança são registradas no registro do controlador.

Para obter mais informações sobre acesso ao log do controlador, consulte o Manual de programação de status e informações de controlador dos controladores Logix5000, publicação 1756-PM015.

Quando existir uma assinatura de tarefa de segurança, as seguintes ações não serão permitidas na parte de segurança da aplicação:

- Edição ou programação on-line/off-line (inclusive Instruções add-on de segurança)
- Forçar a E/S de segurança
- Mudar o estado de inibição da E/S de segurança ou os controladores produtores
- Manipulação de dados de segurança (exceto pela lógica de rotina de segurança)

Copiar a assinatura da tarefa de segurança

Você pode usar o botão Copy para criar um registro de uma assinatura da tarefa de segurança para usar na documentação, na comparação e na validação do projeto de segurança. Clique em Copy, para copiar os componentes de ID, Date e Time para a área de transferência do Windows.

Excluir a assinatura da tarefa de segurança

Clique em Delete para excluir a assinatura da tarefa de segurança. A assinatura da tarefa de segurança não pode ser excluída quando o seguinte for verdade:

- O controlador estiver protegido.
- O controlador está no modo de operação com a chave seletora no RUN.
- O controlador está no de operação ou modo de operação remota com a proteção do modo de operação habilitada.

ATENÇÃO: Se remover a assinatura da tarefa de segurança, você deve testar e validar novamente seu sistema para atender a SIL 3/PLe.

Consulte o Manual de referência de segurança dos sistemas de controle GuardLogix 5570 e Compact GuardLogix 5370, publicação 1756-RM099, para obter mais informações sobre requisitos SIL 3/PLe.

Restrições de programação

As restrições que limitam a disponibilidade de alguns itens e funções de menus (ou seja, cortar, colar, remover, pesquisar e substituir) são impostas pela aplicação Logix Designer para ajudar a proteger os componentes de segurança de modificações sempre que o seguinte for verdade:

- o controlador estiver protegido.
- existe uma assinatura de tarefa de segurança.
- existirem falhas de segurança.
- O status de segurança é como segue:
  - parceiro faltante.
  - parceiro não disponível.
  - hardware incompatível.
  - firmware incompatível.

Se mesmo só uma dessas condições se aplicar, não se pode fazer o seguinte:

- criar ou modificar objetos de segurança, incluindo programas, rotinas, tags, instruções adicionais e módulos de E/S de segurança.

  IMPORTANTE Os tempos de varredura da tarefa de segurança e de programas de segurança podem ser reiniciados quando se está on-line.

- aplicar imposições a tags de segurança.
- criar novos mapeamentos de tags de segurança.
- modificar ou remover mapeamentos de tags.
- modificar ou remover tipos de dados definidos pelo usuário utilizados por tags de segurança.
- modificar o nome, a descrição, o tipo de rack, o slot e o SNN do controlador.
- modificar ou remover a assinatura da tarefa de segurança quando estiver com bloqueio de segurança.

Desenvolver Movimento Integrado em uma aplicação de rede EtherNet/IP

Estes controladores CompactLogix® 5370 suportam Movimento Integrado por meio de uma rede EtherNet/IP:

Movimento Integrado em aplicações EtherNet/IP usa o seguinte:

- Rede EtherNet/IP padrão
- Inversores de alto desempenho, incluindo os seguintes:
  - Inversores Kinetix® 350
  - Inversores Kinetix® 5500 e Kinetix® 5700
  - Inversores Kinetix® 6500
  - Inversores PowerFlex® 527
  - Inversores PowerFlex® 755
- Componentes de infraestrutura padrão
- Software de programação

Além disso, os inversores Kinetix 5500(1), Kinetix 5700 e PowerFlex 527 suportam safe torque-off integrado (STO) por meio de uma conexão única de segurança e movimentação com um controlador de segurança Compact GuardLogix 5370. O controlador Compact GuardLogix emite o comando STO por meio de uma rede EtherNet/IP através do CIP Safety e o inversor de segurança executa o comando.

Para obter mais informações sobre como configurar inversores que usam Movimento Integrado em uma rede EtherNet/IP, consulte os manuais do usuário dos inversores listados em Recursos adicionais na página 12 e o Manual do usuário para configuração e inicialização do movimento integrado na rede EtherNet/IP, publicação MOTION-UM003.

(1) Aplica-se apenas às unidades Kinetix 5500 com Códigos de catálogos -ERS2.

Suporte aos eixos de movimento

Os controladores 1769-L30ERMS, 1769-L33ERMS, 1769-L33ERMOS, 1769-L36ERMS, 1769-L36ERMOS e 1769-L37ERMOS suportam estes eixos:

- AXIS_VIRTUAL
- AXIS_CIP_DRIVE

Eixo AXIS_VIRTUAL

O eixo AXIS_VIRTUAL é uma representação de eixo interno que não é associado com nenhum inversor físico. Ou seja, você pode configurar o eixo mas ele não causa nenhum movimento físico no seu sistema.

Eixo AXIS_CIP_DRIVE

O eixo AXIS_CIP_DRIVE é um eixo de movimento usado com inversores físicos para causar movimento físico no seu sistema conforme determinado pela sua aplicação.

Tipos de Configuração

Ao adicionar um eixo ao seu projeto, você precisa associar o eixo a um inversor. Entre outros parâmetros de configuração, você precisa selecionar um tipo de configuração. O tipo de configuração do eixo também é configurado o tipo de configuração do inversor.

Por exemplo, um eixo AXIS_CIP_DRIVE pode usar uma configuração Posição de malha e ser associado com um inversor Kinetix 350. O eixo é considerado como configurado em Posição de malha e o inversor associado é considerado como também configurado em Posição de malha.

Os seguintes inversores suportam estes tipos de configuração:

- Inversores Kinetix 350, Kinetix 5500, Kinetix 5700, e Kinetix 6500.
  - Malha de posição
  - Malha de velocidade
  - Malha de torque
- Inversores PowerFlex 527 e PowerFlex 755
  - Malha de posição
  - Malha de velocidade
  - Malha de torque
  - Controle de frequência

Número máximo de inversores configurados em malha de posição

Qualquer equipamento adicionado ao nó Ethernet local na configuração de E/S é contado para a limitação de nós do controlador. Consulte Nós em uma Rede EtherNet/IP na página 71 para obter mais informações.

Inversores são contados entre o número de nós na seção Configuração de E/S de um aplicativo Logix Designer. Se for utilizado o número máximo de inversores que um controlador Compact GuardLogix 5370 suporta em um único sistema, não é possível adicionar outros dispositivos EtherNet/IP àquele projeto.

Limites de Inversor configurado em Malha de Posição

Entre o número máximo de inversores suportados pelos controladores, existe um número máximo de inversores configurados como Posição de Malha suportados no projeto do controlador.

Por exemplo, o controlador 1769-L30ERMS suporta um máximo de quatro inversores configurados em Malha de Posição.

Tabela 30 lista informações de especificação relacionadas a movimento para os controladores que suportam Movimento Integrado em uma rede EtherNet/IP.

Tabela 30 – Controladores Compact GuardLogix 5370 que suportam movimento integrado na rede EtherNet/IP

Tipo do Controlador	Número de Inversores Suportados, máx.	Número de Inversores Configurados em Malha de Posição Suportados, máx.
1769-L30ERMS	16	4
1769-L33ERMS 1769-L33ERMOS	32	8
1769-L36ERMS 1769-L36ERMOS 1769-L37ERMOS(1)	48	16

(1) Disponível na versão do firmware 30.

Se a sua solução requerer mais do que 16 inversores configurados em Malha de Posição, considere usar a plataforma ControlLogix®. A plataforma ControlLogix permite até 100 inversores configurados em Malha de Posição.

Sincronização de tempo

O Movimento Integrado por meio de uma rede EtherNet/IP requer Sincronização de Tempo, também conhecida como CIP Sync. CIP Sync fornece sincronização precisa em tempo real (hora do mundo real) ou de Hora Universal Coordenada (UTC) de Controladores CompactLogix 5370 e equipamentos conectados por meio de uma rede EtherNet/IP.

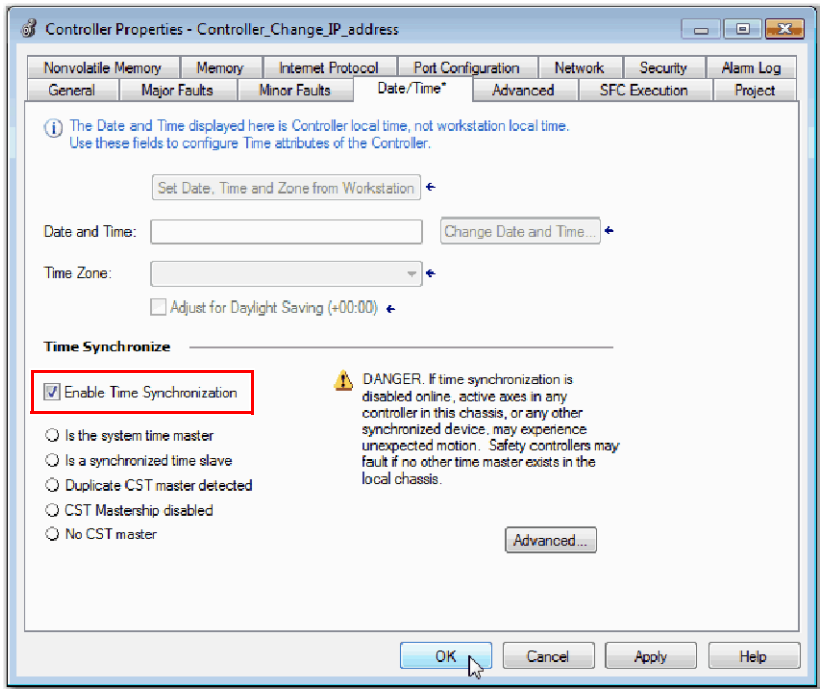
CIP Sync é um protocolo de sincronização de tempo que pode ser usado em diversas aplicações. Este capítulo concentra-se em usar o protocolo em aplicações com Movimento Integrado por meio de uma rede EtherNet/IP.

Todos os controladores e módulos de comunicação precisam ter sincronização de tempo habilitadas para participar de CIP Sync.

CIP Sync requer que equipamentos no sistema funcionem nos seguintes papéis:

- Grandmaster, também conhecido como mestre do tempo de sistema (CST) – Configura o tempo para o sistema todo e passa o tempo para um Mestre
- Mestre – Configura o tempo para o seu backplane
- Escravo – Usa o tempo configurado por um Mestre

Você pode habilitar a sincronização de tempo na guia data/tempo da caixa de diálogo Propriedades do Controlador.



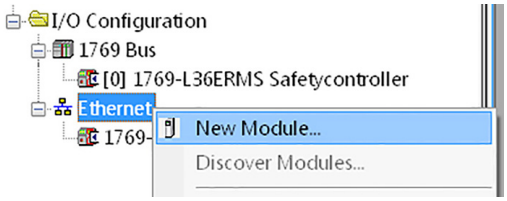
Configurar Movimento Integrado em uma rede EtherNet/IP

Configurar Movimento Integrado por meio de uma rede EtherNet/IP

IMPORTANTE Estas etapas mostram um controlador 1769-L36ERMS e uma unidade Kinetix 350. As mesmas etapas se aplicam para os controladores CompactLogix® 5370 e outros inversores que suportam Movimento Integrado por meio de uma rede EtherNet/IP:

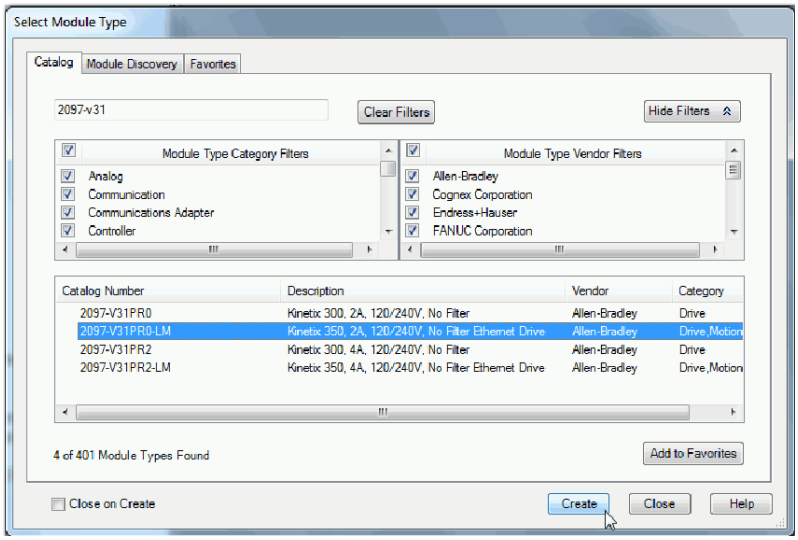
IMPORTANTE Esta seção assume que você já criou um projeto para o seu controlador 1769-L36ERMS e habilitou a sincronização de tempo no controlador. Se você não fez isso, faça antes de prosseguir.

1. Na árvore de configuração de E/S, clique com o botão direito na rede Ethernet e selecione Novo módulo.



A caixa de diálogo Selecionar tipo de Módulo aparecerá.

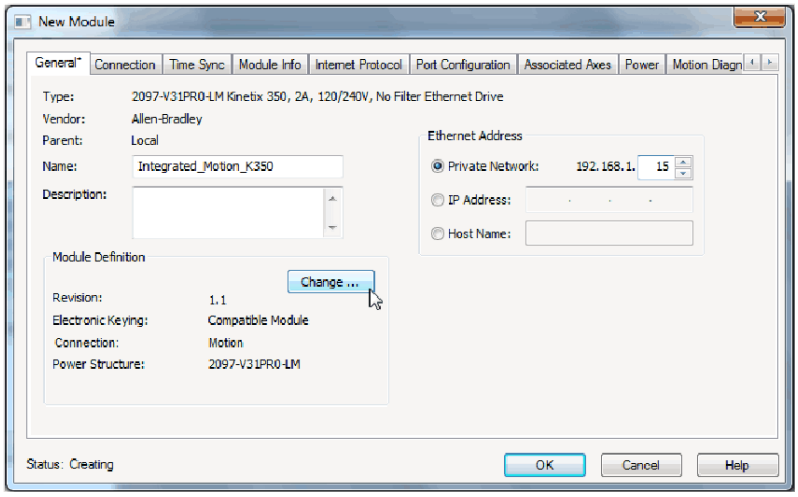
2. Selecione o inversor desejado e clique em Criar.



A caixa de diálogo Novo Módulo aparecerá.

3. Digite um nome para o módulo.
4. Digite uma descrição, se desejado.
5. Atribua um endereço de EtherNet/IP.

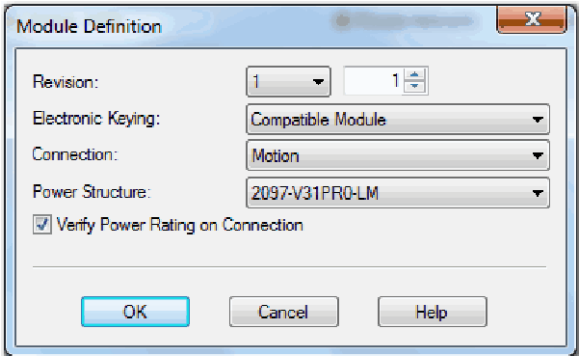
   Para obter informações sobre como configurar endereços IP, consulte as publicações para cada tipo de inversor listado em Recursos adicionais na página 12.



6. Se precisar alterar a configuração para qualquer parâmetro seguinte, clique em Alterar na área Definição de Módulo.
   - Revisão
   - Codificação eletrônica
   - Conexão

     Para unidades que suportam segurança e movimento em uma única conexão, é possível escolher Apenas Movimento, Movimento e Segurança ou Apenas Segurança.
   - Estrutura de alimentação
   - Verificar potência nominal na conexão

   A caixa de diálogo Módulo aparecerá.



7. Faça as alterações desejadas e clique em OK.
8. Clique em OK para criar o inversor no seu projeto.
9. Adicionar outros componentes necessários ao projeto.

Comunicação com o Controlador

Considerações

O software de programação determina se é possível entrar em comunicação com um controlador-alvo verificando se o projeto off-line é novo ou se ele sofreu alterações. Se o projeto for novo, será necessário primeiro fazer o download do projeto no controlador. Se ocorreram mudanças ao projeto, será solicitado para que você faça o upload ou o download. Caso contrário, será possível entrar em comunicação para monitorar a execução do projeto.

Vários fatores afetam esses processos, incluindo a função de correspondência entre o projeto e o controlador de, as falhas e o status de segurança, a existência de uma assinatura de tarefa de segurança e o status da trava/destravamento de segurança do projeto e do controlador do projeto e do controlador.

Função Correspondência entre o controlador e o projetor

A função Correspondência entre o projeto e o controlador afeta os processos de download, upload e a comunicação dos projetos padrão e de segurança.

Se a função Correspondência entre o projeto e o controlador estiver habilitada no projeto off-line, o software de programação compara o número de série do controlador no projeto off-line com o do controlador conectado. Se não corresponderem, é preciso cancelar o download/upload, conectar-se ao controlador correto ou confirmar se você está conectado ao controlador correto, o que atualizará o número de série no projeto para corresponder ao controlador alvo.

Revisão de Firmware Compatível

A Revisão de Firmware Compatível afeta o processo de download. Se a revisão do controlador não for compatível com a do projeto, será necessário atualizar o firmware do controlador. A aplicação Logix Designer lhe permite atualizar o firmware como parte da sequência de download se o controlador estiver desbloqueado de segurança.

IMPORTANTE	Para atualizar o firmware do controlador, instale primeiro um kit de atualização do firmware. Um kit de atualização vem acompanhado de um Cd suplementar, juntamente com o aplicativo Logix Designer.

DICA	Também é possível fazer a atualização do firmware escolhendo ControlFLASH™ a partir do menu Ferramentas no aplicativo Logix Designer.

Falhas/status de segurança

É permitido fazer o upload da lógica do programa e entrar em comunicação independentemente do status de segurança. As falhas e o status de segurança afetam somente o processo de download.

É possível visualizar o status de segurança na guia Segurança da caixa de diálogo Propriedades do controlador.

Assinatura de tarefa de segurança e status de bloqueio de segurança e desbloqueio de segurança

A existência de uma assinatura de tarefa de segurança e do status de trava e destravamento de segurança do controlador afeta os processos de upload e download.

No upload

Se o controlador tiver uma assinatura de tarefa de segurança, é feito o upload da assinatura da tarefa de segurança do status de bloqueio da tarefa de segurança com o projeto. Por exemplo, se o projeto no controlador estiver sem a trava de segurança, o projeto off-line permanece assim após o upload, mesmo se tiver sido bloqueado antes.

Após um upload, a assinatura da tarefa de segurança no projeto off-line corresponde com a assinatura da tarefa de segurança do controlador.

Em download

A existência de uma assinatura de tarefa de segurançae o status de trava de segurança do controlador determinam se um download pode ser feito ou não.

Tabela 31 – O efeito da trava de segurança e da assinatura de tarefa de segurança sobre a operação de download

Status da trava de segurança	Status da assinatura da tarefa de segurança	Funcionalidade de download
Controlador Desprotegido	A assinatura de tarefa de segurança no projeto off-line corresponde à do controlador.	Fez-se download de todos os componentes do projeto padrão. Os tags de segurança serão reinicializados com os valores da assinatura de tarefa de segurança criada. Não se fez download da tarefa de segurança. O status da trava de segurança combina com o status no projeto off-line.
	As assinaturas da tarefa de segurança não correspondem.	Se o controlador tiver uma assinatura da tarefa de segurança, ele é automaticamente excluído e se faz download de todo o projeto. O status da trava de segurança combina com o status no projeto off-line.
Controlador Protegido	As assinaturas da tarefa de segurança correspondem.	Se o projeto off-line e o controlador forem bloqueados por segurança, se faz download de todos os componentes-padrão do projeto e a tarefa de segurança é reiniciada com os valores de quando a assinatura da tarefa de segurança foi criada. Se o projeto off-line não estiver protegido, mas o controlador estiver, o download é bloqueado e é necessário primeiro desbloquear o controlador para permitir que o download continue.
	As assinaturas da tarefa de segurança não correspondem.	É necessário desproteger primeiro o controlador para permitir que o download continue. Se o controlador tiver uma assinatura da tarefa de segurança, ele é automaticamente excluído e se faz download de todo o projeto. O status da trava de segurança combina com o status no projeto off-line.

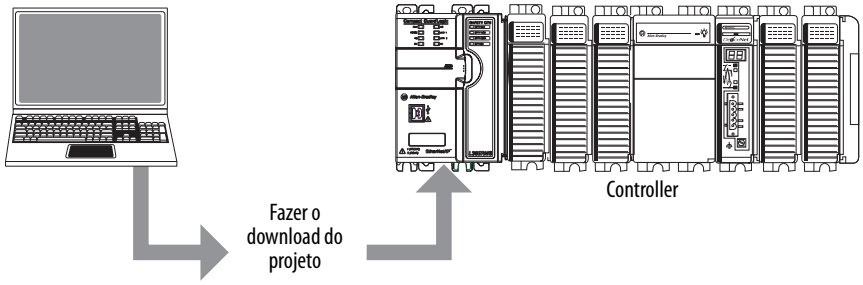
IMPORTANTE Durante o download para um controlador que está desbloqueado de segurança, caso o firmware no controlador seja diferente daquele no projeto off-line, faça um dos seguintes:

- Atualize o controlador para que combine com o projeto off-line. Uma vez que a atualização esteja concluída, se faz download de todo o projeto.
- Atualize o projeto para a versão do controlador.

Se atualizar o projeto, a assinatura da tarefa de segurança é excluída e o sistema precisa ser revalidado.

Download

Siga essas etapas para transferir o projeto do computador para o controlador.



1. Gire a chave seletora do controlador até REM.
2. Abra o projeto do controlador do que deseja fazer download.
3. Defina o caminho até o controlador.
   a. Clique em Quem está Ativo .
   b. Selecione o controlador.

      Para abrir um nível, clique no sinal +. Se já houver um controlador selecionado, verifique se é o correto.
4. Clique em Download.

   O software compara as seguintes informações no projeto off-line e no controlador:

   - número de série do controlador (se a função Projeto to para correspondência do controlador for selecionada)
   - firmware principal e revisões secundárias
   - status de segurança
   - assinatura da tarefa de segurança (caso exista uma)
   - status da trava de segurança

5. Siga as orientações nesta tabela para concluir o download com base na resposta do software.

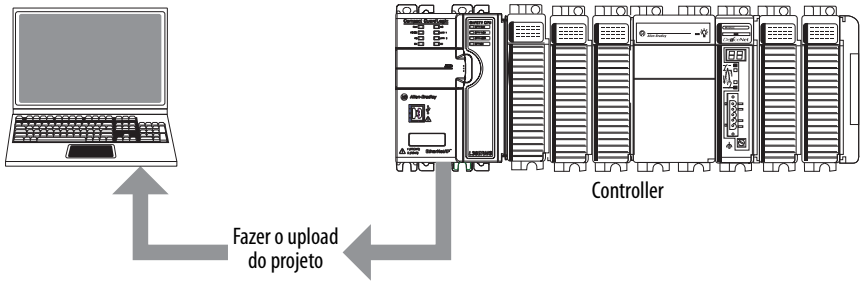
Se o software indicar	Então
Faça download para o controlador.	Escolha Download. O projeto faz o download para o controlador e o aplicativo Logix Designer entra online.
Não é possível fazer download no controlador. Diferença entre o projeto off-line e o número de série do controlador. O controlador selecionado pode ser o controlador errado.	Conecte-se ao controlador correto ou verifique se ele é o controlador correto. Se este for o controlador correto, marque a caixa de verificação Atualizar número de série do projeto para permitir que o download continue. O número de série do projeto será modificado para corresponder ao número de série do controlador.
Não é possível fazer download no controlador. A revisão principal do projeto off-line e o firmware do controlador não são compatíveis.	Escolha Atualizar firmware(1). Escolha a revisão necessária e clique em Update. Confirme a seleção clicando em Sim.
Não é possível fazer download para o controlador. O hardware do parceiro de segurança interno falhou.	Substitua o controlador.
Não é possível fazer download no controlador. A atualização do firmware do controlador está incompleta.	Escolha Atualizar Firmware(1). Escolha a revisão necessária e clique em Update. Confirme a seleção clicando em Sim.
Não é possível fazer download para o controlador. A parceria de segurança não foi estabelecida.	Cancele este processo de download e tente outra vez.
Não é possível fazer download para o controlador. A assinatura da tarefa de segurança incompatível não pode ser excluída enquanto o projeto estiver com trava de segurança.	Cancele o download. Para fazer download do projeto, é preciso desbloquear com segurança o projeto off-line, excluir a assinatura da tarefa de segurança e fazer o download do projeto. **IMPORTANTE:** O sistema de segurança requer revalidação.
Não é possível fazer download de uma maneira que preserve a assinatura da tarefa de segurança. A revisão secundária do firmware do controlador não é compatível com a assinatura da tarefa de segurança no projeto off-line.	• Se a revisão secundária de firmware for incompatível, para preservar a assinatura de segurança, atualize a revisão do firmware no controlador para corresponder exatamente ao projeto off-line. Em seguida, faça download do projeto off-line. • Para continuar a fazer download apesar da incompatibilidade da assinatura da tarefa de segurança, clique em Download. A assinatura da tarefa de segurança é excluída. **IMPORTANTE:** O sistema de segurança requer revalidação.
Não é possível fazer download para o controlador. O controlador está bloqueado. As assinaturas da tarefa de segurança do projeto off-line e o controlador não correspondem.	Escolha Desbloquear. A caixa de diálogo Desbloquear em segurança para download é exibida. Se a caixa de seleção Excluir Assinatura estiver marcada e você escolher Desbloquear, será necessário confirmar a remoção selecionando Sim.
Irá ocorrer uma falha de segurança não recuperável no controlador de segurança. Não existe um mestre designado no tempo de sistema coordenado (CST).	Selecione Habilitar sincronização do tempo e clique em Download para continuar.

(1) O controlador deve estar desbloqueado de segurança.

Seguindo um download bem-sucedido, o status da trava de segurança e a assinatura de tarefa de segurança do controlador correspondem ao projeto que foi baixado. Os dados de segurança serão inicializados com os valores existentes no momento em que a assinatura da tarefa de segurança foi criada.

Fazer o upload

Siga essas etapas para transferir o projeto do controlador para o computador.



1. Defina o caminho até o controlador.
   a. Clique em Quem está Ativo .
   b. Selecione o controlador.
   Para expandir um nível, clique no sinal +. Se já houver um controlador selecionado, verifique se é o correto.
2. Clique em Upload.
3. Se o arquivo não existir, selecione Arquivo>Selecionar>Sim
4. Caso contrário, selecione-o.

   Se a função Correspondência entre o projeto e o controlador estiver habilitada no projeto off-line, o software de programação compara o número de série do controlador no projeto off-line com o do controlador conectado.

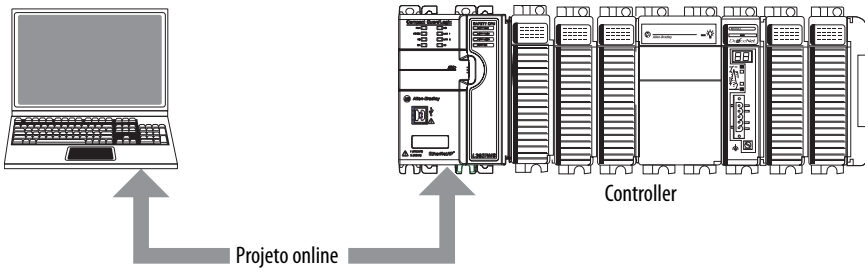
   Se os números de série do controlador não forem compatíveis, pode-se fazer um dos seguintes:
   - Cancele o upload e conecte-se a um controlador compatível. Em seguida, reinicie o procedimento de upload.
   - Selecione um novo projeto do que a ser feito upload ou selecione outro escolhendo Selecionar arquivo.
   - Atualize o número de série do projeto para casar com o do controlador marcando a caixa de seleção Atualizar o número de série do projeto e escolhendo Upload.
5. O software verificará se o projeto aberto corresponde ao do controlador.
   a. Se não forem, será necessário selecionar um arquivo correspondente ou cancelar o processo de upload.
   b. Se forem, o software verificará se há alterações no projeto off-line (aberto).
6. O software verifica mudanças no projeto off-line.
   a. Se não houver, será possível entrar em comunicação sem fazer upload. Clique em Ir Online.
   b. Se houver alterações no projeto aberto que não existam no controlador, será possível optar entre fazer upload do projeto, cancelar o upload ou selecionar um arquivo diferente.

Se você escolher Upload, se fará upload das aplicações padrão e de segurança. Caso haja uma assinatura de tarefa de segurança, também se fará upload dela. O status Bloqueio de segurança do projeto refletirá o status original do projeto on-line (controlador).

DICA Antes de fazer upload, se existir uma assinatura de tarefa de segurança ou o projeto off-line estiver protegido, mas o controlador estiver desprotegido ou não tiver assinatura, a assinatura de tarefa de segurança off-line e o estado de proteção serão substituídos por valores on-line (desprotegido sem assinatura de tarefa de segurança). Se você não quiser realizar alterações permanentes, não salve o projeto off-line após o upload.

Entrar On-line

Siga essas etapas para ficar on-line para monitorar um projeto executado pelo controlador.



1. Defina o caminho até o controlador.
   a. Clique em Quem está Ativo .
   b. Selecione o controlador.
   Para expandir um nível, clique no sinal +. Se já houver um controlador selecionado, verifique se é o correto.
2. Clique em Ir Online.

   As verificações do software são as seguintes:
   - Os números de série do projeto off-line e do controlador combinam (se a função Projeto para correspondência do controlador estiver selecionada)?
   - O projeto off-line contém alterações não existentes no projeto do controlador?
   - As revisões do projeto off-line e do firmware do controlador combinam?
   - O projeto off-line ou o controlador estão protegidos com trava de segurança?
   - O projeto off-line e o controlador têm assinaturas de tarefas de segurança compatíveis?

3. Siga as orientações na tabela abaixo para conectar ao controlador.

Tabela 32 – Conexão com o controlador

Se o software indicar	Então
Não é possível conectar-se ao controlador. Diferença entre o projeto off-line e o número de série do controlador. O controlador selecionado pode ser o controlador errado.	Conecte-se ao controlador correto, selecione outro arquivo de projeto diferente ou escolha a caixa de seleção Atualizar número de série do projeto … e escolha Go Online… para conectar-se ao controlador e atualizar o número de série do projeto off-line para que corresponda ao do controlador.
Não é possível conectar-se ao controlador. A revisão do projeto off-line e o firmware do controlador não são compatíveis.	Selecione uma das seguintes opções: • Escolha Update firmware. Escolha a revisão necessária e clique em Update. Confirme a seleção clicando em Sim. **IMPORTANTE:** O projeto online é excluído. • Para preservar o projeto online, cancele o processo online e instale uma versão do aplicativo Logix Designer compatível com a revisão do firmware do controlador.
É preciso fazer upload ou download para ficar on-line usando o projeto aberto.	Selecione uma das seguintes opções: • fazer upload para atualizar o projeto off-line. • fazer download para atualizar o projeto do controlador. • Escolher Selecionar arquivo para selecionar outro projeto off-line.
Não é possível conectar-se de uma maneira que preserve a assinatura da tarefa de segurança. A revisão secundária do firmware do controlador não é compatível com a assinatura da tarefa de segurança no projeto off-line.	• Para manter a assinatura de tarefa de segurança quando a revisão secundária de firmware não corresponder, atualize a revisão de firmware no controlador para uma idêntica ao projeto off-line. Em seguida, entre em comunicação com o controlador. • Para continuar a fazer download apesar da incompatibilidade da assinatura da tarefa de segurança, clique em Download. A assinatura da tarefa de segurança é excluída. **IMPORTANTE:** O sistema de segurança requer revalidação.
Não é possível conectar-se ao controlador. A assinatura da tarefa de segurança incompatível não pode ser excluída enquanto o projeto estiver com trava de segurança.	Cancele o processo on-line. É necessário desproteger o projeto off-line antes de tentar entrar em comunicação.

Seguindo um download bem sucedido, a trava de segurança e a assinatura de tarefa de segurança do controlador correspondem ao projeto que foi baixado. O status bloqueio de segurança e a assinatura de tarefa de segurança do projeto off-line são substituídos pelo controlador. Se você não quiser que as alterações no projeto off-line sejam permanentes, não salve o arquivo do projeto após o processo de entrar em comunicação.

Monitorar o Status e Controlar Falhas

Consulte Apêndice A, Indicadores de status para obter informações sobre interpretações dos indicadores de status do controlador.

Visualizando o status via barra on-line

A barra on-line exibe informações sobre o projeto e o controlador, inclusive o status do controlador, o status de force, o status de edição on-line e o status de segurança.

Figura 39 – Botões de status

Quando o botão Status do controlador é selecionado conforme exibido anteriormente, a barra on-line exibe o modo do controlador (RUN) e o status (OK). O indicador da E/S corresponde ao status da E/S padrão e de segurança e se comporta da mesma forma que o indicador de status no controlador. A E/S com o status de erro mais importante é exibida próxima ao indicador de status.

Quando o botão Status de segurança é selecionado conforme exibido abaixo, a barra on-line exibe a assinatura da tarefa de segurança.

Figura 40 – Tela on-line de assinatura de segurança

O próprio botão de status de segurança indica se o controlador está protegido ou não, ou com falha. Ele exibe também um ícone que mostra o status de segurança.

Tabela 33 – Ícone de status de segurança

Se o status de segurança for	Este ícone será exibido
Tarefa de segurança OK.	
Tarefa de segurança inoperável.	
Segurança não disponível.	
Off-line.	

Os ícones ficam verdes quando o controlador está protegido, amarelos quando o controlador está desprotegido e vermelhos quando o controlador apresenta falha na segurança. Quando existe uma assinatura de tarefa de segurança, o ícone inclui uma pequena marca de verificação  .

Monitore conexões

É possível monitorar o status das conexões padrão e de segurança.

Todas as conexões

Se a comunicação com um dispositivo na configuração de E/S do controlador não ocorrer em 100 ms, o tempo-limite de comunicação acaba e o controlador produz as advertências a seguir:

- Um código de estado de falha de E/S é indicado no display de status do controlador Compact GuardLogix® 5370.
- O indicador de E/S na frente do controlador piscará em verde.
- Um símbolo de alerta ⚠ aparecerá sobre a pasta configuração de E/S e sobre o dispositivo que atingiu o tempo-limite.
- Uma falha de módulo é produzida, que pode ser acessada através da guia Conexões da caixa de diálogo Propriedades do módulo para o módulo ou pela instrução GSV.

ATENÇÃO: A E/S de segurança e as conexões produzidas/consumidas não podem ser configuradas para causar uma falha automaticamente no controlador quando uma conexão for perdida. Portanto, é preciso monitorar falhas de conexão para assegurar que o sistema de segurança mantenha a integridade SIL 3/PLe.

Consulte Conexões de segurança na página 177.

Conexões de segurança

Para as tags associadas a dados de segurança produzidos ou consumidos, é possível monitorar o status de conexões de segurança por meio do membro CONNECTION_STATUS. Para monitorar conexões de entrada e saída, os tags de E/S de segurança contêm um membro de status de conexão denominado SafetyStatus. Os dois tipos de dados contêm dois bits: RunMode e ConnectionFaulted.

O valor RunMode indica se os dados consumidos estão sendo ativamente atualizados por um dispositivo que está no Modo de operação (1) ou Estado inativo (0). Estado inativo será indicado se a conexão for fechada, se houver falha na Tarefa de Segurança ou o controlador ou dispositivo remoto estiver no modo programa ou modo teste.

O valor ConnectionFaulted indica se a conexão de segurança entre o produtor e o consumidor de segurança está Válida (0) ou Com Falha (1). Se ConnectionFaulted for definido como Faulted (1) em decorrência de uma perda de conexão física, os dados de segurança serão zerados.

A tabela a seguir descreve as combinações dos estados RunMode e ConnectionFaulted.

Tabela 34 – Status da conexão de segurança

Status RunMode	Status ConnectionFaulted	Operação de conexão de segurança
1 = Execução	0 = Válido	Dados ativamente controlados por um dispositivo em produção, No modo de operação.
0 = Inativo	0 = Válido	Conexão ativa e dispositivo em produção no estado Inativo. Dados de segurança zerados.
0 = Inativo	1 = Falha	Conexão de segurança apresenta falha. Estado do dispositivo em produção desconhecido. Dados de segurança zerados.
1 = Execução	1 = Falha	Estado inválido.

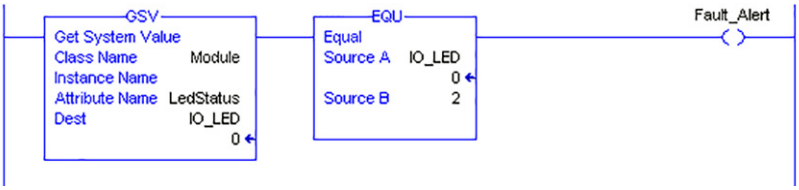
Se um módulo está inibido, o bit ConnectionFaulted é definido como Com Falha(1) e o bit RunMode como Inativo (0) para cada conexão associada ao módulo. Como resultado, os dados consumidos de segurança são zerados.

Determinar se a comunicação de E/S atingiu o tempo-limite

Este exemplo pode ser usado com os Controladores Compact GuardLogix 5370

- A instrução GSV obtém o status do indicador de status de E/S (através do atributo LEDStatus do objeto do Módulo), armazenando-o no tag IO_LED.
- IO_LED é um tag DINT que armazena o status do indicador de status de E/S ou display de status na frente do controlador.
- Se IO_LED for igual a 2, em ao menos uma conexão de E/S foi perdida e Fault_Alert é definido.

Figura 41 – GSV usada para identificar tempo-limite de E/S



Para obter mais informações sobre atributos disponíveis com o objeto Módulo, consulte o Manual de referência de instruções dos controladores Logix, publicação 1756-RM009.

Determinar se a comunicação de E/S atingiu o tempo-limite

Se a comunicação com um dispositivo (módulo) na configuração de E/S do controlador expirar, o controlador produz um código de falha e uma informação de falha para o módulo. É possível utilizar instruções GSV para obter código de falhas e informações através dos atributos FaultCode e FaultInfo do objeto Módulo.

Para obter mais informações sobre atributos disponíveis com o objeto Módulo, consulte o Manual de referência de instruções dos controladores Logix, publicação 1756-RM009.

Monitorar flags de status

Os controladores Logix, incluindo os controladores Compact GuardLogix, oferecem suporte a palavras-chave de status que podem ser usadas na sua lógica para monitorar eventos específicos.

Para obter mais informações sobre como usar estas palavras-chave, consulte o Manual de programação de status e informações de controlador dos controladores Logix5000™, publicação 1756-PM015.

Monitorar o status do segurança

Visualizar o status de segurança no botão de status de segurança na barra on-line na guia Segurança da caixa de diálogo Propriedades do Controlador.

Figura 42 – Status da tarefa de segurança

Os valores possíveis para o status de segurança são:

- Parceiro de segurança não disponível.
- Firmware de segurança incompatível
- Tarefa de segurança inoperável.
- Tarefa de segurança OK.

Com exceção de "Tarefa de segurança OK", as descrições indicam que existem falhas de segurança irrecuperáveis.

Consulte Falhas graves de segurança (Tipo 14) na página 181 para ver os códigos de falha e as ações corretivas.

Falhas do controlador

As falhas no sistema Compact GuardLogix podem ser falhas irrecuperáveis do controlador, falhas irrecuperáveis de segurança no aplicativo de segurança ou falhas recuperáveis de segurança no aplicativo de segurança.

Falhas irrecuperáveis do controlador

Ocorrem quando o diagnóstico interno do controlador falha. Se ocorrer uma falha irrecuperável do controlador, a execução da tarefa de segurança é interrompida e os módulos de E/S CIP Safety são colocados no estado seguro. A recuperação requer que você faça download do programa aplicativo novamente.

Falhas de segurança irrecuperáveis na aplicação de segurança

Se ocorrer uma falha de segurança irrecuperável na aplicação de segurança, a lógica de segurança e o protocolo de segurança são terminados. Falhas de watchdog da tarefa de segurança entram nesta categoria.

Quando a tarefa de segurança encontrar uma falha de segurança irrecuperável que for removida de forma programática no Manipulador de falhas do controlador, a aplicação padrão continuará a ser executada.

ATENÇÃO: O cancelamento da falha de segurança não a apaga! Se a falha de segurança for cancelada, será sua responsabilidade provar que este procedimento manterá a operação segura.

Será necessário fornecer a prova à sua agência de certificação que permitirá que parte do sistema continue a funcionar mantendo a operação segura.

Se a assinatura da tarefa de segurança existir, você precisa apenas limpar a falha para habilitar a operação da tarefa de segurança. Se não existir uma assinatura da tarefa de segurança, a tarefa de segurança não pode ser executada novamente até se fazer download da aplicação inteira outra vez.

Falhas recuperáveis na aplicação de segurança

Se ocorrer uma falha recuperável na aplicação de segurança, o sistema pode ou não parar a execução da tarefa de segurança, dependendo se a falha foi ou não controlada pelo Manipulador de Falhas do Programa na aplicação de segurança.

Quando uma falha recuperável for apagada de forma programática, a tarefa de segurança pode continuar a ser executada sem interrupção.

Quando uma falha recuperável não for removida na aplicação de segurança de forma programática, ocorre uma falha de segurança recuperável tipo 14, código 2. A execução do programa de segurança é interrompida e as conexões do protocolo de segurança são fechadas e reabertas para reiniciá-las. Saídas de segurança são colocadas no estado seguro e o produtor de tags consumidos de segurança comanda os consumidores para colocá-los em um estado seguro, também.

As falhas recuperáveis permitem editar a aplicação padrão e de segurança conforme necessário para corrigir a causa da falha. No entanto, se existir uma assinatura de tarefa de segurança ou o controlador estiver protegido, será necessário desprotegê-lo primeiro e remover a Assinatura de Segurança antes de ser possível editar a aplicação de segurança.

Visualização de falhas

A caixa de diálogo falhas recentes na guia Falhas Graves na caixa de diálogo Propriedades do controlador contém duas subguias, uma para falhas-padrão e outra para falhas de segurança.

Códigos de Falhas

Tabela 35 mostra os códigos de falha específicos para Compact GuardLogix controladores. O tipo e o código correspondem ao tipo e ao código exibidos na guia Falhas graves da caixa de diálogo Propriedades do controlador e no objeto PROGRAM, atributo MAJORFAULTRECORD (ou MINORFAULTRECORD).

Tabela 35 – Falhas graves de segurança (Tipo 14)

Código	Causa	Status	Ação Corretiva
01	Watchdog da tarefa expirado. Tarefa do usuário não foi concluída em um período especificado. Um erro de programa causou uma malha infinita, o programa é muito complexo para ser executado na rapidez especificada, uma tarefa de prioridade mais alta impede a conclusão desta tarefa.	Irrecuperável	Apague a falha. Se existir uma assinatura de tarefa segura, a memória de tarefa é reiniciada e a tarefa começa a executar. Caso contrário, é necessário fazer download novamente do programa para permitir a execução da tarefa de segurança novamente.
02	Existe um erro em uma rotina da tarefa de segurança.	Recuperável	Corrija o erro na lógica do programa do usuário.
07	Tarefa de segurança inoperante. Esta falha ocorre quando a lógica de segurança é inválida, por exemplo, um tempo limite de watchdog ocorreu ou a memória está corrupta.	Irrecuperável	Apague a falha. Se existir uma assinatura de tarefa de segurança, a memória de segurança será reinicializada por meio da assinatura e a tarefa de segurança será executada. Caso contrário, é necessário fazer download novamente do programa para permitir a execução da tarefa de segurança.
08	Tempo de sistema (CST) não localizado.	Irrecuperável	Apague a falha. Configure um dispositivo para ser o CST principal.

O Manual de programação de falhas graves e secundárias dos controladores Logix5000, publicação 1756-PM014, contém descrições dos códigos de falha comuns aos controladores Logix.

Desenvolvimento de uma rotina de falha

Se ocorrer uma condição de falha que seja grave o bastante para desligar o controlador, este gera uma falha grave e para a execução da lógica.

De acordo com a aplicação, pode ser que você não queira que todas as falhas de segurança desliguem o sistema inteiro. Nessa situação, é possível usar uma rotina de falha para apagar uma falha específica e permitir que parte do controle padrão do sistema continue a funcionar ou configurar algumas saídas para permanecerem ativas.

ATENÇÃO: Será necessário fornecer a prova à sua agência de certificação que permitirá que parte do sistema continue a funcionar mantendo a operação segura.

O controlador suporta dois níveis de manuseio de falhas graves:

- rotina de falha do programa
- manipulador de falhas do controlador

As duas rotinas podem utilizar instruções GSV e SSV conforme descrito na página 182.

Rotina de falha do programa

Cada programa pode ter sua própria rotina de falha. O controlador a executa quando ocorre uma falha de instrução. Se a rotina de falha do programa não apagar a falha ou se não existir, o controlador continuará a executar o manipulador de falhas do controlador, caso exista um.

Manipulador de falhas do controlador

O manipulador de falha do controlador é um componente opcional que é executado quando a rotina de falha do programa não pode limpar a falha ou não existe.

É possível criar somente um programa para o manipulador de falhas do controlador. Depois de criado, é necessário configurar uma rotina como a principal.

O Manual de programação de falhas graves e secundárias dos controladores Logix5000, publicação 1756-PM014, contém detalhes sobre a criação e teste de rotinas de falha.

Usar instruções GSV/SSV

Os controladores Logix armazenam dados do sistema em objetos, e não em arquivos de status. É possível utilizar as instruções GSV (Obter valor do sistema) e SSV (Definir valor do sistema) para recuperar e definir dados do controlador.

A instrução GSV recupera as informações especificadas e as coloca no destino especificado. A instrução SSV altera o atributo especificado com dados na fonte da instrução. Ao inserir uma instrução GSV ou SSV, o software de programação exibe as classes e os nomes de objetos e os nomes de atributos válidos para cada instrução.

Para tarefas padrão, é possível usar a instrução GSV para obter os valores dos atributos disponíveis. Ao utilizar a instrução SSV, o software exibe somente os atributos que podem ser definidos.

Para a tarefa de segurança, as instruções GSV e SSV são mais restritas. Observe que as instruções SSV em tarefas padrão e de segurança não podem energizar o bit 0 (falha grave em erro) no atributo do modo de um módulo de E/S de segurança.

Para objetos de segurança, a Tabela 36 mostra para quais atributos podem-se obter valores usando a instrução GSV e quais podem ser ajustados por meio da instrução SSV em tarefas de segurança e padrão.

ATENÇÃO: Utilize as instruções GSV/SSV com cuidado. Fazer alterações em objetos pode causar uma operação inesperada do controlador ou ferimentos pessoais.

Tabela 36 – Possibilidade de Acesso GSV/SSV

Objeto de Segurança	Nome do Atributo	Tipo de dados	Descrição do Atributo	Acessível da Tarefa de Segurança		Acessível de Tarefas Padrão	
				GSV	SSV	GSV[4]	SSV
Tarefa de segurança	Instância	DINT	Fornece o número de instâncias deste objeto de tarefa. Os valores válidos são de 0 a 31.	X		X	
	MaximumInterval	DINT[2]	O intervalo máximo entre execuções sucessivas desta tarefa.			X	X
	MaximumScanTime	DINT	Tempo de execução máximo registrado (ms) para esta tarefa.			X	X
	MinimumInterval	DINT[2]	O intervalo mínimo entre execuções sucessivas desta tarefa.			X	X
	Prioridade	INT	Prioridade relativa desta tarefa em comparação com outras. Os valores válidos são de 0 a 15.	X		X	
	Rate	DINT	Período (em ms) ou valor de tempo-limite da tarefa (em ms).	X		X	
	Watchdog	DINT	Limite de tempo (em ms) para execução de todos os programas associados e esta tarefa.	X		X	
Programa de Segurança	Instância	DINT	Fornece o número de instâncias do objeto do programa.	X		X	
	MajorFaultRecord[1]	DINT[11]	Registra falhas graves neste programa.	X	X	X	
	MaximumScanTime	DINT	Tempo de execução máximo registrado (ms) neste programa.			X	X
Rotina de Segurança	Instância	DINT	Fornece o número de instâncias deste objeto de rotina. Os valores válidos são de 0 a 65,535.	X			
Controlador de Segurança	SafetyLocked	SINT	Indica se o controlador está protegido ou não.	X		X	
	SafetyStatus[2]	INT	Especifica o status de segurança conforme o seguinte: • tarefa de segurança OK. (1000000000000000) • tarefa de segurança inoperável. (1000000000000001) • firmware incompatível. (0000000000000011)			X	
	SafetySignatureExists	SINT	Indica se há ou não a assinatura de tarefa de segurança.	X		X	
	SafetySignatureID	DINT	Número de identificação de 32 bits.			X	
	SafetySignature	String[3]	Número de identificação de 32 bits.			X	
	SafetyTaskFaultRecord[1][2]	DINT[11]	Registra as falhas da Tarefa de Segurança.			X	
AOI (Segurança)	LastEditDate	LINT	Registro de data e hora da última edição de uma definição de instrução adicional.			X	
	SignatureID	DINT	Número de ID.			X	
	SafetySignatureID	DINT	Número de identificação de 32 bits.			X	

(1) Consulte Acessar os atributos FaultRecord na página 184 para obter informações sobre como acessar este atributo.
(2) Consulte Capturar informações sobre a falha na página 184 para obter informações sobre como acessar este atributo.
(3) Comprimento = 37.
(4) Na tarefa-padrão, a possibilidade de acesso GSV a atributos do objeto de segurança é igual à possibilidade de atributos do objeto-padrão.

Acessar os atributos FaultRecord

Criar uma estrutura definida pelo usuário para simplificar o acesso aos atributos MajorFaultRecord e SafetyTaskFaultRecord.

Tabela 37 – Parâmetros para acessar os atributos FaultRecord

Nome	Tipo de dados	Estilo	Descrição
TimeLow	DINT	Decimal	32 bits inferiores do valor do registro de data e hora da falha
TimeHigh	DINT	Decimal	32 bits superiores do valor do registro de data e hora da falha
Tipo	INT	Decimal	Tipo de falha (programa, E/S ou outro)
Código	INT	Decimal	Código exclusivo para esta falha (depende do tipo de falha)
Informação	DINT[8]	Hexadecimal	Informação específica da falha (depende do tipo de falha e código)

Para obter mais informações sobre como usar as instruções GSV e SSV, consulte o capítulo de instruções de E/S no Manual de referência de instruções dos controladores Logix, publicação 1756-RM009.

Capturar informações sobre a falha

Os atributos SafetyStatus e SafetyTaskFaultRecord podem captar informações sobre falhas irrecuperáveis. Use uma instrução GSV no manipulador de falhas do controlador para capturar e armazenar as informações da falha. A instrução GSV pode ser utilizada em uma tarefa padrão juntamente com uma rotina do manipulador de falhas do controlador que remove as falhas e deixa as tarefas padrão continuarem a execução.

Guardar e carregar programas com um cartão Secure Digital

IMPORTANTE A expectativa de vida de mídia flash é altamente dependente do número de ciclo de gravações que são realizados. Mídia não volátil utiliza uma técnica de nivelamento de utilização, ou tecnologia para prolongamento do tempo de serviço, mas deve-se evitar gravações frequentes.

Evitar gravações frequentes quando carregar os dados Recomendamos que você grave dados em um buffer na memória do seu controlador e limite o número de gravações dos dados na mídia removível.

Usando cartões de memória para memórias não voláteis

Compact GuardLogixControladores ®5370 suportam um cartão Secure Digital (SD) para memória não volátil:

- Cartão 1784-SD1 – Sai de fábrica com o controlador CompactLogix 5370 e oferece 1 GB de memória Você pode pedir cartões 1784-SD1 adicionais se desejar.
- Cartão 1784-SD2 – Disponível para compra em separado e oferece 2 GB de memória

A memória não volátil permite que você mantenha uma cópia do projeto no controlador. O controlador não precisa de alimentação ou bateria para manter a cópia.

É possível carregar o projeto armazenado a partir da memória não volátil na memória do usuário do controlador

- A cada energização.
- Sempre que não houver projeto no controlador e ele for energizado
- A qualquer momento, por meio do software de programação

IMPORTANTE A memória não volátil armazena os conteúdos da memória do usuário no momento em que o projeto é armazenado

- As alterações feitas após armazenar o projeto não são refletidas na memória não volátil.
- Se fizer alguma mudança ao projeto, mas não armazená-las, elas serão substituídas quando carregar o projeto da memória não volátil. Se isso acontecer, você deve fazer upload ou download do projeto para entrar em comunicação.
- Se quiser armazenar as mudanças como edições on-line, valores de tags ou o programa da rede ControlNet, armazene o projeto novamente depois de fizer as mudanças.

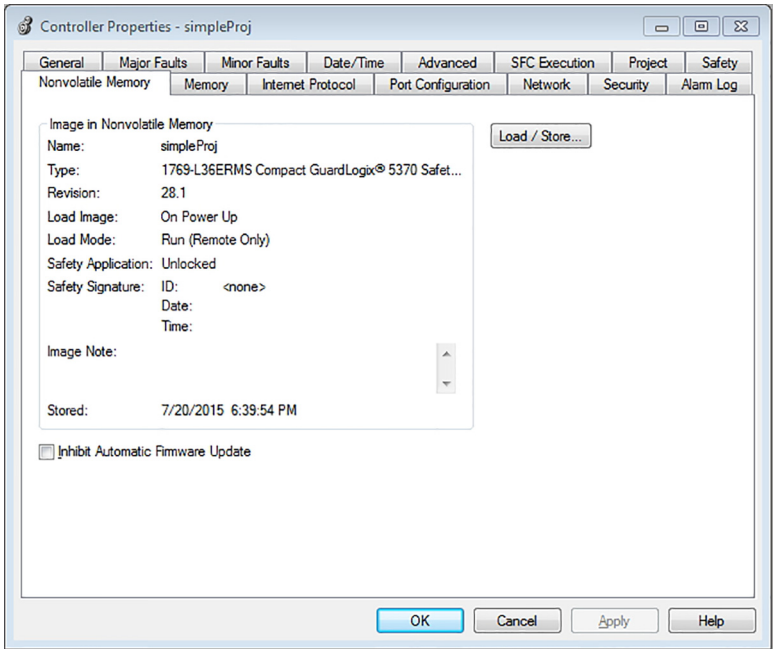
ATENÇÃO: Não remova o cartão SD enquanto o controlador estiver lendo ou gravando nele, como indicado por um indicador de status SD piscando em verde. Isso pode corromper os dados no cartão ou no controlador, além de corromper o firmware mais recente no controlador. Deixe o cartão no controlador até que o indicador de status OK fique verde e sem piscar.

ADVERTÊNCIA: Ao inserir ou remover o cartão SD enquanto a alimentação estiver ligada, um arco elétrico pode ocorrer. Isto pode causar uma explosão em instalações reconhecidas como área classificada.

Antes de continuar, certifique-se de que não haja energia ou que a área não apresenta risco

Se um cartão SD estiver instalado, você pode ver seu conteúdo na guia de Memória não volátil da caixa de diálogo de Propriedades do Controlador. Se uma aplicação de segurança for armazenada no cartão, o status de bloqueio por segurança e a assinatura da tarefa de segurança aparecem.

Figura 43 – Guia Nonvolatile Memory



Para obter informações detalhadas sobre a utilização de memória não volatil, consulte o Manual de programação me memória não volátil dos controladores Logix5000, publicação 1756-PM017.

Armazenamento de um projeto de segurança

Não é possível armazenar um projeto de segurança, caso o status da tarefa seja tarefa de segurança inoperável. Quando você armazena um projeto de segurança, o firmware do controlador fica guardado no cartão SD.

Se não existir nenhuma aplicação no controlador, é possível salvar somente o firmware do controlador de segurança somente se houver uma parceria válida. Uma carga de firmware somente não irá apagar a condição inoperável da tarefa de segurança.

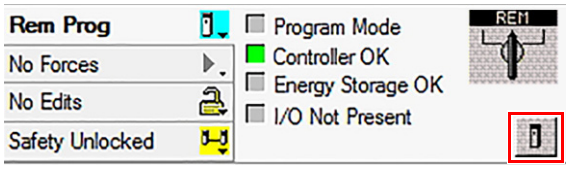
Se existe uma assinatura de tarefa de segurança quando você salva um projeto, ocorre o seguinte:

- As tags de segurança armazenadas com o valor da assinatura criada.
- As tags padrão são atualizadas.
- A assinatura atual da tarefa de segurança é salva.

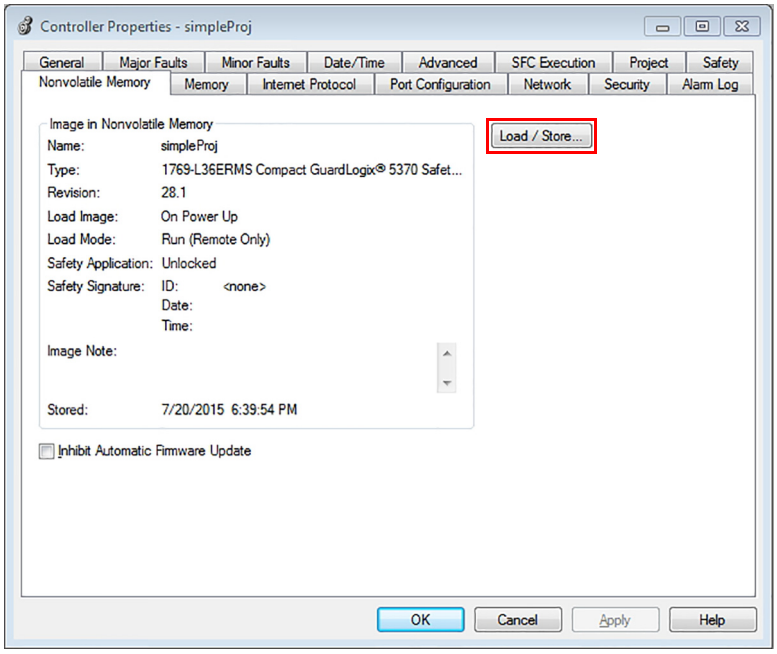
Ao armazenar um projeto de aplicação de segurança em um cartão de memória, recomendamos selecionar Programa (somente remoto) e também o modo carregar, isto é, o modo em que o controlador deve entrar após a carga. Consulte Carregamento de um projeto de segurança na página 190 para obter mais informações.

Siga estas etapas para armazenar um projeto.

1. Comunicação com o Controlador
2. Coloque o controlador em modo de Programa, ou seja, Programa Remoto ou Programa.
3. Na barra de ferramentas Online, clique no ícone Propriedades do controlador.



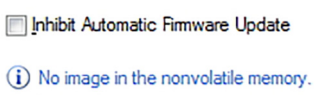
4. Clique na guia Nonvolatile Memory.
5. Clique em Load/Store.



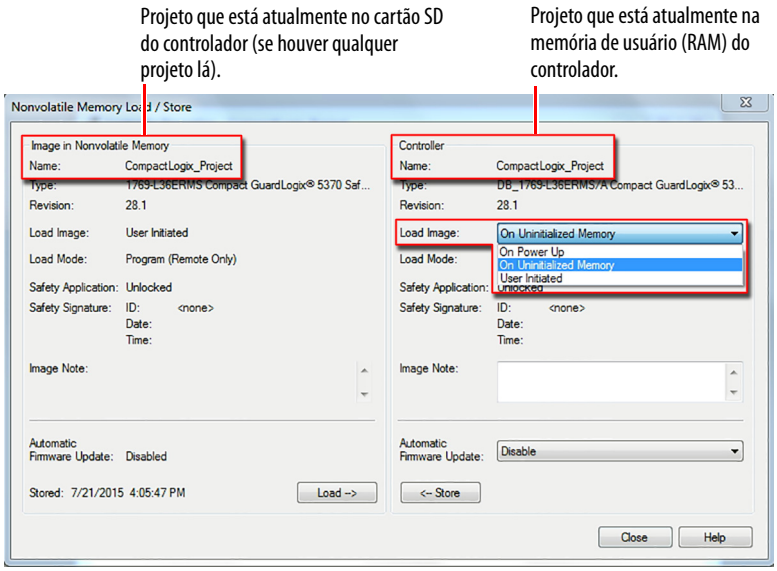
DICA Se Load/Store estiver apagado (indisponível), verifique o seguinte:

- Que você tenha especificado o caminho de comunicação correto e esteja online com o controlador.
- O cartão SD está instalado.

Se o cartão de memória não estiver instalado, uma mensagem no canto inferior esquerdo da guia Memória não volátil indica a falta do cartão, conforme exibido aqui.

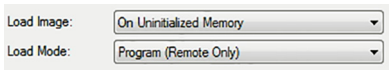


6. Escolha sob quais condições carregar um projeto na memória do usuário do controlador.



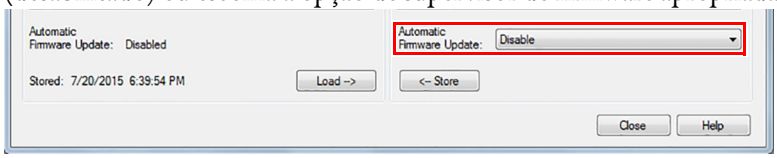
Se você escolher Na inicialização ou Na memória corrompida, você precisa escolher também o modo para o qual você quer que o controlador vá após o carregamento:

- Programa (somente remoto)
- Operação (somente remota)



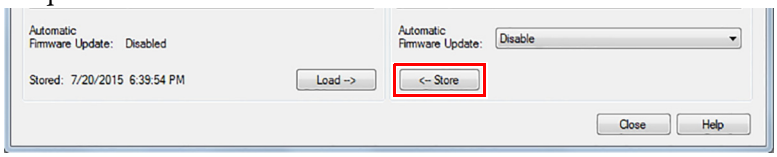
DICA Ao armazenar um projeto de aplicação de segurança em um cartão de memória, recomendamos selecionar Programa (somente remoto) e também o modo carregar, isto é, o modo em que o controlador deve entrar após a carga.

7. Na caixa Atualização de firmware automática, use o padrão (desabilitado) ou escolha a opção de supervisor de firmware apropriada.



IMPORTANTE A opção Firmware Supervisor não é utilizada para atualizar o firmware do controlador.

8. Clique em Atualizar.



IMPORTANTE Store não fica ativo se um cartão SD estiver travado.

Uma caixa de diálogo pede que você confirme o armazenamento.

9. Para armazenar o projeto, clique em Yes.

Após ter clicado em Store, o projeto é armazenado no cartão SD como indicado pelos indicadores de status do controlador. Estas condições podem existir:

- Enquanto o carregamento estiver em andamento, o seguinte ocorre:
  - O indicador de OK estiver piscando em verde.
  - O indicador SD estiver piscando em verde.
  - Uma caixa de diálogo indica que o armazenamento está em progresso.
- Quando o armazenamento estiver completo, o seguinte acontecerá:
  - O controlador se reseta.

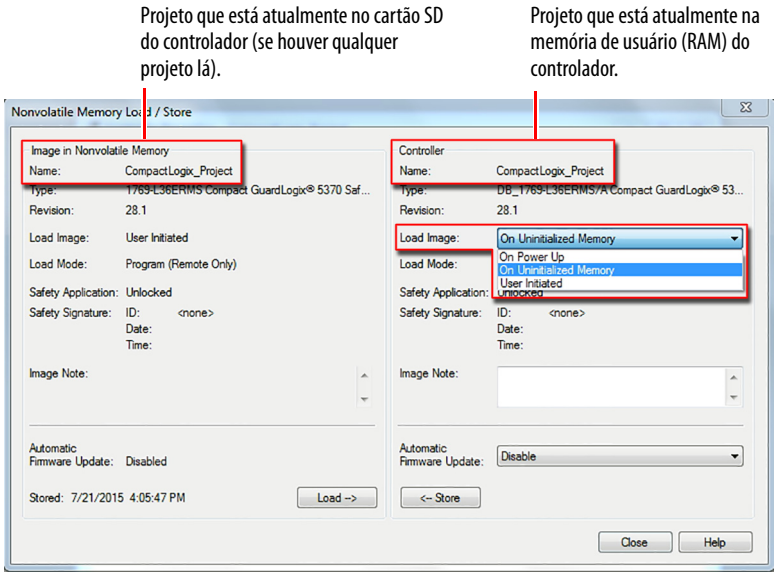
    Quando o controlador está se resetando, os indicadores de status executam uma sequência de mudanças de estado, por exemplo, um período breve de tempo com o indicador de status de OK em um estado sólido na cor vermelha. Espere que o controlador complete a sequência.
  - Após o controlador ter se resetado totalmente, o indicador de OK estará em verde sólido.
  - O indicador SD está desligado.

IMPORTANTE	Permita que o armazenamento seja completado sem interrupção. Se você interromper o armazenamento, os dados podem ser corrompidos ou perdidos.

Carregamento de um projeto de segurança

É possível iniciar uma carga a partir da memória não volátil somente se o seguinte for verdadeiro:

- O tipo do controlador especificado pelo projeto armazenado na memória não volátil corresponde ao tipo de controlador.
- As revisões principais e secundárias do projeto em memória não volátil correspondem às revisões principais e secundárias do controlador.
- Seu controlador não está no modo de operação.



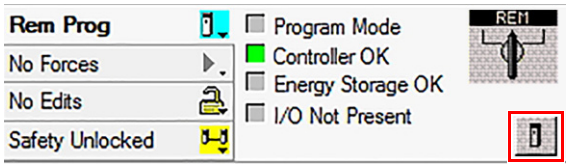
Existem várias opções para quando (sob essas condições) carregar um projeto na memória do usuário para o controlador.

Tabela 38 – Opções para carregar um projeto

Se deseja carregar o projeto	Então selecione esta opção Load Image	Observação
Sempre que ligar ou desligar e ligar a alimentação	Na energização	• Quando desligar e ligar a alimentação, você perde todas as alterações on-line, o valor do tag e programa de rede não armazenados na memória não volátil. • O controlador carrega o projeto armazenado e o firmware em qualquer partida independente do firmware ou aplicação no controlador. A carga ocorre se o controlador estiver ou não com bloqueio de segurança ou tenha uma assinatura de tarefa de segurança. • Sempre é possível utilizar o software de programação para carregar o projeto.
Sempre que não houver projeto no controlador e ele for energizado	Na memória não inicializada	• The controlador faz a atualização do firmware no controlador, se necessário. A aplicação armazenada na memória não volátil também é carregada e o controlador insere o modo selecionado, seja programação ou operação. • Sempre é possível utilizar o software de programação para carregar o projeto.
Somente pelo software RSLogix 5000®	Iniciado pelo usuário	• Se o tipo do controlador e também as revisões principais e secundárias do projeto na memória não volátil correspondem ao tipo e às revisões do controlador, é possível iniciar uma carga, independente do status da Tarefa de segurança. • Carregar um projeto em um controlador com travamento de segurança só é permitido quando a assinatura da tarefa de segurança armazenada no projeto na memória não volátil corresponder ao projeto no controlador. • Se as assinaturas não correspondem ou o controlador tem trava de segurança sem uma assinatura, será possível desbloquear o controlador. **IMPORTANTE:** Ao desbloquear o controlador e iniciar a carga a partir de memória não volátil, o status de trava de segurança, senhas e assinatura de tarefa de segurança são definidos nos valores presentes na memória não volátil uma vez que a carga estiver completa. • Se o firmware no controlador primário corresponder à revisão na memória não volátil, o firmware do parceiro de segurança é atualizado, se necessário, a aplicação armazenada na memória não volátil é carregada para que o status de tarefa segura se torne operável e o controlador entre no modo selecionado, seja programação ou operação.

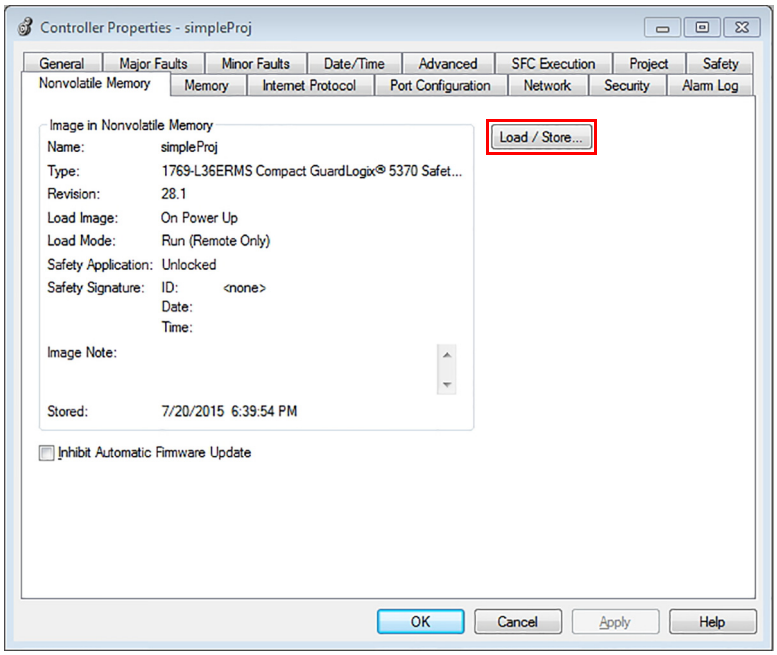
Siga estas etapas para usar a aplicação para carregar o projeto a partir de um cartão SD.

1. Comunicação com o Controlador
2. Coloque o controlador em modo de Programa, ou seja, Remote Program ou Program.
3. Na barra de ferramentas Online, clique no ícone Propriedades do controlador.

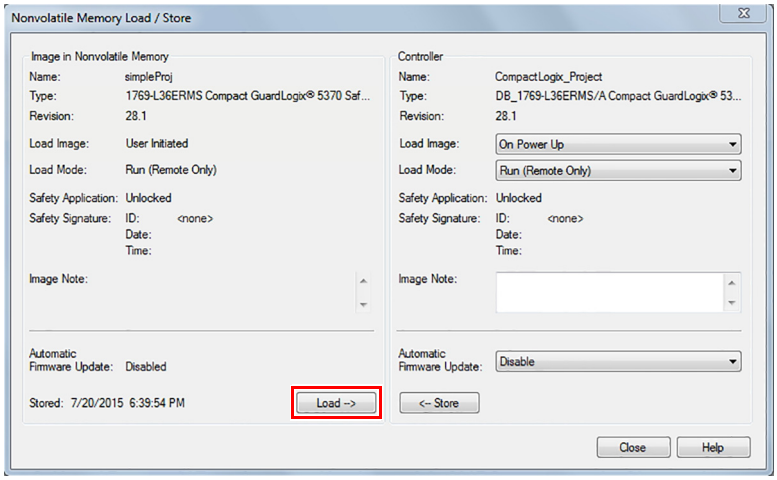


4. Clique na guia Nonvolatile Memory.

5. Clique em Load/Store.



6. Na caixa de diálogo grardar/armazenar memória não volatil, clique na guia Carregar.



Uma caixa de diálogo pede que você confirme o carregamento.

7. Para carregar o projeto, clique em Yes.

Após ter clicado em Load, o projeto é carregado no controlador conforme indicado pelos seus indicadores de status. Estas condições podem existir:

- Enquanto o carregamento estiver em andamento, o seguinte ocorre:
  - O controlador se reseta.

    Quando o controlador está se resetando, os indicadores de status executam uma sequência de mudanças de estado, por exemplo, um período breve de tempo com o indicador de status de OK em um estado sólido na cor vermelha. Espere que o controlador complete a sequência.
  - Após o controlador ter se resetado totalmente, o indicador de OK estará em verde sólido.
  - O indicador SD está desligado..

Gestão do firmware com supervisor de firmware

Pode-se usar a função Firmware Supervisor no aplicativo Logix Designer para gerenciar firmwares emCompact GuardLogixcontroladores 5370. O supervisor de firmware permite que os controladores atualizem automaticamente os dispositivos:

- Os módulos locais e remotos podem ser atualizados enquanto estiverem nos modos programação ou operação.
- A codificação eletrônica deve estar configurada para Exact Match.
- O kit do firmware para o dispositivo-alvo deve estar no cartão de memória do controlador.
- O dispositivo deve suportar atualizações do firmware por meio do software ControlFLASH™.

O supervisor do firmware é compatível com os produtos de E/S distribuída e não modulares que se assentam diretamente na rede sem um adaptador, incluindo os módulos de E/S CIP Safety nas redes EtherNet/IP.

Siga estas etapas para habilitar o Firmware Supervisor.

1. Na caixa de diálogo Controller Properties, clique na guia Nonvolatile Memory.
2. Clique em Load/Store.
3. A partir do menu Atualizações de firmware automáticas, selecione Habilitar e salvar arquivos para imagem.

A aplicação Logix Designer move os kits de firmware do seu computador para o cartão de memória do controlador para que o supervisor de firmware os use.

DICA Se desabilitar o supervisor de firmware, você desabilitará somente as atualizações do supervisor. Isso não inclui as atualizações de firmware do controlador que ocorrem quando a imagem do controlador for carregada a partir do cartão de memória.

Observações:

Indicadores de status

Esta seção explica como interpretar os indicadores de status nos seus controladores Compact GuardLogix® 5370.

Figura 44 – Indicadores de Status

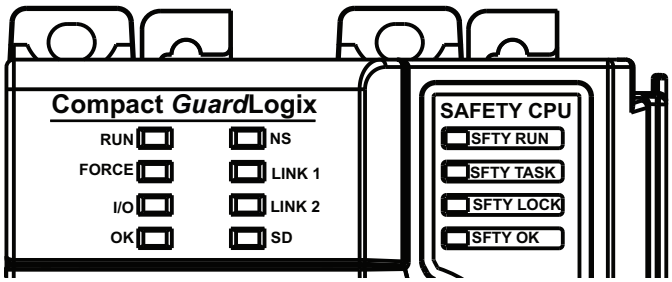


Tabela 39 – Indicador de Status (RUN) de Modo do Controlador

Status	Descrição
Desligado	O controlador está no modo de programa ou teste.
Verde	Controlador no modo de operação.

Tabela 40 – Indicador de Status de Estado Forçado (FORCE)

Status	Descrição
Desligado	Não há tags contendo valores de força de E/S. As forças de E/S estão inativas (desabilitadas).
Amarelo	As forças de E/S estão ativas (habilitadas). Podem existir valores forçados de E/S.
Amarelo intermitente	Um ou mais endereços de entrada ou saída foram forçados a um estado energizado ou desenergizado, mas as forças não foram habilitadas.

Tabela 41 – Indicador de Status de Estado de E/S (I/O)

Status	Descrição
Desligado	Uma das seguintes condições existe: • Não existem equipamentos na configuração de E/S do controlador. • O controlador não contém um projeto.
Verde	O controlador está se comunicando com todos os dispositivos na configuração de E/S.
Verde intermitente	Um ou mais dispositivos na configuração E/S do controlador não está respondendo.
Vermelho intermitente	Uma das seguintes condições existe: • O controlador não está se comunicando com nenhum equipamento. • Ocorreu uma falha no controlador.

Tabela 42 – Indicador de Status de Estado do Controlador (OK)

Status	Descrição
Desligado	Nenhuma energização aplicada.
Verde	O controlador está OK.
Verde intermitente	O controlador está armazenando um projeto em ou carregando um projeto a partir de um cartão SD.
Vermelho	O controlador detectou uma falha grave irrecuperável e removeu o projeto da memória.
Vermelho intermitente	Um dos seguintes: • O controlador requer uma atualização de firmware. • Ocorreu uma falha grave recuperável no controlador. • Uma falha grave irrecuperável ocorreu no controlador e removeu o programa da sua memória.

Tabela 43 – Indicador de Status de Estado de Rede Ethernet (NS)

Status	Descrição
Desligado	A porta não está inicializada; ela não tem um endereço IP e está operando em modo BOOTP ou DHCP.
Verde	A porta tem um endereço IP e conexões CIP estão estabelecidas.
Verde intermitente	A porta tem um endereço IP, mas não há conexões CIP estabelecidas.
Vermelho	A porta detectou que o endereço IP atribuído já está em uso.
Vermelho/verde, piscando	A porta está realizando seu auto-teste de energização.

Tabela 44 – Indicador de Status de Estado de Link Ethernet (LINK 1/LINK 2)

Status	Descrição
Desligado	Uma das seguintes condições existe: • Não há link. • Porta desabilitada administrativamente. • Porta desabilitada devido a condição de falha em anel rápida ter sido detectada (LINK2).
Verde	Uma das seguintes condições existe: • Um link de 100 Mbps (half- ou full-duplex) existe, sem atividade. • Um link de 10 Mbps (half- ou full-duplex) existe, sem atividade. • Rede de anel está operando normalmente e o controlador é o supervisor ativo. • Rede de anel encontrou uma falha de rede parcial rara e o controlador é o supervisor ativo.
Verde intermitente	Um link de 100 Mbps existe e há atividade.

Tabela 45 – Indicador de Status de Atividade do Cartão SD (SD)

Status	Descrição
Desligado	Não há atividade no cartão SD.
Verde intermitente	O controlador está lendo ou gravando no cartão SD.
Vermelho intermitente	O cartão SD não tem um sistema de arquivos válido.

Tabela 46 – Indicador de status SFTY RUN

Status	Descrição
Desligado	As saídas de segurança ou de tarefa de segurança do usuário estão desabilitadas. O controlador no modo PROG, modo de teste ou há uma falha na tarefa de segurança.
Verde	As saídas de segurança e de tarefa de segurança do usuário estão habilitadas. A tarefa de segurança está em execução. A assinatura da tarefa de segurança está presente.
Verde intermitente	As saídas de segurança e de tarefa de segurança do usuário estão habilitadas. A tarefa de segurança está em execução. A assinatura da tarefa de segurança não está presente.

Tabela 47 – Indicador de status SFTY TASK

Status	Descrição
Desligado	Nenhuma parceria estabelecida.
Verde	O status do controlador de segurança está OK. O tempo do sistema coordenado (CST) não está sincronizado.
Verde intermitente	O status do controlador de segurança está OK. O tempo de sistema (CST) não está sincronizado.
Vermelho	A parceria de segurança foi perdida.
Vermelho intermitente	Tarefa de segurança inoperante.

Tabela 48 – Indicador de status SFTY LOCK

Status	Descrição
Desligado	A tarefa de segurança não está bloqueada.
Verde	A tarefa de segurança está bloqueada.

Tabela 49 – Indicador de status SFTY OK

Status	Descrição
Desligado	Nenhuma energização aplicada.
Verde	A parceria de segurança está OK.
Verde intermitente	O parceiro de segurança está armazenando ou carregando um projeto na memória não volátil ou a partir dela.
Vermelho	O parceiro de segurança detectou uma falha grave irrecuperável, por isso removeu o projeto de sua memória.
Vermelho intermitente	O parceiro de segurança interno requer uma atualização de firmware ou esta já está em andamento.

Observações:

Trocar Tipo de Controlador

Como os controladores de segurança têm requisitos especiais e não suportam certos recursos padrão, é preciso entender o comportamento do sistema ao mudar o tipo do controlador de padrão para segurança ou vice-versa no seu projeto. Mudar o tipo de controlador afeta:

- Recursos suportados
- A configuração física do projeto, ou seja, o parceiro de segurança e a E/S de segurança
- Propriedades do controlador
- Componentes do projeto, como tarefas, programas, rotinas e tags
- Instruções adicionais de segurança

Mudança de um controlador padrão para segurança

Ao confirmar a mudança de um projeto de controlador-padrão para controlador de segurança, os componentes de segurança são criados para atender às especificações mínimas para um controlador de segurança:

- Os componentes de segurança são criados (ou seja, tarefa de segurança, programa de segurança e assim por diante).

  A tarefa de segurança é criada somente se o número máximo de tarefas descarregáveis não for obtido. A tarefa de segurança é inicializada com os respectivos valores padrão.
- Um número da rede de segurança baseado em tempo (SNN) é gerado para o rack local.
- As funções padronizadas do controlador que não são suportadas pelo controlador de segurança, como a redundância, são removidas da caixa de diálogo Controller Propriedades (se elas existiam).

Mudança de um controlador de segurança para padrão

Na confirmação de mudança de um projeto de controlador de segurança para um controlador padrão, alguns componentes são alterados e outros removidos, conforme descrito abaixo:

- Os módulos de E/S de segurança e os tags são removidos.
- As tarefas, programas e rotinas de segurança são modificadas para tarefas, programas e rotinas padrões.
- Todos os tags de segurança, exceto os tags de consumo de segurança são alterados para tags padrão. Os tags de consumo de segurança são removidos.
- Mapeamentos de tags de segurança são removidos.
- O número da rede de segurança (SNN) é removido.
- As senhas de bloqueio e desbloqueio de segurança são removidas.
- Se o controlador padrão suportar os recursos que não estavam disponíveis ao controlador de segurança, esses recursos são visíveis na caixa de diálogo das Controller Propriedades.

  DICA Controles de segurança peer não são removidos, mesmo quando não apresentam conexões remanescentes.

- As instruções podem ainda fazer referência aos módulos que foram excluídos e irão produzir erros de verificação.
- Os tags consumidos serão excluídos quando o módulo de produção for excluído.
- Como resultado das alterações anteriores no sistema, as instruções específicas de segurança e as tags da E/S de segurança não serão verificadas.

Se o projeto do controlador de segurança tiver instruções adicionais de segurança, é necessário removê-las do projeto ou mudar sua classe para padrão antes de alterar o tipo do controlador.

Mudando os tipos de controlador de segurança

Ao mudar de um tipo de controlador de segurança para outro, a classe de tags, as rotinas e os programas continuam inalterados. Qualquer módulo de E/S que não for mais compatível com o controlador alvo será excluído.

EXEMPLO Os módulos Compact I/O™ 1768 não são compatíveis com o sistema de controlador Compact GuardLogix® 5370 (1769).

A representação do parceiro de segurança é atualizada para aparecer adequadamente para o controlador-alvo nestes casos:

- O parceiro de segurança é criado no slot *x* (slot primário + 1) ao mudar de um controlador Compact GuardLogix 5370 para um GuardLogix 5570.
- Ao mudar de um controlador Compact GuardLogix 5370 para um GuardLogix 5570, o parceiro de segurança é removido, pois é interno ao controlador Compact GuardLogix.

A

B

C

I

K

L

M

N

O

P

R

S

T

U

V

Observações:

Suporte Rockwell Automation

Use os seguintes recursos para acessar as informações de suporte.

Centro de Suporte Técnico	Artigos de base de conhecimento, vídeos tutoriais, FAQs, chat, fóruns de usuários e atualizações de notificações do produto.	https://rockwellautomation.custhelp.com/
Números de telefone do suporte técnico local	Localize o número de telefone para o seu país.	http://www.rockwellautomation.com/global/support/get-support-now.page
Códigos de marcação direta	Encontre o Códigos de marcação direta para o seu produto. Utilize o código para direcionar sua chamada diretamente para um engenheiro de suporte técnico.	http://www.rockwellautomation.com/global/support/direct-dial.page
Biblioteca de literatura	Instruções de instalação, Manuais, brochuras e dados técnicos.	http://www.rockwellautomation.com/global/literature-library/overview.page
Product Compatibility and Download Center (Centro de download e compatibilidade de produto)	Obtenha ajuda sobre quais produtos combinam, verifique funcionalidades e capacidades e encontre firmware associado.	http://www.rockwellautomation.com/global/support/pcdc.page

Comentários sobre a documentação

Seus comentários irão ajudar-nos a melhor atender a suas necessidades. Se tiver sugestões para melhorar este documento, preencha o formulário Como estamos nos saindo? em http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.

A Rockwell Automation mantém informações ambientais atualizadas sobre os produtos no site em http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

www.rockwellautomation.com

Sede Mundial para Soluções de Potência, Controle e Informação

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

Brasil: Rockwell Automation do Brasil Ltda., Rua Comendador Souza, 194-Água Branca, 05037-900, São Paulo, SP, Tel: (55) 11.3618.8800, Fax: (55) 11.3618.8887, www.rockwellautomation.com.br
Portugal: Rockwell Automation, Tagus Park, Edifício Inovação II, n 314, 2784-521 Porto Salvo, Tel.: (351) 21.422.55.00, Fax: (351) 21.422.55.28, www.rockwellautomation.com.pt

Publicação 1769-UM022B-PT-P – Dezembro 2016