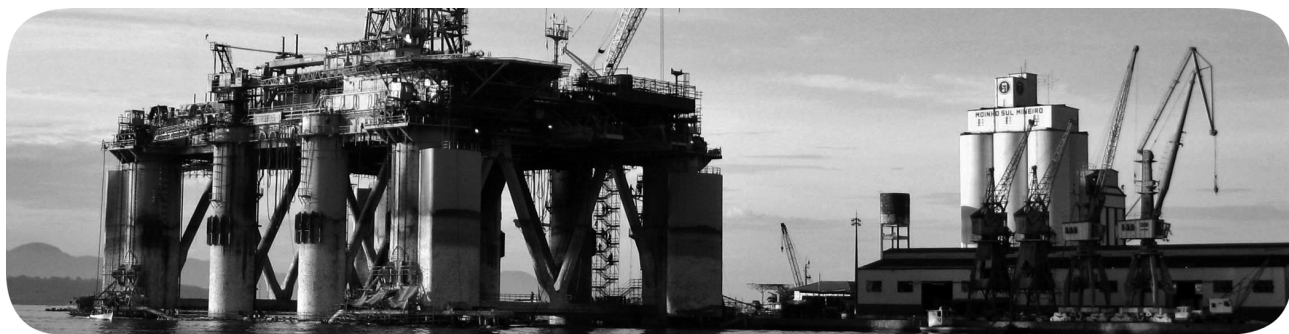


Controladores GuardLogix 5570

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

Studio 5000 Automation Engineering & Design Environment



Tradução das instruções originais

Informações Importantes ao 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, e com os 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 para finalidade ilustrativa. 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 considerações de segurança.



ADVERTÊNCIA: Identifica informações sobre práticas ou situações que podem causar uma explosão em um ambiente classificado e resultar em ferimentos pessoais ou fatais, danos à propriedade ou perda econômica.



ATENÇÃO: Identifica informações sobre práticas ou situações que podem levar a ferimentos pessoais ou fatais, danos à propriedade ou perda econômica. As atenções ajudam a identificar e evitar um risco e reconhecer a consequência.

IMPORTANTE

Identifica informações importantes relacionadas à utilização bem-sucedida e a familiarização com o produto.

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



PERIGO DE CHOQUE: As etiquetas podem estar no ou dentro do equipamento, por exemplo, um inversor ou um motor, para alertar as pessoas que tensão perigosa pode estar presente.



PERIGO DE QUEIMADURA: As etiquetas podem estar no ou dentro do equipamento, 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 pode causar 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).

Allen-Bradley, Armor, ControlFLASH, ControlLogix, DriveLogix, FlexLogix, Guard I/O, GuardLogix, Integrated Architecture, Kinetix, Logix5000, PanelView, PhaseManager, PLC-5, POINT Guard I/O, PowerFlex, Rockwell Automation, Rockwell Software, RSLinx, RSLogix, RSNetWorx, Studio 5000, Studio 5000 Automation Engineering Design Environment, e Studio 5000 Logix Designer são marcas comerciais da Rockwell Automation, Inc.

ControlNet, DeviceNet e EtherNet/IP são marcas comerciais da ODVA. As marcas comerciais que não pertencem à Rockwell Automation são propriedade de suas respectivas empresas.

Este manual contém as informações novas e atualizadas.

Informações novas e atualizadas

Esta tabela contém as alterações feitas nessa revisão.

Tópico	Página
Título da seção alterado de Mais recursos para Para obter mais informações.	11
Descrição da coluna de recursos alterada de Inversores servo Kinetix® para Inversores.	12
Manual do usuário do Kinetix 5700 Servo Drives e Manual do usuário do Inversor PowerFlex 527 CA com Frequência Ajustável adicionados ao material de recursos sobre Inversores.	12
Informações sobre versões anteriores removidas da tabela Funções suportadas.	19
Título da coluna alterado de Versão 24 para Versão 24 e posterior.	19
Frase inicial e Figura 10 adicionadas.	48
Conteúdo de atribuição de SNN adicionado à tabela Importante.	49
Figura 14 revisada para incluir inversores PowerFlex 527 e Kinetix 5700.	56
Inversores Kinetix 5700 e PowerFlex 527 adicionados às informações sobre endereços dos inversores.	73
Título da Tabela 20 e informações da tabela revisados para incluir mais inversores.	73
Inversores Kinetix 5700 e PowerFlex 527 adicionados à referência para obter mais informações.	75

Observações:

Prefácio	Sobre os controladores GuardLogix.....	9
	Controladores de ambientes extremos	10
	Controladores Armor GuardLogix	10
	Ambiente Studio 5000	10
	Terminologia.....	11
	Para mais informações.....	11
	Capítulo 1	
Características gerais do sistema	Requisitos da Aplicação de Segurança.....	13
	Número da rede de segurança	13
	Assinatura de tarefa de segurança	14
	Diferença entre componentes padrão e de segurança	14
	Dispositivos IHM.....	14
	Recursos de fluxo de dados do controlador	15
	Seleção do hardware do sistema	16
	Controlador primário	16
	Parceiro de segurança.....	17
	Rack	17
	Fonte de Alimentação	17
	Selecionar dispositivo de E/S de segurança	17
	Seleção das redes de comunicação	18
	Especificações de programação	18
	Capítulo 2	
Instale o controlador	Precauções	21
	Informações sobre Ambiente e Gabinete	21
	Sistemas eletrônicos programáveis (PES)	22
	Remoção e inserção sob alimentação (RIUP)	22
	Aprovação Norte-Americana para Uso em Áreas	
	Classificadas	22
	Aprovação para uso em áreas classificadas na Europa	23
	Prevenção de descarga eletrostática	23
	Certifique-se de que você tem todos os componentes.....	24
	Instale um rack e fonte de alimentação.....	24
	Instale o controlador no rack.....	25
	Insira ou remova um cartão de memória	26
	Remova o cartão SD.....	27
	Instale o cartão SD	27
	Faça conexões de comunicação	29
	Atualize o controlador	31
	Usando o software ControlFLASH para atualizar o firmware	31
	Usando AutoFlash para atualizar o firmware	32
	Escolha o modo de operação do controlador.....	33
	Use a chave seletora para mudar o modo de operação	33
	Use a aplicação Logix Designer para mudar o modo	
	de operação.....	34
	Desinstale um módulo de armazenamento de energia (ESM)	34
	Instale um módulo de armazenamento de energia (ESM).....	36

Configuração do controlador**Capítulo 3**

Criação de um projeto do controlador	39
Chaveamento eletrônico.....	42
Obter mais informações.....	42
Definir senhas de-bloqueio e desbloqueio de segurança	42
Protegendo a assinatura da tarefa de segurança em modo de operação.....	43
Gerenciamento da substituição do dispositivo de E/S	44
Habilitação da sincronia de tempo.....	45
Configure um Controlador de Segurança Peer.....	45

Comunicar-se nas Redes**Capítulo 4**

Rede de Segurança	47
Administração do número da rede de segurança (SNN).....	47
Atribuição do número da rede de segurança (SNN)	49
Alteração do número da rede de segurança (SNN).....	50
Comunicação EtherNet/IP	53
Produção e consumo de dados por uma rede EtherNet/IP	54
Conexão em rede EtherNet/IP	54
Exemplo de comunicação EtherNet/IP.....	55
Conexões EtherNet/IP para dispositivos de E/S de segurança	56
Conexões padrão de EtherNet/IP.....	57
Comunicação ControlNet.....	58
Produção e consumo de dados por uma rede ControlNet	58
Conexões na rede ControlNet.....	59
Exemplo de comunicação ControlNet	59
Conexões ControlNet para E/S distribuídas.....	60
Comunicação DeviceNet	60
Conexões do DeviceNet para dispositivos de E/S de segurança....	61
Conexões DeviceNet Padrão	61

**Adição, configuração,
monitoração e substituição de
dispositivos de E/S de CIP Safety****Capítulo 5**

Adicione Dispositivos de E/S de segurança	63
Configure os dispositivos de E/S de segurança	64
Configure o endereço IP por meio da conversão de endereços de rede (NAT).....	65
Definição do número da rede de segurança (SNN)	67
Usando conexões Unicast em redes EtherNet/IP	67
Definição do limite de tempo de reação da conexão	67
Especificar o intervalo do pacote requisitado (RPI)	67
Visualização do atraso máximo observado na rede	68
Definição dos parâmetros de limite de tempo de reação da conexão avançada	69
Compreensão da assinatura de configuração.....	71
Configuração por meio da aplicação Logix Designer	71
Proprietário de configuração diferente (conexão em modo de escuta)	71
Reset a Propriedade do dispositivo de E/S de Segurança	71
Endereçar dados à Dados de Endereço das E/S de Segurança	72
Formato do endereço dos módulos de E/S de segurança.....	72

Formato do endereço do inversor Kinetix 5500, Kinetix 5700 e PowerFlex 527	73
Monitorar o Status do dispositivo de E/S de segurança	74
Reiniciando um módulo para a condição pronto para usar	75
Substituindo um dispositivo usando a aplicação Logix Designer	75
Substituição com “Configure only when no safety signature exists” habilitado	76
Substituição com “Configure Always” habilitado	80
Substitua um módulo POINT Guard I/O usando o software RSNetWorx for DeviceNet	81

Capítulo 6

Criação de Aplicações de Segurança

Tarefa de Segurança	86
Especificação do Período da Tarefa de Segurança	86
Execução da Tarefa de Segurança	87
Programas de Segurança	87
Rotinas de Segurança	88
Tags de Segurança	88
Tipo de tag	89
Tipo de dados	90
Escopo	90
Classe	91
Valor constante	92
Acesso externo	92
Tags de segurança produzidas/consumidas	92
Configure os números de rede de segurança dos controladores de segurança peer	93
Produzir um tag de segurança	95
Consumir dados de tags de segurança	96
Mapeamento de tags de segurança	98
Restrições	98
Criar pares para mapeamento de tags	99
Monitorar o status de mapeamento de tags	100
Proteção de aplicações de segurança	100
Bloqueio de segurança do controlador	100
Criação de uma assinatura de tarefa de segurança	102
Restrições de programação	103

Capítulo 7

Comunicação com o Controlador

Conexão do controlador à rede	105
Conecte seu dispositivo e o computador EtherNet/IP	105
Conectar o modo de comunicação ControlNet ou o scanner DeviceNet e o seu computador	106
Configuração de um driver EtherNet/IP, ControlNet ou DeviceNet	106
Compreensão dos fatores que afetam a entrada em comunicação	106
Função Project to Controller Match	106
Revisão de Firmware Compatível	107
Falhas/status de segurança	107
Assinatura de tarefa de segurança e status de travamento e destravamento de segurança	107

	Download.....	108
	Upload.....	110
	Ficar on-line.....	111
	Capítulo 8	
Armazenamento e carregamento de projetos usando memória não volátil	Usando cartões de memória para memórias não voláteis.....	113
	Armazenamento de um projeto de segurança.....	114
	Carregamento de um projeto de segurança.....	115
	Use módulos de armazenamento de energia.....	115
	Salve o programa na memória NVS integrada.....	116
	Apague o programa da memória NVS integrada.....	117
	Estime o suporte ESM do WallClockTime.....	117
	Gestão do firmware com supervisor de firmware.....	117
	Capítulo 9	
Monitorar o Status e Controlar Falhas	Visualizando o status via barra online.....	119
	Monitorar as conexões.....	120
	Todas as conexões.....	120
	Conexões de Segurança.....	121
	Monitorar os sinalizadores de Status.....	121
	Monitorar o Status de segurança.....	122
	Falhas do controlador.....	122
	Falhas irre recuperáveis do controlador.....	123
	Falhas de segurança irre recuperáveis na aplicação de segurança....	123
	Falhas recuperáveis na aplicação de segurança.....	123
	Visualização de falhas.....	124
	Códigos de Falhas.....	124
	Desenvolvimento de uma rotina de falha.....	124
	Rotina de falha do programa.....	125
	Manipulador de falhas do controlador.....	125
	Usar instruções GSV/SSV.....	125
	Apêndice A	
Indicadores de status	Indicadores de status dos controladores.....	129
	Tela de status do controlador.....	130
	Mensagens de status de segurança.....	130
	Mensagens gerais de status.....	131
	Mensagens de falha.....	132
	Mensagens de falhas graves recuperáveis.....	133
	Códigos de falha de E/S.....	134
	Apêndice B	
Mudar o tipo de controlador	Mudança de um controlador padrão para segurança.....	137
	Mudança de um controlador de segurança para padrão.....	138
	Mudando os tipos de controlador de segurança.....	138
	Mais recursos.....	139
Índice		141

Tópico	Página
Sobre os controladores GuardLogix	9
Ambiente Studio 5000	10
Terminologia	11
Para mais informações	11

Este manual é um guia para quando um controlador GuardLogix® 5570 é usado em uma aplicação Studio 5000 Logix Designer™. Ele descreve os procedimentos específicos do GuardLogix usados para configurar, operar e localizar falhas nos controladores.

Use este manual se você for o responsável pela criação, instalação, programação ou localização de falhas em sistemas de controle que utilizam controladores GuardLogix 5570.

É necessário ter um conhecimento básico dos circuitos elétricos e familiaridade com a lógica de relé. Da mesma forma, é necessário ter treinamento e experiência em criação, operação e manutenção de sistemas de segurança.

Use este manual se você for o responsável pela criação, instalação, programação ou localização de falhas em sistemas de controle que utilizam controladores GuardLogix controlador, o nível de integridade de segurança (SIL) 3 e requisitos de nível de desempenho (e) (SIL 3/PL) ou informações sobre componentes Logix padrão, consulte a lista de [Para mais informações na página 11](#).

Sobre os controladores GuardLogix

Duas linhas de controladores GuardLogix 1756 estão disponíveis. Esses controladores compartilham diversas características, mas também têm algumas diferenças. [Tabela 1](#) oferece uma visão geral dessas diferenças.

Tabela 1 - Diferenças entre os controladores GuardLogix 5570 e GuardLogix 5560

Recurso	Controladores GuardLogix 5570 (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP, 1756-L73SXT, 1756-L7SPXT) (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT)	Controladores GuardLogix 5560 (1756-L61S, 1756-L62S, 1756-L63S, 1756-L6P)
Suporte de relógio e backup usado para retenção de memória no desligamento	Módulo de armazenamento de energia (ESM)	bateria
Portas de comunicação (incorporadas)	USB	serial
Conexões, controlador	500	250
Memória, não volátil	Cartão Secure Digital (SD)	Cartão CompactFlash (CF)
Indicadores de status	Rolar tela de status e indicadores de status	Indicadores de status
Ferramenta de programação	Ambiente Studio 5000, versão 21 ou posterior Software RSLogix RSLogix™ 5000, versão 20 ou posterior	Software RSLogix 5000, versão 14 Software RSLogix 5000, versão 16 ou posterior
Manual do usuário	- Ambiente Studio 5000: este manual - Software RSLogix 5000: 1756-UM020	1756-UM020
Manual de referência de segurança	- Ambiente Studio 5000: 1756-RM099 - Software RSLogix 5000: 1756-RM093	1756-RM093

Controladores de ambientes extremos

O controlador GuardLogix de ambientes extremos, os números de catálogo 1756-L73SXT e 1756-L7SPXT, fornecem a mesma funcionalidade que o controlador 1756-L73S, mas é projetado para suportar temperaturas de -25 a 70 °C (-13 a 158 °F).

IMPORTANTE Os componentes do sistema Logix-XT são classificados para condições ambientais extremas apenas quando usados adequadamente com outros componentes de sistema Logix-XT. O uso de componentes Logix-XT com componentes de sistema Logix tradicional anula as classificações de ambientes extremos.

Controladores Armor GuardLogix

O controlador Armor™ GuardLogix (número de catálogo 1756-L72EROMS) combina controlador 1756-L72S GuardLogix e parceiro de segurança com dois EtherNet/IP™, os canais de comunicação capazes de DLR em um invólucro classificado IP67 para montagem em uma máquina. Para obter mais informações sobre o controlador Armor GuardLogix, consulte as instruções de instalação do controlador Armor GuardLogix, publicação [1756-IN060](#).

Ambiente Studio 5000

O Ambiente de Engenharia e Design Studio 5000™ combina elementos de engenharia e design em um ambiente comum. O primeiro elemento é a aplicação Studio 5000 Logix Designer. A aplicação Logix Designer é a nova marca do software RSLogix™ 5000 e continuará a ser o produto para programar os controladores Logix5000™ para soluções discretas, de processo, de batelada, movimento, segurança e com base em inversores.



O ambiente Studio 5000 é a base para o futuro da engenharia das ferramentas de projeto e recursos Rockwell Automation®. O ambiente de Studio 5000 é o único lugar para engenheiros de projeto desenvolverem todos os elementos de seu sistema de controle.

Terminologia

Esta tabela define os termos usados neste manual.

Tabela 2 - Termos e definições

Abreviação	Termo completo	Definição
1oo2	One Out of Two	Refere-se ao projeto comportamental de um sistema de segurança de multicontroladores.
CIP	Common Industrial Protocol	Protocolo de comunicação criado para aplicações de automação industrial.
CIP safety	Protocolo Industrial Comum – Certificado de Segurança	SIL 3/PLc versão classificada de CIP.
DC	Abrangência do diagnóstico	A relação de taxa de falha detectada no total.
EN	Norma Europeia.	Norma europeia oficial.
ESM	Módulo de armazenamento de energia	Usado para suporte de relógio e backup para retenção de memória no desligamento dos controladores GuardLogix 5570.
GSV	Get System Value	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 outro endereço IP em outra rede.
PFD	Probability of Failure on Demand	Probabilidade média de um sistema falhar ao executar sua função de projeto quando solicitado.
PFH	Probability of Failure per Hour	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.

Para mais informações

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

Tabela 3 - Publicações relacionadas aos controladores e sistemas GuardLogix

Recursos	Descrição
Requisitos de aplicação de segurança	Manual de referência de segurança dos sistemas de controladores GuardLogix 5570, publicação 1756-RM099
	Manual de referência de segurança dos sistemas de controladores GuardLogix, publicação 1756-RM093
CIP Sync (sincronização de tempo)	Técnica de aplicação de configuração CIP Sync e Arquitetura integrada®, publicação 1A-AT003
Módulos Guard I/O™	Manual do usuário dos módulos de segurança Guard I/O DeviceNet™, publicação 1791DS-UM001
	Guard I/O EtherNet/IP Safety Modules User Manual, publicação 1791ES-UM001
	Manual do usuário dos módulos de segurança POINT Guard I/O™, publicação 1734-UM013
	Instruções de instalação do controlador Armor GuardLogix, publicação 1756-IN060

Tabela 3 - Publicações relacionadas aos controladores e sistemas GuardLogix (Continuação)

Recursos		Descrição
Drives	Manual do usuário do Kinetix 5500 Servo Drives, publicação 2198-UM001	Fornece informações sobre a instalação, configuração, inicialização e localização de falhas de seu sistema de acionamento servo Kinetix 5500. Também inclui requisitos para uso de inversores Kinetix 5500 em aplicações de segurança.
	Manual do usuário do Kinetix 5700 Servo Drives, publicação 2198-UM002	Fornece informações sobre a instalação, configuração, inicialização e localização de falhas de seu sistema de acionamento servo Kinetix 5700. Também inclui requisitos para uso de inversores Kinetix 5700 em aplicações de segurança.
	Manual do usuário do Inversor PowerFlex 527 CA com Frequência Ajustável, publicação 520-UM002	Fornece informações sobre a instalação, configuração, inicialização e localização de falhas do Inversor da série PowerFlex 520 CA com frequência ajustável.
Instalação de hardware	Instruções de instalação das fontes de alimentação e racks ControlLogix®, publicação 1756-IN005	Descreve como instalar e aterrar o rack ControlLogix e fontes de alimentação.
	Orientações de fiação e aterramento na automação industrial, publicação 1770-4.1	Fornece informações detalhadas sobre aterramento e fiação dos controladores programáveis.
Instruções (programação)	Manual de referência do conjunto de instruções da aplicação de segurança GuardLogix, publicação 1756-RM095	Fornece informações sobre o conjunto de instruções para aplicações de segurança do GuardLogix.
	Manual de referência de instruções gerais dos controladores Logix5000, publicação 1756-RM003	Oferece aos programadores detalhes sobre cada instrução disponível para um controlador Logix5000.
	Manual de referência de instruções de posicionamento dos controladores Logix5000, publicação MOTION-RM002	Oferece aos programadores detalhes sobre as instruções de movimento disponíveis para um controlador Logix5000.
Movimento	Manual do usuário de partida e configuração do posicionamento SERCOS, publicação MOTION-UM001	Detalha como configurar um sistema de aplicação de movimento SERCOS.
	Manual do usuário de sistemas coordenados de posicionamento, publicação MOTION-UM002	Detalha como criar e configurar um sistema de aplicação de movimento coordenado.
	Posicionamento integrado sobre a configuração de rede EtherNet/IP e o Manual do usuário de partida, publicação MOTION-UM003	Detalha como configurar um controle de movimento Integrado em um sistema de aplicação de redes EtherNet/IP.
	Manual de referência do controle de movimento integrado na rede EtherNet/IP, publicação MOTION-RM003	Informações detalhadas sobre os modos de controle de eixo e atributos para o controle de movimento em redes EtherNet/IP.
Redes (ControlNet™, DeviceNet, EtherNet/IP)	Manual do usuário dos módulos EtherNet/IP em sistemas de controle Logix5000, publicação ENET-UM001	Descreve como configurar e operar os módulos EtherNet/IP em um sistema de controle Logix5000.
	Manual do usuário dos módulos ControlNet em sistemas de controle Logix5000, publicação CNET-UM001	Descreve como configurar e operar os módulos ControlNet em um sistema de controle Logix5000.
	Manual do usuário dos módulos DeviceNet nos sistemas de controle Logix5000, publicação DNET-UM004	Descreve como configurar e operar os módulos DeviceNet em um sistema de controle Logix5000.
PhaseManager™	Manual do usuário do PhaseManager, publicação LOGIX-UM001	Fornece etapas, orientação e exemplos para definir e programar um controlador Logix5000 para usar fases de equipamentos.
Tarefas e procedimentos de programação	Manual de programação de procedimentos comuns aos controladores Logix5000, publicação 1756-PM001	Fornece acesso ao conjunto de controladores Logix5000 dos manuais de programação, que cobrem tópicos sobre gerenciamento de arquivos de projeto, organização de tags, lógica de programação, testes de rotina, criação de instruções add-on, dados de status do controlador, manuseio de falhas, importação e exportação dos componentes do projeto e mais.
	Manual de referência de uso de memória e tempo de execução dos controladores Logix5000, publicação 1756-RM087	Ajuda na estimativa de uso de memória e tempo de execução de lógica programada e na seleção entre diferentes opções de programação.

Podem-se visualizar ou fazer download das publicações em <http://www.rockwellautomation.com/literature>. Para solicitar cópias impressas da documentação técnica, entre em contato com o distribuidor local Allen-Bradley ou o representante de vendas da Rockwell Automation.

Características gerais do sistema

Tópico	Página
Requisitos da Aplicação de Segurança	13
Diferença entre componentes padrão e de segurança	14
Recursos de fluxo de dados do controlador	15
Seleção do hardware do sistema	16
Selecionar dispositivo de E/S de segurança	17
Seleção das redes de comunicação	18
Especificações de programação	18

Requisitos da Aplicação de Segurança

O sistema do controlador GuardLogix 5570 é certificado para uso em aplicações de segurança até e incluindo o Limite de reclamação de Nível de Integridade de Segurança (SIL CL) 3 e o Nível de Desempenho (e) no qual o estado desenergizado é o estado seguro. Requisitos de aplicação de segurança incluem avaliar probabilidade de taxas de falha, como:

- Probabilidade de falha sob solicitação (PFD)
- Probabilidade de falha por hora (PFH)
- Configurações de tempo de resposta do sistema
- Testes de verificação funcional que cumprem critérios SIL 3/PLc

As aplicações de segurança SIL 3/PLc baseadas no GuardLogix 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 as especificações do sistema de segurança SIL 3 e PLc, 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, publicação [1756-RM099](#). É preciso ler, entender e satisfazer esses requisitos antes de operar um sistema de segurança GuardLogix SIL 3, PLc.

Número da rede de segurança

O SNN precisa ser um número exclusivo que identifique sub-redes de segurança. Cada sub-rede de segurança que o controlador usa para a comunicação de segurança deve ter um SNN único. Cada dispositivo de E/S de segurança também deve ser configurado com o SNN da sub-rede de segurança. O SNN pode ser atribuído de forma automática ou manual.

Para informações sobre atribuição de SNN, consulte [Administração do número da rede de segurança \(SNN\) na página 47](#).

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. Esta assinatura inclui a lógica, dados e configuração de segurança. O sistema GuardLogix utiliza a assinatura da tarefa de segurança para determinar a integridade do projeto e para que seja possível verificar se fez o download do projeto correto no controlador destino. A capacidade de criar, registrar e verificar a assinatura da tarefa de segurança é um item obrigatório do processo de criação de uma aplicação de segurança.

Consulte [Criação de uma assinatura de tarefa de segurança na página 102](#) para obter mais informações.

Diferença entre componentes padrão e de segurança

Os slots de um rack do sistema GuardLogix que não são utilizados pela função de segurança podem ser utilizados por outros módulos ControlLogix certificados como Baixa Tensão e Diretivas EMC. Consulte a <http://www.rockwellautomation.com/rockwellautomation/certification/ce.page> para encontrar o certificado CE para o controle programável ControlLogix da família de produtos e determinar os módulos que são certificados.

É necessário criar e documentar uma diferença clara, lógica e visível entre as partes padrão e de segurança do projeto do controlador. Como parte 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 add-on de segurança forem exibidas.

O controlador não permite gravar dados de tags de segurança em dispositivos de interface homem-máquina (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 GuardLogix estiver desbloqueado por segurança, não tiver uma assinatura de tarefa de segurança e estiver operando sem falhas de segurança.

O Manual do usuário dos controladores ControlLogix, publicação [1756-UM001](#), fornece informações sobre o uso de dispositivos ControlLogix em aplicações-padrão (não seguras).

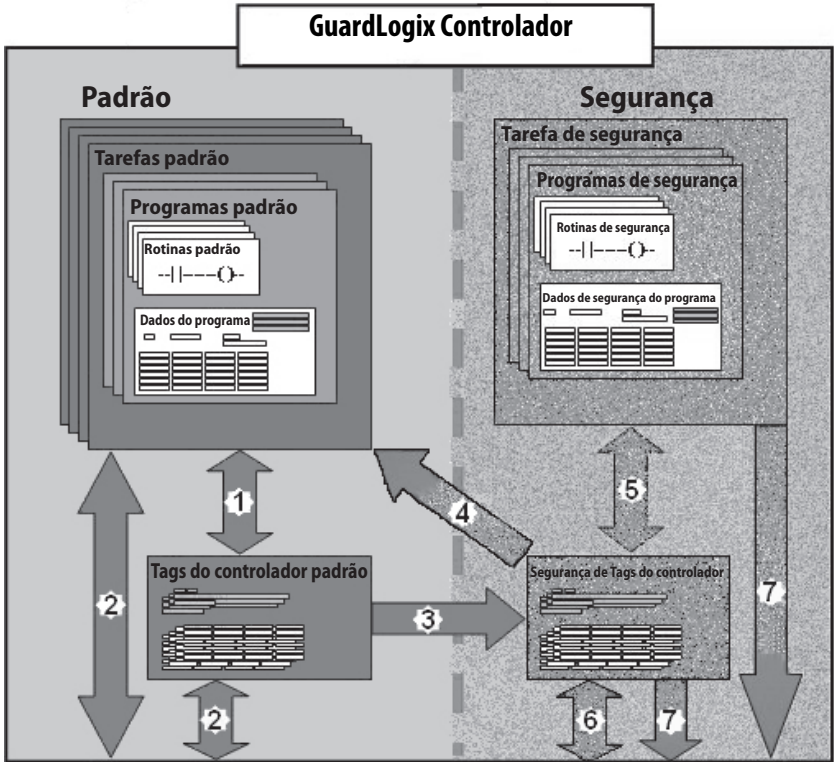
Dispositivos IHM

Os dispositivos de IHM podem ser usados com GuardLogix controladores. 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

Esta ilustração explica os recursos de fluxo de dados padrão e de segurança do GuardLogix controlador.

Figura 1 - Recursos de fluxo de dados



Cat.	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	Os controladores GuardLogix 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/PL.
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	Os tags de segurança podem ser trocados entre os controladores de segurança pelas redes ControlNet ou EtherNet, incluindo os controladores 1756 e 1768 GuardLogix.
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/PL.

Seleção do hardware do sistema

O sistema GuardLogix oferece suporte a aplicações de segurança SIL 3 e PL_e. O controlador GuardLogix é feito de um controlador primário e um parceiro de segurança que funcionam juntos em uma arquitetura 1oo2. A [Tabela 4](#) lista números de catálogo para controladores primários e parceiros de segurança.

O Parceiro de Segurança precisa ser instalado no slot à direita do Controlador Primário. O firmware principal e as revisões secundárias do controlador principal e do parceiro de segurança precisam corresponder exatamente para estabelecer a parceria de controle necessária em aplicações de segurança.

Tabela 4 - Códigos de catálogo do controlador primário e parceiros de segurança correspondentes

Controlador primário	Parceiro de segurança
1756-L71S, 1756-L72S, 1756-L73S	1756-L7SP
1756-L73SXT	1756-L7SPXT

Controlador primário

O controlador primário é o processador que realiza as funções-padrão e de segurança e se comunica com o parceiro de segurança para funções relacionadas à segurança no sistema de controle GuardLogix. As funções padrão incluem o seguinte:

- controle de E/S
- lógica
- temporização
- contagem
- geração de relatório
- comunicação
- cálculos aritméticos
- manipulação de arquivos de dados

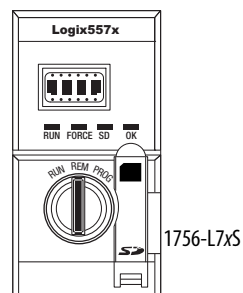
O controlador principal consiste em um controlador central, uma interface de E/S e uma memória.

Tabela 5 - Capacidade de memória

Nº. Cat.	Memória do usuário (capacidade RAM)	
	Tarefas e Componentes Padrão	Tarefa de Segurança e Componentes
1756-L71S	2 MB	1 MB
1756-L72S	4 MB	2 MB
1756-L73S, 1756-L73SXT	8 MB	4 MB

Uma chave seletora com três posições localizada na parte frontal do Controlador Primário regula os modos operacionais do controlador. Os seguintes modos estão disponíveis:

- RUN
- PROGram
- REMote – este modo de software habilitado pode ser Program, Run ou Test

Figura 2 - Posições da chave seletora

Parceiro de segurança

O parceiro de segurança é um coprocessador que fornece um segundo canal isolado (redundância) para funções relacionadas à segurança no sistema.

O parceiro de segurança não tem chave seletora nem porta de comunicação. A configuração e operação são controladas pelo controlador primário.

Rack

O rack ControlLogix fornece conexões físicas entre os módulos e o controlador GuardLogix.

Fonte de Alimentação

As fontes de alimentação ControlLogix listadas na [página 25](#) são adequadas para o uso nas aplicações SIL 3. Não é necessário nenhuma configuração ou fiação adicional para a operação de fontes de alimentação SIL 3.

Selecionar dispositivo de E/S de segurança

Os dispositivos de entrada e saída de segurança, como sensores e atuadores, podem ser conectados a E/S nas redes DeviceNet ou EtherNet/IP. Essa conexão controla dispositivos de saída por um GuardLogix sistema de controlador através da comunicação DeviceNet ou EtherNet/IP.

Para obter as informações mais atualizadas sobre números de catálogo de E/S de segurança, série de certificado e revisões de firmware, consulte os certificados de segurança em <http://www.rockwellautomation.com/rockwellautomation/certification/safety.page>.

Seleção das redes de comunicação

O controlador GuardLogix é compatível com comunicação que permita a ele fazer o seguinte:

- Distribuir e controlar E/S de segurança nas redes DeviceNet ou EtherNet/IP
- Distribuir e controlar E/S de segurança remota nas redes DeviceNet, EtherNet/IP ou ControlNet
- Produzir e consumir os dados de tag de segurança entre os controladores GuardLogix 1756 e 1768 pelas redes Ethernet/IP ou ControlNet ou no mesmo rack ControlLogix
- Distribuir e controlar E/S padrão nas redes DeviceNet, ControlNet ou EtherNet

Usar esses módulos de comunicação para fornecer uma interface entre os dispositivos de rede e os controladores GuardLogix.

Tabela 6 - Módulos de comunicação

Para fazer a interface entre	Use este módulo	Consulte as seguintes Instruções de Instalação
O controlador GuardLogix e os dispositivos DeviceNet	1756-DNB	DNET-IN001
O controlador GuardLogix e os dispositivos EtherNet/IP	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR 1756-EN3TR 1756-EN2TXT 1756-EN2TRXT	ENET-IN002
Controladores na rede ControlNet	1756-CN2 1756-CN2R 1756-CN2RXT	CNET-IN005

O controlador GuardLogix pode se conectar à aplicação Logix Designer através de uma porta USB, um módulo EtherNet ou um módulo ControlNet.

Consulte [Para mais informações na página 11](#) para mais informações sobre o uso de módulos de comunicação de rede.

Especificações de programação

Use [Tabela 7](#) para identificar a ferramenta de programação e as versões para o uso com os controladores GuardLogix 5570.

Tabela 7 - Versões de software

Nº. Cat.	Ambiente Studio 5000	Versão de software RSLogix 5000 ⁽¹⁾	Versão de software RSLinx
1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT	21 ou posterior	20 ou posterior	2.59 ou posterior

(1) Para informações sobre o uso de um controlador GuardLogix com software RSLogix 5000, consulte o Manual do usuário dos controladores GuardLogix, publicação [1756-UM020](#), e o Manual de referência de segurança de sistemas de controladores GuardLogix, publicação [1756-RM093](#).

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 8 - Funções suportadas

Recurso	Aplicação Studio 5000 Logix Designer	
	Versão 24 e posterior	
	Tarefa de segurança	Tarefa padrão
Instruções Add-on	X	X
Alarmes e eventos		
Registro no controlador	X	
Dados de controle de acesso		
Rotinas de Fase de Equipamento		
Tarefas de Evento		
Supervisor de firmware	X	
FBD (Diagramas de Blocos de Funções)		
Movimento Integrado		
Lógica ladder	X	
Troca de idiomas		
Cartão de memória		
Conversão de endereço de rede (NAT)		
Exportação e importação on-line de componentes de programação		
Segurança e conexões padrão	X	
Rotinas SFC (Controle Sequencial de Funções)		
Texto Estruturado		
Conexões unicast para tags de segurança produzidos e consumidos	X	
Conexões unicast para módulos de E/S de segurança em redes EtherNet/IP		

Para informações sobre o uso destas funções, consulte o Manual de programação de procedimentos comuns aos controladores Logix5000, publicação [1756-PM001](#), as publicações listadas em [Para mais informações na página 11](#), e suporte online.

Observações:

Instale o controlador

Tópico	Página
Precauções	21
Certifique-se de que você tem todos os componentes	24
Instale um rack e fonte de alimentação	24
Instale o controlador no rack	25
Insira ou remova um cartão de memória	26
Faça conexões de comunicação	29
Atualize o controlador	31
Escolha o modo de operação do controlador	33
Desinstale um módulo de armazenamento de energia (ESM)	34
Instale um módulo de armazenamento de energia (ESM)	36

Precauções

Leia e siga estas precauções para uso.

Informações sobre Ambiente e Gabinete



ATENÇÃO: Este equipamento foi projetado para utilização em ambientes industriais com grau de poluição 2, em categorias de sobretensão II (conforme definido na publicação 60664-1 do IEC), em altitudes de até 2000 m (6562 pés) sem redução de capacidade.

Este equipamento não deve ser usado em ambientes residenciais e pode não fornecer a proteção adequada para serviços de comunicação com rádio em tais ambientes.

Este equipamento é fornecido como tipo aberto. Deve ser instalado dentro de um gabinete apropriado às respectivas condições ambientais específicas existentes e projetado corretamente para impedir ferimentos pessoais resultantes da possibilidade de acesso a peças móveis. O gabinete deve ter propriedades à prova de fogo adequadas para evitar ou minimizar as chamas, de acordo com a classificação de dispersão de chama 5VA ou ser aprovado para a aplicação se for não metálico. O interior do gabinete só pode ser acessado com o uso de uma ferramenta. As próximas seções desta publicação podem apresentar informações adicionais relacionadas ao grau de proteção do gabinete necessário para cumprir determinadas certificações de segurança do produto.

Além desta publicação, consulte essas publicações para obter mais informações:

- Orientações sobre fiação e aterramento na automação industrial, publicação [1770-4.1](#), para especificações de instalações adicionais
- Padrão NEMA 250 e IEC 60529, se aplicáveis, para as explicações dos graus de proteção fornecidos pelo gabinete

Sistemas eletrônicos programáveis (PES)



ATENÇÃO: O pessoal responsável pela aplicação de sistemas eletrônicos programáveis (PES) com relação à segurança deve estar ciente das especificações de segurança e deve ser treinado no uso do sistema.

Remoção e inserção sob alimentação (RIUP)



ADVERTÊNCIA: Quando você insere ou remove o módulo enquanto o backplane está energizado, 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. Arcos elétricos repetidos causam desgaste excessivo nos contatos tanto do módulo quanto do conector correspondente. Contatos desgastados podem criar uma resistência elétrica que pode afetar a operação do módulo.

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 com "CL I, DIV 2, GP A, B, C, D" são adequados para uso somente em áreas não classificadas e classificadas de Classe I Divisão 2 Grupos A, B, C, D. Cada produto é fornecido com indicações na placa de identificação informando o código de temperatura da área classificada. Na combinação de produtos em um mesmo sistema, o código de temperatura mais adverso (o número "T" mais baixo) pode ser usado para ajudar a determinar o código de temperatura geral do sistema. Combinações do equipamento no sistema estão sujeitas à investigação pelas autoridades locais no momento da instalação.	
	WARNING: EXPLOSION HAZARD		ADVERTÊNCIA: RISCO DE EXPLOÇÃO
	- 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.		- 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 quaisquer conexões externas necessárias neste equipamento por meio de parafusos, travas deslizantes, conectores rosqueados ou outros meios fornecidos com este produto. - A substituição de componentes pode prejudicar a adequação com a Classe I, Divisão 2. - Se o produto utilizar baterias, elas devem ser trocadas somente em uma área não classificada.

Aprovação para uso em áreas classificadas na Europa

O seguinte se aplica quando o produto tiver a identificação Ex.

Este equipamento destina-se para uso em atmosferas potencialmente explosivas conforme definido pela Diretriz da União Europeia 94/9/EC e foi considerado de acordo com as Especificações de Segurança e Saúde com relação ao projeto e construção de equipamentos de Categoria 3 destinados a uso em atmosferas potencialmente explosivas de Zona 2, dado no Anexo II desta Diretriz.

A compatibilidade com as Especificações de Segurança e Saúde Essenciais foi garantida pela conformidade com EN 60079-15 e EN 60079-0.



ATENÇÃO: Este equipamento não é resistente à luz do sol ou outras fontes de radiação UV.



ADVERTÊNCIA: Siga estas orientações para instalar e usar o equipamento.

- Instale em um gabinete certificado ATEX com um grau de proteção de entrada mínima de IP54 (conforme definido em IEC 60529) e use em um ambiente não acima de Grau de Poluição 2 (conforme definido em IEC 60664-1) quando aplicado em ambientes de Zona 2. O gabinete deve utilizar uma tampa ou porta removível por ferramenta.
- Use dentro das suas taxas de especificação definidas pela Rockwell Automation.
- Use apenas com backplanes da Rockwell Automation.
- Não desconecte a menos que não haja energia ou a área não apresente risco.

Tome 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.

Fixe quaisquer conexões externas necessárias neste equipamento por meio de parafusos, travas deslizantes, conectores rosqueados ou outros meios fornecidos com este produto.

Prevenção de descarga eletrostática



ATENÇÃO: Este equipamento é sensível à descarga eletrostática, que pode causar danos internos e afetar a operação normal. Siga estas orientações quando for lidar com este equipamento:

- Toque um objeto aterrado para descarregar a estática potencial.
- Use uma pulseira de aterramento aprovada.
- Não toque nos conectores ou pinos das placas de componentes.
- Não toque nos componentes do circuito dentro do equipamento.
- Use uma estação de trabalho protegida contra estática, se disponível.
- Armazene o equipamento em uma embalagem protegida contra estática quando não estiver em uso.

Certifique-se de que você tem todos os componentes

Antes de começar, certifique-se de que você tem todos os componentes necessários.

IMPORTANTE Deve-se usar um controlador primário e um parceiro de segurança para obter SIL 3/PL.

Estas partes estão incluídas com o controlador primários e o parceiro de segurança.

Nº. Cat.	Descrição	Enviado com
1756-L71S 1756-L72S 1756-L73S	Controlador primário	- Módulo de armazenamento de energia (ESM) com base em capacitor 1756-ESMCAP 1784-SD1 cartão de memória SD, 1 GB - Chave 1747-KY
1756-L7SP	Parceiro de segurança	Módulo de armazenamento de energia 1756-SPESMNSE (ESM)
1756-L73SXT	Controlador primário de temperatura extrema	- Módulo de armazenamento de energia (ESM) com base em capacitor 1756-ESMCAPXT - Chave 1747-KY
1756-L7SPXT	Parceiro de segurança de temperatura extrema	Módulo de armazenamento de energia (ESM) com base em capacitor 1756-SPESMNSEXT

O seguinte equipamento opcional pode ser usado.

Se sua aplicação necessita de	Então use esta peça
Memória não volátil	1784-SD1 (1 GB) ou 1784-SD2 (2 GB)
Que o ESM instalado esgote sua energia residual armazenada para 200 µJ ou menos antes de transportá-lo para dentro ou fora da sua aplicação ⁽¹⁾	1756-ESMNSE para o controlador primário 1756-SPESMNSE para o parceiro de segurança ⁽²⁾ Este ESM não tem alimentação backup WallClockTime. Além disso, você pode usar apenas este ESM com um 1756-L73S (8 MB) ou controlador de memória de tamanho menor.
ESM que fixa o controlador impedindo a conexão USB e uso de cartão SD ⁽¹⁾	1756-ESMNRM para o controlador primário 1756-SPESMNRM para o parceiro de segurança ⁽³⁾ Este ESM fornece à sua aplicação um grau avançado de segurança.

(1) Para informações sobre o tempo de espera dos ESMs, consulte a seção [Estime o suporte ESM do WallClockTime na página 117](#).

(2) Para controladores primários e parceiros de segurança de temperatura extrema, use 1756-ESMNSEXT e 1756-SPESMNSEXT respectivamente.

(3) Para controladores primários e parceiros de segurança de temperatura extrema, use 1756-ESMNRMT e 1756-SPESMNRMT respectivamente.

Instale um rack e fonte de alimentação

Antes de instalar um controlador, precisa-se instalar um rack e uma fonte de alimentação.

1. Instale um rack ControlLogix de acordo com as instruções de instalação correspondentes.

Nº. Cat.	Número de Slots Disponíveis	Série	Consulte as seguintes Instruções de Instalação
1756-A4	4	B	1756-IN005
1756-A7	7		
1756-A10	10		
1756-A13	13		
1756-A17	17		
1756-A4LXT	4	B	
1756-A5XT	5	B	
1756-A7XT	7	B	
1756-A7LXT	7	B	

Controladores de ambiente extremo (XT) precisam de um rack XT.

2. Instale uma fonte de alimentação ControlLogix de acordo com as instruções de instalação correspondentes.

Nº. Cat.	Descrição	Série	Consulte as seguintes Instruções de Instalação
1756-PA72	Fonte de alimentação, CA	C	1756-IN005
1756-PB72	Fonte de alimentação, CC		
1756-PA75	Fonte de alimentação, CA	B	
1756-PB75	Fonte de alimentação, CC		
1756-PAXT	fonte de alimentação XT, CA	B	
1756-PBXT	fonte de alimentação XT, CC		

Controladores de ambiente extremo (XT) precisam de uma fonte de alimentação XT.

Instale o controlador no rack

Pode-se instalar ou remover um controlador enquanto a alimentação do rack estiver ligada e o sistema estiver operando.



ADVERTÊNCIA: Quando você insere ou remove o módulo enquanto a energia backplane 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. Arcos elétricos repetidos causam desgaste excessivo nos contatos tanto do módulo quanto do conector correspondente. Contatos desgastados podem criar uma resistência elétrica que pode afetar a operação do módulo.

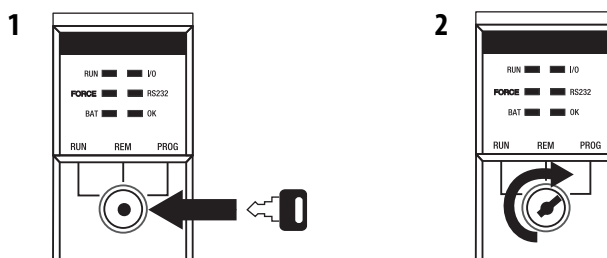
IMPORTANTE

O ESM começa a carregar quando uma destas ações ocorrer:

- O controlador e ESM estão instalados em um rack energizado.
- A energia é aplicada a um rack que contém um controlador com o ESM instalado.
- Um ESM é instalado em um controlador energizado.

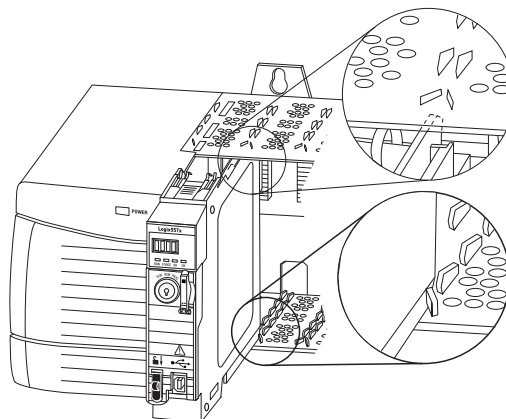
Depois que a energia é aplicada, o ESM carrega por até dois minutos conforme indicado por CHRG ou ESM Charging na tela de status.

1. Insira a chave no controlador primário.
2. Gire a chave para a posição PROG.



O parceiro de segurança não tem uma chave seletora.

3. Alinhe a placa de circuito com as guias superiores e inferiores no rack.



4. Deslize o controlador no rack.

O controlador está completamente instalado quando estiver rente à fonte de alimentação ou outros módulos instalados e as travas superiores e inferiores estiverem encaixadas.

IMPORTANTE Deve-se instalar o parceiro de segurança no slot imediatamente à direita do controlador primário. Siga as etapas [3](#) e [4](#) acima para instalar o parceiro de segurança.

Depois que o controlador foi inserido no rack, consulte [Capítulo 9](#) para informações sobre a interpretação dos indicadores de status no controlador primário e no parceiro de segurança.

Insira ou remova um cartão de memória



ADVERTÊNCIA: Quando você insere ou remove o cartão de memória enquanto a energia está 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.



ATENÇÃO: Se **não** se tem certeza do conteúdo do cartão de memória, **antes** de instalar o cartão, gire a chave seletora do controlador para a posição PROG. Dependendo do conteúdo do cartão, um ciclo de energia ou uma falha pode fazer com que o cartão carregue um projeto ou sistema operacional diferente no controlador.

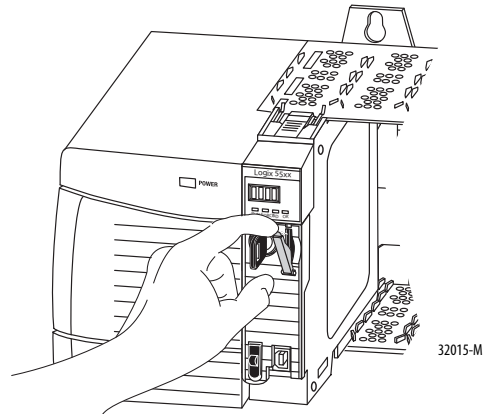
O controlador é entregue com um cartão SD instalado. Recomendamos que você deixe um cartãoSD instalado.

Remova o cartão SD

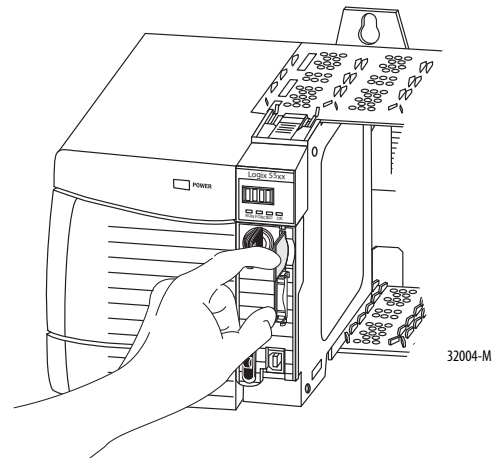
Siga estas etapas para remover o cartão SD.

IMPORTANTE Certifique-se de que o indicador de status do cartão SD está desligado e que o cartão não está em uso antes de removê-lo.

1. Gire a chave seletora para a posição PROG.
2. Abra a porta para acessar o cartão SD.



3. Pressione e libere o cartão SD para ejetá-lo.

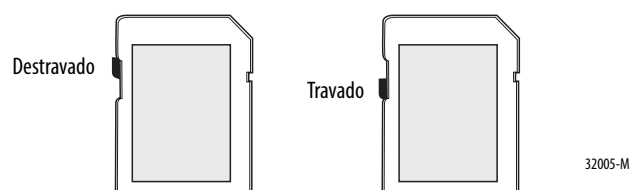


4. Remova o cartão SD e feche a porta.

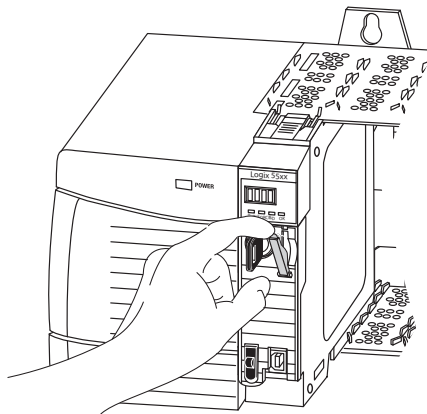
Instale o cartão SD

Siga estas etapas para instalar o cartão SD.

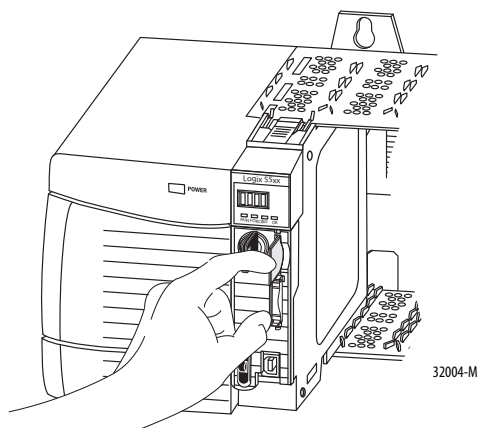
1. Verifique se o cartão SD está travado ou destravado de acordo com a sua preferência.



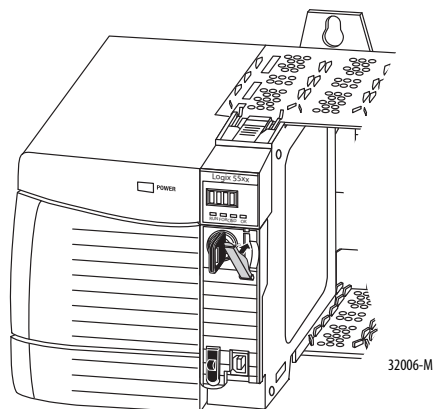
2. Abra a porta para o cartão SD.



3. Insira o cartão SD no slot do cartão SD.
4. Pressione gentilmente o cartão até que clique no lugar.



5. Feche a porta do cartão SD.



Faça conexões de comunicação

O controlador tem uma porta USB que usa um receptáculo Tipo B. A conexão é USB 2.0-compatível e opera a 12 M.

Para usar a porta USB do controlador, deve-se ter o software RSLinx, versão 2.59 ou posterior, instalado na sua estação de trabalho. Use um cabo USB para conectar a sua estação de trabalho à porta USB. Com esta conexão, pode-se atualizar o firmware e fazer download de programas para o controlador diretamente da sua estação de trabalho.



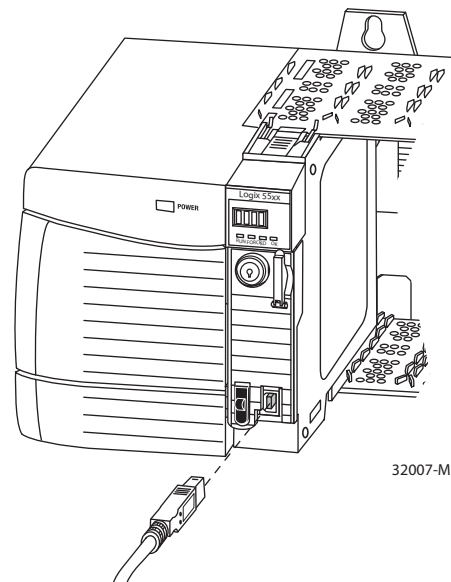
ATENÇÃO: Use a porta USB para a programação local temporária. Não use a porta USB como uma conexão permanente.

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



ADVERTÊNCIA: Não use a porta USB em áreas classificadas.

Figura 3 - Porta USB



Para configurar o software RSLinx para usar uma porta USB, é preciso primeiro definir um driver USB. Para definir um driver USB, realize este procedimento.

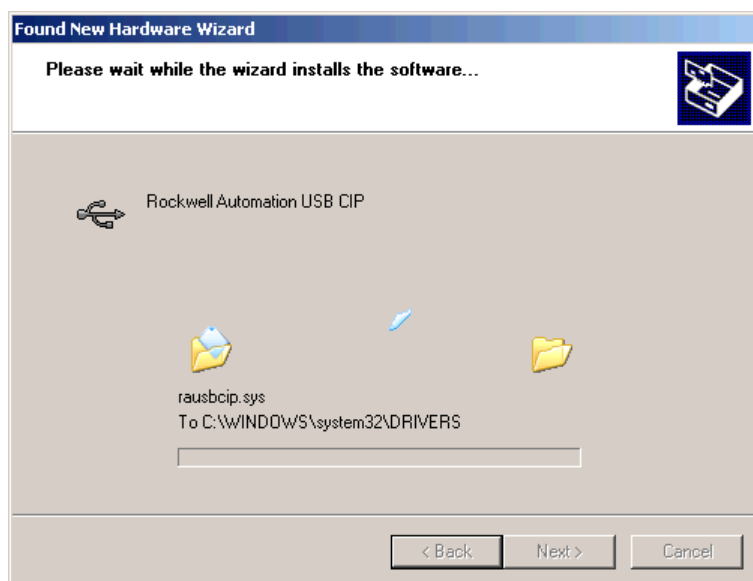
1. Conecte seu controlador e estação de trabalho usando um cabo USB.
2. Na caixa de diálogo Found New Hardware Wizard, clique em qualquer uma das opções de conexão Windows Update e clique em Next.



DICA Se o software para o driver USB não for encontrado e a instalação for cancelada, certifique-se de que está instalado o software RSLinx Classic, versão 2.59 ou posterior.

3. Clique em Install the software automatically (Recommended) e clique em Next.

O software é instalado.

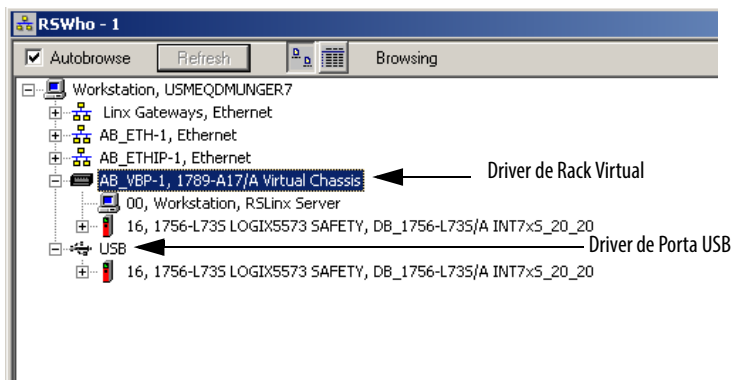


4. Clique em Finish para definir seu driver USB.

- Para buscar seu controlador no software RSLinx, clique em



No organizador RSLinx Workstation, seu controlador aparece sob dois drivers diferentes, um rack virtual e a porta USB. Pode-se usar qualquer driver para buscar o seu controlador.



Atualize o controlador

Os controladores são entregues sem o firmware. O firmware do controlador é incluído com o ambiente Studio 5000. E ainda, o firmware do controlador está também disponível para download no site de Suporte Técnico Rockwell Automation em: <http://www.rockwellautomation.com/support/>.

Pode-se atualizar seu firmware usando o software ControlFLASH™ ou usando a função AutoFlash da aplicação Logix Designer.

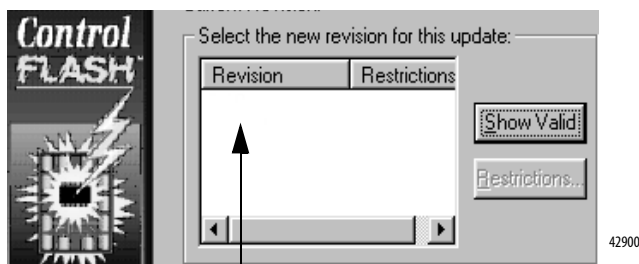
Usando o software ControlFLASH para atualizar o firmware

O parceiro de segurança atualiza automaticamente quando o controlador primário é atualizado.

IMPORTANTE Se o cartão SD estiver travado e a opção Load Image armazenada do projeto estiver configurada para On Power Up, o firmware do controlador não é atualizado como resultado destas etapas. Em vez disso, qualquer firmware e projeto armazenados anteriormente são carregados.

1. Certifique-se de que a conexão de rede apropriada seja feita e que o driver de rede foi configurado no software RSLinx.
2. Inicie o software ControlFLASH.
3. Escolha Next.
4. Selecione o código de catálogo do controlador e clique em Next.
5. Expanda sua rede até que veja o controlador.

6. Selecione o controlador e clique em Next.



7. Selecione o nível de revisão para atualização do controlador e clique em próximo.
8. Para iniciar a atualização do controlador, clique em Finish e então clique em Yes.

Depois que o controlador for atualizado, a caixa de diálogo de status exibe 'Update complete'.

IMPORTANTE Deixe que o firmware atualize completamente antes de desligar e ligar a alimentação, ou a atualização será interrompida.

DICA Se a atualização ControlFLASH do controlador for interrompida, o controlador reverte ao firmware de inicialização do sistema, que é a revisão 1.xxx.

9. Clique em OK.
10. Feche o software ControlFLASH.

Usando AutoFlash para atualizar o firmware

Para atualizar o firmware de seu controlador com a função AutoFlash, siga estas etapas.

1. Certifique-se de que a conexão de rede apropriada seja feita e que o driver de rede esteja configurado no software RSLinx.
2. Use a aplicação Logix Designer para criar um projeto de controlador na versão de que você precisa.



3. Clique RSWho para especificar o caminho do controlador.



4. Selecione seu controlador e clique em Update Firmware.

5. Selecione a revisão do firmware que deseja.
6. Clique em Update.
7. Clique em Yes.

Deixe que o firmware atualize sem interrupção. Quando a atualização do firmware estiver completa, a caixa de diálogo Who Active se abre. Pode-se completar outras tarefas na aplicação Logix Designer.

Escolha o modo de operação do controlador

Use esta tabela como referência quando determinar seu modo de operação do controlador.

Tabela 9 - Modos de operação do controlador

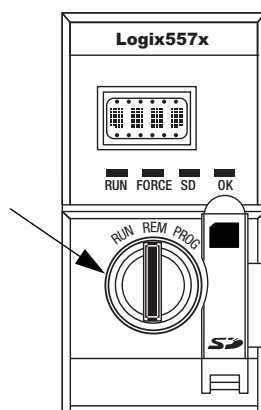
Se deseja	Selecione um destes modos				
	Run	Remoto			Program
		Run	Teste	Program	
Modifique as saídas ao estado comandado pela lógica do projeto	X	X			
Modifique as saídas ao seu estado configurado para o modo do programa			X	X	X
Execute as tarefas (varredura)	X	X	X		
Mude o modo do controlador por meio do software		X	X	X	
Faça o download de um projeto		X	X	X	X
Agende uma rede ControlNet				X	X
Enquanto estiver on-line, edite o projeto		X	X	X	X
Envie mensagens	X	X	X		
Envie e receba dados em resposta à mensagem de outro controlador	X	X	X	X	X
Produza e consuma tags	X	X	X	X	X

Use a chave seletora para mudar o modo de operação

A chave seletora na frente do controlador pode ser usada para mudar o controlador para um destes modos:

- Programa (PROG)
- Remoto (REM)
- Operação (RUN)

Figura 4 - Chave seletora do controlador



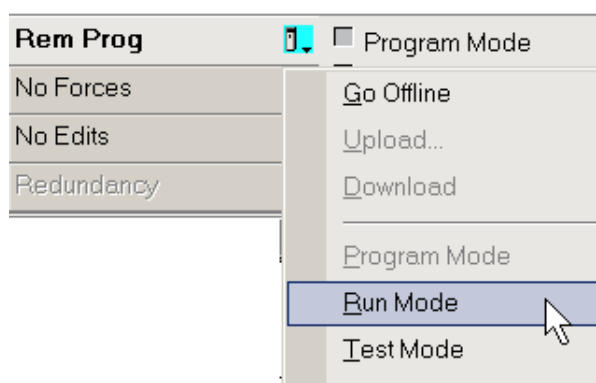
Use a aplicação Logix Designer para mudar o modo de operação

Dependendo do modo do controlador que você especificar usando a chave seletora, pode-se mudar o modo de operação usando a aplicação Logix Designer.

Depois que estiver on-line com o controlador e a chave de seletora do controlador estiver ajustada para Remoto (REM ou posição central), pode-se usar o menu Controller Status no canto superior esquerdo da janela da aplicação Logix Designer para especificar estes modos de operação:

- Programa remoto
- Operação remota
- Teste remoto

Figura 5 - Modo de operação por meio da aplicação Logix Designer



DICA

Para este exemplo, a chave seletora do controlador é ajustada para o modo Remoto. Se a chave seletora do controlador está ajustada para o modo Operação ou Programa, as opções do menu mudam.

Desinstale um módulo de armazenamento de energia (ESM)

Os controladores são entregues com um ESM instalado.

Controlador	No. Cat. do ESM instalado
Controlador 1756-L7xS	1756-ESMCAP
Controlador de temperatura extrema 1756-L7xSXT	1756-ESMCAPXT
Parceiro de segurança 1756-L7SP	1756-SPESMNSE
Parceiro de segurança de temperatura extrema 1756-L7SPXT	1756-SPESMNSEXT

Considere estes pontos antes de remover o ESM:

- Depois que o controlador perde a alimentação, porque a energia do rack é desligada ou porque o controlador foi removido de um rack energizado, não remova o ESM imediatamente.
Espere até que o indicador de status OK do controlador mude de verde para vermelho para OFF antes de remover o ESM.
- Use o módulo 1756-ESMNSE se sua aplicação precisa que o ESM instalado esgote sua energia armazenada residual para 40 µJ ou menos antes de transportá-lo para dentro ou fora da sua aplicação.
- Uma vez que foi instalado, não se pode remover o módulo 1756-ESMNRM do controlador.

IMPORTANTE Antes de remover um ESM, faça os ajustes necessários no seu programa para contabilizar mudanças em potencial para o atributo WallClockTime.

Siga estas etapas para remover um módulo 1756-ESMCAP(XT), 1756-ESMNSE(XT) ou 1756-SPESMNSE(XT).



ADVERTÊNCIA: Se sua aplicação necessita que o ESM esgote sua energia residual armazenada para 40μJoule ou menos antes de transportá-lo para dentro ou fora da sua aplicação, use apenas o módulo 1756-ESMNSE(XT) para o controlador primário e 1756-SPESMNSE(XT) para o parceiro de segurança. Neste caso, complete estas etapas antes de remover o ESM.

- a. Desligue a alimentação do rack.
Depois que desligar o rack, o indicador de status OK do controlador muda de verde para vermelho para OFF.
 - b. Espere **pelo menos 20 minutos** para que a energia residual diminua para 40 μJ ou menos antes de remover o ESM.
Não há indicação visual de quando os 20 minutos se passaram. **Deve-se controlar este período de tempo.**
-



ADVERTÊNCIA: Quando se insere ou remove o módulo de armazenamento de energia enquanto o backplane está energizado, um arco elétrico pode ocorrer. Isto pode causar uma explosão em instalações reconhecidas como área classificada.

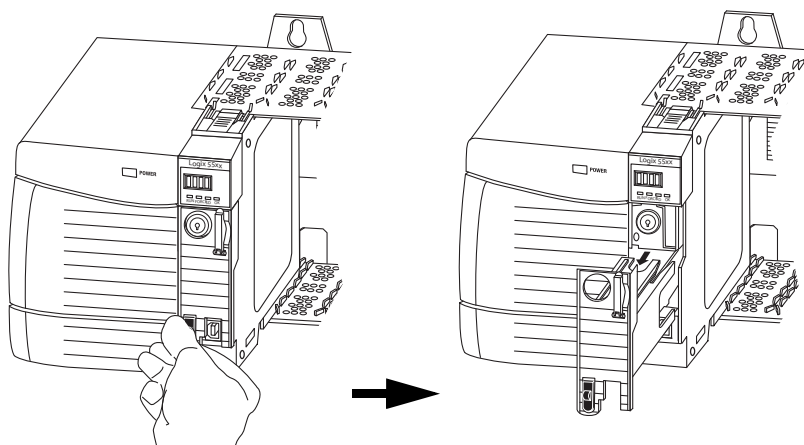
Antes de continuar certifique-se de que não haja energia ou que a área não apresenta risco. Arcos elétricos repetidos causam desgaste excessivo nos contatos tanto do módulo quanto do conector correspondente.

1. Remova a chave da chave seletora.

IMPORTANTE A próxima etapa depende das condições que se aplicam à sua aplicação:

- Se estiver removendo o ESM de um controlador energizado, vá para [etapa 2](#).
- Se estiver removendo o ESM de um controlador que não está energizado, porque a alimentação do rack está desligada ou porque o controlador foi removido de um rack energizado, **não remova** o ESM imediatamente.
Espere até que o indicador de status OK do controlador mude de verde para vermelho para OFF antes de remover o ESM.
Depois que o indicador de status OK mudar para OFF, vá para [etapa 2](#).

2. Use seu polegar para pressionar o desarme preto e puxar o ESM para fora do controlador.



Instale um módulo de armazenamento de energia (ESM)

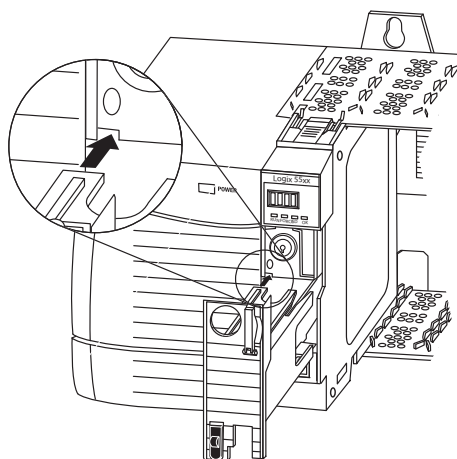
[Tabela 10](#) listas do ESMs e os controladores de GuardLogix compatíveis.

Tabela 10 - Módulos de armazenamento de energia compatíveis

Nº. Cat.	ESMs compatíveis
1756-L7xS	1756-ESMCAP, 1756-ESMNSE, 1756-ESMNRM
1756-L7xSXT	1756-ESMCAPXT, 1756-ESMNSEXT, 1756-ESMNRMXT
1756-L7SP	1756-SPESMNSE, 1756-SPESMNRM
1756-L7SPXT	1756-SPESMNSEXT, 1756-SPESMNRMXT

Para instalar um ESM, complete estas etapas. Siga as mesmas etapas para o parceiro de segurança.

1. Alinhe os slots macho e fêmea do ESM e do controlador.



2. Deslize o ESM no rack até que se fixe no lugar.



ATENÇÃO: Para evitar danos potenciais ao produto quando for inserir o ESM, alinhe o ESM na trilha e deslize para frente com força mínima até que o ESM se fixe no lugar.

O ESM começa a carregar depois da instalação. O status de carregamento é indicado por umas destas mensagens de status:

- ESM carregando
- CHRG

Depois que instalar o ESM, pode demorar até 15 segundos para que as mensagens de status de carregamento sejam exibidas.

IMPORTANTE Deixe que o ESM termine o carregamento antes de remover a energia do controlador. Para se certificar de que o ESM esteja completamente carregado, verifique a tela de status para confirmar que as mensagens 'CHRG' ou 'ESM Charging' não estão mais indicadas.

DICA Verifique os atributos de objeto WallClockTime depois de instalar um ESM para se certificar de que o tempo do controlador está correto.

Observações:

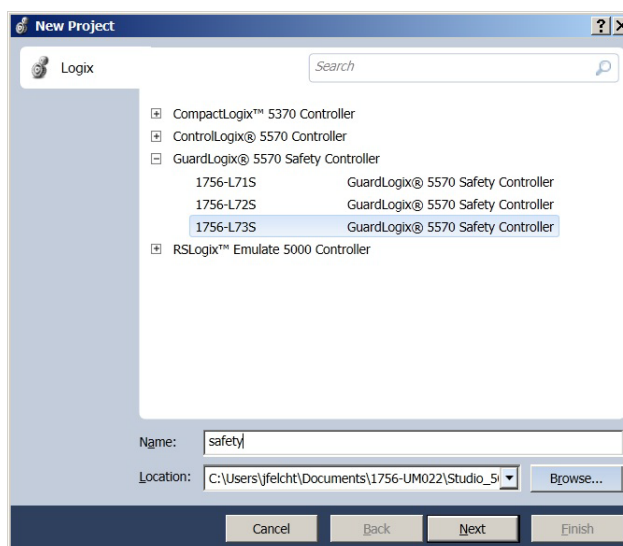
Configuração do controlador

Tópico	Página
Criação de um projeto do controlador	39
Chaveamento eletrônico	42
Definir senhas de bloqueio e desbloqueio de segurança	42
Protegendo a assinatura da tarefa de segurança em modo de operação	43
Gerenciamento da substituição do dispositivo de E/S	44
Habilitação da sincronia de tempo	45
Configure um Controlador de Segurança Peer	45

Criação de um projeto do controlador

Para configurar e programar seu controlador, utilize a aplicação Logix Designer para criar e gerenciar um projeto para o controlador.

1. Clique no botão novo  na barra de ferramentas principal para criar um projeto.
2. Clique duas vezes no controlador de segurança GuardLogix 5570 para expandir a lista de opções de controlador.
3. Escolha um GuardLogix controlador:
 - 1756-L71S Controlador de segurança GuardLogix 5570
 - 1756-L72S Controlador de segurança GuardLogix 5570
 - 1756-L73S Controlador de segurança GuardLogix 5570

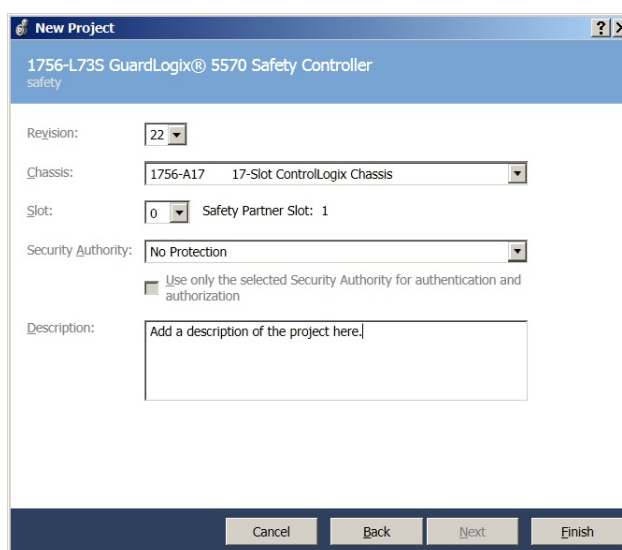


4. No campo Name, digite o nome do projeto.
5. Clique em Browse para especificar a pasta para armazenar o projeto do controlador de segurança.
6. Clique em Next.

7. No menu Revision, escolha a revisão principal de firmware para o controlador.
8. No menu Rack, escolha o tamanho do rack.
9. No menu de Slot, escolha o slot para o parceiro de segurança.

A caixa de diálogo New Project exibe a localização do slot do parceiro de segurança com base no número de slot informado para o controlador primário.

Se você selecionar um número de slot para o controlador primário que não acomoda a colocação do parceiro de segurança logo à direita do controlador primário, será solicitado que insira novamente um número de slot válido.



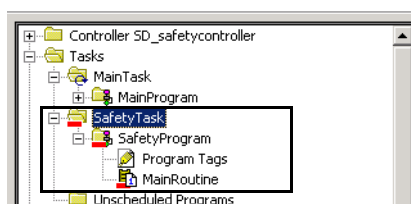
10. No menu Security Authority, escolha uma opção de autoridade de segurança.

Para informações detalhadas sobre segurança, consulte o Manual de programação de segurança dos controladores Logix5000, publicação [1756-PM016](#).

11. Marque a caixa abaixo de autoridade de segurança se você deseja usar a proteção selecionada para autenticação e autorização.
12. No campo Description, digite uma descrição do projeto.
13. Clique em Finish.

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 6 - Tarefa de segurança no organizador do controlador



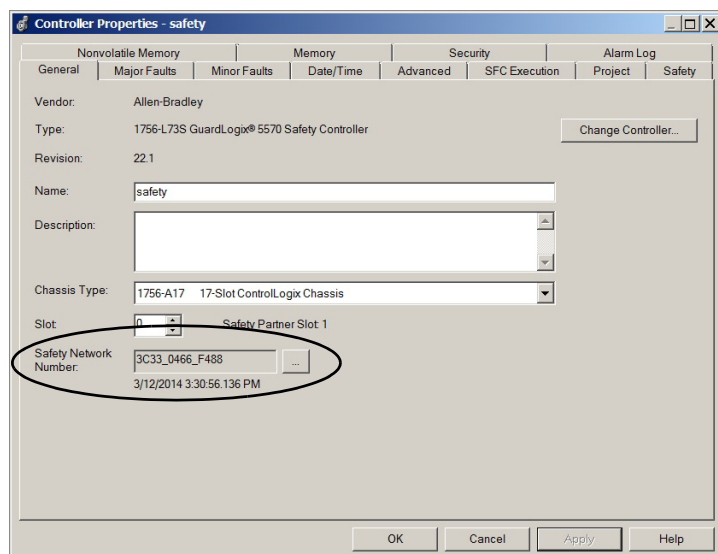
Uma barra vermelha abaixo do ícone diferencia os programas e as rotinas de segurança dos componentes-padrão do projeto no organizador do controlador.

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.

Esse SNN define o backplane do rack local como uma sub-rede de segurança. Ela pode ser vista e modificada através da guia General na caixa de diálogo Controller Properties.

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

Figura 7 - Número da rede de segurança



DICA

Você pode usar a caixa de diálogo Properties do controlador para mudar o controlador de padrão para segurança ou segurança para o padrão, clicando no botão Change Controller. No entanto, os projetos padrão e de segurança serão muito afetados.

Consulte o [Apêndice B, Mudar o tipo de controlador](#), para obter detalhes sobre as ramificações de troca de controladores.

Tabela 11 - Recursos adicionais

Recursos	Descrição
Capítulo 6, Criação de Aplicações de Segurança	Contém mais informações sobre a tarefa, os programas e as rotinas de segurança
Capítulo 4, Comunicar-se nas Redes	Fornece mais informações sobre como gerenciar o SNN

Chaveamento eletrônico

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 do 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.
-------------------	---

Obter mais informações

Para mais informações detalhadas sobre chaveamento eletrônico, consulte Keying eletrônico na técnica de aplicação de sistemas de controle de Logix5000, publicação [LOGIX-AT001](#).

Definir senhas de bloqueio e desbloqueio de segurança

O bloqueio de segurança do controlador ajuda a proteger componentes de controle de segurança de modificações. 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 Tools > Safety > Change Passwords.
2. No menu What Password, escolha Safety Lock ou Safety Unlock.



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. Letras, números e os seguintes símbolos podem ser usados:

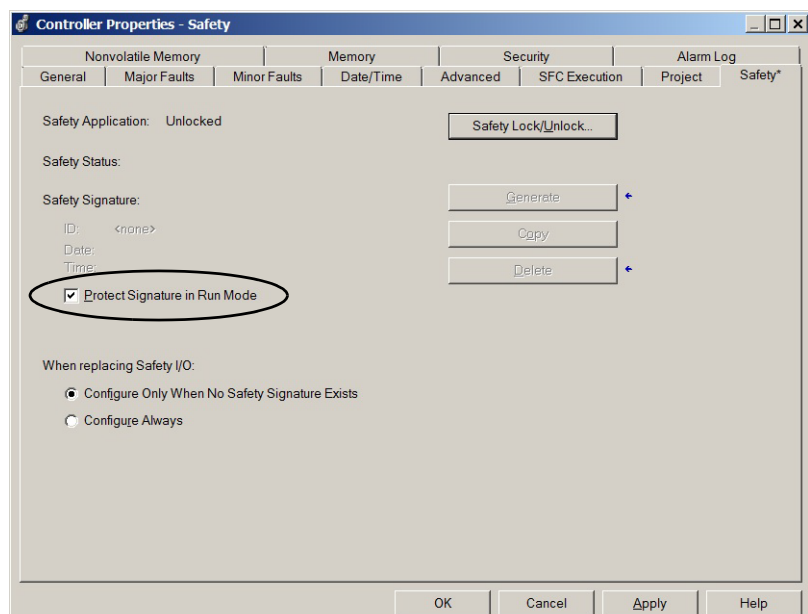
‘ ~ ! @ # \$ % ^ * () _ + , - = { } | [] \ : ; ? / .

Protegendo a assinatura da tarefa de segurança em 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 Controller Properties.
2. Clique na guia Safety.
3. Verifique Protect Signature in Run Mode.
4. Clique em OK.



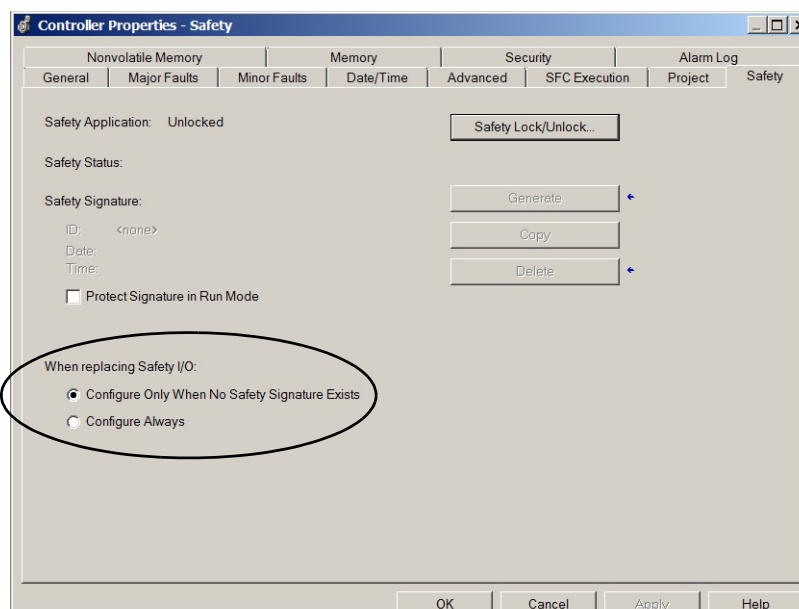
Gerenciamento da substituição do dispositivo de E/S

A guia Safety da caixa de diálogo Controller Properties permite definir como o controlador lida com a substituição de um módulo de E/S no sistema. Essa opção determina se o controlador ajusta o número de rede de segurança (SNN) de um dispositivo de E/S que ele estiver conectado e tem dados de configuração para quando uma assinatura de tarefa de segurança⁽¹⁾ existe.

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 Controller Properties.
2. Clique na guia Safety.
3. Selecione a opção configurar para o controlador para usar quando substituir a E/S de segurança.
4. Clique em OK.

Figura 8 - Opções de substituição do dispositivo de E/S



ATENÇÃO: Habilite a função Configure Always somente se o sistema de controle CIP Safety inteiro roteável não estiver escalado para manter o SIL 3 durante a substituição e o teste funcional de um módulo.

Consulte [Capítulo 5, Adição, configuração, monitoração e substituição de dispositivos de E/S de CIP Safety](#) para obter mais informações.

(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 14](#) e [Criação de uma assinatura de tarefa de segurança na página 102](#) para mais informações.

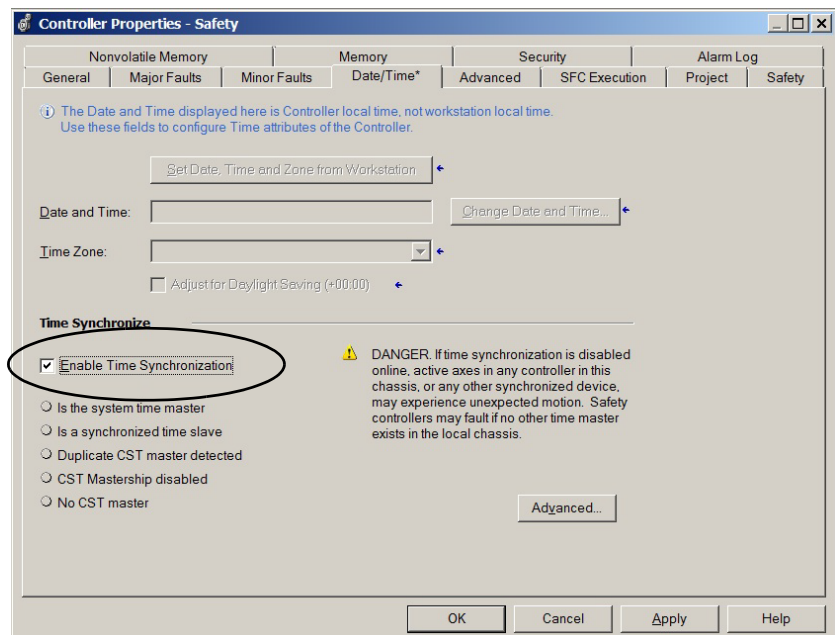
Habilitação da sincronia de tempo

Em um sistema do controlador GuardLogix, um dispositivo no rack local deve ser designado como o mestre para o tempo de sistema coordenado (CST). A opção Time Synchronization oferece um mecanismo padrão para sincronizar relógios por uma rede de dispositivos distribuídos.

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

1. Abra a caixa de diálogo Controller Properties.
2. Clique na guia data/hora.
3. Marque Enable Time Synchronization.
4. Clique em OK.

Figura 9 - Guia Date/Time



Para mais informações sobre a sincronização de tempo, consulte a Solução de aplicação de configuração CIP Sync e Integrated Architecture, publicação [IA-AT003](#).

Configure um Controlador de Segurança Peer

É possível adicionar um controlador de segurança peer à pasta I/O Configuration de seu projeto de segurança para permitir que os tags padrão ou de segurança sejam consumidos. Para compartilhar dados de segurança entre controladores peer, você produz e consome tags de segurança com escopo no controlador.

Para detalhes sobre a configuração dos controladores de segurança peer e a produção e o consumo de tags de segurança, consulte [Tags de segurança produzidas/consumidas na página 92](#).

Observações:

Comunicar-se nas Redes

Tópico	Página
Rede de Segurança	47
Comunicação EtherNet/IP	53
Comunicação ControlNet	58
Comunicação DeviceNet	60

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 de E/S de segurança 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.

Administração do número da rede de segurança (SNN)

O SNN atribuído aos dispositivos de segurança em um segmento de rede precisa ser exclusivo. É necessário garantir que um SNN exclusivo seja atribuído aos seguintes:

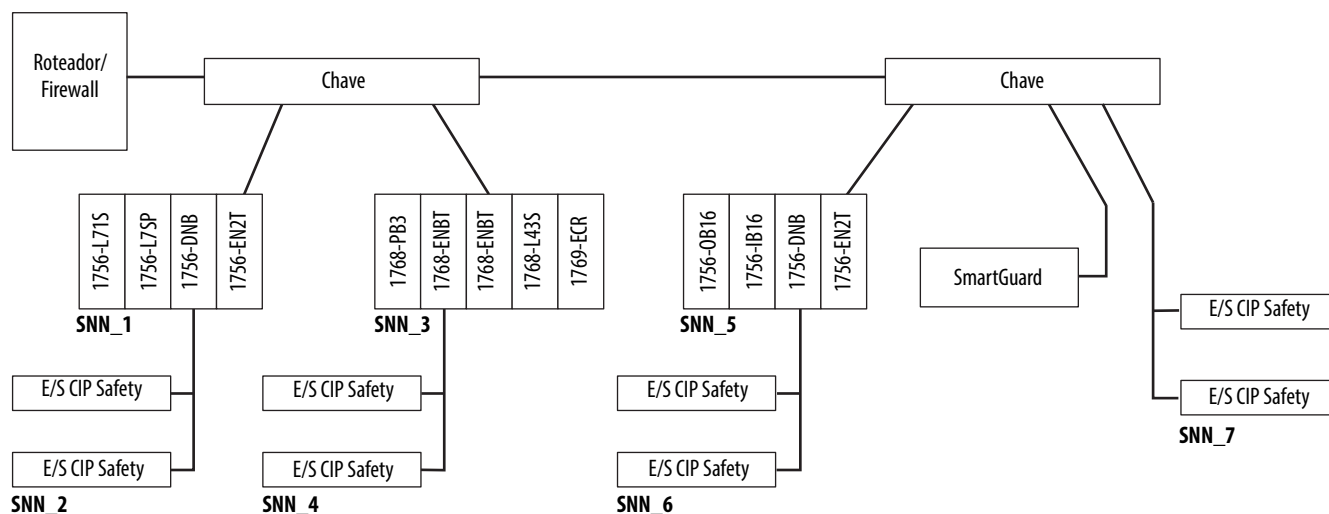
- Cada rede de segurança CIP que contém os dispositivos de segurança
- Cada rack que contenha um ou mais controladores GuardLogix

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. No entanto, para simplificar, recomendamos que cada sub-rede de segurança CIP tenha apenas um único SNN.

Figura 10 mostra um sistema de segurança CIP com sete sub-redes diferentes, em que cada sub-rede tem um único SNN.

Figura 10 - Exemplo de segurança CIP com mais de um SNN



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.

Número da rede de segurança baseado em tempo

Se o formato de tempo é selecionado, o valor de SNN é a data e hora quando o número foi gerado, de acordo com o computador executando o software de configuração.

Figura 11 - Formato com base na hora

A janela 'Safety Network Number' apresenta duas opções de formato: 'Time-based' (selecionada) e 'Manual'. O formato 'Time-based' mostra a data e hora '4/7/2014 10:40:49.36 AM' e um botão 'Generate'. O formato 'Manual' possui um campo 'EtherNet/IP:' com o texto '(Decimal)' e um campo 'Number:' com o valor '3C4D_035D_580C' e o texto '(Hex)'. Botões 'Copy', 'Paste' e 'Set' (com uma seta azul) estão disponíveis para o formato manual. Na base da janela, há botões 'OK', 'Cancel' e 'Help'.

Número da rede de segurança manual

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

Figura 12 - Entrada 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 dispositivo é criado, um SNN baseado em tempo é atribuído automaticamente. As adições subsequentes do novo dispositivo 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 para sistemas CIP safety roteáveis onde o número de sub-redes da rede e interconexão de redes é pequeno, e pode gerenciar e atribuir o SNN de uma maneira lógica para sua aplicação específica.

Consulte [Alteração do número da rede de segurança \(SNN\) na página 50](#).

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.

No Logix Designer versão 24, um erro de verificação ocorre se seu projeto contém SNN e combinações de endereço do nó duplicados.

No Logix Designer versão 26, é exibida uma advertência se seu projeto contém SNN e combinações de endereço do nó duplicados. Você ainda pode verificar o projeto, mas a Rockwell Automation recomenda corrigir 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 consumidos 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.

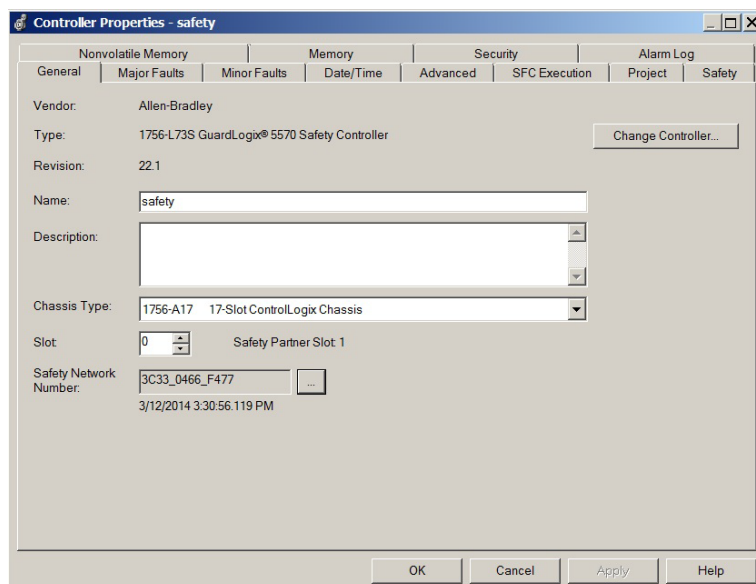
Alteração do número da rede de segurança (SNN)

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

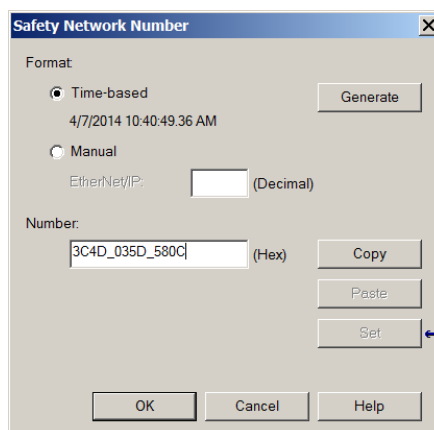
- desproteger o projeto, caso esteja protegido.
Consulte [Bloqueio de segurança do controlador na página 100](#).
- excluir a assinatura da tarefa de segurança, caso exista uma.
Consulte [Remover a assinatura da tarefa de segurança na página 103](#).

Alterar o número da rede de segurança (SNN) do controlador

1. No organizador do controlador, clique com o botão direito do mouse no controlador e escolha Properties.
2. Na guia General da caixa de diálogo Controller Properties, clique  à direita de Safety Network Number para abrir a caixa de diálogo Safety Network Number.



3. Clique em Time-based e em Generate.

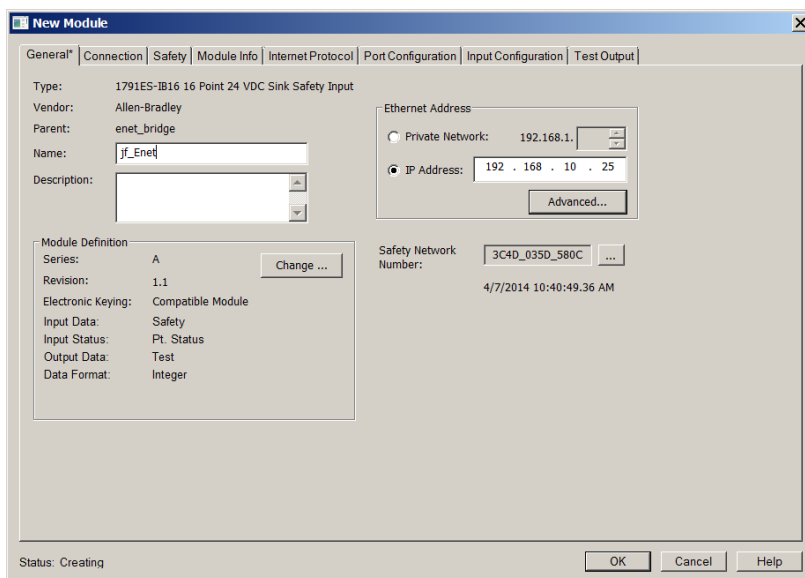


4. Clique em OK.

Altere o número de rede de segurança (SNN) dos dispositivos de E/S de segurança na rede CIP Safety

Este exemplo usa uma rede EtherNet/IP.

1. Encontre o primeiro módulo de comunicação EtherNet/IP na árvore I/O Configuration.
2. Aumente os dispositivos de E/S de segurança disponíveis através do módulo de comunicação EtherNet/IP.
3. Clique duas vezes no primeiro dispositivo de E/S de segurança para visualizar a guia General.



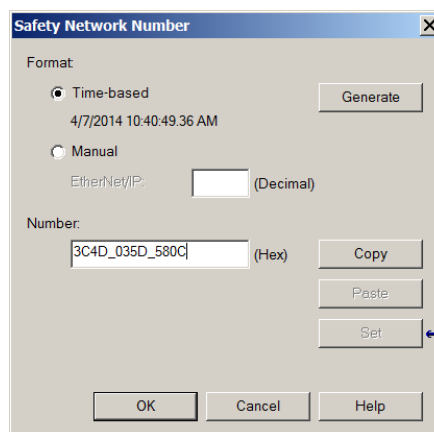
4. Clique em [...] à direita do número da rede de segurança para abrir a caixa de diálogo Safety Network Number.
5. Escolha Time-based e clique em Generate para criar um novo SNN referente à rede EtherNet/IP.
6. Clique em OK.
7. Clique em Copy para copiar o novo SNN para a área de transferência do Windows.

8. Abra a guia General da caixa de diálogo Module Properties do próximo dispositivo de E/S de segurança no módulo EtherNet/IP.
9. Clique em  à direita do número da rede de segurança para abrir a caixa de diálogo Safety Network Number.
10. Escolha Time-based e clique em Paste para colar o SNN da rede EtherNet/IP para este dispositivo.
11. Clique em OK.
12. Repita as etapas 8 a 10 para os dispositivos de E/S de segurança remanescentes sob o módulo de comunicação EtherNet/IP.
13. Repita as etapas 2 a 10 para quaisquer módulos de comunicação de rede remanescentes sob a árvore de Configuração E/S.

Cópia e colagem de um número da rede de segurança (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 de E/S.

1. Na ferramenta de configuração de software do proprietário da configuração do módulo, abra a caixa de diálogo Safety Network Number do módulo.



2. Clique em Copy.
3. Clique na guia General da caixa de diálogo Module Properties do dispositivo de E/S na árvore I/O Configuration 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 Safety Network Number.
5. Clique em Paste.
6. Clique em OK.

Comunicação EtherNet/IP

Para a comunicação de rede EtherNet/IP em um sistema GuardLogix, você pode escolher entre vários módulos. Para a comunicação CIP Safety, incluindo o controle do dispositivo de E/S de segurança, escolha qualquer um dos módulos mostrados em [Tabela 12](#), exceto o módulo 1756-EWEB, que não suporta a comunicação CIP Safety.

[Tabela 12](#) lista os módulos e suas funções primárias.

Tabela 12 - Módulos de comunicação EtherNet/IP e recursos

Módulo	Recursos
1756-ENBT	- Conecta os controladores aos dispositivos de E/S (é necessário um adaptador para E/S distribuída). - Faz a comunicação com outros dispositivos EtherNet/IP (mensagens). - Serve como caminho para o compartilhamento de dados entre os controladores Logix5000 (produção/consumo). - Une os nós EtherNet/IP para direcionar as mensagens a dispositivos em outras redes.
1756-EN2T	- Realiza as mesmas funções que o módulo 1756-ENBT, com o dobro da capacidade para aplicações mais exigentes. - Fornecer uma conexão de configuração temporária por meio da porta USB. - Configura os endereços IP rapidamente usando chaves rotativas.
1756-EN2F	- Realiza as mesmas funções que o módulo 1756-EN2T. - Conecta a mídia de fibra por um conector de fibra LC no módulo.
1756-EN2TXT	- Realiza as mesmas funções que o módulo 1756-EN2T. - Opera em ambientes extremos com temperaturas de -25 a 70 °C (-13 a 158 °F).
1756-EN2TR	- Realiza as mesmas funções que o módulo 1756-EN2T. - Suporta a comunicação em uma topologia de anel para uma rede em anel tolerante a uma única falha do tipo Anel de Nível de Dispositivo (DLR).
1756-EN2TRXT	- Realiza as mesmas funções que o módulo 1756-EN2T. - Suporta a comunicação em uma topologia de anel para uma rede em anel tolerante a uma única falha do tipo Anel de Nível de Dispositivo (DLR). - Opera em ambientes extremos com temperaturas de -25 a 70 °C (-13 a 158 °F).
1756-EN3TR	- Realiza as mesmas funções que o módulo 1756-EN2TR. - Duas portas para conexão DLR.
1756-EWEB	- Fornecer páginas da internet personalizáveis para acesso externo às informações do controlador. - Fornecer acesso remoto via um navegador de internet para tags em um controlador ControlLogix local. - Faz a comunicação com outros dispositivos EtherNet/IP (mensagens). - Une os nós EtherNet/IP para direcionar as mensagens a dispositivos em outras redes. - Suporta dispositivos Ethernet que não são baseados em EtherNet/IP com uma interface de soquete. Este módulo não fornece suporte para tags de E/S produzidas ou consumidas, e não suporta comunicação CIP Safety.

Os módulos de comunicação EtherNet/IP fornecem as seguintes funções:

- Suporte para envio de mensagem, tags produzidos/consumidos, IHM e E/S distribuídas
- Mensagens encapsuladas dentro do protocolo-padrão TCP/UDP/IP
- Uma mesma camada de aplicação com as redes ControlNet e DeviceNet
- Interface por meio de cabo de par trançado RJ45, categoria 5, sem blindagem
- Suporte para transmissão half e full duplex de operação 10 M ou 100 M
- Trabalho com chaves-padrão
- Não requerem sequenciamento de rede
- Não requerem tabelas de roteamento

Esses produtos estão disponíveis para redes EtherNet/IP.

Tabela 13 - Produtos para módulos EtherNet/IP

Produto	É usado para	Necessário
Ambiente Studio 5000	- Configuração do projeto do controlador - Definição de comunicação EtherNet/IP	Sim
Utilitário BOOTP/DHCP ⁽¹⁾	Atribuição de endereços IP a dispositivos em uma rede EtherNet/IP	Negativo
Software RSNetWorx para EtherNet/IP	Configuração dos dispositivos EtherNet/IP por endereços IP e/ou nomes de hosts	Negativo
Software RSLinx	- Configura os dispositivos - Estabelece comunicação entre os dispositivos - Fornece diagnósticos	Sim

(1) Este utilitário vem com ambiente Studio 5000.

Produção e consumo de dados por uma rede EtherNet/IP

O controlador suporta a capacidade de produzir (enviar) e consumir (receber) tags por uma rede EtherNet/IP. Tags produzidos e consumidos cada um necessita de conexões. O número total de tags que podem ser produzidos ou consumidos é limitado pelo número de conexões disponíveis.

Conexão em rede EtherNet/IP

Você determina de forma indireta o número de conexões que o controlador de segurança usa ao configurar o controlador para comunicar-se com outros dispositivos no sistema. As conexões são alocações de recursos que fornecem comunicação mais confiável entre os dispositivos comparado às mensagens não conectadas (instruções de mensagem).

Todas as conexões EtherNet/IP são não programáveis. Uma conexão não programável é disparada pelo intervalo do pacote requisitado (RPI) para controle de E/S ou para o programa (como uma instrução MSG). O envio de mensagem não programável permite enviar e receber dados quando necessário.

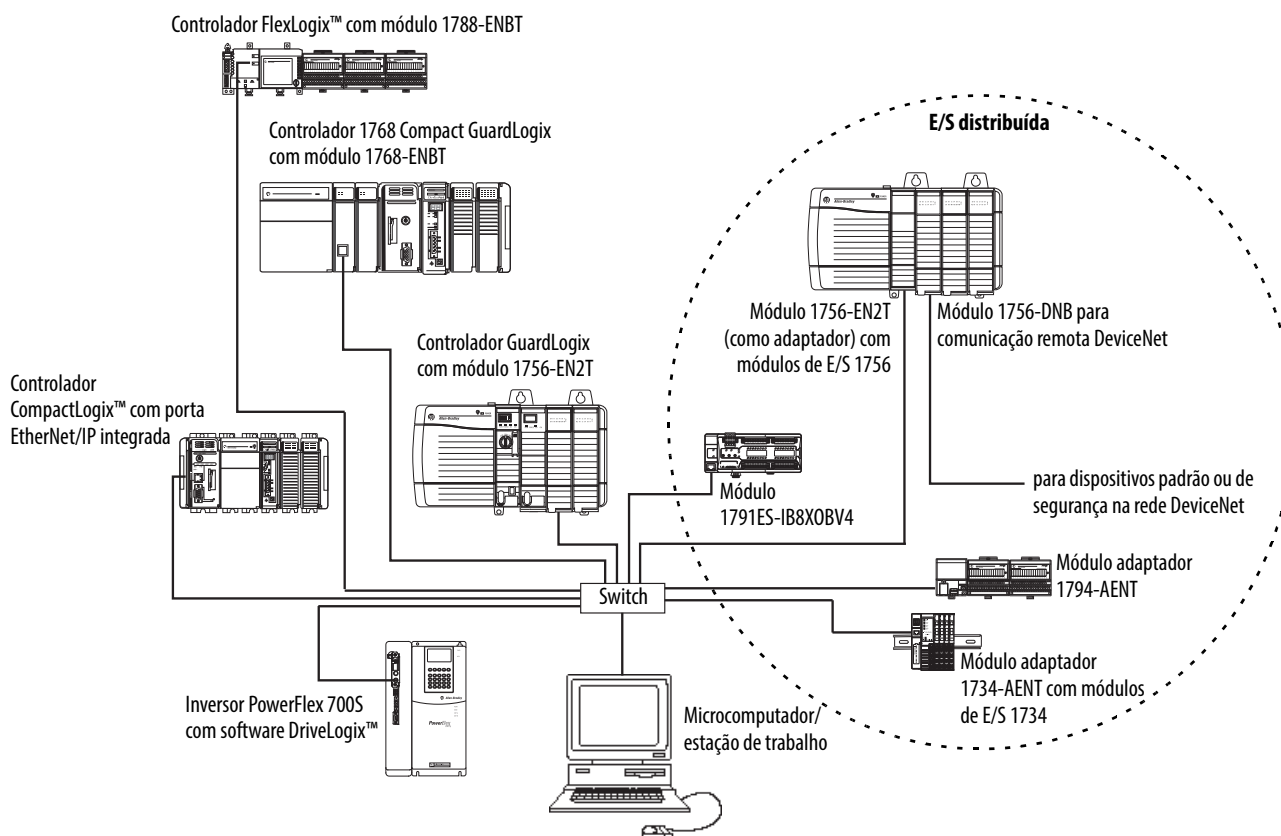
Os módulos de comunicação EtherNet/IP suportam com 128 conexões do protocolo industrial comum (CIP) em uma rede EtherNet/IP.

Exemplo de comunicação EtherNet/IP

Figura 13 ilustra as seguintes funções de comunicação:

- os controladores podem produzir e consumir tags padrão e de segurança entre si.
- os controladores podem iniciar instruções MSG que enviam/recebem dados padrão ou configuram dispositivos.⁽¹⁾
- o módulo de comunicação EtherNet/IP é utilizado como uma ponte, deixando o controlador de segurança produzir e consumir dados-padrão e de segurança.
- a estação de trabalho pode fazer upload/download de projetos para os controladores.
- a estação de trabalho pode configurar os dispositivos na rede EtherNet/IP.

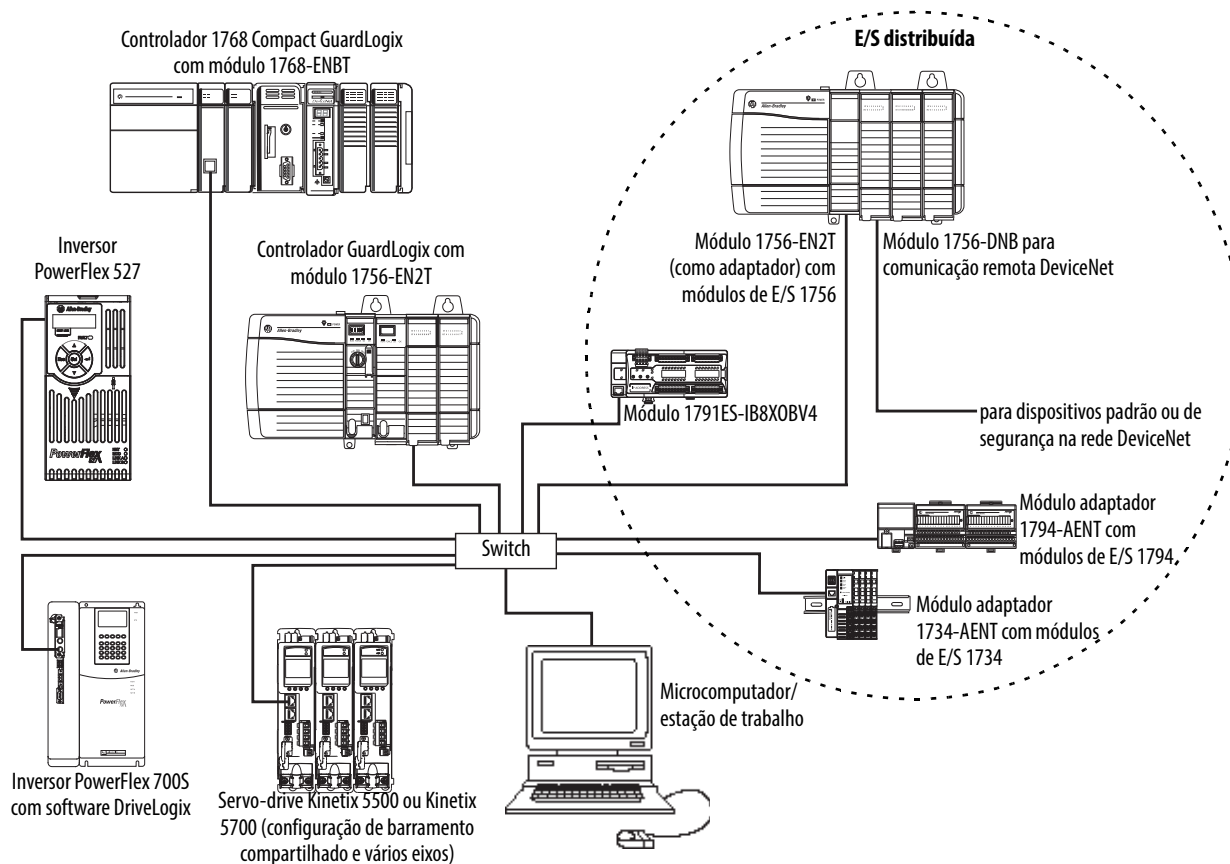
Figura 13 - Exemplo de comunicação EtherNet/IP



(1) Os controladores GuardLogix não suportam as instruções MSG para os dados de segurança.

Na aplicação do Logix Designer, versão 24 e posterior, o controlador suporta o padrão e segurança através de uma conexão simples.

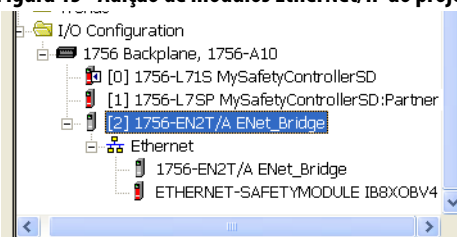
Figura 14 - Comunicação EtherNet/IP com o padrão e exemplo de conexão de segurança



Conexões EtherNet/IP para dispositivos de E/S de segurança

Os dispositivos de E/S de segurança nas redes EtherNet são adicionados ao projeto sob o módulo de comunicação EtherNet/IP, conforme descrito em [Adicione Dispositivos de E/S de segurança na página 63](#). Quando você adicionar um dispositivo de E/S de segurança, a aplicação do Logix Designer cria automaticamente tags de dados de segurança de escopo do controlador para esse dispositivo.

Figura 15 - Adição de módulos EtherNet/IP ao projeto



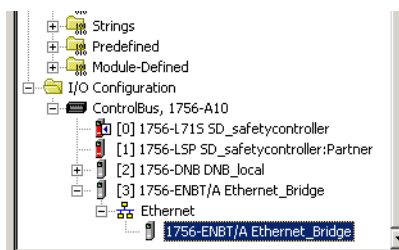
Conexões padrão de EtherNet/IP

Para usar um módulo-padrão de EtherNet/IP com o controlador de segurança, adicione o módulo ao projeto do controlador de segurança e faça download do projeto no GuardLogix controlador.

1. Para configurar o módulo, defina o endereço IP, a máscara de sub-rede e o conversor de protocolos.

Parâmetro EtherNet/IP	Descrição
Endereço IP	O endereço IP identifica exclusivamente o módulo. O endereço IP está no formato xxx.xxx.xxx.xxx, onde cada xxx é um número entre 0 e 255. Porém, há alguns valores que não podem ser usados na primeira oitava do endereço. Porém, há alguns valores que não podem ser usados na primeira oitava do endereço: • 000.xxx.xxx.xxx • 127.xxx.xxx.xxx • 223...255.xxx.xxx.xxx
Máscara de sub-rede	O endereçamento de sub-rede é uma extensão do esquema de endereço IP que permite a um site utilizar um ID de rede simples em várias redes físicas. O roteamento externo do site continua pela divisão do endereço IP em um ID de rede e um ID do computador principal pela classe. Dentro do site, a máscara de sub-rede é usada para dividir outra vez o endereço IP em parte de ID da rede personalizada e a parte de ID do computador principal. Por padrão, este campo está definido como 0.0.0.0. Se você mudar a máscara de sub-rede de um módulo já configurado, será necessário desligar e ligar a alimentação para a mudança ser executada.
Conversor de protocolos	Um conversor de protocolos conecta redes físicas individuais em um sistema de redes. Quando um nó precisa se comunicar com outro em outra rede, um conversor de protocolos transfere os dados entre as duas redes. Por padrão, este campo está definido como 0.0.0.0.

2. Depois de instalar fisicamente um módulo EtherNet/IP e definir o endereço IP, é necessário adicionar o módulo ao organizador do controlador no GuardLogix projeto do controlador.



3. Use a aplicação Logix Designer para fazer download do projeto.

Comunicação ControlNet

Para comunicação ControlNet, escolha um módulo 1756-CNB ou 1756-CNBR para comunicação-padrão ou um módulo 1756-CN2, 1756-CN2R ou 1756-CN2RXT para comunicação de segurança.

Tabela 14 - módulos ControlNet

Se sua aplicação	Selecione
- Controla módulos de E/S padrão - Requer um módulo adaptador para E/S distribuída em links ControlNet - Comunica-se com outros dispositivos ControlNet (mensagens) - Compartilha dados padrão com outros controladores Logix5000 (produz/consome) - Conecta-se com links ControlNet para rotear mensagens para dispositivos em outras redes	1756-CNB
- Desempenha as mesmas funções que o módulo 1756-CNB - Também suporta mídia ControlNet redundante	1756-CNBR
- Desempenha as mesmas funções compatíveis com o módulo 1756-CNB com melhor desempenho - Suporta comunicação CIP Safety	1756-CN2
- Desempenha as mesmas funções que o módulo 1756-CN2 - Também suporta mídia ControlNet redundante	1756-CN2R
- Desempenha as mesmas funções que o módulo 1756-CN2R - Opera em ambientes extremos com temperaturas de -25 a 70 °C (-13 a 158 °F)	1756-CN2RXT

Esses produtos estão disponíveis para redes ControlNet.

Tabela 15 - Produtos para módulos ControlNet

Produto	É usado para	Necessário
Ambiente Studio 5000	- Configuração do projeto GuardLogix - Definição de comunicação ControlNet	Sim
Software RSNetWorx for ControlNet	- Configuração da rede ControlNet - Definição do tempo de atualização da rede (NUT) - Programação da rede ControlNet	Sim
Software RSLinx	- Configura os dispositivos - Estabelece comunicação entre os dispositivos - Fornecer diagnósticos	Sim

Os módulos de comunicação ControlNet fornecem o seguinte:

- Suporte para envio de mensagem, tags de segurança e padrão produzidos/consumidos e E/S distribuída
- Suportam o uso de repetidores coaxiais e de fibra para isolamento e aumento da distância.

Produção e consumo de dados por uma rede ControlNet

O controlador GuardLogix suporta a capacidade de produzir (enviar) e consumir (receber) tags por uma rede ControlNet. O número total de tags que podem ser produzidos ou consumidos é limitado pelo número de conexões disponíveis no GuardLogix controlador.

Conexões na rede ControlNet

O número de conexões que o controlador usa é determinado pela forma como você configura o controlador para comunicar-se com outros dispositivos no sistema. As conexões são alocações de recursos que fornecem comunicação mais confiável entre os dispositivos se comparados às mensagens não conectadas.

As conexões ControlNet podem ser programáveis ou não programáveis.

Tabela 16 - Conexões ControlNet

Tipo de conexão	Descrição
Programável (exclusiva para a rede ControlNet)	Uma conexão programável é exclusiva para comunicação ControlNet. Uma conexão programável permite enviar e receber dados repetidamente em um intervalo predefinido que é o intervalo do pacote requisitado (RPI). Por exemplo, uma conexão com um dispositivo de E/S é uma conexão programável porque dados são recebidos repetidamente do módulo em um intervalo especificado. Outras conexões programáveis incluem conexões com: • Dispositivos de comunicação • Tags produzidos/consumidos Em uma rede ControlNet, é necessário usar o software RSNetWorx for ControlNet para habilitar as conexões programáveis e estabelecer um tempo de atualização de rede (NUT). A programação de uma conexão reserva largura de banda de rede para lidar especificamente com a conexão.
Não programável	Uma conexão não programável é uma transferência de mensagem entre os controladores que é disparada pelo intervalo do pacote requisitado (RPI) ou pelo programa (como uma instrução MSG). O envio de mensagem não programável permite enviar e receber dados quando necessário. As conexões não programáveis usam o restante da largura de banda da rede depois que as conexões programáveis são alocadas. As conexões de segurança produzidas/consumidas não são programáveis.

Os módulos de comunicação 1756-CNB e 1756-CNBR são compatíveis com 64 conexões CIP em uma rede ControlNet. Entretanto, recomendamos que não sejam configuradas mais de 48 conexões para manter um desempenho otimizado.

O módulo 1756-CN2 suporta 128 conexões CIP em uma rede ControlNet.

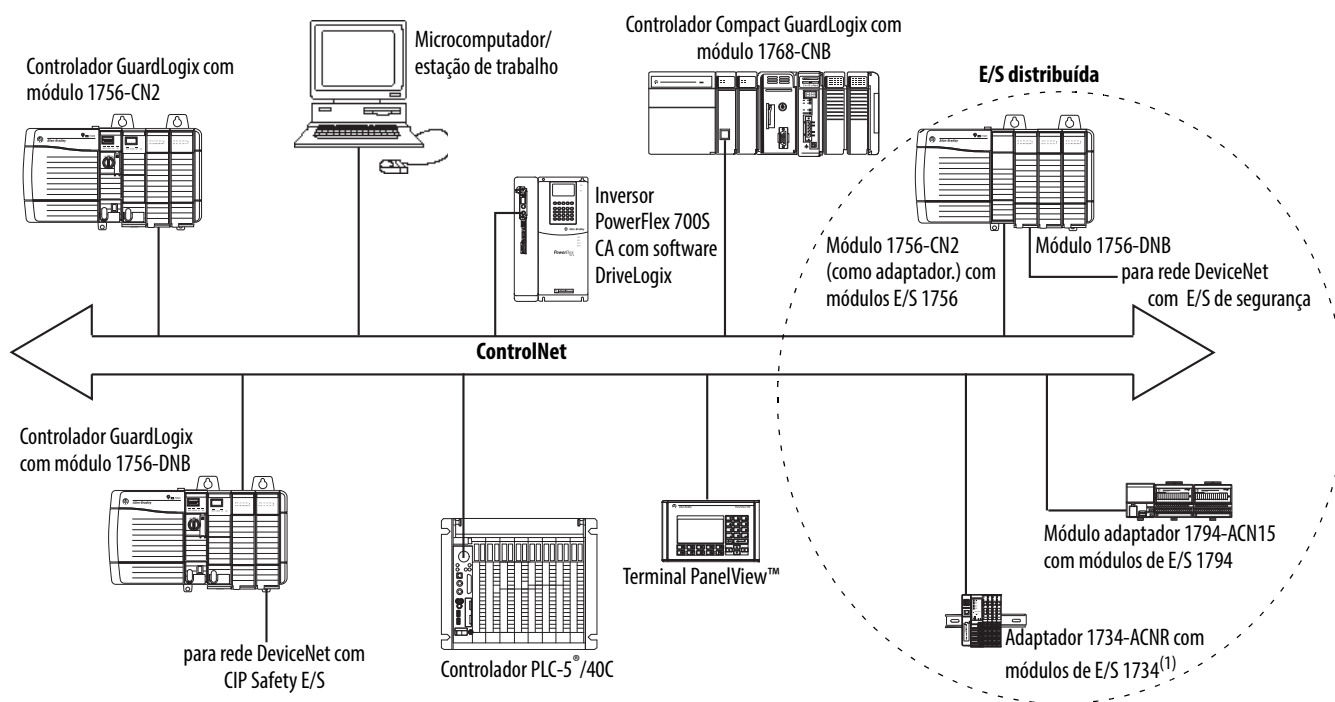
Exemplo de comunicação ControlNet

Este exemplo ilustra o seguinte:

- Os controladores GuardLogix podem produzir e consumir tags padrão e de segurança entre si.
- Os controladores GuardLogix podem iniciar instruções MSG que enviam/recebem dados padrão ou configuram dispositivos.⁽¹⁾
- O módulo 1756-CN2 pode ser usado como uma ponte, permitindo que o controlador GuardLogix produza e consuma os dados padrão e de segurança de e para dispositivos de E/S.
- O microcomputador pode fazer upload/download de projetos nos controladores.
- O microcomputador pode configurar dispositivos na rede de ControlNet e configurar a própria rede.

(1) Os controladores GuardLogix não suportam as instruções MSG para os dados de segurança.

Figura 16 - Exemplo de comunicação ControlNet



(1) O adaptador 1734-ACN não suporta módulos POINT Guard Safety I/O.

Conexões ControlNet para E/S distribuídas

Para comunicar com os dispositivos de E/S distribuídas pela rede ControlNet, acrescente uma ponte ControlNet, um adaptador ControlNet e dispositivos de E/S à pasta I/O Configuration do controlador.

Comunicação DeviceNet

Para se comunicar e trocar dados com os dispositivos de E/S de segurança em redes DeviceNet, é necessário um módulo 1756-DNB no rack local.

Para obter informações sobre como instalar o módulo 1756-DNB, consulte ControlLogix DeviceNet Scanner Module Installation Instructions, publicação [1756-IN566](#).

O módulo 1756-DNB é compatível com comunicação com dispositivos DeviceNet Safety e DeviceNet padrão. Você pode usar os dois tipos.

Estes produtos são usados com as redes DeviceNet e módulo 1756-DNB.

Tabela 17 - Produto para uso com redes DeviceNet

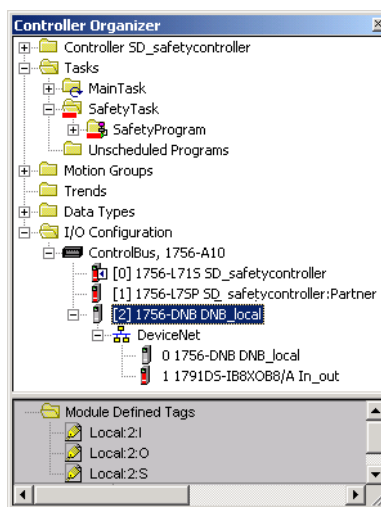
Produto	É usado para	Necessário
Ambiente Studio 5000	- Configure os projetos ControlLogix. - Defina a comunicação DeviceNet.	Sim
Software RSNetWorx para DeviceNet	- Configura dispositivos DeviceNet. - Defina a lista de varredura para esses dispositivos.	Sim
Software RSLinx Classic ou RSLinx Enterprise	- Configura os dispositivos de comunicação. - Fornece diagnósticos. - Estabelece comunicação entre os dispositivos.	Sim

Conexões do DeviceNet para dispositivos de E/S de segurança

Para acessar os dispositivos de E/S de segurança nas redes DeviceNet, adicione um 1756-DNB à árvore I/O Configuration do projeto do controlador GuardLogix.

Os dispositivos de E/S de segurança em redes DeviceNet são adicionados ao projeto no módulo 1756-DNB, conforme descrito no [Capítulo 5. Adição, configuração, monitoração e substituição de dispositivos de E/S de CIP Safety](#). Quando você adicionar um dispositivo de E/S de segurança, a aplicação do Logix Designer cria automaticamente tags de dados de segurança de escopo do controlador para esse dispositivo.

Figura 17 - Módulo DeviceNet no controlador na árvore I/O Configuration



Conexões DeviceNet Padrão

Se você usar a DeviceNet I/O padrão com seu controlador GuardLogix, precisará alocar duas conexões para cada módulo 1756-DNB. Uma é para o status e a configuração do módulo. A outra é para uma conexão otimizada para rack de dados DeviceNet I/O.

Para usar o módulo 1756-DNB a fim de acessar dados-padrão pela rede DeviceNet, você deve usar o software RSNetWorx para DeviceNet para:

- criar um arquivo de configuração para a rede.
- configurar cada dispositivo padrão na rede.
- configurar o 1756-DNB.
- adicionar os dispositivos de E/S padrão à lista de varredura do 1756-DNB.

Ao adicionar o módulo 1756-DNB à configuração E/S do controlador, a aplicação Logix Designer cria automaticamente um conjunto de tags-padrão para dados de entrada, saída e status da rede.

Observações:

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

Tópico	Página
Adicione Dispositivos de E/S de segurança	63
Configure os dispositivos de E/S de segurança	64
Configure o endereço IP por meio da conversão de endereços de rede (NAT)	65
Definição do número da rede de segurança (SNN)	67
Usando conexões Unicast em redes EtherNet/IP	67
Definição do limite de tempo de reação da conexão	67
Compreensão da assinatura de configuração	71
Reset a Propriedade do dispositivo de E/S de Segurança	71
Endereçar dados à Dados de Endereço das E/S de Segurança	72
Monitorar o Status do dispositivo de E/S de segurança	74
Reiniciando um módulo para a condição pronto para usar	75
Substituindo um dispositivo usando a aplicação Logix Designer	75
Substitua um módulo POINT Guard I/O usando o software RSNetWorx for DeviceNet	81

Para obter mais informações sobre a instalação, configuração e operação de segurança Dispositivos de E/S, consulte a [Para mais informações na página 11](#).

Adicione 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 do nó para redes DeviceNet

Você não pode definir o endereço de nó de um dispositivo de E/S de segurança em redes DeviceNet pela aplicação do Logix Designer. Endereços do nó estão ajustados através de chaves rotativas sobre os dispositivos.

- Endereços de IP para redes EtherNet/IP

Para ajustar o endereço IP, você pode ajustar os comutadores rotativos no dispositivo; usar o software DHCP (disponível da Rockwell Automation), usar a aplicação do Logix Designer; ou recuperar o endereço padrão de memória não volátil.

- Número da rede de segurança (SNN)

Consulte a página [67](#) para obter informações sobre a configuração do SNN.

- Assinatura de configuração

Consulte a página 71 para obter informações sobre quando a assinatura de configuração é definida automaticamente e quando é necessário defini-la.

- Limite de tempo de reação

Consulte a página 67 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 GuardLogix usando aplicação do Logix Designer.

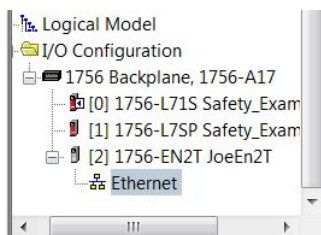
DICA Os dispositivos de E/S de segurança são compatíveis com os dados padrão e de segurança. A configuração do dispositivo define quais dados estão disponíveis.

Configure os dispositivos de E/S de segurança

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

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

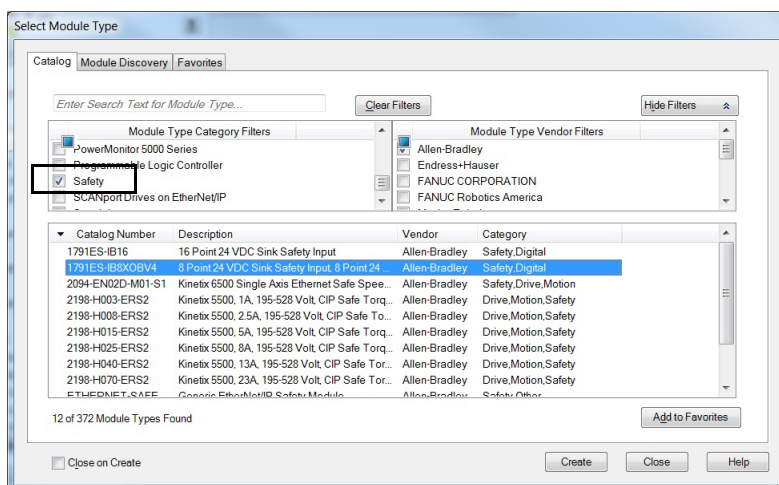
- Clique com o botão direito na rede DeviceNet ou Ethernet e escolha New Module.



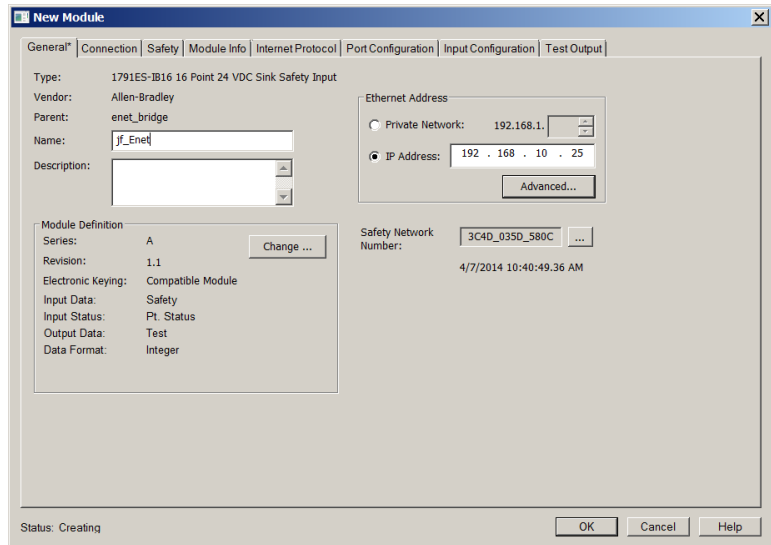
Este exemplo usa uma rede Ethernet.

- Na guia Catalog, selecione o dispositivo de E/S de segurança.

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



- Clique em Create.

4. Digite o nome do novo dispositivo.

5. Para modificar as configurações de definição de módulo, clique em Change (se necessário).
6. Digite o endereço do nó para redes DeviceNet, ou o endereço IP para redes EtherNet/IP.

Somente números de nó não utilizados estão incluídos no menu.

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 65.](#)

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

Consulte a página [67](#) para obter detalhes.

8. Defina Connection Reaction Time Limit na guia Safety.

Consulte a página [67](#) 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.

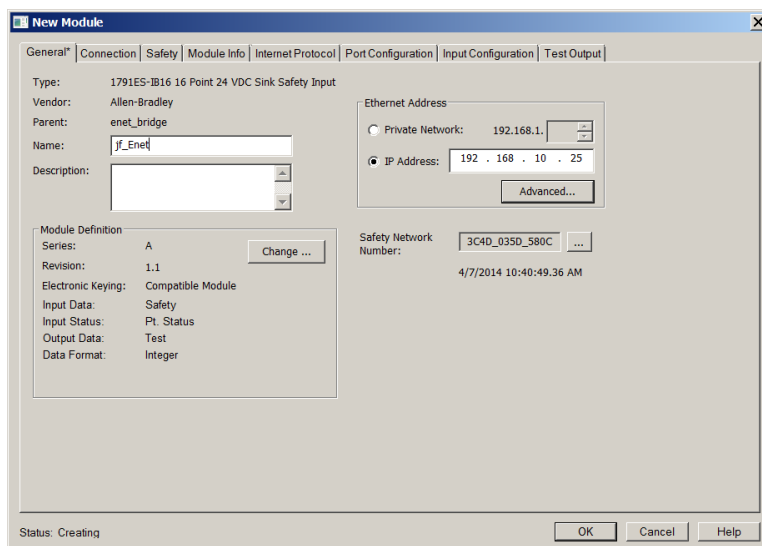
Configure o endereço IP por meio da conversão de endereços de rede (NAT)

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

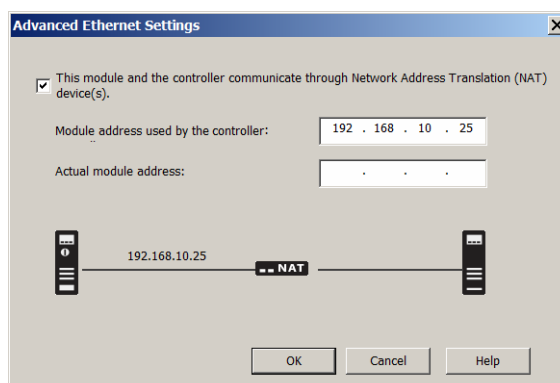
Este serviço é útil se você precisa reutilizar os endereços IP ao longo de uma rede. Por exemplo, NAT torna possível para os dispositivos serem segmentados em várias sub-redes particulares idênticas mantendo identidades únicas na sub-rede pública.

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

1. No campo IP Address, digite o endereço IP que o controlador usará.
Esse geralmente é o endereço IP na rede pública quando usando NAT.



2. Clique em Advanced para abrir a caixa de diálogo Advanced Ethernet Settings.



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 Internet Protocol do dispositivo.

5. Clique em OK.

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

Definição do número da rede de segurança (SNN)

A atribuição de um SNN baseado na hora 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 49](#).

Usando 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 Connection e selecione Use Unicast Connection over Ethernet/IP.

Definição do limite de tempo de reação da conexão

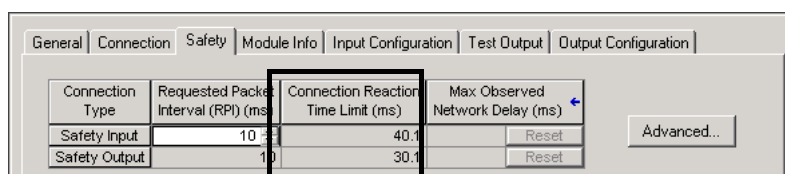
O limite de tempo de reação da conexão é a idade máxima dos pacotes de segurança na conexão associada. Se o período dos dados usado pelo dispositivo em consumo exceder o limite de tempo de reação da conexão, ocorrerá uma falha de conexão. Esse Limite é determinado pelas seguintes equações:

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 saída =
 período da tarefa de segurança x [multiplicador de tempo-limite + multiplicador de atraso da rede - 1]

O limite de tempo de reação da conexão é exibido na guia Safety da caixa de diálogo Module Properties.

Figura 18 - Limite do tempo de reação de conexão



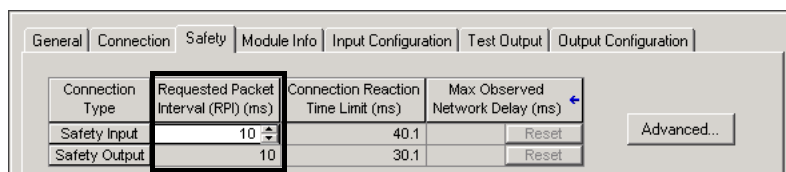
Especificar o intervalo do pacote requisitado (RPI)

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 Safety da caixa de diálogo Module Properties. O RPI é inserido em incrementos de 1 ms, com uma faixa 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 19 - 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 Safety Task Properties.

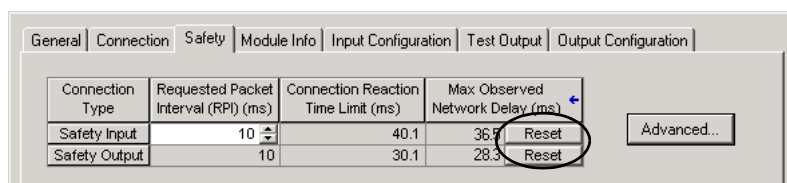
Consulte [Especificação do Período da Tarefa de Segurança na página 86](#) para mais informações sobre o período de tarefa de segurança.

Para aplicações normais, o RPI padrão é normalmente suficiente. Para requisitos mais complexos, use o botão Advanced para modificar os parâmetros do campo Connection Reaction Time Limit, conforme descrito na página 69.

Visualização do atraso máximo observado na rede

Quando o controlador 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 Properties. Quando online, clique em Reset para reiniciar o atraso de rede máximo observado.

Figura 20 - Removendo o atraso de rede máximo observado



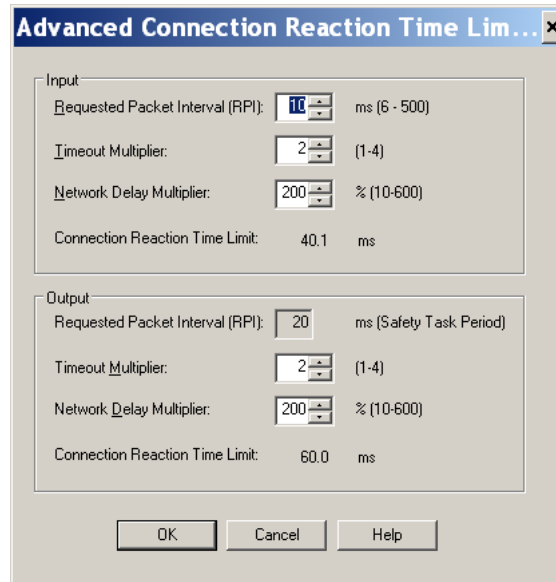
IMPORTANTE

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.

Definição dos parâmetros de limite de tempo de reação da conexão avançada

Configure os parâmetros de conexão como o multiplicador de tempo-limite e multiplicador de atraso de rede na caixa de diálogo Advanced Connection Reaction Time Limit.

Figura 21 - Configuração avançada



Multiplicador de tempo-limite

O campo Timeout Multiplier determina o número de RPIS para aguardar 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 Network Delay Multiplier define o tempo de transporte da mensagem imposto pelo protocolo CIP Safety. Esse multiplicador especifica o atraso do desarme completo do produtor ao consumidor e o conhecimento de volta ao produtor. É possível utilizá-lo para reduzir ou aumentar o valor exibido no campo Connection Reaction Time Limit quando o tempo de transporte da mensagem imposto é muito inferior ou superior ao RPI. Por exemplo, ajustar o campo Network Delay Multiplier pode ser útil quando o RPI de uma conexão de saída é igual ao Período da Tarefa de Segurança estendido.

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 relação 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:

$$200\% \times [10 \div 20] = 100\%$$

Método 2: Usar o Atraso Máximo Observado na Rede. Se o sistema for executado por muito tempo em condições problemáticas de carregamento, o campo Network Delay Multiplier 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 Network Delay Multiplier pode apresentar um valor aproximado de acordo com a seguinte equação:

$$[\text{atraso de rede máximo observado} + \text{Margin_Factor}] \div \text{RPI}$$

EXEMPLO

Cálculo do campo Network Delay Multiplier de acordo com o atraso máximo observado na rede

Se:

RPI = 50 ms

Atraso máximo observado na rede = 20 ms

Margin_Factor = 10

Portanto, multiplicador de atraso da rede será igual a:

$$[20 + 10] \div 50 = 60\%$$

Tabela 18 - Obter mais informações

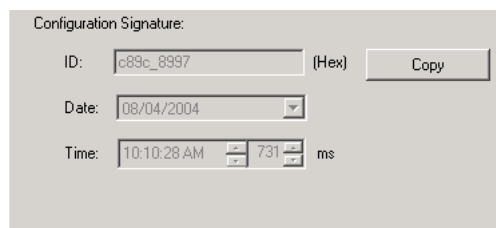
Recursos	Descrição
Manual de referência de segurança dos sistemas de controladores GuardLogix 5570, publicação 1756-RM099	Fornece informações sobre o cálculo de tempos de reação.
Guard I/O DeviceNet Safety Modules User Manual, publicação 1791DS-UM001	
Guard I/O EtherNet/IP Safety Modules User Manual, publicação 1791ES-UM001	

Compreensão da 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 visualizá-la e copiá-la na guia Safety da caixa de diálogo Module Properties.

Figura 22 - Visualize e copie a assinatura de configuração

Proprietário de configuração diferente (conexão em modo de escuta)

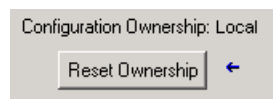
Quando a configuração do dispositivo de E/S é controlada por outro controlador, é necessário copiar a assinatura de configuração do módulo de seu projeto do proprietário e colá-la na guia Safety da caixa de diálogo Module Properties.

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.

Reset a Propriedade do dispositivo de E/S de Segurança

Quando o projeto do controlador está on-line, a guia Safety da caixa de diálogo Module Properties exibe a propriedade da configuração atual. Quando a configuração pertence ao projeto aberto, Local é exibido. Quando a configuração pertence a um segundo dispositivo, Remote 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 Communication error é exibida quando a leitura do dispositivo falha.

Quando online, clique em Reconfigurar Propriedade para reconfigurar o dispositivo para sua configuração pronta para uso.



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.

Endereçar dados à Dados de Endereço das 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 endereço do módulo de E/S de segurança segue este exemplo.

EXEMPLO Modulename.Type.Member

Tabela 19 - Formato de endereço de dispositivo de E/S de segurança

Em que	É	
Modulename	O nome do dispositivo de E/S de segurança	
Tipo	Tipo de dados	Entrada I Saída: O
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 do endereço do inversor Kinetix 5500, Kinetix 5700 e PowerFlex 527

Um endereço do inversor Kinetix 5500, Kinetix 5700, and PowerFlex 527 segue este exemplo.

EXEMPLO DriveName:Type.member

Tabela 20 - Formato de endereço de dispositivo de e/s de segurança Kinetix

Em que	É
DriveName	O nome do inversor Kinetix ou PowerFlex
Tipo	Tipo de dados Entrada IS 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 21 - Mais recursos

Recursos	Descrição
Capítulo 9, Monitorar o Status e Controlar Falhas	Contém informações sobre como monitorar dados de tags de segurança
Logix5000 Controllers I/O and Tag Data Programming Manual, publicação 1756-PM004	Fornecer 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 módulos de E/S. Consulte os manuais de Guard I/O listados na [Para mais informações na página 11](#) para obter mais informações sobre I/O a localização de falhas do módulo.

Tabela 22 - Indicador de status Operação para os módulos de Guard I/O

Indicador	Status	Descrição		
		Módulos Guard I/O DeviceNet	Módulos Guard I/O EtherNet/IP	Módulos POINT Guard I/O
Status do módulo (MS)	Desligado	Sem energia.		
	Verde, ativado	Em operação normal.		
	Verde, intermitente	Dispositivo inativo.		
	Vermelho, intermitente	Existência de uma falha recuperável.	Existe uma falha recuperável ou a atualização de um firmware está em andamento.	
	Vermelho, ativado	Existência de uma falha irrecuperável.		
	Vermelho/Verde, intermitente	Testes automáticos em andamento.	Os autotestes estão em andamento ou o módulo não está configurado corretamente. Consulte o indicador de status de rede para mais informações.	
Status da rede (NS)	Desligado	Dispositivo não online ou sem energia.		
	Verde, ativado	Dispositivo on-line; conexões estabelecidas.		
	Verde, intermitente	Dispositivo on-line; sem conexões estabelecidas.		
	Vermelho, intermitente	Tempo-limite de comunicação.	Tempo-limite de comunicação ou atualização de firmware em andamento.	
	Vermelho, ativado	Falha na comunicação. O dispositivo detectou um erro que impediu a comunicação da rede.		
	Vermelho/Verde, intermitente	O dispositivo está em estado Comunicação com falha ou o número da rede de segurança (SNN) está sendo ajustado.	Auto-teste em andamento.	Não aplicável.
Pontos de entrada (INx)	Desligado	Entrada de segurança OFF.		
	Amarelo, ativado	Entrada de segurança ON.		
	Vermelho, ativado	Erro no circuito de entrada.		
	Vermelho, intermitente	Quando a operação de canal duplo estiver selecionada, ocorrerá um erro no circuito de entrada do parceiro.		
Pontos de saída (Ox)	Desligado	Entrada de segurança OFF.		
	Amarelo, ativado	Entrada de segurança ON.		
	Vermelho, ativado	Erro no circuito de saída.		
	Vermelho, intermitente	Quando a operação de canal duplo estiver selecionada, ocorrerá um erro no circuito de saída do parceiro.		
Pontos de saída de teste (Tx)	Desligado	Não aplicável.	A saída está desenergizada.	Não aplicável.
	Amarelo, ativado		A saída está energizada.	
	Vermelho, ativado		Erro no circuito de saída.	
LOCK	Amarelo, ativado	Configuração do dispositivo protegida.	A aplicação Logix Designer não suporta esta função.	
	Amarelo, intermitente	Configuração do dispositivo válida, mas dispositivo desprotegido.		
	Amarelo, desativado	Inválido, sem dados de configuração, ou o dispositivo foi configurado.		
IN PWR	Verde, desativado	Sem alimentação de entrada.		Não aplicável.
	Verde, ativado	A tensão de alimentação de entrada está dentro da especificação.		
	Amarelo, ativado	A tensão de alimentação de entrada está fora da especificação.		
OUT PWR	Verde, desativado	Sem potência de saída.		
	Verde, ativado	A tensão da potência de saída está dentro da especificação.		
	Amarelo, ativado	A tensão da potência de saída está fora da especificação.		
PWR	Verde, desativado	Não aplicável.		Sem energia.
	Verde, ativado			A tensão de alimentação está dentro da especificação.
	Amarelo, ativado			A tensão de alimentação está fora da especificação.

Consulte [página 11](#) para obter mais informações sobre os indicadores de status do inversor Kinetix 5500, Kinetix 5700 e PowerFlex 527.

Reiniciando um módulo para a condição pronto para usar

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 “pronto para usar”.

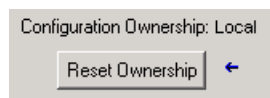
Quando o projeto do controlador está on-line, a guia Safety da caixa de diálogo Module Properties exibe a propriedade da configuração atual. Quando a configuração pertence ao projeto aberto, Local é exibido. Quando a configuração pertence a um segundo dispositivo, Remote é exibido, com o número da rede de segurança (SNN) e o endereço de nó ou o número de slot do controlador da configuração. A mensagem Communication error 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 estas etapas para inibir o módulo.

1. Com o botão direito, clique no módulo e escolha Properties.
2. Clique na guia Connection.
3. Marque Inhibit Connection.
4. Clique em Apply e então OK.

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

1. Com o botão direito, clique no módulo e escolha Properties.
2. Clique na guia Safety.
3. Clique em Reset Ownership.



Substituindo um dispositivo usando a aplicação Logix Designer

Pode-se usar a aplicação Logix Designer para substituir um dispositivo Guard I/O em uma rede Ethernet. Para substituir um módulo Guard I/O em uma rede DeviceNet, a sua escolha depende do tipo de módulo.

Tabela 23 - Software

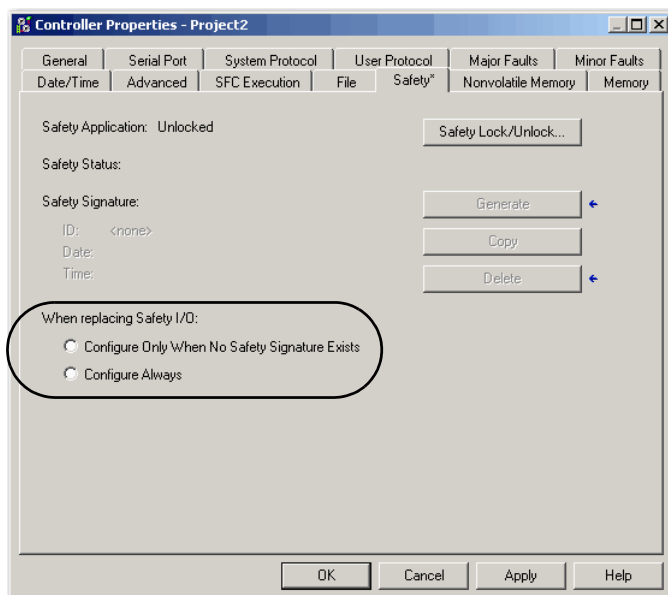
Se você está usando um	Use	Consulte
Módulo 1791DS Guard I/O com adaptador 1756-DNB	A aplicação Logix Designer	Abaixo
Módulo 1734 POINT Guard I/O com um adaptador 1734-PDN	Software RSNetWorx para DeviceNet	Substitua um módulo POINT Guard I/O usando o software RSNetWorx for DeviceNet na página 81

Se você estiver considerando uma parte do sistema CIP Safety para manter o comportamento SIL 3 durante a substituição e o teste funcional de um dispositivo, a função Configure Always não pode ser usada. Vá para [Substituição com “Configure only when no safety signature exists” habilitado na página 76](#).

Se o sistema de controle CIP Safety inteiro roteável não precisar manter o SIL 3/PL durante a substituição e o teste de funcionamento de um módulo, a função Configure Always poderá ser usada. Vá para [Substituição com “Configure Always” habilitado na página 80](#).

Substituição de dispositivo de segurança de E/S é configurada na Guia de segurança do GuardLogix controlador.

Figura 23 - Substituição de dispositivo de E/S de segurança



Substituição com “Configure only when no safety signature exists” habilitado

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.

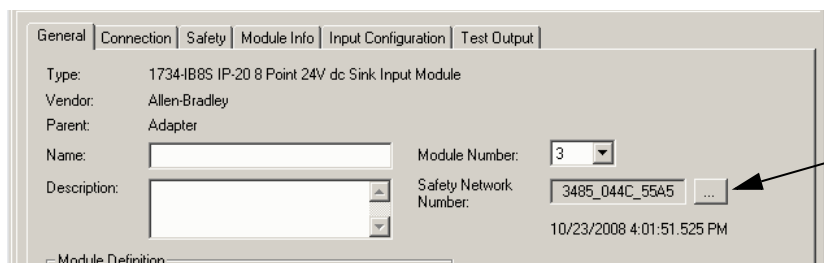
Se o projeto for configurado como “Configure only when no safety signature exists”, siga as etapas adequadas em [Tabela 24](#) para substituir um dispositivo de E/S de segurança baseado na sua situação. Uma vez que você completou as etapas corretamente, o DeviceID irá combinar com o original, habilitando o controlador de segurança para fazer download da configuração de dispositivo adequada e restabelecer a conexão de segurança.

Tabela 24 - Substituindo um módulo

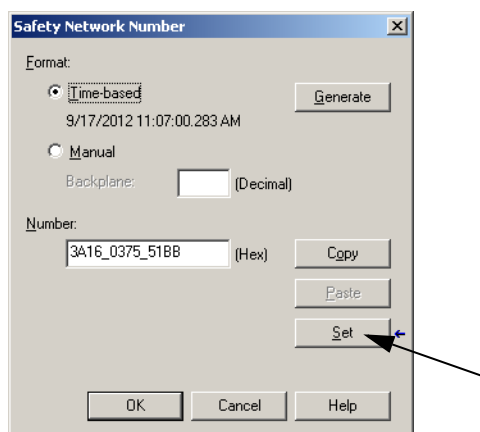
Quando existir a assinatura de segurança GuardLogix	Condição de substituição de módulo	Ação necessária
Negativo	Sem SNN (fora da caixa)	Nenhuma. O dispositivo está pronto para o uso.
Sim ou Não	O mesmo SNN conforme a configuração de tarefa de segurança original	Nenhuma. O dispositivo está pronto para o uso.
Sim	Sem SNN (fora da caixa)	Consulte Situação 1 – O dispositivo de substituição está Pronto para uso e a assinatura de segurança existe na página 77.
Sim	SNN diferente da configuração de tarefa de segurança original	Consulte Situação 2 – O dispositivo de substituição SNN é diferente do original e a assinatura de segurança existe na página 78.
Negativo	SNN diferente da configuração de tarefa de segurança original	Consulte Situação 3 – O dispositivo de substituição SNN é diferente do original e a assinatura de segurança não existe na página 79.

Situação 1 – O dispositivo de substituição está Pronto para uso e a assinatura de segurança existe

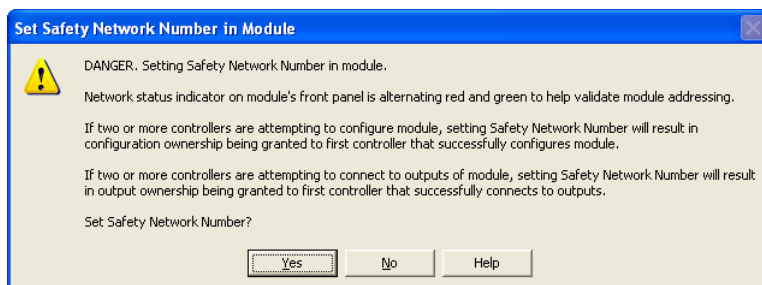
1. Remoção do dispositivo de E/S antigo e instalação de um novo dispositivo.
2. Clique com o botão direito no dispositivo de E/S de segurança de substituição e escolha Propriedades.
3. Clique em à direita do número da rede de segurança para abrir a caixa de diálogo Safety Network Number.



4. Clique em Set.



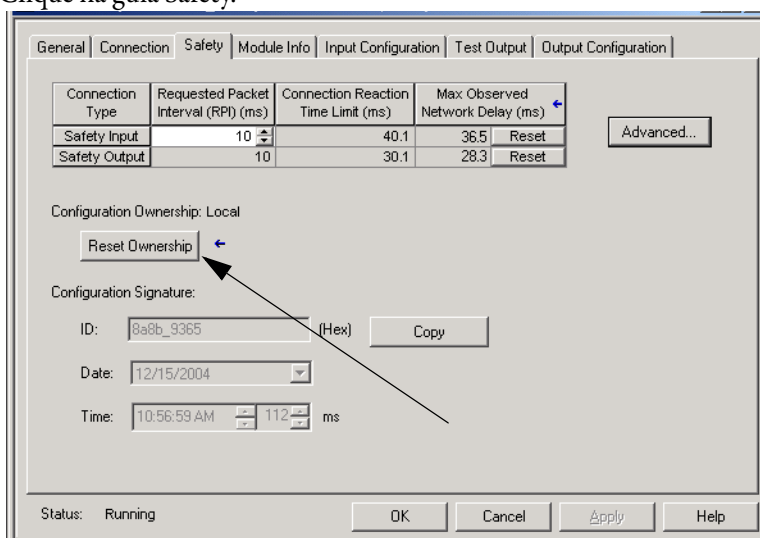
5. Verifique que o indicador de status de rede (NS) esteja alternando vermelho/verde no módulo correto antes de clicar Yes na caixa de diálogo de confirmação para ajustar o SNN e aceitar o dispositivo de substituição.



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.

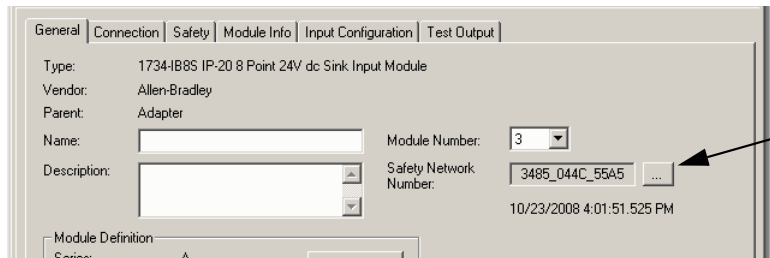
Situação 2 – O dispositivo de substituição SNN é diferente do original e a assinatura de segurança existe

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 Properties.
3. Clique na guia Safety.

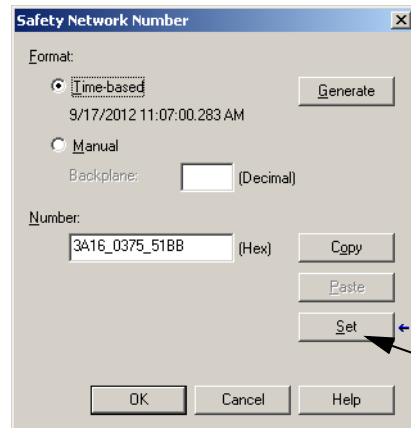


4. Clique em Reset Ownership.
5. Clique em OK.
6. Com o botão direito no dispositivo e escolha Properties.

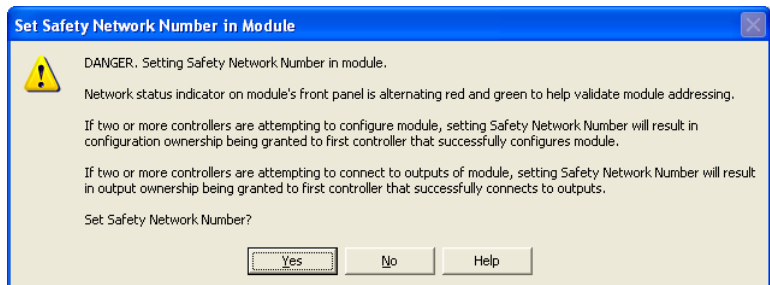
7. Clique em [...] à direita do número da rede de segurança para abrir a caixa de diálogo Safety Network Number.



8. Clique em Set.



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

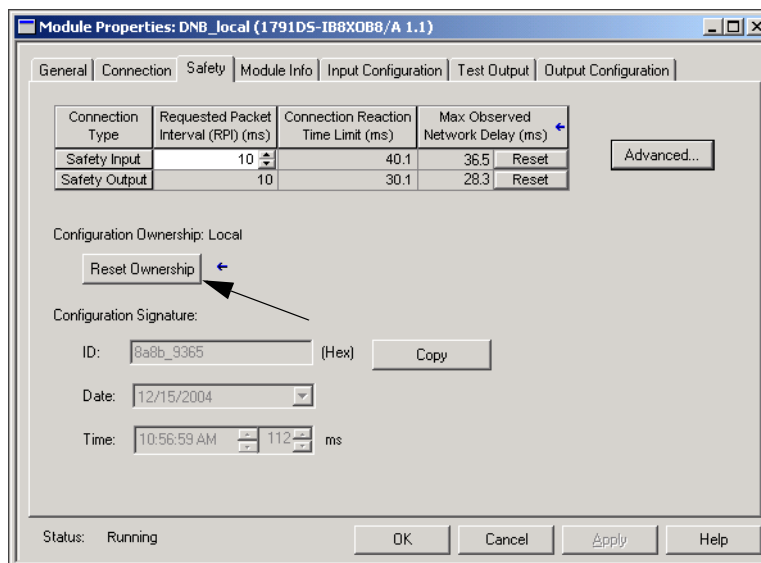


10. Siga os procedimentos descritos pela empresa para testar a funcionalidade do dispositivo e sistema de E/S substituído e autorizar o sistema para uso.

Situação 3 – O dispositivo de substituição SNN 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 Properties.

3. Clique na guia Safety.



4. Clique em Reset Ownership.

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 “Configure Always” habilitado



ATENÇÃO: Habilite a função “Configure Always” apenas se todo o sistema de controle de segurança CIP **não** estiver sendo responsável por manter o comportamento SIL 3 durante a substituição e teste funcional de um dispositivo.

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

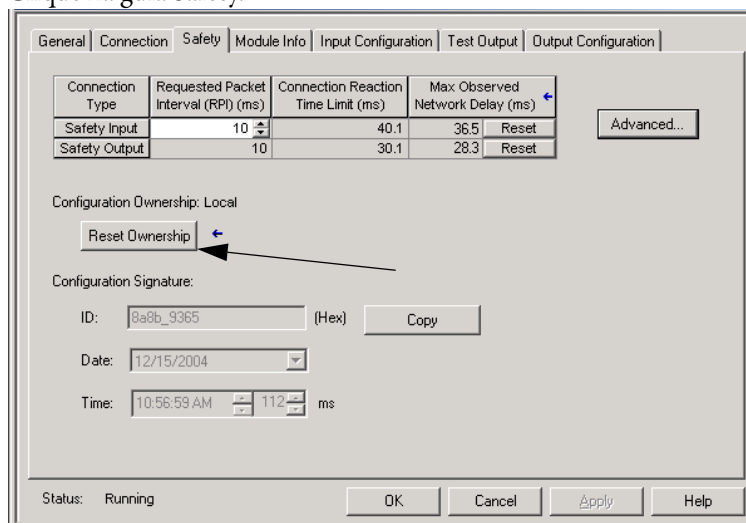
Quando a função “Configure Always” estiver habilitada no projeto do controlador, o controlador verificará automaticamente e se conectará a um dispositivo de substituição que atenda a todas as especificações a seguir:

- 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 “Configure Always”, 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 fora da caixa, vá para a etapa 6. Nenhuma ação é necessária para que o controlador 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 Properties.
3. Clique na guia Safety.



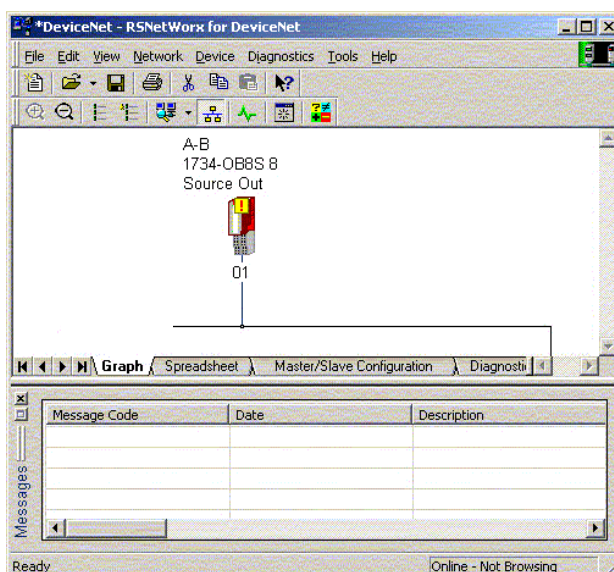
4. Clique em Reset Ownership.
5. Clique em OK.
6. Siga os procedimentos descritos pela empresa para testar a funcionalidade do dispositivo e sistema de E/S substituído e autorizar o sistema para uso.

Substitua um módulo POINT Guard I/O usando o software RSNetWorx for DeviceNet

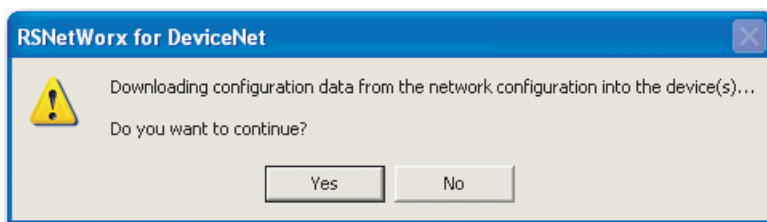
Siga estas etapas para substituir um módulo POINT Guard I/O quando o módulo e o controlador estiverem em uma rede DeviceNet.

1. Substitua o módulo e combine o número de nó com o do módulo original.
2. No software RSNetWorx for DeviceNet, abra o seu projeto.

Se o módulo de substituição estiver na condição “pronto para usar” ou tiver um SNN que não combina com o módulo original, o módulo aparece com um ponto de exclamação.



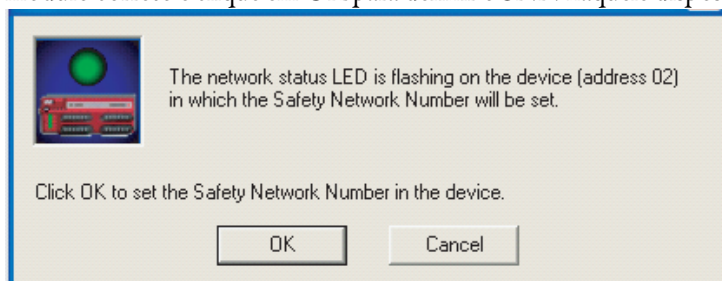
3. Com o botão direito, clique no módulo e escolha Download to Device.



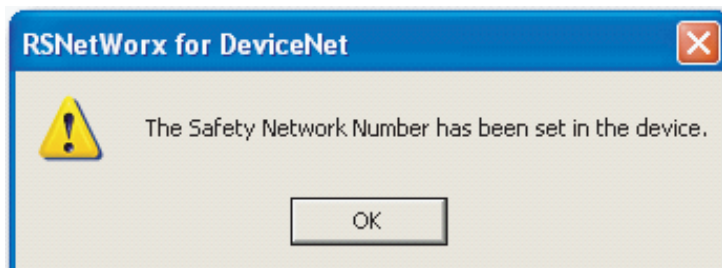
4. Clique em Yes para confirmar.
5. Clique em Download na caixa de diálogo Safety Network Number Mismatch para definir o SNN no módulo de substituição.



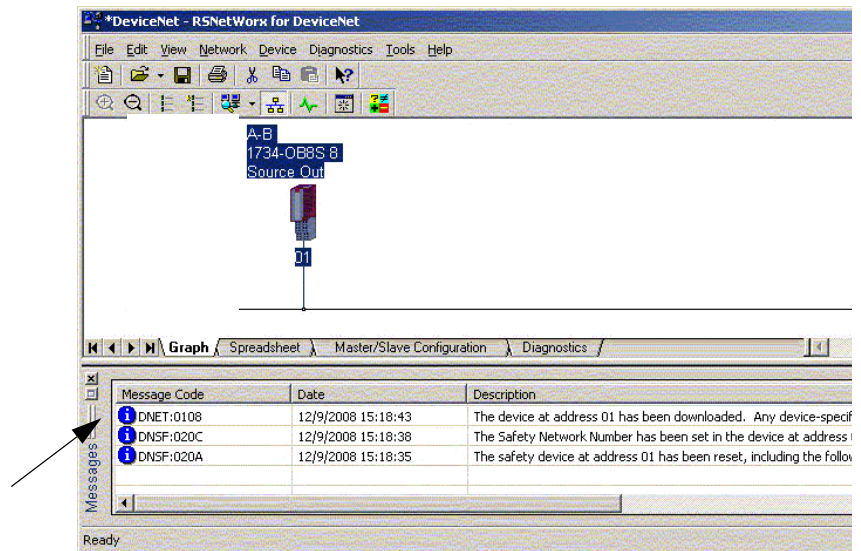
6. Certifique-se de que o indicador de status de rede (NS) está piscando no módulo correto e clique em OK para definir o SNN naquele dispositivo.



O software RSNetWorx for DeviceNet confirma que o SNN foi definido.



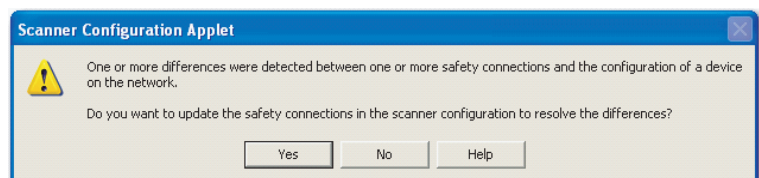
Uma vez que o download for completado com sucesso, a visualização do projeto principal exibe esta mensagem: “The device at address .xx has been downloaded. Any device-specific messages related to the download operation are displayed separately.”



Considerando que esta seja a configuração adequada a partir do arquivo DNT original, o SNN e a assinatura de configuração agora combinam com o original. Se você já estiver conectado ao controlador, uma conexão é feita. O controlador não precisa ser tirado do modo de operação para fazer download do módulo de substituição.

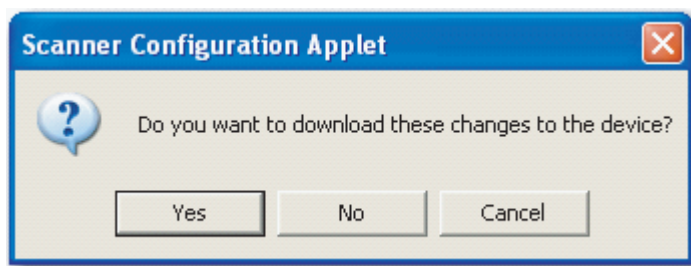
Se fez-se download desta configuração em um ajuste temporário, coloque o módulo na rede e ele se conectará automaticamente ao controlador.

Se a configuração da que se fez download no módulo não for do arquivo DNT original, a assinatura de configuração não combinará com o original. Mesmo que você recrie os mesmos parâmetros em um novo arquivo DNT, as porções de hora e data da assinatura serão diferentes, portanto, a conexão ao controlador não é feita. Se isto ocorrer, clique na guia Safety Connection para o controlador que indicou que a assinatura de configuração é diferente e ele oferece a opção de combinar a nova assinatura de configuração. Entretanto, deve-se primeiro revalidar o sistema de segurança, porque não está usando o arquivo DNT original.



7. Clique em Yes.

Isto tira o controlador do modo de operação e solicita que faça download destas mudanças.



8. Clique em Yes para fazer download da nova configuração de conexão ao controlador.

Depois que o download estiver completo, coloque o controlador novamente no modo de operação e a conexão com o módulo de substituição é estabelecida.

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

Criação de Aplicações de Segurança

Tópico	Página
Tarefa de Segurança	86
Programas de Segurança	87
Rotinas de Segurança	88
Tags de Segurança	88
Tags de segurança produzidas/consumidas	92
Mapeamento de tags de segurança	98
Proteção de aplicações de segurança	100
Restrições de programação	103

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 controladores GuardLogix 5570, publicação [1756-RM099](#).

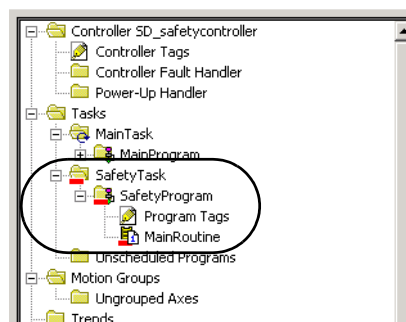
Esse manual de referência de segurança abrange o seguinte:

- A criação de uma especificação de projeto detalhada
- A escrita, a documentação e o teste da aplicação
- A criação da 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
- O bloqueio da aplicação de segurança
- O cálculo do tempo de reação do sistema

Tarefa de Segurança

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

Figura 24 - Tarefa de segurança no organizador do controlador



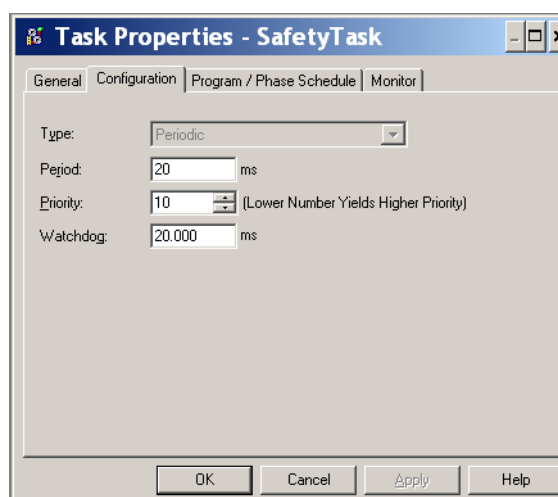
Na tarefa de segurança, você pode usar vários programas de segurança, compostos por várias rotinas de segurança. O controlador GuardLogix suporta uma tarefa de segurança. A tarefa de segurança não pode ser removida.

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 Task Properties – Safety Task. Abra a caixa de diálogo, clique com o botão direito na tarefa de segurança e escolha Properties.

Figura 25 - 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 máximo pode ser 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 irreversível 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 controladores GuardLogix 5570, publicação [1756-RM099](#), fornece informações detalhadas sobre o cálculo do tempo de reação do sistema.

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 [98](#) 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

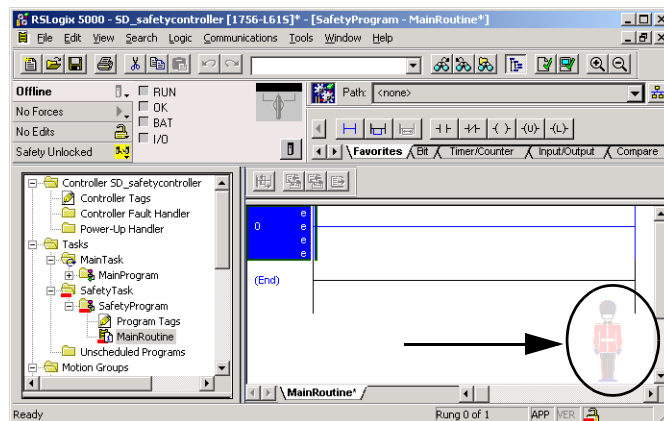
Os programas de segurança apresentam todos os atributos de programas padrão, porém eles só podem ser programados na tarefa de segurança e podem conter somente componentes de segurança. Programas de segurança podem conter apenas rotinas de segurança. Uma rotina de segurança deve ser considerada a rotina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

Um 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. Os 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 New Tag clicando com o botão direito em Controller Tags ou Program Tags e escolha New Tag.

Figura 26 - Criando um novo tag

The 'New Tag' dialog box contains the following fields and options:

- Name:** Text input field.
- Description:** Text area.
- Usage:** Dropdown menu with '<normal>' selected.
- Type:** Dropdown menu with 'Base' selected, and a 'Connection...' button.
- Alias For:** Text input field.
- Data Type:** Dropdown menu with 'DINT' selected, and an ellipsis button.
- Scope:** Dropdown menu with 'SafetyProgram' selected.
- Class:** Dropdown menu with 'Safety' selected.
- External Access:** Dropdown menu with 'Read/Write' selected.
- Style:** Dropdown menu with 'Decimal' selected.
- Constant:** Unchecked checkbox.
- Open Configuration:** Unchecked checkbox.
- Buttons:** OK, Cancel, and Help.

Tipo de tag

[Tabela 25](#) define os quatro tipos de tags.

Tabela 25 - Quatro tipos de tags

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 98 .
tag produzido	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 do tag produzido são enviados noRPI do tag em consumo.
Tag consumido	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 dos dados que a tag armazena, como um bit ou um 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 26 - 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

Os tags de segurança do controlador são todos os programas que 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 98](#) para obter mais informações.

É possível fazer a leitura de tags de segurança com escopo no controlador, porém 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 associados a dados de segurança produzidos ou consumidos e à E/S de segurança 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 27 - Recursos adicionais

Recursos	Descrição
Conexões de Segurança na página 121	Fornecer mais informações sobre o membro CONNECTION_STATUS
Logix5000 Controllers I/O and Tag Data Programming Manual, publicação 1756-PM004	Fornecer instruções para a criação de tipos de dados definidos pelo usuário

Tags com escopo do programa

Quando os tags são do programa, os dados são isolados de outros programas. A reutilização de nomes de tags do programa é permitida entre programas.

Os tags de segurança do programa de segurança podem ser lidos ou gravados somente por meio de uma rotina com escopo no mesmo programa de segurança.

Classe

Os tags podem ser classificados 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 um tag como um valor constante, não é possível modificá-lo pela lógica no controlador ou por uma aplicação externa, como uma IHM. Os tags de valor de constante não podem ser forçados.

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. Os tags de segurança não podem ser modificados se uma assinatura da tarefa de segurança estiver presente.

Acesso externo

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

Tabela 28 - 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 transferir dados de segurança entre controladores GuardLogix, você utiliza tags de segurança produzidos e consumidos. Tags produzidos e consumidos precisam de conexões. O tipo de conexão-padrão para tags produzidos e consumidos é unicast.

Tabela 29 - Conexões produzidas e consumidas

Tag	Descrição da conexão
Produzida	Um controlador GuardLogix pode produzir (enviar) tags de segurança a outros controladores GuardLogix 1756 ou 1768. O controlador produtor utiliza uma única conexão para cada consumidor.
Consumida	GuardLogix Os controladores podem consumir (receber) tags de segurança de outros controladores GuardLogix 1756 ou 1768. 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 intervalo do pacote requisitado (RPI) do tag de segurança consumido deve corresponder ao período da tarefa de segurança do controlador GuardLogix produtor.

Para configurar adequadamente os tags de segurança produzidos e consumidos para compartilhar os dados entre controladores de segurança peer, deve-se configurar adequadamente os controladores de segurança peer, produzir um tag de segurança e consumir um tag de segurança, conforme descrito abaixo.

Configure os números de 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 precisa ter também um número da rede de segurança (SNN). Esse SNN de segurança peer depende de sua colocação no sistema.

Tabela 30 - Posicionamento do SNN e do controlador

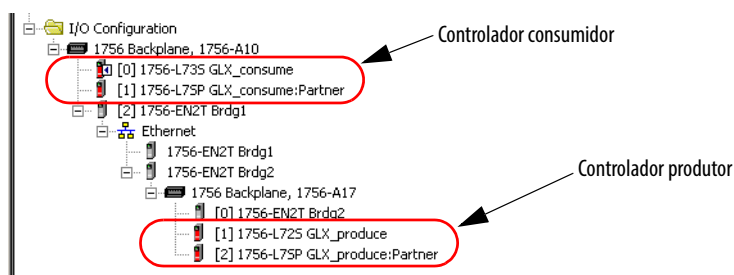
Localização do controlador de segurança peer	SNN
Colocado no rack local	Controladores GuardLogix em um rack comum têm a mesma SNN.
Colocado em outro rack	O controlador precisa ter um SNN exclusivo.

Siga estas etapas para copiar e colar o SNN.

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

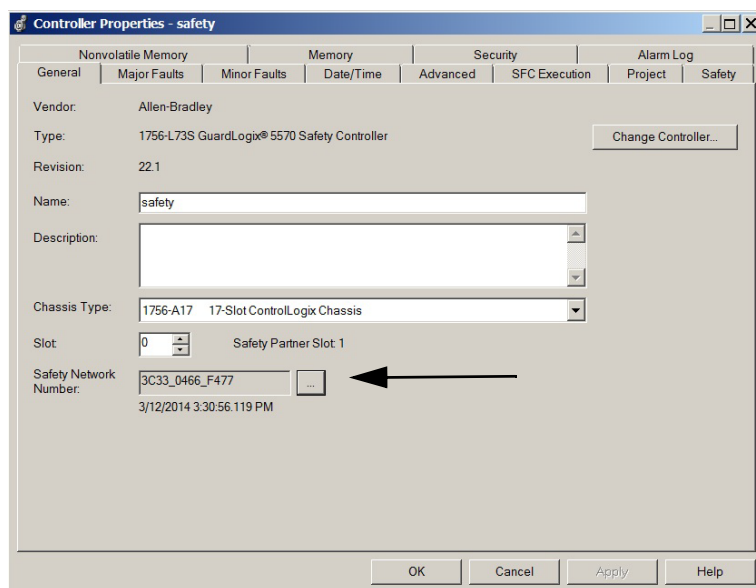
DICA

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.

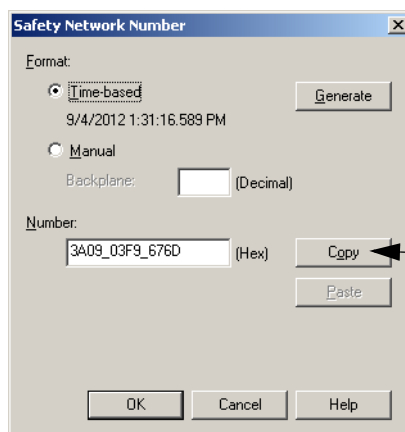


2. No projeto do controlador produtor, clique com o botão direito do mouse no controlador produtor e escolha Controller Properties.

3. Clique em  para abrir a caixa de diálogo Safety Network Number.



4. Copie o SNN do controlador produtor.



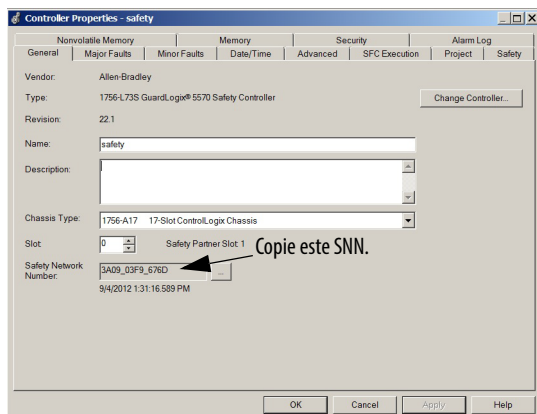
5. No projeto do controlador consumidor, clique com o botão direito do mouse no controlador produtor e escolha Module Properties.

6. Clique em  para abrir a caixa de diálogo Safety Network Number.

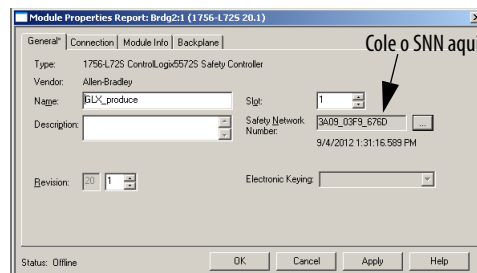
7. Cole o SNN do controlador produtor no campo SNN e clique em OK.

Os números da rede de segurança combinam.

Caixa de diálogo Controller Properties do produtor no projeto produtor



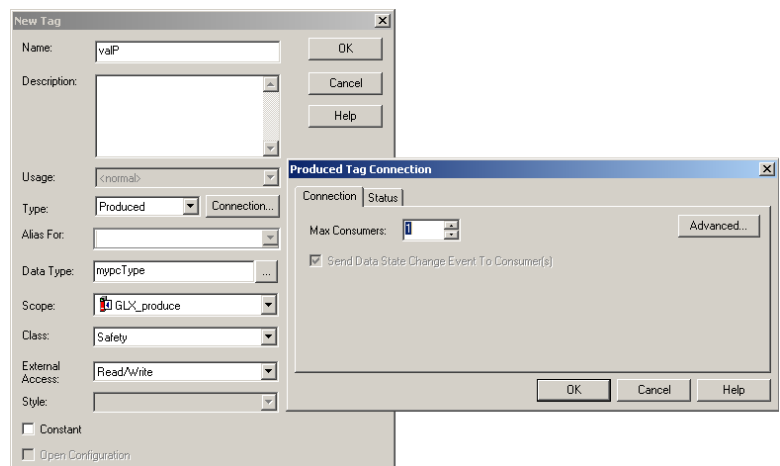
Caixa de diálogo Module Properties no projeto do consumidor



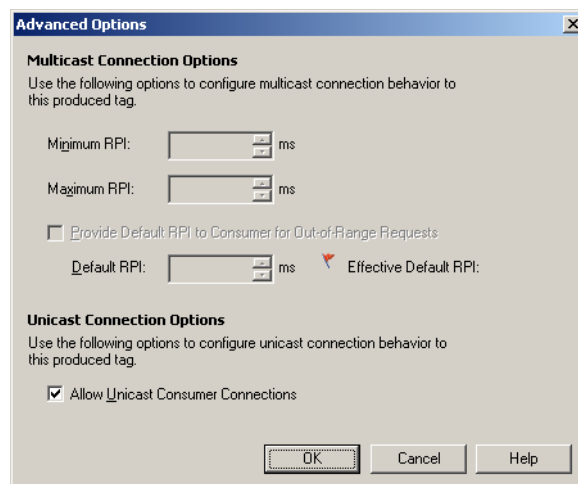
Produzir um tag de segurança

Siga este procedimento para produzir um 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 Controller Tags e escolha New Tag.
3. Defina o tipo como Produced, a classe como Safety e o tipo de dados como o tipo definido pelo usuário que foi criado na etapa 1.
4. Clique em Connection e insira o número de consumidores.



5. Clique em Advanced se quiser mudar o tipo de conexão desselecionando “Allow Unicast Consumer Connections”.



6. Clique em OK.

Consumir dados de tags de segurança

Siga estas etapas para consumir 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 Controller Tags e escolha New Tag.
3. Defina o tipo como Consumed, a classe como Safety e o tipo de dados como o tipo definido pelo usuário que foi criado na etapa [1](#).



4. Clique em Connection para abrir a caixa de diálogo Consumed Tag Connection.

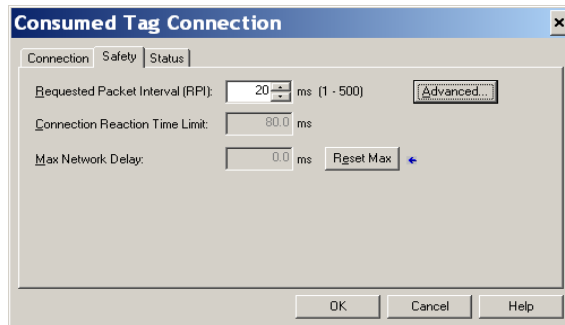


5. No menu suspenso produtor, selecione o controlador que produz os dados.
6. No campo de dados remoto, digite o nome da tag produzida.
7. Clique na guia Safety.

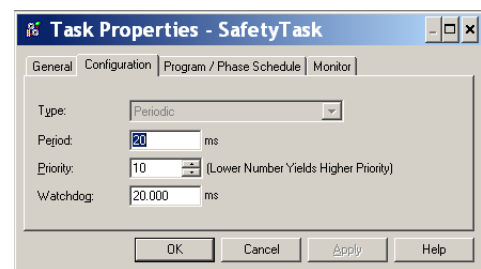
8. No campo Requisitado intervalo do pacote (RPI), digite o RPI para a conexão em incrementos de 1 MS.

O padrão é 20 ms.

Projeto Consumidor



Projeto Produtor

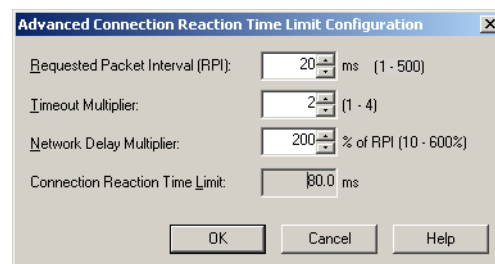


A RPI especifica o período quando os dados atualizam através de uma conexão. O RPI do tag de segurança consumido precisa ser compatível com o período da tarefa de segurança do projeto produtor de segurança.

O limite de tempo de reação da conexão é a idade máxima dos pacotes de segurança na conexão associada. Para restrições simples de temporização, o limite de tempo de reação da conexão pode ser obtido por meio do ajuste do RPI.

Max. Network Delay 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 Max Reset para reiniciar o atraso de rede Max.

9. Se o limite do tempo Connection Reaction for aceitável, clique em OK; ou para especificações mais complexas, clique em Advanced para definir os parâmetros Advanced Connection Reaction Time Limit.



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

O campo Network Delay Multiplier define o tempo de transporte da mensagem imposto pelo protocolo CIP Safety. Esse campo especifica o atraso do ciclo completo do produtor até o consumidor e de volta ao produtor. Você pode usar o campo Network Delay Multiplier para aumentar ou diminuir o valor do campo Connection Reaction Time Limit.

Tabela 31 - Mais recursos

Recursos	Descrição
Páginas 67...69	Fornecer mais informações sobre ajuste de RPI e uma explicação sobre como o atraso de rede máximo, o multiplicador de tempo-limite e os multiplicadores de atraso de rede afetam o tempo de reação de conexão
Capítulo 9	Contém informações sobre o tipo de dados predefinido CONNECTION_STATUS
Logix5000 Controllers Produced and Consumed Tags Programming Manual, publicação publicação 1756-PM011	Fornecer 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 do 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 do tag de segurança está sujeito a estas 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 um tag padrão em um tag de segurança que foi designado 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.

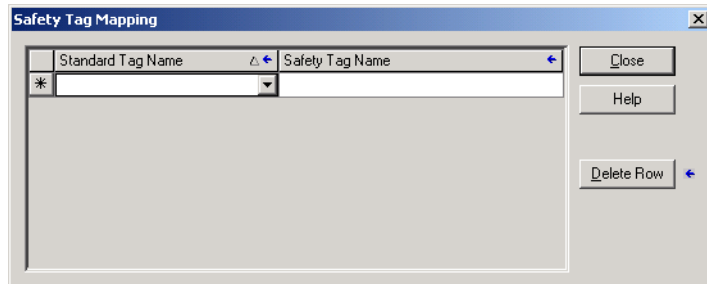


ATENÇÃO: Quando usar dados padrão em uma rotina de segurança, você deve verificar que os dados são usados de forma adequada. O uso de dados padrão em um tag de segurança não os torna dados de segurança. Não é possível controlar diretamente uma saída de segurança SIL 3/PL com dados de tag padrão.

Consulte o Manual de referência dos sistemas de controladores GuardLogix 5570, publicação [1756-RM099](#), para mais informações.

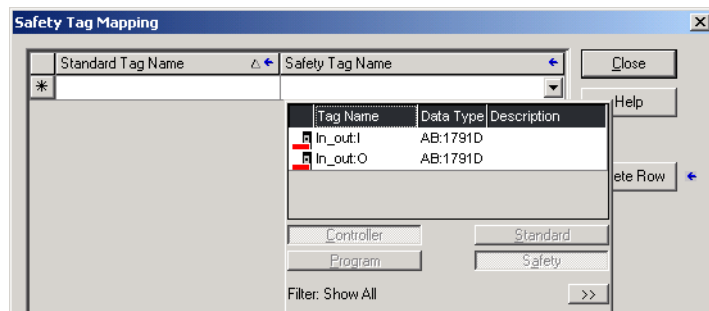
Criar pares para mapeamento de tags

1. Escolha Map Safety Tags no menu Logic para abrir a caixa de diálogo Safety Tag Mapping.



2. Adicione um tag existente à coluna Standard Tag Name ou Safety Tag Name 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 Standard Tag Name ou Safety Tag Name clicando com o botão direito do mouse na célula vazia e selecionado New Tag e digitando o nome do tag na célula.
4. Clique com o botão direito do mouse na célula e escolha New tagname, onde tagname é o texto inserido na célula.

Monitorar o status de mapeamento de tags

A coluna à esquerda da caixa de diálogo Safety Tag Mapping indica o status do par mapeado.

Tabela 32 - 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 Safety Tag Mapping. ⁽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 Safety Tag Mapping se ocorrer um erro de mapeamento de tags.
	Indica a sequência atualmente em enfoque.
	Representa a sequência Create New Mapped Tag.
	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 mais informações, consulte as restrições de mapeamento de tag na página [98](#).

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.

Bloqueio de segurança do controlador

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 somente aos componentes de segurança, como tarefas, programas, rotinas, instruções Add-On, tags de segurança, E/S de segurança e assinatura de tarefa de segurança.

As ações a seguir não são permitidas na parte de segurança da aplicação quando o controlador estiver com trava de segurança:

- edição e programação on-line/off-line (inclusive Instruções Add-On 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 online indica o status de 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 com bloqueio de segurança
-  = controlador sem bloqueio de segurança

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.

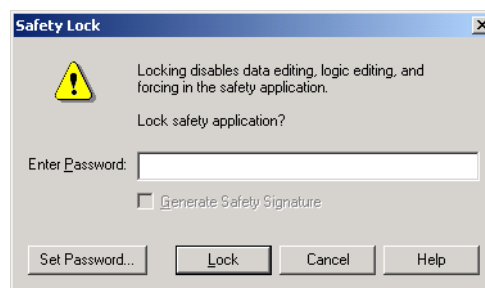
Os status bloqueado por segurança e desbloqueado por segurança não podem ser alterados quando a chave seletora está na posição RUN.

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 Logix5000 Controllers Controller Information and Status Programming Manual, publicação [1756-PM015](#).

Você pode travar e destravar por segurança o controlador na guia Safety da caixa de diálogo Controller Properties ou ao selecionar Tools>Safety>Safety Lock/Unlock.

Figura 27 - Bloqueando o controlador com trava de segurança



Se configurar uma senha para a função de trava de segurança, você deve digitá-la no campo Enter Password. Caso contrário, clique em Lock.

Você também pode configurar ou mudar a senha na caixa de diálogo Safety Lock. Consulte a página [42](#).

O recurso de trava de segurança, descrito nesta seção, e as medidas-padrão de segurança na aplicação Logix Designer são aplicáveis aos GuardLogix projetos do controlador.

Consulte o Manual de programação de segurança dos controladores Logix5000, publicação [1756-PM016](#), para informações sobre os recursos de segurança do Logix Designer.

Criação de uma assinatura de tarefa de segurança

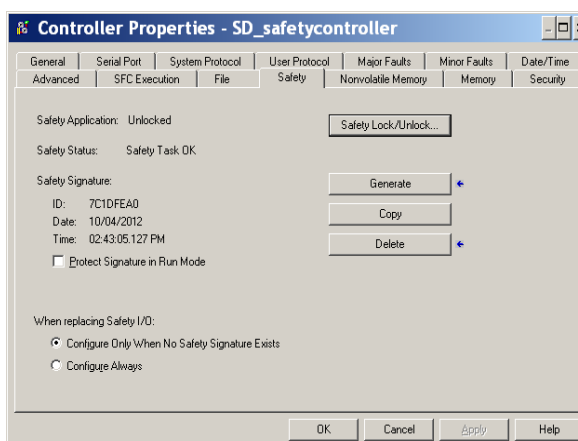
Antes de executar o teste de verificação, é necessário gerar a assinatura de tarefa de segurança. Você pode criá-la somente quando o controlador GuardLogix on-line, no modo programa, desprotegido e sem imposições de segurança, edições de segurança on-line pendentes ou falhas de segurança. O status de segurança deve ser Safety Task OK.

E ainda, você não pode gerar uma assinatura de tarefa de segurança se o controlador estiver no modo de operação com a proteção ao modo de operação habilitada.

DICA Você pode visualizar o status de segurança por meio do botão Safety Status na barra on-line (consulte a página [120](#)) ou na guia Safety da caixa de diálogo Controller Properties, conforme exibido na página [102](#).

Clique em Generate para gerar a assinatura de tarefa de segurança na guia Safety da caixa de diálogo Controller Properties. Você também pode escolher ferramentas Tools>Safety>Generate Signature.

Figura 28 - Guia safety



Se já existir uma assinatura, será necessário sobrescrevê-la.

DICA A criação e a exclusão da assinatura da tarefa de segurança são registradas no controlador.

Para mais informações sobre acesso ao log do controlador, consulte o Logix5000 Controllers Controller Information and Status Programming Manual, publicação [1756-PM015](#).

Quando existir uma assinatura de tarefa de segurança, as seguintes ações não serão permitidas na parte de segurança da aplicação:

- Edição e programação on-line/off-line (inclusive instruções add-on de segurança)
- Forçando 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)

Cópia da 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.

Remover 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 estiver no modo de operação com a chave seletora em RUN.
- O controlador estiver no modo 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/PL.

Consulte o Manual de referência de segurança dos sistemas de controladores GuardLogix 5570, publicação [1756-RM099](#), para mais informações sobre as especificações SIL 3/PL.

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 proteger os componentes de segurança de modificações sempre que o seguinte for verdade:

- o controlador estiver protegido.
- Uma assinatura de tarefa de segurança existir.
- existirem falhas de segurança.
- o status de segurança for conforme o seguinte:
 - 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 add-on 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 estiverem 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.

Comunicação com o Controlador

Tópico	Página
Conexão do controlador à rede	105
Compreensão dos fatores que afetam a entrada em comunicação	106
Download	108
Upload	110
Ficar on-line	111

Conexão do controlador à rede

Caso ainda não tenha realizado este procedimento, conecte o controlador à rede.

Tabela 33 - Conexões de comunicação

Para este tipo de conexão	Use	Consulte
USB	Cabo USB 2.0	Faça conexões de comunicação na página 29
EtherNet/IP	Dispositivo EtherNet/IP em um slot aberto no mesmo rack do controlador	Conecte seu dispositivo e o computador EtherNet/IP na página 105
DeviceNet	Módulo 1756-DNB em um slot aberto no mesmo rack do controlador	Conectar o modo de comunicação ControlNet ou o scanner DeviceNet e o seu computador na página 106
ControlNet	Módulo 1756-CN2 em um slot aberto no mesmo rack do controlador	

Conecte seu dispositivo e o computador EtherNet/IP

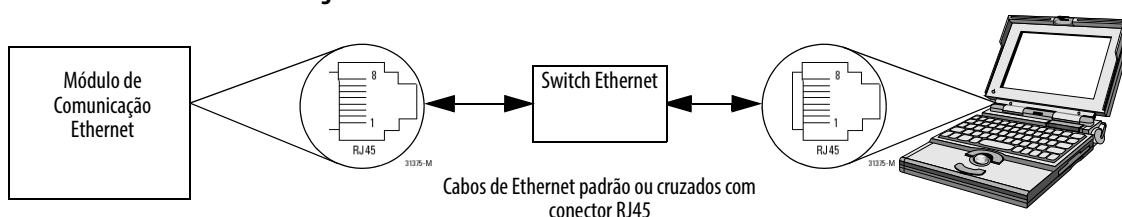


ADVERTÊNCIA: Se o cabo de comunicação for conectado ou desconectado com a aplicação aplicada a este módulo ou a qualquer dispositivo na rede, um arco elétrico pode ocorrer. Isto pode causar uma explosão em instalações reconhecidas como área classificada.

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

Conecte o dispositivo e o computador à EtherNet/IP usando um cabo Ethernet.

Figura 29 - Conexões Ethernet



Conectar o modo de comunicação ControlNet ou o scanner DeviceNet e o seu computador

Para acessar a rede ControlNet ou DeviceNet, pode-se fazer um dos seguintes:

- conectar-se diretamente à rede.
- conectar-se a uma rede serial ou EtherNet/IP e navegar (fazer ponte) até a rede desejada. Isto não requer uma programação adicional.

Configuração de um driver EtherNet/IP, ControlNet ou DeviceNet

Para informações sobre a configuração de um driver, consulte a publicação apropriada:

- Módulos de EtherNet/IP em sistemas de controle de Logix5000, publicação [ENET-UM001](#)
- Manual do usuário dos módulos ControlNet em sistemas de controle Logix5000, publicação [CNET-UM001](#)
- Módulos DeviceNet em sistemas de controle Logix5000 Control Systems, publicação [DNET-UM004](#)

Compreensão dos fatores que afetam a entrada em comunicação

A aplicação Logix Designer 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 ocorrerem 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 Project to Controller Match, 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 Project to Controller Match

A função Project to Controller Match afeta os processos de download, upload e entrar em comunicação dos projetos padrão e de segurança.

Se a função Project to Controller Match estiver habilitada no projeto off-line, a aplicação Logix Designer 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 permite que o firmware seja atualizado como parte da sequência de download.

IMPORTANTE	Para atualizar o firmware do controlador, instale primeiro um kit de atualização do firmware. É possível localizar esse kit no DVD complementar do ambiente Studio 5000.
-------------------	--

DICA	É possível atualizar o firmware selecionando ControlFLASH no menu Tools na aplicação Logix Designer.
-------------	--

Falhas/status de segurança

É permitido carregar a lógica de programação 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 Safety da caixa de diálogo Controller Properties.

Assinatura de tarefa de segurança e status de travamento e destravamento 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, se faz upload da assinatura e 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.

No download

A existência de uma assinatura de tarefa de segurança e o status de trava de segurança do controlador determinam se um download pode ser feito ou não.

Tabela 34 - 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

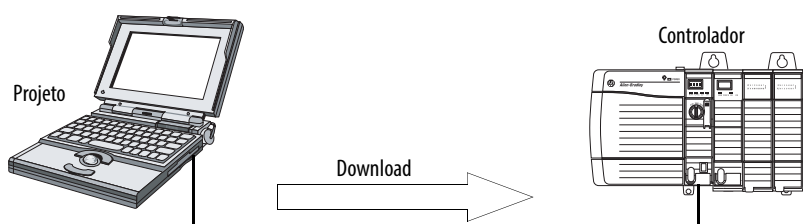
Durante o download em um controlador que está desbloqueado de segurança, caso o firmware no controlador seja diferente daquele no projeto off-line, faça um dos seguintes:

- 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 de seu computador para seu 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 Who Active .
 - b. Seleção do controlador.
Para abrir um nível, clique o sinal de +. Se já houver um controlador selecionado, verifique se é o correto.

4. Clique em Download.

A aplicação Logix Designer compara as seguintes informações entre o projeto off-line e o controlador:

- número de série do controlador (se a função Project to controller match for selecionada)
- firmware principal e revisões secundárias
- status de segurança
- assinatura da tarefa de segurança (caso exista uma)
- status da trava de segurança

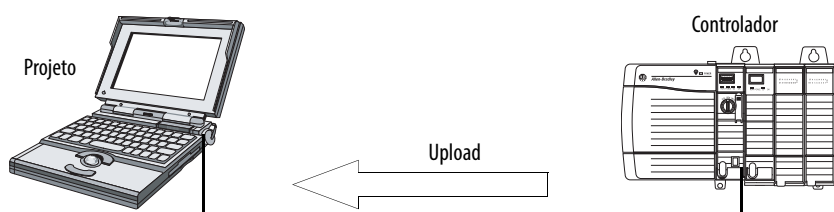
5. Siga as orientações nesta tabela para concluir o download com base na resposta da aplicação Logix Designer.

Se o software indicar	Faça o seguinte:
Faça download para o controlador.	Selecione Download. Se faz download do projeto no controlador e entra em comunicação.
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 Update project serial number 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 Update firmware. Escolha a revisão necessária e clique em Update. Clique em Yes para confirmar sua seleção.
Não é possível fazer download para o controlador. O parceiro de segurança está faltando ou não disponível.	Cancele o processo de download. Instale um parceiro de segurança compatível antes de tentar fazer download.
Não é possível fazer download para o controlador. A revisão do firmware do parceiro de segurança não é compatível com o controlador primário.	Atualize a revisão de firmware do Parceiro de Segurança. Escolha Update firmware. Escolha a revisão necessária e clique em Update. Clique em Yes para confirmar sua seleção.
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 e fazer 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 Unlock. A caixa de diálogo Safety Unlock for Download é exibida. Se a caixa de seleção Delete Signature é selecionada, e você escolher destravar, clique em Yes para confirmar a eliminação.
Irá ocorrer uma falha de segurança não recuperável no controlador de segurança. Não existe nenhum mestre de tempo de sistema (CST).	Marque Enable Time Synchronization e clique em Download para continuar.

Após um download bem-sucedido, o status de trava de segurança e a assinatura da tarefa de segurança do controlador serão compatíveis com os do projeto do que se fez download. Os dados de segurança serão inicializados com os valores existentes no momento em que a assinatura da tarefa de segurança foi criada.

Upload

Siga essas etapas para transferir o projeto do controlador para o computador.



1. Defina o caminho até o controlador.

a. Clique em Who Active .

b. Seleção do controlador.

Para expandir um nível, clique no sinal de +. Se já houver um controlador selecionado, verifique se é o correto.

2. Clique em Upload.

3. Se o arquivo de projeto não existe, escolha File>Select>Yes.

4. Caso contrário, selecione-o.

Se a função project to controller match estiver habilitada, a aplicação Logix Designer verificará se os números de série do projeto aberto e do controlador são compatíveis.

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 Select File.
- Atualize o número de série do projeto para casar com o do controlador marcando a caixa de seleção Update Project Serial Number e escolhendo Upload.

5. A aplicação Logix Designer 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. A aplicação Logix Designer verifica mudanças no projeto off-line.

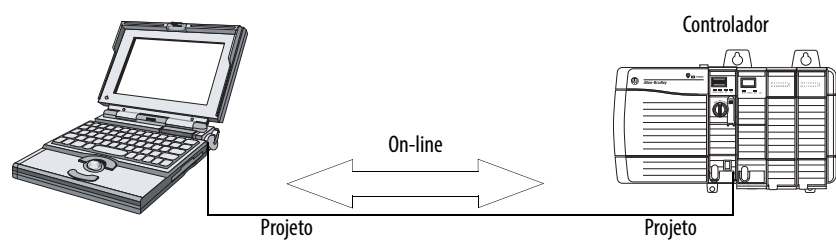
- a. Se não houver, será possível entrar em comunicação sem fazer upload. Clique em Go Online.
- b. Se houver alterações no projeto aberto que não existam no controlador, será possível optar entre fazer upload do projeto, cancelar o upload ou selecionar um arquivo diferente.

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 Safety-Lock 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.

Ficar 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 Who Active .
- b. Seleção do controlador.

Para expandir um nível, clique no sinal de +. Se já houver um controlador selecionado, verifique se é o correto.

2. Clique em Go Online.

A aplicação Logix Designer verifica o seguinte:

- Os números de série do projeto off-line e do controlador combinam (se a função Project to Controller Match 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 35 - Conexão com o controlador

Se o software indicar	Faça o seguinte:
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 Update project serial number ... 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. Clique em Yes para confirmar sua seleção. IMPORTANTE: O projeto online é excluído. - Para preservar o projeto on-line, cancele o processo on-line e instale uma versão do ambiente Studio 5000 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 Select File para selecionar outro projeto off-line.
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.	- 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.

Quando o controlador e a aplicação Logix Designer estão on-line, o status de proteção por trava de segurança e a assinatura de tarefa de segurança do controlador são compatíveis com o projeto do controlador. O status Safety-Lock 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.

Armazenamento e carregamento de projetos usando memória não volátil

Tópico	Página
Usando cartões de memória para memórias não voláteis	113
Armazenamento de um projeto de segurança	114
Carregamento de um projeto de segurança	115
Use módulos de armazenamento de energia	115
Estime o suporte ESM do WallClockTime	117
Gestão do firmware com supervisor de firmware	117

Usando cartões de memória para memórias não voláteis

Os controladores GuardLogix 5570 suportam um cartão de memória para memória não volátil. 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 pela aplicação Logix Designer

IMPORTANTE

A memória não volátil armazena os conteúdos da memória do usuário no momento em que o projeto é armazenado:

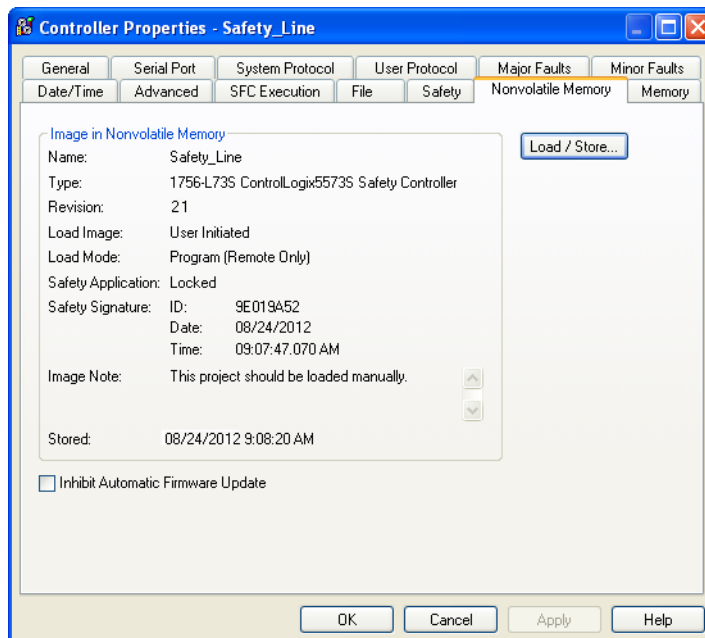
- As alterações feitas após armazenar o projeto não são refletidas na memória não volátil.
- Se fizer alguma mudança ao projeto, mas não armazená-las, elas serão substituídas quando carregar o projeto da memória não volátil. Caso isso ocorra, é preciso fazer upload ou download do projeto para ficar on-line.
- Se deseja armazenar as mudanças como edições off-line, valores de tag ou um programa ControlNet, armazene o projeto novamente depois de fazer as alterações.



ATENÇÃO: Não remova o cartão de memória enquanto o controlador estiver lendo ou gravando no cartão, conforme indicado por um indicador de status OK verde piscando. Isso pode corromper os dados no cartão ou no controlador e também corromper o último firmware no controlador. Deixe o cartão no controlador até que o indicador de status OK fique verde e sem piscar.

Se um cartão de memória estiver instalado, é possível visualizar os conteúdos do cartão na guia Nonvolatile Memory da caixa de diálogo Controller Properties. Se uma aplicação de segurança for armazenada no cartão, o status de bloqueio por segurança e a assinatura da tarefa de segurança aparecem.

Figura 30 - Guia Nonvolatile Memory



Para informações detalhadas sobre o uso de memória não volátil, consulte o Logix5000 Controllers Nonvolatile Memory Programming Manual, 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. Ao armazenar um projeto de segurança, o firmware do controlador primário e do parceiro de segurança é salvo no cartão de memória.

Se não existir nenhum projeto de aplicação no controlador, é possível salvar somente o firmware do controlador de segurança se houver uma parceria válida. Uma carga de firmware somente não irá apagar a condição inoperável da tarefa de segurança.

Se existir uma assinatura de tarefa de segurança quando um projeto for armazenado, o seguinte ocorre:

- os tags de segurança armazenados com o valor da assinatura criada.
- os tags padrão são atualizados.
- a assinatura atual da tarefa de segurança é salva.

Ao armazenar um projeto de aplicação de segurança em um cartão de memória, recomendamos selecionar Program (Remote Only) e também o modo load, isto é, o modo em que o controlador deve entrar após a carga.

Carregamento de um projeto de segurança

Você pode iniciar uma carga de memória não volátil quando as seguintes situações forem verdadeiras:

- 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 36 - Opções para carregar um projeto

Se deseja carregar o projeto	Então selecione esta opção Load Image	Observações
Sempre que ligar ou desligar e ligar a alimentação	Ao energizar	• 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 energização, independentemente do firmware ou projeto de aplicação no controlador. A carga ocorre se o controlador estiver ou não com bloqueio de segurança ou tenha uma assinatura de tarefa de segurança. • Você sempre pode usar a aplicação Logix Designer para carregar o projeto.
Sempre que não houver nenhum projeto no controlador e ligar ou desligar e ligar a alimentação do rack	Na memória corrompida	• Por exemplo, se a bateria descarregar e o controlador perder a alimentação, o projeto será apagado da memória. Quando a energia for restabelecida, esta opção carrega o projeto de volta ao controlador. • O controlador atualiza o firmware no controlador primário ou no parceiro de segurança, se necessário. O projeto de aplicação armazenado na memória não volátil também é carregado e o controlador entra no modo selecionado, seja programação ou operação. • Você sempre pode usar a aplicação Logix Designer para carregar o projeto.
Apenas pela aplicação Logix Designer	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 a um controlador de trava de segurança é permitido somente quando a assinatura de tarefa de segurança do projeto armazenado 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.

IMPORTANTE

Antes de usar software ControlFLASH, certifique-se de que o cartão SD está desbloqueado se configurado para carregar na energização. De outro modo, os dados atualizados podem ser substituídos pelo firmware no cartão de memória.

Use módulos de armazenamento de energia

Podem-se usar os GuardLogix ESMs para executar uma das seguintes tarefas:

- Fornecer energia para o controlador para salvar o programa na memória de armazenamento não volátil integrada (NVS) do controlador depois que a alimentação for removida do rack ou o controlador for removido de um rack energizado.

IMPORTANTE

Quando estiver usando um ESM para salvar o programa na memória NVS integrada, **não** se está salvando o programa para o cartão SD instalado no controlador.

- Apagar o programa da memória integrada NVS do controlador. Para mais informações, consulte [Apague o programa da memória NVS integrada](#)

A seguinte tabela descreve os ESMs.

Tabela 37 - Módulos de armazenamento de energia

Nº. Cat.	Descrição
1756-ESMCAP(XT)	ESM com base em capacitor Os controladores são entregues com este ESM instalado.
1756-ESMNSE(XT)	ESM com base em capacitor sem energia de recuperação WallClockTime Use este módulo ESM se sua aplicação precisa que o ESM instalado esgote sua energia armazenada residual para 40 μ J ou menos antes de transportá-lo para dentro ou fora da sua aplicação. E ainda, pode-se usar este ESM apenas com um controlador 1756-L73S (8 MB) ou de memória menor.
1756-ESMNRM(XT)	ESM com base em capacitor fixo (não removível) Este ESM fornece à sua aplicação um grau aumentado de segurança impedindo o acesso físico ao conector USB e ao cartão SD.
1756-SPESMNSE(XT)	ESM com base em capacitor sem energia de recuperação WallClockTime para o parceiro de segurança Use este módulo ESM se sua aplicação precisa que o ESM instalado esgote sua energia armazenada residual para 40 μ J ou menos antes de transportá-lo para dentro ou fora da sua aplicação. O parceiro de segurança 1756-L7SPXT de temperatura extrema é enviado com o 1756-SPESMNSEXT instalado.
1756-SPESMNRM(XT)	ESM com base em capacitor fixo (não removível) para o parceiro de segurança

Salve o programa na memória NVS integrada

Siga estas etapas para salvar o programa para a memória NVS quando o controlador perder a alimentação.

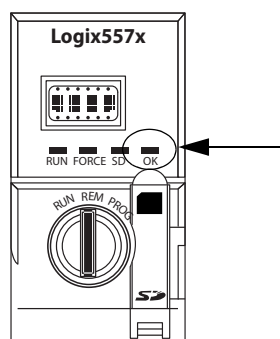
1. Remova a energização do controlador.

Pode-se remover a energia de qualquer umas das maneiras:

- Desligue a energia do rack enquanto o controlador está instalado no rack.
- Remova o controlador de um rack energizado.

Imediatamente depois que o controlador não está mais energizado, o indicador de status OK muda para vermelho sólido e permanece desta forma o tempo suficiente para salvar o programa.

Figura 31 - Indicador de status OK.



2. Deixe o ESM no controlador até que o indicador de status OK esteja desligado.
3. Se necessário, remova o ESM do controlador depois que o indicador de status OK mudar de vermelho para desligado.

Apague o programa da memória NVS integrada

Se sua aplicação permite que você remova programas, siga estas etapas para desenergizar o programa na memória NVS integrada do controlador.

1. Remova o ESM do controlador.
2. Remova a energia do controlador desligando a energia do rack enquanto o controlador é instalado no rack, ou pela remoção do controlador de um rack energizado.
3. Reinstale o ESM no controlador.
4. Restabeleça a energia para o controlador.
 - a. Se o controlador já estiver instalado no rack, ligue novamente a energia do rack.
 - b. Se o controlador não estiver instalado no rack, reinstale o controlador no rack e ligue novamente a energia do rack.

Estime o suporte ESM do WallClockTime

O ESM fornece suporte para a manutenção do atributo WallClockTime do controlador quando a energia não é aplicada. Use esta tabela para estimar o tempo de espera do ESM, com base na temperatura do controlador e ESM instalado.

Tabela 38 - Temperatura versus tempo de espera

Temperatura	Tempo de espera (em dias)		
	1756-ESMCAP(XT)	1756-ESMNRM(XT) 1756-SPESMNRM(XT)	1756-ESMNSE(XT) 1756-SPESMNSE(XT)
20 °C (68 °F)	12	12	0
40 °C (104 °F)	10	10	0
60 °C (140 °F)	7	7	0

Gestão do firmware com supervisor de firmware

Pode-se usar a função Firmware Supervisor para gerenciar firmwares em controladores. 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 modular que se assentam diretamente na rede sem um adaptador, incluindo os dispositivos de E/S de segurança nas redes EtherNet/IP. Dispositivos de E/S de segurança em redes DeviceNet e módulos de E/S POINT Guard ainda não são suportados.

Siga essas etapas para habilitar o supervisor de firmware.

1. Na caixa de diálogo Controller Properties, clique na guia Nonvolatile Memory.
2. Clique em Load/Store.
3. A partir do menu Automatic Firmware Updates, selecione Enable e Store Files to Image.

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.

Monitorar o Status e Controlar Falhas

Tópico	Página
Visualizando o status via barra online	119
Monitorar as conexões	120
Monitorar os sinalizadores de Status	121
Monitorar o Status de segurança	122
Falhas do controlador	122
Desenvolvimento de uma rotina de falha	124

Consulte [Apêndice A, Indicadores de status](#) para informações sobre interpretações dos indicadores de status e mensagens exibidas pelo controlador.

Visualizando o status via barra online

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.

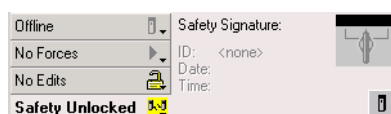
Figura 32 - Botões de status



Quando o botão Controller Status é selecionado conforme exibido anteriormente, a barra on-line exibe o modo do controlador (RUN) e o status (OK). O indicador BAT combina o status do controlador primário e do parceiro de segurança. Se um deles ou ambos apresentarem falha na bateria, o indicador de status acende. 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 Safety Status é selecionado conforme exibido abaixo, a barra on-line exibe a assinatura de tarefa de segurança.

Figura 33 - Tela on-line de assinatura de segurança



O botão Safety Status indica se o controlador está travado ou destravado por segurança ou com falha. Ele exibe também um ícone que mostra o status de segurança.

Tabela 39 - Ícone de status de segurança

Se o status de segurança indicar	Este ícone será exibido
Tarefa de segurança OK	
Tarefa de segurança inoperável	
Falta parceiro Parceiro não disponível Hardware incompatível Firmware incompatível	
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. 

Monitorar as 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:

- O indicador de E/S na frente do controlador piscará em verde.
- Um símbolo de alerta  aparecerá sobre a pasta I/O configuration e sobre o dispositivo temporizado.
- Uma falha de dispositivo é produzida, que pode ser acessada através da guia Connections da caixa de diálogo Module Properties para o dispositivo 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/PL.

Consulte [Conexões de Segurança na página 121](#).

Conexões de Segurança

Para os tags associados a dados de segurança produzidos e 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 no Run Mode (1) ou Idle State (0). Idle state 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 é Valid (0) ou Faulted (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 40 - Status de Conexão de Segurança

Status RunMode	Status ConnectionFaulted	Operação de conexão de segurança
1 = Run	0 = Valid	Dados ativamente controlados por um dispositivo em produção, no modo de operação.
0 = Idle	0 = Valid	Conexão ativa e dispositivo em produção no estado Inativo. Dados de segurança zerados.
0 = Idle	1 = Faulted	Conexão de segurança apresenta falha. Estado do dispositivo em produção desconhecido. Dados de segurança zerados.
1 = Run	1 = Faulted	Estado inválido.

Se um dispositivo está inibido, o bit ConnectionFaulted é definido como Faulted (1) e o bit RunMode como Idle (0) para cada conexão associada ao dispositivo. Como resultado, os dados consumidos de segurança são zerados.

Monitorar os sinalizadores de Status

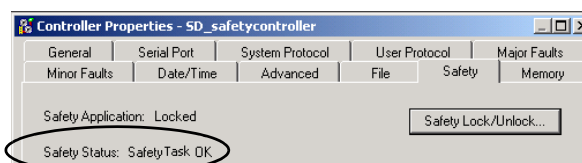
Os controladores Logix, incluindo os controladores GuardLogix, oferecem suporte a palavras-chave de status que podem ser usadas na lógica para monitorar eventos específicos.

Para mais informações sobre como usar esses teclados, consulte o Logix5000 Controllers Controller Information and Status Programming Manual, publicação [1756-PM015](#).

Monitorar o Status de segurança

Visualize as informações de status de segurança do controlador no botão de status de segurança na barra on-line e na guia Safety da caixa de diálogo Controller Properties.

Figura 34 - Status da tarefa de segurança



Os valores possíveis para o status de segurança são:

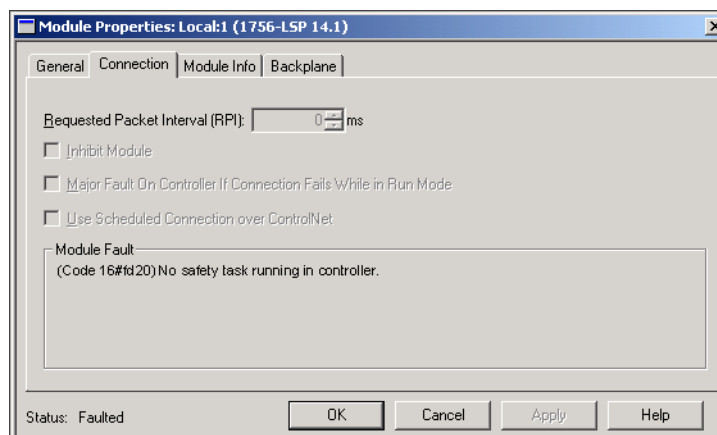
- falta um parceiro de segurança ou ele não está disponível.
- o hardware do parceiro de segurança é incompatível com o controlador principal.
- o firmware do parceiro de segurança é incompatível com o controlador primário.
- tarefa de segurança inoperável.
- tarefa de segurança OK.

Com exceção de “Safety Task OK”, as descrições indicam que existem falhas de segurança irreversíveis.

Consulte [Falhas graves de segurança \(Tipo 14\) na página 124](#) para ver os códigos de falha e as ações corretivas.

O status do parceiro de segurança pode ser visualizado na guia Connections na caixa de diálogo Module Properties.

Figura 35 - Status do parceiro de segurança



Falhas do controlador

As falhas no sistema GuardLogix podem ser falhas irreversíveis do controlador, falhas irreversíveis de segurança na aplicação de segurança ou falhas recuperáveis de segurança na aplicação de segurança.

Falhas irre recuperáveis do controlador

Ocorrem quando o diagnóstico interno do controlador falha. Se ocorrer uma falha irre recuperável do controlador, a execução da tarefa de segurança é interrompida e os dispositivos de E/S de segurança são colocados no estado seguro. A recuperação requer que você faça download do programa aplicativo novamente.

Falhas de segurança irre recuperáveis na aplicação de segurança

Se ocorrer uma falha de segurança irre recuperável na aplicação de segurança, a lógica e o protocolo de segurança são finalizados. As falhas no watchdog da tarefa de segurança e na parceria de controle são desta categoria.

Quando a tarefa de segurança encontrar uma falha de segurança irre recuperável que for removida de forma programática no Program Fault Handler, a aplicação padrão continuará a ser executada.



ATENÇÃO: Cancelar uma falha de segurança não a apaga. Se você substituir uma falha de segurança é sua responsabilidade provar de que o funcionamento de seu sistema ainda é seguro.

Você deve fornecer prova para sua certificadora que seu sistema pode continuar a operar com segurança após uma substituição de uma falha de segurança.

Se houver uma assinatura de tarefa de segurança, será possível remover a falha para habilitar a execução da tarefa de segurança. Caso contrário, a assinatura da 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 parar a execução da tarefa de segurança, dependendo se a falha foi ou não controlada pelo Program Fault Handler na aplicação de segurança.

Quando uma falha recuperável for removida de forma programática, a tarefa de segurança continua 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 Recent Faults na guia Major Faults na caixa de diálogo Controller Properties contém duas subguias, uma para falhas padrão e outra para falhas de segurança.

A tela de status no controlador também mostra códigos de falha com uma curta mensagem de status, conforme descrição no início da página [127](#).

Códigos de Falhas

A [Tabela 41](#) mostra os códigos de falha específicos para GuardLogixcontroladores. O tipo e o código correspondem ao tipo e ao código exibidos na guia Major da caixa de diálogo Controller Properties e no objeto PROGRAM, atributo MAJORFAULTRECORD (ou MINORFAULTRECORD).

Tabela 41 - 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 ou o parceiro de segurança foi removido.	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 refazer o download do programa para permitir a execução da tarefa de segurança. Reinstale o parceiro de segurança, caso tenha sido removido.
02	Existe um erro em uma rotina da tarefa de segurança.	Recuperável	Corrija o erro na lógica do programa do usuário.
03	Parceiro de segurança ausente.	Irrecuperável	Instale um parceiro de segurança compatível.
04	Parceiro de segurança não disponível.	Irrecuperável	Instale um parceiro de segurança compatível.
05	Hardware do parceiro de segurança incompatível.	Irrecuperável	Instale um parceiro de segurança compatível.
06	Firmware do parceiro de segurança incompatível.	Irrecuperável	Atualize o parceiro de segurança para que o firmware principal e a revisão secundária sejam compatíveis com o controlador primário.
07	Tarefa de segurança inoperante. Esta falha ocorre quando a lógica de segurança é inválida, por exemplo, uma divergência na lógica entre o controlador primário e o parceiro de segurança, ocorreu um intervalo de watchdog ou se a memória estiver corrompida.	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.
09	Falha irrecuperável do controlador no parceiro de segurança.	Irrecuperável	Apague a falha e faça download do programa. Se o problema continuar, substitua o Parceiro de Segurança.

O Logix5000 Controllers Major and Minor Faults Programming Manual, 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 pára a execução da lógica.

Algumas aplicações não precisam de todas as falhas de segurança para desligar todo o sistema. 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: Você deve fornecer prova para sua certificadora que seu sistema pode continuar a operar com segurança após uma substituição de uma falha de segurança.

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 [125](#).

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 falhas do controlador é um componente opcional executado quando a rotina de falha do programa não apaga 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 Logix5000 Controllers Major and Minor Faults Programming Manual, publicação [1756-PM014](#), oferece detalhes sobre a criação e o teste de uma rotina de falhas.

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 usar a instrução SSV, o software exibe apenas os atributos que você pode configurar.

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 42](#) mostra os atributos que você pode obter para os valores usando a instrução GSV e os atributos que você pode definir usando a instrução SSV, a segurança e tarefas padrão.



ATENÇÃO: Utilize as instruções GSV/SSV com cuidado. Fazer alterações em objetos pode causar uma operação inesperada do controlador ou ferimentos pessoais.

Tabela 42 - 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	Instance	DINT	Fornecer 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
	Priority	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	Instance	DINT	Fornecer 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	Instance	DINT	Fornecer 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) - parceiro faltante. (0000000000000000) - parceiro não disponível. (0000000000000001) - hardware incompatível. (0000000000000010) - 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 add-on.			X	
	SignatureID	DINT	Número de ID.			X	
	SafetySignatureID	DINT	Número de identificação de 32 bits.			X	

(1) Consulte [Acesso aos atributos de FaultRecord na página 127](#) para informações sobre como acessar este atributo.

(2) Consulte [Captção de informações de falha na página 127](#) para 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 a atributos do objeto padrão.

Acesso aos atributos de FaultRecord

Cria uma estrutura definida pelo usuário para simplificar o acesso aos atributos MajorFaultRecord e SafetyTaskFaultRecord.

Tabela 43 - 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 mais informações sobre o uso das instruções GSV e SSV, consulte o capítulo Input/Output Instructions do Logix5000 Controllers General Instructions Reference Manual, publicação [1756-RM003](#).

Captação de informações de falha

Os atributos SafetyStatus e SafetyTaskFaultRecord podem captar informações sobre falhas irreversíveis. 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.

Observações:

Indicadores de status

Tópico	Página
Indicadores de status dos controladores	129
Tela de status do controlador	130

Indicadores de status dos controladores

O status do controlador primário é exibido por meio de quatro indicadores de status.

Tabela 44 - Descrições do indicador de status do controlador primário

Indicador	Status	Descrição
RUN	Desligado	Sem execução de tarefas do usuário. Controlador no modo PROGram.
	Verde	Controlador no modo RUN.
FORCE	Desligado	Não há imposições, padrão ou de Segurança habilitadas no controlador.
	Âmbar	Imposições padrão e/ou de segurança habilitadas. Tenha cuidado se for instalar (adicionar) uma imposição. Se instalar uma imposição, ela será executada imediatamente.
	Âmbar, intermitente	Um ou mais endereços de E/S, padrão e/ou de segurança foram forçados nos estado energizado ou desenergizado, mas as imposições não estão habilitadas. Tenha cuidado se habilitar imposições de E/S. Se habilitar as imposições de E/S, todas as imposições de E/S existentes também serão executadas.
SD	Desligado	Nenhuma atividade está ocorrendo com o cartão de memória.
	Verde, intermitente	O controlador está lendo ou gravando no cartão de memória. Não remova o cartão de memória enquanto o controlador está lendo ou gravando.
	Verde	
	Vermelho, intermitente	O cartão de memória não tem um sistema de arquivo válido.
	Vermelho	O cartão de memória não é reconhecido pelo controlador.
OK	Desligado	Nenhuma energização aplicada.
	Verde	O controlador está operando sem falhas.
	Vermelho, intermitente	- Falha irreversível ou reversível não controlada no manipulador de falhas. Todas as tarefas do usuário, padrão e de Segurança foram interrompidas. - Se o controlador for novo, pronto para usar, requer a atualização do firmware. A tela de status indica Firmware Installation Required.
	Vermelho	- O controlador está completando o diagnóstico de energização. - Uma falha grave irreversível ocorreu e o programa foi apagado da memória. - A carga do capacitor no Módulo de Armazenamento de Energia (ESM) está sendo descarregada na desenergização. - O controlador está energizado, mas não opera. - O controlador está carregando um projeto para uma memória não volátil.

O parceiro de segurança tem um indicador de status OK.

Tabela 45 - Indicador de status 1756-L7SP

Indicador	Status	Descrição
OK	Desligado	Nenhuma energização aplicada.
	Verde	O parceiro de segurança está operando sem falhas.
	Vermelho	Energizando ou falha irreversível no controlador.

Tela de status do controlador

A tela de status do controlador exibe mensagens de rolagem que fornecem informações sobre a revisão do firmware do controlador, o estado do módulo de armazenamento de energia (ESM), o estado do projeto e falhas graves.

Mensagens de status de segurança

A tela do controlador primário pode exibir as seguintes mensagens. O parceiro de segurança exibe “L7SP”.

Tabela 46 - Tela de status de segurança

Mensagem	Interpretação
Sem assinatura de segurança	A tarefa de segurança está em modo de operação sem uma assinatura de tarefa de segurança.
Parceiro de segurança ausente	O parceiro de segurança está faltando ou não disponível.
Hardware incompatível	O parceiro de segurança e o hardware do controlador primário são incompatíveis.
Firmware incompatível	O parceiro de segurança e os níveis da revisão do firmware do controlador primário são incompatíveis.
No CST Master	Um mestre de tempo de sistema coordenado (CST) não foi encontrado.
Tarefa de segurança inoperável	A lógica de segurança é inválida. Por exemplo, uma diferença ocorreu entre o controlador primário e o parceiro de segurança, um tempo-limite de watchdog ocorreu, ou a memória está corrompida.
Segurança desbloqueada	O controlador está em modo de operação com uma assinatura de segurança, mas não está com trava de segurança.

Mensagens gerais de status

As mensagens descritas na [Tabela 47](#) são tipicamente indicadas na energização, desenergização e enquanto o controlador estiver operando. Essas mensagens indicam o status do controlador e do ESM.

Tabela 47 - Tela de status geral

Mensagem	Interpretação
Nenhuma mensagem é indicada	O controlador está desligado ou uma falha grave irreversível (MNRF) ocorreu. Verifique o indicador OK para determinar se o controlador está energizado e determinar o estado do controlador.
TEST	Os testes de energização estão sendo conduzidos pelo controlador.
PASS	Os testes de energização foram completados com sucesso.
SAVE	Um projeto está sendo salvo para o cartão SD na desenergização. Pode-se visualizar o indicador SD (consulte a página 129) para mais informações de status. Permita a finalização do salvamento antes de remover o cartão SD ou desligar a energia.
LOAD	Um projeto está sendo carregado a partir do cartão SD na energização do controlador. Pode-se visualizar o indicador SD (consulte a página 129) para mais informações de status. Permita a finalização do carregamento antes de remover o cartão SD, removendo o módulo ESM, ou desligando a energia.
UPDT	Uma atualização do firmware está sendo conduzida a partir do cartão SD na energização. Pode-se visualizar o indicador SD (consulte a página 129) para mais informações de status. Caso não queira atualizar o firmware na energização, altere a propriedade Load Image do controlador.
CHRG	O ESM baseado em capacitor está sendo carregado.
1756-L7x/X	O código de catálogo e série do controlador.
Rev XX.xxx	A revisão principal e secundária do firmware do controlador.
No Project	Nenhum projeto está carregado no controlador. Para carregar um projeto, use a aplicação Logix Designer para fazer o download do projeto para o controlador, ou use um cartão SD para carregar um projeto para o controlador.
Project Name	O nome do projeto que está sendo carregado atualmente no controlador. O nome indicado é baseado no nome do projeto especificado na aplicação Logix Designer.
BUSY	Os módulos de E/S associados com o controlador ainda não estão completamente energizados. Possibilite tempo para a energização e o auto-teste do dispositivo de E/S.
Corrupt Certificate Received	O certificado de segurança associado ao firmware está corrompido. Vá até http://www.rockwellautomation.com/support/ e faça o download da revisão do firmware que deseja atualizar. Substitua a revisão do firmware previamente instalada por aquela situada no website do Suporte Técnico.
Corrupt Image Received	O arquivo do firmware está corrompido. Vá até http://www.rockwellautomation.com/support/ e faça o download da revisão do firmware que deseja atualizar. Substitua a revisão do firmware previamente instalada por aquela situada no website do Suporte Técnico.
ESM Not Present	Um ESM está ausente e o controlador não pode salvar a aplicação na desenergização. Insira um ESM compatível e, caso use um ESM baseado em capacitor, não desenergize até que o ESM esteja carregado.
ESM Incompatible	O ESM é incompatível com o tamanho da memória do controlador. Substitua o ESM incompatível por um compatível.
ESM Hardware Failure	Uma falha com o ESM ocorreu e o controlador é incapaz de salvar o programa no momento da desenergização. Substitua o ESM antes de desenergizar o controlador para que o programa do controlador seja salvo.
ESM Energy Low	O ESM baseado em capacitor não tem energia suficiente para habilitar o controlador a salvar o programa no momento de uma desenergização. Substitua o ESM.
ESM Charging	O ESM baseado em capacitor está carregando. Não desenergize até que o carregamento esteja completo.
Flash in Progress	Uma atualização do firmware iniciada via software ControlFLASH ou AutoFlash está em progresso. Permita que a atualização do firmware complete sem interrupção.
Firmware Installation Required	O controlador está usando o firmware de inicialização do sistema (ou seja, revisão 1.xxx) e requer uma atualização do firmware. Atualizar o firmware do controlador.
SD Card Locked	Um cartão SD bloqueado está instalado.

Mensagens de falha

Se o controlador está com falha, essas mensagens podem ser indicadas na tela de status.

Tabela 48 - Mensagens de falha⁽¹⁾

Mensagem	Interpretação
Major Fault TXX:CXX message	Uma falha grave do tipo XX e código XX foi detectada. Por exemplo, se a tela de status indicar Major Fault T04:C42 Invalid JMP Target, então uma instrução JMP é programada para saltar para uma instrução LBL inválida.
I/O Fault Local:X #XXXX message	Uma falha de E/S ocorreu em um módulo no rack local. O número de slot e código de falha são indicados juntamente com uma breve descrição. Por exemplo, I/O Fault Local:3 #0107 Connection Not Found indica que uma conexão para o módulo E/S local no slot três não está aberta. Atue de acordo com a ação específica para o tipo de falha indicada.
I/O Fault ModuleName #XXXX message	Uma falha de E/S ocorreu em um módulo em um rack remoto. O nome do módulo com falha, como configurado na árvore de configuração de E/S da aplicação Logix Designer, é indicado com o código da falha e sua breve descrição. Por exemplo, I/O Fault My_Module #0107 Connection Not Found indica que uma conexão ao módulo denominado 'My_Module' não está aberta. Atue de acordo com a ação específica para o tipo de falha indicada.
I/O Fault ModuleParent:X #XXXX message	Uma falha de E/S ocorreu em um módulo em um rack remoto. O nome de origem do módulo é indicado porque nenhum nome de módulo está configurado na árvore de configuração de E/S da aplicação Logix Designer. Além disso, o código da falha é indicado com uma breve descrição da falha. Por exemplo, I/O Fault My_CNet:3 #0107 Connection Not Found indica que uma conexão a um módulo no slot 3 do rack com o módulo de comunicação denominado 'My_CNet' não está aberta. Atue de acordo com a ação específica para o tipo de falha indicada.
X I/O Faults	Falhas de E/S estão presentes e X = ao número de falhas de E/S presentes. No caso de múltiplas falhas de E/S, o controlador indica a primeira falha reportada. A cada falha de E/S resolvida, o número de falhas indicadas diminui e a próxima falha reportada é indicada pela mensagem de falha de E/S. Atue de acordo com a ação específica para o tipo de falha indicada.

(1) Para detalhes sobre códigos de falha, consulte o Manual de programação de códigos de falhas pequenas, grandes e de E/S do Logix5000, publicação [1756-PM014](#).

Mensagens de falhas graves recuperáveis

Falhas graves recuperáveis são indicadas pela mensagem Major Fault TXX:CXX na tela de status do controlador. [Tabela 49 na página 133](#) relaciona tipos de falha específicos, códigos e as mensagens associadas conforme são mostrados na tela de status.

Para descrições detalhadas e métodos de recuperação sugeridos para falhas graves recuperáveis, consulte o Manual de programação de códigos de falha pequenas, grandes e de E/S do Logix5000, publicação [1756-PM014](#).

Tabela 49 - Mensagens de status de falhas graves recuperáveis

Tipo	Código	Mensagem	Tipo	Código	Mensagem
1	1	Run Mode Powerup	7	41	Bad Restore Type
1	60	Non-recoverable	7	42	Bad Restore Revision
1	61	Non-recoverable – Diagnostics Saved	7	43	Bad Restore Checksum
1	62	Non-recoverable – Program Saved	8	1	key switch Change Ignored
3	16	I/O Connection Failure	11	1	Positive Overtravel Limit Exceeded
3	20	Chassis Failure	11	2	Negative Overtravel Limit Exceeded
3	21		11	3	Position Error Tolerance Exceeded
3	23	Connection Failure	11	4	Encoder Channel Connection Fault
4	16	Unknown Instruction	11	5	Encoder Noise Event Detected
4	20	Invalid Array Subscript	11	6	SERCOS Drive Fault
4	21	Control Structure LEN or POS < 0	11	7	Synchronous Connection Fault
4	31	Invalid JSR Parameter	11	8	Servo Module Fault
4	34	Timer Failure	11	9	Asynchronous Connection Fault
4	42	Invalid JMP Target	11	10	Motor Fault
4	82	SFC Jump Back Failure	11	11	Motor Thermal Fault
4	83	Value Out of Range	11	12	Drive Thermal Fault
4	84	Stack Overflow	11	13	SERCOS Communications Fault
4	89	Invalid Target Step	11	14	Inactive Drive Enable Input Detected
4	90	Invalid Instruction	11	15	Drive Phase Loss Detected
4	91	Invalid Context	11	16	Drive Guard Fault
4	92	Invalid Action	11	32	Motion Task Overlap Fault
4	990	User-defined	11	33	CST Reference Loss Detected
4	991		18	1	CIP Motion Initialization Fault
4	992		18	2	CIP Motion Initialization Fault Mfg
4	993		18	3	CIP Motion Axis Fault
4	994		18	4	CIP Motion Axis Fault Mfg
4	995		18	5	CIP Motion Fault
4	996		18	6	CIP Module Fault
4	997		18	7	Motion Group Fault
4	998		18	8	CIP Motion Configuration Fault
4	999		18	9	CIP Motion APR Fault
6	1	Task Watchdog Expired	18	10	CIP Motion APR Fault Mfg
7	40	Save Failure	18	128	CIP Motion Guard Fault

Códigos de falha de E/S

As falhas de E/S indicadas pelo controlador são exibidas na tela de status em um desses formatos:

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

A primeira parte do formato é usada para indicar a localização do módulo com falha. A forma da localização indicada depende da configuração de E/S e das propriedades do módulo especificadas na aplicação Logix Designer.

A última parte do formato, #XXXX *message*, pode ser usada para diagnosticar o tipo de falha de E/S e as ações corretivas potenciais. Para detalhes sobre cada código de falha de E/S, consulte o Manual de programação de códigos de falhas pequenas, grandes e de E/S do Logix5000, publicação [1756-PM014](#).

Tabela 50 - Mensagens de falha E/S

Código	Mensagem	Código	Mensagem
#0001	Connection Failure	#0115	Wrong Device Type
#0002	Insufficient Resource	#0116	Wrong Revision
#0003	Invalid Value	#0117	Invalid Connection Point
#0004	IOI Syntax	#0118	Invalid Configuration Format
#0005	Destination Unknown	#0119	Module Not Owned
#0006	Partial Data Transferred	#011A	Out of Connection Resources
#0007	Connection Lost	#0203	Connection Timeout
#0008	Service Unsupported	#0204	Unconnected Message Timeout
#0009	Invalid Attribute Value	#0205	Invalid Parameter
#000A	Attribute List Error	#0206	Message Too Large
#000B	State Already Exists	#0301	No Buffer Memory
#000C	Object Mode Conflict	#0302	Bandwidth Not Available
#000D	Object Already Exists	#0303	No Bridge Available
#000E	Attribute Not Settable	#0304	ControlNet Schedule Error
#000F	Permission Denied	#0305	Signature Mismatch
#0010	Device State Conflict	#0306	CCM Not Available
#0011	Reply Too Large	#0311	Invalid Port
#0012	Fragment Primitive	#0312	Invalid Link Address
#0013	Insufficient Command Data	#0315	Invalid Segment Type
#0014	Attribute Not Supported	#0317	Connection Not Scheduled
#0015	Data Too Large	#0318	Invalid Link Address
#0100	Connection In Use	#0319	No Secondary Resources Available
#0103	Transport Not Supported	#031E	No Available Resources
#0106	Ownership Conflict	#031F	No Available Resources
#0107	Connection Not Found	#0800	Network Link Offline
#0108	Invalid Connection Type	#0801	Incompatible Multicast RPI
#0109	Invalid Connection Size	#0802	Invld Safety Conn Size
#0110	Module Not Configured	#0803	Invld Safety Conn Format
#0111	RPI Out of Range	#0804	Invld Time Correct Conn Format
#0113	Out of Connections	#0805	Invld Ping Intrvl EPI Multiplier
#0114	Wrong Module	#0806	Time Coord Msg Min Multiplier

Mensagens de falha de E/S (continuação)

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

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

Observações:

Mudar o tipo de controlador

Tópico	Página
Mudança de um controlador padrão para segurança	137
Mudança de um controlador de segurança para padrão	138
Mudando os tipos de controlador de segurança	138
Mais recursos	139

Como os controladores de segurança têm especificações 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 projeto de seu controlador. Mudar o tipo de controlador afeta:

- Funções suportadas
- Configuração física do projeto (parceiro de segurança e a E/S de segurança)
- Propriedades do controlador
- Componentes do projeto, como tarefas, programas, rotinas e tags
- Instruções add-on de segurança

IMPORTANTE Os controladores GuardLogix® 5560 e Compact GuardLogix® 1768 não são suportados no Studio 5000 versão 21 ou posterior.

Mudança de um controlador padrão para segurança

Para a troca bem-sucedida de um tipo de controlador padrão por um controlador de segurança, o slot do rack imediatamente à direita do principal controlador de segurança precisa estar disponível para o parceiro de 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:

- 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.
- Os componentes de segurança são criados (ou seja, tarefa de segurança, programa de segurança e assim por diante).
- 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 Properties (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:

- O parceiro de segurança é removido do rack de E/S.
- Os dispositivos 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 Properties.

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 os tags da E/S de segurança não serão verificados.

Se o projeto do controlador de segurança tiver instruções add-on 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

IMPORTANTE Os controladores Compact GuardLogix 1768 e GuardLogix 5560 não são suportados na aplicação Logix Designer, versão 21.

Ao mudar de um tipo de controlador de segurança para outro, a classe de tags, as rotinas e os programas continuam inalterados. Qualquer dispositivo de E/S que não for mais compatível com o controlador alvo será excluído.

A representação do parceiro de segurança é atualizada para aparecer adequadamente para o controlador-alvo:

- O parceiro de segurança é criado no slotx (slot primário + 1) ao mudar de um controlador Compact GuardLogix 1768 para um GuardLogix 5570.

- Ao mudar para um controlador Compact GuardLogix 1768, o parceiro de segurança é removido, pois é interno ao controlador Compact GuardLogix.

DICA Um controlador GuardLogix 5570 suporta 100 programas de segurança na tarefa de segurança, enquanto o controlador Compact GuardLogix 1768 suporta 32.

As instruções de ponto flutuante, como FAL, FLL, FSC, SIZE, CMP, SWPB e CPT são suportadas nos controladores GuardLogix 5570, mas não nos controladores GuardLogix 5560 e Compact GuardLogix 1768. Se o programa de segurança contiver essas instruções, erros de verificação ocorrerão na mudança de um controlador GuardLogix 5570 para um GuardLogix 5560 ou Compact GuardLogix 1768.

Mais recursos

Consulte o Manual de programação de instruções add-on dos controladores Logix5000, publicação [1756-PM010](#), para mais informações sobre Instruções Add-On.

Observações:

Números

1756-Axx 24
1756-CN2 58
1756-CN2R 58
1756-CN2RXT 58
1756-CNB 58
1756-CNBR 58
1756-DNB 60, 61, 105
1756-EN2F 53
1756-EN2T 53
1756-EN2TR 53
1756-EN2TRXT 53
1756-EN2TXT 53
1756-EN3TR 53
1756-ENBT 53
1756-ESMCAP 24, 34, 36, 116, 117
1756-ESMCAPXT 24, 34, 36, 116, 117
1756-ESMNR 24, 34, 36, 116, 117
1756-ESMNRMT 24, 36, 116, 117
1756-ESMNSE 24, 34, 36, 116, 117
1756-ESMNSEXT 24, 36, 116, 117
1756-EWEB 53
1756-PA72 25
1756-PA75 25
1756-PAXT 25
1756-PB72 25
1756-PB75 25
1756-PBXT 25
1756-SPESMCAP 24, 34
1756-SPESMNR 24, 36, 116
1756-SPESMNRMT 24, 36, 116
1756-SPESMNSE 24, 35, 36, 116
1756-SPESMNSEXT 24, 34, 36, 116
1784-SD1 24
1784-SD2 24

A

abrangência do diagnóstico 11
acesso externo 88, 92
ambiente 21
ambiente extremo
 componentes do sistema 10
 controlador 10
 fonte de alimentação 24
 rack 24
apagar
 falhas 123
 programa 117
aprovação para uso em áreas classificadas
 Europa 23
 Norte-América 22
armazenar um projeto 114
arquivo DNT 83

assinatura de configuração

componentes 71
 copiar 71
 definição 71

assinatura de tarefa de segurança 92

armazenando um projeto 114
 copiar 103
 descrição 14
 efeito sobre o download 108
 efeito sobre o upload 107
 gerar 102
 operações restritas 102
 remover 103
 restrições 103
 visualização 119

atraso máximo de rede observado 68

reset 97

atributos

objeto de segurança 126

atualização

firmware 31, 32

atualizações automáticas de firmware 118

AutoFlash

atualização do firmware 32

B

barra on-line 119

bateria

falha 119

bit ConnectionFaulted 121

bit RunMode 121

C

caixa de diálogo new controller 39

capacidade de RAM 16

carregar um projeto 115

ao energizar 115
 iniciado pelo usuário 115
 na memória corrompida 115

cartão de memória 113, 115, 117

instalação 26
 remoção 26

cartão SD

Consulte cartão Secure Digital.

cartão Secure Digital 24

Consulte também cartão de memória.
 instale 27
 remova 27

chave seletora 16, 33

CIP Safety 11, 47, 81

classe 91

codificação eletrônica 117

códigos de falhas

falhas graves de segurança 124
 mensagens de E/S 134
 tela de status 124

colar

número da rede de segurança 52

componentes de sistema Logix-XT

Consulte ambiente extremo.

comunicação 18

- módulos 18
- rede ControlNet 58
- rede DeviceNet 60
- rede EtherNet/IP 53

conexão

- monitor 120
- não programável 59
- programável 59
- rede ControlNet 59
- rede EtherNet/IP 54
- status 121
- USB 29

conexão em modo de escuta 71**conexões não programáveis** 59**conexões programáveis** 59**configure sempre** 80

- caixa de seleção 44

CONNECTION_STATUS 92, 121**consume dados de tag** 96**controlador**

- ambiente extremo 10
- armazenamento
 - assinatura de tarefa de segurança 102
 - travamento de segurança, destravamento 101
- configuração 39
- corresponder 106
- diferença de número de série 109, 112
- diferenças de função 9
- instalação 25
- manipulador de falhas 125
- modo 33
- modo de operação 33, 34
- mudar tipo 137-139
- número de série 106
- propriedades 41

controlador Compact GuardLogix 139**controlador Compact GuardLogix 1768** 139**controlador de segurança peer**

- compartilhamento de dados 93
- configuração 45
- localização 93
- SNN 93

controlador primário

- características gerais de hardware 16
- descrição 16
- memória do usuário 16
- modos 16

controladores GuardLogix

- diferenças 9

ControlNet

- características gerais 58
- conexões 59, 106
- configurar driver 106
- exemplo 59
- módulo 58, 105
- módulos de comunicação 18
- não programável 59
- programável 59
- software 58

conversão de endereço de rede (NAT)

- configure o endereço IP 65
- definição 11
- recursos suportados 19

conversor de protocolos 57**copiar**

- assinatura de tarefa de segurança 103
- número da rede de segurança 52

criação de um projeto 39**D****dados-padrão em uma rotina de segurança** 98**desbloqueio de segurança**

- controlador 101
- ícone 101

descarga eletrostática 23**destravar controlador** 101**DeviceNet**

- comunicação 60
- conexões 61, 106
- configurar driver 106
- módulo 105
- software 60

dispositivos IHM 14**download**

- efeito da revisão de firmware compatível 107
- efeito do controlador compatível 106
- efeito sobre a assinatura da tarefa de segurança 108
- efeito sobre a proteção 108
- efeito sobre o status de segurança 107
- processo 108-109

driver

- ControlNet 106
- DeviceNet 106
- EtherNet/IP 106
- USB 30

E**E/S**

- códigos de falhas 134
- indicador 120
- substituição de módulo 44

E/S CIP Safety

- adicionando 63
- assinatura de configuração 71
- dados de status 74
- endereço de nó 63
- reset propriedade 72
- status do monitor 74

edição 102**endereço**

- Dispositivo de E/S de segurança Kinetix 73

endereço de nó 63**endereço IP** 57, 63**erros de verificação**

- mudando o tipo de controlador 139

ESM

- Consulte o módulo de armazenamento de energia

estado seguro 13

EtherNet/IP

- características gerais 53
- conexões 54, 105
- configurar driver 106
- dispositivo 105
- dispositivo de E/S de segurança 56
- exemplo 55
- módulos 53
- módulos de comunicação 18
- módulos de E/S padrão 57
- parâmetros de rede 57
- recursos do módulo 53
- uso da conexão 54

F**falha**

- apagar 123
- controlador irreversível 123
- mensagens 132, 133
- recuperável 123, 133
- rotinas 124-126
- segurança irreversível 122, 123

falha de segurança irreversível 122, 123

- reiniciando a tarefa de segurança 123

falha do controlador irreversível 123**falha grave recuperável**

- mensagens 133

falha recuperável 123, 133

- apagar 123

falhas graves de segurança 124**falhas graves recuperáveis 133****ficar on-line 111**

- fatores 106

flags de status 121**fonte de alimentação**

- códigos de catálogo 17, 25

forçando 102**G****gabinete 21****GSV (obter valor do sistema)**

- definição 11
- possibilidade de acesso 126
- usando 125

guia major faults 124**guia minor faults 124****guia safety 101, 102, 122**

- assinatura de configuração 71
- controlador com trava de segurança 101
- criação de uma assinatura de tarefa de segurança 102
- dados de conexão 67
- destravar 101
- substituição de módulo 76
- trava de segurança 101
- visualizar o status de segurança 107, 122

I**indicador BAT 119****indicadores de status 129-130**

- módulos de E/S 74

Instruções Add-on 19, 138**intervalo do pacote requisitado 93**

- dados de tags produzidos 89
- definição 11
- E/S de segurança 67
- tag consumido 97
- tags consumidos 89

K**kit de atualização do firmware 107, 117****L****leitura de controle de configuração 71**

- identificando 71
- reset 71, 75

limite de tempo de reação

- E/S CIP Safety 67

limite do tempo de reação de conexão 67, 97**M****MajorFaultRecord 127****máscara de sub-rede 57****memória**

- capacidade 16

memória do usuário 16**memória não volátil 113-118**

- guia 114

mensagem

- tela de status 131

mensagens

- falha 132
- status de segurança 130
- status geral 131

mensagens gerais de status 131**modo**

- em operação 33

modo de operação 33**modo de programa 33****Modo remoto 33, 34****módulo**

- ControlNet 18
- DeviceNet 18
- EtherNet/IP 18
- indicador de status 74
- propriedades
- guia connection 71

módulo de armazenamento de energia 24

- 1756-ESMCAP 24
- armazenamento não volátil 115
- carregando 25, 37
- definição 11
- desinstale 34
- instale 36
- tempo de espera 117

módulo Guard I/O

- substituição 81-84

módulos

- EtherNet/IP 53

monitor
 conexões 120
 status 74
mudando controladores 138
multicast 11
multiplicador de atraso de rede 69, 97
multiplicador de tempo-limite 69, 97

N

Nível de desempenho 11, 13
número da rede de segurança
 ao gerenciamento 47
 atribuição 47
 atribuição automática 49
 atribuição manual 49
 colar 52
 com base na hora 48
 copiar 52
 copiar e colar 52
 definição 11
 definir 67
 descrição 13
 diferença 82
 manual 49
 modificação 50
 mudando o SNN de E/S 51
 mudando o SNN do controlador 50
 visualização 41
número de série 106
número de slot 40

O

objeto de segurança
 atributos 126

P

parceiro de segurança
 configuração 17
 descrição 17
 status 122
período da tarefa de segurança 68, 87, 93
probabilidade de falha por hora (PFH)
 definição 11
probabilidade de falha sob solicitação (PFD)
 definição 11
produza um tag 95
produzir e consumir tags 54, 58, 92
programação 102
programas de segurança 87
projeto para combinar o controlador 106
projetos de segurança
 recursos 19
pronto para usar 77
 reinicialize o módulo 75
propriedade
 configuração 71
 reset 71

proteção da aplicação de segurança 100-103
 assinatura de tarefa de segurança 102
 segurança 101
 trava de segurança 100
proteção do modo de operação 102, 103
proteja a assinatura em modo de operação 43
protocolo de controle e informação
 definição 11

R

rack 17
 códigos de catálogo 24
radiação UV 23
reinicialize o módulo 75
remoção e inserção sob alimentação 22
remover
 assinatura de tarefa de segurança 103
reset
 módulo 75
 propriedade 72, 75
restrições
 mapeamento de tags de segurança 98
 programação 103
 quando com trava de segurança 100
 quando existir a assinatura de segurança 102
 software 103
restrições de programação 103
revisão do firmware
 atualização 31, 32
 corresponder 107
 diferença 108, 109, 112
 gestão 117
RIUP
 Consulte remoção e inserção sob alimentação
rotina de falha do programa 125
rotina de segurança 88
 usando dados-padrão 98
RPI
 consulte intervalo do pacote requisitado

S

SafetyTaskFaultRecord 127
salve o programa
 memória não volátil 116
senha
 caracteres válidos 43
 definir 42
servo-drive Kinetix 5500 56
símbolo de alerta 120
sincronia de tempo 45, 109
software
 rede ControlNet 58
 redes DeviceNet 60
 restrições 103
 USB 29
software ControlFLASH 31, 107, 115, 117
software RSLinx Classic
 versão 18
software RSLogix 5000
 restrições 103

Software RSNetWorx para DeviceNet

substitua o módulo 81

SSV (definir valor do sistema)

possibilidade de acesso 126
usando 125

status

mensagens 130
mensagens de falha 132
mensagens, tela 131
parceiro de segurança 122
tela 130-135

status de rede

indicador 74, 78, 79, 82

status de segurança

assinatura de tarefa de segurança 102
botão 102, 120
efeito sobre o download 107
restrições de programação 103
visualização 107, 119, 122

substitua

configure only... habilitado 76
configure sempre habilitado 80
módulo Guard I/O 75-84

supervisor de firmware 117, 118**T****tag consumido 89, 92****tag de valor constante 92****tag produzido 89, 92****tags**

acesso externo 88, 92
alias 89
base 89
características gerais 88
classe 91
com escopo no controlador 91
Consulte também tags de segurança.
consumidos 89, 92
dados de segurança produzidos/consumidos 90, 91
do programa 91
E/S de segurança 90, 91
escopo 90
nomeação 72
produzidos 89, 92
tipo 89
tipo de dados 90
valor constante 92

tags alias 89**tags com escopo no controlador 91****tags de base 89****tags de segurança**

com escopo no controlador 91
criar 88
descrição 88
do programa de segurança 91
mapeamento 98-100
tipos de dados válidos 90

tags do programa 91**tarefa de segurança 86**

execução 87
prioridade 86
tempo de watchdog 86

tempo de espera

módulo de armazenamento de energia 117

tempo de reação 87**tempo de reação da conexão avançada 69****tempo de sistema 109, 130****tempo de watchdog 86****tempos de varredura**

reset 103

terminologia 11**tipos de dados**

CONNECTION_STATUS 92

trava

Consulte a trava de segurança.

trava de segurança 100

controlador 101
efeito sobre o download 108
efeito sobre o upload 107
icone 101
senha 101

U**unicast 11**

conexões 92, 95

upload

efeito do controlador compatível 106
efeito sobre a assinatura da tarefa de segurança 107
efeito sobre a proteção 107
processo 110

USB

cabo 29, 105
conexão 29
driver 30
porta 29
software necessário 29
tipo 29

V**visualização**

status de segurança 107

W**WallClockTime 116, 117**

módulo de armazenamento de energia 117
objeto 37

X**XT**

Consulte ambiente extremo.

Observações:

Suporte Rockwell Automation

A Rockwell Automation fornece informações técnicas sobre a página da Web para auxiliá-lo na utilização de seus produtos. Em <http://www.rockwellautomation.com/support> Você pode encontrar notas técnicas e notas de aplicação, código de amostra e links para service packs de software. Você também pode visitar nosso centro de suporte em <https://rockwellautomation.custhelp.com/> para atualizações de software, chats de suporte e fóruns, informações técnicas, perguntas frequentes e para se inscrever para atualizações de notificação de produto.

Além disso, oferecemos vários programas de suporte para instalação, configuração e localização de falhas. Para mais informações, entre em contato com seu distribuidor local ou representante Rockwell Automation ou visite o site <http://www.rockwellautomation.com/services/online-phone>.

Assistência na Instalação

Se surgir algum problema nas primeiras 24 horas de instalação, revise as informações deste manual. É possível entrar em contato com o suporte ao cliente para obter ajuda para ligar o produto e colocá-lo em operação.

Estados Unidos ou Canadá	1.440.646.3434
Fora dos Estados Unidos ou Canadá	Use o Worldwide Locator em http://www.rockwellautomation.com/rockwellautomation/support/overview.page , ou entre em contato com o seu representante local Rockwell Automation.

Retorno de Produtos Novos

A Rockwell Automation testa todos os seus produtos para assegurar que estejam funcionando perfeitamente quando deixam as instalações industriais. Porém, se o seu produto não estiver funcionando e precisar ser devolvido, siga esses procedimentos.

Estados Unidos	Entre em contato com seu distribuidor. É necessário fornecer o número de caso fornecido pelo Suporte ao Cliente (ligue para o número de telefone acima) ao distribuidor para concluir o processo de devolução.
Fora dos Estados Unidos	Entre em contato com um representante Rockwell Automation local para obter informações sobre o procedimento de devolução de produto.

Comentários sobre a documentação

Seus comentários irão ajudar-nos a melhor atender suas necessidades. Se tiver alguma sugestão sobre como melhorar este documento, preencha este formulário, publicação [RA-DU002](#), disponível em <http://www.rockwellautomation.com/literature/>.

A Rockwell Automation mantém informações atuais ambientais do produto em seu 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