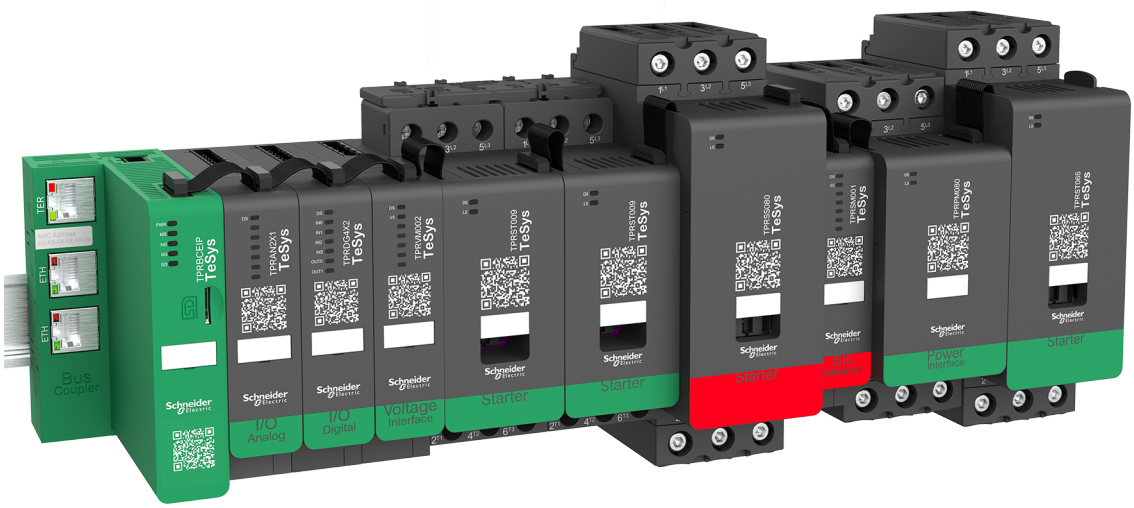
TeSys Ativo

TeSys™ island – Solução Digital de Gerenciamento de Motores

Guia de Segurança Funcional

A TeSys oferece soluções inovadoras e conectadas para partidas de motores**.**

8536IB1904PTBR-04
08/2023



www.schneider-electric.com

Informações legais

As informações fornecidas neste documento contêm descrições gerais, características técnicas e/ou recomendações relacionadas a produtos e soluções.

Este documento não se destina a substituir um estudo detalhado ou um plano esquemático ou de desenvolvimento operacional e específico do local. Não deve ser usado para determinar a adequação ou a confiabilidade dos produtos e soluções para aplicações específicas do usuário. É dever de todo usuário realizar ou fazer com que qualquer especialista profissional de sua escolha (integrador, especificador ou similar) realize a análise de risco, avaliação e teste adequados e abrangentes dos produtos e soluções com relação à aplicação específica relevante ou uso desses produtos e soluções.

A marca Schneider Electric e quaisquer marcas comerciais da Schneider Electric SE e suas subsidiárias mencionadas neste documento são de propriedade da Schneider Electric SE e de suas subsidiárias. Todas as outras marcas podem ser marcas registradas de seus respectivos proprietários.

Este guia e seu conteúdo são protegidos pelas leis de direitos autorais aplicáveis e fornecidos somente para fins informativos. Nenhuma parte deste guia pode ser reproduzida ou transmitida de qualquer forma ou por qualquer meio (eletrônico, mecânico, fotográfico, gravação ou outro), para qualquer finalidade, sem a permissão prévia por escrito da Schneider Electric.

A Schneider Electric não concede nenhum direito ou licença para uso comercial do documento ou de seu conteúdo, exceto para uma licença não exclusiva e pessoal para consultá-lo "no estado em que se encontra".

A Schneider Electric reserva o direito de fazer alterações ou atualizações em relação a ou no conteúdo deste documento ou no seu formato, a qualquer momento, sem aviso prévio.

Na medida permitida pela lei aplicável, a Schneider Electric e suas subsidiárias não assumem nenhuma responsabilidade ou obrigação por quaisquer erros ou omissões no conteúdo informativo deste documento ou consequências decorrentes do uso das informações aqui contidas.

Schneider Electric, Preventa e TeSys são marcas comerciais e de propriedade da Schneider Electric SE, suas subsidiárias e empresas afiliadas. Todas as outras marcas comerciais são de propriedade dos respectivos donos.

Índice analítico

Informações de segurança

Informações importantes

Leia estas instruções com atenção e analise o equipamento para se familiarizar com o dispositivo antes de tentar instalá-lo, operá-lo ou repará-lo. As mensagens especiais a seguir podem ser exibidas ao longo deste documento ou no equipamento para avisar sobre riscos potenciais ou chamar a atenção para informações que esclarecem ou simplificam um procedimento.

A adição desse símbolo a uma etiqueta de segurança de "Perigo" ou "Advertência" inc risco elétrico que resultará em ferimentos caso as instruções não sejam seguidas.

Este é o símbolo de alerta de segurança. Ele é usado para alertar você sobre possíve pessoas. Obedeça a todas as mensagens de segurança que se seguirem a este símb morte.

⚠ PERIGO

PERIGO indica uma situação de risco que, se não evitada, **resultará em** morte ou ferimentos graves.

⚠ ADVERTÊNCIA

ADVERTÊNCIA indica uma situação de risco que, se não evitada, **poderá resultar em** morte o ferimentos graves.

⚠ CUIDADO

CUIDADO indica uma situação de risco que, se não evitada, **poderá resultar** em ferimentos lev moderados.

AVISO

ATENÇÃO é usado para tratar de práticas não relacionadas a ferimentos.

Observações

Os equipamentos elétricos devem ser instalados, operados e reparados apenas por profissionais qualificados. A Schneider Electric não assume nenhuma responsabilidade por consequências do uso deste material.

Uma pessoa qualificada é aquela que tem habilidades e conhecimento relacionados à construção e operação de equipamentos elétricos e à sua instalação, e que recebeu treinamento em segurança para reconhecer e evitar os riscos envolvidos.

Sobre o guia

Escopo do documento

Use este documento para saber mais sobre os seguintes recursos de segurança funcional do TeSys™ island:

- compreensão geral
- principais aspectos a considerar
- desempenhos
- descrição do hardware
- configurações típicas
- exemplos de arquitetura
- referências de normas

Aviso de validade

Este guia é válido para todas as configurações do TeSys island. A disponibilidade de algumas funções descritas neste guia depende do protocolo de comunicação usado e dos módulos físicos instalados na TeSys island.

Para ver a conformidade do produto com diretivas ambientais, como RoHS, REACH, PEP e EOLI, acesse www.se.com/green-premium.

Para ver as características técnicas dos módulos físicos descritos neste guia, acesse www.se.com.

As características técnicas apresentadas neste guia devem ser as mesmas que aparecem on-line. Poderemos revisar o conteúdo ao longo do tempo para melhorar a clareza e a precisão. Se você notar uma diferença entre as informações contidas neste guia e as informações on-line, use as informações on-line.

Documentação relacionada

Título do documento	Descrição	Número do documento
TeSys island - Guia de sistema, instalação e operação	Descreve as principais funções, instalação mecânica, fiação, comissionamento do TeSys island e como operar e manter TeSys island.	DOCA0270PTBR
TeSys island - EtherNet/IP™ - Guia de início rápido e da biblioteca de blocos de funções	Descreve como integrar o TeSys island e as informações da biblioteca do TeSys island usadas no ambiente EtherNet/IP do Rockwell Software® Studio 5000®.	DOCA0271PTBR
TeSys island - Guia de segurança funcional	Descreve os recursos de segurança funcional do TeSys island.	8536IB1904PTBR
TeSys island - Guia do bloco de funções de terceiros	Contém as informações necessárias para criar blocos funcionais para hardware de terceiros.	8536IB1905PTBR
TeSys island - Guia de ajuda on-line do DTM	Descreve como instalar e usar diferentes funções do software de configuração do TeSys island e como configurar os parâmetros do TeSys island.	8536IB1907PT
TeSys island - Perfil ambiental do produto	Descreve os materiais usados na fabricação, o potencial de reciclagem e as informações de impacto ambiental do TeSys island.	ENVPEP1904009
TeSys island - Instruções sobre o final da vida útil do produto	Contém instruções sobre o fim da vida útil do TeSys island.	ENVEOLI1904009
TeSys island - Folha de instruções, interface de rede, TPRBCEIP	Descreve como instalar a interface de rede Ethernet/IP do TeSys island	MFR44097
TeSys island - Folha de instruções, interface de rede, TPRBCPFN	Descreve como instalar a interface de rede PROFINET do TeSys island	MFR44098
TeSys island - Folha de instruções, interface de rede, TPRBCPFB	Descreve como instalar a interface de rede PROFIBUS DP do TeSys island	GDE55148
TeSys island – Folha de Instruções, Partidas e Módulos de Interface de Potência, Tamanhos 1 e 2	Descreve como instalar as partidas e os módulos de interface de potência tamanhos 1 e 2 do TeSys island.	MFR77070
TeSys island – Folha de Instruções, Partidas e Módulos de Interface de Potência, Tamanho 3	Descreve como instalar as partidas e os módulos de interface de potência tamanho 3 do TeSys island.	MFR77085
TeSys island - Folha de instruções: Módulos de entrada/saída	Descreve como instalar os módulos de E/S analógica e digital do TeSys island	MFR44099
TeSys island - Folha de instruções: Módulos de Interface SIL e de Interface de Tensão	Descreve como instalar os módulos de interface de tensão e os módulos de interface SIL[1] do TeSys island.	MFR44100

1. Nível de integridade de segurança de acordo com a norma IEC 61508.

Terminologia derivada de normas

Os termos técnicos, a terminologia e as descrições correspondentes neste guia normalmente utilizam os termos ou as definições das normas relevantes. Essas normas incluem, entre outras:

- **EN ISO 13849-1:** Segurança de máquinas – Peças de sistemas de controle relacionados à segurança – Parte 1: Princípios gerais de projeto
- **EN ISO 13849-2:** Segurança de máquinas – Peças de sistemas de controle relacionados à segurança – Parte 2: Validação
- **IEC 61508:** Segurança funcional de sistemas elétricos/eletrônicos/eletrônicos programáveis relacionados à segurança
- **EN 62061:** Segurança de máquinas – Segurança funcional de sistemas de controle elétricos, eletrônicos e eletrônicos programáveis relacionados à segurança
- **IEC 61511:** Segurança funcional – Sistemas instrumentados de segurança para o setor da indústria de processos
- **EN/IEC 60204-1:** Segurança de máquinas – Equipamentos elétricos de máquinas – Parte 1: Requisitos gerais
- **IEC 61000-6-7:** Compatibilidade eletromagnética (EMC) – Parte 6-7: Normas genéricas – Requisitos de imunidade para equipamentos destinados a executar funções em um sistema relacionado à segurança (segurança funcional) em locais industriais
- **IEC 60664-5:** Coordenação de isolamento para equipamentos dentro de sistemas de baixa tensão – Parte 5: Método abrangente para determinar vãos livres e distâncias de fuga iguais ou menores que 2 mm
- **IEC 60947-4-1:** Equipamentos de distribuição e mecanismos de controle de baixa tensão – Parte 4-1: Contatores e partidas de motores – Contatores e partidas de motores eletromecânicos
- **IEC 60947-5-1:** Equipamentos de distribuição e mecanismos de controle de baixa tensão – Parte 5-1: Dispositivos de circuito de controle e elementos de comutação – Dispositivos eletromecânicos de circuito de controle
- **IEC 60947-7-1:** Equipamentos de distribuição e mecanismos de controle de baixa tensão – Parte 7-1: Equipamentos auxiliares – Blocos de terminal para condutores de cobre
- **IEC 60947-7-2:** Equipamentos de distribuição e mecanismos de controle de baixa tensão – Parte 7-2: Equipamentos auxiliares – Blocos de terminal de condutor de proteção para condutores de cobre
- **EN 50205:** Relés com contatos de orientação forçada (vinculados mecanicamente)
- **IEC TR 62380:** Manual de dados sobre confiabilidade – Modelo universal para previsão de confiabilidade de componentes eletrônicos, PCBs e equipamentos

Terminologia de segurança funcional

ATTENTION

A terminologia de segurança funcional utilizada neste guia é definida a seguir.

Termo	Norma	Definição
Tolerância a falhas	IEC 61511-1	Capacidade de um item funcional de continuar a execução de uma função exigida na presença de falhas ou erros
Segurança funcional	IEC 61508-4	Parte da segurança geral relacionada ao Equipamento sob controle (EUC – do inglês Equipment Under Control) e ao controle do EUC que depende do funcionamento correto dos sistemas elétricos/eletrônicos/eletrônicos programáveis (E/E/PE) relacionados à segurança e outras medições de redução de riscos
Falha de segurança	IEC 61508-4	Falha de um elemento e/ou subsistema e/ou sistema que tem um papel na implementação da função de segurança que: 1. resulta na operação falsa da função de segurança para colocar o EUC[2] (ou parte dele) em modo seguro ou manter um estado seguro; ou 2. aumenta a probabilidade da operação falsa da função de segurança para colocar o EUC[2] (ou parte dele) em modo seguro ou manter um estado seguro.
Fração de falha de segurança	IEC 61508-4	A proporção da taxa de falhas de segurança em relação à taxa total de falhas do sistema.
Estado seguro	IEC 61511-1	Estado do processo quando a segurança é atingida
	IEC 61800-5-2	Estado dos PDS(SR)[3] quando a segurança é atingida
Parada segura	IEC 61800-5-2	As funções Parada segura são definidas como: • **Safe Torque Off (STO)** ◦ Esta função impede que a energia produtora de força (ou torque) seja fornecida ao motor. ◦ Essa *subfunção de segurança* corresponde a uma parada não controlada de acordo com a categoria de parada 0 da IEC 60204-1. • **Parada segura 1 (SS1)** ◦ Parada segura 1 - desaceleração controlada: SS1-d inicia e controla a taxa de desaceleração do motor dentro de limites selecionados para parar o motor e executa a função STO (consulte 4.2.3.2) quando a velocidade do motor está abaixo de um limite especificado; ou ◦ Parada segura 1 - elevação monitorada: SS1-r e inicia e monitora a taxa de desaceleração do motor dentro de limites selecionados para parar o motor e executa a função STO quando a velocidade do motor está abaixo de um limite especificado; ou ◦ Parada segura 1 - tempo controlado SS1-t inicia a desaceleração do motor e executa a função STO após um atraso de tempo específico da aplicação.
Função de segurança	IEC 61800-5-2	Função a ser implementada por um sistema relacionado à segurança ou outras medições de redução de riscos que se destina a atingir ou manter um estado seguro para o equipamento ou maquinário acionado por PDS (SR)[3], em relação a um evento perigoso específico
Nível de integridade de segurança (SIL)	IEC 61508	A norma IEC 61508 define quatro Níveis de integridade de segurança (SIL) para funções de segurança: SIL 1 é o nível de integridade mais baixo, e SIL 4 é o mais elevado.

2. EUC: equipamento sob controle
3. Sistemas de acionamento de energia relacionados à segurança

Termo	Norma	Definição
		Uma análise e avaliação de riscos serve de base para determinar o nível de integridade de segurança exigido.
Sistema relacionado à segurança	IEC 61800-5-2	Sistema designado que • implementa as funções de segurança exigidas, necessárias para atingir ou manter um estado seguro para o equipamento ou maquinário acionado por PDS(SR)[4]; e • destina-se a atingir, por conta própria ou com outras medições de redução de riscos, a integridade de segurança necessária para as funções de segurança exigidas
Subsistema	IEC 61800-5-2	Parte do projeto arquitetônico de nível superior de um sistema relacionado à segurança; sua falha resulta na falha de uma função relacionada à segurança

Declaração de conformidade com a CE

As Declarações de conformidade com a CE para o TeSys™ island podem ser obtidas em www.schneider-electric.com.

4. Sistemas de acionamento de energia relacionados à segurança

Precauções

Leia e compreenda as seguintes precauções antes de executar qualquer procedimento deste guia.

⚠⚠PERIGO

RISCO DE CHOQUE ELÉTRICO, EXPLOSÃO OU ARCO VOLTAICO

- A instalação e a manutenção deste equipamento devem ser realizadas apenas por profissionais eletricistas qualificados.
- Desligue toda a energia que alimenta este equipamento antes de trabalhar no equipamento ou dentro dele.
- Use somente a tensão indicada ao operar este equipamento e qualquer produto associado.
- Sempre use um dispositivo de detecção de tensão apropriado para confirmar que a alimentação está desligada.
- Use os intertravamentos apropriados onde houver riscos para pessoas e/ou equipamentos.
- Os circuitos do ponto de energia devem ser conectados e protegidos em conformidade com os requisitos regulamentares locais e nacionais.
- Use equipamentos de proteção individual (EPI) apropriados e siga as práticas de trabalho seguro com eletricidade conforme a NFPA 70E, a NOM-029-STPS ou a CSA Z462, ou equivalente local, como a NR-10 e NR-12, no caso do Brasil.

O não cumprimento destas instruções poderá resultar em morte ou ferimentos graves.

⚠ATENÇÃO

OPERAÇÃO NÃO INTENCIONAL DO EQUIPAMENTO

- Para obter instruções completas sobre a segurança funcional, consulte o Guia de Segurança Funcional do TeSys™ island, 8536IB1904
- Não desmonte, repare nem modifique este equipamento. Não há peças que possam ser reparadas pelo usuário.
- Instale e opere este equipamento em um gabinete devidamente classificado para o ambiente de aplicação previsto.
- Cada implementação deste equipamento deve ser testada de forma individual e exaustiva para avaliar a operação adequada do produto antes de ser colocado em serviço.

O não cumprimento destas instruções poderá resultar em morte, ferimentos graves ou danos do equipamento.

⚠ **AVISO:** Este produto pode expor você a produtos químicos, incluindo óxido de antimônio (trióxido de antimônio), que é conhecido no estado da Califórnia por causar câncer. Para obter mais informações, acesse www.P65Warnings.ca.gov.

Funcionários qualificados

Somente pessoas treinadas adequadamente que estejam familiarizadas e entendam o conteúdo deste guia e de todas as outras documentações relacionadas ao produto estão autorizadas a trabalhar com ele.

A pessoa qualificada deve ser capaz de detectar possíveis riscos que surjam da modificação de valores de parâmetros e, em geral, de equipamentos mecânicos, elétricos ou eletrônicos. A pessoa qualificada deve estar familiarizada com os padrões, as provisões e as regulamentações para a prevenção de acidentes industriais, que devem observar ao projetar e implementar o sistema.

O uso e a aplicação das informações contidas neste guia exigem conhecimento do projeto e da programação de sistemas de controle automatizados. Somente você, o usuário, o fabricante da máquina ou o integrador pode estar ciente de todas as condições e fatores presentes durante a instalação, a configuração, a operação e a manutenção da máquina ou do processo e, portanto, deve determinar a automação e os equipamentos associados, bem como os dispositivos de segurança e intertravamentos relacionados, que devem ser usados de forma eficaz e adequada.

Ao selecionar equipamentos de automação e controle, e qualquer outro equipamento ou software relacionado, para uma aplicação específica, você também deve considerar as normas e/ou regulamentações locais, regionais ou nacionais aplicáveis.

Preste especial atenção à conformidade com quaisquer informações de segurança, requisitos elétricos e padrões normativos aplicáveis à sua máquina ou processo no uso deste equipamento.

Uso previsto

Os produtos descritos neste guia, juntamente com o software, os acessórios e os opcionais, são partidas de cargas elétricas de baixa tensão destinadas ao uso industrial de acordo com as instruções, as diretrizes, os exemplos e as informações de segurança contidas neste documento e em outras documentações de apoio.

O produto só pode ser usado em conformidade com todos os regulamentos e diretivas de segurança aplicáveis, os requisitos especificados e os dados técnicos.

Antes de usar o produto, você deve executar uma análise de risco e uma avaliação de risco da aplicação planejada. Com base nos resultados, medições apropriadas relacionadas à segurança devem ser implementadas.

Como o produto é usado como um componente de uma máquina ou um processo, você deve garantir a segurança das pessoas por meio do projeto geral do sistema.

Opere o produto apenas com os cabos e acessórios especificados. Use apenas acessórios e peças de reposição originais.

Qualquer uso que não seja o uso explicitamente permitido é proibido e pode resultar em perigos imprevistos.

Visão geral de segurança funcional do TeSys™ island

Linha principal: TeSys

O TeSys™ é uma solução inovadora de controle e gerenciamento de motores da líder global do mercado. TeSys oferece produtos e soluções conectados e eficientes para comutação e proteção de motores e cargas elétricas em conformidade com todas as principais normas elétricas globais.

Conceito de TeSys island

O TeSys island é um sistema modular e multifuncional que fornece funções integradas em uma arquitetura de automação, essencialmente para o controle direto e o gerenciamento de cargas de baixa tensão. O TeSys island pode comutar, ajudar a proteger e gerenciar motores e outras cargas elétricas de até 80 A (AC1) instalados em um painel de controle elétrico.

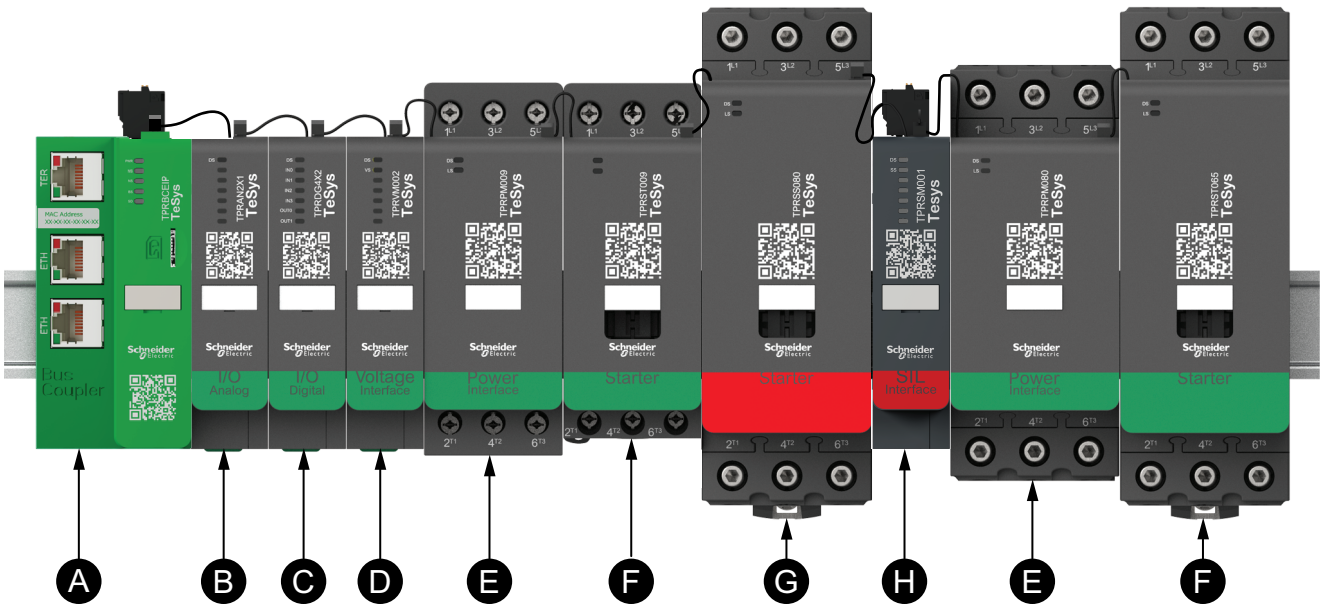
Esse sistema foi projetado com base no conceito de TeSys avatars. Estes avatars:

- Representam os aspectos lógicos e físicos das funções de automação
- Determine a configuração do TeSys island

Os aspectos lógicos da TeSys island são gerenciados com ferramentas de software, abrangendo todas as fases do produto e o ciclo de vida da aplicação: projeto, engenharia, comissionamento, operação e manutenção.

A TeSys island física consiste em um conjunto de dispositivos instalados em um único trilho DIN e conectados com cabos planos para fornecer a comunicação interna entre os módulos. A comunicação externa com o ambiente de automação é feita por meio de um único módulo de interface de rede e a TeSys island é considerada como um nó único na rede. Os outros módulos incluem partidas, módulos de interface de potência, módulos de E/S analógicos e digitais, módulos de interface de tensão e módulos de interface SIL (Nível de integridade de segurança, de acordo com o padrão IEC 61508), abrangendo uma ampla variedade de funções operacionais.

Figura 1 - Visão geral do TeSys island



A	Interface de rede	E	Módulo de interface de potência
B	Módulo de E/S analógico	F	Partida convencional
C	Módulo de E/S digital	G	Partida SIL
D	Módulo de interface de tensão	H	Módulo de interface SIL

Segurança funcional no TeSys island

O TeSys™ island fornece avatares e dispositivos físicos específicos para criar configurações para funções de Categoria de parada 0 e Categoria de parada 1, de acordo com a EN/IEC 60204-1. Os avatares do TeSys são representações digitais dos módulos físicos na ilha. No entanto, a função de segurança do TeSys island depende apenas de componentes de hardware eletromecânicos. Os dispositivos específicos são a partida SIL[5] e o módulo de interface SIL. Outro conceito importante é o grupo SIL: um conjunto de avatares que são associados a um módulo de interface SIL e seguem a mesma função de segurança. Uma ilha pode conter vários grupos SIL.

O TeSys island deve ser integrado a outros elementos relacionados à segurança em um sistema relacionado à segurança mais amplo para ajudar a garantir a segurança funcional de uma máquina ou de um sistema/processo.

5. Nível de integridade de segurança de acordo com a norma IEC 61508.

Características de segurança funcional do TeSys island

O TeSys™ island oferece recursos de segurança em conformidade com as seguintes condições específicas:

Normas e características certificadas

O TeSys island segue as seguintes diretivas e normas:

- Diretiva de máquinas 2006/42/CE:
  - EN ISO 13849-1: 2015
  - EN 62061: 2016 ou IEC 62061: 2015 (edição 1.2)
- Segurança funcional de sistemas elétricos/eletrônicos/eletrônicos programáveis relacionados à segurança: IEC 61508 edição 2: 2010
- Segurança funcional – Sistemas instrumentados de segurança para o setor da indústria de processos: IEC 61511 edição 2: 2016
- As funções de Categoria de parada 0 e Categoria de parada 1 do TeSys island seguem a EN/IEC 60204-1.

Em monocanal, os desempenhos mais altos dessas funções são:

- Categoria 2 com Nível de desempenho “d” em conformidade com a EN ISO 13849-1
- SIL[6] Capacidade 2 em conformidade com a IEC 61508 Ed 2 e a IEC 61511 Ed 2
- Capacidade SIL CL 2 em conformidade com a EN 62061 Ed 1

Em duplo canal, os desempenhos mais altos dessas funções são:

- Categoria 4 com Nível de desempenho “e” em conformidade com a EN ISO 13849-1
- Capacidade SIL 3 em conformidade com a IEC 61508 Ed 2 e a IEC 61511 Ed 2
- Capacidade SIL CL 3 em conformidade com a EN 62061: 2016 ou IEC 62061: 2015 (edição 1.2)

O TeSys island foi projetado para dar suporte a diferentes níveis de desempenho de segurança funcional e de integridade de segurança, dependendo de sua arquitetura de fiação, e é compatível com as características de segurança funcional descritas na tabela a seguir.

Tabela 1 - Características de segurança funcional

Função	Função de parada relacionada à segurança
Posição de fallback	Contator aberto
Tempo de resposta (pior cenário)	145 ms
Categoria de parada EN/IEC 60204-1	Cat. 0/Cat. 1
Diretiva de máquinas	Sim

6. Nível de integridade de segurança de acordo com a norma IEC 61508.

Tabela 1 - Características de segurança funcional (Continuação)

Arquitetura de sistema do TeSys island	Monocanal	Duplo canal
Nível de desempenho EN ISO 13849-1	PL c, d	PL c, d, e
Categoria de fiação ISO 13849-1	Cat. 1, 2	Cat. 3, 4
SIL CL EN 62061	SIL CL 2	SIL CL 3
SIL IEC 61508/IEC 61511	SIL 2	SIL 3

O certificado de segurança funcional pode ser acessado em www.se.com/tesys/.

NOTA: Para essa certificação, apenas um TeSys island será considerado para uso em aplicações relacionadas à segurança, não ao sistema completo ao qual ele é integrado para ajudar a garantir a segurança funcional de uma máquina ou um sistema/processo.

Condições de operação

O TeSys island foi projetado para suportar as condições a seguir. Outras condições podem ser aplicáveis a módulos específicos, conforme descrito em suas respectivas folhas de dados disponíveis em www.se.com/tesys-island.

- 40 °C (104 °F) de temperatura ambiente
- Motor de 400 ou 480 V
- Umidade de 50%
- Carga de 80%
- Orientação de montagem horizontal
- Todas as entradas ativadas
- Todas as saídas ativadas
- Funcionamento 24 horas/dia, 365 dias/ano

Arquitetura monocanal (ISO 13849)

O TeSys island é aplicável a arquiteturas monocanal nas quais uma falha detectada pode levar à perda da função de segurança.

Arquitetura de duplo canal (ISO 13849)

O TeSys island é aplicável a arquiteturas de duplo canal nas quais uma única falha detectada (incluindo falhas de modo comum) não leva à perda da função de segurança.

Categorias de parada (EN/IEC 60204-1)

A categoria de parada está relacionada à forma como a carga acionada é desenergizada e depende do subsistema relacionado à segurança externa que aciona a função de parada. Um subsistema relacionado à segurança externa pode ser implementado com dispositivos como os módulos Preventa™ XPS.

Categoria de parada 0

A Categoria de parada 0 é definida como a parada da movimentação da máquina pela remoção imediata da energia elétrica dos mecanismos da máquina. A Categoria de parada 0 é uma parada não controlada.

Categoria de parada 1

A Categoria de parada 1 é definida como a parada da movimentação da máquina com a energia elétrica mantida para os mecanismos da máquina durante o processo de parada. A energia é removida quando a parada é concluída. A Categoria de parada 1 é uma parada controlada.

Categorias de fiação[7]

As categorias de fiação se relacionam à forma como o módulo Preventa™ XPS externo (ou equivalente) é cabeado e ao nível adicional associado de controle da função de segurança.

Categoria de fiação 1

Uma única falha detectada pode levar à perda da função de segurança, e não é necessária cobertura de diagnóstico.

O sensor relacionado à segurança pode ser cabeado diretamente às entradas SIL-IN/SIL Common.[8] As entradas Mirror In/Mirror Out não são usadas. Para obter mais informações sobre a fiação das entradas SIL-IN/SIL Common, consulte Sensor relacionado à segurança, página 24.

Categoria de fiação 2

O sensor relacionado à segurança é cabeado a um módulo Preventa XPS (ou equivalente). As saídas do módulo Preventa XPS (ou equivalente) são cabeadas às entradas SIL-IN/SIL Common do módulo de interface SIL[8].

Para atender aos requisitos da Categoria 2, o feedback do contato espelho (Mirror In/Mirror Out) deve ser monitorado com um módulo Preventa XPS (ou equivalente) que execute o monitoramento de diagnóstico externo do contato espelho. Se o contato espelho não for aberto na parada, o próximo reinício será bloqueado para todas as partidas SIL do grupo SIL.

Implementando o monitoramento indireto para a Categoria 2

Para atingir os requisitos da categoria 2 para cobertura de diagnóstico (DC > 60%), o monitoramento externo do status do grupo deve ser implementado para acionar um mecanismo secundário que pare a máquina (desarme de disjuntor, etc.) ou impeça o acesso a áreas perigosas (cadeados).

7. Categorias de fiação 1 e 2 de acordo com a ISO 13849.
8. Nível de integridade de segurança de acordo com a norma IEC 61508.

Cada grupo SIL[9] tem cinco estados associados a ele para indicar o estado operacional. O estado 0 indica que não há nenhum grupo SIL presente no slot. O TeSys island dá suporte para até 10 grupos SIL na ilha.

Status do grupo SIL para a função de Parada SIL:

- 0 = Grupo SIL não presente na configuração do sistema
- 1 = Grupo SIL afetado por Evento de dispositivo do avatar
- 2 = Comando de parada recebido, partidas SIL ainda não abertas
- 3 = Comando de parada executado com êxito, todas as partidas SIL estão abertas
- 4 = Comando de parada executado para apenas um módulo de interface SIL (SIM) (o barramento jumper ou a fiação da entrada do SIM está causando um problema), mas as partidas SIL foram abertas com êxito
- 5 = Operação normal, as partidas SIL podem estar abertas ou fechadas

O estado 5 é o estado em regime normal, e o estado 3 é o estado de Parada SIL normal. O estado 1 indica um problema de firmware ou comunicação com uma partida SIL. Os estados 2 e 4 indicam problemas relacionados à Parada SIL com a fiação do SIM, das partidas SIL ou da Parada SIL. O monitoramento indireto deve procurar pelos estados 2 ou 4 que persistem por mais tempo do que o de acionamento de uma Parada SIL e usar as informações de status para acionar um mecanismo secundário que pare a máquina (SIB de disjuntor, etc.).

Para ler o status do grupo SIL, o monitoramento externo deve usar o bloco de funções SystemDiagnostics. Cada grupo SIL do sistema tem uma saída nesse bloco de funções para o status de seu grupo SIL, etiquetada no bloco de funções como “SILStarterStopMsgGrp *n*”, onde *n* é o número do grupo SIL na ilha. O status do grupo SIL segue a enumeração mostrada acima.

Monitoramento de diagnóstico

Uma vez que o monitoramento de diagnóstico ocorre imediatamente com a demanda da função de segurança, o tempo total para detectar a falha e colocar a máquina em condição sem risco deve ser menor do que o tempo até atingir a área perigosa.

De acordo com a ISO 13849-2, 9.2.3, para a Categoria 2: O $MTTF_d$[10] do equipamento de monitoramento deve ser superior à metade do $MTTF_d$ da lógica. A contribuição do TeSys island para o $MTTF_d$ do monitoramento de diagnóstico é $MTTF_d > 100$ anos.

Categoria de fiação 3

Uma única falha não levará à perda da função de segurança e, sempre que praticável, a falha única deverá ser detectada na ou antes da próxima demanda da função de segurança.

Para atender aos requisitos da Categoria 3, o feedback do contato espelhado (Mirror In/Mirror Out) deve ser monitorado com um módulo Preventa XPS (ou equivalente) que execute o monitoramento de diagnóstico externo do contato espelhado da partida SIL[9]. Se o contato espelho não for aberto na parada, o próximo reinício será bloqueado para todas as partidas SIL no grupo SIL. O sensor relacionado à segurança é cabeado a um módulo Preventa XPS (ou equivalente). As saídas do módulo Preventa XPS (ou equivalente) são cabeadas às entradas SIL-IN/SIL Common do módulo de interface SIL.

Em caso de monitoramento indireto, o monitoramento externo do status do grupo deve procurar pelos estados 2 ou 4 para persistir por mais tempo do que o tempo de acionamento de uma parada SIL. Use as informações de status para bloquear o próximo reinício das partidas SIL do grupo.

9. Nível de integridade de segurança de acordo com a norma IEC 61508.
10. Tempo médio até uma falha perigosa conforme definido na ISO 13849-1.

Categoria de fiação 4

Uma única falha não levará à perda da função de segurança. A falha única é detectada na ou antes da próxima demanda da função de segurança. Se essa detecção não for possível, um acúmulo de falhas não detectadas não deverá levar à perda da função de segurança.

Para atender aos requisitos da Categoria 4, o feedback do contato espelhado (Mirror In/Mirror Out) deve ser monitorado com um módulo Preventa XPS (ou equivalente) que execute o monitoramento de diagnóstico externo do contato espelhado da partida SIL[11]. Se o contato espelho não for aberto na parada, o próximo reinício será bloqueado para todas as partidas SIL no grupo SIL. O sensor relacionado à segurança é cabeado a um módulo Preventa XPS (ou equivalente). As saídas do módulo Preventa XPS (ou equivalente) são cabeadas às entradas SIL-IN/SIL Common do módulo de interface SIL.

Teste de aceitação

O integrador de sistemas/fabricante de máquinas deve realizar um teste de aceitação da função de segurança para verificar e documentar sua funcionalidade correta. Dessa forma, o integrador de sistemas/fabricante de máquinas certifica que testou a eficácia das funções de segurança utilizadas. O teste de aceitação deve ser realizado com base na análise e avaliação de riscos. No caso do modo de baixa demanda com categoria 4, a função de segurança deve ser testada ao menos uma vez por mês. Todas as normas e regulamentações aplicáveis devem ser observadas.

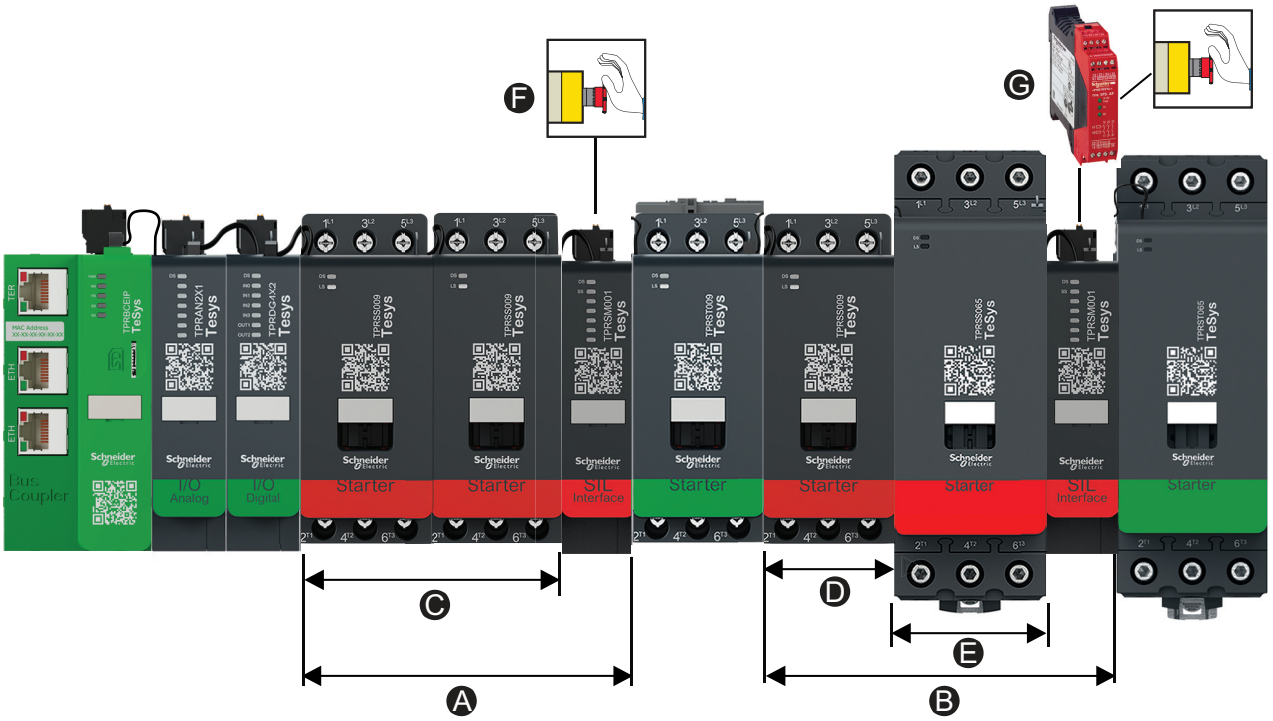
11. Nível de integridade de segurança de acordo com a norma IEC 61508.

Conceitos e componentes

Estrutura típica do TeSys™ island

A ilustração a seguir mostra um exemplo de TeSys™ island composto por dois grupos SIL[12]. A composição da ilha é definida pelas ferramentas digitais do TeSys, de acordo com as necessidades funcionais indicadas pelo usuário.

Figura 2 - TeSys island com dois grupos SIL



A	Grupo SIL 1	E	Avatar A4
B	Grupo SIL 2	F	Categoria de fiação 1, Categoria de parada 0[13]
C	Avatar A1	G	Categoria de fiação 2, Categoria de parada 1[14]
D	Avatar A3		

Grupo SIL 1: inclui um avatar com duas partidas SIL; por exemplo, um avatar “Motor com dois sentidos de rotação – Parada SIL, Cat. W. 1/2” (Avatar A1). O motor real é cabeado a essas partidas SIL e segue a lógica do avatar e os comandos operacionais vindos do PLC através da rede de campo. O comando de parada SIL vem do botão de parada de emergência cabeado ao módulo de interface SIL (Categoria de fiação 1) e faz com que as partidas SIL desenergizem a carga e entrem no estado seguro (o contator é aberto e o motor é desenergizado).

Grupo SIL 2: inclui dois avatares, por exemplo, um “Contator - Parada SIL, Cat. W. 1/2" (Avatar A3) e um “Motor com um sentido de rotação - Parada SIL, Cat. W. 1/2" (Avatar A4), cada um deles composto por uma única partida SIL. Ambos os

12. Nível de integridade de segurança de acordo com a norma IEC 61508.
13. Categoria de fiação 1 de acordo com a ISO 13849. Categoria de parada 0 de acordo com a EN/IEC 60204-1.
14. Categoria de fiação 2 de acordo com a ISO 13849. Categoria de parada 1 de acordo com a EN/IEC 60204-1.

avatares seguem a lógica do avatar e os comandos operacionais vindos do PLC através da rede de campo. O comando de parada SIL vem do módulo Preventa™ XPS externo (ou equivalente) cabeado ao módulo de interface SIL e faz com que as partidas SIL desenergizem a carga e entrem no estado seguro (Categoria de fiação 2).

Grupo SIL

Um grupo SIL[15] é composto por um ou mais avatares SIL, todos atribuídos a um único módulo de interface SIL. Todos os avatares SIL do grupo SIL reagem a um único comando de parada SIL. O módulo de interface SIL é sempre instalado à direita da última partida SIL incluída no grupo SIL (na extremidade da interface de rede).

Uma ilha pode incluir vários grupos SIL.

Avatares SIL

Os avatares SIL[15] disponíveis para as funções de Parada SIL são:

- Contator - Parada SIL, Cat. W. 1/2
- Contator - Parada SIL, Cat. W. 3/4
- Motor com um sentido de rotação - Parada SIL, Cat. W. 1/2
- Motor com um sentido de rotação - Parada SIL, Cat. W. 3/4
- Motor com dois sentidos de rotação - Parada SIL, Cat. W. 1/2
- Motor com dois sentidos de rotação - Parada SIL, Cat. W. 3/4
- Motor de duas velocidades - Parada SIL, Cat. W. 1/2
- Motor de duas velocidades - Parada SIL, Cat. W. 3/4
- Motor de duas velocidades e com dois sentidos de rotação - Parada SIL, Cat. W. 1/2
- Motor de duas velocidades e com dois sentidos de rotação - Parada SIL, Cat. W. 3/4
- Transportador com um sentido de rotação - Parada SIL, Cat. W. 1/2
- Transportador com dois sentidos de rotação - Parada SIL, Cat. W. 3/4

Os avatares SIL consistem em dispositivos de hardware específicos, incluindo partidas SIL, partidas convencionais e o módulo de interface SIL necessário, que gerencia o grupo SIL ao qual são atribuídos os avatares SIL.

NOTA: Os avatares SIL são projetados para aplicações com baixa frequência de comandos operacionais — abaixo da média anual de 15 ciclos de partida/parada por hora.

Partida SIL

Partida convencional

Módulo de interface SIL

15. Nível de integridade de segurança de acordo com a norma IEC 61508.

Módulo de interface SIL

O módulo de interface SIL[16] (SIM) do TeSys™ island é um módulo acessório necessário para habilitar o recurso de Segurança funcional da ilha.

A função de Parada SIL é atingida por meios puramente eletromecânicos e sem qualquer comunicação digital ou envolvimento da interface de rede.

O SIM:

- faz interface com um módulo Preventa™ XPS externo (ou equivalente)
- comanda a função de parada de seu grupo SIL
- troca dados operacionais com a interface de rede
- reporta informações operacionais por meio dos LEDs da face frontal

Status de contato das partidas SIL

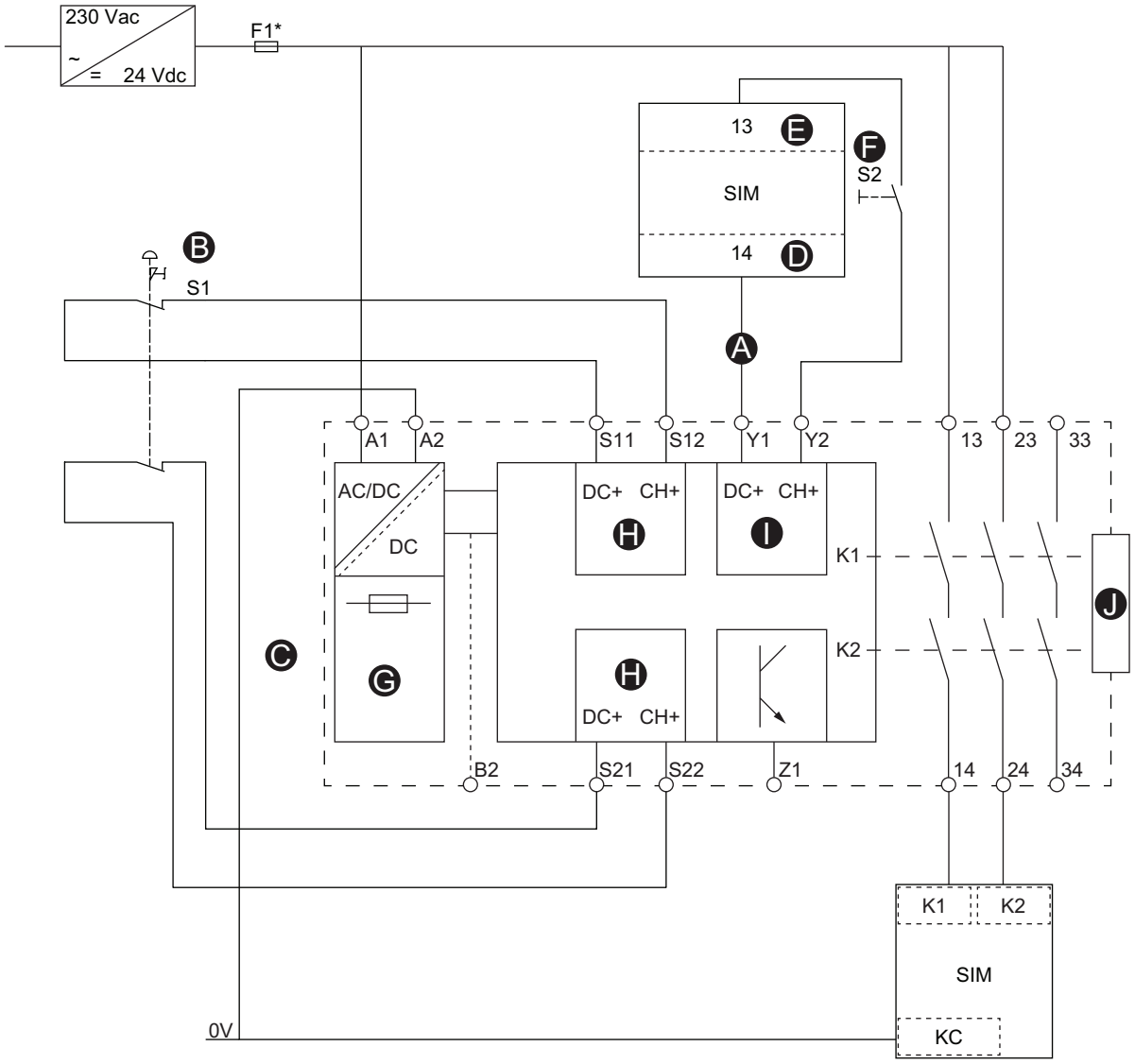
O status das partidas SIL[16] pertencentes a um grupo SIL é reportado por meio das conexões SIM Mirror In/Out. Isso permite a implementação de arquiteturas de Categoria de fiação 2[17], nas quais os contatos espelhados são conectados ao módulo Preventa XPS (ou equivalente). Essas configurações fornecem recursos de monitoramento direto de dispositivos eletromecânicos por meio de um elemento de contato vinculado mecanicamente, que oferece cobertura de diagnóstico de até 99%. Consulte a EN ISO 13849-1, Tabela E.1 – Estimativas para cobertura de diagnóstico (DC).

Tabela 2 - Status de contato das partidas SIL

Status do grupo SIL	Status de Mirror In/Out
Todas as partidas SIL estão abertas	O contato Mirror In/Out está fechado
Pelo menos uma partida SIL está fechada	O contato Mirror In/Out está aberto
TeSys island desligado ou falha detectada pela função de segurança	O contato Mirror In/Out está aberto

16. Nível de integridade de segurança de acordo com a norma IEC 61508.
17. Categoria de fiação 2 de acordo com a ISO 13849.

Figura 3 - Fiação do SIM para o módulo Preventa XPS-AF



A	Condições de partida externa (ESC)	F	Botão Iniciar (S2)
B	Botão de parada de emergência (S1)	G	Fonte de alimentação
C	Módulo Preventa XPS-UAF	H	Entrada
D	SIM Mirror Out	I	Partindo
E	SIM Mirror In	J	Extensão

Sensor relacionado à segurança

O módulo SIM é conectado a montante:

- da fonte de 24 VCC
- do sensor relacionado à segurança ou de um módulo Preventa XPS (ou equivalente)

O módulo SIM é projetado com dois canais de entrada para acomodar sensores relacionados à segurança de duplo canal. Para atingir um nível de tolerância a falhas mais alto, é recomendável a arquitetura de canal com duas entradas.

Para os diagramas elétricos a seguir, consulte a Legenda dos diagramas elétricos de canais do SIM, página 24.

Figura 4 - SIM — Fiação de um canal

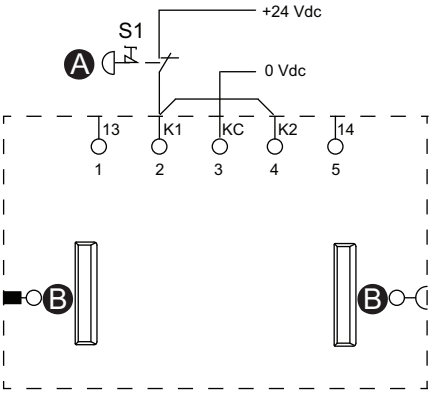


Figura 5 - SIM — Fiação de dois canais

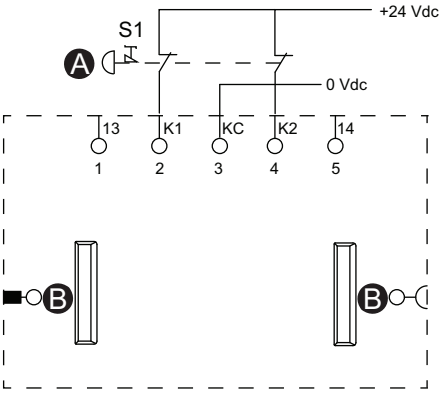


Tabela 3 - Legenda dos diagramas elétricos de canais do SIM

A	Botão de parada de emergência (S1)
B	Conector de cabo flat

Partidas SIL

⚠ATENÇÃO

OPERAÇÃO NÃO INTENCIONAL DO EQUIPAMENTO

Para obter instruções completas sobre a segurança funcional, consulte o Guia de Segurança Funcional do TeSys™ island, 8536IB1904

O não cumprimento destas instruções poderá resultar em morte, ferimentos graves ou danos do equipamento.

As partidas SIL[18] fornecem funções similares às das partidas convencionais, mas são associadas a um módulo de interface SIL.

As principais funções das partidas SIL são as seguintes:

- Fornecer a funcionalidade de Categorias de parada 0 e 1[19]
- Fornecer controle operacional para cargas
- Medir os dados elétricos da carga associada
- Fornecer dados de monitoramento de energia quando um módulo de interface de tensão está instalado na TeSys island

Várias partidas SIL podem ser necessárias para uma única função de TeSys avatar. Por exemplo, o avatar Motor com dois sentidos de rotação - Parada SIL, Cat. W. 1/2[20] inclui duas partidas SIL. Além disso, os avatars que usam partidas SIL sempre incluem um módulo de interface SIL.

As partidas SIL são conectadas:

- A montante de um disjuntor
- A jusante da carga

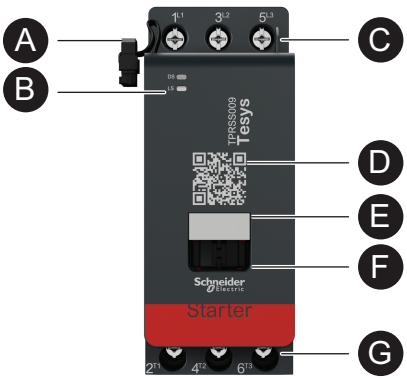
As partidas SIL se comunicam com a interface de rede, enviando dados operacionais e recebendo comandos.

Tabela 4 - Classificações de partida SIL

Classificações de potência		Corrente (A)	Referência
kW	hp		
4	5	0,18 – 9	TPRSS009
11	15	0,5 – 25	TPRSS025
18,5	20	0,76 – 38	TPRSS038
30	40	3,25 – 65	TPRSS065
37	40	4 – 80	TPRSS080

18. Nível de integridade de segurança de acordo com a norma IEC 61508.
19. Categorias de parada 0 e 1 de acordo com a EN/IEC 60204-1.
20. Categorias de fiação 1 e 2 de acordo com a ISO 13849.

Figura 6 - Recursos da partida SIL



A	Cabo plano (para conexão com o módulo à esquerda)	E	Etiqueta para identificação
B	Indicadores de status com LED	F	Ponte móvel
C	Conexões de energia a montante	G	Conexões de energia a jusante
D	Código QR		

Elemento externo relacionado à segurança

O TeSys™ island deve ser integrado a outros elementos relacionados à segurança em um sistema relacionado à segurança mais amplo para ajudar a garantir a segurança funcional de uma máquina ou de um sistema/processo.

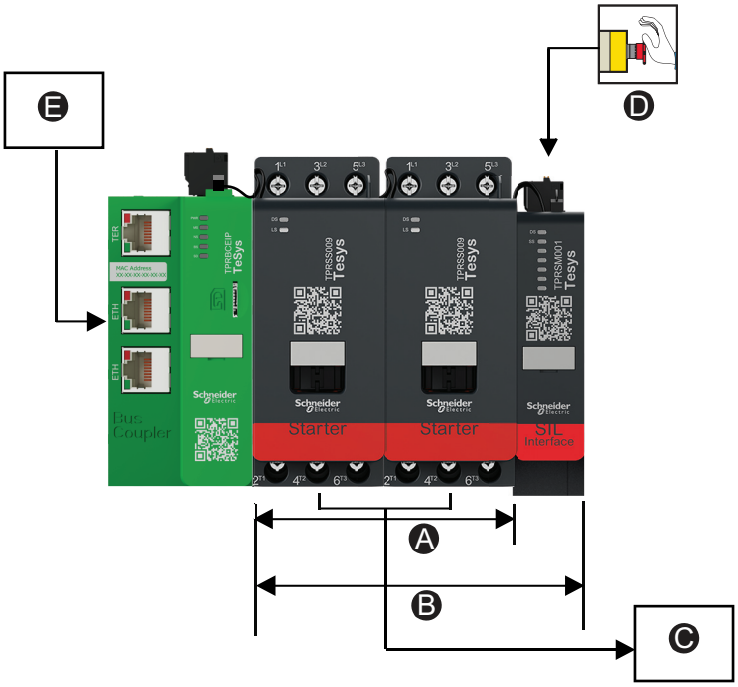
As configurações a seguir ilustram os dispositivos típicos.

Configuração de Parada SIL, Categoria de parada 0, Categoria de fiação 1

NOTA: Nível de integridade de segurança de acordo com a norma IEC 61508. Categoria de fiação 1 de acordo com a ISO 13849. Categoria de parada 0 de acordo com a EN/IEC 60204-1.

A Parada SIL do motor é controlada diretamente pela abertura do contato do botão de parada de emergência.

Figura 7 - Parada SIL



A	Avatar A1	D	Categoria de fiação 1, Categoria de parada 0
B	Grupo SIL 1	E	PLC
C	Motor		

Configuração de Parada SIL, Categoria de parada 0, Categoria de fiação 2

NOTA: Nível de integridade de segurança de acordo com a norma IEC 61508. Categoria de fiação 2 de acordo com a ISO 13849. Categoria de parada 0 de acordo com a EN/IEC 60204-1.

Figura 8 - Exemplo: Motor com dois sentidos de rotação - Parada SIL, Cat. W. 1/2 — Configuração de Categoria de parada 0, Categoria de fiação 2 (Monitoramento indireto)

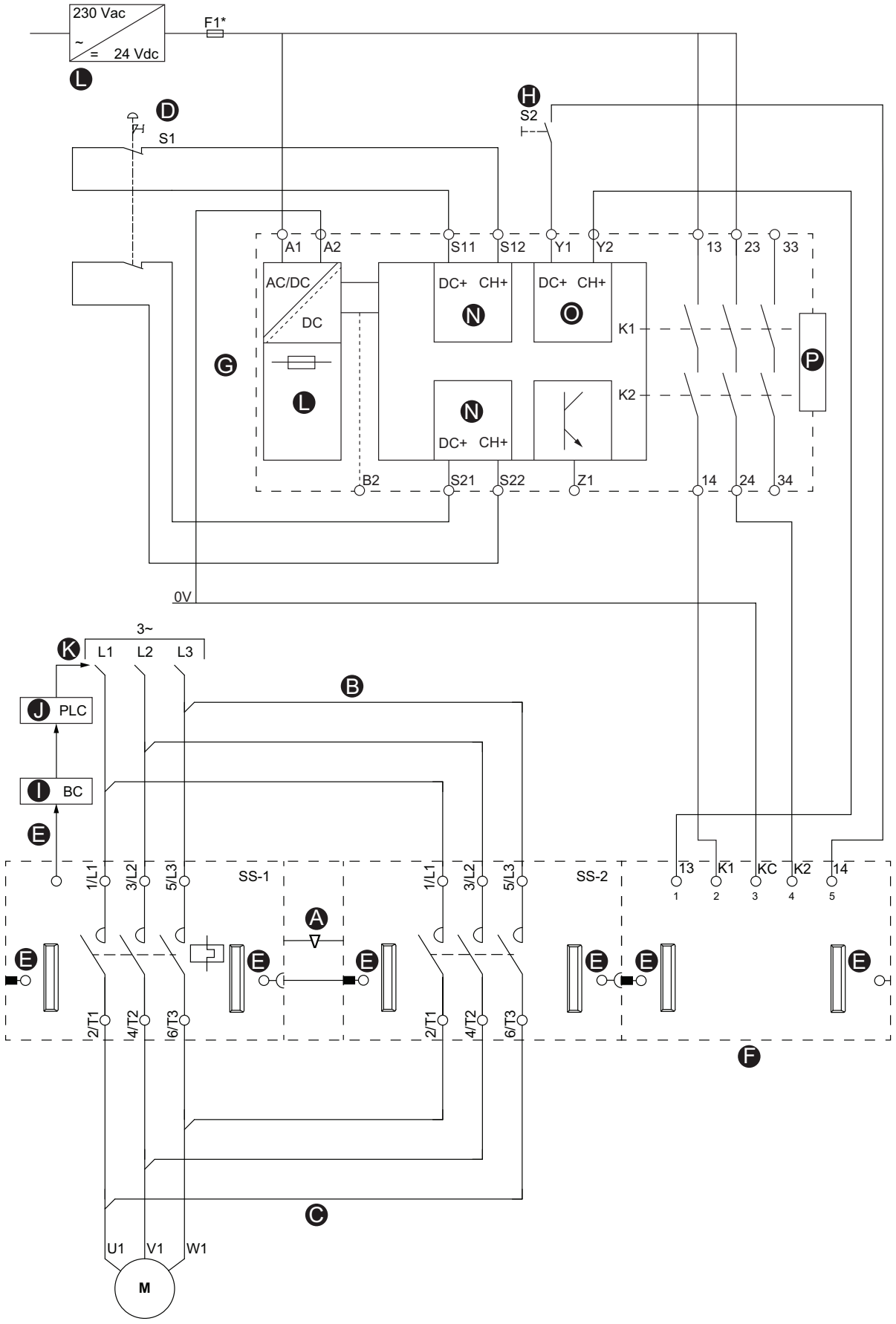
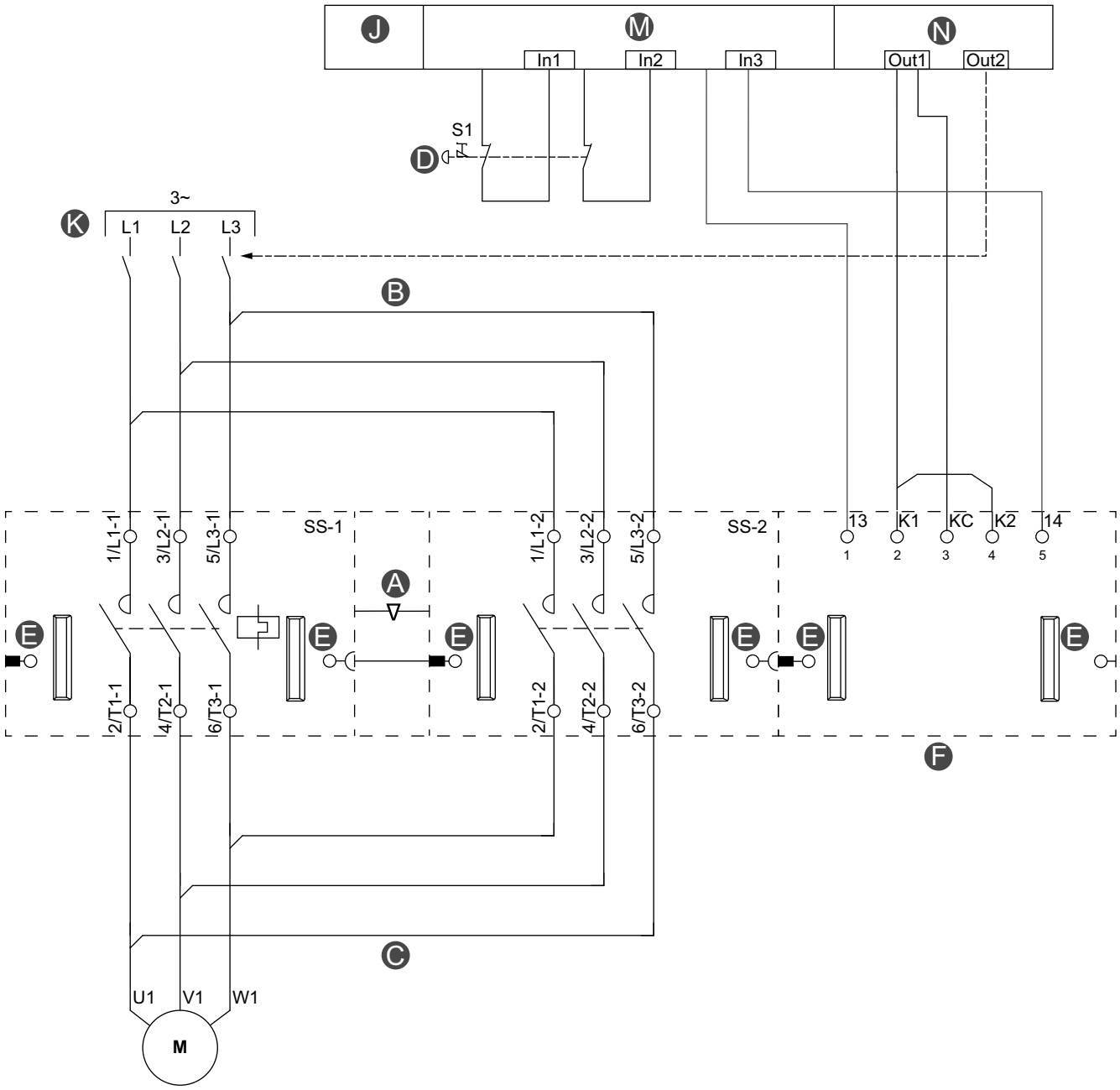


Tabela 5 - Legenda para Exemplo: Motor com dois sentidos de rotação - Parada SIL, Cat. W. 1/2 — Configuração de Categoria de parada 0, Categoria de fiação 2 (Monitoramento indireto), página 28

A	Intertravamento mecânico	I	Interface de rede
B	Barramento superior	J	PLC
C	Barramento inferior	K	Disjuntor a montante
D	Botão de parada de emergência (S1)	L	Fonte de alimentação
E	Conector de cabo flat	N	Entrada
F	Módulo de interface SIL (SIM)	O	Partindo
G	Módulo Preventa XPS-UAF	P	Extensão
H	Botão Iniciar (S2)		

Figura 9 - Exemplo: Motor com dois sentidos de rotação - Parada SIL, Cat. W. 1/2 — Configuração de Categoria de parada 0, Categoria de fiação 2 (Monitoramento direto)



A	Intertravamento mecânico	F	Módulo de interface SIL (SIM)
B	Barramento superior	J	PLC da função de segurança
C	Barramento inferior	K	Disjuntor a montante
D	Botão de parada de emergência (S1)	M	Entrada digital
E	Conector de cabo flat	N	Saída digital

Configuração de Parada SIL, Categoria de parada 1, Categoria de fiação 2

NOTA: Nível de integridade de segurança de acordo com a norma IEC 61508. Categoria de fiação 2 de acordo com a ISO 13849. Categoria de parada 1 de acordo com a EN/IEC 60204-1.

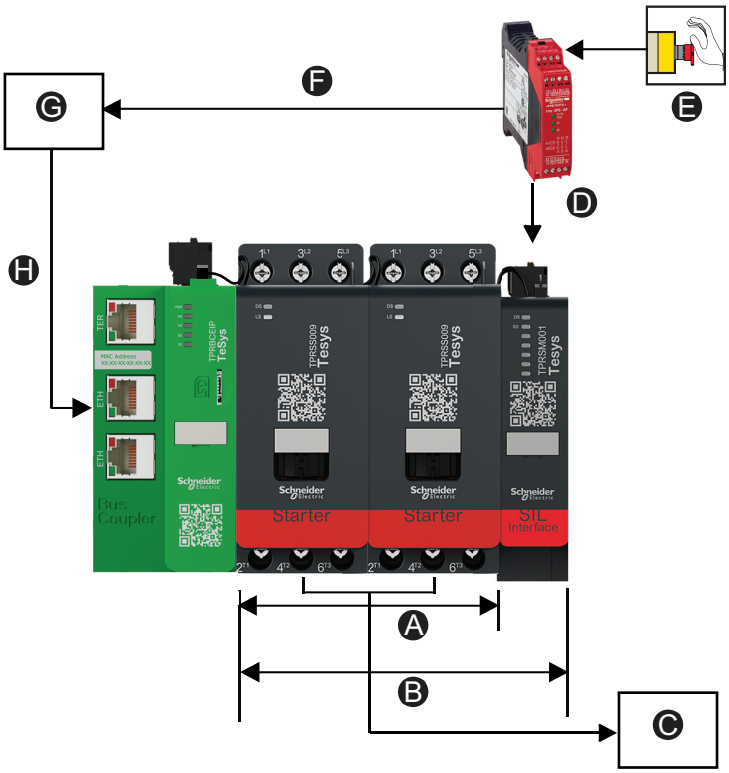
A Categoria de parada 1 é definida como “uma parada controlada com energia disponível para os mecanismos da máquina a fim de atingir a parada e, depois, a remoção da energia, quando a parada for atingida”.

Quando a parada de emergência é acionada, o comando de parada é enviado primeiramente para um dispositivo externo (como um PLC ou uma unidade). Dessa forma, o processo é interrompido de maneira controlada, e não por meio da remoção imediata da energia. Após um tempo predefinido, o comando de parada SIL é enviado ao SIM para desenergizar as cargas nos avatares SIL do grupo SIL associado.

A configuração recomendada é usar um PLC para ajudar a garantir que o processo seja interrompido corretamente antes da parada SIL.

O comando de parada pode ser passado diretamente para uma entrada digital do PLC ou para um avatar do Módulo de E/S digital do TeSys™ island utilizando uma de suas entradas digitais lidas pelo PLC. Mediante o recebimento de uma entrada de comando de parada, o PLC inicia uma parada controlada emitindo um comando de parada operacional para o avatar do TeSys island de destino.

Figura 10 - Comando de parada



A	Avatar A1	E	Categoria de fiação 2, Categoria de parada 1
B	Grupo SIL 1	F	Comando de Categoria de parada controlada 1

C	Motor	G	PLC
D	Parada não controlada	H	Comando de parada operacional

Figura 11 - Exemplo: Motor com dois sentidos de rotação - Parada SIL, Cat. W. 1/2 — Configuração de Categoria de parada 1, Categoria de fiação 2

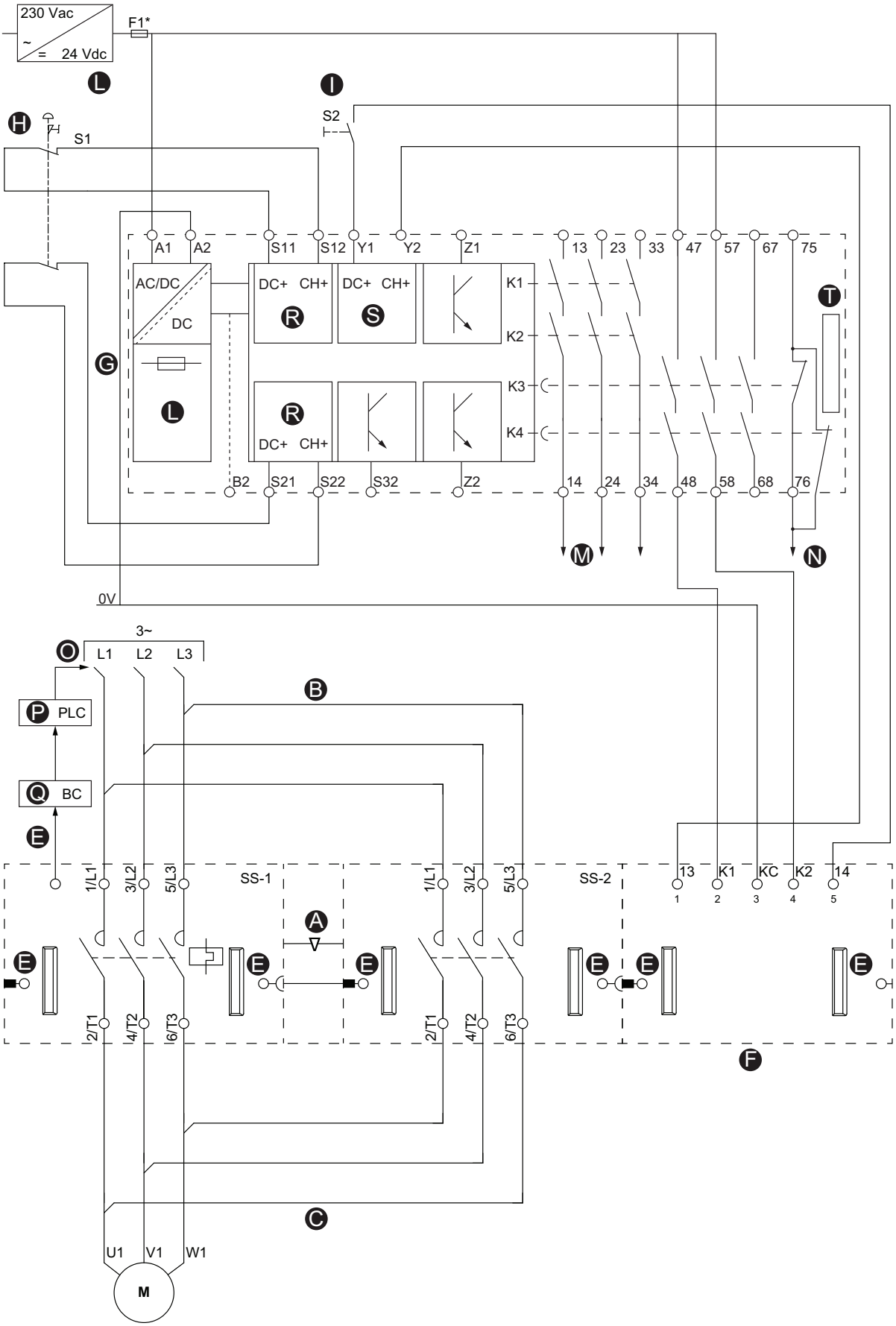


Tabela 6 - Legenda para Exemplo: Motor com dois sentidos de rotação - Parada SIL, Cat. W. 1/2 — Configuração de Categoria de parada 1, Categoria de fiação 2, página 33

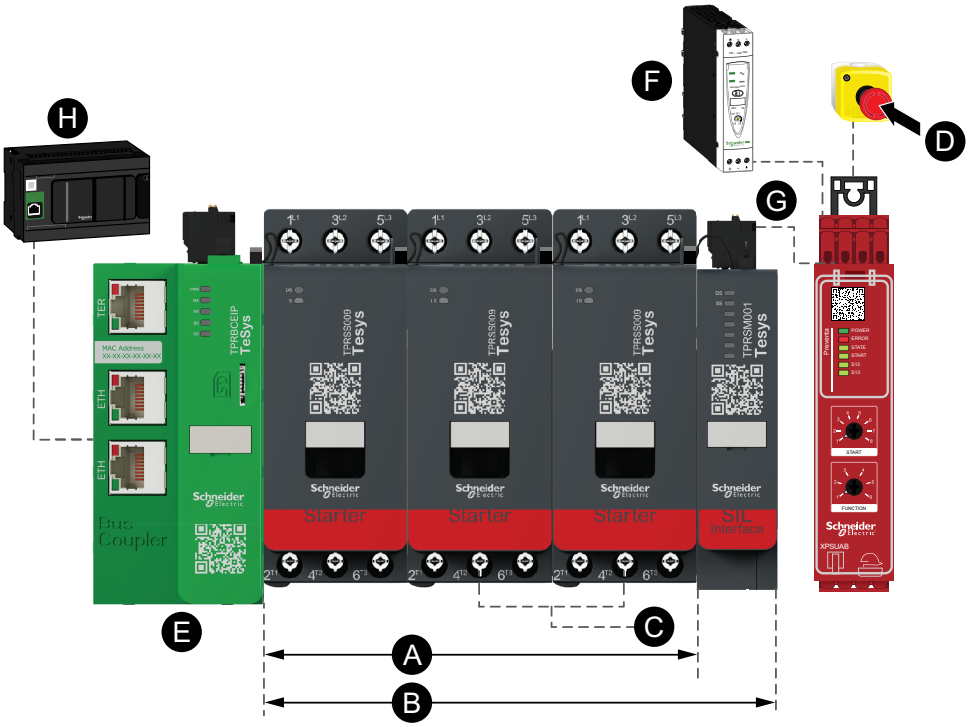
A	Intertravamento mecânico	M	Parada controlada
B	Barramento superior	N	Categoria de parada 1
C	Barramento inferior	O	Disjuntor a montante
E	Conector de cabo flat	P	PLC
F	Módulo de interface SIL (SIM)	Q	Interface de rede
G	Módulo Preventa XPS-UAF	R	Entrada
H	Botão de parada de emergência	S	Partindo
I	Botão de partida S2	T	Extensão
L	Fonte de alimentação		

Configuração de Parada SIL, Categoria de parada 0, Categoria de fiação 3/4

NOTA: Nível de integridade de segurança de acordo com a norma IEC 61508. Categoria de fiação 3/4 de acordo com a ISO 13849. Categoria de parada 0 de acordo com a EN/IEC 60204-1.

A Parada SIL do motor é controlada diretamente pela abertura do contato do botão de parada de emergência.

Figura 12 - Parada SIL, Categoria de fiação 3/4



A	Avatar A1	E	Interface de rede
B	Grupo SIL 1	F	24 VCC
C	Motor	G	Módulo Preventa XPS-UAF
D	Categoria de fiação 3/4, Categoria de parada 0	H	PLC

Figura 13 - Exemplo: Motor com um sentido de rotação - Parada SIL, Cat. W. 3/4 — Configuração de Categoria de parada 0, Categoria de fiação 3/4

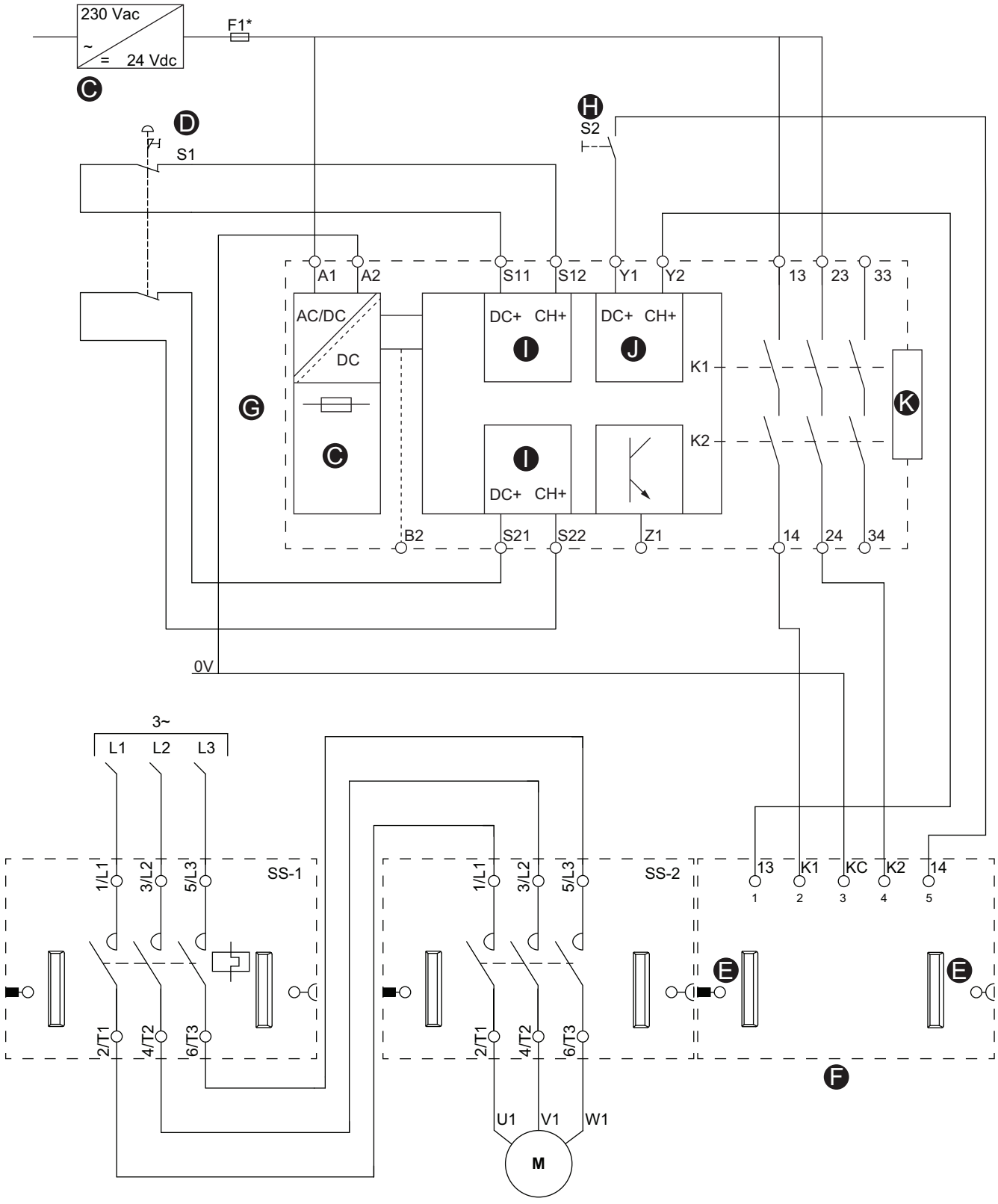


Tabela 7 - Legenda para Exemplo: Motor com um sentido de rotação - Parada SIL, Cat. W. 3/4 — Configuração de Categoria de parada 0, Categoria de fiação 3/4, página 36

C	Fonte de alimentação	H	Botão Iniciar (S2)
D	Botão de parada de emergência (S1)	I	Entrada
E	Conector de cabo flat	J	Partindo
F	Módulo de interface SIL (SIM)	K	Extensão
G	Módulo Preventa XPS-UAF		

Configuração de Parada SIL, Categoria de parada 1, Categoria de fiação 3/4

NOTA: Nível de integridade de segurança de acordo com a norma IEC 61508. Categoria de fiação 3/4 de acordo com a ISO 13849. Categoria de parada 1 de acordo com a EN/IEC 60204.

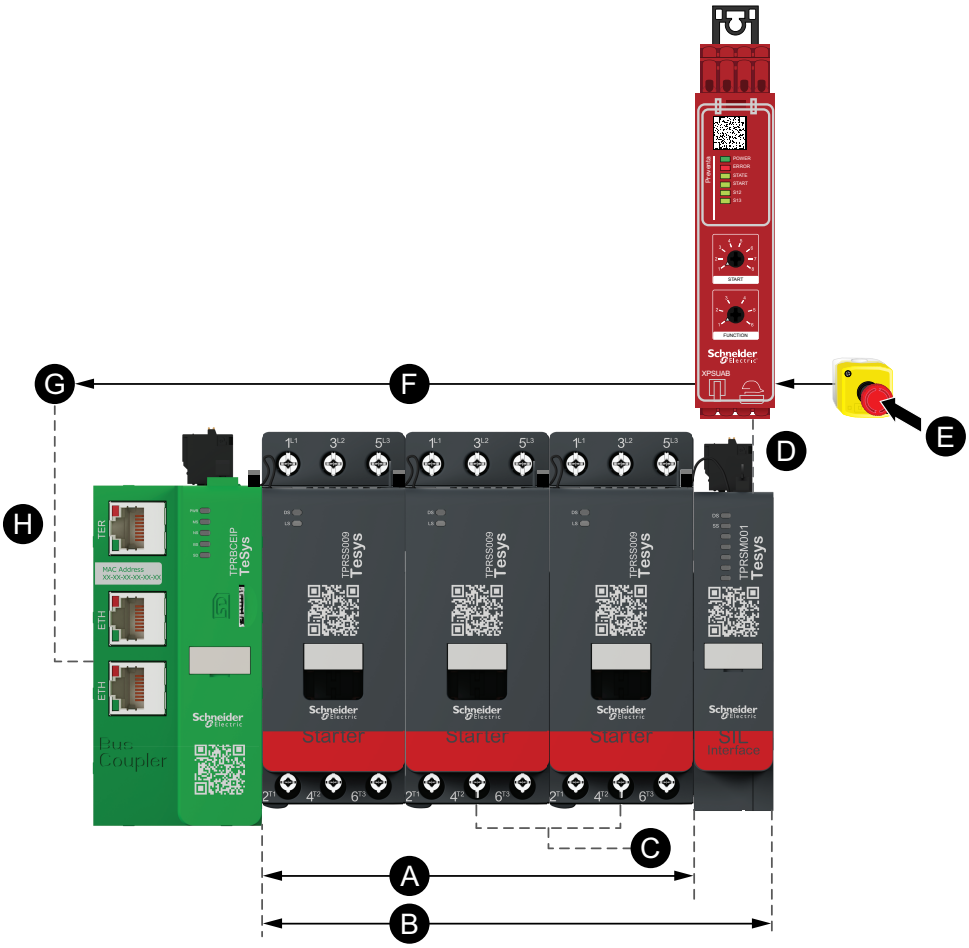
A Categoria de parada 1 é definida como “uma parada controlada com energia disponível para os mecanismos da máquina a fim de atingir a parada e, depois, a remoção da energia, quando a parada for atingida”.

Quando a parada de emergência é acionada, o comando de parada é enviado primeiramente para um dispositivo externo (como um PLC ou uma unidade). Dessa forma, o processo é interrompido de maneira controlada, não por meio da remoção imediata da alimentação. Após um tempo predefinido, o comando de parada SIL é enviado ao SIM para desenergizar as cargas nos avatares SIL do grupo SIL associado.

Para a configuração, a recomendação é usar um PLC para ajudar a garantir que o processo seja interrompido corretamente antes da parada SIL.

O comando de parada pode ser passado diretamente para uma entrada digital do PLC ou para um avatar do Módulo de E/S digital do TeSys™ island utilizando uma de suas entradas digitais lidas pelo PLC. Mediante o recebimento de uma entrada de comando de parada, o PLC inicia uma parada controlada emitindo um comando de parada operacional para o avatar do TeSys island de destino.

Figura 14 - Comando de parada, Categoria de fiação 3/4



A	Avatar A1	E	Categoria de fiação 3/4, Categoria de parada 1
B	Grupo SIL 1	F	Comando de Categoria de parada controlada 1
C	Motor	G	PLC
D	Parada não controlada	H	Comando de parada operacional

Figura 15 - Exemplo: Motor com dois sentidos de rotação - Parada SIL, Cat. W. 3/4 — Configuração de Categoria de parada 1, Categoria de fiação 3/4

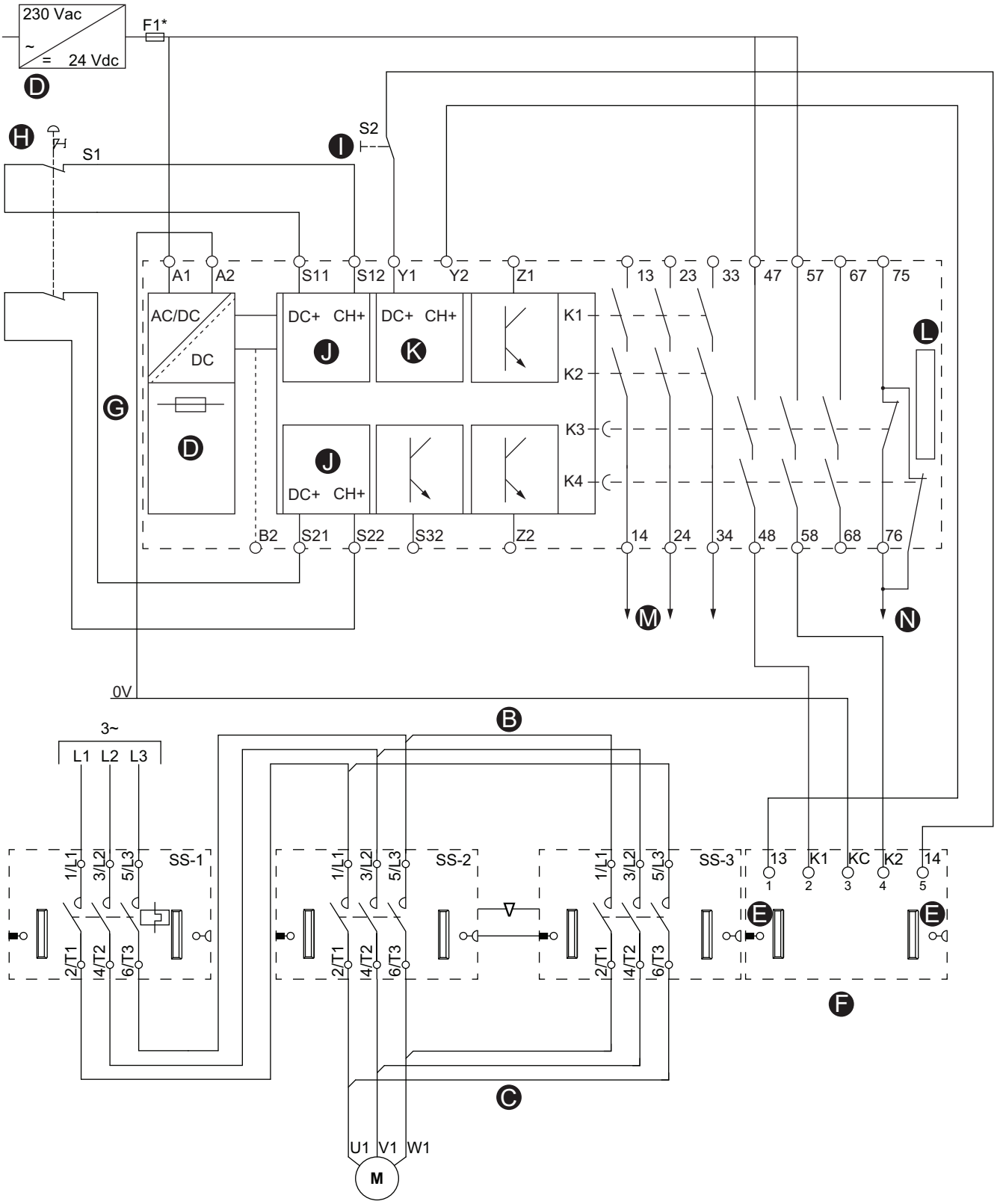


Tabela 8 - Legenda para Exemplo: Motor com dois sentidos de rotação - Parada SIL, Cat. W. 3/4 — Configuração de Categoria de parada 1, Categoria de fiação 3/4, página 39

B	Barramento superior	I	Botão de partida S2
C	Barramento inferior	J	Entrada
D	Fonte de alimentação	K	Partindo
E	Conector de cabo flat	L	Extensão
F	Módulo de interface SIL (SIM)	M	Parada controlada
G	Módulo Preventa XPS-UAF	N	Categoria de parada 1
H	Botão de parada de emergência (S1)		

Isolamento de cabo protegido

⚠ PERIGO

OPERAÇÃO NÃO INTENCIONAL DO EQUIPAMENTO

Certifique-se de instalar os cabos do sistema relacionado à segurança de acordo com a ISO 13849-2.

O não cumprimento destas instruções poderá resultar em morte ou ferimentos graves.

Se puderem ocorrer curtos-circuitos e circuitos cruzados nos cabos do sistema relacionado à segurança e se eles não forem detectados pelos dispositivos a montante, será necessária a instalação de um cabo protegido de acordo com a ISO 13849-2.

No caso de uma instalação de cabo não protegido, os dois sinais (ambos os canais) de uma função de segurança em estado de curto-circuito podem ser conectados à tensão externa se um cabo for danificado. Nesse caso, a função de segurança não estará mais operacional.

Arquitetura de comutação de baixa/alta frequência

É possível usar as informações desta seção para determinar se você está operando em uma arquitetura de baixa ou alta frequência.

A parte eletromecânica da partida SIL[21] é caracterizada por um B10d.

Para calcular o $MTTF_d$ (de acordo com a ISO 13849-1) ou o λd (de acordo com a IEC 62061), aplique a seguinte fórmula:

$$MTTF_d = B10d/(0,1*Nop)$$

com $\lambda d = 1/MTTF_d$

Nop: número médio de operações anuais

De acordo com a ISO 13849, o tempo de operação de um componente eletromecânico é limitado a T10d (o tempo médio até que 10% dos componentes falhem perigosamente[22]).

Portanto, o tempo de operação de uma partida SIL é limitado a:

$$T10d = B10d/Nop$$

O B10d da partida SIL é B10d = 1.369.863 e, supondo-se um T10d de 10 anos, o número de ciclos para uma partida SIL do TeSys island é limitado a Nop = B10d/T10 = 131.400/ano (ou uma média anual de 15 ciclos/h).

Se a aplicação exigir um Nop inferior a esse valor, ela se enquadrará na categoria de baixa frequência de comutação (na qual os avatares SIL podem ser usados como estão). Caso contrário, ela se enquadrará na categoria de alta frequência de comutação (na qual a função de segurança deve ser implementada com um avatar SIL dedicado, como descrito a seguir).

21. Nível de integridade de segurança de acordo com a norma IEC 61508.
22. Falha perigosa, de acordo com a ISO 13849

Baixa frequência de comutação (< 15 ciclos por hora)

Em baixa frequência de comutação, a parada SIL[23] e as funções de controle ligar/desligar operacionais podem ser executadas em conjunto com um avatar SIL.

Figura 16 - Exemplo de avatar com partida SIL

Tabela 9 - Baixa frequência de comutação – Funções operacionais e de segurança

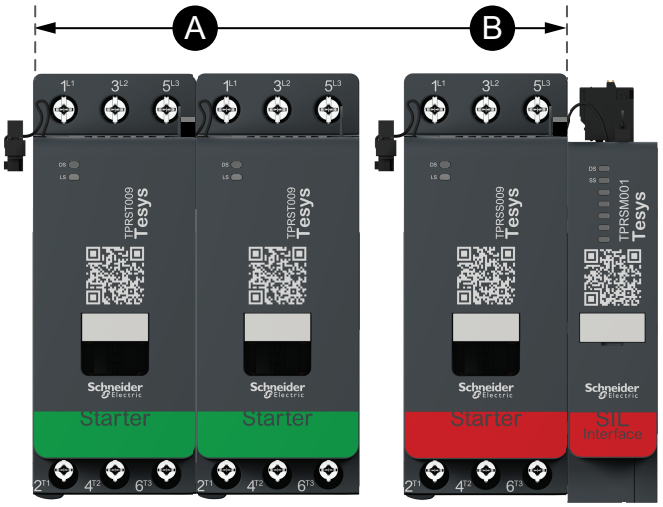
Avatar SIL	Módulo 1	Módulo 2	Módulo 3	Módulo 4	Módulo 5
Contator - Parada SIL, Cat. W. 1/2[24]	Partida SIL	SIM	—	—	—
Contator - Parada SIL, Cat. W. 3/4[25]	Partida SIL	Partida SIL	SIM	—	—
Motor com um sentido de rotação - Parada SIL, Cat. W. 1/2	Partida SIL	SIM		—	—
Motor com um sentido de rotação - Parada SIL, Cat. W. 3/4	Partida SIL	Partida SIL	SIM	—	—
Motor com dois sentidos de rotação - Parada SIL, Cat. W. 1/2	Partida SIL	Partida SIL	SIM	—	—
Motor com dois sentidos de rotação - Parada SIL, Cat. W. 3/4	Partida SIL	Partida SIL	Partida SIL	SIM	—
Motor de duas velocidades - Parada SIL, Cat. W. 1/2	Partida SIL	Partida SIL	SIM	—	—
Motor de duas velocidades - Parada SIL, Cat. W. 3/4	Partida SIL	Partida SIL	Partida SIL	SIM	—
Motor de duas velocidades e com dois sentidos de rotação - Parada SIL, Cat. W. 1/2	Partida convencional	Partida convencional	Partida SIL	Partida SIL	SIM
Motor de duas velocidades e com dois sentidos de rotação - Parada SIL, Cat. W. 3/4	Partida SIL	Partida SIL	Partida SIL	Partida SIL	SIM
Transportador com um sentido de rotação - Parada SIL, Cat. W. 1/2	Partida SIL	SIM	—	—	—
Transportador com dois sentidos de rotação - Parada SIL, Cat. W. 1/2	Partida SIL	Partida SIL	SIM	—	—

23. Nível de integridade de segurança de acordo com a norma IEC 61508.
24. Categorias de fiação 1 e 2 de acordo com a ISO 13849.
25. Categorias de fiação 3 e 4 de acordo com a ISO 13849.

Alta frequência de comutação (≥ 15 ciclos por hora)

Para uso em alta frequência, a função de segurança deve ser isolada da função operacional utilizando um avatar SIL[26] para a função de segurança e um avatar padrão para a função operacional. As partidas convencionais são, então, cabeadas em série a jusante da(s) partida(s) SIL. Alta frequência de comutação – Funções operacionais e de segurança mostra exemplos de avatares padrão usados a jusante da(s) partida(s) SIL para arquiteturas de Parada SIL, Cat. W. 1/2[27] e Parada SIL, Cat. W. 3/4[28].

Figura 17 - Avatar padrão para a função operacional + Avatar SIL usado para a função de segurança — Parada SIL, Cat. W. 1/2



A	Avatar padrão
B	Avatar SIL

Tabela 10 - Alta frequência de comutação - Parada SIL, Cat. W. 1/2 — Funções operacionais e de segurança

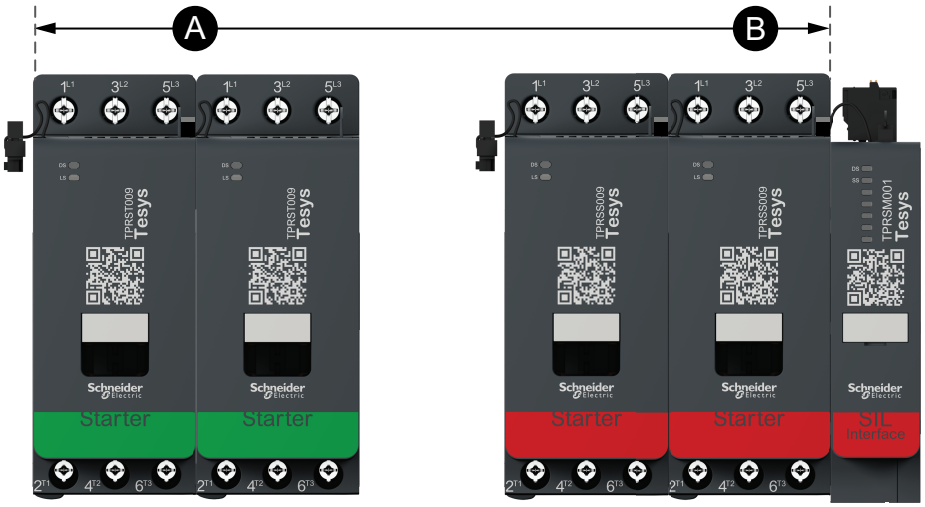
Avatar padrão	Avatar SIL	Módulo 1	Módulo 2	Módulo 3	Módulo 4	Módulo 5	Módulo 6
Contator	Contator - Parada SIL, Cat. W. 1/2	Partida convencional	Partida SIL	SIM	—	—	—
Motor com um sentido de rotação	Contator - Parada SIL, Cat. W. 1/2	Partida convencional	Partida SIL	SIM	—	—	—
Motor com dois sentidos de rotação	Contator - Parada SIL, Cat. W. 1/2	Partida convencional	Partida convencional	Partida SIL	SIM	—	—
Motor de duas velocidades	Contator - Parada SIL, Cat. W. 1/2	Partida convencional	Partida convencional	Partida SIL	SIM	—	—
Motor de duas velocidades e com dois sentidos de rotação	Contator - Parada SIL, Cat. W. 1/2	Partida convencional	Partida convencional	Partida convencional	Partida convencional	Partida SIL	SIM
Transportador com um sentido de rotação	Contator - Parada SIL, Cat. W. 1/2	Partida convencional	Partida SIL	SIM	—	—	—
Transportador com dois sentidos de rotação	Contator - Parada SIL, Cat. W. 1/2	Partida convencional	Partida convencional	Partida SIL	SIM	—	—

26. Nível de integridade de segurança de acordo com a norma IEC 61508.
27. Categorias de fiação 1 e 2 de acordo com a ISO 13849.
28. Categorias de fiação 3 e 4 de acordo com a ISO 13849.

Tabela 10 - Alta frequência de comutação - Parada SIL, Cat. W. 1/2 — Funções operacionais e de segurança (Continuação)

Avatar padrão	Avatar SIL	Módulo 1	Módulo 2	Módulo 3	Módulo 4	Módulo 5	Módulo 6
Motor Y/D com um sentido de rotação	Contator - Parada SIL, Cat. W. 1/2	Partida convencional	Partida convencional	Partida convencional	Partida SIL	SIM	—
Motor Y/D com dois sentidos de rotação	Contator - Parada SIL, Cat. W. 1/2	Partida convencional	Partida convencional	Partida convencional	Partida convencional	Partida SIL	SIM

Figura 18 - Avatar padrão para a função operacional + Avatar SIL usado para a função de segurança — Parada SIL, Cat. W. 3/4



A	Avatar padrão
B	Avatar SIL

Tabela 11 - Alta frequência de comutação - Parada SIL, Cat. W. 3/4 — Funções operacionais e de segurança

Avatar padrão	Avatar SIL	Módulo 1	Módulo 2	Módulo 3	Módulo 4	Módulo 5	Módulo 6	Módulo 7
Interruptor	Contator - Parada SIL, Cat. W. 3/4	Partida convencional	Partida SIL	Partida SIL	SIM	—	—	—
Motor com um sentido de rotação	Contator - Parada SIL, Cat. W. 3/4	Partida convencional	Partida SIL	Partida SIL	SIM	—	—	—
Motor com dois sentidos de rotação	Contator - Parada SIL, Cat. W. 3/4	Partida convencional	Partida convencional	Partida SIL	Partida SIL	SIM	—	—
Motor de duas velocidades	Contator - Parada SIL, Cat. W. 3/4	Partida convencional	Partida convencional	Partida SIL	Partida SIL	SIM	—	—
Motor de duas velocidades e com dois sentidos de rotação	Contator - Parada SIL, Cat. W. 3/4	Partida convencional	Partida convencional	Partida convencional	Partida convencional	Partida SIL	Partida SIL	SIM
Motor Y/D com um sentido de rotação	Contator - Parada SIL, Cat. W. 3/4	Partida convencional	Partida convencional	Partida convencional	Partida convencional	Partida SIL	Partida SIL	SIM
Motor Y/D com dois sentidos de rotação	Contator - Parada SIL, Cat. W. 3/4	Partida convencional	Partida convencional	Partida convencional	Partida convencional	Partida SIL	Partida SIL	SIM

Exemplos de arquitetura

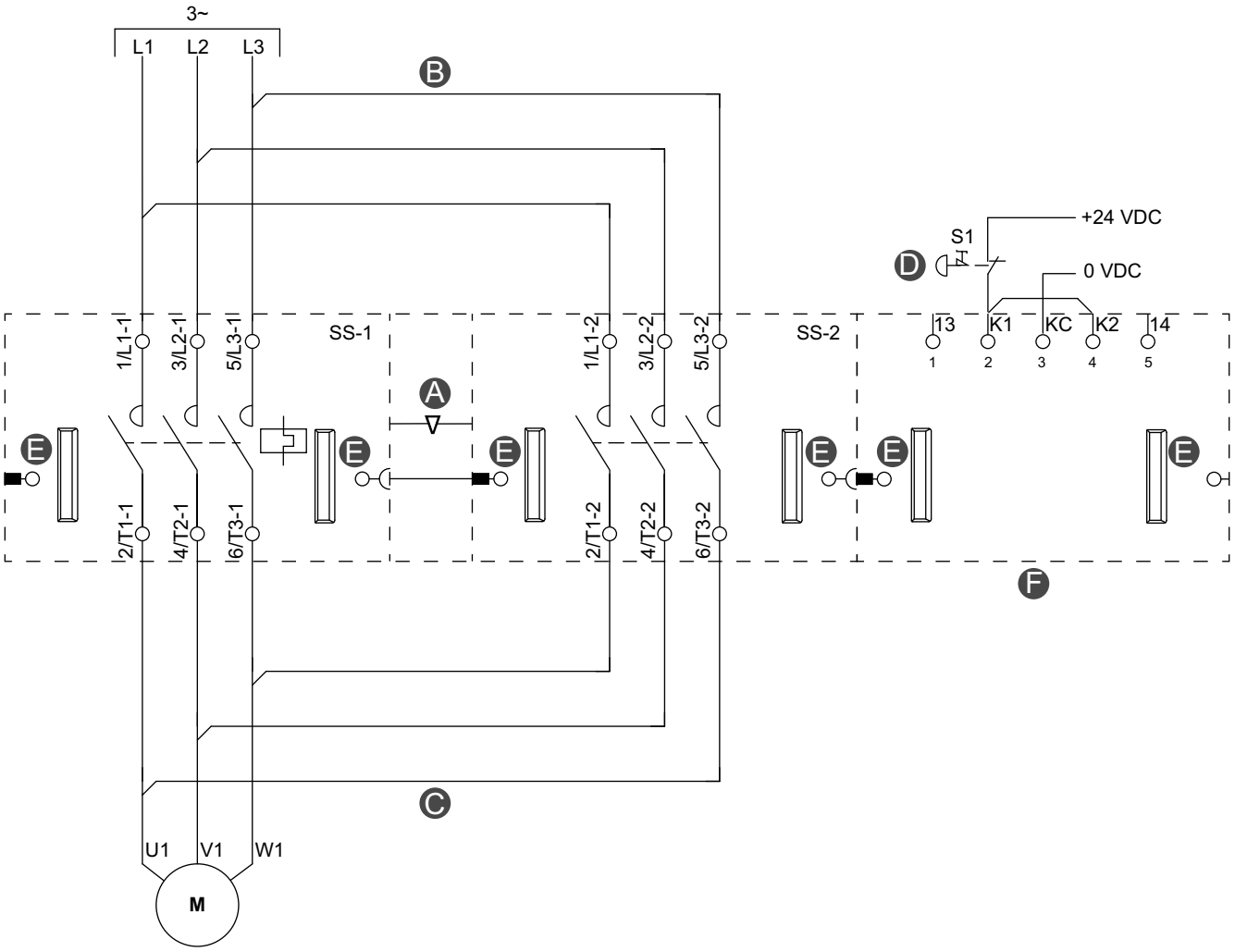
As arquiteturas a seguir estão disponíveis para a segurança funcional do TeSys™ island:

- Parada SIL, Categoria de parada 0, Categoria de fiação 1[29]
- Parada SIL, Categoria de parada 0, Categoria de fiação 2
- Parada SIL, Categoria de parada 1, Categoria de fiação 2
- Parada SIL, Categoria de parada 0, Categoria de fiação 3/4
- Parada SIL, Categoria de parada 1, Categoria de fiação 3/4

29. Nível de integridade de segurança de acordo com a norma IEC 61508. Categorias de fiação 1, 2 e 3/4 de acordo com a ISO 13849. Categorias de parada 0 e 1 de acordo com a EN/IEC 60204-1.

Parada SIL, Categoria de parada 0, Categoria de fiação 1

Figura 19 - Exemplo: Parada SIL, Categoria de parada 0, Categoria de fiação 1[30]

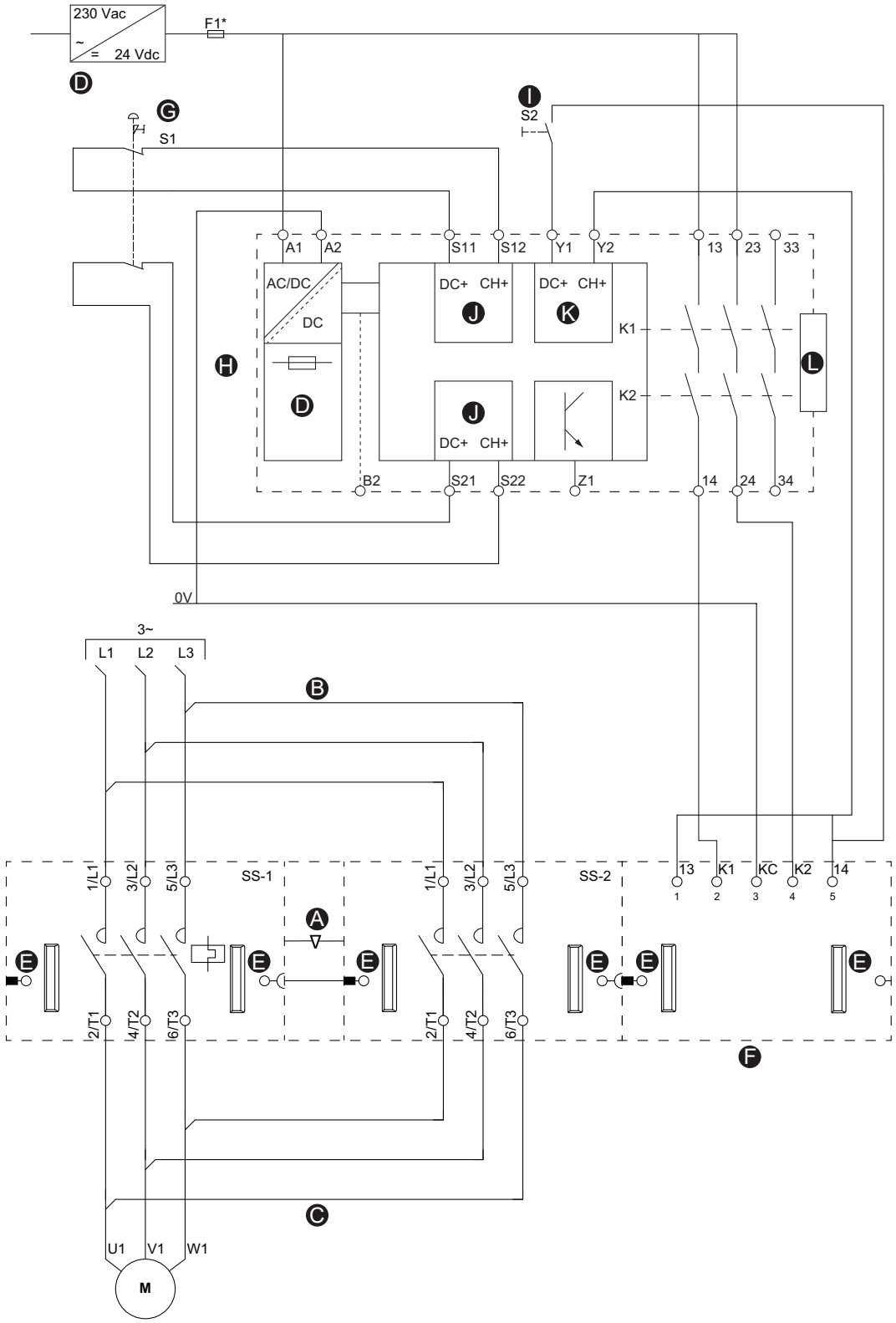


A	Intertravamento mecânico	D	Botão de parada de emergência (S1)
B	Barramento superior	E	Conector de cabo flat
C	Barramento inferior	F	Módulo de interface SIL (SIM)

30. Nível de integridade de segurança de acordo com a norma IEC 61508. Categoria de fiação 1 de acordo com a ISO 13849. Categoria de parada 0 de acordo com a EN/IEC 60204-1.

Parada SIL, Categoria de parada 0, Categoria de fiação 2

Figura 20 - Exemplo: Parada SIL, Categoria de parada 0, Categoria de fiação 2[31]



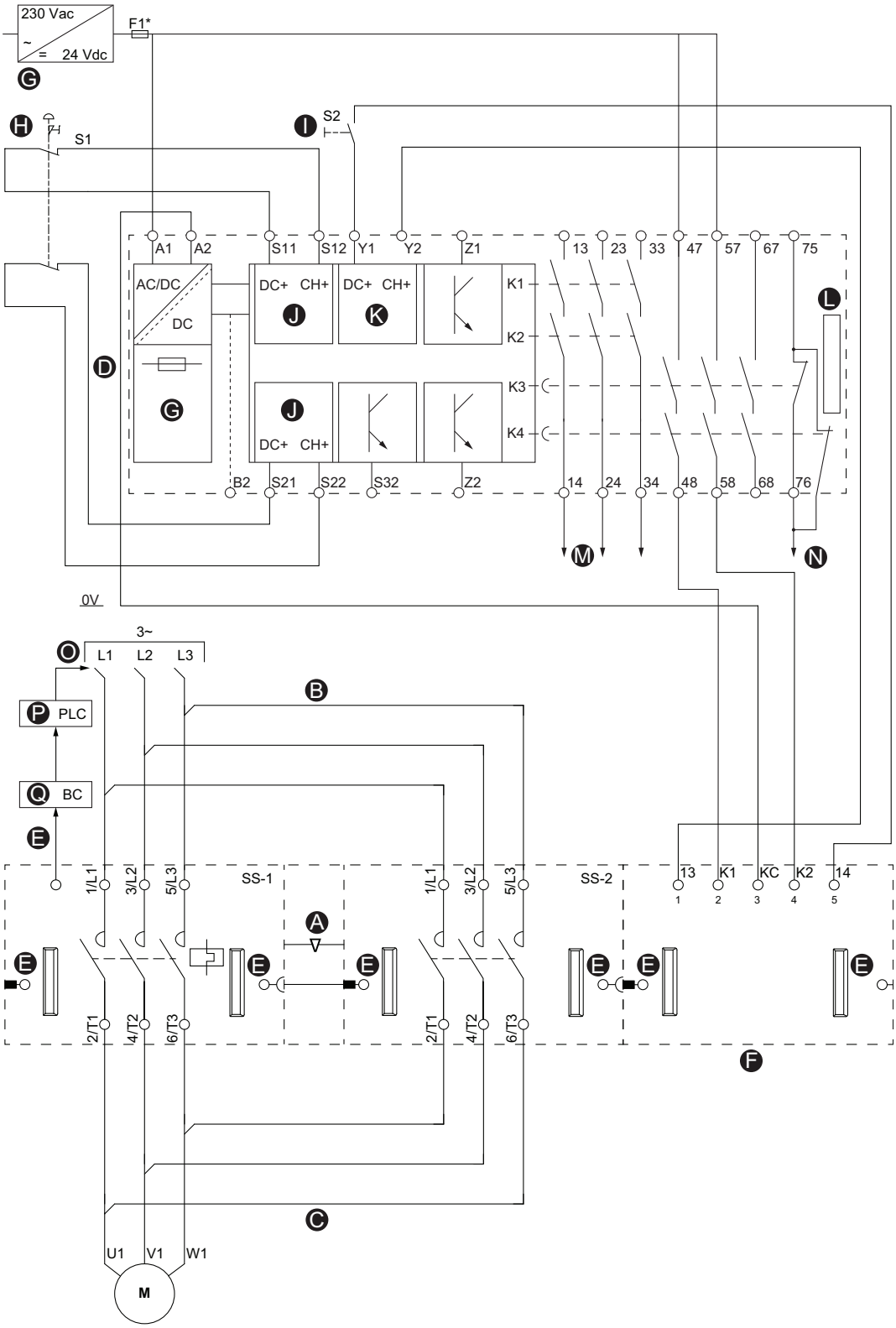
31. Nível de integridade de segurança de acordo com a norma IEC 61508. Categoria de fiação 2 de acordo com a ISO 13849. Categoria de parada 0 de acordo com a EN/IEC 60204-1.

Tabela 12 - Legenda para exemplo de : Parada SIL, Categoria de parada 0, Categoria de fiação 2, página 48

A	Intertravamento mecânico	G	Botão de parada de emergência (S1)
B	Barramento superior	H	Módulo Preventa XPS-UAF
C	Barramento inferior	I	Botão Iniciar (S2)
D	Fonte de alimentação	J	Inib.
E	Conector de cabo flat	K	Partindo
F	Módulo de interface SIL (SIM)	L	Extensão

Parada SIL, Categoria de parada 1, Categoria de fiação 2

Figura 21 - Exemplo: Parada SIL, Categoria de parada 1, Categoria de fiação 2[32]



32. Nível de integridade de segurança de acordo com a norma IEC 61508. Categoria de fiação 2 de acordo com a ISO 13849. Categoria de parada 1 de acordo com a EN/IEC 60204-1.

Tabela 13 - Legenda para exemplo de : Parada SIL, Categoria de parada 1, Categoria de fiação 2, página 50

A	Intertravamento mecânico	J	Inib.
B	Barramento superior	K	Partindo
C	Barramento inferior	L	Extensão
E	Conector de cabo flat	M	Parada controlada
F	Módulo de interface SIL (SIM)	N	Categoria de parada 1
G	Fonte de alimentação	O	Disjuntor a montante
H	Botão de parada de emergência (S1)	P	PLC
I	Botão de partida S2	Q	Interface de rede

Parada SIL, Categoria de parada 0, Categoria de fiação 3/4

Figura 22 - Exemplo: Parada SIL, Categoria de parada 0, Categoria de fiação 3/4[33]

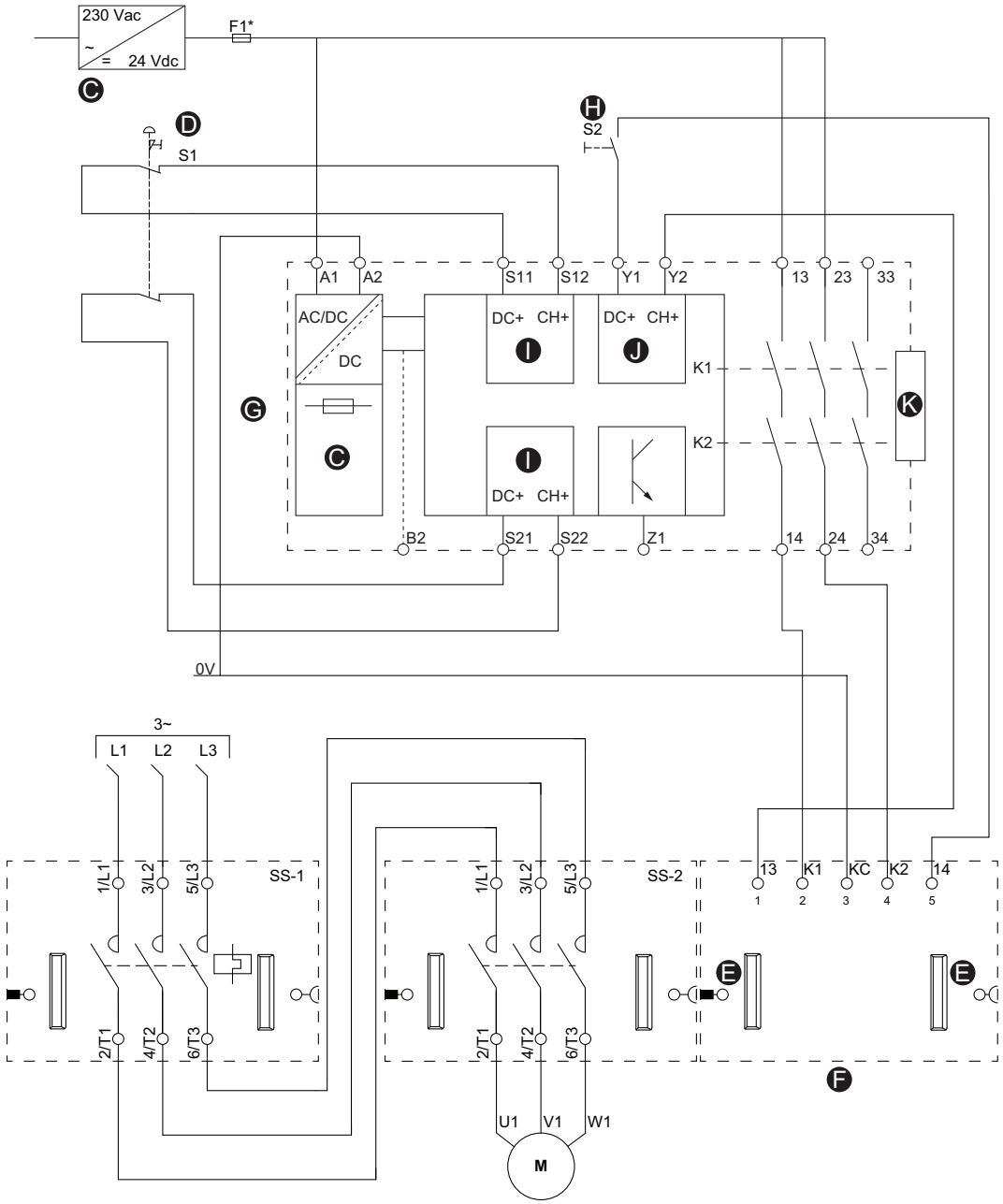


Tabela 14 - Legenda para exemplo de : Parada SIL, Categoria de parada 0, Categoria de fiação 3/4, página 52

C	Fonte de alimentação	H	Botão Iniciar (S2)
D	Botão de parada de emergência (S1)	I	Inib.
E	Conector de cabo flat	J	Partindo

33. Nível de integridade de segurança de acordo com a norma IEC 61508. Categoria de fiação 3/4 de acordo com a ISO 13849. Categoria de parada 0 de acordo com a EN/IEC 60204-1.

Tabela 14 - Legenda para exemplo de : Parada SIL, Categoria de parada 0, Categoria de fiação 3/4 (Continuação)

F	Módulo de interface SIL (SIM)	K	Extensão
G	Módulo Preventa XPS-UAF		

Parada SIL, Categoria de parada 1, Categoria de fiação 3/4

Figura 23 - Exemplo: Parada SIL, Categoria de parada 1, Categoria de fiação 3/4[34]

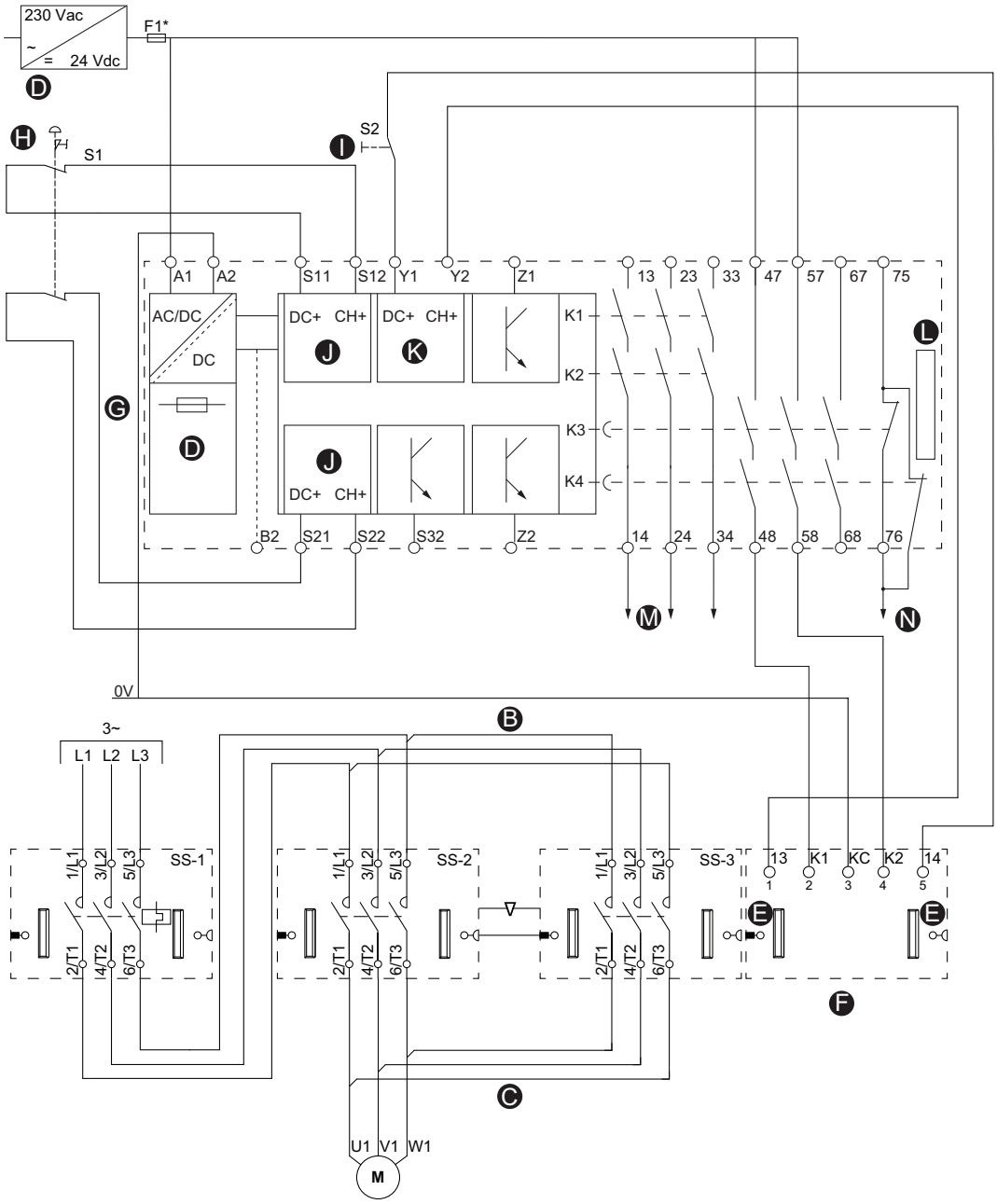


Tabela 15 - Legenda para exemplo de : Parada SIL, Categoria de parada 1, Categoria de fiação 3/4, página 54

B	Barramento superior	I	Botão de partida S2
C	Barramento inferior	J	Inib.
D	Fonte de alimentação	K	Partindo
E	Conector de cabo flat	L	Extensão

34. Nível de integridade de segurança de acordo com a norma IEC 61508. Categoria de fiação 3/4 de acordo com a ISO 13849. Categoria de parada 1 de acordo com a EN/IEC 60204-1.

Tabela 15 - Legenda para exemplo de : Parada SIL, Categoria de parada 1, Categoria de fiação 3/4 (Continuação)

F	Módulo de interface SIL (SIM)	M	Parada controlada
G	Módulo Preventa XPS-UAF	N	Categoria de parada 1
H	Botão de parada de emergência (S1)		

Especificações técnicas

Módulo de interface SIL

Tabela 16 - Valores calculados do Módulo de interface SIL[35] (SIM)

Arquitetura	SIM					
	PFH[36]	PFD[37]	SFF[38]	HFT[39]	$MTTF_d$ (anos)	DC[40]
Categoria de fiação 1[41]	$2,10^{-10}$	$2,10^{-5}$	> 90%	1	17.459	Não relevante
Categoria de fiação 2			> 99%			90%
Categoria de fiação 3			> 99%			90%
Categoria de fiação 4			99%			99%

NOTA: Os valores de PFD e PFH são calculados com o seguinte:

- Intervalo de teste = 20 anos
- MTTR[42]=MRT[43] = 24 horas

Os requisitos arquitetônicos definidos na Tabela 3 da IEC 61508-2 e na Tabela 5 da EN 62061 são atendidos para níveis até SIL 3.

Partida SIL

Os dados a seguir ajudam a definir o nível de desempenho das partidas SIL[35].

B10: **1.000.000**

% de falhas perigosas[44]: **73%**

$B10_d$: **1.369.863**

Supondo-se um número de operações = 131.400 ciclos/ano (média de 15 ciclos/hora)

Os valores calculados da partida SIL são fornecidos nas tabelas a seguir:

Tabela 17 - Partida SIL em monocanal

Categoria de fiação[41]	SFF	HFT	$MTTF_d$ (anos)	CC
Categoria 1	27%	0	100 anos	Não relevante
Categoria 2 – Monitoramento direto	90%	0	100 anos	≥ 90%

35. Nível de integridade de segurança de acordo com a norma IEC 61508.
36. Frequência média de falha perigosa [h-1], conforme definida na IEC 61508-4
37. Probabilidade de falha perigosa sob demanda, conforme definida na IEC 61509-4.
38. Fração de falha de segurança, conforme definida na IEC 61509-4.
39. Tolerância a falhas de hardware, conforme definida na IEC 61509-4.
40. Cobertura de diagnóstico, conforme definida na IEC 61509-4.
41. Categorias de fiação 1, 2, 3 e 4 de acordo com a ISO 13849.
42. Tempo médio até o reparo, conforme definido na IEC 61509-4
43. Tempo médio de reparo, conforme definido na IEC 61509-4
44. Falha perigosa conforme definida na IEC 61508-4

Tabela 18 - Partida SIL em duplo canal

Categoria de fiação	SFF	HFT	$MTTF_d$ (anos)	CC
Categoria 3	27%	0	100 anos	≥ 90%
Categoria 4	90%	0	100 anos	≥ 99%

A relação entre PFH_d e PFD das partidas SIL, dependendo da arquitetura e do intervalo de teste, é indicada na tabela a seguir:

Tabela 19 - Partidas SIL — PFH_d e PFD

Categoria de fiação	PFH (IEC 61508)	PFD (IEC 61508) Ti=10 anos[45]	PFD (IEC 61508) Ti=5 anos[45]
Categoria 1	1,10E-06	4,80E-02	4,82E-03
Categoria 2 – Monitoramento direto	1,10E-06	4,82E-03	5,06E-04
Categoria 3	4.5E-09	—	1.30E-04
Categoria 4	2.5E-10	—	2.5E-06

Os requisitos arquitetônicos definidos na Tabela 3 da IEC 61508-2 e na Tabela 5 da EN 62061 são atendidos para níveis até SIL 2.

Uma arquitetura de Categoria 2 é necessária para atender às restrições arquitetônicas de SIL 2 (atingida utilizando Mirror In/Mirror Out de monitoramento direto).

NOTA: A detecção de falhas e a reação a falhas especificadas devem ser realizadas antes que a situação de risco seja tratada pela função de controle de segurança.

45. Intervalo de testes

Dados sobre confiabilidade

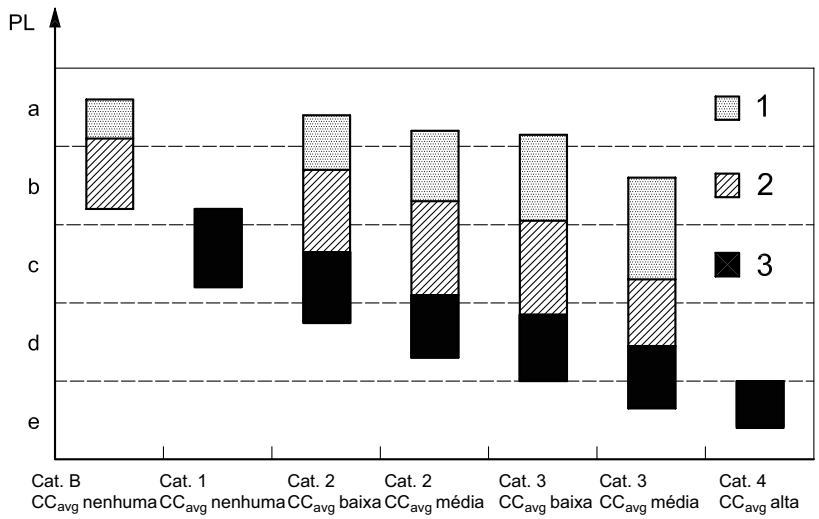
Referência de normas de função de segurança

A função de Parada SIL[46] tem prioridade sobre uma parada acionada por motivos operacionais (EN ISO 13849-1, 5.2.1).

O nível de desempenho depende da categoria de fiação[47], do $MTTF_d$ e da DC_{avg}.

O diagrama a seguir mostra o posicionamento do TeSys™ island de acordo com o requisito da categoria.

Figura 24 - Posicionamento do TeSys island por requisito de categoria



Chave

PL - Nível de desempenho

1 $MTTF_d$ de cada canal = baixa

2 $MTTF_d$ de cada canal = média

3 $MTTF_d$ de cada canal = alta

Tabela 20 - Procedimento simplificado de avaliação de PL atingido pelas partes relacionadas à segurança de sistemas de controle (SRP/CS)

Categoria	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**nenhuma**	**nenhuma**	**baixa**	**média**	**baixa**	**média**	**alta**
$MTTF_d$ de cada canal							
Baixo	a	Não coberto	a	b	b	c	Não coberto
Médio	b	Não coberto	b	c	c	d	Não coberto
Alto	Não coberto	c	v	d	d	d	e

De acordo com a arquitetura do TeSys island e a categoria de fiação, os indicadores-chave (DC_{avg}, $MTTF_d$, PL) do TeSys island são compatíveis com os valores mostrados na tabela a seguir.

46. Nível de integridade de segurança de acordo com a norma IEC 61508.
47. Categorias de fiação de acordo com a ISO 13849.

Tabela 21 - Valores de indicadores-chave para arquiteturas monocanal ou de duplo canal

Arquitetura de sistema do TeSys island	Categoria	Tolerância a falha única[48]	DC_{avg}	$MTTF_d$ de cada canal	PL de destino
Monocanal	1	Não	Nenhum	Alto (≥ 30 anos)	c
	2	Não	Baixo (≥ 60%) a médio (≥ 90%)	Baixo (≥ 3 anos) a alto (≥ 30 anos)	c, d
Duplo canal	3	Sim			c, d, e
	4	Sim	Alto (≥ 99%)	Alto (≥ 30 anos)	e

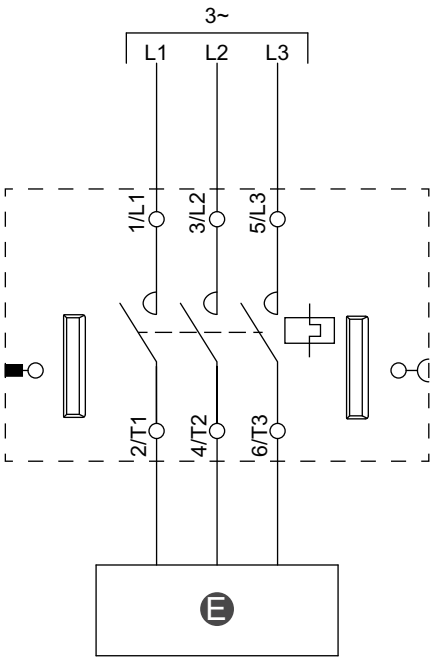
Fiação de avatares SIL

Os diagramas elétricos desta seção estão relacionados aos avatares SIL[49]. A tabela a seguir é uma legenda para os diagramas desta seção.

Tabela 22 - Legenda dos diagramas elétricos

A	Intertravamento mecânico
B	Barramento superior
C	Barramento inferior
E	Circuito elétrico

Figura 25 - Contator - Parada SIL, Cat. W. 1/2[50]



48. Tolerância a falha única significa que uma única falha (incluindo eventos de modo comum) não deve levar à perda da função de segurança.
49. Nível de integridade de segurança de acordo com a norma IEC 61508.
50. Categorias de fiação 1 e 2 de acordo com a ISO 13849.

Figura 26 - Motor com um sentido de rotação - Parada SIL, Cat. W. 1/2

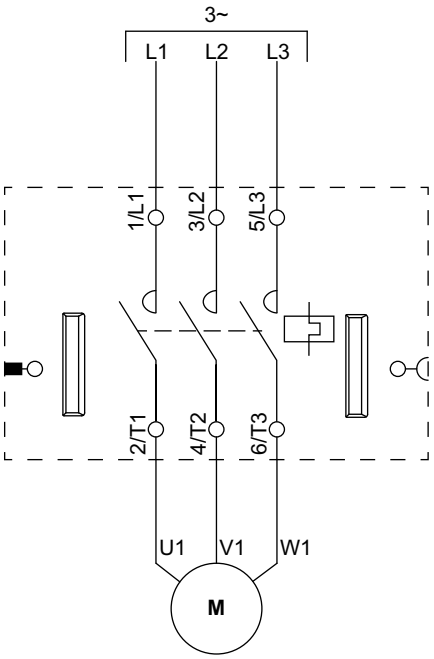


Figura 27 - Motor com dois sentidos de rotação - Parada SIL, Cat. W. 1/2

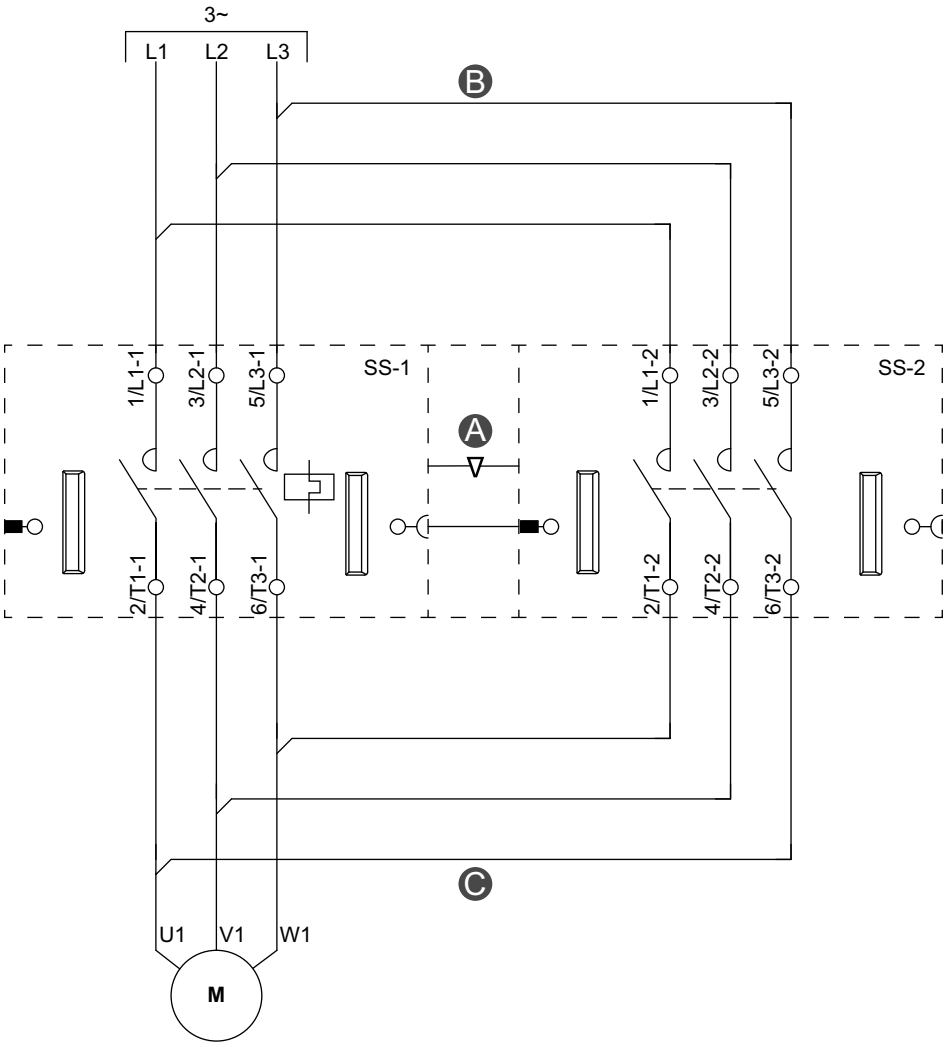


Figura 28 - Motor de duas velocidades - Parada SIL, Cat. W. 1/2

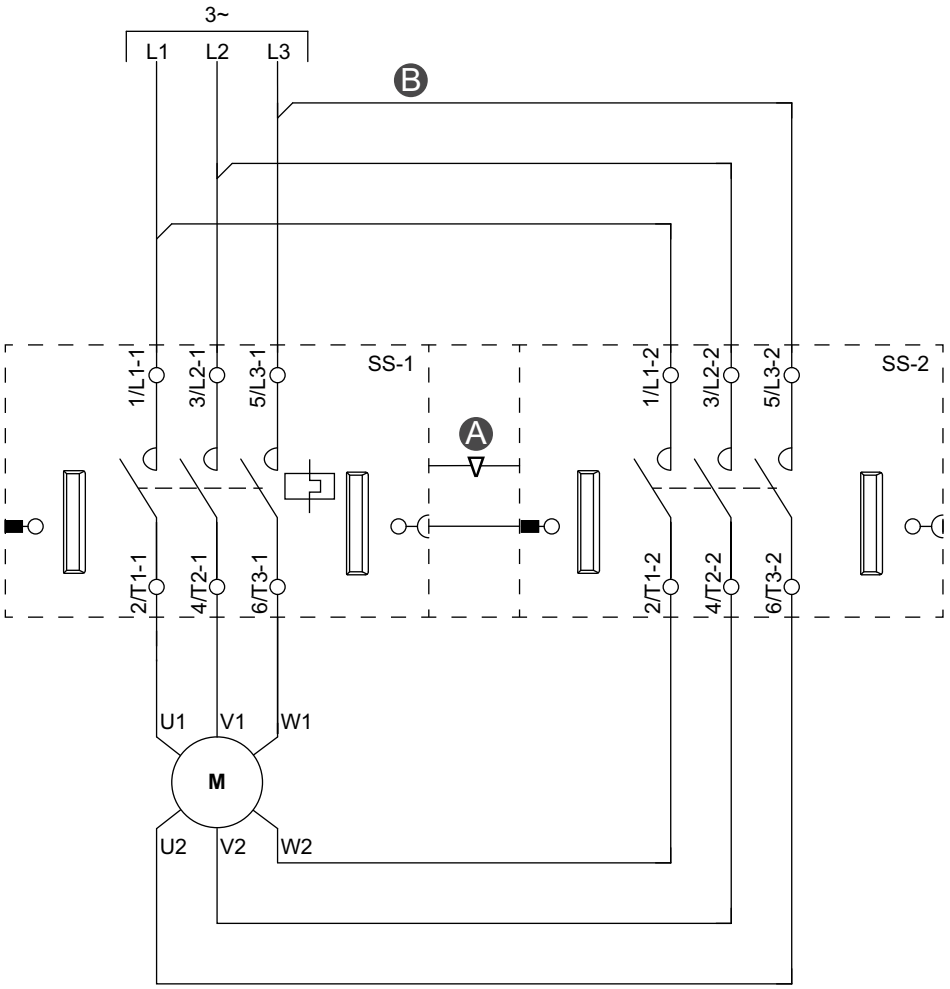


Figura 29 - Motor de duas velocidades e com dois sentidos de rotação - Parada SIL, Cat. W. 1/2

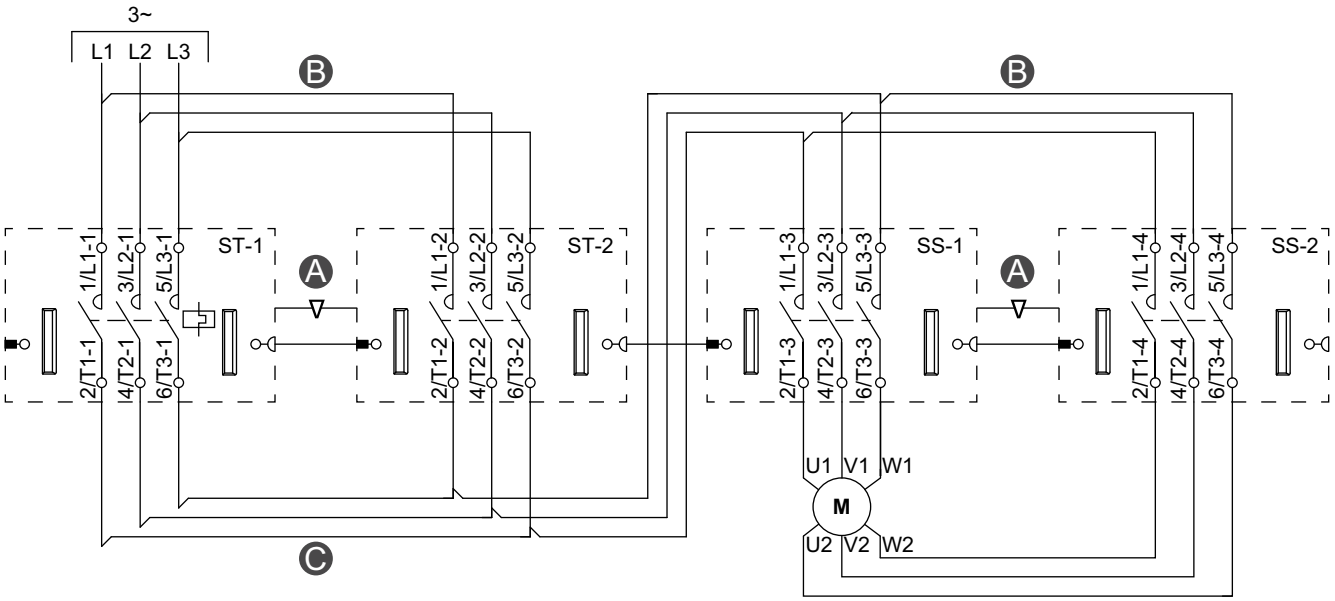


Figura 30 - Contator - Parada SIL, Cat. W. 3/4[51]

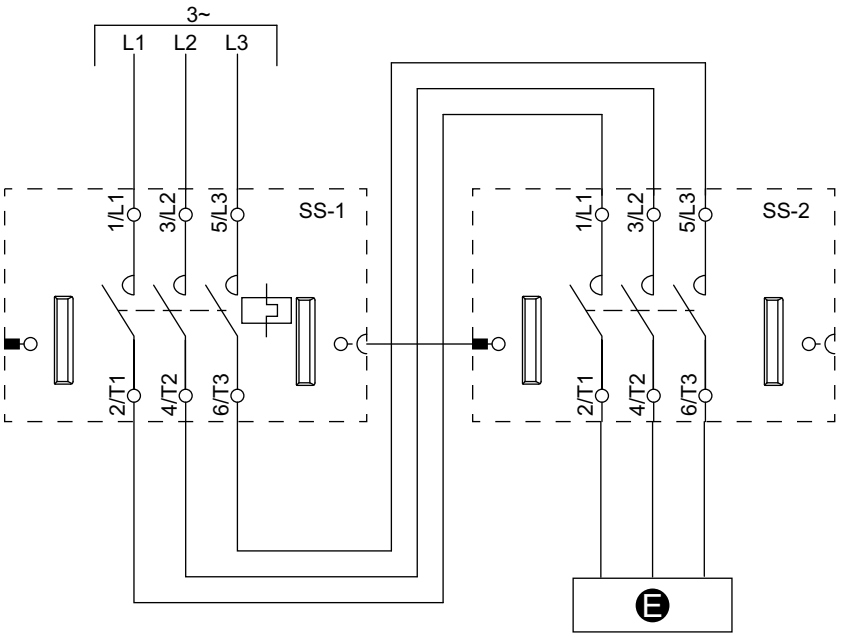
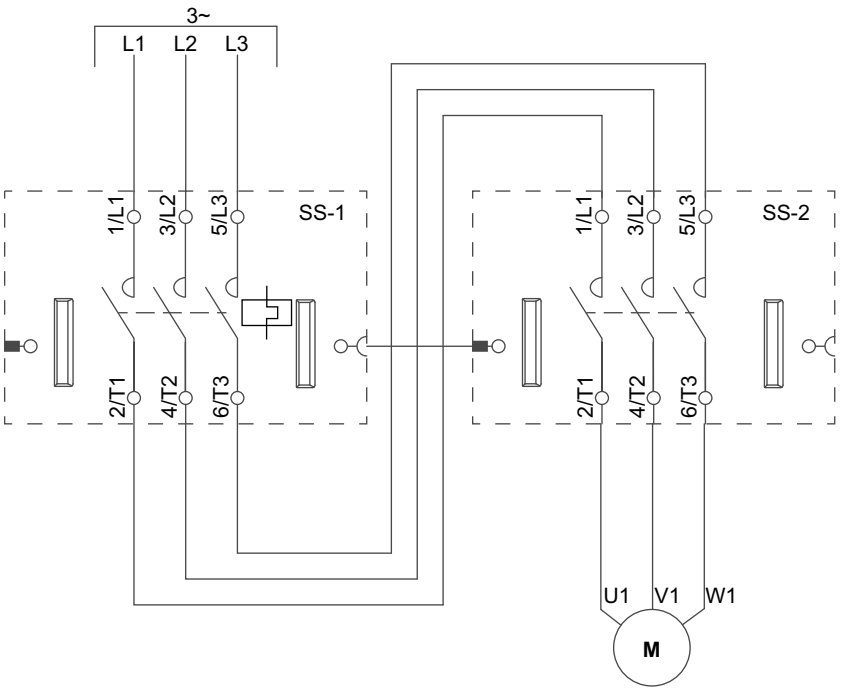


Figura 31 - Motor com um sentido de rotação - Parada SIL, Cat. W. 3/4



51. Categorias de fiação 3 e 4 de acordo com a ISO 13849.

Figura 32 - Motor com dois sentidos de rotação - Parada SIL, Cat. W. 3/4

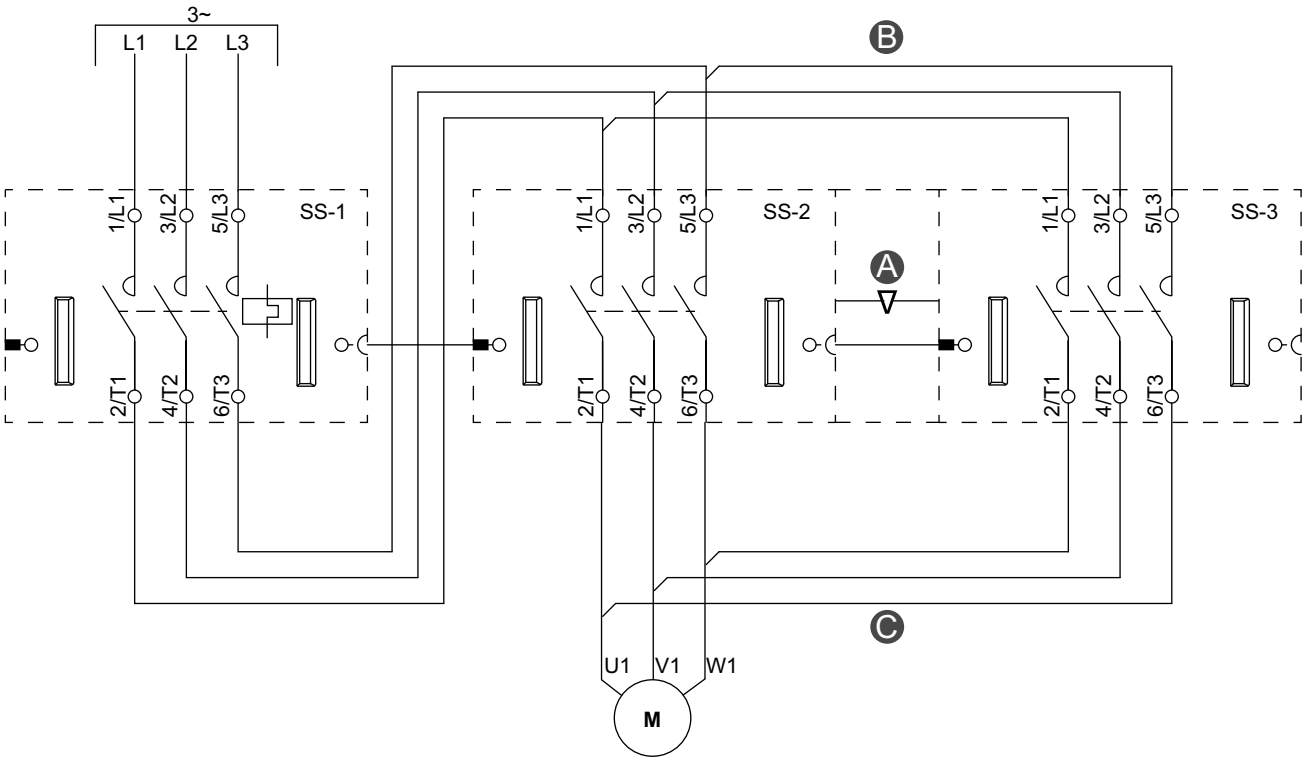


Figura 33 - Motor de duas velocidades - Parada SIL, Cat. W. 3/4

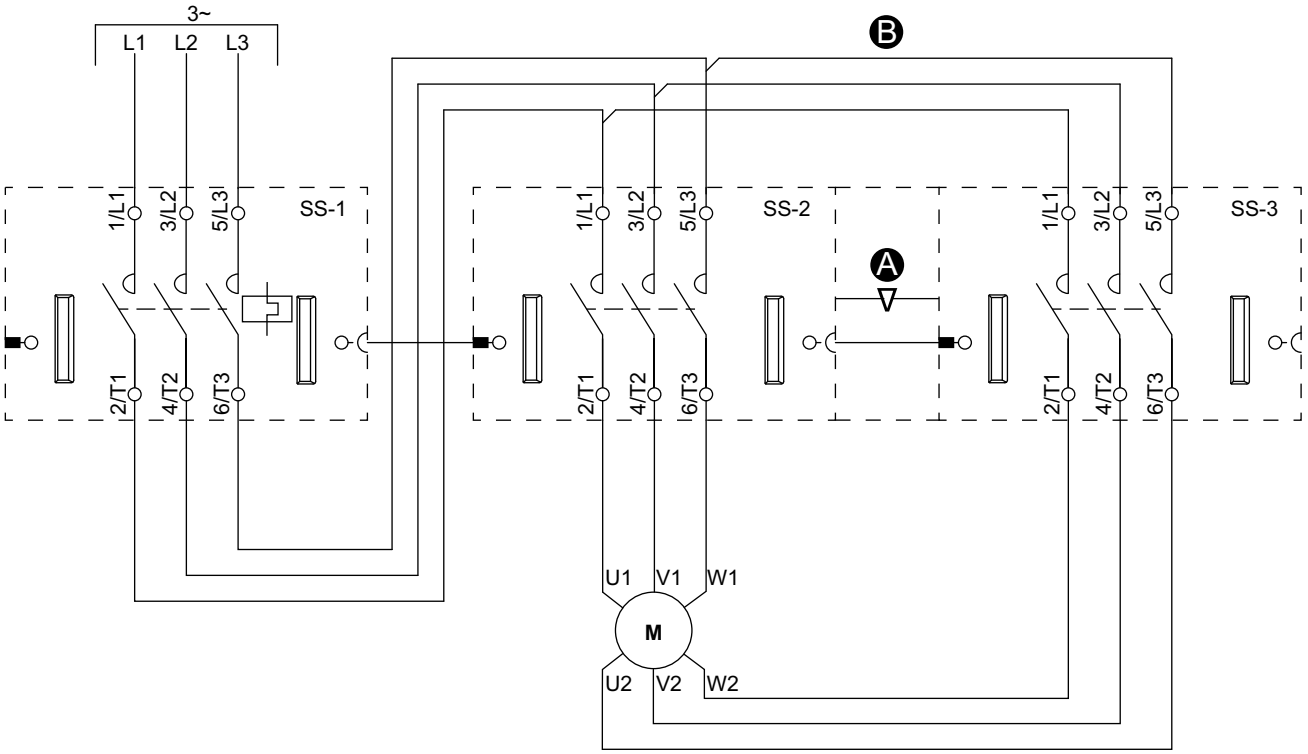


Figura 34 - Motor de duas velocidades e com dois sentidos de rotação - Parada SIL, Cat. W. 3/4

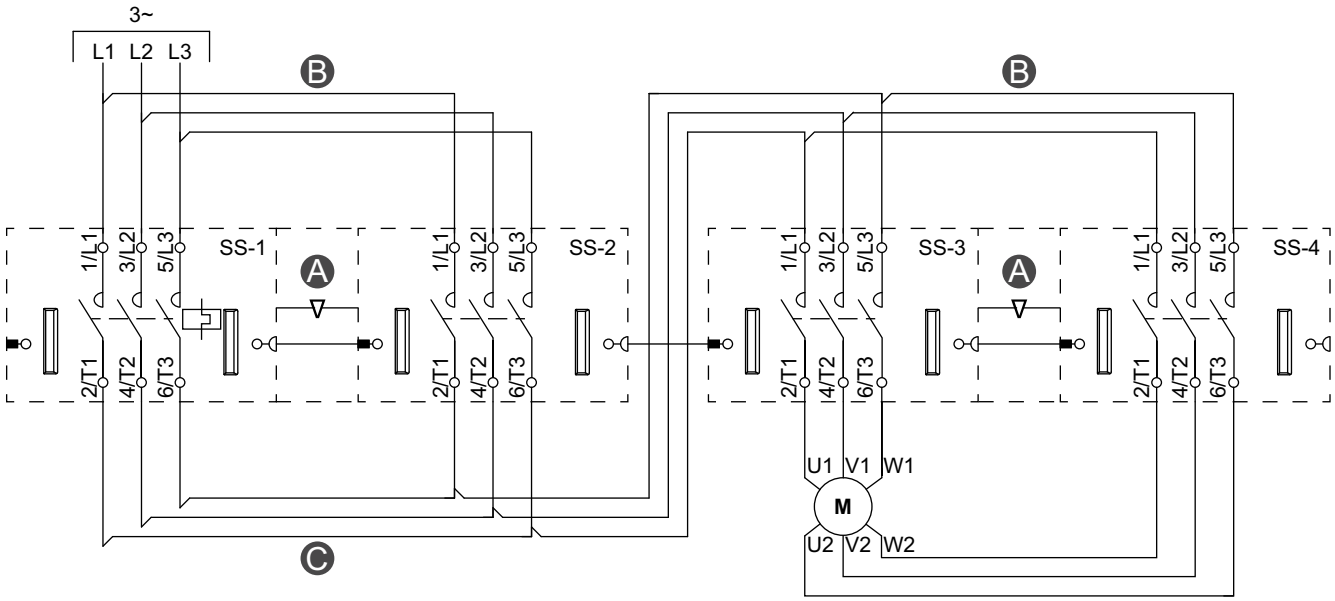


Figura 35 - Transportador com um sentido de rotação - Parada SIL, Cat. W. 1/2

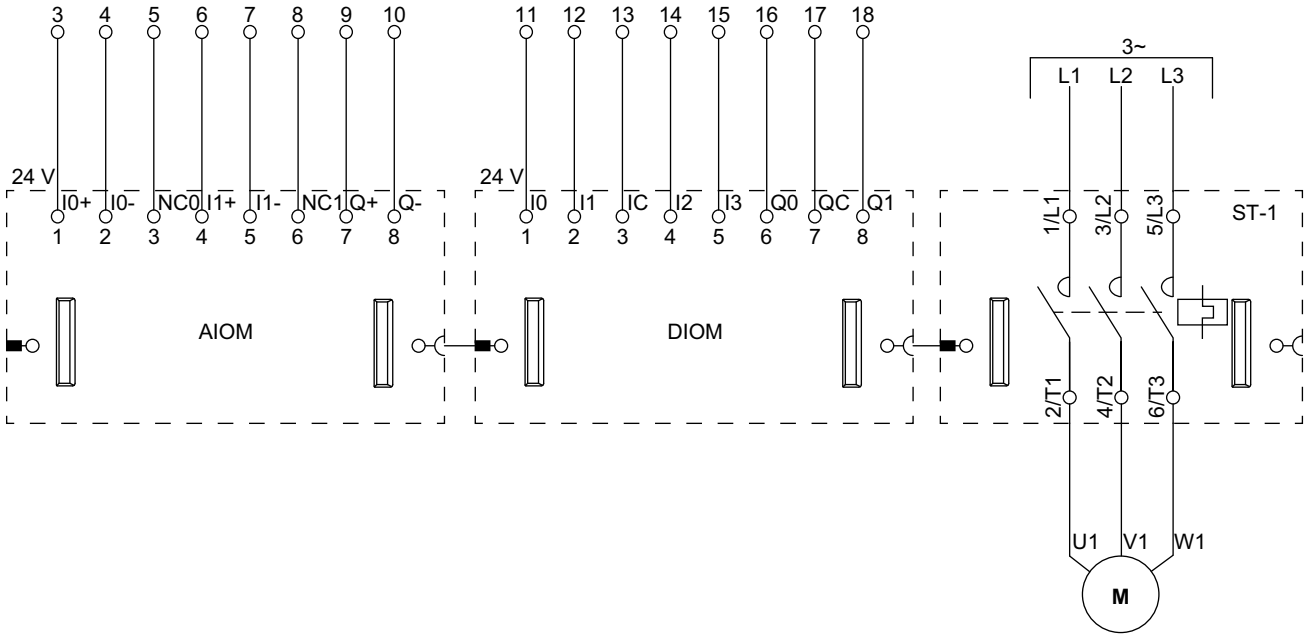
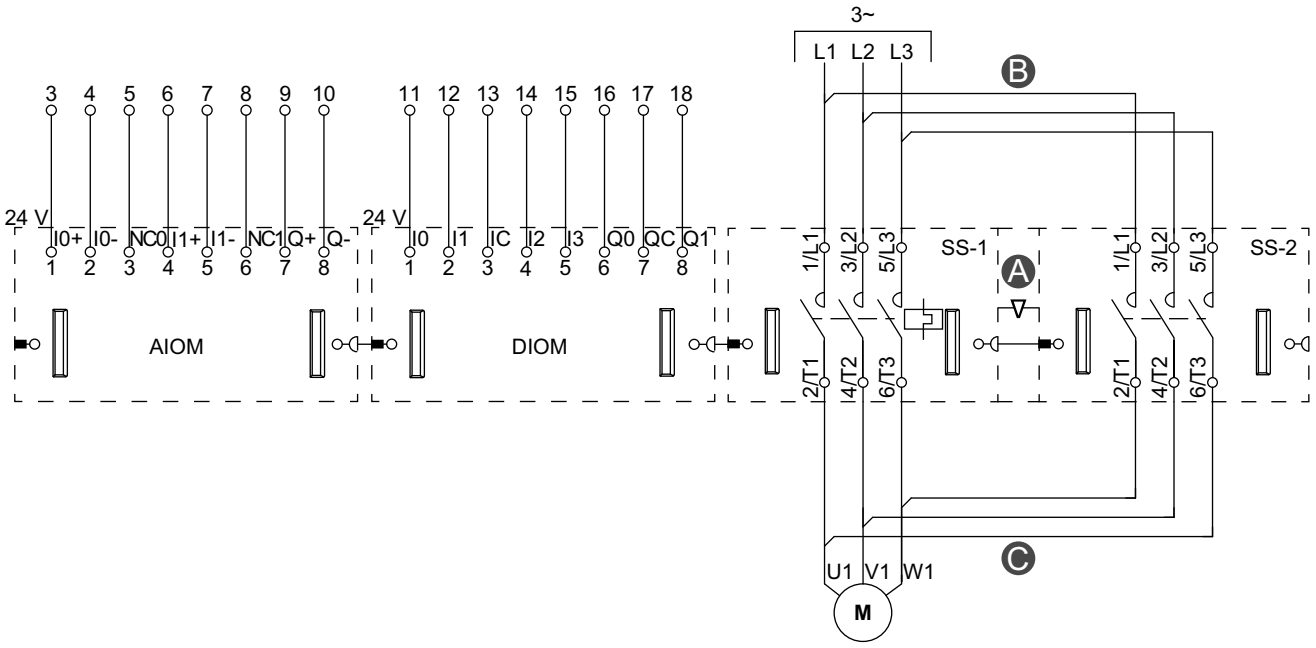


Figura 36 - Transportador com dois sentidos de rotação - Parada SIL, Cat. W. 1/2



Comissionando a função de segurança

Utilize este procedimento para comissionar a função de segurança. O procedimento tem duas etapas:

- Testes de instalação
- Testes de prova da função de segurança[52]

Testes de instalação

Execute as etapas da tabela a seguir para testar a instalação da função de segurança.

Tabela 23 - Teste de instalação

1	No painel **DIAGNÓSTICO** do DTM do TeSys ™ island, verifique se a topologia física corresponde à topologia lógica.
2	No painel **MEU AVATAR** do DTM do TeSys island, verifique nos **PARÂMETROS DE AVATAR** se os avatares SIL[53] estão associados ao grupo SIL apropriado.

Teste de prova da função de segurança

O teste de prova da função de segurança é realizado para cada grupo SIL[53] na ilha. Um grupo SIL pode compreender vários avatares SIL gerenciados por um módulo de interface SIL (SIM).

O teste de prova da função de segurança será bem-sucedido se, na ativação do dispositivo de parada de emergência associado a um grupo SIL, todas as partidas SIL pertencentes a esse grupo SIL entrarem no estado seguro (a carga é desenergizada).

NOTA: Para a Categoria de parada 0 (parada não controlada), a parada deve ser imediata. Para a Categoria de parada 1 (parada controlada), a parada é eficaz após um atraso.[54]

Execute as etapas na tabela a seguir para cada grupo SIL na ilha para realizar o teste de prova da função de segurança.

52. Teste de prova segundo definido na IEC 62061
53. Nível de integridade de segurança de acordo com a norma IEC 61508.
54. Categorias de parada 0 e 1 de acordo com a EN/IEC 60204-1.

Tabela 24 - Teste de prova da função de segurança

1	Ative o dispositivo de parada de emergência associado ao grupo SIL e verifique se todas as partidas SIL pertencentes ao grupo entram no estado seguro (a carga é desenergizada). **NOTA:** O LED de Status do dispositivo (DS) piscará em vermelho nas partidas SIL, indicando um estado de Evento menor do dispositivo. Se o teste falhar: • O dispositivo de parada de emergência pode estar conectado ao SIM errado. Verifique essas conexões. • O dispositivo de parada de emergência pode não estar corretamente cabeado ao SIM. Verifique essas conexões. • Alguns avatares SIL podem não estar conectados ao Grupo SIL esperado. Verifique a configuração.
2	No painel **AVATARES** da OMT ou do DTM do TeSys™ island, na seção **DIAGNÓSTICO**, verifique no **STATUS** e nos **REGISTROS DE EVENTOS** se o **Status do grupo SIL** é igual a "**Comando de parada**". No Registro de eventos, ele será “SIL Group Stop cmd, Safe State achieved”. Se o teste falhar: • Alguns avatares SIL podem não estar conectados ao Grupo SIL esperado. Verifique a configuração.
3	Na seção **DISPOSITIVOS** do painel **DIAGNÓSTICO**, verifique se o **Status do módulo de interface SIL (SIM)** é igual a "**Comando de parada**". No Registro de eventos, ele será “SIL Group Stop cmd, Safe State achieved”. Se o teste falhar: • O dispositivo de parada de emergência pode estar conectado ao SIM errado. Verifique essas conexões. • O dispositivo de parada de emergência pode não estar corretamente cabeado ao SIM. Verifique essas conexões.
4	Aplique um comando de Partida a um avatar SIL pertencente ao grupo SIL e verifique se a partida falha: as partidas devem permanecer abertas, e o comando de Partida deve ser desconsiderado até que o dispositivo de parada de emergência seja reinicializado. Se o teste falhar: • Alguns avatares SIL podem não estar conectados ao Grupo SIL esperado. Verifique a configuração. Se algum desses testes continuar a falhar apesar das medidas corretivas, não continue operando a ilha. Substitua os dispositivos que falharam nos testes.
5	Depois que o teste de prova da função de segurança estiver concluído, reinicialize o dispositivo de parada de emergência e verifique se todas as partidas SIL e os módulos de interface SIL estão no estado Pronto (o LED DS fica verde estático).

Requisitos de manutenção da função de segurança

Esta seção descreve a manutenção de rotina exigida para manter a segurança funcional em seu TeSys ™ island.

Cronograma de manutenção

Os intervalos de manutenção dependem do modo de frequência.

- Para o modo de Baixa frequência (o número médio anual de ciclos de contator é inferior a 15 ciclos/hora), realize a manutenção a cada 12 meses.
- Para o modo de Alta frequência (o número médio anual de ciclos de contator é superior a 15 ciclos/hora ou 136.986 ciclos/ano), realize a manutenção em intervalos que sejam iguais a 1/10 do tempo de vida estimado do dispositivo.

Tempo de vida estimado (em anos) do dispositivo = B10d (=1.369.863)/número médio anual de ciclos de contator

Verificações de manutenção

Verificações de utilização de dispositivo

Execute as verificações descritas na tabela a seguir para determinar se os ciclos de contator da partida SIL[55] estão dentro dos valores de tempo de vida útil aceitáveis.

1	Com o recurso de **DIAGNÓSTICO** de dispositivos da OMT ou do DTM do TeSys™ island, acesse as informações de ativo do dispositivo de cada partida SIL.
2	Se o **Número de ciclos de contator** for maior do que B10d (= 1.369.863), substitua a partida SIL.
3	Se não, use o valor do **Número de ciclos de contator** para agendar a próxima manutenção. Consulte Cronograma de manutenção, página 68.

Teste de prova da função de segurança

Execute o Teste de prova da função de segurança em cada grupo SIL[55] . Consulte Teste de prova da função de segurança, página 66.

55. Nível de integridade de segurança de acordo com a norma IEC 61508.

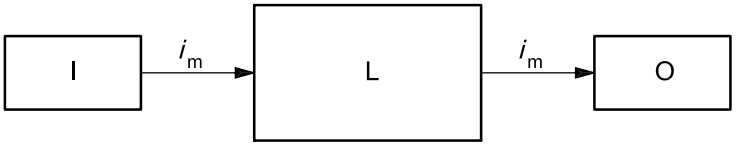
Apêndice: Arquitetura monocanal

Essa arquitetura monocanal abrange as Categorias de fiação 1 e 2.

Requisitos arquitetônicos para a Categoria de fiação 1

A arquitetura designada para a **Categoria 1** é definida na norma EN ISO 13849-1, 6.2.4.

Figura 37 - Arquitetura designada para a Categoria 1 (EN ISO 13849-1)



I: dispositivo de entrada

L: lógica

O: dispositivo de saída

^{i}m: meio de interconexão

O SRP/CS, a parte relacionada à segurança do sistema de controle da Categoria de fiação 1, deve ser projetado e construído utilizando **componentes comprovados**.

Um “componente comprovado” para uma aplicação relacionada à segurança é um componente que foi:

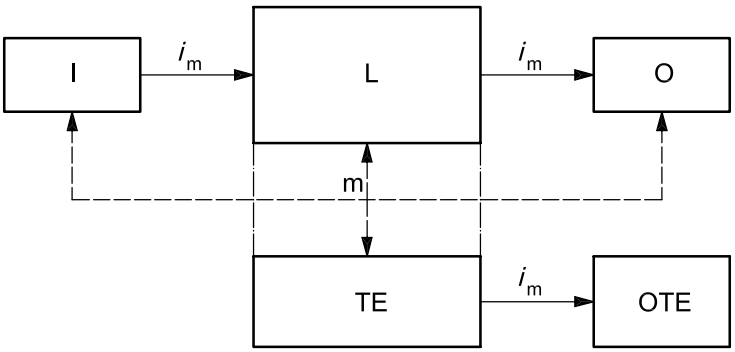
- amplamente utilizado no passado com resultados bem-sucedidos em aplicações similares; ou
- produzido e verificado utilizando princípios que demonstram sua adequação e confiabilidade para aplicações relacionadas à segurança.

Não há cobertura de diagnóstico (DC_{avg} = nenhuma) dentro de sistemas de Categoria 1.

Requisitos arquitetônicos para a Categoria de fiação 2

A arquitetura designada para a **Categoria 2** é definida na norma EN ISO 13849-1, 6.2.5.

Figura 38 - Arquitetura designada para a Categoria 2 (EN ISO 13849-1)



I: dispositivo de entrada

L: lógica

O: dispositivo de saída

^{i}**m**: meio de interconexão

m: monitoramento

TE: equipamento de teste

OTE: saída de TE

O SRP/CS, a parte relacionada à segurança do sistema de controle da Categoria de fiação 2, deve ser projetado de formada que sua(s) função(ões) seja(m) verificada(s) em intervalos apropriados pelo sistema de controle da máquina.

Na arquitetura monocanal, um SIM é associado a uma partida SIL[56].

Especificamente, para a Categoria de fiação 2, o contato espelho é conectado ao módulo Preventa™ XPS (ou equivalente). Se o estado da linha de feedback do contato espelho não for igual ao estado de saída do módulo Preventa XPS (ou equivalente), o módulo Preventa XPS (ou equivalente) bloqueará uma segunda partida.

NOTA: O feedback do contato espelho transmite apenas informações de diagnóstico.

56. Nível de integridade de segurança de acordo com a norma IEC 61508.

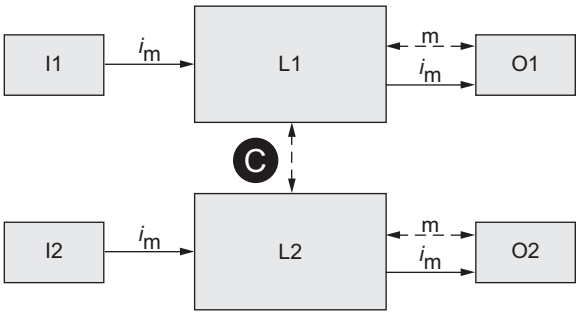
Apêndice: Arquitetura de duplo canal

Essa arquitetura de duplo canal abrange as Categorias de fiação 3 e 4.

Requisitos arquitetônicos para a Categoria de fiação 3

A arquitetura designada para a Categoria 3 é definida na EN ISO 13849-1, 6.2.6.

Figura 39 - Arquitetura designada para a Categoria 3 (EN ISO 13849-1)



im: meio de interconexão

L1, L2: lógica

c: monitoramento cruzado

m: monitoramento

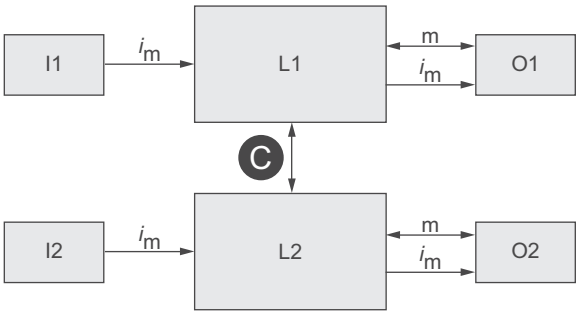
I1, I2: dispositivo de entrada, por ex.: um sensor

O1, O2: dispositivo de saída, por ex.: contator principal

Requisitos arquitetônicos para a Categoria de fiação 4

A arquitetura designada para a Categoria 4 é definida na EN ISO 13849-1, 6.2.7.

Figura 40 - Arquitetura designada para a Categoria 4 (EN ISO 13849-1)



im: meio de interconexão

L1, L2: lógica

c: monitoramento cruzado

m: monitoramento

I1, I2: dispositivo de entrada, por ex.: um sensor

O1, O2: dispositivo de saída, por ex.: contator principal

Linhas sólidas para monitoramento representam uma cobertura de diagnóstico superior à da arquitetura designada para a categoria 3.

Glossário

A

Frequência média de falha perigosa [h^{-1}] (PFH). (Falha perigosa conforme definida na IEC 61508-4)

Para manter a função de segurança, a norma IEC 61508 requer vários níveis de medidas para evitar e controlar erros detectados, dependendo do SIL[57] exigido.

Todos os componentes de uma função de segurança devem ser submetidos a uma avaliação de probabilidade para avaliar a eficácia das medidas implementadas para controlar falhas detectadas.

Essa avaliação determinou a PFH (Frequência média de falha perigosa[58] [h^{-1}]) para um sistema relacionado à segurança. Essa é a probabilidade, por hora, de que um sistema relacionado à segurança falhe de forma perigosa e de que a função de segurança não possa ser executada corretamente.

Dependendo do SIL, a PFH não deve exceder determinados valores para todo o sistema relacionado à segurança.

Os valores de PFH individuais de uma cadeia de funções são somados. O resultado não deve exceder o valor máximo especificado na norma.

Nível de integridade de segurança	**Frequência média de falha perigosa[58] [h^{-1}] (PFH) em alta demanda ou demanda contínua**
4	$10^{-9} \leq — < 10^{-8}$
3	$10^{-8} \leq — < 10^{-7}$
2	$10^{-7} \leq — < 10^{-6}$
1	$10^{-6} \leq — < 10^{-5}$

E

Norma EN ISO 13849

Essa Norma Europeia especifica o processo de validação, incluindo análise e avaliação de riscos e testes, para as funções de segurança e categorias das partes relacionadas à segurança de sistemas de controle. As descrições das funções de segurança e os requisitos das categorias são apresentados na ISO 13849-1, que abrange os princípios gerais de projeto. Alguns requisitos para validação são gerais e outros são específicos à tecnologia utilizada. A EN ISO 13849-2 também especifica as condições sob as quais deve ser executada a validação por meio de testes das partes relacionadas à segurança de sistemas de controle.

Norma EN/IEC 60204-1

A Categoria de parada 0 é definida como “a parada pela remoção imediata da energia dos mecanismos da máquina (ou seja, uma parada não controlada)”.

57. Nível de integridade de segurança de acordo com a norma IEC 61508.
58. Falha perigosa conforme definida na IEC 61508-4

A Categoria de parada 1 é definida como “uma parada controlada com energia disponível para os mecanismos da máquina a fim de atingir a parada e, depois, a remoção da energia, quando a parada for atingida”.

F

Medidas de contenção de falhas

Os erros sistemáticos nas especificações, no hardware e no software, as falhas de uso e as falhas de manutenção no sistema relacionado à segurança devem ser evitados ao máximo possível. Para atender a esses requisitos, a IEC 61508 especifica várias medidas de contenção de falhas que devem ser implementadas, dependendo do SIL[59] necessário. Essas medidas devem cobrir todo o ciclo de vida do sistema relacionado à segurança, ou seja, do projeto ao descomissionamento do sistema.

Segurança funcional

A automação e a engenharia de segurança funcional são duas áreas que antes ficavam completamente separadas, mas recentemente se tornaram mais integradas.

A engenharia e instalação de soluções complexas de automação são simplificadas pelas funções de segurança integradas.

Geralmente, os requisitos de engenharia de segurança funcional dependem da aplicação.

O nível de requisitos resulta do risco e do potencial de danos da aplicação específica.

H

Tolerância a falhas de hardware (HFT) e Fração de falha de segurança (SFF)

Dependendo do SIL[59] do sistema relacionado à segurança, a norma IEC 61508 requer uma tolerância a falhas de hardware (HFT) específica em conexão a uma proporção específica de falhas de segurança, mostrada como Fração de falha de segurança (SFF).

A HFT é a capacidade de um sistema de executar a função de segurança necessária a despeito da presença de uma ou mais falhas de hardware.

A SFF de um sistema é definida como a proporção da taxa de falhas de segurança em relação à taxa total de falhas do sistema.

De acordo com a IEC 61508, o SIL máximo para um sistema é parcialmente determinado pela HFT e pela SFF do sistema.

Esses tipos são especificados de acordo com os critérios definidos pela norma para os elementos relacionados à segurança.

SFF	**Subsistema HFT tipo A**			**Subsistema HFT tipo B**		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	—	SIL 1	SIL 2
60% – < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% – < 99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

59. Nível de integridade de segurança de acordo com a norma IEC 61508.

I

Norma IEC 61508

A norma IEC 61508 abrange a segurança funcional de sistemas elétricos/eletrônicos/eletrônicos programáveis relacionados à segurança.

Em vez de um único componente, uma cadeia de funções inteira (por exemplo, de um sensor, através das unidades de processamento lógico e até o mecanismo) é considerada uma unidade.

Essa cadeia de funções deve atender aos requisitos do nível de integridade de segurança específico como um todo.

L

Modo de baixa/alta demanda

A IEC 61508 define o modo de demanda de função de segurança da operação:

- alta demanda ou modo contínuo (PFH)
- modo de baixa demanda (PFDavg, PTI)

M

Tempo médio até uma falha perigosa ($MTTF_d$)

A norma ISO 13849-1 define o $MTTF_d$ como a expectativa do tempo médio até uma falha perigosa.

P

Nível de desempenho (PL)

A norma IEC 13849-1 define cinco níveis de desempenho (PL) para funções de segurança.

O nível a é o nível mais baixo, e o nível e é o mais alto.

Os cinco níveis (a, b, c, d, e e) correspondem a diferentes valores de probabilidade média de falha perigosa[60] por hora.

Nível de desempenho	Probabilidade de falha perigosa[60] por hora
e	$\geq 10^{-8}$ a $< 10^{-7}$
d	$\geq 10^{-7}$ a $< 10^{-6}$
c	$\geq 10^{-6}$ a $< 3 \times 10^{-6}$
b	$\geq 3 \times 10^{-6}$ a $< 10^{-5}$
a	$\geq 10^{-5}$ a $< 10^{-4}$

S

60. Falha perigosa conforme definida na IEC 61508-4

Nível de integridade de segurança (SIL)

A norma IEC 61508 define quatro níveis de integridade de segurança (SIL) para funções de segurança.

SIL 1 é o nível de integridade mais baixo, e SIL 4 é o mais elevado.

Uma análise e avaliação de riscos serve de base para determinar o nível de integridade de segurança exigido.

Isso é usado para decidir se a cadeia de funções relevante deve ser considerada como uma função de segurança e qual risco potencial ela deve cobrir.

Schneider Electric
800 Federal Street
01810 Andover, MA
EUA

https://www.schneider-electric.com/en/work/support/

www.schneider-electric.com

Uma vez que padrões, especificações e design mudam de vez em quando, peça para confirmar as informações fornecidas nesta publicação.

8536IB1904PTBR-04