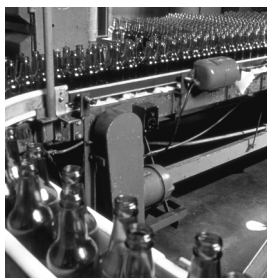


Controladores SmartGuard 600



Manual do usuário

Códigos de catálogo 1752-L24BBB,
1752-L24BBBE

Informações importantes para o usuário

Equipamentos de estado sólido têm características operacionais diferentes dos equipamentos eletromecânicos. Orientações de segurança para a aplicação, instalação e manutenção dos controles de estado sólido (publicação [SGI-1.1](#) disponível no escritório de vendas local da Rockwell Automation em <http://literature.rockwellautomation.com>) descreve algumas diferenças importantes entre equipamentos de estado sólido e dispositivos eletromecânicos com fio. Por conta dessa diferença e também da grande variedade de usos para o equipamento de estado sólido, todas as pessoas responsáveis por aplicar esse equipamento devem ter a certeza de que todas as aplicações pretendidas do equipamento são aceitáveis.

Sob hipótese alguma a Rockwell Automation, Inc. será responsável por danos indiretos ou consequentes que resultem do uso ou da aplicação desses equipamentos.

Os exemplos e diagramas deste manual estão incluídos aqui apenas para fins ilustrativos. Por conta das muitas variáveis e especificações associadas a determinadas instalações, a Rockwell Automation, Inc. não pode ser responsabilizada pelo uso real com base nos exemplos e diagramas.

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

É proibida a reprodução do conteúdo deste manual, no todo ou em parte, sem a autorização por escrito da Rockwell Automation, Inc.

Em todo o manual, usamos observações para alertá-lo das considerações sobre segurança quando necessário.

ADVERTÊNCIA 	Identifica informações sobre práticas ou circunstâncias que podem causar explosão em ambiente classificado, com possibilidade de ferimentos pessoais ou morte, prejuízos a propriedades ou perdas econômicas.
IMPORTANTE	Identifica informações críticas para uma aplicação correta e melhor compreensão sobre o produto.
ATENÇÃO 	Identifica informações sobre práticas ou circunstâncias que podem causar ferimentos pessoais ou morte, prejuízos a propriedades ou perdas econômicas. As chamadas de Atenção ajudam você a identificar um perigo, evitá-lo e reconhecer sua consequência.
PERIGO DE CHOQUE 	As etiquetas podem estar fora ou dentro do equipamento, por exemplo, um inversor ou motor, para alertar as pessoas de que uma tensão perigosa pode estar presente.
PERIGO DE QUEIMADURA 	As etiquetas podem estar fora ou dentro do equipamento, por exemplo, um inversor ou motor, para alertar as pessoas de que as superfícies podem atingir temperaturas perigosas.

Allen-Bradley, Rockwell Automation, SmartGuard, Logix, ControlLogix, Guard I/O, POINT I/O, RSLogix 5000, RSNetWorx para DeviceNet, RSLinx e TechConnect são marcas comerciais da Rockwell Automation, Inc.

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

As informações abaixo resumem as mudanças neste manual desde a última impressão.

Tópico	Página
Adicionado o controlador 1752-L24BBBE	ao longo deste manual
Adicionada a comunicação Ethernet	28
Adicionado o aterramento do controlador 1752-L24BBBE	30
Atualizada a conexão à ilustração da porta DeviceNet	32
Adicionado conectando a porta Ethernet	33
Atualizado o exemplo de fiação de parada de emergência	38, 285
Atualizado o exemplo de fiação do gate de segurança	38, 287
Adicionado o capítulo Configure sua rede EtherNet/IP	Capítulo 4
Atualizada a comunicação DeviceNet	Capítulo 7
Adicionado o capítulo Configure seu controlador para a comunicação EtherNet/IP	Capítulo 8
Adicionada a tabela de mensagens de erro EtherNet/IP	188
Atualizadas as especificações do controlador	197
Atualizadas as tabelas de indicador de status de módulo	203
Adicionado Identificando erros EtherNet/IP	212
Atualizado o exemplo de fiação de zona dupla	288
Atualizado o exemplo de fiação do tapete de segurança	290

Observações:

	Prefácio	
	A Quem se Destina este Manual	13
	Finalidade deste Manual	13
	Recursos adicionais	13
	Técnicas Comuns Usadas neste Manual	14
	Capítulo 1	
Características gerais	Introdução.....	15
	Sobre o controlador SmartGuard 600	15
	Hardware	17
	Comunicação	20
	Configuração e programação.....	20
	Monitoração de erros e status	20
	Conceito de segurança do controlador.....	21
	Recurso adicional.....	21
	Capítulo 2	
Instalação e aplicação da fiação no controlador SmartGuard 600	Introdução.....	23
	Informações gerais sobre a segurança	23
	Compreendendo o endereçamento do nó.....	26
	Ajustando o endereço do nó	26
	Ajustando o parâmetro da faixa de comunicação	27
	Comunicação DeviceNet.....	27
	Comunicação Ethernet.....	28
	Instalação do controlador SmartGuard	29
	Aterramento do controlador SmartGuard	30
	Conexão de uma fonte de alimentação	30
	Fazendo conexões de comunicação.....	31
	Conexão à porta do DeviceNet	32
	Conexão à porta USB	33
	Conectando-se à porta Ethernet	33
	Aplicação da fiação ao controlador SmartGuard 600.....	34
	Fiação dos dispositivos de entrada	35
	Fiação dos dispositivos de saída	37
	Exemplos de fiação.....	38
	Capítulo 3	
Ajuste da rede do DeviceNet	Introdução.....	41
	Conexão de um computador à rede DeviceNet.....	41
	Configuração de um driver para a rede.....	42
	Verificação do funcionamento do driver	42
	Comissionamento de todos os nós	42
	Pesquisa da rede	44
	Assinatura da configuração	45
	Reset de segurança (opcional).....	46
	Configurando senhas (opcional)	47
	Definição ou alteração de senha	47
	Senhas esquecidas.....	48

	Capítulo 4	
Configure sua rede EtherNet/IP	Introdução.....	51
	Conexão do computador à rede EtherNet/IP	51
	Configuração de um driver para a rede.....	52
	Verificação do funcionamento do driver	52
	Conectando o controlador SmartGuard 600 à rede EtherNet/IP	53
	Configurando o endereço IP.....	53
	Usando BOOTP para configurar o endereço IP	54
	Use o utilitário Rockwell BOOTP	55
	Use o software RSLinx para configurar o endereço IP	57
	Formando ponte nas redes	59
	Rede EtherNet/IP para uma rede DeviceNet	60
Porta USB para a rede EtherNet/IP	62	
	Capítulo 5	
Gerenciamento do SNN	Introdução.....	63
	Formatos do número da rede de segurança (SNN).....	63
	Número da rede de segurança com base no tempo (recomendável)	64
	Número da rede de segurança (SNN) manual	64
	Atribuição do número da rede de segurança (SNN).....	65
	Automática (com base no tempo)	65
	Manual	65
	Definição do número da rede de segurança (SNN) em todos os nós de segurança	65
	Diferença no número da rede de segurança (SNN)	67
	Número da rede de segurança (SNN) e alterações no endereço do nó.....	67
	Capítulo 6	
Configuração de E/S local	Introdução.....	69
	Configuração das entradas de segurança locais.....	69
	Exemplo: canal de entrada como pulso de teste da saída de teste	73
	Ajuste automático dos tempos de atraso na energização e na desenergização.....	74
	Configuração das saídas de teste locais.....	74
	Capítulo 7	
Configuração do controlador para a comunicação DeviceNet	Introdução.....	79
	Ajustando o controlador como um mestre de segurança.....	79
	Configuração dos alvos de E/S de segurança CIP na rede do DeviceNet	80
	Configuração das conexões de E/S de segurança	83
	Altere uma conexão de E/S	86

Ajustando o controlador como um escravo de segurança	90
Criar dados de E/S do escravo de segurança	90
Uso do perfil genérico da segurança no software	
RSLogix 5000	93
Controlador SmartGuard para intertravamento de segurança	
do controlador SmartGuard	96
Ajustando o controlador como um escravo padrão DeviceNet	98
Criação de dados de E/S do escravo padrão	98
Adição do escravo padrão SmartGuard à lista de varredura	
do mestre padrão	102
Leitura e gravação de e para o controlador SmartGuard para	
uma interface PanelView Plus	103
Leia BOOLs do controlador SmartGuard e os exiba na	
interface PanelView Plus	104
Configure a lista de varredura do scanner PanelView	106
Configure o scanner RN10C DeviceNet	107
Leia e grave do e para o controlador SmartGuard a partir	
da interface PanelView Plus simultaneamente	113
Configure a lista de varredura do scanner PanelView	116
Configure o scanner RN10C DeviceNet	118
Configure os dados que são gravados da interface	
PanelView Plus para o controlador SmartGuard	119
COS Versus com polling	123
Tamanhos máximos de conexão	125

Capítulo 8

Configuração do controlador para a comunicação EtherNet/IP

Introdução	129
Conexões multicast	129
Configure a E/S alvo no software RSNetWorx para DeviceNet	130
Configure seu controlador como escravo usando o perfil genérico	
do software RSLogix 5000	134
Configure a comunicação entre o terminal padrão PanelView e um	
controlador SmartGuard 600 em uma rede EtherNet/IP	136

Capítulo 9

Definição dos modos do controlador

Introdução	139
Definir modo de execução automática (opcional)	139
Definição do modo de comunicação independente (opcional)	140
Alteração do modo do controlador	141

Capítulo 10

Criação do programa aplicativo

Introdução	143
O Logic Editor	143
Programação básica	144
Funções de lógica e blocos de funções	145
Tags de entrada	145
Tags de saída	147
Função de comentário de E/S	148
Restrições de programação	148

Criando um programa de bloco de funções	149
Adição de um tag de entrada ou de saída	149
Adição de um bloco de funções	149
Conexão dos tags ao bloco de funções	150
Edição dos parâmetros de bloco de funções	150
Configurações de E/S	151
Seleções do ponto de saída opcional	152
Comentários	152
Encontrar blocos de funções com conexões abertas	153
Programação em várias páginas	154
Para salvar o programa	155
Para atualizar o programa	155
Para monitorar o programa on-line	156
Seqüência de execução do programa	157
Blocos de funções definidos pelo usuário	158
Criação de blocos de funções definidos pelo usuário	158
Proteção por senha blocos de funções definidos pelo usuário	159
Reutilização de arquivos de blocos de funções definidos pelo usuário	160
Precauções quanto à reutilização dos blocos de funções definidos pelo usuário	162
Recursos adicionais	162

Capítulo 11

Download e verificação

Introdução	163
Download da configuração de rede do DeviceNet	163
Verificando a configuração de segurança de seu DeviceNet	165
Iniciar o Safety Device Verification Wizard	165
Determinação se os equipamentos podem ser verificados	166
Seleção dos equipamentos a serem verificados	167
Revisão dos relatórios de verificação do equipamento de segurança	169
Trava de dispositivos de segurança	170
Visualização do resumo do Safety Device Verification Wizard	171

Capítulo 12

Monitoração do Status e Controle de Falhas

Introdução	173
Indicadores de status	173
Tela alfanumérica	174
Monitoração da entrada da fonte de alimentação de E/S	175
Monitoração das informações de manutenção de E/S	176
Monitoração do contador de operações do contato	176
Monitoração do tempo de ativação total	176
Configuração de um modo de monitoração de manutenção	177
Apagamento dos valores de manutenção	178

	Exibição de dados de status de E/S	179
	Dados de status geral	180
	Status da entrada local	181
	Status da saída local	181
	Saída de teste ou status da lâmpada muting.....	181
	Status de conexão do controlador (função de escravo de segurança).....	182
	Categorias de erro	184
	Tabela do histórico de erros	185
	Área de memória do histórico de erros	185
	Exibição da tabela do histórico de erro para o controlador 1752-L24BBB.....	185
	Exibição da tabela de histórico de erros EtherNet/IP para o controlador 1752-L24BBBE	186
	Tabela de histórico de erros Ethernet.....	187
	Mensagens do histórico de erros e ações corretivas	188
	Erros de download e ações corretivas	192
	Erros de reinicialização e ações corretivas	194
	Erros de alteração do modo e ações corretivas	195
	 Apêndice A	
Especificações do controlador	Introdução.....	197
	Especificações gerais	197
	Especificações ambientais	199
	Certificações	201
	 Apêndice B	
Indicadores de status	Introdução.....	203
	Indicadores de status do módulo	203
	Identificando erros usando indicadores de status de módulo e tela alfanumérica.....	208
	Identificando erros EtherNet/IP usando indicadores de status e tela alfanumérica.....	212
	 Apêndice C	
Referência de comando das funções de lógica	Introdução.....	213
	Instrução complementação (NOT)	213
	Diagrama da instrução complementação	213
	Tabela verdade instrução complementação.....	213
	Instrução AND	214
	Diagrama de instrução AND	214
	Tabelas verdade da instrução AND.....	214
	Instrução OR	216
	Diagrama da instrução OR	216
	Tabelas verdade da instrução OR.....	216
	Instrução OR exclusiva	218
	Diagrama da OR exclusiva.....	218
	Tabela verdade da OR exclusiva.....	219

Instrução NOR exclusiva.....	219
Diagrama da instrução NOR exclusiva.....	219
Tabelas verdade da instrução NOR exclusiva.....	219
Instrução de roteamento.....	220
Diagrama da instrução de roteamento.....	220
Tabela verdade da instrução de roteamento.....	220
Instrução de Reset Set Flip-flop (RS-FF).....	220
Diagrama da instrução de Reset Set Flip-flop.....	220
Manuseio de erro de Reset Set Flip-flop.....	221
Gráfico de temporização da instrução Flip-flop.....	221
Instrução de vários conectores.....	221
Diagrama da instrução de vários conectores.....	221
Tabela verdade da instrução com vários conectores.....	222
Instrução de comparação.....	222
Diagrama da instrução de comparação.....	223
Parâmetros da instrução de comparação.....	223
Tabela verdade da instrução de comparação.....	224
Gráfico de temporização da instrução de comparação.....	225

Apêndice D

Referência de comandos dos blocos de funções

Introdução.....	227
Bloco de funções de reset.....	227
Parâmetros do bloco de funções de reset.....	228
Gráficos de temporização do bloco de funções de reset.....	229
Bloco de funções de reinicialização.....	229
Reinicie os parâmetros do bloco de funções.....	230
Gráficos de temporização do bloco de funções de reinicialização.....	231
Parada de emergência (ESTOP).....	231
Parâmetros do bloco de funções ESTOP.....	232
Tabelas verdade do bloco de funções ESTOP.....	233
Manuseio de erro do bloco de funções ESTOP.....	233
Gráfico de temporização do bloco de funções ESTOP.....	234
Bloco de funções da cortina de luz (LC).....	234
Parâmetros do bloco de funções da cortina de luz.....	235
Tabelas verdade do bloco de funções da cortina de luz.....	235
Manuseio do bloco de funções da cortina de luz.....	236
Gráfico de temporização do bloco de funções da cortina de luz.....	236
Bloco de funções de monitoração do gate de segurança.....	237
Saídas opcionais do bloco de funções de monitoração do gate de segurança.....	237
Ajuste de parâmetro de saída de apresentação da falha no bloco de funções de monitoração do gate de segurança.....	237
Testes de função do bloco de funções de monitoração do gate de segurança.....	237
Parâmetros do bloco de funções de monitoração do gate de segurança.....	238

Tabelas verdade do bloco de funções de monitoração do gate de segurança.....	239
Manuseio de erro do bloco de funções de monitoração do gate de segurança.....	240
Gráficos de temporização do bloco de funções de monitoração do gate de segurança	241
Bloco de funções de controle bidirecional.....	242
Saídas opcionais do bloco de funções de controle bidirecional.	242
Ajuste de parâmetro de saída de apresentação da falha no bloco de funções do controle bidirecional.....	242
Parâmetros de blocos de funções de controle bidirecional.....	243
Tabela verdade de blocos de funções de controle bidirecional	243
Manuseio de erro do bloco de funções de controle bidirecional	244
Gráfico de temporização de blocos de funções de controle bidirecional	244
Bloco de funções do temporizador com atraso na desenergização.....	245
Gráfico de temporização do bloco de funções do temporizador com atraso na desenergização	245
Bloco de funções do temporizador com atraso na energização.....	245
Gráfico de temporização do bloco de funções do temporizador com atraso na energização	246
Bloco de funções da chave no modo do usuário.....	246
Saídas opcionais do bloco de funções da chave em modo de usuário.....	246
Ajuste de parâmetro de saída de apresentação da falha no bloco de funções da chave em modo de usuário.....	247
Tabela verdade do bloco de funções da chave em modo de usuário.....	247
Manuseio de erro do bloco de funções da chave em modo de usuário.....	247
Gráfico de temporização do bloco de funções da chave em modo do usuário	248
Monitoração de dispositivo externo (EDM)	248
Saídas opcionais do bloqueio de funções de EDM.....	249
Configuração da saída de apresentação da falha no bloco de funções de EDM.....	249
Parâmetro do bloco de funções de EDM.....	249
Manuseio de erro do bloco de funções EDM	249
Gráfico de temporização do bloco de funções EDM.....	250
Muting.....	250
Parâmetros do bloco de funções de muting.....	251
Saídas opcionais do bloqueio de funções de muting	252
Ajuste de parâmetro de saída de apresentação da falha no bloco de funções de muting.....	252
Manuseio de erro do bloco de funções de muting	252
Detalhes da função de muting.....	253
Exemplo: Muting paralelo com 2 sensores.....	254
Exemplo: detecção de posição.....	261
Exemplo: função de override.....	263

Chave de habilitação.....	266
Parâmetros do bloco de funções da chave de habilitação	267
Saídas opcionais	267
Ajuste de saída de apresentação padrão	267
Manuseio de erro do bloco de funções da chave de habilitação.....	268
Gráficos de temporização do bloco de funções da chave de habilitação.....	268
Gerador de pulso	269
Parâmetros de blocos de funções do gerador de pulso.....	269
Gráfico de temporização dos parâmetros de blocos de funções do gerador de pulso	270
Contador.....	270
Parâmetros do bloco de funções do contador	270
Condição de reset.....	271
Tipo de contagem	271
Gráficos de temporização do bloco de funções do contador.....	271

Apêndice E

Mensagens explícitas

Introdução.....	273
Recebendo mensagens explícitas	273
Formato do comando	273
Formato de resposta	274
Formato de resposta com erro.....	275
Exemplo de mensagem de leitura de um controlador GuardLogix	276
Envio de mensagens explícitas	276
Restrições de envio das mensagens explícitas	277
Acessando parâmetros do controlador usando mensagens explícitas do DeviceNet	278

Apêndice F

Exemplos de aplicação e de configuração

Introdução.....	285
Aplicação de parada de emergência.....	285
Aplicação de gate de segurança com reset automático	287
Aplicação de gate de segurança de zona dupla usando a chave de parada de emergência com reset manual.....	288
Aplicação de tapete de segurança.....	290
Aplicação de cortina de luz	292

Glossário

Índice

Leia este prefácio para familiarizar-se com a outra parte do manual, que oferece informações sobre:

- a quem se destina este manual
- a finalidade deste manual
- recursos adicionais.
- convenções usadas neste manual.

A Quem se Destina este Manual

Use este caso você seja o responsável pelo projeto, pela instalação, pela programação ou pela localização de falhas em sistemas de controle que usem controladores SmartGuard 600.

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.

Finalidade deste Manual

Este manual é um guia sobre como usar controladores SmartGuard 600. Ele descreve os procedimentos específicos usados por você para configurar, operar e localizar falhas no controlador SmartGuard 600.

Recursos adicionais

A tabela fornece uma listagem das publicações que contêm informações importantes sobre os sistemas do controlador SmartGuard 600.

Recurso	Descrição
Instruções de instalação do controlador SmartGuard 600, publicação 1752-IN001	Obter informações sobre como instalar o controlador SmartGuard 600
Manual de referência de segurança de sistemas de controladores SmartGuard, publicação 1752-RM001	Obter especificações detalhadas sobre como obter e manter o SIL 3 com o sistema do controlador SmartGuard
Instruções de instalação DeviceNet Safety I/O, publicação 1791DS-IN001	Obter informações sobre como instalar módulos do DeviceNet Safety de E/S de proteção
Manual do usuário de módulos Guard I/O DeviceNet Safety, publicação 1791DS-UM001	Obter informações sobre como usar módulos do DeviceNet Safety de E/S de proteção
Guia de instalação de projeto de mídia DeviceNet, publicação DNET-UM072	Informações sobre o planejamento da sua rede EtherNet/IP

Pode-se visualizar ou fazer o download das publicações em <http://literature.rockwellautomation.com>. Para pedir cópias impressas de documentos técnicos, entre em contato com seu distribuidor Rockwell Automation local ou representante de vendas.

Técnicas Comuns Usadas neste Manual

Estas convenções são usadas ao longo deste manual:

- Listas de bullets, como esta fornecem informações, mas não etapas de procedimentos.
- Listas numeradas fornecem etapas seqüenciais ou informações hierárquicas.

Características gerais

Introdução

Tópico	Página
Sobre o controlador SmartGuard 600	15
Conceito de segurança do controlador	21
Recurso adicional	21

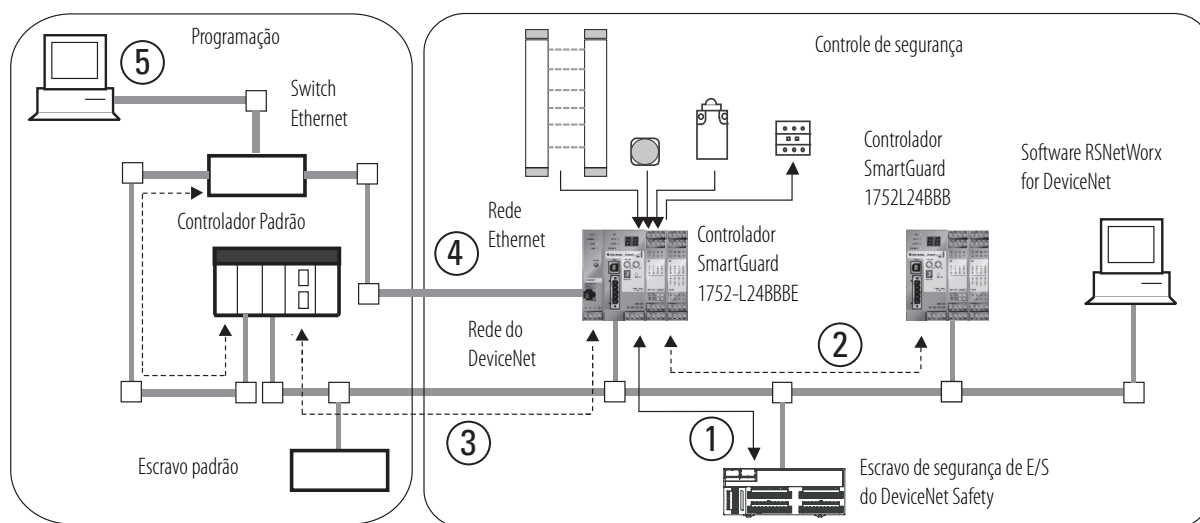
Sobre o controlador SmartGuard 600

Os controladores SmartGuard 600 (códigos de catálogo 1752-L24BBB e 1752-L24BBBE) são sistemas eletrônicos programáveis com recursos de 16 entradas digitais, 8 saídas digitais, 4 fontes de pulso de teste, e conexões para comunicação USB e DeviceNet. E ainda, o controlador 1752-L24BBBE oferece conectividade EtherNet/IP.

O controlador SmartGuard 600 suporta tanto a comunicação padrão quanto CIP Safety nas redes DeviceNet, e suporta a comunicação CIP padrão nas redes EtherNet/IP.

O controlador SmartGuard 600 é certificado para o uso em aplicações de segurança até e inclusive o nível de integridade de segurança (SIL) 3, de acordo com a IEC 61508, nível de desempenho PL(e) de acordo com a ISO 13849-1, e categoria (CAT) 4, de acordo com a EN 954-1.

Exemplo do sistema de controle de segurança do controlador SmartGuard 600

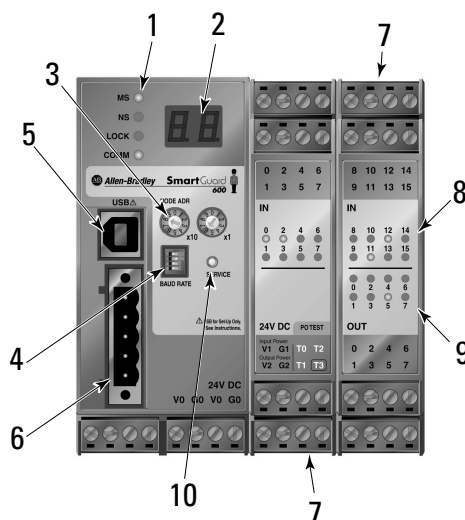


Número	Descrição
1	Como mestre de DeviceNet safety, o controlador SmartGuard 600 pode controlar até 32 módulos Guard I/O modules. Estes módulos 1791DS e 1732DS são os mesmos módulos distributed safety I/O usados com controladores GuardLogix.
2	Como escravo do DeviceNet safety, o controlador SmartGuard 600 parece o distributed safety I/O para um mestre de segurança. Um GuardLogix ou outro mestre de segurança SmartGuard pode ler e gravar dados de segurança no controlador escravo SmartGuard. Isto permite que você faça o controle de segurança distribuído pelo intertravamento de vários controladores através de CIP Safety nas redes DeviceNet.
3	Como escravo padrão DeviceNet, o controlador SmartGuard 600 pode parecer com um módulo padrão de E/S distribuída e responder a mensagens explícitas de forma que os mestres padrão DeviceNet como ControlLogix, SLC 500 ou PLC-5 ou um IHM possam ler e gravar informações para e do controlador SmartGuard 600. Isto facilita a coordenação com sua aplicação CLP padrão, incluindo a exibição das informações do sistema de segurança em um IHM.
4	Como um alvo padrão EtherNet/IP, o controlador SmartGuard 600 se comunica com um originador padrão EtherNet/IP, tal como um controlador CompactLogix ou MicroLogix ou um dispositivo IHM. O controlador SmartGuard não suporta CIP Safety em comunicação EtherNet/IP. Como resultado, o controlador SmartGuard não pode controlar os módulos de segurança 1791ES. Todo o controle de segurança deve ser feito na rede DeviceNet conforme mostrado nos números 1 e 2 acima.
5	Como dispositivo de ponte EtherNet/IP limitado, o controlador SmartGuard 600 permite que as ferramentas de programação façam a ponte para o DeviceNet para visualizar e programar o controlador SmartGuard 600 e configurar outros dispositivos DeviceNet.

Hardware

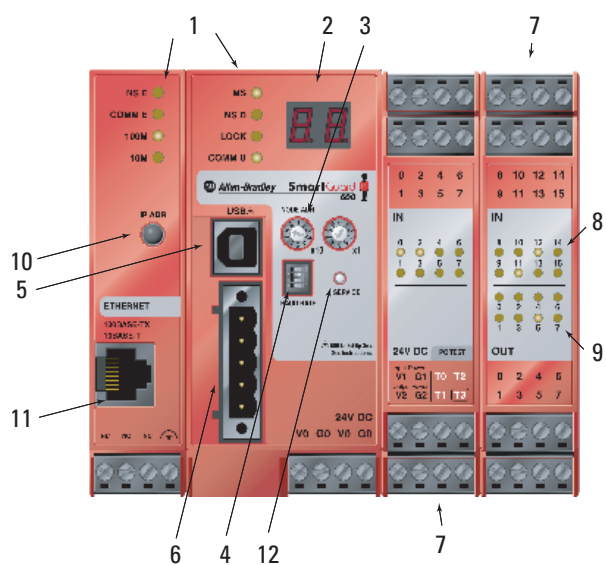
O controlador SmartGuard 600 (códigos de catálogo 1752-L24BBB e 1752-L24BBBE) apresenta 16 entradas digitais, 8 saídas digitais, 4 origens de teste por pulso e conexões USB e o protocolo DeviceNet Safety. E ainda, o controlador 1752-L24BBBE oferece conectividade EtherNet/IP.

Funções do controlador SmartGuard 600 (código de catálogo 1752-L24BBB)



Número	Função
1	Indicadores de status do módulo
2	Tela alfanumérica
3	Chaves de endereço do nó
4	Chaves de taxa de transmissão
5	Porta USB
6	Conector de comunicação do DeviceNet
7	Conectores de terminal
8	Indicadores de status de entrada
9	Indicadores de status de saída
10	Chave de serviço

Funções do controlador SmartGuard 600 (código de catálogo 1752-L24BBBE)



Número	Função
1	Indicadores de status do módulo
2	Tela alfanumérica
3	Chaves de endereço do nó
4	Chaves de taxa de transmissão
5	Porta USB
6	Conector de comunicação DeviceNet
7	Conectores de terminal
8	Indicadores de status de entrada
9	Indicadores de status de saída
10	Chave de exibição do endereço IP
11	Conector Ethernet
12	Chave de serviço

Entradas de segurança

O controlador tem 16 entradas de segurança local que suportam as funções descritas abaixo.

- Diagnóstico do circuito de entrada – origens de pulso de teste podem ser usadas para monitorar circuitos internos, equipamentos externos e fiação externa.
- Atrasos na energização e desenergização de entrada – é possível definir filtros de tempo de entrada de 0 a 126 ms em múltiplos do tempo do ciclo do controlador. Definir atrasos na energização e desenergização ajuda a reduzir a influência da trepidação de contatos e do ruído externo.
- Modo em canal duplo – é possível definir o modo em canal duplo para pares de entradas locais relacionadas. Quando o modo em canal duplo está definido, as discrepâncias de tempo nas alterações de dados ou sinais de entrada entre duas entradas locais emparelhadas podem ser avaliadas.

Saídas de segurança

O controlador tem oito saídas de segurança local que suportam as funções descritas abaixo.

- Diagnóstico do circuito de saída – os pulsos de teste podem ser usados para diagnosticar os circuitos internos do controlador, os equipamentos externos e a fiação externa.
- Detecção de sobrecorrente e proteção – para proteger o circuito, uma saída é bloqueada quando uma sobrecorrente é detectada.
- Modo em canal duplo – as duas saídas emparelhadas podem ser definidas em um estado de segurança sem depender do programa do usuário quando ocorre um erro em uma das duas saídas locais emparelhadas.

Origens de pulso de teste

Quatro saídas de teste independentes são normalmente usadas com as entradas de segurança. Elas também podem ser definidas para serem usadas como sendo terminais de saída de sinal padrão. As saídas de pulso de teste suportam as seguintes funções.

- Detecção de sobrecorrente e proteção – para proteger o circuito, uma saída é bloqueada quando uma sobrecorrente é detectada.
- Monitoração de corrente da lâmpada muting – a desconexão pode ser detectada apenas no terminal T3.

Comunicação

O controlador pode agir como um mestre ou escravo DeviceNet Safety, como um escravo padrão DeviceNet ou como um controlador independente quando a comunicação DeviceNet é desabilitada. Um controlador SmartGuard simples pode funcionar simultaneamente como um mestre de segurança, um escravo de segurança ou um escravo padrão.

As mensagens explícitas podem ser usadas para ler as informações sobre o status do controlador. O programa do usuário pode ser configurado para enviar mensagens explícitas do programa do usuário. As mensagens podem ser roteadas entre as redes DeviceNet e EtherNet/IP.

A porta USB pode ser usada para programar o controlador SmartGuard e configurar os equipamentos na rede do DeviceNet. O SmartGuard fornece uma capacidade limitada de passagem de USB para o DeviceNet, para fins de programação e de configuração. Quando usado no modo independente, o controlador comunica-se com o software de configuração por meio da comunicação USB.

Configuração e programação

Use o software RSNetWorx para DeviceNet, versão 8.0 (mínima) ou posterior (a versão 9.1 é recomendada), para configurar, programar e monitorar o status do controlador 1752-L24BBB. Use o software RSNetWorx para DeviceNet, versão 9.1 ou posterior, para configurar, programar e monitorar o status do controlador 1752-L24BBBE. Com o software RSNetWorx para DeviceNet, é possível configurar o controlador usando a porta USB do controlador SmartGuard ou através da rede DeviceNet ou EtherNet/IP.

Também será necessário o software RSLinx, versão 2.55 ou posterior, que permite que o controlador 1752-L24BBBE seja configurado em EtherNet/IP.

O Logic Editor é aberto dentro do software RSNetWorx for DeviceNet. As operações de lógica básica como, por exemplo, AND e OR, além dos blocos de funções como, por exemplo, ESTOP e a cortina de luz, são suportadas. No máximo 254 funções lógicas e blocos de funções podem ser usados em um máximo de 32 páginas de programação. É possível proteger por senha os dados de configuração e os arquivos de projeto.

Monitoração de erros e status

As informações sobre o status interno do controlador e os dados de E/S podem ser monitoradas on-line usando o software RSNetWorx para DeviceNet com uma conexão USB, ou de rede DeviceNet, ou de rede EtherNet/IP.

Os indicadores de status e a tela alfanumérica do controlador fornecem informações sobre o status e o erro. Quando a chave de serviço na parte frontal do controlador é pressionada, a tela alfanumérica mostra os dois dígitos da assinatura da configuração de segurança do controlador por vez de um total de dez pares de números.

Quando a chave exibição do endereço IP é pressionada por 1 segundo ou mais, a tela mostra o endereço EtherNet/IP que está configurado.

Os erros detectados pelo controlador são gravados em um registro de histórico dos erros e em um registro de histórico EtherNet/IP, juntamente com a hora em que o erro ocorreu. (O tempo é mostrado como de operação total desde que o controlador foi energizado.)

Conceito de segurança do controlador

O controlador SmartGuard 600 é certificado para uso em aplicações de segurança até e inclusive o nível de integridade de segurança (SIL) 3, de acordo com a IEC 61508, nível de desempenho PL(e) de acordo com a ISO 13849-1, e a categoria (CAT) 4, de acordo com a EN 954-1, onde o estado desenergizado é o estado de segurança. As especificações da aplicação de segurança incluem a avaliação da probabilidade da taxa de falhas (PFD e PFH), os cálculos do tempo de reação do sistema e os testes de verificação funcionais que atendem aos critérios SIL 3. Você deve ler, compreender e atender a essas especificações antes de operar um sistema de segurança SIL 3 ou CAT 4 com base no controlador SmartGuard 600.

O controlador usa os seguintes mecanismos para suportar a integridade dos dados de segurança.

- Número de segurança da rede (SNN) – um número exclusivo que identifica a rede de segurança. Os nós de segurança CIP devem ter um SNN e um endereço de rede DeviceNet únicos.
- Assinatura da configuração – a combinação de um número de identificação, data e hora que identifica de maneira exclusiva uma configuração específica de um equipamento de segurança.
- Trava de configuração (ou trava de segurança) – após o download e a verificação dos dados da configuração, é possível travar a configuração do controlador para impedir que ela seja modificada.
- Proteção por senha – a configuração do controlador pode ser protegida pelo uso de uma senha opcional. Caso você defina uma senha, download, travar, soltar, remover e alterar o status do controlador exige uma senha.

Deve-se criar e documentar uma distinção clara, lógica e visível entre a segurança e quaisquer porções padrão da aplicação.

Recurso adicional

Consulte o Manual de referência de segurança dos controladores SmartGuard 600, publicação [1752-RM001](#), para obter informações sobre as especificações do sistema de segurança SIL 3 e CAT 4, inclusive os intervalos de teste de verificação funcional, o tempo de reação do sistema e os valores PFD/PFH.

Observações:

Instalação e aplicação da fiação no controlador SmartGuard 600

Introdução

Tópico	Página
Informações gerais sobre a segurança	23
Compreendendo o endereçamento do nó	26
Ajustando o endereço do nó	26
Ajustando o parâmetro da faixa de comunicação	27
Instalação do controlador SmartGuard	29
Aterramento do controlador SmartGuard	30
Conexão de uma fonte de alimentação	30
Aplicação da fiação ao controlador SmartGuard 600	34

Informações gerais sobre a segurança

ATENÇÃO



Ambiente e Gabinete

Este equipamento deve ser usado em ambiente industrial com nível poluidor 2, em aplicações de categoria de sobretensão II (conforme definição na publicação IEC 60664-1), em 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 outros ambientes devido a perturbações conduzidas assim como irradiadas.

O equipamento é fornecido como sendo do tipo aberto. Ele 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 as propriedades retardantes de chamas apropriadas para evitar ou minimizar a extensão da chama, conforme a taxa de extensão da chama ou 5VA, V2, V1, V0 (ou equivalente) caso não seja 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:

- Orientações de fiação e aterramento de automação industrial, publicação Allen-Bradley [1770-4.1](#).
- Publicações NEMA Standards 250 e IEC 60529, conforme aplicável, para obter explicações sobre os níveis de proteção fornecidos pelos diferentes tipos de gabinete.

Aprovação de área classificada na América do Norte

The following information applies when operating this equipment in hazardous locations		Informations sur l'utilisation de cet équipement en environnements dangereux	
Products marked CL I, DIV 2, GP A, B, C, D are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest T number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.		Les produits marqués CL I, DIV 2, GP A, B, C, D ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.	
WARNING 	EXPLOSION HAZARD - Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. - Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. - Substitution of components may impair suitability for Class I, Division 2. - If this product contains batteries, they must only be changed in an area known to be nonhazardous.	AVERTISSEMENT 	RISQUE D'EXPLOSION - Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. - Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. - La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. - S'assurer que l'environnement est classé non dangereux avant de changer les piles.

As seguintes informações aplicam-se quando este equipamento está em operação em áreas classificadas

Os produtos marcados como CL I, DIV 2, GP A, B, C, D só são adequados ao uso nos grupos A, B, C, D de divisão 2 e classe I, áreas classificadas e locais não classificadas. Cada produto é fornecido com indicações na placa de identificação informando o código de temperatura da área classificada. Durante a combinação de produtos dentro de um sistema, o código de temperatura mais adversa (menor número T) 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 EXPLOÇÃO - 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. Prenda qualquer conexão externa necessária neste equipamento por meio de parafusos, travas deslizantes, conectores rosqueados ou outros dispositivos fornecidos com este produto. - A substituição de componentes pode prejudicar a adequação com a Classe I, Divisão 2. - Caso este produto contenha baterias, estas só devem ser trocadas em uma área reconhecidamente não classificada.
---	---

ATENÇÃO



Sistemas eletrônicos programáveis de segurança (PES)

O pessoal responsável pela aplicação de sistemas eletrônicos programáveis relacionados à segurança (PES) deverá estar atento às especificações de segurança na aplicação do sistema e deverá estar treinado quanto ao seu uso.

ATENÇÃO**Evitar descarga eletrostática**

Este equipamento é sensível à descarga eletrostática, capaz de causar danos internos e afetar a operação normal. Siga estas orientações ao lidar com o equipamento.

- Toque em um objeto aterrado para descarregar o potencial de estática.
- Coloque uma pulseira de aterramento aprovada.
- Não toque nos conectores ou pinos nas placas do componente.
- Não toque nos componentes do circuito dentro do equipamento.
- Use uma estação de trabalho sem estática, caso haja uma disponível.
- Armazene o equipamento em uma embalagem sem estática apropriada quando ele não estiver sendo usado.

ATENÇÃO**Proteção contra detritos**

Não remova a proteção contra detritos até que o controlador e todos os demais equipamentos próximos a ele sejam instalados e a fiação esteja completa.

Assim que a fiação estiver completa, remova a proteção contra detritos. Deixar de removê-la antes de colocá-lo em operação pode causar superaquecimento.

ATENÇÃO

Podem ocorrer ferimentos graves por conta da perda da função de segurança necessária.

- Não use saídas de teste como saídas de segurança.
- Não use dados de E/S padrão do DeviceNet ou dados de mensagem explícita como dados de segurança.
- Não use indicadores de status para operações de segurança.
- Não conecte cargas superiores ao valor classificado às saídas de segurança ou saídas de teste.
- Ligue o controlador corretamente para que a linha de 24 Vcc não toque acidentalmente nas saídas.
- Aterre a linha de 0 V da fonte de alimentação para os equipamentos de saída externos de forma que eles não sejam ativados quando a linha de saída de segurança ou a linha de saída de teste for aterrada.
- Não desmonte, repare ou modifique o controlador. Fazer isso pode prejudicar as funções de segurança.

Compreendendo o endereçamento do nó

Para que se comuniquem na rede do DeviceNet, todos os equipamentos exigem endereços próprios. Siga as recomendações abaixo ao atribuir endereços aos dispositivos em sua rede.

Recomendações quanto ao endereço do nó

Dar ao equipamento	Este endereço	Observações
Scanner	0	Caso você tenha vários scanners, dê a eles os endereços menores em sequência.
Todos os equipamentos na rede, exceto o scanner	1 a 61	Os intervalos entre os endereços são permitidos e não têm efeito sobre o desempenho do sistema. Deixar intervalos dá a você mais flexibilidade no desenvolvimento do sistema.
Estação de trabalho do RSNetWorx for DeviceNet	62	Caso você conecte um computador diretamente à rede do DeviceNet, use o endereço 62 para o computador ou equipamento de formação de ponte/enlace.
Sem equipamento	63	Deixe o endereço 63 aberto. Trata-se do lugar em que um nó não comissionado costuma entrar na rede.

A rede padrão do DeviceNet atribui a prioridade de comunicação com base no número do nó do equipamento. Quanto menor for o número do nó, maior será a prioridade de comunicação do equipamento. Essa prioridade torna-se importante quando vários nós estão tentando se comunicar na rede ao mesmo tempo.

Os nós de segurança do DeviceNet têm prioridade adicional na rede, independentemente do número do nó. A comunicação DeviceNet Safety dos equipamentos com números de nó menores tem prioridade sobre a comunicação DeviceNet Safety dos equipamentos com números de nó maiores.

Ajustando o endereço do nó

Defina o endereço do nó antes de instalar o controlador.

IMPORTANTE

Desligue a alimentação do controlador antes de ajustar o parâmetro do nó do endereço ou a faixa de comunicação usando as chaves.

Não altere as configurações da chave enquanto a fonte de alimentação estiver ligada. O controlador detectará isso como sendo uma alteração na configuração e alternará para o modo de cancelamento.

Use uma chave de fenda pequena para definir o endereço do nó usando as duas chaves rotativas no painel frontal do controlador. Tome cuidado para não arranhar as chaves. Os valores entre 00 e 63 são válidos. A configuração padrão é de 63.

Siga estas etapas para definir o endereço do nó.

1. Defina o dígito da dezena do endereço do nó girando a seccionadora da esquerda.
2. Defina o dígito da unidade girando a seccionadora da direita.

3. Para permitir que o endereço do nó seja definido usando o software RSNetworx para DeviceNet, defina as chaves rotativas para um valor entre 64 e 99.

IMPORTANTE

Ocorrerá um erro de duplicação no endereço do nó se o mesmo endereço for definido para mais de um nó.

Ajustando o parâmetro da faixa de comunicação

Defina a faixa de comunicação antes de instalar o controlador.

IMPORTANTE

Desligue a alimentação do controlador antes de ajustar o parâmetro do nó do endereço ou a faixa de comunicação usando as chaves.

Não altere as configurações da chave enquanto a fonte de alimentação estiver ligada. O controlador detectará isso como sendo uma alteração na configuração e alternará para o modo de cancelamento.

Comunicação DeviceNet

A faixa de comunicação padrão de uma rede do DeviceNet é de 125 Kbps.

Caso você opte por usar uma faixa de comunicação diferente, o comprimento da linha tronco e os tipos de cabo determinam quais faixas de comunicação a aplicação é capaz de suportar.

Faixas de comunicação do DeviceNet e comprimentos de cabo

Faixa de comunicação	Distância, máx.			Comprimento da linha secundária acumulado
	Cabo liso	Cabo espesso	Cabo coaxial fino	
125 Kpbs	420 m (1378 pés)	500 m (1640 pés)	100 m (328 pés)	156 m (512 pés)
250 Kpbs	200 m (656 pés)	250 m (820 pés)	100 m (328 pés)	78 m (256 pés)
500 Kpbs	75 m (246 pés)	100 m (328 pés)	100 m (328 pés)	39 m (128 pés)

Defina a taxa de comunicação usando a minisseletores na parte frontal do controlador.

Minisseletores da faixa de comunicação



Ajuste de parâmetros da minisseletores

Pino da minisseletores				Faixa de comunicação
1	2	3	4	
Desenergizado	Desenergizado	Desenergizado	Desenergizado	125 Kbps
ON	Desenergizado	Desenergizado	Desenergizado	250 Kbps
Desenergizado	ON	Desenergizado	Desenergizado	500 Kbps
ON	ON	Desenergizado	Desenergizado	Definido pelo software
ON ou OFF	ON ou OFF	ON	Desenergizado	Definido pelo software
ON ou OFF	ON ou OFF	ON ou OFF	ON	Deteção automática de taxa de transmissão

IMPORTANTE

Caso você altere a faixa de comunicação da rede, verifique se todos os equipamentos foram alterados para a nova faixa de comunicação. Faixas de comunicação misturadas produzem erros de comunicação.

Caso você defina os demais equipamentos para taxa de transmissão automática, pelo menos um dos equipamentos na rede deve ter uma faixa de comunicação estabelecida. Se você definir todos os equipamentos na rede para taxa de transmissão automática, eles não poderão estabelecer uma faixa de comunicação e não se comunicarão entre si.

Comunicação Ethernet

Recomendamos a conexão do módulo à rede através de um switch Ethernet de 100 Mbps, o que ajudará a reduzir colisões e pacotes perdidos e aumentar a largura da banda.

O controlador 1752-L24BBBE é enviado com BOOTP habilitado para a configuração do endereço IP. Pode-se usar qualquer servidor BOOTP disponível comercialmente. Se não tiver recursos de servidor BOOTP na sua rede, faça o download grátis do servidor BOOTP da Rockwell Automation em <http://www.rockwellautomation.com/rockwellsoftware/download/>.

Para configurar o endereço IP usando o utilitário BOOTP Rockwell Automation, consulte a [página 54](#).

A seguinte tabela fornece informações adicionais EtherNet/IP.

Para informações detalhadas sobre a comunicação EtherNet/IP, consulte Solução de aplicação e desempenho EtherNet/IP, publicação [ENET-AP001](#).

Informações gerais EtherNet/IP

Atributo	Valor
Número de pacotes CIP	2
Largura de banda de comunicação de unidade permissível	3000 pps ⁽¹⁾
Comunicação de mensagem explícita	502 B ⁽²⁾

⁽¹⁾ PPS significa pacotes por segundo. Indica o número de pacotes enviados ou recebidos que podem ser processados por segundo.

⁽²⁾ O comprimento máximo de mensagem para conexão de classe 3 e conexão UCM.

Instalação do controlador SmartGuard

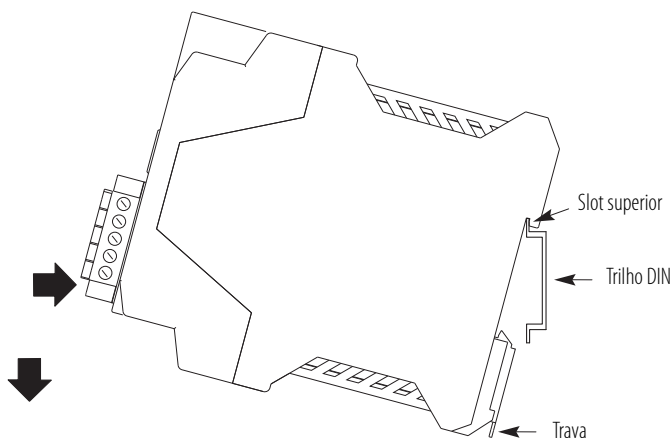
IMPORTANTE

Para obter um resfriamento efetivo:

- instale o controlador em um trilho DIN horizontal. Não instale o controlador verticalmente.
- deixe um espaço de pelo menos 50 mm (2 pol.) acima e abaixo do controlador e 5 mm (0,2 pol.) nas laterais.
- selecione um local em que haja fluxo de ar constante ou use um ventilador adicional.
- não instale o controlador por cima de um equipamento em aquecimento.

O controlador não pode ser instalado no painel. Siga estas etapas para instalar o controlador em um trilho DIN EN50022-35x7,5 ou EN50022-35x15.

1. Prenda o slot superior por cima do trilho DIN.
2. Encaixe a parte inferior do controlador na posição enquanto pressiona o controlador para baixo contra a parte superior do trilho.



3. Conecte as placas de terminação a cada uma das extremidades do trilho DIN.

Para remover o controlador do trilho DIN, use uma chave de fenda para retirar a trava e soltar o controlador do trilho. O controlador 1752-L24BBB tem uma trava e o controlador 1752-L24BBBE tem duas travas no fundo do controlador.

Aterramento do controlador SmartGuard

ATENÇÃO

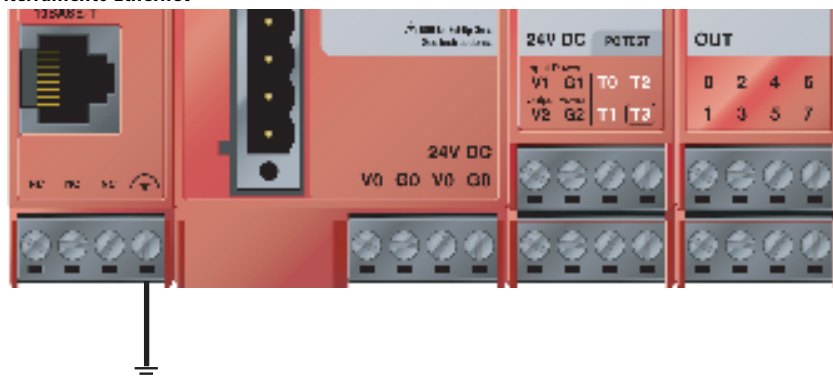


Este produto é aterrado pelo trilho DIN ao aterramento do rack. Use o trilho DIN de aço zincado amarelo para garantir um aterramento adequado. O uso de outros materiais no trilho DIN (por exemplo, alumínio ou plástico) que podem ser corroídos, ou oxidar, ou são maus condutores, pode resultar em um aterramento impróprio ou intermitente. Fixe o trilho DIN à superfície de instalação aproximadamente a cada 200 mm (7,8 pol.) e use os postes adequadamente.

Você deve fornecer um caminho de aterramento aceitável para cada equipamento da aplicação. Aterre o controlador de maneira funcional por meio de sua conexão de alimentação V0/G0.

E ainda, se estiver usando o controlador 1752-L24BBBE, deve-se conectar o terminal de terra Ethernet a um aterramento aceitável.

Aterramento Ethernet



Consulte Orientações de fiação e aterramento de automação industrial, publicação [1770-4.1](#), para informações adicionais.

Conexão de uma fonte de alimentação

A energia do controlador é fornecida por meio de uma fonte de alimentação externa de 24 Vcc. O tempo de retenção da saída deve ser de 20 ms ou mais.

Para respeitar a Diretriz de baixa tensão da Comunidade Européia (LVD), as conexões do DeviceNet e a E/S devem ser alimentadas por uma fonte cc compatível com a baixa tensão extra de segurança (SELV) ou a baixa tensão extra protegida (PELV).

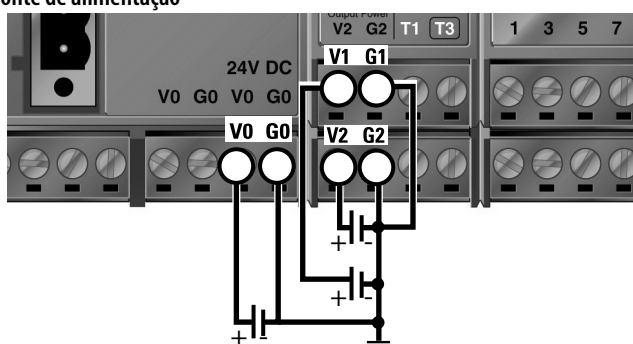
Para respeitar as restrições de UL, as conexões do DeviceNet e a E/S devem ser alimentadas por fontes CC cujos circuitos secundários são isolados do circuito primário por isolamento duplo ou isolamento reforçado. A fonte de alimentação cc deve atender às especificações dos circuitos de classe 2 ou dos circuitos de corrente/tensão limitada definidos na UL 508.

DICA

As seguintes fontes de alimentação Rockwell Automation 1606 são compatíveis com SELV e PELV, além de atenderem às especificações de isolamento e de tempo de desenergização de saída do controlador SmartGuard 600:

- 1606-XLP30E • 1606-XLP72E • 1606-XLSDNET4
- 1606-XLP50E • 1606-XLP95E
- 1606-XLP50EZ • 1606-XLDNET4

O controlador SmartGuard tem três pares de terminais V/G que exigem uma conexão de alimentação. Há dois pares V0/G0, mas como eles estão conectados internamente, você só precisa conectar um par V0/G0. É possível usar o outro par para distribuir a energia aos demais equipamentos.

Conexões da fonte de alimentação

Fazendo conexões de comunicação

ADVERTÊNCIA

Não conecte nem desconecte o cabo de comunicação com energia aplicada a esse controlador ou a qualquer outro equipamento na rede porque pode ocorrer um arco elétrico. 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.

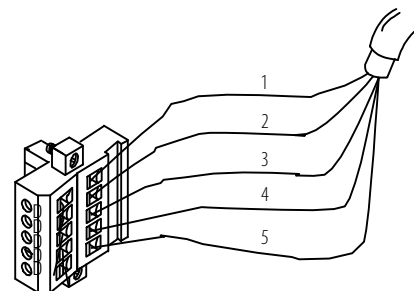
É possível configurar a rede e o controlador na rede do DeviceNet usando uma placa 1784-PCD dentro do microcomputador e o software RSNetWorx para DeviceNet. Você também pode configurar a rede e o controlador usando a porta USB do controlador e o software RSNetWorx para DeviceNet. E ainda, pode-se configurar o controlador usando o software RSNetWorx para DeviceNet conectando a porta EtherNet/IP e roteando até a rede DeviceNet.

Conexão à porta do DeviceNet

Siga estas etapas para se conectar à porta do DeviceNet.

1. Aplique os fios ao conector de acordo com as cores no conector.

Fio Núm.	Cor do fio	Conecta a
V+	Vermelho	V+
CAN H	Branco	CAN H
Dreno	—	Dreno
CAN L	Azul	CAN L
V-	Preto	V-



2. Ligue o conector à porta do DeviceNet.
3. Aperte os parafusos com 0,25 a 0,3 N•m (2,21 a 2,65 lb•pol.).

Para obter informações detalhadas sobre a conexão DeviceNet, consulte o Guia de instalação do projeto de mídia DeviceNet, publicação [DNET-UM072](#). Também consulte Orientações de fiação e aterramento de automação industrial, publicação [1770-4.1](#).

Conexão à porta USB

Ligue o conector de comunicação USB ao microcomputador quando quiser configurar a rede e o controlador usando o software RSNetWorx para DeviceNet. Use um cabo do tipo macho/macho USB-A para USB-B disponível no mercado para estabelecer a conexão.

ATENÇÃO



Para reduzir o potencial de interferência eletromagnética, o comprimento do cabo USB deve ser menor que 3 m (10 pés).

A porta USB tem apenas finalidades de programação e não deve ser usada em uma conexão permanente.

ADVERTÊNCIA



Caso você conecte ou desconecte o cabo USB com energia aplicada ao módulo ou a qualquer outro equipamento na rede USB, pode ocorrer um arco elétrico. 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.

Conectando-se à porta Ethernet

Dependendo de onde planeja rotear seu cabo, deve-se selecionar o cabo correto para o ambiente. Cabos blindados têm melhor desempenho que cabos não blindados em ambientes industriais. Em particular, se a sua aplicação estiver em um ambiente de alto ruído ou o seu cabo precisar estar em proximidade a fontes de radiação de ruído, então deve-se planejar o uso de cabos blindados.

Devem-se considerar cabos blindados se a sua aplicação incluir um ou mais dos seguintes:

- controle de solda no local
- centro de controle de motores
- inversores maiores que 10 HP
- indução de processos de solda
- proximidade a radiação RF de alta energia
- processos eletrostáticos
- dispositivos de alta corrente (maiores que 100 A)

IMPORTANTE

A blindagem tem um papel importante no fornecimento de imunidade a ruído para o seu sistema. Entretanto, um cabo blindado que não for instalado corretamente pode causar problemas devido a defasagens de tensão no seu sistema de aterramento. Para ajudar a minimizar os efeitos de defasagens de aterramento, será necessário isolar a blindagem em uma extremidade do cabo. Neste caso, a blindagem deve ser isolada no dispositivo, não na chave.

Use um conector RJ45 para conectar o controlador à rede EtherNet/IP. Quando conectar o controlador SmartGuard a uma chave ou hub, use um cabo Ethernet padrão. Quando conectar o controlador SmartGuard diretamente ao seu microcomputador ou uma placa NIC, use um cabo atravessado (de modem nulo).

ATENÇÃO



O comprimento do cabo deve ser menor que 100 m (328 pés) entre o hub e os nós.

ADVERTÊNCIA



Se conectar ou desconectar o cabo de Ethernet com energia aplicada ao controlador ou a qualquer outro equipamento na rede, pode ocorrer um arco elétrico. 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.

Colocação do pino Ethernet

Núm. do pino	Nome do pino	Colocação do pino
8	Não usado	
7	Não usado	
6	RD–	
5	Não usado	
4	Não usado	
3	RD+	
2	TD–	
1	TD+	

Aplicação da fiação ao controlador SmartGuard 600

Use cabos de 30 m (98 pés) ou menos.

Informações gerais sobre a fiação

Atributo	Valor
Tipo de fio	Cobre
Categoria de fiação ⁽¹⁾	2 – nas portas de alimentação, sinal e comunicação
Bitola do cabo	Para a fonte de alimentação e a E/S, use um fio sólido de 0,2 a 2,5 mm ² (12 a 24 AWG) ou um fio flexível trançado de 0,34 a 1,5 mm ² (16 a 22 AWG). Antes da conexão, prepare os fios trançados envolvendo-os com ferros com anéis plásticos de isolamento (padrão compatível com DIN 46228-4).
Torque no parafuso do terminal de E/S	0,56 a 0,79 N•m (5 a 7 lb•pol.)

⁽¹⁾ Use estas informações sobre a categoria do condutor para planejar a rota dos cabos. Consulte Orientações de fiação e aterramento de automação industrial, publicação [1770-4.1](#).

Descrições de terminal do controlador

Designação do terminal	Descrição
V0	Borne de alimentação do circuito interno (lógica).
G0	Borne de alimentação do circuito interno (lógica).
V1	Borne de alimentação dos circuitos de entrada e das saídas de teste.
G1	Borne de alimentação dos circuitos de entrada e das saídas de teste.
V2	Borne de alimentação das saídas de segurança.
G2	Borne de alimentação das saídas de segurança.
INO a IN15	Terminais das entradas de segurança.
T0 a T3	Estes são os terminais de saída de teste capazes de fornecer origens de teste por pulso para as entradas de segurança IN0 a IN15. T3 também pode suportar a detecção do desligamento do fio e a detecção de lâmpada queimada de uma carga como, por exemplo, uma lâmpada muting.
OUT0 a OUT7	Terminais das saídas de segurança.

ADVERTÊNCIA



Caso você conecte ou desconecte a fiação enquanto a energia no lado do campo está aplicada, pode ocorrer um arco elétrico. 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.

ADVERTÊNCIA



Caso você conecte ou desconecte o borne removível (RTB) enquanto a energia no lado do campo está aplicada, pode ocorrer um arco elétrico. 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

Prepare os fios trançados envolvendo-os com ferros com anéis plásticos de isolamento (compatíveis com o padrão DIN 46228-4). Os ferros com aparência semelhante, mas não compatíveis, talvez não correspondam ao borne no controlador.

Fiação dos dispositivos de entrada

ATENÇÃO

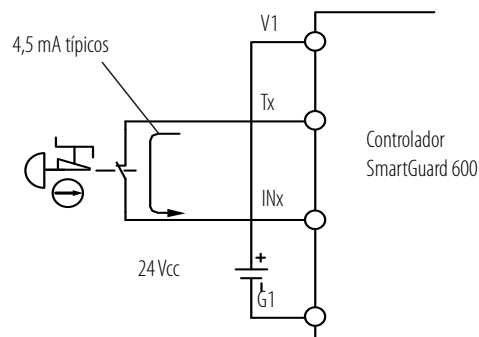


Aplicar uma tensão cc inadequada ou qualquer tensão ca pode resultar em uma perda da função de segurança, danos ao produto ou ferimentos graves. Aplique de maneira apropriada apenas a tensão especificada às entradas do controlador.

Os dispositivos de entrada com saídas de contato mecânico como, por exemplo, os botões de parada de emergência e as chaves fim de curso de segurança, usam um terminal de entrada de segurança e um terminal de saída de teste. Isso habilita o circuito a alcançar uma classificação de categoria 4.

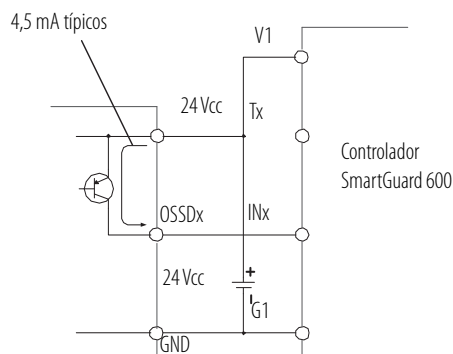
Quando os dispositivos de segurança estão conectados via saídas de teste a um circuito de entrada no controlador SmartGuard, recomendamos que o comprimento do fio seja de 30 m (98,4 pés) ou menos.

Dispositivos de entrada com saídas de contato mecânico



Os dispositivos como, por exemplo cortinas de luz, com saídas de semiconductor PNP com fonte de corrente enviam um sinal para o terminal de entrada de segurança do controlador SmartGuard 600 e não usam uma saída de teste.

Dispositivos de entrada com saídas de semiconductor PNP



Fiação dos dispositivos de saída

ATENÇÃO



Podem ocorrer ferimentos graves por conta de uma perda das funções de segurança necessárias.

Não conecte cargas superiores ao valor classificado de segurança ou às saídas de teste.

Não use saídas de teste como saídas de segurança.

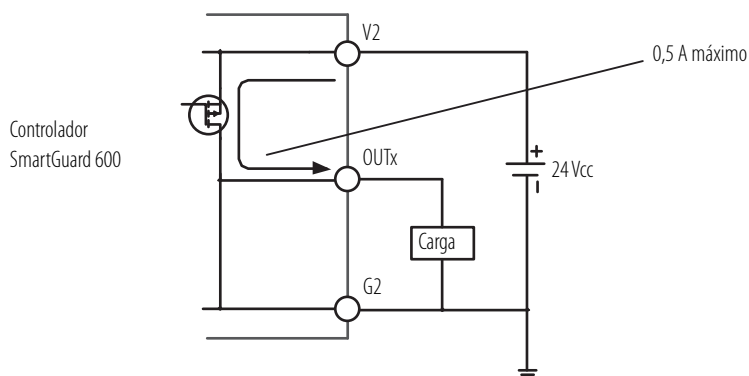
Ligue o controlador corretamente para que as linhas de 24 Vcc não toquem nas saídas de segurança ou de teste.

Não aplique a fonte de alimentação aos terminais de saída de teste.

Aterre a linha de 0 V da fonte de alimentação para os equipamentos de saída externos de forma que eles não sejam ativados quando a linha de saída de segurança ou a linha de saída de teste for aterrada.

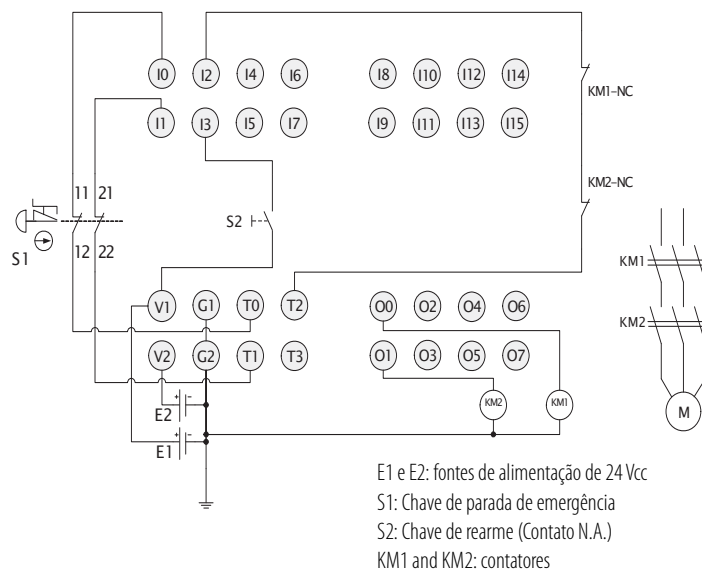
Separe os cabos de E/S das linhas de alta corrente ou de alta tensão.

Fiação do dispositivo de saída



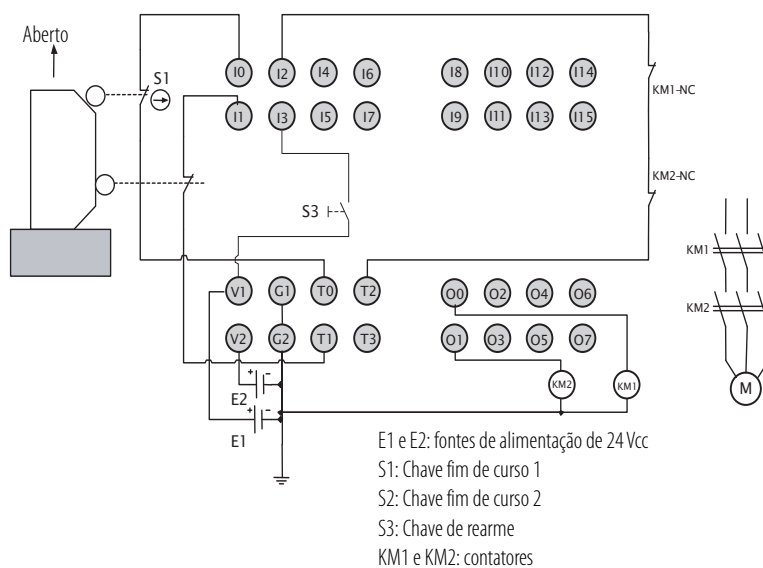
Exemplos de fiação

ESTOP



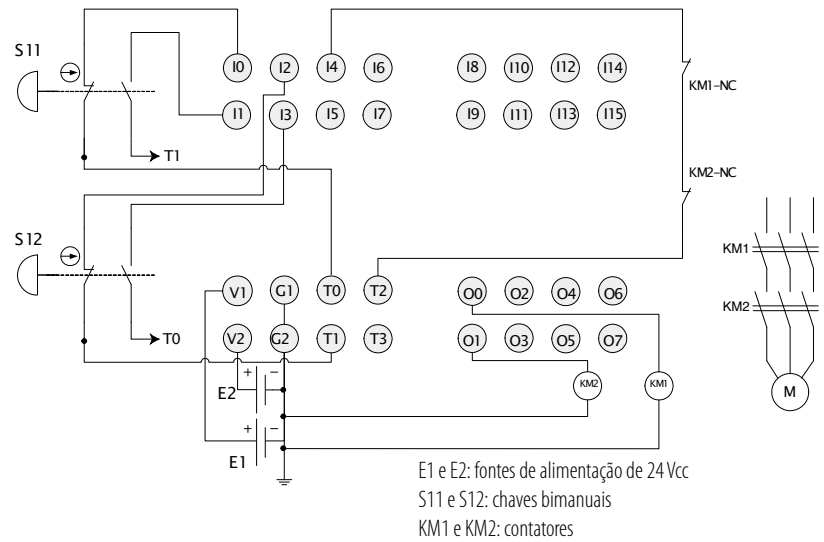
Conecte uma fonte de alimentação de 24 Vcc aos terminais V0 e G0, os terminais da fonte de alimentação dos circuitos internos.

Gate de segurança



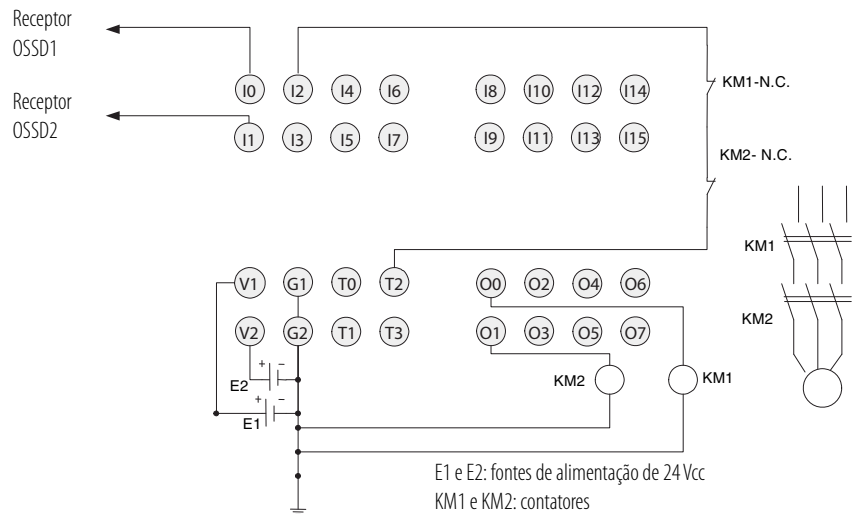
Conecte uma fonte de alimentação de 24 Vcc aos terminais V0 e G0, os terminais da fonte de alimentação dos circuitos internos.

Chave bimanual



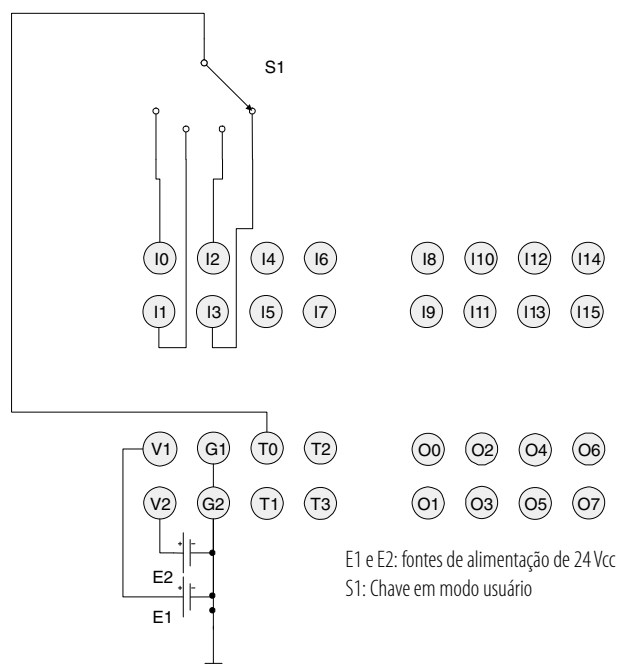
Conecte uma fonte de alimentação de 24 Vcc aos terminais V0 e G0, os terminais da fonte de alimentação dos circuitos internos.

Cortina de luz



Conecte uma fonte de alimentação de 24 Vcc aos terminais V0 e G0, os terminais da fonte de alimentação dos circuitos internos.

Chave em modo usuário



E1 e E2: fontes de alimentação de 24 Vcc
S1: Chave em modo usuário

Conecte uma fonte de alimentação de 24 Vcc aos terminais V0 e G0, os terminais da fonte de alimentação dos circuitos internos.

Ajuste da rede do DeviceNet

Introdução

Tópico	Página
Conexão de um computador à rede DeviceNet	41
Comissionamento de todos os nós	42
Pesquisa da rede	44
Assinatura da configuração	45
Reset de segurança (opcional)	46
Configurando senhas (opcional)	47

Conexão de um computador à rede DeviceNet

Para acessar uma rede:

- conecte-se diretamente à rede.
- conecte-se a uma rede diferente e procure a rede desejada usando um equipamento de enlace.

DICA

É possível observar as redes DeviceNet e EtherNet/IP usando a porta USB do controlador SmartGuard.

A capacidade de formação de ponte entre a USB do SmartGuard e o DeviceNet é limitada. Por exemplo, não é possível configurar 1734-ADN ou módulos POINT I/O. Também não é possível configurar um módulo 1753-DNSI usando o controlador SmartGuard. Use um cartão 1784-PCD para essas operações.

Depois de escolher uma rede:

- instale o cartão de comunicação, se necessário.
- determine todos os parâmetros de rede do computador como, por exemplo, um endereço de rede.
- conecte o computador à rede usando o cabo correto.

IMPORTANTE

Na primeira vez em que conectar um controlador SmartGuard ao microcomputador usando a porta USB, o Windows passará por sua sequência de reconhecimento do equipamento e solicitará a você os drivers USB. O driver está no CD RSLinx Classic, na pasta SmartGuardUSB-KernelDrivers.

Configuração de um driver para a rede

1. Inicie o software RSLinx.
2. Clique em Configure Driver.
3. Na lista Available Driver Types, adicione o driver para a rede.

Rede	Driver
RS-232	Dispositivos RS-232 DF1
EtherNet/IP	Dispositivos Ethernet
DeviceNet	Drivers DeviceNet
USB	Driver SmartGuard USB

4. Configure o driver.

Os ajustes de parâmetros feitos dependem da rede escolhida e da possibilidade de uso de um cartão de comunicação ou módulo de interface.

Verificação do funcionamento do driver

1. Verifique a caixa de diálogo Configure Drivers para ter certeza de que o driver esteja em execução.
2. Feche a caixa de diálogo.
3. Abra a caixa de diálogo RSWho.
4. Clique duas vezes no driver para ver a rede.

Comissionamento de todos os nós

Se não tiver definido especificamente o endereço do nó e a taxa de comunicação de seus equipamentos usando as chaves de hardware, você precisará comissionar todos eles usando o software RSNetWorx para DeviceNet.

Para poder usar a ferramenta Node Commissioning do RSNetWorx for DeviceNet, o computador e os equipamentos do DeviceNet devem ser conectados à rede DeviceNet.

Use a ferramenta Node Commissioning do software RSNetWorx for DeviceNet para definir o endereço do nó e/ou a faixa de comunicação do controlador SmartGuard e os demais equipamentos do DeviceNet.

Siga as orientações na [página 26](#) ao selecionar os endereços de nó para a sua rede DeviceNet.

IMPORTANTE

Para permitir que o endereço do nó seja definido usando a ferramenta Node Commissioning do RSNetWorx para DeviceNet, defina a chave rotativa de endereço do nó no controlador para um valor entre 64 e 99.

Consulte a [página 26](#) para obter informações sobre como definir o endereço do nó usando a chave rotativa.

Siga estas etapas para usar a ferramenta Node Commissioning.

1. No software RSNetWorx para DeviceNet, escolha Tools > Node Commissioning.

2. Clique em Browse na caixa de diálogo Node Commissioning para selecionar um dispositivo pesquisando a rede.

Pode-se procurar na porta USB SmartGuard ou na porta Ethernet/IP para alcançar a porta DeviceNet.

3. Selecione a rede do DeviceNet no painel à esquerda.
4. Selecione o equipamento que você deseja comissionar no painel à direita e clique em OK.
5. Selecione o valor desejado caso você queira alterar a faixa de comunicação do equipamento.

IMPORTANTE

A faixa de comunicação do equipamento não será atualizada até que ele seja desligado e ligado, ou reinicializado.

6. Na caixa de diálogo Node Commissioning, digite o novo endereço do equipamento e clique em Apply.

Uma mensagem de confirmação informa se a operação estava correta.

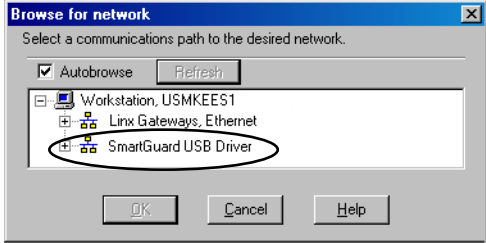
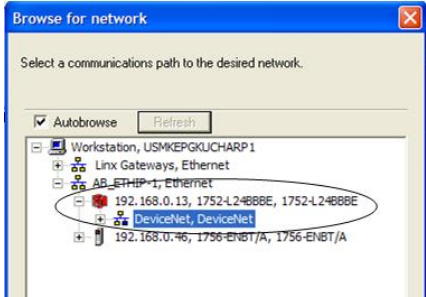
IMPORTANTE

Para alterar o endereço do nó de um equipamento de segurança, você deve primeiro reinicializar o número da rede de segurança (SNN) para um estado não inicializado realizando um reset de segurança conforme a descrição na [página 46](#).

Pesquisa da rede

Siga estas etapas para pesquisar a rede.

1. Determine o tipo de conexão.

Caso você esteja usando este tipo de conexão	Faça o seguinte:
Rede DeviceNet	Vá para a etapa 2.
Porta USB	Siga estas etapas para configurar um caminho para a rede do DeviceNet. A. No menu Network, escolha Properties. B. Na caixa de diálogo DeviceNet, clique em Set Online Path. C. Na caixa de diálogo Browse for Network, selecione o caminho desejado e clique em OK. 
Rede EtherNet/IP	Siga estas etapas para configurar um caminho para a rede do DeviceNet. A. No menu Network, escolha Properties. B. Na caixa de diálogo DeviceNet, clique em Set Online Path. C. Na caixa de diálogo Browse for Network, selecione o caminho desejado e clique em OK. 

2. Clique no ícone online .

3. Aguarde a conclusão da operação de pesquisa da rede.

Enquanto a rede for pesquisada, todos os equipamentos dela aparecerão no software RSNetWorx for DeviceNet.

4. Verifique se todos os nós estão visíveis.

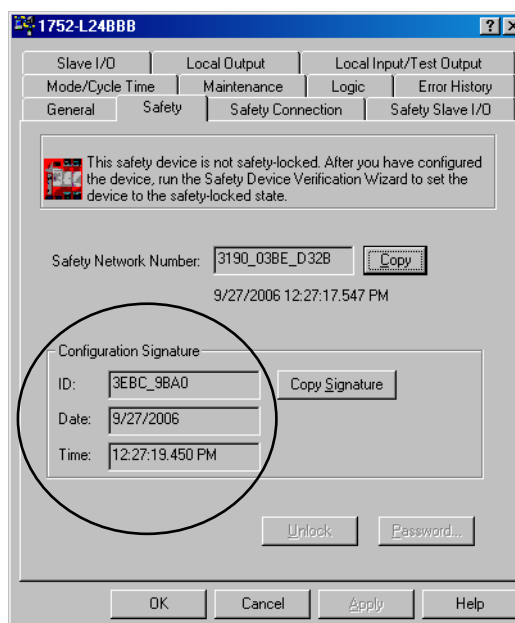
5. Salve o projeto no software RSNetWorx for DeviceNet.

Assinatura da configuração

Cada dispositivo de segurança tem uma assinatura de configuração exclusiva, que identifica a configuração a fim de verificar a integridade dos dados da configuração durante os downloads, o estabelecimento da conexão e a substituição do módulo.

A assinatura da configuração é composta de um número de identificação, uma data e hora, além de ser definida automaticamente pelo software RSNetWorx for DeviceNet durante a aplicação de uma atualização de configuração ao equipamento. A assinatura da configuração é encontrada na guia Safety da caixa de diálogo Device Properties. Ela também é exibida na tela alfanumérica, um caractere por vez, quando a chave do serviço é pressionada.

Assinatura da configuração do controlador SmartGuard 600

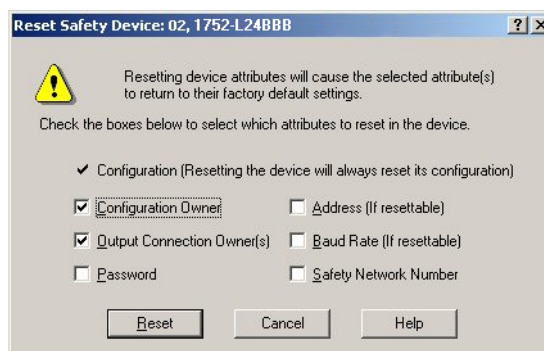


A assinatura de configuração é lida durante cada busca e sempre que a caixa de diálogo Device Properties é lançada enquanto o software está em modo Online. O software RSNetWorx for DeviceNet compara a assinatura da configuração no arquivo de configuração do equipamento no software (off-line) com a assinatura da configuração no equipamento on-line. Caso as assinaturas da configuração não casem, você é solicitado a carregar a configuração do equipamento on-line ou fazer download da configuração do equipamento no software para resolver a diferença.

Reset de segurança (opcional)

Caso você precise reinicializar os atributos do equipamento de segurança para o estado padrão pronto para ser usado, é possível fazer isso na caixa de diálogo Reset Safety Device.

É possível reinicializar os atributos mostrados na caixa de diálogo Reset Safety Device marcando a caixa de seleção associada. Deixar uma caixa de seleção do atributo desmarcada preserva o ajuste de parâmetro do atributo durante a operação de reset da segurança.



1. Abra a caixa de diálogo Reset Safety Device clicando no equipamento na exibição gráfica do software RSNetWorx para DeviceNet e selecionando Reset Safety Device no menu Device.
2. Marque os atributos que você deseja reinicializar.

Atributo	Comportamento de Reset
Configuração	A configuração do equipamento é apagada em decorrência de uma ação de reset da segurança.
Configuration Owner	Marque a caixa de seleção para reinicializar a leitura de controle da configuração do dispositivo. O software de configuração é sempre a leitura de controle da configuração dos controladores SmartGuard.
Output Connection Owner(s)	Marque a caixa de seleção para reinicializar todas as leituras de controle da conexão de saída existentes. O próximo equipamento que acessar um ponto de conexão de saída depois que o reset de segurança se tornar a leitura de controle da conexão de saída.
Password	Marque a caixa de seleção para reinicializar a senha do equipamento. Você deve conhecer a senha atual do equipamento para reinicializá-la na caixa de diálogo Reset Safety Device.
Address	Marque a caixa de seleção para reinicializar o endereço do nó configurado pelo software do equipamento para 63. Caso o endereço de nó do equipamento tenha sido definido usando as chaves, a operação de reset não tem efeito sobre o endereço do nó.
Baud Rate	Marque a caixa de seleção para reinicializar a taxa de comunicação do equipamento para 125 Kbps. Caso a taxa de comunicação do equipamento tenha sido definida usando as chaves, a operação de reset não tem efeito sobre a taxa de comunicação.
Safety Network Number	Marque a caixa de seleção para reinicializar o número da rede de segurança do equipamento (SNN).

3. Clique em Reset.

Caso o equipamento apresente uma trava de segurança, você é solicitado a primeiro soltá-lo.

ATENÇÃO

Depois de destravado, o equipamento não pode oferecer a garantia de realizar operações de segurança.

Você deve testar e verificar a operação do equipamento, além de executar o Safety Device Verification Wizard para colocar a trava de segurança no equipamento antes de operá-lo em uma aplicação de segurança.

4. Digite a senha quando solicitado, caso você tenha definido uma senha para o equipamento.

Configurando senhas (opcional)

É possível proteger os equipamentos de segurança com uma senha a fim de evitar alterações na configuração do equipamento feitas por pessoal não autorizado. Quando uma senha é definida, as seguintes operações exigem a digitação da senha.

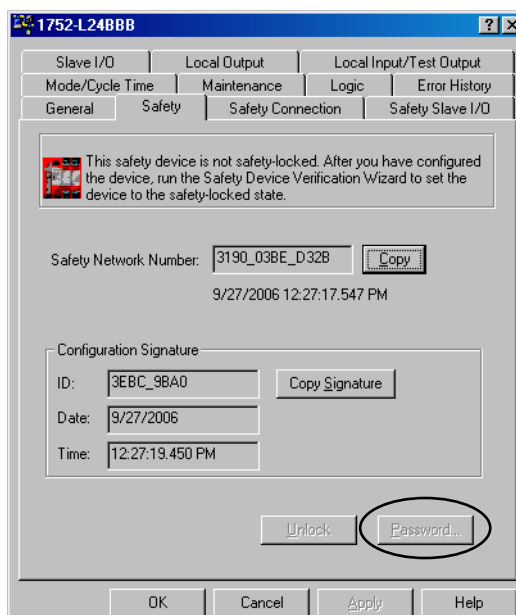
- Download
- Reset da configuração de segurança
- Trava de segurança
- Desproteção

Definição ou alteração de senha

Siga as etapas abaixo para definir uma senha para um módulo.

1. Clique duas vezes no módulo para abrir a caixa de diálogo Device Properties.
2. Selecione a guia Safety.

3. Clique em Password.



DICA

Também é possível acessar a caixa de diálogo Set Device Password:

- clicando no módulo e escolhendo Set Password no menu Device.
- clicando com o botão direito do mouse no módulo e escolhendo Set Password.

4. Digite a senha antiga, caso haja uma.

5. Digite e confirme a nova senha.

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

6. Clique em OK.

Senhas esquecidas

Caso você se esqueça da senha, é possível reinicializá-la.

1. Na guia Safety da caixa de diálogo Device Properties, clique em Password para abrir a caixa de diálogo Set Device Password.
2. Clique em Reset Password.

3. Entre em contato com o suporte técnico da Rockwell Automation e forneça o número de série do equipamento e o código de segurança na caixa de diálogo Reset Password.



4. Digite a senha do fornecedor obtida no suporte técnico da Rockwell Automation na caixa de diálogo Reset Device Password e clique em OK.

Observações:

Configure sua rede EtherNet/IP

Introdução

Tópico	Página
Conexão do computador à rede EtherNet/IP	51
Conectando o controlador SmartGuard 600 à rede EtherNet/IP	53
Formando ponte nas redes	59

Conexão do computador à rede EtherNet/IP

Para acessar a rede EtherNet/IP:

- conecte-se diretamente à rede.
- conecte-se a uma rede diferente e procure a rede desejada usando um equipamento de enlace.

DICA

É possível procurar a rede Ethernet usando a porta USB do controlador SmartGuard.

A capacidade de formação de ponte entre a USB do SmartGuard e Ethernet é limitada.

Depois de escolher uma rede:

- instale o cartão de comunicação, se necessário.
- determine todos os parâmetros de rede do computador como, por exemplo, um endereço de rede.
- conecte o computador à rede usando o cabo correto.

IMPORTANTE

Na primeira vez em que conectar um controlador SmartGuard ao seu microcomputador usando a porta USB, o sistema operacional Windows passará por sua sequência de reconhecimento do equipamento e solicitará a você os drivers USB. O driver está no CD RSLinx Classic, na pasta SmartGuardUSB-KernelDrivers.

Configuração de um driver para a rede

1. Inicie o software RSLinx.

Para o software RSLinx localizar novos dispositivos na rede EtherNet/IP, o driver pode ser ajustado (busque a opção remota de sub-rede) para procurar por uma máscara e endereços IP específicos.

2. Clique em Configure Driver.
3. No menu Available Driver Types, escolha o driver para a sua rede.

Rede	Driver
RS-232	Dispositivos RS-232 DF1
EtherNet/IP	Dispositivos Ethernet
DeviceNet	Driver EtherNet/IP
USB	Driver SmartGuard USB

4. Configure o driver.

Os ajustes de parâmetros feitos dependem da rede escolhida e da possibilidade de uso de um cartão de comunicação ou módulo de interface.

Verificação do funcionamento do driver

1. Marque a caixa de diálogo Configure Drivers para ter certeza de que o driver esteja em execução.

DICA

Pode-se configurar o driver pelo uso da seleção de sub-rede remota e pela configuração do endereço IP e máscara para o valor do controlador SmartGuard. Isto permite que o software RSLinx encontre rapidamente o dispositivo.

2. Feche a caixa de diálogo.
3. Abra a caixa de diálogo RSWho.
4. Clique duas vezes no driver para ver a rede.

Conectando o controlador SmartGuard 600 à rede EtherNet/IP

IMPORTANTE

Os controladores SmartGuard não devem estar conectados diretamente a nenhuma rede que não esteja protegida de intrusão externa. Por exemplo, não conecte o controlador SmartGuard 600 a uma rede Ethernet que não esteja protegida com um firewall ou outras medidas de segurança.

Configurando o endereço IP

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

Parâmetros EtherNet/IP

Parâmetro EtherNet/IP	Descrição
Endereço IP	O endereço IP identifica o controlador de forma única. O endereço IP está na forma xxx.xxx.xxx.xxx, onde cada xxx é um número entre 0 e 255. Os seguintes valores reservados não podem ser usados: • 127.0.0.1 • 0.0.0.0 • 255.255.255.255
Máscara de sub-rede	O endereçamento de sub-rede é uma extensão do esquema de endereço IP que permite que um local use um ID de rede único para várias redes físicas. O roteamento fora do local continua, dividindo o endereço IP em um ID de rede e um ID de host através da classe. Dentro de um local, a máscara de sub-rede é usada para redividir o endereço IP em uma porção de ID de rede personalizada e porção ID do host. Este campo é configurado para 0.0.0.0 por padrão. Se a máscara de sub-rede de um controlador já configurado for modificada, deve-se desligar e ligar a alimentação para que a mudança seja executada.
Conversor de protocolos	Um conversor de protocolos conecta redes físicas individuais em um sistema de redes. Quando um nó precisa se comunicar com um nó em outra rede, um conversor de protocolos transfere os dados entre as duas redes. Este campo é configurado para 0.0.0.0 por padrão.

Pode-se configurar o controlador por meio de duas opções; pelo software RSLinx Classic ou pelo utilitário BOOTP. Consulte a [página 54](#) para o uso de BOOTP ou a [página 57](#) para o uso do software RSLinx.

Usando BOOTP para configurar o endereço IP

BOOTP (protocolo bootstrap) é um protocolo de nível baixo que os nós TCP/IP usam para obter informações de partida. Um endereço IP não é configurado até que uma resposta BOOTP tenha sido recebida. BOOTP permite que você atribua dinamicamente os endereços IP a processadores no link Ethernet.

Para usar o BOOTP, um servidor BOOTP deve existir na sub-rede Ethernet local. O servidor é um computador que tem um software de servidor BOOTP instalado e lê um arquivo de texto contendo informações de rede para nós individuais na rede.

O arquivo de configuração BOOTP do sistema do host deve ser atualizado para pedidos de serviço do controlador SmartGuard. No estado padrão (pronto para usar), o controlador SmartGuard necessita do uso de um servidor BOOTP para configurar o seu endereço IP.

Consulte [Configurando o endereço IP](#) para os parâmetros que precisam ser configurados.

DICA

Pode-se usar qualquer servidor BOOTP disponível comercialmente. Se não tiver recursos de servidor BOOTP na sua rede, e quiser configurar dinamicamente o controlador SmartGuard, pode-se fazer o download grátis do servidor BOOTP da Rockwell Automation em <http://www.rockwellautomation.com/rockwellsoftware/download/>.

Quando o BOOTP está habilitado, os seguintes eventos ocorrem na energização:

- O processador transmite uma mensagem de pedido BOOTP contendo o endereço do hardware na rede ou sub-rede local.
- O servidor BOOTP compara o endereço de hardware com os endereços na tabela de consulta.
- O servidor BOOTP envia uma mensagem de volta ao processador com o endereço IP e outras informações de rede que correspondem ao endereço de hardware que recebeu.

Com todo o hardware e endereços de IP em um local, podem-se modificar os endereços IP no arquivo de configuração BOOTP se as necessidades da sua rede mudaram.

O pedido BOOTP pode ser desabilitado pela remoção do parâmetro de habilitação de BOOTP na guia Port Configuration. Quando a habilitação de BOOTP é apagada (desabilitada), o controlador SmartGuard usa os dados de configuração do canal existentes.

IMPORTANTE

Quando o protocolo BOOTP é usado para configurar o endereço IP em um controlador SmartGuard, o controlador SmartGuard deve receber um endereço IP inicial do servidor antes que o protocolo BOOTP possa ser desligado. Pode ser desabilitado pelo uso da função de configuração de módulo no software RSLinx.

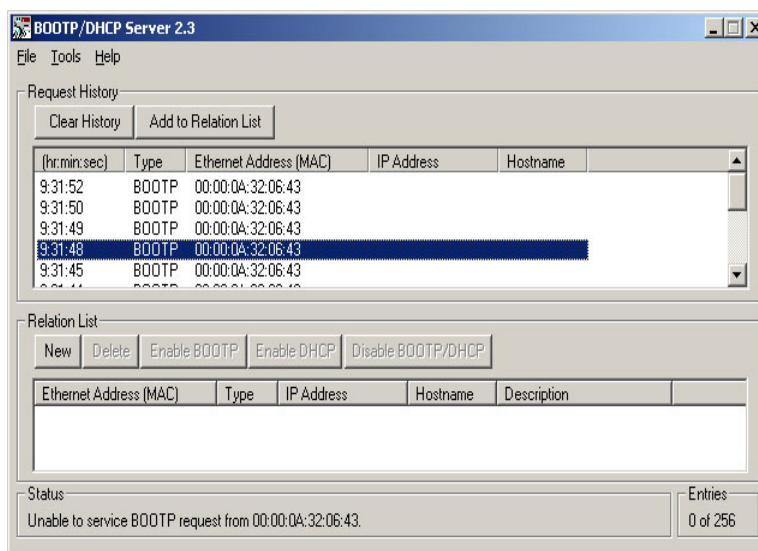
Use o utilitário Rockwell BOOTP

O utilitário Rockwell BOOTP é um programa independente que incorpora a funcionalidade do software padrão BOOTP com uma interface gráfica amigável. Pode-se fazer o download em <http://www.rockwellautomation.com/rockwellsoftware/download/>. O dispositivo deve estar habilitado para BOOTP (ajuste de fábrica) para usar o utilitário.

Para configurar o seu dispositivo usando o utilitário BOOTP, realize as seguintes etapas.

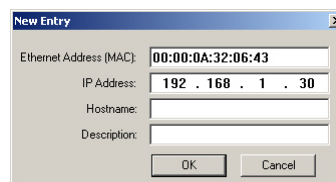
1. Execute o software BOOTP.

No painel de histórico de pedidos do BOOTP você verá os endereços de hardware dos dispositivos que emitem pedidos BOOTP.



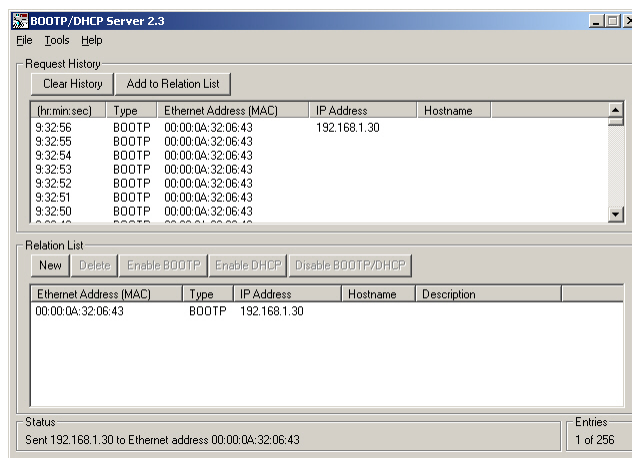
2. Clique duas vezes no endereço de hardware do dispositivo que você deseja configurar.

Você verá a janela New Entry com o endereço Ethernet do dispositivo (MAC).



3. Insira o endereço IP (nome do host e descrição são opcionais) que deseja atribuir ao dispositivo, e clique em OK.

O dispositivo será adicionado à lista de relações, exibindo o endereço Ethernet (MAC) e endereço IP correspondente, máscara de sub-rede e conversor de protocolos (se aplicável).

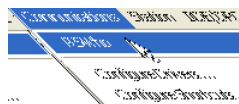


Use o software RSLinx para configurar o endereço IP

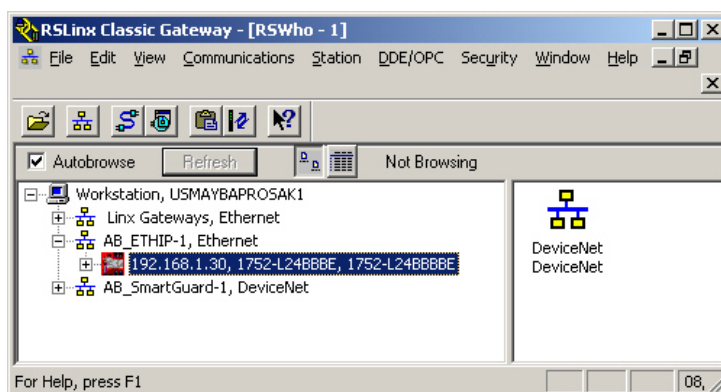
Depois de ter usado o utilitário BOOTP para configurar inicialmente o endereço IP de um novo controlador SmartGuard 600, você pode usar o software RSLinx para mudar o endereço IP. Se esta é a funcionalidade que deseja, certifique-se de desabilitar o utilitário BOOTP no controlador SmartGuard, ou então, todas as vezes que a energia for aplicada ao controlador SmartGuard, ele irá iniciar no modo BOOTP.

Para usar o software RSLinx para configurar os parâmetros de endereço de IP no controlador 1752-L24BBBE, siga este procedimento.

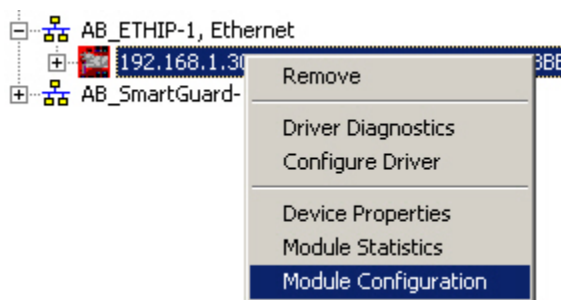
1. Certifique-se de que o controlador 1752-L24BBBE esteja instalado e energizado.
2. Inicie o software RSLinx.
3. No menu Communications, escolha RSWho.



A caixa de diálogo RSWho aparece.



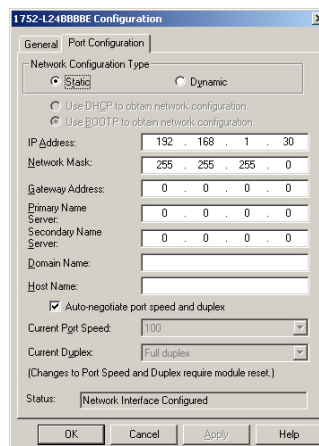
4. Navegue em RSWho à rede Ethernet.
5. Clique com o botão direito do mouse no controlador SmartGuard e escolha Module Configuration.



DICA

A opção de configuração do módulo também é mostrada quando o controlador SmartGuard é visualizado a partir do software DeviceNet, mas a configuração IP é aplicada apenas quando for executada diretamente da rede EtherNet/IP.

A caixa de diálogo Module Configuration aparece.



6. Clique na guia Port Configuration.

7. Para o tipo de configuração de rede, clique em Static para atribuir permanentemente esta configuração à porta.

IMPORTANTE

Se Dynamic for selecionado em um ciclo de alimentação, o controlador remove a configuração IP atual e volta a enviar pedidos BOOTP. Consulte a [página 55](#) para mais informações.

- a. No campo IP Address, digite o endereço IP.
- b. No campo Network Mask, digite o endereço de máscara de rede.
- c. No campo Gateway Address, digite o endereço de conversor de protocolos ou deixe todos os zeros.
- d. No campo Primary Name Server, digite o endereço do servidor de nome primário ou deixe todos os zeros.
- e. No campo Secondary Name Server, digite o endereço do servidor de nome secundário ou deixe todos os zeros.
- f. No campo Domain Name, digite o nome de domínio ou deixe em branco.
- g. No campo Host Name, digite o nome do host ou 'SmartGuard ENIP'.

8. Configure os ajustes de parâmetro de porta.

Para	Faça o seguinte:
Usar a velocidade de porta padrão e configurações duplex	Deixe marcada a caixa de verificação Auto-negotiate port speed and duplex. Importante: A velocidade de porta padrão é 100, e a configuração duplex padrão é Full.
Configurar manualmente a velocidade de porta e configurações duplex.	a. Desmarque a caixa de verificação Auto-negotiate port speed and duplex. b. No menu Current Port Speed, escolha uma velocidade de porta. c. No menu Current Duplex, escolha Half Duplex.

9. Clique em OK.**Formando ponte nas redes**

O controlador 1752-L24BBBE suporta a habilidade de formar a ponte ou rotear a comunicação com vários dispositivos, dependendo dos recursos dos dispositivos de plataforma e comunicação.

Há uma ponte quando há uma conexão entre os dispositivos de comunicação em duas redes. Por exemplo, um dispositivo de ponte tem as conexões EtherNet/IP e DeviceNet, habilitando o dispositivo 1 na rede EtherNet/IP para se comunicar com o dispositivo 2 em uma rede DeviceNet através da ponte.

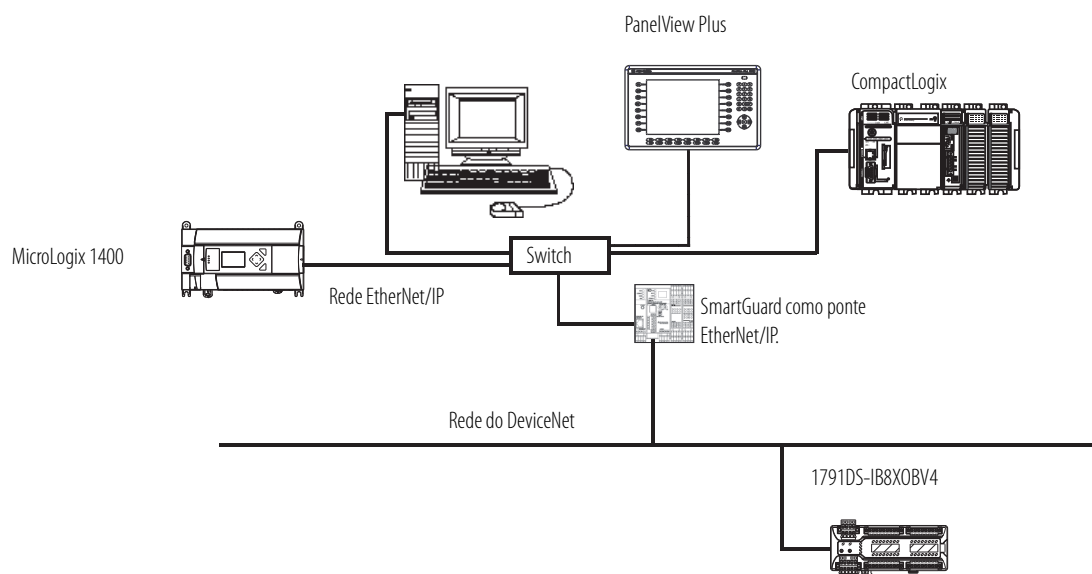
Rede EtherNet/IP para uma rede DeviceNet

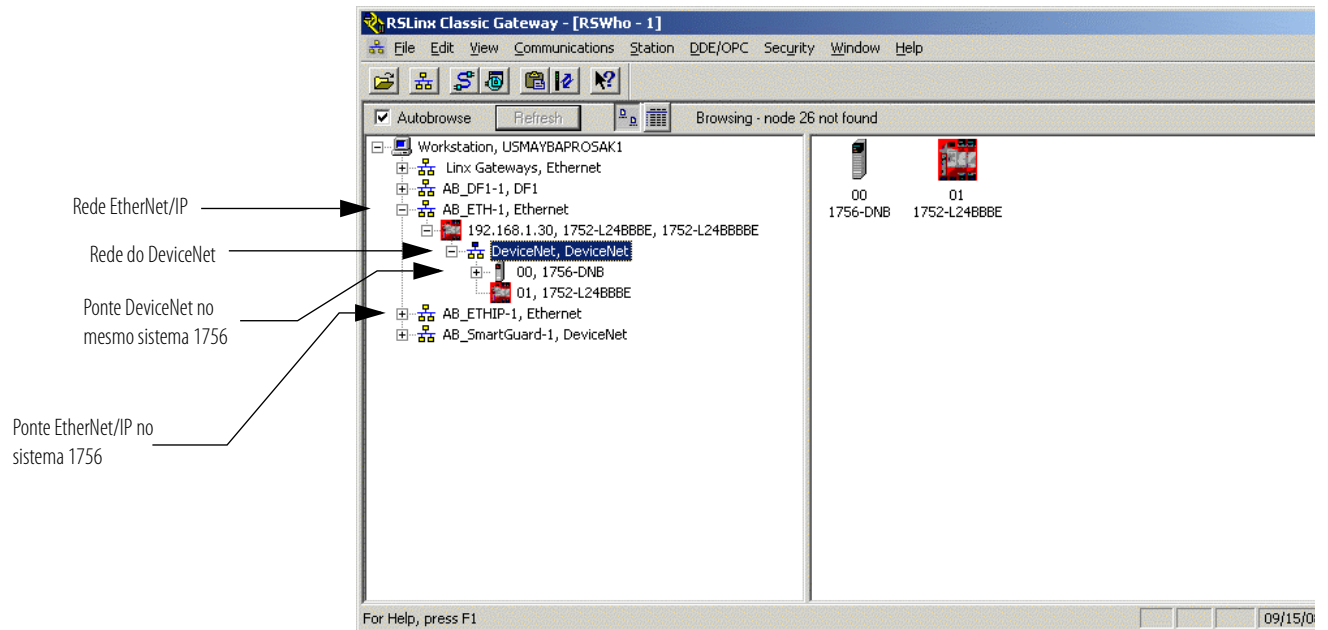
Aqui há uma conexão entre a rede EtherNet/IP e a rede DeviceNet. O controlador SmartGuard permite que você use seu microcomputador que está conectado à rede EtherNet/IP para configurar o módulo 1791DS na rede DeviceNet fazendo a ponte pelo controlador SmartGuard.

IMPORTANTE

Os recursos de formação de ponte do controlador SmartGuard são limitados. São projetados para configurar os módulos de segurança DIO ou outra rede, mas não devem ser usados para programar outros CLPs e não devem ser usados como dispositivo de formação de ponte durante a operação de máquina.

Rede EtherNet/IP para uma rede DeviceNet



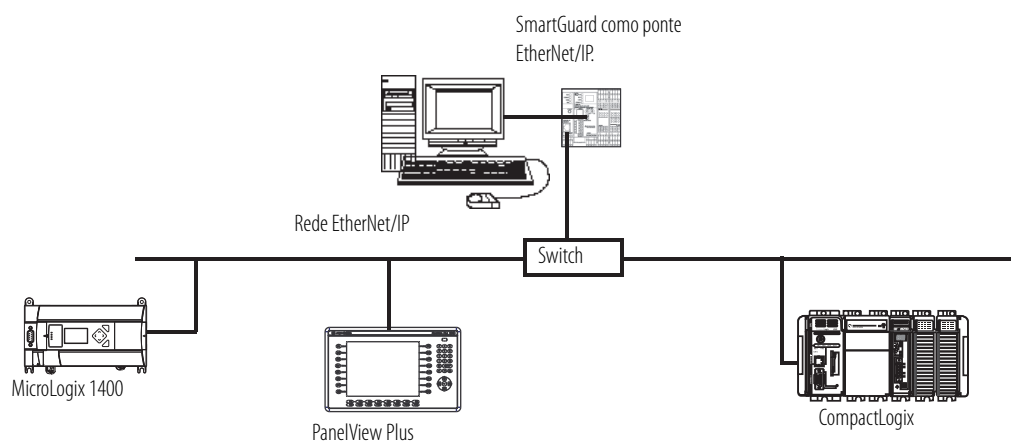
Linking de ponte EtherNet/IP para uma rede DeviceNet

Porta USB para a rede EtherNet/IP

O controlador SmartGuard suporta a formação de ponte da porta USB à rede EtherNet/IP. Entretanto, recomendamos que esta função não seja utilizada, mas seja feita a conexão direta à rede EtherNet/IP para configurar dispositivos além do controlador SmartGuard.

O controlador SmartGuard pode apenas explorar a sub-rede Ethernet a que está conectado. Pode-se procurar um controlador MicroLogix 1400 ou um controlador CompactLogix, mas não se pode procurar um controlador ControlLogix porque não se pode rotear pelo módulo 1756-ENBT no rack ControlLogix.

Porta USB para rede EtherNet/IP



Gerenciamento do SNN

Introdução

Tópico	Página
Formatos do número da rede de segurança (SNN)	63
Atribuição do número da rede de segurança (SNN)	65
Definição do número da rede de segurança (SNN) em todos os nós de segurança	65
Diferença no número da rede de segurança (SNN)	67
Número da rede de segurança (SNN) e alterações no endereço do nó	67

Todos os equipamentos do DeviceNet devem ser configurados com um número da rede segurança (SNN). A combinação do SNN e dos endereços de nó do DeviceNet proporciona um identificador exclusivo para cada nó de segurança em uma rede industrial complexa. O identificador exclusivo impede que os dados destinados a um endereço de nó alvo específico em uma sub-rede do DeviceNet sejam roteados incorretamente e aceitos por um nó com o mesmo endereço do nó em uma sub-rede do DeviceNet diferente.

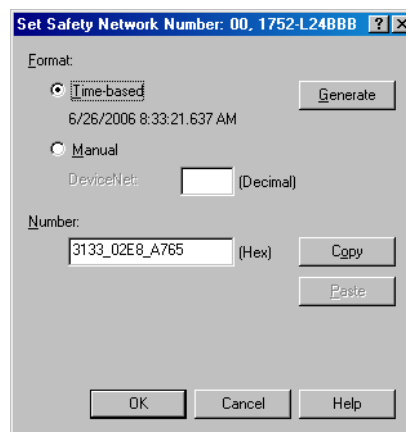
Os SNN atribuídos a cada rede de segurança ou sub-rede da rede devem ser exclusivos. Você deve ter a certeza de que haja um número da rede de segurança (SNN) exclusivo atribuído a cada rede do DeviceNet que contém os nós de segurança.

Formatos do número da rede de segurança (SNN)

O número da rede de segurança (SNN) pode ser atribuído pelo software (com base no tempo) ou pelo usuário (manual). Os dois formatos do SNN são descritos nas seções a seguir.

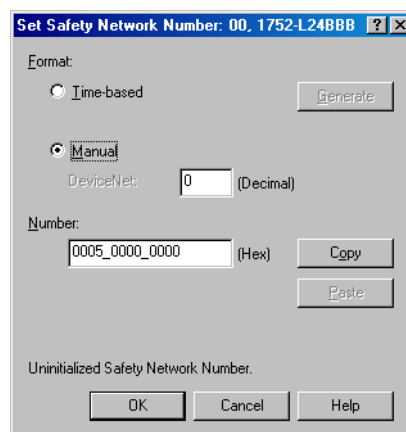
Número da rede de segurança com base no tempo (recomendável)

No formato com base no tempo, o número da rede de segurança (SNN) representa data e hora em que o número foi gerado, de acordo com o microcomputador que está executando o software RSNetWorx for DeviceNet.



Número da rede de segurança (SNN) manual

No formato manual, o SNN representa valores digitados entre 1 e 9999 em decimal.



DICA

Clique em Copy na caixa de diálogo Set Safety Network Number para copiar o SNN para a área de transferência do Windows.

Atribuição do número da rede de segurança (SNN)

Um SNN pode ser gerado automaticamente pelo software RSNetWorx for DeviceNet ou é possível atribuir um manualmente. Um SNN gerado automaticamente é suficiente e recomendado para a maioria dos aplicativos.

Automática (com base no tempo)

Quando um novo equipamento de segurança é adicionado à configuração da rede do DeviceNet, um SNN padrão é atribuído automaticamente pelo software de configuração da seguinte forma:

- Caso haja pelo menos um equipamento de segurança na configuração da rede do DeviceNet, as adições de segurança subsequentes a essa configuração de rede são atribuídas ao mesmo SNN conforme o dispositivo de segurança com o endereço mais baixo.
- Caso não haja nenhum outro equipamento de segurança na configuração da rede do DeviceNet, um SNN com base no tempo é gerado automaticamente pelo software RSNetWorx for DeviceNet.

Manual

A opção manual destina-se aos sistemas em que o número das sub-redes do DeviceNet e das redes de interconexão é pequeno, quando você talvez queira gerenciar e atribuir todos os SNNs de maneira lógica que pertençam à aplicação específica.

IMPORTANTE

Caso você atribua um SNN manualmente, tome cuidado para ter a certeza de que a expansão do sistema não resulte na duplicação do SNN e nas combinações de endereços do nó.

Para definir o SNN em um equipamento de segurança usando o software RSNetWorx for DeviceNet, selecione o equipamento na exibição gráfica do hardware e escolha Set Safety Network Number no menu Device.

IMPORTANTE

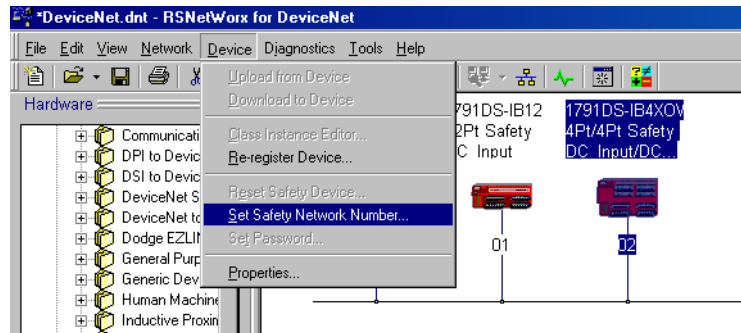
Quando você define o SNN, o equipamento retorna ao ajuste de fábrica.

Definição do número da rede de segurança (SNN) em todos os nós de segurança

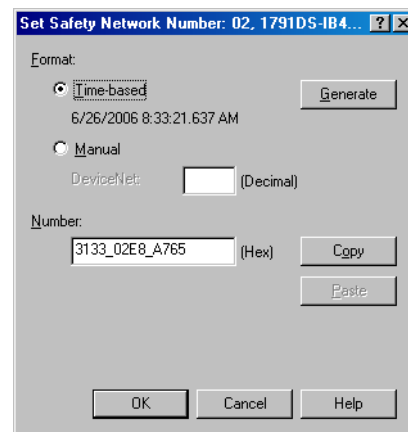
Um SNN com base no tempo é gerado automaticamente quando o primeiro equipamento de segurança novo é adicionado à rede. As adições subsequentes à rede recebem o mesmo SNN conforme o dispositivo de segurança com o endereço mais baixo. O SNN automático, com base no tempo, é suficiente e recomendável para a maioria das aplicações.

Siga estas etapas caso você precise definir o SNN para um determinado equipamento.

1. Clique no dispositivo alvo na exibição gráfica de hardware e escolha Set Safety Network Number no menu Device.



2. Escolha Time-based e clique em Generate ou escolha Manual e preencha usando um número decimal entre 1 e 9999.

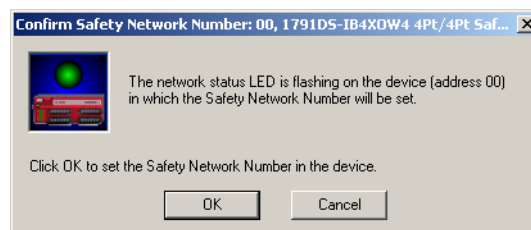


3. Clique em OK.

DICA

É possível usar os botões de copiar e colar na caixa de diálogo Set Safety Network Number para copiar e colar um SNN entre equipamentos e fazer um registro do SNN.

4. Verifique se o indicador Network Status está alternando rapidamente entre vermelho e verde no equipamento correto e clique em OK.



Diferença no número da rede de segurança (SNN)

O software RSNetWorx for DeviceNet compara o SNN off-line com o SNN on-line durante cada operação de pesquisa, monoestável ou contínuo e durante as operações de upload e de download. Caso os SNNs não casem, o software RSNetWorx for DeviceNet indica um erro com o SNN. A exibição gráfica de hardware exibe o símbolo ! sobre o ícone do equipamento de segurança.

Quando estiver on-line, o software RSNetWorx para DeviceNet também verifica se há diferença no SNN sempre que a caixa de diálogo Device Properties do equipamento de segurança é selecionada, no menu Device > Properties ou clicando duas vezes no equipamento. Caso haja uma condição de diferença de SNN, a caixa de diálogo Safety Network Number Mismatch é exibida.

A caixa de diálogo Safety Network Number Mismatch exibe o SNN on-line (equipamento) e o SNN off-line (software). É possível optar por fazer upload o SNN do equipamento ou fazer download do SNN off-line para resolver a diferença.



Caso o SNN do equipamento não tenha sido inicializado, o campo Device Safety Network Number exibe o SNN padrão: FFFF_FFFF_FFFF. Quando o SNN do equipamento é FFFF_FFFF_FFFF, o botão Upload permanece obscurecido e indisponível.

Número da rede de segurança (SNN) e alterações no endereço do nó

Caso você queira alterar o endereço de um equipamento de segurança, o SNN deve ser desinicializado, ou você deve primeiro reinicializar o SNN.

Siga estas etapas para reinicializar o SNN.

1. Selecione o equipamento na exibição gráfica do hardware.
2. No menu Device, escolha Reset Safety Device.
3. Marque a caixa de seleção Safety Network Number na caixa de diálogo Reset Safety Device e clique em Reset.

Apenas os atributos selecionados na caixa de diálogo são reinicializados de acordo com o ajuste de fábrica. O reset de segurança só afeta o equipamento de segurança; a configuração no projeto RSNetWorx não é perdida.

Consulte [Reset de segurança \(opcional\)](#) na [página 46](#) para mais informações sobre a função de reset de segurança.

DICA

Após o reset de segurança, o endereço do nó pode ser alterado no software RSNetWorx for DeviceNet clicando duas vezes no endereço do nó do dispositivo de segurança na exibição gráfica. Após a alteração do endereço do nó, clique com o botão direito do mouse no equipamento e clique em Download to Device para restaurar o SNN e a configuração do equipamento de segurança.

Configuração de E/S local

Introdução

Tópico	Página
Configuração das entradas de segurança locais	69
Configuração das saídas de teste locais	74
Configuração de saídas de segurança locais	76

Configuração das entradas de segurança locais

O controlador tem 16 entradas de segurança local que suportam as seguintes funções.

- Diagnóstico do circuito de entrada – origens de pulso de teste podem ser usadas para monitorar circuitos internos, equipamentos externos e fiação externa.
- Atrasos na energização e desenergização de entrada – é possível definir filtros de tempo de entrada de 0 a 126 ms em múltiplos do tempo do ciclo do controlador. Definir atrasos na energização e desenergização ajuda a reduzir a influência da trepidação de contatos e do ruído externo.

IMPORTANTE

Os atrasos na energização e na desenergização devem ser adicionados ao tempo de resposta de E/S. Isso afetará os cálculos do tempo de reação do sistema.

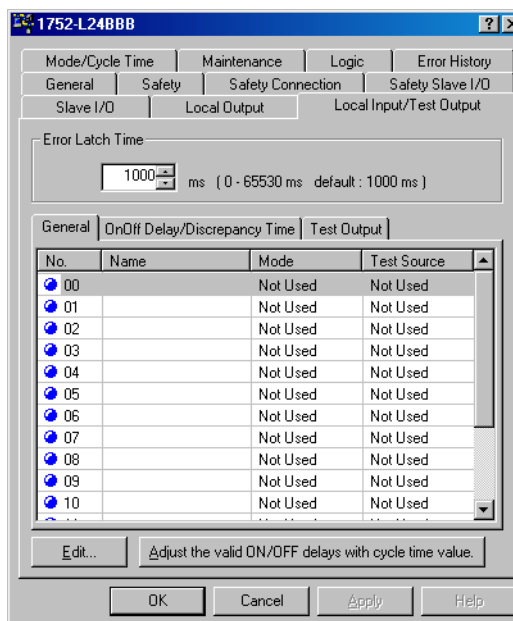
Consulte o Manual de referência de segurança dos controladores SmartGuard, publicação [1752-RM001](#), para informações sobre o cálculo dos tempos de reação.

- Modo em canal duplo – é possível definir o modo em canal duplo para pares de entradas locais relacionadas. Quando o modo de canal duplo está definido, as discrepâncias de tempo nas alterações de dados ou sinais de entrada entre duas entradas locais emparelhadas podem ser avaliadas.

Siga estas etapas para configurar entradas de segurança locais.

1. Clique com o botão direito do mouse no controlador SmartGuard e escolha Properties.

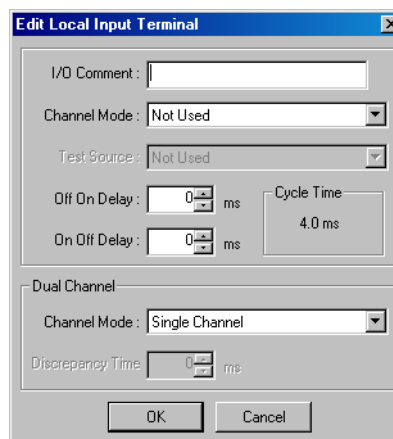
2. Selecione a guia Local Input/Test Output.



3. Defina o tempo de fixação do erro.

O tempo de fixação do erro aplica-se a todas as entradas de segurança e saídas de teste. Ele define o tempo de fixação do estado do erro quando este ocorre em uma entrada ou saída. Mesmo que o erro seja removido, o estado do erro está sempre fixado pelo tempo de fixação do erro configurado. O tempo de trava do erro é definido de 0 a 65,530 ms em incrementos de 10 ms. O padrão é 1000 ms.

4. Selecione um terminal de entrada de segurança e clique em Edit.



5. Digite um comentário de E/S.

O comentário de E/S digitado aqui é usado como sendo o nome da tag de E/S no Logic Editor.

6. Defina o Modo do canal da entrada de segurança.

Modo de canal	Descrição
Não usado	O canal de entrada não está conectado a um equipamento externo. Trata-se do padrão.
Pulso de teste da saída de teste	Use o modo ao obter um circuito de entrada de categoria 4. Esse modo presume que você tenha conectado o dispositivo de entrada a uma origem de teste de pulso e ligado ao terminal de entrada. Isso habilita a detecção de curto-circuitos com a linha da fonte de alimentação (lado positivo), falhas para terra e curto-circuitos com outras linhas de sinal de entrada (curtos entre canais). O controlador deve saber que o sinal de entrada está sendo testado por pulso ou que desarmes por ruído podem ocorrer. Consulte o Exemplo: canal de entrada como pulso de teste da saída de teste na página 73 .
Usado como sendo uma entrada de segurança	Use o modo para se conectar a um equipamento de segurança com uma saída de semiconductor como, por exemplo, uma cortina de luz.
Usado como sendo uma entrada padrão	Use o modo para se conectar a um equipamento padrão (não-segurança).

7. Caso você defina o modo de canal para pulso de teste em saída de teste, escolha a saída de teste a ser usada com a entrada de segurança selecionando-a na lista Test Source.**DICA**

O modo de canal da saída de teste selecionada é definido automaticamente como Pulse Test Output.

8. Defina o Modo de canal duplo e o Tempo de discrepância.

Definir o modo de canal duplo permite que o status de duas entradas seja avaliado e refletido nas tags de E/S. O tempo de discrepância entre as alterações no status de duas entradas também pode ser avaliado. As combinações que podem ser definidas são predefinidas. O tempo de discrepância pode ser definido entre 0 e 65,530 ms em incrementos de 10 ms. Ambas as entradas devem ter o estado alterado dentro do tempo de discrepância, ou ocorre um erro.

Modo de canal	Descrição
Canal único	O terminal de entrada de segurança é usado de maneira independente.
Equivalente a canal duplo	O terminal de entrada de segurança é usado como sendo um equivalente a canal duplo com um terminal de entrada de segurança do par.
Canal duplo complementar	O terminal de entrada de segurança é usado como sendo um canal duplo complementar com um terminal de entrada de segurança emparelhado.

DICA

O controlador suporta blocos de funções com funcionalidade equivalente ao modo de canal duplo. Em muitos casos, o anúncio e localização das falhas do sistema é mais fácil quando os blocos de funções são usados para detectar falhas em vez do hardware SmartGuard. Se desejar usar os blocos de funções para detectar as falhas de sistema, as entradas de segurança devem ser configuradas para o canal único.

9. Especifique um tempo de atraso na energização e um tempo de atraso na desenergização.

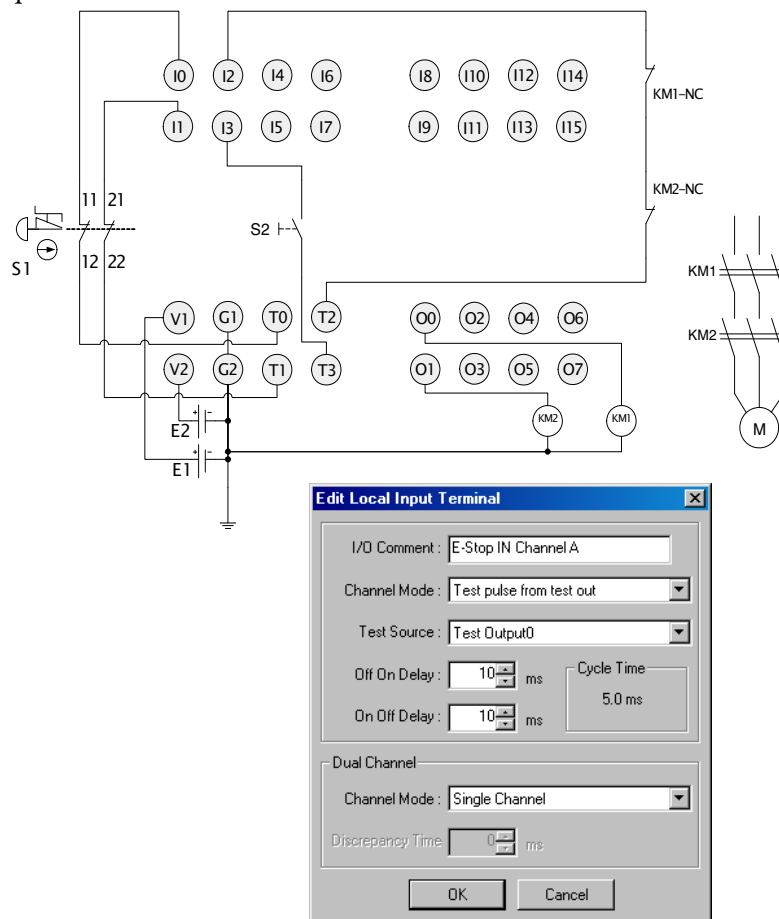
A faixa válida é 0 a 126 ms, embora o tempo de atraso deva ser um múltiplo do tempo de ciclo.

IMPORTANTE

O valor ideal do tempo de ciclo do controlador é calculado automaticamente com base nas configurações e nos programas aplicativos. Por isso, defina os tempos de atraso na energização e na desenergização por último.

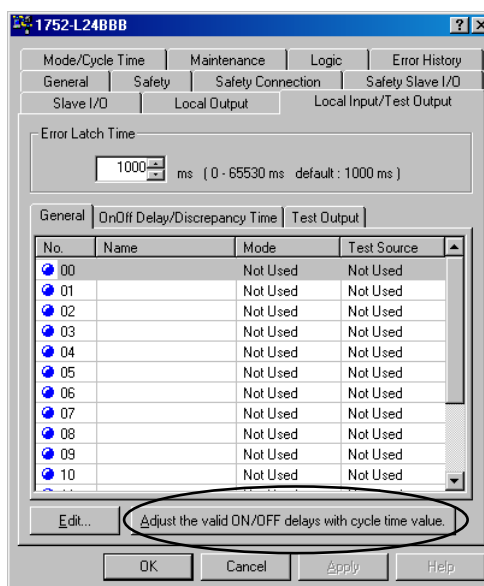
Exemplo: canal de entrada como pulso de teste da saída de teste

Para o seguinte esquema elétrico, o modo de canal deve ser configurado como sendo o pulso de teste da saída de teste, conforme mostrado.



Ajuste automático dos tempos de atraso na energização e na desenergização

Caso os parâmetros que afetam o tempo do ciclo sejam alterados após a definição dos atrasos na energização e na desenergização, você talvez não consiga fechar a caixa de diálogo Controller Properties por conta de um erro nos ajustes dos parâmetros. Caso isso ocorra, é possível reajustar os tempos de atraso na energização e na desenergização com base no tempo de ciclo usando os atrasos válidos de ajuste com o botão do valor de tempo do ciclo na guia Local Input/Test Output.



Configuração das saídas de teste locais

Estas quatro saídas de teste podem ser usadas com as entradas de segurança. Elas também podem ser definidas para serem usadas como sendo terminais de saída padrão. As funções da saída do pulso de teste estão listadas abaixo.

- Monitoração de corrente da lâmpada muting – um fio desligado ou uma lâmpada queimada podem ser detectados apenas no terminal T3.
- Detecção de sobrecorrente e proteção – para proteger o circuito, uma saída é bloqueada quando uma sobrecorrente é detectada.

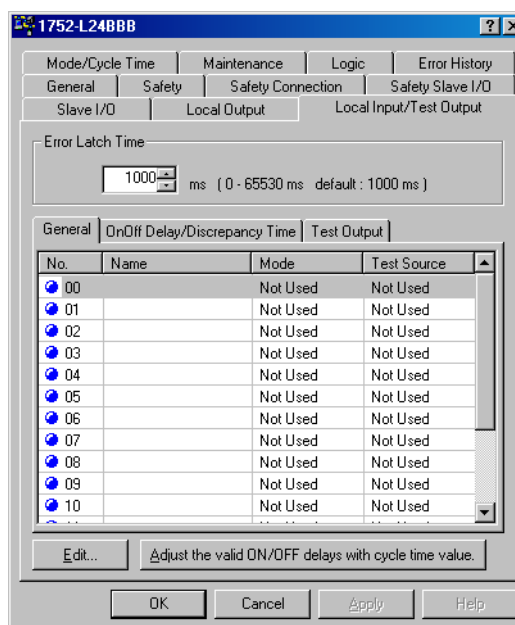
ATENÇÃO



As saídas de pulso não devem ser usadas como saídas relacionadas à segurança (por exemplo, para o controle dos atuadores relacionados à segurança) porque elas não são classificadas para segurança.

Siga estas etapas para configurar uma saída de teste.

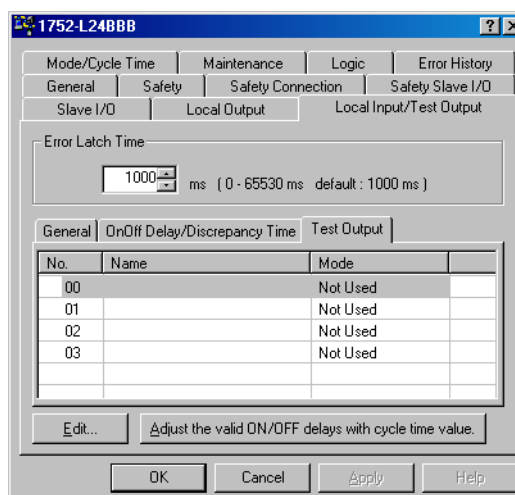
1. Clique com o botão direito do mouse no controlador SmartGuard e escolha Properties.
2. Selecione a guia Local Input/Test Output.



3. Defina o tempo de fixação do erro.

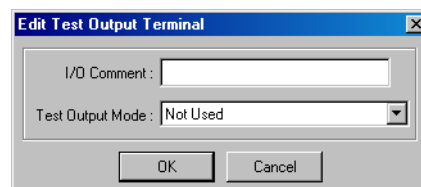
O tempo de fixação do erro aplica-se a todas as entradas de segurança e saídas de teste. Ele define o tempo de fixação do estado do erro quando este ocorre em uma entrada ou saída. Mesmo que o erro seja removido, o estado do erro está sempre fixado pelo tempo de fixação do erro configurado. O tempo de trava do erro é definido de 0 a 65,530 ms em incrementos de 10 ms. O padrão é 1000 ms.

4. Selecione a guia Test Output.
5. Selecione um terminal de saída de teste e clique em Edit.



6. Digite um comentário de E/S.

O comentário de E/S digitado aqui é usado como sendo o nome da tag de E/S no Logic Editor.



7. Escolha um modo de saída de teste na lista.

Modo de saída de teste	Descrição
Não usado	A saída de teste correspondente não é usada.
Saída padrão	Escolha esse modo ao se conectar à saída a partir de uma lâmpada muting ou de um controlador lógico programável. A saída é usada como sendo a saída do monitor.
Saída de teste por pulso	Escolha esse modo ao se conectar um equipamento com uma saída de contato com uma entrada de segurança.
Saída da lâmpada muting	Escolha esse modo para especificar uma saída da lâmpada muting. Essa configuração só é suportada no terminal T3. Quando a saída está ativada, a desconexão da lâmpada muting pode ser detectada.

Configuração de saídas de segurança locais

O controlador tem oito saídas de segurança locais que suportam as funções listadas abaixo.

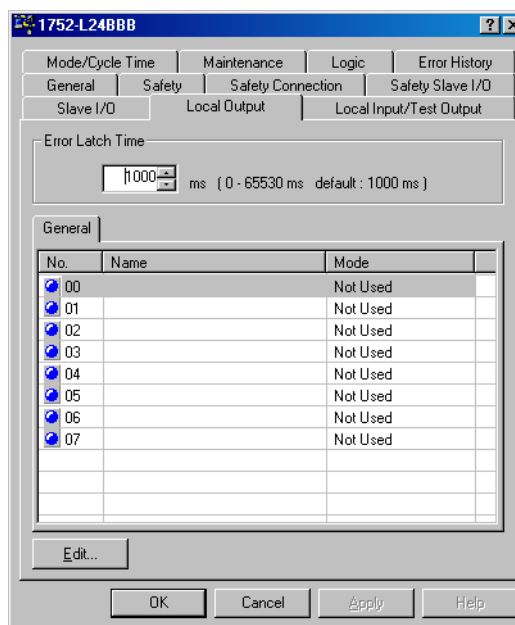
- Diagnóstico do circuito de saída – os pulsos de teste podem ser usados para diagnosticar os circuitos internos do controlador, os equipamentos externos e a fiação externa.
- Detecção de sobrecorrente e proteção – para proteger o circuito, uma saída é bloqueada quando uma sobrecorrente é detectada.
- Modo de canal duplo – as duas saídas emparelhadas podem ser definidas em um estado de segurança quando ocorre um erro em uma das duas saídas locais emparelhadas sem depender do programa do usuário.

Siga estas etapas para configurar uma saída de segurança local.

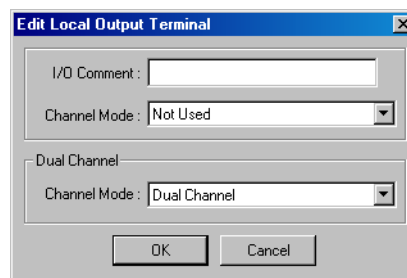
1. Clique com o botão direito do mouse no controlador SmartGuard e escolha Properties.
2. Selecione a guia Local Output.

3. Defina o tempo de fixação do erro.

O tempo de fixação do erro aplica-se a todas as saídas de segurança. Ele define o tempo de fixação do estado do erro quando este ocorre em uma entrada ou saída. Mesmo que o erro seja removido, o estado do erro está sempre fixado pelo tempo de fixação do erro configurado. O tempo de trava do erro é definido de 0 a 65,530 ms em incrementos de 10 ms. O padrão é 1000 ms.



4. Selecione um terminal de saída de segurança e clique em Edit.



5. Digite um comentário de E/S.

O comentário de E/S digitado aqui é usado como sendo o nome da tag de E/S no Logic Editor.

6. Defina o modo de canal da saída de segurança.

Modo de canal	Descrição
Não usado	O terminal de saída não está conectado a um equipamento de saída.
Segurança	Um pulso de teste não é enviado quando a saída está ativada. Quando a saída está desativada, os curto-circuitos com a linha da fonte de alimentação podem ser detectados. As faltas à terra também podem ser detectadas.
Teste de pulso de segurança	Um pulso de teste é enviado quando a saída está ativada. Isso habilita a detecção de curto-circuitos com a linha da fonte de alimentação (lado positivo), independentemente da saída estar ativada ou desativada. As faltas à terra e os curto-circuitos entre os sinais de saída também podem ser detectados.

IMPORTANTE

Caso um teste de pulso de segurança esteja definido, um sinal de pulso desativado (largura do pulso de 580 μ s) é produzido para diagnosticar o circuito de saída quando a saída de segurança é ativada. Verifique o tempo de resposta de entrada do equipamento de controle para garantir que o pulso de saída não cause falhas.

7. Defina o modo de canal duplo da saída de segurança.

Definir o modo de canal duplo permite que um erro seja detectado caso as duas saídas de um programa do usuário não sejam equivalentes.

Se um erro for detectado em um dos circuitos de saída, ambas as saídas para o equipamento se tornarão inativas.

Configurações do modo de canal duplo de saída

Modo de canal	Descrição
Canal único	O terminal de saída de segurança é usado de maneira independente.
Canal duplo	O terminal de saída de segurança é emparelhado com outro terminal de saída. A saída pode ser ativada quando a saída e a saída de segurança emparelhada são consistentes.

Configuração do controlador para a comunicação DeviceNet

Introdução

O controlador SmartGuard pode funcionar simultaneamente como um mestre de segurança, um escravo de segurança ou um escravo padrão.

Tópico	Página
Ajustando o controlador como um mestre de segurança	79
Ajustando o controlador como um escravo de segurança	90
Ajustando o controlador como um escravo padrão DeviceNet	98
Leitura e gravação de e para o controlador SmartGuard para uma interface PanelView Plus	103

Ajustando o controlador como um mestre de segurança

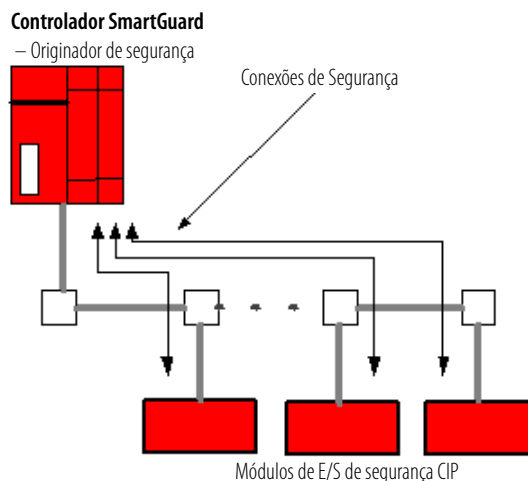
Como um mestre de segurança, o controlador pode realizar comunicação de E/S de segurança com até 32 conexões, usando até 16 bytes por conexão. As conexões podem ser singlecast ou multicast.

Tipos diferentes de módulos de E/S distribuída de segurança consomem quantias distintas das 32 conexões disponíveis. Por exemplo, um módulo somente entrada pode consumir 1 das 32 conexões (conexão de entrada), ao passo que um módulo com entradas e saídas pode consumir 2 das 32 conexões de segurança (1 conexão de entrada e 1 conexão de saída).

A configuração do módulo também informa quantas conexões de segurança ele consome. Por exemplo, o módulo 1791DS-IB12 tem 12 entradas de segurança, nenhuma saída de segurança e 4 saídas de teste de pulso ou padrão. Caso seja configurado apenas para entradas de segurança, o módulo consome 1 conexão de segurança. No entanto, se for configurado para usar entradas de segurança e saídas padrão, ele consumirá 2 conexões de segurança. Em linhas gerais, o número e o tipo dos módulos de E/S distribuída de segurança conectados ao controlador SmartGuard determinará o número máximo de módulos compatíveis com o controlador.

Um relacionamento mestre/escravo é estabelecido para cada conexão na rede de segurança do DeviceNet, à parte da comunicação mestre/escravo na rede-padrão do DeviceNet. Isso habilita o controlador, que é o mestre de segurança, a controlar as conexões de segurança.

Controlador SmartGuard como sendo o mestre de segurança

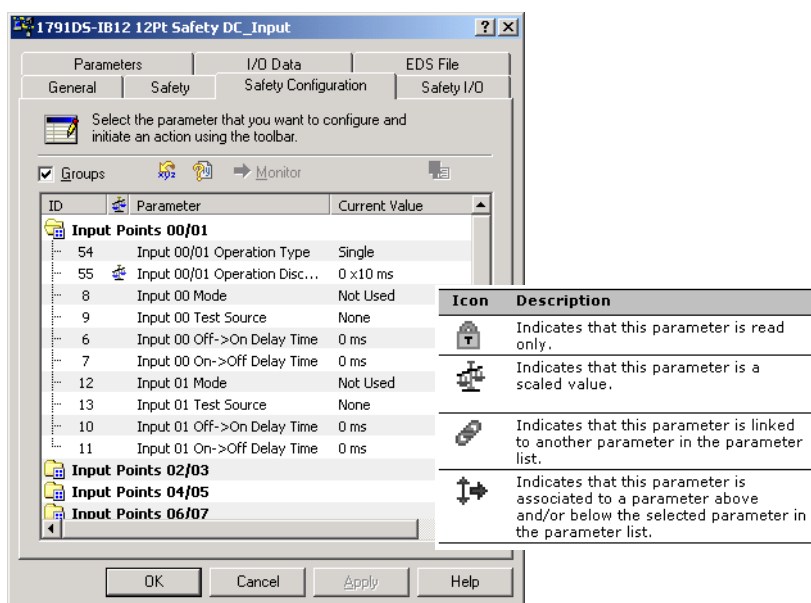


Configuração dos alvos de E/S de segurança CIP na rede do DeviceNet

Para configurar o módulo, clique duas vezes no módulo na visualização gráfica ou clique com o botão direito do mouse no módulo e selecione Properties.

Parâmetros Safety Input, Output e Test

Os parâmetros de segurança são configurados usando a guia Safety Configuration na caixa de diálogo Module Properties.



Canal único versus canal duplo equivalente ou canal duplo complementar

Podem-se configurar as entradas de módulos de E/S distribuídas tanto para o modo de canal simples como duplo. Isto informa ao módulo Guard I/O se são visualizadas as entradas individualmente (canal simples) ou como pares de entrada (canal duplo). As entradas de canal duplo podem ser configuradas como equivalentes, quando ambas as entradas devem sempre ser as mesmas ou como complementares, quando ambas as entradas devem sempre ser opostas.

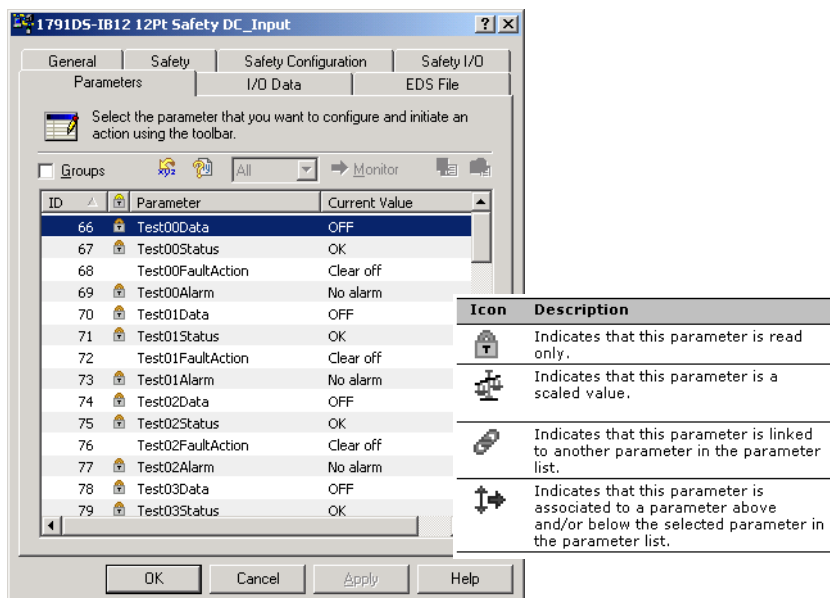
Se configurado como canal duplo, o módulo Guard I/O irá sempre enviar os dados de canal para o controlador SmartGuard como ambos os canais LO ou ambos os canais HI. Isto significa que as falhas de inconsistência de entrada na instrução SmartGuard nunca irão ocorrer.

Se desejar que a instrução SmartGuard faça o diagnóstico da entrada de segurança nos módulos Guard I/O, configure os módulos Guard I/O como canal simples. Isto permitirá que você use os indicadores de falha fornecidos pelas instruções SmartGuard no seu programa, o que é recomendado.

Se desejar realizar os diagnósticos da entrada de segurança no módulo Guard I/O com os indicadores de status do módulo e bits de status e não pelo uso de diagnósticos de instruções SmartGuard, configure o módulo Guard I/O como canal duplo complementar ou equivalente.

Parâmetros de entrada e saída padrão

Os módulos 1791DS mostrados aqui suportam dados padrão e dados de segurança. Configure os parâmetros-padrão de entrada e de saída usando a guia Parameters na caixa de diálogo Module Properties.



DICA

Outros equipamentos talvez tenham opções de configuração diferentes. Consulte o manual do usuário do seu equipamento para obter mais informações.

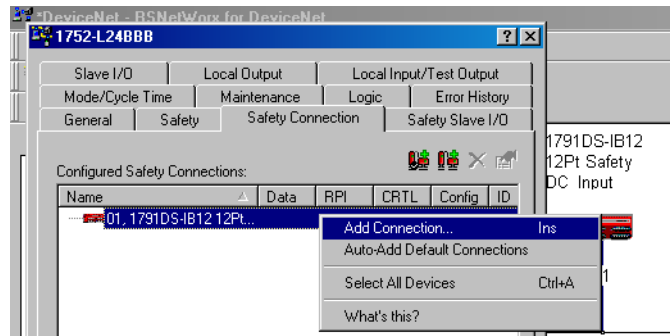
Fazer download das configurações do equipamento

Uma vez que você tiver configurado os parâmetros-padrão de módulo de E/S, faça o download da configuração para os módulos. Para fazê-lo no software RSNetWorx para DeviceNet, no menu Device, escolha Download to Device.

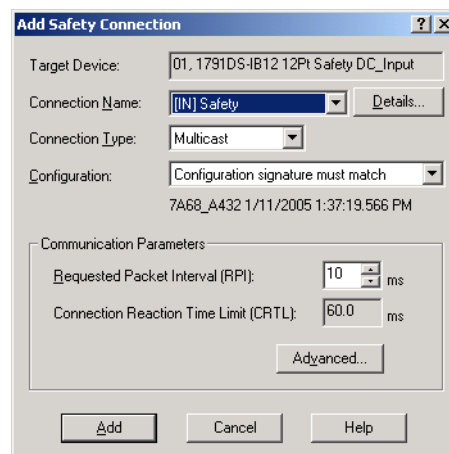
Configuração das conexões de E/S de segurança

As conexões de E/S de segurança são usadas para trocar dados automaticamente com os escravos de segurança sem a programação do usuário. Para realizar a comunicação de E/S de segurança com outros escravos, você deve configurar a conexão com o controlador SmartGuard.

1. Na guia Safety Connections, clique com o botão direito do mouse no módulo de E/S e selecione Add Connections para exibir todas as conexões disponíveis.



A caixa de diálogo Add Safety Connection permite que você configure uma conexão.



2. Selecione a conexão desejada, escolhendo o Nome da conexão.
3. Selecione um tipo de conexão, Multicast (somente conexões de entrada) ou Point-to-point (conexões de entrada ou de saída).
4. Selecione Configuration signature must match.

Esta seleção fará com que o controlador SmartGuard inclua a assinatura de configuração quando conectar ao módulo de E/S e o módulo de E/S irá aceitar a conexão apenas se a assinatura combinar com a que há no dispositivo.

IMPORTANTE

Caso não escolha Configuration signature must match, você é responsável por verificar a integridade da segurança do sistema por outros meios.

5. Verifique o limite de tempo de reação da conexão.

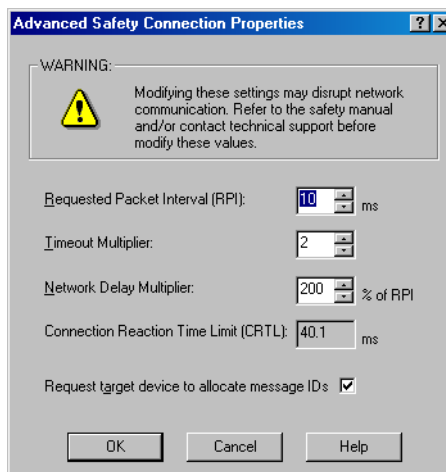
O limite de tempo de reação da conexão é a idade máxima dos pacotes de segurança na conexão associada. Se o período dos dados usado pelo dispositivo em consumo exceder o Limite de Tempo de Reação da Conexão, ocorrerá uma falha de conexão. Ajuste o limite de tempo de reação da conexão alterando o intervalo do pacote requisitado ou as propriedades de comunicação avançada conforme descrição nas etapas 6 e 7.

6. Defina o intervalo do pacote requisitado (RPI).

O RPI especifica o período no qual os dados são atualizados em uma conexão. O intervalo do pacote requisitado é inserido em incrementos de 1 ms, e o controlador suporta uma faixa válida de 5 a 500 ms com um padrão de 10 ms. Outros dispositivos alvo talvez tenham mais restrições de RPI limitado. Consulte a documentação de cada tipo de dispositivo alvo para determinar sua faixa suportada e os valores incrementais.

Modificar o RPI afeta o limite de tempo de reação da conexão. Para restrições de temporização simples, configurar o RPI geralmente é suficiente. No entanto, para especificações mais complexas, clique em Advanced para ajustar os valores de temporização que afetam o limite de tempo de reação da conexão com mais precisão.

7. Defina as propriedades da conexão de segurança avançada (se necessário).



- Multiplicador de tempo-limite (Timeout Multiplier) – o Multiplicador de tempo-limite determina o número de RPIs para aguardar um pacote antes de declarar um 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. Um Multiplicador de tempo-limite igual a 2 indica que uma mensagem pode estar perdida desde que pelo menos uma mensagem seja recebida em 2 vezes o RPI (2 x RPI).
- Multiplicador de atraso da rede (Network Delay Multiplier) – o Multiplicador de atraso da rede define o tempo de transporte da mensagem aplicado pelo protocolo de comunicação. Esse campo especifica o atraso do ciclo completo do produtor até o consumidor e de volta ao produtor. É possível usar o multiplicador de atraso da rede para reduzir ou aumentar o limite de tempo de reação da conexão nos casos em que o tempo de transporte da mensagem aplicado é significativamente menor ou maior que o RPI.

8. No menu File, escolha Save para salvar a sua configuração.

Altere uma conexão de E/S

ATENÇÃO

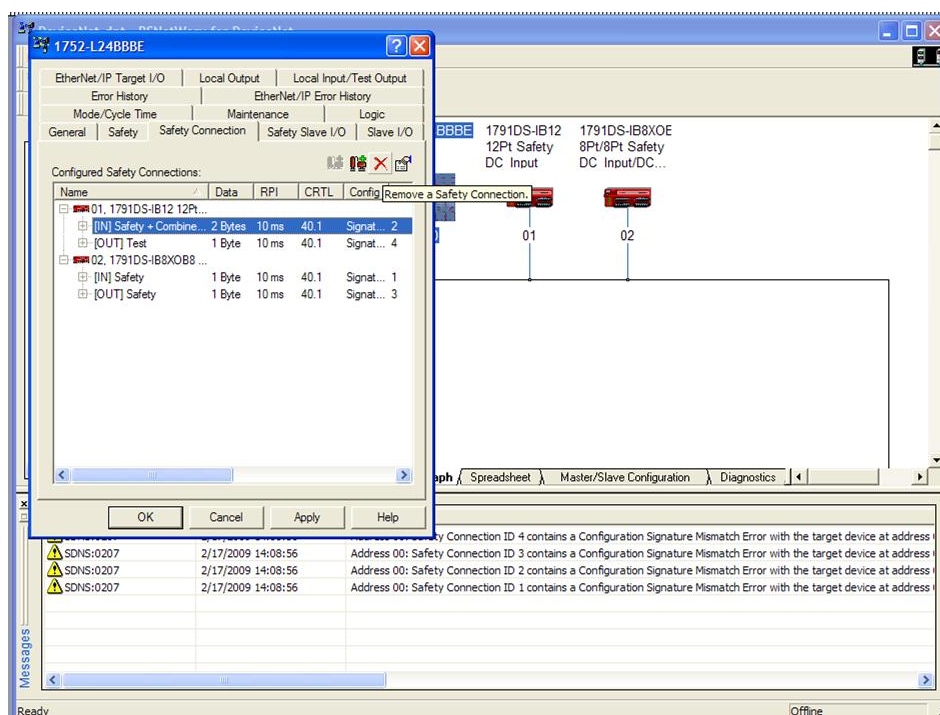


Quando a lógica é programada usando os módulos de E/S distribuída (DIO) com o controlador SmartGuard, e uma conexão de segurança a um módulo DIO for apagada (ou apagada e re-adicionada), as conexões de E/S remotas no logic editor serão marcadas como inválidas e podem ser movidas para o bloco de funções errado. Não será possível fazer o download até que esses erros sejam corrigidos.

Se uma conexão a um módulo DIO for apagada depois que a lógica foi escrita, deve-se retornar à lógica e verificar ou ajustar as marcações no seu programa aos blocos de funções corretos. Tome nota das conexões de segurança e mapeamentos antes de apagar ou restaurar as conexões. Verifique estas conexões antes de operar a lógica na sua aplicação.

Siga este procedimento para modificar suas conexões de segurança.

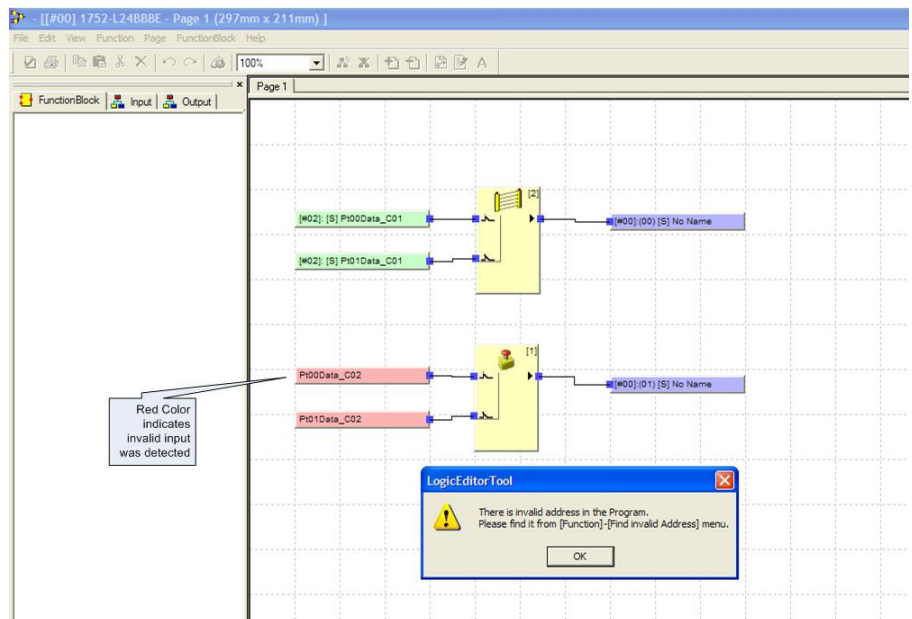
1. Destaque a conexão de E/S que deseja modificar ou remover.



2. Clique no botão 'x'.

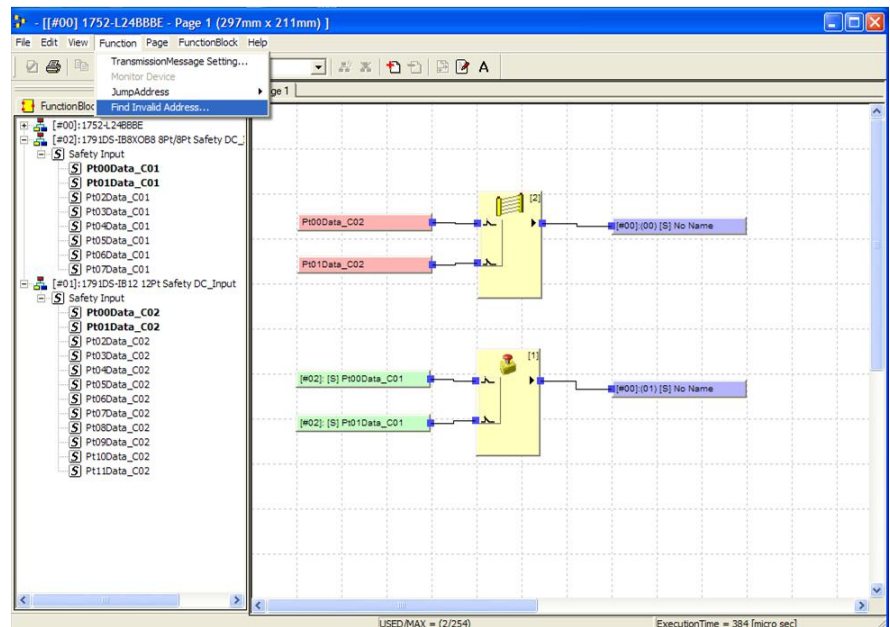
Isto permitirá que a conexão de E/S seja removida.

Neste exemplo, na próxima vez que você visualizar sua lógica, uma caixa de diálogo de mensagem de erro aparecerá.

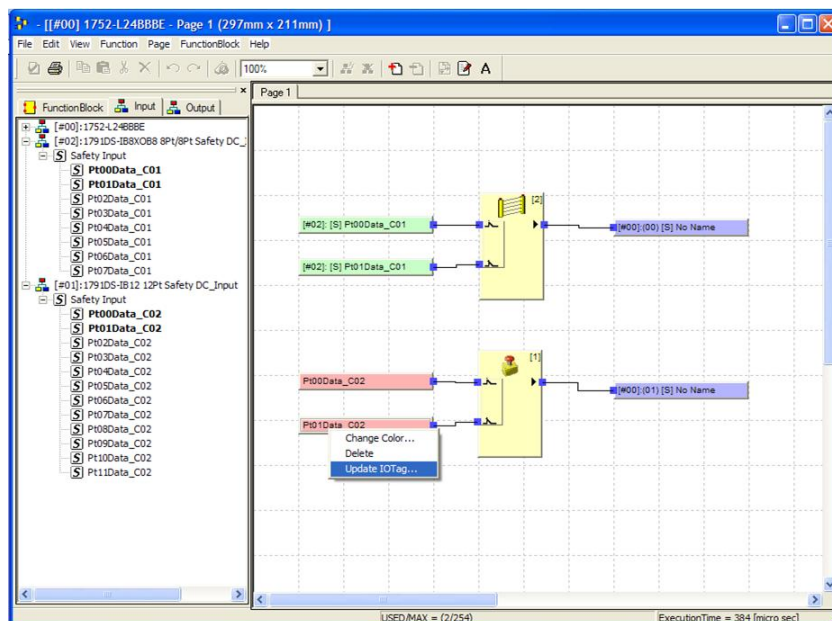


3. Clique em OK.

4. Para localizar endereços inválidos, escolha **Function>Find Invalid Address** ou localize todas as marcações vermelhas de E/S e clique com o botão direito na marcação vermelha.



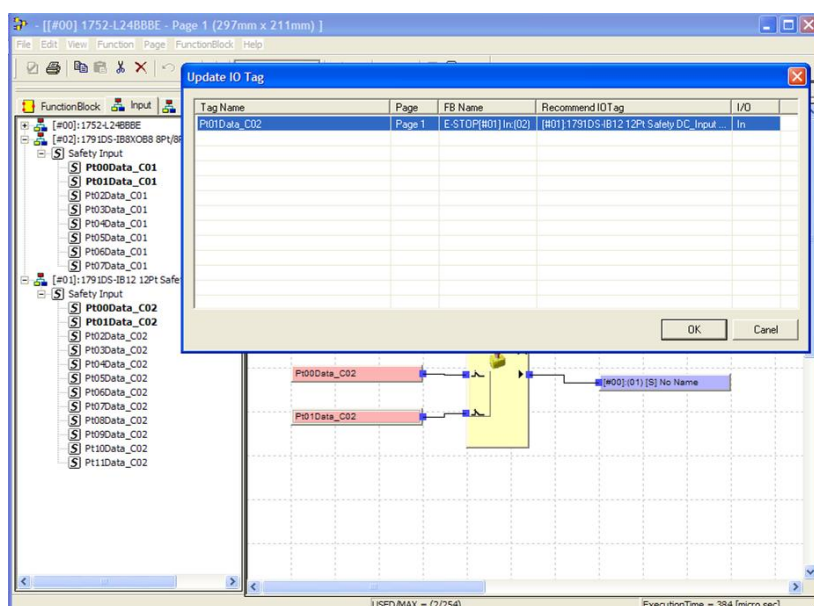
O menu aparece na marcação inválida.



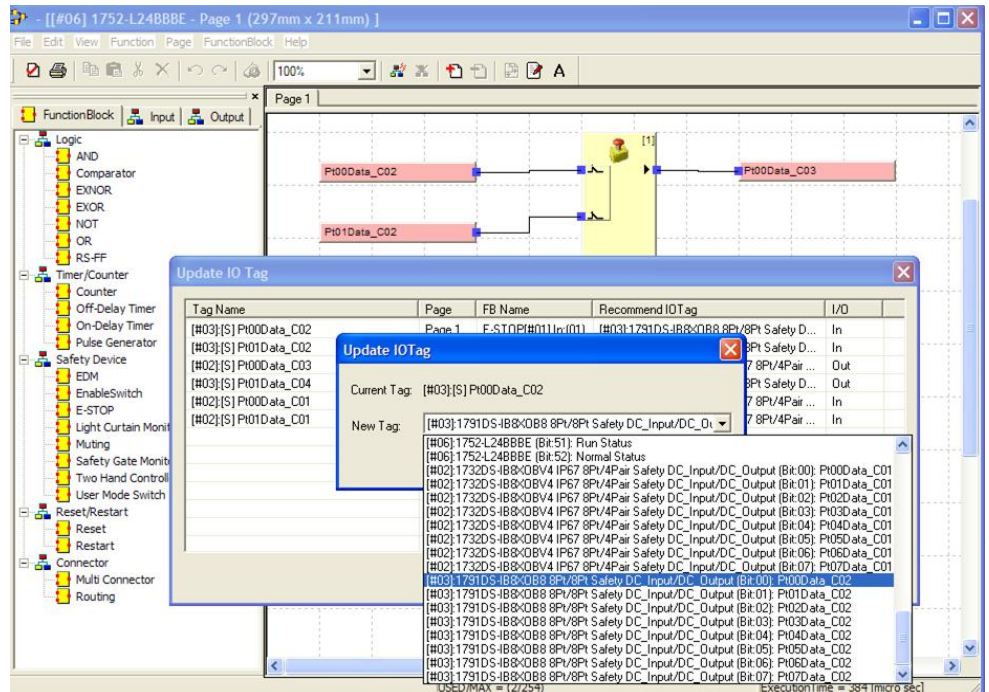
5. Clique com o botão direito na marcação inválida.

O menu Update IO Tag aparece.

A caixa de diálogo mostra o erro de marcação com a marcação recomendada. A marcação recomendada é uma sugestão do software de que ponto de E/S a marcação foi conectada originalmente. Mas deve-se verificar e confirmar clicando duas vezes na opção sugerida.



6. Se a marcação recomendada estiver correta, destaque a marcação e clique OK. Se a marcação recomendada não estiver correta, clique duas vezes na linha e uma nova caixa de diálogo aparece e permite que uma outra marcação seja selecionada. Também pode ser rolada para mais opções.



7. Clique em OK.

ATENÇÃO



Se várias marcações aparecerem na caixa de diálogo Update I/O Tag, todas as marcações devem ser aceitas ou as alternativas escolhidas antes de selecionar OK. De outra forma, será usada a marcação E/S recomendada.

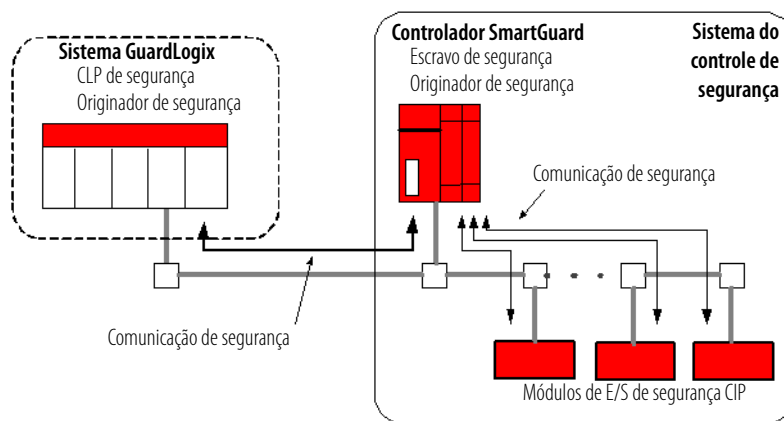
Consulte o Manual de referência de segurança de controladores SmartGuard 600, publicação [1752-RM001](#), para recomendações sobre o ajuste do seu sistema de segurança.

Ajustando o controlador como um escravo de segurança

Por ser um escravo de segurança, o controlador pode realizar comunicação de E/S de segurança com um máximo de 4 conexões, usando até 16 bytes por conexão. As conexões podem ser singlecast ou multicast. No entanto, para uma conexão multicast, o número total de mestres que podem se comunicar é de 15.

Para que o controlador SmartGuard realize a comunicação de E/S de segurança como sendo um escravo de segurança, os dados de E/S do escravo de segurança devem ser criados e as conexões de E/S de segurança, configuradas no mestre de segurança.

Controlador SmartGuard como escravo de segurança e originador de segurança



Quando o controlador é operado como sendo um escravo de segurança, é possível configurar as montagens do escravo de segurança para transferir os dados de E/S local (dados do monitor), do controlador e do status de E/S e os dados de E/S distribuída para um mestre de segurança. O mestre de segurança também pode gravar dados de segurança no controlador SmartGuard escravo, que pode ser usado em seu programa aplicativo.

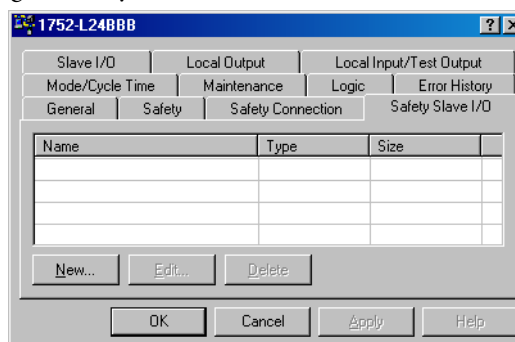
Quando os dados de status são definidos, o status é alocado no início da área de E/S remota, com os dados de status antes dos dados de E/S local. Os tags registrados pelo usuário vêm em seguida. As áreas de status não definidas não são reservadas. Todos os dados válidos são alocados sem áreas não atribuídas.

Criar dados de E/S do escravo de segurança

Siga estas etapas para criar uma montagem do escravo de segurança.

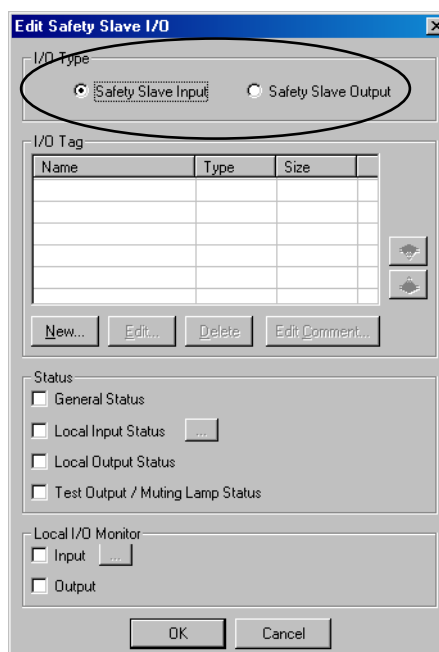
1. No software RSNetWorx para DeviceNet, clique com o botão direito do mouse no controlador SmartGuard que agirá como o escravo de segurança e escolha Properties.

2. Clique na guia Safety Slave I/O.



3. Clique em New.

4. Na caixa de diálogo Edit Safety Slave I/O, escolha I/O Type, Safety Slave Input ou Safety Slave Output.



Tipo de E/S	Sentido dos dados da segurança
Entrada do escravo de segurança	Escravo de segurança do controlador SmartGuard —> Mestre de segurança
Saída do escravo de segurança	Mestre de segurança —> Escravo de segurança do controlador SmartGuard

5. Para adicionar informações de status para tipos de entrada de segurança, verifique a caixa de verificação de status apropriada.

Nome do tag	Dimensões dos dados	Tipo do atributo
Status geral	Byte	Não segurança
Status da entrada local	Palavra	Segurança
Status da saída local	Byte	Segurança
Saída de teste/status da lâmpada muting	Byte	Não segurança

Entre os tipos de saída de segurança não podem estar os dados de status. Só é possível ler os dados de status, e não gravá-los.

6. Para adicionar os dados de monitoração de E/S locais para tipos de entrada de segurança, selecione a caixa de verificação de monitoração de E/S local adequada.

Nome do tag	Dimensões dos dados	Tipo do atributo
Monitor de entrada local 1 (entradas 0 a 7)	Byte	Segurança
Monitor de entrada local 2 (entradas 8 a 15)	Byte	Segurança
Monitor de saída local (saídas 0 a 7)	Byte	Segurança

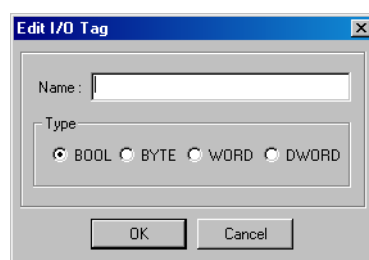
Entre os tipos de saída de segurança não podem estar os dados do monitor de E/S local. Só é possível ler os valores de entrada e de saída; não é possível gravá-los.

7. Clique em New para criar um tag de E/S da montagem de segurança.

Vários tags de E/S podem ser definidos em uma montagem de E/S. Tags de E/S para até 16 bytes podem ser definidos em cada montagem de E/S. Os tags de E/S definidos aqui podem ser usados no Logic Editor.

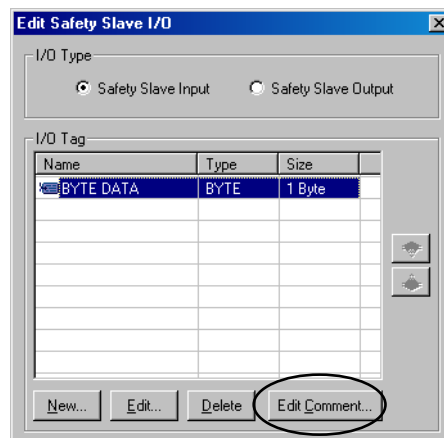
Insira pontos de entrada ou de saída específicos caso você não queira compartilhar todos eles. Também é possível compartilhar entradas ou saídas de E/S distribuídas digitando os nomes dos tags aqui.

8. Digite um nome para o tag e escolha o tipo: BOOL, BYTE, WORD ou DWORD.

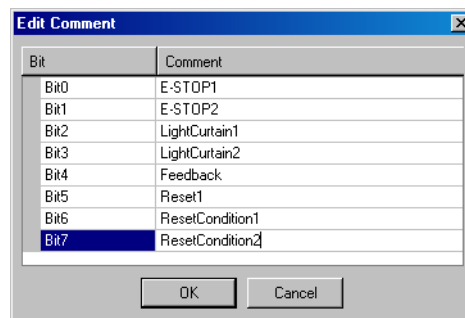


9. Clique em OK.

10. Para criar um nome de marcação para cada bit em uma montagem de E/S, siga estas etapas.
 - a. Selecione a montagem aplicável e clique em Edit Comment.



- b. Digite um comentário para cada bit no tag.



Os comentários do nome do tag digitados aqui são exibidos no Logic Editor.

- c. Clique em OK.
11. Clique em OK novamente para retornar à guia Safety Slave I/O.
12. Crie montagens adicionais de entrada ou de saída do escravo de segurança conforme necessário para a aplicação, repetindo as etapas 3 a 11.
13. Para salvar suas configurações, no menu File, escolha Save.

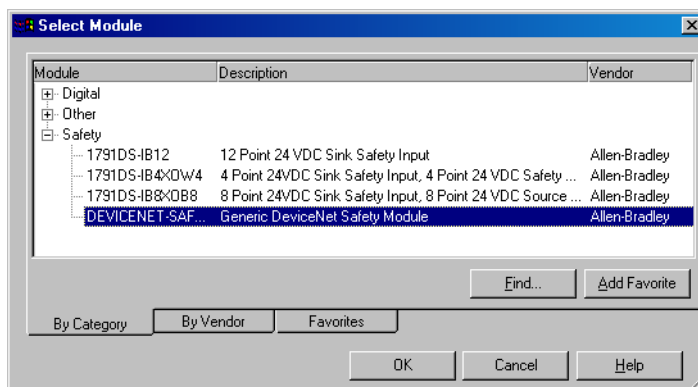
Uso do perfil genérico da segurança no software RSLogix 5000

É possível conectar-se ao controlador escravo SmartGuard usando o perfil genérico da segurança no software RSLogix 5000.

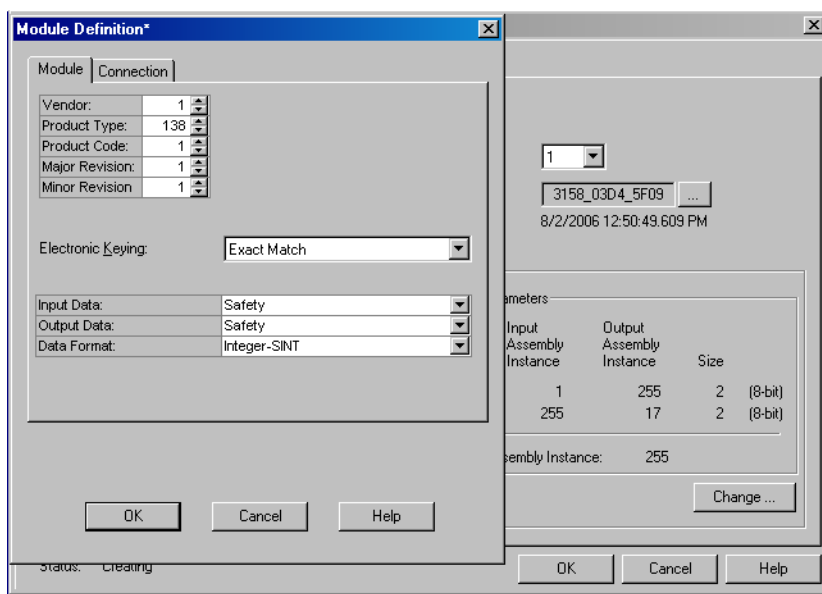
Siga estas etapas para se conectar ao controlador.

1. No software RSLogix 5000, clique com o botão direito do mouse na rede do DeviceNet e escolha New Module.

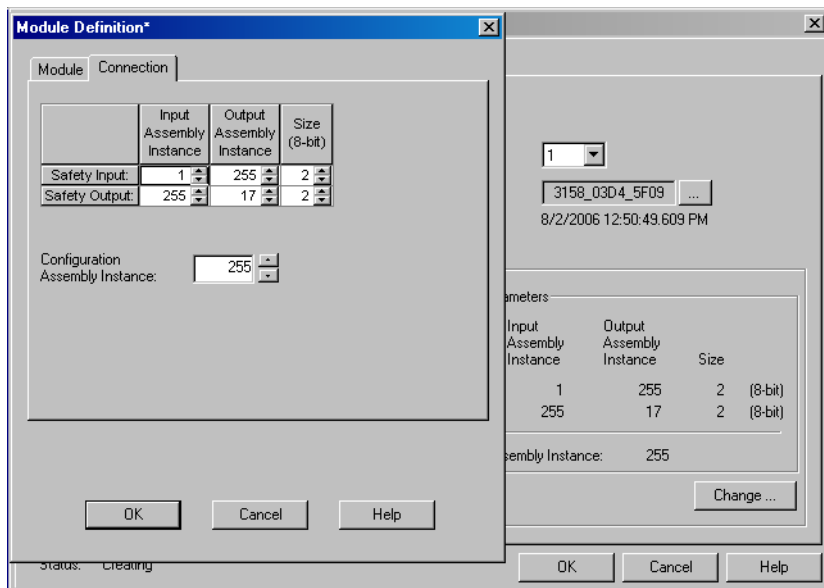
2. Selecione Generic DeviceNet Safety Module e clique em OK.



3. Na caixa de diálogo New Module, clique em Change.
4. Na caixa de diálogo Module Definition, defina os parâmetros conforme mostrados.



5. Na guia Module Definition, clique na guia Connection.



6. Defina os parâmetros de entrada e de saída da segurança usando as seguintes tabelas.

Montagens de entrada

Quando o nome da entrada do escravo de segurança for	Defina o número de instância de entrada do perfil genérico como	Defina o número de instância de saída do perfil genérico como
Entrada de segurança 1	1	255
Entrada de segurança 2	2	255
Entrada de segurança 3	3	255
Entrada de segurança 4	4	255

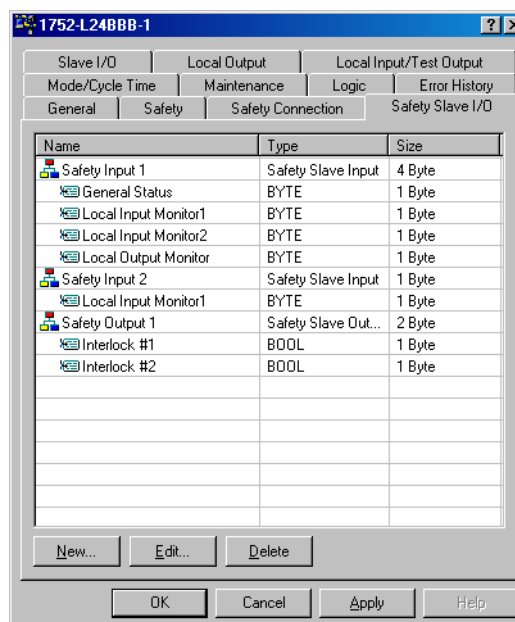
Montagens de saída

Quando o nome da saída do escravo de segurança for	Defina o número de instância de entrada do perfil genérico como	Defina o número de instância de saída do perfil genérico como
Saída de segurança 1	255	17 (para 0x11)
Saída de segurança 2	255	18 (para 0x12)
Saída de segurança 3	255	19 (para 0x13)
Saída de segurança 4	255	20 (para 0x14)

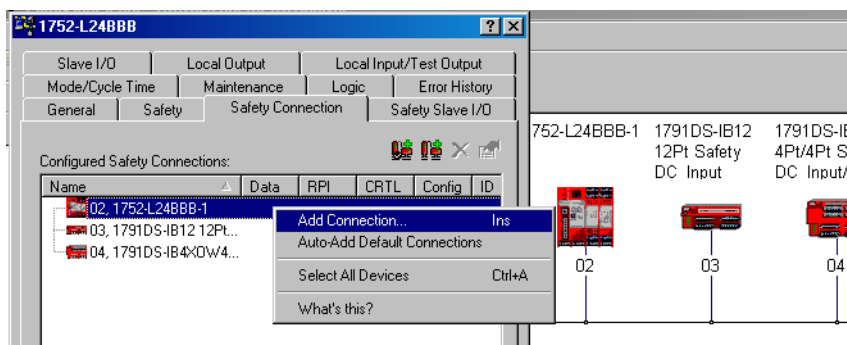
Controlador SmartGuard para intertravamento de segurança do controlador SmartGuard

O intertravamento de segurança permite que os controladores SmartGuard compartilhem dados de segurança e tomem decisões com base nas entradas e saídas um do outro. O intertravamento de segurança permite que você distribua o controle de segurança para vários controladores SmartGuard que funcionam juntos.

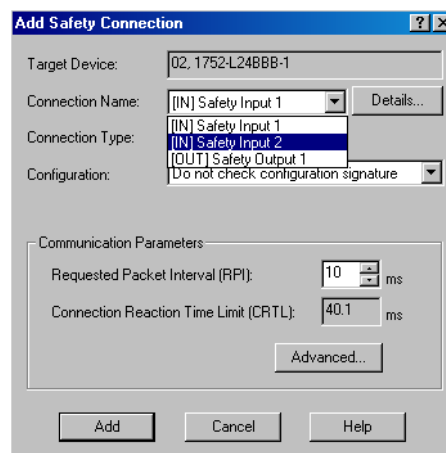
1. Configure uma das E/S do escravo de segurança do SmartGuard conforme descrição em [Criar dados de E/S do escravo de segurança](#) na [página 90](#).



2. Na guia Safety Connections do outro controlador SmartGuard, o que será o mestre de segurança, clique com o botão direito do mouse no controlador SmartGuard e escolha Add Connection.

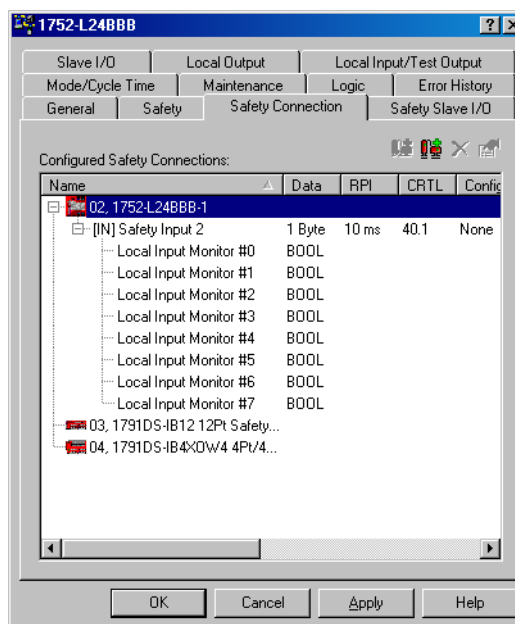


3. No menu Connection Name, escolha a montagem de E/S de segurança que deseja usar.



4. Clique em Add.

Agora o controlador SmartGuard que está agindo como o mestre de segurança conseguirá ler as entradas do outro controlador SmartGuard, 0 a 7.



Ajustando o controlador como um escravo padrão DeviceNet

Por ser um escravo padrão DeviceNet, o controlador pode realizar a comunicação de E/S padrão com 1 mestre padrão com até 2 conexões usando até 16 bytes por conexão (128 bytes para dados de entrada para a comunicação EtherNet/IP). O controlador SmartGuard também pode responder a mensagens padrão explícitas.

As informações de status interno do controlador e uma área especificada de E/S podem ser alocadas no mestre padrão.

IMPORTANTE

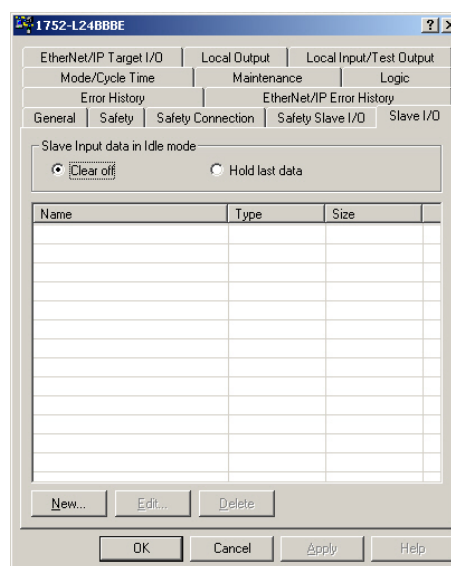
Os dados gravados no controlador SmartGuard por meio da sua conexão de escravo padrão devem ser considerados como sendo de não segurança e não devem ser usados para controlar as funções de segurança no programa aplicativo do SmartGuard.

Para que o controlador SmartGuard realize a comunicação de E/S padrão como sendo um escravo padrão, os dados de E/S do escravo padrão devem ser criados e as conexões de E/S configuradas no mestre padrão.

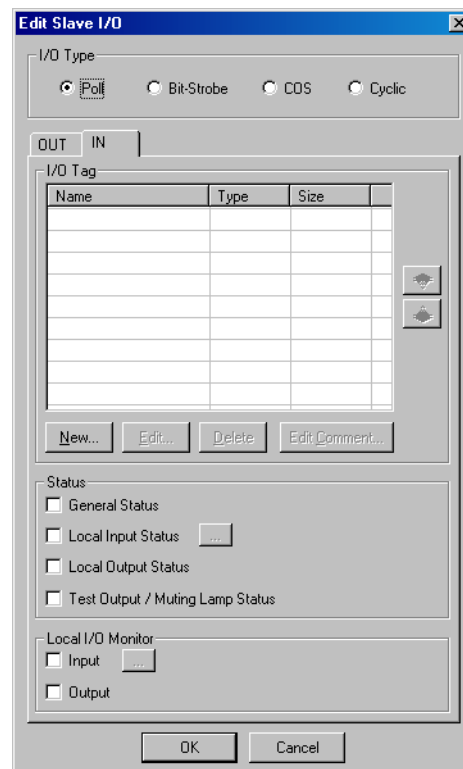
Criação de dados de E/S do escravo padrão

Siga estas etapas para criar montagens de E/S de escravo padrão.

1. No software RSNetWorx for DeviceNet, clique com o botão direito do mouse no controlador SmartGuard que agirá como o escravo padrão e escolha Properties.
2. Clique na guia Slave I/O.



3. Configure o controlador escravo para limpar ou manter os dados mais recentes de uma montagem de entrada transmitidos pelo controlador escravo para o mestre padrão quando:
 - o controlador escravo é alterado do modo em operação para o modo inativo.
 - o controlador detecta um erro como, por exemplo, um erro de comunicação em uma cadeia de segurança que define os dados para um tag de E/S em uma montagem de entrada.
4. Clique em New.
5. Clique no tipo de E/S: Poll, Bit-Strobe, COS ou Cyclic.



Os dados de saída não podem usar um tipo de conexão bit-strobe porque os dados bitstrobe não podem ser produzidos pelo mestre padrão. Além disso, o tamanho máximo da entrada de dados bitstrobe para o mestre padrão é de 8 bytes. As conexões COS e cíclica não podem ser usadas simultaneamente.

6. Para adicionar informações de status para tipos de entrada, selecione as caixas de verificação de status (opcional).

Quando o tipo de E/S é Entrada, é possível incluir as seguintes informações sobre o status na montagem de E/S.

Nome do tag	Dimensões dos dados	Tipo do atributo
Status geral	Byte	Não segurança
Status da entrada local	Palavra	Não segurança
Status da saída local	Byte	Não segurança
Saída de teste/status da lâmpada muting	Byte	Não segurança

7. Para adicionar dados de monitoração de E/S locais para tipos de entrada, selecione a caixa de verificação de monitoração de E/S local apropriada.

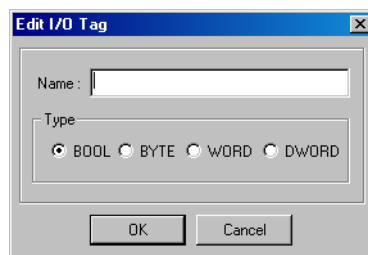
Nome do tag	Dimensões dos dados	Tipo do atributo
Monitor de entrada local 1 (entradas 0 a 7)	Byte	Não segurança
Monitor de entrada local 2 (entradas 8 a 15)	Byte	Não segurança
Monitor de saída local (saídas 0 a 7)	Byte	Não segurança

Entre os tipos de saída não podem estar os dados do monitor de E/S local. Só é possível ler os valores de entrada e de saída; não é possível gravá-los.

8. Clique em New para criar um tag de E/S.

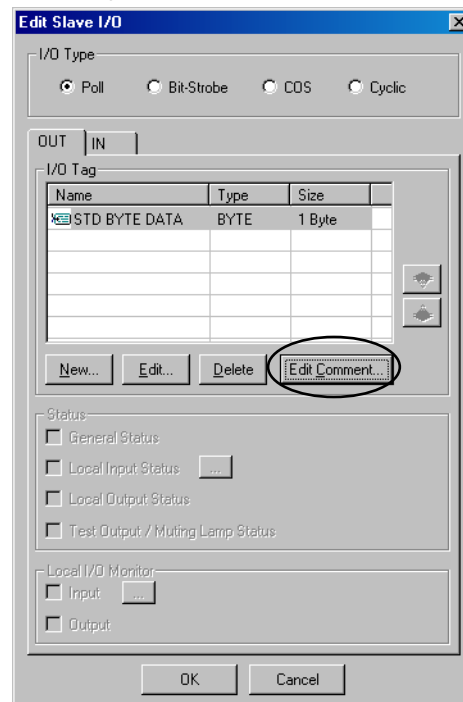
Vários tags de E/S podem ser definidos em uma montagem de E/S. Tags de E/S para até 16 bytes podem ser definidos em cada montagem de E/S. Os tags de E/S definidos aqui podem ser usados no Logic Editor.

9. Digite um nome para a marcação e clique no tipo: BOOL, BYTE, WORD ou DWORD.



10. Clique em OK.

11. Para criar um nome de marcação para cada bit em uma montagem de E/S, siga estas etapas.
 - a. Selecione a montagem aplicável e clique em Edit Comment.

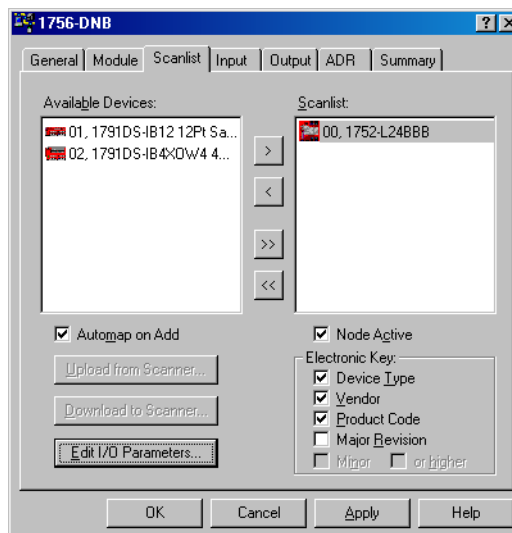


- b. Digite um comentário para cada bit no tag.

Os comentários do nome do tag digitados aqui são exibidos no Logic Editor.
 - c. Clique em OK.
12. Clique em OK novamente para retornar à guia Slave I/O.
13. Crie montagens adicionais de entrada ou de saída do escravo conforme necessário para a aplicação repetindo as etapas 4 a 12.
14. No menu File, escolha Save para salvar a sua configuração.

Adição do escravo padrão SmartGuard à lista de varredura do mestre padrão

Para disponibilizar as montagens de E/S do escravo padrão para o mestre padrão, adicione o controlador escravo padrão SmartGuard à lista de varredura do mestre.



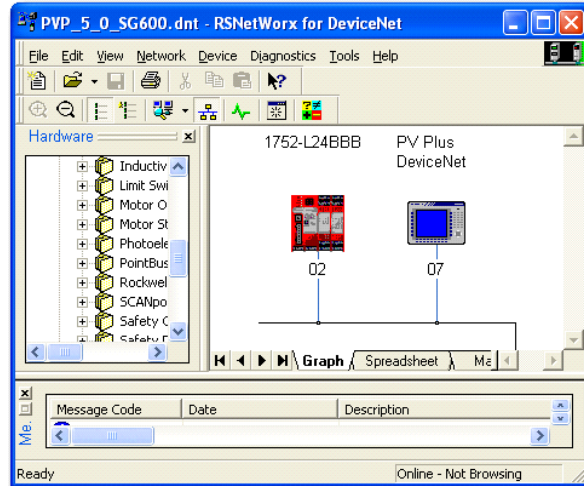
Consulte a documentação de usuário do mestre padrão para obter mais informações sobre como configurar o dispositivo específico.

Salve a configuração no software RSNetWorx for DeviceNet escolhendo File>Save.

Leitura e gravação de e para o controlador SmartGuard para uma interface PanelView Plus

Esta seção descreve como ler e gravar do controlador SmartGuard e a interface PanelView Plus. O controlador SmartGuard é um escravo padrão dentro desta arquitetura. Consulte [página 98](#) para mais informações.

Controlador SmartGuard e interface PanelView Plus na rede

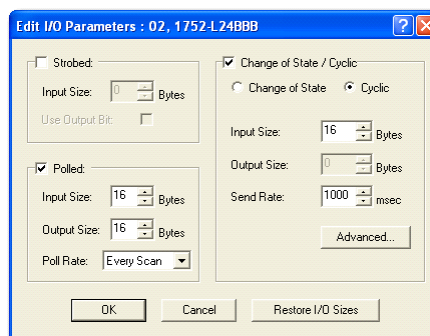


Até duas conexões podem ser selecionadas dos quatro tipos de conexões, mas apenas uma conexão de cada tipo pode ser feita. Por exemplo, uma conexão com polling e uma conexão COS podem ser feitas, mas não duas conexões com polling. Tanto com polling quanto COS/Cíclico permitem tanto entradas como saídas (leitura e gravação) em uma conexão simples.

Uma conexão com polling que usa tanto entradas como saídas pode ter 16 bytes de dados de entrada e 16 bytes de dados de saída. Se outra conexão for adicionada, podem-se ter 16 bytes adicionais de dados.

Se for usada uma conexão com polling e então for adicionada uma conexão COS/Cíclica, a saída fica indisponível. A configuração máxima de dados é mostrada abaixo.

Caixa de diálogo Edit I/O Parameters



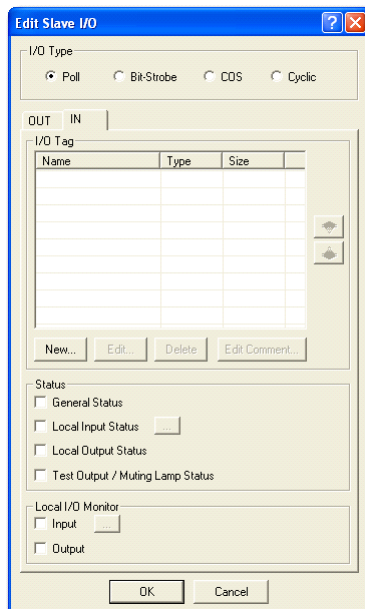
Esta configuração permite 32 bytes de dados de entrada (16 via polling e 16 via COS ou Cíclico) e 16 bytes de dados de saída via conexão com polling. Esta configuração é descrita em mais detalhes neste capítulo.

Leia BOOLs do controlador SmartGuard e os exiba na interface PanelView Plus

Siga este procedimento para ler BOOLs do controlador SmartGuard e os exiba na interface PanelView Plus.

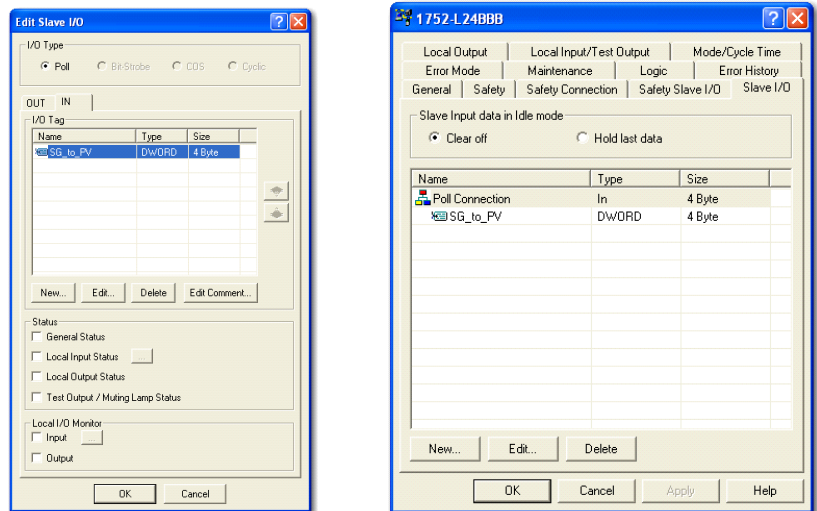
1. Abra o software RSNetWorx.
2. Abra as propriedades SmartGuard.
3. Clique na guia Slave I/O.

A seguinte caixa de diálogo aparece.



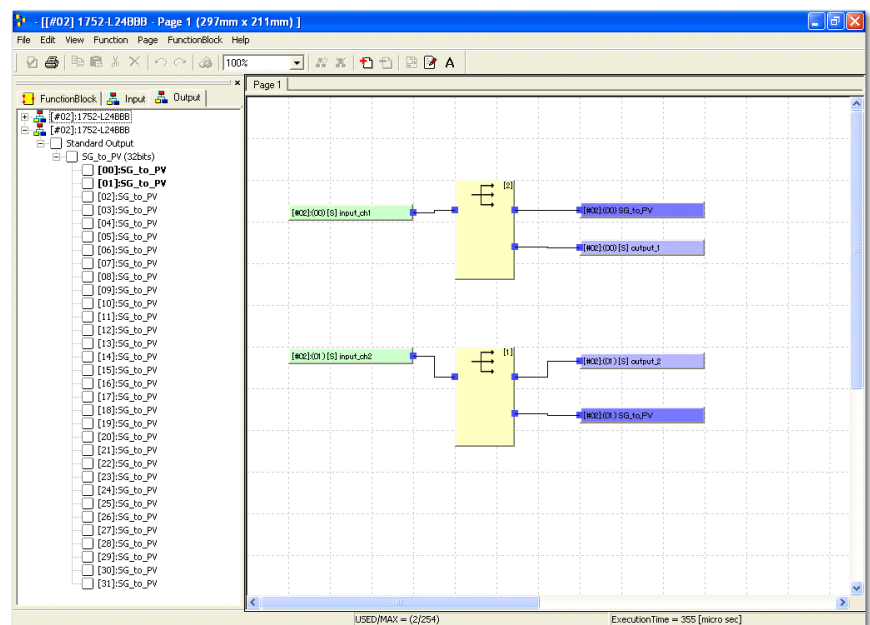
4. Clique na guia IN.
5. Insira os nomes dos tags que serão lidos pela interface PanelView Plus.

Neste caso, um tag simples de 4 bytes foi criado e usará uma conexão com polling. Estes 4 bytes são lidos pela interface PanelView Plus.



Mesmo que tenha sido criado um tag DWORD, você terá acesso a todos os 32 bits do DWORD no editor SmartGuard. O código de amostra SmartGuard está controlando dois dos 32 bits.

Os tags em negrito na lista de tags são usados em código.

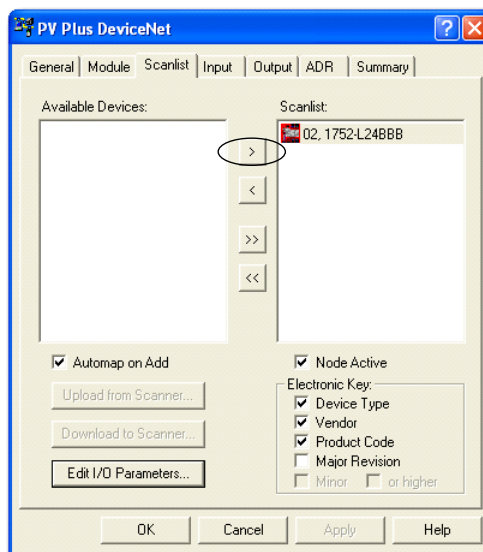


6. Faça o download da configuração do controlador SmartGuard 600.

Configure a lista de varredura do scanner PanelView

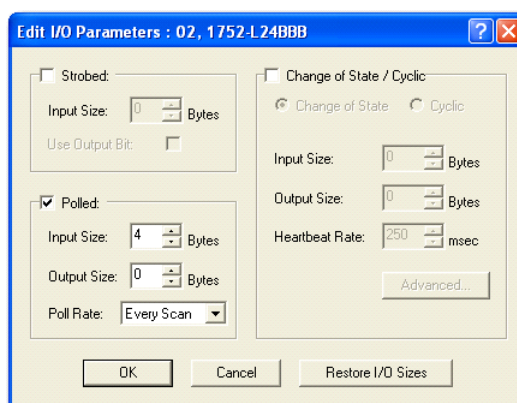
Siga este procedimento para configurar a lista de varredura do scanner DeviceNet PanelView Plus.

1. Clique na guia Scanlist.
2. Clique na seta à direita para mover o controlador SmartGuard para a lista de varredura.



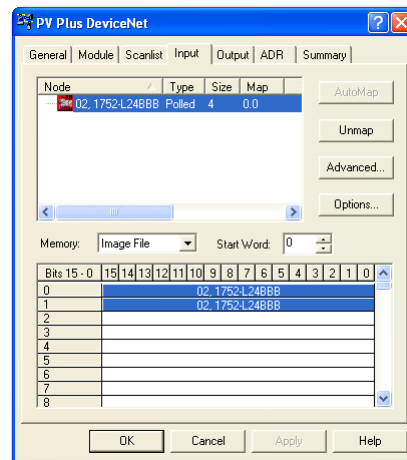
3. Clique em Edit I/O Parameters e verifique se está configurado conforme mostrado abaixo.

O exemplo tem uma conexão com polling de 4 bytes que será uma entrada à interface PanelView Plus.



Como o Automap on Add foi verificado, o seguinte mapeamento ocorreu automaticamente.

- Verifique que os 4 bytes de dados de entrada estão mapeados conforme mostrado.



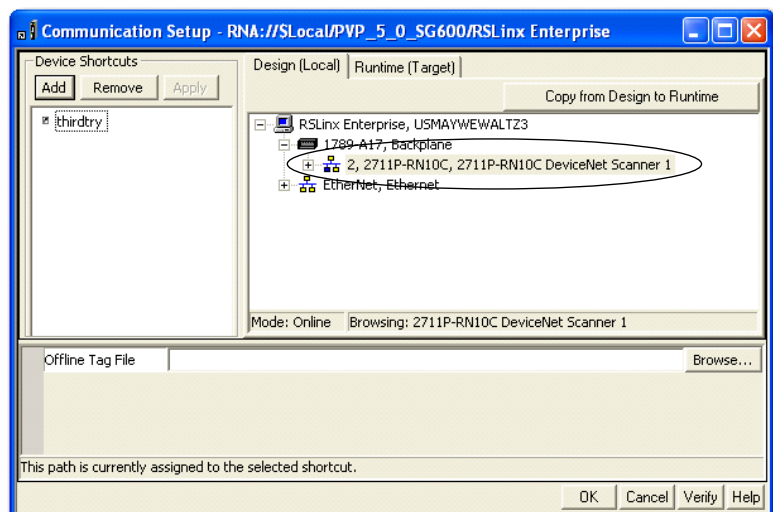
- Clique com o botão direito na interface PanelView Plus no software RSNetWorx e escolha Download to Device.

Configure o scanner RN10C DeviceNet

Siga este procedimento para configurar o scanner RN10C DeviceNet.

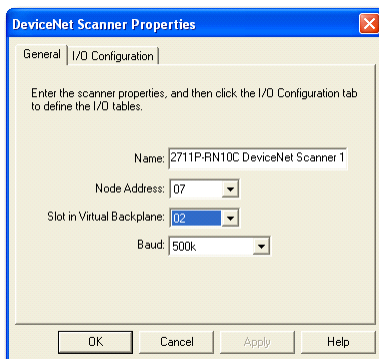
O atalho no software RSLinx Enterprise deve aparecer similar ao mostrado.

Observe que o número de slot do scanner RN10C é 2.



- Clique com o botão direito no scanner RN10C e escolha Properties.
- Insira o nome do scanner.

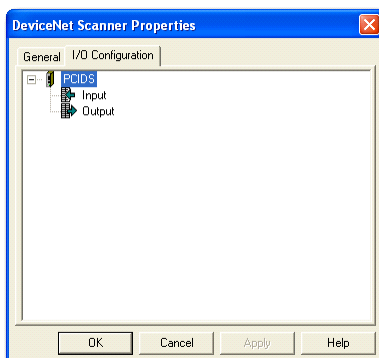
3. No menu apropriado, escolha o endereço do nó, slot no backplane virtual, e Baud rate.



A interface PanelView Plus é configurada para o nó 7 DeviceNet. O controlador SmartGuard tem as minisseletores configuradas para uma detecção automática (esquerda/esquerda/esquerda/direita de cima para baixo). Escolha a baud rate apropriada para a sua aplicação.

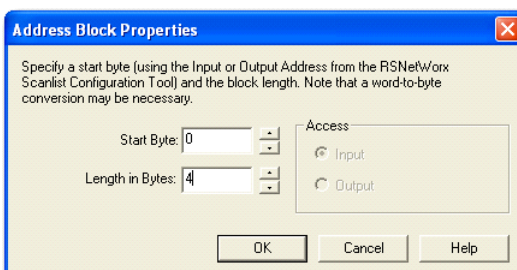
4. Clique na guia I/O Configuration.

A seguinte caixa de diálogo aparece.



5. Clique com o botão direito em Input e escolha Add Address Block.

A seguinte caixa de diálogo aparece.

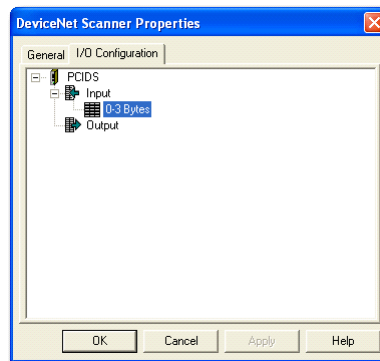


6. Insira 4 como o comprimento em bytes.

Isto irá combinar com o que o scanner está lendo no controlador SmartGuard.

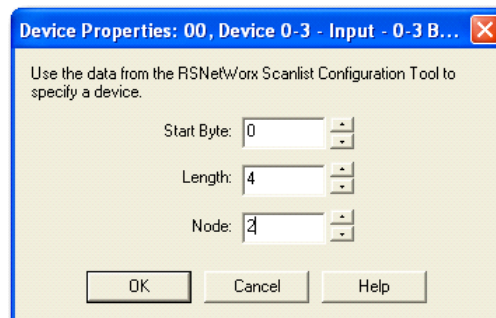
7. Clique em OK.

A configuração de E/S aparece.



8. Clique com o botão direito em 0-3 Bytes e escolha Add Devices.

A seguinte caixa de diálogo aparece.

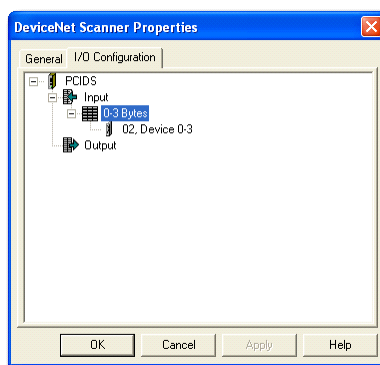


9. Configure o número do nó para combinar com o seu controlador SmartGuard.

O número do nó é 2 neste exemplo.

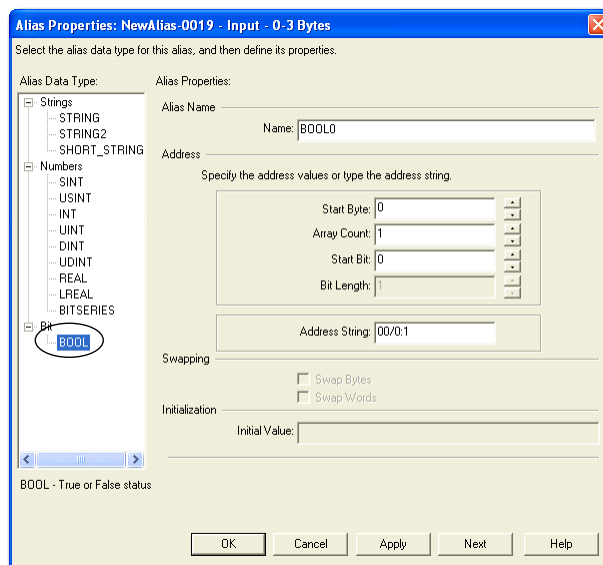
10. Clique em OK.

A seguinte caixa de diálogo aparece.



11. Clique com o botão direito em 0-3 Bytes e escolha Add Alias.

A seguinte caixa de diálogo aparece.

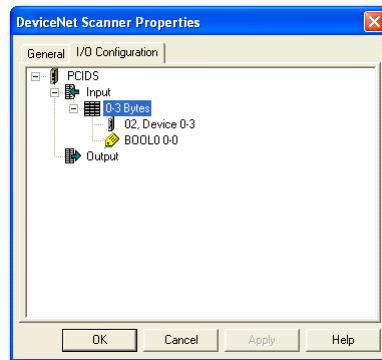


12. Selecione o tipo de dados em negrito (BOOL) e, no menu apropriado, escolha o byte inicial, a contagem de faixa e o bit inicial.

Os valores mostrados acima representam o bit 0 do primeiro byte.

13. Insira o nome.
14. Clique em OK.

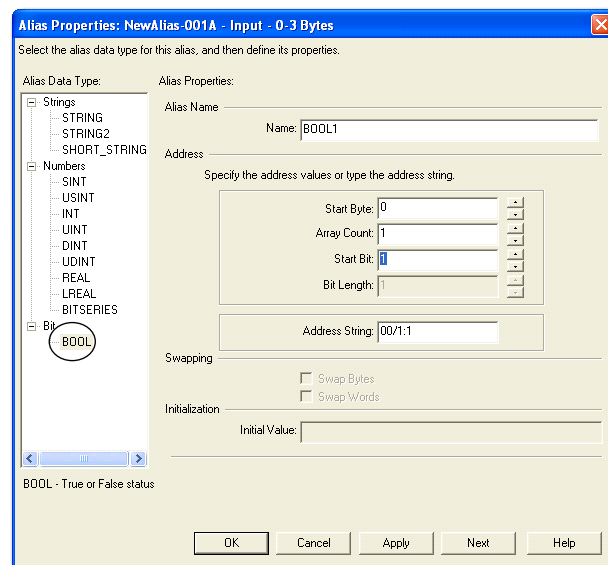
A seguinte caixa de diálogo aparece.



Para adicionar um segundo BOOL que representa o bit 1 do primeiro byte, siga este procedimento.

1. Clique com o botão direito em 0-3 Bytes e escolha Add Alias.

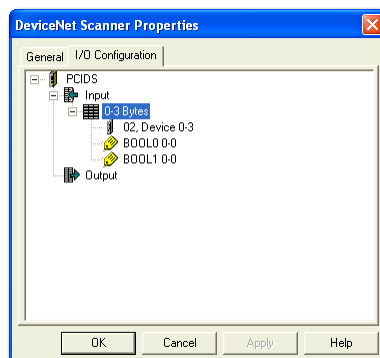
A seguinte caixa de diálogo aparece quando o tipo de dados BOOL é selecionado.



2. No menu apropriado, escolha o byte inicial, a contagem de faixa e o bit inicial.
3. Insira o nome.

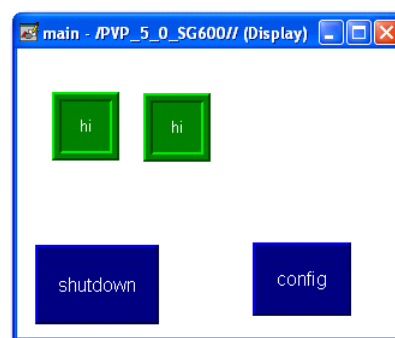
4. Clique em OK.

A seguinte caixa de diálogo aparece.

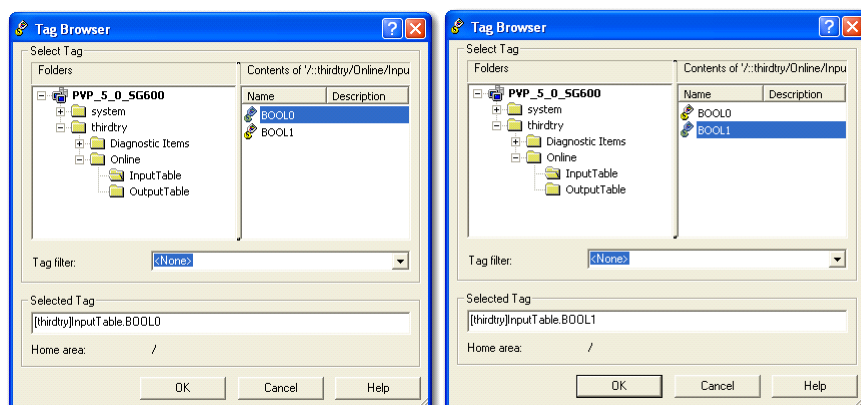


5. Clique em OK.

A etapa final é a criação do gráfico PanelView Plus que lê os tags alias. Este exemplo usará dois indicadores de múltiplos estados que leem os dois aliases.



Os tags para cada um dos indicadores de múltiplos estados podem ser procurados usando o software RSLinx Enterprise. Selecione os tags conforme mostrado.



Finalmente, você precisará salvar seu projeto, gerar um arquivo Runtime, e fazer o download para a interface PanelView Plus.

Leia e grave do e para o controlador SmartGuard a partir da interface PanelView Plus simultaneamente

Este exemplo mostra como usar os dois botões pulsadores mantidos em uma tela PanelView Plus para controlar dois tags no controlador SmartGuard 600. Para realizar isto, um único byte de dados é enviado da interface PanelView Plus para o controlador SmartGuard. BOOL não existe em propriedades do scanner PanelView Plus nem no controlador SmartGuard. Mesmo que você crie um tag BOOL no controlador SmartGuard para aceitar os dados da interface PanelView Plus, ele usa um byte de dados.

Também não há valores de números inteiros no controlador SmartGuard que podem ser acessados programaticamente. Como apenas os valores de dados booleanos são enviados ao controlador SmartGuard, e já que o menor tipo de dados no controlador SmartGuard é um byte, não há razão para enviar menos que um byte da interface PanelView Plus para o controlador SmartGuard, mesmo se você estiver usando apenas alguns bits. Este exemplo configura um byte de dados de saída que deverá ser enviado ao controlador SmartGuard, mas usa apenas dois botões. Se você precisar enviar mais de oito BOOLs para o controlador SmartGuard da interface PanelView Plus, edite o seguinte exemplo e modifique 1 byte para *x* bytes nos parâmetros de saída.

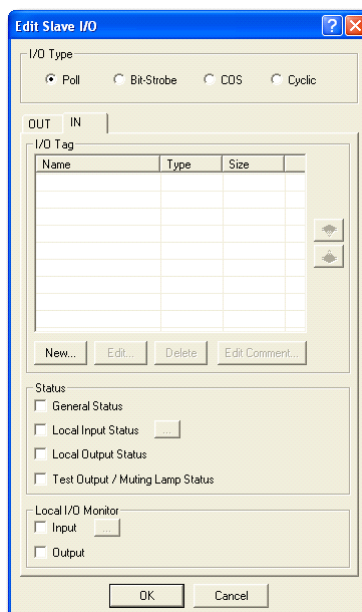
As marcações que estão sendo lidas pela interface PanelView Plus devem ser inseridas sob a guia IN.

As marcações que estão sendo gravadas pela interface PanelView Plus devem ser inseridas sob a guia OUT.

Siga este procedimento para ler e gravar do e para o controlador SmartGuard a partir da interface PanelView Plus simultaneamente.

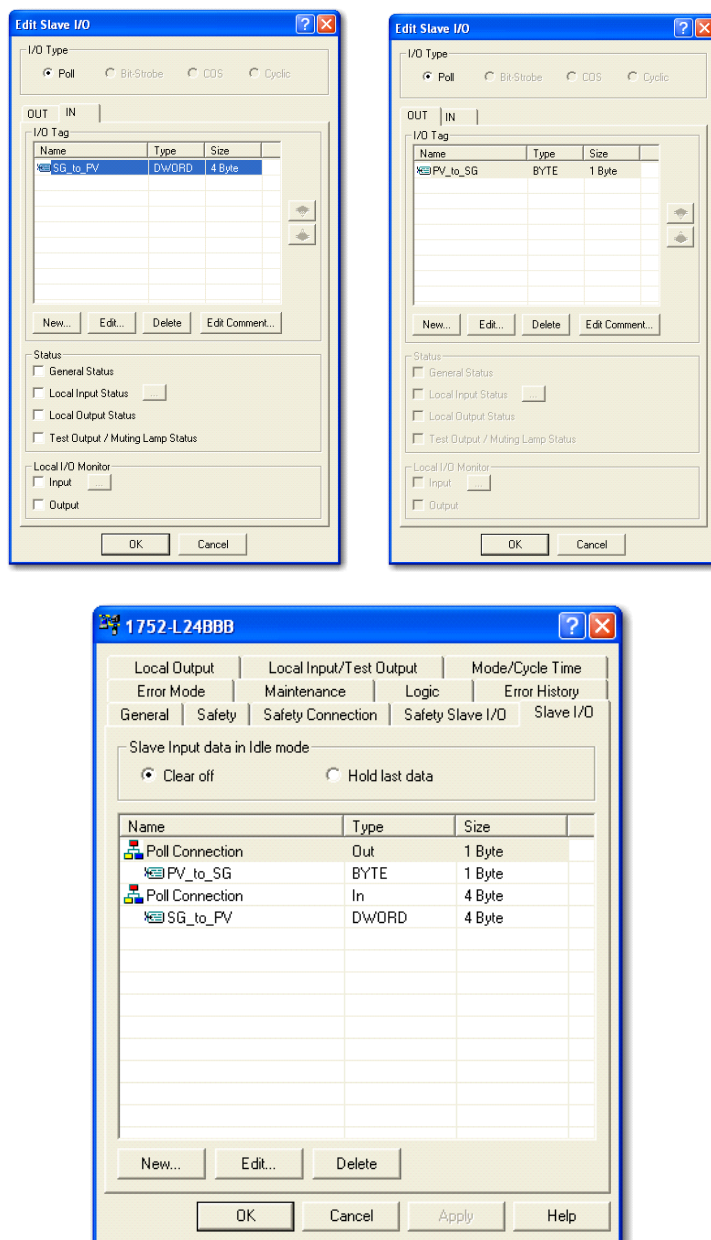
1. Abra o software RSNetWorx.
2. Abra as propriedades SmartGuard.
3. Clique na guia Slave I/O.

A seguinte caixa de diálogo aparece.



4. Clique na guia IN.
5. Insira os nomes dos tags que serão lidos pela interface PanelView Plus.
6. Clique na guia OUT.
7. Insira os nomes das marcações que serão gravadas pela interface PanelView Plus.

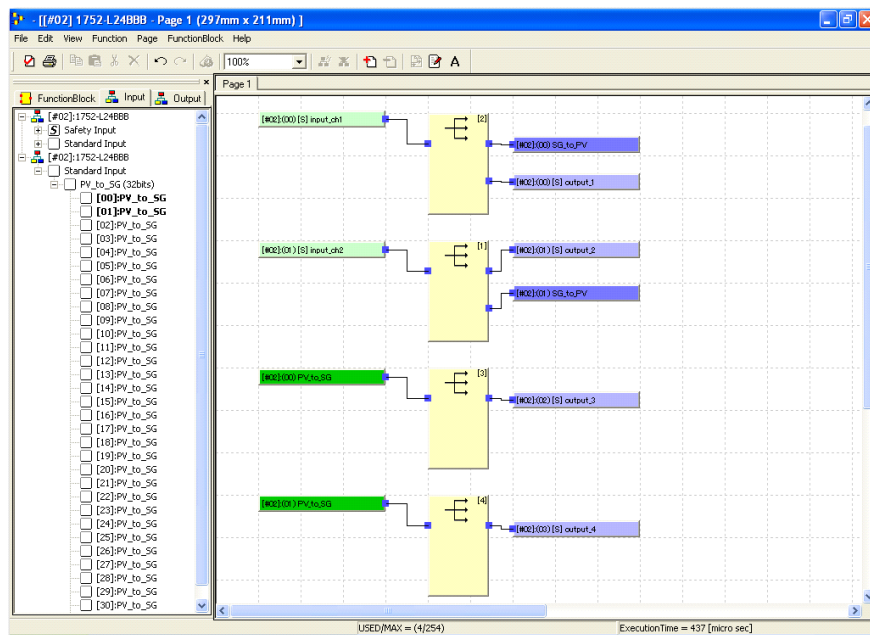
Neste caso, será usada uma conexão com polling com 4 bytes que podem ser lidos e 1 byte que pode ser gravado.



Você também tem acesso a todos os bits do DWORD e BYTE no editor SmartGuard. O código de amostra SmartGuard está usando dois bits em ambos os buffers.

As quatro marcações em negrito na lista de marcações são usadas em código.

A guia Input é mostrada abaixo e então as marcações PV_to_SG são exibidas. Para visualizar as marcações SG_to_PV, clique na guia Output.



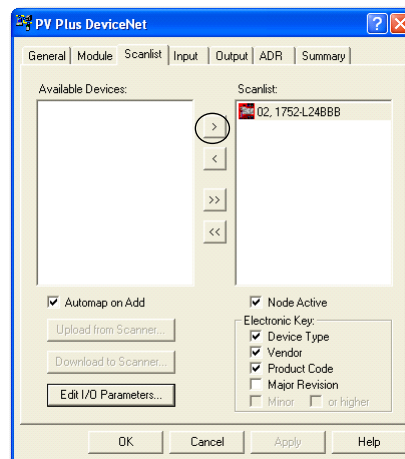
8. Faça o download da configuração do controlador SmartGuard 600.

Configure a lista de varredura do scanner PanelView

Para o scanner DeviceNet PanelView Plus, deve-se configurar a lista de varredura.

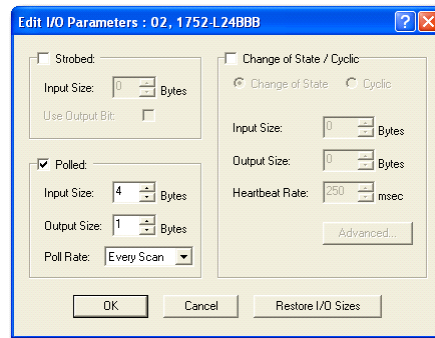
Siga este procedimento para adicionar o controlador SmartGuard 600 à lista de varredura.

1. Clique na guia Scanlist.
2. Clique na seta à direita para mover o controlador SmartGuard para a lista de varredura.



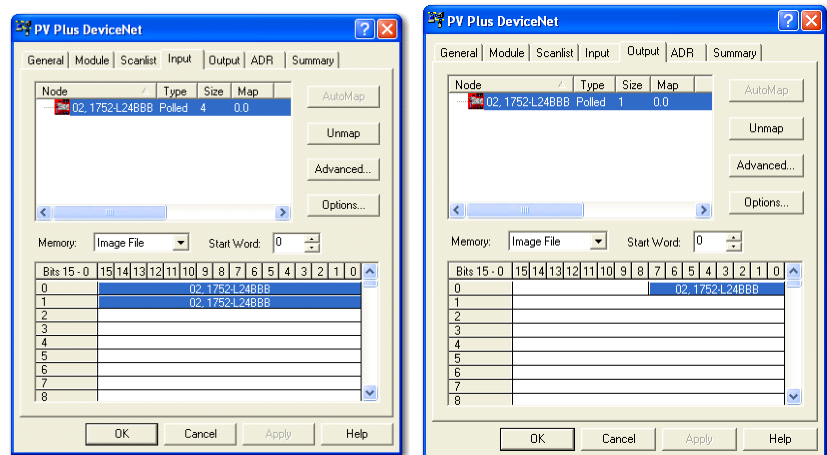
3. Clique em Edit I/O Parameters e verifique se está configurado conforme mostrado abaixo.

O exemplo tem uma conexão com polling que irá ler 4 bytes e gravar 1 byte entre o controlador SmartGuard e a interface PanelView Plus.



Como o Automap on Add foi selecionado, o seguinte mapeamento ocorreu automaticamente.

4. Verifique que os 4 bytes de dados de entrada e o único byte de saída estão mapeados conforme mostrado.

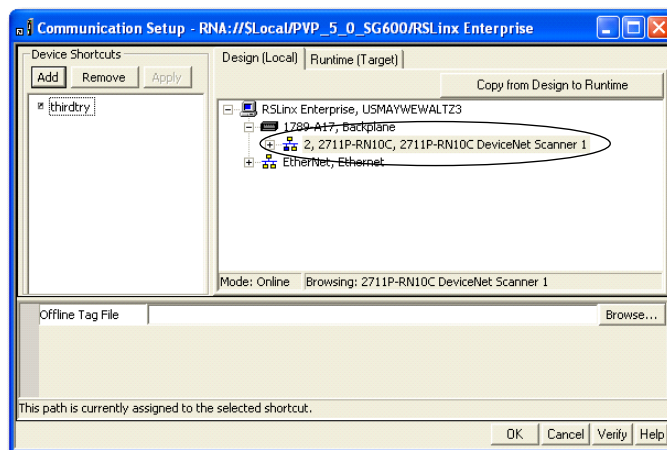


5. No software RSNetWorx, clique com o botão direito na interface PanelView Plus e escolha Download to Device para fazer o download desta configuração para a interface PanelView Plus.

Configure o scanner RN10C DeviceNet

Siga este procedimento para configurar o scanner RN10C DeviceNet.

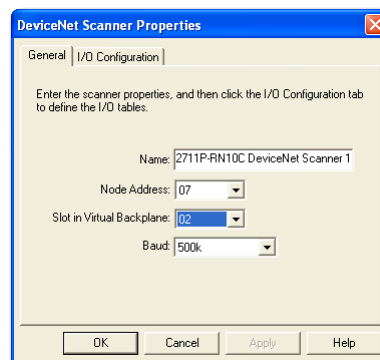
O atalho no software RSLinx Enterprise deve aparecer similar ao mostrado.



Observe que o número de slot do RN10C é 2.

1. Clique com o botão direito no scanner RN10C e escolha Properties.

A seguinte caixa de diálogo aparece.

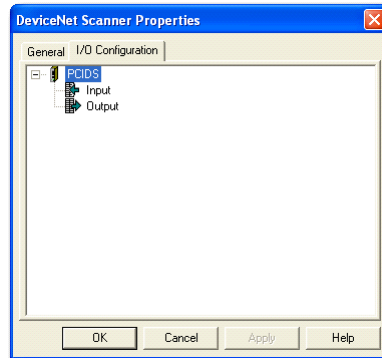


2. Insira o nome do scanner.
3. No menu apropriado, escolha o endereço do nó, slot no backplane virtual e Baud rate.

A interface PanelView Plus é configurada para o nó 7 DeviceNet. O controlador SmartGuard tem as minisseletores configuradas para uma detecção automática (esquerda/esquerda/esquerda/direita de cima para baixo). Escolha a baud rate que é apropriada para a sua aplicação.

4. Clique na guia I/O Configuration.

A seguinte caixa de diálogo aparece.



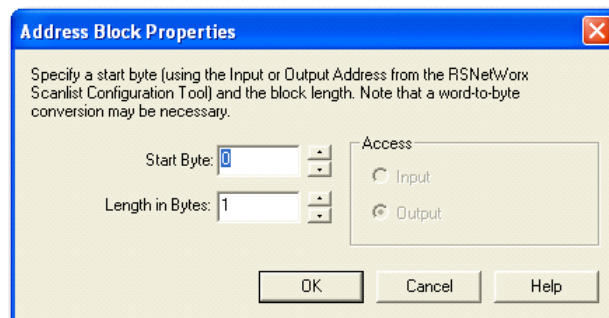
A configuração do bloco de entrada está coberta na seção 'Como ler BOOLS' neste documento. Consulte essa seção para configurar os dados que serão lidos a partir do controlador SmartGuard e exibidos na interface PanelView Plus.

Configure os dados que são gravados da interface PanelView Plus para o controlador SmartGuard

Siga este procedimento para configurar os dados que são gravados da interface PanelView Plus para o controlador SmartGuard.

1. Clique com o botão direito em Output e escolha Add Address Book.

A seguinte caixa de diálogo aparece.

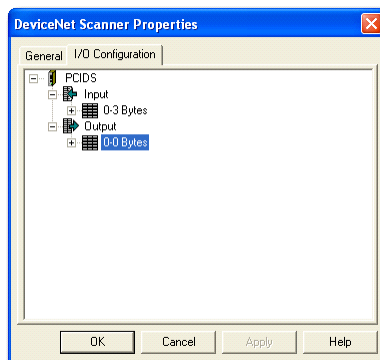


2. Insira um como o comprimento em bytes.

Isto irá combinar com o que o scanner está gravando no controlador SmartGuard.

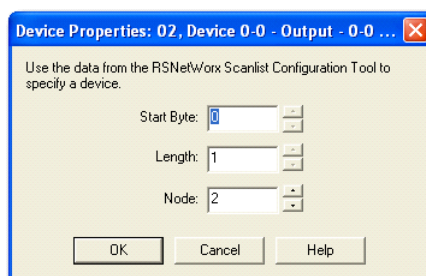
3. Clique em OK.

A seguinte caixa de diálogo aparece.



4. Clique com o botão direito em 0-0 Bytes e escolha Add Devices.

A seguinte caixa de diálogo aparece.

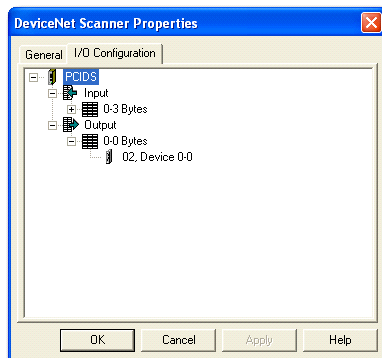


5. Configure o número do nó para combinar com o seu controlador SmartGuard.

O número do nó é 2 neste exemplo.

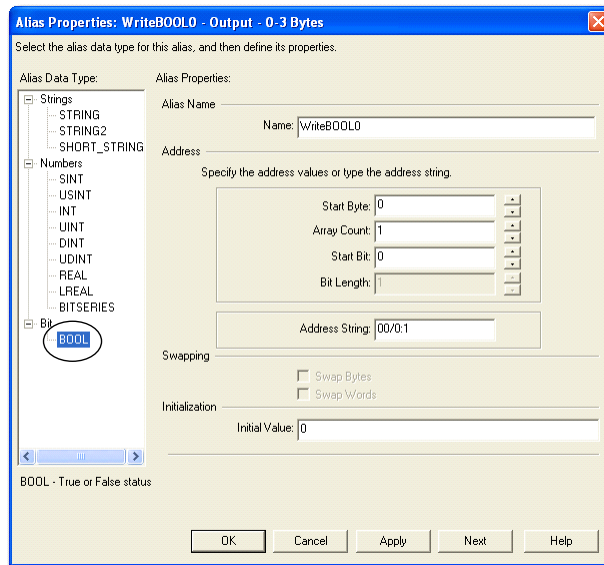
6. Clique em OK.

A seguinte caixa de diálogo aparece.



7. Clique com o botão direito em 0-0 Bytes e escolha Add Alias.

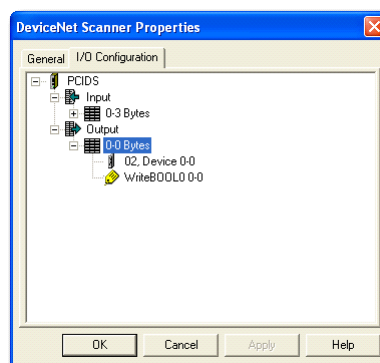
A seguinte caixa de diálogo aparece quando o tipo de dados BOOL é seleccionado.



Os valores mostrados acima representam o bit 0 do primeiro byte.

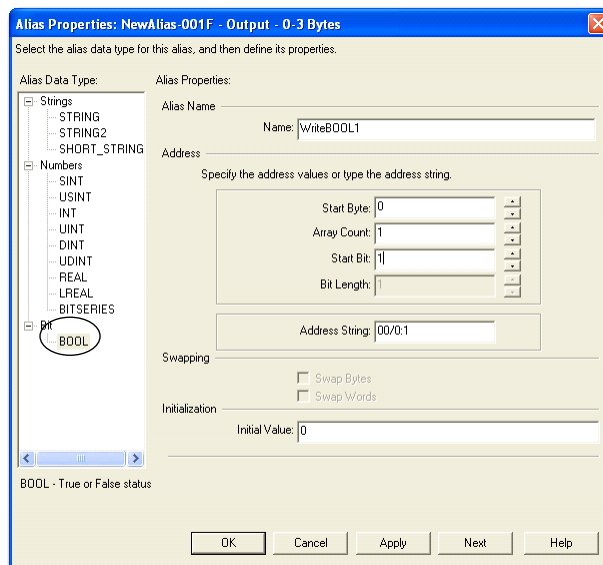
8. No menu apropriado, escolha o byte inicial, a contagem de faixa e o bit inicial.
9. Insira o nome.
10. Insira o valor inicial de 0.
11. Clique em OK.

A seguinte caixa de diálogo aparece.



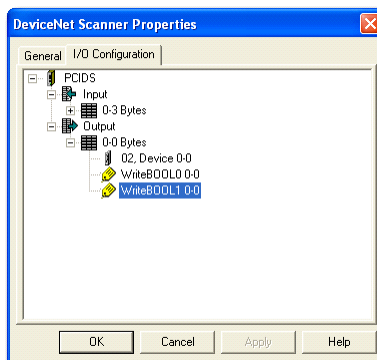
Para adicionar um segundo BOOL que representa o bit 1 do primeiro byte, siga este procedimento.

1. Clique com o botão direito em 0-0 Bytes e escolha Add Alias.



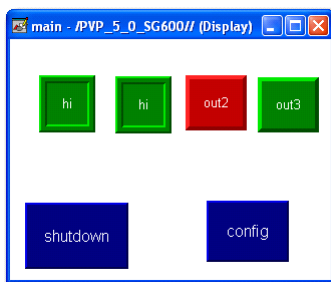
2. Selecione o tipo de dados BOOL e, no menu apropriado, escolha o byte inicial, a contagem de faixa e o bit inicial.
3. Insira o nome.
4. Insira o valor inicial de 0.
5. Clique em OK.

A seguinte caixa de diálogo aparece.

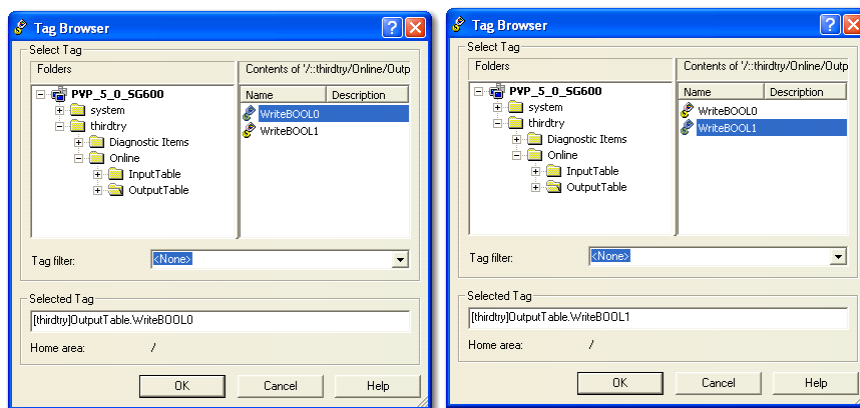


6. Clique em OK.

A etapa final é a criação do gráfico PanelView Plus que lê as marcações alias. Este exemplo usará 2 botões mantidos que lerão os dois aliases.

Gráfico PanelView Plus

As marcações para cada um dos botões mantidos podem ser observadas usando o software RSLinx Enterprise. Selecione as marcações conforme mostrado.

Observe as marcações para botões mantidos

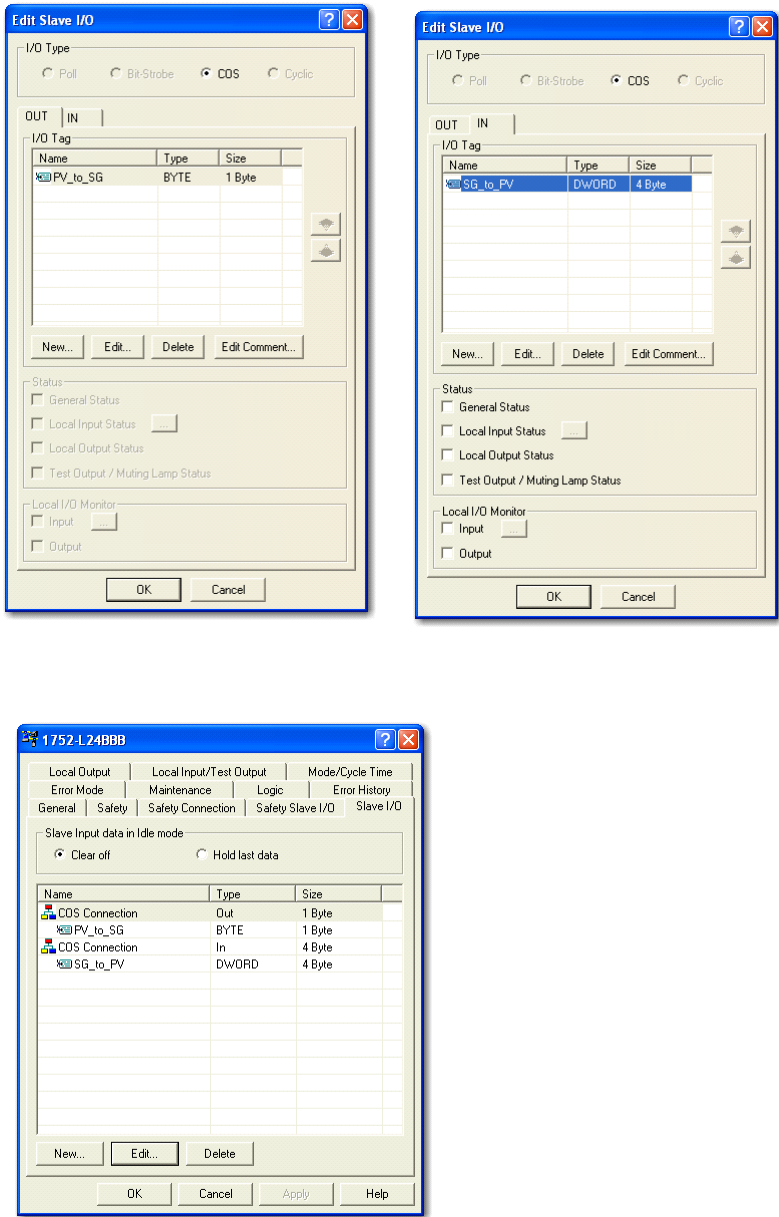
Finalmente, você precisará salvar seu projeto, gerar um arquivo Runtime, e fazer o download para a interface PanelView Plus.

COS Versus com polling

Para usar Mudança de estado (COS) em vez de com polling, faça as modificações apropriadas da [página 113](#) até esta seção conforme mostrado nas seguintes caixas de diálogo.

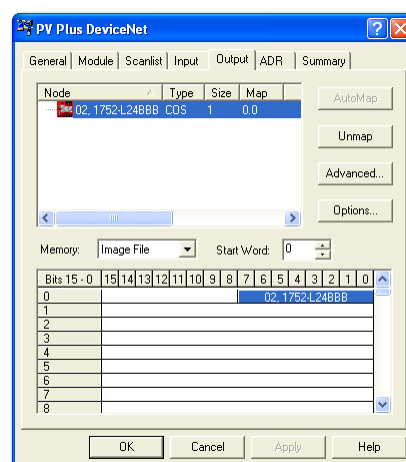
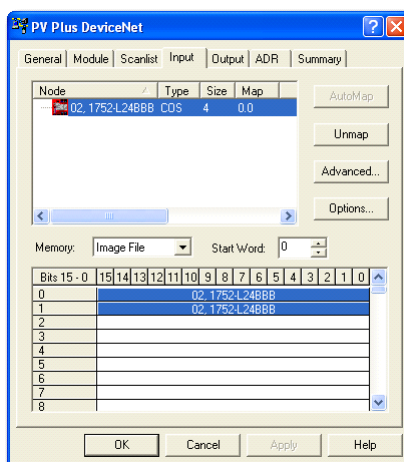
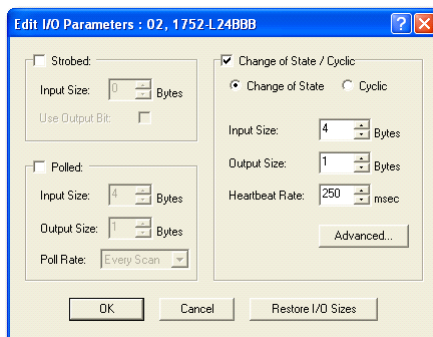
As seguintes edições ocorrem na configuração SmartGuard de E/S escrava.

Modificações de configuração SmartGuard de E/S escrava



As seguintes edições ocorrem na configuração do scanner DeviceNet RN10C no software RSNetWorx.

Modificações de configuração do scanner DeviceNet RN10C

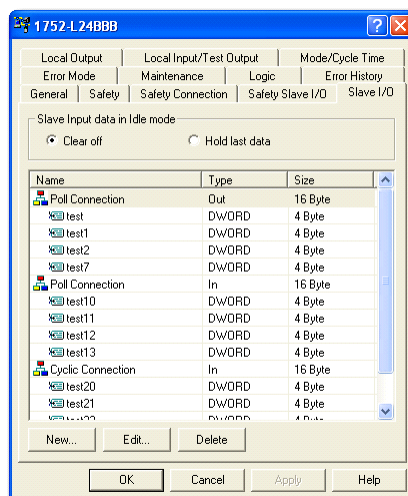


Tamanhos máximos de conexão

Este exemplo tem uma conexão com polling com entrada de 16 bytes e saída de 16 bytes. Foi adicionada uma segunda conexão (cíclica) de entrada de 16 bytes. A seguir são mostradas as modificações necessárias para suportar a configuração.

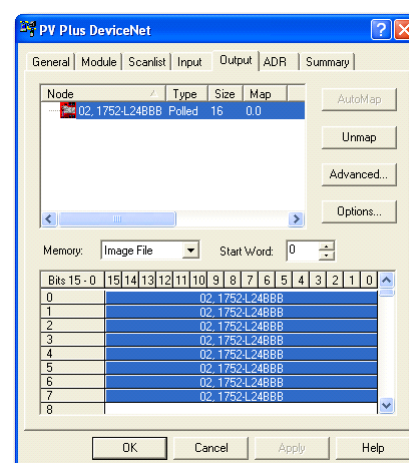
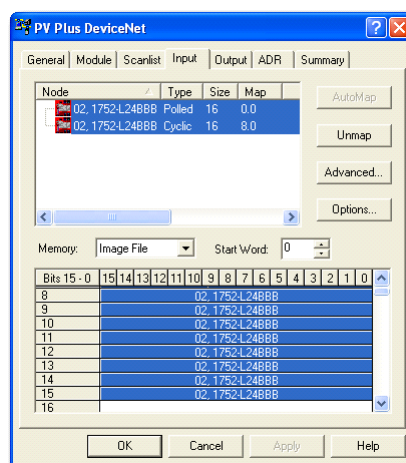
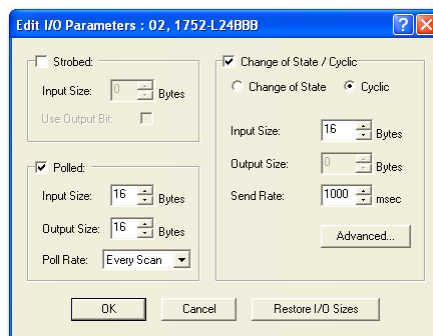
A configuração de E/S escrava SmartGuard aparece conforme mostrado.

Configuração de E/S escrava SmartGuard

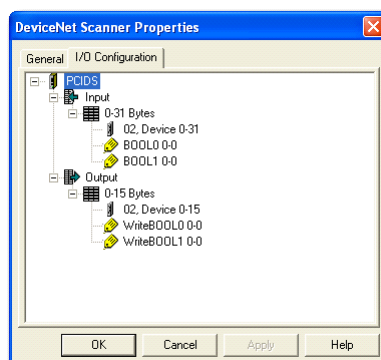


As propriedades de conexão do scanner DeviceNet aparecem conforme mostrado.

Configuração do scanner DeviceNet



A configuração do FactoryTalk para o software de E/S RSVIEW Enterprise aparece como mostrado.

Configuração do FactoryTalk para o software de E/S RSView Enterprise

Observações:

Configuração do controlador para a comunicação EtherNet/IP

Introdução

O controlador SmartGuard (código de catálogo 1752-L24BBBE) oferece conectividade EtherNet/IP.

Tópico	Página
Configure a E/S alvo no software RSNetWorx para DeviceNet	130
Configure seu controlador como escravo usando o perfil genérico do software RSLogix 5000	134
Configure a comunicação entre o terminal padrão PanelView e um controlador SmartGuard 600 em uma rede EtherNet/IP	136

Conexões multicast

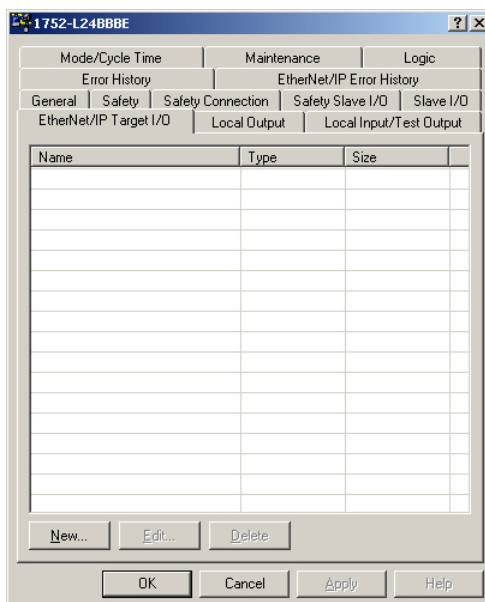
Podem ser feitas apenas duas conexões ao controlador SmartGuard a qualquer momento. Pode ser uma entrada e uma saída, ou duas entradas, ou duas saídas. Mesmo que as conexões sejam multicast, uma vez que duas conexões forem feitas, não serão aceitas outras conexões.

Por exemplo, podem-se ter dois controladores conectados a uma conexão de entrada na montagem de entrada multicast do controlador SmartGuard, e isto consumiria as duas conexões EtherNet/IP.

Configure a E/S alvo no software RSNetWorx para DeviceNet

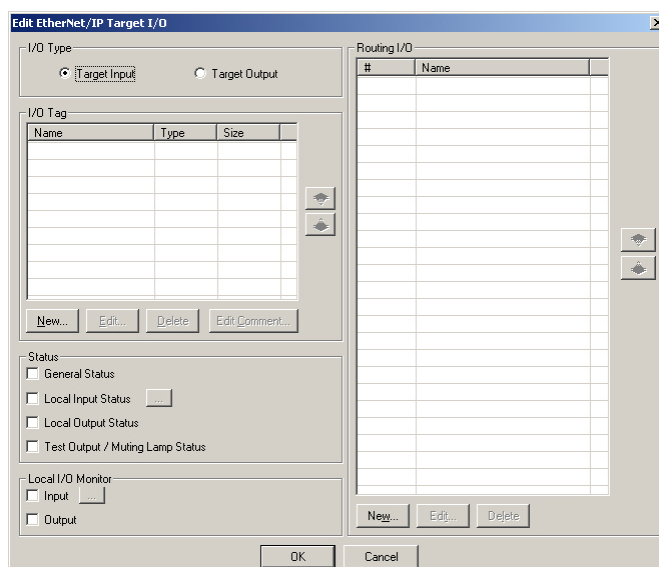
Siga estas etapas para criar montagens de E/S alvo padrão EtherNet/IP.

1. No software RSNetWorx para DeviceNet, clique com o botão direito no controlador SmartGuard e escolha properties.
2. Clique na guia EtherNet/IP Target I/O.



3. Clique em New.

A seguinte caixa de diálogo aparece.



4. Sob o tipo de E/S, clique em Target Input ou Target Output.

Entrada de alvo (target input) significa que este dado é produzido pelo controlador SmartGuard e lido pelo dispositivo de origem. Saída de alvo (target output) significa que este dado é produzido pelo dispositivo de origem e enviado ao controlador SmartGuard.

Se for selecionado Target Input, pode-se incluir a seguinte informação de status na montagem de E/S.

Nome do tag	Dimensões dos dados	Tipo do atributo
Status geral	Byte	Não segurança
Status da entrada local	Palavra	
Status da saída local	Byte	
Saída de teste/status da lâmpada muting		

5. Adicione informações de status para tipos de entrada pela seleção das caixas de verificação de status.

6. Adicione dados do monitor de E/S locais para tipos de entrada marcando a caixa de seleção Local I/O Monitor apropriada.

Nome do tag	Dimensões dos dados	Tipo do atributo
Monitor de entrada local 1 (entradas 0 a 7)	Byte	Não segurança
Monitor de entrada local 2 (entradas 8 a 15)		
Monitor de saída local (saídas 0 a 7)		

Entre os tipos de saída não podem estar os dados do monitor de E/S local. Só é possível ler os valores de entrada e de saída; não é possível gravá-los.

7. Adicione dados de E/S de roteamento para os módulos.

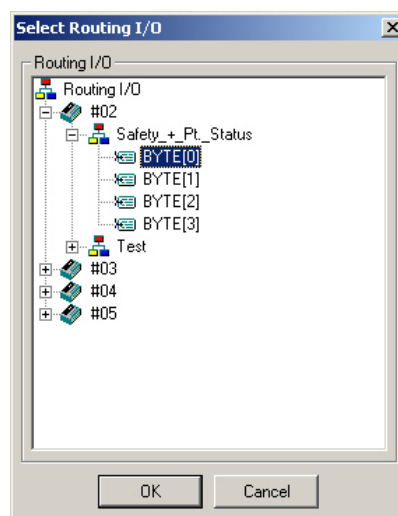
Se o controlador SmartGuard está controlando módulos de segurança DIO na rede DeviceNet, o uso da função de E/S de roteamento permite que os valores dos pontos de E/S nos módulos DIO sejam passados para um controlador padrão ou uma interface IHM na rede EtherNet/IP.

DICA

Os módulos somente aparecem na tabela de E/S de roteamento depois que foram adicionados à lista de varredura de segurança e clicou-se em Apply.

- Em Routing I/O, clique em New.
- Expanda o nó que para o qual gostaria de adicionar os dados de roteamento.
- Expanda uma das montagens listadas.

- d. Selecione o byte que gostaria de adicionar.

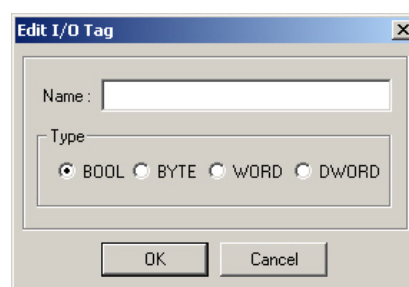


- e. Clique em OK.
f. Repita as etapas a até e para adicionar E/S adicionais de roteamento.

8. Em I/O Tag, clique em New para criar um tag de E/S.

Vários tags de E/S podem ser definidos em uma montagem de E/S. Tags de E/S de até 16 bytes podem ser definidos em cada montagem de E/S. Os tags de E/S aqui podem ser usados no Logic Editor. Por exemplo, podem-se criar tags que representem falhas das instruções no seu código de bloco de funções, e então os exibir em um dispositivo IHM.

A seguinte caixa de diálogo aparece.

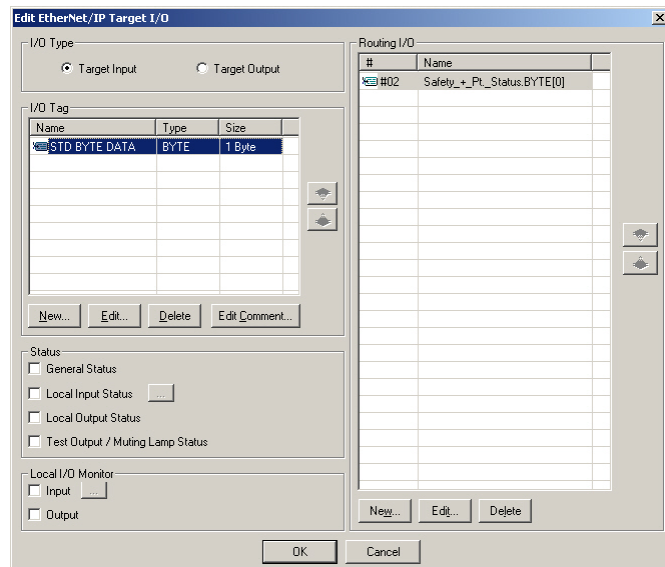


9. Insira um nome para o tag e selecione o tipo.

As opções são BOOL, BYTE, WORD ou DWORD.

10. Clique em OK.

A seguinte caixa de diálogo aparece.

**11.** Crie um nome de tag para cada bit em uma montagem de E/S.

a. Em I/O Tag, selecione a montagem aplicável e clique em Edit Comment.

b. Insira um comentário para cada bit no tag.

Os comentários do nome de tag inseridos aqui são exibidos no Logic Editor.

c. Clique em OK.

12. Clique OK para retornar à guia EtherNet/IP Target I/O.

Podem-se criar montagens adicionais de entrada ou de saída necessárias para a aplicação repetindo as etapas 2 a 11.

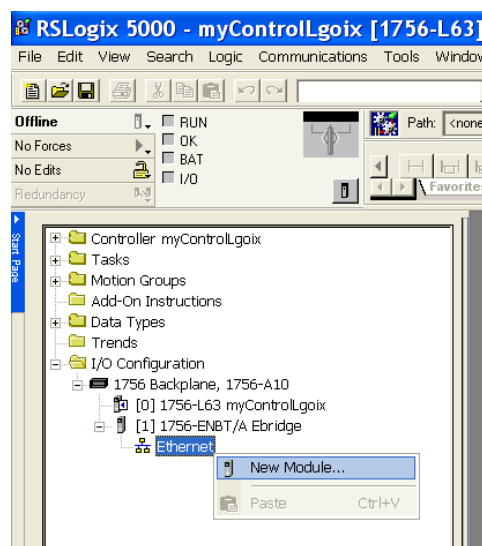
13. Para salvar suas configurações, no menu File, escolha Save.

Configure seu controlador como escravo usando o perfil genérico do software RSLogix 5000

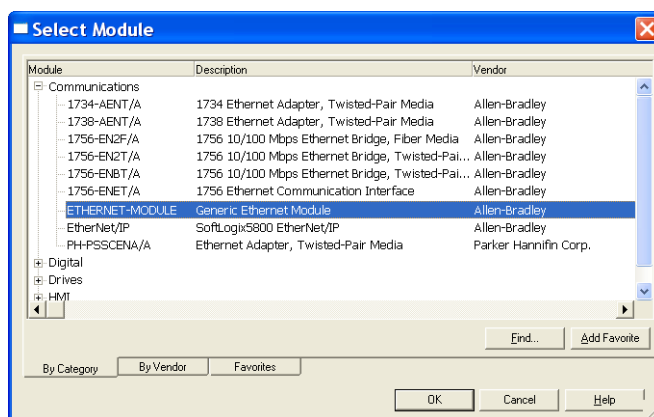
Quando tiver configurado os dados a serem compartilhados no controlador SmartGuard, pode-se usar o software RSLogix 5000 e o perfil genérico padrão para trocar estes dados com um controlador logix.

Siga estas etapas para se conectar ao controlador.

1. Clique com o botão direito na rede Ethernet no organizador do controlador e escolha New Module.

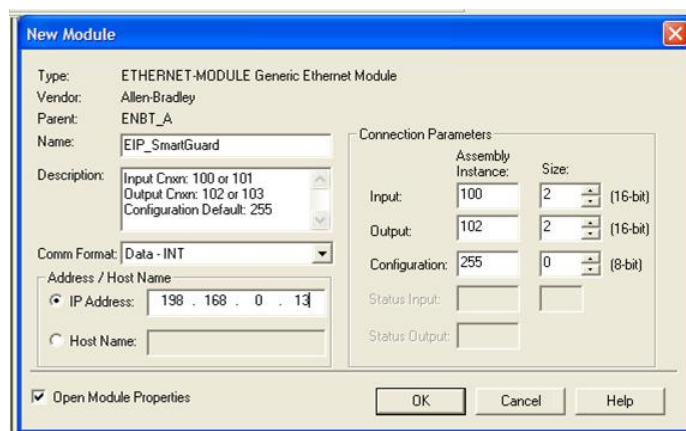


2. Expanda o grupo de Comunicações e selecione ETHERNET-MODULE.



3. Clique em OK.
4. Na caixa de diálogo New Module, defina os parâmetros conforme necessário.

Esta caixa de diálogo mostra os valores de instância para uma conexão de entrada/saída.



A tabela fornece os valores de instância para uma conexão de entrada/saída e conexão de apenas entrada.

Tipo de conexão		Número de instância
Entrada/Saída	Entrada (controlador SmartGuard para controlador)	100, 101
	Saída (controlador para controlador SmartGuard)	102, 103
Apenas entrada	Entrada	100, 101
	Saída	199

5. Clique em OK.

Configure a comunicação entre o terminal padrão PanelView e um controlador SmartGuard 600 em uma rede EtherNet/IP

Siga estas etapas para configurar um terminal padrão PanelView para ser capaz de se comunicar com um controlador SmartGuard 600 em uma rede EtherNet/IP.

1. Abra sua aplicação PanelView no software PanelBuilder32.

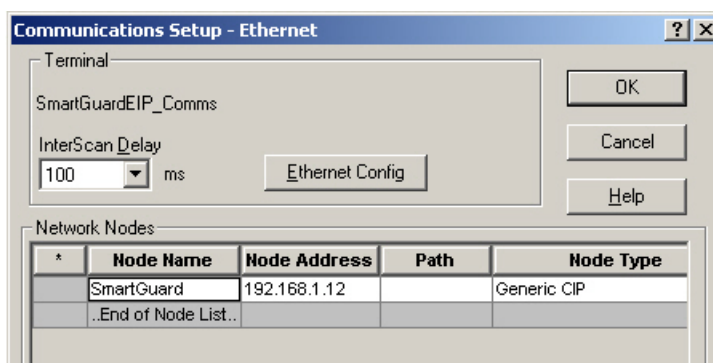
Você precisará definir o caminho de comunicação entre o terminal PanelView e o controlador SmartGuard 600.

2. Clique em Communications Setup.



A caixa de diálogo Communications Setup – Ethernet aparece.

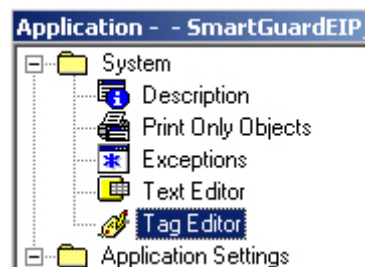
3. Clique em Insert.
4. Insira o nome do nó e o endereço do nó do controlador SmartGuard.
5. Insira o tipo de nó como Generic CIP.



6. Clique em OK.

Siga este procedimento para definir tags no banco de dados de tags PanelView que irá acessar as montagens de E/S alvo no controlador SmartGuard 600.

1. Clique em Tag Editor no explorador da aplicação.

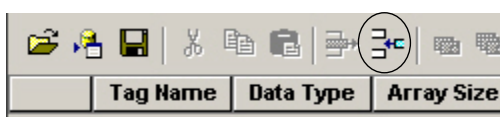


O editor de tag da aplicação abre.

2. Na parte de baixo do editor de tags, clique na guia ENet-CIP.



3. Clique em Insert para adicionar um novo tag.



4. Nas novas células de tag, digite o nome do tag, o tipo de dado e o nome do nó (que combina com o nome de nó que você definiu para o controlador SmartGuard na configuração de comunicações).

Neste exemplo, escolhemos DINT como tipo de dados.

	Tag Name	Data Type	Descrip	Node Name
1	SG_InputAssembly	DINT		SmartGuard

Pode haver até quatro montagens de E/S de alvo configuradas no controlador SmartGuard (duas entradas e duas saídas).

Para montagens de entrada, os códigos de mensagem CIP incluem o seguinte:

- Serviço: 0xE – Obter atributo simples
- Classe: 4
- Instância: 100 ou 101 (entrada 1 ou entrada 2 respectivamente)
- Atributo: 3

Para montagens de saídas, os códigos de mensagem CIP incluem o seguinte:

- Serviço: 0x10 – Configurar o atributo simples
- Classe: 4
- Instância: 102 ou 103 (saída 1 ou saída 2 respectivamente)
- Atributo: 3

Este exemplo mostra um código de mensagem CIP que acessa a montagem de entrada 1 do controlador SmartGuard.

O campo do membro é sempre definido como 1.

1. No menu Service Code, escolha o código de serviço CIP.
2. Digite a classe, instância e códigos de atributos para o tag para acessar a montagem correta de E/S de alvo no controlador SmartGuard.

	Tag Name	Data Type	Descrip	Node Name	Initial Value	Array Size	Service Code	Class	Instance	Attribute	Member	Byte Offset
1	SG_InputAssembly	DINT		SmartGuard	0	0	Get Attribute Single (0xE)	4	100	3	1	0

O tamanho máximo de um tag de membro simples definido no terminal PanelView é um DINT (4 bytes). Uma montagem de E/S de alvo no controlador SmartGuard pode ser tão grande quanto 16 bytes. Para acessar todos os bytes na montagem alvo, pode ser necessário criar até 4 tags DINT, onde um Offset é definido para cada tag para corresponder com os bytes alvo daquele tag.

Definição dos modos do controlador

Introdução

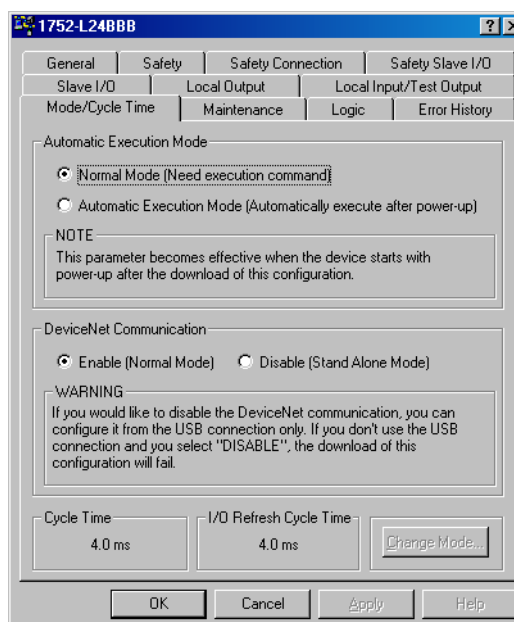
Tópico	Página
Definir modo de execução automática (opcional)	139
Definição do modo de comunicação independente (opcional)	140
Alteração do modo do controlador	141

Definir modo de execução automática (opcional)

O controlador pode ser configurado para o modo normal ou o modo de execução automática. Só defina o modo de execução automática após a configuração do sistema. A configuração torna-se efetiva depois que você desliga e liga a alimentação após o download de uma configuração.

Siga estas etapas para definir o modo.

1. Clique com o botão direito do mouse no controlador e escolha Properties.
2. Selecione a guia Mode/Cycle Time.



3. Escolha Normal Mode ou Automatic Execution Mode.

Modo	Descrição
Normal	O controlador começa no modo inativo quando a fonte de alimentação é ativada. Você deve usar o software RSNetWorx para DeviceNet para alterar para o modo de execução clicando em Change Mode na guia Mode/Cycle Time da caixa de diálogo Controller Properties.
Execução automática	O controlador começa no modo em execução quando a fonte de alimentação é ativada, caso a configuração tenha sido fixada e o controlador estivesse no modo em execução antes da fonte de alimentação ser desativada.

4. Clique em OK.

Definição do modo de comunicação independente (opcional)

O controlador SmartGuard pode ser operado com ou sem a comunicação DeviceNet habilitada. A configuração padrão é habilitada.

No modo independente, o tempo do ciclo do controlador é menor, embora nenhuma das funções de comunicação do DeviceNet possa ser usada.

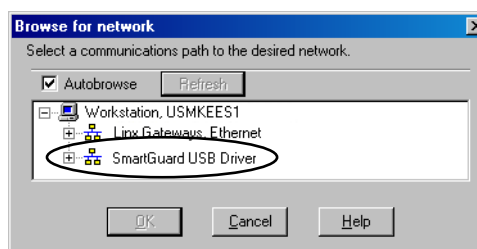
Caso você queira usar o controlador SmartGuard no modo independente, é possível desabilitar a comunicação DeviceNet e usar a conexão USB para configurar o módulo.

IMPORTANTE

Se você desabilitar a comunicação DeviceNet e não usar a conexão USB, o download da configuração falhará.

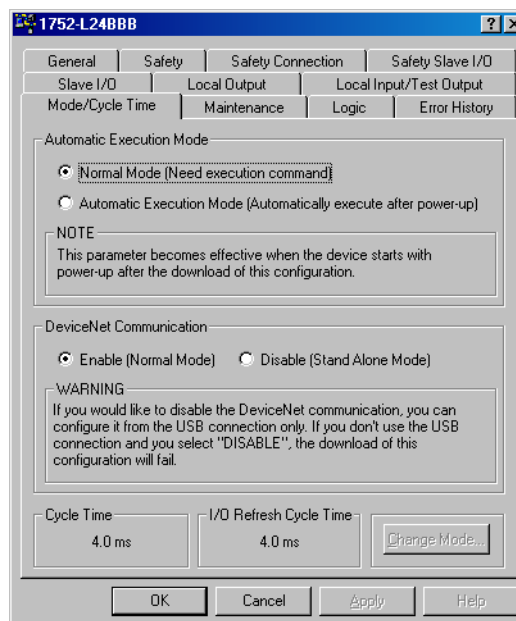
Siga estas etapas para desabilitar a comunicação DeviceNet.

1. Verifique se você está conectado ao equipamento de programação usando a conexão USB.
2. Caso ainda não esteja, configure um caminho para usar a conexão USB no software RSNetWorx for DeviceNet.
 - a. No menu Network, escolha Properties.
 - b. Na caixa de diálogo DeviceNet, clique em Set Online Path.
 - c. Na caixa de diálogo Browse for Network, selecione o caminho desejado e clique em OK.



3. No software RSNetWorx for DeviceNet, clique com o botão direito do mouse no controlador e escolha Properties.

4. Selecione a guia Mode/Cycle Time.



5. Escolha Disable (Stand Alone Mode) e clique em OK.

Alteração do modo do controlador

Siga estas etapas para alterar o modo do controlador.

1. Entre em comunicação com o controlador SmartGuard.
2. Clique com o botão direito do mouse no controlador e escolha Properties.
3. Selecione a guia Mode/Cycle Time na caixa de diálogo Controller Properties.
4. Clique em Change Mode.
5. Selecione o botão de opção Idle ou Execute.
6. Clique em OK.

Observações:

Criação do programa aplicativo

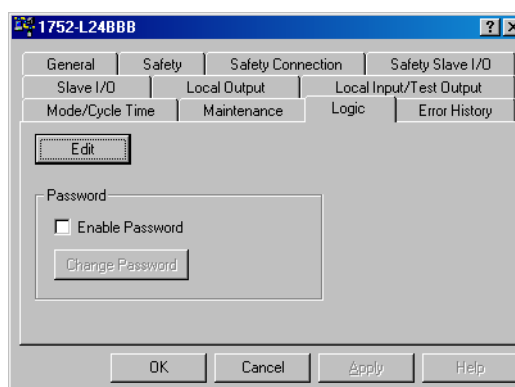
Introdução

Tópico	Página
O Logic Editor	143
Programação básica	144
Criando um programa de bloco de funções	149
Edição dos parâmetros de bloco de funções	150
Encontrar blocos de funções com conexões abertas	153
Programação em várias páginas	154
Para salvar o programa	155
Para atualizar o programa	155
Para monitorar o programa on-line	156
Seqüência de execução do programa	157
Blocos de funções definidos pelo usuário	158
Recursos adicionais	162

O Logic Editor

A programação do controlador SmartGuard 600 é feita usando o Logic Editor no software RSNetWorx para DeviceNet. O Logic Editor consiste em uma lista de objetos, em que os blocos de funções, os tags de E/S e os demais elementos de programação são registrados e um espaço de trabalho, em que a programação é realizada.

Abra o Logic Editor escolhendo a guia Logic na caixa de diálogo Edit Device Parameters e clicando em Edit.



É possível proteger por senha o programa aplicativo para impedir a edição não autorizada, a verificação ou a impressão de programas. Para criar uma senha, siga estas etapas.

1. Na guia Logic da caixa de diálogo Controller Properties, marque a caixa de seleção Enable Password.
2. Na caixa de diálogo Change Password, digite a senha no campo New Password.

As senhas podem conter até seis caracteres.

3. Digite novamente a senha no campo Confirm Password.
4. Clique em OK.

A senha será solicitada sempre que o botão Edit for clicado para abrir o Logic Editor. É possível carregar ou descarregar o programa sem a senha, embora as funções de edição, verificação, impressão e relatório do programa não estejam disponíveis.

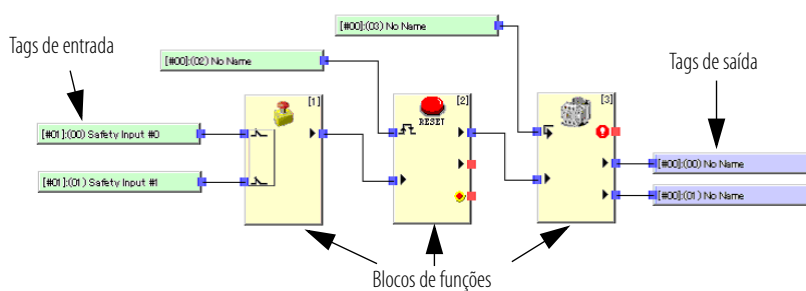
IMPORTANTE

Caso você se esqueça da senha, ela não pode ser recuperada.

Programação básica

Os programas são criados em funções de lógica e blocos de funções que indicam comandos, em tags de entrada que indicam origens de entrada de dados e em tags de saída que indicam os destinos de saída de dados. As E/S são conectadas às linhas de conexão.

Conexões de E/S



Funções de lógica e blocos de funções

Um máximo de 254 funções lógicas e blocos de funções pode ser usado.

Instruções de lógica suportadas e blocos de funções

Instruções de lógica	Blocos de funções
• NOT • AND • OR • OR exclusiva • NOR exclusiva • Roteamento • RS Flip-Flop • Vários conectores • Comparador	• Reset • Reinicialização • Monitoração do botão de parada de emergência • Monitoração da cortina de luz • Monitoração do gate de segurança • Controlador bimanual • Temporizador do atraso na desenergização • Temporizador do atraso na energização • Chave em modo usuário • Monitoração de dispositivo externo • Muting • Chave de habilitação • Gerador de pulso • Contador

Tags de entrada

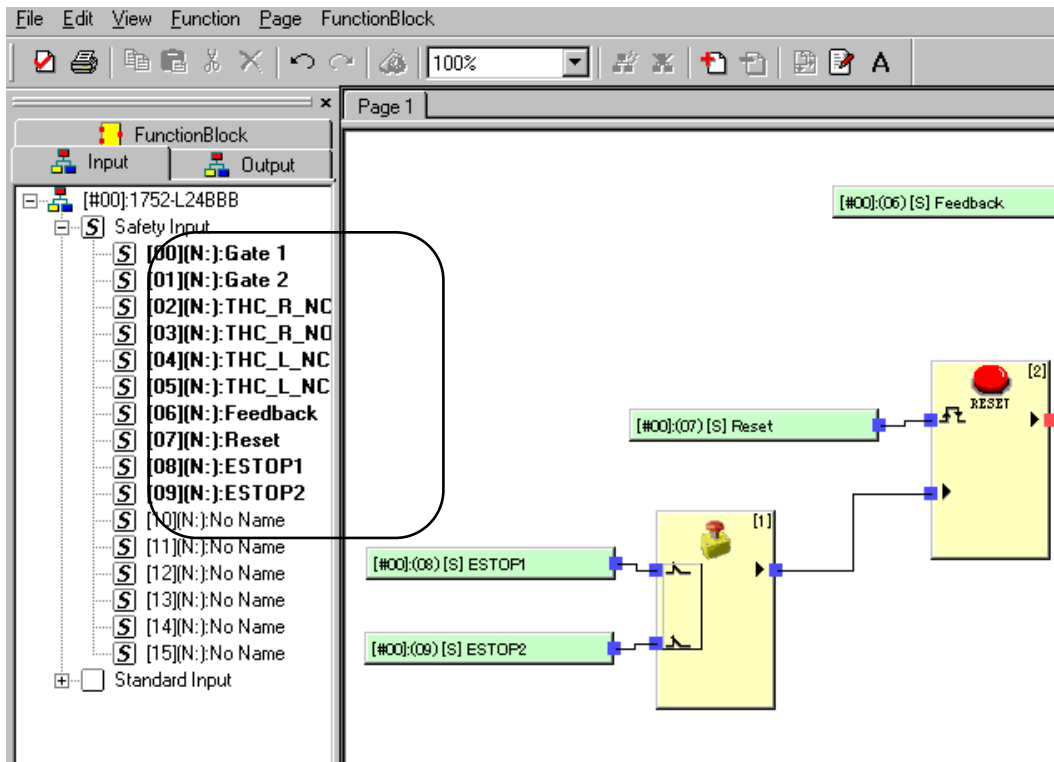
Os tags de entrada refletem o status das entradas nestas áreas de E/S:

- Os terminais locais do controlador
- Área de entrada dos escravos de segurança registrados como parceiros de comunicação
- A área de entrada refletida a partir dos dados do mestre de segurança
- A área de entrada refletida a partir dos dados do mestre padrão

Os dados são refletidos nestas áreas de E/S:

- status da entrada local
- status da saída local
- status da unidade geral
- status da saída de teste
- status da lâmpada muting

Na lista de objetos, os tags de E/S são exibidas com símbolos para indicar como elas são configuradas.

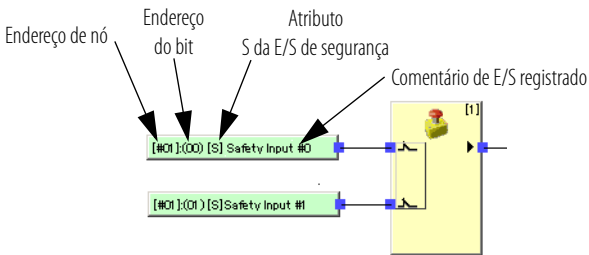


Símbolos do tag de entrada

Modo de entrada	Símbolo	Modo de canal	Símbolo
Não usado	N	Simple	Nenhum
Pulso de teste da saída de teste	P	Equivalente a canal duplo	e
Usado como entrada de segurança	S	Canal duplo complementar	c
Usado como entrada padrão	ST		—

Quando usadas no espaço de trabalho, os tags de entrada incluem o endereço do nó, o endereço do bit, o atributo (S para segurança, nenhum para padrão) e o comentário de E/S registrado.

Tags de entrada



Tags de saída

Os tags de saída refletem o status das saídas nestas áreas de E/S:

- Os terminais locais do controlador
- Área de saída dos escravos de segurança registrados como parceiros de comunicação
- A área de saída refletida a partir dos dados do mestre de segurança
- A área de saída refletida a partir dos dados do mestre padrão

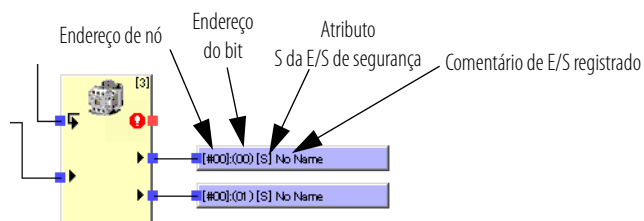
Na lista de objetos, os tags de E/S são exibidos com símbolos para indicar como eles são configurados.

Símbolos do tag de saída

Modo de saída	Símbolo	Modo de canal	Símbolo
Não usado	N	Simplex	Nenhum
Segurança	S	Duplo	d
Teste de pulso de segurança	P		—

Quando usadas no espaço de trabalho, os tags de saída incluem o endereço do nó, o endereço do bit, o atributo (S para segurança, nenhum para padrão) e o comentário de E/S registrado.

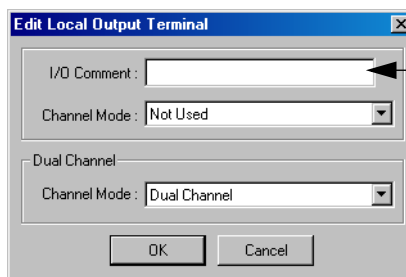
Tags de saída



Função de comentário de E/S

O comentário de E/S é um nome opcional, consistindo de até 32 caracteres ASCII que podem ser registrados no controlador para cada terminal de E/S pelo uso do software RSNetWorx para DeviceNet. Esses comentários de E/S podem ser usados na lista de objetos do Logic Editor como tags de E/S, o que simplifica a programação.

Comentário de E/S



Restrições de programação

Itens como, por exemplo, tags de E/S e blocos de funções, podem ser usados em todas as páginas com as seguintes restrições:

- O mesmo tag de entrada pode ser colocado em mais de uma página.
- O mesmo tag de entrada só pode ser usado uma vez em cada página.
- Cada tag de saída só pode ser usado uma vez no programa aplicativo.
- Apenas os blocos de funções podem ser copiados. Os tags de E/S, as conexões de E/S e as conexões entre os blocos de funções não podem ser copiados.
- Quando é colado, um bloco de funções é colocado na mesma posição do bloco de funções copiado. Ao colar um bloco de funções na mesma página, mova o bloco de funções de origem.
- Pode ser usado um máximo de 254 blocos de funções.
- Pode ser usado um máximo de 128 endereços de salto do número.
- Pode ser usado um máximo de 32 páginas.
- Pode ser usado um máximo de 128 caixas de texto para comentários do programa.
- O ajuste da página não pode ser alterado caso haja algum item no espaço de trabalho. Ajuste as dimensões do espaço de trabalho primeiro escolhendo File>Page Setup.

Criando um programa de bloco de funções

Para criar um programa usando blocos de funções, você cria conexões no bloco de funções com os tags de entrada e de saída.

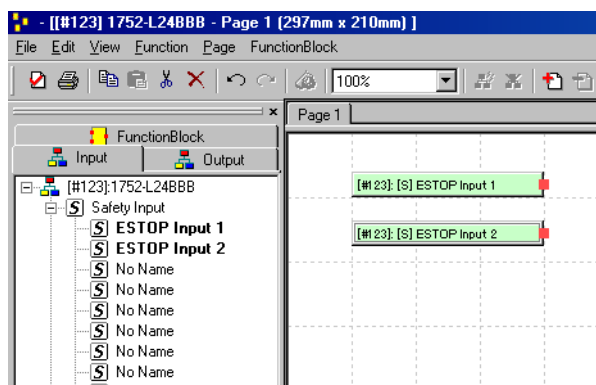
Adição de um tag de entrada ou de saída

Siga estas etapas para adicionar um tag.

1. Clique na guia Input ou Output na lista de objetos.
2. Selecione o tag que você deseja usar e arraste e solte-o na posição dentro do espaço de trabalho.

É possível selecionar vários tags de E/S e posicioná-los simultaneamente.

Inserção de tags de entrada



DICA

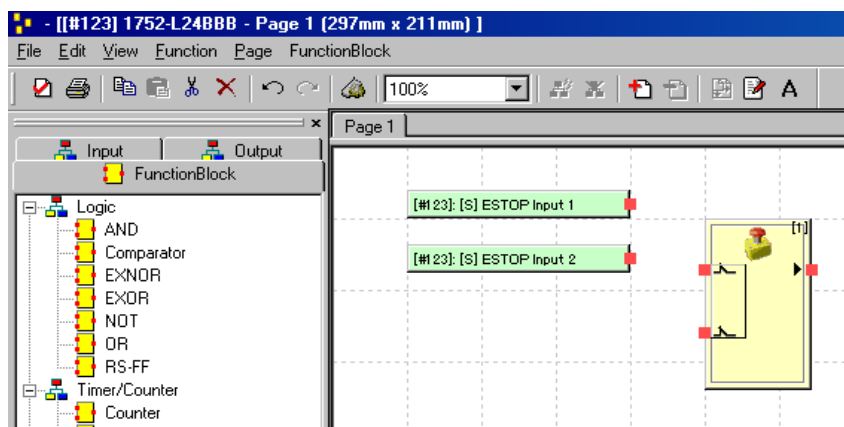
Os tags de entrada e de saída usados no programa aplicativo aparecem em negrito na lista de objetos.

Adição de um bloco de funções

Siga estas etapas para adicionar um bloco de funções ao espaço de trabalho.

1. Clique na guia Function Block na lista de objetos.
2. Selecione o bloco de funções que você deseja usar e arraste e solte-o na posição dentro do espaço de trabalho.

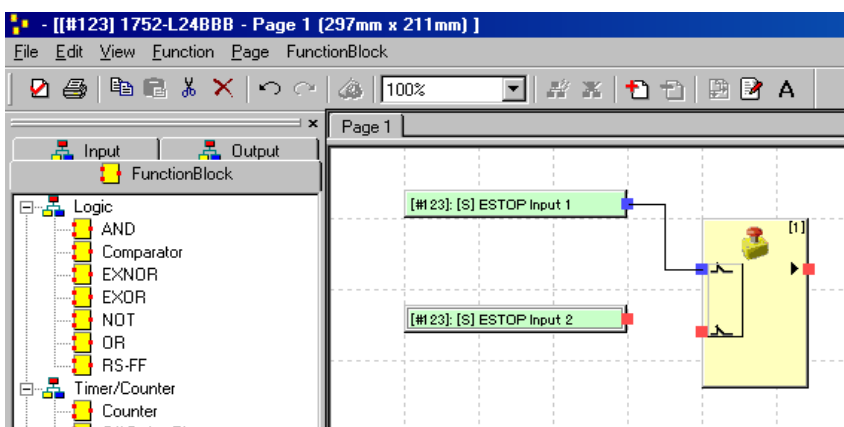
Inserção de um bloco de funções



Conexão dos tags ao bloco de funções

Para conectar os tags de E/S ao bloco de funções, clique no conector de origem (■) e arraste-o ao conector de destino (■).

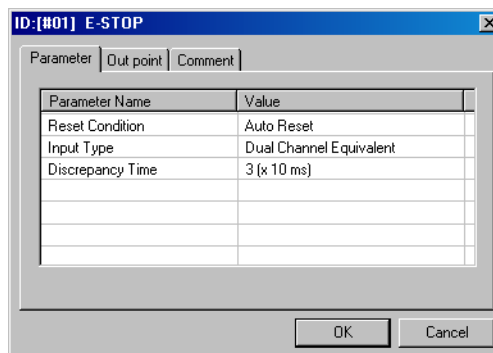
Conexão dos tags aos blocos de funções



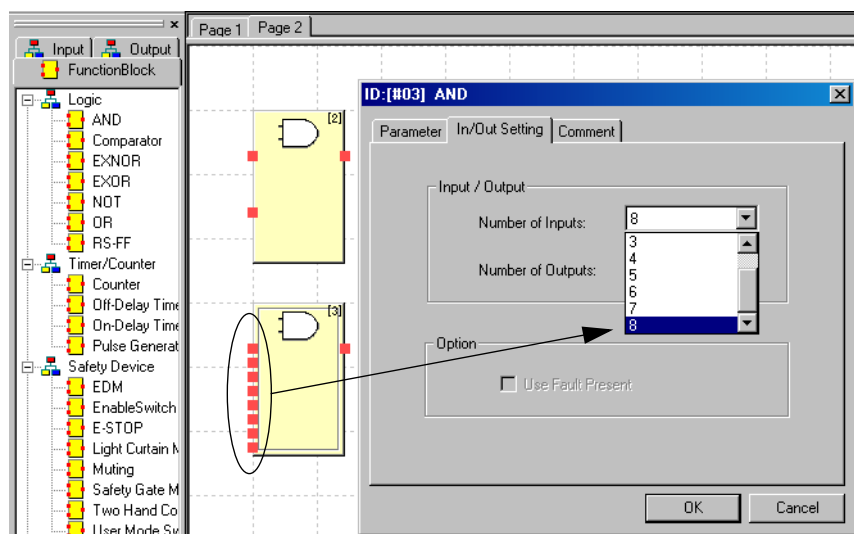
Edição dos parâmetros de bloco de funções

É possível editar os blocos de funções alterando os ajustes de parâmetro, alterando o número de entradas ou de saídas, adicionando E/S opcional e adicionando comentários que pertencem à aplicação. Os parâmetros que podem ser editados dependem do tipo de bloco de funções.

Para abrir a caixa de diálogo Function Block Properties, clique com o botão direito do mouse no bloco de funções e escolha Edit.

Guia Parameter**Configurações de E/S**

É possível editar o ajuste dos parâmetros Number of Inputs, Number of Outputs e, em alguns casos, Fault Present para muitas instruções.

Guia In/Out Setting*Número de entradas*

O número de entradas das funções de lógica pode ser aumentado ou a entrada opcional dos blocos de funções pode ser habilitada.

Número de saídas

O número de saídas das funções de lógica pode ser aumentado ou as saídas opcionais como, por exemplo, as saídas de erro, nos blocos de funções podem ser habilitadas.

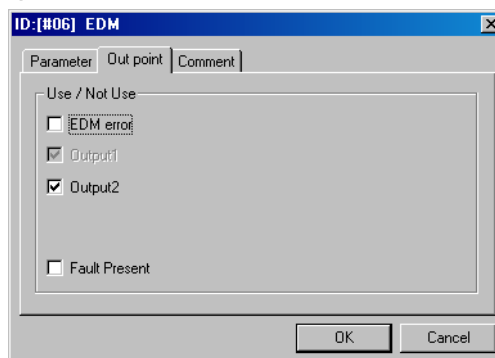
Bit de presença de falha

É possível habilitar o bit de status de diagnóstico Presença de falha em alguns blocos de função marcando a caixa de seleção localizada na guia In/Out Setting da caixa de diálogo Function Block Properties. Caso a caixa de seleção Use Fault Present esteja marcada, é exibida uma saída Presença de falha adicional no bloco de funções.

Seleções do ponto de saída opcional

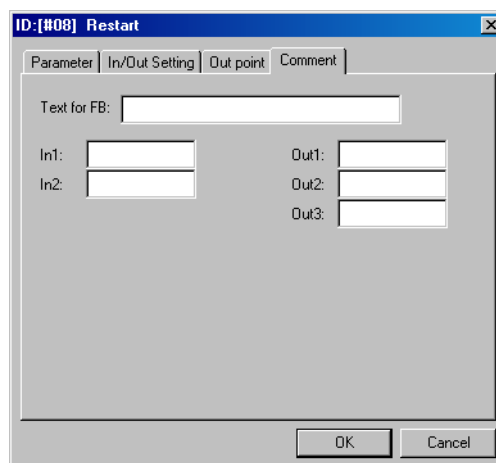
É possível habilitar saídas opcionais, inclusive o bit Presença de falha em alguns blocos de funções, marcando as caixas de seleção apropriadas na guia Out point da caixa de diálogo Function Block Properties. Quando estão marcadas, as saídas opcionais são exibidas no bloco de funções.

Guia Out point



Comentários

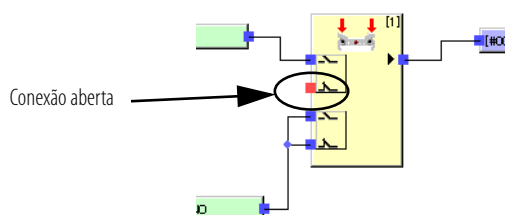
Escolha a guia Comments para digitar um nome do bloco de funções ou dos sinais de E/S. Os nomes dos sinais de E/S não são exibidos no espaço de trabalho, embora o nome do bloco de funções seja exibido no bloco dentro do espaço de trabalho. Todos os nomes digitados nessa caixa de diálogo são impressos quando o programa aplicativo é impresso.

Guia Comments

Encontrar blocos de funções com conexões abertas

Programas recém-criados que contenham blocos de funções com entradas ou saídas abertas não podem ser descarregados. Todas as E/S devem ser usadas.

Bloco de funções com conexões abertas



Para encontrar todas as conexões abertas no Logic Editor, escolha Edit>Search OpenConnection.

A caixa de diálogo Open Connection mostra todos os blocos de funções com conexões abertas. Clique duas vezes em um item na lista para exibir o bloco de funções. As conexões abertas são mostradas em vermelho no espaço de trabalho.

DICA

Se um endereço de salto for usado para o ponto de E/S e o endereço de salto correspondente não for usado, o ponto de E/S não será exibido em vermelho e aparecerá como estando conectado.

Consulte Programação em várias páginas na [página 154](#) para informações sobre endereços de salto.

Programação em várias páginas

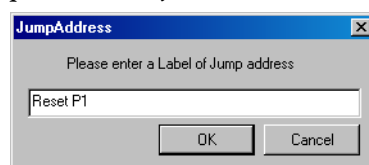
O controlador SmartGuard 600 suporta até 32 páginas de lógica de programação.

Para criar uma nova página, clique no ícone Add Page .

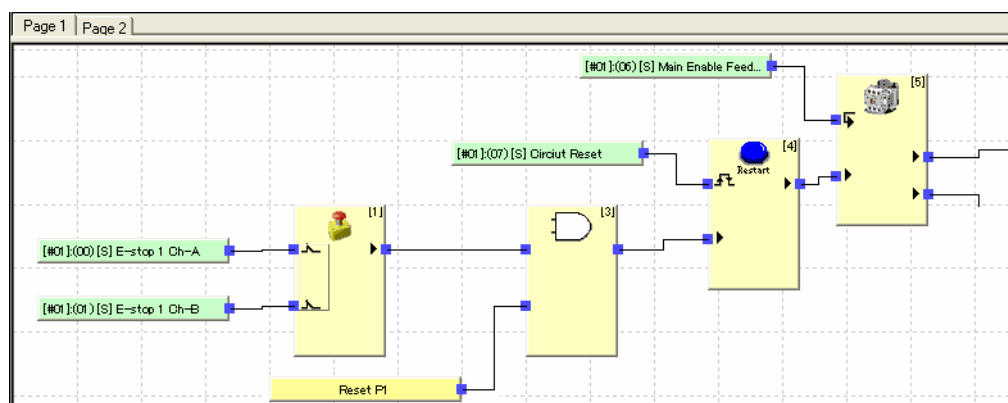
Use endereços de salto para conectar a lógica entre as páginas. Um programa do controlador SmartGuard 600 pode conter até 128 endereços de salto.

Siga estas etapas para criar um endereço de página.

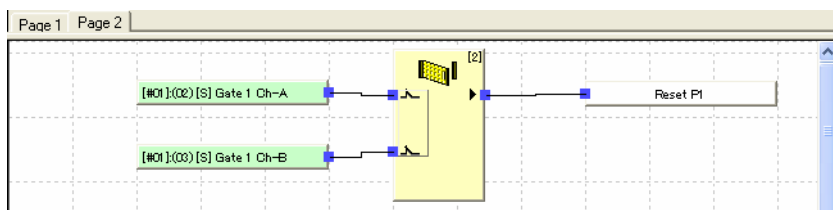
1. Clique com o botão direito do mouse em qualquer lugar da página de programação e escolha Make JumpAddress.
2. Digite um nome para o endereço de salto.



3. Conecte o endereço de salto ao bloco de funções.



4. Selecione a página à qual você deseja conectar a lógica.
5. Clique com o botão direito do mouse em qualquer lugar da página e escolha Select JumpAddress.
6. Selecione o endereço de salto no menu.
7. Conecte o endereço de salto ao bloco de funções.



Para salvar o programa

Siga estas etapas para salvar o programa aplicativo.

1. Escolha File>Apply.

O programa é salvo temporariamente no software RSNetWorx for DeviceNet.

2. Saia do Logic Editor escolhendo File>Exit.

3. Clique em OK ou Apply na caixa de diálogo Edit Device Parameters.

Se você não clicar em OK ou em Apply, ou se clicar em Cancel, nenhuma das alterações no programa é salva. Qualquer programação salva temporariamente usando File>Apply é excluída.

4. Escolha Save ou Save As na caixa de diálogo principal do software RSNetWorx para DeviceNet.

Para atualizar o programa

Caso os tags de E/S dos escravos de segurança que configuram a E/S local do controlador SmartGuard sejam alteradas, você deve abrir o Logic Editor e verificar o programa.

Caso você carregue os parâmetros no controlador sem abrir o Logic Editor, ocorre um erro de download no Logic Editor por conta da inconsistência dos dados. Caso ocorra o erro, abra o Logic Editor e verifique o programa, fazendo todas as modificações necessárias.

Para monitorar o programa on-line

Os valores do tag de E/S e os estados de sinal das conexões com os blocos de funções podem ser monitorados on-line no Logic Editor. Verifique se o software RSNetWorx for DeviceNet está conectado à rede e se o controlador que está sendo monitorado está no modo de operação antes de iniciar a monitoração do programa on-line.

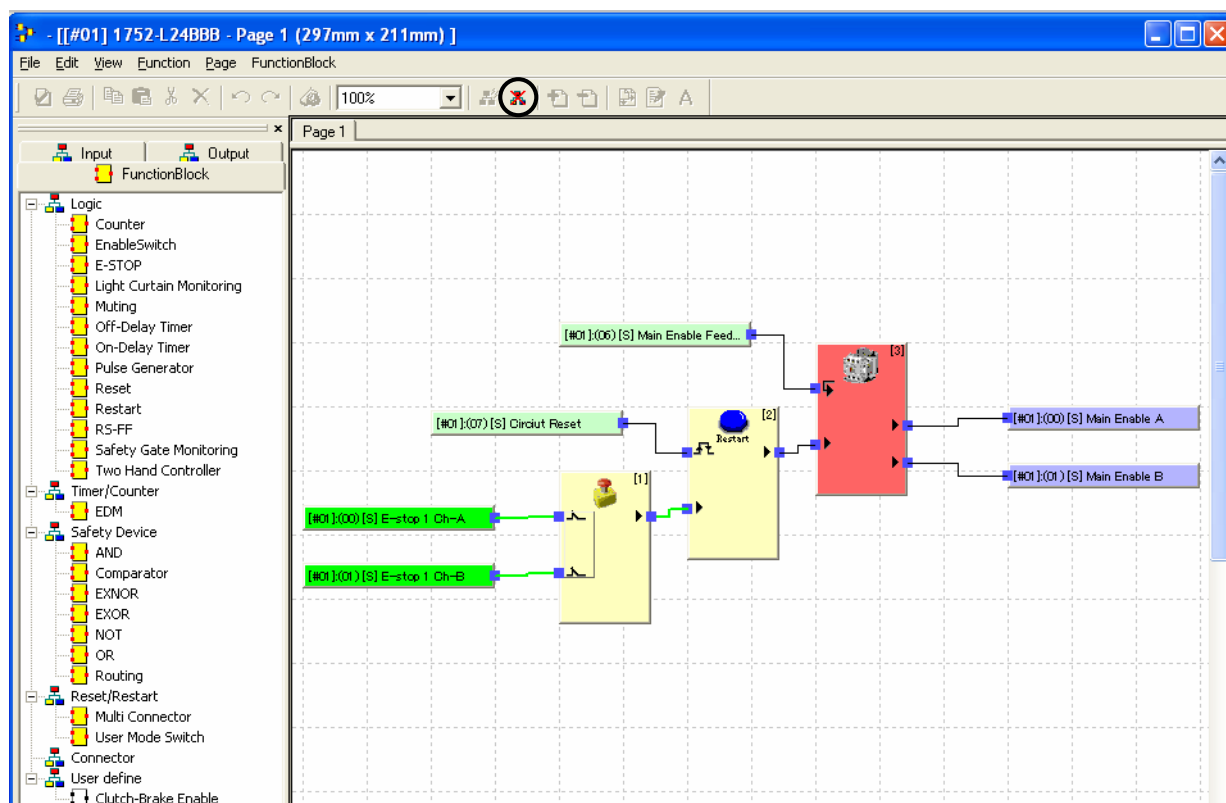
IMPORTANTE

Talvez seja necessário alterar o modo do controlador para Em execução a fim de monitorar on-line.

Para iniciar a monitoração on-line, clique em Monitoring  na barra de ferramentas.

Durante a monitoração, os tags de E/S ou conexões ativadas são exibidos em uma cor mais escura.

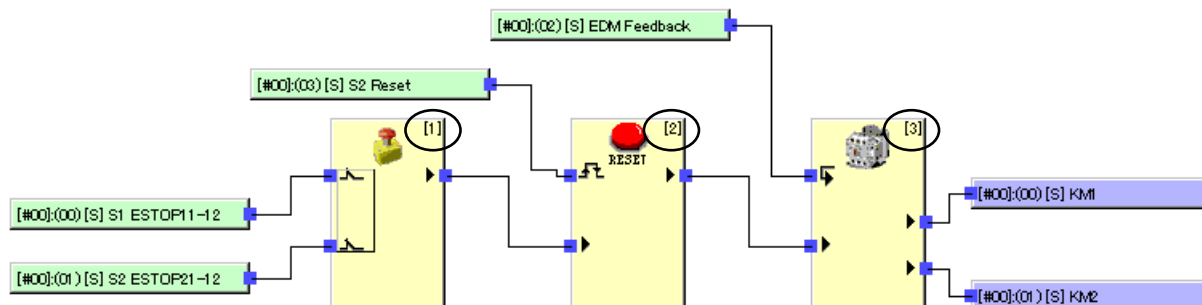
Para interromper a monitoração on-line, clique em Stop Monitoring na barra de ferramentas.



Sequência de execução do programa

A ordem de execução dos blocos de funções é definida automaticamente pelo Logic Editor e exibida no canto direito de cada bloco de funções.

Programa de exemplo

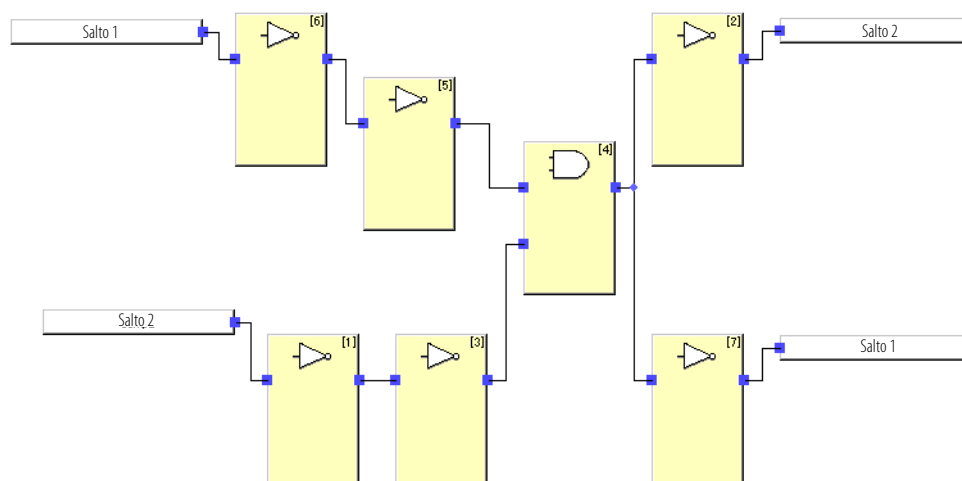


Neste exemplo, a ordem de execução é:

1. Parada de emergência
2. Reset
3. Monitoração de dispositivo externo (EDM)

Os endereços de salto podem ser usados em programas para criar retornos de malha. Caso um programa contenha mais de um retorno de malha, por exemplo um salto 1 para salto 1 e um salto 2 para salto 2, a sequência da execução permanece na ordem em que os blocos de funções estão posicionados. Teste com cuidado todos os programas que contenham mais de um retorno a fim de verificar se eles estão sendo executados corretamente.

Exemplo de retorno da malha



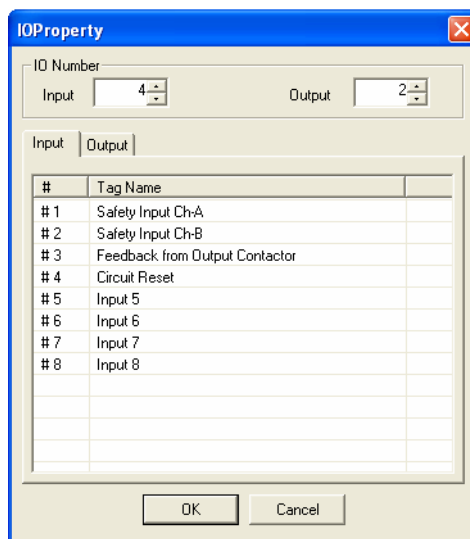
Blocos de funções definidos pelo usuário

O Logic Editor permite que você crie blocos de funções definidos pelo usuário que consistem na lógica do bloco de funções existente. Uma vez criados, esses blocos de funções são armazenados em uma biblioteca definida pelo usuário e podem ser usados em qualquer aplicação do controlador SmartGuard.

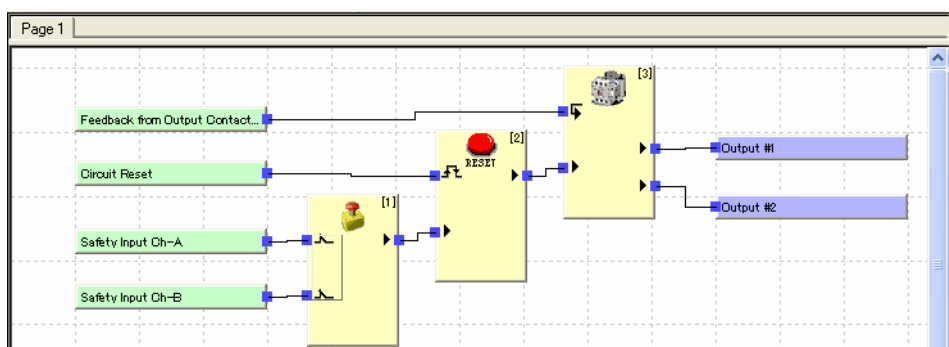
Criação de blocos de funções definidos pelo usuário

Siga estas etapas para criar um bloco de funções definido pelo usuário.

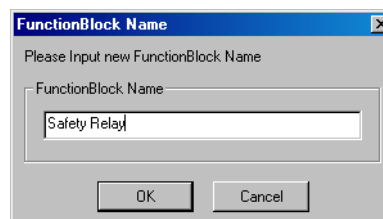
1. Abra o Logic Editor clicando com o botão direito do mouse no controlador, escolhendo Properties e clicando na guia Logic.
2. Escolha FunctionBlock>Create.
3. Na caixa de diálogo IOProperty, defina o número de entradas e de saídas do bloco de funções.



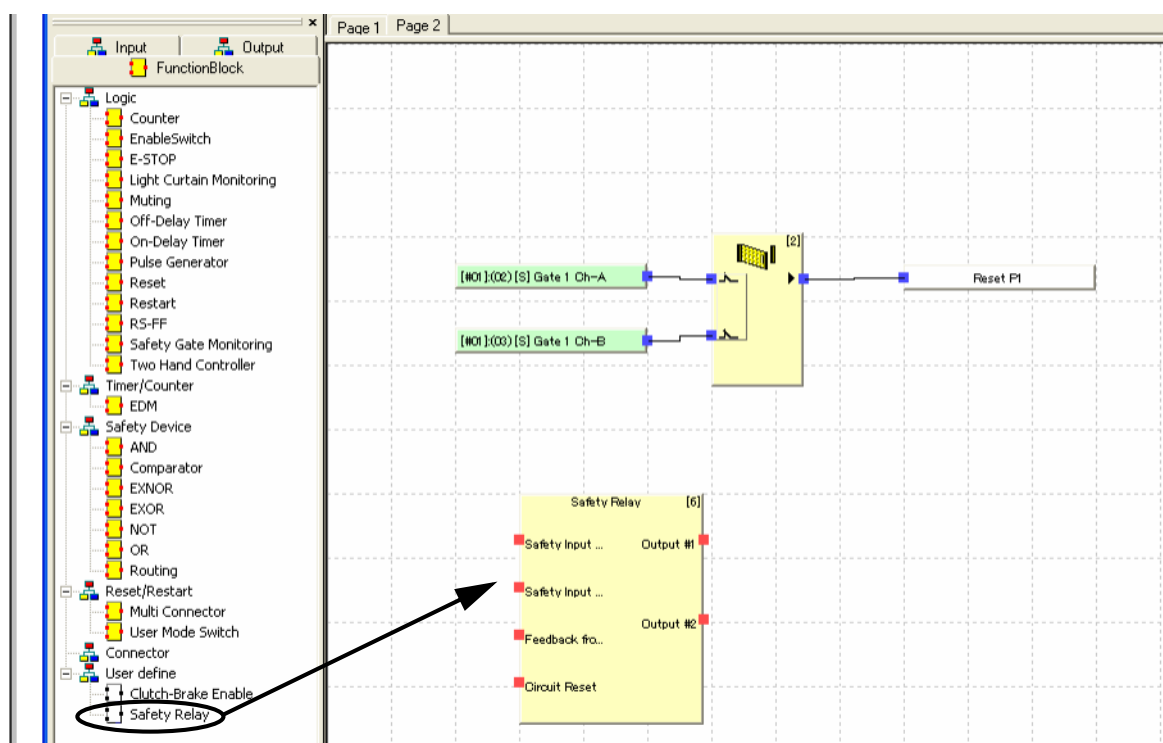
4. Atribua nomes a cada entrada e a cada saída.
5. Clique em OK para abrir o Function Block Logic Editor.
6. Escreva a lógica do bloco de funções.



7. Escolha File>Save e digite um nome para o bloco de funções, quando solicitado.



8. Adicione o novo bloco de funções à lógica da aplicação.



DICA

Caso você queira editar o bloco de funções definido pelo usuário, ele não pode ser usado na aplicação atual. Se ele for usado, a opção de edição estará indisponível.

IMPORTANTE

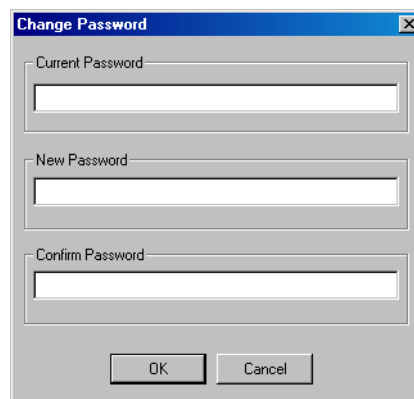
Sempre descarregue os programas com blocos de funções definidos pelo usuário no controlador, verifique a configuração e a operação antes de usá-los em uma aplicação.

Proteção por senha blocos de funções definidos pelo usuário

É possível definir uma senha para proteger arquivos do bloco de funções definido pelo usuário de edições não autorizadas. As operações de verificação, relatório e impressão não são protegidas por senha.

Para definir uma senha, siga estas etapas.

1. Para abrir a caixa de diálogo Function Block Editor, clique com o botão direito do mouse no bloco de funções definido pelo usuário e escolha Edit.
2. No Function Block Editor, escolha File>Change Password.



3. Digite uma senha de até seis caracteres alfanuméricos no campo New Password.
4. Digite novamente a senha no campo Confirm Password.
5. Clique em OK.

O bloco de funções definido pelo usuário não pode ser editado ou excluído sem digitar a senha.

É recomendável usar uma senha para proteger blocos de funções definidos pelo usuário que foram testados para evitar as alterações não autorizadas ou não intencionais assim que o bloco de funções for alocado em um programa do usuário.

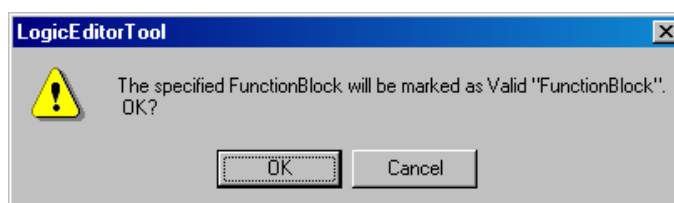
Reutilização de arquivos de blocos de funções definidos pelo usuário

Os arquivos de projeto (*.dnt) e os arquivos de blocos de funções definidos pelo usuário (*.fbd) existem como arquivos separados. É possível reutilizar arquivos de blocos de funções definidos pelo usuário durante a criação de programas. Você deve ter direitos de administrador do Windows para importar, salvar, excluir, verificar ou editar blocos de funções definidos pelo usuário.

Para reutilizar blocos de funções definidos pelo usuário, siga estas etapas.

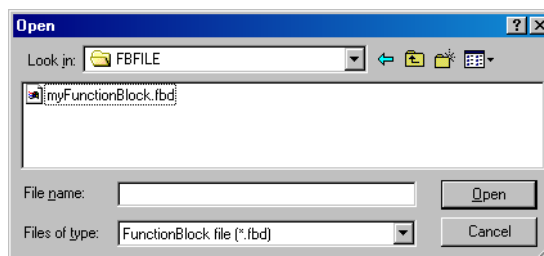
1. Crie o bloco de funções definido pelo usuário conforme descrição na [página 158](#).
2. Verifique a operação do bloco de funções definido pelo usuário.
 - a. Na lista de objetos do Logic Editor, clique com o botão direito do mouse no novo bloco de funções e escolha Edit.
 - b. Consulte o programa do bloco de funções e corrija todos os problemas.

- c. Salve o programa do bloco de funções, caso você tenha feito alguma alteração.
 - d. Feche o Function Block Logic Editor.
3. Valide o bloco de funções definido pelo usuário.
 - a. Na lista de objetos do Logic Editor, clique com o botão direito do mouse no novo bloco de funções e escolha Validate.
 - b. Clique em OK na caixa de diálogo de confirmação.



O ícone do novo bloco de funções muda de branco para amarelo para indicar que o bloco de funções foi validado.

4. Exporte o bloco de funções definido pelo usuário para um arquivo.
 - a. Na lista de objetos do Logic Editor, clique no bloco de funções salvo e definido pelo usuário.
 - b. No menu principal, escolha FunctionBlock>Export.
 - c. Na caixa de diálogo Save As, digite um nome para o arquivo e clique em Save.
5. Mova ou copie o arquivo para outros microcomputadores, caso isso seja necessário.
6. Importe o bloco de funções definido pelo usuário.
 - a. No software RSNetWorx for DeviceNet, crie um novo projeto e adicione um controlador SmartGuard.
 - b. Clique com o botão direito do mouse no controlador, escolha Properties e selecione a guia Logic.
 - c. Clique em Edit para iniciar o Logic Editor.
 - d. Escolha FunctionBlock>Import.



- e. Selecione o arquivo apropriado e clique em Open.
- O bloco de funções definido pelo usuário importado é exibido na lista de objetos do Logic Editor.

IMPORTANTE

Sempre importe arquivos do bloco de funções definido pelo usuário antes de editar ou verificar os programas aplicativos que os usarão.

Precauções quanto à reutilização dos blocos de funções definidos pelo usuário

Esta tabela indica quais ações exigem arquivos do bloco de funções definido pelo usuário e descreve o que acontece caso a ação seja tentada sem o arquivo do bloco de funções.

Resultados sem os arquivos do bloco de funções

Ação	Arquivo	Resultado
Fazer download	Não requerido	Opera normalmente
Fazer upload	Não requerido	Opera normalmente
Salvar arquivo de projeto	Não requerido	Opera normalmente
Carregar arquivo de projeto	Não requerido	Opera normalmente
Verificação	Requerido	A verificação do programa pode ser concluída mesmo sem o arquivo do bloco de funções assim que o arquivo é descarregado no controlador, embora a configuração do bloco de funções não possa ser verificada.
Editar o programa	Requerido	Uma mensagem de advertência aparecerá se o Logic Editor for aberto sem o arquivo do bloco de funções. O bloco de funções definido pelo usuário sem um arquivo aparecerá com um ícone  e todas as suas conexões serão excluídas. Recursos de edição como, por exemplo, copiar e colar não estão disponíveis. Caso seja editado de alguma forma, o programa não pode ser salvo ou descarregado.
Aplicar programa	Requerido	O comando não pode ser executado sem o arquivo do bloco de funções definido pelo usuário.

DICA

Se você importar o arquivo do bloco de funções definido pelo usuário com o programa aberto, ele não será atualizado automaticamente. Feche o programa e abra-o novamente para exibir o bloco de funções corretamente.

IMPORTANTE

Sempre verifique o programa original depois de editar os blocos de funções definidos pelo usuário. Caso você tenha criado um bloco de funções definido pelo usuário, usado-o no programa original e editado o bloco de funções após a gravação do programa original, a ocorrência do bloco de funções no programa não é atualizada.

Recursos adicionais

Recurso	Descrição
Apêndice C , Referência de comando das funções de lógica	Fornecer informações detalhadas sobre as funções de lógica.
Apêndice D , Referência de comandos dos blocos de funções	Fornecer informações detalhadas sobre os blocos de funções.

Download e verificação

Introdução

Tópico	Página
Download da configuração de rede do DeviceNet	163
Verificando a configuração de segurança de seu DeviceNet	165
Iniciar o Safety Device Verification Wizard	165
Determinação se os equipamentos podem ser verificados	166
Seleção dos equipamentos a serem verificados	167
Revisão dos relatórios de verificação do equipamento de segurança	169
Trava de dispositivos de segurança	170
Visualização do resumo do Safety Device Verification Wizard	171

Download da configuração de rede do DeviceNet

Antes de fazer o download, você deve entrar em comunicação com a rede DeviceNet usando o software RSNetWorx para DeviceNet. O computador e os equipamentos com os quais você deseja entrar em comunicação devem estar conectados à rede do DeviceNet. Ou caso você esteja executando o controlador no modo independente, o computador deve estar conectado à porta USB do controlador SmartGuard.

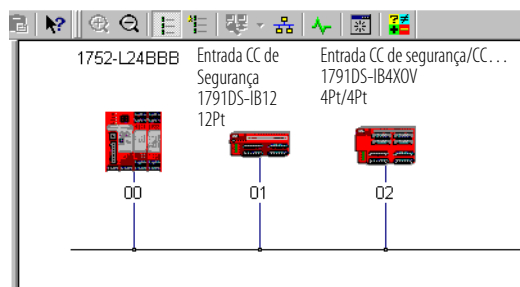
Se você estiver conectado ao controlador SmartGuard usando o protocolo EtherNet/IP, é necessário seguir as etapas nesta seção. Quando estiver conectado ao SmartGuard pelo protocolo EtherNet/IP, você está essencialmente fazendo a ponte pelo controlador SmartGuard até a rede DeviceNet, e então entrando em comunicação, fazendo o download e a monitoração. Embora este capítulo trate do uso do protocolo DeviceNet, é necessário seguir as mesmas etapas para o protocolo EtherNet/IP.

Quando você entra em comunicação com uma rede do DeviceNet, o software RSNetWorx for DeviceNet pesquisa a rede uma vez e lhe mostra os equipamentos na rede. Ele não lê (faz upload) ou altera (faz download) os parâmetros de nenhum dos equipamentos.

A representação gráfica da rede criada pela operação de pesquisa permanece estática. Ela não é atualizada automaticamente para mostrar as alterações desde a última pesquisa, a menos que a opção Continuous Browse esteja marcada.

Siga estas etapas para fazer download da configuração de rede do DeviceNet.

1. Entre em comunicação clicando no ícone on-line .
2. Navegue até a rede do DeviceNet e clique em OK no prompt.



Durante todas as operações de pesquisa, o software RSNetWorx for DeviceNet lê os seguintes atributos de todos os equipamentos.

Atributo de segurança	Descrição
Combinação entre o número da rede de segurança (SNN) e endereço do nó	O endereço do nó e o SNN armazenados no arquivo de configuração do RSNetWorx for DeviceNet devem corresponder ao endereço do nó e ao SNN do equipamento on-line. Caso os SNNs não casem, o equipamento entra no estado de erro do SNN. Consulte a página 67 para informações sobre a resolução de um erro de diferença SNN.
Assinatura da configuração	O software RSNetWorx for DeviceNet compara a assinatura da configuração em seu arquivo de configuração com a assinatura da configuração no equipamento on-line.
Trava de segurança	Caso o equipamento esteja com uma trava de segurança, a sua configuração não pode ser modificada sem antes soltá-la.

3. Faça download da configuração na rede, clicando com o botão direito do mouse no dispositivo e escolhendo Download to Device.
4. Confirme a intenção de fazer download clicando em Yes.

Caso um equipamento seja protegido por senha, o software RSNetWorx for DeviceNet solicita a você que digite a senha de cada dispositivo protegido.

Caso um equipamento tenha uma trava de segurança, você deve primeiro destravar o equipamento e, em seguida, fazer download.

IMPORTANTE

Caso você retire a trava de segurança de um equipamento, você deve executar o Safety Device Verification Wizard para verificar novamente e colocar a trava de segurança no equipamento antes de operar o equipamento no sistema de segurança.

DICA

Caso nenhum dos equipamentos esteja protegido por senha ou por trava de segurança, é possível escolher Download to Network no menu Network para fazer download da configuração na rede. No entanto, esse processo ignora os equipamentos protegidos por senha ou por trava de segurança.

Verificando a configuração de segurança de seu DeviceNet

IMPORTANTE

Antes de executar o Safety Device Verification Wizard, você deve pesquisar e fazer upload da rede, além de testar os equipamentos de segurança e todas as suas funções de segurança para verificar se elas estão funcionando corretamente. Você deve testar integralmente a aplicação antes de colocar uma trava de segurança nos equipamentos.

Consulte o Manual de referência de segurança do controlador SmartGuard, publicação [1752-RM001](#), para informações sobre o teste de verificação para aplicações de segurança.

O Safety Device Verification Wizard, acessado no software RSNetWorx for DeviceNet, orienta você durante o processo de verificação da configuração dos equipamentos de segurança e fornece os meios para colocar uma trava de segurança nesses equipamentos. O processo de verificação inclui o upload e a comparação da configuração armazenada no equipamento com a configuração armazenada no arquivo de configuração do software RSNetWorx for DeviceNet. A configuração é exibida em um relatório para facilitar a verificação visual e a manutenção dos registros.

IMPORTANTE

Alguns equipamentos na rede talvez não suportem a verificação feita pelo Safety Device Verification Wizard. Consulte a documentação do usuário para determinar o método necessário à verificação desses equipamentos.

Iniciar o Safety Device Verification Wizard

Siga estas etapas para executar o Safety Device Verification Wizard.

1. Escolha Network>Safety Device Verification Wizard.

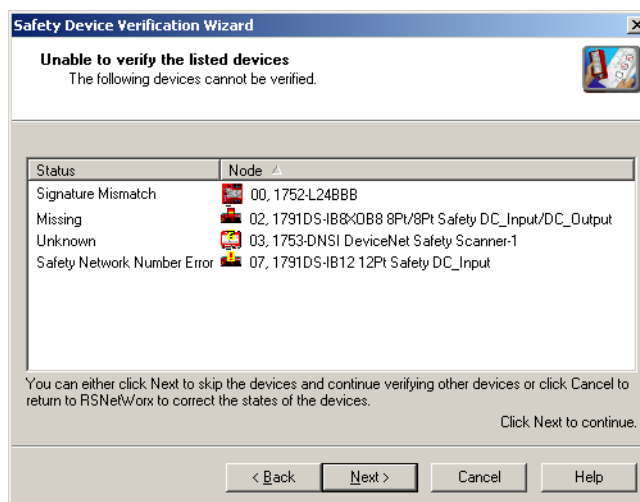
A caixa de diálogo Welcome, que descreve o processo de verificação, aparece.

2. Clique em Next.

Determinação se os equipamentos podem ser verificados

Quando o Safety Device Verification Wizard pesquisa a rede, ele verifica o status de segurança dos equipamentos na rede para determinar se eles podem ser verificados.

Se algum dispositivo estiver em um estado que impede o assistente de continuar o processo de verificação, a caixa de diálogo Unable to verify the listed devices aparece, listando aqueles dispositivos e seu status atual, incluindo um ícone de dispositivo encoberto com um ícone de status.



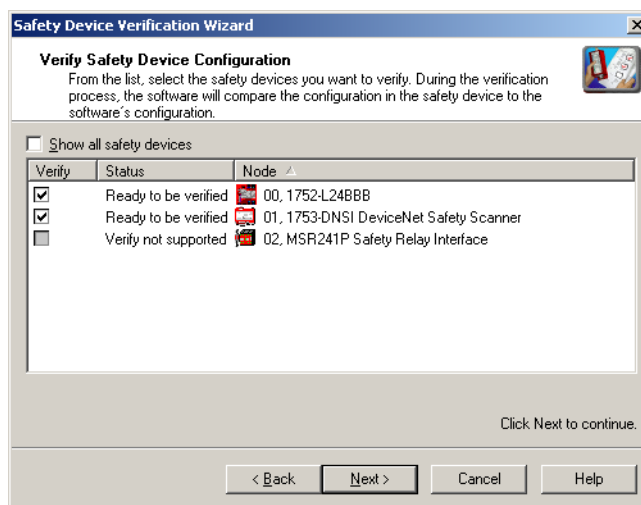
Status	Ícone sobreposto	Descrição
Não encontrado		O equipamento faz parte da configuração da rede, mas não foi encontrado durante a operação de pesquisa.
Diferença		A identidade do equipamento na configuração da rede não corresponde à identidade do equipamento on-line.
Desconhecido		O equipamento está na configuração, mas ainda não foi detectado na rede.
Erro no número da rede de segurança		O número da rede de segurança (SNN) do equipamento é inválido ou não corresponde ao SNN do dispositivo no arquivo de configuração do RSNetWorx for DeviceNet.
Diferença de assinatura	Nenhum	A assinatura da configuração no equipamento não corresponde à assinatura de configuração no arquivo de configuração do RSNetWorx for DeviceNet.
Com trava de segurança		O equipamento já está com trava de segurança.

Para retornar ao software RSNetWorx for DeviceNet para que seja possível corrigir o status dos equipamentos indicados, feche o Safety Device Verification Wizard clicando em Cancel.

Para ignorar os equipamentos listados e continuar o processo de verificação para outros equipamentos de segurança na rede, clique em Next.

Seleção dos equipamentos a serem verificados

Escolha quais dispositivos devem ser verificados usando as caixas de seleção na coluna Verify da caixa de diálogo Verify Safety Device Configuration. Só é possível selecionar os equipamentos cujo status seja Ready to be verified.



Caso a caixa de seleção Show all safety devices esteja marcada, a caixa de diálogo lista todos os dispositivos de segurança na rede e mostra seu status atual. Caso ela esteja desmarcada, que é o padrão, apenas os equipamentos com o seguinte status são mostrados:

- Verify FAILED

A operação de upload e de comparação indicou que a configuração no dispositivo não corresponde à configuração do arquivo do RSNetWorx for DeviceNet.

- Ready to be verified

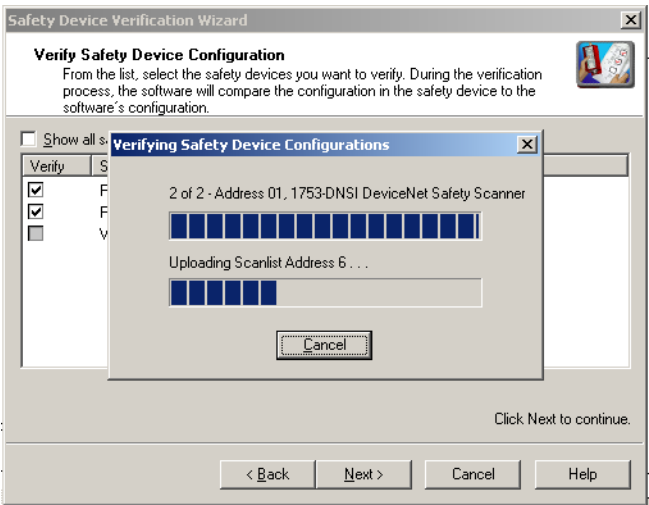
O equipamento não tem uma trava de segurança e pode ser selecionado para verificação.

- Verificação não suportada

O equipamento não tem uma trava de segurança, embora não suporte a verificação do Safety Device Verification Wizard.

Consulte a documentação de usuário para obter informações sobre como verificá-lo. Assim que é verificado, o equipamento pode receber a trava de segurança do assistente.

Clique em Next para iniciar o processo de upload e de comparação.



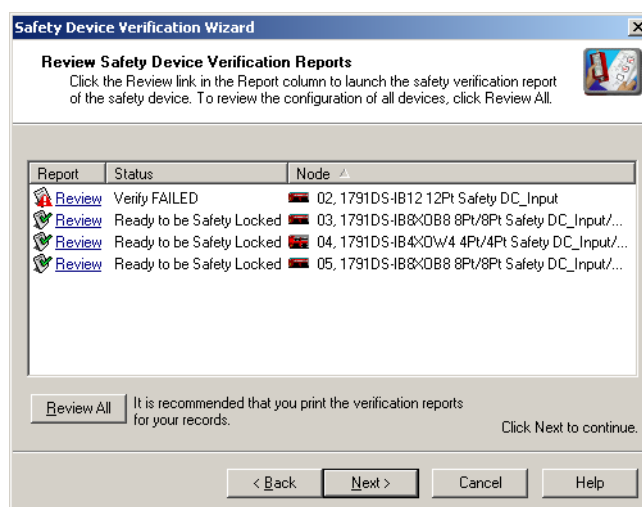
DICA

Caso você clique em Next sem selecionar um equipamento a ser verificado, o assistente verifica se algum equipamento foi verificado ou está pronto para ser travado nessa execução do assistente.

Se	O assistente exibirá
os equipamentos forem verificados	a caixa de diálogo Review listando esses dispositivos.
os equipamentos estiverem prontos para receberem a trava de segurança	a caixa de diálogo Lock listando esses dispositivos.
nenhum equipamento for verificado	a caixa de diálogo Finish.
nenhum equipamento estiver pronto para receber a trava de segurança	a caixa de diálogo Finish.

Revisão dos relatórios de verificação do equipamento de segurança

A página Review exibe os equipamentos de segurança com o status Verify FAILED ou Ready to be Safety Locked.



1. Clique em Review na coluna Report para abrir o relatório em HTML do equipamento no navegador padrão.
2. Clique em Review All para gerar um relatório de verificação em HTML de todos os equipamentos listados.

DICA

Caso o status de um equipamento seja Verify FAILED, mais informações são fornecidas no relatório de falha na verificação.

3. Consulte e imprima os relatórios de verificação dos registros.

IMPORTANTE

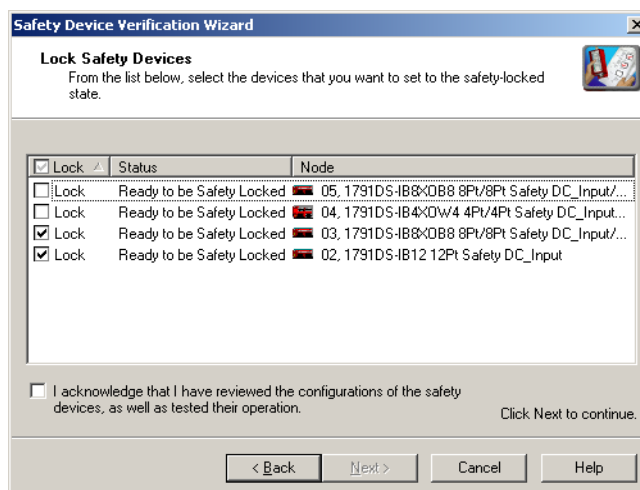
Você deve consultar as configurações do equipamento e gravar as assinaturas da configuração antes de operar uma aplicação de segurança.

Trava de dispositivos de segurança

IMPORTANTE

Antes de travar as configurações do equipamento de segurança, você deve realizar todas as etapas de verificação necessárias à sua aplicação.

1. Escolha os equipamentos a receberem a trava de segurança marcando a caixa de seleção na coluna Lock de cada equipamento pronto para recebê-la.



2. Você deve marcar a caixa de seleção de confirmação para que o processo de travamento possa continuar.
3. Clique em Next.

O assistente realiza uma comparação final da assinatura de configuração em cada equipamento de segurança com sua assinatura de configuração no software RSNetWorx for DeviceNet antes de travá-lo.

4. Se algum dos equipamentos selecionados for protegido por senha, você será solicitado a digitar a senha desse equipamento.



Caso você queira ignorar o equipamento e permitir que o processo de travamento continue para os demais equipamentos, clique em Skip.

Visualização do resumo do Safety Device Verification Wizard

Antes do fechamento, o assistente exibe um resumo de todos os equipamentos de segurança que receberam a trava, o número de equipamentos de segurança que ainda precisam receber a trava e permite que você veja o estado verificado e com trava de segurança de todos os equipamentos na rede.

Clique em Finish para fechar o assistente.

Observações:

Monitoração do Status e Controle de Falhas

Introdução

Tópico	Página
Indicadores de status	173
Tela alfanumérica	174
Monitoração da entrada da fonte de alimentação de E/S	175
Monitoração das informações de manutenção de E/S	176
Exibição de dados de status de E/S	179
Status de conexão do controlador (função de escravo de segurança)	182
Categorias de erro	184
Tabela do histórico de erros	185
Mensagens do histórico de erros e ações corretivas	188
Erros de download e ações corretivas	192
Erros de reinicialização e ações corretivas	194
Erros de alteração do modo e ações corretivas	195

Indicadores de status

O controlador SmartGuard 600 conta com indicadores de status para módulos, status de rede DeviceNet e EtherNet/IP, trava, comunicação USB e EtherNet/IP, status de entrada e saída individual, assim como uma tela alfanumérica para códigos de erro DeviceNet, endereços de nó DeviceNet e informações de endereço EtherNet/IP.

Para obter uma descrição das combinações entre cor e status dos indicadores de status e das ações recomendáveis, consulte o [Apêndice B](#).

Tela alfanumérica

A tela alfanumérica do controlador fornece códigos de erro DeviceNet, endereço de nó DeviceNet e informações de endereço EtherNet/IP. Em condições normais de operação, a tela mostra o endereço de nó do módulo, de 00 a 63 em formato decimal. Caso o controlador esteja em operação na configuração independente (não em rede), a tela mostra 'nd'. Ela pisca quando o controlador está em auto-teste, configuração ou no modo inativo. Caso haja uma falha, a tela alterna entre o código de erro e o endereço do nó em que ocorreu o erro. Caso tenha ocorrido um erro fatal, a tela mostra apenas o código de erro.

Quando a chave de serviço é pressionada, a tela mostra a assinatura da configuração de segurança do controlador dois dígitos por vez. A assinatura da configuração também pode ser visualizada na guia Safety da caixa de diálogo Controller Properties do software RSNetWorx para DeviceNet. É possível usar a assinatura da configuração para verificar se o programa e a configuração do controlador não foram alterados.

Quando a chave de exibição do endereço IP é pressionada por 1 segundo ou mais, a tela mostra o endereço EtherNet/IP que está configurado. O código de erro 'n4' é exibido se um erro ocorrer na configuração EtherNet/IP.

Explicação da operação da tela

Status		Tela	
Condições normais com o DeviceNet habilitado	Modo de operação: Operação de comunicação Safety I/O: em operação	O endereço de nó do controlador.	Acesa
	Modo de operação: Operação de comunicação Safety I/O: fora de operação		Intermitente
	Modo de operação: auto-teste, configuração ou inativo		Intermitente
Condições normais com o DeviceNet desabilitado	Modo de operação: Run	nd	Acesa
	Modo de operação: auto-teste, configuração ou inativo		Intermitente
Condições de erro	Erro crítico	Somente código de erro	Acesa
	Cancelamento	Somente código de erro	Acesa
	Erro não fatal	Alterna entre o código do erro e o endereço do nó em que ocorreu o erro.	

Para obter uma descrição das combinações entre os indicadores de status e os códigos de exibição alfanumérica, inclusive as ações corretivas, consulte o [Apêndice B](#).

Monitoração da entrada da fonte de alimentação de E/S

É possível monitorar a entrada da fonte de alimentação de E/S usando a tela alfanumérica na parte frontal do controlador, bem como os dados de status geral na comunicação de E/S DeviceNet.

Caso um terminal de E/S no controlador esteja definido para algo que não seja Not Used e a tensão da fonte de alimentação normal não seja fornecida, a tela alfanumérica exibe:

- P4: a fonte de alimentação para entradas (V1,G1) está fora da faixa.
- P5: a fonte de alimentação para saídas (V2,G2) está fora da faixa.

Monitoração das informações de manutenção de E/S

É possível configurar um modo de manutenção e um limite de alarme para cada entrada local, saída de teste e terminal de saída local usando a guia Maintenance da caixa de diálogo Controller Properties do software RSNetWorx para DeviceNet. É possível configurar um terminal para o contador de operação do contato ou para a monitoração do tempo de ativação total.

Monitoração do contador de operações do contato

Esta função de manutenção conta o número de operações de desativação e ativação em uma entrada local, saída de teste ou terminal de saída local e armazena a contagem internamente na memória não volátil.

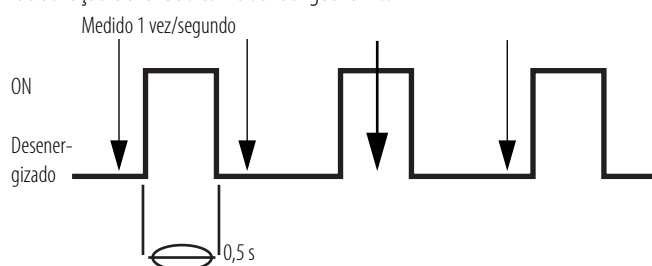
Monitoração do tempo de ativação total

Esta função de manutenção conta por quanto tempo uma entrada local, saída de teste ou saída local permanece ativada e armazena esse tempo de ativação total internamente na memória não volátil. A função de monitor verifica se o equipamento conectado está ativado, em intervalos de um segundo. Caso o equipamento esteja ativado por menos de um segundo, o tempo total de ativação talvez não seja preciso.

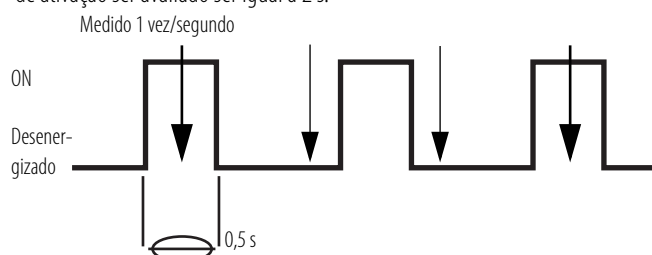
EXEMPLO

Calculando o tempo total de ativação com pulsos de 0,5 segundo

Neste primeiro exemplo, o bit está realmente ativado para $0,5\text{ s} \times 3 = 1,5\text{ s}$. No entanto, como o bit só é ativado quando o status é verificado, o tempo total de ativação é avaliado como sendo igual a 1 s.



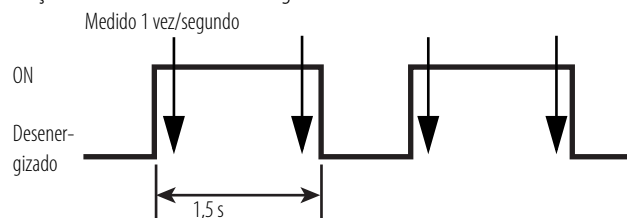
No segundo exemplo, o bit está realmente ativado para $0,5\text{ s} \times 3 = 1,5\text{ s}$, embora seja ativado duas vezes quando o status é verificado, o que faz o tempo de total de ativação ser avaliado ser igual a 2 s.



EXEMPLO

Calculando o tempo total de ativa  o com pulsos de 1,5 segundo

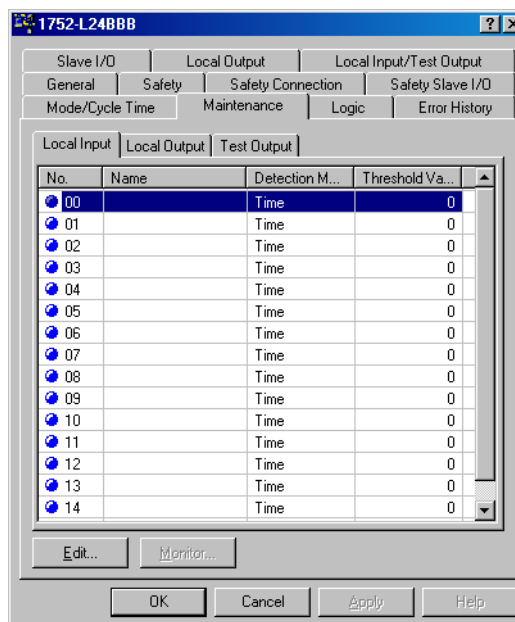
No segundo exemplo, o bit est  realmente ativado para $1,5 \text{ s} \times 2 = 3 \text{ s}$, embora seja ativado 4 vezes quando o status   verificado, o que faz o tempo de total de ativa  o ser avaliado como sendo igual a 4 s.



Configura  o de um modo de monitora  o de manuten  o

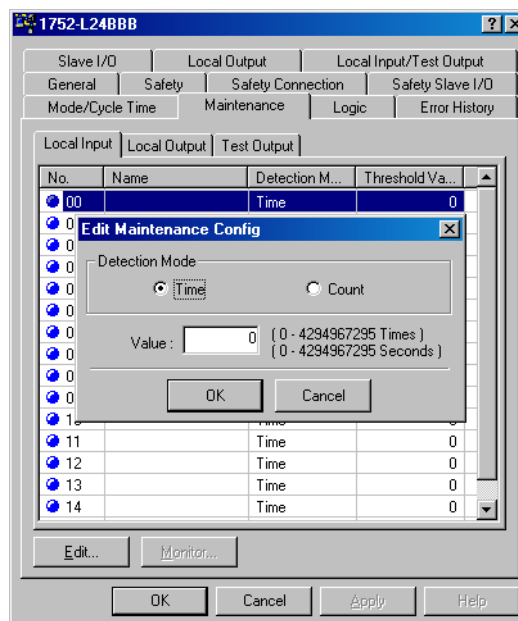
Siga estas etapas para configurar o modo do contador de opera  o do contato de um terminal.

1. No software RSNetWorx for DeviceNet, clique com o bot o direito do mouse no controlador e escolha Properties.
2. Selecione a guia Maintenance.



3. Selecione a guia Local Input, Local Output ou Test Output.

4. Selecione o terminal desejado e clique em Edit.



5. Na caixa de diálogo Edit Maintenance Config, escolha o modo de detecção, Count ou Time.
6. Digite um valor de limite de alarme para o modo de detecção especificado.

Modo de detecção	Faixa de valores válida
Tempo	0 a 4.294.967.295 segundos
Contagem	0 a 4.294.967.295 vezes

7. Clique em OK.
8. Clique em OK.

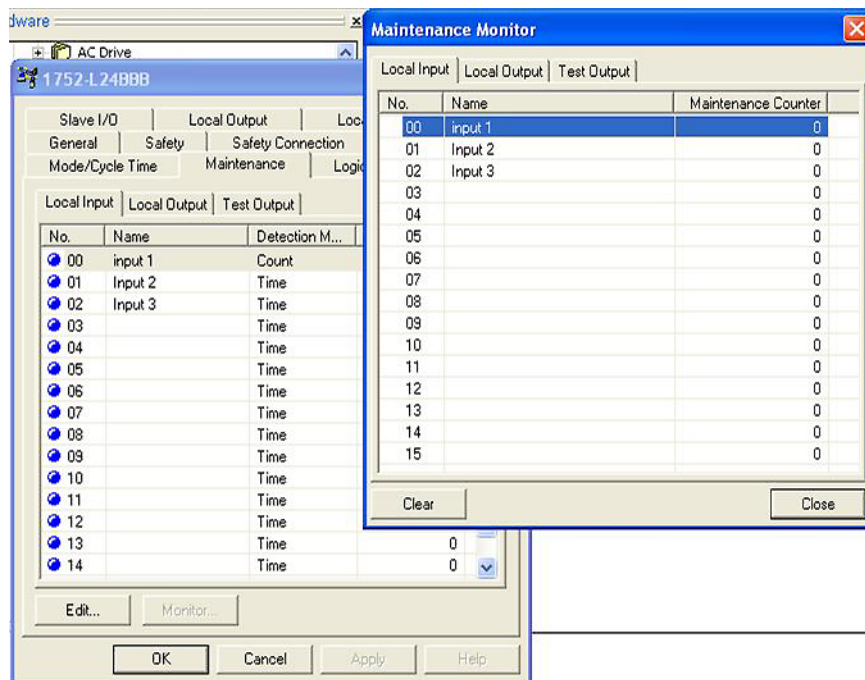
Quando você está on-line com o controlador, é possível monitorar os terminais configurados clicando em Monitor na guia Maintenance.

Apagamento dos valores de manutenção

Siga estas etapas para apagar os valores acumulados de contagem ou de tempo enquanto estiver on-line com o controlador.

1. Na guia Maintenance, clique em Monitor.

2. Clique em Clear na caixa de di logo Maintenance Monitor.



Exibi  o de dados de status de E/S

Quando o controlador opera como sendo um escravo de seguran a ou um escravo alvo padr o, as informa  es de status podem ser adicionadas   primeira linha dos dados de transmiss o. As informa  es podem ser armazenadas em um controlador e usadas para estabelecer um sistema de monitora  o.

Dados de status do controlador

Nome do tag	Dimens�es dos dados	Tipo do atributo
Status geral	1 byte	N�o seguran�a
Status da entrada local	Palavra	Seguran�a
Status da sa�da local	Byte	Seguran�a
Sa�da de teste/status da l�mpada muting	Byte	N�o seguran�a

ATEN  O



N o use dados com um atributo de n o seguran a para configurar o sistema de controle de seguran a. As medidas necess rias para os dados de seguran a n o s o tomadas durante a gera  o de dados de n o seguran a.

Dados de status geral

Os flags de status geral são atributos de não segurança que indicam o status do sistema.

Detalhes dos dados de status geral

Bit	Nome	Descrição
0	Flag de status da tensão da fonte de alimentação de entrada	Indica o status da tensão da fonte de alimentação para as entradas. OFF: a fonte de alimentação normal está ativa. ON: Erro na tensão da fonte de alimentação ou a fonte de alimentação está desativada.
1	Flag de status da tensão da fonte de alimentação de saída	Indica o status da tensão da fonte de alimentação para as saídas. OFF: a fonte de alimentação normal está ativa. ON: Erro na tensão da fonte de alimentação ou a fonte de alimentação está desativada.
2	Indicação de erro da comunicação de E/S padrão	Indica se há um erro na comunicação de E/S padrão. OFF: sem erro. ON: um erro foi detectado em uma ou mais conexões padrão.
3	Flag de status da comunicação de E/S padrão	Indica se a comunicação de E/S padrão está em andamento. O flag está em ON caso a comunicação normal esteja em andamento para todas as conexões padrão.
4	Indicação de erro da comunicação de E/S de segurança	Indica se há um erro na comunicação de E/S de segurança. OFF: sem erro. ON: um erro foi detectado em uma ou mais conexões de segurança.
5	Flag de status da comunicação de E/S de segurança	Indica se a comunicação de E/S de segurança está em andamento. O flag está em ON caso a comunicação normal esteja em andamento para todas as conexões de segurança.
6	Flag de modo de operação	Indica o modo de operação do controlador. OFF: o controlador não está no modo de operação. ON: o controlador está no modo de operação.
7	Flag de status do controlador	Indica o status do controlador. OFF: há um erro. ON: o controlador está operando normalmente.

Status da entrada local

Quando o bit está ativado, o status da entrada é normal. Quando o bit está desativado, um erro foi detectado

Status do terminal de entrada de segurança local

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Terminal 7	Terminal 6	Terminal 5	Terminal 4	Terminal 3	Terminal 2	Terminal 1	Terminal 0
1	Terminal 15	Terminal 14	Terminal 13	Terminal 12	Terminal 11	Terminal 10	Terminal 9	Terminal 8

Status da saída local

Quando o bit está ativado, o status da saída é normal. Quando o bit está desativado, um erro foi detectado

Status do terminal de saída de segurança local

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Terminal 7	Terminal 6	Terminal 5	Terminal 4	Terminal 3	Terminal 2	Terminal 1	Terminal 0

Saída de teste ou status da lâmpada muting

Quando o bit está ativado, o status da saída de teste é normal. Quando o bit está desativado, um erro foi detectado

Saída de teste/status da lâmpada muting

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Status de desconexão do terminal 3 detectado	Reservado			Terminal 3	Terminal 2	Terminal 1	Terminal 0

Status de conexão do controlador (função de escravo de segurança)

Código	Status	Ação Corretiva
00:0001	Comunicação normal	O status da conexão de E/S de segurança é normal.
01:0001	Tempo-limite da conexão de E/S de segurança	O tempo-limite da conexão de E/S de segurança foi atingido. Verifique o seguinte: • Todos os nós têm a mesma taxa de transmissão? • O comprimento do cabo está correto? • O cabo está desconectado ou frouxo? • A resistência de terminação está apenas nas extremidades da linha principal? • Há ruído excessivo?
01:0106	Erro de leitura de controle da conexão de saída	O escravo de segurança estabeleceu uma conexão de E/S de segurança de saída com um mestre de segurança que tinha um endereço do nó diferente em relação à última vez.
01:0109	Erro nas dimensões dos dados	As dimensões da E/S do escravo de segurança definidas para o escravo de segurança do controlador SmartGuard e as dimensões definidas no ajuste de parâmetro da conexão de segurança do mestre de segurança não casam. Como o ajuste de parâmetro de E/S do escravo de segurança talvez tenha sido alterado, exclua e configure novamente as conexões registradas no mestre de segurança.
01:0110	Equipamento não configurado	O escravo de segurança ainda não foi configurado. Faça download dos parâmetros do equipamento no escravo de segurança.
01:0111	Erro de RPI	O RPI definido na conexão de segurança do mestre de segurança é menor que o tempo de ciclo do escravo de segurança.
01:0113	Número de erros na conexão	O ajuste de parâmetro excede o número máximo de conexões de E/S de segurança suportadas pelo escravo de segurança. Verifique os ajustes de parâmetros relevantes da conexão de segurança do mestre de segurança.
01:0114	Identificação do erro ou erro do código de produto	Os dados do equipamento no arquivo de configuração do RSNetWorx for DeviceNet e o equipamento físico no sistema não casam. Use o Safety Device Verification Wizard para verificar se o equipamento no sistema e o equipamento no arquivo de configuração casam. Caso eles não casem, reconfigure as conexões com o mestre de segurança.
01:0115	Erro do tipo de equipamento	Os dados do equipamento no arquivo de configuração do RSNetWorx for DeviceNet e o equipamento físico no sistema não casam. Use o Safety Device Verification Wizard para verificar se o equipamento no sistema e o equipamento no arquivo de configuração casam. Caso eles não casem, reconfigure as conexões com o mestre de segurança.
01:0116	Erro de revisão do firmware	Os dados do equipamento no arquivo de configuração do RSNetWorx for DeviceNet e o equipamento físico no sistema não casam. Use o Safety Device Verification Wizard para verificar se o equipamento no sistema e o equipamento no arquivo de configuração casam. Caso eles não casem, reconfigure as conexões registradas com o mestre de segurança.

Código	Status	Ação Corretiva
01:0117	Erro de caminho da conexão	Duas ou mais conexões de E/S de segurança singlecast ou uma conexão de E/S de segurança multicast com um RPI diferente foram definidas para uma E/S de escravo de segurança. Para compartilhar uma E/S do escravo de segurança em um escravo de segurança com mais de um mestre de segurança, unifique todos os RPIs e defina o tipo de conexão para multicast. Os escravos de segurança do controlador SmartGuard não podem ter mais de uma conexão de E/S de segurança singlecast para cada E/S de escravo de segurança. Defina vários caminhos de conexão para a E/S do escravo de segurança do controlador. Caso as soluções anteriores não tenham resolvido o problema, exclua e reconfigure as conexões do mestre de segurança.
01:031E	Número de erros na conexão	O ajuste do número de conexões de E/S de segurança excede o limite superior suportado pelo escravo de segurança. Ajuste o parâmetro da conexão de segurança do mestre de segurança relevante. Em especial, verifique se não haja mais de 15 mestres de segurança definidos para cada conexão multicast, com um total máximo de 60.
01:031F	Erro no recurso de identificação da conexão	O número máximo de identificações da conexão de um mestre de segurança (12) foi excedido. Clique em Advanced na caixa de diálogo Safety Connection Properties. Marque a caixa de seleção Request target device to allocate message IDs. Faça download dos parâmetros do equipamento no mestre de segurança.
01:07FF	Escravo de segurança inexistente	O escravo de segurança talvez não tenha sido adicionado à rede corretamente. Verifique se o escravo de segurança correspondente está on-line. Caso o escravo de segurança não esteja on-line, verifique se os seguintes itens: • O endereço do nó do escravo de segurança está correto? • Todos os nós têm a mesma faixa de comunicação? • O comprimento do cabo está correto? • O cabo está desconectado ou frouxo? • A resistência de terminação está apenas nas extremidades da linha principal? • Há ruído excessivo?
01:080C	Casamento da assinatura da segurança	A assinatura da segurança do escravo de segurança monitorado pelo mestre de segurança não casa com a assinatura do próprio escravo. Reinicialize o escravo de segurança para o ajuste de parâmetro padrão e faça download dos parâmetros do equipamento. Caso a solução acima não funcione, exclua e reconfigure as conexões configuradas no mestre de segurança.
01:080E	Descasamento do número da rede de segurança (SNN)	O SNN do escravo de segurança monitorado pelo mestre de segurança não casa com o SNN do próprio escravo. Reinicialize o escravo de segurança para o ajuste de parâmetro padrão e faça download dos parâmetros do equipamento corretos novamente. Caso a solução acima não funcione, exclua e reconfigure as conexões configuradas no mestre de segurança.
D0:0001	Modo inativo	Como o mestre de segurança do controlador SmartGuard está no modo inativo, as conexões de E/S de segurança não foram estabelecidas. Altere o modo de operação do controlador SmartGuard para em execução.

Categorias de erro

Os erros do controlador podem ser categorizados em erros não fatais, de cancelamento e críticos.

Categorias de erro do controlador

Categoria do erro	Descrição
Erros não fatais	Um erro que desliga o terminal de conexão de E/S de segurança ou de E/S local e coloca-o no estado de segurança. O controlador continua operando no modo de operação.
Erros de cancelamento	O controlador sai do modo de operação, vai para o modo inativo e coloca toda a E/S de segurança em seu estado de segurança. As funções de comunicação por mensagens explícitas ou parciais do software RSNetWorx para DeviceNet são suportadas para habilitá-lo a verificar o estado do erro.
Erro crítico	O controlador pára de funcionar completamente quando esse tipo de erro ocorre. Consulte a página 192 para erros de download. Consulte Erros de reinicialização e ações corretivas para erros de reset. Consulte Erros de alteração do modo e ações corretivas para erros que podem ocorrer quando se modificam os modos.

Tabela do histórico de erros

Quando um erro é detectado, é feito um registro na tabela do histórico de erros na RAM do controlador. Caso o número de registros de erro exceda o máximo de 100, os registros mais antigos são excluídos na sequência, e os dados de erro mais recentes são armazenados como sendo um novo registro.

A tabela do histórico de erros armazena o status do controlador quando o erro ocorreu, a hora em que ele ocorreu (tempo de operação total do controlador⁽¹⁾) e o endereço do nó em que ocorreu o erro.

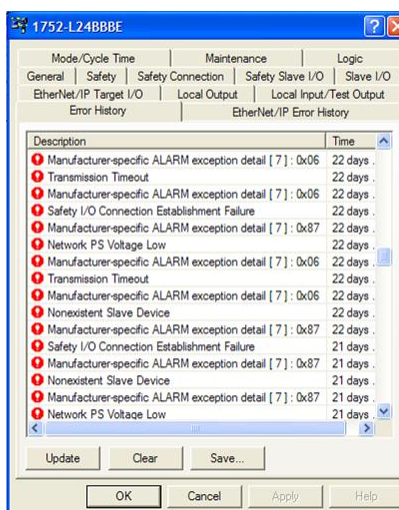
Área de memória do histórico de erros

A descrição de um erro é registrada como sendo uma entrada de histórico do erro na RAM do controlador. Caso o erro seja crítico, ele também é salvo na memória não volátil. O histórico de erros registrado na memória não volátil é mantido mesmo quando o controlador não tem energia ou o controlador é reinicializado. O histórico de erros na memória não volátil é copiado para a RAM do controlador durante a inicialização do desligamento e do ligamento do controlador. Esse histórico na RAM é lido durante a leitura do histórico de erros do software RSNetWorx for DeviceNet. No entanto, durante a remoção, ambos os históricos de erros na RAM e na memória não volátil são removidos.

Exibição da tabela do histórico de erro para o controlador 1752-L24BBB

Siga estas etapas para exibir o histórico de erros em tempo real usando o software RSNetWorx para DeviceNet enquanto estiver on-line com o controlador.

1. Clique com o botão direito do mouse no controlador SmartGuard e escolha Properties.
2. Selecione a guia Error History.



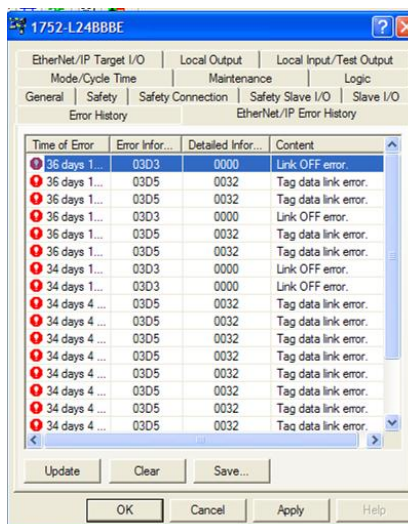
⁽¹⁾ O tempo de operação total do controlador é registrado como sendo a hora acumulada em incrementos de 6 minutos enquanto a fonte de alimentação de V0, G0 está ligada. O tempo de operação total é zerado pelo comando de reset do controlador.

- Clique em Save para salvar os dados do histórico de erros, que também pode ser salvo em um arquivo CSV separado.
- Clique em Clear para apagar o histórico de erros salvo no controlador.
- Clique em Update para atualizar as informações do histórico de erros.

Exibição da tabela de histórico de erros EtherNet/IP para o controlador 1752-L24BBBE

Siga estas etapas para exibir o histórico de erros em tempo real usando o software RSNetWorx para DeviceNet enquanto estiver on-line com o controlador.

- Clique com o botão direito do mouse no controlador SmartGuard e escolha Properties.
- Clique na guia EtherNet/IP Error History.



- Clique em Save para salvar os dados do histórico de erros, que também pode ser salvo em um arquivo CSV separado.
- Clique em Clear para apagar o histórico de erros salvo no controlador.
- Clique em Update para atualizar as informações do histórico de erros.

Tabela de histórico de erros Ethernet

Código do erro	Erro	Código de detalhes		Exibição de 7 segmentos
		Primeiro Byte ⁽¹⁾	Segundo Byte ⁽¹⁾	
0602	Memória de unidade da via CPU	01: Erro de leitura	Variável	E9<->n4
		02: Erro de gravação		
020F	Controlador de comunicação	00	01	F4<->n4
0211	Endereço IP duplicado	02	Byte baixo do endereço IP	F0<->n4
021A	Erro de lógica na tabela de configurações	00	Variável	UF
03C4	Conexão do servidor	04: BOOTP	01: O host específico não existe	E3<0>n4
			07: Erro de transmissão	
			08: Erro de recepção	
			0A: Obtendo erro de endereço IP	
03D0	Ajuste de parâmetro básico Ethernet	01: Erro de ajuste de parâmetro Ethernet	01: Erro checksum	F2<->n4
			11: Ajuste de parâmetro inconsistente	
			12: A taxa de transmissão especificada não é suportada	
		02: Erro de ajuste de parâmetro básico TCP/IP	01: Erro checksum	
			11: Endereço IP inválido	
			12: Máscara de sub-rede inválida	
			13: Endereço de conversor de protocolos padrão inválido	
			14: Nome do servidor primário inválido	
			15: Nome do servidor secundário inválido	
			16: Servidor de domínio inválido	
			17: Nome de host inválido	
03D5	Tag do enlace de dados	00	Byte baixo do endereço IP	L9<->n4
03D3	Link desenergizado	00	00	E1<->n4

⁽¹⁾ O primeiro byte combinado com o segundo byte aparece com um caractere simples, 4-hex na coluna de informações detalhadas na guia EtherNet/IP Error History. Consulte a caixa de diálogo na seção [Exibição da tabela de histórico de erros EtherNet/IP para o controlador 1752-L248BBE](#) para exemplos.

Mensagens do histórico de erros e ações corretivas

Use as mensagens do histórico de erros para identificar e corrigir os erros.

Mensagens de erro de falha no sistema do controlador

Mensagem	Descrição	Ação Corretiva
Falha no sistema	Ocorreu uma falha no sistema.	Substitua o controlador caso ocorra novamente uma falha no sistema após o desligamento e a retomada de energia.
Invalid Configuration	A configuração é inválida.	A configuração atual é diferente da configuração original. Reconfigure após a verificação.

Mensagens de erro relacionadas à programação

Mensagem	Descrição	Ação Corretiva
Function Block Status Error	Uma entrada de sinal incompatível foi definida como sendo uma condição de entrada em Set Parameters do bloco de funções.	Verifique as entradas inseridas no bloco de funções ou a lógica do programa.

Mensagens de erro de comunicação do DeviceNet

Mensagem	Descrição	Ação Corretiva
Switch Setting Mismatch	Os ajustes de parâmetros da chave não casam.	Verifique se o endereço do nó é o mesmo endereço da última configuração. Caso não seja, altere-o novamente para o endereço do nó original ou reconfigure. Caso o erro ocorra novamente, substitua o controlador.
Duplicação de MAC ID	Um ou mais endereços do nó foram duplicados.	Verifique os endereços dos demais nós. Corrija a configuração para que todos os endereços do nó sejam usados apenas uma vez e desligue e ligue a fonte de alimentação.
Baixa tensão da rede PS	A tensão da fonte de alimentação da rede é baixa.	Verifique se a tensão da fonte de alimentação está definida dentro da faixa de especificação. Verifique se não há um cabo ou fio desconectado.
Via desenergizada	A comunicação foi cortada por erros de dados frequentes.	Verifique se a taxa de comunicação de todos os nós é a mesma. Verifique se os comprimentos dos cabos das linhas principal ou ramificadas não são muito longos. Verifique se não há um cabo ou fio desconectado ou solto. Verifique se a resistência de terminação está em ambas as extremidades da linha principal e apenas nelas. Verifique se não há ruído em excesso no sistema.
Tempo-limite de transmissão	O tempo-limite da transmissão foi atingido.	
Tempo-limite da conexão de E/S padrão	O tempo-limite da conexão de E/S padrão foi atingido.	
Relevant Safety I/O Communication Stopped Because of a Safety I/O Communication Error	A conexão de E/S de segurança correspondente foi interrompida porque o tempo-limite da conexão de E/S de segurança foi atingido.	
All Safety I/O Communication Stopped Because of a Safety I/O Communication Error	Todas as conexões de E/S de segurança foram interrompidas porque o tempo-limite da conexão de E/S de segurança foi atingido.	
Tempo-limite da conexão de E/S de segurança	O tempo-limite da conexão de E/S de segurança foi atingido.	Verifique se o equipamento está configurado e operando normalmente.
Dispositivo escravo não existente	Não há dispositivo escravo no sistema.	
Falha de estabelecimento de conexão de E/S de segurança	Ocorreu um erro durante o estabelecimento de uma conexão de segurança.	Verifique o equipamento escravo e conecte um equipamento escravo apropriado.
Dispositivo escravo inválido	Um equipamento escravo não autorizado está na rede (erro de verificação).	
EM Transmission Error (Duplicate MAC ID)	Não foi possível transmitir por conta da duplicação do endereço do nó.	Verifique os endereços dos demais nós. Corrija a configuração para que todos os endereços do nó sejam usados apenas uma vez e desligue e ligue a fonte de alimentação.

Mensagens de erro de comunicação do DeviceNet

Mensagem	Descrição	Ação Corretiva
EM Transmission Error (Invalid Header)	Não foi possível transmitir por conta do cabeçalho inválido.	Verifique o endereço do nó, a identificação da classe e a identificação da instância da mensagem de transmissão.
EM Transmission Error (Device Offline)	Não foi possível transmitir porque o equipamento local não está na rede.	Verifique se a taxa de comunicação de todos os nós é a mesma.
EM Transmission Error (Message ID Error)	Não foi possível transmitir por conta de um erro na identificação da mensagem.	Verifique se os comprimentos dos cabos das linhas principal ou ramificadas não são muito longos.
EM Transmission Error (Response Timeout)	Não foi possível transmitir por conta do tempo limite de resposta excedido.	Verifique se a resistência de terminação está em ambas as extremidades da linha principal e apenas nelas. Tome precauções contra o ruído excessivo. Verifique se a tensão da fonte de alimentação da rede está definida dentro da faixa de especificação.
EM Transmission Error (Destination Device Absence)	Não foi possível transmitir porque o equipamento de destino não está na rede.	Verifique o endereço do nó de destino e o endereço do nó da mensagem de transmissão. Verifique se a tensão da fonte de alimentação do nó de destino está definida dentro da faixa de especificação. Verifique se a taxa de comunicação de todos os nós é a mesma. Verifique se os comprimentos dos cabos das linhas principal e ramificadas não são muito longos. Verifique se não há um cabo ou fio desconectado ou solto. Verifique se a resistência de terminação está em ambas as extremidades da linha principal e apenas nelas. Tome precauções contra o ruído excessivo.
EM Transmission Error (Destination Buffer Full)	Não foi possível transmitir porque o buffer de destino estava ocupado.	Verifique o tamanho de recebimento da mensagem no nó de destino.
EM Transmission Error (Command Length Error)	Não foi possível transmitir porque o comando é maior que o comprimento máximo.	Verifique as dimensões da mensagem de resposta no destino. Também verifique se as dimensões da resposta esperada na mensagem de solicitação estão corretas.
EM Transmission Error (New Request Received)	A mensagem foi excluída por conta do recebimento da nova solicitação.	Nenhuma.
Received Error Response (UEM)	É recebida uma resposta de erro quando a função de mensagem explícita do usuário é usada.	Verifique se o serviço ou as dimensões dos dados na mensagem explícita do usuário casam com as especificações do objeto de destino.

Mensagens de erro de falha do sistema do controlador EtherNet/IP

Mensagem	Descrição	Ação Corretiva
Falha no sistema	Ocorreu uma falha no sistema.	Desligue e ligue a fonte de alimentação. Caso uma falha ocorra novamente, substitua o controlador.
	Ocorreu um erro de memória EtherNet/IP.	
	Ocorreu um erro do controlador de comunicação EtherNet/IP.	
	O mesmo endereço IP está configurado para outro dispositivo na rede.	Verifique os endereços de IP dos outros dispositivos, e configure um endereço que não duplique nenhum outro.
	Ocorreu um erro de lógica na tabela de configurações.	Verifique a configuração. Caso uma falha ocorra novamente, substitua o controlador.
	Ocorreu um erro de conexão do servidor BOOTP.	Certifique-se de que o cabo está conectado corretamente. Certifique-se de que o servidor BOOTP está operando normalmente.
	Ocorreu um erro de lógica de configuração básica EtherNet/IP.	Verifique a configuração. Caso uma falha ocorra novamente, substitua o controlador.
	Ocorreu um erro de comunicação do alvo padrão EtherNet/IP.	Certifique-se de que as mesmas configurações de comunicação são usadas para cada nó. Certifique-se de que os cabos não estejam desconectados nem dobrados. Certifique-se de que a alimentação está sendo fornecida ao originador.
	Ocorreu um erro Link Off.	Certifique-se de que as mesmas configurações de comunicação são usadas para cada nó. Certifique-se de que os cabos não estejam desconectados nem dobrados. Certifique-se de que a alimentação está sendo fornecida ao hub.

Mensagens de erro relacionadas à fonte de alimentação de E/S

Mensagem	Descrição	Ação Corretiva
Baixa tensão PS de entrada	A fonte de alimentação de E/S (V1, G1) não está conectada.	Verifique se a tensão da fonte de alimentação está definida dentro da faixa de especificação. Verifique se não há um cabo ou fio desconectado.
Baixa tensão PS de saída	A fonte de alimentação de E/S (V2, G2) não está conectada.	

Mensagens de erro de segurança

Mensagem	Descrição	Ação Corretiva
Falha de sinal do teste externo na entrada de segurança	Ocorreu uma falha na fiação externa na entrada de segurança.	Verifique se o fio de sinal de entrada não está em contato com a fonte de alimentação (lado positivo).
Erro de discrepância na entrada de segurança	Existe uma discrepância entre duas entradas configuradas como sendo de canal duplo.	Verifique se o fio de sinal de entrada não tenha uma falha para terra. Verifique se o fio de sinal de entrada não está desconectado. Verifique se não há um curto-circuito entre os fios de sinal de entrada. Verifique se não ocorreu uma falha no equipamento conectado. Verifique se o valor configurado do tempo de discrepância é válido. Para se recuperar desse estado de erro, o tempo do erro de entrada da trava deve ter passado e a causa do erro deve ter sido corrigida. As entradas de segurança alvo devem ser desativadas. Para alterar o tempo de discrepância, você deve reconfigurar a entrada de segurança.
Falha de entrada interna na entrada de segurança	Ocorreu uma falha de circuito interno na entrada de segurança.	Substitua a unidade caso ocorra novamente uma falha no sistema após desligar e ligar a fonte de alimentação.

Mensagens de erro da saída de teste

Mensagem	Descrição	Ação Corretiva
Sobrecarga detectada na saída de teste	Muita corrente está sendo consumida na saída de teste.	Verifique se o fio de sinal de saída apresenta uma falha para terra ou se está sobrecarregado.
Preso no nível alto detectado na saída de teste	Há uma saída de teste presa.	Verifique se a fonte de alimentação está em contato com o fio de sinal de saída. Após a passagem do tempo de erro de entrada de fixação, desative a entrada quando a causa do erro for removida, e o erro será reinicializado. Caso não haja nenhuma falha nos fios, substitua a unidade.
Under-current Detected Using Muting Lamp	Foi detectado um erro de limite inferior da corrente na saída de teste T3.	Verifique se o fio de sinal de saída está desconectado ou se a lâmpada muting está queimada. Caso não haja nenhuma falha nos fios, verifique os indicadores de status.

Mensagens de erro da saída de segurança

Mensagem	Descrição	Ação Corretiva
Over Current Detected at Safety Output	Uma sobrecorrente foi detectada na saída de segurança.	Verifique se não há nenhuma sobrecorrente na saída.
Short Circuit Detected at Safety Output	Um curto-circuito foi detectado na saída de segurança.	Verifique se o fio de sinal de saída não tem uma falha para terra.
Preso no nível alto detectado na saída de segurança	Uma saída de segurança está presa no nível alto.	Verifique se o fio de sinal de saída não está em contato com a fonte de alimentação (lado positivo).
Conexão cruzada detectada na saída de segurança	Foi detectado um curto-circuito entre os fios de sinal de saída de sinal em uma saída de segurança.	Verifique se não há um curto-circuito entre os fios de sinal de saída.
Violação de canal duplo na saída de segurança	Ocorreu um erro de dados de saída em uma saída de segurança.	Verifique se os dados das duas saídas no modo em canal duplo estão configurados como sendo canais equivalentes.

Erros de download e ações corretivas

O controlador pode retornar uma resposta de erro durante o download dos dados no controlador. Use as mensagens exibidas no software RSNetWorx for DeviceNet para identificar o erro.

Mensagens de erro de download do software RSNetWorx para DeviceNet e ações corretivas

Mensagem	Descrição	Ação Corretiva
Cannot be executed in the current mode.	Ocorreu um erro fatal (de cancelamento), e o indicador de MS pisca em vermelho.	Verifique as chaves para ver se elas foram definidas corretamente. Do contrário, execute um reset para limpar os dados da configuração.
The device is locked.	A configuração está travada e o indicador de status LOCK está aceso.	Destrave o equipamento.
The TUNID is different.	O número da rede de segurança (SNN) não foi definido desde o reset do equipamento (o indicador de status NS pisca em verde e em vermelho) ou o SNN no dispositivo difere do SNN descarregado no software RSNetWorx para DeviceNet.	1. Reinicialize o equipamento com seus ajustes de parâmetro padrão e faça download dos parâmetros novamente. - O SNN talvez seja diferente dos demais equipamentos. Caso a tela alfanumérica do controlador mostre d6 e uma mensagem Safety I/O Connection Establishment Failure apareça na tabela do histórico de erros após a alteração do modo de operação, vá para a próxima etapa. 2. Escolha Network > Upload em Network no software RSNetWorx for DeviceNet. Unifique o SNN em toda a rede e reinicialize todos os equipamentos de acordo com os ajustes de parâmetros padrão. Assim que eles forem reinicializados, faça download dos parâmetros nos equipamentos novamente.
Privilege violation.	1. A senha usada não tem o direito de alterar a configuração. 2. Foi feita uma tentativa de definir o modo independente por meio de uma conexão do DeviceNet.	1. Verifique se a senha está correta. 2. Conecte-se ao controlador SmartGuard usando o conector USB e faça download novamente da configuração. Com o controlador 1752-L24BBBE, pode-se também fazer um download via rede EtherNet/IP.
Cannot be executed in the current device mode.	Estão sendo descarregados dados de mais de uma instância do software RSNetWorx for DeviceNet.	Aguarde a conclusão do download da outra instância.
An error was found during parameter check.	Há uma inconsistência entre os parâmetros de configuração.	Corrija os ajustes de parâmetros. Verifique o seguinte: • Um parâmetro do tempo configurado do bloco de funções é menor que o tempo de desligamento e retomada do controlador. • O intervalo do pacote requisitado (RPI) de uma conexão de segurança é menor que o tempo de desligamento e retomada. • Embora uma entrada de segurança seja configurada como sendo 'Used with test pulse', a origem de teste não está definida. • Quando as entradas de segurança foram configuradas para o modo em canal duplo, uma entrada foi configurada como sendo uma entrada padrão, embora a outra tenha um ajuste de parâmetro diferente. • Quando as entradas de segurança foram configuradas para o modo em canal duplo, uma entrada foi definida para não ser usada, embora a outra tenha um ajuste de parâmetro diferente. • Quando as saídas de segurança foram configuradas para o modo em canal duplo, uma saída foi definida para não ser usada, embora a outra tenha um ajuste de parâmetro diferente. • Para uma configuração de E/S de segurança, foi feito um ajuste de parâmetro que fez com que o número máximo de identificações da conexão (12) mantidas pelo mestre fosse excedido. Clique em Advanced na caixa de diálogo Safety Connection Properties. Marque a caixa de seleção Request target device to allocate message IDs.

Mensagens de erro de download do software RSNetWorx para DeviceNet e ações corretivas

Mensagem	Descrição	Ação Corretiva
The data used by the logic program is not aligned with other data.	Uma alteração na configuração da rede fez com que os dados usados pela lógica do programa fossem diferentes dos demais dados.	Use o Logic Editor para verificar os locais de E/S que alteraram e reinicialize os dados.
Could not access the device.	O controlador foi reinicializado em outro nó enquanto um download estava sendo executado e o número da rede de segurança (SNN) ainda não tinha sido definido. O indicador de status NS pisca em vermelho/verde.	Defina o SNN e faça download novamente dos dados.
Could not open connection.	Uma conexão com o controlador não pôde ser criada durante o download para o controlador por meio da rede DeviceNet ou EtherNet/IP.	1. Verifique se a energia do equipamento foi ligada e tente fazer download dos dados novamente. 2. Altere o modo de operação do mestre de segurança para inativo. 3. Também é possível que o ruído ou outro fator tenha tornado a comunicação instável. • Verifique se a taxa de comunicação de todos os nós é a mesma. • Verifique se os comprimentos dos cabos das linhas principal e ramificadas não são muito longos. • Verifique se não há um cabo ou fio desconectado ou solto. • Verifique se os resistores de terminação estão em ambas as extremidades da linha principal. • Tome precauções contra o ruído excessivo.
A mensagem não pôde ser enviada.	Uma conexão com o controlador não pôde ser criada durante o download para o controlador por meio da porta USB ou rede EtherNet/IP.	Verifique se a energia do equipamento foi ligada e tente fazer download dos dados novamente.
Connection failed.	Foi feita uma tentativa de configurar um dispositivo na rede DeviceNet ou EtherNet/IP através da porta USB, mas a conexão não pôde ser feita.	Verifique se a energia do equipamento foi ligada e tente fazer download dos dados novamente. Também é possível que o ruído ou outro fator tenha tornado a comunicação instável. • Verifique se a taxa de comunicação de todos os nós é a mesma. • Verifique se os comprimentos dos cabos das linhas principal e ramificadas não são muito longos. • Verifique se não há um cabo ou fio desconectado ou solto. • Verifique se os resistores de terminação estão em ambas as extremidades da linha principal. • Tome precauções contra o ruído excessivo.
Program incomplete. Start Logic Editor and check program.	Há entradas ou saída abertas em um bloco de funções usado no programa de lógica.	No Logic Editor do software RSNetWorx for DeviceNet, conecte as entradas ou as saídas abertas ou altere o número de E/S definido para o bloco de funções a fim de excluir as entradas ou as saídas sem conexão.

Erros de reinicialização e ações corretivas

O controlador pode retornar uma resposta de erro ao ser reinicializado. Use as mensagens exibidas no software RSNetWorx for DeviceNet para identificar o erro.

Mensagens de erro de reset do software RSNetWorx para DeviceNet e ações corretivas

Mensagem	Descrição	Ação Corretiva
Cannot execute in current mode.	O reset especificado não pode ser executado enquanto o controlador estiver em seu estado atual.	Altere o modo de operação ou o status de retenção da configuração e execute o reset.
The device has a different TUNID. the device TUNID will be used to reset. Is that OK?	O número da rede de segurança (SNN) salvo no equipamento não corresponde ao SNN especificado no software RSNetWorx for DeviceNet.	Verifique se a identificação da MAC ou do equipamento casa. Caso a identificação da MAC casar e você quiser reinicializar usando o SNN salvo no equipamento, continue o reset.
Access error.	A senha usada não dá autoridade para alterar as configurações.	Verifique se a senha correta está sendo usada.
The device cannot be accessed or the device type or password is different.	1. O equipamento foi reinicializado recentemente ou a energia foi desligada e ligada e o equipamento não está pronto para a comunicação. 2. O equipamento especificado para reset talvez não suporte o serviço. 3. Os dados da configuração estão travados. O indicador de status LOCK está aceso. 4. O equipamento está realizando a comunicação de E/S de segurança e não pode executar a solicitação especificada.	1. Verifique se o equipamento está pronto para a comunicação e tente o reset novamente. 2. Verifique se a identificação da MAC do equipamento está correta. 3. Remova a trava e execute o reset especificado. 4. Altere o modo de operação do mestre de segurança relevante para inativo e execute o reset especificado.
Connection failed.	Foi feita uma tentativa de reinicializar um dispositivo na rede DeviceNet ou EtherNet/IP através da porta USB, mas a conexão não pôde ser feita.	Verifique se a energia do equipamento foi ligada e tente reinicializar novamente. Também é possível que o ruído ou outro fator tenha tornado a comunicação instável. • Verifique se a taxa de comunicação de todos os nós é a mesma. • Verifique se os comprimentos dos cabos das linhas principal e ramificadas não são muito longos. • Verifique se não há um cabo ou fio desconectado ou solto. • Verifique se os resistores de terminação estão em ambas as extremidades da linha principal. • Tome as precauções contra o ruído excessivo.

Erros de alteração do modo e ações corretivas

O controlador pode retornar uma resposta de erro quando você altera os modos. Use as mensagens exibidas no software RSNetWorx for DeviceNet para identificar o erro.

Mensagens de erro de alteração do modo do software RSNetWorx for DeviceNet e ações corretivas

Mensagem	Descrição	Ação Corretiva
Cannot be executed in the current mode.	1. O equipamento não foi configurado. 2. Um erro fatal (cancelamento) ocorreu.	1. Faça download dos parâmetros do equipamento. 2. Defina as chaves do equipamento corretamente ou execute um reset para limpar os dados da configuração e faça download dos parâmetros do equipamento novamente.
Already set to the specified mode.	O equipamento já está no modo especificado.	
The device has a different TUNID.	O número da rede de segurança (SNN) salvo no equipamento não corresponde ao SNN especificado no software RSNetWorx for DeviceNet.	Verifique se a identificação da MAC do equipamento casa. Em caso positivo, o endereço da rede do equipamento não é o mesmo endereço da rede no arquivo de configuração do RSNetWorx for DeviceNet. Faça upload da rede no software RSNetWorx for DeviceNet para que o endereço da rede seja o mesmo.
Access error.	A senha usada não dá autoridade para alterar o modo de operação.	Verifique se a senha correta está sendo usada.
The device cannot be accessed, or the device type or password is different.	1. O equipamento foi reinicializado recentemente ou a energia foi desligada e ligada e o equipamento não está pronto para a comunicação. 2. O equipamento para o qual a solicitação do modo de alteração foi feita pode não suportar o serviço.	1. Verifique se o equipamento está pronto para a comunicação e tente alterar o modo novamente. 2. Verifique se a identificação da MAC do equipamento está correta.
Connection failed.	Foi feita uma tentativa de mudar o modo de operação de um dispositivo na rede DeviceNet ou EtherNet/IP através da porta USB, mas a conexão não pôde ser feita.	Verifique se a energia do equipamento foi ligada e tente alterar o modo novamente. Também é possível que o ruído ou outro fator tenha tornado a comunicação instável. • Verifique se a taxa de comunicação de todos os nós é a mesma. • Verifique se os comprimentos dos cabos das linhas principal e ramificadas não são muito longos. • Verifique se não há um cabo ou fio desconectado ou solto. • Verifique se os resistores de terminação estão em ambas as extremidades da linha principal. • Tome precauções contra o ruído excessivo.

Observações:

Especificações do controlador

Introdução

Este apêndice contém informações de especificações para os controladores SmartGuard 600.

Tópico	Página
Especificações gerais	197
Especificações ambientais	199
Certificações	201

Especificações gerais

Atributo	1752-L24BBB	1752-L24BBBE
Dimensões (AxLxP), aprox.	99,0 ⁽⁴⁾ x 99,4 x 131,4 mm ⁽⁵⁾ (3,90 ⁽⁴⁾ x 3,91 x 5,18 ⁽⁵⁾ pol.)	99,0 ⁽⁴⁾ x 113,0 x 131,4 mm ⁽⁵⁾ (3,90 ⁽⁴⁾ x 4,48 x 5,18 ⁽⁵⁾ pol.)
Peso, aprox.	460 g (1,23 lb)	575 g (1,54 lb)
Carga de corrente DeviceNet, máx	15 mA a 24 Vcc	
Tensão de alimentação ⁽¹⁾	20,4 a 26,4 Vcc (24 Vcc, –15 a 10%)	
Corrente de energização – fonte de alimentação da unidade	4,8 A pico por 600 µs a V0/G0	
Corrente de energização – fonte de alimentação de entrada de segurança	2,6 A pico por 3 ms a V1/G1	
Faixa de tensão DeviceNet	11 a 25 Vcc	
Consumo de corrente (V0 – circuito lógico interno)	230 mA a 24 Vcc	280 mA a 24 Vcc
Proteção de sobrecarga	Encerramento da saída afetada com reconexão cíclica	
Tensão de isolamento	Tipo de isolamento funcional, 50 V Testado a 600 VCA por 60 s, entre todos os grupos	
Tipo de fio	Cobre	
Categoria de fiação ⁽²⁾	2 – nas portas de alimentação, sinal e comunicação	2 – na alimentação, 1 – no sinal, 1 – porta de comunicação
Bitola do cabo	Para a fonte de alimentação e E/S, use 0,2 a 2,5 mm ² fiação sólida (12 a 24 AWG) ou 0,34 a 1,5 mm ² fiação padrão flexível (16 a 22 AWG). Antes da conexão, prepare os fios padrão engatando ferros com anéis plásticos de isolamento (padrão compatível com DIN 46228-4) Para conexões Ethernet: Conector RJ45 de acordo com IEC 60603-7, 2 ou 4 pares Categoria 5e Cabo mínimo de acordo com TIA 569-B.1 ou Categoria de cabo 5 de acordo com ISO/IEC 24701	

Atributo	1752-L24BBB	1752-L24BBBE
Torque no parafuso do terminal de E/S	0,56 a 0,79 Nm (5 a 7 lb.pol.)	
Código de temperatura norte americano	T4A	
Tipo de entrada	Entrada de corrente	
Tensão, entrada de estado ligado, mín	11 Vcc	
Tensão, entrada de estado desligado, máx	5 Vcc	
Corrente, entrada de estado desligado, máx	1 mA	
Corrente de entrada	4,5 mA	
Impedância de entrada	2,6 k Ω	
Tipo de saída de teste	Fonte de corrente	
Corrente de saída de teste por pulso ⁽³⁾	0,7 A	
Corrente de pico de saída de teste	0,7 A	
Tensão de estado desligado de teste de pulso, máx	1,2 V	
Corrente de fuga de saída de teste por pulso, máx	0,1 mA	
Corrente de saída de lâmpada muting (T3) • Mais de 25 mA • Menos de 5 mA	• Operação normal (para evitar falhas quando usada como saída de lâmpada muting) • Falha (uma indicação de falha é gerada quando usada como saída de lâmpada muting)	
Tipo de saída	Fonte de corrente	
Corrente de saída	0,5 A	
Corrente de pico de saída	0,5 A	
Tensão, saída de estado desligado, máx	1,2 V	
Corrente de fuga, saída de estado desligado, máx	0,1 mA	
Dissipação de calor	9,3 W sob carga máxima	

Atributo	1752-L24BBB	1752-L24BBBE
Comunicação Ethernet		
Conexões CIP	Não aplicável	2
Autonegociação	Não aplicável	Suportado
Taxa de dados	Não aplicável	10/100 Mbps
Duplex	Não aplicável	Total/metade
Largura de banda de comunicação de unidade permissível	Não aplicável	3000 pps ⁽⁶⁾
Comunicação de mensagem explícita	Não aplicável	502 bytes ⁽⁷⁾

⁽¹⁾ V0/G0 para circuito lógico interno; V1/G1 para dispositivos de entrada externos e saídas de teste; V2/G2 para dispositivos de saída externos.

⁽²⁾ Use estas informações sobre a categoria do condutor para planejar a rota dos cabos. Consulte Orientações de fiação e aterramento de automação industrial, publicação [1770-4.1](#).

⁽³⁾ T0 a T3 corrente total ao mesmo tempo: 1,4 A.

⁽⁴⁾ A altura inclui os conectores de terminal.

⁽⁵⁾ A profundidade inclui o conector DeviceNet.

⁽⁶⁾ PPS significa pacotes por segundo. Indica o número de pacotes enviados ou recebidos que podem ser processados por segundo.

⁽⁷⁾ O comprimento máximo de mensagem para conexão de classe 3 e conexão UCM.

Especificações ambientais

Atributo	1752-L24BBB	1752-L24BBBE
Temperatura, armazenamento	IEC 60068-2-1 (Teste Ab, desembalado não operacional frio), IEC 60068-2-2 (Teste Bb, desembalado não operacional calor seco), IEC 60068-2-14 (Teste Na, desembalado não operacional choque térmico): –40 a 70 °C (–40 a 158 °F)	
Temperatura, em operação	IEC 60068-2-1 (Teste Ad, em operação, frio), IEC 60068-2-2 (Teste Bd, em operação, calor seco), IEC 60068-2-14 (Teste Nb, em operação choque térmico): –10 a 55 °C (14 a 131 °F)	
Umidade relativa	IEC 60068-2-30 (Teste Db, desembalado não operacional calor úmido): 10 a 95% sem condensação	
Vibração	IEC 60068-2-6 (Teste Fc, em operação): 0,35 mm a 10 a 57 Hz 5 g a 57 a 150 Hz	IEC 60068-2-6 (Teste Fc, em operação): 5 g a 10 a 500 Hz
Choque, em operação	IEC 60068-2-27 (Teste Ea, desembalado choque): 15 g	
Choque, não operação	IEC 60068-2-27 (Teste Ea, desembalado choque): 30 g	
Grau de proteção do gabinete	Cumprir IP20	
Emissões	CISPR 11: Grupo 1, Classe A	
Imunidade ESD	IEC 61000-4-2: • Descargas de contato 4 kV • Descargas pelo ar 8 kV	IEC 61000-4-2: • Descargas de contato 6 kV • Descargas pelo ar 8 kV

Atributo	1752-L24BBB	1752-L24BBBE
Imunidade RF radiada	IEC 61000-4-3: • 10 V/m com onda senoidal de 1 kHz 80% AM de 80 a 1000 MHz • 10 V/m com onda senoidal de 1 kHz 80% AM de 1,4 a 2,0 MHz • 10 V/m com 200 Hz 50% Pulso 100% AM a 900 MHz • 10 V/m com 200 Hz 50% Pulso 100% AM a 1200 MHz • 3 V/m com onda senoidal de 1 kHz 80% AM de 2000 a 2700 MHz	IEC 61000-4-3: • 10 V/m com onda senoidal 1 kHz 80% AM de 80 a 1000 MHz • 10 V/m com onda senoidal 1 kHz 80% AM de 1,4 a 2,0 MHz • 20 V/m com 200 Hz 50% Pulso 100% AM a 800, 900, 1200 MHz • 3 V/m com onda senoidal 1 kHz 80% AM de 2000 a 2700 MHz
Imunidade EFT/B	IEC 61000-4-4: • ± 2 kV a 5 kHz em portas de alimentação • ± 2 kV a 5 kHz em portas de sinal • ± 2 kV a 5 kHz em portas de comunicação	IEC 61000-4-4: • ± 2 kV a 5 kHz em portas de alimentação • ± 1 kV a 5 kHz em portas de sinal • ± 1 kV a 5 kHz em portas de comunicação
Imunidade de supressor de transiente	IEC 61000-4-5: • ± 1 kV linha-linha (DM) e ± 2 kV linha-terra (CM) em portas de alimentação • ± 1 kV linha-linha (DM) e ± 2 kV linha-terra (CM) em portas de sinal • ± 1 kV linha-terra (CM) em portas de comunicação	IEC 61000-4-5: • ± 500 V linha-linha (DM) e ± 1 kV linha-terra (CM) em portas de alimentação • ± 1 kV linha-terra (CM) em portas de sinal • ± 1 kV linha-terra (CM) em portas de comunicação
Imunidade RF conduzida	IEC 61000-4-6: • 10 V rms com onda senoidal de 1 kHz 80% AM de 150 kHz a 80 MHz	

Certificações

Certificação ⁽¹⁾ (quando o produto é marcado)	Valor
c-UL-us	UL Listado para Classe I, Divisão 2 Grupo A,B,C,D Área classificada, certificado para EUA e Canadá. Consulte o arquivo UL E194810
CE	Diretriz da União europeia 2004/108/EEC EMC, compatível com: • EN 61000-6-4; Emissões industriais • EN 61131-2; Controladores programáveis (Cláusula 8, Zona A & B) • EN 61326-1; Med./Controle/Lab., Especificações industriais • EN 61000-6-2; Imunidade industrial
C-Tick	Ato de radiocomunicações australianas, compatível com: AS/NZS CISPR 11; Emissões industriais
TÜV	Certificação TÜV para segurança funcional Segurança funcional: SIL 1 a 3, de acordo com IEC 61508; Desempenho Nível PL(e) de acordo com ISO 13849-1, Categoria 1 a 4, de acordo com EN954-1; NFPA79
UL	Certificação UL para segurança funcional. Consulte o arquivo UL E256621
ODVA	Testado em conformidade com ODVA para especificações DeviceNet e Ethernet/IP

⁽¹⁾ Consulte o link de certificação de produto em <http://ab.com> para declarações de conformidade, certificados e outros detalhes de certificação.

Observações:

Indicadores de status

Introdução

Tópico	Página
Indicadores de status do módulo	203
Identificando erros usando indicadores de status de módulo e tela alfanumérica	208
Identificando erros EtherNet/IP usando indicadores de status e tela alfanumérica	212

Indicadores de status do módulo

Use estas tabelas para interpretar a cor dos indicadores de status e tomar as medidas recomendadas quando for necessário.

ATENÇÃO



Os indicadores de status não são indicadores confiáveis para funções de segurança. Eles só devem ser usados para o diagnóstico geral durante o comissionamento e a localização de falhas. Não use indicadores de status como indicadores operacionais.

Descrições do indicador de status do módulo (MS)

Se o indicador de status do módulo (MS) estiver	Significa	Faça isto
Apagado	Sem energia.	Consulte a ação corretiva seguindo esta tabela.
Verde, aceso	O controlador está em operação no modo de operação e em condições normais.	Nenhuma ação requerida.
Verde, intermitente	O controlador está inativo.	
Vermelho, intermitente	Existência de uma falha recuperável.	Consulte a ação corretiva seguindo esta tabela.
Vermelho, aceso	Existência de uma falha irrecurável.	
Vermelho/verde intermitente	Auto-teste em andamento. Ou a configuração do controlador está sendo descarregada, ou está incompleta ou incorreta. Por exemplo, a identificação da rede (UNID) não está definida.	

Se o seu indicador de status de módulo estiver desligado, siga estas etapas.

1. Desligue e ligue a fonte de alimentação.
2. Tome as ações corretivas com relação ao ruído.
3. Entre em contato com a Rockwell Automation.

Se o seu indicador de status de módulo estiver piscando em vermelho, siga estas etapas.

1. Configure as chaves corretamente.
2. Reinicialize os dados da configuração.

Se o seu indicador de status de módulo estiver vermelho (ligado), siga estas etapas.

1. Desligue e ligue a fonte de alimentação.
2. Verifique a fiação externa.
3. Tome as ações corretivas com relação ao ruído.
4. Entre em contato com a Rockwell Automation.

Se o seu indicador de status de módulo estiver piscando em vermelho e verde, siga estas etapas.

1. Configure as chaves corretamente.
2. Defina o número da rede de segurança.
3. Reconfigure o equipamento.

Descrições de indicador de status de rede DeviceNet (NS D)

Se o indicador de status de rede DeviceNet (NS D) estiver	Significa	Faça isto
Apagado	O controlador não está on-line ou talvez não haja energia na rede do DeviceNet.	Consulte a ação corretiva seguindo esta tabela.
Verde, aceso	O controlador está on-line; as conexões estão estabelecidas.	Nenhuma ação requerida.
Verde, intermitente	O controlador está on-line; não há nenhuma conexão estabelecida.	
Vermelho, aceso	Falha de comunicação por conta de uma identificação de MAC duplicada (código de erro F0) ou do barramento desenergizado (código de erro Fe).	Consulte a ação corretiva seguindo esta tabela.
Vermelho, intermitente	Tempo-limite de comunicação.	Nenhuma ação requerida.
Vermelho/verde intermitente	O Número de segurança da rede (SNN) está sendo definido.	

Se o seu indicador de status de rede estiver desligado, siga estas etapas.

1. Desligue e ligue a fonte de alimentação.
2. Verifique a fiação externa.
3. Tome as ações corretivas com relação ao ruído.
4. Entre em contato com a Rockwell Automation.

Se o seu indicador de status de rede estiver ligado ou piscando em vermelho, siga estas etapas.

1. Veja a exibição alfanumérica do endereço de nó do erro e o código de erro.
2. Verifique se os endereços de nó não foram duplicados.
3. Verifique se a faixa de comunicação é a mesma para todos os nós.
4. Verifique se os cabos não estão soltos, desconectados ou se são muito compridos.
5. Verifique se os resistores de terminação foram instalados apenas em ambas as extremidades da linha principal.
6. Tome as ações corretivas com relação ao ruído.
7. Verifique se os dispositivos alvo estão configurados, verificados e no estado em operação normal.

Descrições de indicador de status (trava) de configuração de trava

Se o indicador (trava) de configuração de trava estiver	Significa	Faça isto
Amarelo, aceso	Existe uma configuração válida travada.	Nenhuma ação requerida.
Amarelo, intermitente	Existe uma configuração válida destravada.	Trave a configuração antes do sistema de segurança ser colocado em operação.
Apagado	A configuração é inválida.	Reconfigure o controlador.

Descrições de indicador de status de configuração USB (Comm U)

Se o indicador de comunicação USB (Comm U) estiver	Significa	Faça isto
Amarelo, intermitente	O controlador está se comunicando.	Nenhuma ação requerida.
Apagado	O controlador não está se comunicando.	

Descrições de indicador de status de E/S (entradas 0 a 15, saídas 0 a 7)

Se o indicador de status de E/S estiver	Significa	Faça isto
Vermelho, aceso	Foi detectada uma falha no circuito de entrada ou de saída, ou ocorreu um erro de discrepância na E/S definida para o modo em canal duplo.	Consulte a ação corretiva seguindo esta tabela.
Vermelho, intermitente	Foi detectada uma falha na configuração do canal duplo do circuito de E/S associado.	
Apagado	O sinal de entrada ou de saída está desativado.	
Amarelo, aceso	O sinal de entrada ou de saída está ativado.	Nenhuma ação requerida.

Se o seu indicador de status de E/S estiver ligado ou piscando em vermelho, siga estas etapas.

1. Verifique se o fio de sinal:
 - não está fazendo contato com a fonte de alimentação (lado positivo).
 - não apresenta uma falha para terra.
 - não está desconectado.
2. Verifique se não há um curto-circuito entre os fios de sinal.
3. Verifique se não há nenhuma sobrecorrente na saída.
4. Verifique se não há nenhuma falha nos equipamentos conectados.
5. Verifique se os ajustes de parâmetro do tempo de discrepância são válidos.

Se o seu indicador de status de E/S estiver desligado, siga estas etapas.

1. Verifique se a tensão da fonte de alimentação está definida dentro da faixa especificada.
2. Verifique se não há um cabo ou fio desconectado.

Descrições de indicador de status de rede (NS E) EtherNet/IP

Se o indicador de status EtherNet/IP (NS E) estiver	Significa	Faça isto
Apagado	O controlador não tem um endereço IP ou não está ligado.	Consulte a ação corretiva seguindo esta tabela.
Verde, intermitente	O controlador não tem conexões estabelecidas mas obteve um endereço IP.	
Verde, aceso	O controlador tem pelo menos uma conexão estabelecida (mesmo ao roteador de mensagens).	Nenhuma ação requerida.
Vermelho, intermitente	Uma ou mais das conexões nas quais este dispositivo é o alvo terminou a temporização. Isto deve ser deixado apenas se todas as conexões com temporização terminada forem restabelecidas ou se o dispositivo for reiniciado.	Consulte a ação corretiva seguindo esta tabela.
Vermelho, aceso	O controlador detectou que seu endereço IP já está em uso.	

Se o seu indicador de status EtherNet/IP estiver desligado, siga estas etapas.

1. Alimente o controlador.
2. Configure o endereço IP.

Se o seu indicador de status EtherNet/IP estiver piscando em verde, siga estas etapas.

1. Verificando a fiação para o controlador.
2. Configure o originador para conectar ao alvo.

Se o seu indicador de status EtherNet/IP estiver piscando em vermelho, siga estas etapas.

1. Verifique a fiação externa.
2. Verifique os pontos finais.
3. Verifique as chaves.

Descrições de indicador de status de comunicação (COMM E) EtherNet/IP

Se o indicador de comunicação (COMM E) estiver	Significa	Faça isto
Verde, aceso	O controlador está se comunicando na rede Ethernet.	Nenhuma ação requerida.
Apagado	O controlador não está se comunicando na rede Ethernet.	

Descrições de indicador de status de velocidade de rede Ethernet (100)

Se o indicador de velocidade de rede (100) estiver	Significa	Faça isto
Amarelo, aceso	A taxa de comunicação é 100 Mbps.	Nenhuma ação requerida.
Apagado ⁽¹⁾	A taxa de comunicação é 10 Mbps.	Verifique se o indicador de velocidade de rede (10) está ligado.

⁽¹⁾ Se este indicador estiver desligado, juntamente com o indicador de velocidade de rede (10), verifique sua conexão Ethernet.

Descrições de indicador de velocidade de rede Ethernet (10)

Se o indicador de velocidade de rede (10) estiver	Significa	Faça isto
Amarelo, aceso	A taxa de comunicação é 10 Mbps.	Nenhuma ação requerida.
Apagado ⁽¹⁾	A taxa de comunicação é 100 Mbps.	Verifique se o indicador de velocidade de rede (100) está ligado.

⁽¹⁾ Se este indicador estiver desligado, juntamente com o indicador de velocidade de rede (10), verifique sua conexão Ethernet.

Identificando erros usando indicadores de status de módulo e tela alfanumérica

Use estas tabelas para interpretar as combinações de cores e status dos indicadores de status e de exibição alfanumérica e tomar as ações corretivas quando aplicável.

Erros críticos

MS	Indicadores		Registro do erro	Causa	Ação Corretiva
	NS	Código de exibição alfanumérico			
Apagado	Apagado	Apagado	Nenhum	Falha crítica de hardware. Nível de ruído acima do esperado.	1. Desligue e ligue a fonte de alimentação. 2. Verifique a fiação externa.
Vermelho, aceso	Apagado	Esquerda: H Direita: ---	Falha no sistema	Falha crítica de hardware. Nível de ruído acima do esperado. Terminal de saída curto-circuitado a 24 Vcc antes da operação.	3. Tome as ações corretivas com relação ao ruído. 4. Entre em contato com a Rockwell Automation.
Vermelho, aceso	Apagado	P6	Falha no sistema	Terminal de saída curto-circuitado a 24 Vcc antes da operação.	1. Desligue e ligue a fonte de alimentação. 2. Verifique a fiação externa.

Erro de cancelamento

MS	Indicadores		Registro do erro	Causa	Ação Corretiva
	NS	Código de exibição ⁽¹⁾ alfanumérico			
Vermelho, intermi- tente	Verde, aceso ou intermi- tente	E8	Diferença no ajuste de parâmetro da chave	O endereço do nó e o baud rate foram alterados após a conclusão normal do download da configuração.	1. Defina as chaves corretamente. 2. Reconfigure o equipamento.

⁽¹⁾ A tela alterna entre o código do erro e o endereço de nó do erro.

Erros não fatais

MS	Indicadores		Registro do erro	Causa	Ação Corretiva
	Código de exibição ⁽¹⁾	I/O			
Vermelho, aceso	F0	---	Duplicação de MAC ID	O mesmo endereço está definido para mais de um nó.	Verifique se os endereços de nó não foram duplicados e reconfigure o equipamento se necessário.
Vermelho, aceso	F1	---	Via desenergizada	A comunicação é cortada por conta de erros de dados frequentes.	1. Verifique se a faixa de comunicação é a mesma para todos os nós.
Vermelho, intermitente	L9	---	Tempo-limite da conexão padrão de E/S	Tempo-limite da conexão de E/S padrão.	2. Verifique se os cabos não estão soltos, desconectados ou se são muito compridos.
Vermelho, intermitente	dA	---	Tempo-limite da conexão de E/S de segurança	Tempo-limite da conexão de E/S de segurança.	3. Verifique se os resistores de terminação foram instalados apenas em ambas as extremidades da linha principal.
Vermelho, intermitente	d5	---	Dispositivo escravo não existente	Nenhum escravo detectado.	4. Tome as ações corretivas com relação ao ruído. 5. Desligue e ligue a fonte de alimentação.
Vermelho, intermitente	d6	---	Falha de estabelecimento de conexão de segurança de E/S	Não foi possível estabelecer a conexão de E/S de segurança.	Verifique se o equipamento escravo está configurado e em um estado em operação normal.
Vermelho, intermitente	d6	---	Dispositivo escravo inválido	Equipamento escravo inválido por conta de um erro de verificação.	1. Verifique a configuração do equipamento escravo. 2. Conecte um equipamento escravo compatível.
Apagado	E0	---	Baixa tensão PS da rede	A tensão da fonte de alimentação da rede é baixa.	1. Verifique se a tensão da fonte de alimentação está definida dentro da faixa especificada. 2. Verifique se os cabos ou os fios não estão soltos ou desconectados.
---	E2	---	Tempo-limite de transmissão	Tempo-limite da transmissão do DeviceNet ou não há nada conectado à rede do DeviceNet.	1. Verifique se a faixa de comunicação é a mesma para todos os nós.
Vermelho, intermitente	A0	---	Comunicação relevante de E/S de segurança interrompida por conta de um erro de comunicação da E/S de segurança	Tempo-limite da conexão de E/S de segurança interrompendo a conexão relevante de E/S de segurança.	2. Verifique se os cabos não estão soltos, desconectados ou se são muito compridos. 3. Verifique se os resistores de terminação foram instalados apenas em ambas as extremidades da linha principal.
Vermelho, intermitente	A1	---	Toda a comunicação de E/S de segurança interrompida por conta de um erro de comunicação da E/S de segurança	Tempo-limite da conexão de E/S de segurança interrompendo toda a conexão de E/S de segurança.	4. Tome as ações corretivas com relação ao ruído.
---	P4	Tudo desativado	Baixa tensão PS de entrada	Alimentação de E/S das entradas (V1, G1) não está conectada, embora um terminal de entrada de segurança ou um terminal de saída de teste seja usado.	1. Verifique se a tensão da fonte de alimentação está definida dentro da faixa especificada.
---	P5	Tudo desativado	Baixa tensão PS de saída	Alimentação de E/S das saídas (V2, G2) não está conectada, embora um terminal de saída de segurança seja usado.	2. Verifique se os cabos ou os fios não estão soltos ou desconectados.

Erros não fatais

MS	Indicadores		Registro do erro	Causa	Ação Corretiva
	Código de exibição ⁽¹⁾ alfanumérico	I/O			
---	P1	Terminal alvo vermelho, aceso Terminal pareado vermelho, intermi- tente	Falha de sinal do teste externo na entrada de segurança	Ocorreu um erro na fiação externa de uma entrada de segurança.	1. Verifique se o fio de sinal: • não está em contato com a fonte de alimentação (lado positivo). • não apresenta uma falha para terra. • não está desconectado. 2. Verifique se não há um curto-circuito entre os fios de sinal.
---	P1	Terminal alvo vermelho, aceso	Erro de discrepância na entrada de segurança	Ocorreu um erro de discrepância entre duas entradas configuradas para canal duplo.	3. Verifique se não há nenhuma falha nos equipamentos conectados.
---	P1	Terminal alvo vermelho, aceso Terminal em par vermelho, intermi- tente	Falha de entrada interna na entrada de segurança	Ocorreu uma falha de circuito interno na entrada de segurança.	4. Verifique se os ajustes de parâmetro do tempo de discrepância são válidos. Para se recuperar desse estado de erro, o tempo do erro de entrada da trava deve ter passado e a causa do erro deve ter sido corrigida. As entradas de segurança alvo devem ser desativadas. Para alterar o tempo de discrepância, você deve reconfigurar a entrada de segurança.
---	P2	N/D	Sobrecarga detectada na saída de teste	A sobrecarga foi detectada na saída de teste, quando uma saída de teste foi configurada como sendo uma saída de sinal padrão.	Verifique se o fio de sinal de saída apresenta uma falha para terra ou se está sobrecarregado.
---	P2	N/D	Preso no nível alto detectado na saída de teste	Uma saída de teste, configurada como sendo uma saída de sinal padrão, ficou presa.	1. Verifique se a fonte de alimentação (lado positivo) não está em contato com o fio de sinal de saída. Após a passagem do tempo de erro da entrada de trava e a correção da causa do erro, desative a entrada. O erro será reinicializado. 2. Caso não haja nenhuma falha nos fios, substitua a unidade.
---	P2	N/D	Subcorrente detectada usando a lâmpada muting	Desconexão detectada da luz indicadora na saída de teste, quando o terminal T3 é configurado como sendo a saída de sinal da lâmpada muting.	1. Verifique se o fio de sinal de saída não está desconectado. 2. Verifique se a luz indicadora não está queimada.

Erros não fatais

MS	Indicadores		Registro do erro	Causa	Ação Corretiva
	Código de exibição ⁽¹⁾	I/O			
---	P3	Terminal alvo vermelho, aceso Terminal pareado vermelho, intermi- tente	Sobrecorrente detectada na saída de segurança	Uma sobrecorrente foi detectada na saída de segurança.	1. Verifique se não há nenhuma sobrecorrente na saída. 2. Verifique se o fio de sinal: • não está em contato com a fonte de alimentação (lado positivo). • não apresenta uma falha para terra.
---	P3	Terminal alvo vermelho, aceso Terminal pareado vermelho, intermi- tente	Curto-circuito detectado na saída de segurança	Um curto-circuito foi detectado na saída de segurança.	3. Verifique se não há um curto-circuito entre os fios de sinal. Para se recuperar desse estado de erro, o tempo do erro de entrada da trava deve ter passado e a causa do erro deve ter sido corrigida. O sinal de saída da aplicação do usuário para a saída de segurança alvo deve ser desativado.
---	P3	Terminal alvo vermelho, aceso Terminal pareado vermelho, intermi- tente	Preso no nível alto detectado na saída de teste	Uma saída de segurança ficou presa.	
---	P3	Terminal alvo vermelho, aceso Terminal pareado vermelho, intermi- tente	Conexão cruzada detectada na saída de segurança	Uma conexão cruzada foi detectada na saída de segurança.	
---	P3	Terminal alvo vermelho, aceso	Violação de canal duplo na saída de segurança	Ocorreu um erro de dados de saída na saída de segurança. Por exemplo, uma saída é configurada para canal duplo, mas apenas um dos bits de saída está sendo ativado pelo programa.	Verifique se os dados de saída do programa das duas saídas no modo em canal duplo estão configurados como sendo canais equivalentes.

⁽¹⁾ A tela alterna entre o código do erro e o endereço de nó do erro.

Identificando erros EtherNet/IP usando indicadores de status e tela alfanumérica

Use estas tabelas para interpretar as combinações de cores e status dos indicadores de status e de exibição alfanumérica e tomar as ações corretivas quando aplicável.

Para o controlador 1752-L24BBBE, quando a chave exibe o endereço IP por um segundo ou mais, a tela mostra o endereço EtherNet/IP que está configurado. O código de erro 'n4' é exibido se um erro ocorrer na configuração EtherNet/IP.

Erros do controlador EtherNet/IP

MS	Indicadores		Registro do erro	Causa	Ação Corretiva
	NS	Código de exibição ⁽¹⁾ alfanumérico			
Apagado	Vermelho, aceso	UF	Falha no sistema	Ocorreu uma falha do hardware do módulo adaptador EtherNet/IP.	Desligue e ligue a fonte de alimentação. Caso uma falha ocorra novamente, substitua o controlador.
Vermelho, aceso	---	F0		Ocorreu uma falha de duplicação de endereço IP.	Verifique o endereço IP dos outros dispositivos, e configure um endereço que não duplique nenhum outro.
Apagado	---	E3		Ocorreu uma falha de conexão do servidor BOOTP.	1. Certifique-se de que o cabo está conectado corretamente. 2. Certifique-se de que o servidor BOOTP está operando normalmente.
Apagado	---	F2		Ocorreu uma falha de processamento de lógica de configuração básica.	Verifique a configuração. Caso uma falha ocorra novamente, substitua o controlador.
Apagado	Vermelho, intermitente	E9		Ocorreu uma falha de memória EtherNet/IP.	Desligue e ligue a fonte de alimentação. Caso uma falha ocorra novamente, substitua o controlador.
Apagado	Vermelho, intermitente	F4		Ocorreu uma falha do controlador de comunicação EtherNet/IP.	
Vermelho, intermitente	---	L9		Ocorreu um erro de comunicação do alvo padrão EtherNet/IP.	1. Certifique-se de que as mesmas configurações de comunicação são usadas para cada nó 2. Certifique-se de que os cabos não estejam desconectados nem dobrados. 3. Certifique-se de que a alimentação é fornecida ao originador.
Apagado	---	E1		Ocorreu um erro Link Off.	1. Certifique-se de que as mesmas configurações de comunicação são usadas para cada nó 2. Certifique-se de que os cabos não estejam desconectados nem dobrados. 3. Certifique-se de que a alimentação é fornecida ao hub.

⁽¹⁾ A tela alterna entre o código do erro e n4.

Referência de comando das funções de lógica

Introdução

Este apêndice descreve as funções de lógica usadas na programação.

Tópico	Página
Instrução complementação (NOT)	213
Instrução AND	214
Instrução OR	216
Instrução OR exclusiva	218
Instrução NOR exclusiva	219
Instrução de roteamento	220
Instrução de Reset Set Flip-flop (RS-FF)	220
Instrução de vários conectores	221
Instrução de comparação	222

Instrução complementação (NOT)

A saída é o inverso da entrada.

Diagrama da instrução complementação

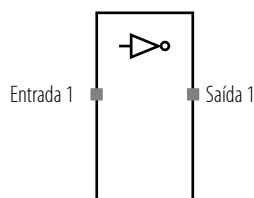


Tabela verdade instrução complementação

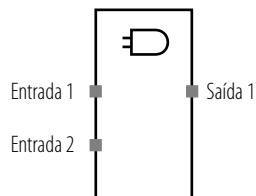
Na tabela verdade, 0 é desativado e 1, ativado.

Entrada 1	Saída 1
0	1
1	0

Instrução AND

A saída é AND lógica de até oito condições de entrada. O número de entradas pode ser configurado usando a guia In/Out Setting na caixa de diálogo Function Block Properties. A configuração padrão é de duas entradas.

Diagrama de instrução AND



Tabelas verdade da instrução AND

Na tabela verdade, 0 é desativado e 1, ativado. x minúsculo pode ser 1 ou 0.

Tabela verdade da avaliação AND de uma entrada

Entrada 1	Saída 1
0	0
1	1

Tabela verdade da avaliação AND de duas entradas

Entrada 1	Entrada 2	Saída 1
0	x	0
x	0	0
1	1	1

Tabela verdade da avaliação AND de três entradas

Entrada 1	Entrada 2	Entrada 3	Saída 1
0	x	x	0
x	0	x	0
x	x	0	0
1	1	1	1

Tabela verdade da avaliação AND de quatro entradas

Entrada 1	Entrada 2	Entrada 3	Entrada 4	Saída 1
0	x	x	x	0
x	0	x	x	0
x	x	0	x	0
x	x	x	0	0
1	1	1	1	1

Tabela verdade da avaliação AND de cinco entradas

Entrada 1	Entrada 2	Entrada 3	Entrada 4	Entrada 5	Saída 1
0	x	x	x	x	0
x	0	x	x	x	0
x	x	0	x	x	0
x	x	x	0	x	0
x	x	x	x	0	0
1	1	1	1	1	1

Tabela verdade da avaliação AND de seis entradas

Entrada 1	Entrada 2	Entrada 3	Entrada 4	Entrada 5	Entrada 6	Saída 1
0	x	x	x	x	x	0
x	0	x	x	x	x	0
x	x	0	x	x	x	0
x	x	x	0	x	x	0
x	x	x	x	0	x	0
x	x	x	x	x	0	0
1	1	1	1	1	1	1

Tabela verdade da avaliação AND de sete entradas

Entrada 1	Entrada 2	Entrada 3	Entrada 4	Entrada 5	Entrada 6	Entrada 7	Saída 1
0	x	x	x	x	x	x	0
x	0	x	x	x	x	x	0
x	x	0	x	x	x	x	0
x	x	x	0	x	x	x	0
x	x	x	x	0	x	x	0
x	x	x	x	x	0	x	0
x	x	x	x	x	x	0	0
1	1	1	1	1	1	1	1

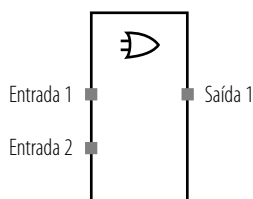
Tabela verdade da avaliação AND de oito entradas

Entrada 1	Entrada 2	Entrada 3	Entrada 4	Entrada 5	Entrada 6	Entrada 7	Entrada 8	Saída 1
0	x	x	x	x	x	x	x	0
x	0	x	x	x	x	x	x	0
x	x	0	x	x	x	x	x	0
x	x	x	0	x	x	x	x	0
x	x	x	x	0	x	x	x	0
x	x	x	x	x	0	x	x	0
x	x	x	x	x	x	0	x	0
x	x	x	x	x	x	x	0	0
1	1	1	1	1	1	1	1	1

Instrução OR

A saída é OR lógica de até oito condições de entrada. O número de entradas pode ser configurado usando a guia In/Out Setting na caixa de diálogo Function Block Properties. A configuração padrão é de duas entradas.

Diagrama da instrução OR



Tabelas verdade da instrução OR

Na tabela verdade, 0 é desativado e 1, ativado. x minúsculo pode ser 1 ou 0.

Tabela verdade da avaliação OR de uma entrada

Entrada 1	Saída 1
0	0
1	1

Tabela verdade da avaliação OR de duas entradas

Entrada 1	Entrada 2	Saída 1
0	0	0
1	x	1
x	1	1

Tabela verdade da avaliação OR de três entradas

Entrada 1	Entrada 2	Entrada 3	Saída 1
0	0	0	0
1	x	x	1
x	1	x	1
x	x	1	1

Tabela verdade da avaliação OR de quatro entradas

Entrada 1	Entrada 2	Entrada 3	Entrada 4	Saída 1
0	0	0	0	0
1	x	x	x	1
x	1	x	x	1
x	x	1	x	1
x	x	x	1	1

Tabela verdade da avaliação OR de cinco entradas

Entrada 1	Entrada 2	Entrada 3	Entrada 4	Entrada 5	Saída 1
0	0	0	0	0	0
1	x	x	x	x	1
x	1	x	x	x	1
x	x	1	x	x	1
x	x	x	1	x	1
x	x	x	x	1	1

Tabela verdade da avaliação OR de seis entradas

Entrada 1	Entrada 2	Entrada 3	Entrada 4	Entrada 5	Entrada 6	Saída 1
0	0	0	0	0	0	0
1	x	x	x	x	x	1
x	1	x	x	x	x	1
x	x	1	x	x	x	1
x	x	x	1	x	x	1
x	x	x	x	1	x	1
x	x	x	x	x	1	1

Tabela verdade da avaliação OR de sete entradas

Entrada 1	Entrada 2	Entrada 3	Entrada 4	Entrada 5	Entrada 6	Entrada 7	Saída 1
0	0	0	0	0	0	0	0
1	x	x	x	x	x	x	1
x	1	x	x	x	x	x	1
x	x	1	x	x	x	x	1
x	x	x	1	x	x	x	1
x	x	x	x	1	x	x	1
x	x	x	x	x	1	x	1
x	x	x	x	x	x	1	1

Tabela verdade da avaliação OR de oito entradas

Entrada 1	Entrada 2	Entrada 3	Entrada 4	Entrada 5	Entrada 6	Entrada 7	Entrada 8	Saída 1
0	0	0	0	0	0	0	0	0
1	x	x	x	x	x	x	x	1
x	1	x	x	x	x	x	x	1
x	x	1	x	x	x	x	x	1
x	x	x	1	x	x	x	x	1
x	x	x	x	1	x	x	x	1
x	x	x	x	x	1	x	x	x
x	x	x	x	x	x	1	x	1
x	x	x	x	x	x	x	1	1

Instrução OR exclusiva

A saída é a OR exclusiva das condições de entrada.

Diagrama da OR exclusiva

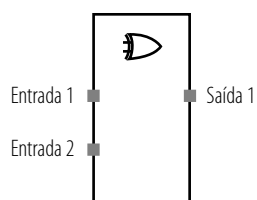


Tabela verdade da OR exclusiva

Na tabela verdade, 0 é desativado e 1, ativado.

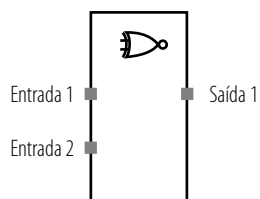
Tabela verdade da avaliação OR exclusiva

Entrada 1	Entrada 2	Saída 1
0	0	0
0	1	1
1	0	1
1	1	0

Instrução NOR exclusiva

A saída é uma NOR exclusiva das condições de entrada.

Diagrama da instrução NOR exclusiva



Tabelas verdade da instrução NOR exclusiva

Na tabela verdade, 0 é desativado e 1, ativado.

Tabela verdade da avaliação NOR exclusiva

Entrada 1	Entrada 2	Saída 1
0	0	1
0	1	0
1	0	0
1	1	1

Instrução de roteamento

A instrução de roteamento encaminha um sinal de entrada para um máximo de oito sinais de saída. Ela é usada para produzir um sinal para mais de um endereço físico como, por exemplo, um tag de saída. O número de saídas pode ser definido usando a guia I/O Setting da caixa de diálogo Function Block Properties. A configuração padrão é de um.

Diagrama da instrução de roteamento

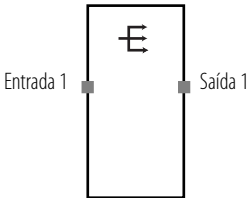


Tabela verdade da instrução de roteamento

Na tabela verdade, 0 é desativado e 1, ativado.

Tabela verdade da avaliação de roteamento

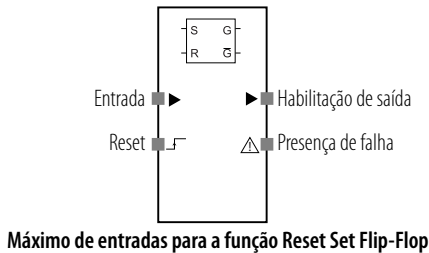
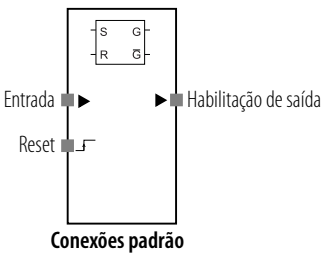
Entrada 1	Saída 1	Saída 2	Saída 3	Saída 4	Saída 5	Saída 6	Saída 7	Saída 8
0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1

Instrução de Reset Set Flip-flop (RS-FF)

Quando o sinal de entrada está ativado, o sinal habilitação de saída também está. O sinal habilitação de saída permanece ativado mesmo que os sinais de entrada estejam desativados. Quando o sinal de reset está ativado, o sinal habilitação de saída está desativado.

Também é possível usar uma saída de apresentação da falha na programação. Para habilitar essa saída opcional, marque a caixa de seleção Use Fault Present na guia I/O Settings da caixa de diálogo Function Block Properties no software RSNetWorx para DeviceNet.

Diagrama da instrução de Reset Set Flip-flop



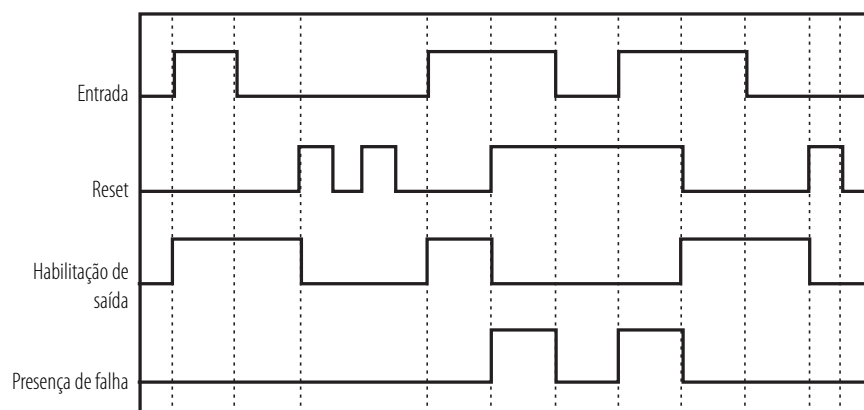
Manuseio de erro de Reset Set Flip-flop

Use a tabela para diagnosticar e reinicializar uma condição de erro de discrepância na instrução RS Flip-flop.

Deteção de erro e reset da instrução RS Flip-flop

Condição de erro	Status quando ocorre um erro		Para reinicializar a condição de erro
	Habilitação de saída	Presença de falha	
Entrada e reset são ativados simultaneamente	OFF (estado de segurança)	ON	Desative um dos sinais.

Gráfico de temporização da instrução Flip-flop



Instrução de vários conectores

A instrução de vários conectores converte sinais de entrada de até oito entradas para sinais de saída de até oito saídas. Os sinais de entrada e de saída são associações individuais para sinais de um a oito. O status dos demais sinais de entrada não tem efeito.

O número de entradas e saídas pode ser aumentado para oito na guia I/O Settings da caixa de diálogo Function Block Properties no software RSNetWorx para DeviceNet. A configuração padrão é de um.

Diagrama da instrução de vários conectores

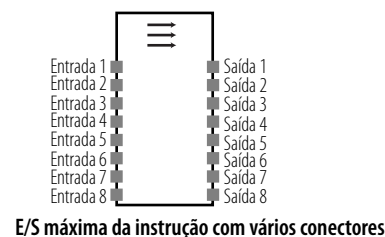
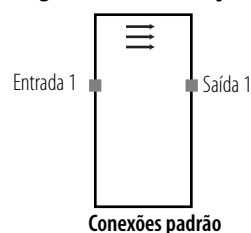


Tabela verdade da instrução com vários conectores

Na tabela verdade, 0 é desativado e 1, ativado.

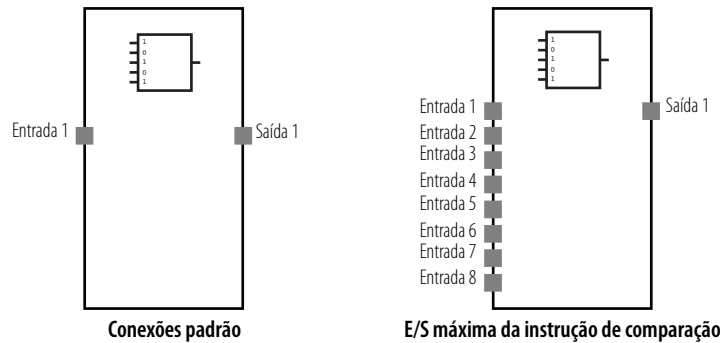
Tabela verdade da instrução com vários conectores

Entradas								Saídas							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
0	x	x	x	x	x	x	x	0	x	x	x	x	x	x	x
1	x	x	x	x	x	x	x	1	x	x	x	x	x	x	x
x	0	x	x	x	x	x	x	x	0	x	x	x	x	x	x
x	1	x	x	x	x	x	x	x	1	x	x	x	x	x	x
x	x	0	x	x	x	x	x	x	x	0	x	x	x	x	x
x	x	1	x	x	x	x	x	x	x	1	x	x	x	x	x
x	x	x	0	x	x	x	x	x	x	x	0	x	x	x	x
x	x	x	1	x	x	x	x	x	x	x	1	x	x	x	x
x	x	x	x	0	x	x	x	x	x	x	x	0	x	x	x
x	x	x	x	1	x	x	x	x	x	x	x	1	x	x	x
x	x	x	x	x	0	x	x	x	x	x	x	x	0	x	x
x	x	x	x	x	1	x	x	x	x	x	x	x	1	x	x
x	x	x	x	x	x	0	x	x	x	x	x	x	x	0	x
x	x	x	x	x	x	1	x	x	x	x	x	x	x	1	x
x	x	x	x	x	x	x	0	x	x	x	x	x	x	x	0
x	x	x	x	x	x	x	1	x	x	x	x	x	x	x	1

Instrução de comparação

A instrução de comparação compara os sinais de entrada especificados de até oito entradas com o padrão de comparação configurado e ativa o sinal de saída 1 quando todos os sinais de entrada correspondem ao padrão de comparação. O sinal de saída 1 é desativado quando os sinais de entrada deixam de corresponder ao valor de comparação.

Diagrama da instrução de comparação



Parâmetros da instrução de comparação

Defina estes parâmetros para a instrução de comparação.

Parâmetros do bloco de funções de comparação

Parâmetro	Faixa válida	Configuração padrão
Valor de comparação	00000000 a 11111111 (bit 7 a 0)	00000001

É possível definir o padrão de comparação e aumentar o número de entradas de uma para oito na guia In/Out Setting da caixa de diálogo Function Block Properties do software RSNetWorx para DeviceNet. O padrão é de uma entrada. Você define o padrão de comparação usando uma combinação de 0 (entrada desativada), 1 (entrada ativada) e X (entrada ativada ou desativada).

Tabela verdade da instrução de comparação

Na tabela verdade, 0 é desativado e 1, ativado. CV é o valor de comparação.
X indica que o status da entrada (correspondente ou não) não é aplicável.

Tabela verdade da instrução de comparação

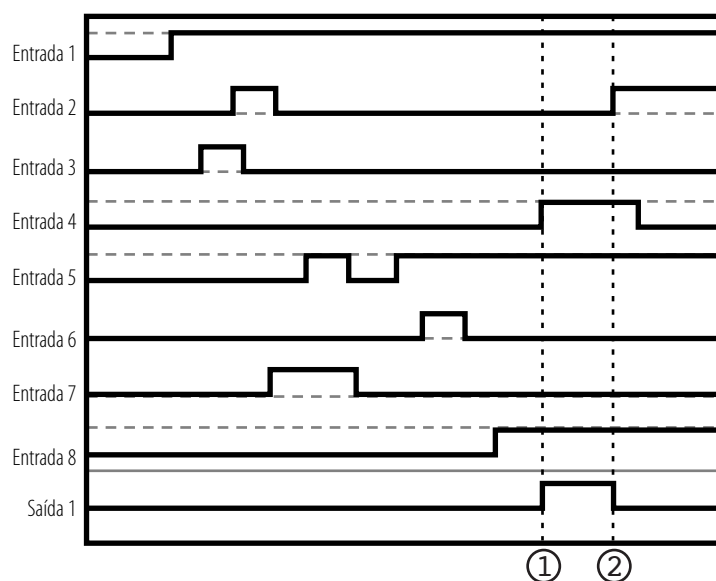
Entrada 8	Entrada 7	Entrada 6	Entrada 5	Entrada 4	Entrada 3	Entrada 2	Entrada 1	Saída 1
≠VC para bit 7	X	X	X	X	X	X	X	0
X	≠VC para bit 6	X	X	X	X	X	X	0
X	X	≠VC para bit 5	X	X	X	X	X	0
X	X	X	≠VC para bit 4	X	X	X	X	0
X	X	X	X	≠VC para bit 3	X	X	X	0
X	X	X	X	X	≠VC para bit 2	X	X	0
X	X	X	X	X	X	≠VC para bit 1	X	0
X	X	X	X	X	X	X	≠VC para bit 0	0
= VC para bit 7	= VC para bit 6	= VC para bit 5	= VC para bit 4	= VC para bit 3	= VC para bit 2	= VC para bit 1	= VC para bit 0	1

Gráfico de temporização da instrução de comparação

As linhas horizontais pontilhadas no gráfico representam os valores de comparação (VC) de cada entrada.

1. A saída 1 é ativada quando todos os sinais de entrada correspondem ao valor de comparação.
2. A saída 1 é desativada quando um dos sinais de entrada não correspondem ao valor de comparação.

Gráfico de temporização da comparação



Observações:

Referência de comandos dos blocos de funções

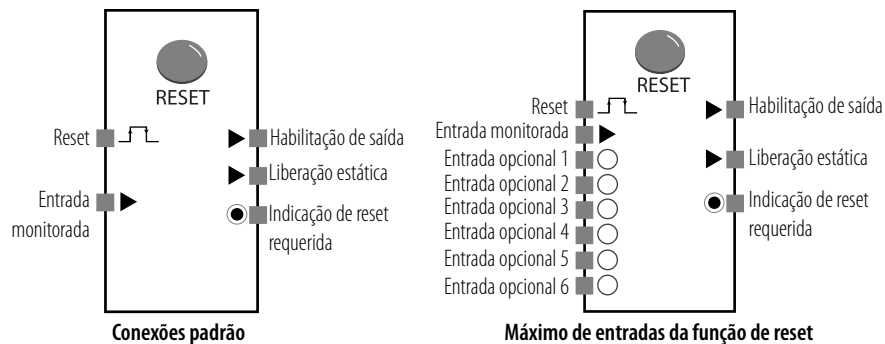
Introdução

Este apêndice descreve os blocos de funções usados na programação.

Tópico	Página
Bloco de funções de reset	227
Bloco de funções de reinicialização	229
Parada de emergência (ESTOP)	231
Bloco de funções da cortina de luz (LC)	234
Bloco de funções de monitoração do gate de segurança	237
Bloco de funções de controle bidirecional	242
Bloco de funções do temporizador com atraso na desenergização	245
Bloco de funções do temporizador com atraso na energização	245
Bloco de funções da chave no modo do usuário	246
Monitoração de dispositivo externo (EDM)	248
Muting	250
Chave de habilitação	266
Gerador de pulso	269
Contador	270

Bloco de funções de reset

Diagrama de blocos de funções de reset



O número de entradas pode ser aumentado de duas para oito na guia I/O Settings da caixa de diálogo Function Block Properties no software RSNetWorx para DeviceNet. O número padrão de entradas é de duas.

O sinal de habilitação de saída é ativado caso o sinal de reset seja recebido corretamente enquanto a condição de entrada monitorada com o bloco de funções de reset está ativada. O bloco de funções pode ser usado para impedir que a máquina seja reiniciada automaticamente quando a alimentação para o controlador é ativada, quando o modo em operação é alterado do modo inativo para o modo de operação ou quando um sinal de um dispositivo de entrada de segurança é ativado.

A liberação estática e a indicação de reset requerida são saídas opcionais. Para habilitar uma dessas saídas, marque a caixa de seleção na guia Out point da caixa de diálogo Function Block Properties.

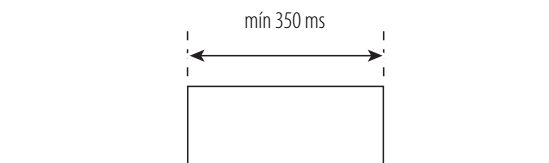
Condições de ativação das saídas

Saída	Condição de ativação
Habilitação de saída	A entrada monitorada e todas as entradas opcionais habilitadas devem estar em ON, e o sinal de reset deve ser recebido corretamente.
Liberação estática	A entrada monitorada e todas as entradas opcionais habilitadas devem estar em ON.
Indicação de reset requerida	A indicação de reset requerida se torna uma saída de pulso em 1 Hz caso a entrada monitorada e todas as entradas opcionais habilitadas estejam em ON e o sinal de habilitação de saída esteja em OFF. A indicação de reset requerida só permanece em ON quando o sinal de reset está em ON.

Parâmetros do bloco de funções de reset

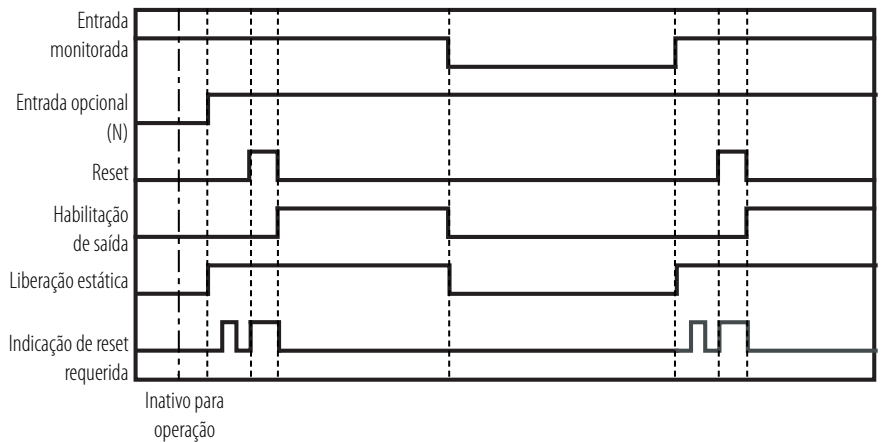
É possível definir o sinal de reset como Low-High-Low (baixo-alto-baixo) ou Rising Edge (borda ascendente) usando a guia Parameter da caixa de diálogo Function Block Properties. A configuração padrão é Low-High-Low.

Quando configurado para Low-High-Low, o sinal de reset deve atender às seguintes condições.

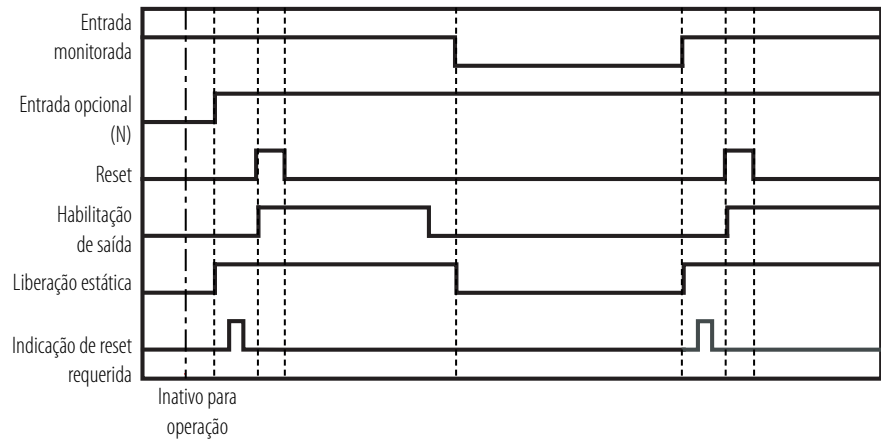


Gráficos de temporização do bloco de funções de reset

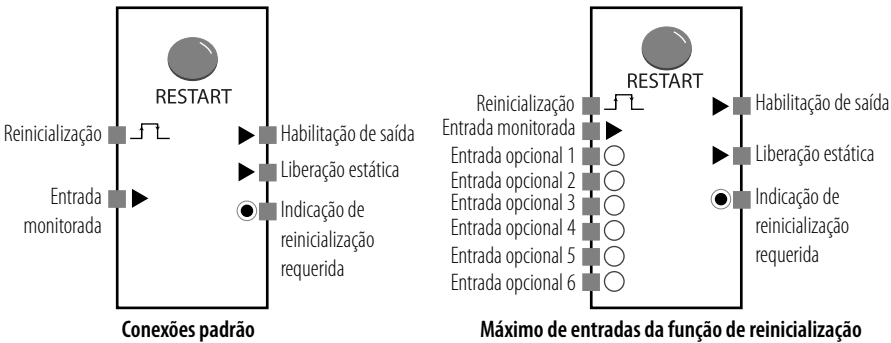
Sinal de reset baixo-alto-baixo



Sinal de reset de borda ascendente



Bloco de funções de reinicialização Diagrama de blocos de funções de reinicialização



O número de entradas pode ser aumentado de duas para oito na guia I/O Settings da caixa de diálogo Function Block Properties no software RSNetWorx para DeviceNet. O número padrão de entradas é de duas.

O sinal de habilitação de saída é ativado caso o sinal de reinicialização seja recebido corretamente enquanto a condição de entrada monitorada com o bloco de funções de reinicialização está ativada. O bloco de funções pode ser usado para impedir que a máquina seja reiniciada automaticamente quando a alimentação para o controlador é ativada, quando o modo em operação é alterado ou quando um sinal de um dispositivo de entrada de segurança é ativado. Reset e reinicialização são funcionalmente idênticos.

A Liberação estática e a indicação de Reinicialização requerida são saídas opcionais. Para habilitar uma dessas saídas, marque a caixa de seleção na guia Out point da caixa de diálogo Function Block Properties.

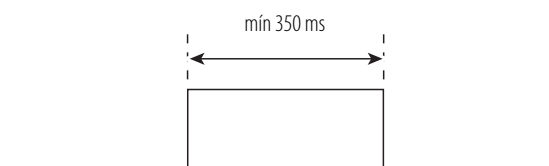
Condições de ativação das saídas

Saída	Condição de ativação
Habilitação de saída	A entrada monitorada e todas as entradas opcionais habilitadas devem estar em ON, e o sinal de reinicialização deve ser recebido corretamente.
Liberação estática	A entrada monitorada e todas as entradas opcionais habilitadas devem estar em ON.
Indicação de reinicialização requerida	A indicação de reinicialização requerida se torna uma saída de pulso em 1 Hz caso a entrada monitorada e todas as entradas opcionais habilitadas estejam em ON e o sinal de habilitação de saída esteja em OFF. A indicação de reinicialização requerida só permanece em ON quando o sinal de reinicialização está em ON.

Reinicie os parâmetros do bloco de funções

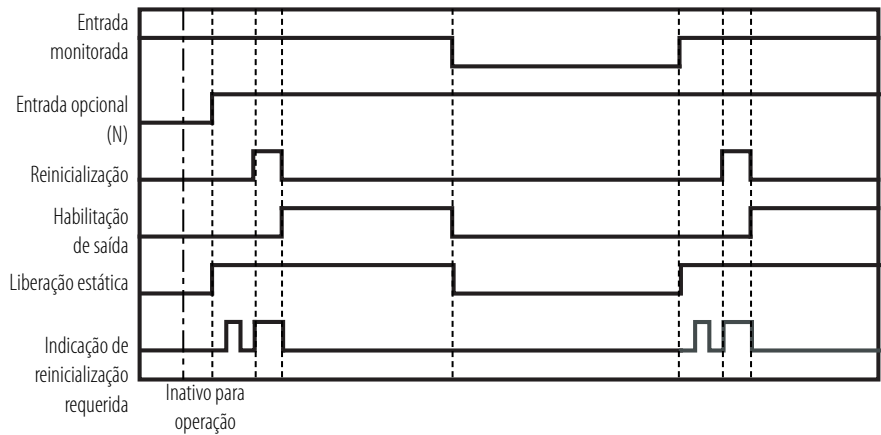
É possível definir o sinal de reinicialização para Low-High-Low (baixo-alto-baixo) ou Rising Edge (borda ascendente) na guia Parameter da caixa de diálogo Function Block Properties. A configuração padrão é Low-High-Low.

Quando configurado para Low-High-Low, o sinal de reinicialização deve atender às seguintes condições.

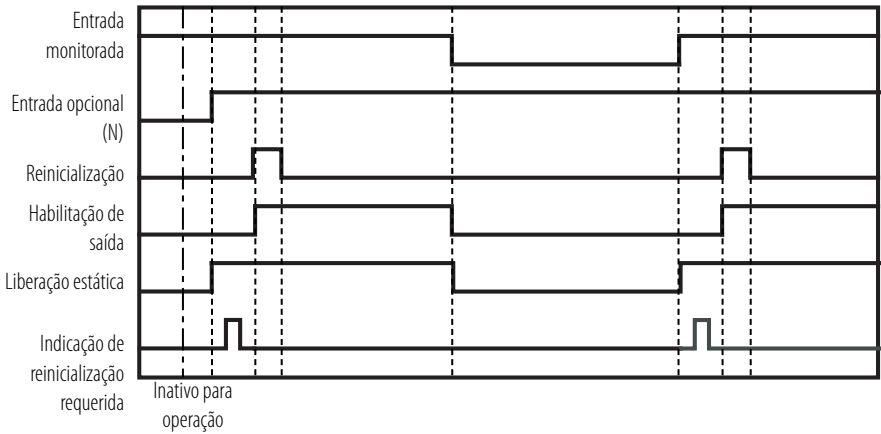


Gráficos de temporização do bloco de funções de reinicialização

Sinal de reinicialização baixo-alto-baixo

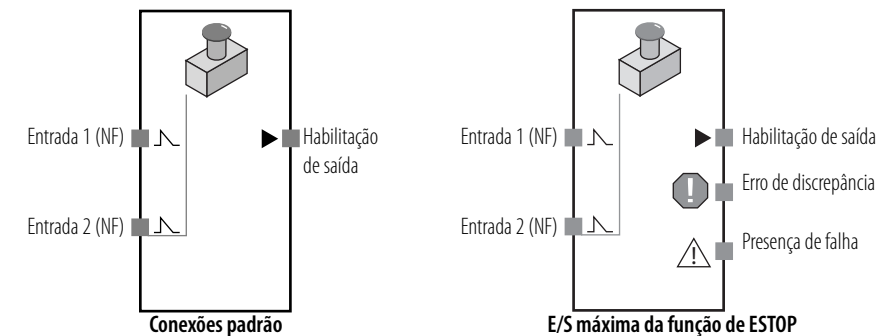


Sinal de reinicialização de borda ascendente



Parada de emergência (ESTOP)

Diagrama de blocos de funções ESTOP



A função de monitoração do botão pulsador de parada de emergência permite que você monitore uma chave do botão pulsador de parada de emergência. O sinal de habilitação de saída é ativado caso as entradas do botão pulsador de emergência que está sendo monitorado estejam ativas. A habilitação de saída é desativada caso as entradas se tornem inativas ou caso um erro seja detectado no bloco de funções.

IMPORTANTE

Uma função de reset manual é requerida em aplicações de parada de emergência. Ao usar o bloco de funções do botão pulsador de parada de emergência, você também deve usar o bloco de funções de reset.

A saída do erro de discrepância pode ser usada durante a programação do bloco de funções ESTOP. Para exibir essa saída opcional, marque a caixa de seleção Discrepancy Error na guia Out point da caixa de diálogo Function Block Properties no Logic Editor do software RSNetWorx para DeviceNet.

Também é possível usar uma saída de apresentação da falha na programação. Para habilitar essa saída opcional, marque a caixa de seleção Fault Present na guia Out point da caixa de diálogo Function Block Properties.

Parâmetros do bloco de funções ESTOP

Defina estes parâmetros para o bloco de funções ESTOP.

Parâmetros do bloco de funções ESTOP

Parâmetro	Faixa válida	Configuração padrão
Tipo de entrada	Canal único, equivalente a canal duplo canal duplo complementar	Equivalente a canal duplo
Tempo de discrepância	0 a 30 s em incrementos de 10 ms. ⁽¹⁾ O tempo de discrepância deve corresponder a ou ser maior que o tempo de ciclo do controlador.	30 ms

⁽¹⁾ Uma verificação do tempo de discrepância não é realizada quando o tempo de discrepância é definido como 0.

Tabelas verdade do bloco de funções ESTOP

Na tabela verdade, 0 é desativado e 1, ativado.

Tabela verdade do bloco de funções ESTOP

Canal único		Equivalente a canal duplo			Canal duplo complementar		
Entrada 1 (NF)	Habilitação de saída	Entrada 1 (NF)	Entrada 2 (NF)	Habilitação de saída	Entrada 1 (NF)	Entrada 2 (NA)	Habilitação de saída
0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	0
--	--	1	0	0	1	0	1
--	--	1	1	1	1	1	0

Manuseio de erro do bloco de funções ESTOP

Um erro de discrepância é gerado quando uma das entradas não permanece em seu estado correto por mais do que o tempo de discrepância. Por exemplo, no modo Equivalente a canal duplo, ambas as entradas devem estar ativas (ligadas) dentro do tempo de discrepância, ou ocorre um erro.

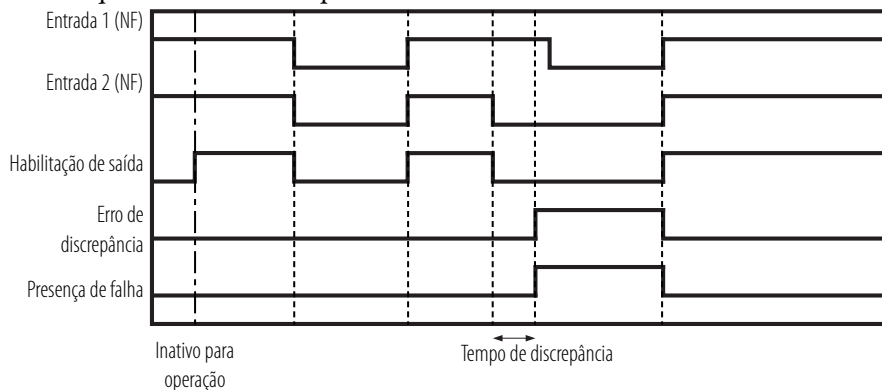
Use a tabela para diagnosticar e reinicializar uma condição de erro de discrepância no bloco de funções ESTOP.

Deteção de erro e reinicialização do bloco de funções ESTOP

Condição de erro	Status quando ocorre um erro			Para reinicializar a condição de erro
	Habilitação de saída	Presença de falha	Saída do erro	
Erro de discrepância	OFF (estado de segurança)	ON	Saída do erro de discrepância: ON	Remova a causa do erro e: 1. Ative e desative as entradas novamente. 2. Altere o modo em operação do controlador para inativo e novamente para em operação.

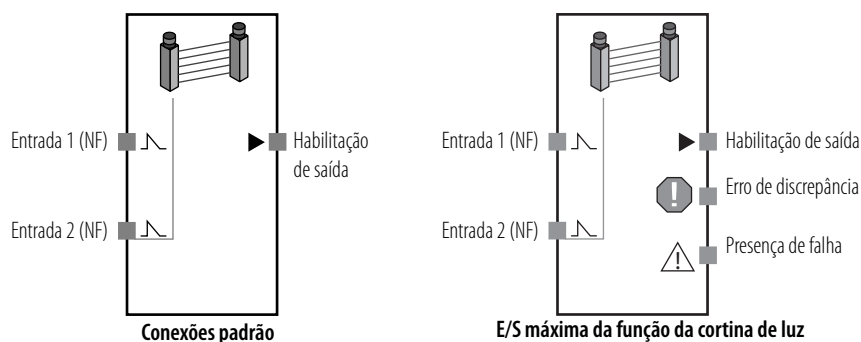
Gráfico de temporização do bloco de funções ESTOP

O gráfico mostra a temporização de E/S quando o bloco de funções está ajustado como Equivalente a canal duplo.



Bloco de funções da cortina de luz (LC)

Diagrama do bloco de funções da cortina de luz



O bloco de funções de monitoração da cortina de luz monitora uma cortina de luz de proteção do tipo 4. O sinal habilitação de saída é ativado quando as entradas da cortina de luz de proteção que está sendo monitorada estão ativas. O sinal habilitação de saída é desativado caso as entradas se tornem inativas ou caso um erro seja detectado no bloco de funções.

É possível usar uma saída do erro de discrepância durante a programação do bloco de funções LC. Para exibir essa saída de diagnóstico opcional, marque a caixa de seleção Discrepancy Error na guia Out point da caixa de diálogo Function Block Properties no Logic Editor do software RSNetWorx para DeviceNet.

Também é possível usar uma saída de apresentação da falha na programação. Para habilitar essa saída opcional, marque a caixa de seleção Fault Present na guia Out point da caixa de diálogo Function Block Properties.

Parâmetros do bloco de funções da cortina de luz

Defina estes parâmetros para o bloco de funções LC.

Parâmetros do bloco de funções LC

Parâmetro	Faixa válida	Configuração padrão
Tipo de entrada	Equivalente a canal duplo Canal duplo complementar	Equivalente a canal duplo
Tempo de discrepância	0 a 30 s em incrementos de 10 ms. ⁽¹⁾ O tempo de discrepância deve corresponder a ou ser maior que o tempo de ciclo do controlador.	30 ms

⁽¹⁾ Uma verificação do tempo de discrepância não é realizada quando o tempo de discrepância é definido como 0.

Tabelas verdade do bloco de funções da cortina de luz

Na tabela verdade, 0 é desativado e 1, ativado.

Tabela verdade do bloco de funções LC

Equivalente a canal duplo			Canal duplo complementar		
Entrada 1 (NF)	Entrada 2 (NF)	Habilitação de saída	Entrada 1 (NF)	Entrada 2 (NF)	Habilitação de saída
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	1
1	1	1	1	1	0

Manuseio do bloco de funções da cortina de luz

Um erro de discrepância é gerado quando uma das entradas não permanece em seu estado correto por mais do que o tempo de discrepância. Por exemplo, no modo Equivalente a canal duplo, ambas as entradas devem estar ativas (ligadas) dentro do tempo de discrepância, ou ocorre um erro.

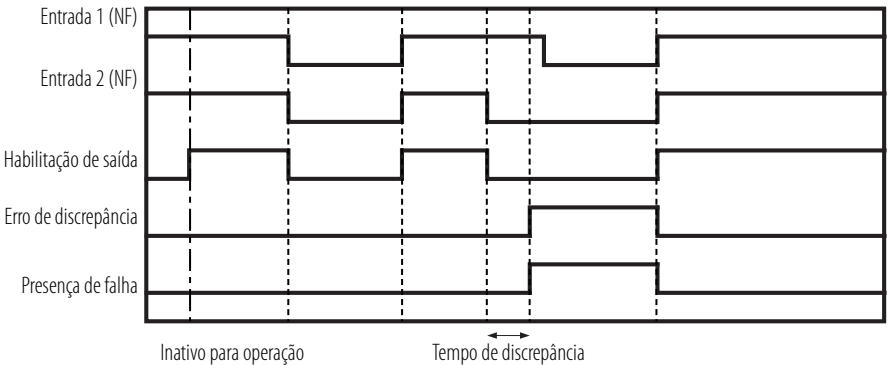
Use a tabela para diagnosticar e reinicializar uma condição de erro de discrepância no bloco de funções LC.

Detecção de erro e reinicialização do bloco de funções LC

Condição de erro	Status quando ocorre um erro			Para reinicializar a condição de erro
	Habilitação de saída	Presença de falha	Saída do erro	
Erro de discrepância	OFF (estado de segurança)	ON	Saída do erro de discrepância: ON	Remova a causa do erro e: 1. Desative e ative as entradas novamente. 2. Altere o modo em operação do controlador para inativo e novamente para em operação.

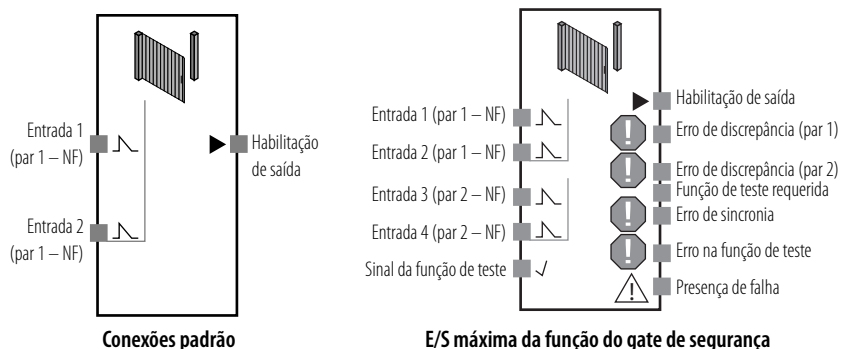
Gráfico de temporização do bloco de funções da cortina de luz

O gráfico mostra a temporização de E/S quando o bloco de funções está ajustado como Equivalente a canal duplo.



Bloco de funções de monitoração do gate de segurança

Diagrama do bloco de funções de monitoração do gate de segurança



A função de monitoração do gate de segurança monitora o status de um gate de segurança usando sinais de entrada de uma chave de porta de segurança ou uma chave fim de curso de segurança conectada à porta. O sinal habilitação de saída é ativado caso as entradas da chave que está sendo monitorada estejam ativas. O sinal habilitação de saída é desativado caso as entradas se tornem inativas ou caso um erro seja detectado no bloco de funções.

Saídas opcionais do bloco de funções de monitoração do gate de segurança

As saídas opcionais também podem ser usadas na programação. Para exibir essas saídas opcionais, marque a caixa de seleção apropriada na guia Out point da caixa de diálogo Function Block Properties no Logic Editor do software RSNetWorx para DeviceNet.

- Erro de discrepância no par 1
- Erro de discrepância no par 2
- Sinal da função de teste requerida
- Erro de sincronia
- Erro na função de teste

Ajuste de parâmetro de saída de apresentação da falha no bloco de funções de monitoração do gate de segurança

Também é possível usar a saída de apresentação da falha na programação. Para habilitar essa saída, marque a caixa de seleção Fault Present na guia Out point da caixa de diálogo Function Block Properties.

Testes de função do bloco de funções de monitoração do gate de segurança

Em algumas aplicações do gate de segurança como, por exemplo, de categoria 2, os equipamentos de proteção e segurança exigem a verificação física para que o gate continue operando corretamente.

Caso o teste de função esteja habilitado para o bloco de funções de monitoração do gate de segurança, um teste do gate de segurança, em que ele deve ser aberto e fechado fisicamente, pode ser adicionado como sendo uma condição para a ativação do sinal habilitação de saída.

Caso esteja habilitado, o teste do gate de segurança deve ser executado sob as seguintes condições:

- Partida – o teste do gate de segurança deve ser executado quando a partida é dada no controlador, ou seja, quando o modo em operação muda de inativo para em operação. Caso o teste seja concluído normalmente, o sinal habilitação de saída é ativado.
- Solicitação de teste de função a partir da máquina – o teste do gate de segurança deve ser executado depois que o controlador detectar o sinal de teste de função da máquina, ativar e antes do sinal de teste de função ser ativado novamente. Caso o sinal de teste de função seja ativado uma segunda vez antes do gate de teste de segurança ser concluído normalmente, ocorre um erro de teste de função, o sinal habilitação de saída é desativado e o sinal de erro de teste de função é ativado.
- Erro detectado no bloco de funções de monitoração do gate de segurança – caso ocorra um erro de teste de função, um erro de discrepância ou outro erro no bloco de funções, o teste do gate de segurança deve ser executado depois que a causa do erro for removida.

O sinal requerido do teste de função no bloco de funções de monitoração do gate de segurança é ativado quando um teste do gate de segurança é requerido. Ele permanece ativado até que o teste do gate de segurança tenha sido concluído normalmente.

Parâmetros do bloco de funções de monitoração do gate de segurança

Defina estes parâmetros para o bloco de funções de monitoração do gate de segurança.

Parâmetros do bloco de funções de monitoração do gate de segurança

Parâmetros	Faixa	Padrão
Tipo de entrada	Canal único Equivalente a canal duplo (1 par) Canal duplo complementar (1 par) Dois equivalentes a canal duplo (2 pares) Dois canais duplos complementares (2 pares)	Equivalente a canal duplo
Teste de função	Sem função de teste/função de teste requerida	Sem função de teste
Par 1 do tempo de discrepância	0 a 30 s em incrementos de 10 ms Uma verificação do tempo de discrepância não é realizada caso 0 esteja definido.	30 ms
Par 2 do tempo de discrepância		
Tempo de sincronia	0 a 30 s em incrementos de 10 ms Uma verificação do tempo de sincronização não é realizada caso 0 esteja definido.	300 ms

Tabelas verdade do bloco de funções de monitoração do gate de segurança

Nas tabelas verdade, 0 é desativado e 1, ativado.

Tabela verdade do bloco de funções de monitoração do gate de segurança com canal único e canal duplo (1 par)

Canal único		Equivalente a canal duplo			Canal duplo complementar		
Entrada 1 (NF)	Habilitação de saída	Entrada 1 (NF)	Entrada 2 (NF)	Habilitação de saída	Entrada 1 (NF)	Entrada 2 (NF)	Habilitação de saída
0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	0
--	--	1	0	0	1	0	1
--	--	1	1	1	1	1	0

Tabela verdade do bloco de funções de monitoração do gate de segurança com canal duplo (2 pares)

Equivalente a canal duplo (2 pares)					Canal duplo complementar (2 pares)				
Entrada 1 (NF)	Entrada 2 (NF)	Entrada 3 (NF)	Entrada 4 (NF)	Habilitação de saída	Entrada 1 (NF)	Entrada 2 (NF)	Entrada 3 (NF)	Entrada 4 (NF)	Habilitação de saída
0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	1	0
0	0	1	0	0	0	0	1	0	0
0	0	1	1	0	0	0	1	1	0
0	1	0	0	0	0	1	0	0	0
0	1	0	1	0	0	1	0	1	0
0	1	1	0	0	0	1	1	0	0
0	1	1	1	0	0	1	1	1	0
1	0	0	0	0	1	0	0	0	0
1	0	0	1	0	1	0	0	1	0
1	0	1	0	0	1	0	1	0	1
1	0	1	1	0	1	0	1	1	0
1	1	0	0	0	1	1	0	0	0
1	1	0	1	0	1	1	0	1	0
1	1	1	0	0	1	1	1	0	0
1	1	1	1	1	1	1	1	1	0

Manuseio de erro do bloco de funções de monitoração do gate de segurança

Um erro de discrepância é gerado quando uma das entradas não permanece em seu estado correto por mais do que o tempo de discrepância. Por exemplo, no modo Equivalente a canal duplo, ambas as entradas devem estar ativas (ligadas) dentro do tempo de discrepância, ou ocorre um erro.

Caso dois pares de entradas sejam selecionados e um tempo de sincronia seja inserido, ambos os pares devem estar no mesmo estado dentro do tempo de sincronia, ou ocorre um erro de sincronia. O tempo de discrepância aplica-se a ambas as entradas do mesmo par no mesmo estado dentro de um determinado tempo, ao passo que o tempo de sincronia aplica-se a ambos os conjuntos de pares de entrada no mesmo estado dentro de um determinado tempo.

Use a tabela para diagnosticar e reinicializar uma condição de erro de discrepância no bloco de funções de monitoração do gate de segurança.

Detecção de erro e reset para o bloco de funções de monitoração do gate de segurança

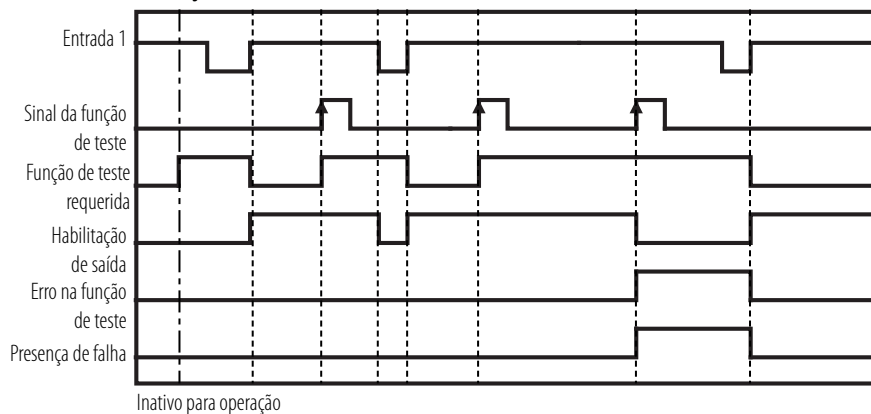
Condição de erro	Status quando ocorre um erro			Para reinicializar a condição de erro	
	Habilitação de saída	Presença de falha	Saída do erro	Quando o teste de função está desabilitado	Quando o teste de função está habilitado
Erro de discrepância no par 1	OFF (estado de segurança)	ON	Erro de discrepância no par 1: ON	Remova a causa do erro e: 1. Ative e desative as entradas novamente. ⁽²⁾ 2. Altere o modo em operação do controlador para inativo e novamente para em operação.	Remova a causa do erro e ative as entradas e desative novamente (ou seja, realize o teste do gate de segurança).
Discrepância no par 2			Erro de discrepância no par 2: ON		
Erro na função de teste ⁽¹⁾			Erro na função de teste: ON		
Erro de sincronia			Erro de teste de sincronia: ON		

⁽¹⁾ O teste do gate de segurança não foi realizado normalmente entre os sinais de teste de função.

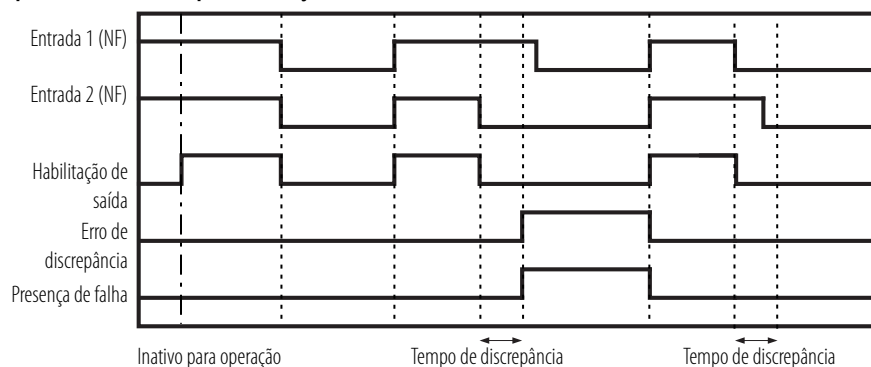
⁽²⁾ Caso ocorra um erro de discrepância em um dos pares quando definido para equivalente a canal duplo (2 pares) ou canal duplo complementar (2 pares), desative os pares de entrada 1 e 2 e, em seguida, ative-os.

Gráficos de temporização do bloco de funções de monitoração do gate de segurança

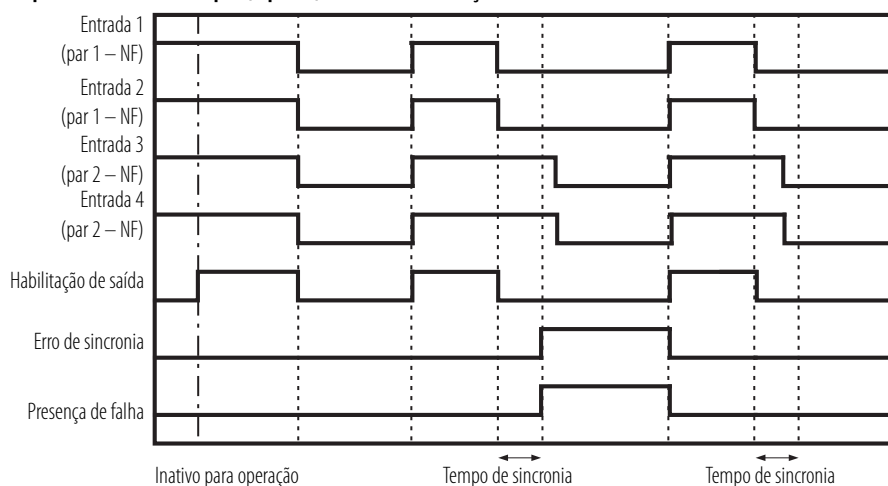
Canal único com a função de teste habilitada



Equivalente a canal duplo com função de teste desabilitada

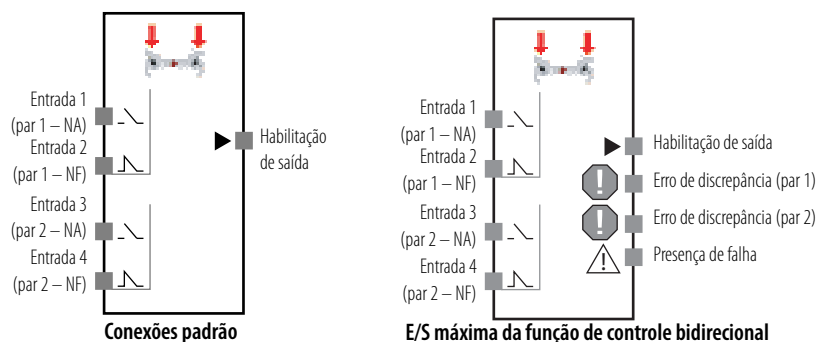


Equivalente a canal duplo (2 pares) com teste de função desabilitado



Bloco de funções de controle bidirecional

Diagramas de blocos de funções de controle bidirecional



O bloco de funções de controle bidirecional permite a monitoração do status de uma chave bidirecional. O bloco de funções de controle bidirecional pode ser usado com uma chave bidirecional apropriada para atender às especificações do tipo III C em EN 574, Dispositivos de controle bidirecional, aspecto funcional – princípio do projeto.

O sinal de saída só é ativado caso ambas as entradas da chave bidirecional estejam ativas e atendam às especificações da EN 574. O sinal habilitação de saída é desativado caso as entradas da chave bidirecional não atendam às especificações da EN 574, uma entrada esteja inativa ou caso um erro seja detectado no bloco de funções.

Saídas opcionais do bloco de funções de controle bidirecional

As saídas opcionais também podem ser usadas na programação. Para exibir essas saídas opcionais, marque a caixa de seleção apropriada na guia Out point da caixa de diálogo Function Block Properties no Logic Editor do software RSNetWorx para DeviceNet.

- Erro de discrepância no par 1
- Erro de discrepância no par 2

Ajuste de parâmetro de saída de apresentação da falha no bloco de funções de controle bidirecional

Também é possível usar a saída de apresentação da falha na programação. Para habilitar essa saída, marque a caixa de seleção Fault Present na guia Out point da caixa de diálogo Function Block Properties.

Parâmetros de blocos de funções de controle bidirecional

Defina estes parâmetros para o bloco de funções do controle bidirecional.

Parâmetros de blocos de funções de controle bidirecional

Parâmetro	Faixa	Padrão
Par 1 de entrada do tempo de discrepância	0 a 500 ms em incrementos de 10 ms ⁽¹⁾ Os tempos de discrepância devem ser iguais ou maiores que o tempo de ciclo do controlador.	30 ms
Par 2 de entrada do tempo de discrepância		

⁽¹⁾ Uma verificação do tempo de discrepância não é realizada caso 0 esteja definido.

Tabela verdade de blocos de funções de controle bidirecional

Na tabela verdade, 0 é desativado e 1, ativado.

Tabela verdade de blocos de funções de controle bidirecional

Entrada 1 (par 1 – NA)	Entrada 2 (par 1 – NF)	Entrada 3 (par 2 – NA)	Entrada 4 (par 2 – NF)	Habilitação de saída
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Manuseio de erro do bloco de funções de controle bidirecional

Um erro de discrepância é gerado quando uma das entradas não permanece em seu estado correto por mais do que o tempo de discrepância. Por exemplo, no modo Equivalente a canal duplo, ambas as entradas devem estar ativas (ligadas) dentro do tempo de discrepância, ou ocorre um erro.

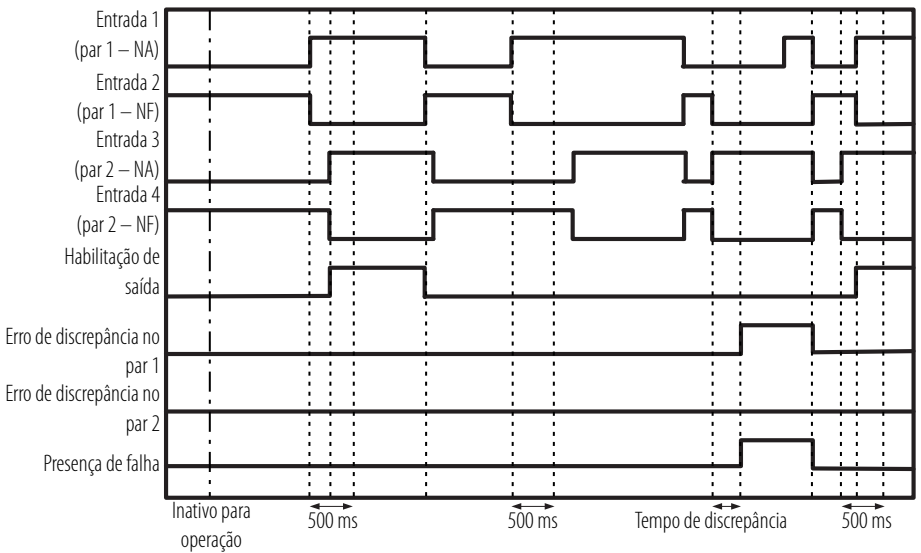
Use a tabela para diagnosticar e reinicializar uma condição de erro de discrepância no bloco de funções do controle bidirecional.

Deteção de erro e reset para o bloco de funções do controle bidirecional

Condição de erro	Status quando ocorre um erro			Para reinicializar a condição de erro
	Habilitação de saída ⁽¹⁾	Presença de falha	Saída do erro	
Erro de discrepância no par 1	OFF (estado de segurança)	ON	Erro de discrepância no par 1: ON	Remova a causa do erro e: 1. Desative ambos os pares de entradas 1 e 2 e ative-os novamente. 2. Altere o modo em operação do controlador para inativo e novamente para em operação.
Erro de discrepância no par 2			Erro de discrepância no par 2: ON	

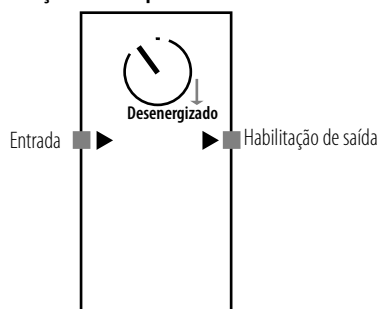
⁽¹⁾ O sinal habilitação de saída não será ativado caso a especificação do tempo de sincronia não seja atendida (ou seja, as entradas de operação de nos dois sentidos devem ser concluídas em 500 ms), embora isso não seja considerado um erro.

Gráfico de temporização de blocos de funções de controle bidirecional



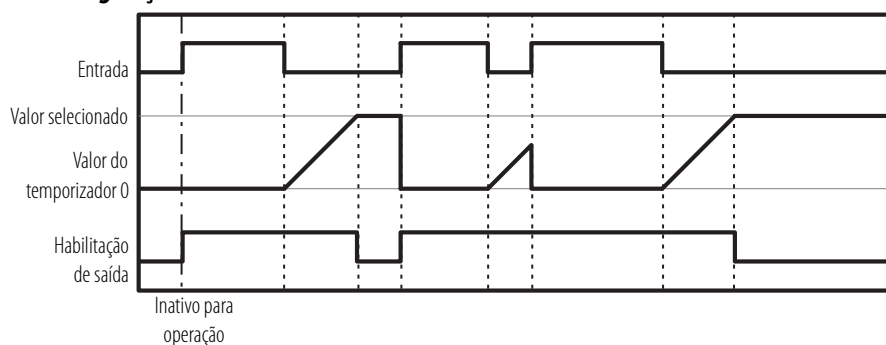
Bloco de funções do temporizador com atraso na desenergização

Diagrama do bloco de funções do temporizador com atraso na desenergização



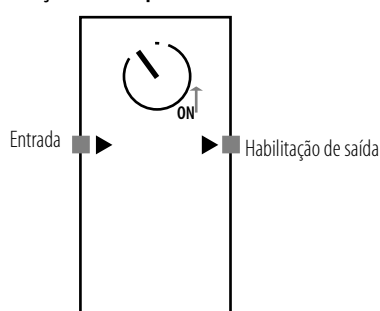
O bloco de funções do temporizador com atraso na desenergização realiza uma operação de temporizador definido em incrementos de 10 ms. A faixa de atraso varia de 0 ms a 300 segundos. O ajuste de parâmetro padrão é de 0 ms.

Gráfico de temporização do bloco de funções do temporizador com atraso na desenergização



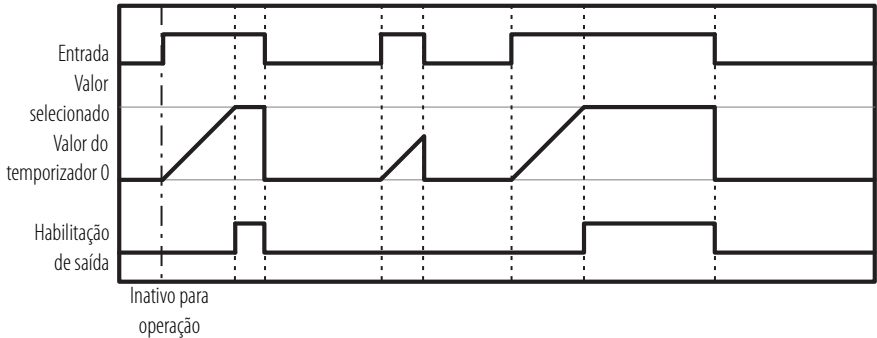
Bloco de funções do temporizador com atraso na energização

Diagrama do bloco de funções do temporizador com atraso na energização



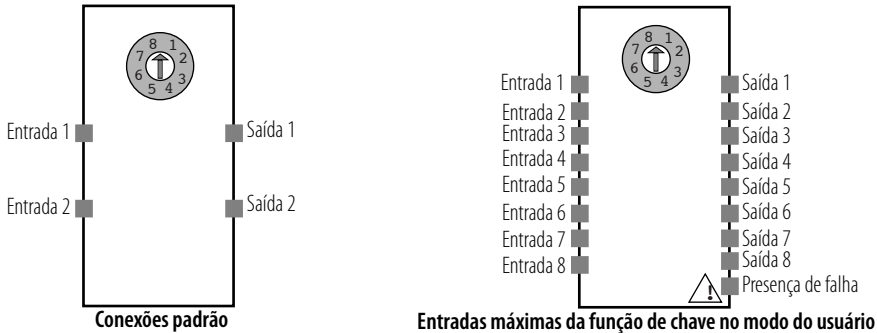
O bloco de funções do temporizador com atraso na energização realiza uma operação de temporizador definido em incrementos de 10 ms. A faixa de atraso varia de 0 ms a 300 segundos. O ajuste de parâmetro padrão é de 0 ms.

Gráfico de temporização do bloco de funções do temporizador com atraso na energização



Bloco de funções da chave no modo do usuário

Diagrama do bloco de funções da chave no modo do usuário



O bloco de funções da chave no modo do usuário é usado para monitorar uma chave em modo em operação no sistema do usuário ou equipamento. A chave em modo em operação que pode ser conectada ao bloco de funções deve ser do tipo 1-de-N, ou seja, um dos N contatos está ativado. O bloco de funções suporta um máximo de oito entradas e oito saídas correspondentes.

Saídas opcionais do bloco de funções da chave em modo de usuário

O número de E/S pode ser aumentado na guia In/Out Settings da caixa de diálogo Function Block Properties.

Defina estes parâmetros para as saídas opcionais.

Parâmetros de saída opcional da chave em modo do usuário

Parâmetro	Faixa	Padrão
Número de entradas	2 a 8	2
Número de saídas	2 a 8	2

Ajuste de parâmetro de saída de apresentação da falha no bloco de funções da chave em modo de usuário

Também é possível usar a saída de apresentação da falha na programação. Para habilitar essa saída, marque a caixa de seleção Use Fault Present na guia In/Out Settings da caixa de diálogo Function Block Properties.

Tabela verdade do bloco de funções da chave em modo de usuário

Na tabela verdade, 0 é desativado e 1, ativado.

Tabela verdade do bloco de funções da chave em modo de usuário

Entradas								Saídas							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1

Manuseio de erro do bloco de funções da chave em modo de usuário

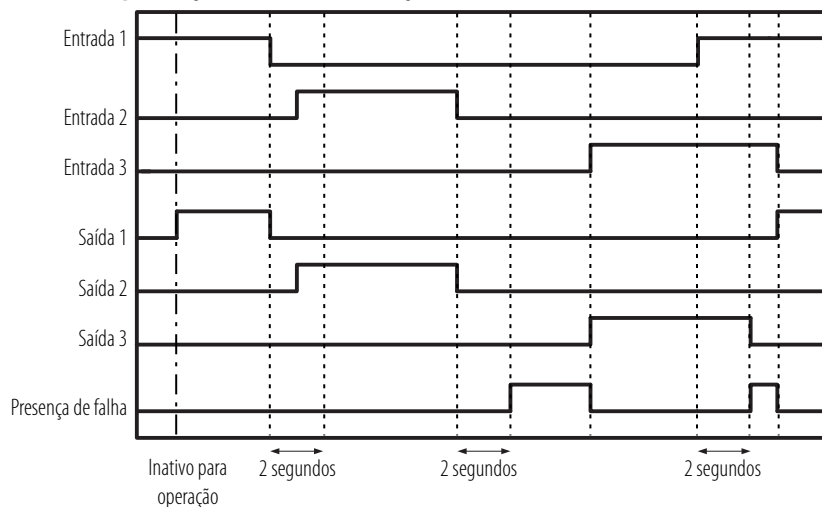
Use a tabela para diagnosticar e reinicializar uma condição de erro de discrepância no bloco de funções da chave em modo de usuário.

Deteção de erro e reset para o bloco de funções da chave em modo de usuário

Condição de erro	Status quando ocorre um erro		Para reinicializar a condição de erro
	Saída	Presença de falha	
Mais de uma entrada esteve ativada por mais de 2 segundos. ⁽¹⁾	OFF (estado de segurança)	ON	Corrija o sistema para que apenas um contato permaneça ativado.
Todas as entradas estiveram desativadas por mais de 2 segundos.			

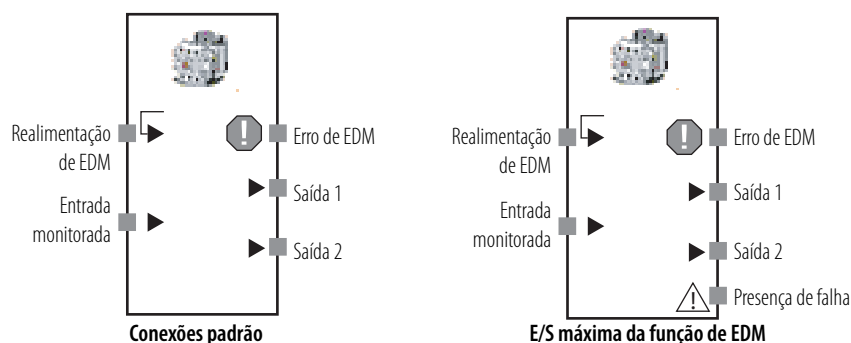
⁽¹⁾ Se mais de uma entrada estiver ativada ao mesmo tempo, a saída correspondente da primeira entrada de ativação será ativada por 2 segundos.

Gráfico de temporização do bloco de funções da chave em modo do usuário



Monitoração de dispositivo externo (EDM)

Diagrama de blocos de funções da monitoração de dispositivo externo



O bloco de funções da Monitoração de dispositivo externo (EDM) avalia o sinal saída monitorada e o status de um sinal de realimentação do equipamento externo (realimentação de EDM) e ativa as saídas de segurança para um dispositivo externo.

Caso o sinal entrada monitorada seja ativado, os sinais de saída 1 e 2 são ativados. Quando isso ocorre, o status do sinal de realimentação deve ser alterado dentro do tempo especificado. Caso o sinal entrada monitorada seja desativado, os sinais de saída 1 e 2 são desativados. Quando isso ocorre, o status do sinal de realimentação deve ser alterado dentro do tempo especificado.

Caso o status do sinal de realimentação não seja alterado dentro do tempo especificado, ocorre um erro de EDM, os sinais de saída 1 e 2 são desativados, e o sinal do erro de EDM é ativado.

Saídas opcionais do bloqueio de funções de EDM

As saídas opcionais também podem ser usadas na programação. Para usar essas saídas opcionais, marque a caixa de seleção apropriada na guia Out point da caixa de diálogo Function Block Properties no Logic Editor do software RSNetWorx para DeviceNet.

- Erro de EDM
- Saída 2

Configuração da saída de apresentação da falha no bloco de funções de EDM

Também é possível usar a saída de apresentação da falha na programação. Para habilitar essa saída, marque a caixa de seleção Use Fault Present na guia Out point da caixa de diálogo Function Block Properties.

Parâmetro do bloco de funções de EDM

Defina este parâmetro para o bloco de funções de EDM.

Parâmetro do bloco de funções de EDM

Parâmetro	Faixa	Padrão
Atraso máximo da realimentação de EDM (T_{EDM})	100 a 1000 ms em incrementos de 10 ms	300 ms

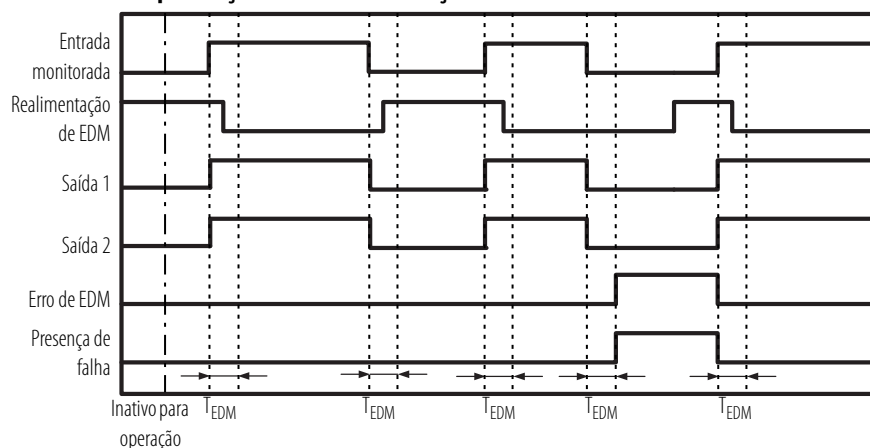
Manuseio de erro do bloco de funções EDM

Use a tabela para diagnosticar e reinicializar uma condição de erro de discrepância no bloco de funções EDM.

Deteção de erro e reinicialização do bloco de funções EDM

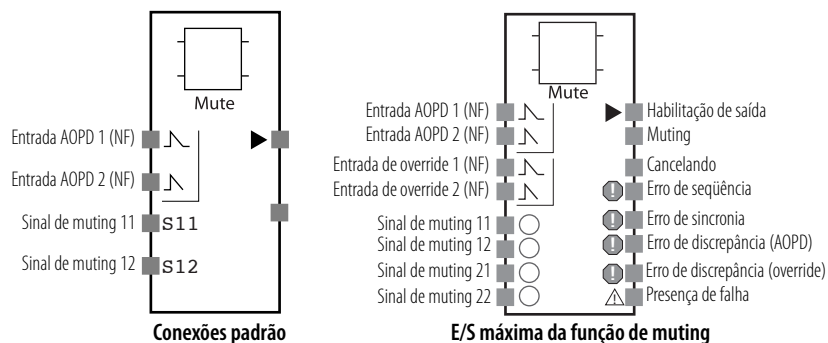
Condição de erro	Status quando ocorre um erro			Para reinicializar a condição de erro
	Habilitação de saída	Presença de falha	Saída do erro	
Erro de realimentação de EDM	OFF (estado de segurança)	ON	Saída de erro de EDM: ON	Remova a causa do erro e ative a entrada de segurança.

Gráfico de temporização do bloco de funções EDM



Muting

Diagramas de blocos de funções de muting



O bloco de funções de muting desabilita temporariamente o sinal de interrupção da luz (entrada AOPD) em uma cortina de luz enquanto o sensor de muting é disparado. Enquanto a função de muting está em operação, a máquina não é desligada, logo, um objeto pode ser removido da zona de detecção da cortina de luz. Além disso, o bloco de funções de muting tem uma função de override capaz de desabilitar o sinal de interrupção da luz da cortina e fazer com que a máquina opere enquanto a luz da cortina é obstruída. Por exemplo, quando um objeto for desligado na zona de detecção da cortina de luz, a máquina poderá ser operada para removê-lo.

Parâmetros do bloco de funções de muting

Defina estes parâmetros para o bloco de funções do controle bidirecional.

Parâmetros do bloco de funções de muting

Parâmetro	Ajuste de parâmetro/faixa	Padrão
Modo de muting	- Muting paralelo com 2 sensores O padrão é adequado às aplicações na entrada de um transportador. Use o padrão quando dois sensores fotoelétricos retrorreflexivos forem ajustados como sendo sensores de muting com zonas de detecção com interseção. - Muting sequencial (direção para frente) O padrão é adequado às aplicações na entrada de um transportador. Use o padrão quando quatro sensores fotoelétricos de feixe forem ajustados como sensores de muting. - Muting sequencial (nos dois sentidos) O padrão é adequado às aplicações na entrada ou na saída de um transportador. Use o padrão quando quatro sensores fotoelétricos de feixe forem ajustados como sensores de muting. - Deteção de posição O padrão é adequado às aplicações em que o muting é controlado por uma entrada de chave. Use o padrão para desabilitar temporariamente o sinal de interrupção de luz da cortina quando um operador está colocando um objeto na partida da máquina, e a máquina está em um estado em que ele não prejudicará o operador (perigos estão em uma zona diferente da máquina). Em todas essas explicações sobre o ajuste de parâmetro, os sensores de muting são ativados quando a detecção é realizada e desativados quando a detecção não é realizada.	Muting paralelo com 2 sensores
Tempo de sincronia ⁽¹⁾	30 ms a 3 s em incrementos de 10 ms. O SV do temporizador deve ser maior que o tempo de ciclo do controlador.	3 segundos
Tipo de entrada de AOPD	- Equivalente a canal duplo (NF/NF) - Canal duplo complementar (NF/NA)	Equivalente a canal duplo
Tempo de discrepância (AOPD)	10 a 500 ms em incrementos de 10 ms ⁽²⁾ O SV do temporizador deve ser maior que o tempo de ciclo do controlador.	30 ms
Tipo de entrada do sinal de override	- Canal único - Equivalente a canal duplo (NA/NA) - Canal duplo complementar (NF/NA) - Não usado	Não usado
Tempo de discrepância (override)	10 a 500 ms em incrementos de 10 ms ⁽²⁾ O SV do temporizador deve ser maior que o tempo de ciclo do controlador.	30 ms
Tempo de muting máximo	500 ms a 127,5 s em incrementos de 500 ms 0 a 500 ms em incrementos de 10 ms	60 segundos
Tempo de override máximo	500 ms a 127,5 s em incrementos de 500 ms	60 segundos

⁽¹⁾ Entre o sinal de muting 11 e o sinal de muting 12 ou entre o sinal de muting 21 e o sinal de muting 22.

⁽²⁾ Uma verificação do tempo de discrepância não será realizada se 0 estiver definido.

Saídas opcionais do bloqueio de funções de muting

As saídas opcionais também podem ser usadas na programação. Para usar essas saídas opcionais, marque a caixa de seleção apropriada na guia In/Out Setting da caixa de diálogo Function Block Properties no Logic Editor do software RSNetWorx para DeviceNet.

- Cancelando
- Erro de sincronia
- Erro de seqüência
- Erro de discrepância (AOPD)
- Erro de discrepância (override)

Ajuste de parâmetro de saída de apresentação da falha no bloco de funções de muting

Também é possível usar a saída de apresentação da falha na programação. Para habilitar essa saída, marque a caixa de seleção Use Fault Present na guia In/Out Setting da caixa de diálogo Function Block Properties.

Manuseio de erro do bloco de funções de muting

Use a tabela para diagnosticar e reinicializar condições de erro de reset no bloco de funções de muting.

Detecção de erro e reinicialização do bloco de funções de muting

Condição de erro	Status quando ocorre um erro			Para reinicializar a condição de erro
	Habilitação de saída	Presença de falha	Saída do erro ⁽³⁾	
Erro de sincronização (entre o sinal de muting 11 e o sinal de muting 12 ou entre o sinal de muting 21 e o sinal de muting 22) ⁽¹⁾	ON ⁽²⁾	OFF ⁽²⁾	Erro de sincronia: ON	Aplique novamente o muting ou altere o modo em operação do controlador para inativo e retorne ao modo de operação.
Erro de seqüência			Erro de seqüência ON	
Erro de discrepância (AOPD)	OFF (estado de segurança)	ON	Erro de discrepância (AOPD) ON	Reinicialize quando ambos os sinais de entrada da cortina de luz forem alterados de desativados para o status ativado ou você alterar o modo de operação do controlador para inativo e retornar ao modo de operação.
Erro de discrepância (override)			Erro de discrepância (override): ON	Reinicialize quando ambos os sinais de cancelamentos forem alterados de desativados para o status ativado ou você alterar o modo de operação do controlador para inativo e retornar ao modo de operação.

⁽¹⁾ O erro só é detectado quando o modo de muting está configurado como sendo seqüencial (nos dois sentidos).

⁽²⁾ Se a cortina de luz sair desse status de erro para inativo (sem luz), o sinal habilitação de saída será desativado e o sinal presença de falha, ativado. Se a cortina de luz for ativada (incidência de luz) ou a função de override for executada, o sinal habilitação de saída será ativado e o sinal presença de falha, desativado.

⁽³⁾ Se houver mais de um erro, os erros serão indicados em todas as saídas de erro afetadas.

Detalhes da função de muting

As condições de reset, partida e parada do bloco de funções de muting são descritas nas seguintes seções.

Condições de reset

A saída de segurança (habilitação de saída) permanece ativada quando todas as seguintes condições são atendidas:

- O sinal da cortina de luz está ativado (incidência de luz).
- Um erro de discrepância não ocorreu.

Condições de partida

Se os sensores de muting atenderem às seguintes condições enquanto o sinal habilitação de saída estiver ativado, o muting será aplicado e o sinal de muting, ativado:

- Os sensores de muting estão todos desativados.
- Enquanto os sensores de muting estão desativados, dois sensores de muting detectam um objeto na sequência correta.
- Enquanto os sensores de muting estão desativados, os tempos de sincronização dos dois sensores de muting estão dentro da faixa normal (sem incluir o ajuste de parâmetro de detecção da posição).

Caso ocorra um erro, uma saída de alarme é gerada. O sinal de erro da sequência permanece ativado caso haja uma sequência inválida. O sinal de erro da sincronia permanece ativado caso um objeto não possa ser detectado dentro do tempo de sincronia. A saída de segurança (habilitação de saída) é desativada caso o sinal da cortina de luz esteja inativo (sem luz) antes do controlador passar para o estado de muting.

Condições de parada

Caso as seguintes condições sejam atendidas enquanto muting estiver ligado, o muting é desligado, e o sinal de muting é desativado:

- Dois ou mais sensores não estão ativados.
- O tempo de muting máximo transcorreu.
- Um erro de discrepância ocorreu.

A saída de segurança (habilitação de saída) é desativada caso o muting seja desativado e a cortina de luz, obstruída.

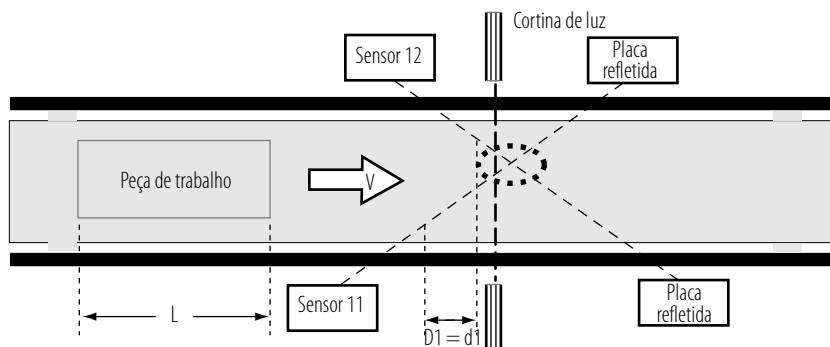
IMPORTANTE

Quando o modo operacional do controlador SmartGuard for alterado de inativo para o modo de operação, os dados de entrada dos escravos serão desativados até que a comunicação seja estabelecida. Se os dados de entrada do escravo forem usados para a entrada AOPD, as saídas presença de falha e erro de sequência serão ativadas assim que o modo em operação for alterado para o modo de operação. Quando a entrada AOPD for ativada, a saída presença de falha será desativada. Quando a condição de partida do muting for atendida, a saída erro de sequência será desativada.

Exemplo: Muting paralelo com 2 sensores

Neste exemplo, os dois sensores fotoelétricos retrorreflexivos são ajustados como sendo sensores de muting com zonas de detecção de interseção. A interseção dos dois sensores deve estar atrás da cortina de luz. Use essa configuração quando o comprimento da peça de trabalho (L) não é fixo ou extenso o bastante para ativar os sensores de muting sequenciais.

Ajuste da aplicação



O sensor 12 é conectado ao sinal de muting 12. Já o sensor 11 é conectado ao sinal de muting 11.

Sequência de muting

Neste exemplo, a sequência de muting está descrita abaixo.

1. Como a luz não é interrompida entre os sensores 11 e 12 e a cortina de luz, o sinal habilitação de saída permanece ativado.
2. À medida que a peça de trabalho move-se para a direita e os sensores 11 e 12 são ativados na ordem, o muting é habilitado.
3. À medida que a peça de trabalho continua avançando, o sinal habilitação de saída é mantido ativado, mesmo que a cortina de luz esteja obstruída.

4. À medida que a peça de trabalho continua avançando, a luz do sensor 11 deixa de ser interrompida pela peça, e o status de muting é limpo e o sinal de muting, desativado.

Ajustes de distância

Durante o ajuste desse tipo de aplicação de muting, os ajustes de distância devem impedir que uma pessoa de passagem habilite a função de muting, e os sensores da cortina de luz e do muting devem ser ajustados de forma que uma peça de trabalho passe por todos os sensores de muting antes da chegada da próxima peça aos sensores de muting.

Para calcular as distâncias de ajuste apropriadas para o exemplo, use estas fórmulas, em que:

D1 = distância mínima requerida para o desempenho do sensor de muting

d1 = distância máxima requerida para o desempenho do sensor de muting

L = comprimento da peça de trabalho

V = velocidade de trânsito da peça de trabalho

T1mín = tempo de ciclo do controlador

T1máx = ajuste do tempo de sincronia (o ajuste padrão é de 3 segundos)

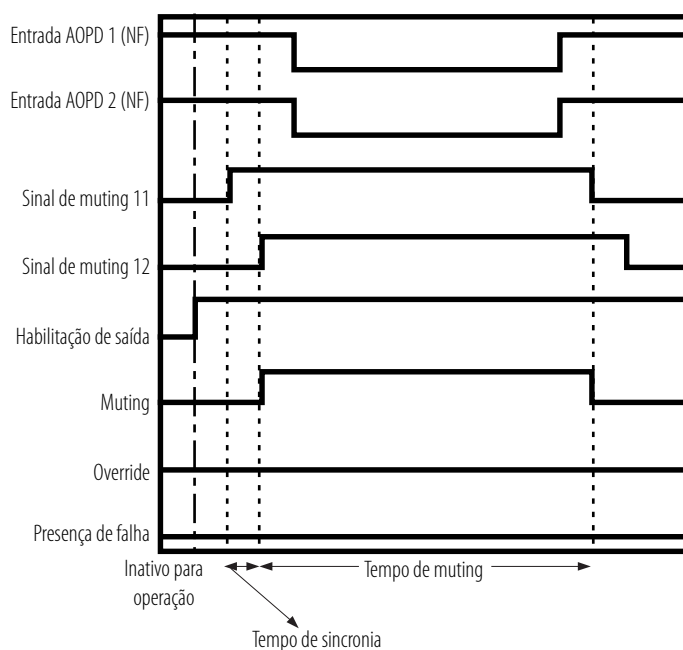
Fórmula 1: $D1 < L$

Fórmula 2: $V \times T1mín < d1 < V \times T1máx$

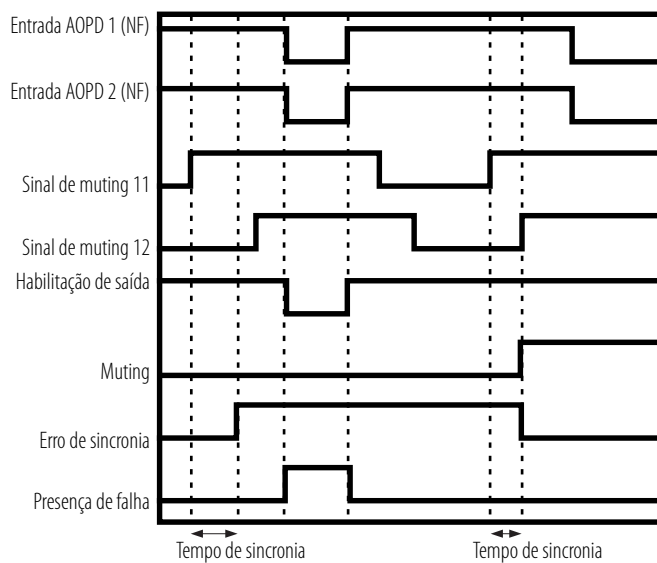
Para que a função de muting opere de maneira efetiva, ambas as fórmulas devem ser atendidas.

Gráficos de temporização do muting seqüencial (sentido para frente)

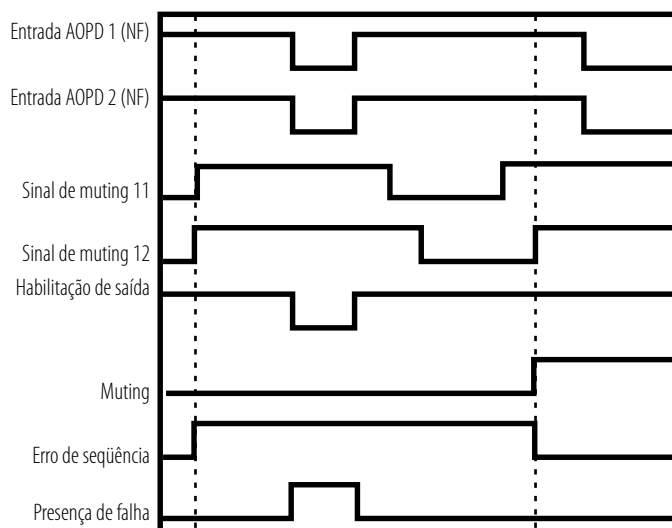
Operação normal



Erro de sincronia



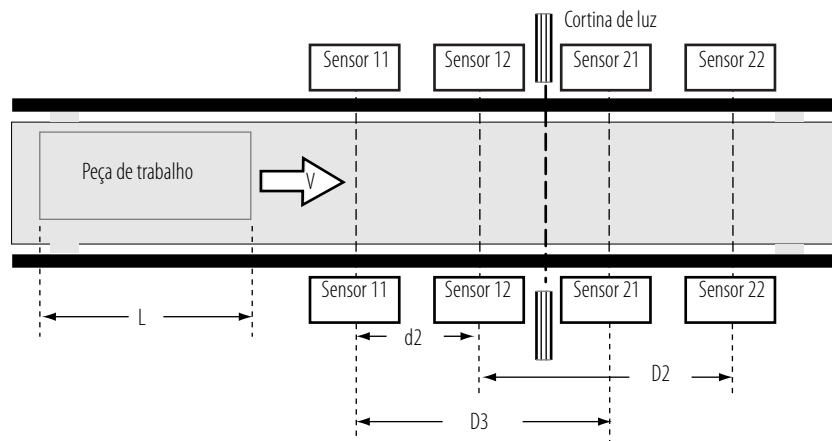
Erro de seqüência



Exemplo: muting seqüencial com 4 sensores (sentido para frente)

Neste exemplo, os quatro sensores fotoelétricos com feixe são ajustados como sendo sensores de muting com zonas de detecção de interseção. Use essa configuração quando o comprimento da peça de trabalho transportada tiver um comprimento fixo extenso o bastante para ativar os sensores de muting instalados em seqüência.

Ajuste da aplicação



O sensor 11 está conectado ao sinal de muting 11. O sensor 12, ao sinal de muting 12. Já o sensor 21 está conectado ao sinal de muting 21. O sensor 22 está conectado ao sinal de muting 22.

Seqüência de muting

A seqüência de muting do exemplo está descrita abaixo.

1. Como a luz não é interrompida entre os sensores 11, 12, 21 e 22 e a cortina de luz, o sinal habilitação de saída permanece ativado.
2. À medida que a peça de trabalho move-se para a direita e os sensores 11 e 12 são ativados na ordem, o muting é habilitado e o sinal de muting, ativado.
3. À medida que a peça de trabalho continua avançando, o sinal habilitação de saída é mantido ativado, mesmo que a cortina de luz esteja obstruída.
4. À medida que a peça de trabalho continua avançando, a luz do sensor 21 deixa de ser interrompida pela peça, e o status de muting é apagado e o sinal de muting, desativado.

Ajustes de distância

Durante o ajuste desse tipo de aplicação de muting, os ajustes de distância devem impedir que uma pessoa de passagem habilite a função de muting, e os sensores da cortina de luz e do muting devem ser ajustados de forma que uma peça de trabalho passe por todos os sensores de muting antes da chegada da próxima peça aos sensores de muting.

Para calcular as distâncias de ajuste apropriadas para o exemplo, use estas fórmulas, em que:

- D2 e D3 = distância mínima requerida para o desempenho do sensor de muting
- d2 = distância máxima requerida para o desempenho do sensor de muting
- L = comprimento da peça de trabalho
- V = velocidade de trânsito da peça de trabalho
- T1mín = tempo de ciclo do controlador
- T1máx = ajuste do tempo de sincronia (o ajuste padrão é de 3 segundos)

Fórmula 3: $D2 < L$

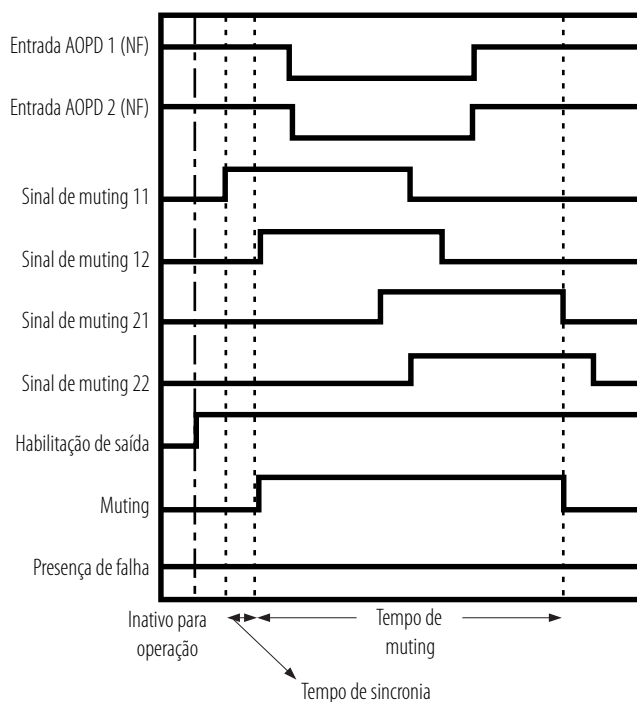
Fórmula 4: $D3 < L$

Fórmula 5: $V \times T1mín < d2 < V \times T1máx$

Para que a função de muting opere de maneira efetiva, as fórmulas 3, 4 e 5 devem ser atendidas.

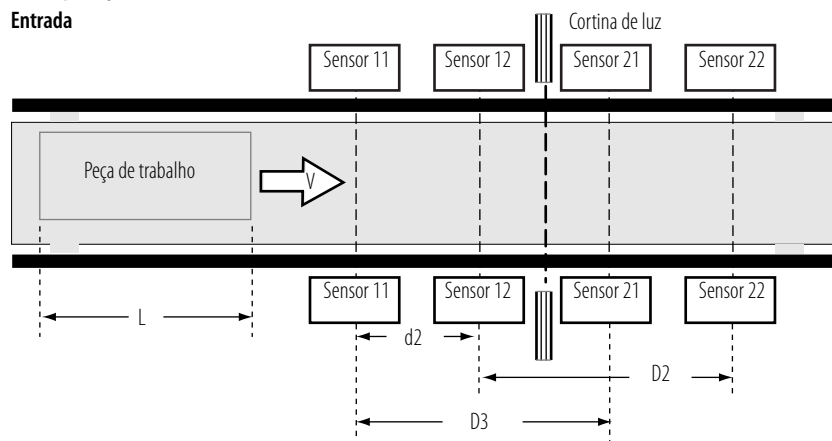
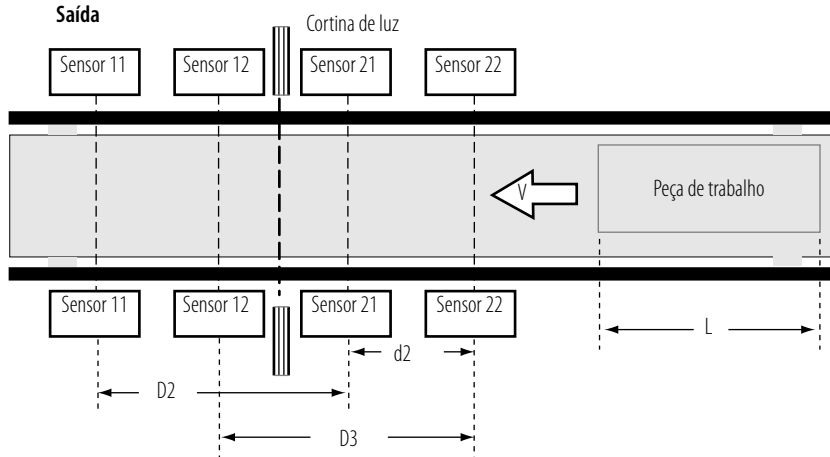
Gráfico de temporização do muting sequencial (sentido para frente)

Operação normal



Exemplo: muting sequencial com 4 sensores (nos dois sentidos)

Neste exemplo, os quatro sensores fotoelétricos com feixe são ajustados como sendo sensores de muting com zonas de detecção de intersecção.

Ajuste da aplicação**Entrada****Saída**

O sensor 11 está conectado ao sinal de muting 11. O sensor 12, ao sinal de muting 12. Já o sensor 21 está conectado ao sinal de muting 21. O sensor 22 está conectado ao sinal de muting 22.

Seqüência de muting

A seqüência de muting do exemplo está descrita abaixo.

1. Como a luz não é interrompida entre os sensores 11, 12, 21 e 22 e a cortina de luz, o sinal habilitação de saída permanece ativado.
2. Para a entrada, à medida que a peça de trabalho move-se para a direita e os sensores 11 e 12 permanecem ativados na ordem (sensores 21 e 22 são ativados quando a peça de trabalho sai), o muting é habilitado e o sinal de muting é ativado.
3. À medida que a peça de trabalho continua avançando, o sinal habilitação de saída é mantido ativado, mesmo que a cortina de luz esteja obstruída.
4. À medida que a peça de trabalho continua avançando, o sensor 21 deixa de detectar a peça na entrada (sensor 12 durante a saída da peça de trabalho), o status de muting é apagado e o sinal de muting, desativado.

Ajustes de distância

Durante o ajuste desse tipo de aplicação de muting, os ajustes de distância devem impedir que uma pessoa de passagem habilite a função de muting, e os sensores da cortina de luz e do muting devem ser ajustados de forma que uma peça de trabalho passe por todos os sensores de muting antes da chegada da próxima peça aos sensores de muting.

Para calcular as distâncias de ajuste apropriadas para o exemplo, use estas fórmulas, em que:

- D2 e D3 = distância mínima requerida para o desempenho do sensor de muting
- d2 = distância máxima requerida para o desempenho do sensor de muting
- L = comprimento da peça de trabalho
- V = velocidade de trânsito da peça de trabalho
- T1mín = tempo de ciclo do controlador
- T1máx = ajuste do tempo de sincronia (o ajuste padrão é de 3 segundos)

Fórmula 3: $D2 < L$

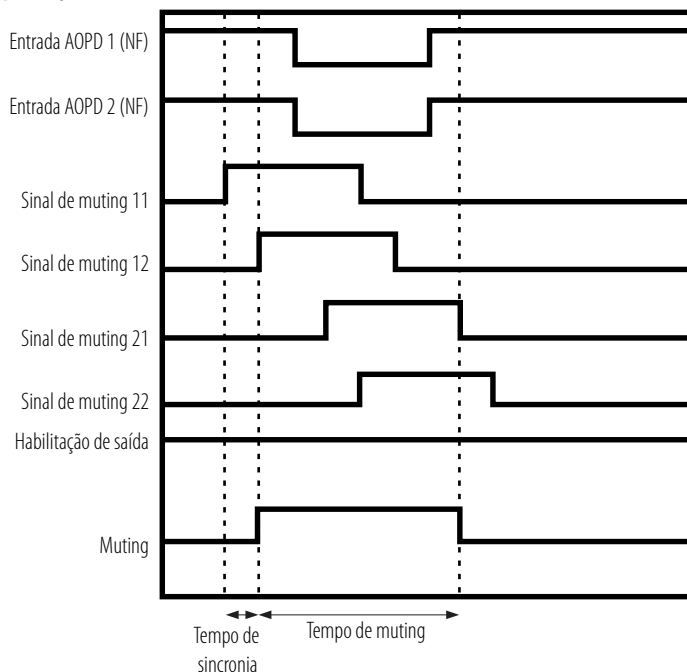
Fórmula 4: $D3 < L$

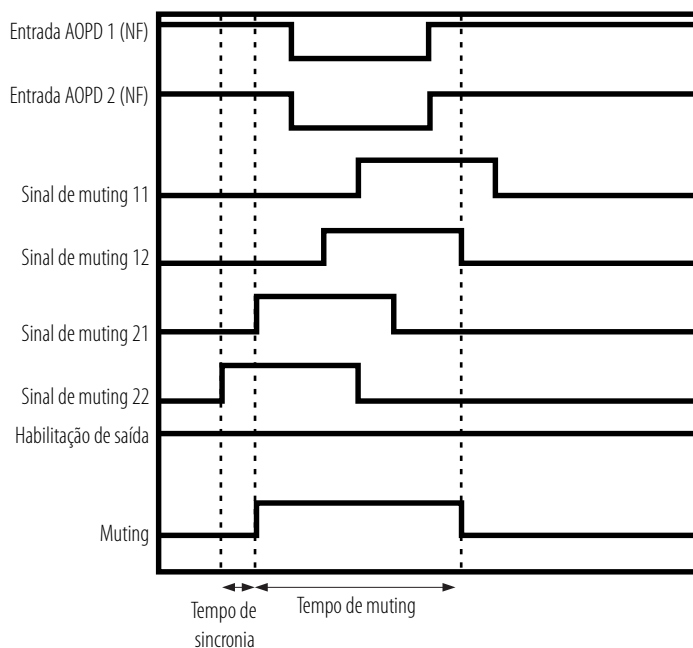
Fórmula 5: $V \times T1mín < d2 < V \times T1máx$

Para que a função de muting opere de maneira efetiva, as fórmulas 3, 4 e 5 devem ser atendidas.

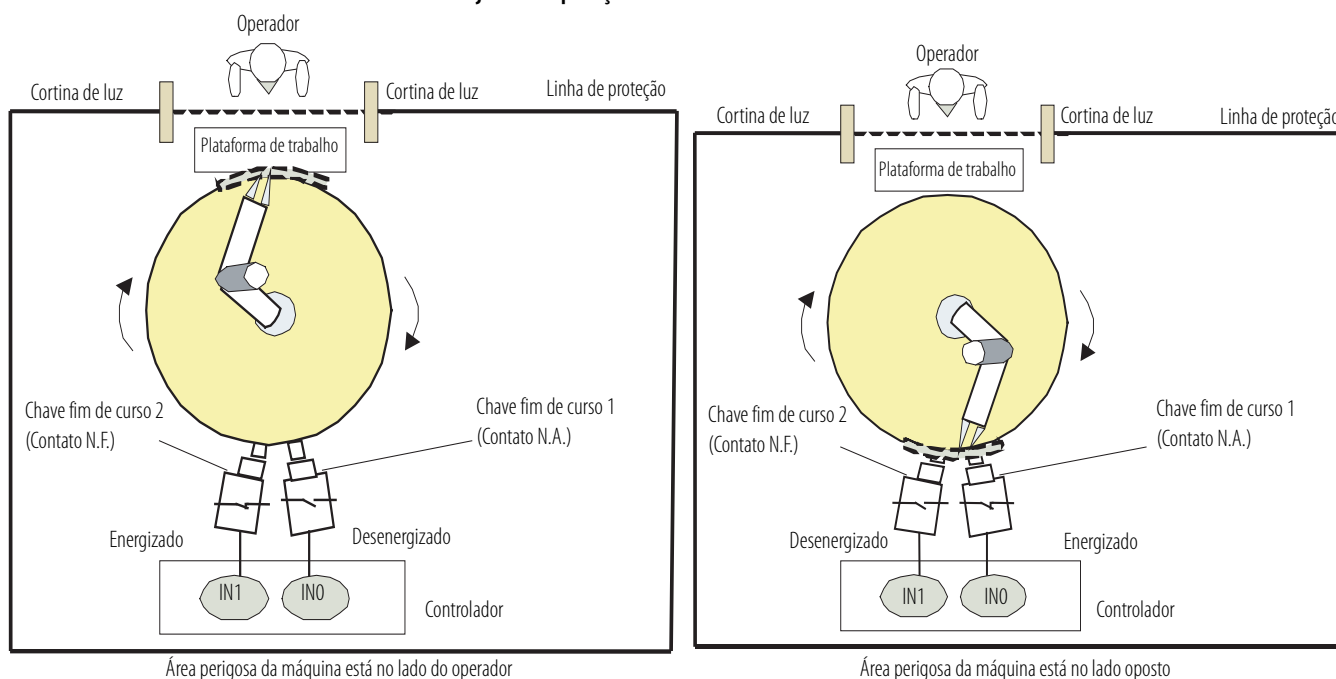
Gráficos de temporização do muting seqüencial (nos dois sentidos)

Gráfico de temporização de entrada



Padrão de entrada de diferença do tempo 2: Gráfico de temporização de saída

Exemplo: detecção de posição

Nesta aplicação de exemplo, a peça de trabalho é instalada em uma mesa giratória cercada por uma linha de proteção. O operador pode desabilitar o sinal de interrupção da função de proteção da cortina para ajustar uma peça de trabalho na mesa giratória quando a área perigosa da máquina está no lado oposto do operador.

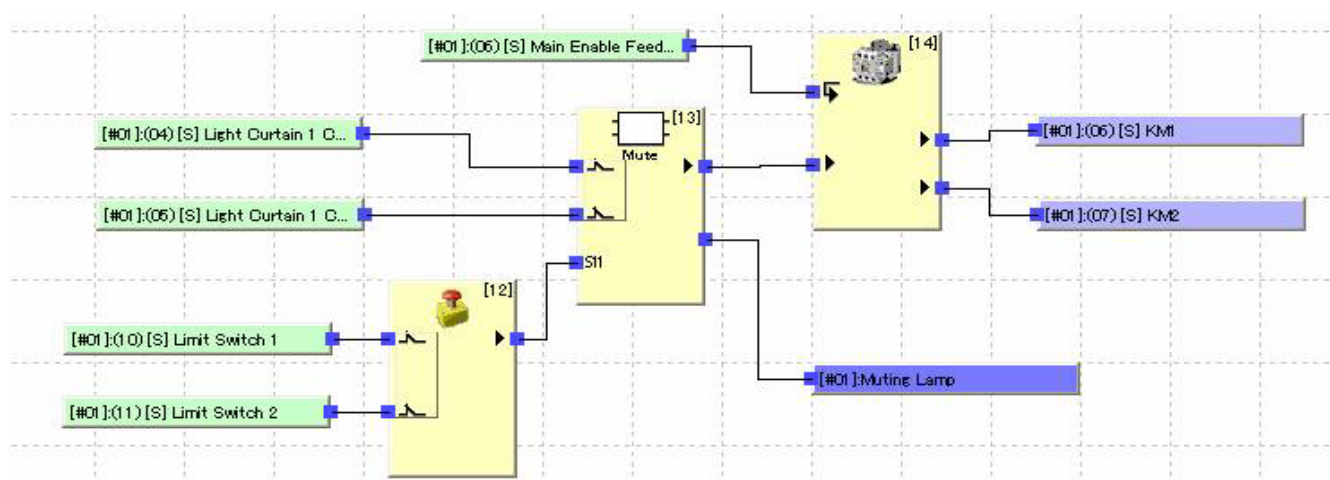
Ajuste da aplicação


Configure a entrada local no controlador como sendo um canal duplo complementar.

Exemplo do programa

As chaves fim de curso 1 e 2 conectam-se ao sinal de muting 11 do bloco de funções de muting usando uma instrução Estop. As chaves fim de curso 1 e 2 são ajustadas de acordo com o canal duplo complementar das entradas locais para avaliar os dados de entrada das duas chaves.

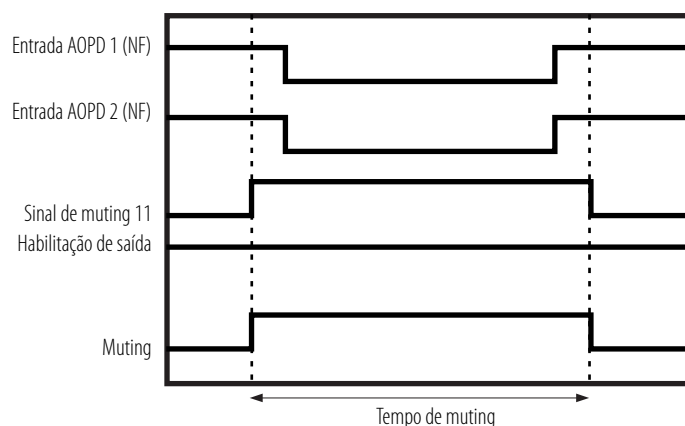
Lógica do programa



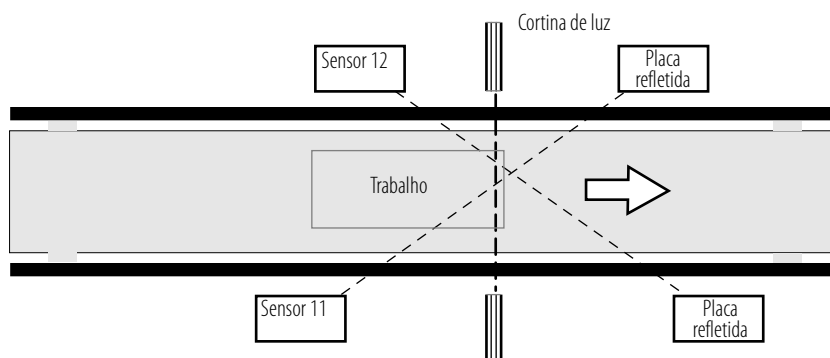
Seqüência de muting

A seqüência de muting do exemplo está descrita abaixo.

1. Quando a área perigosa da máquina está no mesmo lado do operador, a chave fim de curso N.A. 1 é desativada e a chave fim de curso N.F. 2, ativada. Além disso, como a cortina de luz não é obstruída, o sinal habilitação de saída é ativado. O sinal de muting 11, que insere o sinal de canal duplo complementar das chaves fim de curso 1 e 2, é desativado.
2. À medida que o braço robótico desloca-se, a chave fim de curso 1 é ativada e a chave fim de curso 2, é desativada quando a área perigosa está na direção oposta do operador. Como o resultado da instrução Estop, que insere o sinal de canal duplo complementar para as chaves fim de curso 1 e 2, é ativado, o muting é desabilitado e o sinal de muting é ativado.
3. Neste ponto, o sinal habilitação de saída é mantido ativado mesmo que a cortina de luz seja obstruída de forma que o operador possa acessar a plataforma de trabalho.
4. Quando o operador conclui sua tarefa e a cortina de luz é desobstruída na medida em que o braço robótico desloca-se, o resultado da instrução Estop é desativado, o status do muting é limpo e o sinal de muting é desativado.

*Gráfico de temporização***Operação normal****Exemplo: função de override**

A função de override pode ativar a saída de segurança mesmo que o sinal de interrupção da luz da cortina seja inativo. Caso uma peça de trabalho emperre durante o trânsito, o sistema não pode retornar à operação normal sem remover a peça de maneira forçada. Nesse tipo de situação, a função de override pode ser usada para retirar a peça de trabalho da zona de detecção da cortina de luz.

Ajuste da aplicação

O sensor 11 é conectado ao sinal de muting 11. Já o sensor 12 é conectado ao sinal de muting 12.

Seqüência de override

A seqüência de override do exemplo está descrita abaixo.

1. O sinal habilitação de saída é desativado.
2. Quando as entradas de override são ativadas, é dada a partida na função de override e o sinal de override é ativado. Desde que as entradas de override estejam ativadas, o status de muting é habilitado de maneira forçada, e os sinais de muting e habilitação de saída são ativados.
3. Quando a peça de trabalho move-se para a direita até deixar de ser detectada pelo sensor (sensor 12, no caso), o status de muting forçado pela função de override é apagado, e os sinais de muting e habilitação de saída são desativados.

Condições de partida de override

Caso as seguintes condições sejam atendidas, é dada a partida na função de override, e os sinais habilitação de saída, de muting e sinais de override são ativados.

- Pelo menos um sensor de muting está ativado.
- A cortina de luz está desativada (obstruída).
- A habilitação de saída está desativada.
- O sinal de entrada de override está ativado (quando definido como sendo uma única entrada) ou ativo (quando definido como entradas duplas).

Condições de parada de override

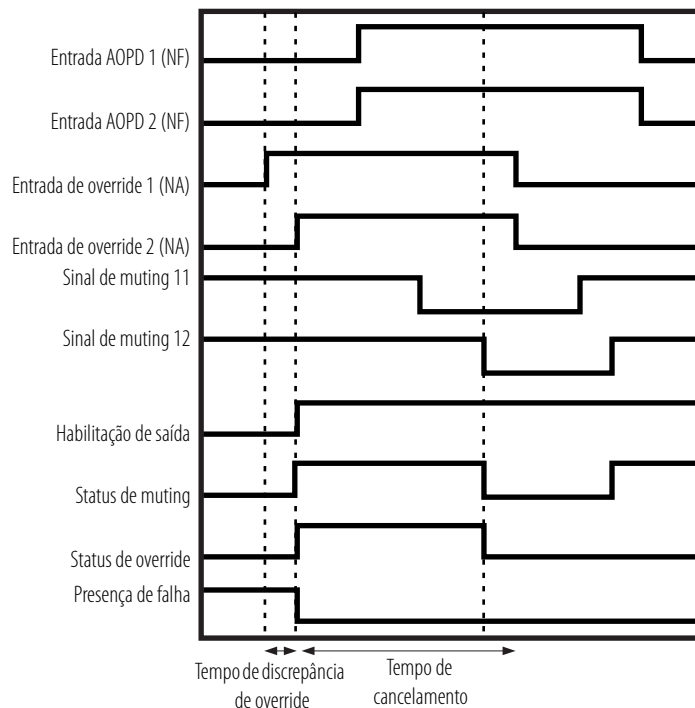
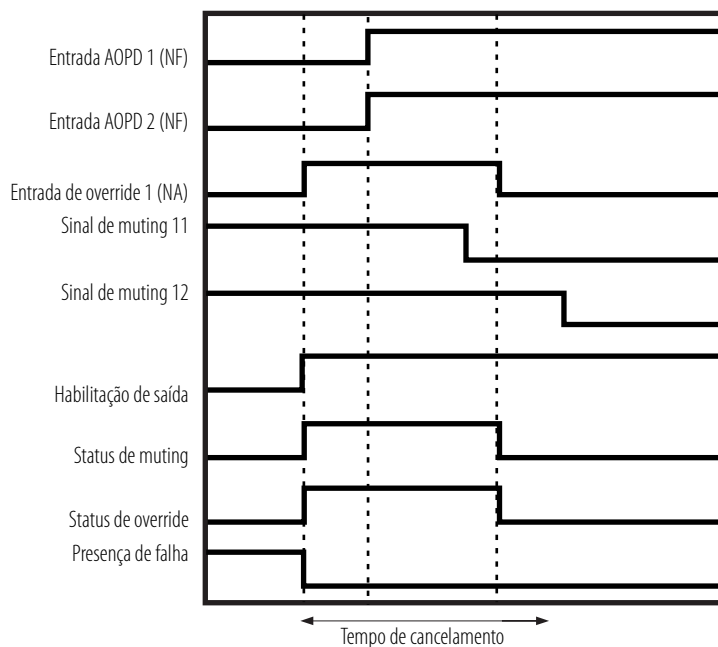
Caso uma das seguintes condições seja atendida, a função de override é desligada, e os sinais de muting e de override são desativados.

- Os sinais de muting estão todos desativados.
- O tempo de override máximo transcorreu.
- O sinal de entrada de override está desativado (quando definido como sendo uma única entrada) ou inativo (quando definido como entradas duplas).

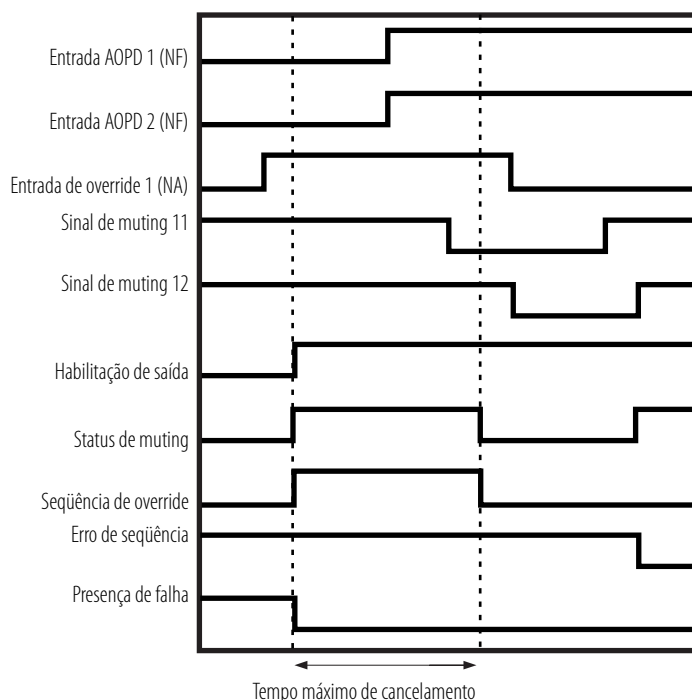
Quando a função de override é interrompida, a habilitação de saída é desativada caso a cortina de luz esteja obstruída.

Gráfico de temporização

O modo de muting nos seguintes gráficos está em paralelo com 2 sensores.

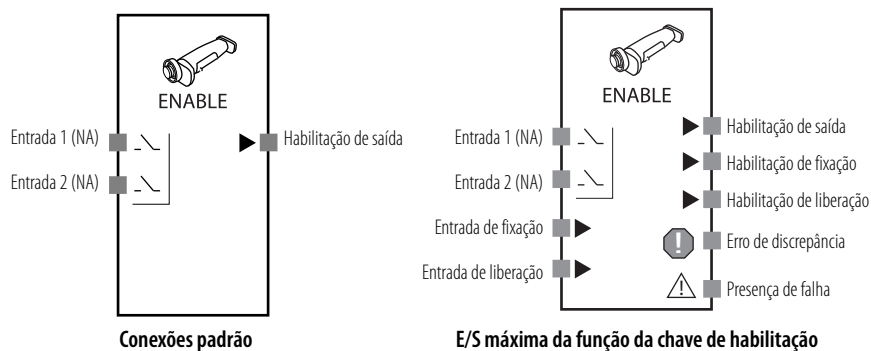
Operação normal da função de override**Sinal de override desativado durante o override**

Tempo-limite de override durante override



Chave de habilitação

Diagrama de blocos de chaves de habilitação



O bloco de funções da chave de habilitação monitora o status do equipamento da chave de habilitação. O sinal habilitação de saída é ativado quando as entradas do equipamento da chave de habilitação que está sendo monitorado estão ativas. O sinal habilitação de saída é desativado quando as entradas não estão ativas ou um erro é detectado no bloco de funções.

Além disso, caso o equipamento da chave de habilitação seja do tipo que produz um sinal de fixação e um sinal de liberação, a entrada de fixação do equipamento e o status do sinal de entrada de liberação podem ser monitorados. A entrada de fixação recebida e os sinais de entrada de liberação não afetam o status do sinal Habilitação de saída.

Parâmetros do bloco de funções da chave de habilitação

Defina estes parâmetros para o bloco de funções da chave de habilitação.

Parâmetros do bloco de funções da chave de habilitação

Parâmetro	Faixa válida	Configuração padrão
Tipo de entrada	Canal único Equivalente a canal duplo	Equivalente a canal duplo
Tempo de discrepância	0 a 30 s em incrementos de 10 ms. ⁽¹⁾ O tempo de discrepância deve corresponder a ou ser maior que o tempo de ciclo do controlador.	30 ms

⁽¹⁾ Uma verificação do tempo de discrepância não é realizada quando o tempo de discrepância é definido como 0.

O número de entradas pode ser aumentado de duas para quatro na guia In/Out Settings da caixa de diálogo Function Block Properties no software RSNetWorx para DeviceNet. Há duas entradas mesmo quando o tipo de entrada está definido como Canal único. Os sinais de entrada de fixação e de liberação podem ser usados quando três ou quatro entradas são definidas. O ajuste de parâmetro padrão é de dois.

Saídas opcionais

As saídas opcionais também podem ser usadas na programação. Para habilitar essas saídas opcionais, marque as caixas de seleção na guia Out point da caixa de diálogo Function Block Properties.

- Habilitação de fixação
- Habilitação de liberação
- Erro de discrepância

Ajuste de saída de apresentação padrão

Também é possível usar a saída de apresentação da falha na programação. Para habilitar essa saída, marque a caixa de seleção Fault Present na guia Out point da caixa de diálogo Function Block Properties.

Manuseio de erro do bloco de funções da chave de habilitação

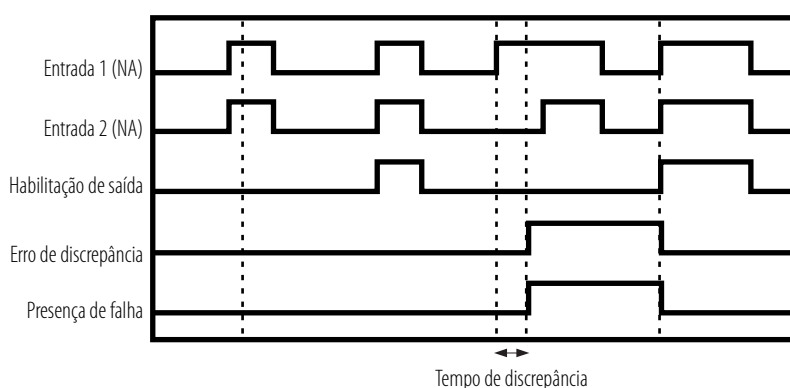
Use a tabela para diagnosticar e reinicializar uma condição de erro de discrepância no bloco de funções da chave de habilitação.

Detecção de erro e reset para o bloco de funções da chave de habilitação

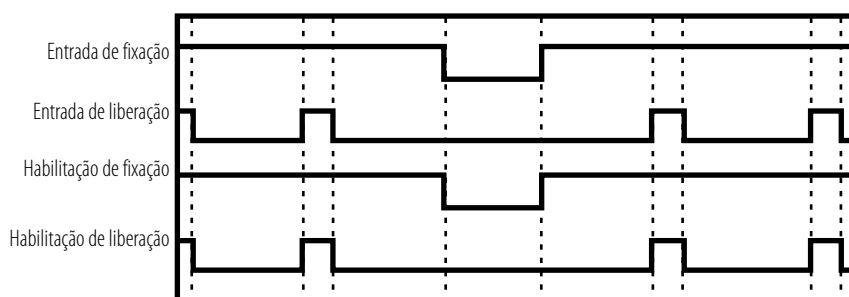
Condição de erro	Status quando ocorre um erro			Para reinicializar a condição de erro
	Habilitação de saída	Presença de falha	Saída do erro	
Erro de discrepância no par de entrada	OFF (estado de segurança)	ON	Erro de discrepância: ON	Remova a causa do erro e: - Desative ambos os pares de entradas 1 e 2 e ative-os novamente. - Altere o modo em operação do controlador para inativo e novamente para em operação.

Gráficos de temporização do bloco de funções da chave de habilitação

Operação normal e erro de discrepância

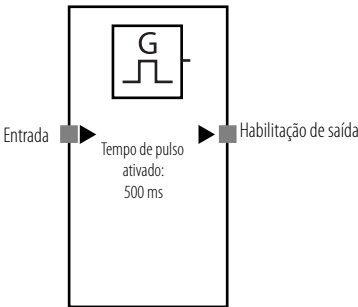


Sinal de fixação e sinal de liberação



Gerador de pulso

Diagrama de blocos de funções do gerador de pulso



O bloco de funções do gerador de pulso gera uma saída ativada/desativada no sinal de habilitação de saída enquanto o sinal de entrada do bloco de funções está ativado.

O tempo ativado e desativado do pulso pode ser definido de maneira independente entre 10 ms e 3 segundos em incrementos de 10 ms. Quando o tempo ativado estiver definido como 100 ms e o tempo desativado estiver definido como 500 ms, o sinal será repetidamente ativado por 100 ms e desativado em 500 ms.

A largura do pulso de saída terá um erro de temporização equivalente ao tempo de ciclo do controlador SmartGuard. Por exemplo, se o tempo de ciclo do controlador SmartGuard for de 7 ms e a largura do pulso estiver definida como 100 ms, o pulso de saída estará entre 93 e 107 ms.

Parâmetros de blocos de funções do gerador de pulso

Defina estes parâmetros para o bloco de funções do gerador de pulso.

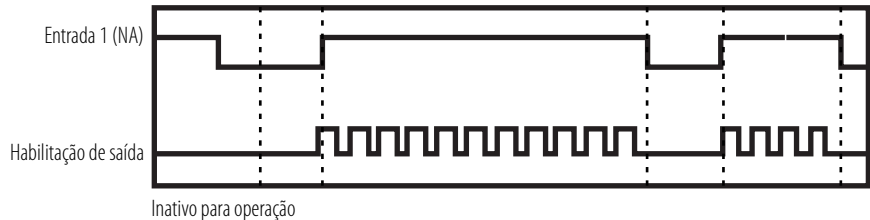
Parâmetros de blocos de funções do gerador de pulso

Parâmetro	Faixa válida	Configuração padrão
Tempo de pulso ativado	10 ms a 3 s em incrementos de 10 ms ⁽¹⁾	500 ms
Tempo de pulso desativado	10 ms a 3 s em incrementos de 10 ms ⁽¹⁾	500 ms

⁽¹⁾ O valor selecionado deve ser maior que o tempo de ciclo do controlador.

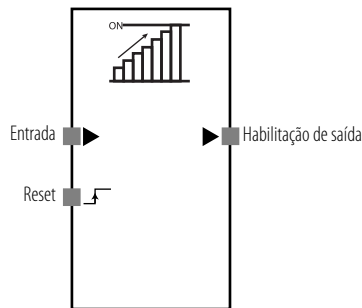
Gráfico de temporização dos parâmetros de blocos de funções do gerador de pulso

Gráfico de temporização do gerador de pulso



Contador

Diagrama de blocos de funções de contador



O bloco de funções do contador conta os pulsos em uma entrada e ativa o sinal habilitação de saída quando a contagem atinge um valor pré-selecionado. Define-se esse valor usando o software RSNetWorx para DeviceNet.

Quando a contagem de entrada alcança o valor pré-selecionado, o sinal habilitação de saída é ativado e retido assim. Para detectar pulsos no sinal de entrada, o tempo desativado e o tempo ativado do pulso de entrada devem ser maiores que o tempo de ciclo do controlador. Caso o tempo desativado e o tempo ativado do sinal do pulso de entrada sejam menores que o tempo de ciclo do controlador, os pulsos talvez sejam perdidos.

Parâmetros do bloco de funções do contador

Defina estes parâmetros para o bloco de funções do controlador.

Parâmetros do bloco de funções do contador

Parâmetro	Faixa válida	Configuração padrão
Condição de reset	Reset automático Reset manual	Reset manual
Tipo de contagem	Contador decrescente (decrementando) Contador crescente (incrementando)	Contador decrescente (decrementando)
Contador	1 a 65.535 contagens	1 contagem

Condição de reset

A condição de reset usada para reinicializar a contagem de entrada pode ser definida para manual ou automática. Quando a condição de reset é definida para automática e a contagem de entrada atinge o valor pré-selecionado, o sinal habilitação de saída é ativado e permanece assim enquanto o sinal de entrada estiver ativado. Quando o sinal de entrada é desativado, a contagem de entrada é reinicializada.

Já quando a condição de reset é definida para manual, a contagem de entrada é reinicializada e o sinal habilitação de saída é desativado quando o sinal de reset é ativado. Os pulsos de entrada não são contados enquanto o sinal de reset estiver ativado.

Tipo de contagem

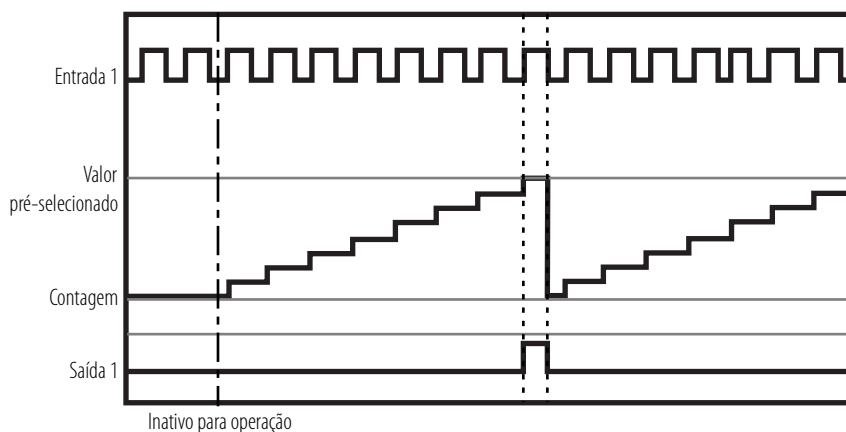
O tipo de contagem pode ser definido para decrescente (decrementando) ou crescente (incrementando).

Com um contador decrescente, o valor pré-selecionado é o valor inicial do contador e o contador é decrementado em uma contagem sempre que um pulso de entrada é detectado. O sinal habilitação de entrada é ativado quando a contagem chega a zero. Esse valor pré-selecionado do bloco de funções é armazenado na área de trabalho interna do bloco, e pode ser monitorado com um equipamento de programação.

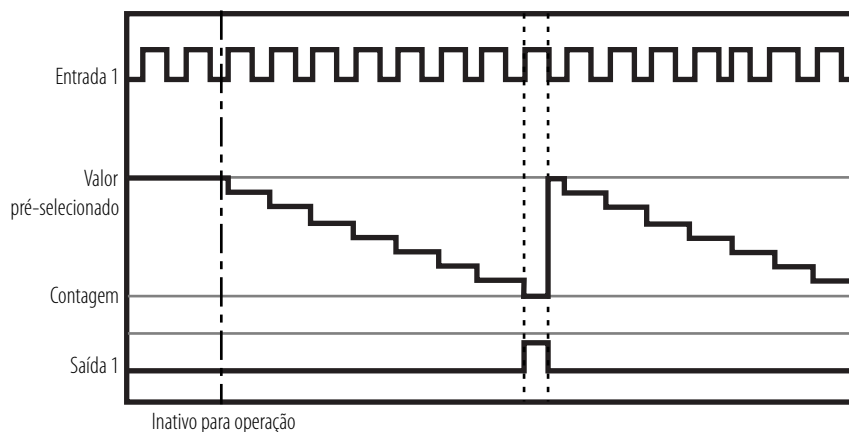
Com um contador crescente, o valor inicial do contador é zero e o contador é incrementado em uma contagem sempre que um pulso de entrada é detectado. O sinal habilitação de entrada é ativado quando a contagem chega ao valor pré-selecionado.

Gráficos de temporização do bloco de funções do contador

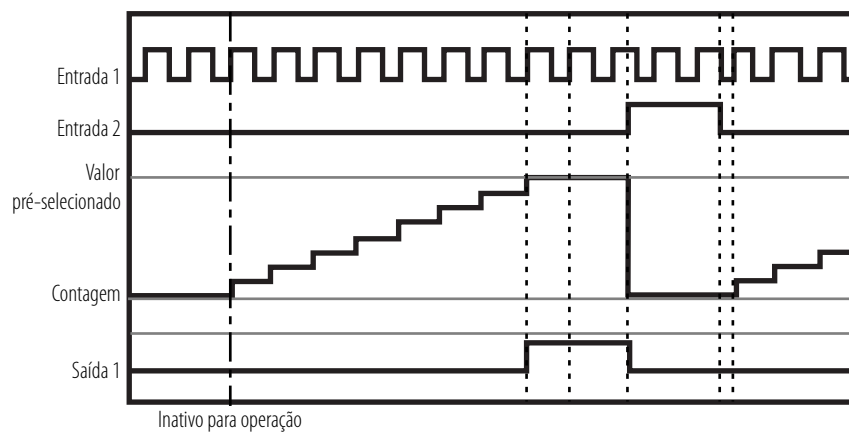
Contador crescente de reset automático



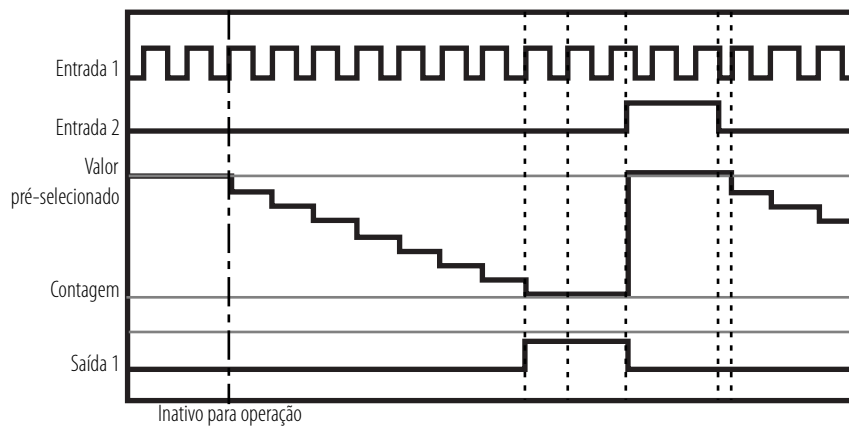
Contador decrescente de reset automático



Contador crescente de reset manual



Contador decrescente de reset manual



Mensagens explícitas

Introdução

Tópico	Página
Recebendo mensagens explícitas	273
Envio de mensagens explícitas	276
Acessando parâmetros do controlador usando mensagens explícitas do DeviceNet	278

Recebendo mensagens explícitas

Enviar uma mensagem explícita de um mestre DeviceNet padrão para o controlador SmartGuard possibilita a leitura ou a gravação de qualquer dado ou parâmetro especificado do controlador SmartGuard. O controlador realiza uma ação de acordo com um comando enviado pelo mestre e retorna uma resposta.

Um comando de leitura lê a área de E/S local do SmartGuard ou a área de E/S escrava de segurança alocada para o controlador SmartGuard a partir do mestre.

O formato básico do comando e a resposta são mostrados abaixo.

Formato do comando

Endereço do nó de destino	Código do serviço	Identificação da classe		Identificação da instância		Endereço do offset		Dimensões dos dados	
	4B	03	56						

Formato de resposta normal

Número de bytes recebidos	Endereço do nó de origem	Código do serviço	Dados da leitura					
		CB						

Formato de resposta com erro

Número de bytes recebidos		Endereço do nó de origem	Código do serviço	Código do erro	
00	04		94		

Formato do comando

O endereço do nó de destino especifica, em 1 byte hexadecimal, o endereço do nó dos dados a serem lidos.

Para comandos, especifique 4B (hex) para o código do serviço.

A identificação da classe é sempre 0356 para um controlador SmartGuard.

A identificação da instância depende do tipo de mensagem.

Valores de identificação da instância

Tipo de mensagem explícita	Serviço	Identificação da instância
Ler área de entrada local	Leitura	0001 (hex)
Ler área de saída local	Leitura	0002 (hex)
Ler área de entrada remota de segurança	Leitura	0005 (hex)
Ler área de saída remota de segurança	Leitura	0006 (hex)

Os dados do comando incluem as dimensões do offset e dos dados. As dimensões de offset especificam o endereço a partir do qual a leitura deve começar. Trata-se de um offset em bytes em relação à primeira linha da área. Já as dimensões dos dados especificam o número de bytes a serem lidos de 1 a 256. A faixa de valores mostrada abaixo deve ser usada como um guia para o ajuste de parâmetro do offset e das dimensões das várias áreas de dados.

Faixa de valores

Área	Faixa
Área de entrada local	0 ou 1
Área de saída local/teste	0 ou 1
Área de entrada remota de segurança	0 a 551
Área de saída remota de segurança	0 a 551

Formato de resposta

O número de bytes recebidos para respostas indica o número de bytes dos dados recebidos do endereço do nó de origem para a terminação da resposta retornada (em formato hexadecimal).

O nó de origem das respostas retorna o endereço do nó do controlador SmartGuard em 1 byte hexadecimal.

Para as respostas, o bit superior permanece ativado, e o CB hex é retornado para o código do serviço.

Os dados da leitura para respostas são os dados de E/S retornados da área especificada. Os offsets do endereço e as atribuições de bit para leitura das entradas locais, das saídas locais e das saídas de teste são mostrados abaixo. Para esses bits, 1 corresponde a normal e 0, a um erro.

Entradas locais (2 bytes)

Offset (bytes)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Terminal de entrada de segurança número 7	Terminal de entrada de segurança número 6	Terminal de entrada de segurança número 5	Terminal de entrada de segurança número 4	Terminal de entrada de segurança número 3	Terminal de entrada de segurança número 2	Terminal de entrada de segurança número 1	Terminal de entrada de segurança número 0
1	Terminal de entrada de segurança número 15	Terminal de entrada de segurança número 14	Terminal de entrada de segurança número 13	Terminal de entrada de segurança número 12	Terminal de entrada de segurança número 11	Terminal de entrada de segurança número 10	Terminal de entrada de segurança número 9	Terminal de entrada de segurança número 8

Saídas locais e de teste (2 bytes)

Offset (bytes)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Terminal de saída de segurança número 7	Terminal de saída de segurança número 6	Terminal de saída de segurança número 5	Terminal de saída de segurança número 4	Terminal de saída de segurança número 3	Terminal de saída de segurança número 2	Terminal de saída de segurança número 1	Terminal de saída de segurança número 0
1	Reservado				Terminal de saída de teste número 3	Terminal de saída de teste número 2	Terminal de saída de teste número 1	Terminal de saída de teste número 0

Formato de resposta com erro

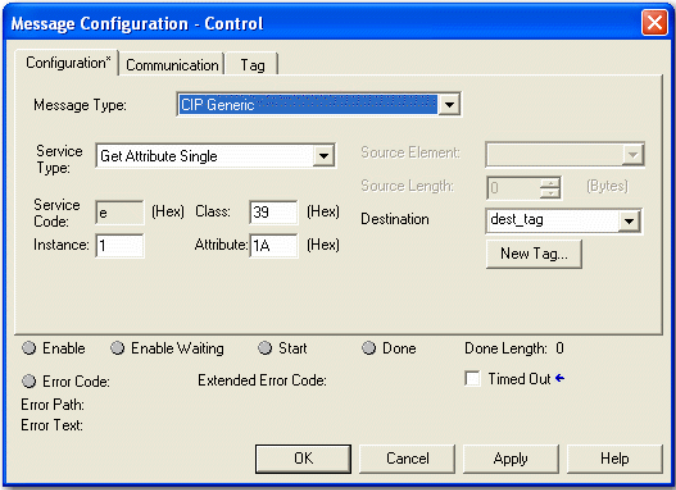
Assim como a resposta normal, a resposta com erro inclui o número de bytes recebidos, o endereço do nó original e o código do serviço. Ela também inclui estes códigos de erro DeviceNet.

Códigos de erro de mensagem explícita DeviceNet

Código de resposta	Nome do erro	Descrição
08FF	Serviço não suportado	Há um erro no código do serviço.
16FF	Objeto não existe	A identificação da instância especificada não é suportada.
15FF	Muitos dados	Os dados são maiores do que as dimensões especificadas.
13FF	Dados insuficientes	Os dados são menores do que as dimensões especificadas.
20FF	Parâmetro inválido	Os dados do comando operacional especificado não são suportados.

Exemplo de mensagem de leitura de um controlador GuardLogix

Esta instrução de mensagem do GuardLogix, programada no software RSLogix 5000 usando os parâmetros de formato do comando da [página 273](#), lê os dados do SmartGuard.



Envio de mensagens explícitas

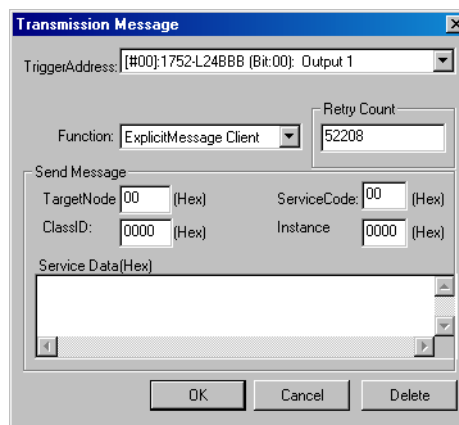
Um controlador SmartGuard pode enviar mensagens explícitas a partir de um programa aplicativo do usuário. As mensagens registradas pelo usuário são enviadas pela rede quando as condições de disparo especificadas pelo usuário são atingidas. Isso pode ser usado para notificar os dispositivos de monitoração e de controle ou como um método para especificar saídas para dispositivos de exibição. É possível enviar até 32 bytes de dados em mensagens explícitas.

Formato de dados da mensagem explícita

Nome do parâmetro	Dimensões dos dados
Identificação de MAC	1 byte
Código do serviço	1 byte
Identificação da classe	2 bytes
Identificação da instância	2 bytes
Dados do serviço	0 a 26 bytes

Siga estas etapas para enviar uma mensagem explícita usando o Logic Editor no software RSNetWorx para DeviceNet.

1. Na barra de menus, escolha Function > Transmission Message Setting.



2. Use o menu TriggerAddress para selecionar o tag de saída que você deseja usar como sendo o disparo para enviar a mensagem explícita.

Sempre que o tag de saída especificado mudar de desativado para ativado, a mensagem explícita definida como sendo a mensagem de envio será enviada.

3. No campo Retry Count, digite o número de vezes em que se deve reenviar a transmissão em caso de falha.

Digite 0 para que não haja novas tentativas.

4. Verifique o formato da mensagem explícita do nó de destino e se ele criou uma mensagem de envio com base nas especificações do nó de destino, inclusive TargetNode, ServiceCode, identificação da classe e identificação da instância.

Restrições de envio das mensagens explícitas

As mensagens explícitas estão sujeitas às seguintes restrições.

- Um endereço pode ser definido no programa do usuário para o endereço de disparo.
- A memória de E/S interna do controlador SmartGuard é enviada como sendo uma resposta para uma mensagem explícita. As mensagens explícitas podem ser enviadas de um programa do usuário no controlador, embora as informações internas no controlador não possam ser usadas como dados da mensagem de envio.

- Os dados de resposta para mensagens explícitas não podem ser usados em um programa do controlador SmartGuard.

ATENÇÃO


Os atributos dos dados manuseados pela comunicação de E/S padrão e pela comunicação por mensagens explícitas não são dados de segurança. As medidas necessárias para os dados de segurança não são tomadas durante a geração de dados padrão ou de mensagens explícitas. Não use esses dados para operar um sistema de controle de segurança.

Acessando parâmetros do controlador usando mensagens explícitas do DeviceNet

É possível ler e gravar em parâmetros do controlador enviando mensagens explícitas do DeviceNet para o controlador SmartGuard. O controlador processa as mensagens recebidas e retorna uma resposta. As mensagens descritas nestas tabelas são suportadas pelo controlador SmartGuard.

Status geral de leitura

Mensagem explícita	Serviço	Função	Código do serviço	Comando				Resposta
				Identificação da classe hexadecimal	Identificação da instância hexadecimal	Identificação do atributo	Dimensões dos dados	
Ler status geral da unidade	Leitura	Lê o status geral do controlador	0E hex	39 hex	01 hex	6E hex	--	1 byte

Lendo a assinatura de segurança

Mensagem explícita	Serviço	Função	Código do serviço	Comando				Resposta
				Identificação da classe hexadecimal	Identificação da instância hexadecimal	Identificação do atributo	Dimensões dos dados	
Ler status de segurança da unidade	Leitura	Ler a assinatura de segurança do SmartGuard e registro de data e hora	0E hex	39 hex	01 hex	1A hex	--	10 bytes

Configuração e monitoração dos terminais de entrada de segurança

Mensagem explícita	Serviço	Função	Comando				Dimensões dos dados	Resposta
			Código do serviço	Identificação da classe	Identificação da instância	Identificação do atributo		
Modo de monitoração das informações sobre a manutenção do terminal	Leitura	Lê o modo de monitoração das informações sobre a manutenção da entrada (1 a 16) especificado pela identificação da instância.	0E hex	3D hex	01 a 10 hex	65 hex	—	1 byte 00 hex: Total em modo de temporização 01 hex: Modo de contador da operação do contato
	Gravação	Grava o modo de monitoração das informações sobre a manutenção da entrada (1 a 16) especificado pela identificação da instância.	10 hex	3D hex	01 a 10 hex	65 hex	1 byte 00 hex: Total no modo de temporização 01 hex: Modo de contador da operação do contato	
SV para total de entrada em temporização ou contador de operações do contato	Leitura	Lê o SV do total em temporização ou do contador de operações do contato de entrada (1 a 16) especificado pela identificação da instância.	0E hex	3D hex	01 a 10 hex	68 hex	—	4 bytes 0000 0000 a FFFF FFFF hex (0 a 4,294,967,295)
	Gravação	Grava o SV do total em temporização ou do contador de operações do contato de entrada (1 a 16) especificado pela identificação da instância.	10 hex	3D hex	01 a 10 hex	68 hex	4 bytes 0000 0000 a FFFF FFFF hex (0 a 4,294,967,295)	—
Total de entrada de leitura em temporização ou contador de operações do contato	Leitura	Lê o total em temporização ou do contador de operações do contato de entrada (1 a 16) especificado pela identificação da instância.	0E hex	3D hex	01 a 10 hex	66 hex	—	4 bytes 0000 0000 a FFFF FFFF hex (0 a 4,294,967,295)
Reinicializar o total de entrada em temporização ou contador de operações do contato	Reset	Reinicializa o total em temporização ou do contador de operações do contato de entrada (1 a 16) especificado pela identificação da instância.	05 hex	3D hex	01 a 10 hex	66 hex	—	—
Ler status do monitor do total da entrada em temporização ou contador de operações do contato	Leitura	Lê o status do monitor do total em temporização ou do contador de operações do contato de entrada (1 a 16) especificado pela identificação da instância.	0E hex	3D hex	01 a 10 hex	67 hex	—	1 byte 00 hex: na faixa 01 hex: fora da faixa (acima do valor do monitor)
Ler flag normal de entrada de segurança	Leitura	Lê o status do flag normal do número (1 a 16) especificado pela identificação da instância.	0E hex	3D hex	01 a 10 hex	04 hex	—	1 byte 00 hex: erro 01 hex: normal

Configuração e monitoração dos terminais de entrada de segurança

Mensagem explícita	Serviço	Função	Comando				Dimensões dos dados	Resposta
			Código do serviço	Identificação da classe	Identificação da instância	Identificação do atributo		
Ler causa de informações sobre o erro de entrada de segurança	Leitura	Lê a causa do flag normal do número (1 a 16) especificado pela identificação da instância que está sendo desativada (erro).	0E hex	3D hex	01 a 10 hex	6E hex	—	1 byte 00 hex: sem erro 01 hex: configuração inválida 02 hex: erro do sinal de teste 03 hex: erro do circuito interno 04 hex: erro de discrepância 05 hex: erro em outro canal de canais duplos
Ler AND dos flags normais de entrada de segurança	Leitura	Lê a causa do flag normal do número (1 a 16) especificado pela identificação da instância que está sendo desativada (erro).	0E hex	3E hex	01 hex	05 hex	—	1 byte 00 hex: erro 01 hex: tudo normal
Ler OR do status do monitor do total de entrada em tempo ou contadores de operações do contato	Leitura	Lê o OR lógico do status do monitor do total em temporização ou do contador de operações do contato de todas as entradas 1 a 16.	0E hex		01 hex	72 hex	—	1 byte 00 hex: tudo na faixa 01 hex: entrada fora da faixa (acima do valor do monitor)

Configuração e monitoração os terminais de saída de segurança

Mensagem explícita	Serviço	Função	Comando					Resposta
			Código do serviço	Identificação da classe	Identificação da instância	Identificação do atributo	Dimensões dos dados	
Modo de monitoração das informações sobre a manutenção do terminal	Leitura	Lê o modo de monitoração das informações sobre a manutenção da saída (1 a 8) especificado pela identificação da instância.	0E hex	3B hex	01 a 08 hex	65 hex	—	1 byte 00 hex: Total em modo de temporização 01 hex: Modo de contador da operação do contato
	Gravação	Grava o modo de monitoração das informações sobre a manutenção da saída (1 a 8) especificado pela identificação da instância.	10 hex	3B hex	01 a 08 hex	65 hex	1 byte 00 hex: Total em modo de temporização 01 hex: Modo de contador da operação do contato	—
SV para total de saída em temporização ou contador de operações do contato	Leitura	Lê o SV do total em temporização ou do contador de operações do contato de entrada (1 a 8) especificado pela identificação da instância.	0E hex	3B hex	01 a 08 hex	68 hex	—	4 bytes 0000 0000 a FFFF FFFF hex (0 a 4,294,967,295)
	Gravação	Grava o SV do total em temporização ou do contador de operações do contato de entrada (1 a 8) especificado pela identificação da instância.	10 hex	3B hex	01 a 08 hex	68 hex	4 bytes 0000 0000 a FFFF FFFF hex (0 a 4,294,967,295)	—
Ler total de saída em temporização ou contador de operações do contato	Leitura	Lê o total em temporização ou do contador de operações do contato de entrada (1 a 8) especificado pela identificação da instância.	0E hex	3B hex	01 a 08 hex	66 hex	—	4 bytes 0000 0000 a FFFF FFFF hex (0 a 4,294,967,295)
Reinicializar o total de saída em temporização ou contador de operações do contato	Reset	Reinicializa o total em temporização ou do contador de operações do contato de saída (1 a 8) especificado pela identificação da instância.	05 hex	3B hex	01 a 08 hex	66 hex	—	—
Status do monitor de leitura da saída total em temporização ou contador de operações do contato	Leitura	Lê o status do monitor do total em temporização ou do contador de operações do contato de saída (1 a 8) especificado pela identificação da instância.	0E hex	3B hex	01 a 08 hex	67 hex	—	1 byte 00 hex: na faixa 01 hex: fora da faixa (acima do valor do monitor)

Configuração e monitoração os terminais de saída de segurança

Mensagem explícita	Serviço	Função	Comando					Resposta
			Código do serviço	Identificação da classe	Identificação da instância	Identificação do atributo	Dimensões dos dados	
Ler flag normal de saída de segurança	Leitura	Lê o status do flag normal do número (1 a 8) especificado pela identificação da instância.	0E hex	3B hex	01 a 08 hex	05 hex	—	1 byte 00 hex: erro 01 hex: normal
Ler causa de informações sobre o erro de saída de segurança	Leitura	Lê a causa do flag normal do número (1 a 8) especificado pela identificação da instância que está sendo desativada (erro).	0E hex	3B hex	01 a 08 hex	6E hex	—	1 byte 00 hex: sem erro 01 hex: configuração inválida 02 hex: detecção de sobrecorrente 03 hex: detecção de curto-circuito 04 hex: erro de constante alta 05 hex: erro em um dos canais duplos 06 hex: erro do circuito de relé interno 07 hex: erro de relé 08 hex: erro de dados entre saídas de canal duplo 09 hex: detecção do curto-circuito entre fios
Ler AND dos flags normais de saída de segurança	Leitura	Lê a causa do flag normal do número (1 a 8) especificado pela identificação da instância que está sendo desativada (erro).	0E hex	3C hex	01 hex	05 hex	—	1 byte 00 hex: erro 01 hex: tudo normal
Ler OR do status do monitor do total de saída em tempo ou contadores de operações do contato	Leitura	Lê o OR lógico do status do monitor do total em temporização ou do contador de operações do contato de todas as saídas 1 a 8.	0E hex	3C hex	01 hex	72 hex	—	1 byte 00 hex: tudo na faixa 01 hex: entrada fora da faixa (acima do valor do monitor)

Monitorando terminais de saída do teste

Mensagem explícita	Serviço	Função	Comando					Resposta
			Código do serviço	Identificação da classe	Identificação da instância	Identificação do atributo	Dimensões dos dados	
Modo de monitoração das informações sobre a manutenção do terminal	Leitura	Lê o modo de monitoração das informações sobre a manutenção da saída de teste (1 a 4) especificado pela identificação da instância.	0E hex	35B hex	01 a 04 hex	83 hex	—	1 byte 00 hex: Total em modo de temporização 01 hex: Modo de contador da operação do contato
	Gravação	Grava o modo de monitoração das informações sobre a manutenção da saída de teste (1 a 4) especificado pela identificação da instância.	10 hex	35B hex	01 a 04 hex	83 hex	1 byte 00 hex: Total em modo de temporização 01 hex: Modo de contador da operação do contato	—
SV para total de saída de teste em temporização o ou contador de operações do contato	Leitura	Lê o SV do total em temporização ou do contador de operações do contato de entrada (1 a 4) especificado pela identificação da instância.	0E hex	35B hex	01 a 04 hex	86 hex	—	4 bytes 0000 0000 to FFFF FFFF hex (0 to 4,294,967,295)
	Gravação	Grava o SV do total em temporização ou do contador de operações do contato de entrada (1 a 4) especificado pela identificação da instância.	10 hex	35B hex	01 a 04 hex	86 hex	4 bytes 0000 0000 a FFFF FFFF hex (0 a 4,294,967,295)	—
Ler total de saída de teste em temporização ou contador de operações do contato	Leitura	Lê o total em temporização ou do contador de operações do contato de entrada (1 a 4) especificado pela identificação da instância.	0E hex	35B hex	01 a 04 hex	84 hex	—	4 bytes 0000 0000 a FFFF FFFF hex (0 a 4,294,967,295)
Reinicializar o total de saída de teste em temporização ou contador de operações do contato	Reset	Reinicializa o total em temporização ou do contador de operações do contato de saída de teste (1 a 4) especificado pela identificação da instância.	05 hex	35B hex	01 a 04 hex	84 hex	—	—
Ler status do monitor da saída total de teste em temporização ou contador de operações do contato	Leitura	Lê o status do monitor do total em temporização ou do contador de operações do contato de saída de teste (1 a 4) especificado pela identificação da instância.	0E hex	35B hex	01 a 04 hex	85 hex	—	1 byte 00 hex: na faixa 01 hex: fora da faixa (acima do valor do monitor)

Monitorando terminais de saída do teste

Mensagem explícita	Serviço	Função	Comando					Resposta
			Código do serviço	Identificação da classe	Identificação da instância	Identificação do atributo	Dimensões dos dados	
Ler flag de segurança de saída de teste	Leitura	Lê o status do flag normal da saída de teste (1 a 4) especificado pela identificação da instância.	0E hex	35B hex	01 a 04 hex	68 hex	—	1 byte 00 hex: normal 01 hex: erro
Ler causa de informações sobre o erro de saída de teste	Leitura	Lê a causa do flag normal da saída de teste (1 a 4) especificado pela identificação da instância que está sendo desativada (erro).	0E hex	35B hex	01 a 04 hex	76 hex	—	1 byte 00 hex: sem erro 01 hex: configuração inválida 02 hex: detecção de sobrecorrente 05 hex: erro de constante alta 06 hex: detecção de subcorrente
Ler OR dos flags de segurança de saída	Leitura	Lê o OR lógico d flag normal de todas as saídas de teste (1 a 4).	0E hex	35C hex	01 hex	69 hex	—	1 byte 00 hex: tudo normal 01 hex: erro
Ler OR do status do monitor do total de saída de teste em tempo ou contadores de operações do contato	Leitura	Lê o OR lógico do status do monitor do total em temporização ou do contador de operações do contato de todas as saídas de teste 1 a 4.	0E hex	35C hex	01 hex	72 hex	—	1 byte 00 hex: tudo na faixa 01 hex: saída de teste fora da faixa (acima do valor do monitor)

Exemplos de aplicação e de configuração

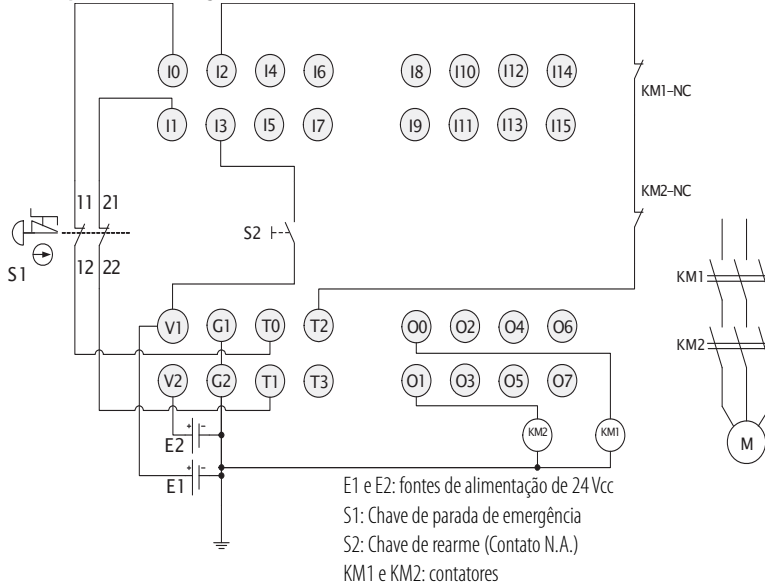
Introdução

Tópico	Página
Aplicação de parada de emergência	285
Aplicação de gate de segurança com reset automático	287
Aplicação de gate de segurança de zona dupla usando a chave de parada de emergência com reset manual	288
Aplicação de tapete de segurança	290
Aplicação de cortina de luz	292

Aplicação de parada de emergência

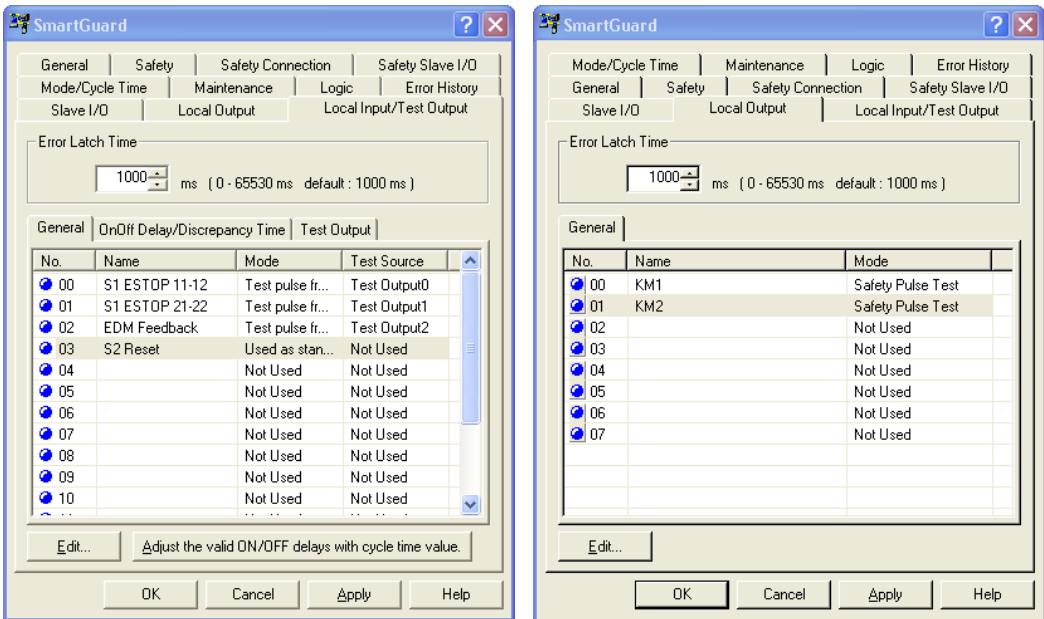
Este exemplo mostra uma chave de parada de emergência de canal duplo com reset manual.

Esquema elétrico da parada de emergência



Conecte uma fonte de alimentação de 24Vcc aos terminais V0 e G0, os terminais da fonte de alimentação dos circuitos internos.

Configuração



Programação

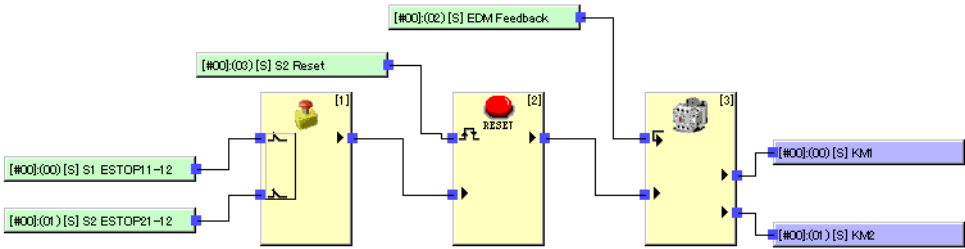
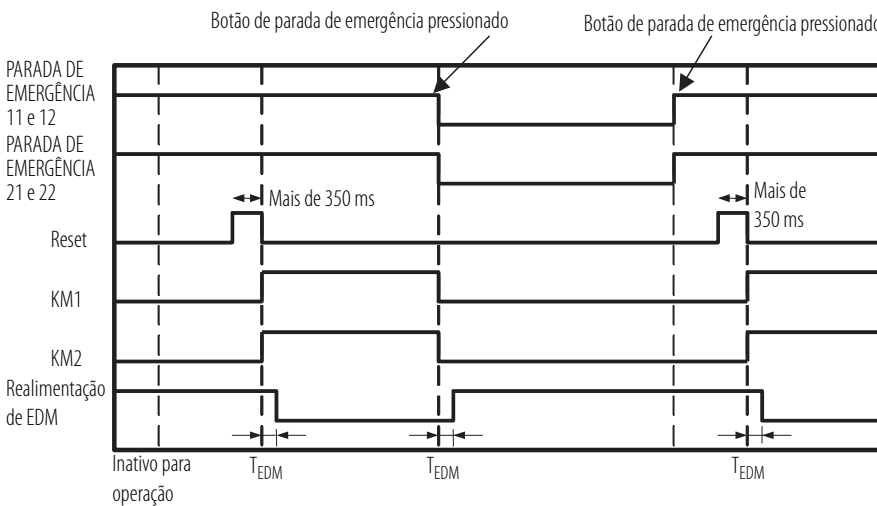


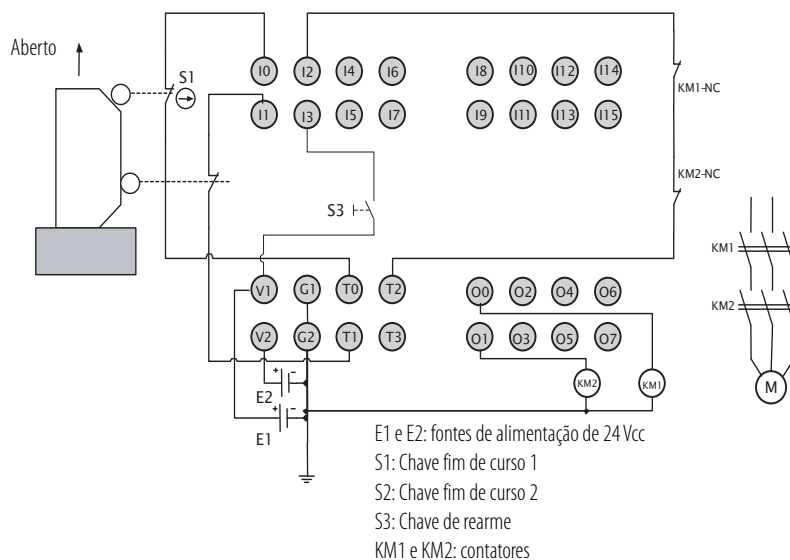
Diagrama de temporização



Aplicação de gate de segurança com reset automático

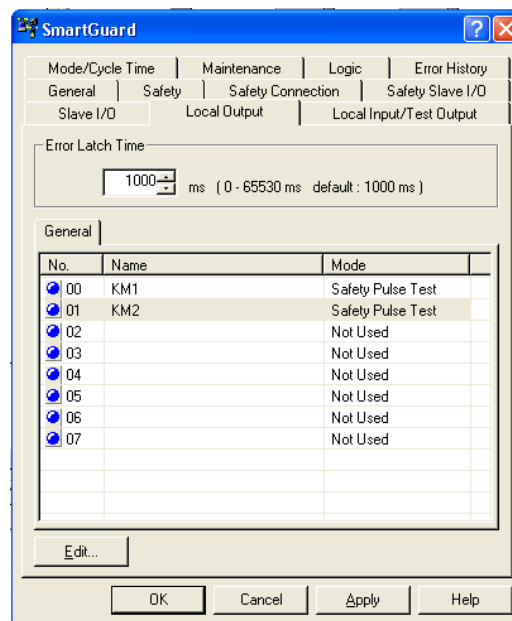
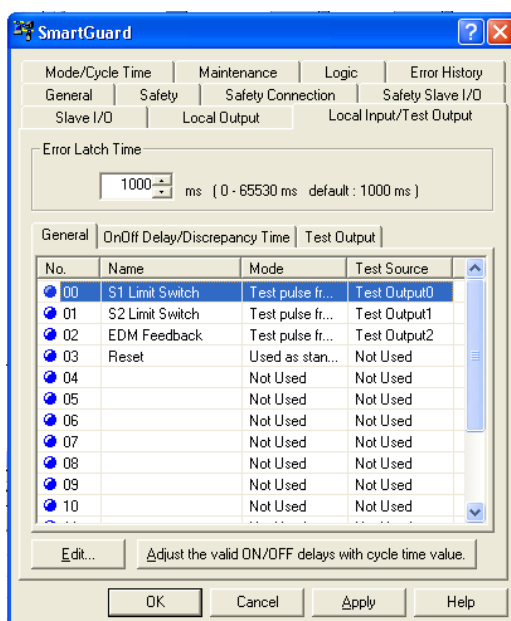
Este exemplo mostra chaves fim de curso em modo de canal duplo com reset automático.

Esquema elétrico



Conecte uma fonte de alimentação de 24Vcc aos terminais V0 e G0, os terminais da fonte de alimentação dos circuitos internos.

Configuração



Programação

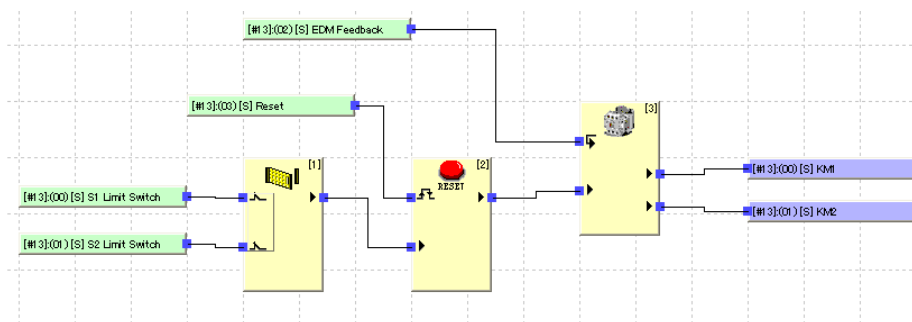
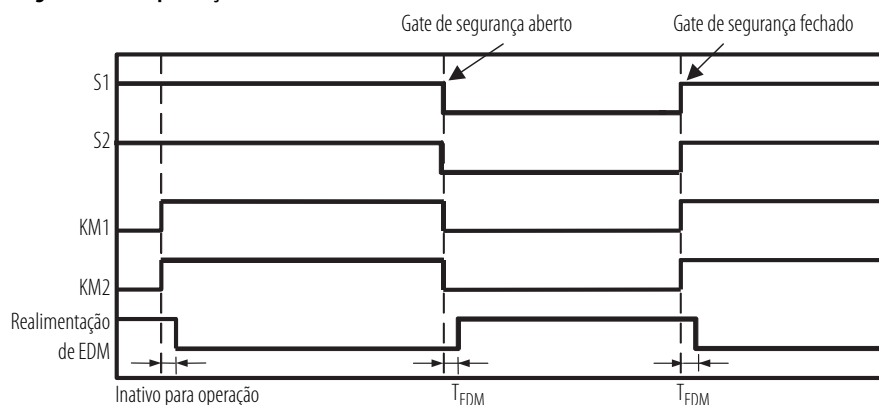


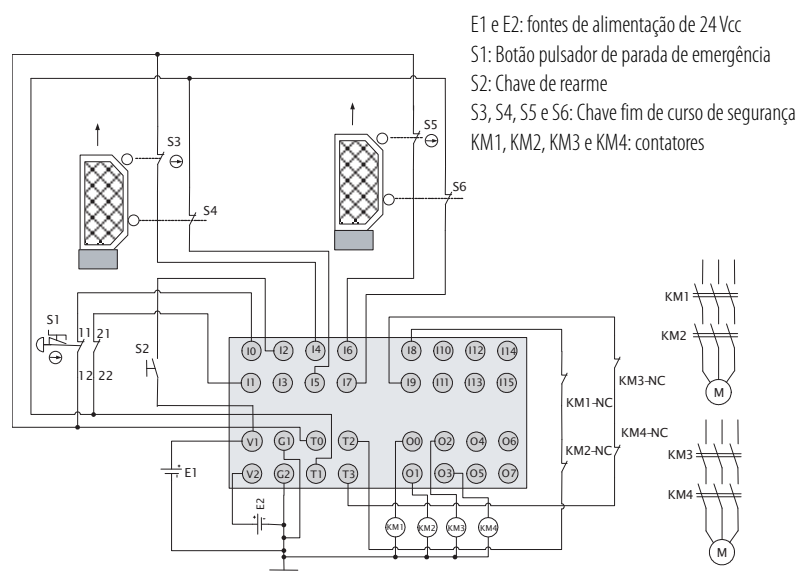
Diagrama de temporização



Aplicação de gate de segurança de zona dupla usando a chave de parada de emergência com reset manual

Este exemplo mostra chaves de porta de canal duplo com reset automático e uma chave de parada de emergência de canal duplo com reset manual. Como cada par de chaves de porta controla uma zona separada, parte da máquina pode continuar em execução caso sua porta esteja fechada. Uma parada de emergência desligará ambas as zonas.

Esquema elétrico



Conecte uma fonte de alimentação de 24 Vcc aos terminais V0 e G0, os terminais da fonte de alimentação dos circuitos internos.

Configuração

1752-L248BB

Mode/Cycle Time | Maintenance | Logic | Error History

General | Safety | Safety Connection | Safety Slave I/O

Slave I/O | Local Output | Local Input/Test Output

Error Latch Time

1000 ms (0 - 65530 ms default : 1000 ms)

General | OnOff Delay/Discrepancy Time | Test Output

No.	Name	Mode	Test Source
00	ESTOP1-1	Test pulse from test out	Test Output0
01	ESTOP1-2	Test pulse from test out	Test Output1
02	ResetSW	Test pulse from test out	Not Used
03		Used as standard i...	Not Used
04[e]	DoorSW1-1	Test pulse from test out	Test Output0
05[e]	DoorSW1-2	Test pulse from test out	Test Output1
06[e]	DoorSW2-1	Test pulse from test out	Test Output0
07[e]	DoorSW2-2	Test pulse from test out	Test Output1
08	FeedbackKM12	Test pulse from test out	Test Output2
09	FeedbackKM34	Test pulse from test out	Test Output3

Edit... Adjust the valid ON/OFF delays with cycle time value.

OK Cancel Apply Help

1752-L248BB

Mode/Cycle Time | Maintenance | Logic | Error History

General | Safety | Safety Connection | Safety Slave I/O

Slave I/O | Local Output | Local Input/Test Output

Error Latch Time

1000 ms (0 - 65530 ms default : 1000 ms)

General

No.	Name	Mode
00	KM1	Safety Pulse Test
01	KM2	Safety Pulse Test
02	KM3	Safety Pulse Test
03	KM4	Safety Pulse Test
04		Not Used
05		Not Used
06		Not Used
07		Not Used

Edit...

OK Cancel Apply Help

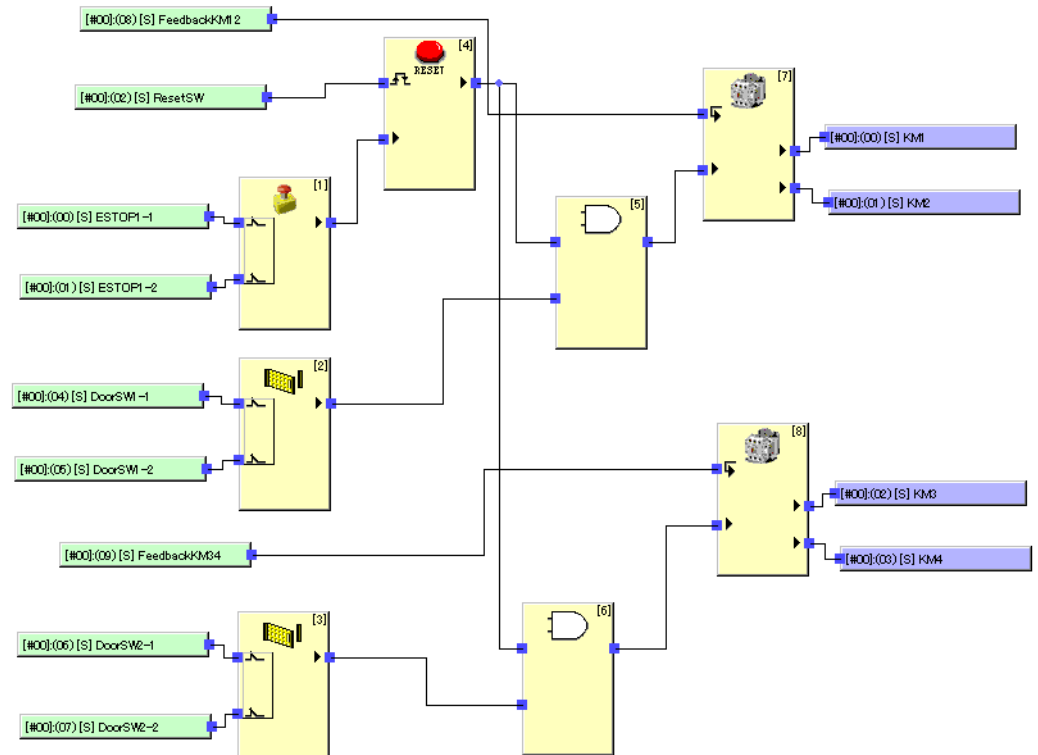
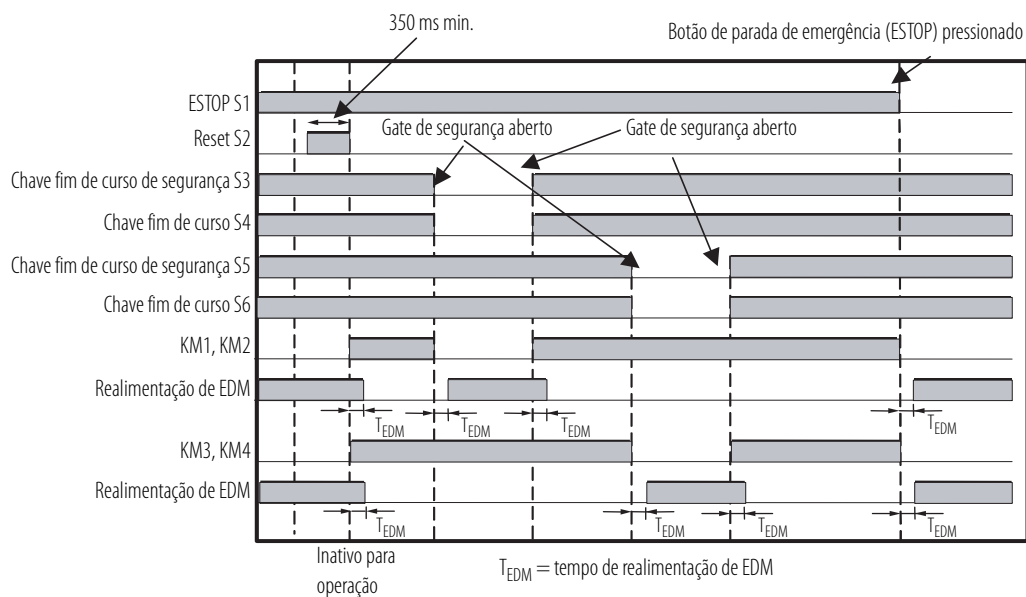
Programação

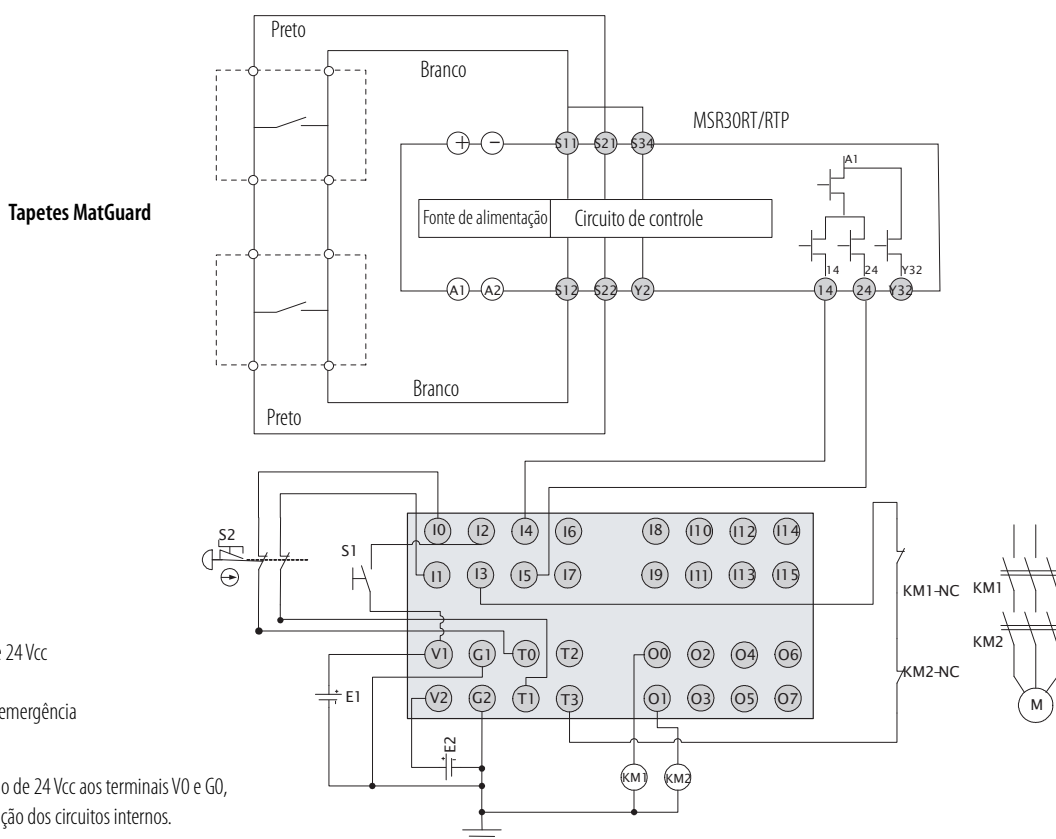
Diagrama de temporização

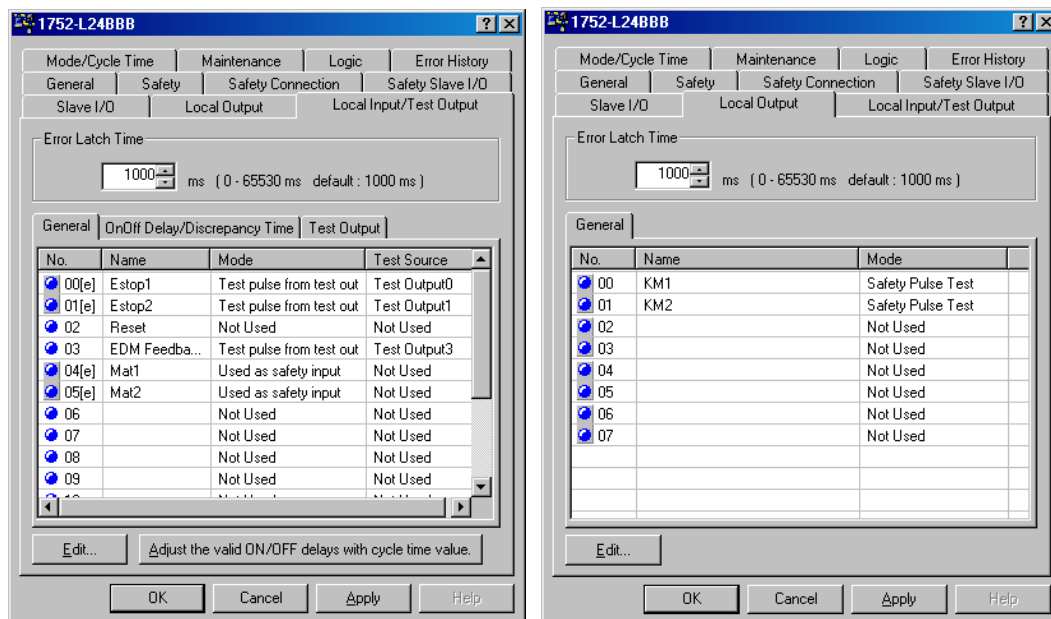
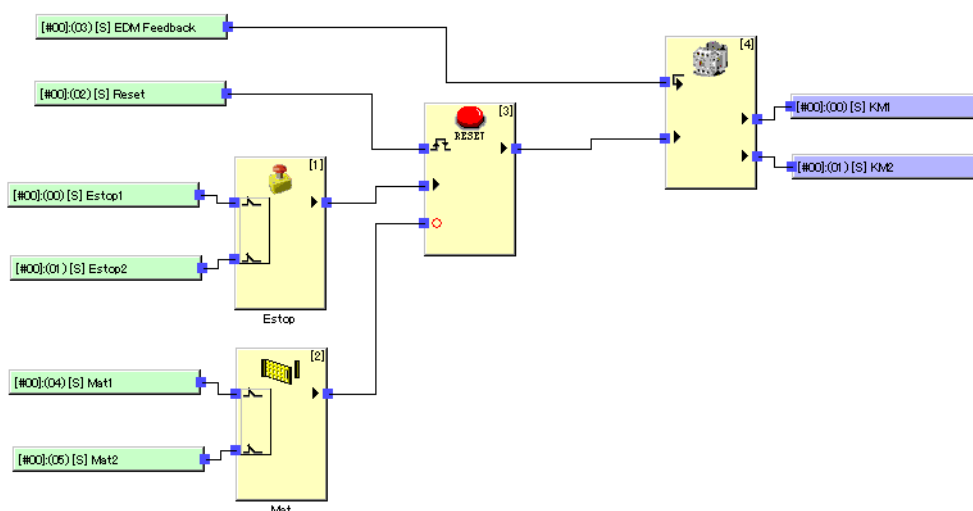
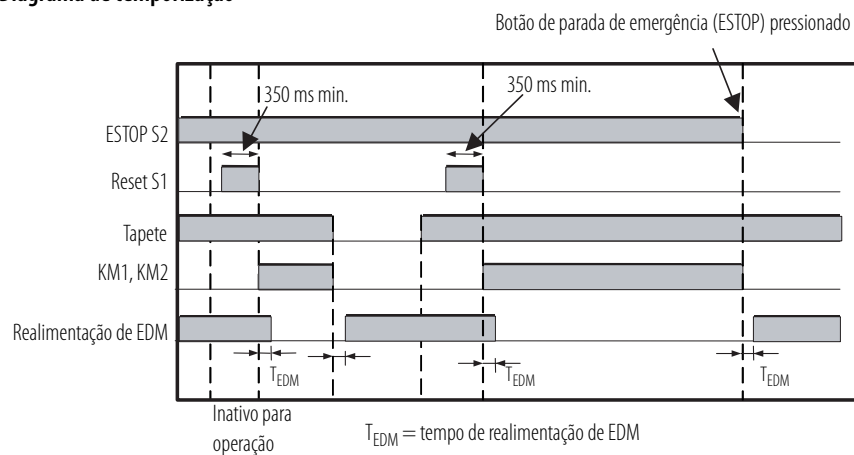


Aplicação de tapete de segurança

Este exemplo mostra um tapete de segurança de canal duplo com reset manual e uma chave de parada de emergência de canal duplo com reset manual. Como esta aplicação usa um relé MSR30RT/RTP, que tem suas próprias saídas e entradas de pulso, não é usada uma entrada de teste a partir do controlador SmartGuard.

Esquema elétrico

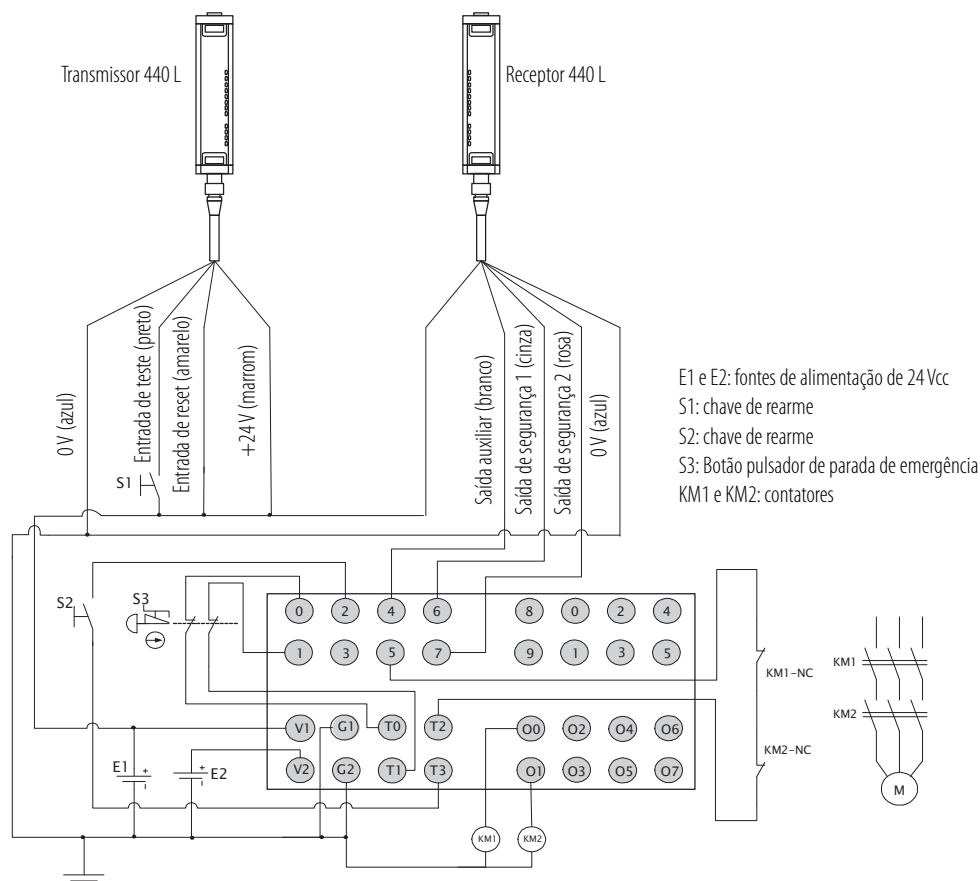


Configuração**Programação****Diagrama de temporização**

Aplicação de cortina de luz

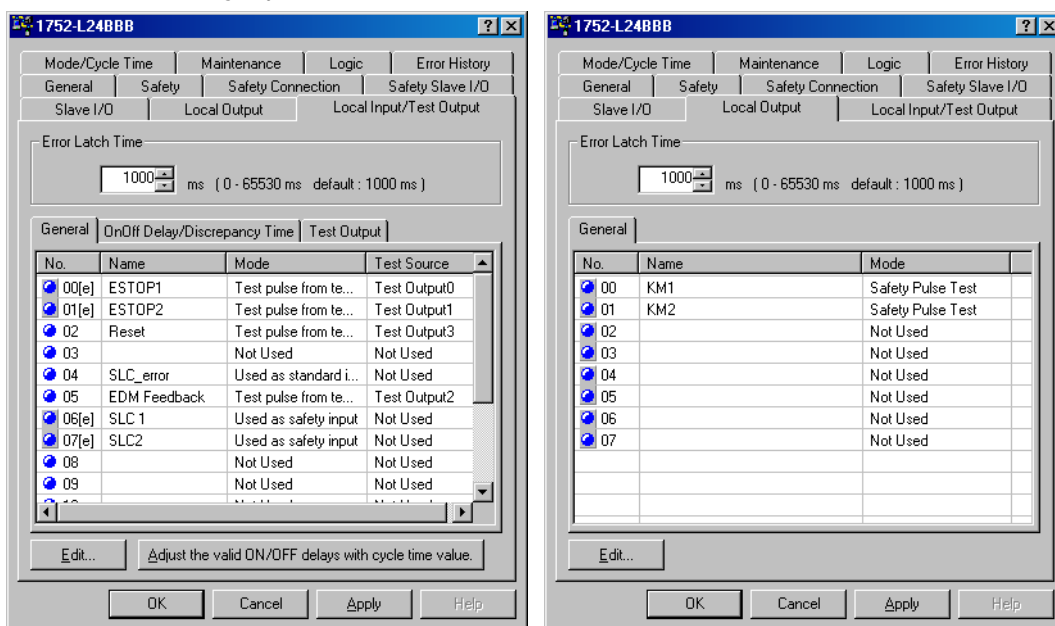
Este exemplo mostra uma cortina de luz de proteção de canal duplo com reset manual e uma chave de parada de emergência de canal duplo com reset manual.

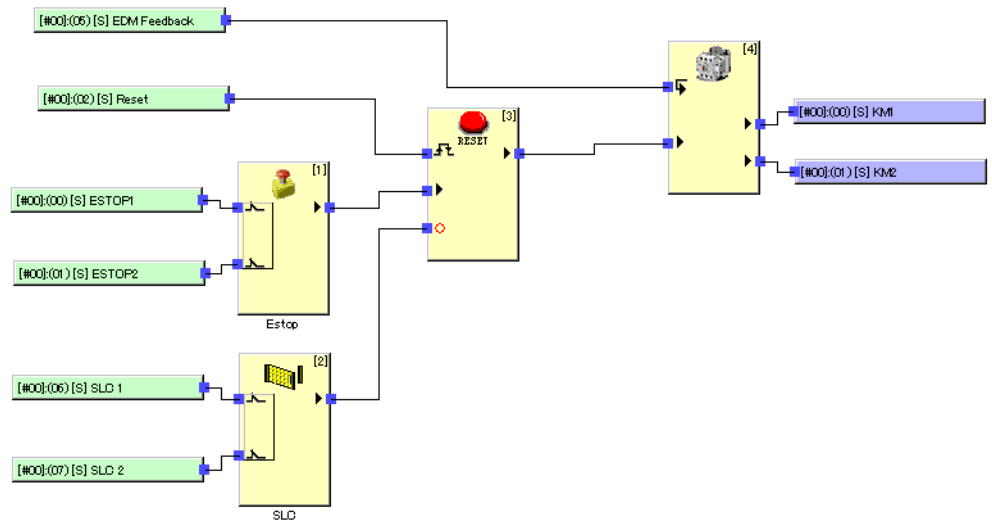
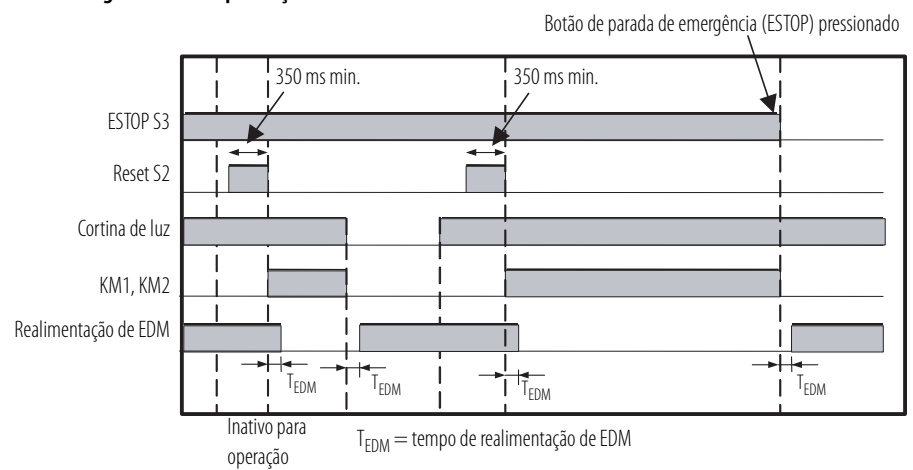
Esquema elétrico



Conecte uma fonte de alimentação de 24Vcc aos terminais V0 e G0, os terminais da fonte de alimentação dos circuitos internos.

Configuração



Programação**Diagrama de temporização**

Observações:

alteração de estado (COS)

Um tipo de comunicação de E/S padrão no qual o controlador pode enviar e receber dados com equipamentos escravos sempre que ocorrer uma alteração dos dados no equipamento escravo configurado ou no controlador. Os dados são atualizados na mesma taxa da pulsação.

assinatura da configuração

A combinação de um número de identificação, data e hora que identifica de maneira exclusiva uma configuração específica de um equipamento.

busoff

Status que ocorre quando a taxa de erros é extremamente alta em um cabo de comunicação. Um erro é detectado quando o contador de erros internos excede um valor-limite.

canal duplo

O uso de duas entradas ou saídas como sendo a entrada ou a saída para redundância.

canal duplo complementar

Uma configuração para avaliar se dois estados lógicos são complementares.

cíclico

Um tipo de comunicação de dados de E/S padrão em que o controlador pode enviar e receber dados com equipamentos escravos que suportam a função cíclica. Os dados só são enviados na taxa especificada pelo usuário.

com polling

Um tipo de comunicação de dados de E/S padrão em que uma mensagem com polling solicita uma resposta de um único equipamento especificado na rede (uma transferência de dados ponto a ponto).

E/S de segurança

A E/S de segurança tem a maior parte dos atributos da E/S padrão, exceto por fornecer mecanismos certificados para SIL 3 destinados à verificação da integridade dos dados e sua permanência.

equivalente a canal duplo

Uma configuração para avaliar se dois estados lógicos são equivalentes.

folha de dados eletrônica (EDS)

Um gabarito apresentado pelo fornecedor que o software RSNetWorx para DeviceNet usa para exibir os parâmetros de configuração, o perfil de dados de E/S e o suporte ao tipo de conexão de um determinado módulo DeviceNet ou DeviceNet Safety.

intervalo do pacote requisitado (RPI)

Ao se comunicar em uma rede, é a taxa esperada no tempo de produção de dados.

mensagens explícitas

Um tipo de mensagem usada para tarefas de prioridade menor como, por exemplo, a configuração e a monitoração de status.

microcomputador (PC)

Computador usado na interface com um sistema de controle por meio de um software de programação.

montagem

Dados internos de um equipamento reunidos como sendo um grupo a ser acessado externamente.

nó

O hardware que recebeu um endereço único na rede (também conhecido como equipamento ou módulo).

número de Rede de Segurança (SNN)

Identifica exclusivamente uma rede entre todas as redes no sistema de segurança. O usuário final é responsável por atribuir um número exclusivo para cada rede de segurança ou sub-rede de segurança dentro de um sistema. O SNN faz parte do Identificador de Nó Exclusivo (UNID).

padrão

Qualquer objeto, tarefa, tag, programa ou componente no projeto que não se trata de um item relacionado à segurança.

probabilidade de falha por hora (PFH)

A probabilidade de um sistema operacional apresentar uma falha grave por hora.

probabilidade de falha sob solicitação (PFD)

Média de probabilidade de um sistema operacional falhar ao executar sua função de projeto quando solicitado.

protocolo industrial comum (CIP)

Protocolo de comunicação criado para aplicações de automação industrial.

pulsada

Um tipo de comunicação de dados de E/S padrão em que uma mensagem solicita uma resposta de cada equipamento pulsado (uma transferência multicast). Trata-se de uma mensagem de 64 bits que contém 1 bit para cada equipamento escravo na rede.

Cada nó escravo pode retornar um máximo de 8 bytes em resposta ao estroboscópico do mestre.

pulso de teste

Um sinal usado para detectar quando a fiação externa entra em contato com a fonte de alimentação (positiva) ou para identificar curto-circuitos entre linhas de sinal.

tempo de discrepância

O período desde uma alteração feita em uma ou duas entradas até as demais alterações na entrada.

tempo de reação do sistema

O tempo da condição mais grave desde um evento relacionado à segurança como entrada no sistema ou como uma falha no sistema, até que o tempo no qual o sistema está esteja no estado de segurança. O Tempo de Reação do Sistema inclui Tempos de Reação do sensor e do ativado, além do Tempo de Reação do Controlador.

tempo de retenção do erro

O período de retenção de um estado de erro (inclusive os dados de controle relacionados, os dados de status e as indicações de status).

um de dois (1oo2)

Refere-se ao projeto comportamental de um sistema de segurança com vários processadores.

Observações:

A**assinatura da configuração** 45

- comparação 170
- componentes 45
- definição 45
- diferença 166

atraso na desenergização 69**atraso na energização** 69**B****baud rate**

- consulte faixa de comunicação

bloco de funções 71**BOOTP**

- configure o endereço IP 54
- use o utilitário Rockwell 55

botão on-line 164**C****categorias de erro** 184**comissionamento de nó** 42–43

- ferramenta 42

comunicação ponto a ponto 83**conexões multicast** 83**configuração**

- nós alvo do DeviceNet Safety 45
- parâmetros de segurança 80
- parâmetros padrão 82
- reset 46
- verificar 165–171

configurar um driver 42, 52**conversor de protocolos** 53**D****dados de status** 179

- entrada local 181
- gerais 180
- lâmpada muting 181
- saída de teste 181
- saída local 181

detecção de sobrecorrente

- origens de teste por pulso 74
- saídas 76

diferença

- assinatura da configuração 166
- SNN 67

E**E/S de segurança CIP**

- assinatura da configuração 45

endereço de nó 43

- alterações 67
- reset 46
- selecionar 26

endereço IP

- características gerais 53
- use BOOTP para configurar 54
- use o software RSLinx para configurar 57

equipamento desconhecido

- ícone 166

equipamento não encontrado

- ícone 166

especificações

- gerais 197

exemplos

- formação de ponte 61
- formação de ponte RSLinx 60, 62
- rede EtherNet/IP para uma porta USB 62
- rede EtherNet/IP para uma rede DeviceNet 60

F**faixa de comunicação**

- reset 46

falha na verificação 167**fazer download da configuração do****DeviceNet** 163–164**fazer upload e comparar**

- Safety Device Verification Wizard 168

G**guia Parameters** 82**guia Safety Configuration** 80**guia Safety Connections** 83**I****ícone**

- status do equipamento 166

identificador de nó exclusivo 63**indicador de status de rede**

- intermitente 204

intervalo do pacote requisitado

- definir 84
- e limite de tempo de reação da conexão 84

L**lâmpada muting**

dados de status 181

leituras de controle da conexão de entrada

reset 46

limite de tempo de reação da conexão 84

DeviceNet Safety I/O 84

e multiplicador de atraso da rede 85

locais

entradas 69–72

saídas 76–78

lógica

funções 145

M**máscara de sub-rede 53****mensagem explícita**

enviando 276

recebendo 273

restrições 277

mensagens de erro

alterações de modo 195

comunicação 188

entradas de segurança 191

erros de download 192

erros de reinicialização 194

falha no sistema 188

fonte de alimentação 190

saídas de segurança 191

saídas de teste 191

modo de canal duplo

entradas 69

saídas 76

módulo EtherNet/IP

formação de ponte 59

parâmetros de configuração 53

multiplicador de atraso de rede 85**multiplicador de tempo-limite 85****N****número de rede de segurança 63**

atribuição 65

atribuição automática 65

atribuição manual 65

automático 64

com base na hora 64

copiar 64

diferença 67

formatos 63

gerenciando 63

ícone de erro 166

manual 64, 65

reset 46, 67

O**origens de pulso de teste**

com entradas 69

com saídas 76

origens de teste por pulso 74**P****página Welcome 165****ponte 59****pronto para receber a trava de segurança 169****pronto para ser verificado 167****publicações relacionadas 13****R****rede**

ponte 59

rede DeviceNet

conectando-se 41, 51

configurar um driver 42, 52

rede EtherNet/IP

conecte a um computador 51

parâmetros 53

relatórios de verificação

relatório de falha 169

Safety Device Verification Wizard 169

reset

atributos de segurança 46

Configuration Owner 46

equipamento de segurança 46, 67

reset de segurança 46**RPI**

consulte o intervalo do pacote requisitado

S**Safety Device Verification Wizard** 47

- definição 165
- executar 165
- fazer upload e comparar 168
- página Welcome 165
- relatórios 169
- resumo 171
- selecionar equipamentos 167
- status do equipamento 166
- trava de segurança

scanner

- reset 67

senha

- caracteres válidos 48
- definir ou alterar 47
- esquecida 48
- operações protegidas 47
- reset 46, 48

software RSLinx

- configurando parâmetros de rede 57
- formação de ponte 60, 62

software RSLogix 5000

- perfil genérico de software 134

software RSNetWorx para DeviceNet

- comissionamento de nó 42

status

- indicadores 203

status do equipamento

- Safety Device Verification Wizard 166
- verificação 167

T**tela alfanumérica**

- identifique erros 208

tipos de driver 42, 52**trava**

- consulte trava de segurança

trava de segurança

- durante a reinicialização 47
- equipamentos
- ícone 166

U**utilitário Rockwell BOOTP** 55**V****verificação não suportada** 167**verificar**

- configuração de segurança do DeviceNet 165–171
- FALHA 169
- selecionar equipamentos 167

Suporte da Rockwell Automation

A Rockwell Automation fornece informações técnicas na Web para ajudar você a usar seus produtos. Em <http://support.rockwellautomation.com>, podem-se encontrar manuais técnicos, uma base de conhecimento de perguntas frequentes, observações técnicas e de aplicação, códigos de exemplo e links para service packs de software, e uma função MySupport que pode ser personalizada para ter o melhor uso destas ferramentas.

Para obter um nível adicional de suporte técnico por telefone para instalação, configuração e localização de falhas, oferecemos programas de suporte TechConnect. Para mais informações, entre em contato com o seu distribuidor local ou representante Rockwell Automation, ou visite <http://support.rockwellautomation.com>.

Assistência para instalação

Caso enfrente um problema nas primeiras 24 horas após a instalação, consulte as informações contidas neste manual. Também é possível ligar para um número especial de atendimento ao cliente para obter ajuda inicial para a instalação e a operação do produto.

Estados Unidos	1.440.646.3434 Segunda – Sexta, 8h – 17h EST
Fora dos Estados Unidos	Entre em contato com o representante local da Rockwell Automation em caso de problemas de suporte técnico.

Devolução do produto novo devido a falhas

A Rockwell Automation testa todos os seus produtos para assegurar que eles estejam completamente operacionais quando enviados das instalações industriais. No entanto, caso o produto não esteja funcionando e precise ser devolvido, siga estes procedimentos.

Estados Unidos	Entre em contato com o seu distribuidor. Você deve fornecer um número de ocorrência do atendimento ao cliente (ligue para o número de telefone acima para obter um) ao seu distribuidor para concluir o processo de devolução.
Fora dos Estados Unidos	Entre em contato com o representante local da Rockwell Automation para o procedimento de devolução.

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