

Controladores GuardLogix

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



Informações Importantes ao Usuário

Equipamentos de estado sólido apresentam características operacionais distintas de equipamentos eletromecânicos. As Orientações de segurança para a aplicação, instalação e manutenção de controles de estado sólido (publicação [SGI-1.1](#) disponível no escritório de vendas da Rockwell Automation local ou on-line em <http://literature.rockwellautomation.com/literature/>) descrevem algumas diferenças importantes entre equipamentos de estado sólido e dispositivos eletromecânicos conectados fisicamente. Em decorrência dessas diferenças e também da ampla variedade de aplicabilidade de equipamentos de estado sólido, todos os responsáveis pela utilização do equipamento devem estar cientes de que a aplicação pretendida seja aceitável.

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 tópicos relacionados à 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.



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.

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

Rockwell Automation, Allen-Bradley, TechConnect, Integrated Architecture, ControlLogix, ControlLogix-XT, GuardLogix, Logix-XT, Guard I/O, CompactBlock Guard I/O, POINT Guard I/O, PowerFlex, PanelView, PLC-5, DriveLogix, FlexLogix, PhaseManager, ControlFLASH, Logix5000, RSLogix 5000, FactoryTalk, RSNetWorx para EtherNet/IP, RSNetWorx para DeviceNet, RSNetWorx para ControlNet e RSLinx são marcas comerciais da Rockwell Automation, Inc.

As marcas comerciais que não pertencem à Rockwell Automation são propriedade de suas respectivas empresas.

As informações a seguir resumem as alterações neste manual desde a última publicação.

Tópico	Páginas
Informações sobre os controladores 1756-L71S	11, 18, 21, 27, 47
Orientações sobre a instalação do módulo de armazenamento de energia	46

Observações:

	Prefácio	
	Sobre os controladores GuardLogix 1756	11
	Familiarizando-se com a Terminologia	12
	Recursos adicionais	13
	Capítulo 1	
Características gerais do sistema	Requisitos da Aplicação de Segurança	15
	Número da rede de segurança	15
	Assinatura de tarefa de segurança	16
	Diferença entre componentes padrão e de segurança	16
	Dispositivos IHM	16
	Recursos de fluxo de dados do controlador	16
	Seleção do hardware do sistema	18
	Controlador Primário	18
	Parceiro de segurança	19
	Rack	19
	Fonte de Alimentação	19
	Selecionar módulos de E/S de segurança	20
	Seleção das redes de comunicação	20
	Especificações de programação	21
	Capítulo 2	
Instale o controlador	Precauções	23
	Informações sobre Ambiente e Gabinete	23
	Sistemas eletrônicos programáveis (PES)	24
	Remoção e inserção sob alimentação (RIUP)	24
	Aprovação Norte-Americana para Uso em Áreas Classificadas	24
	Aprovação para uso em áreas classificadas na Europa	26
	Prevenção de descarga eletrostática	26
	Certifique-se de que você tem todos os componentes	26
	Controladores 1756-L6xS	27
	Controladores 1756-L7xS	27
	Instale um rack e fonte de alimentação	28
	Instalação da bateria (somente controladores 1756-L6xS)	28
	Instale o controlador no rack	29
	Insira ou remova um cartão de memória	30
	Cartão secure digital (controladores 1756-L7xS)	31
	Cartão CompactFlash (controladores 1756-L6xS)	33
	Faça conexões de comunicação	35
	Conecte-se à porta USB do controlador 1756-L7xS	35
	Conecte-se à porta serial do controlador 1756-L6xS	37
	Atualize o controlador	39
	Usando o software ControlFLASH para atualizar o firmware	40
	Usando AutoFlash para atualizar o firmware	41
	Escolha o modo de operação do controlador	42
	Use a chave seletora para mudar o modo de operação	42
	Use o software RSLogix 5000 para mudar o modo de operação	43

	Desinstale um módulo de armazenamento de energia (ESM)	44
	Instale um módulo de armazenamento de energia (ESM)	46
Configuração do controlador	Capítulo 3	
	Criação de um projeto do controlador	47
	Definir senhas de bloqueio e desbloqueio	49
	Protegendo a assinatura da tarefa de segurança em modo de operação	50
	Gerenciamento da substituição do módulo de E/S	51
	Habilitação da sincronia de tempo	51
	Configurar um Controlador de Segurança Peer	52
Comunicar-se nas Redes	Capítulo 4	
	Rede de Segurança	53
	Administração dos parâmetros do número da rede de segurança (SNN)	53
	Atribuição dos parâmetros do número da rede de segurança (SNN)	55
	Alteração dos parâmetros do número da rede de segurança (SNN)	55
	Comunicação EtherNet/IP	59
	Produção e consumo de dados por uma rede EtherNet/IP	60
	Conexão em rede EtherNet/IP	60
	Exemplo de comunicação EtherNet/IP	61
	Conexões EtherNet/IP para módulos de E/S CIP Safety	61
	Conexões padrão de EtherNet/IP	62
	Comunicação ControlNet	63
	Produção e consumo de dados por uma rede ControlNet	63
	Conexões na rede ControlNet	63
	Exemplo de comunicação ControlNet	64
	Conexões ControlNet para E/S distribuídas	65
	Comunicação DeviceNet	65
	Conexões DeviceNet para módulos CIP Safety E/S	66
	Conexões DeviceNet Padrão	66
	Comunicação em série	67
	Recursos adicionais	68
Adição, configuração, monitoração e substituição da E/S de segurança CIP	Capítulo 5	
	Adição dos módulos de E/S CIP Safety	69
	Configurar módulos de E/S CIP Safety por meio do software RSLogix 5000	70
	Definição dos parâmetros do número da rede de segurança (SNN)	71
	Usando conexões Unicast em redes EtherNet/IP	71
	Definição do limite de tempo de reação da conexão	71
	Especificar o intervalo do pacote requisitado (RPI)	72
	Visualização do atraso máximo observado na rede	72
	Definição dos parâmetros de limite de tempo de reação da conexão avançada	73

Compreensão da assinatura de configuração	75
Configuração por meio do software RSLogix 5000	75
Leitura de controle de configuração diferente (conexão em modo de escuta)	76
Reset a Propriedade do Módulo de E/S de Segurança	76
Endereçar dados à E/S de Segurança	76
Monitorar o Status do Módulo Safety I/O	77
Reiniciando um módulo para a condição “pronto para usar”	79
Substituindo um módulo usando o software RSLogix 5000	79
Substituição com “Configure only when no safety signature exists” habilitado	80
Substituição com “Configure Always” habilitado	84
Substitua um módulo POINT Guard I/O usando o software RSNNetWorx para DeviceNet	86

Capítulo 6

Criação de Aplicações de Segurança

Tarefa de Segurança	90
Especificação do Período da Tarefa de Segurança	90
Execução da Tarefa de Segurança	91
Programas de Segurança	92
Rotinas de Segurança	92
Tags de Segurança	92
Tipo de tag	93
Tipo de dados	94
Escopo	95
Classe	96
Valor constante	96
Acesso externo	96
Tags de segurança produzidos/consumidos	97
Configure os números de rede de segurança dos controladores de segurança peer	97
Produzir um tag de segurança	99
Consumir dados de tags de segurança	100
Mapeamento de tags de segurança	102
Restrições	103
Criar pares para mapeamento de tags	103
Monitorar o status de mapeamento de tags	104
Proteção em aplicações de segurança	104
Bloqueio de segurança do controlador	105
Criação de uma assinatura de tarefa de segurança	106
Restrições do software	108

Capítulo 7

Comunicação com o Controlador

Conexão do controlador à rede	109
Conecte seu dispositivo e o computador EtherNet/IP	110
Conectar o modo de comunicação ControlNet ou o scanner DeviceNet e o seu computador	110
Configuração de um driver EtherNet/IP, ControlNet ou DeviceNet	110

Compreensão dos fatores que afetam a entrada em comunicação.....	111
Função Project to Controller Match.....	111
Revisão de Firmware Compatível	111
Falhas/status de segurança.....	111
Assinatura de tarefa de segurança e status de trava e destravamento de segurança	112
Download	113
Upload	115
Entrar em Comunicação	116

Capítulo 8

Armazenamento e carregamento de projetos usando memória não volátil

Usando cartões de memória para memórias não voláteis.....	119
Armazenamento de um projeto de segurança.....	120
Carregamento de um projeto de segurança.....	121
Use módulos de armazenamento de energia (somente controladores 1756-L7xS).....	122
Salve o programa na memória NVS integrada	122
Apague o programa da memória NVS integrada	123
Estime o suporte ESM do WallClockTime	124
Gestão do firmware com supervisor de firmware	124

Capítulo 9

Monitorar o Status e Controlar Falhas

Visualizando o status via barra on-line.....	125
Monitoração de conexões	126
Todas as conexões	126
Conexões de Segurança.....	127
Monitoração dos flags de status	127
Status de monitoração de segurança.....	128
Falhas do controlador.....	128
Falhas irrecuperáveis do controlador.....	129
Falhas de segurança irrecuperáveis na aplicação de segurança.....	129
Falhas recuperáveis na aplicação de segurança.....	129
Visualização de falhas	130
Códigos de Falhas.....	130
Desenvolvimento de uma rotina de falha	131
Rotina de falha do programa.....	131
Manipulador de falhas do controlador.....	131
Usar instruções GSV/SSV.....	132

Apêndice A

Indicadores de status

Indicadores de status do controlador 1756-L6xS	135
Indicadores de status dos controladores 1756-L7xS.....	136
Tela de status do controlador 1756-L7xS.....	137
Mensagens de status de segurança	137
Mensagens gerais de status.....	138
Mensagens de falha	139
Mensagens de falhas graves recuperáveis	139
Códigos de falha de E/S	140

	Apêndice B	
Manutenção da bateria	Estimativa da Vida Útil da Bateria	143
	Antes do indicador BAT acender	143
	Depois que o indicador BAT acender	144
	Quando Substituir a Bateria.....	145
	Substituição da Bateria	145
	Armazene baterias substituição	147
	Recursos adicionais.....	147
	Apêndice C	
Alteração do tipo do controlador nos projetos RSLogix 5000	Mudança de um controlador padrão para segurança.....	149
	Mudança de um controlador de segurança para padrão	150
	Mudança de um controlador 1756 GuardLogix para um 1768 GuardLogix ou vice-versa	151
	Mudando de um controlador 1756-L7xS para um 1756-L6xS ou 1768-L4xS.....	151
	Recursos adicionais.....	151
	Apêndice D	
Histórico de mudanças	1756-UM020H-EN-P, Abril de 2012.....	153
	1756-UM020G-EN-P, Fevereiro de 2012	153
	1756-UM020F-EN-P, Agosto de 2010.....	154
	1756-UM020E-EN-P, Janeiro de 2010	154
	1756-UM020D-EN-P, Julho de 2008.....	154
	1756-UM020C-EN-P, Dezembro de 2006.....	155
	1756-UM020B-EN-P, Outubro de 2005.....	155
	1756-UM020A-EN-P, Janeiro de 2005	155
Índice		

Tópico	Página
Sobre os controladores GuardLogix 1756	11
Familiarizando-se com a Terminologia	12
Recursos adicionais	13

Este manual é um guia para o uso dos controladores GuardLogix™. 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.

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.

Para informações detalhadas sobre os tópicos relacionados, como programação do controlador GuardLogix, especificações SIL 3/PLC ou informações sobre componentes Logix padrão, consulte a lista de [Recursos adicionais](#) na página [13](#).

Sobre os controladores GuardLogix 1756

Duas linhas de controladores GuardLogix™ 1756 estão disponíveis. Estes controladores compartilham muitas funções, mas também têm algumas diferenças. [Tabela 1](#) fornece as características gerais destas diferenças.

Tabela 1 – Diferenças entre os controladores 1756-L7xS e 1756-L6xS

Recurso	1756-L7xS (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT)	1756-L6xS (1756-L61S, 1756-L62S, 1756-L63S, 1756-L6SP)
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
Indicadores de status	Tela de status com movimento para cima e para baixo e indicadores de status de LED	Indicadores de status de LED

O controlador GuardLogix de ambientes extremos, códigos de catálogo 1756-L73SXT e 1756-L7SPXT, fornece a mesma funcionalidade que o controlador 1756-L73S, mas é projetado para resistir a 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.

Familiarizando-se com a 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/PLe 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 do relógio e backup para retenção da memória na desenergização em controladores 1756-L7xS e 1756-L73SXT.
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.
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.

Recursos adicionais

Estes documentos contêm informações adicionais com relação a produtos da Rockwell Automation.

Tabela 3 – Publicações relacionadas aos controladores e sistemas GuardLogix

Para mais informações sobre	Consulte este recurso	Descrição
Especificações da aplicação (segurança)	Manual de referência de segurança dos sistemas de controladores GuardLogix, publicação 1756-RM093	Contém especificações detalhadas para alcançar e manter SIL 3/PLC com o sistema de controladores GuardLogix.
Baterias	Guidelines for Handling Lithium Batteries, publicação AG-5.4	Fornecer informações sobre armazenamento, manuseio, transporte e descarte de baterias de lítio.
	Referência de baterias de controladores programáveis, http://www.ab.com/programmablecontrol/batteries.html	Fornecer folhas de dados de segurança de materiais (MSDS) para baterias de substituição individuais.
CIP Sync (sincronização de tempo)	Técnica de aplicação de configuração CIP Sync e arquitetura integrada, publicação IA-AI003	Fornecer informações detalhadas e completas sobre como aplicar a tecnologia CIP Sync para sincronizar os relógios em um sistema de controle Logix.
Projeto e seleção	Manual de referência de considerações de projeto de controladores Logix5000, publicação 1756-RM094	Fornecer a usuários avançados as orientações para a otimização do sistema e as informações do sistema para guiar as escolhas de projeto do sistema.
	Guia de seleção ControlLogix, publicação 1756-SG001	Fornecer um processo de seleção de alto nível para componentes do sistema ControlLogix®, informações de especificações críticas para tomar decisões iniciais e links para as informações de especificações completas.
Guard I/O	Manual do usuário dos módulos de segurança Guard I/O DeviceNet, publicação 1791DS-UM001	Fornecer informações sobre o uso de módulos de segurança Guard I/O DeviceNet.
	Manual do usuário dos módulos de segurança Guard I/O EtherNet/IP, publicação 1791ES-UM001	Fornecer informações sobre o uso dos módulos de segurança Guard I/O EtherNet/IP.
	Manual do usuário dos módulos de segurança POINT Guard I/O, publicação 1734-UM013	Fornecer informações sobre a instalação, configuração e uso de módulos POINT Guard I/O™.
Instalação de hardware	Instruções de instalação das fontes de alimentação e racks ControlLogix, publicação 1756-IN005	Descrever como instalar e aterrar o rack ControlLogix e fontes de alimentação.
	Orientações de fiação e aterramento na automação industrial, publicação 1770-4.1	Fornecer 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	Fornecer informações sobre o conjunto de instruções para aplicações de segurança do GuardLogix.
	Manual de referência de instruções gerais dos controladores Logix5000, publicação 1756-RM003	Oferecer aos programadores detalhes sobre cada instrução disponível para um controlador Logix5000.
	Manual de referência de instruções de posicionamento dos controladores Logix5000, publicação MOTION-RM002	Oferecer 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	Detalhar como configurar um sistema de aplicação de movimento SERCOS.
	Manual do usuário de sistemas coordenados de posicionamento, publicação MOTION-UM002	Detalhar como criar e configurar um sistema de aplicação de movimento coordenado.
	Manual do usuário de partida e configuração do posicionamento CIP, publicação MOTION-UM003	Detalhar como configurar um Posicionamento Integrado em um sistema de aplicação de redes EtherNet/IP.
	Manual de referência de posicionamento CIP, publicação MOTION-RM003	Informações detalhadas sobre os modos de controle de eixo e atributos para Posicionamento Integrado em redes EtherNet/IP.
Redes (ControlNet, DeviceNet EtherNet/IP)	Manual do usuário dos módulos EtherNet/IP em sistemas de controle Logix5000, publicação ENET-UM001	Descrever 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	Descrever 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	Descrever como configurar e operar os módulos DeviceNet em um sistema de controle Logix5000.
PhaseManager™	Manual do usuário do PhaseManager, publicação LOGIX-UM001	Fornecer etapas, orientação e exemplos para definir e programar um controlador Logix5000 para usar fases de equipamentos.

Tabela 3 – Publicações relacionadas aos controladores e sistemas GuardLogix

Para mais informações sobre	Consulte este recurso	Descrição
Tarefas e procedimentos de programação	Manual de programação de procedimentos comuns aos controladores Logix5000, publicação 1756-PM001	Fornecer acesso ao conjunto de controladores Logix5000 dos manuais de programação, que cobrem a gestão dos arquivos de projeto, organização de tags, programação de lógica ladder, 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	Auxilia na estimativa de uso de memória e tempo de execução de lógica programada e na seleção entre diferentes opções de programação.
Redundância	Manual do usuário do sistema de redundância ControlLogix, publicação 1756-UM523	Orienta o projeto, desenvolvimento e implementação de um sistema de redundância padrão ControlLogix.
	Manual do usuário do sistema de redundância aprimorado ControlLogix, publicação 1756-UM535	Orienta o projeto, desenvolvimento e implementação de um sistema de redundância aprimorado ControlLogix.

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	15
Diferença entre componentes padrão e de segurança	16
Recursos de fluxo de dados do controlador	16
Seleção do hardware do sistema	18
Selecionar módulos de E/S de segurança	20
Seleção das redes de comunicação	20
Especificações de programação	21

Requisitos da Aplicação de Segurança

O sistema do controlador GuardLogix é certificado para uso em aplicações de segurança até e incluindo o Nível de Integridade de Segurança (SIL) 3 e o Nível de Desempenho (e) no qual o estado desenergizado é o estado seguro. As especificações para a aplicação de segurança incluem a avaliação de probabilidade de taxas de falha (PFD e PFH), as configurações de tempo de reação do sistema e os testes de verificação de funcionamento que atendem critérios SIL 3/PL.

Para obter as especificações do sistema de segurança SIL 3 e PL, inclusive os intervalos de teste de validação de funcionamento, tempo de reação do sistema e cálculos PFD/PFH, consulte GuardLogix Controller Systems Safety Reference Manual, publicação [1756-RM093](#). É preciso ler, entender e satisfazer esses requisitos antes de operar um sistema de segurança GuardLogix SIL 3, PL.

As aplicações de segurança SIL 3/PL 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.

Consulte GuardLogix Controller Systems Safety Reference Manual, publicação [1756-RM093](#), para obter detalhes.

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 segurança CIP deve também 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 dos parâmetros do número da rede de segurança \(SNN\) na página 53](#).

Assinatura de tarefa de segurança

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

Consulte [Criação de uma assinatura de tarefa de segurança na página 106](#) para mais informações.

Diferença entre componentes padrão e de segurança

Os slots de um rack do sistema GuardLogix não utilizados pela função de segurança podem ser utilizados por outros módulos ControlLogix certificados como Baixa Tensão e Diretivas EMC. Consulte o site <http://ab.com/certification/ce> para localizar o certificado CE para o controle programável – a família de produtos ControlLogix e determinar quais módulos são certificados.

É necessário criar e documentar uma diferença objetiva, lógica e visível entre os itens padrão e de segurança da aplicação. Para ajudar na criação dessa distinção, o software de programação RSLogix 5000 fornece ícones de identificação de segurança para indicar a Tarefa de Segurança, programas, rotinas e componentes de segurança. Além disso, o software RSLogix 5000 usa um atributo de classe de segurança que é visível sempre que os recursos de tarefa de segurança, programas de segurança, tag de segurança ou instrução add-on de segurança são exibidos.

O controlador não permite gravar dados de tags de segurança em dispositivos de IHM externos ou por meio de instruções de mensagem de controladores peer. O software RSLogix 5000 pode escrever tags de segurança quando o controlador GuardLogix estiver com o status sem o bloqueio de segurança, não tem uma assinatura da tarefa de segurança e está em operação sem falha 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).

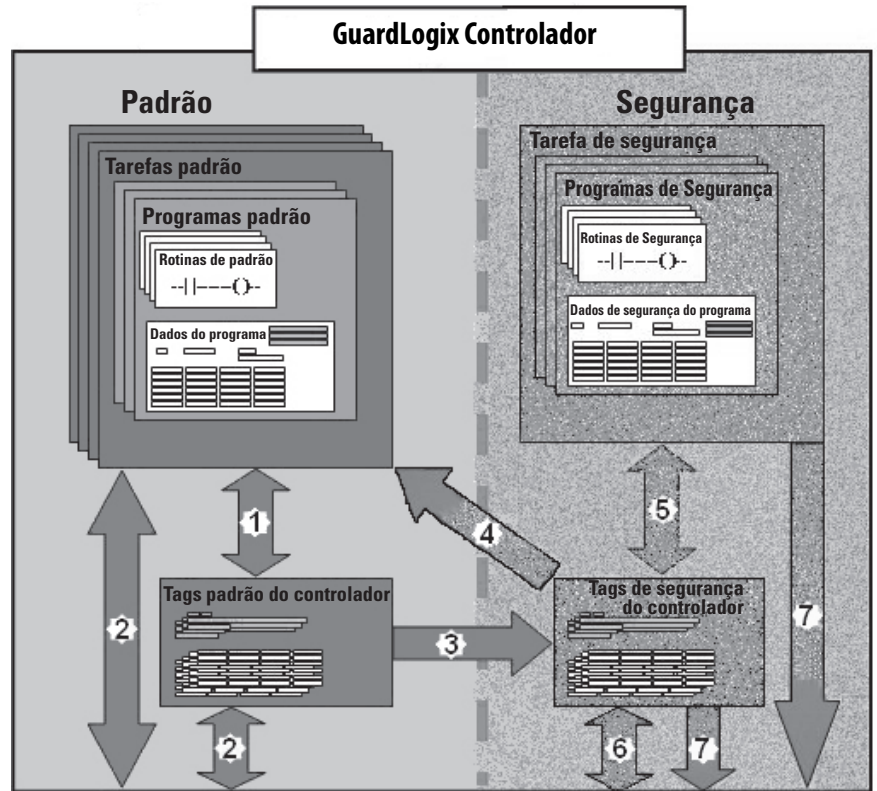
Dispositivos IHM


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

Recursos de fluxo de dados do controlador

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

Figura 1 – Recursos de fluxo de dados



Nº.	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/PLc.
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/PLc.

Seleção do hardware do sistema

O sistema GuardLogix oferece suporte a aplicações de segurança SIL 3 e PL. O controlador GuardLogix é constituído de um controlador primário e um parceiro de segurança que funcionam juntos em uma arquitetura 1oo2. A [Tabela 4](#) lista códigos 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-L61S, 1756-L62S, 1756-L63S	1756-LSP
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

Cód. cat.	Memória do usuário (capacidade RAM)	
	Tarefas e Componentes Padrão	Tarefa de Segurança e Componentes
1756-L61S	2 MB	1 MB
1756-L62S	4 MB	1 MB
1756-L63S	8 MB	3,75 MB
1756-L71S	2 MB	1 MB
1756-L72S	4 MB	2 MB
1756-L73S, 1756-L73SXT	8 MB	4 MB

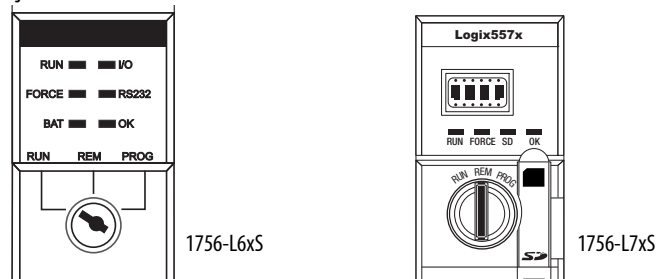
No software RSLogix 5000, versão 18 ou posterior, o controlador GuardLogix suporta atualizações do sistema operacional ou armazenamento e recuperação do programa do usuário pelo uso de um cartão de memória. Contudo, nas versões 16 e 17 do software RSLogix 5000, somente era possível visualizar o conteúdo de um cartão de memória se houvesse um instalado no controlador primário. Antes da versão 16, os cartões de memória não eram suportados.

Consulte [Capítulo 8, Armazenamento e carregamento de projetos usando memória não volátil](#), para mais informações.

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 28](#) 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 módulos de E/S de segurança

Os dispositivos de entrada e saída de segurança podem ser conectados a E/S CIP Safety nas redes DeviceNet ou EtherNet/IP, permitindo que os dispositivos de saída sejam controlados por um sistema de controlador GuardLogix através da comunicação DeviceNet ou EtherNet/IP.

Para informações mais atualizadas sobre os códigos de catálogo de E/S CIP Safety disponíveis, séries certificadas e revisões de firmware, consulte <http://ab.com/certification/safety>.

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 em redes DeviceNet ou EtherNet/IP.
- Distribuir e controlar E/S de segurança remotas em redes DeviceNet, EtherNet/IP ou ControlNet.
- Produzir e consumir dados de tags entre controladores GuardLogix 1756 e 1768 em 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	ENET-IN002
Controladores na rede ControlNet	1756-CN2, 1756-CN2R 1756-CN2RXT	CNET-IN005

O controlador GuardLogix pode se conectar ao software de programação RSLogix 5000 por conexão serial ou USB, um módulo EtherNet ou um módulo ControlNet.

Os controladores 1756-L6xS têm uma porta serial. Os controladores 1756-L7 xS têm uma porta USB.

Consulte [Recursos adicionais na página 13](#) para mais informações sobre o uso de módulos de comunicação de rede.

Especificações de programação

O software RSLogix 5000 é a ferramenta de programação para as aplicações do controlador GuardLogix.

Use a [Tabela 7](#) para identificar as versões mínimas do software para usar em seus controladores GuardLogix. O software RSLogix 5000, versão 15, não é compatível com o nível de integridade de segurança (SIL) 3.

Tabela 7 – Versões de software

Cód. cat.	Versão de software RSLogix 5000 ⁽¹⁾	Versão de software RSLinx® Classic ⁽¹⁾
1756-L61S, 1756-L62S	14	Qualquer versão
1756-L63S	16	
1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT	20	2.59

(1) Esta versão ou posterior.

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 – Recursos suportados pela versão do software RSLogix 5000

Recurso	Versão 14		Versão 16		Versão 17		Versão 18		Versão 19		Versão 20	
	Tarefa de segurança	Tarefa padrão	Tarefa de segurança	Tarefa padrão	Tarefa de segurança	Tarefa padrão	Tarefa de segurança	Tarefa padrão	Tarefa de segurança	Tarefa padrão	Tarefa de segurança	Tarefa padrão
Instruções Add-on				X		X	X	X	X	X	X	X
Alarmes e eventos				X		X		X		X		X
Armazenamento no controlador					X	X	X	X	X	X	X	X
Controle de acesso aos dados							X	X	X	X	X	X
Rotinas de Fase de Equipamento				X		X		X		X		X
Tarefas de Evento				X		X		X		X		X
Supervisor de firmware				X		X	X	X	X	X	X	X
FBD (Diagramas de Blocos de Funções)				X		X		X		X		X
Movimento Integrado				X		X		X		X		X
Lógica ladder	X	X	X	X	X	X	X	X	X	X	X	X
Troca de idiomas					X	X	X	X	X	X	X	X
Cartão de memória							X	X	X	X	X	X
Exportação e importação on-line de componentes de programação						X		X		X		X
Rotinas SFC (Controle Sequencial de Funções)				X		X		X		X		X
Texto Estruturado				X		X		X		X		X
Conexões unicast para tags de segurança produzidos e consumidos									X	X	X	X
Conexões unicast para módulos de segurança de E/S em redes EtherNet/IP											X	X

Para mais informações sobre o uso desses recursos, consulte o Logix5000 Controllers Common Procedures Programming Manual, publicação [1756-PM001](#), as publicações listadas no [Recursos adicionais na página 13](#), e ajuda on-line do software RSLogix 5000.

Observações:

Instale o controlador

Tópico	Página
Precauções	23
Certifique-se de que você tem todos os componentes	26
Instale um rack e fonte de alimentação	28
Instalação da bateria (somente controladores 1756-L6xS)	28
Instale o controlador no rack	29
Insira ou remova um cartão de memória	30
Faça conexões de comunicação	35
Atualize o controlador	39
Escolha o modo de operação do controlador	42
Desinstale um módulo de armazenamento de energia (ESM)	44
Instale um módulo de armazenamento de energia (ESM)	46

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 é considerado um equipamento industrial Grupo 1, Classe A de acordo com a publicação 11 do IEC/CISPR. Sem as devidas precauções, pode ser difícil garantir a compatibilidade eletromagnética em ambiente residencial e em outros ambientes devido a perturbações conduzidas e irradiadas.

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 o seguinte:

- 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 a energia backplane 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. 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:	Informations sur l'utilisation de cet équipement en environnements dangereux:
<p>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.</p>	<p>Les produits marqués « CL I, DIV 2, GP A, B, C, D » ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.</p>
<div style="display: flex; align-items: center;">  <div> <p>WARNING: EXPLOSION HAZARD</p> <ul style="list-style-type: none"> • 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. </div> </div>	<div style="display: flex; align-items: center;">  <div> <p>AVERTISSEMENT : RISQUE D'EXPLOSION</p> <ul style="list-style-type: none"> • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles. </div> </div>

As informações a seguir destinam-se à operação deste equipamento em áreas classificadas:

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.

**ADVERTÊNCIA: RISCO DE EXPLOSÃO**

- Não desconecte o equipamento a menos que não haja energia ou a área não apresente risco.
 - Não remova conexões deste equipamento a menos que não haja energia ou a área não apresente risco. Fixe 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:

- Este equipamento deve ser instalado em um gabinete que forneça pelo menos proteção IP54 quando aplicado em ambientes de Zona 2.
- Este equipamento deve ser usado dentro das suas taxas de especificação definidas pela Rockwell Automation.
- Este equipamento deve ser usado apenas com backplanes da Rockwell Automation com certificação ATEX.
- Fixe quaisquer conexões externas necessárias neste equipamento por meio de parafusos, travas deslizantes, conectores rosqueados ou outros meios fornecidos com este produto.
- Não desconecte o equipamento a menos que não haja energia ou a área não apresente risco.

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/PLe.

Controladores 1756-L6xS

Uma chave 1747-KY e uma bateria 1756-BA2 são enviadas com o controlador 1756-L6xS, enquanto o parceiro de segurança 1756-LSP é enviado com uma bateria 1756-BA2.

Se desejar conectar um dispositivo à porta serial do controlador (por exemplo, conectar um computador ao controlador), use um cabo serial 1756-CP3.

Para memória não volátil, é possível usar um cartão CompactFlash 1784-CF128 com os controladores GuardLogix 1756-L6xS, revisão do firmware 18 ou posterior.

Controladores 1756-L7xS

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

Cód. cat.	Descrição	Enviado com
1756-L71S 1756-L72S 1756-L73S	Controlador primário	<ul style="list-style-type: none"> Módulo de armazenamento de energia (ESM) com base em capacitor 1756-ESMCAP Cartão de memória Secure Digital (SD) 1784-SD1, 1 GB Chave 1747-KY
1756-L7SP	Parceiro de segurança	<ul style="list-style-type: none"> Módulo de armazenamento de energia 1756-SPESMNSE (ESM)
1756-L73SXT	Controlador primário de temperatura extrema	<ul style="list-style-type: none"> Módulo de armazenamento de energia (ESM) com base em capacitor 1756-ESMCAPXT Chave 1747-KY
1756-L7SPXT	Parceiro de segurança de temperatura extrema	<ul style="list-style-type: none"> 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. E ainda, pode-se usar este ESM apenas com um controlador 1756-L73S (8 MB) ou de memória 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 124](#).

(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-ESMNRMXT e 1756-SPESMNRMXT 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.

Cód. 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.

Cód. 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.

Instalação da bateria (somente controladores 1756-L6xS)

Os controladores 1756-L6xS e o parceiro de segurança 1756-LSP contêm uma bateria de lítio que deve ser substituída durante a vida útil do produto.



ADVERTÊNCIA: Pode ocorrer um arco elétrico ao conectar ou desconectar uma bateria. 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.

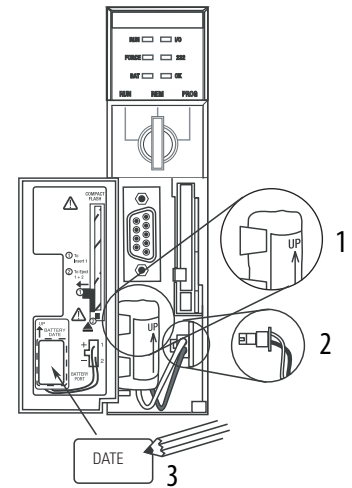
Para obter informações sobre o manuseio de baterias de lítio, inclusive o manuseio e descarte de baterias com vazamento, consulte as Orientações para o manuseio de baterias de lítio, publicação [AG 5-4](#).

Para manter a memória do controlador enquanto ele está sem alimentação, conecte uma bateria. Siga o procedimento tanto para o controlador 1756-L6xS quanto para o parceiro de segurança 1756-LSP.

IMPORTANTE Conecte somente uma bateria 1756-BA2 ao controlador. Caso seja conectada uma bateria diferente, o controlador poderá ser danificado.

Siga estas etapas para instalar uma bateria 1756-BA2 nova.

1. Instale a bateria conforme exibido.
2. Conecte a bateria:
+ Vermelho
- Preto
3. Anote a data de instalação na etiqueta da bateria e fixe-a no lado de dentro da porta do controlador.



Consulte o [Apêndice B](#) para obter mais informações sobre a manutenção da bateria.

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.

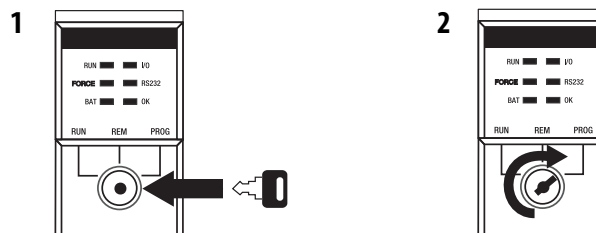
IMPORTANTE

Para controladores 1756-L7xS e parceiros de segurança 1756-L7SP, o ESM começa o carregamento quando uma destas ações ocorre:

- 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.

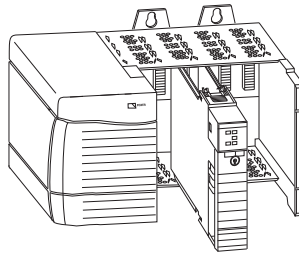
Depois que a energia é aplicada, o ESM carrega por até dois minutos conforme indicado por CHRG ou ESM Charging na tela de status.

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 acionadas.

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.

Os controladores 1756-L7xS usam cartões Secure Digital (SD). Consulte [Página 31](#).

O controlador 1756-L6xS usa cartões CompactFlash (CF). Consulte [Página 33](#).

Cartão secure digital (controladores 1756-L7xS)

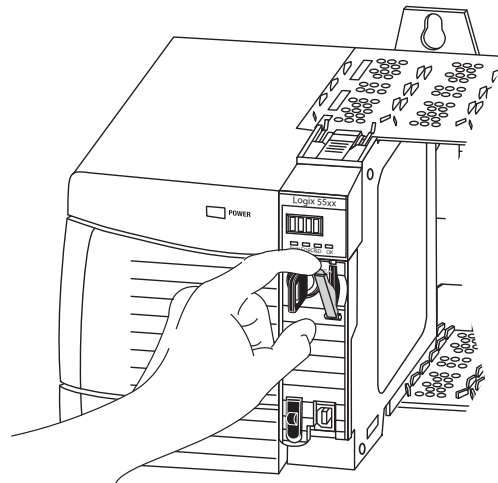
O controlador 1756-L7xS é entregue com um cartão SD instalado. Recomendamos que você deixe um cartão SD instalado.

Remova o cartão SD

Se quiser remover o cartão SD do controlador 1756-L7xS, siga estas etapas.

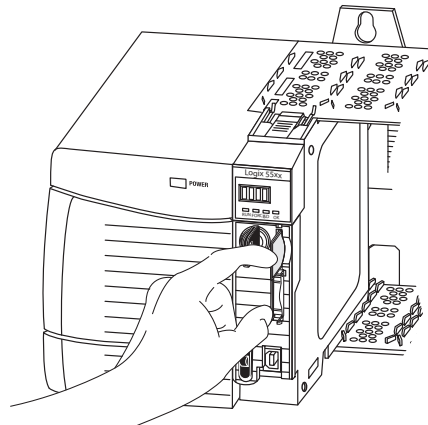
IMPORTANTE Certifique-se de que o indicador de status do cartão SD está desligado e que o cartão não está em uso antes de removê-lo.

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



32015-M

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



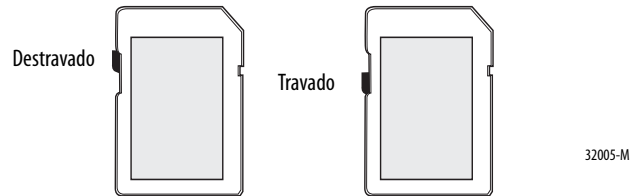
32004-M

4. Remova o cartão SD e feche a porta.

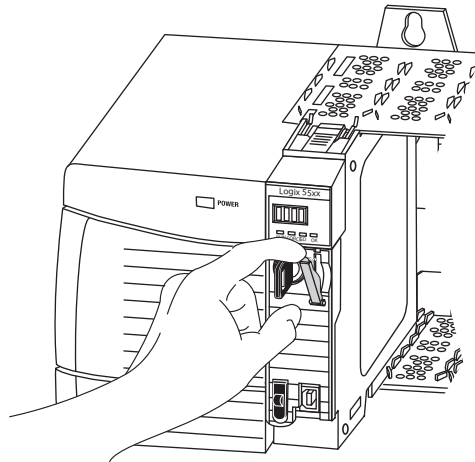
Instale o cartão SD

Siga estas etapas para instalar o cartão SD nos controladores 1756-L7xS.

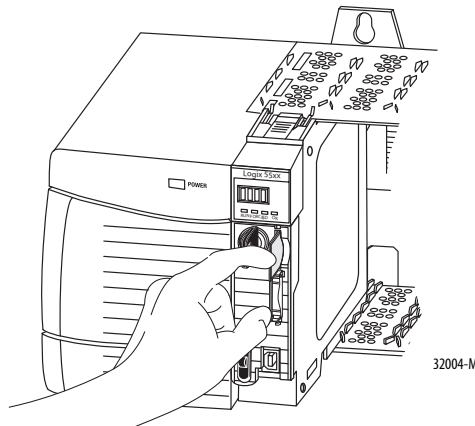
1. Verifique se o cartão SD está travado ou destravado de acordo com a sua preferência.



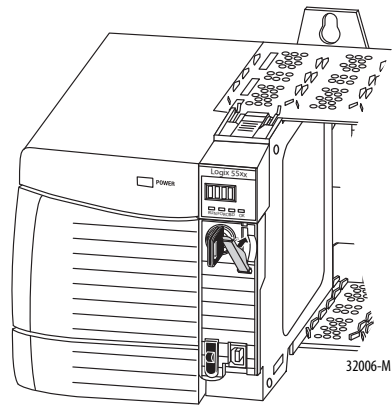
2. Abra a porta para o cartão SD.



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.



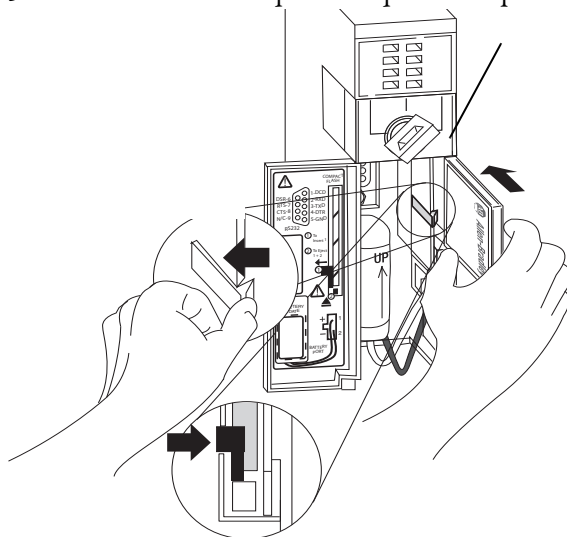
Cartão CompactFlash (controladores 1756-L6xS)

Os controladores 1756-L6xS não são enviados com cartões CompactFlash instalados.

Instale um cartão CF

Siga estas etapas para inserir o cartão de memória.

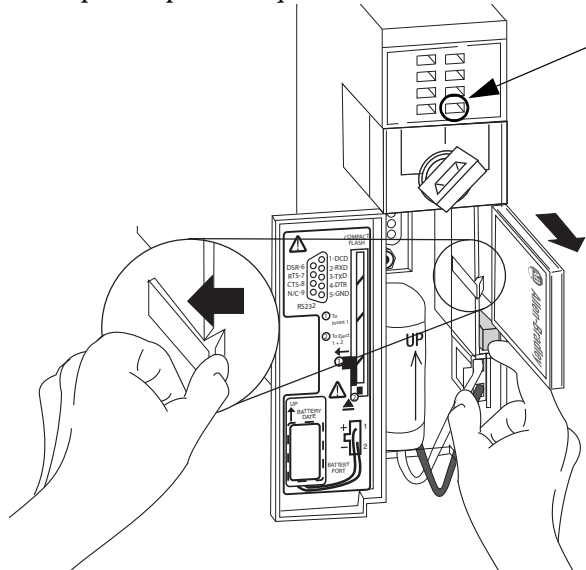
1. Gire a chave seletora para a posição PROG.
2. Abra a porta do controlador.
3. Empurre a trava para a esquerda.
4. Insira o cartão de memória com o logo A-B virado para a esquerda.
5. Solte a trava e certifique-se de que deslize por sobre o cartão de memória.



Remova um cartão CF

Siga estas etapas para remover o cartão de memória.

1. Se o indicador de status OK estiver piscando em verde, aguarde até que pare de piscar e fique verde.



2. Abra a porta do controlador.
3. Empurre e segure a trava para a esquerda.
4. Pressione o botão de ejeção e remova o cartão.
5. Libere a trava.

Faça conexões de comunicação

Os controladores 1756-L7 xS têm uma porta USB. Consulte [Conecte-se à porta USB do controlador 1756-L7xS](#).

Os controladores 1756-L6xS têm uma porta serial. Consulte [Conecte-se à porta serial do controlador 1756-L6xS na página 37](#).

Conecte-se à porta USB do controlador 1756-L7xS

O controlador tem uma porta USB que usa um receptáculo Tipo B. A porta é compatível com USB 2.0 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.



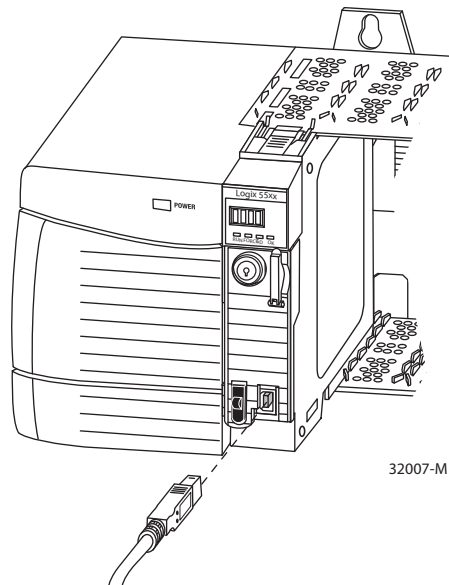
ATENÇÃO: A porta USB destina-se apenas para fins de programação local temporária e não para conexão permanente.

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 – Conexão 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.

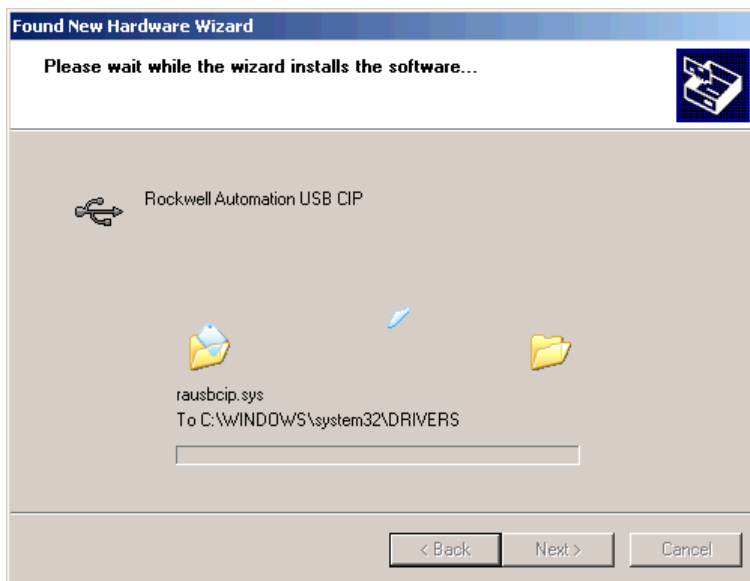
1. Conecte seu controlador e estação de trabalho usando um cabo USB.
2. Na caixa de diálogo Found New Hardware Wizard, clique em qualquer uma das opções de conexão Windows Update e clique em Next.




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.

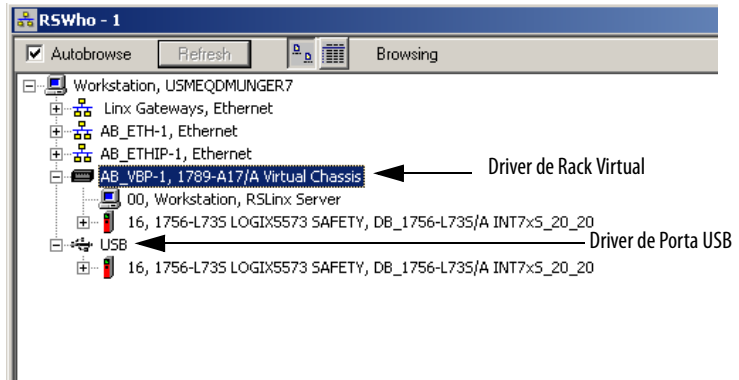
O software é instalado.



4. Clique em Finish para definir seu driver USB.

5. Para buscar seu controlador no software RSLinx, clique em RSWho .

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



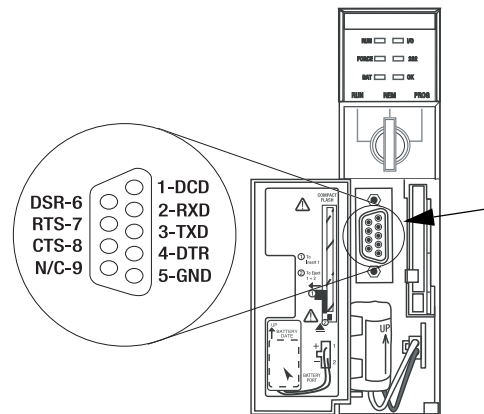
Conecte-se à porta serial do controlador 1756-L6xS



ADVERTÊNCIA: Se o cabo serial for conectado ou desconectado com a alimentação aplicada a este módulo ou ao dispositivo serial na outra extremidade do cabo, 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.

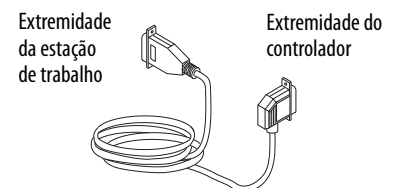
Use a porta serial no controlador 1756-L6xS para comunicação RS-232.

Figura 4 – Porta serial



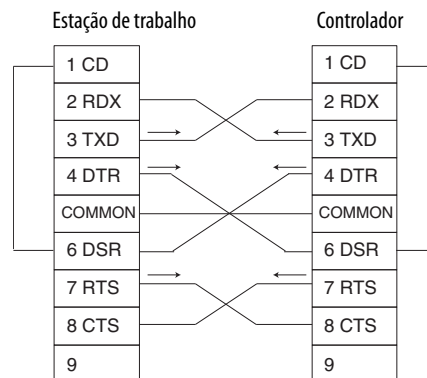
Para conectar uma estação de trabalho à porta serial, use um destes cabos:

- Cabo serial 1756-CP3
- Cabo 1747-CP3 da família de produtos SLC (se utilizar este cabo, a porta do controlador pode não fechar.)



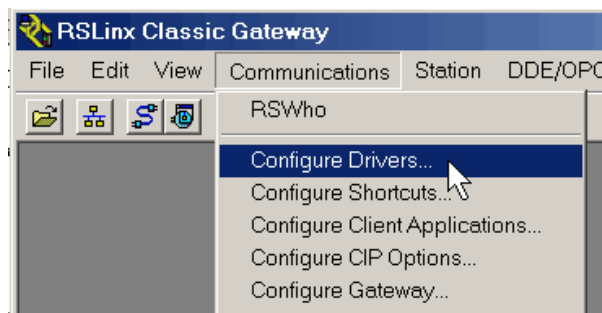
Se você fabricar seu próprio cabo serial, siga estas orientações.

- Limite o comprimento a 15,2 m (50 pés).
- Ligue os conectores como mostrado.
- Conecte a blindagem a ambos os conectores.

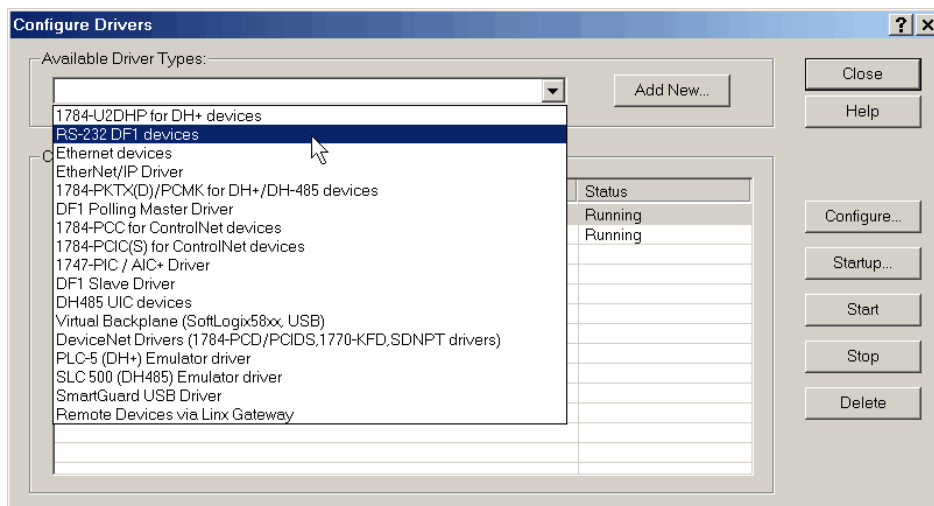


Siga estas etapas para usar o software RSLinx para configurar o driver de dispositivo RS-232 DF1 para comunicação serial.

1. No software RSLinx, no menu Communications, selecione Configure Drivers.

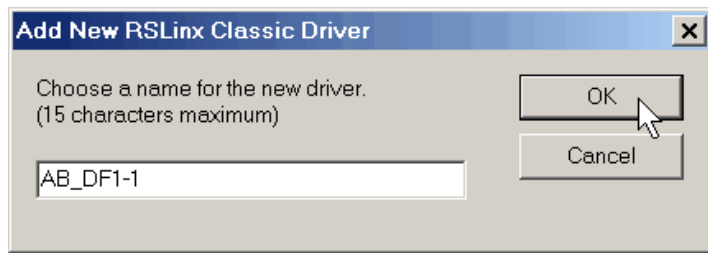


A caixa de diálogo Configure Drivers aparecerá.

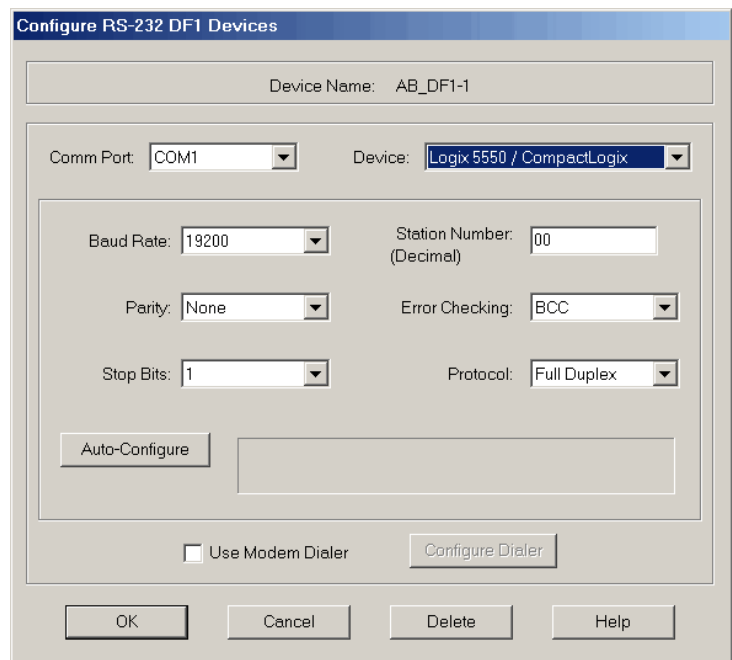


2. A partir da lista do menu Available Driver Types, escolha o driver de dispositivo RS-232 DF1.
3. Clique em Add New.

A caixa de diálogo Add New RSLinx Driver aparecerá.



4. Digite o nome do driver e clique em OK.
5. Especifique as configurações da porta serial.
 - a. No menu Comm Port, selecione a porta serial na estação de trabalho à qual o cabo está conectado.
 - b. No menu Device, selecione Logix 5550/CompactLogix.
 - c. Clique em Auto-Configure.



6. Se a autoconfiguração for realizada com sucesso, clique em OK.
Se a autoconfiguração não tiver sucesso, certifique-se de que a Comm Port correta foi selecionada.
7. Clique em Close.

Atualize o controlador

Os controladores são entregues sem o firmware. O firmware do controlador está integrado ao software de programação RSLogix 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/>.

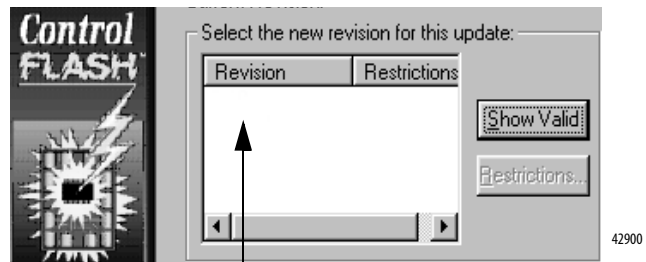
É possível atualizar o firmware usando o software ControlFLASH™, que está integrado ao software RSLogix 5000 ou utilizando o recurso AutoFlash do software RSLogix 5000.

Usando o software ControlFLASH para atualizar o firmware

Com o software ControlFLASH, versão 8 ou posterior (software RSLogix 5000, versão 18 ou posterior), o parceiro de segurança é automaticamente atualizado, quando o controlador primário é atualizado.

IMPORTANTE Nos controladores 1756-L7xS, se o cartão SD estiver travado e a opção Load Image armazenada do projeto estiver configurada para a 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 a que se quer atualizar o controlador e clique em Next.
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.

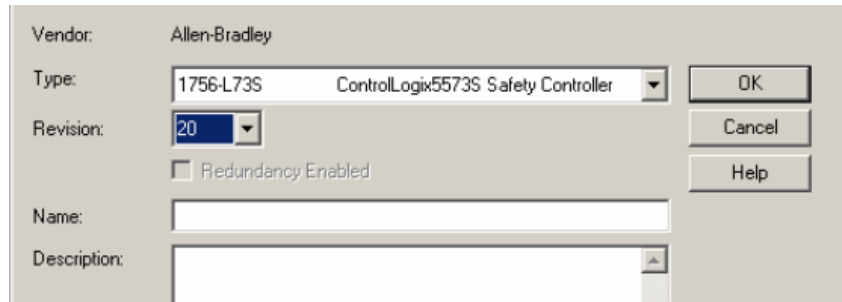
DICA Se a atualização ControlFLASH do controlador for interrompida, o controlador 1756-L7xS reverte ao firmware de inicialização do sistema, que é a revisão 1.xxx do firmware.

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 do software RSLogix 5000, siga estas etapas.

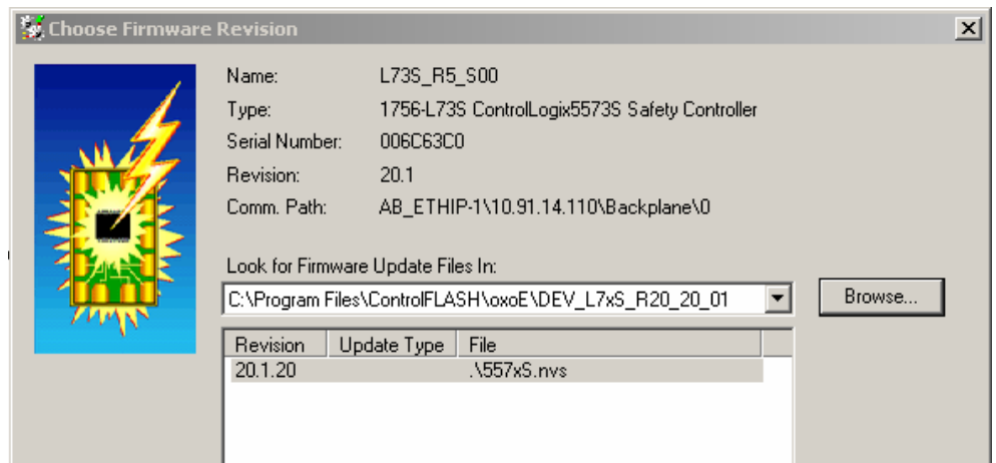
1. Certifique-se de que a conexão de rede apropriada seja feita e que o driver de rede esteja configurado no software RSLinx.
2. Use o software de programação RSLogix 5000 para criar um projeto de controlador na versão de que você precisa.



3. Clique RSWho para especificar o caminho do controlador.



4. Selecione seu controlador e clique em Update Firmware.
5. Selecione a revisão do firmware a ser atualizada.



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. É possível completar outras tarefas no software RSLogix 5000.

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

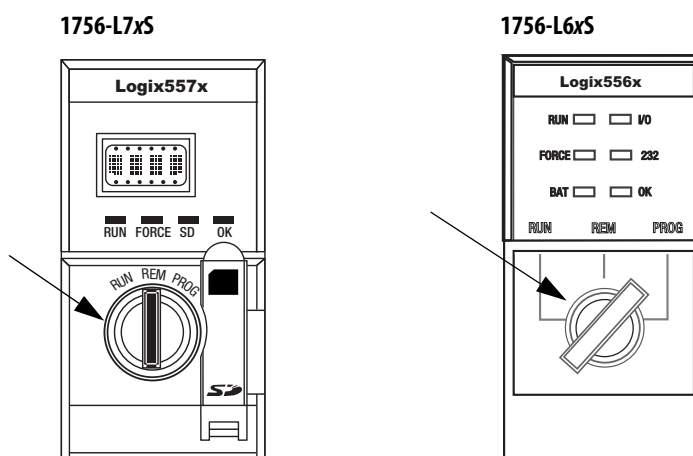
Se deseja	Selecione um destes modos				
	Run	Remoto			Program
		Run	Teste	Program	
Modifique as saídas ao estado comandado pela lógica do projeto	X	X			
Modifique as saídas ao seu estado configurado para o modo do programa			X	X	X
Execute as tarefas (varredura)	X	X	X		
Mude o modo do controlador por 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 5 – Chave seletora do controlador



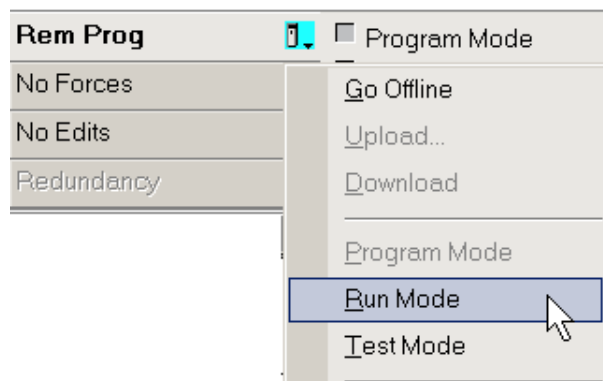
Use o software RSLogix 5000 para mudar o modo de operação

Dependendo do modo do controlador que você especificar usando a chave seletora, pode-se mudar o modo de operação usando o software RSLogix 5000.

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 do software RSLogix 5000 para especificar estes modos de operação:

- Programa remoto
- Operação remota
- Teste remoto

Figura 6 – Modo de operação via software RSLogix 5000



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 1756-L7xS são enviados com um ESM instalado.

Controlador	Código de catálogo de 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 os controladores 1756-L7xS perdem 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 de um controlador 1756-L7xS.

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 a sua aplicação necessita que o ESM esgote sua energia residual armazenada para 40 µJoule 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.

- Desligue a alimentação do rack.
Depois que desligar o rack, o indicador de status OK do controlador muda de verde para vermelho para OFF.
- Espere **pelo menos 20 minutos** para que a energia residual diminua para 40 µJoules 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 a energia backplane 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. Arcos elétricos repetidos causam desgaste excessivo nos contatos tanto do módulo quanto do conector correspondente.

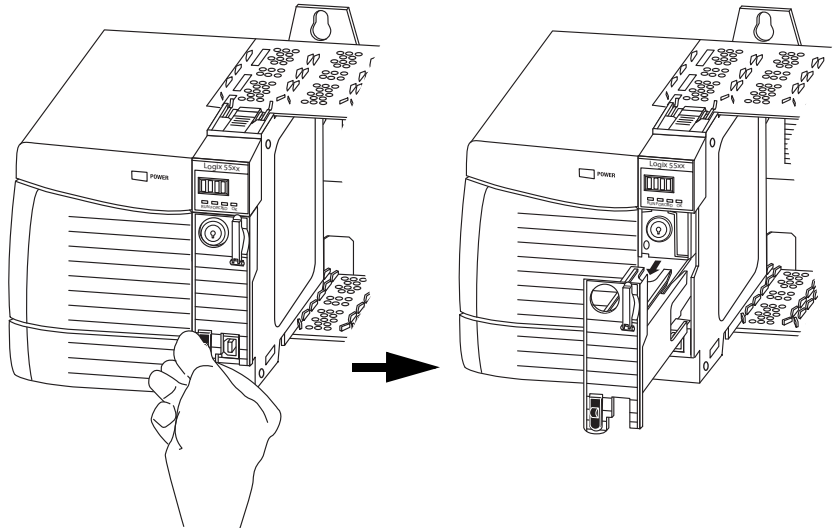
1. Remova a chave da chave seletora.

IMPORTANTE A próxima etapa depende de quais das condições seguintes se aplicam à sua aplicação:

- Se estiver removendo o ESM de um controlador 1756-L7xS(XT) energizado, vá para a [etapa 2](#).
- Se estiver removendo o ESM de um controlador 1756-L7xS(XT) 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.

Espera 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.

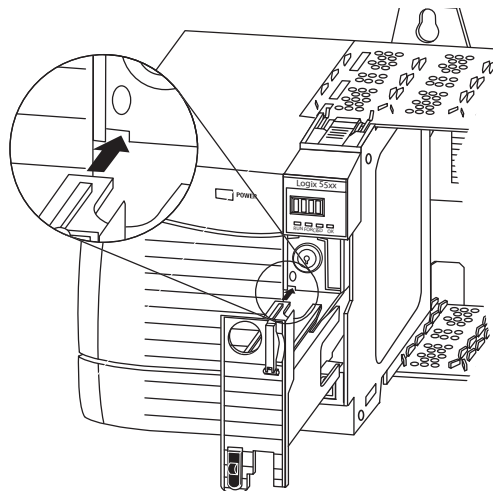
Instale um módulo de armazenamento de energia (ESM)

Tabela 10 – Módulos de armazenamento de energia compatíveis

Cód. 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
- CHRGR

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 'CHRGR' 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.

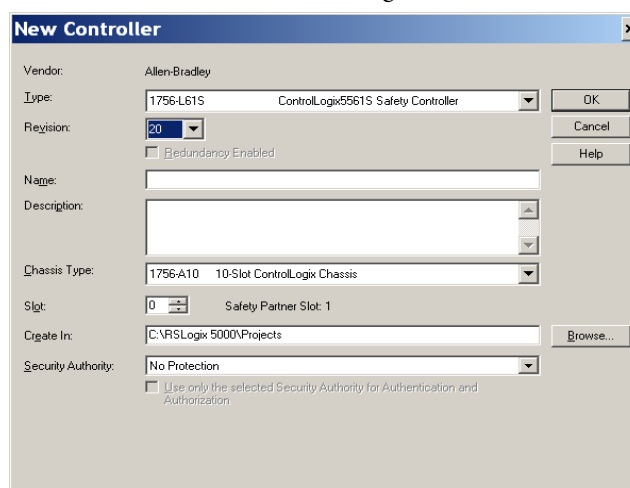
Configuração do controlador

Tópico	Página
Criação de um projeto do controlador	47
Definir senhas de bloqueio e desbloqueio	49
Gerenciamento da substituição do módulo de E/S	51
Habilitação da sincronia de tempo	51
Configurar um Controlador de Segurança Peer	52

Criação de um projeto do controlador

Para configurar e programar seu controlador GuardLogix, utilize o software RSLogix 5000 para criar e gerenciar um projeto para o controlador.

1. Crie um projeto no software RSLogix 5000 clicando no botão New na barra de ferramentas principal.
2. A partir do menu Type, selecione um controlador GuardLogix:
 - Controlador 1756-L61S ControlLogix5561S
 - Controlador 1756-L62S ControlLogix5562S
 - Controlador 1756-L63S ControlLogix5563S
 - Controlador 1756-L71S ControlLogix5571S
 - Controlador 1756-L72S ControlLogix5572S
 - Controlador 1756-L73S ControlLogix5573S



3. Insira a revisão principal de firmware do controlador.
4. Digite um nome para o controlador.

Quando você cria um projeto, o nome é igual ao do controlador. No entanto, é possível renomear o projeto ou o controlador.

5. Selecione as dimensões do rack.
6. Insira o número de slot do controlador.

A caixa de diálogo New Controller 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.

7. Especifique a pasta na qual armazenar o projeto do controlador de segurança.
8. Para RSLogix 5000, versão 20 ou posterior, selecione a opção Security Authority.

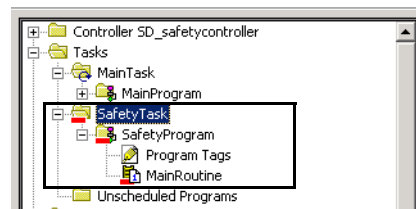
Para informações detalhadas sobre segurança, consulte o Manual de programação de segurança dos controladores Logix5000, publicação [1756-PM016](#).

9. Clique em OK.

O software RSLogix 5000 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 7 – Tarefa de segurança no organizador do controlador

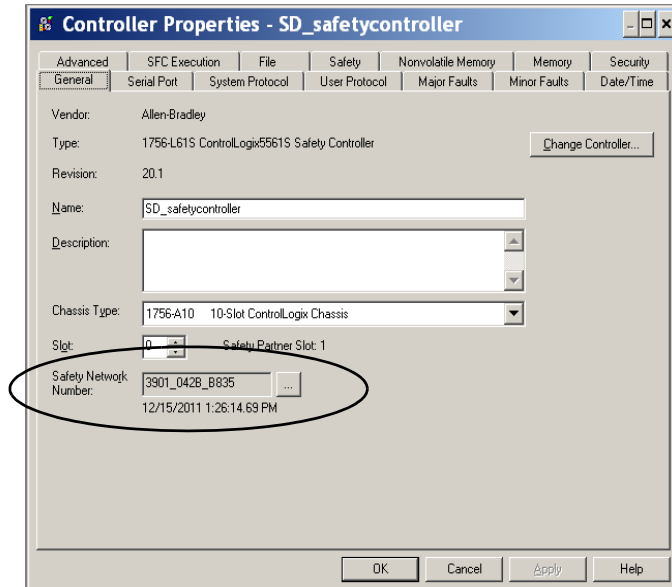


Uma barra vermelha abaixo do ícone da pasta diferencia os programas e as rotinas dos componentes do projeto padrão no organizador do controlador do RSLogix 5000.

Quando um novo projeto de segurança é criado, o software RSLogix 5000 também cria automaticamente um número da rede de segurança (SNN).

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, há casos em que você pode querer inserir um SNN específico.

Figura 8 – Número da rede de segurança**DICA**

É possível usar a caixa de diálogo Controller Properties para mudar o controlador padrão para segurança e vice-versa, clicando em Change Controller. No entanto, os projetos padrão e de segurança serão muito afetados.

Consulte o [Apêndice C, Alteração do tipo do controlador nos projetos RSLogix 5000](#), 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	Fornecer mais informações sobre como gerenciar o SNN

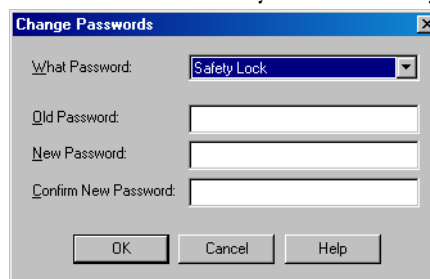
Definir senhas de bloqueio e desbloqueio

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. Escolha Tools > Safety > Change Password.
2. No menu What Password, escolha Safety Lock ou Safety Unlock.

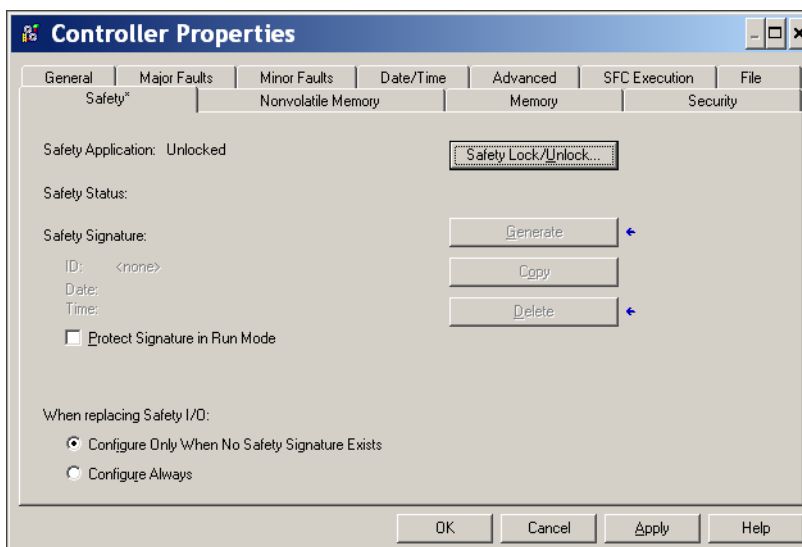


3. Digite a senha antiga, se houver uma.
4. Digite e confirme a nova senha.
5. Clique em OK.

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

Protegendo a assinatura da tarefa de segurança em modo de operação

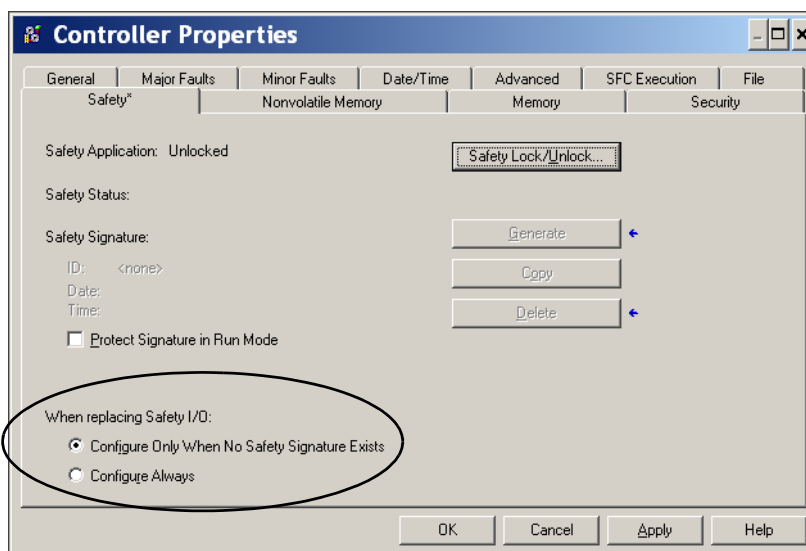
Pode-se impedir que a assinatura da tarefa de segurança seja gerada ou apagada enquanto o controlador está em modo de operação ou em modo de operação remoto, independentemente se a aplicação de segurança está bloqueada ou desbloqueada, verificando Protect Signature in Run Mode na guia Safety da caixa de diálogo Controller Properties.



Gerenciamento da substituição do módulo 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 definirá o número da rede de segurança (SNN) de um módulo de E/S com uma conexão que apresenta dados de configuração quando existir uma assinatura de segurança⁽¹⁾.

Figura 9 – Opções de substituição do módulo 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.

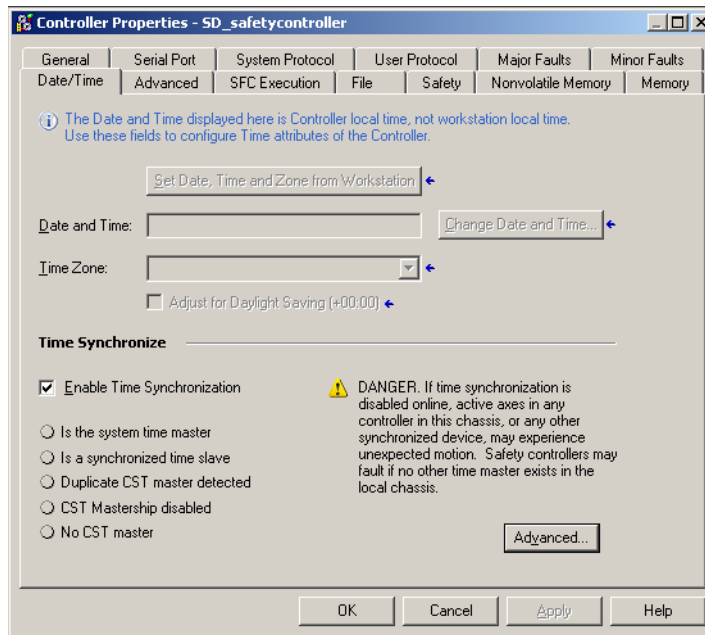
Consulte [Capítulo 5, Adição, configuração, monitoração e substituição da E/S de segurança CIP](#) para mais informações.

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). Para permitir que o controlador se torne mestre CST, habilite Time Synchronization na aba Date/Time da caixa de diálogo Controller Properties. A opção Time Synchronization oferece um mecanismo padrão para sincronizar relógios por uma rede de dispositivos distribuídos.

(1) A assinatura da tarefa de segurança é um número usado exclusivamente para identificar a lógica, os dados e a configuração de cada projeto, protegendo assim o nível de integridade de segurança do sistema (SIL). Consulte [Assinatura de tarefa de segurança na página 16](#) e [Criação de uma assinatura de tarefa de segurança na página 106](#) para mais informações.

Figura 10 – 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](#).

Configurar 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 produzidos/consumidos na página 97](#).

Comunicar-se nas Redes

Tópico	Página
Rede de Segurança	53
Comunicação EtherNet/IP	59
Comunicação ControlNet	63
Comunicação DeviceNet	65
Comunicação em série	67
Recursos adicionais	68

Rede de Segurança

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

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

Administração dos parâmetros do número da rede de segurança (SNN)

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

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

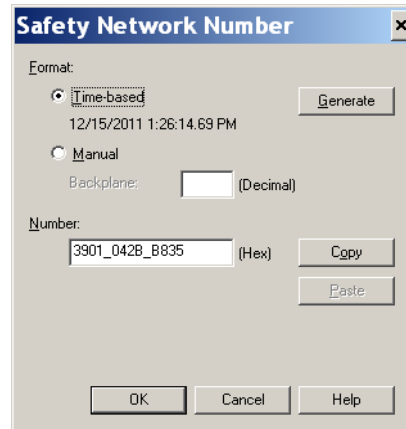
DICA Vários números de rede de segurança podem ser atribuídos a uma sub-rede CIP Safety ou a um rack ControlBus contendo vários dispositivos de segurança. **Porém, para simplificar, recomendamos que cada sub-rede CIP Safety tenha um e somente um SNN exclusivo.**

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

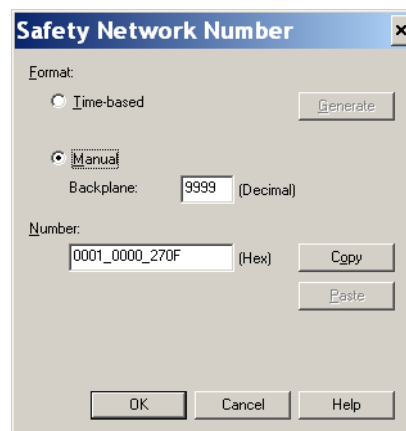
Figura 11 – Formato com base na hora



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 dos parâmetros do número da rede de segurança (SNN)

Você pode permitir que o software RSLogix 5000 atribua automaticamente um SNN ou você pode atribuir o SNN manualmente.

Atribuição automática

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

Atribuição manual

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

Consulte [Alteração dos parâmetros do número da rede de segurança \(SNN\) na página 55](#).

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.

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.

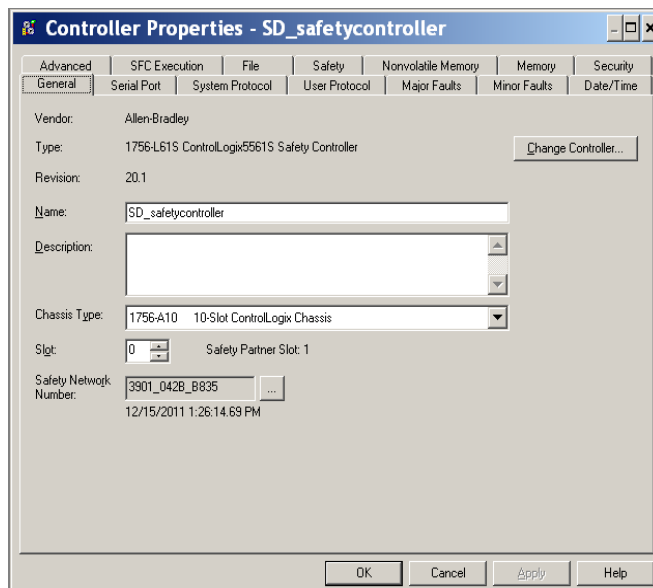
Alteração dos parâmetros do número da rede de segurança (SNN)

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

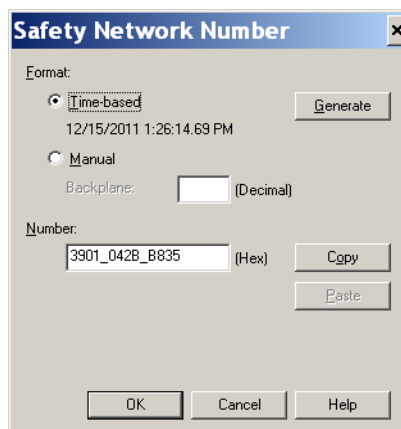
- desproteger o projeto, caso esteja protegido.
Consulte [Bloqueio de segurança do controlador na página 105](#).
- excluir a assinatura da tarefa de segurança, caso exista uma.
Consulte [Remover a assinatura da tarefa de segurança na página 108](#).

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.



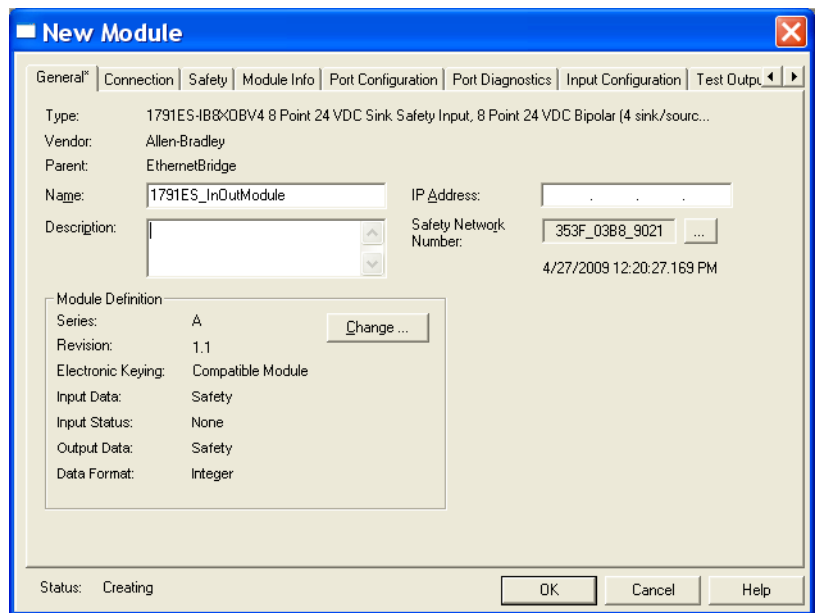
4. Clique em OK.

Altere o numero de rede de segurança (SNN) dos módulos 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 módulos de E/S de segurança disponíveis através do módulo de comunicação EtherNet/IP.

3. Clique duas vezes no primeiro módulo de E/S de segurança para visualizar a guia General.

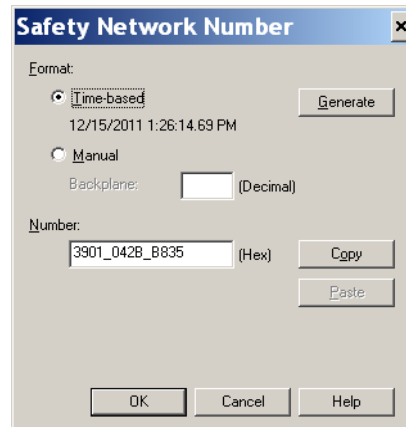


4. Clique em à direita do número da rede de segurança para abrir a caixa de diálogo Safety Network Number.
5. Escolha Time-based e clique em Generate para criar um novo SNN referente à rede EtherNet/IP.
6. Clique em OK.
7. Clique em Copy para copiar o novo SNN para a área de transferência do Windows.
8. Abra a guia General da caixa de diálogo Module Properties do próximo módulo 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 equipamento.
11. Clique em OK.
12. Repita as etapas [8](#) a [10](#) para os módulos safety I/O 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 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 módulo 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 módulo safety I/O, escolha qualquer um dos módulos mostrados na [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	<ul style="list-style-type: none"> • Conecta os controladores aos módulos 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	<ul style="list-style-type: none"> • Realiza as mesmas funções que o módulo 1756-ENBT, com o dobro da capacidade para aplicações mais exigentes. • Fornece uma conexão de configuração temporária por meio da porta USB. • Configura os endereços IP rapidamente usando chaves rotativas.
1756-EN2F	<ul style="list-style-type: none"> • Realiza as mesmas funções que o módulo 1756-EN2T. • Conecta a mídia de fibra por um conector de fibra LC no módulo.
1756-EN2TXT	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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-EN3TR	<ul style="list-style-type: none"> • Realiza as mesmas funções que o módulo 1756-EN2TR. • Três portas para conexão DLR.
1756-EWEB	<ul style="list-style-type: none"> • Fornece páginas da internet personalizáveis para acesso externo às informações do controlador. • Fornece 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. <p>Este módulo não fornece suporte para tags de E/S produzidos ou consumidos, e não suporta comunicação CIP Safety.</p>

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 de software estão disponíveis para rede EtherNet/IP.

Tabela 13 – Software para módulos EtherNet/IP

Software	Objetivo	Necessário
Software de programação RSLogix 5000	Este software é necessário para configurar o projeto do controlador e definir a comunicação EtherNet/IP.	Sim
Utilitário BOOTP/DHCP	Este utilitário vem com o software RSLogix 5000. É possível usar este utilitário para atribuir endereços IP a dispositivos em uma rede EtherNet/IP.	Negativo
Software RSNetWorx para EtherNet/IP	É possível usar este software para configurar dispositivos EtherNet/IP por meio de endereços IP ou nomes de host.	Negativo
Software RSLinx	É possível usar este software para configurar dispositivos, estabelecer comunicação entre dispositivos e fornecer diagnósticos.	Sim

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.

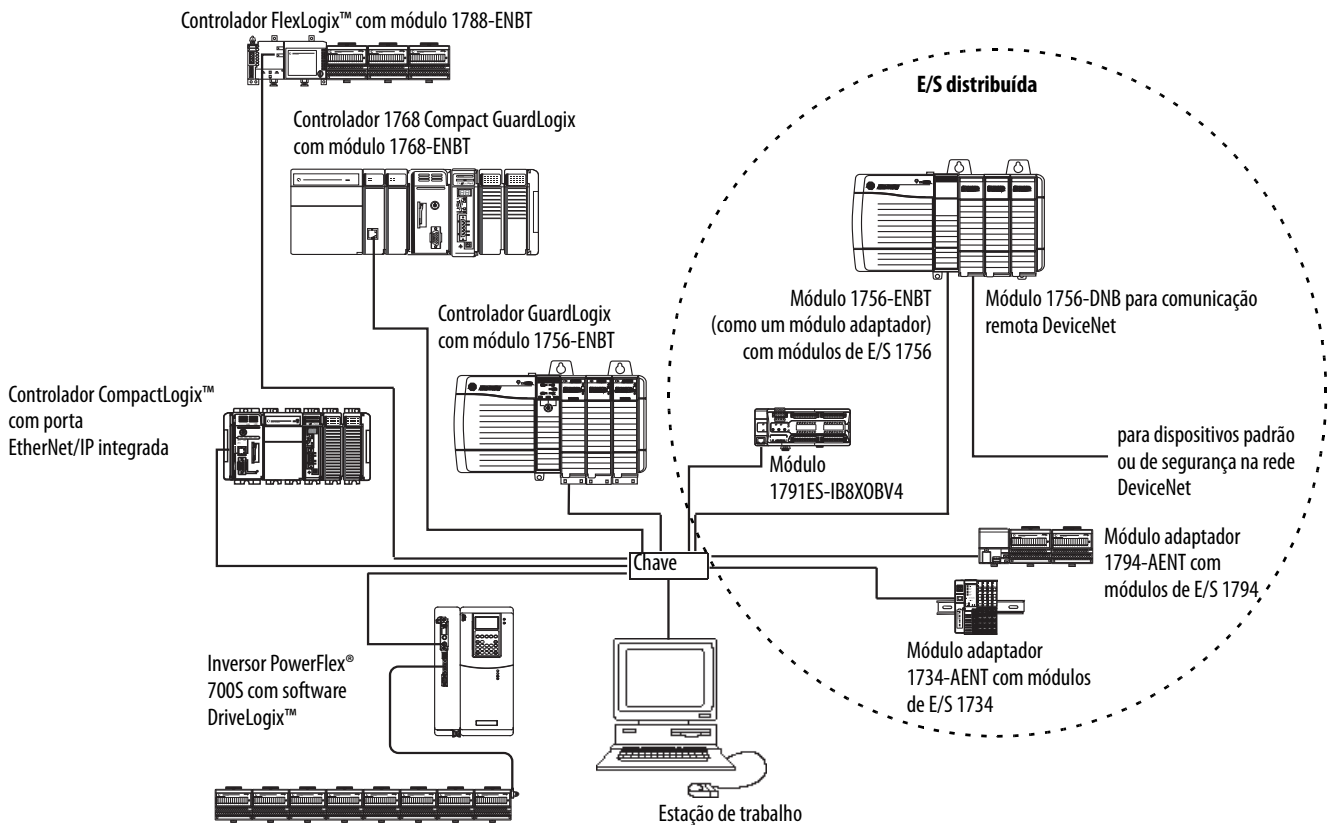
Os módulos de comunicação EtherNet/IP suportam com 128 conexões do protocolo industrial comum (CIP) em uma rede EtherNet/IP.

Exemplo de comunicação EtherNet/IP

Este exemplo ilustra o seguinte:

- 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.
- o microcomputador pode fazer upload/download de projetos nos controladores.
- o microcomputador pode configurar equipamentos na rede EtherNet/IP.

Figura 13 – Exemplo de comunicação EtherNet/IP

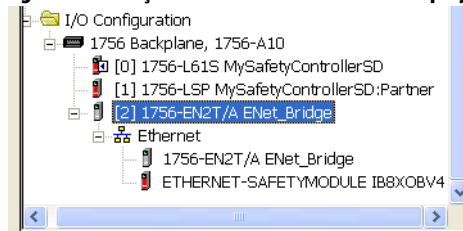


Conexões EtherNet/IP para módulos de E/S CIP Safety

Os módulos de E/S CIP Safety nas redes EtherNet são adicionados ao projeto sob o módulo de comunicação EtherNet/IP, conforme descrito em [Capítulo 5. Adição, configuração, monitoração e substituição da E/S de segurança CIP](#). Ao adicionar um módulo de E/S CIP Safety, o software RSLogix 5000 cria automaticamente tags de dados de segurança do controlador para o respectivo módulo.

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

Figura 14 – Adição de módulos EtherNet/IP ao projeto



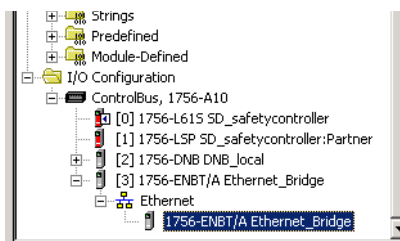
Conexões padrão de EtherNet/IP

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 controlador GuardLogix.

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	<p>O endereço IP identifica exclusivamente o módulo e. 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</p> <ul style="list-style-type: none"> • 000.xxx.xxx.xxx • 127.xxx.xxx.xxx • 223 a 255.xxx.xxx.xxx
Máscara de sub-rede	<p>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.</p> <p>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.</p>
Conversor de protocolos	<p>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.</p>

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



3. Use o software RSLogix 5000 para descarregar o 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
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> desempenha as mesmas funções que o módulo 1756-CNB também suporta mídia ControlNet redundante 	1756-CNBR
<ul style="list-style-type: none"> desempenha as mesmas funções compatíveis com o módulo 1756-CNB com melhor desempenho suporta comunicação CIP Safety 	1756-CN2
<ul style="list-style-type: none"> desempenha as mesmas funções que o módulo 1756-CN2 também suporta mídia ControlNet redundante 	1756-CN2R
<ul style="list-style-type: none"> 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 de software estão disponíveis para rede ControlNet.

Tabela 15 – Software para módulos ControlNet

Software	Objetivo	Necessário
Software de programação RSLogix 5000	Este software é necessário para configurar o projeto GuardLogix e definir a comunicação ControlNet.	Sim
Software RSNetWorx for ControlNet	Este software é necessário para configurar a rede ControlNet, definir o tempo de atualização da rede (NUT) e programar a rede ControlNet.	Sim
Software RSLinx	É possível usar este software para configurar dispositivos, estabelecer comunicação entre dispositivos e 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 controlador GuardLogix.

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 confiáveis 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 módulo de E/S é uma conexão programável porque dados são recebidos repetidamente do módulo em um intervalo especificado. Outras conexões programáveis incluem conexões com: <ul style="list-style-type: none"> • 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. <p>As conexões não programáveis usam o restante da largura de banda da rede depois que as conexões programáveis são alocadas.</p> <p>As conexões de segurança produzidas/consumidas não são programáveis.</p>

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.

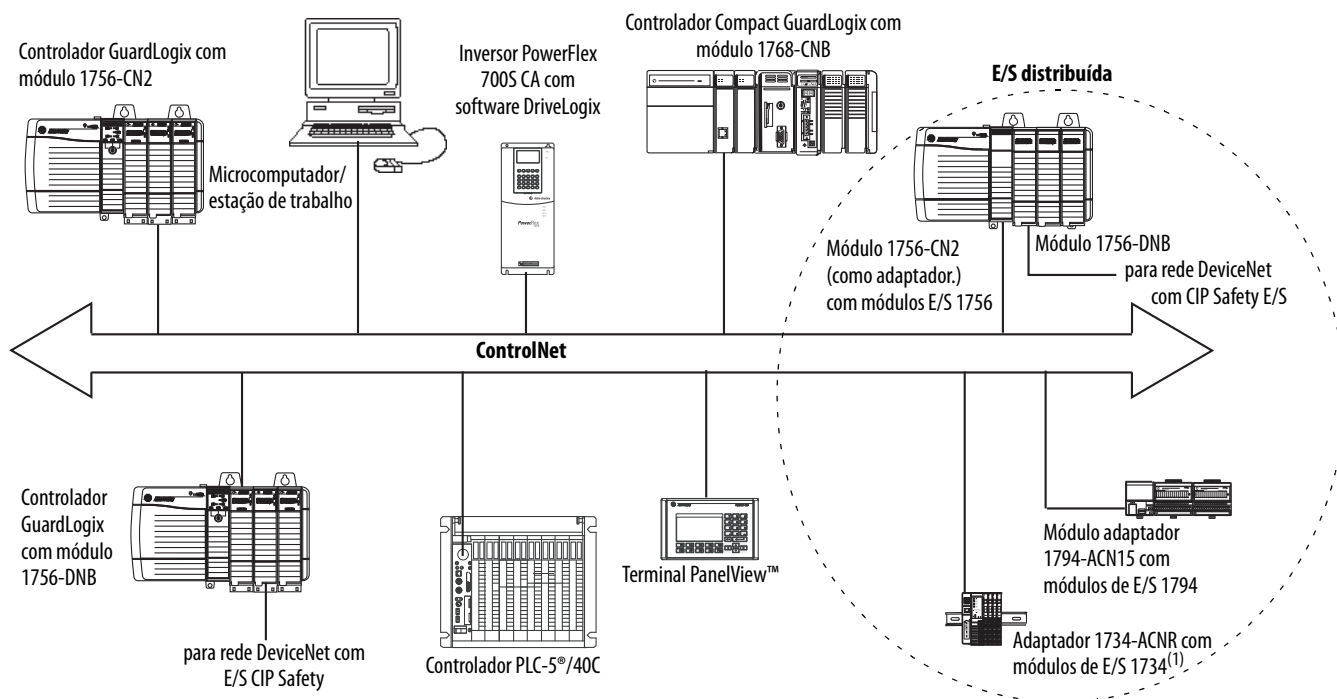
O módulo 1756-CN2 suporta 128 conexões CIP em uma rede ControlNet.

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 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 15 – 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 módulos de E/S distribuídas pela rede ControlNet, acrescente uma ponte ControlNet, um módulo adaptador ControlNet e módulos de E/S à pasta I/O Configuration do controlador.

Comunicação DeviceNet

Para se comunicar e trocar dados com os módulos de E/S CIP Safety 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 de software são usados com as redes DeviceNet e módulo 1756-DNB.

Tabela 17 – Software para uso com redes DeviceNet

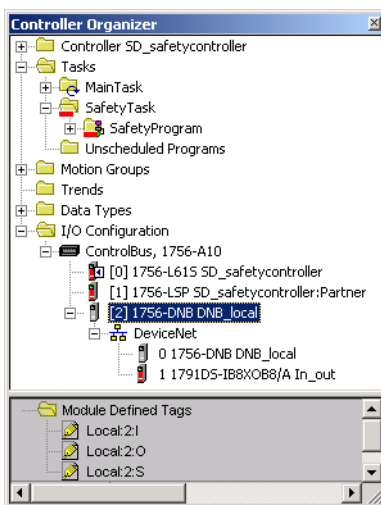
Software	É usado para	Necessário/Opcional
RSLogix 5000	<ul style="list-style-type: none"> • Configure os projetos ControlLogix. • Defina a comunicação DeviceNet. 	Necessário
RSNetWorx™ para DeviceNet	<ul style="list-style-type: none"> • Configura dispositivos DeviceNet. • Define a lista de varredura para esses dispositivos. 	
RSLinx Classic ou RSLinx Enterprise	<ul style="list-style-type: none"> • Configura os dispositivos de comunicação. • Fornece diagnósticos. • Estabelece comunicação entre os dispositivos. 	

Conexões DeviceNet para módulos CIP Safety E/S

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

Os módulos de E/S CIP Safety em redes DeviceNet são adicionados ao projeto no módulo 1756-DNB, conforme descrito no [Capítulo 5, Adição, configuração, monitoração e substituição da E/S de segurança CIP](#). Ao adicionar um módulo de E/S CIP Safety, o software RSLogix 5000 cria automaticamente tags de dados de segurança do controlador para o respectivo módulo.

Figura 16 – 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 I/O Configuration do controlador, o software RSLogix 5000 cria automaticamente um conjunto de tags padrão para dados de entrada, saída e status da rede.

Comunicação em série

Para operar o controlador GuardLogix em uma rede serial, é necessário fazer o seguinte:

- Uma estação de trabalho com uma porta serial
- Software RSLinx para configurar o driver de comunicação serial
- Software RSLogix 5000 para configurar a porta serial do controlador

Para o controlador comunicar-se com uma estação de trabalho ou outro dispositivo pela rede serial, é necessário seguir estas etapas.

1. Configurar o driver de comunicação serial da estação de trabalho.
2. Configurar a porta serial do controlador.

Tabela 18 – Modos de comunicação serial

Use este modo:	Para
Ponto a ponto DF1	Comunicação entre o controlador e outro dispositivo compatível com o protocolo DF1. Este é o modo padrão do sistema. Este modo é usado normalmente para programar o controlador pela porta serial.
DF1 mestre	Controle de polling e transmissão de mensagens entre os nós mestres e escravos. A rede mestra/escrava inclui um controlador configurado como o nó mestre e até 254 nós escravos. Relacione os nós escravos usando modems ou linhas de comando. Uma rede mestre/escravo pode ter números de nós de 0 a 254. Cada um deve ter um endereço exclusivo. Da mesma forma, pelo menos dois nós precisam existir para definir o link como uma rede (1 estação mestra e uma escrava são dois nós).
DF1 escravo	Um controlador que opere como uma estação escrava em uma rede de comunicação serial mestra/escrava. Quando houver várias estações mestras na rede, faça o link das estações escravas usando modems ou linhas de comando na mestra. Com uma única estação escrava, não é necessário um modem para conectar a estação escrava à mestra. É possível configurar os parâmetros de controle como sem reconhecimento. Você pode conectar de 2 a 255 nós em um único link. No modo escravo DF1, um controlador utiliza o protocolo de transmissão half-duplex DF1. Um nó é designado como o mestre e controla quem tem acesso ao link. Todos os outros nós são estações escravas e precisam de permissão da mestra antes da transmissão.
DH-485	Comunicação com outros dispositivos DH-485 múltiplos mestres, rede de passagem de token permitindo a programação e a transmissão de mensagens peer-to-peer.

Recursos adicionais

Recursos	Descrição
Manual do usuário dos módulos EtherNet/IP em sistemas de controle Logix5000, publicação ENET-UM001	Contém informações detalhadas sobre a configuração e o uso de módulos de comunicação EtherNet/IP em um sistema de controle Logix5000
Manual do usuário dos módulos ControlNet em sistemas de controle Logix5000, publicação CNET-UM001	Contém informações detalhadas sobre a configuração e o uso de módulos de comunicação ControlNet em um sistema de controle Logix5000
Manual do usuário dos módulos DeviceNet nos sistemas de controle Logix5000, publicação DNET-UM004	Contém informações detalhadas sobre a configuração e o uso do 1756-DNB em um sistema de controle Logix5000

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

Tópico	Página
Adição dos módulos de E/S CIP Safety	69
Configurar módulos de E/S CIP Safety por meio do software RSLogix 5000	70
Definição dos parâmetros do número da rede de segurança (SNN)	71
Usando conexões Unicast em redes EtherNet/IP	71
Definição do limite de tempo de reação da conexão	71
Compreensão da assinatura de configuração	75
Reset a Propriedade do Módulo de E/S de Segurança	76
Endereçar dados à E/S de Segurança	76
Monitorar o Status do Módulo Safety I/O	77
Reiniciando um módulo para a condição “pronto para usar”	79
Substituindo um módulo usando o software RSLogix 5000	79
Substitua um módulo POINT Guard I/O usando o software RSNetWorx para DeviceNet	86

Para mais informações sobre instalação, configuração e operação dos módulos de E/S CIP Safety, consulte essas fontes:

- Manual do usuário dos módulos de segurança DeviceNet Guard I/O, publicação [1791DS-UM001](#)
- Manual do usuário dos módulos de segurança Guard I/O EtherNet/IP, publicação [1791ES-UM001](#)
- Manual do usuário e de instalação dos módulos de segurança POINT Guard I/O™, publicação [1734-UM013](#)
- Ajuda on-line do software RSLogix 5000

Adição dos módulos de E/S CIP Safety

Ao adicionar um módulo ao sistema, é necessário definir uma configuração específica para o módulo, incluindo:

- Endereço do nó para redes DeviceNet

Não é possível ajustar o endereço do nó de um módulo de E/S CIP Safety em redes DeviceNet por meio do software RSLogix 5000. Os endereços do nó do módulo são ajustados por meio das seccionadoras nos módulos.

- Endereços de IP para redes EtherNet/IP

Para configurar o endereço IP, é possível ajustar as chaves rotativas no módulo, usar o software DHCP, disponível na Rockwell Automation ou recuperar o endereço-padrão a partir da memória não volátil.

- Número da rede de segurança (SNN)
Consulte a página 71 para obter informações sobre a configuração do SNN.
- Assinatura de configuração
Consulte a página 75 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 71 para informações sobre configuração do limite do tempo de reação.
- Parâmetros Safety Input, Output e Test

É possível configurar os módulos de E/S CIP Safety pelo controlador GuardLogix usando o software RSLogix 5000.

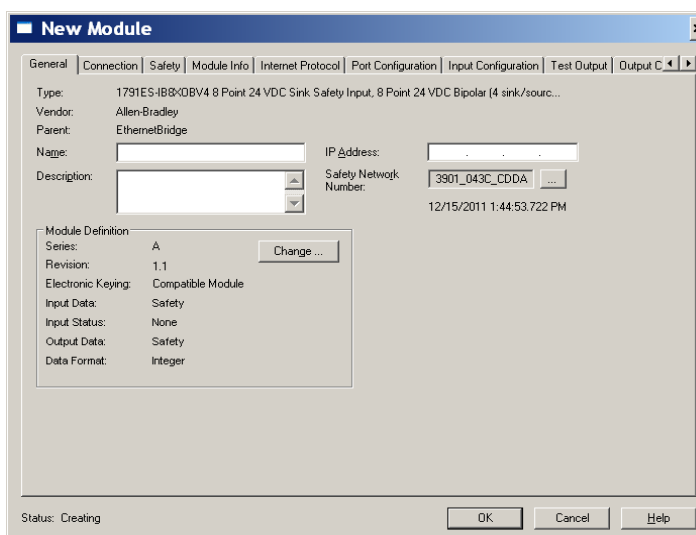
DICA Os módulos de E/S de segurança são compatíveis com os dados padrão e de segurança. A configuração do módulo define quais dados estão disponíveis.

Configurar módulos de E/S CIP Safety por meio do software RSLogix 5000


Adicionar o módulo de E/S CIP Safety ao módulo de comunicação na pasta de I/O Configuration do projeto RSLogix 5000.

DICA Não é possível adicionar ou remover um módulo de E/S CIP Safety enquanto estiver on-line.

1. Clique com o botão direito do mouse na rede apropriada e selecione New Module.
2. Expanda a categoria Safety e selecione um módulo de E/S CIP Safety.
3. Especifique as propriedades do módulo.



- a. Modifique os ajustes dos parâmetros do Module Definition, se necessário, clicando em Change.
- b. Digite o nome do novo módulo.
- c. Insira o endereço do nó ou o endereço IP dos módulos na rede de conexão.
Somente números de nó não utilizados estão inclusos no menu.

- d. Modifique o número da rede de segurança (SNN), se necessário, clicando no botão .

Consulte a página [71](#) para obter detalhes.

- e. Defina os parâmetros de configuração do módulo nas guias Input Configuration, Test Output e Output Configuration.

Consulte a ajuda on-line do RSLogix 5000 para obter mais informações sobre a configuração do módulo de E/S CIP Safety.

- f. Defina Connection Reaction Time Limit na guia Safety.

Consulte a página [71](#) para obter detalhes.

Definição dos parâmetros do número da rede de segurança (SNN)

A atribuição de um SNN baseado na hora é automática quando novos módulos Safety I/O são adicionados. As adições subsequentes do módulo 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 dos parâmetros do número da rede de segurança \(SNN\) na página 55](#).

Usando conexões Unicast em redes EtherNet/IP

No software RSLogix 5000, versão 20 ou posterior, é possível configurar os módulos de E/S EtherNet/IP para utilizar conexões unicast. 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

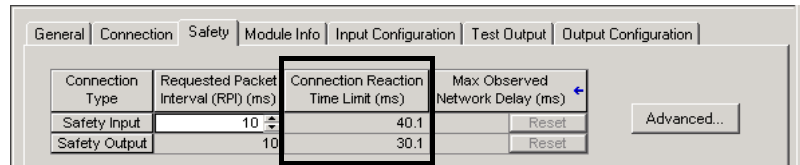
O limite de tempo de reação da conexão é a idade máxima dos pacotes de segurança na conexão associada. Se o período dos dados usado pelo dispositivo em consumo exceder o limite de tempo de reação da conexão, ocorrerá uma falha de conexão. Esse Limite é determinado pelas seguintes equações:

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

Saída do limite de tempo de reação da conexão = 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 17 – Limite do tempo de reação de conexão



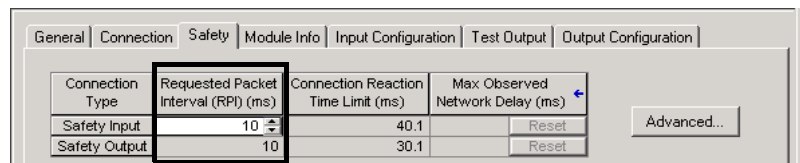
Especificar o intervalo do pacote requisitado (RPI)

O RPI especifica o período no qual ocorrerão atualizações de dados em 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 aumentos de 1 ms, com um intervalo de 1 a 100 ms. O padrão é 10 ms.

O limite de tempo de reação da conexão é ajustado assim que o RPI é alterado por meio do RSLogix 5000.

Figura 18 – Intervalo do pacote requisitado



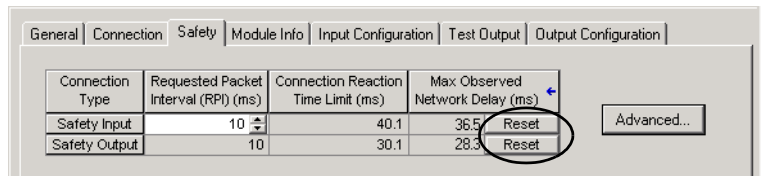
Para conexões de saída de segurança, o RPI é fixado no período da tarefa de segurança. Se o limite de reação do tempo de conexão correspondente não for satisfatório, você pode ajustar o período da tarefa de segurança na caixa de diálogo Safety Task Properties.

Consulte [Especificação do Período da Tarefa de Segurança na página 90](#) 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 73.

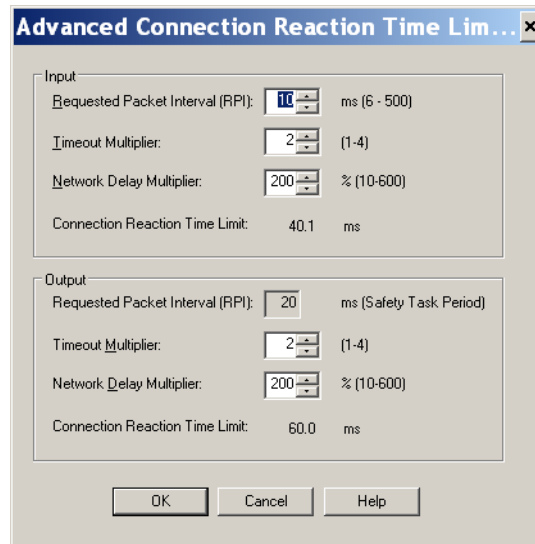
Visualização do atraso máximo observado na rede

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 estiver on-line, você pode reinicializar o atraso de rede máximo observado clicando em Reset Max.

Figura 19 – Removendo o atraso máximo de rede observado

IMPORTANTE O tempo de atraso de rede máximo real do produtor para o consumidor é menor que o valor exibido no campo de atraso de rede máximo na guia Safety. Em geral, o atraso de mensagem máximo real é de aproximadamente metade do valor de atraso de rede máximo que é exibido.

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

Figura 20 – 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: Usar a relação entre o RPI de entrada e o Período da Tarefa de Segurança. Utilize este método em todas as seguintes condições:

- 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:

$$[\text{Atraso máximo observado na rede} + \text{Margin_Factor}] \div \text{RPI}$$

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

Se:

$$\text{RPI} = 50 \text{ ms}$$

$$\text{Atraso máximo observado na rede} = 20 \text{ ms}$$

$$\text{Margin_Factor} = 10$$

Portanto, multiplicador de atraso da rede será igual a:

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

Tabela 19 – Recursos adicionais

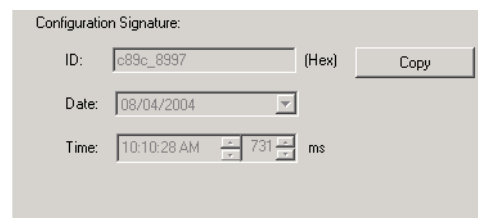
Recursos	Descrição
GuardLogix Controllers Systems Safety Reference Manual, publicação 1756-RM093	Fornece informações sobre o cálculo de tempos de reação.
Manual do usuário dos módulos de segurança Guard I/O DeviceNet, publicação 1791DS-UM001	
Manual do usuário dos módulos de segurança Guard I/O EtherNet/IP, 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 do software RSLogix 5000

Quando o módulo de E/S é configurado por meio do software RSLogix 5000, a assinatura de configuração é gerada automaticamente. É possível visualizá-la e copiá-la na guia Safety da caixa de diálogo Module Properties.

Figura 21 – Visualize e copie a assinatura de configuração

Leitura de controle de configuração diferente (conexão em modo de escuta)

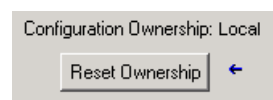
Quando a configuração do módulo de E/S é controlada por outro controlador, é necessário copiar a assinatura de configuração do módulo de seu projeto de leitura de controle e colá-la na guia Safety da caixa de diálogo Module Properties.

DICA Se o módulo é configurado para entradas apenas, é possível copiar e colar a assinatura de configuração. Se o módulo 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 Módulo de E/S de Segurança

Quando o software RSLogix 5000 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.

Quando estiver on-line, você pode reinicializar o módulo na configuração padrão clicando no botão Reset Ownership.



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 E/S de Segurança

Quando você adiciona um módulo à pasta I/O configuration, o software RSLogix 5000 cria automaticamente tags do controlador para o módulo.

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 módulo de E/S. O nome de um tag é baseado no nome do módulo no sistema.

Um endereço de dispositivo de E/S CIP Safety segue o seguinte formato:

Modulename:Type.Member

Tabela 20 – Formato de endereço do módulo de E/S CIP Safety

Em que	É	
Modulename	O nome do módulo de E/S CIP Safety	
Tipo	Tipo de dados	
	Entrada I	
	Saída: O	
Membro	Dados específicos do módulo 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:I.Output Members
	Combinação de E/S:	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members Modulename:O.Output Members

Tabela 21 – Recursos adicionais

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 módulos de E/S padrão

Monitorar o Status do Módulo Safety I/O

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

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

- Manual do usuário dos módulos de segurança Guard I/O DeviceNet, publicação [1791DS-UM001](#)
- Manual do usuário dos módulos Guard I/O EtherNet/IP, publicação [1791ES-UM001](#)
- Manual do usuário e de instalação dos módulos de segurança POINT Guard I/O, publicação [1734-UM013](#)

Tabela 22 – Operação do indicador de status

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, Piscando	Dispositivo inativo.		
	Vermelho, Piscando	Existência de uma falha recuperável.	Existe uma falha recuperável ou a atualização de um firmware está em andamento.	
	Vermelho, Ativado	Existência de uma falha irrecoverável.		
	Vermelho/Verde, Piscando	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 on-line ou sem energia.		
	Verde, Ativado	Dispositivo on-line; conexões estabelecidas.		
	Verde, Piscando	Dispositivo on-line; sem conexões estabelecidas.		
	Vermelho, Piscando	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, Piscando	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, Piscando	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, Piscando	Quando a operação de canal duplo estiver selecionada, ocorrerá um erro no circuito de saída do parceiro.		
Pontos de saída de teste (Tx)	Desligado		A saída está desenergizada.	Não aplicável.
	Amarelo, Ativado	Não aplicável.	A saída está energizada.	
	Vermelho, Ativado		Erro no circuito de saída.	
LOCK	Amarelo, Ativado	Configuração do dispositivo protegida.		
	Amarelo, Piscando	Configuração do dispositivo válida, mas dispositivo desprotegido.		
	Amarelo, Desativado	Inválido, sem dados de configuração ou o dispositivo foi configurado pelo RSLogix 5000.		
IN PWR	Verde, Desativado	Sem alimentação de entrada.		
	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	Sem energia.		
	Verde, Ativado	Não aplicável.	A tensão de alimentação está dentro da especificação.	
	Amarelo, Ativado		A tensão de alimentação está fora da especificação.	

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”.

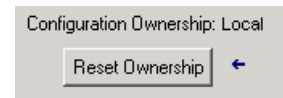
Quando o software RSLogix 5000 está on-line, a guia Safety da caixa de diálogo Module Properties exibe a propriedade da configuração atual. Quando a configuração pertence ao projeto aberto, Local é exibido. Quando a configuração pertence a um segundo dispositivo, Remote é exibido, com o número da rede 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.



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.

Substituindo um módulo usando o software RSLogix 5000

Pode-se usar o software RSLogix 5000 para substituir um módulo Guard I/O em uma rede Ethernet. Para substituir um módulo Guard I/O em uma rede DeviceNet, a sua escolha de software depende do tipo de módulo.

Tabela 23 – Software

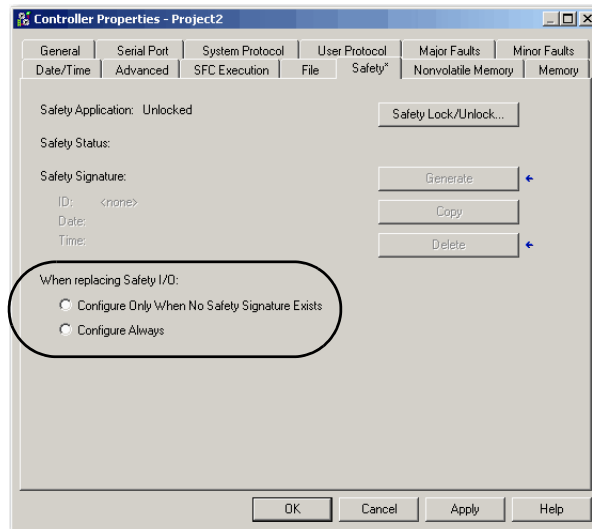
Se você está usando um	Use	Consulte
Módulo 1791DS Guard I/O com adaptador 1756-DNB	Software RSLogix 5000	abaixo
Módulo 1734 POINT Guard I/O com um adaptador 1734-PDN	Software RSNetWorx para DeviceNet	Substitua um módulo POINT Guard I/O usando o software RSNetWorx para DeviceNet na página 86

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 módulo, a função Configure Always não pode ser usada. Vá para [Substituição com “Configure only when no safety signature exists” habilitado na página 80.](#)

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 84](#).

A substituição de módulo é configurada na guia Safety do controlador GuardLogix.

Figura 22 – Substituição de módulo Safety I/O



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

Quando um módulo é substituído, se fará download da configuração do controlador de segurança se o DeviceID do novo módulo combinar com o original. 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.

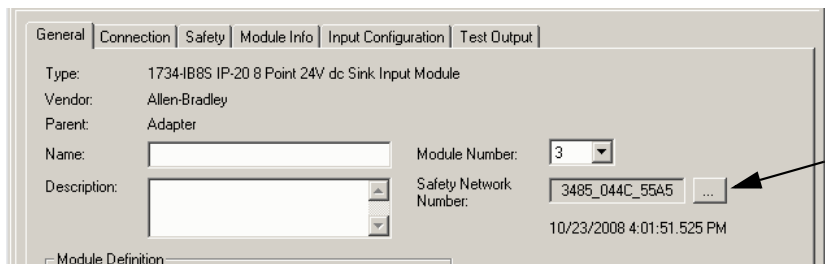
Se o projeto for configurado como “Configure only when no safety signature exists”, siga as etapas adequadas em [Tabela 24](#) para substituir um módulo POINT Guard I/O baseado na sua situação. Uma vez que você completou as etapas corretamente, o DeviceID irá combinar com o original, habilitando o controlador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

Tabela 24 – Substituindo um módulo

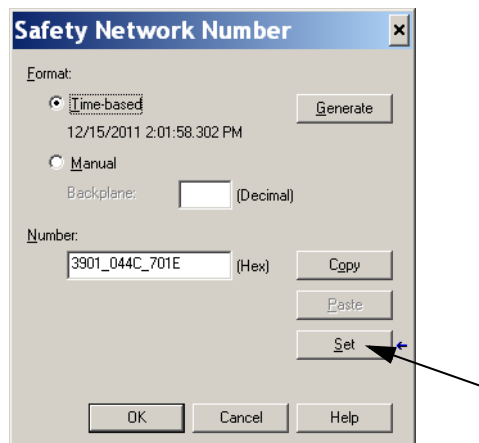
Quando existir a assinatura de segurança GuardLogix	Condição de substituição de módulo	Ação necessária
Negativo	Sem SNN (pronto para usar)	Nenhuma. O módulo está pronto para o uso.
Sim ou Não	O mesmo SNN conforme a configuração de tarefa de segurança original	Nenhuma. O módulo está pronto para o uso.
Sim	Sem SNN (pronto para usar)	Consulte Situação 1 – O módulo de substituição está fora da caixa e a assinatura de segurança existe na página 81.
Sim	SNN diferente da configuração de tarefa de segurança original	Consulte Situação 2 – O módulo de substituição SNN é diferente do original e a assinatura de segurança existe na página 82.
Negativo	SNN diferente da configuração de tarefa de segurança original	Consulte Situação 3 – O módulo de substituição SNN é diferente do original e a assinatura de segurança não existe na página 84.

Situação 1 – O módulo de substituição está fora da caixa e a assinatura de segurança existe

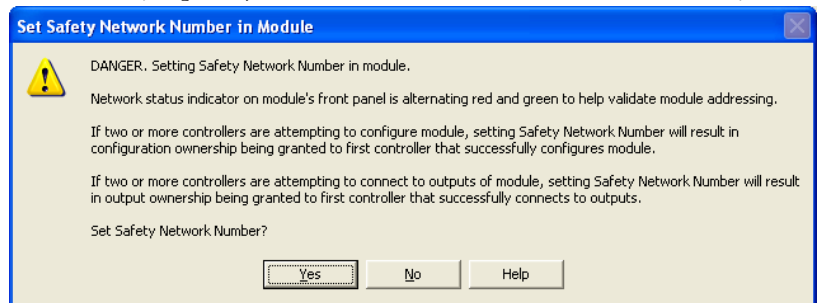
1. Remoção do módulo de E/S antigo e instalação de um novo módulo.
2. Com o botão direito, clique no módulo POINT Guard I/O e escolha Properties.
3. Clique em **...** à direita do número da rede de segurança para abrir a caixa de diálogo Safety Network Number.



4. Clique em Set.



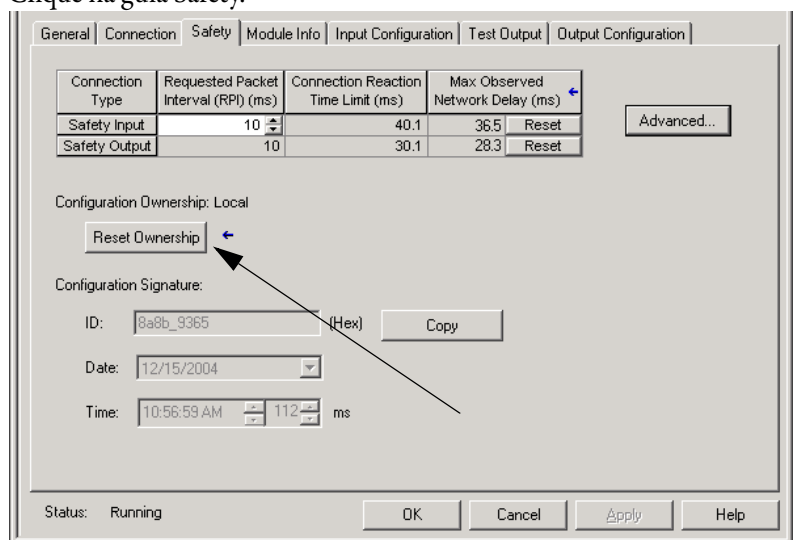
- Verifique que o indicador de status de rede (NS) esteja alternando vermelho/verde no módulo correto antes de clicar Yes na caixa de diálogo de confirmação para ajustar o SNN e aceitar o módulo de substituição.



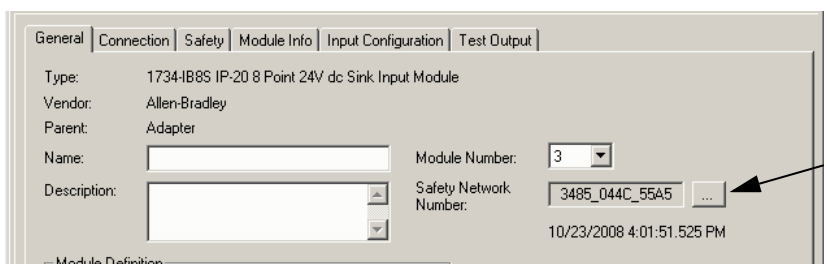
- Siga os procedimentos descritos pela empresa para testar a funcionalidade do módulo e sistema de E/S substituído e autorizar o sistema para uso.

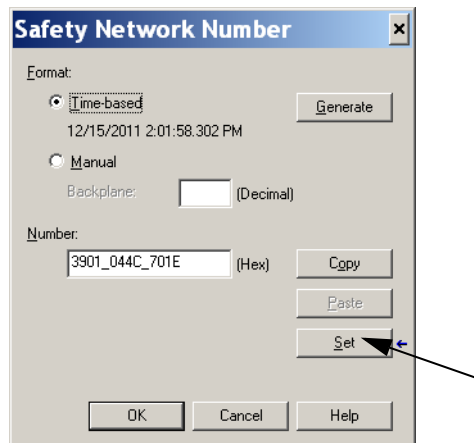
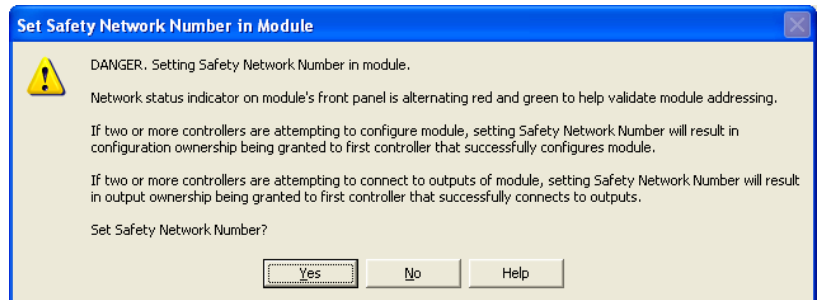
Situação 2 – O módulo de substituição SNN é diferente do original e a assinatura de segurança existe

- Remoção do módulo de E/S antigo e instalação de um novo módulo.
- Com o botão direito, clique no módulo POINT Guard I/O e escolha Properties.
- Clique na guia Safety.



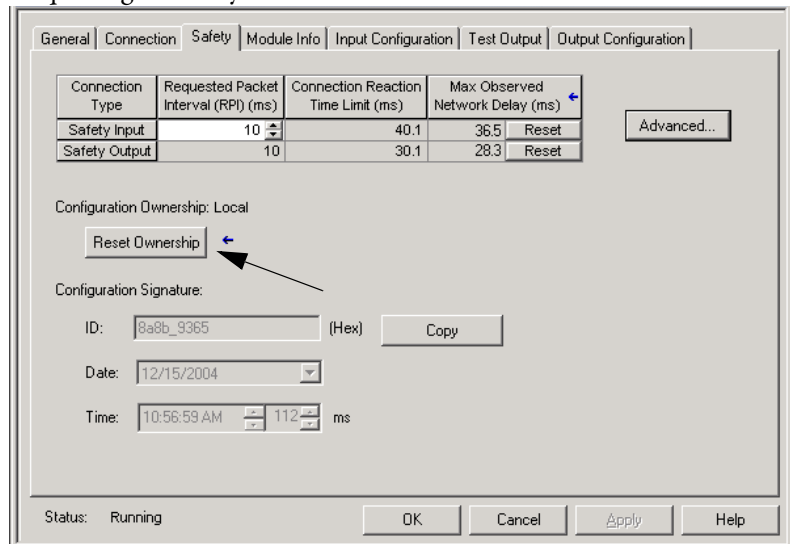
- Clique em Reset Ownership.
- Clique em OK.
- Com o botão direito, clique no controlador e escolha Properties.
- Clique em ... à direita do número da rede de segurança para abrir a caixa de diálogo Safety Network Number.



8. Clique em Set.**9.** Certifique-se de 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 módulo de substituição.**10.** Siga os procedimentos descritos pela empresa para testar a funcionalidade do módulo e sistema de E/S substituído e autorizar o sistema para uso.

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

1. Remoção do módulo de E/S antigo e instalação de um novo módulo.
2. Com o botão direito, clique no módulo POINT Guard I/O 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 módulo e sistema de E/S substituído e autorizar o sistema para uso.

Substituição com “Configure Always” habilitado



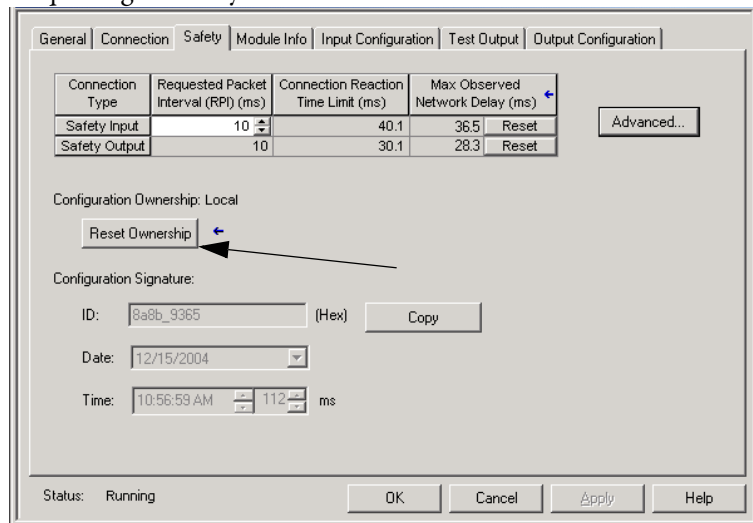
ATENÇÃO: Habilite a função “Configure Always” apenas se todo o sistema de controle de segurança CIP **não** estiver sendo responsável por manter o comportamento SIL 3 durante a substituição e teste funcional de um módulo. Não coloque módulos que estiverem na condição fora da caixa em uma rede CIP Safety quando a função Configure Always estiver habilitada, exceto ao seguir o procedimento de substituição do módulo.

Quando o recurso ‘Configure Always’ está habilitado no software RSLogix 5000, o controlador verifica automaticamente se há e se conecta a um módulo de substituição que atenda a todas as seguintes especificações:

- O controlador tem dados de configuração de um módulo compatível no respectivo endereço de rede.
- O módulo está na condição fora da caixa ou tem um SNN que combina com a configuração.

Se o projeto for configurado para “Configure Always”, siga as etapas apropriadas para substituir um módulo POINT Guard I/O.

1. Remoção do módulo de E/S antigo e instalação de um novo módulo.
 - a. Se o módulo não estiver na condição fora da caixa, vá para a etapa 6. Nenhuma ação é necessária para que o controlador GuardLogix tome a propriedade do módulo.
 - b. Se um erro de combinação SNN ocorrer, vá para a próxima etapa para reiniciar o módulo para a condição fora da caixa.
2. Com o botão direito, clique no módulo POINT Guard I/O e escolha Properties.
3. Clique na guia Safety.



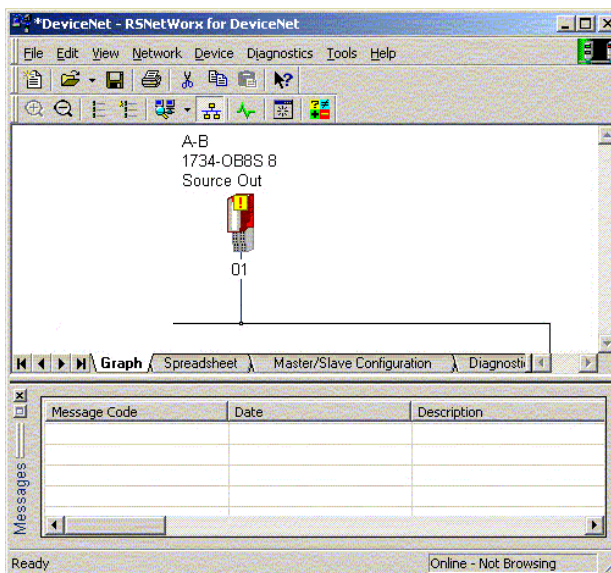
4. Clique em Reset Ownership.
5. Clique em OK.
6. Siga os procedimentos descritos pela empresa para testar a funcionalidade do módulo e sistema de E/S substituído e autorizar o sistema para uso.

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

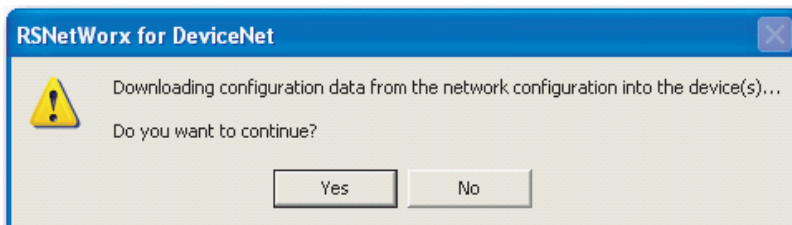
Siga estas etapas para substituir um módulo POINT Guard I/O quando o módulo e o controlador estiverem em uma rede DeviceNet.

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

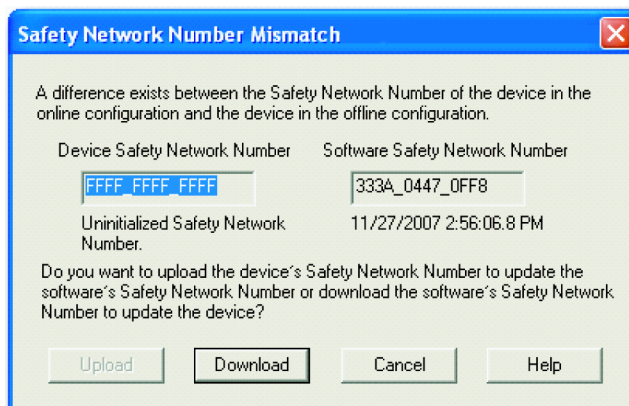
Se o módulo de substituição estiver na condição “pronto para usar” ou tiver um SNN que não combina com o módulo original, o módulo aparece com um ponto de exclamação.



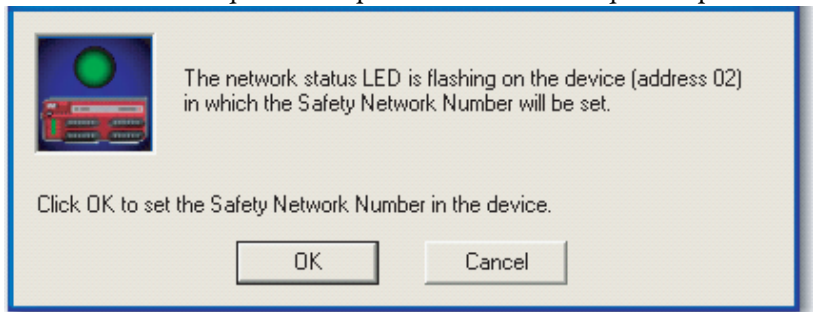
3. Com o botão direito, clique no módulo e escolha Download to Device.



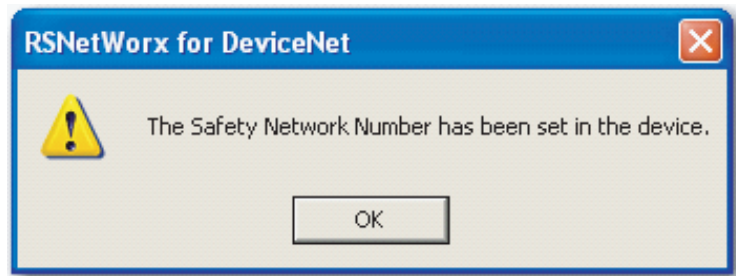
4. Clique em Yes para confirmar.
5. Clique em Download na caixa de diálogo Safety Network Number Mismatch para definir o SNN no módulo de substituição.



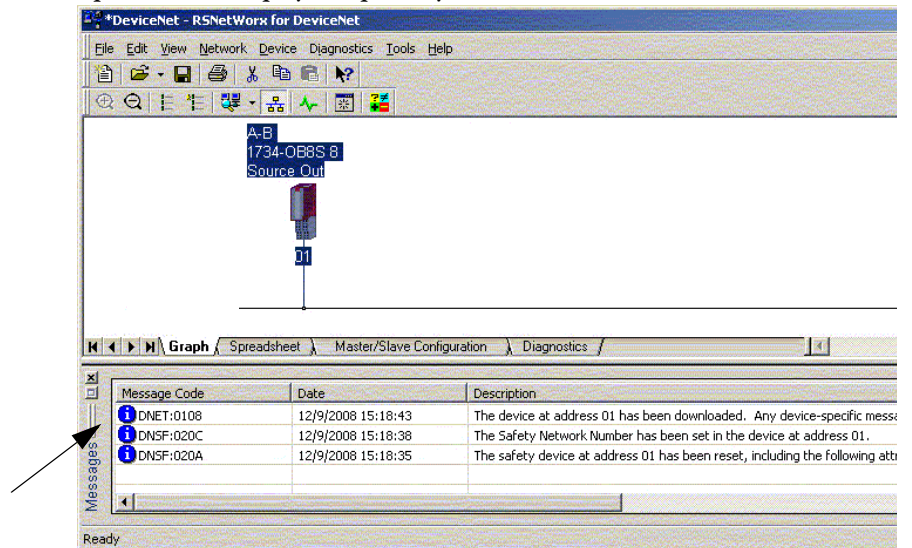
6. Certifique-se de que o indicador de status de rede (NS) está piscando no módulo correto e clique em OK para definir o SNN naquele dispositivo.



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



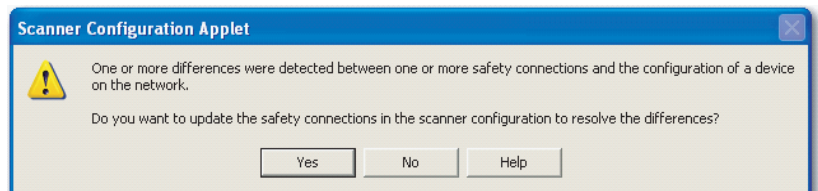
Uma vez que o download for completado com sucesso, a visualização do projeto principal exibe esta mensagem: “The device at address xx has been downloaded. Any device-specific messages related to the download operation are displayed separately.”



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.

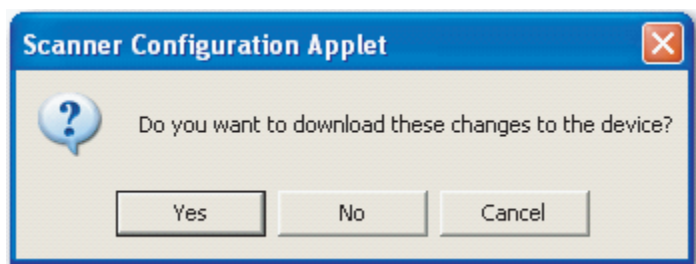
Se fez-se download desta configuração em um ajuste temporário, coloque o módulo na rede e ele se conectará automaticamente ao controlador.

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 SmartGuard.

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	90
Programas de Segurança	92
Rotinas de Segurança	92
Tags de Segurança	92
Tags de segurança produzidos/consumidos	97
Mapeamento de tags de segurança	102
Proteção em aplicações de segurança	104
Restrições do software	108

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 requisitos sobre o desenvolvimento e comissionamento de aplicações de segurança SIL 3 e PLe, consulte GuardLogix Controller Systems Safety Reference Manual, publicação [1756-RM093](#).

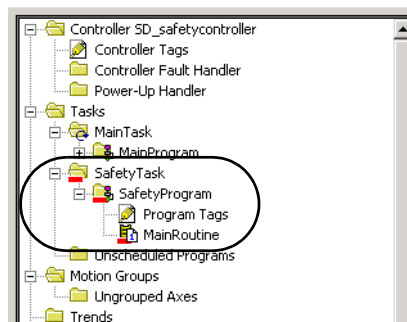
Esse manual de referência de segurança abrange o seguinte:

- 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, o software RSLogix 5000 cria automaticamente uma tarefa de segurança com um programa de segurança e uma rotina principal (de segurança).

Figura 23 – Tarefa de segurança no organizador do controlador



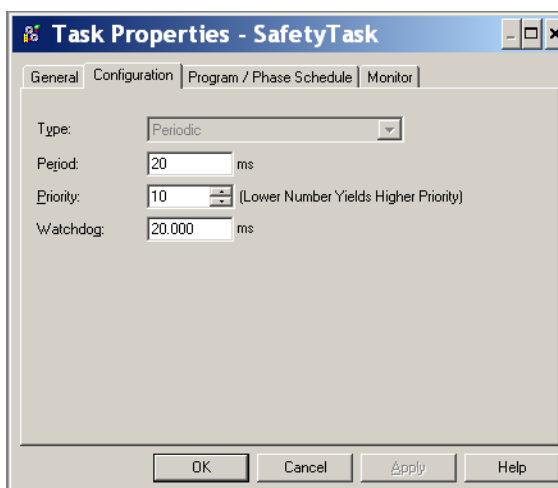
Na tarefa de segurança, você pode usar vários programas de segurança, compostos por várias rotinas de segurança. O controlador GuardLogix suporta uma tarefa de segurança. A tarefa de segurança não pode ser removida.

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 clicando com o botão direito do mouse em Safety Task e escolhendo Properties.

Figura 24 – Configuração do período da tarefa de segurança



A tarefa de segurança deve ter 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 irrecuperável no controlador de segurança.

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

O GuardLogix Controller Systems Safety Reference Manual, publicação [1756-RM093](#), 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 [102](#) 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

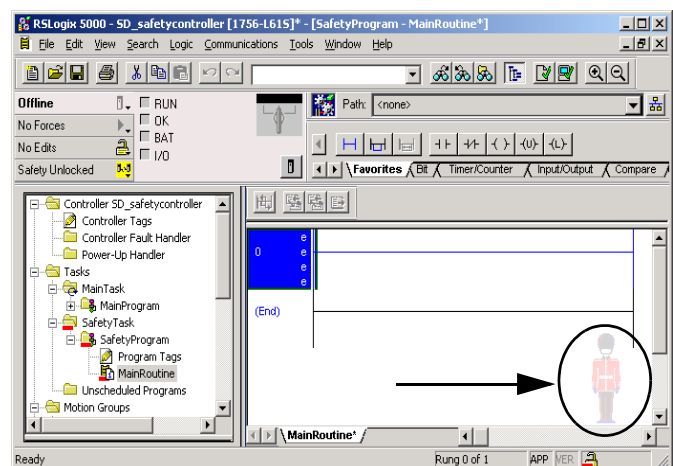
Os programas de segurança apresentam todos os atributos de programas padrão, porém eles só podem ser programados na tarefa de segurança e podem conter somente componentes de segurança. Os programas de segurança podem conter apenas rotinas de segurança, uma delas deve ser designada como a rotina principal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

Eles não podem conter rotinas padrão ou tags de segurança.

Rotinas de Segurança

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

DICA O software RSLogix 5000 utiliza uma função de marca d'água para diferenciar 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 do tag deve ser uma constante.

Para criar um 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 25 – Criando um novo tag

Tipo de tag

A [Tabela 25](#) define os quatro tipos de tags: de base, sinônimo, produzido e consumido.

Tabela 25 – Quatro tipos de tags

Tipo de tag	Descrição
Base	Estes tags armazenam valores para uso pela lógica dentro do projeto.
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: o sinônimo entre tags padrão e de segurança é proibido 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 102 .
Produzidos	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 no RPI do tag em consumo.
Consumidos	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) do tag consumido 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.

Somente esses tipos de dados são permitidos para os 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

Tipos de dados REAIS são válidos em projetos do controlador 1756-L7xS, mas não são válidos em projetos do controlador 1756-L6xS ou 1768-L4xS.

IMPORTANTE

Esta restrição abrange tipos de dados definidos pelo usuário que contêm tipos de dados predefinidos.

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/IHM
- Em mapeamento de tags de segurança
Consulte [Mapeamento de tags de segurança na página 102](#) para mais informações.

É possível fazer a leitura de tags de segurança com escopo no controlador, porém eles não podem ser gravados 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.

Os 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 127	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 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.

O software RSLogix 5000 pode modificar os tags padrão constantes e os tags de segurança forneceram uma assinatura de tarefa de segurança que não está 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 pelo software RSLogix 5000 não é afetado por essa configuração. 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 escritos de fora do controlador.
Leitura/escrita	Os tags padrão podem ser navegados, lidos ou escritos 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 produzidos/consumidos

Para transferir dados de segurança entre controladores GuardLogix, você utiliza tags de segurança produzidos e consumidos. Os tags produzidos e consumidos precisam de conexões. O tipo de conexão padrão para tags produzidos e consumidos é unicast na versão 19 e posterior do software RSLogix 5000.

Tabela 29 – Conexões produzidas e consumidas

Tag	Descrição da conexão
Produzidos	Um controlador GuardLogix pode produzir (enviar) tags de segurança a outros controladores GuardLogix 1756 ou 1768. O controlador produtor utiliza um única conexão para cada consumidor.
Consumidos	Os controladores GuardLogix 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

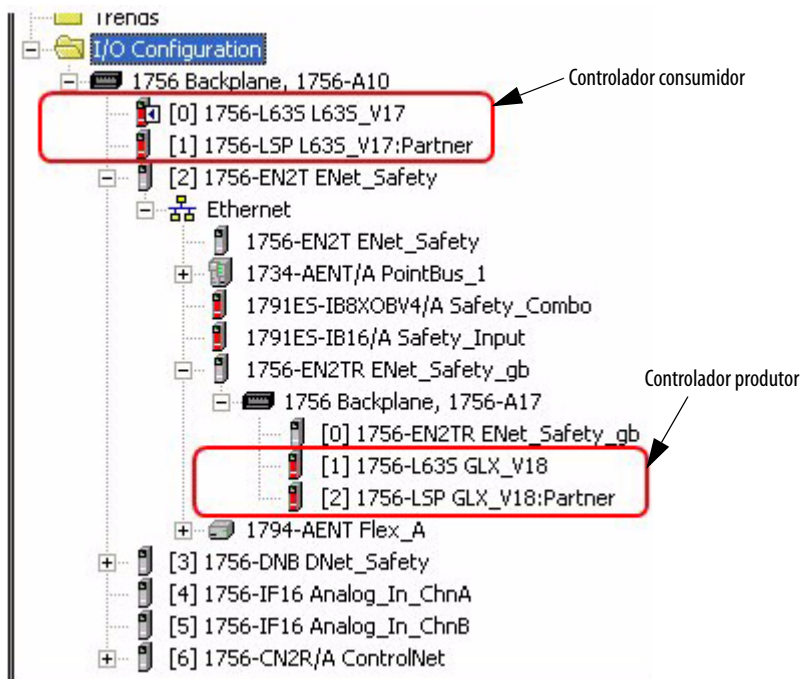
O controlador de segurança peer está sujeito às mesmas especificações de configuração que o controlador de segurança local. O controlador de segurança peer precisa ter também um número da rede de segurança (SNN). Esse SNN dependerá de sua colocação no sistema.

Tabela 30 – Posicionamento do SNN e do controlador

Localização do controlador de segurança peer	SNN
Colocado no rack local	Os controladores GuardLogix localizados em um rack comum devem ter um mesmo SNN.
Colocado em outro rack	O controlador precisa ter um SNN exclusivo.

Siga estas etapas para copiar e colar o SNN.

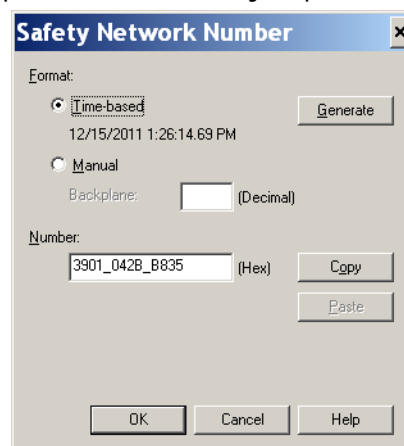
1. Adicione o controlador produtor à árvore de E/S do controlador consumidor.



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

DICA

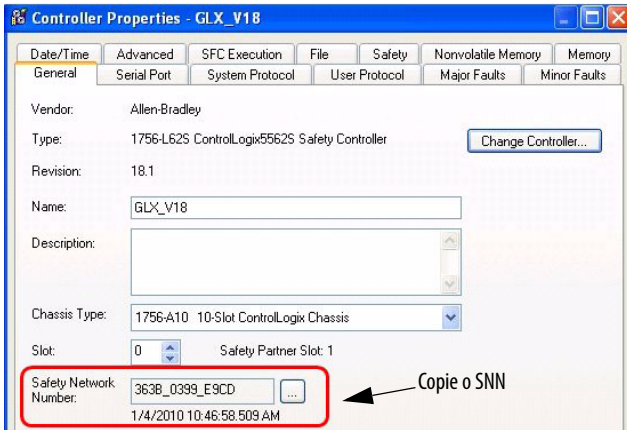
Um SNN pode ser copiado e colado por meio dos botões localizados na caixa diálogo Safety Network Number. Abra as respectivas caixas de diálogos Safety Network Number clicando [...] à direita dos campos SNN nas caixas de diálogo Properties.



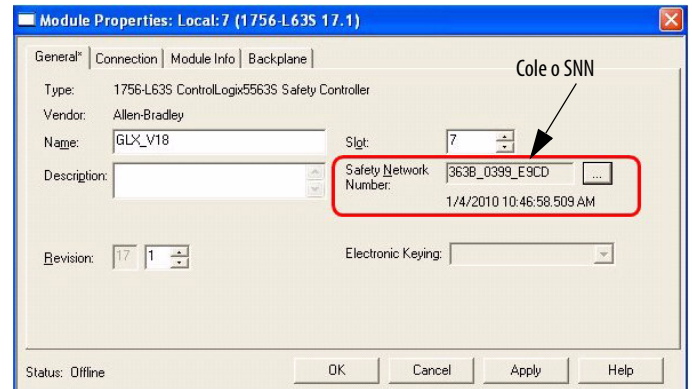
4. No projeto do controlador consumidor, clique com o botão direito do mouse no controlador produtor e escolha Module Properties.

5. Cole o SNN do controlador produtor no campo SNN.

Caixa de diálogo Controller Properties do produtor no projeto produtor



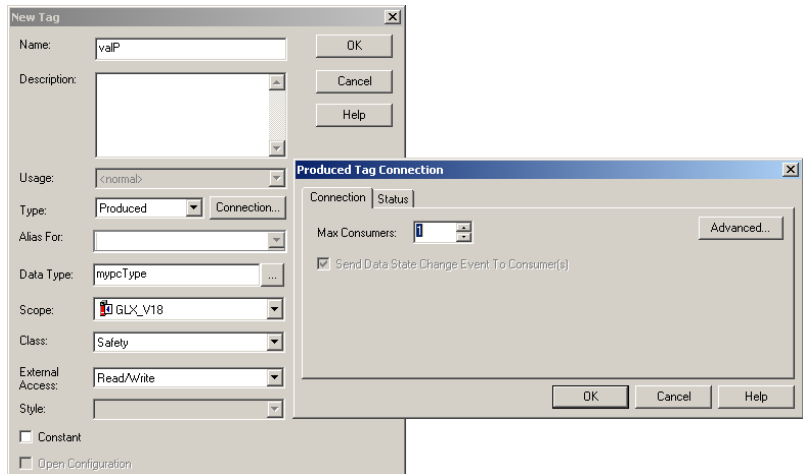
Caixa de diálogo Module Properties no projeto do consumidor



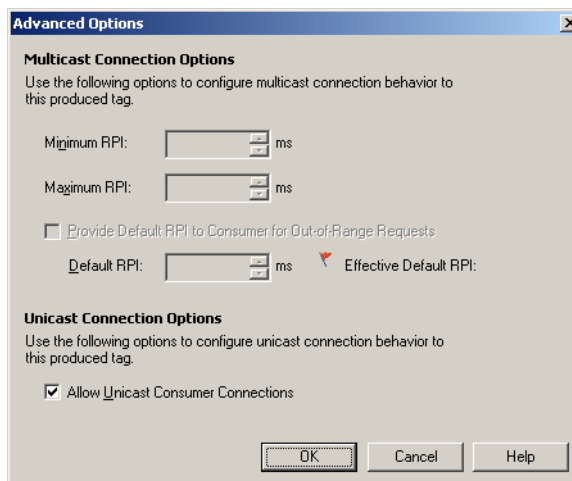
Produzir um tag de segurança

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.

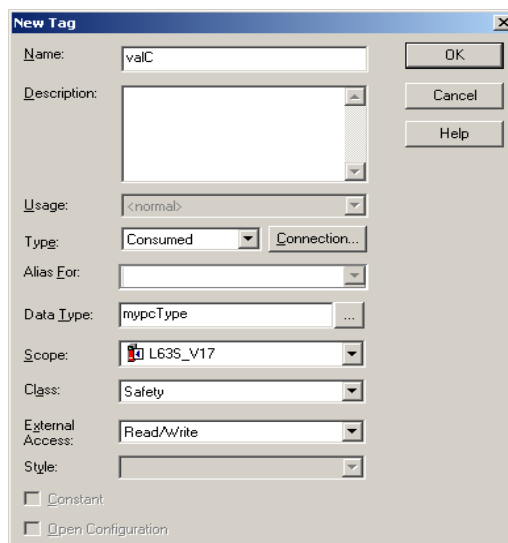
Consumir dados de tags de segurança

Siga estas etapas para consumir dados produzidos por outro controlador.

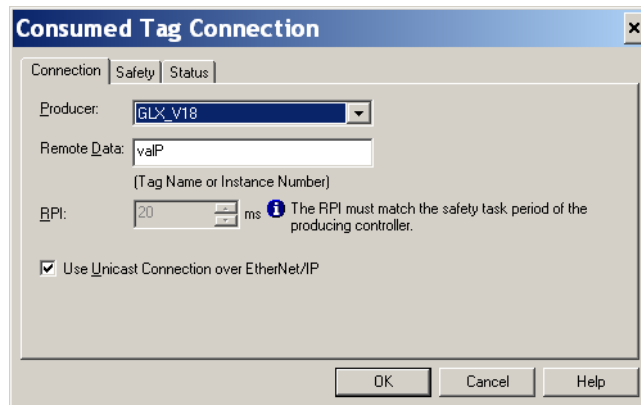
1. No projeto do controlador consumidor, crie um tipo de dado definido pelo usuário idêntico ao criado no projeto do produtor.

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

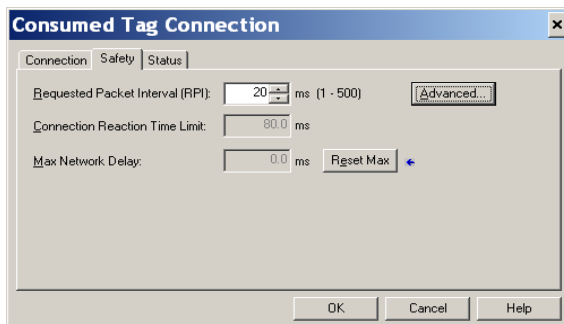
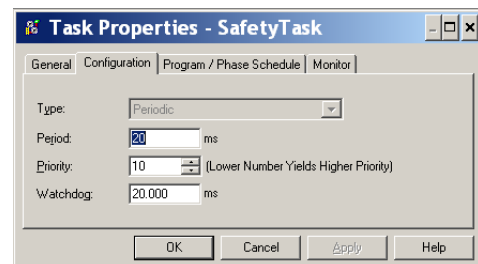
2. Com o botão direito, clique em Controller Tags e escolha New Tag.
3. Defina o tipo como Consumed, a classe como Safety e o tipo de dados como o tipo definido pelo usuário que foi criado na etapa 1.



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



5. Selecione o controlador que produz os dados.
6. Digite o nome do tag produzido.
7. Clique na guia Safety.
8. Insira o intervalo do pacote requisitado (RPI) para a conexão em incrementos de 1 ms.
O padrão é 20 ms.

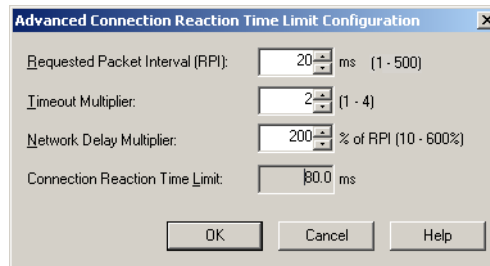
Projeto Consumidor**Projeto Produtor**

O RPI especifica o período no qual ocorrerão atualizações de dados em 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 estiver on-line, você pode reinicializar o atraso máximo de rede clicando em Reset Max.

- 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 – Recursos adicionais

Recursos	Descrição
Páginas 71 a 75	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
Manual de programação de tags consumidos e produzidos por controladores Logix5000, 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 irrecoverável.
 - existir uma parceria inválida entre o controlador principal e o parceiro de segurança.

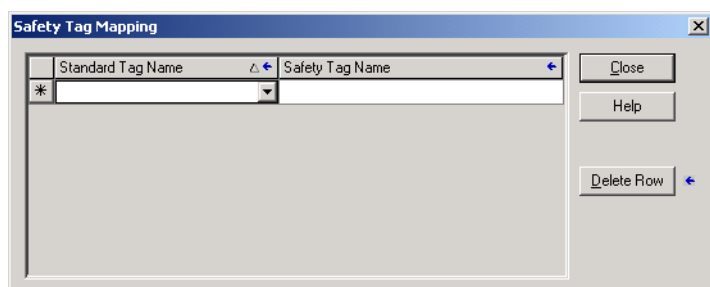


ATENÇÃO: Ao usar dados-padrão em uma rotina de segurança, você é responsável por fornecer um meio confiável de garantir que os dados sejam usados de modo apropriado. O uso de dados padrão em um tag de segurança não os torna dados de segurança. Não é possível controlar diretamente uma saída de segurança SIL 3/PLc com dados de tag padrão.

Consulte o Manual de referência dos sistemas de controladores GuardLogix, publicação [1756-RM093](#), para mais informações.

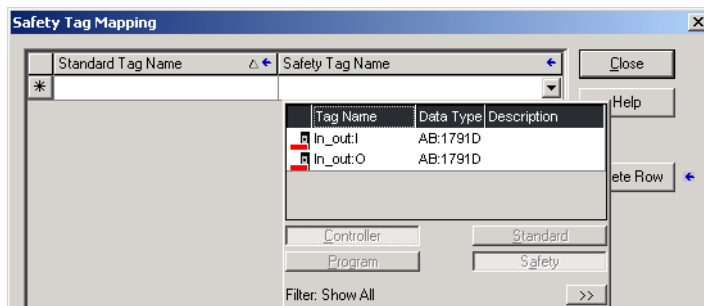
Criar pares para mapeamento de tags

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



- 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.



- 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.
- 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 [103](#).

Proteção em 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 segurança de E/S
- mudança do estado de inibição da E/S de segurança ou as conexões produzidas
- manipulação de dados de segurança (exceto pela lógica de rotina de segurança)
- criação ou remoção da assinatura de tarefa de segurança

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

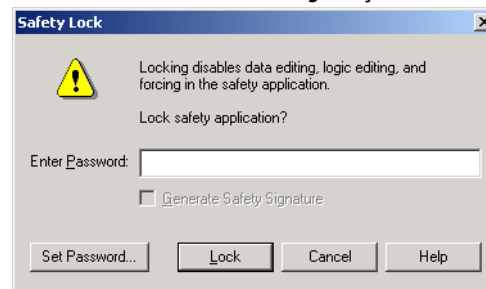
Os status bloqueado por segurança e desbloqueado por segurança não podem ser alterados quando a chave seletora está na posição RUN.

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 26 – 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 [49](#).

O recurso de bloqueio de segurança, descrito nesta seção, e as medidas de segurança RSLogix padrão são aplicáveis às aplicações do controlador GuardLogix.

Consulte o Logix5000 Controllers Security Programming Manual, publicação [1756-PM016](#), para informações sobre os recursos de segurança RSLogix 5000.

Criação de uma assinatura de tarefa de segurança

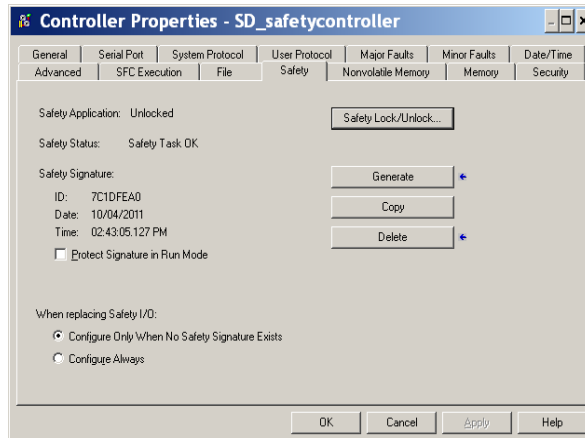
Antes de executar o teste de verificação, é necessário gerar a assinatura de tarefa de segurança. Você pode criá-la somente quando o controlador GuardLogix on-line, no modo programa, desprotegido e sem imposições de segurança, edições de segurança on-line pendentes ou falhas de segurança. O status de 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 [126](#)) ou na guia Safety da caixa de diálogo Controller Properties, conforme exibido na página [107](#).

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

Figura 27 – 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 GuardLogix Controller Systems Safety Reference Manual, publicação [1756-RM093](#), para mais informações sobre as especificações SIL 3/PL.

Restrições do software

As restrições que limitam a disponibilidade de alguns itens e funções de menus (ou seja, cortar, colar, remover, pesquisar e substituir) são impostas pelo software de programação 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 do controlador, descrição, tipo de rack, número de slot e de rede de segurança.
- 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	109
Compreensão dos fatores que afetam a entrada em comunicação	111
Download	113
Upload	115
Entrar em Comunicação	116

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
Serial	Cabo 1756-CP3 ou 1747-CP3	Conecte-se à porta serial do controlador 1756-16xS na página 37
USB	Cabo USB 2.0	Conecte-se à porta USB do controlador 1756-17xS na página 35
EtherNet/IP	Módulo EtherNet/IP em um slot aberto no mesmo rack do controlador	Conecte seu dispositivo e o computador EtherNet/IP na página 110
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 110
ControlNet	Módulo 1756-CN2 em um slot aberto no mesmo rack do controlador	

Conecte seu dispositivo e o computador EtherNet/IP

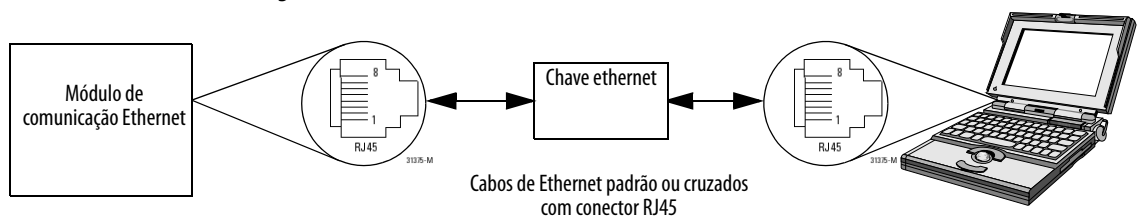


ADVERTÊNCIA: Se o cabo de comunicação for conectado ou desconectado com a aplicação aplicada a este módulo ou a qualquer dispositivo na rede, um arco elétrico pode ocorrer. Isto pode causar uma explosão em instalações reconhecidas como área classificada.

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 28 – 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 EtherNet/IP em sistemas de controle 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, publicação [DNET-UM004](#)

Compreensão dos fatores que afetam a entrada em comunicação

O software RSLogix 5000 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 descarregar primeiro o projeto no controlador. Se ocorreram mudanças ao projeto, será solicitado para que você carregue ou descarregue. 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, o software RSLogix 5000 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. O software RSLogix 5000 permite a atualização do firmware como parte da sequência de descarregamento.

IMPORTANTE Para atualizar o firmware do controlador, instale primeiro um kit de atualização do firmware. É possível localizar esse kit no CD complementar do software RSLogix 5000.

DICA É possível atualizar o firmware selecionando ControlFLASH™ no menu Tools no software RSLogix 5000.

Falhas/status de segurança

É permitido fazer upload da 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 trava 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

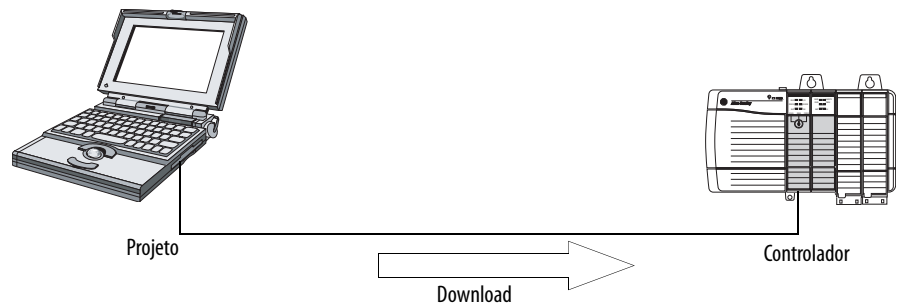
Durante o download em um controlador que está desbloqueado de segurança, caso o firmware no controlador seja diferente daquele no projeto off-line, faça um dos seguintes:


- 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 RSLogix 5000 do que deseja fazer download.
3. Defina o caminho até o controlador.
 - a. Clique em Who Active .
 - b. Selecione o controlador.
Para abrir um nível, clique no sinal +. Se já houver um controlador selecionado, verifique se é o correto.
4. Clique em Download.

O software compara as seguintes informações 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

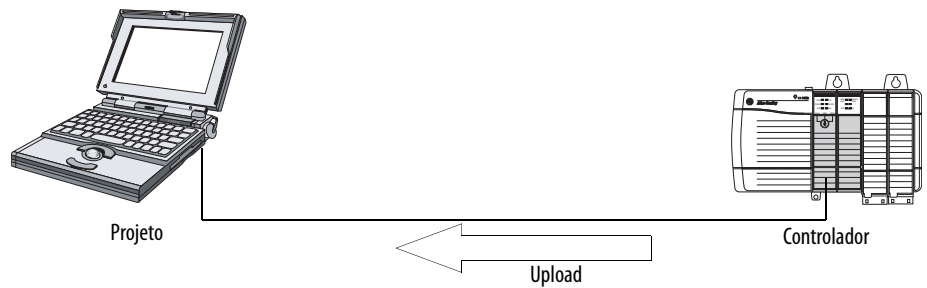
5. Siga as orientações nesta tabela para concluir o download com base na resposta do software.

Se o software indicar	Faça o seguinte:
Faça download para o controlador.	Selecione Download. Faz-se download do projeto no controlador e o software RSLogix 5000 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. Confirme a seleção clicando em Yes.
Não é possível fazer download para o controlador. O parceiro de segurança está faltando ou na disponível ontem.	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. Confirme a seleção clicando em Yes.
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.	<ul style="list-style-type: none"> 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 estiver marcada e você escolher Unlock, será necessário confirmar a remoção selecionando Yes.
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. Selecione o controlador.

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

2. Clique em Upload.

3. Se o arquivo do projeto não existir, selecione File>Select>Yes.

4. Caso contrário, selecione-o.

Se a função Project to controller match estiver habilitada, o software RSLogix 5000 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. O software verificará se o projeto aberto corresponde ao do controlador.

a. Se não forem, será necessário selecionar um arquivo correspondente ou cancelar o processo de upload.

b. Se forem, o software verificará se há alterações no projeto off-line (aberto).

6. O software verifica mudanças no projeto off-line.

a. Se não houver, será possível entrar em comunicação sem fazer upload. Clique em Go Online.

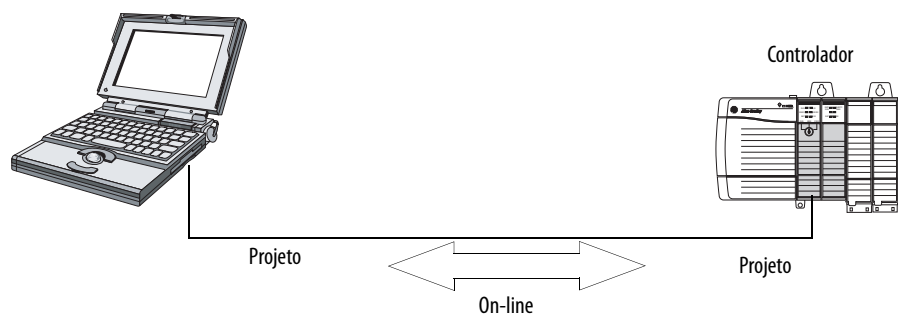
b. Se houver alterações no projeto aberto que não existam no controlador, será possível optar entre fazer upload do projeto, cancelar o upload ou selecionar um arquivo diferente.

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.

Entrar em Comunicação

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. Selecione o controlador.

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

2. Clique em Go Online.

As verificações do software são as seguintes:

- 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: <ul style="list-style-type: none"> • Escolha Update firmware. Escolha a revisão necessária e clique em Update. Confirme a seleção clicando em Yes. • IMPORTANTE: O projeto on-line é excluído. • Para mantê-lo, cancele o processo on-line e instale uma versão do software RSLogix 5000 compatível com a revisão de firmware do controlador.
É preciso fazer upload ou download para ficar on-line usando o projeto aberto.	Selecione uma das seguintes opções: <ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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 o software RSLogix 5000 estão on-line, o status de proteção 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 quiser que as alterações no projeto off-line sejam permanentes, não salve o arquivo do projeto após o processo de entrar em comunicação.

Observações:

Armazenamento e carregamento de projetos usando memória não volátil

Tópico	Página
Usando cartões de memória para memórias não voláteis	119
Armazenamento de um projeto de segurança	120
Carregamento de um projeto de segurança	121
Use módulos de armazenamento de energia (somente controladores 1756-L7xS)	122
Estime o suporte ESM do WallClockTime	124
Gestão do firmware com supervisor de firmware	124

Usando cartões de memória para memórias não voláteis

Os controladores GuardLogix, revisão 18 ou posterior, 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 pelo software RSLogix 5000

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

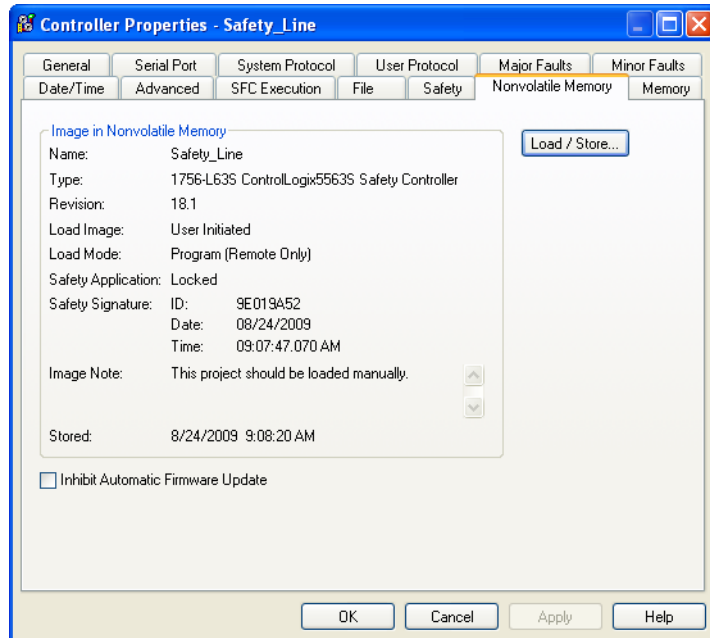
- As alterações feitas após armazenar o projeto não são refletidas na memória não volátil.
 - Se fizer alguma mudança ao projeto, mas não armazená-las, elas serão substituídas quando carregar o projeto da memória não volátil. Caso isso ocorra, é preciso fazer upload ou download do projeto para ficar 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.
-

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.



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.

Figura 29 – Guia Nonvolatile Memory



Para informações detalhadas sobre o uso de memória não volátil, consulte o the 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 nenhuma aplicação no controlador, é possível salvar somente o firmware do controlador de segurança somente se houver uma parceria válida. Uma carga de firmware somente não irá apagar a condição inoperável da tarefa de segurança.

Se 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

É possível iniciar uma carga a partir da memória não volátil somente se o seguinte for verdadeiro:

- O tipo do controlador especificado pelo projeto armazenado na memória não volátil corresponde ao tipo de controlador.
- As revisões principais e secundárias do projeto em memória não volátil correspondem às revisões principais e secundárias do controlador.
- Seu controlador não está no modo de operação.

Existem várias opções para quando (sob essas condições) carregar um projeto na memória do usuário para o controlador.

Tabela 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	<ul style="list-style-type: none"> • Quando desligar e ligar a alimentação, você perde todas as alterações on-line, o valor do tag e programa de rede não armazenados na memória não volátil. • O controlador carrega o projeto armazenado e o firmware em qualquer partida independente do firmware ou aplicação no controlador. A carga ocorre se o controlador estiver ou não com bloqueio de segurança ou tenha uma assinatura de tarefa de segurança. • Sempre é possível usar o software RSLogix 5000 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	<ul style="list-style-type: none"> • 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. A aplicação armazenada na memória não volátil também é carregada e o controlador insere o modo selecionado, seja programação ou operação. • Sempre é possível usar o software RSLogix 5000 para carregar o projeto.
Somente pelo software RSLogix 5000.	Iniciado pelo usuário	<ul style="list-style-type: none"> • 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. <p>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 definidas nos valores presentes na memória não volátil uma vez que a carga estiver completa.</p> <ul style="list-style-type: none"> • 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 o 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 (somente controladores 1756-L7xS)

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

- Fornecer energia para os controladores 1756-L7xS 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 1756-L7xS. Para mais informações, consulte [Apague o programa da memória NVS integrada](#)

A seguinte tabela descreve os ESMs.

Tabela 37 – Módulos de armazenamento de energia

Cód. cat.	Descrição
1756-ESMCAP(XT)	ESM com base em capacitor Os controladores 1756-L7xS 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 200 µJ 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-SPEMNSE(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 200 µJ 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-SPEMNSEXT instalado.
1756-SPEMNRM(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.

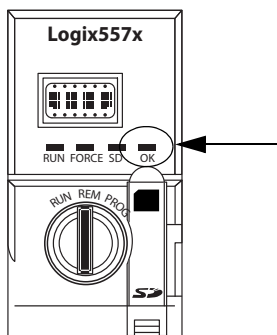
1. Remova a energização do controlador.

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 30 – 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 permitir, siga estas etapas para limpar o programa da memória NVS integrada do controlador 1756-L7xS.

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

Começando com o software RSLogix 5000, versão 18, é possível usar o recurso de supervisor de firmware para gerenciar o firmware nos 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 de firmware por meio do utilitário ControlFLASH.

O supervisor do firmware é compatível com os produtos de E/S distribuída e não modulares que se assentam diretamente na rede sem um adaptador, incluindo os módulos de E/S CIP Safety nas redes EtherNet/IP. Os módulos de E/S CIP Safety nas redes DeviceNet e os módulos POINT Guard I/O ainda não são compatíveis.

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.

O software RSLogix 5000 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 on-line	125
Monitoração de conexões	126
Status de monitoração de segurança	128
Falhas do controlador	128
Desenvolvimento de uma rotina de falha	131

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

Visualizando o status via barra on-line

A barra on-line exibe informações sobre o projeto e o controlador, inclusive o status do controlador, o status de force, o status de edição on-line e o status de segurança.

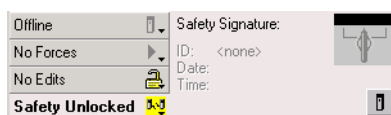
Figura 31 – Botões de status



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 32 – Tela on-line de assinatura de segurança



O botão Safety Status indica se o controlador está traveado 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. 

Monitoração de 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 módulo é produzida, que pode ser acessada através da guia Connections da caixa de diálogo Module Properties para o módulo ou pela instrução GSV.



ATENÇÃO: A E/S de segurança e as conexões produzidas/consumidas não podem ser configuradas para causar uma falha automaticamente no controlador quando uma conexão for perdida. Portanto, é preciso monitorar falhas de conexão para assegurar que o sistema de segurança mantenha a integridade SIL 3/PLe.

Consulte [Conexões de Segurança](#).

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

Monitoração dos flags de status

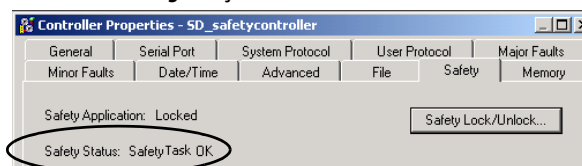
Os controladores Logix, incluindo os controladores GuardLogix, oferecem suporte a palavras-chave de status que podem ser usadas na lógica para monitorar eventos específicos.

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

Status de monitoração 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 33 – Status da tarefa de segurança



Os valores possíveis para o status de segurança são:

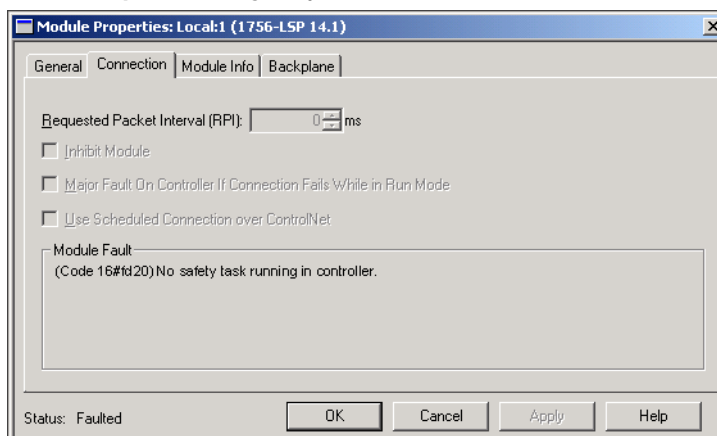
- Falta um parceiro de segurança ou ele não está disponível.
- O hardware do parceiro de segurança é incompatível com o controlador principal.
- O firmware do parceiro de segurança é incompatível com o controlador primário.
- Tarefa de segurança inoperável.
- Tarefa de segurança OK.

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

Consulte [Falhas graves de segurança \(Tipo 14\) na página 130](#) 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 34 – 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 irreversíveis do controlador

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

Falhas de segurança irreversíveis na aplicação de segurança

Se ocorrer uma falha de segurança irreversível 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 irreversível que for removida de forma programática no Program Fault Handler, a aplicação padrão continuará a ser executada.



ATENÇÃO: Cancelar a falha de segurança não a apaga! Se a falha de segurança for cancelada, será sua responsabilidade provar que este procedimento manterá a operação segura.

Será necessário fornecer a prova à sua agência de certificação que permitirá que parte do sistema continue a funcionar mantendo a operação segura.

Se houver uma assinatura de tarefa de segurança, será necessário apenas 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 ou não 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 apagada de forma programática, a tarefa de segurança pode continuar a ser executada sem interrupção.

Quando uma falha recuperável não seja 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 nos controladores 1756-L7xS também mostra códigos de falha com uma curta mensagem de status, conforme descrição no início da página [137](#).

Códigos de Falhas

A [Tabela 41](#) mostra os códigos de falha específicos para controladores GuardLogix. 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 fazer download novamente do programa para permitir a execução da tarefa de segurança novamente. Reinstale outra vez 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.

Uma falha de advertência recuperável tipo (10), código 11, ocorre quando a bateria do parceiro de segurança 1756-LSP está faltando ou precisa ser substituída.

Consulte o [Apêndice B](#) para obter informações sobre a substituição da bateria.

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 para a execução da lógica.

De acordo com a aplicação, pode ser que você não queira que todas as falhas de segurança desliguem o sistema inteiro. Nessa situação, é possível usar uma rotina de falha para apagar uma falha específica e permitir que parte do controle padrão do sistema continue a funcionar ou configurar algumas saídas para permanecerem ativas.



ATENÇÃO: Será necessário fornecer a prova à sua agência de certificação que permitirá que parte do sistema continue a funcionar mantendo a operação segura.

O controlador suporta dois níveis de manuseio de falhas graves:

- Rotina de falha do programa
- Manipulador de falhas do controlador

As duas rotinas podem utilizar instruções GSV e SSV conforme descrito na página [132](#).

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 utilizar a instrução SSV, o software exibe somente os atributos que podem ser definidos.

Para a tarefa de segurança, as instruções GSV e SSV são mais restritas. Observe que as instruções SSV em tarefas padrão e de segurança não podem energizar o bit 0 (falha grave em erro) no atributo do modo de um módulo de E/S de segurança.

Para objetos de segurança, a [Tabela 42](#) mostra para quais atributos podem-se obter valores usando a instrução GSV e quais podem ser ajustados por meio da instrução SSV em tarefas de segurança e padrão.



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

Tabela 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	Fornece o número de instâncias deste objeto de tarefa. Os valores válidos são de 0 a 31.	✓		✓	
	MaximumInterval	DINT[2]	O intervalo máximo entre execuções sucessivas desta tarefa.			✓	✓
	MaximumScanTime	DINT	Tempo de execução máximo registrado (ms) para esta tarefa.			✓	✓
	MinimumInterval	DINT[2]	O intervalo mínimo entre execuções sucessivas desta tarefa.			✓	✓
	Priority	INT	Prioridade relativa desta tarefa em comparação com outras. Os valores válidos são de 0 a 15.	✓		✓	
	Rate	DINT	Período (em ms) ou valor de tempo-limite da tarefa (em ms).	✓		✓	
	Watchdog	DINT	Limite de tempo (em ms) para execução de todos os programas associados e esta tarefa.	✓		✓	
Programa de Segurança	Instance	DINT	Fornece o número de instâncias do objeto do programa.	✓		✓	
	MajorFaultRecord ⁽¹⁾	DINT[11]	Registra falhas graves neste programa.	✓	✓	✓	
	MaximumScanTime	DINT	Tempo de execução máximo registrado (ms) neste programa.			✓	✓
Rotina de Segurança	Instance	DINT	Fornece o número de instâncias deste objeto de rotina. Os valores válidos são de 0 a 65.535.	✓			

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
Controlador de Segurança	SafetyLocked	SINT	Indica se o controlador está protegido ou não.	✓		✓	
	SafetyStatus ⁽²⁾	INT	Especifica o status de segurança conforme o seguinte: <ul style="list-style-type: none"> Tarefa de segurança OK. (1000000000000000) Tarefa de segurança inoperável. (1000000000000001) parceiro faltante. (0000000000000000) parceiro não disponível. (0000000000000001) hardware incompatível. (0000000000000010) firmware incompatível. (0000000000000011) 			✓	
	SafetySignatureExists	SINT	Indica se há ou não a assinatura de tarefa de segurança.	✓		✓	
	SafetySignatureID	DINT	Número de identificação de 32 bits.			✓	
	SafetySignature	String ⁽³⁾	Número de identificação de 32 bits.			✓	
	SafetyTaskFaultRecord ⁽¹⁾⁽²⁾	DINT[11]	Registra as falhas da Tarefa de Segurança.			✓	
AOI (Segurança)	LastEditDate	LINT	Registro de data e hora da última edição de uma definição de instrução add-on.			✓	
	SignatureID	DINT	Número de ID.			✓	
	SafetySignatureID	DINT	Número de identificação de 32 bits.			✓	

(1) Consulte [Acesso aos atributos de FaultRecord na página 133](#) para informações sobre como acessar este atributo.

(2) Consulte [Captação de informações de falha na página 134](#) 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 irrecuperáveis. Use uma instrução `GSV` no manipulador de falhas do controlador para capturar e armazenar as informações da falha. A instrução `GSV` pode ser utilizada em uma tarefa padrão juntamente com uma rotina do manipulador de falhas do controlador que remove as falhas e deixa as tarefas padrão continuarem a execução.

Indicadores de status

Tópico	Página
Indicadores de status do controlador 1756-L6xS	135
Indicadores de status dos controladores 1756-L7xS	136
Tela de status do controlador 1756-L7xS	137

Indicadores de status do controlador 1756-L6xS

O status do controlador primário e do parceiro de segurança são exibidos por indicadores de status de LED.

Tabela 44 – Descrições do indicador de status 1756-L6xS

Indicador	Status	Descrição do Controlador Primário	Descrição do Parceiro de Segurança
RUN	Desligado	Sem execução de tarefas do usuário. Controlador no modo PROGram.	N/D
	Verde	Controlador no modo RUN.	N/D
SAFE RUN	Desligado	N/D	As saídas de segurança ou de tarefa de segurança do usuário estão desabilitadas. O controlador está no modo PROGram, modo de teste ou há uma falha na tarefa de segurança.
	Verde	N/D	As saídas de segurança e de tarefa de segurança do usuário estão habilitadas. A aplicação de segurança está em execução. A assinatura da tarefa de segurança está presente.
	Verde, Piscando	N/D	As saídas de segurança e de tarefa de segurança do usuário estão habilitadas. A aplicação de segurança está em execução. A assinatura da tarefa de segurança não está presente.
FORCE	Desligado	Não há imposições, padrão ou de Segurança, habilitadas no controlador.	N/D
	Âmbar	Imposições padrão e/ou de Segurança habilitadas.	N/D
	Âmbar, Piscando	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.	N/D
BAT	Desligado	A bateria é compatível com a memória.	A bateria é compatível com a memória.
	Vermelho	A bateria não é compatível com a memória.	A bateria não é compatível com a memória.
OK	Desligado	Nenhuma energização aplicada.	Nenhuma energização aplicada.
	Verde	O controlador está operando sem falhas.	O parceiro de segurança está operando sem falhas.
	Vermelho, Piscando	Falha irreversível ou reversível não controlada no manipulador de falhas. Todas as tarefas do usuário, padrão e de Segurança foram interrompidas.	N/D
	Vermelho	Energizando ou falha irreversível no controlador.	Energizando ou falha irreversível no controlador.

Tabela 44 – Descrições do indicador de status 1756-L6xS

Indicador	Status	Descrição do Controlador Primário	Descrição do Parceiro de Segurança
E/S ⁽¹⁾	Desligado	Sem atividade. Sem E/S configurada.	N/D
	Verde	O controlador está se comunicando com todos os dispositivos de E/S configurados, padrão e de segurança.	N/D
	Verde, Piscando	Um ou mais dispositivos de E/S não respondem.	N/D
	Vermelho, Piscando	O controlador não está em comunicação com a E/S configurada.	N/D
RS232	Desligado	Não há atividade.	N/D
	Verde	Dados recebidos ou transmitidos.	N/D
TAREFA DE SEGURANÇA	Desligado	N/D	Nenhuma parceria estabelecida. Controlador Primário ausente, não funciona corretamente ou a revisão de firmware é incompatível com a do Parceiro de Segurança.
	Verde	N/D	Status do controlador de segurança é OK. O tempo de sistema (CST) está sincronizado e as conexões de E/S de segurança foram estabelecidas.
	Verde, Piscando	N/D	Status do controlador de segurança é OK. O tempo de sistema (CST) não está sincronizado no controlador primário ou no parceiro de segurança.
	Vermelho	N/D	A parceria foi perdida e uma nova não foi estabelecida. Controlador Primário ausente, não funciona corretamente ou a revisão de firmware é incompatível com a do Parceiro de Segurança.
	Vermelho, Piscando	N/D	Tarefa de segurança inoperante.

(1) A E/S inclui tags produzidos/consumidos de outros controladores.

Indicadores de status dos controladores 1756-L7xS

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

Tabela 45 – Descrições do indicador de status do controlador primário 1756-L7xS

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 force. Se instalar uma force, ela será executada imediatamente.
	Âmbar, Piscando	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 forces de E/S. Se habilitar as forces de E/S, todas as forces de E/S existentes também serão executadas.
SD	Desligado	Nenhuma atividade está ocorrendo com o cartão de memória.
	Verde, Piscando	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, Piscando	O cartão de memória não tem um sistema de arquivo válido.
	Vermelho	O cartão de memória não é reconhecido pelo controlador.

Tabela 45 – Descrições do indicador de status do controlador primário 1756-L7xS

Indicador	Status	Descrição
OK	Desligado	Nenhuma energização aplicada.
	Verde	O controlador está operando sem falhas.
	Vermelho, Piscando	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 1756-L7SP tem um indicador de status OK.

Tabela 46 – 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 1756-L7xS

A tela de status do controlador 1756-L7xS exibe mensagens de rolagem que fornecem informações sobre a revisão do firmware do controlador, o status do módulo de armazenamento de energia (ESM), o status 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 47 – Tela de status de segurança

Mensagem	Interpretação
No Safety Signature	A tarefa de segurança está em modo de operação sem uma assinatura de tarefa de segurança.
Safety Partner Missing	O parceiro de segurança está faltando ou não disponível ontem.
Hardware Incompatible	O parceiro de segurança e o hardware do controlador primário é incompatível.
Firmware Incompatible	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 (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.
Safety Unlocked	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 48](#) são tipicamente indicadas na energização, desenergização, e enquanto o controlador estiver operando. Essas mensagens indicam o status do controlador e o ESM.

Tabela 48 – Tela de status geral

Mensagem	Interpretação
Nenhuma mensagem é indicada	O controlador está desligado, ou uma falha grave irrecuperável (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 também visualizar o indicador SD (consulte a página 136) para mais informações de status. Permita a finalização do salvamento antes de remover o cartão SD ou desligar a energia.
CARREGAMENTO	Um projeto está sendo carregado a partir do cartão SD na energização do controlador. Pode-se também visualizar o indicador SD (consulte a página 136) 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 também visualizar o indicador SD (consulte a página 136) 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 o software RSLogix 5000 para fazer o download do projeto para o controlador, ou use um cartão SD para carregar um projeto para o controlador.
<i>Project Name</i>	O nome do projeto que está sendo carregado atualmente no controlador. O nome indicado se baseia no nome do projeto especificado no software RSLogix 5000.
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 módulo de E/S.
Corrupt Certificate Received	O certificado de segurança associado com o 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 carregando	O ESM baseado em capacitor está carregando. Não desenergize até que o carregamento esteja completo.
Flash in Progress	Uma atualização do firmware iniciada via utilitários 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 49 – 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 do software RSLogix 5000, 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 ModuleParentX #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 do software RSLogix 5000. 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 I/O Fault. 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 falha pequenas, grandes e de E/S do Logix5000, publicação [1756-PM014](#).

Mensagens de falhas graves recuperáveis

As falhas graves recuperáveis são indicadas pela *mensagem* Major Fault TXX:CXX na tela de status do controlador. A [Tabela 50 na página 140](#) lista os tipos de falha específicos, códigos e as mensagens associadas como são exibidos 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 50 – 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	Keyswitch 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 *ModuleParentX #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 no software RSLogix 5000.

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 falha pequenas, grandes e de E/S do Logix5000, publicação [1756-PM014](#).

Tabela 51 – 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	Invl Max Consumer Number
#080A	Invl CPCRC
#080B	Time Correction Conn ID Invl
#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	Invl 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
–	

Manutenção da bateria

Tópico	Página
Estimativa da Vida Útil da Bateria	143
Quando Substituir a Bateria	145
Substituição da Bateria	145
Armazene baterias substituição	147

Os controladores primários GuardLogix 1756-L6xS e os parceiros de segurança 1756-LSP contêm uma bateria de lítio que pode precisar ser substituída. Os controladores GuardLogix 1756-L7xS e os parceiros de segurança 1756-L7SP não têm bateria.

Estimativa da Vida Útil da Bateria

A vida útil da bateria depende da temperatura do rack, da dimensão do projeto e da frequência na qual você liga e desliga a alimentação do controlador. A vida útil da bateria não depende da energia do controlador.

Antes do indicador BAT acender

Utilize esta tabela para estimar a vida útil da bateria no pior caso antes que o LED indicador BAT fique vermelho.

Tabela 52 – Estimativa do indicador de bateria (pior caso)

Temperatura 2,54 cm (1 pol.) Abaixo do rack	Ciclos de Alimentação Diários	Dimensões do Projeto			
		1 MB	2 MB	4 MB	8 MB
0 a 40 °C (32 a 104 °F)	3	3 anos	3 anos	26 meses	20 meses
	2 ou menos	3 anos	3 anos	3 anos	31 meses
41 a 45 °C (105 a 113 °F)	3	2 anos	2 anos	2 anos	20 meses
	2 ou menos	2 anos	2 anos	2 anos	2 anos
46 a 50 °C (114 a 122 °F)	3 ou menos	16 meses	16 meses	16 meses	16 meses
51 a 55 °C (123 a 131 °F)	3 ou menos	11 meses	11 meses	11 meses	11 meses
56 a 60 °C (132 a 140 °F)	3 ou menos	8 meses	8 meses	8 meses	8 meses

EXEMPLO

Sob as condições a seguir, a bateria durará pelo menos 20 meses antes do LED indicador BAT ficar vermelho.

- Temperatura máxima 2,54 cm (1 pol.) abaixo do rack é 45 °C (113 °F).
- A alimentação é desligada e ligada 3 vezes por dia.
- O controlador contém um projeto de 8 MB.

Depois que o indicador BAT acender

IMPORTANTE Se o indicador BAT acender pela primeira vez quando se aplica alimentação ao controlador, a vida útil da bateria é menor que o indicado na [Tabela 53](#). Há sempre um pequeno dreno constante na bateria. Parte da vida útil da bateria pode ter sido consumida enquanto o controlador estava desligado e incapaz de acender o indicador BAT.

Tabela 53 – Vida útil da bateria depois que o indicador BAT fica vermelho (pior caso)

Temperatura, Máx. 25,4 mm (1 pol.) Abaixo do rack	Ciclos de alimentação	Dimensões do Projeto			
		1 MB	2 MB	4 MB	8 MB
0 a 20 °C (0 a 68 °F)	3 por dia	26 semanas	18 semanas	12 semanas	9 semanas
	1 por dia	26 semanas	26 semanas	26 semanas	22 semanas
	1 por mês	26 semanas	26 semanas	26 semanas	26 semanas
21 a 40 °C (70 a 104 °F)	3 por dia	18 semanas	14 semanas	10 semanas	8 semanas
	1 por dia	24 semanas	21 semanas	18 semanas	16 semanas
	1 por mês	26 semanas	26 semanas	26 semanas	26 semanas
41 a 45 °C (106 a 113 °F)	3 por dia	12 semanas	10 semanas	7 semanas	6 semanas
	1 por dia	15 semanas	14 semanas	12 semanas	11 semanas
	1 por mês	17 semanas	17 semanas	17 semanas	17 semanas
46 a 50 °C (115 a 122 °F)	3 por dia	10 semanas	8 semanas	6 semanas	6 semanas
	1 por dia	12 semanas	11 semanas	10 semanas	9 semanas
	1 por mês	12 semanas	12 semanas	12 semanas	12 semanas
51 a 55 °C (124 a 131 °F)	3 por dia	7 semanas	6 semanas	5 semanas	4 semanas
	1 por dia	8 semanas	8 semanas	7 semanas	7 semanas
	1 por mês	8 semanas	8 semanas	8 semanas	8 semanas
56 a 60 °C (133 a 140 °F)	3 por dia	5 semanas	5 semanas	4 semanas	4 semanas
	1 por dia	6 semanas	6 semanas	5 semanas	5 semanas
	1 por mês	6 semanas	6 semanas	6 semanas	6 semanas

Quando Substituir a Bateria

Quando a bateria estiver cerca de 95% descarregada, o controlador fornece as advertências a seguir.

- O indicador BAT localizado na parte frontal do controlador acende (vermelho sólido).
- Uma falha de advertência ocorre (tipo 10, código 10 para o controlador).



ATENÇÃO: Para evitar que produtos químicos potencialmente perigosos vazem da bateria, substitua-a de acordo com o seguinte programa, mesmo se o indicador BAT estiver desligado.

Tabela 54 – Programa de substituição da bateria

Se a temperatura 2,54 cm (1 pol.) abaixo do rack estiver	Substitua a bateria a cada
-25 a 35 °C (-13 a 95 °F)	Não é necessária substituição
36 a 40 °C (96,8 a 104 °F)	3 anos
41 a 45 °C (105,8 a 113 °F)	2 anos
46 a 50 °C (114,8 a 122 °F)	16 meses
51 a 55 °C (123,8 a 131 °F)	11 meses
56 a 70 °C (132,8 a 158 °F)	8 meses

IMPORTANTE

Como o controlador GuardLogix é um controlador 1oo2 (dois processadores), recomendamos fortemente que as baterias dos dois controladores sejam substituídas ao mesmo tempo.

Substituição da Bateria

Este controlador contém uma bateria de lítio que deve ser substituída durante a vida útil do produto. Devem-se seguir as precauções específicas ao manusear ou eliminar uma bateria.



ATENÇÃO: O controlador utiliza uma bateria de lítio que contém elementos químicos muito perigosos.

Antes de manusear ou descartar uma bateria, consulte Guidelines for Handling Lithium Batteries, publicação [AG-5.4](#).



ADVERTÊNCIA: Pode ocorrer um arco elétrico ao conectar ou desconectar a bateria. 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.

IMPORTANTE

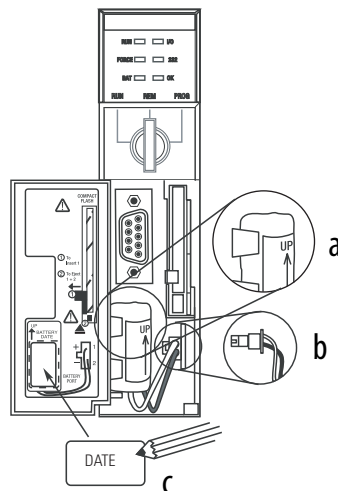
Se você remover a bateria e depois interromper a alimentação, o projeto no controlador será perdido.

Siga este procedimento para substituir a bateria.

1. Ligue a energia do rack.
2. A bateria existente indica sinais de vazamento ou danos?

Se	Faça o seguinte:
Sim	Antes de manusear a bateria, revise Guidelines for Handling Lithium Batteries, publicação AG-5.4 .
Negativo	Passa para a próxima etapa.

3. Remova a bateria.
4. Instale a nova bateria 1756-BA2.
 - a. Instale a bateria conforme exibido.
 - b. Conecte a bateria:
 - + Vermelho
 - Preto
 - c. Anote a data de instalação na etiqueta da bateria e fixe-a no lado de dentro da porta do controlador.



ATENÇÃO: Instale somente uma bateria 1756-BA2. Caso seja instalada uma diferente, poderão ocorrer danos ao controlador.

5. Determine se o indicador BAT na parte dianteira do controlador está desligado.

Se	Faça o seguinte:
Sim	Passa para a próxima etapa.
Negativo	<ol style="list-style-type: none"> 1. Verifique se a bateria está conectada corretamente ao controlador. 2. Se o indicador BAT permanecer aceso, instale outra bateria 1756-BA2. 3. Se o indicador BAT permanecer aceso após a instalação de outra bateria de acordo com a etapa 2, entre em contato com seu distribuidor ou representante Rockwell Automation local.

6. Descarte a bateria antiga de acordo com as regulamentações locais.



ADVERTÊNCIA: Não queime nem descarte baterias de lítio no lixo comum. Elas podem explodir ou se romper violentamente. Siga as leis locais para descartar esses materiais. Você é o responsável legal pelo risco criado durante a eliminação da bateria.



ATENÇÃO: Este produto contém uma bateria de lítio lacrada que pode precisar ser substituída durante a vida útil do produto.

No final desta vida útil, a bateria deste produto deve ser coletada separadamente do lixo comum.

A coleta e a reciclagem de baterias ajudam a proteger o meio ambiente e contribuem para a conservação dos recursos naturais já que materiais valiosos são recuperados.

Armazene baterias substituição



ATENÇÃO: Uma bateria pode liberar produtos químicos potencialmente perigosos se armazenada incorretamente. Armazene as baterias em um ambiente frio e seco. Recomendamos a 25 °C (77 °F) com umidade relativa de 40 a 60%. É possível armazená-las por até 30 dias em temperaturas entre -45 a 85 °C (-49 a 185 °F), como durante o transporte. Para evitar um possível vazamento, não armazene baterias em temperaturas acima de 60 °C (140 °F) por mais de 30 dias.

Recursos adicionais

Consulte as Orientações para o manuseio de baterias de lítio, publicação [AG-5.4](#), para mais informações sobre o manuseio, armazenamento e descarte de baterias de lítio.

Observações:

Alteração do tipo do controlador nos projetos RSLogix 5000

Tópico	Página
Mudança de um controlador padrão para segurança	149
Mudança de um controlador de segurança para padrão	150
Mudança de um controlador 1756 GuardLogix para um 1768 GuardLogix ou vice-versa	151
Mudando de um controlador 1756-L7xS para um 1756-L6xS ou 1768-L4xS	151
Recursos adicionais	151

Como os controladores de segurança têm requisitos especiais e não suportam certos recursos padrão, é preciso entender o comportamento do sistema ao mudar o tipo do controlador de padrão para segurança ou vice-versa no projeto RSLogix 5000. Mudar o tipo de controlador afeta:

- As funções suportadas
- A configuração física do projeto, ou seja, o parceiro de segurança e a E/S de segurança
- Propriedades do controlador
- Componentes do projeto, como tarefas, programas, rotinas e tags
- Instruções add-on de segurança

Mudança de um controlador padrão para segurança

Para a troca bem-sucedida de um 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 1756-LSP é removido do rack de E/S.
- Os módulos de E/S de segurança e os tags são removidos.
- As tarefas, programas e rotinas de segurança são modificadas para tarefas, programas e rotinas padrões.
- Todos os tags de segurança, exceto os tags de consumo de segurança são alterados para tags padrão. Os tags de consumo de segurança são removidos.
- Mapeamentos de tags de segurança são removidos.
- O número da rede de segurança (SNN) é removido.
- As senhas de bloqueio e desbloqueio de segurança são removidas.
- Se o controlador padrão suportar os recursos que não estavam disponíveis ao controlador de segurança, esses recursos são visíveis na caixa de diálogo das Controller 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.

Mudança de um controlador 1756 GuardLogix para um 1768 GuardLogix ou vice-versa

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

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

- Ao mudar para um controlador 1756 GuardLogix, o controlador de segurança é criado no slot x (slot primário + 1).
- 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 1756 suporta 100 programas de segurança na tarefa de segurança, enquanto o controlador Compact GuardLogix 1768 suporta 32.

Mudando de um controlador 1756-L7xS para um 1756-L6xS ou 1768-L4xS

Instruções de ponto flutuante, como FAL, FLL, FSC, SIZE, CMP, SWPB e CPT são suportadas em controladores 1756-L7xS, mas não em controladores 1756-L6xS e 1768-L4xS. Se seu programa de segurança contiver essas instruções, ocorrerão erros de verificação quando se mudar de um controlador 1756-L7xS para um 1756-L6xS ou 1768-L4xS.

Recursos adicionais

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

Observações:

Histórico de mudanças

Com a disponibilidade dos novos controladores, módulos, aplicações e recursos de software RSLogix 5000, este manual foi revisado para incluir as informações atualizadas. Este apêndice resume brevemente as mudanças que foram feitas a cada revisão anterior deste manual.

Consulte este apêndice se precisar determinar que mudanças foram feitas ao longo de diversas revisões. Isso pode ser especialmente útil se você decidir atualizar seu hardware ou software com base nas informações adicionadas nas revisões anteriores deste manual.

1756-UM020H-EN-P, Abril de 2012

Corrigida a lista de fontes de alimentação suportadas.

1756-UM020G-EN-P, Fevereiro de 2012

- Adicionadas informações sobre os controladores 1756-L7xS e 1756-L73SXT
- Atualizada a lista de Recursos Adicionais
- Adicionado um capítulo sobre a instalação do controlador
- Adicionadas informações sobre o uso de conexões unicast para módulos de E/S em redes EtherNet/IP
- Adicionadas informações de instalação
- Adicionadas informações sobre a proteção de modo de operação para a assinatura de tarefa de segurança
- Atualizados os procedimentos de substituição de E/S para incluir diversos cenários de substituição
- Atualizado o valor máximo do intervalo do pacote requisitado
- Adicionados os tipos de dados DCA_INPUT e DCAF_INPUT à lista de tipos válidos para tags de segurança
- Reestruturadas as informações sobre tags de segurança produzidos e consumidos e configuração de controladores de segurança peer para que todas as informações estejam juntas no Capítulo 6
- Adicionadas informações sobre o impacto de um cartão SD travado sobre uma atualização de firmware
- Adicionadas informações sobre o uso do Módulo de Armazenamento de Energia (ESM) para memória não volátil
- Movidas as tabelas de descrição de indicadores de status para um apêndice e adicionadas informações de localização de falhas
- Atualizadas informações sobre quando substituir a bateria em controladores 1756-L6xS

- Adicionadas informações sobre a mudança para um controlador 1756-L7xS
- Adicionado o apêndice Histórico de mudanças

1756-UM020F-EN-P, Agosto de 2010

- Controladores GuardLogix são suportados no RSLogix 5000, versão 19
- O tipo de conexão-padrão para tags produzidos e consumidos é unicast

1756-UM020E-EN-P, Janeiro de 2010

- Instruções Add-on de segurança e alta integridade adicionadas à lista de recursos RSLogix 5000 compatíveis.
- Habilitação da sincronia de tempo
- Atualizados os exemplos de mudança do número da rede de segurança (SNN) de módulos safety I/O na rede CIP safety para mostrar os módulos safety I/O EtherNet/IP
- Informações mais claras no endereçamento da Ethernet
- Conexões ControlNet para módulos de E/S distribuídas
- Definir uma tag como uma constante
- Ajuste do nível de acesso externo para dados de tag
- Procedimentos atualizados para produzir e consumir tags de segurança
- Restrição para mapear as tags de valor constante
- Tabela atualizada de respostas de software durante o descarregamento
- Acessibilidade de GSV/SSV para objeto de segurança AOI
- Armazenamento e carregamento de projetos usando memória não volátil
- Informações atualizadas de descarte da bateria
- Mudança de um controlador 1756 GuardLogix para um 1768 GuardLogix ou vice-versa

1756-UM020D-EN-P, Julho de 2008

- Atualizada a tabela de Recursos Adicionais para incluir novos manuais
- Informações sobre o controlador 1756-L63S
- Informações gerais sobre a programação usando o software RSLogix 5000, versão 17, incluindo versões do software suportadas e aprimoramentos
- O uso de um módulo 1756-EN2T em um sistema baseado em GuardLogix
- Informações sobre módulos de segurança Guard I/O EtherNet/IP
- Atualizada a lista de tipos de dados válidos para tags de segurança
- As ações de trava de segurança e destrave são armazenadas
- A criação e o cancelamento de uma assinatura de segurança são armazenados
- Agora o processo de download inclui verificação para mestre de tempo de sistema (CST)
- Atualizada a descrição do código de falha inoperável de tarefa de segurança
- O valor de assinatura de segurança é acessível via instrução GSV
- Informações de tipo de dados para atributos acessíveis via instruções GSV e SSV
- Acessando as informações sobre falhas usando instruções GSV

- Atualizadas as informações de certificação
- Atualizadas as informações sobre a estimativa da vida útil da bateria
- Atualizadas as informações sobre o descarte adequado da bateria

**1756-UM020C-EN-P,
Dezembro de 2006**

- Entendendo os recursos de fluxo de dados de um controlador GuardLogix
- O controlador não suporta atualizações de sistema operacional usando CompactFlash
- A tarefa de segurança não suporta instruções add-on nem o software de eventos e alarmes FactoryTalk®
- O RPI máximo para conexões de segurança mudou de 500 ms para 100 ms
- A lista dos tipos de dados inválidos para programas de segurança foi substituída por uma lista de tipos de dados válidos
- Revisada a descrição de conexões de segurança produzidas e consumidas
- Revisada a descrição do efeito do recurso de trava de segurança e assinatura de segurança no download
- Adicionada a certificação UL NRGF
- Valores de probabilidade de falha sob solicitação (PFD) e probabilidade de falha por hora (PFH) adicionados às especificações do controlador

**1756-UM020B-EN-P,
Outubro de 2005**

O software de programação RSLogix 5000, versão 14.01 e posteriores, não mais compara a série do hardware entre o parceiro de segurança e o controlador primário ou entre o controlador e a assinatura de segurança no projeto.

**1756-UM020A-EN-P,
Janeiro de 2005**

Lançamento inicial.

Numéricos

1747-CP3 37, 109
1747-KY 27
1756-Axx 28
1756-BA2 27, 28, 146
1756-CN2 63
1756-CN2R 63
1756-CN2RXT 63
1756-CNB 63
1756-CNBR 63
1756-CP3 27, 37, 109
1756-DNB 65, 66, 109
1756-EN2F 59
1756-EN2T 59
1756-EN2TR 59
1756-EN2TXT 59
1756-EN3TR 59
1756-ENBT 59
1756-ESMCAP 27, 44, 46, 122, 124
1756-ESMCAPXT 27, 44, 46, 122, 124
1756-ESMNRM 27, 44, 46, 122, 124
1756-ESMNRMXT 27, 46, 122, 124
1756-ESMNSE 27, 44, 46, 122, 124
1756-ESMNSEXT 27, 46, 122, 124
1756-EWEB 59
1756-PA72 28
1756-PA75 28
1756-PAXT 28
1756-PB72 28
1756-PB75 28
1756-PBXT 28
1756-SPESMCAP 27, 44
1756-SPESMNRM 27, 46, 122
1756-SPESMNRMXT 27, 46, 122
1756-SPESMNSE 27, 44, 46, 122
1756-SPESMNSEXT 27, 44, 46, 122
1784-CF128 27
1784-SD1 27
1784-SD2 27

A

abrangência do diagnóstico 12
acesso externo 92, 96
ambiente 23
ambiente extremo
 componentes do sistema 12
 controlador 12
 fonte de alimentação 28
 rack 28
apagar
 falhas 129
 program 123
aprovação para uso em áreas classificadas
 Europa 26
 Norte-América 24

armazenamento do programa do usuário 19
armazenar um projeto 120
arquivo DNT 87, 88
assinatura de configuração
 componentes 75
 copiar 75
 definição 75
assinatura de tarefa de segurança 96
 armazenando um projeto 120
 copiar 107
 descrição 16
 efeito sobre o download 112
 efeito sobre o upload 112
 gerar 106
 operações restritas 107
 remover 108
 restrições 108
 visualização 125
atraso máximo de rede observado 72
 reset 101
atributos
 objeto de segurança 132
atualização
 firmware 39, 41
atualizações 19
atualizações automáticas de firmware 124
AutoFlash
 atualização do firmware 41

B

barra on-line 125
bateria 27
 armazenamento 147
 conexão 28, 29, 145, 146
 descarte 147
 desconectar 145, 146
 falha 125, 130
 instalação 146
 procedimento de substituição 145
 programa de substituição 145
 vida 143, 144
bateria de lítio 145, 147
bit ConnectionFaulted 127
bit RunMode 127
botão Change Controller 49

C

caixa de diálogo new controller 47
capacidade de RAM 18
carregar um projeto 121
 ao energizar 121
 iniciado pelo usuário 121
 na memória corrompida 121
cartão CF
 Consulte cartão CompactFlash.
cartão CompactFlash 27, 30
 Consulte também cartão de memória.
 inserir 33
 remova 34

- cartão de memória** 119, 120, 121, 124
 - instalação 30
 - remoção 30
 - cartão SD**
 - Consulte cartão Secure Digital.
 - cartão Secure Digital** 27, 30
 - Consulte também cartão de memória.
 - instale 32
 - remova 31
 - chave seletora** 19, 42
 - CIP Safety** 12, 53, 85
 - classe** 96
 - codificação eletrônica** 124
 - códigos de falhas**
 - falhas graves de segurança 130
 - mensagens de E/S 140
 - tela de status 130
 - colar**
 - número da rede de segurança 58
 - componentes de sistema Logix-XT**
 - Consulte ambiente extremo.
 - comunicação** 20
 - módulos 20
 - rede ControlNet 63
 - rede DeviceNet 65
 - rede em série 67
 - rede EtherNet/IP 59
 - conexão**
 - monitore 126
 - não programável 64
 - programável 64
 - rede ControlNet 63
 - rede EtherNet/IP 60
 - status 127
 - USB 35
 - conexão em modo de escuta** 76
 - conexões não programáveis** 64
 - conexões programáveis** 64
 - configure sempre** 84
 - caixa de seleção 51
 - CONNECTION_STATUS** 97, 127
 - consumir dados de tag** 100
 - controlador**
 - ambiente extremo 12
 - armazenamento
 - assinatura de tarefa de segurança 107
 - travamento de segurança,
 - destravamento 105
 - configuração 47
 - corresponder 111
 - diferença de número de série 114, 117
 - diferenças de função 11
 - instalação 29
 - manipulador de falhas 131
 - modo 42
 - modo de operação 42, 43
 - mudar tipo 149–151
 - número de série 111
 - propriedades 48
 - controlador Compact GuardLogix** 151
 - controlador Compact GuardLogix 1768** 151
 - controlador de segurança peer**
 - compartilhamento de dados 97
 - configuração 52
 - localização 97
 - SNN 97, 98
 - controlador primário**
 - características gerais de hardware 18
 - descrição 18
 - memória do usuário 18
 - modos 19
 - controladores GuardLogix**
 - diferenças 11
 - ControlNet**
 - características gerais 63
 - conexões 63, 110
 - configurar driver 110
 - exemplo 64
 - módulo 63, 109
 - módulos de comunicação 20
 - não programável 64
 - programável 64
 - software 63
 - conversor de protocolos** 62
 - copiar**
 - assinatura de tarefa de segurança 107
 - número da rede de segurança 58
 - criação de um projeto** 47
- D**
- dados-padrão em uma rotina de segurança** 103
 - descarga eletrostática** 26
 - destravamento de segurança**
 - controlador 106
 - ícone 105
 - destravar controlador** 106
 - DeviceNet**
 - comunicação 65
 - conexões 66, 110
 - configurar driver 110
 - módulo 109
 - software 66
 - DF1** 67
 - DH-485** 67
 - dispositivos IHM** 16
 - download**
 - efeito da revisão de firmware compatível 111
 - efeito do controlador compatível 111
 - efeito sobre a assinatura da tarefa de segurança 112
 - efeito sobre a proteção 112
 - efeito sobre o status de segurança 111
 - processo 113–114
 - driver**
 - ControlNet 110
 - DeviceNet 110
 - EtherNet/IP 110
 - USB 36
 - driver de dispositivo RS-232 DF1** 38

E

- E/S**
 - códigos de falhas 140
 - indicador 126
 - substituição de módulo 51
- E/S CIP Safety**
 - adicionando 69
 - assinatura de configuração 75
 - dados de status 77
 - endereço de nó 69
 - reset propriedade 76
 - status do monitor 77
- edição** 107
- endereço**
 - módulo de E/S CIP Safety 77
- endereço de nó** 69
- endereço IP** 62, 69
- entrar em comunicação** 116
 - fatores 111
- erros de verificação**
 - mudando o tipo de controlador 151
- ESM**
 - Consulte o módulo de armazenamento de energia
- estado seguro** 15
- EtherNet/IP**
 - características gerais 59
 - conexões 60, 110
 - configurar driver 110
 - exemplo 61
 - exemplo de configuração 61
 - módulo 109
 - módulos 59
 - módulos de comunicação 20
 - módulos de E/S CIP Safety 61
 - módulos de E/S padrão 62
 - parâmetros de rede 62
 - recursos do módulo 59
 - software 60
 - uso da conexão 60

F

- falha**
 - apagar 129
 - controlador irrecuperável 129
 - mensagens 139
 - recuperável 129, 139
 - rotinas 131–133
 - segurança irrecuperável 128, 129
- falha de segurança irrecuperável** 128, 129
 - reiniciando a tarefa de segurança 129
- falha do controlador irrecuperável** 129
- falha grave recuperável**
 - mensagens 139
- falha recuperável** 129, 139
 - apagar 129
- falhas graves de segurança** 130
- falhas graves recuperáveis** 139
- flags de status** 127
- fonte de alimentação**
 - códigos de catálogo 19, 28
- forçando** 107

G

- gabinete** 23
- GSV (obter valor do sistema)**
 - definição 12
 - possibilidade de acesso 132
 - usando 132
- guia major faults** 130
- guia minor faults** 130
- guia safety** 106, 107, 128
 - assinatura de configuração 75
 - controlador com trava de segurança 106
 - criação de uma assinatura de tarefa de segurança 107
 - dados de conexão 72
 - destravar 106
 - substituição de módulo 80
 - trava de segurança 106
 - visualizar o status de segurança 111, 128

I

- indicador BAT** 125, 144, 146
- indicadores de status**
 - módulos de E/S 78
- Instruções Add-on** 21, 150
- intervalo do pacote requisitado** 97
 - dados de tags produzidos 93
 - definição 12
 - E/S CIP Safety 72
 - tag consumido 101
 - tags consumidos 93

K

- kit de atualização do firmware** 111, 124

L

- leitura de controle de configuração** 76
 - identificando 76
 - reset 76, 79
- limite de tempo de reação**
 - E/S CIP Safety 71
- limite de tempo de reação de conexão** 71, 101

M

- MajorFaultRecord** 133
- máscara de sub-rede** 62
- memória**
 - capacidade 18
 - cartão 19
- memória do usuário** 18
- memória não volátil** 119–124
 - guia 119
- mensagem**
 - tela de status 138
- mensagens**
 - falha 139
 - status de segurança 137
 - status geral 138

mensagens gerais de status 138**modo**

em operação 42

modo de operação 42**modo de programa** 42**modo remoto** 42, 43**módulo**

ControlNet 20

DeviceNet 20

EtherNet/IP 20, 59

indicador de status 78

propriedades

guia connection 76

módulo de armazenamento de energia 27

1756-ESMCAP 27

armazenamento não volátil 122

carregando 29, 46

definição 12

desinstale 44

instale 46

tempo de espera 124

módulo Guard I/O

substituição 79–88

monitore

conexões 126

status 77

morphing

Consulte mudar controladores.

mudando controladores 149–150**multicast** 12**multiplicador de atraso de rede** 74, 102**multiplicador de tempo-limite** 73, 102**N****Nível de desempenho** 12**nível de desempenho** 15**número da rede de segurança** 53

ao gerenciamento 53

atribuição 53

atribuição automática 55

atribuição manual 55

colar 58

com base na hora 54

copiar 58

copiar e colar 58

definição 12

definir 71

descrição 15

diferença 86

formatos 53

manual 54

modificação 55

mudando o SNN de E/S 56

mudando o SNN do controlador 56

visualização 48

número de série 111**número de slot** 48**O****objeto de segurança**

atributos 132

P**parceiro de segurança**

configuração 19

descrição 19

indicadores de status 135

status 128

período da tarefa de segurança 72, 91, 97**probabilidade de falha por hora (PFH)**

definição 12

probabilidade de falha sob solicitação (PFD)

definição 12

produza um tag 99**produzir e consumir tags** 60, 63, 97**programa de substituição**

bateria 145

programação 107**programas de segurança** 92**projeto para combinar o controlador** 111**projetos de segurança**

recursos 21

pronto para usar 81

reinicialize o módulo 79

propriedade

configuração 76

reset 76

proteção da aplicação de segurança 104–108

assinatura de tarefa de segurança 106

segurança do RSLogix 106

trava de segurança 105

proteção do modo de operação 106, 108**proteja a assinatura em modo de operação** 50**protocolo de controle e informação**

definição 12

R**rack** 19

códigos de catálogo 28

radiação UV 26**remoção e inserção sob alimentação** 24**remover**

assinatura de tarefa de segurança 108

reset

módulo 79

propriedade 76, 79

restrições

mapeamento de tags de segurança 103

programação 108

quando com trava de segurança 105

quando existir a assinatura de segurança 107

software 108

revisão do firmware

atualização 39, 41

corresponder 111

diferença 112, 114, 117

gestão 124

RIUP

Consulte remoção e inserção sob alimentação

rotina de falha do programa 131**rotina de segurança** 92

usando dados-padrão 103

RPI

consulte intervalo do pacote requisitado

S

- SafetyTaskFaultRecord** 133
- salve o programa**
 - memória não volátil 122
- segurança do RSLogix** 106
- senha**
 - caracteres válidos 50
 - definir 49
- serial**
 - cabo 27
 - comunicação 67
 - driver 38
 - porta 37
 - conexão 37
 - configuração 67
 - rede 67
 - software 67
- símbolo de alerta** 126
- sincronia de tempo** 51, 114
- SNN**
 - Consulte o número da rede de segurança
- software**
 - rede ControlNet 63
 - rede EtherNet/IP 60
 - redes DeviceNet 66
 - restrições 108
 - USB 35
- software ControlFLASH** 40, 111, 121, 124
- software RSLinx Classic**
 - versão 21
- software RSLogix 5000**
 - reinicialize o módulo 79
 - restrições 108
 - versões 21
- software RSNetWorx para DeviceNet**
 - substitua o módulo 86
- SSV (definir valor do sistema)**
 - possibilidade de acesso 132
 - usando 132
- status**
 - indicadores 135–137
 - mensagens 137
 - mensagens de falha 139
 - mensagens, tela 138
 - parceiro de segurança 128
 - tela 137–142
- status de rede**
 - indicador 78, 82, 83, 87
- status de segurança**
 - assinatura de tarefa de segurança 106
 - botão 106, 126
 - efeito sobre o download 111
 - restrições de programação 108
 - visualização 111, 125, 128
- substitua**
 - configure only... habilitado 80
 - configure sempre habilitado 84
 - módulo Guard I/O 79–88
- Supervisor de firmware** 124

T

- tag consumido** 93, 97
- tag de valor constante** 96
- tag produzido** 93, 97
- tags**
 - acesso externo 92, 96
 - alias 93
 - base 93
 - características gerais 92
 - classe 96
 - com escopo no controlador 95
 - Consulte também tags de segurança.
 - consumidos 93, 97
 - dados de segurança
 - produzidos/consumidos 94, 95
 - do programa 95
 - E/S de segurança 94, 95
 - escopo 95
 - nomeação 76
 - produzidos 93, 97
 - tipo 93
 - tipo de dados 94
 - valor constante 96
- tags alias** 93
- tags com escopo no controlador** 95
- tags de base** 93
- tags de segurança**
 - com escopo no controlador 95
 - criar 92
 - descrição 92
 - do programa de segurança 95
 - mapeamento 102–104
 - tipos de dados válidos 94
- tags do programa** 95
- tarefa de segurança** 90
 - execução 91
 - prioridade 90
 - tempo de watchdog 90
- tempo de espera**
 - módulo de armazenamento de energia 124
- tempo de reação** 91
- tempo de reação da conexão avançada** 73
- tempo de sistema** 114, 137
- tempo de watchdog** 90
- tempos de varredura**
 - reset 108
- terminologia** 12
- tipos de dados**
 - CONNECTION_STATUS 97
- tipos de dados REAIS** 94
- trava**
 - Consulte a trava de segurança.
- trava de segurança** 105
 - controlador 106
 - efeito sobre o download 112
 - efeito sobre o upload 112
 - ícone 105
 - senha 106

U

unicast 12
conexões 71, 97, 100

upload
efeito do controlador compatível 111
efeito sobre a assinatura da tarefa de
segurança 112
efeito sobre a proteção 112
processo 115

USB

cabo 35, 109
conexão 35
driver 36
porta 35
software necessário 35
tipo 35

V

visualização
status de segurança 111

W

WallClockTime 122, 124
módulo de armazenamento de energia 124
objeto 46

X

XT
Consulte ambiente extremo.

Suporte Rockwell Automation

A Rockwell Automation fornece informações técnicas na Web para ajudar na utilização de seus produtos. Em <http://www.rockwellautomation.com/support/>, você pode localizar manuais técnicos, uma base de conhecimento de FAQs, notas técnicas e de aplicação, códigos de amostra e links para pacotes de serviços de software e um recurso MySupport que pode ser personalizado para melhorar a utilização dessas ferramentas.

Para um nível adicional de suporte técnico por telefone sobre instalação, configuração e localização de falhas, disponibilizamos os programas de suporte TechConnectSM. Para mais informações, entre em contato com seu distribuidor local ou representante Rockwell Automation ou visite o site <http://www.rockwellautomation.com/support/>.

Assistência na Instalação

Se surgir alguma anomalia 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 Localizador mundial em http://www.rockwellautomation.com/support/americas/phone_en.html , ou entre em contato com o seu representante local Rockwell Automation.

Devolução de Satisfação 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/>.

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