www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publicação: SAFEBK-RM002B-PT-P —Março de 2011
Substitui a publicação: SAFEBK-RM002A-PT-P

SAFEBOOK 4 - Sistemas de controle relacionados à segurança de máquinas / Princípios, padrões e implementação

SAFEBOOK 4

LISTEN. THINK. SOLVE.℠

Allen-Bradley

Guardmaster®

Sistemas de controle relacionados à segurança de máquinas

Princípios, padrões e implementação

Rockwell Automation

Índice

Diretivas e legislação de UE

O objetivo desta seção é atuar como um guia para qualquer pessoa preocupada com a segurança de máquinas, especialmente os sistemas de proteção e guarda da União Europeia. Destina-se a projetistas e usuários de equipamentos industriais.

A fim de promover o conceito de mercado aberto dentro do Espaço Econômico Europeu - EEE (que compreende todos os estados-membros da UE, mais três outros países) todos os estados-membros são obrigados a adotar uma legislação que defina os requisitos essenciais de segurança para o uso de máquinas.

As máquinas que não satisfaçam esses requisitos não podem ser fornecidas para ou dentro dos países do EEE.

Existem várias diretrizes europeias que podem ser aplicadas à segurança de máquinas e equipamentos industriais, mas as duas que apresentam a mais direta relevância são:

1 A diretiva de máquinas

2 O uso de equipamentos no trabalho pelos operários na diretriz de trabalho

Essas duas diretrizes estão diretamente relacionadas como requisitos essenciais de segurança e saúde (EHSR), presentes na diretriz de máquinas, podem ser utilizadas para confirmar a segurança dos equipamentos diretriz de uso de equipamentos no trabalho.

Esta seção trata de aspectos das duas diretrizes e é altamente recomendável que qualquer pessoa preocupada com o projeto, fornecimento, aquisição ou uso de equipamentos industriais dentro ou para o EEE e, também, determinados países europeus, se familiarizem com seus requisitos. A maioria dos fornecedores e usuários de máquinas simplesmente não poderá fornecer ou operar máquinas nesses países, a menos que cumpram com essas diretrizes.

Existem outras diretrizes europeias que podem ter relevância para as máquinas. A maioria delas é bastante especializada em sua aplicação e, portanto, excluída do escopo desta seção, mas é importante observar que, quando pertinentes, seus requisitos também devem ser cumpridos. Os exemplos incluem: a diretriz EMC 2004/108/CE e a diretriz ATEX 94/9/EC.

A diretriz de máquinas

A diretriz de máquinas abrange o fornecimento de novas máquinas e outros equipamentos, inclusive componentes de segurança. É um delito fornecer máquinas dentro da UE, a menos que sejam cumpridas as disposições e requisitos da diretriz.

A definição mais ampla de “máquinas”, conforme a diretriz, é enunciada a seguir: um conjunto, equipado ou destinado a ser equipado com um sistema de inversores, ao invés da aplicação direta do esforço humano ou animal, consistindo em peças ou componentes vinculados, com pelo menos uma peça ou componente móvel, unidas para uma aplicação específica.

Marcação CE afixada na máquina

A diretriz de máquinas atual (2006/42/EC) substitui a versão anterior (98/37/EC) no final de 2009. Ela traz esclarecimentos e alterações, mas não introduz nenhuma mudança radical em seus requisitos essenciais de saúde e segurança (EHSRs). Ela introduz algumas mudanças para atender às alterações na tecnologia e nos métodos. Estende seu escopo para cobrir alguns tipos adicionais de equipamentos (por exemplo, guindastes da construção civil). Agora existe um requisito explícito de avaliação de risco para a determinação dos quais EHSRs são aplicáveis; existem alterações feitas nos procedimentos de avaliação da conformidade de equipamentos do Anexo IV.

As principais disposições da diretriz original (98/37/CE) entraram em vigor para máquinas em 1º de janeiro de 1995 e, para componentes de segurança, em 1º de janeiro de 1997.

As disposições da diretriz atual (2006/42/CE) tornaram-se aplicáveis em 29 de dezembro de 2009. É responsabilidade do fabricante ou de seu representante autorizado a garantia de que o equipamento fornecido está em conformidade com a diretriz. Isso inclui:

- A garantia de cumprimento dos EHSRs aplicáveis contidos no Anexo I da diretriz
- É preparado um arquivo técnico
- É realizada a avaliação de conformidade adequada
- É fornecida uma “Declaração de Conformidade CE”
- A marcação CE é afixada no devido local
- São fornecidas instruções de uso seguro

Requisitos essenciais de saúde e segurança

A máquina deve atender às EHSRs

O Anexo 1 da diretriz fornece uma lista de requisitos essenciais de saúde e segurança (conhecidos como EHSR) que as respectivas máquinas devem cumprir, quando for o caso. O objetivo desta lista é garantir que a máquina seja segura, projetada e construída de forma que possa ser utilizada, ajustada e conservada ao longo de todas as fases da sua vida útil, sem colocar pessoas em risco.
O texto a seguir fornece características gerais rápidas de alguns requisitos típicos, mas é importante considerar todos os EHSR constantes no Anexo 1.

A avaliação de risco deve ser efetuada para determinar quais EHSR são aplicáveis ao equipamento em questão.

Os EHSR do Anexo 1 fornecem uma hierarquia de medidas para eliminação do risco:

(1) Projeto inerentemente seguro. Quando possível, o próprio projeto evitará qualquer perigo.

Quando isso não for possível, devem ser utilizados **(2) dispositivos de proteção adicionais**, por exemplo, guardas com pontos de acesso intertravados, barreiras não-materiais, tais como cortinas de luz, esteiras de detecção, etc.

Quaisquer riscos residuais que não puderem ser resolvidos com os métodos acima devem ser contidos por **(3) equipamentos de proteção individual e/ou treinamento**. O fornecedor da máquina deve especificar o que é adequado.

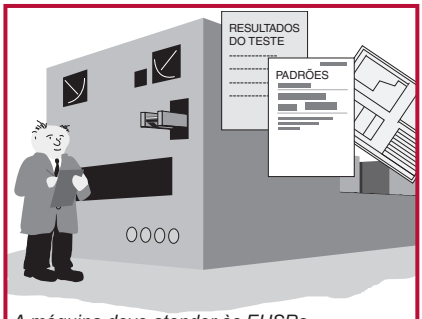
Materiais adequados devem ser utilizados na construção e operação. Devem ser providenciadas instalações adequadas de manuseio e iluminação. Os controles e sistemas de controle devem ser seguros e confiáveis. As máquinas não devem ser capazes de inicializarem inesperadamente e devem ser equipadas com um ou mais dispositivos de parada de emergência. Deve-se tomar cuidado com instalações complexas onde os processos a montante ou a jusante podem afetar a segurança de uma máquina. A falha em uma fonte de alimentação ou no circuito de controle não deve levar a uma situação perigosa. As máquinas devem ser estáveis e capazes de suportar tensões previsíveis. Elas não devem ter bordas expostas ou superfícies suscetíveis de causar lesões.

Devem ser utilizados dispositivos de proteção ou guardas para proteger de riscos, tais como peças móveis. Estes devem ter estrutura robusta e dificuldade para ignorar. As guardas fixas devem ser montadas por métodos que somente as permita remover com ferramentas. As guardas móveis devem ser intertravadas. As guardas ajustáveis devem ser facilmente fixadas, sem o uso de ferramentas.

Devem ser evitados os perigos elétricos e outros riscos do fornecimento de energia elétrica. Deve haver o mínimo risco de lesões por conta de temperatura, explosão, ruído, vibração, poeira, gases ou radiação. Deve haver disposições adequadas de manutenção e serviços. Devem ser fornecidos dispositivos de advertência e indicação suficientes. As máquinas devem vir acompanhadas de instruções de instalação, uso, ajuste, etc., com segurança.

Avaliação de conformidade

O projetista ou outro órgão responsável deve ser capaz de mostrar evidências que comprovem a conformidade com os EHSRs. Este arquivo deve incluir todas as informações relevantes, tais como resultados de testes, diagramas, especificações, etc.



A máquina deve atender às EHSRs

O padrão europeu harmonizado (EN), que consta do Jornal Oficial da União Europeia (JO) no âmbito da diretriz de máquinas e cuja data de cessação da presunção de conformidade não expirou, confere uma presunção de conformidade com determinados EHSRs. (Muitos padrões recentes listados no JO incluem uma referência cruzada identificando os EHSRs abrangidos pelo padrão).

Portanto, nos pontos em que o equipamento está em conformidade com esses atuais padrões europeus harmonizados, a tarefa de demonstrar a conformidade com os EHSRs é bastante simplificada e o fabricante também se beneficia de maior certeza legal. Esses padrões não são legalmente obrigatórios; no entanto, sua utilização é altamente recomendável, pois a prova da conformidade através de métodos alternativos pode ser um problema extremamente complexo. Esses padrões suportam a diretriz de máquinas e são produzidos pelo CEN (Comitê Europeu de Padronização) em cooperação com a ISO e o CENELEC (Comitê Europeu de Padronização Eletrotécnica) e em cooperação com a IEC.

Deve ser realizada uma avaliação de risco completa e documentada para garantir que todos os potenciais perigos da máquina sejam considerados. Da mesma forma, é de responsabilidade do fabricante da máquina garantir que todos os EHSR sejam cumpridos, mesmo aqueles que não são abordados nos padrões harmonizados EN.

Arquivo técnico

O fabricante ou seu representante autorizado deve preparar um arquivo técnico para fornecer evidências da conformidade com os EHSRs. Este arquivo deve incluir todas as informações relevantes, tais como resultados de testes, diagramas, especificações, etc.

Não é essencial que todas as informações estejam permanentemente disponíveis como cópia impressa, mas deve ser possível disponibilizar todo arquivo técnico para inspeção, por solicitação de uma autoridade competente (um órgão indicado por um país da UE para monitorar a conformidade das máquinas).

No mínimo, deve ser incluída a seguinte documentação em um arquivo técnico:

1. Diagramas esquemáticos do equipamento, incluindo diagramas do circuito de controle.

2. Diagramas detalhados, notas de cálculo, etc., necessários à verificação da conformidade da máquina com os EHSRs.

3. Documentação de avaliação de risco, incluindo uma lista dos requisitos essenciais de saúde e segurança aplicáveis às máquinas e uma descrição das medidas de proteção implementadas.

4 Uma lista de padrões e outras especificações técnicas utilizadas, indicando os requisitos essenciais de saúde e segurança cobertos.

5 Uma descrição dos métodos adotados para eliminar os riscos apresentados pelas máquinas.

6 Se for o caso, quaisquer relatórios ou certificados técnicos obtidos de uma instalação de testes ou de outro órgão.

7 Se a conformidade for declarada com um padrão europeu harmonizado, qualquer relatório técnico que contenha os respectivos resultados de testes.

8 Uma cópia das instruções da máquina.

9 Quando for adequado, a declaração de incorporação das máquinas semiacabadas incluídas e as instruções de montagem relevantes para essas máquinas.

10 Quando for adequado, cópias da declaração CE de conformidade de máquinas ou outros produtos incorporados à máquina.

11 Uma cópia da declaração CE de conformidade

Na produção em série, detalhes de medidas internas (sistemas de qualidade, por exemplo) para garantir que todas as máquinas produzidas permaneçam conformes:

- O fabricante deve realizar a pesquisa ou os testes necessários em componentes, acessórios ou em máquinas acabadas para determinar se, através de seu projeto e construção, elas são capazes de serem suspensas e colocadas em funcionamento com segurança.
- O arquivo técnico não precisa existir como um único arquivo permanente, mas deve ser possível sua elaboração para torná-lo disponível em um tempo razoável. Ele deve ficar disponível durante dez anos após a produção da última unidade.

O arquivo técnico não precisa incluir planos detalhados ou qualquer outra informação específica referente aos subconjuntos utilizados na produção das máquinas, a menos que eles sejam essenciais à verificação da conformidade com os EHSRs.

Avaliação da conformidade das máquinas do Anexo IV

Avaliações de conformidade

Determinados tipos de equipamento estão sujeitos a medidas especiais. Este equipamento consta no Anexo IV da diretriz e inclui máquinas perigosas, como algumas máquinas de trabalho com madeira, prensas, máquinas de moldagem por injeção, equipamentos subterrâneos, elevadores para manutenção de veículos, etc.

O Anexo IV também inclui determinados componentes de segurança, tais como dispositivos de proteção projetados para detectar a presença de pessoas (por exemplo, cortinas de luz) e unidades de lógica para garantir as funções de segurança.

Para as máquinas do Anexo IV que não estão em plena conformidade com os padrões europeus harmonizados relevantes, o fabricante ou o seu representante autorizado deve aplicar um dos seguintes procedimentos:

1. Exame do tipo CE. O arquivo técnico deve ser preparado e um exemplo da máquina deve ser submetido a um órgão notificado (local de teste) para o exame de CE. Se passar, a máquina receberá um certificado de exame tipo CE. A validade do certificado deve ser revista a cada cinco anos com o órgão notificado.

2. Garantia de qualidade plena. Um arquivo técnico deve ser preparado e o fabricante deve aplicar um sistema de qualidade aprovado para o projeto, produção, inspeção final e teste. O sistema de qualidade deve garantir a conformidade das máquinas com as disposições desta diretriz. O sistema de qualidade deve ser periodicamente fiscalizado por um órgão notificado.

Exames por órgãos notificados

Para as máquinas que não estão incluídas no Anexo IV ou as máquinas que estão incluídas no Anexo IV, mas estão em plena conformidade com os padrões europeus harmonizados relevantes, o fabricante ou seu representante também tem a opção de preparar a avaliação técnica e a autoavaliação e declarar a conformidade do equipamento. Deve haver verificações internas para garantir que o equipamento fabricado permaneça em conformidade.

Órgãos notificados

Existe uma rede de órgãos notificados que se comunicam uns com os outros e funcionam com critérios comuns em toda a UE. Os órgãos notificados são nomeados pelos governos (não pela indústria) e os detalhes de organizações com status de órgão notificado podem ser obtido em:

http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_ en.htm

Declaração CE do procedimento de conformidade

CE

A marcação “CE” deve ser aplicada a todas as máquinas fornecidas. As máquinas também devem ser fornecidas com uma declaração CE de conformidade.

A marca CE indica que a máquina está em conformidade com todas as diretrizes europeias aplicáveis e que os procedimentos de avaliação de conformidade adequados foram concluídos. É um delito aplicar a marca CE para a diretriz de máquinas, a menos que a máquina cumpra os EHSRs relevantes.

A declaração CE de conformidade deve conter as informações a seguir:

- Razão social e endereço completo do fabricante e, se for o caso, do representante autorizado
- Nome e endereço da pessoa autorizada a compilar o arquivo técnico, que deve estar estabelecida na comunidade (no caso de um fabricante fora da EU, pode ser o “representante autorizado”);
- Descrição e identificação da máquina, incluindo a denominação genérica, função, modelo, tipo, número de série e nome comercial;
- Uma frase declarando expressamente que as máquinas cumprem todas as disposições relevantes desta diretriz e, se for o caso, uma frase semelhante, declarando a conformidade com outras diretrizes e/ou disposições relevantes com as quais as máquinas estão conformes;
- Quando for o caso, é utilizada uma referência aos padrões harmonizados;
- Quando for o caso, a referência a outros padrões e especificações técnicas utilizadas;
- (Para máquinas do anexo IV) Se for o caso, o nome, endereço e número de identificação do órgão notificado que fez o exame de tipo CE mencionado no anexo IX e o número de certificação do exame de tipo CE;
- (Para máquinas do Anexo IV) Se for o caso, o nome, endereço e número de identificação do órgão notificado que aprovou o sistema pleno de garantia de qualidade mencionado no Anexo X;
- O local e a data da declaração;
- A identidade e assinatura da pessoa habilitada para elaborar a declaração em nome do fabricante ou o representante autorizado.

Declaração CE de incorporação para máquinas semiacabadas

Quando o equipamento é fornecido para montagem com outros itens a fim de formar uma máquina completa em uma data posterior, deve ser emitida uma DECLARAÇÃO DE INCORPORAÇÃO para acompanhá-la. A marca CE não deve ser aplicada. A declaração deverá indicar que o equipamento não deve ser posto em funcionamento até que a máquina na qual ele foi incorporado tenha sido declarada conforme. Um arquivo técnico deve ser preparado e as máquinas semiacabadas devem ser fornecidas com informações que contenham uma descrição das condições que devem ser atendidas, tendo em vista a correta incorporação das máquinas acabadas, para não comprometer a segurança.

Esta opção não está disponível para equipamentos que possam funcionar de forma independente ou que modifiquem a função de uma máquina.

A declaração de incorporação deve conter as informações a seguir:

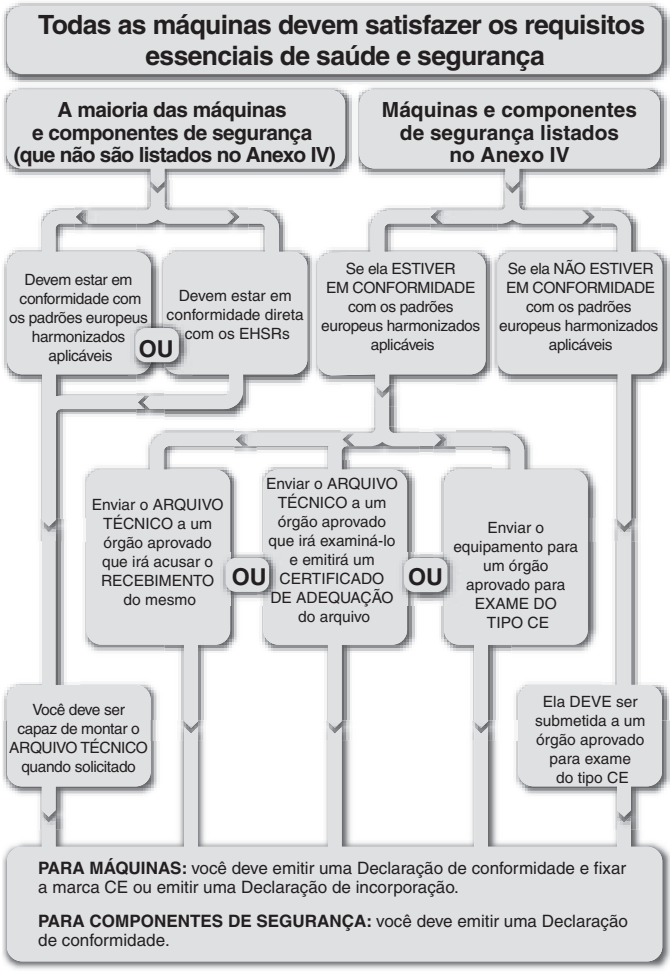
- Razão social e endereço completo do fabricante das máquinas semiacabadas e, se for o caso, do representante autorizado;
- Nome e endereço da pessoa autorizada a compilar a documentação técnica relevante, que deve estar estabelecida na comunidade (no caso de um fabricante fora da EU, esse pode ser o “representante autorizado”);
- Descrição e identificação de máquinas semiacabadas, incluindo: denominação genérica, função, modelo, tipo, número de série e nome comercial;
- Uma frase declarando que os requisitos essenciais desta diretriz são aplicados e cumpridos e que a documentação técnica pertinente é compilada em conformidade com a parte B do Anexo VII e, se for o caso, uma frase declarando a conformidade das máquinas semiacabadas com outras diretrizes relevantes;
- Um plano de ação para transmitir, em resposta a uma solicitação fundamentada das autoridades nacionais, as informações relevantes sobre as máquinas semiacabadas. Isso deve incluir o método de transmissão e deverá ocorrer sem prejuízo dos direitos de propriedade intelectual do fabricante das máquinas semiacabadas;
- Uma declaração de que as máquinas semiacabadas não devem ser postas em funcionamento até que as máquinas acabadas nas quais ela deve ser incorporada sejam declaradas conformes com as disposições da presente diretriz, se for o caso;
- O local e a data da declaração;
- A identidade e assinatura da pessoa habilitada a elaborar a declaração em nome do fabricante ou do representante autorizado.

Máquinas fornecidas de fora da UE – representantes autorizados

Se um fabricante baseado fora da UE (ou EEE) exporta máquinas para a UE, será necessário nomear um representante autorizado.

Um representante autorizado significa qualquer pessoa física ou jurídica estabelecida na Comunidade Europeia que tenha recebido um mandato por escrito do fabricante para executar em seu nome todas ou parte das obrigações e formalidades vinculadas à diretriz de máquinas.

A diretriz do uso do equipamento no trabalho na UE (diretriz U.W.E.)



Procedimento de características gerais para a diretriz de máquinas

Enquanto a diretriz de máquinas destina-se a fornecedores, a presente diretriz (89/655/CEE alterada pela 95/63/CE, 2001/45/CE e 2007/30/CE) destina-se a usuários de máquinas. Ela abrange todos os setores industriais e impõe obrigações gerais aos empregadores, juntamente com os requisitos mínimos para a segurança do equipamento de trabalho. Todos os países da UE estão aplicando suas próprias formas de legislação para implementar esta diretriz.

Serve como exemplo sua implementação no Reino Unido com o nome de Provisão e uso da regulamentação de equipamentos de trabalho (muitas vezes abreviado como P.U.W.E.R.). A forma de implementação pode variar entre países, mas o efeito da diretriz é retido.

Os artigos da diretriz fornecem detalhes de quais tipos de equipamentos e locais de trabalho são cobertos pela diretriz.

Eles também impõem obrigações gerais sobre empregadores, tais como a instituição de sistemas seguros de trabalho e o fornecimento de equipamentos adequados e seguros que devem ter uma manutenção adequada. Os operadores de máquinas devem receber a informação e o treinamento adequados para a utilização segura da máquina.

As novas máquinas (e máquinas de segunda mão de fora da UE) fornecidas depois de 1º de janeiro de 1993 devem satisfazer todas as diretrizes relevantes de produtos, por exemplo, a diretriz de máquinas (sujeitas a disposições transitórias). Os equipamentos de segunda mão de dentro da UE, fornecidos pela primeira vez no local de trabalho, devem imediatamente estabelecer requisitos mínimos constantes em um Anexo da diretriz da U.W.E.

Observação: As máquinas existentes ou de segunda mão que são revisadas ou modificadas significativamente serão classificadas como novos equipamentos, de modo que o trabalho efetuado deve garantir a conformidade com a diretriz de máquinas (mesmo se forem para uso da própria empresa).

A adequação dos equipamentos de trabalho é um requisito importante da diretriz e destaca a responsabilidade do empregador na realização de um processo adequado de avaliação de risco.

É um dos requisitos que as máquinas tenham a manutenção adequada. Isso normalmente significa que deve haver uma rotina e um cronograma de manutenção preventiva planejada. É recomendável que um registro seja compilado e mantido atualizado. Isso é especialmente importante nos casos em que a manutenção e inspeção de equipamentos contribui para a integridade contínua de segurança de um dispositivo ou sistema de proteção.

O Anexo da diretriz U.W.E. fornece requisitos mínimos gerais aplicáveis ao equipamento de trabalho.

Se os equipamentos estiverem em conformidade com as diretrizes relevantes do produto, por exemplo, a diretriz de máquinas, eles automaticamente cumprirão com os respectivos requisitos de projeto de máquinas constantes nos requisitos mínimos do Anexo.

Os Estados-Membros têm competência para elaborar leis sobre o uso de equipamentos de trabalho que vão além dos requisitos mínimos da diretriz do U.W.E.

Pode-se encontrar informações detalhadas sobre o uso da diretriz de equipamentos de trabalho no site oficial da UE:

http://europa.eu/legislation_summaries/employment_and_social_policy/health_hygiene_safety_at_work/c11116_en.htm

Regulamentações dos EUA

Esta seção apresenta algumas das regulamentações de segurança que protegem as máquinas industriais nos EUA. Este é apenas um ponto de partida; os leitores devem investigar mais sobre os requisitos para conhecer suas aplicações específicas e tomar medidas para garantir que seus projetos, utilizações, procedimentos e práticas de manutenção atendam a suas próprias necessidades, bem como às regulamentações e códigos nacionais e locais.

Existem muitas organizações que promovem a segurança industrial nos Estados Unidos. Estas incluem:

1. Corporações, que usam os requisitos estabelecidos, bem como estabelecem seus próprios requisitos internos;

2. A Administração de Segurança e Saúde Ocupacional (OSHA);

3. Organizações industriais, como a Associação Nacional de Proteção contra Incêndios (NFPA), a Associação das Indústrias de Robótica (RIA) e a Associação de Tecnologia de Produção (AMT); além dos fornecedores de produtos e soluções de segurança, como a Rockwell Automation.

Administração de Segurança e Saúde Ocupacional

Nos Estados Unidos, um dos principais impulsionadores da segurança industrial é a Administração de Segurança e Saúde Ocupacional (OSHA). A OSHA foi fundada em 1970 por uma lei do Congresso dos EUA. A finalidade desta lei é fornecer condições de trabalho seguras e saudáveis e preservar os recursos humanos. A lei autoriza o Ministério do Trabalho a definir padrões obrigatórios de saúde e segurança ocupacional aplicáveis às empresas que participam do comércio interestadual. Esta lei deve se aplicar em relação às tarefas realizadas no local de trabalho de um estado, do distrito de Columbia, de Porto Rico, Ilhas Virgens, Samoa Americana, Guam, território chancelado das Ilhas do Pacífico, Ilha Wake, terras de plataformas continentais externas definidas na respectiva lei, Ilha Johnston e Zona do Canal.

O artigo 5º da lei estabelece os requisitos básicos. Cada empregador deve estipular tarefas a cada um de seus funcionários e um local de trabalho que sejam livres de perigos reconhecidos que causem ou possam vir a causar morte ou sérias lesões

físicas a seus funcionários; e devem cumprir os padrões de segurança e saúde ocupacionais promulgados nesta lei.

O artigo 5º também afirma que cada funcionário deve cumprir os padrões de segurança e saúde ocupacionais e todas as regras, regulamentos e ordens de serviço emitidas nos termos da presente lei que sejam aplicáveis às suas próprias ações e condutas.

A lei da OSHA imputa a responsabilidade tanto sobre o empregador quanto o funcionário. Isso é bastante divergente da diretriz de máquinas, a qual exige que os fornecedores coloquem no mercado máquinas que estejam livres de perigos. Nos Estados Unidos, um fornecedor pode vender uma máquina sem qualquer segurança. O usuário deve adicionar a proteção para tornar a máquina segura. Embora essa fosse uma prática comum na época da aprovação da lei, a tendência é que os fornecedores ofereçam máquinas com a proteção, pois projetar a segurança em uma máquina é muito mais econômico do que adicionar a proteção depois que a máquina for projetada e construída. Os padrões estão agora tentando fazer com que os fornecedores e usuários divulguem os requisitos de proteção, para que as máquinas se tornem não apenas seguras, mas também mais produtivas.

O Ministério do Trabalho tem a autoridade para promulgar como padrão de saúde ou segurança ocupacional qualquer padrão de consenso nacional e qualquer padrão federal estabelecido, a menos que a promulgação de tal padrão não resulte em maior segurança ou saúde para funcionários especificamente designados.

A OSHA realiza esta tarefa através da publicação de regulamentos no título 29 do Código de Regulamentação Federal (29 CFR). Os padrões referentes a máquinas industriais são publicados pela OSHA na seção 1910 do 29 CFR. Eles estão disponíveis gratuitamente no site da OSHA em www.osha.gov. Ao contrário da maioria dos padrões, que são voluntários, os padrões da OSHA são leis.

Algumas das seções importantes que dizem respeito à segurança de máquinas são listadas abaixo:

A - Geral
B - Adoção e extensão de padrões federais estabelecidos
C - Disposições gerais sobre segurança e saúde
H - Materiais perigosos
I - Equipamento de proteção individual
J - Controles ambientais em geral - incluem LOTO
O - Máquinas e proteção de máquinas
R - Indústrias especiais
S - Elétrica

Alguns padrões da OSHA referenciam padrões voluntários. O efeito jurídico da incorporação por referência é que o material é tratado como se fosse publicado íntegro no Registro Federal. Quando um padrão de consenso nacional é incorporado por referência em uma das subseções, esse padrão é considerado com força de lei. Por exemplo, o NFPA 70, um padrão voluntário conhecido como o Código Elétrico Nacional dos EUA, é mencionado na subseção S. Isso torna obrigatórios os requisitos do padrão NFPA70.

O CFR 29 1910.147, na subseção J, abrange o controle de energia perigosa. Este é normalmente conhecido como padrão LOTO. O padrão voluntário equivalente é ANSI Z244.1. Essencialmente, este padrão exige que a energia para a máquina seja bloqueada quando submetida a serviços ou manutenção. A finalidade é evitar a energização ou a partida inesperada da máquina que resultaria em lesões aos funcionários.

Os empregadores devem estabelecer um programa e utilizar procedimentos para a instalação de dispositivos de bloqueio ou dispositivos LOTO em dispositivos de isolamento de energia e, por outro lado, desativar máquinas ou equipamentos para impedir a energização, a partida inesperada ou a liberação de energia armazenada para evitar lesões aos funcionários.

Alterações e ajustes mínimos de ferramentas, além de outras atividades de manutenção menos importantes que ocorrem durante as operações normais de produção, não são cobertos por este padrão, caso sejam rotineiros, repetitivos e integrais no uso de equipamentos para produção, desde que o trabalho seja realizado utilizando medidas alternativas que forneçam proteção eficaz. Medidas alternativas são dispositivos de proteção como cortinas de luz, esteiras de segurança, intertravamentos de portão e outros dispositivos similares conectados a um sistema de segurança. O desafio para o projetista e usuário da máquina é determinar o que é “menos importante” e o que é “rotineiro, repetitivo e integral”.

A subseção “O” trata de “Máquinas e proteção de máquinas”. Esta subseção lista os requisitos gerais para todas as máquinas, bem como os requisitos para algumas máquinas específicas. Quando a OSHA foi fundada em 1970, ela adotou muitos padrões ANSI existentes. Por exemplo, o B11.1 para prensas de energia mecânica foi adotado como o 1910.217.

O 1910.212 é o padrão geral da OSHA para máquinas. Ele declara que um ou mais métodos de proteção de máquinas devem ser fornecidos para proteger o operador e outros funcionários na área de máquinas de riscos, tais como aqueles criados pelo ponto de operação, pontos de laminagem de entrada, peças rotativas, lascas e fagulhas que escapam. As proteções deverão ser fixadas na máquina, sempre que possível, e presas em outro lugar para o caso de impossibilidade de integrar à máquina qualquer acessório, por qualquer razão. A proteção deve ser instalada de tal modo que ela mesma não ofereça risco de acidentes.

O “ponto de operação” é a área de uma máquina onde o trabalho é realmente realizado no material sendo processado. O ponto de operação de uma máquina cujo funcionamento expõe um funcionário a lesões deve ser protegido. O dispositivo de proteção deve estar em conformidade com quaisquer padrões adequados ou, na ausência de padrões específicos aplicáveis, deverão ser concebidos e construídos de forma a evitar que o operador exponha qualquer parte de seu corpo à zona de perigo durante o ciclo operacional.

A subseção S (1910.399) trata dos requisitos elétricos da OSHA. Uma instalação ou um equipamento é aceitável para o ministro do trabalho e aprovado na acepção da presente subseção S, caso seja aceito, certificado, listado, rotulado ou, por qualquer outro meio, considerado seguro por um laboratório de testes reconhecido nacionalmente (NRTL).

O que é equipamento? Um termo geral que inclui materiais, acessórios, dispositivos, aparelhos elétricos, fixações, aparatos e similares, utilizados como parte, ou em conexão com uma instalação elétrica.

O que significa “listado”? O equipamento é “listado” se for do tipo mencionado em uma lista que: (a) seja publicada por um laboratório reconhecido nacionalmente e que faça a inspeção periódica da produção desse equipamento e (b) declare que esse equipamento atende os padrões nacionalmente reconhecidos ou que foi testado e considerado seguro para uso de uma maneira especificada.

A partir de agosto de 2009, as seguintes empresas são reconhecidas pela OSHA como NRTLs:

- Canadian Standards Association (CSA)
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- FM Approvals LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- Southwest Research Institute (SWRI)
- TUV America, Inc. (TUVAM)
- TUV Product Services GmbH (TUVPSG)
- TUV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

Alguns estados adotaram suas próprias OSHAs locais. Vinte e quatro estados, Porto Rico e Ilhas Virgens têm projetos estaduais aprovados pela OSHA e adotaram

seus próprios padrões e políticas de execução. Na maior parte, esses estados adotam padrões que são idênticos à OSHA federal. Contudo, alguns estados adotaram diferentes padrões aplicáveis a este tópico ou podem ter políticas de execução distintas. Os empregadores devem relatar o histórico de incidentes à OSHA. A OSHA compila as taxas de incidentes e transmite as informações para escritórios locais e utiliza essas informações para priorizar inspeções. São os seguintes os principais motivos de inspeção:

- Perigo iminente
- Catástrofes e fatalidades
- Reclamações de funcionários
- Indústrias de alto risco
- Inspeções locais planejadas
- Inspeções de acompanhamento
- Programas com focos nacionais e locais

As violações de padrões da OSHA podem resultar em multas. A classificação das multas pode ser:

- Graves: até US$ 7000 por violação
- Outras: discricionárias, porém, não mais que US$ 7000
- Reincidentes: até US$ 70.000 por violação
- Intencionais: até US$ 70.000 por violação
- Violações que resultem em morte: penalidades adicionais
- Sem mitigação: US$ 7000/dia

A tabela abaixo mostra as 14 principais citações da OSHA entre outubro de 2004 e setembro 2005.

Padrão	**Descrição**
1910.147	Controle de energia perigosa (LOTO)
1910.1200	Comunicação perigosa
1910.212	Requisitos gerais para todas as máquinas
1910.134	Proteção respiratória
1910.305	Métodos de fiação, componentes e equipamentos de uso geral
1910.178	Caminhões com potência industrial
1910.219	Transmissão de energia mecânica
1910.303	Requisitos gerais
1910.213	Máquinas de carpintaria
19102.215	Máquinas de rodas abrasivas
19102.132	Requisitos gerais
1910.217	Prensas com energia mecânica
1910.095	Exposição a ruídos do trabalho
1910.023	Proteção contra aberturas e perfurações no piso e na parede

Regulamentações canadenses

No Canadá, a segurança industrial é regida ao nível de província. Cada província tem seus próprios regulamentos que são mantidos e cumpridos. Por exemplo, Ontário estabeleceu a Lei de segurança e saúde ocupacional, que dispõe sobre os direitos e deveres de todos os funcionários no local de trabalho. Seu principal objetivo é proteger os trabalhadores contra riscos de saúde e segurança no trabalho. A lei estabelece procedimentos para lidar com os perigos no local de trabalho e prevê a aplicação da lei nos casos em que a conformidade não tenha sido atingida voluntariamente.

No âmbito dessa lei, há o Regulamento 851, seção 7, que define a revisão prévia de saúde e segurança. Essa revisão é um requisito da região de Ontário válido para qualquer máquina nova, reconstruída ou modificada e é necessária a elaboração de um relatório por um profissional de engenharia.

Padrões

Esta coluna fornece uma lista de alguns dos padrões internacionais e nacionais típicos que são relevantes à segurança de máquinas. Ela não pretende formar uma lista exaustiva, mas sim oferecer uma visão sobre quais questões de segurança de máquinas constituem o objeto da padronização.

Esta coluna deve ser lida em conjunto com a coluna de regulamentação.

Os países do mundo estão trabalhando para a harmonização global de padrões. Isso fica especialmente evidente na área de segurança de máquinas. Os padrões globais de segurança para máquinas são regidos por duas organizações: ISO e IEC. Os padrões regionais e do país ainda existem e continuam a oferecer suporte aos requisitos locais, mas em muitos países houve um avanço com a utilização dos padrões internacionais produzidos pela ISO e IEC.

Por exemplo, os padrões EN (norma europeia) são utilizados em todos os países do EEE. Todos os novos padrões EN se alinham e, na maioria dos casos, apresentam texto idêntico aos padrões ISO e IEC.

A IEC aborda problemas de eletrotécnica e a ISO abrange todas as outras questões. A maioria dos países industrializados são membros da IEC e ISO. Os padrões de segurança de máquinas são escritos por grupos de trabalho compostos de especialistas de muitos países industrializados de todo o mundo.

Na maioria dos países, os padrões podem ser considerados voluntários, enquanto as regulamentações são obrigatórias legalmente. Contudo, os padrões geralmente são utilizados como a interpretação prática das regulamentações. Portanto, os mundos dos padrões e das regulamentações estão estreitamente interligados.

Consulte o catálogo de segurança, disponível em: www.ab.com/safety para obter uma lista abrangente de padrões.

ISO (Organização Internacional de Padronização)

A ISO é uma organização não-governamental formada por órgãos de padronização nacionais da maioria dos países do mundo (157 países no momento da impressão deste). A Secretaria Central, localizada em Genebra, na Suíça, coordena o sistema. A ISO gera padrões para o projeto, fabricação e utilização de máquinas com mais eficiência, segurança e limpeza. Os padrões também tornam o comércio entre os países mais fácil e mais justo. Os padrões da ISO podem ser identificados pelas três letras: ISO.

Os padrões de máquinas da ISO estão organizados da mesma forma que os padrões EN, em três níveis: Tipo A, B e C (consulte a seção adiante sobre os padrões europeus harmonizados EN).

Para obter mais informações, acesse o site da ISO: *www.iso.org*.

IEC (Comissão Eletrotécnica Internacional)

A IEC prepara e publica padrões internacionais para tecnologias elétricas, eletrônicas e correlatas. Através de seus membros, a IEC promove a cooperação internacional sobre todas as questões de padronização eletrotécnica e temas relacionados, tais como a avaliação da conformidade de padrões eletrotécnicos.

Para obter mais informações, acesse o site da IEC: www.iec/ch

Padrões europeus harmonizados EN

Esses padrões são comuns a todos os países do EEE e são produzidos pelas organizações de padronização europeias CEN e CENELEC. Sua utilização é voluntária, mas o projeto e fabricação de equipamentos de acordo com eles representam a forma mais direta de demonstrar a conformidade com os EHSRs da diretriz de máquinas.

Eles são divididos em 3 tipos: padrões A, B e C.

PADRÕES Tipo A: tratam de aspectos aplicáveis a todos os tipos de máquinas.

PADRÕES Tipo B: subdivididos em 2 grupos.
PADRÕES Tipo B1: tratam de aspectos ergonômicos e de segurança específicos das máquinas.
PADRÕES Tipo B2: tratam de componentes de segurança e dispositivos de proteção.

PADRÕES Tipo C: tratam de tipos ou grupos específicos de máquinas.

É importante observar que o cumprimento de um padrão C oferece a presunção automática de conformidade com os EHSRs. Na ausência de um padrão C adequado, podem ser utilizados os padrões A e B como prova parcial ou total de conformidade do EHSR, indicando a conformidade com as seções relevantes.

Foram firmados acordos de cooperação entre CEN/CENELEC e órgãos como a ISO e a IEC. Em última análise, isso deve resultar em padrões globais comuns. Na maioria dos casos, um padrão EN possui um equivalente na IEC ou ISO. Em geral, os dois textos serão iguais e quaisquer diferenças regionais serão fornecidas com o avanço do padrão.

Para obter uma lista completa dos padrões de segurança de máquinas EN, acesse:

http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_ en.htm.

Padrões dos EUA

Padrões da OSHA

Quando possível, a OSHA promulga padrões de consenso nacional ou padrões federais estabelecidos como padrões de segurança. As disposições compulsórias (por exemplo, a palavra “deve” implica obrigação) dos padrões, incorporadas por referência, possuem a mesma força e efeito que os padrões listados na seção 1910. Por exemplo, o padrão de consenso NFPA 70 nacional está listado como um documento de referência no Apêndice A da subseção S- Elétrica da seção 1910 do CFR 29. O NFPA 70 é um padrão voluntário, que foi desenvolvido pela Associação Nacional de Proteção contra Incêndios (NFPA). O NFPA 70 é também conhecido como o Código Elétrico Nacional (NEC). Por incorporação, todos os requisitos obrigatórios do NEC são obrigatórios conforme a OSHA.

Padrões ANSI

O Instituto Americano de Padrões Nacionais (ANSI) serve como administrador e coordenador do sistema de padronização voluntária do setor privado dos Estados Unidos. É uma organização privada e sem fins lucrativos de associados, apoiada por uma circunscrição diversificada de organizações do setor público e privado.

O ANSI, por si só, não desenvolve padrões; ele facilita o desenvolvimento de padrões estabelecendo consenso entre grupos qualificados. O ANSI também garante que sejam seguidos os princípios orientadores de consenso, o devido processo e a transparência pelos grupos qualificados. Abaixo se encontra uma lista parcial de padrões de segurança industrial que podem ser obtidos entrando em contato com o ANSI.

Esses padrões são classificados como padrões de aplicação ou padrões de construção. Os padrões de aplicação definem como aplicar uma proteção à máquina. Os exemplos incluem o ANSI B11.1, que fornece informações sobre o uso da proteção de máquina em prensas de força, e o ANSI/RIA R15.06, que descreve o uso da proteção para a segurança de robôs.

Associação Nacional de Proteção contra Incêndios

A Associação Nacional de Proteção contra Incêndios (NFPA) foi organizada em 1896. Sua missão é reduzir o impacto de incêndios sobre a qualidade de vida, ao defender códigos e padrões de consenso com base científica, a pesquisa e treinamento sobre incêndios e questões relacionadas à segurança. A NFPA patrocina muitos padrões para ajudar a cumprir sua missão. Dois padrões muito importantes relacionados à segurança industrial e à proteção são o Código Elétrico Nacional (NEC) e o padrão elétrico para máquinas industriais.

A Associação Nacional de Proteção contra Incêndios atua como patrocinadora do NEC desde 1911. O documento do código original foi desenvolvido em 1897 como resultado dos esforços combinados de vários interesses do setor de seguros, elétrico, arquitetônico e correlatos. O NEC foi atualizado inúmeras vezes, desde então e é revisado, mais ou menos, a cada três anos. O artigo 670 do NEC aborda alguns detalhes sobre máquinas industriais e remete o leitor ao Padrão Elétrico para Máquinas Industriais, NFPA 79.

O NFPA 79 aplica-se a equipamentos elétricos e eletrônicos, aparelhos ou sistemas de máquinas industriais que operam a partir de uma tensão nominal de 600 volts ou menos. O objetivo do NFPA 79 é fornecer informações detalhadas para a aplicação de equipamentos elétricos e eletrônicos, aparelhos ou sistemas fornecidos como parte de máquinas industriais que promovam segurança à vida e à propriedade. O NFPA 79, que foi adotado oficialmente pelo ANSI em 1962, apresenta um conteúdo muito semelhante ao padrão IEC 60204-1.

As máquinas que não são cobertas pelos padrões específicos da OSHA têm a obrigação de estar livres de perigos que reconhecidamente podem causar morte ou lesões graves. Essas máquinas devem ser projetadas e mantidas para atender ou superar os requisitos dos padrões aplicáveis da indústria. O NFPA 79 é um padrão que deveria ser aplicado às máquinas não especificamente cobertas pelos padrões da OSHA.

Padrões canadenses

Os padrões da CSA refletem um consenso nacional de produtores e usuários, incluindo fabricantes, consumidores, varejistas, sindicatos e organizações profissionais, além de órgãos governamentais. Os padrões são amplamente utilizados pela indústria e comércio e, muitas vezes, adotados pelos governos municipais, federais e estaduais/provinciais em seus regulamentos, particularmente nas áreas de saúde, segurança, construção civil e no meio ambiente.

Pessoas físicas, jurídicas e associações em todo o Canadá demonstram seu apoio ao desenvolvimento de padrões da CSA, voluntariando seu tempo e habilidades para o trabalho do Comitê da CSA e apoiando os objetivos da associação através da sustentação de adesões. Os mais de 7000 voluntários do comitê e os 2000 associados pagantes, juntos, formam a lista de associados da CSA.

O Conselho de Padrões do Canadá é o órgão de coordenação do Sistema Nacional de Padrões, uma federação de organizações autônomas e independentes que trabalham para o desenvolvimento e melhoria adicionais da padronização voluntária no interesse nacional.

Padrões australianos

A maioria desses padrões está proximamente alinhada com o padrões equivalentes da ISO/IEC/EN

Standards Australia Limited
286 Sussex Street, Sydney, NSW 2001
Fone: +61 2 8206 6000
E-mail: mail@standards.org.au
Site: www.standards.org.au

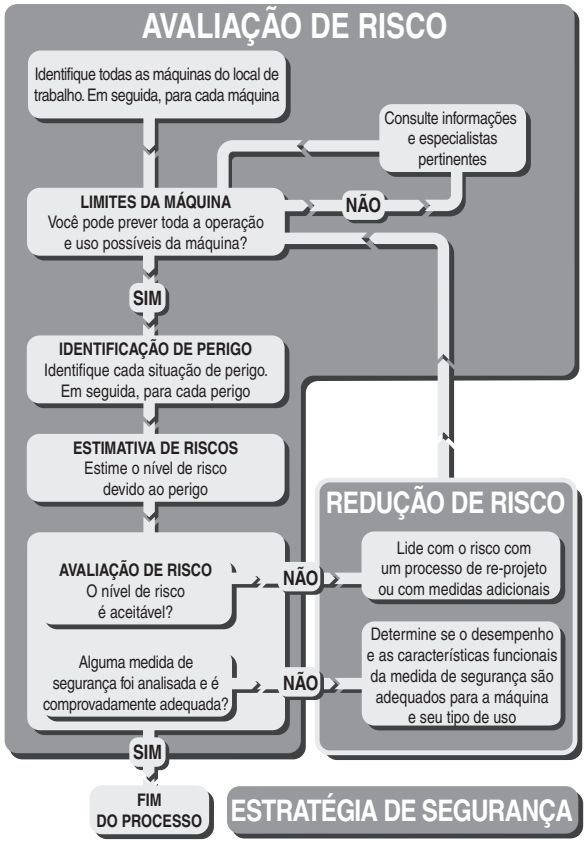
Para adquirir cópias de padrões:
SAI Global Limited
286 Sussex Street, Sydney, NSW 2001
Fone: +61 2 8206 6000
Fax: +61 2 8206 6001
E-mail: mail@sai-global.com
Site: www.saiglobal.com/shop

Consulte o catálogo de segurança, disponível em: www.ab.com/safety para obter uma lista abrangente de padrões.

Estratégia de segurança

Do ponto de vista puramente funcional, quanto maior a eficiência de uma máquina ao realizar sua tarefa de processamento de materiais, melhor ela será. Mas, para que uma máquina seja viável, ela também deve ser segura. Sem dúvida, a segurança deve ser uma das principais considerações.

A fim de elaborar uma estratégia de segurança adequada, deve haver duas etapas principais que funcionam juntas, como mostrado abaixo.



AVALIAÇÃO DE RISCO baseada em uma compreensão clara dos limites e funções da máquina, além das tarefas que pode ser necessário executar na máquina em toda a sua vida útil.

REDUÇÃO DE RISCO é realizada em seguida, se necessário, e as medidas de segurança são selecionadas com base nas informações derivadas da fase de avaliação de risco. O modo como isso é realizado é a base da ESTRATÉGIA DE SEGURANÇA da máquina.

Precisamos de uma lista de verificação para seguir e assegurar que todos os aspectos sejam considerados e que o princípio de supressão não se perca nos detalhes. Todo o processo deve ser documentado. Isso não somente garantirá um trabalho mais completo, mas também disponibilizará os resultados para verificação por outras partes.

Esta seção se aplica tanto aos fabricantes quanto aos usuários de máquinas. O fabricante precisa garantir que sua máquina seja capaz de ser utilizada com segurança. A avaliação de riscos deve ser iniciada na fase de projeto da máquina e deve considerar todas as tarefas previsíveis que terão que ser executadas na máquina. Esta abordagem baseada em tarefas nas iterações iniciais da avaliação de riscos é muito importante. Por exemplo, pode haver uma necessidade regular de ajuste de peças móveis na máquina. Na fase de projeto, deve ser possível planejar as medidas que permitam a execução segura desse processo. Se isso não for observado na fase inicial, pode ser difícil ou impossível de implementar em uma fase posterior. O resultado pode ser que o ajuste das peças móveis ainda precise ser realizado, mas que deva ser feito de forma insegura ou ineficiente (ou ambas). Uma máquina na qual todas essas tarefas foram consideradas durante a avaliação de risco será uma máquina mais segura e mais eficiente.

O usuário (ou empregador) precisa garantir que as máquinas de seu ambiente de trabalho sejam seguras. Mesmo que uma máquina tenha sido declarada segura pelo fabricante, o usuário da máquina ainda deve realizar uma avaliação de riscos para determinar se o equipamento é seguro em seu ambiente. Muitas vezes, as máquinas são utilizadas em circunstâncias imprevistas pelo fabricante. Por exemplo, uma máquina de ensilagem utilizada em um workshop de treinamento precisará de considerações adicionais em relação àquela utilizada em uma sala de ferramentas industriais.

Deve-se lembrar também que, se a empresa do usuário adquire duas ou mais máquinas independentes e as integra em um processo, ela será considerada a fabricante da máquina combinada resultante.

Então, agora consideremos as etapas essenciais da rota para uma estratégia de segurança adequada. Os itens a seguir podem ser aplicados a uma instalação existente na fábrica ou a uma única máquina nova.

Avaliação de risco

É incorreto considerar a avaliação de risco como uma despesa. Ela é um processo útil que fornece informações vitais e permite que o usuário ou projetista tome decisões lógicas sobre as formas de alcançar segurança.

Existem vários padrões que tratam desse assunto. ISO 14121: “Princípios para a avaliação de risco” e ISO 12100: “Segurança das máquinas – princípios básicos” contêm as orientações mais aplicadas mundialmente.

Qualquer que seja a técnica utilizada para realizar uma avaliação de risco, uma equipe de pessoas com múltiplas funções geralmente produz resultados com cobertura mais ampla e melhor equilíbrio do que um só indivíduo.

A avaliação de risco é um processo iterativo; será realizada em diferentes fases da vida útil da máquina. As informações disponíveis variam de acordo com a fase do ciclo da vida útil. Por exemplo, uma avaliação de risco realizada por um fabricante de máquinas terá acesso a todos os detalhes dos mecanismos materiais de fabricação da máquina, mas, provavelmente, terá apenas uma suposição aproximada do principal ambiente de trabalho da máquina. A avaliação de risco realizada pelo usuário da máquina não teria necessariamente acesso aos detalhes técnicos em profundidade, mas terá acesso a todos os detalhes do ambiente de trabalho da máquina. O ideal é que o resultado de uma iteração sirva como subsídio para a próxima iteração.

Determinação do limite da máquina

Isso envolve a coleta e análise de informações relativas às peças, mecanismos e funções de uma máquina. Também será necessário considerar todos os tipos de interação de tarefas humanas com a máquina e o ambiente em que a máquina funcionará. O objetivo é obter uma compreensão clara da máquina e de sua utilização.

Quando máquinas separadas são interligadas mecanicamente ou através de sistemas de controle, elas devem ser consideradas como uma única máquina, a menos que eles sejam “zoneadas” por medidas de proteção apropriadas.

É importante considerar todos os limites e fases da vida útil de uma máquina, inclusive instalação, comissionamento, manutenção, desativação, correta utilização e operação, bem como as consequências da má utilização ou do mau funcionamento razoavelmente previsíveis.

Identificação de tarefas e perigos

Todos os perigos da máquina devem ser identificados e listados em termos de sua natureza e localização. Os tipos de perigo incluem: trituração, corte, emaranhamento, ejeção de peças, vapores, radiação, substâncias tóxicas, calor, ruído, etc.

Os resultados da análise de tarefas devem ser comparados com os resultados da identificação de perigos. Isso mostrará onde há uma possibilidade de convergência entre um perigo e uma pessoa, ou seja, uma situação de perigo. Devem ser listadas todas as situações de risco. Talvez o mesmo perigo possa produzir um tipo diferente de situação de risco, dependendo da natureza da pessoa ou da tarefa. Por exemplo, a presença de um técnico de manutenção altamente qualificado e treinado pode ter implicações diferentes do que na presença de um faxineiro, não qualificado, que não tenha conhecimento da máquina. Nessa situação, se cada caso for listado e tratado separadamente, talvez seja possível justificar diferentes medidas de proteção para o técnico de manutenção em relação àquelas do faxineiro. Se os casos não forem listados e tratados separadamente, o pior caso deverá ser utilizado, a manutenção e a limpeza serão cobertas pela mesma medida de proteção.

Às vezes, será necessário realizar uma avaliação de risco geral em uma máquina existente que já possui medidas de proteção instaladas (por exemplo, uma máquina com peças móveis perigosas protegida por uma porta com intertravamento). As peças móveis perigosas representam um perigo potencial que pode tornar-se um perigo real, em caso de falha do sistema de intertravamento. A menos que o sistema de intertravamento já tenha sido validado (por exemplo, pela avaliação de risco ou projeto de acordo com um padrão apropriado), sua presença não deve ser levada em consideração.

Estimativa de riscos

Este é um dos aspectos mais fundamentais da avaliação de risco. Existem muitas formas de lidar com esse assunto e as páginas seguintes ilustram os princípios básicos.

Qualquer máquina que tenha o potencial para situações de perigo apresenta o risco de um evento perigoso (ou seja, danos). Quanto maior a quantidade de risco, mais importante se torna fazer algo sobre isso. Em uma situação de perigo, o risco pode ser tão pequeno que podemos tolerar e aceitá-lo, mas em outra situação de perigo, o risco pode ser tão grande que é preciso recorrer a medidas extremas para se proteger contra ele. Portanto, para tomar uma decisão sobre “se e o que fazer sobre o risco” precisamos ser capazes de quantificar isso.

O risco é muitas vezes considerado apenas em termos da gravidade das lesões de um acidente. Tanto a gravidade do dano potencial QUANTO a probabilidade de sua ocorrência precisam ser consideradas para estimar a quantidade do risco presente.

A sugestão para a estimativa de risco indicada nas páginas a seguir não é defendida como o método definitivo, já que as circunstâncias individuais podem ditar uma abordagem diferente. ELA SE DESTINA APENAS A SERVIR COMO UMA DIRETRIZ GERAL PARA ENCORAJAR UMA ESTRUTURA METÓDICA E DOCUMENTADA.

O sistema de pontos utilizado não foi calibrado para nenhum tipo específico de aplicação; portanto, não é necessariamente adequado para nenhuma aplicação específica. A ISO TR (relatório técnico) 14121-2 “Avaliação de risco – orientações práticas e exemplos de métodos” fornece orientações práticas e algumas mostram diferentes métodos de quantificação de riscos.

Os seguintes fatores são considerados:

- A GRAVIDADE DA POTENCIAL LESÃO.
- A PROBABILIDADE DE SUA OCORRÊNCIA.

A probabilidade de ocorrência inclui dois fatores:

- FREQUÊNCIA DE EXPOSIÇÃO.
- PROBABILIDADE DE DANO.

Lidando com cada fator de forma independente, nós atribuiremos valores a cada um deles.

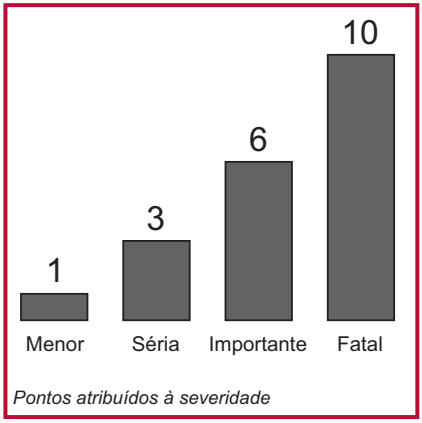
Faça uso de todos os dados e conhecimentos disponíveis para você.
Você está lidando com todas as fases da vida útil da máquina; a fim de evitar muita complexidade, tome suas decisões com base no pior caso para cada fator.

Também é importante manter o senso comum. As decisões precisam levar em conta o que é viável, realista e plausível. É aí que reside o valor de uma abordagem de múltiplas funções da equipe.

Lembre-se: para os fins deste exercício, você geralmente não deve considerar qualquer sistema de proteção existente. Caso a estimativa de risco mostre a necessidade de um sistema de proteção, existem algumas metodologias, conforme mostrado mais adiante neste capítulo, que podem ser utilizadas para determinar as características necessárias.

1. Gravidade de potenciais lesões

Para esta consideração, nós estamos presumindo que ocorreu o acidente ou incidente, talvez como resultado do perigo. Um estudo cuidadoso do perigo revelará qual é a mais grave lesão possível. Lembre-se: para esta consideração, nós estamos presumindo que uma lesão é inevitável e estamos preocupados apenas com sua gravidade. Você deve presumir que o operador fica exposto ao movimento ou processo perigoso. A gravidade da lesão deve ser avaliada como:



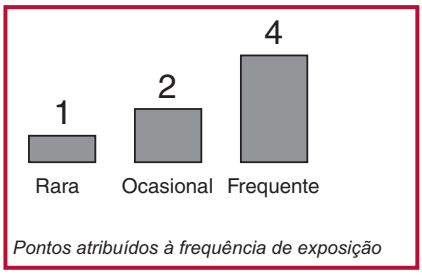
Pontos atribuídos à severidade

- FATAL: Morte
- MAIOR: (Normalmente irreversível) Deficiência permanente, perda da visão, amputação de membro, danos respiratórios...
- SÉRIA: (Normalmente reversível) Perda da consciência, queimaduras, fraturas...
- MENOR: Contusões, cortes, abrasões leves...

É atribuído um valor de pontuação a cada descrição, conforme mostrado.

2. Frequência de exposição

A frequência de exposição responde à pergunta sobre quantas vezes o operador ou o funcionário de manutenção fica exposto ao perigo. A frequência de exposição ao perigo pode ser classificada como:



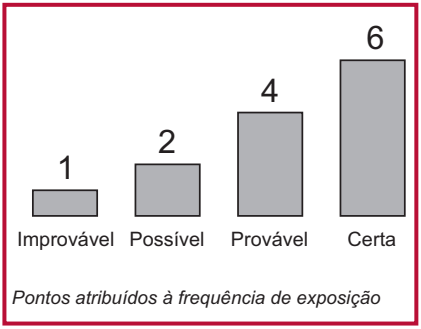
Pontos atribuídos à frequência de exposição

- FREQUENTE: Várias vezes por dia
- OCASIONAL: Diária
- RARA: Semanal ou menor

É atribuído um valor de pontuação a cada descrição, conforme mostrado.

3. Probabilidade de dano

Você deve presumir que o operador fica exposto ao movimento ou processo perigoso. Considerando a forma pela qual o operador está envolvido com a máquina e outros fatores (velocidade de arranque, por exemplo), a probabilidade de dano pode ser classificada como:



Pontos atribuídos à frequência de exposição

- IMPROVÁVEL
- PROVÁVEL
- POSSÍVEL
- CERTA

É atribuído um valor de pontuação a cada descrição, conforme mostrado.

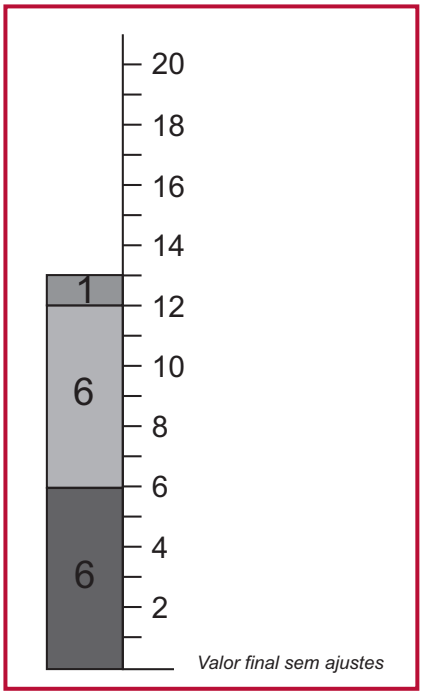
É atribuído um valor de pontuação a cada título e agora são reunidos para fornecer uma estimativa inicial. A soma dos três componentes acrescenta-se a um valor de 13. Mas devemos considerar mais alguns fatores. (Observação: Isso não se baseia necessariamente nas fotos do exemplo anterior).

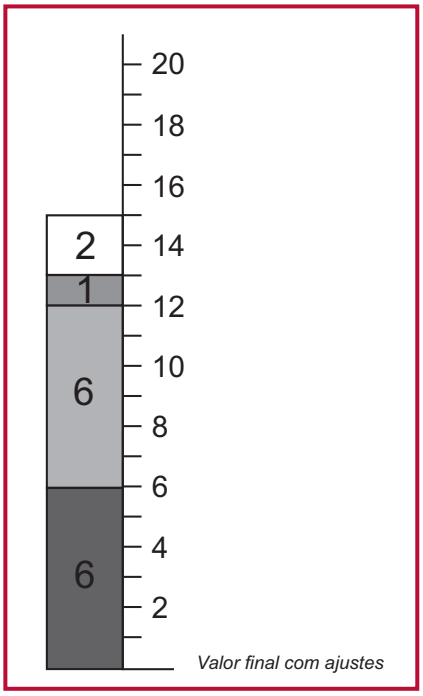
O próximo passo é ajustar a estimativa inicial, considerando fatores adicionais, tais como os mostrados na tabela a seguir. Muitas vezes, eles só podem ser devidamente considerados quando a máquina está instalada em seu local permanente.

Fator Típico	**Ação Sugerida**
Mais de uma pessoa exposta ao perigo	Multiplicar a severidade pelo número de pessoas
Tempo prolongado na zona de perigo sem isolamento completo da energia	Se o tempo gasto em cada acesso for superior a 15 minutos, adicionar 1 ponto ao fator de frequência
O operador é inexperiente ou sem treinamento	Adicionar 2 pontos ao total
Intervalos muito longos (por ex., 1 ano) entre os acessos. (Pode haver falhas progressivas e não detectadas, especialmente nos sistemas de monitoração).	Adicionar os pontos equivalentes ao fator de frequência máximo

Considerações adicionais para a estimativa de risco

Os resultados de quaisquer fatores adicionais são, então, adicionados ao total anterior conforme mostrado.





Redução de risco

Agora, devemos considerar cada máquina e seus respectivos riscos, separadamente, e tomar medidas para resolver todos os seus perigos.

O diagrama mostrado a seguir é uma sugestão de parte de um processo documentado de contabilidade para todos os aspectos de segurança das máquinas em utilização. Ele serve como um guia para usuários de máquinas, mas os fabricantes ou fornecedores de máquinas também podem usar o mesmo princípio para confirmar se todos os equipamentos foram avaliados. Ele também servirá como um índice para relatórios mais detalhados sobre avaliação de risco.

Isso mostra que, onde uma máquina leva a marca CE, ela simplifica o processo, pois os perigos da máquina já foram avaliados pelo fabricante e que já foram tomadas todas as medidas necessárias. Mesmo com o equipamento identificado como CE, ainda pode haver riscos devido à natureza de sua aplicação ou ao material que está sendo processado que o fabricante não previu.

Empresa - MAYKIT WRIGHT LTD
Instalação - Sala de ferramentas - Fábrica do leste.
Data - 29/08/95
Perfil do operador - capacitado.

Identificação do equipamento e data	Conformidade com a diretriz	Nº do relatório de avaliação de risco	Histórico de acidentes	Observações	Identificação de perigos	Tipo de perigo	Ação necessária	Implementado e inspecionado - referência
Torno central de Fulano. Nº de série 8390726, instalado em 1978	Nenhuma alegada	RA302	Nenhum	Equipamento elétrico em conformidade com a BS EN 60204, Paradas de emergência instaladas (substituídas em 1989)	Rotação do mandril com a proteção aberta	Corte por aprisionamento mecânico	Instalar chave de proteção de intertravamento	25/11/94 J Kershaw, relatório nº 9567
					Fluido de corte	Tóxico	Mudar para um tipo atóxico	30/11/94 J Kershaw, relatório nº 9714
					Remoção da limalha	Corte	Fornecer luvas	30/11/94 J Kershaw, relatório nº 9715
Fresa de cabeçote em torre m/c de Fulano, Nº de série 17304294, fabricada em 1995, instalada em maio de 95	Dir. m/c Dir. EMC	RA416	Nenhum		Movimento do leito (em direção à parede)	Esmagamento	Mover a máquina para fornecer espaço suficiente	13/04/95 J Kershaw, relatório nº 10064

Hierarquia das medidas de redução de risco

Existem três métodos básicos a ser considerados e utilizados, na seguinte ordem:

1. Eliminar ou reduzir os riscos, na medida do possível (projeto e construção de máquinas inerentemente seguras).

2. Instalar as medidas e sistemas de proteção necessários (por exemplo, proteções intertravadas, cortinas de luz, etc.) em relação aos riscos que não podem ser eliminados pelo projeto.

3. Informar os usuários sobre os riscos residuais devido à eventuais deficiências das medidas de proteção adotadas, indicar se é necessário qualquer treinamento especial e especificar qualquer necessidade de proporcionar equipamentos de proteção individual.

Cada medida originária da hierarquia deve ser considerada a partir do topo e utilizada onde for possível. Isso geralmente resultará no uso de uma combinação de medidas.

Projeto inerentemente seguro

Na fase de projeto da máquina será possível evitar muitos dos possíveis riscos bastando considerar com cuidado os fatores como materiais, requisitos de acesso, superfícies quentes, métodos de transmissão, pontos de travamento, níveis de tensão, etc.

Por exemplo, se não é necessário o acesso a uma área perigosa, a solução é protegê-la dentro da armação da máquina ou por algum tipo de proteção fixa delimitada.

Sistemas e medidas de proteção

Se for necessário o acesso, então a vida se torna um pouco mais de difícil. Será necessário garantir que o acesso só possa ser obtido enquanto a máquina estiver segura. Serão necessárias medidas tais como portas de proteção intertravadas e/ou sistemas de disparo. A escolha do dispositivo ou sistema de proteção deve ser fortemente influenciada pelas características operacionais da máquina. Isso é extremamente importante já que um sistema que impacte a eficácia da máquina estará sujeito a remoção não autorizada ou bypass.

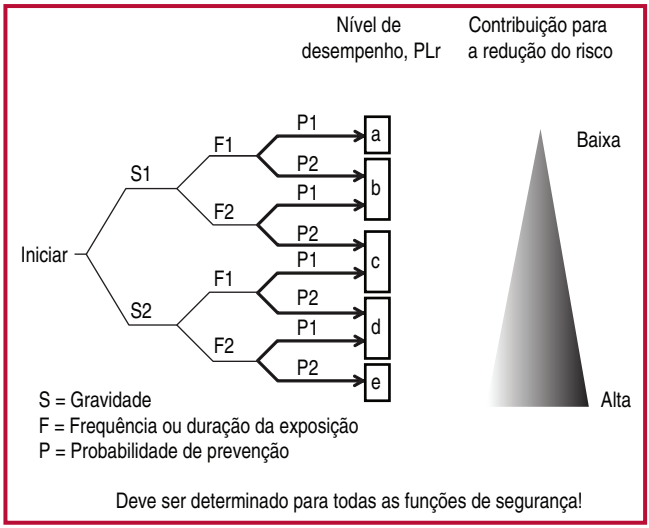
A segurança da máquina nesse caso, dependerá da aplicação adequada e do funcionamento correto do sistema de proteção mesmo em condições de falha.

Agora, deve ser considerado o funcionamento correto do sistema. Dentro de cada tipo, é provável que haja uma escolha de tecnologias, com variados graus de desempenho da monitoração, detecção ou prevenção de falhas.

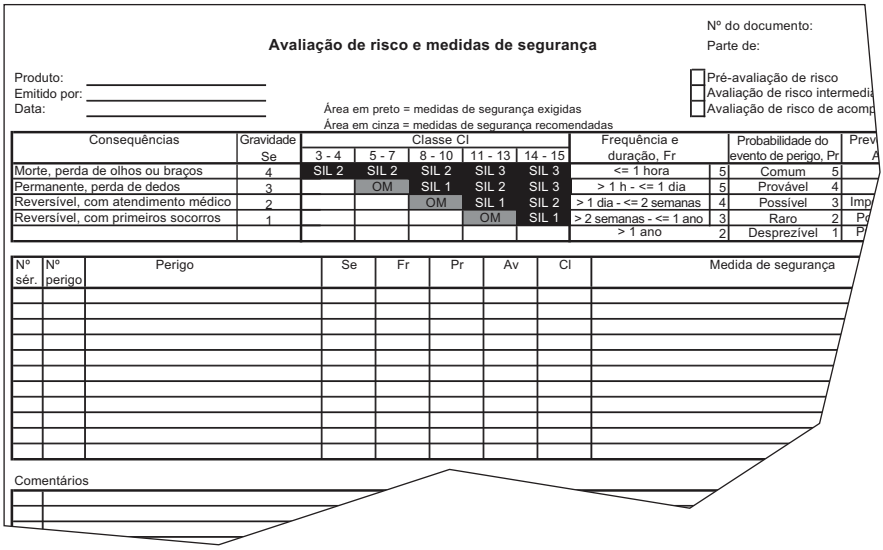
Em um mundo ideal, cada sistema de proteção deveria ser perfeito sem absolutamente nenhuma possibilidade de falhas em uma condição de perigo. No mundo real, entretanto, ficamos restritos pelos atuais limites do conhecimento e de materiais. Outra restrição muito real são os custos. Com base nesses fatores, torna-se óbvio que uma detecção de proporção seja necessária. O senso comum nos diz que seria ridículo insistir em que a integridade de um sistema de segurança de uma máquina, na pior das hipóteses, pode causar contusões leves, seja a mesma que é necessária para manter no ar um avião jumbo. As consequências da falha são drasticamente diferentes e portanto precisamos ter alguma forma de relacionar a extensão das medidas de proteção ao nível de risco obtido na fase de estimativa de risco.

Qualquer que seja o tipo de dispositivo de proteção escolhido, deve-se lembrar que um “sistema relacionado à segurança” pode conter muitos elementos incluindo o dispositivo de proteção, fiação, dispositivo de chaveamento e às vezes, peças do sistema de controle operacional da máquina. Todos esses elementos do sistema (incluindo proteções, montagem, fios, etc.) devem ter características de desempenho adequadas, relevantes ao seu princípio de projeto e tecnologia. Os IEC/EN 62061 e EN ISO 13849-1 classificam os níveis hierárquicos de desempenho das peças relacionadas à segurança dos sistemas de controle e proporcionam métodos de avaliação de risco em seus anexos para determinar os requisitos de integridade de um sistema de proteção.

O EN ISO 13849-1:2008 fornece um gráfico de risco aumentado em seu anexo A.



IEC 62061 também fornece um método em seu anexo A, que assume a forma mostrada abaixo.



Avaliação de risco e medidas de segurança

Nº do documento:
Parte de:

Produto:
Emitido por:
Data:

☐ Pré-avaliação de risco
☐ Avaliação de risco intermedi
☐ Avaliação de risco de acomp

Área em preto = medidas de segurança exigidas
Área em cinza = medidas de segurança recomendadas

Consequências	Gravidade Se	Classe CI 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Frequência e duração, Fr		Probabilidade do evento de perigo, Pr		Prev
Morte, perda de olhos ou braços	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hora	5	Comum	5	
Permanente, perda de dedos	3		OM	SIL 1	SIL 2	SIL 3	> 1 h - <= 1 dia	5	Provável	4	
Reversível, com atendimento médico	2			OM	SIL 1	SIL 2	> 1 dia - <= 2 semanas	4	Possível	3	Imp
Reversível, com primeiros socorros	1				OM	SIL 1	> 2 semanas - <= 1 ano	3	Raro	2	Pr
							> 1 ano	2	Desprezível	1	P

Nº sér.	Nº perigo	Perigo	Se	Fr	Pr	Av	Cl	Medida de segurança

Comentários

O uso de qualquer um dos métodos acima deve fornecer resultados equivalentes. Cada método destina-se a levar em conta o conteúdo detalhado do padrão ao qual pertence.

Em ambos os casos, é extremamente importante que as orientações fornecidas no texto do padrão sejam utilizadas. O gráfico ou tabela de risco não deve ser utilizado isoladamente ou de uma forma demasiadamente simplista.

Avaliação

Depois que a medida de proteção for escolhida e antes que ela seja implementada, é importante repetir a estimativa de risco. Esse é um procedimento que muitas vezes é ignorado. Pode ser que se nós instalarmos uma medida de proteção, o operador da máquina pode sentir que todos estão total e completamente protegidos contra o risco originalmente previsto. Como eles já não têm a consciência original do perigo, podem intervir com a máquina de uma forma diferente. Eles podem ficar expostos ao perigo com mais frequência ou podem entrar ainda mais na máquina, por exemplo. Isso significa que se houver falha na medida de proteção, eles estarão sujeitos a um risco maior do que o previsto anteriormente. Esse é o risco atual que nós precisamos estimar. Portanto, a estimativa de risco precisa ser repetida considerando as alterações previsíveis na forma como as pessoas podem intervir com a máquina. O resultado dessa atividade é utilizado para verificar se as medidas de proteção propostas são realmente adequadas. Para obter mais informações, recomenda-se o Anexo A do IEC/ EN 62061.

Treinamento, equipamentos de proteção individual, etc.

É importante que os operadores tenham o treinamento necessário sobre os métodos de trabalho seguro para uma máquina. Isso não significa que as outras medidas possam ser omitidas. Não é aceitável simplesmente dizer a um operador que ele não deve se aproximar de áreas perigosas (como alternativa para protegê-las).

Talvez também seja necessário que o operador utilize equipamentos como luvas especiais, óculos, respiradores, etc. O projetista de máquinas deve especificar que tipo de equipamento é necessário. O uso de equipamentos de proteção individual geralmente não formará o principal método de proteção mas complementará as medidas mostradas acima.

Padrões

Muitos padrões e relatórios técnicos fornecem orientação sobre avaliação de risco. Alguns são escritos para uma vasta aplicabilidade e outros são escritos para aplicações específicas. Encontra-se a seguir uma lista de padrões que incluem informações sobre avaliação de risco.

ANSI B11.TR3: Avaliação de risco e redução de risco—Um guia para estimar, avaliar e reduzir os riscos associados com ferramentas de máquinas.

ANSI PMMI B155.1: Requisitos de segurança para máquinas de embalagem e máquinas de conversão relacionadas a embalagem.

ANSI RIA R15.06: Requisitos de segurança para robôs industriais e sistemas de robôs.

AS 4024.1301-2006: Princípios de avaliação de risco CSA Z432-04: Proteção de máquinas.

CSA Z434-03: Robôs industriais e sistemas de robôs—Requisitos gerais de segurança.

IEC/EN 61508: Segurança funcional de sistemas elétricos, eletrônicos e eletrônicos programáveis relacionados à segurança.

IEC/EN 62061: Segurança de máquinas—Segurança funcional de sistemas de controle elétricos, eletrônicos e eletrônicos programáveis relacionados à segurança.

EN ISO 13849-1: Segurança de máquinas—Peças de sistemas de controle relacionadas à segurança.

EN ISO 14121-1: Princípios de avaliação de risco.

ISO TR 14121-2: Avaliação de risco—Orientações práticas e exemplos de métodos.

Medidas de proteção e equipamentos complementares

Quando a avaliação de risco mostra que uma máquina ou processo apresenta um risco de lesões, o perigo deve ser eliminado ou contido. A forma pela qual isso é conseguido dependerá da natureza da máquina e do perigo. As medidas de proteção juntamente com a vigilância, impedem o acesso a um perigo ou evitam movimentos perigosos em uma situação de risco quando o acesso está disponível. São exemplos típicos de medidas de proteção: proteções intertravadas, cortinas de luz, tapetes de segurança, controles bimanuais e botões de habilitação.

Os sistemas e dispositivos de parada de emergência estão associados com sistemas de controle relacionados à segurança mas não são sistemas de proteção direta, eles só devem ser considerados como medidas de proteção complementares.

Prevenção de acesso com proteções delimitadoras fixas

Se o perigo estiver em uma peça das máquinas que não precise de acesso, uma proteção deverá ser fixada à máquina permanentemente. Esses tipos de proteções devem exigir ferramentas para a remoção. As proteções fixas devem ser capazes de 1) suportar seu ambiente operacional, 2) conter projéteis, quando necessário e 3) não criar riscos por terem, por exemplo, bordas afiadas. As proteções fixas podem ter aberturas onde a proteção se encontra com as máquinas ou aberturas devido ao uso de um gabinete tipo de malha de cabos.

As janelas proporcionam formas convenientes para monitorar o desempenho da máquina, ao acessar essa parte da máquina. Deve-se tomar cuidado na seleção do material utilizado, pois as interações químicas com fluidos de corte, os raios ultravioletas e o envelhecimento simples causam a redução dos materiais da janela ao longo do tempo.

O tamanho das aberturas deve impedir que o operador alcance a zona de perigo. As Tabela O-10 nos EUA. OHSA 1910.217 (f) (4), ISO 13854, Tabela D-1 do ANSI B11.19, Tabela 3 da CSA Z432 e o AS4024.1 fornecem orientação sobre a distância adequada que uma abertura deve manter em relação ao perigo.

Detecção de acesso

As medidas de proteção podem ser utilizadas para detectar o acesso a um perigo. Quando a detecção é selecionada como o método de redução de riscos, o projetista deve entender que deve ser utilizado um sistema de segurança completa; o dispositivo de proteção, por si só, não oferece a redução de risco necessária.

Este sistema de segurança consiste geralmente em três blocos: 1) um dispositivo de entrada que detecta o acesso ao perigo, 2) um dispositivo de lógica que processa os sinais do dispositivo de detecção, verifica o status do sistema de segurança e ativa ou desativa dispositivos de saída e 3) um dispositivo de saída que controla o atuador (por exemplo, um motor).

Dispositivos de detecção

Muitos dispositivos alternativos estão disponíveis para detectar a presença de uma pessoa que entra ou já está dentro de uma área de risco. A melhor escolha para uma aplicação específica depende de uma série de fatores.

- Frequência de acesso,
- Tempo de parada do perigo,
- Importância de completar o ciclo de máquina e
- Contenção de projéteis, fluidos, névoas, vapores, etc.

As proteções móveis selecionadas adequadamente podem ser intertravadas para fornecer proteção contra projéteis, fluidos, névoas e outros tipos de perigos e, muitas vezes, são utilizadas quando o acesso ao perigo não é frequente. As proteções intertravadas também podem ser bloqueadas para impedir o acesso enquanto a máquina está no meio do ciclo e quando a máquina leva muito tempo para chegar a uma parada.

A presença de dispositivos de detecção, como cortinas de luz, tapetes e scanners, fornece acesso rápido e fácil à área de perigo e, muitas vezes, são selecionados quando os operadores frequentemente precisam acessar a área de perigo. Esses tipos de dispositivos não fornecem proteção contra projéteis, névoas, fluidos ou outros tipos de perigos.

A melhor escolha da medida de proteção é um dispositivo ou sistema que forneça a proteção máxima com o mínimo obstáculo para a operação normal da máquina. Todos os aspectos da utilização da máquina devem ser considerados, pois a experiência mostra que um sistema que é difícil de utilizar é mais suscetível de ser removido ou desviado.

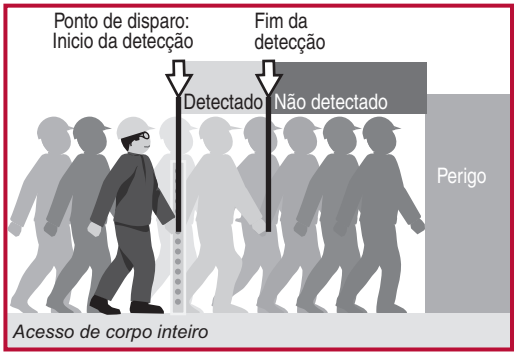
Presença de dispositivos de detecção

Ao decidir como proteger uma zona ou área, é importante ter uma compreensão clara sobre exatamente quais funções de segurança são necessárias. Em geral, haverá pelo menos duas funções.

- Desligue ou desative a alimentação quando uma pessoa entrar na área de perigo.
- Evite ligar ou ativar a alimentação quando uma pessoa estiver na área de perigo.

Em uma primeira análise, essas podem parecer formar uma única função, mas embora estejam obviamente ligadas e, muitas vezes, sejam realizadas pelo mesmo equipamento, elas são na verdade duas funções separadas. Para alcançar o primeiro ponto precisamos utilizar alguma forma de dispositivo de travamento. Em outras palavras, um dispositivo que detecta que uma parte de uma pessoa passou de um determinado ponto e dá um sinal de desligamento da alimentação. Caso a pessoa seja capaz, então, de ultrapassar esse ponto de travamento e sua

presença não for mais detectada, o segundo ponto (que evita a ativação) talvez não seja atingido.



O diagrama a seguir mostra um exemplo de acesso de corpo inteiro com uma cortina de luz montada verticalmente como dispositivo de travamento. As portas de proteção intertravadas também podem ser consideradas como um dispositivo exclusivo de travamento quando não há nada que impeça o fechamento da porta após a entrada.

Caso não seja possível o acesso de corpo inteiro de modo que uma pessoa não seja capaz de ultrapassar o ponto de travamento, sua presença sempre será detectada e o segundo ponto (que evita a ativação) será atingido.

Para aplicações corporais parciais, os mesmos tipos de dispositivos executam o travamento e a detecção de presença. A única diferença reside no tipo de aplicação.

Os dispositivos de detecção de presença são utilizados para detectar a presença de pessoas. A família de dispositivos inclui cortinas de luz de proteção, barreiras de segurança de feixe simples, scanners da área de segurança, tapetes de segurança e bordas de segurança.

Cortinas de luz de proteção

As cortinas de luz de proteção são descritas de forma mais simples como sensores de presença fotoelétricos projetados especificamente para proteger os funcionários de lesões relacionadas com o movimento perigoso da máquina. Também conhecidas como AOPDs (dispositivos ativos de proteção optoeletrônica) ou ESPE (equipamento de proteção eletrossensível), as cortinas de luz oferecem a segurança ideal e ainda permitem maior produtividade e representam a solução mais íntegra ergonomicamente, quando comparada às proteções mecânicas. Elas são ideais para aplicações onde os funcionários precisam de acesso frequente e fácil a um ponto de perigo operacional.

As cortinas de luz são projetadas e testadas para atender o IEC 61496-1 e -2. Não há nenhuma versão EN harmonizada da parte 2, por isso, o Anexo IV da diretriz de máquinas europeias exige certificação das cortinas de luz por terceiros antes de colocá-las no mercado da Comunidade Europeia. Os terceiros testam as cortinas de luz para atender este padrão internacional. O laboratório do tomador adotou o IEC 61496-1 como o padrão nacional dos EUA.

Scanners de proteção a laser

Os scanners de proteção a laser utilizam um espelho rotativo que desvia pulsos de luz ao longo de um arco, criando um plano de detecção. A localização do objeto é determinada pelo ângulo da rotação do espelho. Ao utilizar a técnica de “tempo de voo” de um feixe refletido de luz invisível, o scanner também pode detectar a distância do objeto até o scanner. A partir da distância medida e da localização do objeto, o scanner a laser determina a posição exata do objeto.

Tapetes de segurança com detecção de pressão

Esses dispositivos são utilizados para fornecer a proteção de uma área de pavimento em torno de uma máquina. Uma matriz de tapetes interconectados é colocada em torno da área de perigo e a pressão aplicada no tapete (por exemplo, uma pisada do operador) fará com que a unidade controladora do tapete desligue a alimentação diante do perigo. Os tapetes sensíveis à pressão muitas vezes são utilizados dentro de uma área fechada contendo várias máquinas—sistemas flexíveis de manufatura ou células robóticas, por exemplo. Quando é necessário o acesso à célula (por exemplo, para configuração ou “treinamento” de robôs), eles impedem o movimento perigoso, caso o operador se desvie da área segura ou precise ficar atrás de um equipamento.

O tamanho e posicionamento do tapete devem levar em conta a distância de segurança.

Bordas sensíveis à pressão

Esses dispositivos são tiras de rebordo flexível que podem ser montadas na borda de uma peça móvel, como uma mesa de máquina ou porta energizada que represente o risco de um esmagamento ou corte.

Se a peça móvel atingir o operador (ou vice-versa), a borda sensível flexível será pressionada e ativará um comando para desligar a fonte de alimentação perigosa. As bordas sensíveis também podem ser utilizadas para proteger as máquinas quando houver um risco de enroscamento do operador. Caso um operador fique preso na máquina, o contato com a borda sensível desligará a alimentação da máquina.

Há uma série de tecnologias utilizadas para criar bordas de segurança. Uma tecnologia popular é inserir, essencialmente, o que é um interruptor longo dentro da borda. Essa abordagem fornece bordas axiais e geralmente utiliza a técnica da conexão de 4 fios.

Cortinas de luz, scanners, tapetes de assoalho e bordas sensíveis são classificados como “dispositivos de disparo”. Na verdade, eles não restringem o acesso, mas apenas o “detectam”. Eles dependem inteiramente de sua capacidade tanto de detecção quanto de comutação para proporcionar segurança. Em geral, eles só são adequados nas máquinas que param com razoável rapidez após o desligamento da fonte de alimentação. Como um operador pode andar ou chegar diretamente à área de perigo, é obviamente necessário que o tempo gasto com a parada do movimento seja menor que o necessário para o operador alcançar o perigo, após o disparo do dispositivo.

Interruptor de segurança

Quando o acesso à máquina não é frequente, preferem-se as proteções (operáveis) móveis. A proteção é intertravada com a fonte de alimentação do perigo de forma a garantir que sempre que a porta de proteção não estiver fechada, a fonte do perigo será desligada. Essa abordagem envolve o uso de um interruptor de intertravamento equipado com a porta de proteção. O controle da fonte de alimentação do perigo é roteado através da seção de interruptores da unidade. A fonte de alimentação é geralmente elétrica, mas também pode ser pneumática ou hidráulica. Quando é detectado o movimento (abertura) da porta de proteção, o interruptor de intertravamento ativará um comando para isolar a fonte de alimentação do perigo diretamente ou através de um contator (ou válvula) de potência.

Alguns interruptores de intertravamento também incorporam um dispositivo de travamento que bloqueia a porta de proteção e não a libera até que a máquina esteja em uma condição segura. Para a maioria das aplicações, a combinação de uma proteção móvel e uma chave de intertravamento, com ou sem bloqueio, é a solução mais confiável e rentável.

Há uma grande variedade de opções de interruptor de segurança, incluindo:

- **Chaves de intertravamento com linguetas** - esses dispositivos exigem que um atuador em forma de lingueta seja inserido e retirado do interruptor para operação
- **Chaves de intertravamento com dobradiças** - esses dispositivos são colocados no pino com dobradiças de uma porta de proteção e utilizam o movimento de abertura da proteção para atuarem.
- **Chaves de travamento de proteção** - em algumas aplicações, é necessário o travamento da proteção fechada ou o retardo da abertura da proteção. Os dispositivos apropriados para este requisito são denominados chaves de intertravamento de proteção. Eles são adequados para máquinas com características de redução de funcionamento mas também podem fornecer um aumento significativo do nível de proteção para a maioria dos tipos de máquinas.

- **Chaves de intertravamento sem contato** - esses dispositivos não exigem nenhum contato físico para acionarem algumas versões que incorporam uma função de codificação para maior resistência a adulterações.
- **Intertravamentos de posição (chave fim de curso)** - o acionamento operado por came geralmente adquire a forma de um interruptor de limite (ou posição) de modo positivo e um came linear ou giratório. É geralmente utilizado em dispositivos corrediços.
- **Intertravamentos de chaves com segredo** - as chaves com segredo podem realizar o intertravamento de controles, bem como o intertravamento da alimentação. Com o “intertravamento de controles”, um dispositivo de intertravamento inicia um comando de interrupção de um dispositivo intermediário, que desativa um dispositivo subsequente para desligar a energia do atuador. Com o “intertravamento da alimentação” o comando de parada interrompe diretamente o fornecimento de energia para os atuadores da máquina.

Dispositivos de interface do operador

Função de parada - nos EUA, Canadá, Europa e em nível internacional, a harmonização de padrões existe com relação às descrições das categorias de parada de máquinas ou sistemas de fabricação.

OBSERVAÇÃO: essas categorias são diferentes para as categorias de EN 954-1 (ISO 13849-1). Consulte os padrões NFPA79 e IEC/EN60204-1 para obter mais detalhes. As paradas recaem em três categorias:

Categoria 0 é a parada pela remoção imediata da alimentação dos atuadores de máquinas. Essa é considerada uma parada incontrolável. Com a remoção da alimentação, a ação de frenagem, que requer alimentação, não surtirá efeito. Isso permitirá que os motores girem livremente e parem por inércia durante um período prolongado de tempo. Em outros casos, o material pode ser descartado por gabaritos de suporte, exigindo que a alimentação retenha o material. Os meios de parada mecânica, que não precisam de alimentação, também podem ser utilizados com uma parada de categoria 0. A parada de categoria 0 tem prioridade sobre as paradas de categoria 1 ou categoria 2.

Categoria 1 é uma parada controlada com alimentação disponível para que os atuadores da máquina alcancem a parada. A alimentação é então, removida dos atuadores quando a paragem é atingida. Esta categoria de parada permite a frenagem energizada no intuito de interromper rapidamente movimentos perigosos e então, a alimentação pode ser retirada dos atuadores.

Categoria 2 é uma parada controlada com a alimentação disponibilizada para os atuadores da máquina. Uma parada da produção normal é considerada uma parada de categoria 2.

Essas categorias de parada devem ser aplicadas a cada função de parada, onde a função de parada é a ação executada pelas peças do sistema de controle relacionadas à segurança em resposta a uma entrada, deve ser utilizada a categoria 0 ou 1. As funções de parada devem inibir as funções relacionadas à partida. A seleção da categoria de parada para cada função de parada deve ser determinada por uma avaliação de risco.

Função de parada de emergência

A função de parada de emergência deve funcionar como uma parada de categoria 0 ou categoria 1, conforme determinado por uma avaliação de risco. Ela deve ser iniciada por uma única ação humana. Quando executada, ela deve inibir todas as outras funções e modos operacionais da máquina. O objetivo é remover a alimentação o mais rápido possível, sem criar perigos adicionais.

Até recentemente, os componentes eletromecânicos ligados por cabos eram necessários para os circuitos de parada de emergência. As recentes alterações em padrões tais como IEC 60204-1 e NFPA 79 significam que as PLCs de segurança e outras formas de lógica eletrônica que satisfaçam os requisitos de padrões como o IEC61508 podem ser utilizadas no circuito de parada de emergência.

Dispositivos de parada de emergência

Onde quer que haja o perigo de um operador se envolver em problemas com uma máquina, deve haver uma facilidade para acesso rápido a um dispositivo de parada de emergência. O dispositivo de parada de emergência deve estar continuamente operável e prontamente disponível. Os painéis do operador devem conter pelo menos, um dispositivo de parada de emergência. Podem ser utilizados dispositivos adicionais de parada de emergência em outros locais, conforme necessário. Os dispositivos de parada de emergência são fornecidos em diversos formatos. Os botões e chaves de acionamento por cabos são exemplos dos dispositivos do tipo mais popular. Quando um dispositivo de parada de emergência é acionado, ele deve travar por dentro e não deve ser possível gerar o comando de parada sem travar. A remoção do dispositivo de parada de emergência não deve causar uma situação de perigo. Uma ação separada e deliberada deve ser utilizada para reiniciar a máquina.

Para obter mais informações sobre dispositivos de parada de emergência, leia: ISO/EN13850, IEC 60947-5-5, NFPA79 e IEC60204-1, AS4024.1, Z432-94.

Botões de parada de emergência

Os dispositivos de parada de emergência são considerados equipamentos de proteção de cortesia. Eles não são considerados dispositivos de proteção primários, pois não impedem o acesso a um perigo nem detectam o acesso.

A maneira normal de proporcionar isso é sob a forma de um botão pulsador com cabeçote tipo cogumelo de cor vermelha em um fundo amarelo, que o operador pressiona, em caso de emergência. Eles devem ser colocados estrategicamente

em quantidade suficiente em volta da máquina para garantir que haja sempre um botão acessível em uma situação de risco.

Os botões de parada de emergência devem estar prontamente acessíveis e devem estar disponíveis em todos os modos de operação de máquinas. Quando um botão pulsador é utilizado como dispositivo de parada de emergência, ele deve ser em forma de cogumelo (ou operado na palma), na cor vermelha e com fundo amarelo. Quando o botão é pressionado, os contatos devem alterar, ao mesmo tempo, o estado das travas do botão na posição pressionada.

Uma das mais recentes tecnologias a ser aplicada às paradas de emergência é a técnica de automonitoração. Mais um contato é adicionado à parada de emergência da parte traseira que monitora se a parte traseira dos componentes do painel ainda está presente. Isso é conhecido como bloco de contatos Self-Monitoring. Ele consiste em um contato acionado por mola que se fecha quando o bloco de contatos é encaixado no lugar adequado do painel. A Figura 80 mostra o contato de automonitoração conectado em série com um dos contatos diretos da segurança de abertura.

Chaves de acionamento por cabo

Para máquinas como transportadores, muitas vezes, é mais conveniente e eficaz utilizar um dispositivo de acionamento por cabo ao longo da zona de perigo, como os dispositivos de parada de emergência. Esses dispositivos utilizam uma corda de cabos de aço conectada aos interruptores de acionamento de travas para que, ao puxar a corda em qualquer direção e em qualquer ponto ao longo de seu comprimento, ocorra o disparo do interruptor e o corte da alimentação da máquina.

As chaves de acionamento por cabos devem detectar tanto uma tração sobre o cabo como a ocorrência de folgas no cabo. A detecção de folgas garante que o cabo não seja cortado e esteja pronto para uso.

A distância do cabo afeta o desempenho do interruptor. Para curtas distâncias, o interruptor de segurança é montado em uma extremidade e uma mola de tensão é montada na outra extremidade. Para distâncias mais longas, um interruptor de segurança deve ser montado em ambas as extremidades do cabo para garantir que uma única ação do operador inicie um comando de parada. A força necessária de acionamento por cabo não deve exceder 200 N (45 libras) ou uma distância de 400 mm (15,75 pol.) em uma posição centralizada entre dois suportes de cabos.

Controles bimanuais

O uso de controles de duas mãos (também denominados controles bimanuais) é um método comum de impedir o acesso, enquanto a máquina estiver em uma condição de perigo. Dois controles devem ser operados simultaneamente (com um intervalo de 0,5 s um do outro) para ativar a máquina. Isso garante que as duas mãos do operador estejam ocupadas em uma posição segura (ou seja, no comando) e portanto, não possam estar na zona de perigo. Os controles devem ser operados continuamente durante as condições de perigo. A operação da máquina deve

cessar quando um dos controles for liberado; se um controle for liberado, o outro controle também deve ser liberado antes que a máquina possa ser reiniciada.

Um sistema de controle bimanual depende fortemente da integridade de seu controle e sistema de monitoração para detectar quaisquer falhas; por isso, é importante que este aspecto seja projetado para a especificação correta. O desempenho do sistema de segurança bimanual é caracterizado em tipos pelo ISO 13851 (EN 574) conforme mostrado e estão relacionados às categorias do ISO 13849-1. Os tipos mais comumente utilizados para a segurança de máquinas são IIIB e IIIC. A tabela abaixo mostra o relacionamento dos tipos de categorias do desempenho de segurança.

Requisitos	Tipos				
	I	II	III		
			A	B	C
Atuação síncrona			X	X	X
Uso da Categoria 1 (do ISO 13849-1)	X		X		
Uso da Categoria 3 (do ISO 13849-1)		X		X	
Uso da Categoria 4 (do ISO 13849-1)					X

O espaçamento do projeto físico deve impedir a operação inadequada (por exemplo, pela mão e cotovelo). Isso pode ser realizado pela distância ou blindagens. A máquina não deve passar de um ciclo para outro, sem a liberação e o pressionamento de ambos os botões. Isso evita a possibilidade de os dois botões serem bloqueados, deixando a máquina em funcionamento contínuo. A liberação de um dos botões deve causar a parada da máquina.

O uso do controle bimanual deve ser considerado com cautela, pois geralmente deixa exposta alguma forma de risco. O controle bimanual protege apenas a pessoa que o utiliza. O operador protegido deve ser capaz de observar todo o acesso ao perigo, pois talvez outros funcionários não estejam protegidos.

O ISO 13851 (EN574) fornece orientação adicional sobre o controle bimanual.

Dispositivos de habilitação

Dispositivos de habilitação são controles que permitem que um operador entre em uma zona de perigo durante a ocorrência do perigo, somente enquanto o operador estiver segurando o dispositivo de habilitação na posição acionada. Os dispositivos de habilitação utilizam interruptores do tipo com duas posições ou com três posições. Os tipos com duas posições ficam desativados quando o atuador não é operado e ficam ativados quando o atuador é operado. Os interruptores de três posições ficam desativados quando não acionados (posição 1) e ativados quando retidos na posição central (posição 2) e desligados quando o atuador é operado após a posição média

(posição 3). Além disso, ao retornar da posição 3 para a 1, o circuito de saída não deve fechar ao passar pela posição 2.

Os dispositivos de habilitação devem ser utilizados em conjunto com outra função relacionada à segurança. Um exemplo típico é a disposição do movimento em um modo lento controlado. Uma vez em modo lento, um operador pode entrar na área de perigo, segurando o dispositivo de habilitação.

Ao utilizar um dispositivo de habilitação, um sinal deve indicar que esse dispositivo está ativo.

Dispositivos de lógica

Os dispositivos de lógica desempenham uma função central na parte do sistema de controle relacionada à segurança. Os dispositivos de lógica executam a verificação e monitoração do sistema de segurança e permitem que a máquina seja inicializada ou execute comandos de parada da máquina.Os dispositivos de lógica executam a verificação e monitoração do sistema de segurança e permitem que a máquina seja inicializada ou execute comandos de parada da máquina.

Uma gama de dispositivos lógicos está disponível para criar uma arquitetura de segurança correspondente à complexidade e funcionalidade exigidas para a máquina. Relés de segurança de monitoração menores com fios são mais econômicos para máquinas menores onde um dispositivo lógico dedicado é necessário para concluir a função de segurança. Relés de segurança de monitoração modulares e configuráveis são preferidos onde um número amplo e diverso de dispositivos de segurança e controle de zona mínimo são necessários. O meio para máquinas maiores e mais complexas encontrará sistemas programáveis com E/S distribuída como preferível.

Relés de segurança de monitoração

Módulos de relé de segurança de monitoração (MSR) desempenham um papel essencial em vários sistemas de segurança. Esses módulos geralmente são formados por dois ou mais relés guiados positivamente com circuitos adicionais para assegurar o desempenho da função de segurança.

Relés guiados positivos são relés “cubo de gelo” especializados. Relés guiados positivamente devem atender às exigências de desempenho do EN50025. Essencialmente, eles são projetados para evitar que os contatos normalmente fechados e normalmente abertos fechem simultaneamente. Projetos mais recentes substituem as saídas eletromecânicas por saídas de estado sólido nominais de segurança.

Relés de segurança de monitoração realizam várias verificações no sistema de segurança. Ao serem energizados, eles realizam autoverificações em seus componentes internos. Quando os dispositivos de entrada são ativados, o MSR compara os resultados das entradas redundantes. Caso seja aceitável, o MSR verifica os atuadores externos. Caso esteja tudo bem, o MSR aguarda um sinal de reset para energizar suas saídas.

A seleção do relé de segurança apropriado depende de uma série de fatores: tipo de dispositivo que monitora, o tipo de reset, o número e o tipo de saídas.

Tipos de entradas

Dispositivos de segurança têm diferentes tipos de métodos para indicar que algo aconteceu:

Intertravamentos de contato e paradas de emergência: Contatos mecânicos, canal único com um contato normalmente fechado ou canal duplo, ambos normalmente fechados. O MSR deve ser capaz de aceitar um canal único ou duplo e proporcionar detecção de falha cruzada para a distribuição do canal duplo.

Intertravamentos sem contatos e paradas de emergência: Contatos mecânicos, canal duplo, um contato normalmente aberto e um normalmente fechado. O MSR deve ser capaz de processar várias entradas.

Dispositivos de chaveamento de estado sólido de saída: Cortinas de luz, scanners a laser, sem contatos de estado sólido têm duas saídas de alimentação e realizam sua própria detecção de falha cruzada. O MSR deve ser capaz de ignorar o método de detecção de falha cruzada dos dispositivos.

Tapetes sensíveis à pressão: Os tapetes criam um curto-circuito entre dois canais. O MSR deve ser capaz de suportar os curtos-circuitos repetidos.

Bordas sensíveis à pressão: Algumas bordas são projetadas como tapetes de 4 fios. Algumas são dispositivos de dois fios que criam mudança na resistência. O MSR deve ser capaz de detectar um curto-circuito ou a alteração na resistência.

Tensão: Mede a força contra eletromotriz de um motor durante reduções. O MSR deve ser capaz de tolerar altas tensões e detectar baixas tensões à medida que o motor diminui a rotação.

Movimento interrompido: O MSR deve detectar fluxos de pulso de sensores diversos e redundantes.

Controle bimanual: O MSR deve detectar entradas diversas normalmente abertas e normalmente fechadas, além de fornecer temporização de 0,5 s e lógica de sequenciamento.

Relés de segurança de monitoração devem ser projetados especificamente para realizar interface com cada um desses tipos de dispositivo, pois têm diferentes características elétricas. Alguns MSRs podem se conectar a poucos tipos diferentes de entradas, porém, após o dispositivo ser escolhido, o MSR somente pode realizar interface com esse dispositivo. O projetista deve selecionar um MSR compatível com o dispositivo de entrada.

Impedância de entrada

A impedância de entrada dos relés de segurança de monitoração determina quantos dispositivos de entrada podem ser conectados ao relé e a distância na qual os dispositivos de entrada podem ser montados. Por exemplo, um relé de segurança pode ter uma impedância de entrada permitida máxima de 500 ohms (~). Quando a impedância de entrada for superior a 500~, ela não comutará em suas saídas. O usuário deve ter cuidado para assegurar que a impedância de entrada permaneça abaixo da especificação máxima. O comprimento, tamanho e tipo de fio usado afetam a impedância de entrada.

Número de dispositivos de entrada

O processo de avaliação de risco deve ser usado para ajudar a determinar quantos dispositivos de entrada devem ser conectados a um MSR de unidade de relé de segurança de monitoração e com que frequência os dispositivos devem ser verificados. Para assegurar que as paradas de emergência e os intertravamentos de porta estejam em estado operacional, eles devem ser verificados para operação em intervalos regulares, conforme determinado pela avaliação de risco. Por exemplo, um MSR de entrada de canal duplo conectado a uma porta de intertravamento que deve ser aberta a cada ciclo da máquina (por ex.: várias vezes ao dia) pode não precisar de verificação. Isso ocorre porque abrir a proteção faz com que o MSR realize uma autoverificação em suas entradas e saídas (dependendo da configuração) para identificar falhas únicas. Quanto maior a abertura da proteção, maior a integridade do processo de verificação.

Outro exemplo pode ser a parada de emergência. Como as paradas de emergência são tipicamente usadas apenas para emergências, são raramente utilizadas. Portanto, um programa deve ser estabelecido para exercitar as paradas de emergência e confirmar sua eficácia periodicamente. Exercitar o sistema de segurança desse modo é chamado de Teste de prova, o intervalo entre os Testes de prova é chamado de Intervalo de teste de provas. Um terceiro exemplo pode ser as portas de acesso para ajustes de máquina, que, assim como as paradas de emergência, raramente são usadas. Aqui, novamente, um programa deve ser estabelecido para exercitar a função de verificação periodicamente.

A avaliação de risco ajudará a determinar se os dispositivos de entrada precisam ser verificados e com que frequência devem ser verificados. Quanto maior o nível de risco, maior a integridade necessária do processo de verificação. E quanto menos frequente a verificação “automática”, mais frequente deve ser a verificação “manual” imposta.

Detecção de falha cruzada de entrada

Em sistemas de canal duplo, falhas de curto-circuito de canal a canal dos dispositivos de entrada, também conhecidas como falhas cruzadas, devem ser detectadas pelo sistema de segurança. Isso é alcançado pelo dispositivo de detecção ou pelo relé de segurança de monitoração.

Relés de segurança de monitoração baseados em microprocessador, como cortinas de luz, scanners a laser e sensores sem contato avançados detectam esses curtos de várias formas diferentes. Uma forma comum de detectar falhas cruzadas é utilizar testes de pulso diversos. Os sinais de saída são pulsados com muita rapidez. O pulso do canal 1 é desviado do pulso do canal 2. Caso ocorra um curto, os pulsos ocorrem ao mesmo tempo e são detectados pelo dispositivo.

Relés de segurança de monitoração baseados em eletromecânica usam uma técnica de diversidade diferente: uma entrada de energização e uma entrada de desenergização. Um curto do Canal 1 para o Canal 2 tornará o dispositivo de proteção de sobrecorrente ativo e o sistema de segurança desligará.

Saídas

Os MSRs vêm com vários números de saídas. Os tipos de saídas ajudam a determinar qual MSR deve ser usado em aplicações específicas.

A maioria dos MSRs tem no mínimo 2 saídas de segurança operando imediatamente. As saídas de segurança de MSR são caracterizadas como normalmente abertas. Elas são classificadas como de segurança devido à redundância e verificação interna. Um segundo tipo de saída é representado pelas saídas com atraso. Em geral, saídas com atraso são usadas em paradas de Categoria 1, onde a máquina necessita de tempo para executar a função de parada antes de permitir acesso à área de perigo. Os MSRs também têm saídas auxiliares. Em geral, elas são consideradas normalmente fechadas.

Capacidades de saída

Capacidades de saída descrevem a habilidade do dispositivo de segurança em comutar cargas. Com frequência, as capacidades para dispositivos industriais são descritas como resistivas ou eletromagnéticas. Uma carga resistiva pode ser um elemento de tipo térmico. Cargas eletromagnéticas, em geral, são relés, contatores ou solenoides; onde há uma grande característica indutiva da carga. O anexo A do padrão IEC 60947-5-1, descreve as capacidades para cargas. Isso também é exibido na seção ‘‘princípios’’ do catálogo de Segurança.

Letra de designação: A designação é uma letra seguida por um número, por exemplo, A300. A letra é relacionada com a corrente térmica incluída convencional e se a corrente é contínua ou alternada. Por exemplo, A representa corrente alternada de 10 A. O número representa a tensão de isolamento classificado. Por exemplo, 300 representa 300 V.

Utilização: A utilização descreve os tipos de cargas às quais o dispositivo é designado para comutar. As utilizações relevantes para IEC 60947-5 são exibidas na seguinte tabela.

Utilização	Descrição de carga
AC-12	Controle de cargas resistivas e de estado sólido com isolação por acoplamentos ópticos
AC-13	Controle de cargas de estado sólido com isolamento por transformador
AC-14	Controle de cargas eletromagnéticas pequenas (inferiores a 72 VA)
AC-15	Cargas eletromagnéticas superiores a 72 VA
DC-12	Controle de cargas resistivas e de estado sólido com isolação por acoplamentos ópticos
DC-13	Controle de eletromagnetos
DC-14	Controle de cargas eletromagnéticas com resistores de economia no circuito

Corrente térmica, Ith: A corrente térmica incluída convencional é o valor de corrente usado para testes de elevação de temperatura do equipamento quando montado em um compartimento específico.

Tensão operacional nominal Ue e Corrente Ie; A corrente operacional nominal e a tensão especificam as capacidades de realização e rompimento dos elementos de comutação sob condições operacionais normais. Os produtos Allen-Bradley Guardmaster têm capacidade específica de 125 Vca, 250 Vca e 24 Vcc. Consulte a fábrica para uso em tensões diferentes dessas capacidades especificadas.

VA: As capacidades de VA (Tensão x Amperagem) indicam as capacidades dos elementos de comutação quando realizam o circuito e quando rompem o circuito.

Exemplo 1: Uma capacidade de A150, AC-15 indicam que os contatos podem realizar um circuito de 7200 VA. Em 120 Vca, os contatos podem realizar um circuito de energização de 60 A. Considerando que a AC-15 é uma carga eletromagnética, os 60 A funcionam apenas para curta duração; a corrente de energização da carga eletromagnética. O rompimento do circuito é de apenas 720 VA, pois a corrente de estado estável da carga eletromagnética é de 6 A, que é a corrente operacional nominal.

Exemplo 2: Uma capacidade de N150, CC-13 indica que os contatos podem realizar um circuito de 275 VA. A 125 Vca, os contatos podem realizar um circuito de 2,2 A. As cargas eletromagnéticas de CC não têm corrente de energização como cargas eletromagnéticas de CA. O rompimento do circuito também é de 275 VA, pois a corrente de estado estável da carga eletromagnética é de 2,2, que é a corrente operacional nominal.

Reinicialização da máquina

Se, por exemplo, uma proteção intertravada é aberta em uma máquina em operação, a chave de intertravamento de segurança interromperá a máquina. Na maioria das circunstâncias é imperativo que a máquina não reinicie imediatamente quando a proteção estiver fechada. Uma maneira comum de conseguir isso é providenciar um arranjo inicial do contator de retenção.

Pressionar e soltar o botão PARTIDA momentaneamente energiza a bobina de controle do contator, que fecha os contatos de potência. Enquanto a energia percorrer os contatos de potência, a bobina de controle é mantida energizada (eletricamente retida) por meio dos contatos auxiliares do contator que são mecanicamente vinculados aos contatos de potência. Qualquer interrupção da alimentação principal ou do abastecimento de controle resultará na desenergização da bobina e na abertura dos contatos de alimentação principal e auxiliares. A proteção de intertravamento é conectada ao circuito de controle do contator. Isso significa que a reinicialização somente pode ocorrer ao fechar a proteção e, em seguida, colocar a posição “ON” no botão PARTIDA normal, que redefine o contator e aciona a máquina.

A exigência para situações normais de intertravamento é esclarecida no ISO 12100-1, Parágrafo 3.22.4 (trecho)

“Quando a proteção é fechada, as funções perigosas da máquina fechadas pela proteção podem operar, mas o fechamento da proteção não inicia a operação automaticamente”.

Várias máquinas já têm contatores únicos ou duplos que operam como descrito acima (ou têm um sistema que alcança o mesmo resultado). Quando um intertravamento é instalado nas máquinas existentes, é necessário determinar se o arranjo do controle de potência atende a esse requisito e tomar eventuais medidas adicionais.

Funções de reset

Os relés de segurança de monitoração Allen Bradley Guardmaster são projetados com reset manual monitorado ou reset automático/manual.

Reset manual monitorado

Um reset manual monitorado necessita de mudança de estado do circuito de reset após o fechamento da porta ou o reset da parada de emergência. Os contatos auxiliares normalmente fechados e conectados mecanicamente dos contatores de chaveamento de alimentação são conectados em série com um botão momentâneo. Após abrir e fechar a proteção novamente, o relé de segurança não permitirá que a máquina seja reinicializada até que haja mudança de estado no botão de reset. Isso está em conformidade com o propósito das exigências para reset manual adicional estabelecidas no EN ISO 13849-1. Ou seja, a função reset assegura que ambos os contatores estejam DESLIGADOS e que ambos os circuitos de intertravamento (e portanto, as proteções) estejam fechados e também (devido à necessidade de mudança de estado) que o atuador de reset não seja desviado ou bloqueado de forma alguma. Caso essas verificações sejam bem-sucedidas, a máquina poderá, então, ser reinicializada a partir dos controles normais. O EN ISO 13849-1 menciona a mudança de estado de energizado para desenergizado, no entanto, o mesmo princípio protetor também pode ser alcançado pelo efeito contrário.

A chave de rearme deve ser localizada em um local que ofereça uma boa visão do perigo, para que o operador possa verificar se a área está limpa antes da operação.

Reset automático/manual

Alguns relés de segurança têm reset automático/manual. O modo de reset manual não é monitorado e o reset ocorre quando o botão é pressionado. Uma chave de rearme em curto-circuito ou com interferência não será detectada. Com essa abordagem, pode não ser possível cumprir as exigências para reset manual adicional como informado no EN ISO 13849-1, a menos que meios adicionais sejam usados.

De modo alternativo, a linha de reset pode ter jumper, permitindo um reset automático. O usuário deve oferecer outro mecanismo para evitar a inicialização da máquina quando a porta fechar.

Um dispositivo de reset automático não necessita de ação de chaveamento manual, no entanto, após o fim da atuação, sempre realizará uma verificação de integridade do sistema antes de reiniciá-lo. Um sistema de reset automático não deve ser confundido com um dispositivo sem instalações de reset. Por último, o sistema de segurança será ativado imediatamente após o fim da atuação, porém, não haverá verificação de integridade do sistema.

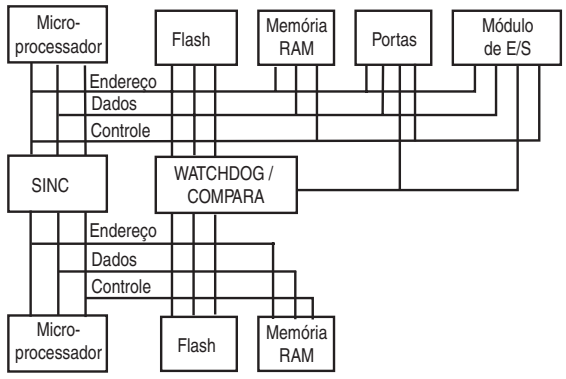
A chave de rearme deve ser localizada em um local que ofereça uma boa visão do perigo, para que o operador possa verificar se a área está limpa antes da operação.

Proteções de controle

Uma proteção de controle interrompe a máquina quando a proteção é aberta e a reinicia diretamente quando a proteção é fechada. O uso de proteções de controle somente é permitido em determinadas condições severas, pois qualquer inicialização ou falha em interromper inesperadas seriam extremamente perigosas. O sistema de intertravamento deve ter a maior confiabilidade possível (geralmente é aconselhável usar o travamento de proteção). O uso de proteções de controle SOMENTE pode ser considerado nas máquinas quando NÃO HOUVER POSSIBILIDADE de um operador ou parte do seu corpo permanecer ou estiver ao alcance da zona de perigo enquanto a proteção estiver fechada. A proteção de controle deve ser o único acesso à área de perigo.

Controles lógicos programáveis de segurança

A necessidade de aplicações flexíveis e escalonáveis motivaram o desenvolvimento de controladores/CLPs de segurança. Controladores de segurança programáveis proporcionam aos usuários o mesmo nível de flexibilidade de controle em uma aplicação de segurança que estão acostumados com controladores programáveis padrão. No entanto, há várias diferenças entre os CLPs padrão e de segurança. Os CLPs de segurança vêm em várias plataformas para acomodar exigências de expansibilidade, funcionalidade e integração dos sistemas de segurança mais complexos.



Arquitetura 1oo2D

Múltiplos microprocessadores são usados para processar a memória de E/S e comunicações de segurança. Circuitos watchdog realizam análise de diagnóstico. Esse tipo de construção é conhecido como 1oo2D, pois um dos dois microprocessadores pode realizar a função de segurança e diagnósticos amplos são realizados para assegurar que ambos os microprocessadores estejam operando em sincronia.

Além disso, cada circuito de entrada é internamente testado várias vezes a cada segundo para assegurar que esteja operando corretamente. É possível acionar a parada de emergência somente uma vez ao mês; porém, quando fizer isso, o circuito terá sido testado continuamente, de modo que a parada de emergência seja percebida de forma correta e internamente para o CLP de segurança.

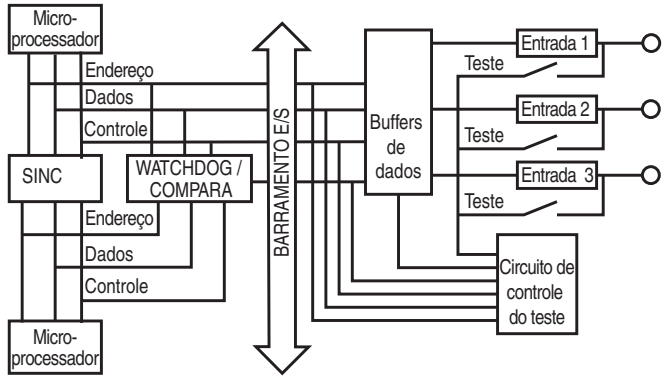


Diagrama de blocos do módulo de entrada de segurança

Saídas de segurança de CLP são de estado sólido classificado como de segurança ou eletromecânico. Como os circuitos de entrada, os circuitos de saída são testados várias vezes a cada segundo para assegurar que conseguem desligar a saída. Caso um dos três falhe, a saída é desligada pelos outros dois e a falha é informada pelo circuito de monitoração interno.

Quando utilizar dispositivos de segurança com contatos mecânicos (paradas de emergência, switches etc.), o usuário poderá aplicar sinais de teste de pulso para detectar falhas cruzadas. Para não usar saídas de segurança caras, vários CLPs de segurança oferecem saídas pulsantes específicas que podem ser conectadas aos dispositivos de contato mecânico.

Software

CLPs de segurança são programados de forma muito semelhante aos CLPs padrão. Todos os diagnósticos adicionais e verificações de erros mencionados anteriormente são feitos pelo sistema operacional, então não é necessário que o programador acompanhe o que está acontecendo. A maioria dos CLPs de segurança terá instruções especiais usadas para escrever o programa para o sistema de segurança e essas instruções tendem a mimetizar a função dos seus equivalentes de relés de segurança. Por exemplo, a instrução Parada de emergência opera de forma muito semelhante a um MSR 127. Embora a lógica por trás de cada uma dessas instruções seja complexa, os programas de segurança parecem relativamente simples, pois o programador simplesmente conecta os blocos. Essas instruções, juntamente com outras instruções lógicas, matemáticas, de manipulação de dados etc. são certificadas por um terceiro para assegurar que sua operação seja coerente com os padrões aplicáveis.

Blocos de funções são métodos predominantes para a programação de funções de segurança. Além dos Blocos de funções e da Lógica ladder, CLPs de segurança também oferecem instruções de aplicação de segurança certificadas. Instruções de segurança certificadas proporcionam um comportamento específico de aplicação. Esse exemplo exibe uma instrução de parada de emergência. Para realizar a mesma função em lógica ladder, seriam necessárias aproximadamente 16 linhas de lógica ladder. Como o comportamento da lógica é embutido na instrução da Parada de emergência, a lógica embutida não precisa ser testada.

Blocos de funções certificados estão disponíveis para interface com quase todos os dispositivos de segurança. Uma exceção a essa lista é o limite de segurança que usa tecnologia resistiva.

CLPs de segurança geram uma “assinatura” que proporciona a capacidade de rastrear possíveis mudanças realizadas. Essa assinatura é, em geral, uma combinação do programa, configuração de entrada/saída e um registro de data e hora. Quando o programa é finalizado e validado, o usuário deve registrar essa assinatura como parte dos resultados de validação para referência futura. Se o programa precisar de modificação, é necessário fazer a revalidação e uma nova assinatura deverá ser registrada. O programa também pode ser bloqueado com uma senha para evitar alterações não autorizadas.

A fiação é simplificada com sistemas de lógica programável comparáveis a relés de segurança de monitoração. Ao contrário da fiação para terminais específicos em relés de segurança de monitoração, dispositivos de entrada são conectados a quaisquer terminais de entrada e dispositivos de saída são conectados a quaisquer terminais de saída. Os terminais são atribuídos por meio de software.

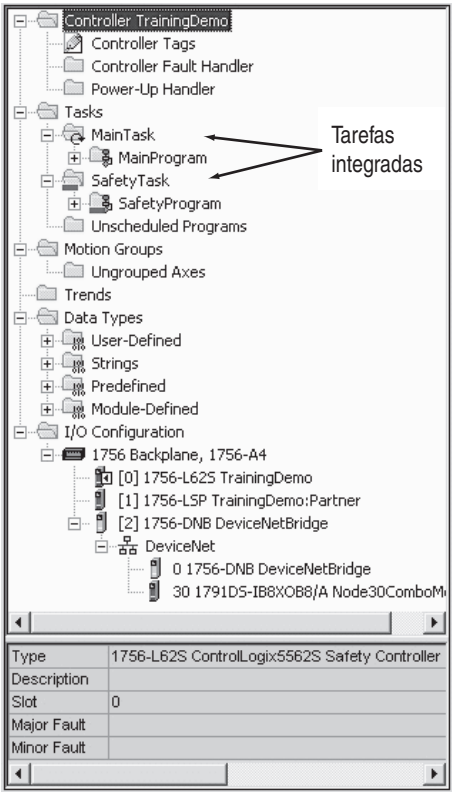
Controladores de segurança integrados

Soluções de controle de segurança agora oferecem integração completa com arquitetura de controle única, onde funções de controle padrão e de segurança residem e trabalham juntas. A capacidade de realizar movimento, acionamento, processo, lote, sequência em alta velocidade e segurança SIL 3 em um controlador proporciona vantagens significativas. A integração de controles padrão e de segurança oferece a oportunidade de usar ferramentas e tecnologias comuns que reduzem custos associados com o projeto, instalação, comissionamento e manutenção. A capacidade de utilizar hardware de controle comum, E/S de segurança distribuída ou dispositivos em redes de segurança e dispositivos IHM comuns reduz os custos de aquisição e manutenção, além de reduzir o tempo de desenvolvimento. Todos esses recursos melhoram a produtividade, a velocidade associada à resolução de problemas e reduzem custos de treinamento devido à simplicidade.

O diagrama a seguir exibe um exemplo da integração de controle e segurança. As funções de controle não relacionadas à segurança padrão residem na Tarefa principal. As funções relacionadas à segurança residem na Tarefa de segurança.

Medidas de proteção e equipamentos complementares

Todas as funções relacionadas ao padrão e segurança são isoladas entre si. Por exemplo, tags de segurança podem ser lidas diretamente pela lógica padrão. Tags de segurança podem ser trocadas entre controladores GuardLogix sobre EtherNet, ControlNet ou DeviceNet. Dados de tag de segurança podem ser lidos diretamente por dispositivos externos, Interfaces homem-máquina (IHM), computadores pessoais (PC) ou outros controladores.



1. Tags e lógica padrão comportam-se igualmente ao ControlLogix.

2. Dados padrão de tags, programa ou controlador no escopo e dispositivos externos, IHM, PCs, outros controladores etc.

3. Como controlador integrado, o GuardLogix proporciona a capacidade de mover (mapear) dados de tag padrão para tags de segurança para uso dentro da tarefa de segurança. Isso proporciona aos usuários a capacidade de ler informações de status a partir do lado padrão do GuardLogix. Esses dados não devem ser usados para controlar diretamente uma saída de segurança.

4. Tags de segurança podem ser lidas diretamente por lógica padrão.

5. Tags de segurança podem ser lidas ou escritas por lógica de segurança.

6. Tags de segurança podem ser trocadas entre controladores GuardLogix sobre EtherNet.

7. Dados de tags de segurança, programa ou controlador no escopo podem ser lidos por dispositivos externos, IHMs, PCs, outros controladores etc. Observe que após esses dados serem lidos, passam a ser considerados dados padrão, não dados de segurança.

Redes de segurança

Redes de comunicação de chão de fábrica tradicionalmente proporcionam aos fabricantes a capacidade de melhorar a flexibilidade, aumentar diagnósticos, aumentar a distância, reduzir custos de instalação e fiação, facilitar a realização de manutenções e melhorar em geral a produtividade de suas operações de fabricação. Essas mesmas motivações também conduzem a implementação de redes de segurança industrial. As redes de segurança permitem aos fabricantes distribuir E/S de segurança e dispositivos de segurança em redor das suas máquinas utilizando um único cabo de rede, reduzindo custos de instalação enquanto melhoram o diagnóstico e permitem o uso de sistemas de segurança de maior complexidade. Elas também permitem comunicações seguras entre controladores/CLPs de segurança, permitindo aos usuários distribuir seu controle de segurança entre vários sistemas inteligentes.

As redes de segurança não evitam a ocorrência de erros de comunicação. As redes de segurança são mais capazes de detectar erros de transmissão e, então, permitem que dispositivos de segurança tomem as medidas apropriadas. Erros de comunicação que são detectados incluem: inserção de mensagem, perda de mensagem, corrupção de mensagem, atraso de mensagem, repetição de mensagem e sequência incorreta de mensagem.

Para a maioria das aplicações, quando um erro é detectado, o dispositivo passará a um estado desenergizado conhecido, tipicamente chamado de “estado de segurança”. O dispositivo de entrada ou saída de segurança é responsável por detectar esses erros de comunicação e, então, passar ao estado seguro caso seja apropriado.

Redes de segurança iniciais foram vinculadas a um tipo de mídia específico ou esquema de acesso de mídia, então os fabricantes necessitaram utilizar cabos específicos, placas de interface de rede, roteadores, pontes etc. que também se tornaram parte da função de segurança. Essas redes foram limitadas no sentido de que apenas suportavam comunicação entre dispositivos de segurança. Isso significava que os fabricantes precisavam usar duas ou mais redes para sua estratégia de controle de máquina (uma rede para controle padrão e outra para controle relacionado à segurança), aumentando os custos de instalação, treinamento e de peças de reposição.

Redes de segurança modernas permitem que um único cabo de rede se comunique com dispositivos de controle de segurança e padrão. Segurança CIP (Common Industrial Protocol) é um protocolo padrão aberto publicado pela ODVA (Open DeviceNet Vendors Association) que permite comunicações de segurança entre dispositivos de segurança em redes DeviceNet, ControlNet e EtherNet/IP. Como a segurança CIP é uma extensão do protocolo CIP, dispositivos de segurança e dispositivos padrão podem residir na mesma rede. Os usuários também podem estabelecer pontes entre redes contendo dispositivos de segurança, permitindo que subdividam dispositivos para fazer o ajuste fino dos tempos de resposta de segurança ou simplesmente realizar a distribuição de dispositivos de segurança com mais facilidade. Como o protocolo

de segurança é de responsabilidade exclusiva dos dispositivos finais (CLP/controlador de segurança, módulo de E/S de segurança, componente de segurança), cabos padrão, placas de interface de rede, pontes e roteadores são usados, eliminando qualquer hardware de rede especial e removendo esses dispositivos da função de segurança.

Dispositivos de saída

Relés de controle de segurança e contatores de segurança

Relés de controle e contatores são usados para remover energia do atuador. Recursos especiais são adicionados a relés de controle e contatores para proporcionar a classificação de segurança.

Contatos normalmente fechados e vinculados mecanicamente são usados para realimentar o status dos relés de controle e os contatores para o dispositivo lógico. O uso de contatos vinculados mecanicamente ajuda a assegurar a função de segurança. Para atender às exigências de contatos mecanicamente vinculados, os contatos normalmente abertos e normalmente fechados não podem estar em estado fechado ao mesmo tempo. O IEC 60947-5-1 define as exigências para contatos vinculados mecanicamente. Se for necessário soldar os contatos normalmente abertos, os contatos normalmente fechados permanecerão abertos em no mínimo 0,5 mm. De modo contrário, se for necessário soldar os contatos normalmente fechados, os contatos normalmente abertos permanecerão abertos.

Os sistemas de segurança somente devem ser iniciados em locais específicos. Relés de controle com classificação padrão e contatores permitem que a armadura seja pressionada para fechar os contatos normalmente abertos. Em dispositivos classificados de segurança, a armadura é protegida contra sobreposição manual para reduzir a inicialização inesperada.

Em relés de controle de segurança, o contato normalmente fechado é acionado pela chave principal. Contatores de segurança utilizam um bloco somador para localizar os contatos vinculados mecanicamente. Caso o bloco de contatos caia fora da base, os contatos vinculados mecanicamente permanecerão fechados. Os contatos vinculados mecanicamente são fixados permanentemente ao relé de controle de segurança ou contator de segurança. Nos contatores maiores, um bloco somador é insuficiente para refletir com precisão o status da chave maior. Contatos espelhados, exibidos na Figura 4.81 estão localizados no lado do contator que estiver sendo utilizado.

O tempo de desenergização de relés de controle ou contatores desempenha uma função no cálculo de distância de segurança. Em geral, um supressor de transiente é colocado em toda a bobina para melhorar a vida útil dos contatos que acionam a bobina. Para bobinas energizadas por CA, o tempo de desenergização não é afetado. Para bobinas energizadas por CC, o tempo de desenergização é aumentado. O aumento depende do tipo de supressão selecionada.

Relés de controle e contatores são projetados para comutar grandes cargas, de 0,5 A a mais de 100 A. O sistema de segurança opera em baixas correntes. O sinal de retorno gerado pelo dispositivo lógico do sistema de segurança pode estar na ordem de poucos miliamperes para dezenas de miliamperes, geralmente em 24 Vcc. Os relés de controle de segurança e os contatores de segurança usam contatos bifurcados revestidos com ouro para comutar essa pequena corrente de forma confiável.

Proteção contra sobrecarga

A proteção contra sobrecarga para motores é exigida por padrões elétricos. O diagnóstico fornecido pela proteção contra sobrecarga melhora não somente a segurança do equipamento, como também a segurança do operador. Tecnologias disponíveis atualmente podem detectar condições de falha como sobrecarga, perda de fase, falha de aterramento, obstrução, travamento, carga baixa, desequilíbrio de corrente e excesso de temperatura. Detectar e comunicar condições anormais antes da ocorrência do problema ajuda a melhorar o tempo de produção e ajuda a evitar que os operadores e o pessoal de manutenção enfrentem condições perigosas imprevistas.

Inversores e Servos

Inversores e servos classificados de segurança podem ser usados para evitar que a energia rotacional seja fornecida para alcançar uma parada de segurança e uma parada de emergência.

Inversores CA atingem a classificação de segurança com canais redundantes para remover energia para os circuitos de controle da porta. Um canal é o canal Ativar, um sinal de hardware que remove o sinal de entrada para os circuitos de controle da porta. O segundo canal é um relé guiado positivo que remove a alimentação de energia dos circuitos de controle da Porta. O relé guiado positivo também proporciona um sinal de status de volta ao sistema lógico. Essa abordagem redundante permite que o inversor classificado de segurança seja aplicado em circuitos de parada de emergência sem a necessidade de um contator.

O Servo atinge um resultado de forma similar aos inversores CA utilizando sinais de segurança redundantes usados para alcançar a função de segurança. Um sinal interrompe o inversor para os Circuitos de controle da porta. Um segundo sinal interrompe a alimentação para a fonte de alimentação dos circuitos de controle da porta. Dois relés guiados positivos são usados para remover os sinais e oferecer retorno ao dispositivos lógico de segurança.

Sistemas de conexão

Sistemas de conexão acrescentam valor ao reduzir custos de instalação e manutenção de sistemas de segurança. Os projetos devem considerar canal único, canal duplo, canal duplo com indicação e múltiplos tipos de dispositivos.

Quando uma conexão em série de intertravamentos de canal duplo é necessária, um bloco de distribuição pode simplificar a instalação. Com uma classificação IP67, esses tipos de caixas podem ser montadas na máquina em locais remotos. Quando um conjunto diverso de dispositivos é necessário, uma caixa de E/S ArmorBlock Guard pode ser usada. As entradas podem ser configuradas por software para acomodar vários tipos de dispositivos.

Cálculo de distância de segurança

Os perigos devem chegar a um estado seguro antes que o operador alcance o perigo. Para o cálculo de distância de segurança, há dois grupos de padrões que proliferaram. Nesse capítulo, esses padrões são agrupados como a seguir:

ISO EN: (ISO 13855 e EN 999)

CAN EUA (ANSI B11.19, ANSI RIA R15.06 e CAN/CSA Z434-03)

Fórmula

A distância de segurança mínima é dependente do tempo necessário para processar o comando de Parada e a distância que o operador pode penetrar na zona de detecção antes da detecção. A fórmula usada em todo o mundo tem a mesma forma e exigências. As diferenças são os símbolos usados para representar as variáveis e as unidades de medida.

As fórmulas são:

ISO EN: $S = K \times T + C$

CAN EUA: $Ds = K \times (Ts + Tc + Tr + Tbm) + Dpf$

Onde: Ds e S são a distância segura mínima da zona de perigo para o ponto de detecção mais próximo

Orientações de abordagem

Quando o cálculo de distância de segurança é considerado onde uma cortina de luz ou scanner de área é usado, a abordagem para o dispositivo de detecção deve ser levada em consideração. Três tipos de abordagem são consideradas:

Normal – uma abordagem perpendicular ao plano de detecção

Horizontal – uma abordagem paralela ao plano de detecção

Em ângulo – uma abordagem em ângulo à zona de detecção.

Constante de velocidade

K é uma constante de velocidade. O valor da constante de velocidade depende dos movimentos do operador (por ex.: velocidades das mãos, velocidades de caminhada

e comprimentos de passos largos). Esse parâmetro é baseado em dados de pesquisa demonstrando que é razoável assumir uma velocidade de mãos de 1600 mm/seg. (63 pol./s) de um operador enquanto o corpo estiver parado. As circunstâncias da aplicação real devem ser levadas em consideração. Como diretriz geral, a velocidade de abordagem variará de 1600 mm/s (63 pol./s) a 2500 mm/seg. (100 pol/s). A constante de velocidade apropriada deve ser determinada pela avaliação de risco.

Tempo de parada

T é o tempo de parada geral do sistema. O tempo total, em segundos, começa do início do sinal de parada até a eliminação do perigo. Esse tempo pode ser dividido em suas partes incrementais (Ts, Tc, Tr e Tbm) para uma análise mais fácil. Ts é o pior tempo de parada da máquina/equipamento. Tc é o pior tempo de parada do sistema de controle. Tr é o tempo de resposta do dispositivo de segurança, incluindo sua interface. Tbm é o tempo de parada adicional permitido pelo monitor de frenagem antes de detectar deterioração de tempo de parada além dos limites pré-determinados dos usuários finais. Tbm é usado com prensas mecânicas de revolução de peça. Ts + Tc + Tr geralmente são medidos por um dispositivo de medição de tempo de parada caso os valores sejam desconhecidos.

Fatores de penetração de profundidade

Os fatores de penetração de profundidade são representados pelos símbolos C e Dpf. É o percurso máximo em direção ao perigo antes da detecção pelo dispositivo de segurança. Os fatores de penetração de profundidade mudarão dependendo do tipo de dispositivo e aplicação. Um padrão apropriado deve ser verificado para determinar o melhor fator de penetração de profundidade. Para uma abordagem normal a uma cortina de luz ou scanner de área, cuja sensibilidade de objeto é inferior a 64 mm (2,5 pol.), os padrões ANSI e canadenses usam:

Dpf = 3,4 x (Sensibilidade do objeto – 6,875 mm), mas não menos que zero.

Para uma abordagem a uma cortina de luz ou scanner de área, cuja sensibilidade de objeto é inferior a 40 mm (1,57 pol.), os padrões ISO e EN usam:

C = 8 x (Sensibilidade do objeto – 14 mm), mas não menos que 0.

Essas duas fórmulas tem um ponto de cruzamento em 19,3 mm. Para uma sensibilidade de objeto inferior a 19 mm, a abordagem CAN EUA é mais restritiva, pois a cortina de luz ou scanner de área deve ser definido novamente para longe do perigo. Para sensibilidades de objeto superiores a 19,3 mm, o padrão ISO EN é mais restritivo. Fabricantes de máquinas, que desejam construir uma máquina para uso em todo o mundo, devem obter as piores condições de caso a partir das duas equações.

Aplicações de contato

Quando sensibilidades maiores de objeto são utilizadas, os padrões CAN EUA e ISO EN diferem ligeiramente no fator de penetração de profundidade e na sensibilidade do objeto. O valor do ISO EN é de 850 mm, enquanto o valor do CAN EUA é de 900 mm. Os padrões também diferem na sensibilidade do objeto. Enquanto o padrão ISO EN permite de 40 a 70 mm, o padrão CAN EUA permite até 600 mm.

Aplicações de alcance superior

Ambos os padrões concordam que a altura mínima do menor feixe deve ser de 300 mm, mas diferem com relação à altura mínima do feixe mais alto. O ISO EN determina 900 mm, enquanto o CAN EUA determina 1200 mm. O valor para o maior feixe parece ser questionável. Quando isso é considerado como uma aplicação de contato, a altura do maior feixe deverá ser muito maior para acomodar um operador em posição em pé. Caso o operador consiga alcançar o plano de detecção, então os critérios de alcance superior são aplicados.

Feixes únicos ou múltiplos

Feixes únicos ou múltiplos são definidos mais adiante pelos padrões ISO EN. Os números abaixo exibem as alturas “práticas” de múltiplos feixes acima do piso. A penetração de profundidade é de 850 mm para a maioria dos casos e 1200 mm para o uso de feixe único. Em comparação, a abordagem CAN EUA leva isso em consideração por meio das exigências de Contato. Ficar sobre, embaixo ou em redor de feixes únicos e múltiplos sempre deve ser considerado.

# Feixes	Altura acima do nível do piso - mm (pol.)	C - mm (pol.)
1	750 (29,5)	1200 (47,2)
2	400 (5,7), 900 (35,4)	850 (33,4)
3	300 (11,8), 700 (27,5), 1100 (43,3)	850 (33,4)
4	300 (11,8), 600 (23,6), 900 (35,4), 1200 (47,2)	850 (33,4)

Cálculos de distância

Para a abordagem normal a cortinas de luz, o cálculo de distância de segurança para ISO EN e para CAN EUA são próximos, no entanto, há diferenças. Para a abordagem normal às cortinas de luz verticais onde a sensibilidade do objeto é um máximo de 40 m, a abordagem ISO EN exige duas etapas. Em primeiro lugar, calcule S usando 2000 para a constante de velocidade.

S = 2000 x T + 8 x (d -1 4)

A distância mínima que S pode ser é de 100 mm.

Uma segunda etapa pode ser usada quando a distância é superior a 500 mm. Então, o valor de K pode ser reduzido a 1600. Quando usar K=1600, o valor mínimo de S é de 500 mm.

A abordagem CAN EUA usa uma abordagem de uma etapa: Ds = 1600 x T * Dpf

Isso leva a diferenças superiores a 5% entre os padrões, quando o tempo de resposta é inferior a 560 ms.

Abordagens em ângulo

A maioria das aplicações de cortinas de luz e scanners são montadas na posição vertical (abordagem normal) ou horizontal (abordagem paralela). Essas montagens não são consideradas em ângulo se estiverem dentro de ±5° do projeto pretendido. Quando o ângulo excede ±5°, os riscos potenciais (por ex.: distância mais curta) de abordagens previsíveis devem ser levados em consideração. Em geral, ângulos superiores a 30° a partir do plano de referência (por ex.: piso) devem ser considerados normais e aqueles inferiores a 30 considerados paralelos.

Tapetes de segurança

Com tapetes de segurança, a distância de segurança deve considerar o ritmo e o passo largo dos operadores. Presumindo que o operador esteja caminhando e que os tapetes de segurança estejam montados no piso. O primeiro passo do operador no tapete é um fator de penetração de profundidade de 1200 mm ou 48 pol. Caso o operador necessite pisar sobre uma plataforma, então o fator de penetração de profundidade pode ser reduzido por um fator de 40% da altura do passo.

Exemplo

Exemplo: Um operador usa uma abordagem normal para uma cortina de luz de 14 mm, que é conectada a um relé de segurança de monitoração, conectado a um contator alimentado por CC com supressor de diodo. O tempo de resposta do sistema de segurança, Tr, é 20 + 15 + 95 = 130 ms. O tempo de parada da máquina, Ts+Tc, é 170 ms. Um monitor de frenagem não é usado. O valor de Dpf é de 1 polegada e o valor de C é zero. O cálculo seria como a seguir

Dpf = 3,4 (14 - 6,875) = 1 pol. (24,2 mm)

Ds = K x (Ts + Tc + Tr + Tbm) + Dpf
Ds = 63 x (0,17 + 0,13 + 0) + 1
Ds = 63 x (0,3) + 1
Ds = 18,9 + 1
Ds = 19,9 pol. (505 mm)

C = 8 (14-14) = 0

S = K x T + C
S = 1600 x (0,3) + 0
S = 480 mm (18,9 pol.)

Portanto, a distância de segurança mínima em que a cortina de luz de segurança deve ser montada do perigo é de 20 polegadas ou 508 mm, para uma máquina a ser usada em qualquer lugar no mundo.

Prevenção de energização inesperada

A prevenção de energização inesperada é abordada por vários padrões. Exemplos incluem ISO14118, EN1037, ISO12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05 e AS 4024.1603. Esses padrões têm um tema em comum: o método primário de prevenção de energização inesperada é remover a energia do sistema e travar o sistema no estado desligado. A finalidade é permitir que as pessoas entrem com segurança em áreas de perigo da máquina.

Trava / Etiqueta

Novas máquinas devem ser construídas com dispositivos de isolamento de energia travável. Os dispositivos se aplicam a todos os tipos de energia, incluindo elétrica, hidráulica, pneumática, gravidade e lasers. Travamento refere-se à aplicação de uma trava em um dispositivo de isolamento de energia. A trava somente deve ser removida por seu proprietário ou por um supervisor sob condições controladas. Quando for necessário que vários indivíduos trabalhem na máquina, cada um deve aplicar suas travas aos dispositivos de isolamento de energia. Cada trava deve ser identificável pelo seu proprietário.

Nos EUA, a etiquetagem é uma alternativa ao travamento para máquinas mais antigas, onde um dispositivo de travamento nunca foi instalado. Nesse caso, a máquina é desligada e uma etiqueta é aplicada para avisar ao pessoal que não devem acionar a máquina enquanto o porta-etiquetas estiver na máquina. Com início em 1990, as máquinas que eram modificadas deviam ser atualizadas para incluir um dispositivo de isolamento de energia travável.

Um dispositivo de isolamento de energia é um dispositivo mecânico que evita fisicamente a transmissão ou liberação de energia. Esses dispositivos podem assumir a forma de um disjuntor, uma chave seccionadora, uma chave operada manualmente, uma combinação de plugue/soquete ou uma válvula operada manualmente. Dispositivos de isolamento elétrico devem comutar todos os condutores de alimentação não aterrados e nenhum polo poderá operar de forma independente.

A finalidade da trava e etiqueta é evitar o acionamento inesperado da máquina. Um acionamento inesperado pode ser o resultado de várias causas: uma falha do sistema de controle; uma ação inapropriada em um controle de acionamento, sensor, contator ou válvula; uma restauração de alimentação após interrupção; ou outro tipo de influência interna ou externa. Após a conclusão do processo de travamento ou etiquetagem, a dissipação da energia deve ser verificada.

Sistemas de isolamento de segurança

Sistemas de isolamento de segurança executam um desligamento ordenado de uma máquina e também oferecem um método simples de bloquear a alimentação para uma máquina. Essa abordagem funciona bem para máquinas maiores e sistemas de fabricação, especialmente quando múltiplas fontes de energia são localizadas em um nível de mezanino ou em locais distantes.

Desconexões de carga

Para o isolamento local de dispositivos elétricos, chaves podem ser colocadas antes do dispositivo que precisa ser isolado e bloqueado. As chaves de carga do cód. cat. 194E são um exemplo de produto capaz de realizar o isolamento e o bloqueio.

Sistemas de chave com segredo

Sistemas de chave com segredo são outro método para a implementação de um sistema de bloqueio. Vários sistemas de chave com segredo iniciam com um dispositivo isolador de energia. Quando a chave é desligada pela chave “primária”, a energia elétrica para a máquina é removida de todos os condutores de alimentação não aterrados de forma simultânea. A chave primária pode, então, ser removida e levada a um local onde o acesso à máquina é necessário. Vários componentes podem ser adicionados para acomodar arranjos de travamento mais complexos.

Medidas alternativas ao travamento

A trava e a etiqueta devem ser usadas durante a realização de manutenções nas máquinas. Intervenções na máquina durante operações de produção normais são abrangidas pela segurança. A diferença entre manutenções e operações normais de produção nem sempre é clara.

Alguns ajustes secundários e tarefas de manutenção, que ocorrem durante operações normais de produção, não têm necessidade de travamento da máquina. Os exemplos incluem o carregamento e descarregamento de materiais, mudanças e ajustes secundários de ferramentas, níveis de lubrificação de manutenções e remoção de refugos. Essas tarefas devem ser rotineiras, repetitivas e integrais para uso do equipamento para produção e o trabalho é realizado utilizando medidas alternativas, como a segurança, que proporcionam proteção efetiva. A segurança inclui dispositivos como proteções de intertravamento, cortinas de luz e tapetes de segurança. Usados com dispositivos apropriados lógicos e de saída classificados como de segurança, os operadores podem acessar zonas de perigo da máquina com segurança durante tarefas normais de produção e manutenções secundárias.

Sistemas de controle relacionados à segurança

Introdução

O que é um sistema de controle relacionado à segurança (em geral abreviado como SRCS)? É parte do sistema de controle de uma máquina que evita a ocorrência de condições perigosas. Ele pode ser um sistema dedicado separado ou pode ser integrado ao sistema de controle normal da máquina.

Sua complexidade variará de um sistema simples, como chave de intertravamento de porta de proteção conectado em série para a bobina de controle do contator de potência, para um sistema composto envolvendo dispositivos simples e complexos comunicando por meio de software e hardware.

Sistemas de controle relacionados são projetados para desempenhar funções de segurança. O SRCS deve continuar a operar corretamente em todas as condições previsíveis. Então, o que é uma função de segurança? Como projetamos um sistema para conseguir isso? E quando conseguirmos isso, como demonstramos?

Função de segurança

Uma função de segurança é implementada pelas peças relacionadas à segurança do sistema de controle da máquina para alcançar ou manter o equipamento sob controle em um estado seguro com relação a um perigo específico. Uma falha da função de segurança pode resultar em um aumento imediato dos riscos de usar o equipamento, ou seja, uma condição perigosa.

Uma máquina deve ter no mínimo um “perigo”, caso contrário, não é uma máquina. Uma “condição perigosa” é quando uma pessoa é exposta a um perigo. Uma condição perigosa não significa que a pessoa será ferida. A pessoa exposta pode ser capaz de reconhecer o perigo e evitar ferimentos. A pessoa exposta pode não ser capaz de reconhecer o perigo ou o perigo pode ser iniciado por uma ativação inesperada. A tarefa principal do projetista do sistema de segurança é evitar condições perigosas e evitar a ativação inesperada.

A função de segurança pode, em geral, ser descrita com exigências de múltiplas peças. Por exemplo, a função de segurança iniciada por uma proteção de intertravamento tem três peças:

1. as funções perigosas protegidas pela proteção não conseguem operar até que a proteção esteja fechada;

2. a abertura da proteção fará com que a função perigosa seja interrompida caso esteja operando no momento da abertura; e

3. o fechamento da proteção não reinicia a função perigosa protegida pela proteção.

Quando iniciar a função de segurança para uma aplicação específica, a palavra "perigo" deverá ser substituída pelo perigo específico. O perigo não deve ser confundido com os resultados do perigo. Esmagamento, cortes e queimaduras são resultados de um perigo. Um exemplo de perigo é um motor, bate-estacas, faca, tocha, bomba, laser, robô, atuador duplo, solenoide, válvula, outro tipo de atuador ou um perigo mecânico que envolve gravidade.

Na discussão de sistemas de segurança, a frase "em ou antes que uma demanda seja colocada na função de segurança" é usada. O que é uma demanda na função de segurança? Exemplos de demandas colocadas na função de segurança são a abertura de uma proteção intertravada, o rompimento de uma cortina de luz, pisar sobre um tapete de segurança ou pressionar um botão de parada de emergência. Um operador está solicitando que o perigo pare ou permaneça desenergizado caso já tenha sido interrompido.

As peças relacionadas à segurança do sistema de controle da máquina executam a função de segurança. A função de segurança não é executada por um único dispositivo, por exemplo, apenas pela proteção. O intertravamento na proteção envia um comando a um dispositivo lógico, que por sua vez, desativa um atuador. A função de segurança inicia com o comando e termina com a implementação.

O sistema de segurança deve ser atribuído com um nível de integridade proporcional aos riscos da máquina. Altos riscos exigem maiores níveis de integridade para assegurar o desempenho da função de segurança. Sistemas de segurança de máquina podem ser classificados em níveis de desempenho da sua capacidade de assegurar o desempenho da sua função de segurança ou, em outras palavras, seu nível de integridade de segurança funcional.

Segurança funcional de sistemas de controle

Importante: *Os padrões e exigências considerados nessa seção são relativamente novos. Trabalhos ainda estão sendo realizados pelos grupos de projeto em alguns aspectos, especialmente com relação a esclarecimento e combinação de alguns desses padrões. Portanto, é possível que ocorram algumas mudanças em alguns dos detalhes fornecidos nessas páginas. Para a informação mais recente, consulte: http://www.ab.com/safety.*

O que é segurança funcional?

Segurança funcional é a parte da segurança geral que depende do funcionamento correto do processo ou equipamento em resposta às suas entradas. O IEC TR 61508-0 oferece o seguinte exemplo para ajudar a esclarecer o significado de segurança funcional. "Por exemplo, um dispositivo de proteção contra excesso de temperatura, usando um sensor térmico nos enrolamentos de um motor elétrico

para desenergizar o motor antes de superaquecer, é um elemento de segurança funcional. No entanto, fornecer isolamento especializado para suportar altas temperaturas não é um elemento de segurança funcional (embora ainda seja um elemento de segurança e possa proteger exatamente contra o mesmo perigo)". Como outro exemplo, compare uma proteção rígida a uma proteção de intertravamento. A proteção rígida não é considerada "segurança funcional", embora seja capaz de proteger contra acesso ao mesmo perigo protegido pela porta intertravada. A porta intertravada é um elemento de segurança funcional. Quando a proteção é aberta, a intertrava serve como "entrada" para um sistema que alcança um estado seguro. Igualmente, equipamentos de proteção individual (EPI) são usados como medida de proteção para ajudar a aumentar a segurança do pessoal. EPI não é considerado segurança funcional.

Segurança funcional foi um termo introduzido no IEC 61508:1998. Desde então, o termo ocasionalmente é associado apenas a sistemas de segurança programáveis. Isso é um conceito equivocado. A segurança funcional abrange uma ampla gama de dispositivos usados para criar sistemas de segurança. Dispositivos como intertravas, cortinas de luz, relés de segurança, CLPs de segurança, contatores de segurança e inversores de segurança são interconectados para formar um sistema de segurança, que realiza uma função específica relacionada à segurança. Isso é segurança funcional. No entanto, a segurança funcional de um sistema de controle elétrico é altamente relevante para o controle de perigos que surgem de peças móveis de máquinas.

Dois tipos de exigências são necessárias para alcançar segurança funcional:

- a função de segurança e
- a integridade de segurança.

A avaliação de riscos desempenha um papel fundamental no desenvolvimento de exigências de segurança funcional. A análise de tarefas e perigos leva às exigências de função para segurança (ou seja, a função de segurança). A quantificação de riscos produz exigências de integridade de segurança (ou seja, a integridade de segurança ou nível de desempenho).

Quatro dos principais padrões de segurança funcional de sistemas de controles para máquinas são:

1. **IEC/EN 61508** "Segurança funcional de segurança relacionada a sistemas de controle elétricos, eletrônicos e eletrônicos programáveis"

   Esse padrão contém as exigências e disposições aplicáveis ao projeto de sistemas e subsistemas complexos eletrônicos e programáveis. O padrão é genérico, então não é restrito ao setor de máquinas.

2. **IEC/EN 62061** “Segurança de máquinas - Segurança funcional de sistemas de controle elétricos, eletrônicos e eletrônicos programáveis”

   Esse padrão é a implementação específica de máquinas de IEC/EN 61508. Ele fornece exigências aplicáveis ao projeto de nível de sistema de todos os tipos de sistemas de controle elétrico relacionados às maquinas e também para o projeto de subsistemas ou dispositivos não complexos. Ele exige que subsistemas complexos ou programáveis satisfaçam o IEC/EN 61508.

3. **EN ISO 13849-1:2008** “Segurança de máquina – Peças relacionadas à segurança de sistemas de controle”

   Esse padrão tem o propósito de oferecer um caminho de transição direta das categorias do EN 954-1 anterior.

4. **IEC 61511** “Segurança funcional — Sistemas instrumentados de segurança para o setor industrial de processamento”

   Esse padrão é a implementação específica do setor de processamento do IEC/EN 61508.

Os padrões de segurança funcional representam uma etapa significativa além das exigências familiares existentes, como controle confiável e sistema de categorias do ISO 13849-1:1999 (EN 954-1:1996) anterior.

As categorias não desaparecerão completamente; elas também são usadas no EN ISO 13849-1 atual, que usa o conceito de segurança funcional e introduziu nova terminologia e exigências. Tem adições e diferenças significativas em relação ao antigo EN 954-1 (ISO 13849-1:1999). Nessa seção nos referiremos à versão atual como EN ISO 13849-1. (EN ISO 13849-1:2008 tem o mesmo texto do ISO 13849-1:2006).

IEC/EN 62061 e EN ISO 13849-1:2008

IEC/EN 62061 e EN ISO 13849-1, ambos abrangem sistemas de controle elétrico relacionados à segurança. Pretende-se que no final das contas eles sejam combinados em um padrão com terminologia comum. Ambos os padrões produzem os mesmos resultados, porém, usam métodos diferentes. Eles pretendem proporcionar aos usuários uma opção para escolher a mais adequada para sua situação. Um usuário pode escolher usar qualquer um dos padrões e ambos são harmonizados sob a Diretiva Europeia sobre Máquinas.

Os produtos de ambos os padrões são níveis comparáveis de desempenho ou integridade de segurança. As metodologias de cada padrão têm diferenças apropriadas para seu público-alvo.

A metodologia em IEC/EN 62061 tem o propósito de permitir funcionalidades de segurança mais complexas, que podem ser implementadas por arquiteturas de sistema anteriormente não convencionais. A metodologia do EN ISO 13849-1 tem o propósito de proporcionar uma rota mais direta e menos complicada para funcionalidades de segurança mais convencionais implementadas por arquiteturas de sistema convencionais.

Uma diferença importante entre esses dois padrões é a aplicabilidade a várias tecnologias. O IEC/EN 62061 é limitado a sistemas elétricos. O EN ISO 13849-1 pode ser aplicado a sistemas pneumáticos, hidráulicos, mecânicos e elétricos.

Relatório técnico conjunto sobre o IEC/EN 62061 e EN ISO 13849-1

Um relatório conjunto foi preparado dentro do IEC e ISO para ajudar os usuários de ambos os padrões.

Ele explica o relacionamento entre os dois padrões e explica como a equivalência pode ser obtida entre PL (Nível de Desempenho) do EN ISO 13849-1 e SIL (Nível de Integridade de Segurança) do IEC.EN 62061, ambos no nível de sistema e subsistema.

Para demonstrar que ambos os padrões fornecem resultados equivalentes, o relatório exibe um sistema de segurança como exemplo, calculado de acordo com as metodologias de ambos os padrões. O relatório também esclarece uma diversidade de problemas sujeitos a diferentes interpretações. Talvez um dos problemas mais significativos seja o aspecto de exclusão de falha.

Em geral, quando PLe se faz necessário para a função de segurança ser implementada por um sistema de controle de segurança, não é normal depender somente de exclusões de falhas para atingir esse nível de desempenho. Isso depende da tecnologia usada e do ambiente operacional pretendido. Portanto, é essencial que o projetista tome cuidado adicional com o uso de exclusões de falhas à medida que a exigência de PL aumenta.

Em geral, o uso de exclusões de falhas não é aplicável a aspectos mecânicos da chaves de posição eletromecânicas e chaves operadas manualmente (por ex.: um dispositivo de parada de emergência) para alcançar PLe no projeto de um sistema de controle relacionado à segurança. Essas exclusões de falha que podem ser aplicadas a condições específicas de falha mecânica (por ex.: desgaste/corrosão, fratura) são descritas na Tabela A.4 do ISO 13849-2.

Por exemplo, um sistema de intertravamento de porta que deve alcançar PLe precisará incorporar uma tolerância mínima a falhas de 1 (por ex.: duas chaves de posição mecânicas convencionais) para alcançar esse nível de desempenho desde que não seja normalmente justificável excluir falhas como atuadores de chave danificados. No entanto, pode ser aceitável excluir falhas, como curto-circuito de fiação dentro de um painel de controle designado de acordo com os padrões relevantes.

SIL e IEC/EN 62061

O IEC/EN 62061 descreve a quantidade de risco a ser reduzido e a capacidade de um sistema de controle de reduzir esse risco em termos de SIL (Nível de Integridade de Segurança). Há três SILs usados no setor de máquinas, o SIL 1 é o menor e o SIL 3 é o maior.

Como o termo SIL é aplicado do mesmo modo em outros setores industriais, como o petroquímico, geração de energia e ferrovias, o IEC/EN 62061 é bastante útil quando a máquina é usada nesses setores. Riscos de maior magnitude podem ocorrer em outros setores, como a indústria de processamento e, por esse motivo, o IEC 61508 e o padrão específico do setor de processamento IEC 61511 incluem SIL 4.

Um SIL aplica-se a uma função de segurança. Os subsistemas que formam o sistema que implementa a função de segurança deve ter um recurso de SIL apropriado. Isso é ocasionalmente chamado de Limite de Reivindicação de SIL (SIL CL). Um estudo detalhado e completo do IEC/EN 62061 é necessário antes de ser possível aplicá-lo corretamente.

PL e EN ISO 13849-1:2008

O EN ISO 13849-1:2008 não usará o termo SIL; em vez disso, usará o termo PL (Nível de Desempenho). Em vários aspectos o PL pode ser relacionado ao SIL. Há cinco níveis de desempenho, PLa é o menor e PLe é o maior.

Comparação de PL e SIL

Essa tabela exibe o relacionamento aproximado entre PL e SIL quando aplicados a estruturas típicas de circuito.

PL (Nível de desempenho)	PFH_D (Probabilidade de falhas perigosas por hora)	SIL (Nível de integridade de segurança)
a	$\geq 10^{-5}$ a $<10^{-4}$	Nenhum
b	$\geq 3 \times 10^{-6}$ a $<10^{-5}$	1
c	$\geq 10^{-6}$ a $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ a $<10^{-6}$	2
e	$\geq 10^{-8}$ a $<10^{-7}$	3

Correspondência aproximada entre PL e SIL

IMPORTANTE: *A tabela exibida acima é apenas para orientação geral e NÃO deve ser usada para fins de conversão. As exigências completas dos padrões devem ser referenciadas.*

Projeto de sistema de acordo com o EN ISO 13849 e SISTEMA

Um estudo completo e detalhado do EN ISO 13849-1:2008 é necessário antes de poder ser aplicado corretamente. O seguinte é uma breve visão geral:

Esse padrão oferece as exigências para o projeto e integração de peças relacionadas à segurança de sistemas de controle, incluindo alguns aspectos de software. O padrão se aplica a um sistema relacionado à segurança, porém também pode ser aplicado às peças de componentes do sistema.

Software SISTEMA, Ferramenta de cálculo de PL

SISTEMA é uma ferramenta de software para a implementação do EN ISO 13849-1. Seu uso simplificará consideravelmente a implementação do padrão.

SISTEMA significa "Safety Integrity Software Tool for the Evaluation of Machine Applications" (Ferramenta de Software de Integridade de Seguranca para a Avaliação de Aplicações de Máquinas). Foi desenvolvido pela BGIA, na Alemanha, e seu uso é gratuito. Ele necessita da entrada de vários tipos de dados de segurança funcional, como descrito adiante nesta seção.

Os dados podem ser inseridos manualmente ou automaticamente utilizando uma Biblioteca de dados SISTEMA do fabricante.

A Biblioteca de dados SISTEMA da Rockwell Automation está disponível para fazer download, juntamente com um link para o site de download do SISTEMA, em: *www.discoverrockwellautomation.com/safety*

Visão geral do EN ISO 13849-1

Esse padrão tem ampla aplicabilidade, pois é aplicável a todas as tecnologias, incluindo elétrica, hidráulica, pneumática e mecânica. Embora o ISO 13849-1 seja aplicável a sistemas complexos, ele também encaminha o leitor ao IEC 62061 e IEC 61508 para sistemas embutidos de software complexos.

Vamos dar uma olhada nas diferenças básicas entre o antigo EN 954-1 e o novo EN ISO 13849-1. As saídas do padrão antigo eram Categorias [B, 1, 2, 3 ou 4]. As saídas do novo padrão são Níveis de Desempenho [PL a, b, c, d ou e]. O conceito de categoria é mantido, porém, há exigências adicionais a serem satisfeitas antes que um PL possa ser reivindicado para um sistema.

As exigências podem ser listadas em formulário básico, como a seguir:

- A arquitetura do sistema. Essencialmente, isso captura o que usamos como categorias.
- Dados de confiabilidade são necessários para as partes constituintes do sistema.
- A Cobertura de Diagnóstico [DC] do sistema é necessária. Isso efetivamente representa a quantidade de monitoração de falha no sistema.
- Proteção contra falha de causa comum.
- Proteção contra falhas sistemáticas.
- Onde relevante, exigências específicas para software.

Mais tarde, nós examinaremos esses fatores de forma detalhada, porém, antes de fazermos isso, será importante considerar o propósito básico e o princípio do todo o padrão. É evidente nesse estágio que há novas coisas a aprender, no entanto, os detalhes farão mais sentido após entendermos o que atingir e por quê.

Em primeiro lugar, por que precisamos do novo padrão? É óbvio que a tecnologia usada nos sistemas de segurança de máquinas evoluiu e mudou consideravelmente ao longo dos últimos dez anos. Até recentemente, sistemas de segurança dependiam de equipamentos “simples” com modos de falha bastante previsíveis. Mais recentemente, observamos um crescente uso de dispositivos eletrônicos e programáveis mais complexos em sistemas de segurança. Isso nos proporcionou vantagens em termos de custo, flexibilidade e compatibilidade, porém, também significou que os padrões pré-existentes não sejam mais adequados. Para saber se um sistema de segurança é bom o suficiente, precisamos saber mais sobre ele. É por isso que o novo padrão solicita mais informações. À medida que os sistemas de segurança começam a usar uma abordagem mais semelhante a uma “caixa preta” nós começamos a depender mais de sua conformidade com os padrões. Portanto, esses padrões devem ser capazes de questionar adequadamente a tecnologia. Para cumprir essa tarefa, eles devem abordar os fatores básicos de confiabilidade, detecção de falhas, integridade arquitetônica e sistemática. Essa é a intenção do EN ISO 13849-1.

Para delinear um curso lógico através do padrão, dois tipos de usuários fundamentalmente diferentes devem ser considerados: o projetista de subsistemas relacionados à segurança e os projetistas de sistemas relacionados à segurança. Em geral, o projetista de subsistemas [tipicamente um fabricante de componentes de segurança] estará sujeito a um nível mais elevado de complexidade. Eles precisarão fornecer os dados exigidos para que o projetista do sistema seja capaz de assegurar que o subsistema tem integridade adequada para o sistema. Isso geralmente exigirá

a realização de testes, análises e cálculos. Os resultados serão expressos na forma de dados exigidos pelo padrão.

O projetista do sistema [tipicamente um projetista de máquinas ou integrador] usará os dados do subsistema para realizar cálculos relativamente simples para determinar o Nível de Desempenho [PL] geral do sistema.

O PLr é usado para identificar o nível de desempenho exigido pela função de segurança. Para determinar o PLr, o padrão fornece um gráfico de risco no qual os fatores de aplicação de gravidade de acidente, frequência de exposição e possibilidade de evitá-los são inseridos.

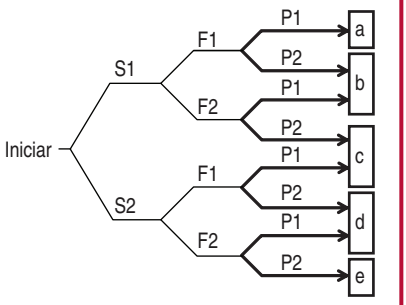


Gráfico de risco do Anexo A do EN ISO 13849-1

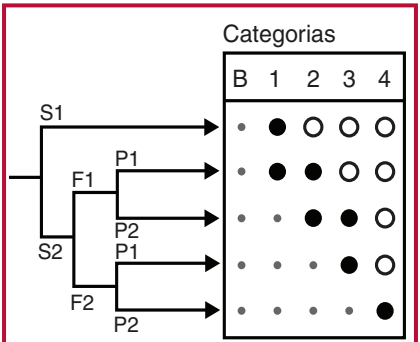


Gráfico de risco do Anexo B do EN ISO 945-1

A saída é o PLr. Usuários do antigo EN 954-1 estarão familiarizados com essa abordagem, porém, observe que a linha S1 agora é subdividida, enquanto o antigo gráfico de risco não era. Observe que isso significa uma possível reconsideração das medidas de integridade de segurança exigida em níveis de risco menores.

No entanto, há uma parte muito importante ainda a ser abordada. Agora sabemos do padrão em que medida o sistema deve ser bom e também como determinar em que medida é bom, mas não sabemos o que precisa fazer. Nós precisamos decidir o que é a função de segurança. Claramente a função de segurança deve ser apropriada para a tarefa, então como garantir isso? Como o padrão nos ajuda?

É importante perceber que a funcionalidade necessária somente pode ser determinada ao considerar as características predominantes na aplicação real. Isso pode ser considerado como a etapa de projeto do conceito de segurança. Não pode ser completamente abrangido pelo padrão, pois o padrão não conhece todas as características da aplicação específica. Em geral, isso também é aplicável ao fabricante de máquinas que produz a máquina, mas nem sempre conhece as condições exatas sob as quais ela será usada.

O padrão fornece ajuda ao listar várias das funções de segurança comumente usadas (por ex.: função de parada relacionada à segurança iniciada pela proteção, função de silenciamento, função iniciar/reiniciar) e ao oferecer algumas exigências normalmente associadas. Outros padrões, como o EN ISO 12100: Princípios básicos de projeto e EN ISO 14121: O uso de avaliações de riscos são extremamente recomendados nesse estágio. Além disso, há uma ampla gama de padrões específicos de máquina que fornecerão soluções para máquinas específicas. Dentro dos padrões da EN Europeia, eles são chamados padrões tipo C, alguns deles têm equivalentes exatos em padrões ISO.

Então, agora é possível ver que a etapa de projeto de conceito de segurança depende do tipo de máquina e também das características da aplicação no meio ambiente no qual será usada. O fabricante de máquinas deve antecipar esses fatores para conseguir projetar o conceito de segurança. As condições de uso pretendidas [ou seja, antecipadas] devem ser fornecidas no manual do usuário. O usuário da máquina precisa verificar se elas correspondem às condições de uso atuais.

Então agora nós temos uma descrição da funcionalidade de segurança. No anexo A do padrão, também solicitamos nível de desempenho [PLr] para peças relacionadas à segurança do sistema de controle [SRP/CS] que será usado para implementar essa funcionalidade. Agora precisamos projetar o sistema e assegurar que cumpra com o PLr.

Um dos fatores significativos na decisão sobre qual padrão utilizar [EN ISO 13849-1 ou EN/IEC 62061] é a complexidade da função de segurança. Na maioria dos casos, para máquinas, a função de segurança será relativamente simples e o EN ISO 13849-1 será a rota mais adequada. Dados confiáveis, cobertura de diagnóstico [DC], a arquitetura do sistema [Categoria], falha de causa comum e, onde relevante, exigências para software são usadas para avaliar o PL.

Isso é uma descrição simplificada, com o propósito de oferecer apenas uma visão geral. É importante entender que todas as disposições fornecidas no corpo do padrão devem ser aplicadas. No entanto, a ajuda está à disposição. A ferramenta de software SISTEMA está disponível para ajudar com a documentação e aspectos de cálculo. Ela também produz um arquivo técnico.

No momento de imprimir essa publicação, o SISTEMA está disponível em alemão e inglês. Outros idiomas serão lançados em breve. A BGIA, desenvolvedora do SISTEMA, é uma instituição de pesquisa e testes com grande reputação sediada na Alemanha. Está particularmente envolvida na solução de problemas científicos e técnicos relacionados à segurança no contexto de seguro e prevenção estatutária de acidentes na Alemanha. Ela trabalha em cooperação com agências de saúde e segurança ocupacional de mais de 20 países. Especialistas da BGIA, juntamente com seus colegas da BG tiveram participação significativa na elaboração do EN ISO 13849-1 e IEC/EN 62061.

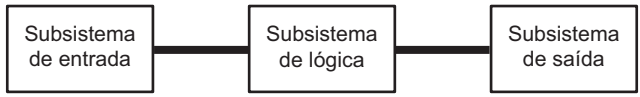
A “biblioteca” de dados de componentes de segurança da Rockwell Automation para uso com o SISTEMA está disponível em:

www.discoverrockwellautomation.com/safety

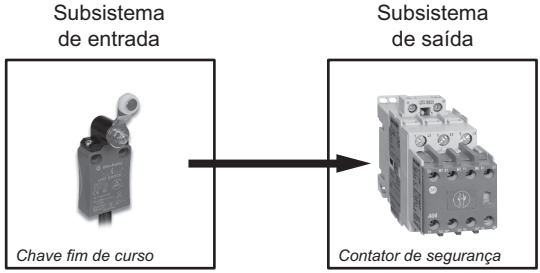
Qualquer que seja o método de cálculo do PL, é importante iniciar a partir da base correta. Precisamos visualizar nosso sistema da mesma maneira que o padrão, então vamos começar os procedimentos.

Estrutura do sistema

Qualquer sistema pode ser dividido em componentes de sistema básicos ou “subsistemas”. Cada subsistema tem sua própria função discreta. A maioria dos sistemas pode ser dividido em três funções básicas; entrada, solução de lógica e atuação [alguns sistemas simples podem não ter solução de lógica]. Os grupos de componentes que implementam essas funções são os subsistemas.

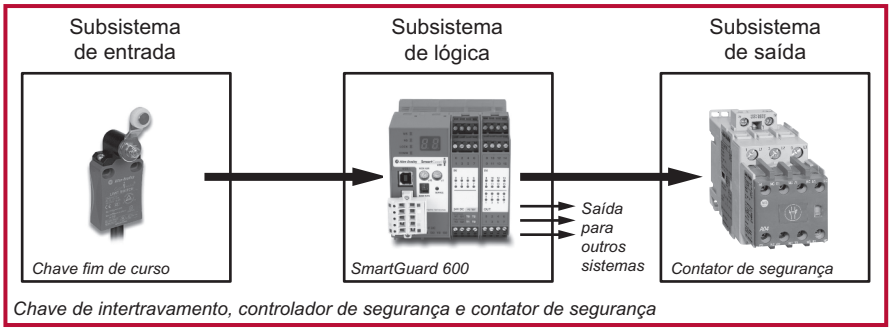


Qualquer sistema pode ser dividido em componentes de sistema básicos ou “subsistemas”. Cada subsistema tem sua própria função discreta. A maioria dos sistemas pode ser dividido em três funções básicas; entrada, solução de lógica e atuação [alguns sistemas simples podem não ter solução de lógica]. Os grupos de componentes que implementam essas funções são os subsistemas.



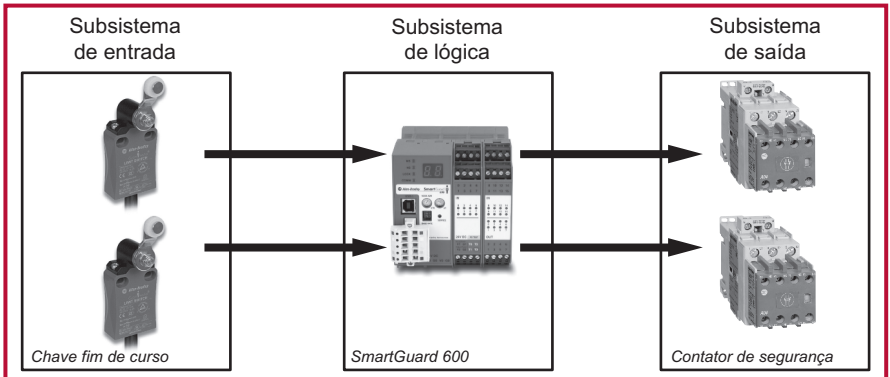
Chave de intertravamento e contator de segurança

Um único exemplo de sistema elétrico de canal único é demonstrado acima. Ele engloba apenas subsistemas de entrada e saída.



Chave de intertravamento, controlador de segurança e contator de segurança

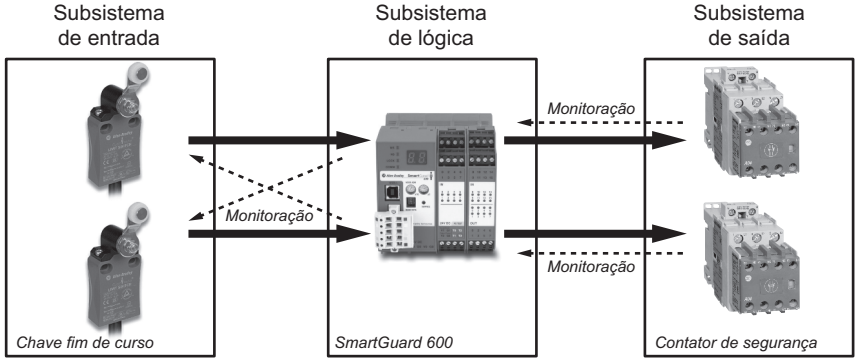
O sistema é um pouco mais complexo, pois alguma lógica também é necessária. O próprio controlador de segurança será tolerante a falhas (por ex.: canal duplo) internamente, porém, o sistema geral ainda é limitado a status de canal único devido à chave fim de curso única e ao contator único.



Sistema de segurança de canal duplo

Considerando a arquitetura básica do diagrama anterior, também há algumas outras coisas a considerar. Em primeiro lugar, quantos “canais” o sistemas possui? Um sistema de canal único falhará caso um dos seus subsistemas falhe. Um sistema de canal duplo [também chamado de redundante] precisaria ter duas falhas, uma em cada canal antes que o sistema falhe. Como tem dois canais, poderia tolerar uma falha única e ainda assim continuaria funcionando. O diagrama acima exibe um sistema de canal duplo.

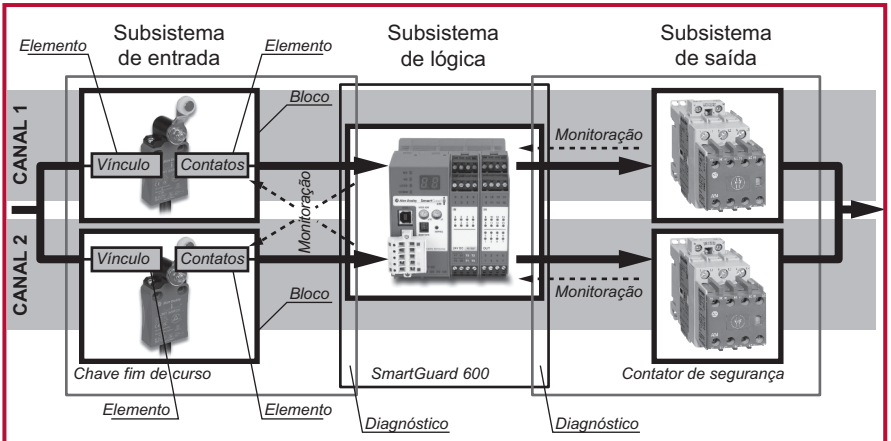
Claramente, um sistema de canal duplo tem menos probabilidade de falhar para uma condição perigosa do que um sistema de canal único. No entanto, é possível torná-lo ainda mais confiável [em termos de função de segurança] se incluirmos medidas de diagnóstico para detecção de falhas. É claro, após detectar a falha, também precisamos reagir a ela e colocar o sistema em um estado seguro. O diagrama a seguir exibe a inclusão de medidas de diagnóstico alcançadas por técnicas de monitoração.



Diagnósticos com um sistema de segurança de canal duplo

Geralmente é o caso [mas nem sempre] que o sistema engloba dois canais em todos os seus subsistemas. Portanto, é possível ver que, nesse caso, cada subsistema tem dois “subcanais”. O padrão descreve-os como “blocos”. Um subsistema de canal duplo terá um mínimo de dois blocos e um subsistema de canal único terá no mínimo um bloco. É possível que alguns sistemas englobem uma combinação de blocos de canal duplo e canal único.

Se desejarmos investigar o sistema de forma mais aprofundada, precisaremos observar as peças de componentes dos blocos. A ferramenta SISTEMA usa o termo “elementos” para essas peças de componentes.



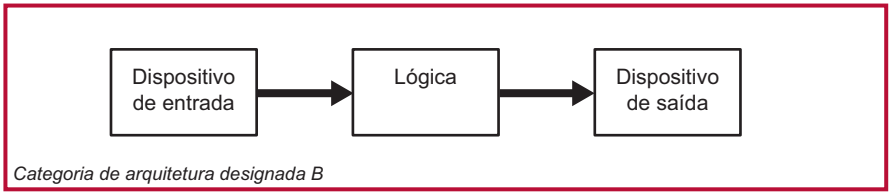
Sistema subdividido com diagnósticos e um sistema de segurança de canal duplo

O subsistema de chaves fim de curso é exibido subdividido até seu nível de elemento. O subsistema do contator de saída é subdividido até seu nível de bloco e o subsistema de lógica não é subdividido de forma alguma. A função de monitoração para as chaves fim de curso e contatores é desempenhada no controlador lógico. Portanto, as caixas representando a chave fim de curso e os subsistemas do contator têm uma pequena sobreposição com a caixa do subsistema lógico.

Esse princípio de subdivisão de sistema pode ser reconhecido na metodologia fornecida no EN ISO 13849-1 e no princípio de estrutura de sistema básico para a ferramenta SISTEMA. No entanto, é importante observar que há algumas ligeiras diferenças. O padrão não é restritivo em sua metodologia, mas para o método simplificado para estimar o PL, o primeiro passo comum é dividir a estrutura do sistema em canais e os blocos dentro de cada canal. Com o SISTEMA o sistema é geralmente dividido, em primeiro lugar, em subsistemas. O padrão não descreve explicitamente um conceito de subsistema, porém, seu uso como informado no SISTEMA proporciona uma abordagem mais compreensiva e intuitiva. É claro, não há efeito sobre o cálculo final. O SISTEMA e o padrão usam os mesmos princípios e fórmulas. Também é interessante observar que a abordagem do subsistema é usada no EN/IEC 62061.

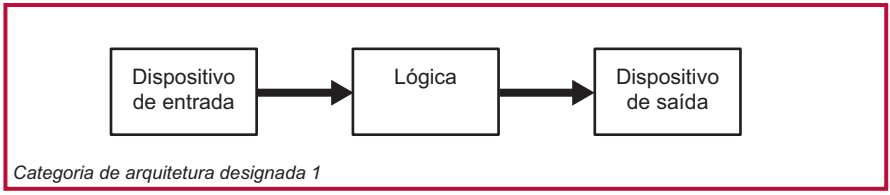
O sistema que utilizamos como exemplo é apenas um dos cinco tipos básicos de arquiteturas de sistema que o padrão designa. Qualquer pessoa familiar com o sistema de categorias reconhecerá nosso exemplo como representativo da categoria 3 ou 4.

O padrão usa as categorias EN 954-1 originais como seus cinco tipos básicos de arquiteturas de sistema designado. Elas são chamadas categorias de arquitetura designadas. As exigências para as categorias são quase [mas não muito] idênticas às informadas no EN 954-1. As categorias de arquitetura designada são representadas pelos números a seguir. É importante observar que podem ser aplicadas tanto em um sistema completo como em um subsistema. Os diagramas não devem ser considerados puramente como estrutura física, sua finalidade maior é de representação gráfica de exigências conceituais.



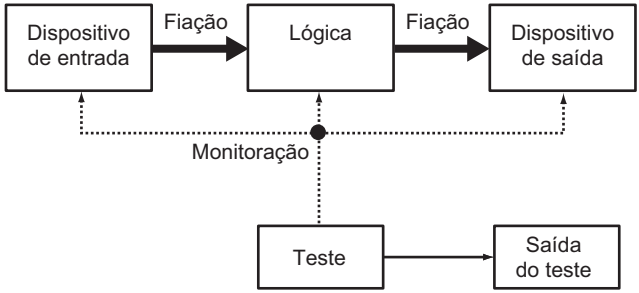
Categoria de arquitetura designada B

A categoria B de arquitetura designada deve usar princípios básicos de segurança [consulte o anexo do EN ISO 13849-2]. O sistema ou subsistema pode falhar no evento de uma falha única. Consulte o EN ISO 13849-1 para as exigências completas.



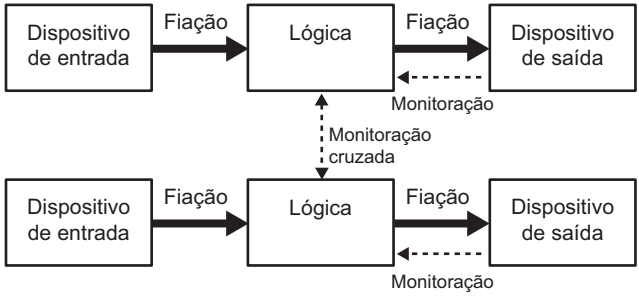
Categoria de arquitetura designada 1

A categoria 1 de arquitetura designada tem a mesma estrutura da categoria B e ainda pode falhar no evento de uma falha única. No entanto, como também deve usar princípios de segurança testados várias vezes [consulte o anexo do EN ISO 13849-2], é menos provável do que para a categoria B. Consulte o EN ISO 13849-1 para exigências completas.



Categoria de arquitetura designada 2

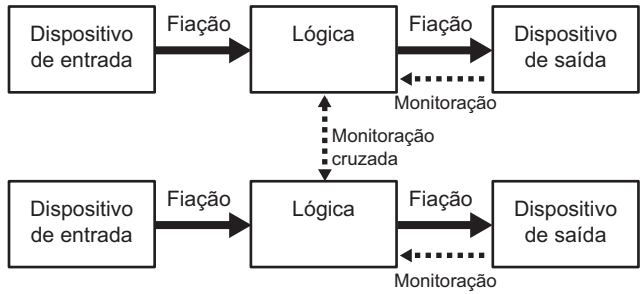
A categoria 2 de arquitetura designada deve usar princípios básicos de segurança [consulte o anexo do EN ISO 13849-2]. Também deve haver monitoração de diagnóstico por meio de um teste funcional do sistema ou subsistema. Isso deve ocorrer na inicialização e, então, periodicamente com uma frequência que iguala no mínimo cem testes a cada demanda na função de segurança. O sistema ou subsistema ainda pode falhar caso uma falha única ocorra entre os testes funcionais, no entanto, isso em geral é menos provável do que para a categoria 1. Consulte o EN ISO 13849-1 para exigências completas.



Categoria de arquitetura designada 3

A categoria 3 de arquitetura designada deve usar princípios básicos de segurança [consulte o anexo do EN ISO 13849-2]. Também há uma exigência de que o sistema/subsistema não deva falhar no evento de uma falha única. Isso significa que o sistema precisa ter tolerância à falha única com relação à sua função de segurança. A forma mais comum de alcançar essa exigência é empregar uma arquitetura de canal duplo, como demonstrado acima. Além disso, também é necessário que, onde praticável, a falha única seja detectada. Essa exigência é igual à exigência original para a categoria 3 do EN 954-1. Nesse contexto, o sentido da expressão

"onde praticável" demonstrou ser, de certo modo, problemático. Significou que a categoria 3 poderia abranger tudo, desde um sistema com redundância mas sem detecção de falha [geralmente descritivamente e apropriadamente chamado de "redundância estúpida"] a um sistema redundante onde todas as falhas únicas são detectadas. Esse problema é abordado no EN ISO 13849-1 pela exigência de estimar a qualidade da Cobertura de Diagnóstico [DC]. Podemos ver que quanto maior a confiabilidade [MTTFd] do sistema, menos DC será necessária. No entanto, também é claro que a DC precisa ser de, no mínimo, 60% para a categoria 3 de arquitetura.



Categoria de arquitetura designada 4

A categoria 4 de arquitetura deve usar princípios básicos de segurança [consulte o anexo do EN ISO 13849-2]. Ele tem um diagrama de exigências semelhante à categoria 3, mas precisa de maior monitoração, ou seja, maior Cobertura de diagnóstico. Isso é demonstrado pelas linhas pontilhadas grossas representando as funções de monitoração. Em essência, a diferença entre as categorias 3 e 4 é que para a categoria 3 a maioria das falhas deve ser detectada, mas para a categoria 4 todas as falhas devem ser detectadas. A DC precisa ser de, no mínimo, 99%. Mesmo combinações de falhas não devem causar uma falha perigosa.

Dados de confiabilidade

O EN ISO 13849-1 usa dados de confiabilidade quantitativos como parte do cálculo do PL alcançado pelas peças relacionadas à segurança de um sistema de controle. Isso é um desvio significativo do EN 954-1. A primeira questão que surge com isso é "de onde conseguimos esses dados?" É possível usar dados de manuais com confiabilidade reconhecida, porém, o padrão esclarece que a fonte preferida é a do fabricante. Para esse propósito, a Rockwell Automation está disponibilizando as informações relevantes na forma de biblioteca de dados para o SISTEMA. No devido momento, os dados também serão publicados em outros formulários. Antes de nos aprofundarmos, devemos considerar quais tipos de dados são necessários e também ter um entendimento de como são produzidos.

O tipo mais recente de dados necessários como parte da determinação do PL no padrão [e no SISTEMA] é o PFH [a probabilidade de falha perigosa por hora]. Esses dados são iguais aos representados pela abreviação PFHd usada no IEC/EN 62061.

PL (Nível de desempenho)	PFH_D (Probabilidade de falhas perigosas por hora)	SIL (Nível de integridade de segurança)
a	$\geq 10^{-5}$ a $<10^{-4}$	Nenhum
b	$\geq 3 \times 10^{-6}$ a $<10^{-5}$	1
c	$\geq 10^{-6}$ a $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ a $<10^{-6}$	2
e	$\geq 10^{-8}$ a $<10^{-7}$	3

A tabela acima exibe o relacionamento entre PFH, PL e SIL. Para alguns subsistemas, o PFH pode estar disponível de fábrica. Isso facilita a realização dos cálculos. O fabricante geralmente precisará realizar alguns cálculos relativamente complexos e/ou testes em seu subsistema para fornecê-lo. Caso não esteja disponível, o EN ISO13849-1 oferecerá uma abordagem de alternativa simplificada baseada no MTTFd [tempo médio para uma falha perigosa] médio de um canal único. O PL [e portanto, o PFH] de um sistema ou subsistema pode ser calculado utilizando a metodologia e fórmulas no padrão. Isso pode ser feito de forma ainda mais conveniente usando o SISTEMA.

OBSERVAÇÃO: É importante entender que, para um sistema de canal duplo (com ou sem diagnóstico), não é correto usar 1/PFHD para determinar o MTTFd necessário pelo EN ISO 13849-1. O padrão requer o MTTFd de canal único. Isso é um valor muito diferente para o MTTFd da combinação de ambos os canais de um subsistema duplo. Caso a PFHD de um sistema de canal duplo seja conhecida, ela pode ser inserida diretamente no SISTEMA.

MTTFd de canal único

Isso representa o tempo médio antes da ocorrência de uma falha que poderia causar uma falha da função de segurança. É expresso em anos. É um valor médio dos MTTFds dos “blocos” de cada canal e pode ser aplicado a um sistema ou subsistema. O padrão oferece a seguinte fórmula, que é usada para calcular a média de todos os MTTFds de cada elemento usado em um único canal ou subsistema.

Nesse estágio, o valor do SISTEMA torna-se aparente. Os usuários economizam tempo ao não precisar consultar tabelas e cálculos de fórmulas, pois essas tarefas são realizadas pelo software. Os resultados finais podem ser impressos em forma de relatório com várias páginas.

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{dj}}$$ (Fórmula D1 do EN ISO 13849-1)

Na maioria dos sistemas de canal duplo, ambos os canais são idênticos, portanto, o resultado das fórmulas representa cada um dos canais.

Caso os canais do sistema/subsistema sejam diferentes, o padrão fornecerá uma fórmula para atender a essa situação.

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

Isso, na verdade, realiza a média das duas médias. Para simplificar, também é possível usar o pior valor de canal de caso.

O padrão agrupa o MTTFd nas três faixas, como a seguir:-

Denotação de MTTFd de cada canal	**Faixa de MTTFd de cada canal**
Baixo	3 anos <= MTTFd < 10 anos
Médio	10 anos <= MTTFd < 30 anos
Alto	30 anos <= MTTFd < 100 anos

Níveis de $MTTF_d$

Observe que o EN ISO 13849-1 limita o MTTFd utilizável de um canal único de um subsistema a um máximo de 100 anos, mesmo que os valores reais derivados sejam muito maiores.

Como veremos adiante, a faixa alcançada da média do MTTFd é, então, combinada à categoria de arquitetura designada e a cobertura de diagnóstico [DC] para fornecer uma classificação de PL preliminar. O termo preliminar é usado aqui, pois outras exigências incluindo integridade sistemática e medidas contra falha de causa comum ainda devem ser atendidas quando for relevante.

Métodos de determinação de dados

Agora precisamos nos aprofundar em um estágio para verificar como um fabricante determina os dados, seja na forma de PFHd ou de MTTFd. Um entendimento disso é essencial quando lidamos com dados de fabricantes. Os componentes podem ser agrupados em três tipos básicos:

- Mecanístico (Eletromecânico, mecânico, pneumático, hidráulico etc.)
- Eletrônico (ou seja, estado sólido)
- Software

Há uma diferença fundamental entre mecanismos de falha comum desses três tipos de tecnologia. Na forma básica é possível ser resumido como a seguir:-

Tecnologia mecânica:

A falha é proporcional à confiabilidade inerente e taxa de uso. Quanto maior a taxa de uso, mais provável que uma das peças de componente seja degradada e falhe. Observe que isso não é a única causa de falhas, no entanto, a menos que limitemos o tempo/ciclos de operação, será a predominante. É auto-evidente que um contator que tem ciclo em comutação de uma vez a cada dez segundos operará de forma confiável por um período muito mais curto do que um contator idêntico que opera um por dia. Dispositivos de tecnologia física geralmente englobam componentes individualmente projetados para seu uso específico. Os componentes são formados, moldados, fundidos, usinados etc. Eles são combinados com ligações, molas, imãs, enrolamentos elétricos etc. para formar um mecanismo. Como as peças de componente em geral não têm qualquer histórico de uso em outras aplicações, não é possível encontrar qualquer dado de confiabilidade pré-existente para elas. A estimativa da PFHD ou o MTTFd para o mecanismo é normalmente baseada em testes. Ambos EN/IEC 62061 e EN ISO 13849-1 defendem um processo de teste conhecido como B10d Testing.

No teste B10d, uma variedade de amostras de dispositivos [em geral, pelo menos dez] são testados sob condições adequadamente representativas. O número médio de ciclos operacionais alcançado antes de 10% das amostras que falha para a condição perigosa é conhecido como o valor B10d. Na prática, geralmente é o caso em que todas as amostras falharão para um estado seguro, mas nesse caso o padrão afirma que o valor B10d [perigoso] pode ser considerado como o dobro do valor B10 [seguro].

Tecnologia eletrônica:

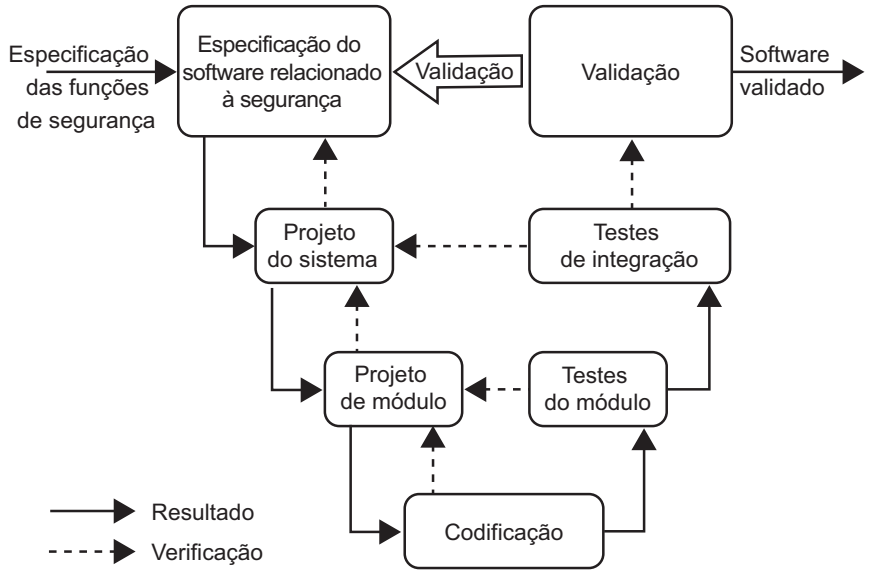
Não há desgaste físico relacionado às partes móveis. Considerando que um ambiente operacional corresponde às características elétricas e de temperatura especificadas [etc], a falha predominante de um circuito eletrônico é proporcional à confiabilidade inerente de seus componentes [ou falta deles]. Há vários motivos para a falha de um componente individual; imperfeições introduzidas durante a fabricação, quedas de energia excessivas, problemas de conexão mecânica etc. Em geral, falhas em componentes eletrônicos são difíceis de prever por análise e parecem ser aleatórias por natureza. Portanto, a realização de testes de um dispositivo eletrônico em condições de laboratório de teste não revelará necessariamente padrões de falha em longo prazo.

Para determinar a confiabilidade de dispositivos eletrônicos, é comum usar análises e cálculos. É possível encontrar bons dados para componentes individuais em manuais de dados confiáveis. É possível usar análises para determinar quais modos de falha de componente são perigosos. É aceitável e comum fazer a média dos modos de falha de componente como 50% seguros e 50% perigosos. Isso normalmente resulta em dados relativamente conservadores.

O IEC 61508 oferece fórmulas que podem ser usadas para calcular a probabilidade geral de falhas perigosas [PFH ou PFD] do dispositivo, ou seja, o subsistema. As fórmulas são bastante complexas e consideram [onde aplicável] a confiabilidade do componente, potencial para falha de causa comum [fator beta], cobertura de diagnóstico [DC], intervalo de teste funcional e intervalo de teste de prova. A boa notícia é que esse cálculo complexo normalmente será feito pelo fabricante do dispositivo. Ambos EN/IEC 62061 e EN ISO 13849-1 aceitam um subsistema calculado desse modo para IEC 61508. A PFHD resultante pode ser usada diretamente no Anexo K do EN ISO 13849-1 ou na ferramenta de cálculo SISTEMA.

Software:

Falhas de software são inerentemente sistemáticas por natureza. Todas as falhas são causadas pelo modo como é concebido, escrito ou compilado. Portanto, todas as falhas são causadas pelo sistema sob o qual é produzido, não por seu uso. Assim, para controlar as falhas, devemos controlar o sistema. Tanto o IEC 61508 quanto o EN ISO 13849-1 fornecem exigências e metodologias para fazer isso. Não precisamos entrar em detalhes aqui, além de dizer que usam o modelo clássico V. O software embutido é um problema para o projetista do dispositivo. A abordagem frequente é desenvolver software embutido com métodos dispostos no IEC 61508, parte 3. Quando se trata do código de aplicação, o software com o qual um usuário faz interface, a maioria dos dispositivos de segurança programáveis é fornecida com blocos de função "certificados" ou rotinas. Isso simplifica a tarefa de validação para o código de aplicação, porém, é necessário lembrar que o programa de aplicação concluído ainda deve ser validado. A maneira como os blocos são vinculados e parametrizados deve ser comprovada como correta e válida para a tarefa pretendida. EN ISO 13849-1 e IEC/EN 62061 oferecem diretrizes para esse processo.



Modelo V para o desenvolvimento do software

Cobertura de diagnóstico

Já abordamos esse assunto quando fizemos considerações sobre as categorias 2, 3 e 4 de arquitetura designada. Essas categorias necessitam de algum modo de teste de diagnóstico para verificar se a função de segurança ainda está funcionando. O termo “cobertura de diagnóstico” [geralmente abreviado como DC] é usado para caracterizar a eficácia desses testes. É importante perceber que a DC não é apenas baseada no número de componentes que podem falhar de forma perigosa. Ela leva em consideração a taxa total de falhas perigosas. O símbolo λ é usado para “taxa de falha”. A DC expressa o relacionamento das taxas de ocorrência dos dois tipos de falha perigosa a seguir;

Falha perigosa detectada [λdd] ou seja, essas falhas que causariam ou poderiam levar a perda da função de segurança, mas que são detectadas. Após a detecção, uma função de reação a falha faz com que o dispositivo ou sistema entre em estado seguro.

Falha perigosa [λd] ou seja, todas as falhas que poderiam potencialmente causar ou levar à perda da função de segurança. Isso inclui as falhas que são detectadas e as que não são. É claro que as falhas realmente perigosas são as perigosas não detectadas [chamadas de λdu].

A DC é expressa pela fórmula;

DC = λdd/λd é expressa como porcentagem.

Esse significado do termo DC é comum para o EN ISO 13849-1 e EN/IEC 62061. No entanto, o modo como é derivado difere. O padrão mencionado por último propõe o uso do cálculo com base na análise de modo de falha, porém, o EN ISO 13849-1 oferece um método simplificado na forma de tabelas de consulta. Várias técnicas típicas de diagnóstico são listadas junto com a porcentagem de DC considerada que seu uso alcança. Em alguns casos, um julgamento racional ainda é necessário, por exemplo, em algumas técnicas, a DC alcançada é proporcional à frequência com que o teste é realizado. Às vezes argumenta-se que essa abordagem é muito vaga. No entanto, a estimativa de DC pode depender de quantas variáveis diferentes e qual seja a técnica usada, o resultado somente pode ser descrito como aproximado.

Também é importante entender que as tabelas no EN ISO 13849-1 são baseadas em amplas pesquisas conduzidas pela BGIA nos resultados alcançados por técnicas de diagnóstico real usadas em aplicações reais. Para simplificar, o padrão divide a DC em quatro faixas básicas.

<60% = nenhuma

60% a <90% = baixa

90% a <99% = média

≥99% = alta

Essa abordagem de lidar com intervalos em vez de valores de porcentagem individuais também pode ser considerada como mais realista em termos de precisão alcançável. A ferramenta SISTEMA usa as mesmas tabelas de consulta que o padrão. À medida que o uso de equipamentos eletrônicos aumenta em dispositivos relacionados à segurança, a DC torna-se um fator mais importante. É provável que trabalhos futuros sobre os padrões se aprofundem no esclarecimento desse problema. Enquanto isso, o uso do julgamento de engenharia e senso comum deve ser suficiente para levar à escolha correta da faixa de DC.

Falha de causa comum

Na maioria dos sistemas ou subsistemas de canais duplos [i.e. tolerante a falhas simples] o princípio de diagnóstico é baseado na premissa de que não haverá falhas perigosas nos dois canais ao mesmo tempo. O termo “ao mesmo tempo” é expresso de forma mais precisa como “dentro do intervalo de teste de diagnóstico”. Se o intervalo de teste de diagnóstico for razoavelmente curto [por exemplo, com menos de oito horas] é razoável supor que duas falhas separadas e independentes são altamente improváveis de ocorrerem dentro desse tempo. No entanto, o padrão deixa claro que precisamos pensar cuidadosamente se as possibilidades de falhas realmente são separadas e independentes. Por exemplo, se uma falha em um componente pode levar a falhas previsíveis em outros componentes, em seguida, o conjunto resultante de falhas é considerado como uma falha simples.

É também possível que um evento que leve um componente a falhar também possa causar a falha de outros componentes. Isto é denominado “Falha de causa comum”, normalmente abreviada como FCC. O grau de propensão para a FCC é normalmente descrito como o fator beta (ß). É muito importante que os projetistas de subsistema

e sistema estejam conscientes das possibilidades de FCC. Existem muitos tipos diferentes de FCC e, correspondentemente, muitas maneiras diferentes de evitá-las. O EN ISO 13849-1 imprime um curso racional entre os extremos de complexidade e simplificação excessiva. Em comum com EN/IEC 62061 adota uma abordagem que é essencialmente qualitativa. Fornece uma lista de medidas conhecidas como eficazes para evitar a FCC.

Nº	Medida contra FCC	Pontuação
1	Separação/segregação	15
2	Diversidade	20
3	Projeto/Aplicação/Experiência	20
4	Avaliação/Análise	5
5	Competência/Treinamento	5
6	Ambiental	35

Marcação da Falha de causa comum

Um número suficiente destas medidas deve ser implementado no projeto de um sistema ou subsistema. Pode ser reclamado, com alguma justificativa, que o uso desta lista sozinha pode não ser adequado para evitar todas as possibilidades de FCC. Entretanto, caso a intenção seja propriamente considerada, fica claro que o espírito deste requerimento é fazer o projetista analisar as possibilidades de FCC e implementar medidas preventivas apropriadas com base em tecnologia e nas características da aplicação. O uso da lista reforça a consideração de algumas das técnicas mais fundamentais e eficazes, tais como a diversidade de modos de falha e as competências do projeto. A ferramenta BGIA SISTEMA também requer a aplicação das tabelas de consulta de FCC do padrão e as disponibiliza em uma forma prática.

Falhas Sistemáticas

Já discutimos dados de confiabilidade de segurança quantificados na forma de MTTFd e a probabilidade de falha perigosa. Entretanto, esta não é a história toda. Quando nos referimos a esses termos, estávamos realmente pensando sobre falhas que parecem ser aleatórias na natureza. De fato, o IEC/EN 62061 refere-se especificamente à abreviatura de PFHd como a probabilidade de falha aleatória de hardware. Mas existem alguns tipos de falhas conhecidas coletivamente como "falhas sistemáticas" que podem ser atribuídas a erros cometidos no projeto ou no processo de fabricação. O exemplo clássico disso é um erro no código do software. O padrão fornece medidas no anexo G para evitar esses erros [e, portanto, as falhas]. Estas medidas incluem disposições como o uso de materiais adequados e técnicas de fabricação, estudos, análises e simulações de computador. Há também eventos e características previsíveis que podem ocorrer no ambiente operacional que poderiam causar o fracasso a menos que seu efeito seja controlado. O anexo G também fornece medidas para isso. Por exemplo, é facilmente previsível que haverá eventuais perdas de energia. Desta forma, a desenergização de componentes deve resultar em um estado seguro para o sistema. Estas medidas podem parecer apenas senso comum, e na verdade elas o são, mas, no entanto, são essenciais. O resto dos requisitos do padrão é inútil, a menos que devidamente levado em conta para o controle e prevenção de falhas sistemáticas. Isso também irá, por vezes, requerer os mesmos tipos de medidas utilizados para o controle da falha de hardware aleatória [a fim de alcançar a desejada PFHd] tal como o teste de diagnóstico automático e hardware redundante.

Exclusão de falha

Uma das ferramentas primárias de análise para sistemas de segurança é a análise de falha. O projetista e o usuário devem entender como o sistema de segurança age na presença de falhas. Muitas técnicas estão disponíveis para realizar a análise. Exemplos incluem Análise de Falha em Árvore; Análise de Módulos, Efeitos e Criticidade das de Falhas; Análise de Árvore de Eventos; e Revisões de Força de Carga.

Durante a análise, certas falhas que não podem ser detectadas com os testes de diagnóstico automáticos podem ser descobertas, sem custos econômicos indevidos. Além disso, a probabilidade de ocorrerem estas falhas pode ser extremamente pequena, por meio de criação, construção e métodos de teste atenuantes. Sob essas condições, as falhas podem ser excluídas da análise mais aprofundada. A exclusão de falha é a exclusão da ocorrência de uma falha porque a probabilidade daquela falha específica do SRCS é insignificante.

O ISO13849-1:2006 permite a exclusão de falhas baseadas na improbabilidade técnica de ocorrência, na experiência técnica geralmente aceita e nos requisitos técnicos relacionados à aplicação. O ISO13849-2:2.003 fornece exemplos e justificativas para a exclusão de certas falhas para sistemas elétricos, pneumáticos, hidráulicos e mecânicos. As exclusões de falha devem ser declaradas com justificativas detalhadas fornecidas na documentação técnica.

Nem sempre é possível avaliar o sistema de controle de segurança, sem assumir que certas falhas podem ser excluídas. Para obter informações detalhadas sobre as exclusões de falhas, consulte o ISO 13849-2.

Na medida em que o nível de risco fica mais alto, a justificativa para a exclusão de falhas torna-se mais rigorosa. Em geral, quando PLe se faz necessário para a função de segurança ser implementada por um sistema de controle de segurança, não é normal depender somente de exclusões de falhas para atingir esse nível de desempenho. Isso depende da tecnologia usada e do ambiente operacional pretendido. Desta forma, é essencial que o projetista tome cuidado adicional com o uso de exclusões de falhas à medida que a exigência de PL aumenta.

Por exemplo, um sistema de intertravamento de porta que deve alcançar PLe precisará incorporar uma tolerância mínima a falhas de 1 (por ex.: duas chaves de posição mecânicas convencionais) para alcançar esse nível de desempenho desde que não seja normalmente justificável excluir falhas como atuadores de chave danificados. No entanto, pode ser aceitável excluir falhas, como curto-circuitos de fiação dentro de um painel de controle projetado de acordo com os padrões relevantes.

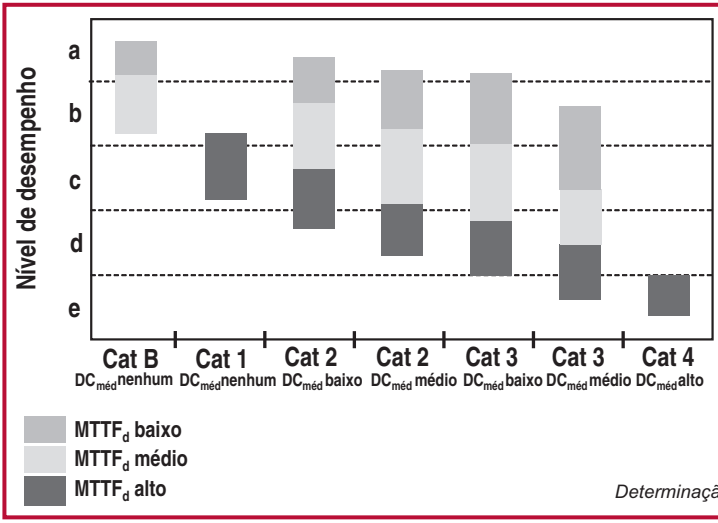
Nível de desempenho (PL)

O nível de desempenho é um nível discreto que especifica a capacidade das partes relacionadas com a segurança do sistema de controle para desempenhar uma função de segurança.

Para avaliar o PL obtido por uma aplicação de qualquer uma das cinco arquiteturas designadas, os dados a seguir são necessários para o sistema (ou subsistema):

- $MTTF_d$ (tempo médio para falha perigosa de cada canal)
- DC (cobertura de diagnóstico)
- Arquitetura (categoria)

O diagrama a seguir mostra um método gráfico para determinar o PL a partir da combinação desses fatores. A tabela no final deste documento apresenta os resultados tabulares de diferentes modelos de Markov que criaram a base deste diagrama. Consulte a tabela quando uma determinação mais precisa for necessária.



Determinação gráfica de PL

Outros fatores também devem ser realizados para satisfazer o PL exigido. Esses requisitos incluem as provisões para falhas de causa comum, falha sistemática, condições ambientais e o tempo de missão.

Caso a PFH_D do sistema ou subsistema for conhecida, a Tabela 10.4 (Anexo K do padrão) pode ser usada para derivar o PL.

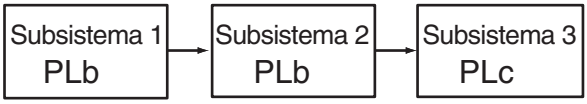
Projeto e combinações de subsistema

Subsistemas que estejam em conformidade com o PL podem ser simplesmente combinados em um sistema usando a tabela 10.3. O raciocínio por trás dessa tabela é claro. Primeiro, o sistema só pode ser tão bom quanto o seu subsistema mais fraco. Segundo, quanto mais subsistemas existirem, maior a possibilidade de falha.

PL_{baixo}	N_{baixo}	PL
a	>3	não permitido
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

Cálculo de PL para séries de subsistemas combinados

No sistema mostrado na figura a seguir, os níveis mais baixos de desempenho estão em subsistemas 1 e 2. Ambos são PLB. Portanto, no uso desta tabela, podemos ler em b (na coluna PL_{baixo}), até 2 (na coluna N_{baixo}) e descobrir que o sistema atingiu PL como b (na coluna PL). Se todos os três subsistemas forem PLb, o PL alcançado seria PLa.



Combinação de subsistemas em série como um sistema de PLb

Validação

A validação desempenha um papel importante ao longo do desenvolvimento do sistema de segurança e do processo de comissionamento. O ISO/EN 13849-2:2003 define os requisitos para validação. Ela pede um plano de validação e discute a validação de técnicas de proba e análise, tais como Modos de Análise de Falhas em Árvore e de Falhas, Efeitos e Análise de Criticidade. A maioria destes requisitos será aplicada ao fabricante do subsistema em vez do usuário do subsistema.

Comissionamento da máquina

Na fase de comissionamento do sistema ou máquina, a validação das funções de segurança deve ser realizada em todos os modos de operação e deve cobrir todas as condições normais e anormais previsíveis. As combinações de entradas e sequências de operação também devem ser levadas em consideração. Este procedimento é importante porque é sempre necessário verificar que o sistema seja adequado para as características operacionais e de ambiente real. Algumas destas características podem ser diferentes das previstas na fase de concepção.

Projeto de sistema de acordo com o IEC/EN 62061

IEC/EN 62061, “Segurança de máquinas - Segurança funcional de segurança relacionada a sistemas elétricos, eletrônicos e de controle eletrônico programável”, é a implementação de máquinas específicas do IEC/EN 61508. Ele oferece requisitos que são aplicáveis ao nível de projeto de sistema de todos os tipos de sistemas de controle de máquinas relacionados com a segurança elétrica e também para o projeto de subsistemas ou dispositivos não-complexos.

A avaliação de risco resulta em uma estratégia de redução de risco que, por sua vez, identifica a necessidade de funções de controle relacionadas à segurança. Estas funções devem ser documentadas e devem incluir:

- a especificação de requisitos funcionais e
- a especificação de requisitos de integridade de segurança.

Os requisitos funcionais incluem detalhes como a frequência de operação, tempo de resposta requerido, modos de funcionamento, ciclos de trabalho, ambiente operacional e as funções de reação de falha. Os requisitos de integridade de segurança são expressos em níveis chamados de níveis de integridade de segurança (SIL). Dependendo da complexidade do sistema, alguns ou todos os elementos da tabela abaixo devem ser considerados para determinar se a concepção do sistema está de acordo com o SIL requerido.

Elemento para consideração de SIL	**Símbolo**
Probabilidade de falha perigosa por hora	PFH_D
Tolerância às falhas de hardware	Sem símbolo
Fração de falha segura	FFS
Intervalo de ensaio	T_1
Intervalo de teste de diagnóstico	T_2
Susceptibilidade a falhas de causa comum	ß
Cobertura de diagnóstico	DC

Elementos para consideração de SIL

Subsistemas

O termo “subsistema” tem um significado especial no IEC/EN 62061. É a subdivisão do primeiro nível de um sistema em duas partes, que, se falharem, podem causar

uma falha da função de segurança. Desta forma, se dois interruptores redundantes forem usados em um sistema, nenhum dos interruptores individuais é um subsistema. O subsistema compreenderia ambos os interruptores e qualquer função de diagnóstico de falha associada.

Probabilidade de Falha Perigosa por Hora (PFHD)

O IEC / EN 62061 usa os mesmos métodos básicos discutidos na seção sobre o EN ISO 13849-1 para determinar as taxas de falhas ao nível de componente. As mesmas disposições e métodos se aplicam para os componentes “mecânicos” e eletrônicos. No IEC/EN 62061, o MTTFd não é considerado em anos. A taxa de falha por hora (λ) é calculada diretamente ou obtida ou fornecida pelo valor de B10 na seguinte fórmula:

λ = 0.1 x C/B10 (onde “C” é o número de ciclos operacionais por hora)

Há uma diferença significativa entre os padrões na metodologia para determinar a PFH_D total para um subsistema ou sistema. Deve ser realizada uma análise dos componentes para determinar a probabilidade de falha nos subsistemas. São fornecidas fórmulas simplificadas para o cálculo das arquiteturas comuns de subsistemas (descrito mais tarde). Onde estas fórmulas não forem apropriadas, será necessário o uso de métodos mais complexos de cálculo, como os modelos de Markov. A Probabilidade de Falha Perigosa (PFH_D) de cada subsistema é então adicionada para determinar a PFH_D total do sistema. A tabela 15 (Tabela 3 do padrão) pode então ser usada para determinar qual Nível de Integridade de Segurança (SIL) é apropriado para esta faixa de PFH_D.

$$\lambda_{DssB} = (1-ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2}) / 2$$

As fórmulas para esta arquitetura levam em conta o arranjo paralelo dos elementos do subsistema e adicionam os dois elementos seguintes da tabela anterior:

ß (Beta) é a susceptibilidade a falhas de causa comum

SIL (nível de integridade de segurança)	**PFH_D (probabilidade de falha perigosa por hora)**
3	$\geq 10^{-8}$ a $<10^{-7}$
2	$\geq 10^{-7}$ a $<10^{-6}$
1	$\geq 10^{-6}$ a $<10^{-5}$

Probabilidades de falha perigosa para SILs

Os dados da PFH_D para um subsistema serão normalmente fornecidos pelo fabricante. Os dados para os componentes e sistemas de segurança da Rockwell Automation estão disponíveis numa série de formas, incluindo:

www.discoverrockwellautomation.com/safety

O IEC / EN 62061 também deixa claro que os manuais de dados de confiabilidade podem ser usados, se e quando aplicável.

Para dispositivos eletromecânicos de baixa complexidade, o mecanismo de falha está geralmente relacionado com o número e frequência de operações em vez de apenas o tempo. Desta forma, para estes componentes os dados serão derivados a partir de algum tipo de teste (por exemplo, testes B10 como descrito no capítulo do EN ISO 13849-1). As informações baseadas em aplicação, como o número previsto de operações por ano são necessárias para converter os dados B10d ou similares para PFH_D.

OBSERVAÇÃO: Em geral, o seguinte é verdadeiro (levando em conta um fator de alteração de anos para horas):

$PFH_D = 1/MTTFd$

Entretanto, é importante compreender que para um sistema de canal duplo (com ou sem diagnóstico), não é correto utilizar 1/ PFH_D para determinar o MTTFd que é exigido pelo EN ISO 13849-1. Esse padrão pede o MTTFd de canal único. Este é um valor muito diferente do MTTFd da combinação de ambos os canais de um subsistema de dois canais

Restrições arquitetônicas

A característica essencial do IEC/EN 62061 é que o sistema de segurança é dividido em subsistemas. O nível de integridade de segurança de hardware que pode ser reivindicado por um subsistema é limitado não só pela PFH_D, mas também pela tolerância a falhas de hardware e da fração de falha dos subsistemas. A tolerância a falhas de hardware é a capacidade do sistema para executar sua função na presença de falhas. Uma tolerância a falhas zero significa que a função não é realizada quando ocorre uma única falha. Uma tolerância a falhas “um” é quando um subsistema desempenha sua função na presença de uma única falha. Fração de falha segura é a parte da taxa de falhas total que não resulte numa falha perigosa. A combinação destes dois elementos é conhecida como a restrição de arquitetura e sua saída é o limite de reivindicação de SIL (SIL CL). A tabela a seguir mostra a relação entre as restrições de arquitetura para o SILCL. Um subsistema (e, portanto, seu sistema) deve satisfazer os requisitos PFH_D e as restrições arquitetônicas, juntamente com as outras disposições pertinentes do padrão.

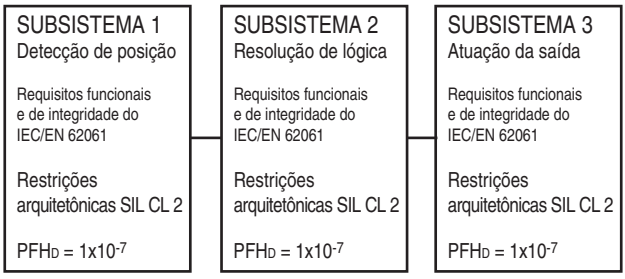
Fração de falha segura (FFS)	Tolerância a falhas de hardware		
	0	1	2
<60%	Não permitido a menos que exceções específicas se apliquem	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - < 99%	SIL2	SIL3	SIL3
≥99%	SIL3	SIL3	SIL3

Restrições Arquitetônicas em SIL

Por exemplo, a arquitetura do subsistema que possui a tolerância a falhas única e uma fração de falha segura de 75% é limitada a não mais do que uma classificação SIL 2, independentemente da probabilidade de falha perigosa. Ao combinar subsistemas, o SIL alcançado por SRCS está restrito a ser inferior ou igual ao menor SIL CL de qualquer dos subsistemas envolvidos na função de controle de segurança.

Realização do sistema

Para calcular a probabilidade de falha perigosa, cada função de segurança tem de ser dividida em blocos funcionais, que são então realizados como subsistemas. Uma implementação do projeto do sistema de uma função de segurança típica inclui um sensor de dispositivo ligado a um dispositivo de lógica ligado a um atuador. Isto cria um arranjo de subsistemas em série. Como já vimos, se pudermos determinar a probabilidade de falhas perigosas para cada subsistema e conhecer seu SIL CL, então a probabilidade de falha no sistema é facilmente calculada pela adição da probabilidade de falhas dos subsistemas. Este conceito é mostrado abaixo.



$= PFH_D\,1$ $+ PFH_D\,2$ $+ PFH_D\,3$
$= 1x10^{-7}$ $+ 1x10^{-7}$ $+ 1x10^{-7}$
$= 3x10^{-7}$ ou seja, adequado para SIL2

Se, por exemplo, quisermos chegar a SIL 2, cada subsistema deve ter um Limite de Exigência de SIL (SIL CL) de ao menos SIL 2, e a soma de PFH_D para o sistema não deve exceder o limite permitido na tabela anterior mostrando “Probabilidade de Falhas Perigosas para SILs”.

Projeto de subsistema – IEC/EN 62061

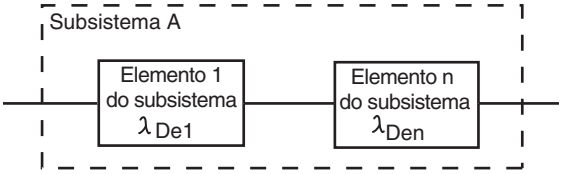
Se um projetista de sistema utiliza componentes prontos “integrados” em subsistemas de acordo com o IEC/EN 62061, isto torna a vida deles muito mais fácil, porque os requisitos específicos para o projeto de subsistemas não se aplicam. Estes requisitos, em geral, serão coberto pelo fabricante do dispositivo (subsistema) e são muito mais complexos do que os necessários para o projeto ao nível de sistema.

O IEC/EN 62061 exige que os subsistemas complexos como CLPs de segurança estejam em conformidade com o IEC 61508 ou outros padrões apropriados. Isto significa que, para dispositivos que utilizam componentes eletrônicos ou programáveis complexos, aplica-se integralmente o rigor do padrão IEC 61508. Este pode ser um processo muito rigoroso e envolvente. Por exemplo, a avaliação de PFH_D atingido por um complexo subsistema pode ser um processo muito complicado, utilizando técnicas como o modelo de Markov, diagramas de blocos de confiabilidade ou de análise de árvore de falhas.

O IEC/EN 62061 fornece os requisitos para o projeto de subsistemas de menor complexidade. Normalmente, isso incluiria componentes elétricos relativamente simples, como interruptores de intertravamento e relés de monitoração de segurança eletromecânicos. As exigências não são tão envolvidas quanto as do IEC 61508, mas ainda podem ser bastante complicadas.

O IEC/EN 62061 fornece quatro arquiteturas lógicas do subsistema com fórmulas de acompanhamento que podem ser utilizadas para avaliar a PFH_D alcançada por um subsistema de baixa complexidade. Estas arquiteturas são representações puramente lógicas e não devem ser tidas como arquiteturas físicas. As quatro arquiteturas de subsistemas lógicos com fórmulas que os acompanham são mostradas nos quatro diagramas seguintes.

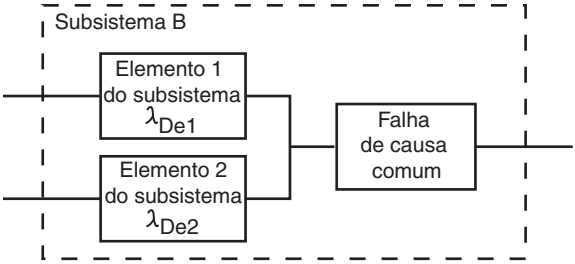
Para a arquitetura de subsistema básica mostrada abaixo, as probabilidades de falhas perigosas são simplesmente somadas.



Arquitetura lógica do subsistema A

$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den}$
$PFH_{DssA} = \lambda_{DssA} \times 1h$

λ, Lambda é usado para designar a taxa de falha. As unidades da taxa de falha são falhas por hora. $?_D$, Lambda sub D é a taxa de falha perigosa. $?_{DssA}$, Lambda sub DssA é a taxa de falha perigosa do subsistema A. A falha lambda sub DSSA é a soma das taxas dos elementos individuais, e1, e2, e3, até en (inclusive). A probabilidade de falha perigosa é multiplicada por 1 hora pela probabilidade de criar falha dentro de uma hora.
O diagrama a seguir mostra um sistema tolerante a falha única, sem uma função de diagnóstico. Quando a arquitetura inclui a tolerância a falhas única, o potencial de falha de causa comum existe e deve ser considerado. A derivação da falha de causa comum é descrita brevemente mais tarde neste capítulo.



Arquitetura lógica do subsistema B

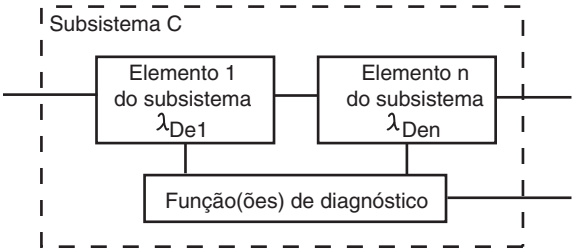
$\lambda_{DssB} = (1-ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2}) / 2$
$PFH_{DssB} = \lambda_{DssB} \times 1h$

As fórmulas para esta arquitetura levam em conta o arranjo paralelo dos elementos do subsistema e adiciona os dois elementos seguintes da tabela anterior “Elementos para Consideração SIL”.

ß – a susceptibilidade a falhas de causa comum (Beta)

T1 – o intervalo do teste ou a vida útil, o que for menor. O teste é projetado para detectar falhas e degradação do subsistema de segurança para que o subsistema possa ser restaurado a uma condição operacional. Em termos práticos, isso significa normalmente a substituição (como o termo “tempo de missão” equivalente no EN ISO 1384-1).

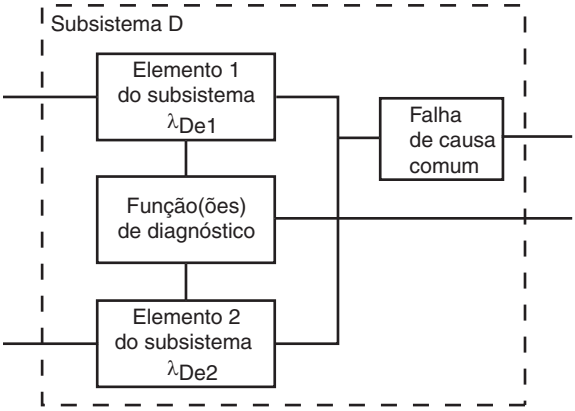
O diagrama a seguir mostra a representação funcional de um sistema de tolerância a falhas zero com uma função de diagnóstico. A cobertura de diagnóstico é utilizada para diminuir a probabilidade de falhas perigosas no hardware. Os testes de diagnóstico são realizados automaticamente. A definição da cobertura de diagnóstico é a mesma que a apresentada no padrão EN ISO 13849-1, ou seja, a relação entre a taxa de falhas perigosas detectadas em comparação com a taxa de todas as falhas perigosas.



Arquitetura lógica do subsistema C

$\lambda_{DssC} = \lambda_{De1} (1\text{-}DC_1) + \ldots + \lambda_{Den} (1\text{-}DC_n)$
$PFH_{DssC} = \lambda_{DssC} \times 1h$

Estas fórmulas incluem a cobertura de diagnóstico, DC, para cada um dos elementos do subsistema. As taxas de falha de cada um dos subsistemas são reduzidas pela cobertura de diagnóstico de cada subsistema.
O quarto exemplo de uma arquitetura de subsistema é mostrado a seguir.
Este subsistema é tolerante a falhas únicas e inclui uma função de diagnóstico.
O potencial para a falha de causa comum também deve ser considerado em sistemas tolerantes a falhas únicas.



Arquitetura lógica do subsistema D

Caso os elementos do subsistema seja diferentes, as seguintes fórmulas são usadas:

$$\lambda_{DssD} = (1 - ß)^2 \{ \lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2 / 2 + \lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \times T_1 / 2 \} + ß \times (\lambda_{De1} + \lambda_{De2}) / 2$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

Se os elementos do subsistema forem os mesmos, as fórmulas seguintes são usadas:

$$\lambda_{DssD} = (1 - ß)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2 / 2 + [\lambda_{De}^2 \times (1-DC)] \times T_1 \} + ß \times \lambda_{De}$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

Observe que ambas as fórmulas usam um parâmetro adicional, o intervalo de diagnóstico T2. Esta é apenas uma verificação periódica da função. É um teste menos abrangente do que o ensaio.
Como exemplo, utilize os seguintes valores para o exemplo, onde os elementos do subsistema são diferentes:

ß = 0,05
$\lambda_{De} = 1 \times 10^{-6}$ falhas/hora
T1 = 87600 horas (10 anos)
T2 = 2 horas
DC = 90%

PFH_{DssD} = 5.791E-08 falhas perigosas por hora. Isto estaria dentro da amplitude necessária para SIL3

Efeito de intervalo de ensaio

O IEC / EN 62061 afirma que um intervalo de ensaio (PTI) de 20 anos é o preferido (mas não obrigatório). Vejamos o efeito do intervalo de ensaio no sistema. Se recalcularmos a fórmula com T1 em 20 anos, dá o resultado PFHDssD = 6.581E-08. Ainda está dentro do intervalo necessário para SIL 3. O projetista deve ter em mente que este subsistema deve ser combinado com outros subsistemas para calcular a taxa global de falha perigosa.

Análise de efeito de Falha de causa comum

Vejamos o efeito das falhas de causa comum no sistema. Digamos que tomemos medidas adicionais e nosso valor ß (Beta) melhore em 1% (0,01), enquanto o intervalo de ensaio permaneça em 20 anos. A taxa de falha perigosa melhora para 2.71E-08, o que significa que o subsistema atual é mais adequado para uso em um sistema de SIL 3.

Falha de Causa Comum (FCC)

Falha de causa comum é quando várias falhas resultantes de uma única causa produzem uma falha perigosa. Informações sobre FCC só serão geralmente exigidas pelo projetista de subsistema, normalmente o fabricante. Ele é usado como parte das fórmulas indicadas para a estimativa de PFHD de um subsistema. Não será normalmente exigido ao nível de projeto do sistema.

O Anexo F do IEC/EN62061 fornece uma abordagem simples para a estimativa de FCC. A tabela abaixo mostra um resumo do processo de pontuação

Nº	Medida contra FCC	Pontuação
1	Separação/segregação	25
2	Diversidade	38
3	Projeto/Aplicação/Experiência	2
4	Avaliação/Análise	18
5	Competência/Treinamento	4
6	Ambiental	18

Pontuação para Medidas contra a Falha de Causa Comum

Os pontos são concedidos para o emprego de medidas específicas contra FCC. A pontuação é somada para determinar o fator de falha de causa comum, mostrada na tabela a seguir. O fator beta é usado nos modelos de subsistema para “ajustar” a taxa de falha.

Pontuação geral	Fator (ß) para Falha de Causa Comum
<35	10% (0,1)
35 - 65	5% (0,05)
65 - 85	2% (0,02)
85 - 100	1% (0,01)

Fator Beta para Falha de Causa Comum

Cobertura de Diagnóstico (DC)

Os testes de diagnóstico automáticos são empregados para diminuir a probabilidade de falhas perigosas no hardware. Ser capaz de detectar todas as falhas perigosas de hardware seria o ideal, mas, na prática, o valor máximo é fixado em 99% (o que também pode ser expresso como 0,99)

A cobertura de diagnóstico é a razão entre a probabilidade de falhas perigosas detectadas e a probabilidade de todas as falhas perigosas.

$$DC = \frac{\text{Probabilidade de falhas perigosas detectadas, } \lambda_{DD}}{\text{Probabilidade de falhas perigosas totais, } \lambda_{Dtotal}}$$

O valor da cobertura de diagnóstico estará entre zero e um.

Tolerância a falhas de hardware

A tolerância a falhas de hardware representa o número de falhas que podem ser sustentadas por um subsistema antes que causem uma falha perigosa. Por exemplo, a tolerância a falhas de hardware de 1 significa que duas falhas podem causar uma perda da função de controle relacionada com a segurança, mas uma falha não.

Gestão de segurança funcional

O padrão apresenta os requisitos para o controle de gestão e atividades técnicas que são necessários para a realização de um sistema de controle elétrico de segurança relacionado.

Intervalo de ensaio

O intervalo do ensaio representa o tempo após o qual um subsistema deve ser totalmente verificado ou substituído para assegurar que ele esteja em condição de agir “como novo”. Na prática, no setor das máquinas, isto é conseguido através de substituição. Então, o intervalo de ensaio é para nós o mesmo que a vida útil. O EN ISO 13849-1:2008 se refere a ele como Tempo de Missão.

Um ensaio é uma verificação que pode detectar falhas e degradação em um SRCS para que o SRCS possa ser restaurado o mais próximo possível da condição “como novo”. O ensaio deve detectar 100% de todas as falhas perigosas. Canais separados devem ser testados separadamente.

Ao contrário dos testes de diagnóstico, que são automáticos, os ensaios são geralmente realizados manualmente, e off-line. Por ser automático, o teste de diagnóstico é executado muitas vezes em comparação com o ensaio, que é feito com pouca frequência. Por exemplo, os circuitos indo para uma chave de intertravamento em uma guarda podem ser testados automaticamente para as condições de curto-circuito e circuito aberto com testes de diagnóstico (por exemplo, de pulso).

O intervalo de ensaio deve ser declarado pelo fabricante. Às vezes, o fabricante irá fornecer uma gama de diferentes de intervalos de ensaio.

Fração de falha segura (FFS)

A fração de falha segura é semelhante à cobertura de diagnóstico, mas também leva em conta qualquer tendência inerente à falha no sentido de um estado seguro. Por exemplo, quando um fusível queima, não é uma falha, mas é altamente provável que a falha será um circuito aberto, o que, na maioria dos casos, seria uma falha “segura”. A FFS é (a soma da taxa de falhas “seguras” com a taxa de falhas perigosas detectadas) dividida por (a soma da taxa de “falhas seguras” mais a taxa de falhas perigosas detectadas e não-detectadas). É importante perceber que os únicos tipos de falhas a serem considerados são aqueles que podem ter algum efeito na função de segurança.

A maior parte dos dispositivos mecânicos de complexidade mais baixa, como botões de parada de emergência e chaves de intertravamento terão (por conta própria) uma FFS. A maior parte dos dispositivos eletrônicos de segurança projetaram redundância e monitoração, portanto, uma FFS superior a 90% é comum, embora seja geralmente completamente devido à capacidade de cobertura de diagnóstico. O valor de FFS normalmente será fornecido pelo fabricante.

A fração de falha segura (FFS) pode ser calculada utilizando a seguinte equação:

$$FFS = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$$

onde

λ_S = a taxa de fração de falha segura,
$\Sigma\lambda_S + \Sigma\lambda_D$ = taxa de falha total,
λ_{DD} = taxa de falha perigosa detectada
λ_D = taxa de falha perigosa.

Falha sistemática

O padrão tem requisitos para o controle e prevenção de falha sistemática. As falhas sistemáticas diferem das falhas aleatórias de hardware que são falhas que ocorrem em um horário aleatório, geralmente resultante da degradação de peças de hardware. Os tipos típicos de uma possível falha sistemática são erros de projeto de software, erros de projeto de hardware, erros de especificação de requisitos e procedimentos operacionais. Exemplos de medidas necessárias para evitar falhas sistemáticas incluem

- a adequada seleção, combinação, arranjos, montagem e instalação de componentes;
- o uso de boas práticas de engenharia;
- o seguimento das especificações do fabricante e instruções de instalação;
- a garantia da compatibilidade entre os componentes;
- o suporte às condições ambientais;
- o uso de materiais adequados.

Sistema de controle relacionado à segurança, considerações estruturais

Visão geral

Este capítulo aborda aspectos estruturais e os princípios gerais que devem ser levados em conta na concepção de um sistema de controle relacionado à segurança de acordo com qualquer padrão. Ele usa muito da linguagem das categorias no EN 954-1, porque as categorias abordam principalmente a estrutura dos sistemas de controle.

Categorias de sistemas de controle

As “Categorias” dos sistemas de controle originadas no EN 954-1:1996 (ISO13849-1:1999). No entanto, elas ainda são muitas vezes usadas para descrever sistemas de controle de segurança e continuam a ser uma parte integrante do EN ISO13849-1 conforme discutido na seção “Introdução à segurança funcional dos sistemas de controle”.

Há cinco categorias que descrevem o desempenho de uma performance de reação a falha relacionados a um sistema de controle relacionado à segurança. Consulte a Tabela 19 para obter um resumo destas categorias. As seguintes observações se aplicam à tabela.

> **Observação 1**: A Categoria B por si só não tem nenhuma medida especial para segurança mas forma a base para outras categorias.
>
> **Observação 2**: Múltiplas falhas causadas por uma causa comum ou como consequências inevitáveis da primeira falha serão contadas como uma única falha.
>
> **Observação 3:** A avaliação de falha pode ser limitada a duas falhas combinadas, se isso for justificável, mas circuitos complexos (por exemplo, os circuitos de microprocessador) podem exigir mais falhas combinadas a serem consideradas.

A categoria 1 tem como objetivo a prevenção de falhas. Ela é alcançada através do uso de princípios de projeto, componentes e materiais adequados. A simplicidade de princípio e projeto, juntamente com as características estáveis e previsíveis do material são as chaves para essa categoria.

As categorias 2, 3 e 4 exigem que se falhas não puderem ser evitadas, devem ser detectadas e tomadas as medidas adequadas.

Redundância, diversidade e monitoração são as chaves para essas categorias. A redundância é a duplicação da mesma técnica. Diversidade é o uso de duas técnicas diferentes. Monitoração é a verificação do estado dos dispositivos e, em seguida, tomada das medidas adequadas com base em resultados do status. O método comum, mas não único, de monitoração é duplicar as funções críticas de segurança e comparar a operação.

Resumo dos requisitos	Comportamento do sistema
CATEGORIA B (consulte a Observação 1) Peças da máquina com relação a segurança de controle de máquinas e/ou seus equipamentos de proteção, tal como seus componentes, deverão ser projetados, construídos, selecionados, montados e combinados de acordo com os padrões pertinentes, para que possam resistir à influência esperada. Princípios básicos de segurança devem ser aplicados.	Quando ocorrer uma falha, ela pode levar a uma perda da função de segurança.
CATEGORIA 1 Os requisitos da categoria B se aplicam juntamente com o uso de componentes de segurança bem testados e com os princípios de segurança.	Como o descrito para a categoria B, mas com mais alta confiabilidade relacionada à segurança da função de segurança. (Quanto maior a confiabilidade, menor a probabilidade de uma falha).
CATEGORIA 2 Aplicam-se os requisitos da categoria B e o uso de componentes de segurança bem testados. As funções de segurança deverão ser verificadas pelo sistema de controle da máquina na partida e periodicamente. Se for detectada uma falha, deverá ser iniciado um estado seguro ou, se este não for possível, deverá ser dada uma advertência. O EN ISO 13849-1 presume que a taxa de teste seja pelo menos 100 vezes mais frequente que a taxa de demanda. O EN ISO 13849-1 presume que o MTTFd do equipamento de testes externo seja superior à metade do MTTFd do equipamento funcional sendo testado.	A perda da função de segurança é detectada pela verificação. A ocorrência de uma falha pode levar a perda da função de segurança entre os intervalos de verificação.
CATEGORIA 3 (consulte as observações 2 e 3) Aplicam-se os requisitos da categoria B e o uso de componentes de segurança bem testados. O sistema deverá ser projetado de tal forma que uma falha única em qualquer de suas partes não leve à perda da função de segurança. Onde praticável, uma falha única deverá ser detectada.	Quando ocorre a falha única, a função de segurança é sempre executada. Serão detectadas algumas falhas, mas não todas. O acúmulo de falhas não detectadas pode levar à perda da função de segurança.
Categoria 4 (consulte as observações 2 e 3) Aplicam-se os requisitos da categoria B e o uso de componentes de segurança bem testados. O sistema deverá ser projetado de tal forma que uma falha única em qualquer de suas partes não leve à perda da função de segurança. A falha simples é detectada na próxima solicitação da função de segurança ou antes. Se esta detecção não for possível, um acúmulo de falhas não deverá levar à perda da função de segurança.	Quando as falhas ocorrem, a função de segurança é sempre executada. As falhas serão detectadas em tempo de evitar a perda das funções de segurança.

Categoria B

A categoria B fornece os requisitos básicos de qualquer sistema de controle, seja um sistema de controle relacionado à segurança ou não. Um sistema de controle deve trabalhar em seu ambiente esperado. O conceito de confiabilidade fornece uma base para o controle de sistemas, como a confiança sendo definida como a probabilidade de um dispositivo realizar sua função pretendida durante um intervalo especificado sob condições esperadas.

A categoria B exige a aplicação de princípios básicos de segurança. O ISO 13849-2 nos fala sobre os princípios básicos de segurança para os sistemas elétricos, pneumáticos, hidráulicos e mecânicos. Os princípios elétricos são resumidos como segue:

- Seleção, combinação, arranjos, montagem e instalação adequados (ou seja, de acordo com as instruções do fabricante)
- Compatibilidade dos componentes com tensões e correntes
- Resistência às condições ambientais
- Uso do princípio da desenergização
- Supressão de transientes
- Redução do tempo de resposta
- Proteção contra partida inesperada
- Fixação segura de dispositivos de entrada (por exemplo, a montagem de intertravamentos)
- Proteção do circuito de controle (de acordo com o NFPA79 e o IEC60204-1)
- Ligação de proteção correta

O projetista deve selecionar, instalar e montar de acordo com as instruções do fabricante. Estes dispositivos devem funcionar dentro da tensão e corrente nominais esperadas. As condições ambientais esperadas, como a compatibilidade eletromagnética, vibração, choque, contaminação, lavagem devem também ser consideradas. O princípio da desenergização é usado. A proteção contra transientes esteja instalada nas bobinas do contator. O motor está protegido contra sobrecargas. A fiação e aterramento atendem aos padrões elétricos apropriados.

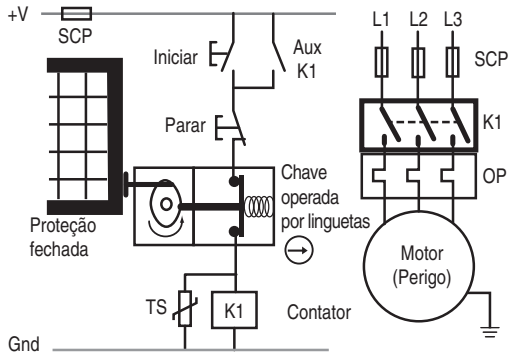
Categoria 1

A categoria 1 exige que o sistema cumpra os termos de categoria B e use os componentes de segurança comprovados. Quais são exatamente os componentes de segurança, e como vamos saber se eles estão bem testados? O ISO 13849-2 ajuda a responder a essas perguntas para equipamentos mecânicos, hidráulicos, pneumáticos e sistemas elétricos. O Anexo D aborda componentes elétricos.

Os componentes são considerados bem testados se forem usados com sucesso em muitas aplicações semelhantes. Os componentes de segurança recentemente concebidos são considerados bem testados se forem projetados e verificados em conformidade com os padrões apropriados.

Componente bem testado	**Padrão**
Chave com modo de atuação positivo (ação de abertura direta)	IEC 60947-5-1
Dispositivo de parada de emergência	ISO 13850, IEC60947-5-5
Fusível	IEC 60269-1
Disjuntor	IEC 60947-2
Contatores	IEC 60947-4-1, IEC 60947-5-1
Contatos ligados mecanicamente	IEC 60947-5-1
Contator auxiliar (por ex., contator, relé de controle, relés guiados positivos)	EN 50205 IEC 60204–1, IEC 60947–5–1
Transformador	IEC 60742
Cabo	IEC 60204-1
Intertravamentos	ISO 14119
Interruptor de temperatura	IEC 60947-5-1
Interruptor de pressão	IEC 60947-5-1 + requisitos pneumáticos ou hidráulicos
Dispositivo ou equipamento de chaveamento de controle e proteção (CPS)	IEC 60947-6-2
Controlador lógico programável	IEC 61508, IEC 62061

Aplicando componentes bem testados em nosso sistema de categoria B, a chave fim de curso seria substituída por uma chave operada por linguetas de abertura direta e o contator seria sobre-dimensionado para maior proteção contra contatos soldados.



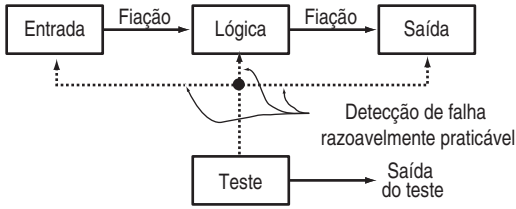
Sistema de segurança de categoria 1 simples

Aqui estão mostradas as mudanças no sistema simples de categoria B para obter a categoria 1. O intertravamento e o contator são os elementos principais na remoção da energia do atuador, quando for necessário o acesso ao perigo. A lingueta intertravada atende aos requisitos do padrão IEC 60947-5-1 para contatos de ação de abertura direta, o que é demonstrado pelo símbolo da seta dentro do círculo. Com os componentes bem testados, a probabilidade de a energia ser removida é maior para a categoria 1 do que para a categoria B. O uso de componentes bem testados destina-se a prevenir a perda da função de segurança. Mesmo com estas melhorias, uma única falha ainda poderia levar à perda da função de segurança..

As categorias B e 1 baseiam-se na prevenção. O projeto se destina a evitar uma situação perigosa. Quando a prevenção por si só não fornecer o suficiente em redução no risco, a detecção de falhas deve ser usada. As categorias 2, 3 e 4 têm como base a detecção de falhas, com exigências cada vez mais rigorosas para alcançar níveis mais altos de redução de risco.

Categoria 2

Além de atender os requisitos da categoria B e utilizar os princípios de segurança bem testados, o sistema de segurança deve ser submetido a testes para atender à categoria 2. Os testes devem ser concebidos para detectar falhas nas peças de segurança relacionadas ao sistema de controle. Se não forem detectadas falhas, a máquina poderá funcionar. Se forem detectadas falhas, o teste deve iniciar um comando. Sempre que possível, o comando deve trazer a máquina para um estado seguro.



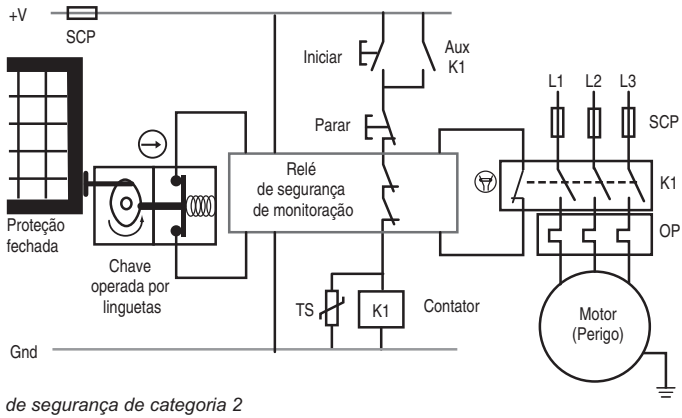
O teste deve fornecer uma detecção razoavelmente prática de falhas. O equipamento fazendo um teste pode ser uma parte integrante do sistema de segurança ou uma peça do equipamento.

O teste deve ser realizado:

- quando a máquina for energizada inicialmente,
- antes do início de um perigo, e
- periodicamente, se julgado necessário na avaliação de risco.

Observação: o EN ISO 138.491-1 assume um função de teste de segurança de demanda por razão de 100:1. O exemplo dado aqui não atende a essa exigência.

As palavras “sempre que possível” e “praticamente razoável” indicam que nem todas as falhas são detectáveis. Como este é um sistema de canal único (ou seja, um fio conecta a entrada até a lógica e à saída), uma única falha pode levar à perda da função de segurança. Em alguns casos, a categoria 2 não pode ser totalmente aplicada a um sistema de segurança, já que nem todos os componentes podem ser verificados.

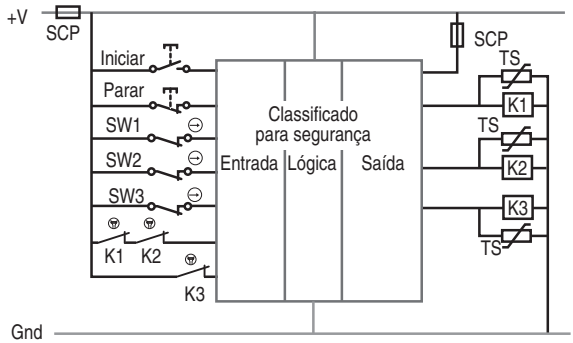


Sistema de segurança de categoria 2

Temos aqui um simples sistema da categoria 1 aprimorado para atender à categoria 2. Um relé de segurança de monitoração (MSR) realiza o teste. Na energização, o MSR verifica seus componentes internos. Se não forem detectados defeitos, o MSR verifica a chave operada por linguetas através da monitoração do ciclo de liga/desliga dos seus contatos. Se nenhuma falha for detectada e a proteção estiver fechada, o MSR verifica o dispositivo de saída: os contatos ligados mecanicamente do contator. Se nenhuma falha for detectada e o contator estiver desligado, o MSR vai energizar sua saída interna e conectar a bobina de K1 para o botão PARADA. Neste ponto, as peças de controle da máquina sem classificação de segurança, o circuito de Partida/Parada/Intertravamento, podem ligar ou desligar a máquina.

Abrir a proteção desliga as saídas do MSR. Quando a proteção é fechada novamente, o MSR repete as verificações do sistema de segurança. Se nenhuma falha for descoberta, o MSR ligará sua saída interna. O MSR permite que este circuito cumpra a categoria 2 fazendo testes no dispositivo de entrada, no dispositivo lógico (ele próprio) e no dispositivo de saída. O teste é realizado na energização inicial e antes do início do perigo.

Com suas capacidades lógicas inerentes, um sistema de segurança baseado em CLP pode ser projetado para atender à categoria 2. Como indicado na categoria 1 discutida acima, a justificativa de “bem testado” do CLP (incluindo suas capacidades de teste) tornam-se o desafio. Para os sistemas de segurança complexos que exigem a classificação de Categoria 2, um CLP de segurança classificado no padrão IEC 61508 deve ser o substituto de um CLP sem classificação de segurança.



Sistema de segurança de categoria 2 complexo

Temos aqui um exemplo de um sistema complexo usando um CLP com classificação de segurança. Um CLP classificado para segurança atende aos requisitos de "bem testado", já que foi projetado para um padrão adequado.

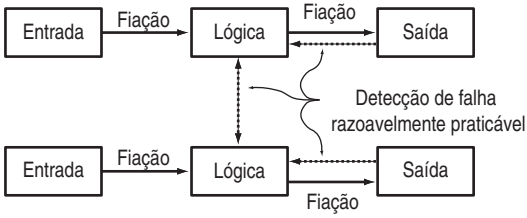
Os contatos ligados mecanicamente dos contatores são alimentados na entrada do CLP para fins de teste. Esses contatos podem ser ligados em série a um terminal de entrada ou aos terminais de entrada individuais, dependendo da lógica do programa.

Embora os componentes de segurança "bem testados" sejam utilizados, uma única falha que ocorra entre as verificações pode levar à perda da função de segurança. Desta forma, os sistemas da categoria 2 são usados em aplicações de menor risco. Quando altos níveis de tolerância a falhas são necessários, o sistema de segurança deve atender às categorias 3 ou 4.

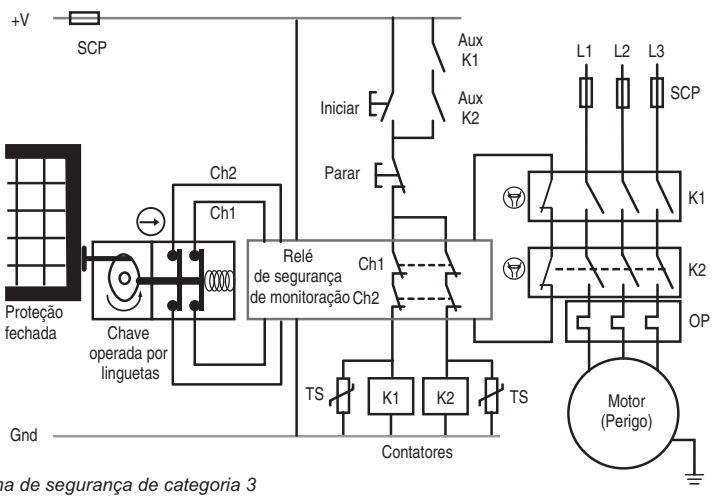
Categoria 3

Além de atender aos requisitos da categoria B e princípios de segurança comprovados, a categoria 3 requer bom desempenho da função de segurança na presença de uma única falha. A falha deve ser detectada antes ou durante a próxima demanda na função de segurança, sempre que razoavelmente praticável.

Aqui, novamente, temos a frase "sempre que razoavelmente praticável". Isto abrange as falhas que não podem ser detectadas. Enquanto a falha indetectável não levar à perda da função de segurança, a função de segurança pode atender à categoria 3. Por consequência, uma acumulação de falhas indetectáveis pode levar à perda da função de segurança.



Aqui temos um diagrama de blocos para explicar os princípios de um sistema de categoria 3. A redundância combinada com monitoramento cruzado razoavelmente prático e monitoração de saída são usados para garantir o desempenho da função de segurança.



Sistema de segurança de categoria 3

Aqui temos um exemplo de um sistema de categoria 3. Um conjunto redundante de contatos é adicionado à chave de intertravamento da lingueta. Internamente, o relé de segurança de monitoração (MSR) contém circuitos redundantes que monitoram um ao outro. Um conjunto redundante de contatores desliga o motor. Os contatores são monitorados pelo MSR através dos contatos ligados mecanicamente “razoavelmente praticáveis”.

A detecção de falha deve ser considerada para cada peça do sistema de segurança, tal como as ligações (isto é, o sistema). Quais são os modos de falha de uma chave da lingueta de canal duplo? Quais são os modos de falha do MSR? Quais são os modos de falha dos contatores K1 e K2? Quais são os modos de falha da fiação?

A chave de intertravamento da lingueta é projetada com contatos de abertura diretos. Portanto, sabemos que abrir a proteção destina-se a abrir um contato soldado. Isso resolve um modo de falha. Existem outros modos de falha?

O interruptor de ação de abertura direta é geralmente projetado com uma mola de retorno. Se o cabeçote for removido ou quebrado, a mola dos contatos de segurança retorna ao estado fechado (seguro). Muitas chaves de intertravamento são projetadas com cabeçotes removíveis para acomodar os requisitos de várias aplicações de instalação. O cabeçote pode ser removido e rodado entre duas a quatro posições.

Uma falha pode ocorrer quando os parafusos de fixação do cabeçote não estiverem apertados corretamente. Com esta condição, a vibração esperada da máquina pode fazer com que o parafusos de fixação do cabeçote afrouxem-se. O cabeçote

de operação, sob a pressão da mola, remove a pressão dos contatos de segurança e os contatos de segurança são fechados. Posteriormente, abrir proteção não abre os contatos de segurança e uma falha perigosa ocorre.

Da mesma forma, o mecanismo de funcionamento do interruptor deve ser revisto. Qual é a probabilidade de que uma falha de um único componente irá levar à perda da função de segurança? Uma prática comum é a utilização do intertravamento de linguetas com contatos duplos em circuitos de categoria 3. Este uso deve ser baseado na exclusão de uma única falha do interruptor para abrir os contatos de segurança. Isto é considerado como “exclusão de falha” e será discutido mais tarde neste capítulo.

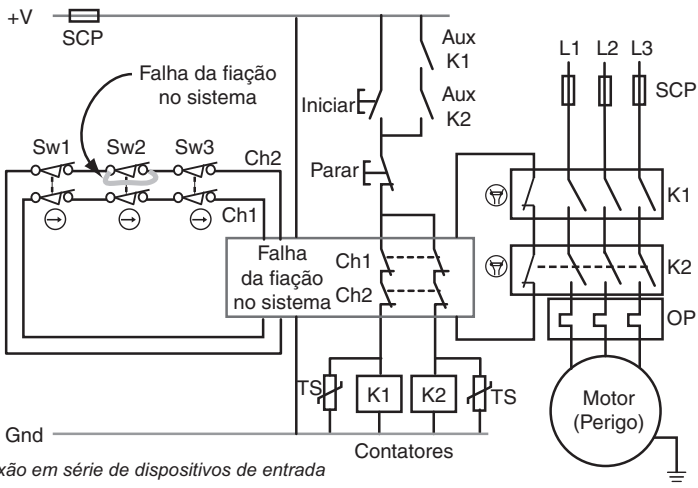
Um relé de segurança de monitoração (MSR) é frequentemente avaliado por um terceiro e recebe um nível de categoria (e/ou um PL e SIL CL). O MSR frequentemente inclui a capacidade de canal duplo, monitoração de vários canais, monitoração de dispositivo externo e de proteção contra curto-circuito. Não há padrões específicos registrados para fornecer orientações sobre o projeto ou uso de relés de monitoração de segurança. Os MSRs são avaliados quanto à sua capacidade de desempenhar a função de segurança de acordo com EN ISO 13849-1 ou com o EN 954-1. A avaliação do MSR deve ser a mesma ou maior do que a classificação necessária ao sistema em que é usado.

Dois contatores ajudam a garantir que a função de segurança seja cumprida pelos dispositivos de saída. Com proteção contra sobrecarga e curto-circuito, a probabilidade de falha do contator pela solda dos contatos é pequena, mas não impossível. Um contator também pode falhar devido a seus contatos de comutação de energia sendo fechados devido a uma armadura presa. Se um contator falhar para um estado perigoso, o segundo contator irá desligar o perigo. O MSR detectará o contator com falha no próximo ciclo da máquina. Quando a porta é fechada e o botão PARTIDA é pressionado, os contatos ligados mecanicamente do contator com falha permanecerão abertos e o MSR não será capaz de fechar os contatos de segurança, assim, revelando a falha.

Falhas não detectadas

Com uma estrutura do sistema de categoria 3, pode haver algumas falhas que não podem ser detectadas, mas que não devem, por si só, levar à perda da função de segurança.

Onde falhas podem ser detectadas precisamos saber se, em algumas circunstâncias, elas poderiam ser mascaradas ou involuntariamente removidas pela operação de outros dispositivos dentro da estrutura do sistema.



Conexão em série de dispositivos de entrada

Aqui temos uma abordagem amplamente utilizada para conectar múltiplos dispositivos a um relé de segurança de monitoração. Cada dispositivo contém dois contatos de ação de abertura direta normalmente fechados. Estes dispositivos podem ser uma mistura de intertravamentos ou botões de parada de emergência. Este abordagem economiza custos com fiação, já que os dispositivos de entrada são ligados em cadeia. Assumindo que uma falha de curto-circuito ocorra em um dos contatos no Sw2 como mostrado. Esta falha pode ser detectada?

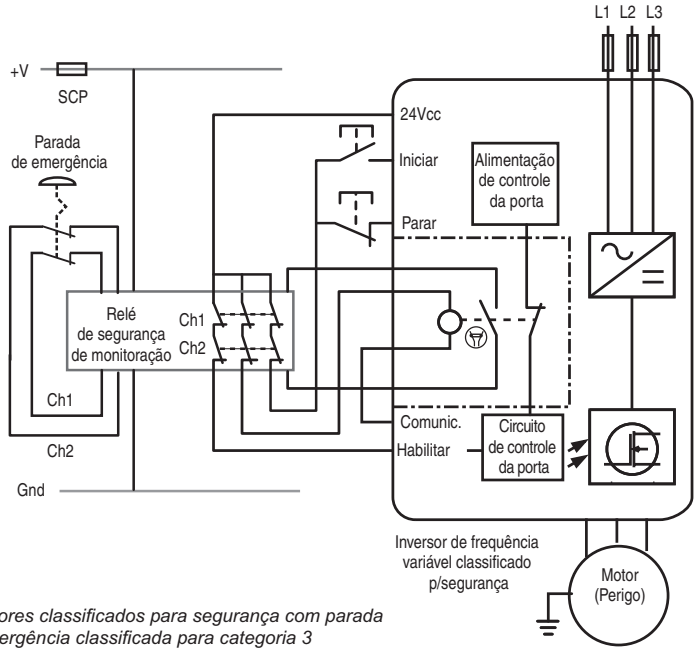
Se Sw1 (ou Sw3) for aberto, tanto Ch1 quanto Ch2 estão com circuito aberto e o MSR desliga o perigo. Se Sw3 abrir e depois fechar de novo, a falha em seus contatos não será detectada porque não há nenhuma mudança de status no MSR: tanto Ch1 quanto Ch2 continuam abertos. Se Sw1 (ou Sw3) for fechado, o perigo pode ser reiniciado ao pressionar o botão PARTIDA. Sob estas circunstâncias, a falha não causou uma perda da função de segurança, mas não foi detectada, permanece no sistema e uma falta subsequente (um curto-circuito entre o segundo contato de Sw2) pode conduzir à perda da função de segurança.

Se o Sw2 só foi aberto e fechado, sem funcionamento das outras chaves, o Ch1 abre e o Ch2 permanece fechado. O MSR desliga o perigo porque Ch1 foi aberto. Quando o Sw2 fecha, o motor não pode ser ligado quando o botão PARTIDA é pressionado, já que Ch2 não foi aberto. A falha é detectada. No entanto, se, por qualquer razão, o Sw1 (ou Sw3) for então aberto e fechado, tanto Ch1 quanto Ch2 terão circuito aberto e depois fechado. Esta sequência simula a remoção da falha e resultará em reset não intencional do MSR.

Isto levanta a questão de que a DC poderia ser reivindicada para as chaves individuais dentro desta estrutura ao usar o EN ISO 13849-1 e IEC 62061. No momento da publicação deste texto, não há nenhuma orientação definitiva específica sobre isso, mas é normal e razoável supor uma DC de 60% sob a condição de que os interruptores sejam testados individualmente em períodos adequados para revelar falhas. Se for previsível que uma (ou mais) das chaves nunca serão testadas individualmente, em seguida, pode-se argumentar que sua DC deve ser descrita como zero. No momento da publicação deste texto, o EN ISO 13849-2 está em fase de revisão. Quando for publicada, poderá fornecer mais orientações sobre esta questão.

A ligação em série de contatos mecânicos é limitada à categoria 3, uma vez que podem conduzir à perda da função de segurança, devido a uma acumulação de erros. Em termos práticos, a redução da DC (e, por conseguinte, FFS) limitaria o máximo alcançável de PL e SIL para PLd e SIL2.

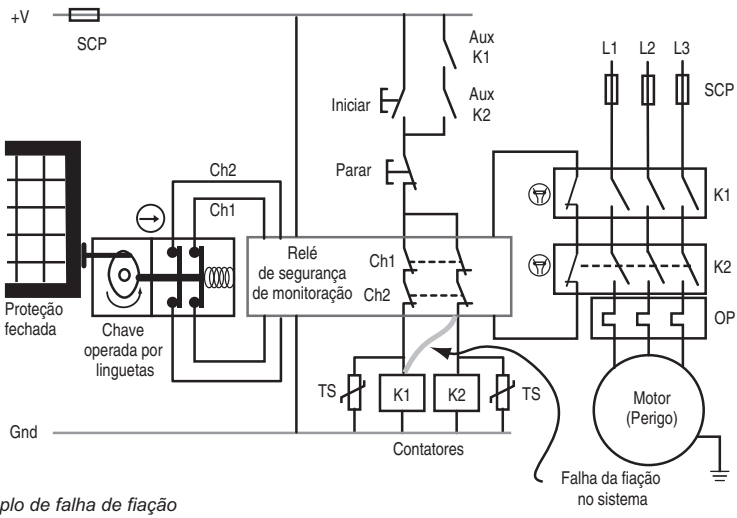
É interessante notar que essas características de uma estrutura de categoria 3 sempre exigiram consideração, mas elas são postas em destaque pelos mais recentes padrões de segurança funcionais.



Inversores classificados para segurança com parada de emergência classificada para categoria 3

Aqui temos um circuito de categoria 3, usando um inversor de frequência classificado para segurança. A evolução da tecnologia do inversor, juntamente com a atualização dos padrões EN/IEC 60204-1 e NFPA79, permitem que a classificação de segurança possa ser utilizada em circuitos de parada de emergência, sem a necessidade de uma desconexão eletromecânica do atuador (por exemplo, o motor).

Pressionar a parada de emergência abre as saídas do MSR. Isto envia um sinal de parada para o inversor, remove o sinal de habilitação e abre a alimentação de controle da porta. O inversor executa uma Parada de categoria 0— para remover imediatamente a energia do motor. Esta função é conhecida como “Desligamento seguro do torque”. O inversor atinge a categoria 3 pois tem sinais redundantes para desligar o motor: a habilitação e um relé guiado positivo. O relé positivo guiado fornece realimentação razoavelmente praticável para o atuador. O próprio inversor é analisado para determinar se uma única falha não conduz à perda da função de segurança.

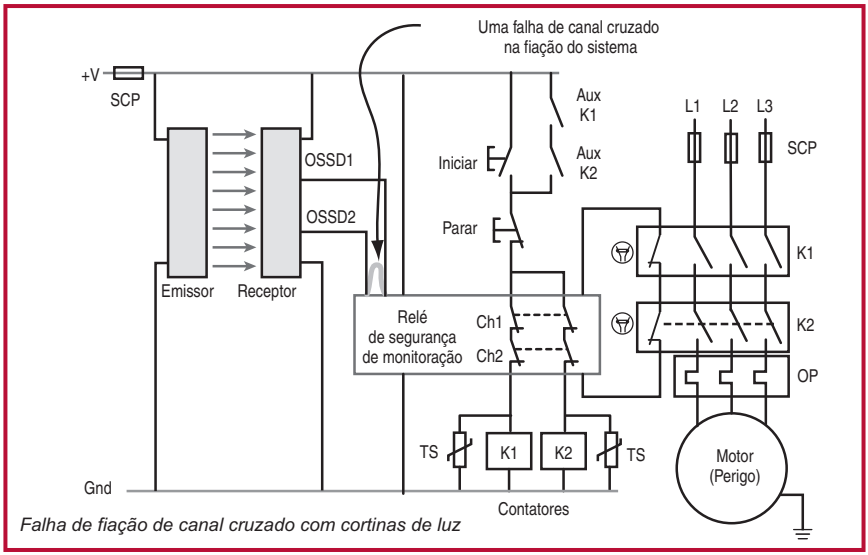


Exemplo de falha de fiação

Temos aqui um exemplo de uma falha na fiação, um curto-circuito, a partir da saída de segurança MSR no Canal 2 da bobina do contator K1. Todos os componentes estão funcionando corretamente. Esta falha na fiação pode ocorrer antes do comissionamento da máquina ou em alguma data posterior durante a manutenção ou aprimoramento.

Esta falha pode ser detectada?

Esta falha não pode ser detectada pelo sistema de segurança, como mostrado. Felizmente ela não pode, por si só, causar a perda da função de segurança. Esta falha, tal como a falha de Ch1 para K2, deve ser detectada durante o comissionamento ou verificação após os trabalhos de manutenção. A lista de possíveis exclusões de falhas indicadas em EN ISO 13849-2, Anexo D, Tabela D4 esclarece que estes tipos de falhas podem ser excluídos se o equipamento estiver contido em um gabinete elétrico e tanto o gabinete quanto a fiação cumprirem os requisitos de IEC/EN 60204-1. O relatório técnico conjunto sobre EN ISO 13849-1 e IEC 62061 também esclarece que esta exclusão de falhas pode ser considerada até PLe e SIL3 (inclusive). Isto também pode ser usado na categoria 4.



Falha de fiação de canal cruzado com cortinas de luz

Aqui temos um sistema de segurança de exemplo, com cortinas de luz (saídas OSSD)

O sistema de segurança pode detectar essa falha?

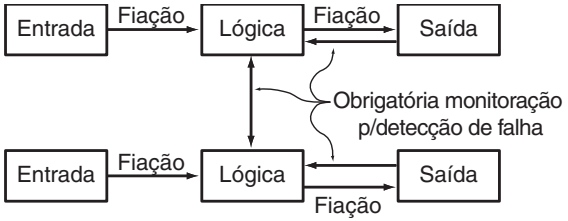
O MSR não consegue detectar esta falha, pois ambas as entradas são puxadas para +V. Neste exemplo, a falha na fiação é detectada pela cortina de luz. Algumas cortinas de luz usam uma técnica de detecção de falhas chamada de teste de pulso. Com essas cortinas de luz, a detecção da falha é imediata, e a cortina de luz desliga sua saída. Em outros, a detecção é feita quando a cortina de luz é apagada. Quando a cortina de luz tenta energizar sua saída, a falha é detectada e a saída permanece desligada. Em ambos os casos, o perigo permanece desligado na presença da falha.

Teste de pulso para detecção de falhas

Os circuitos de segurança são projetados para transportar corrente quando o sistema de segurança estiver ativo e o perigo estiver protegido. O teste de pulso é uma técnica onde a corrente do circuito cai para zero por um período muito curto. A duração é curta demais para o circuito de segurança reagir e desligar o perigo, mas é suficientemente longa para um sistema baseado em microprocessador detectar. Os pulsos nos canais sofrem defasagem um do outro. Se ocorrer um curto-circuito de falha cruzada, o microprocessador detecta os pulsos em ambos os canais e inicia um comando para desligar o perigo.

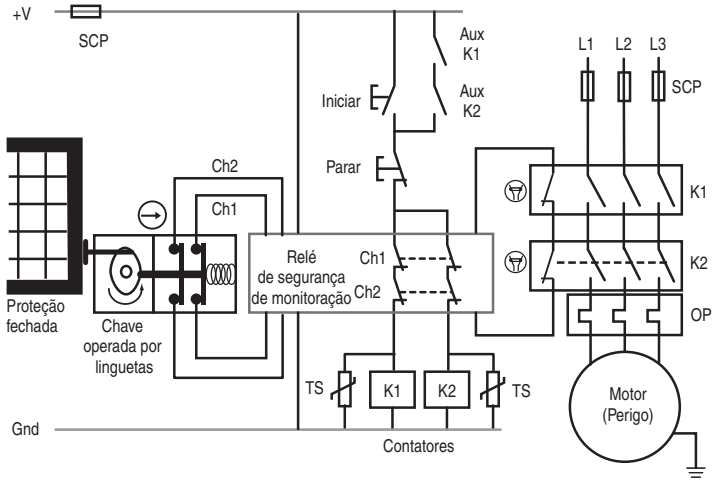
Categoria 4

Como a categoria 3, a categoria 4 exige que o sistema de segurança cumpra a categoria B, utilize princípios de segurança e execute a função de segurança na presença de uma única falha. Diferentemente da categoria 3, onde uma acumulação de falhas pode levar à perda da função de segurança, a categoria 4 exige o desempenho da função de segurança na presença de um acúmulo de falhas. Ao considerar um acúmulo de falhas, duas podem ser suficientes, apesar de três falhas poderem ser necessárias para alguns projetos.



Temos aqui é o diagrama de blocos para a categoria 4. A monitoração de ambos os dispositivos de saída e a monitoração cruzada são essencialmente exigidas, não somente onde razoavelmente praticável.

Isto ajuda a diferenciar a categoria 4 da categoria 3.

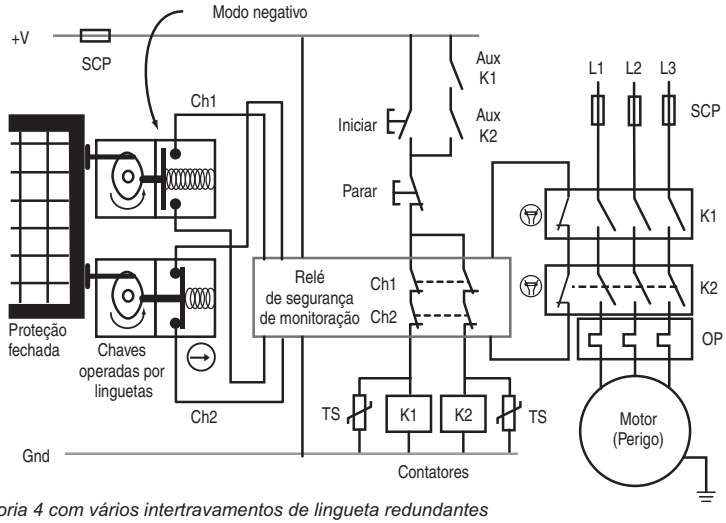


Categoria 4 com exclusão de falha no intertravamento de lingueta

Temos aqui um exemplo de circuito de categoria 4 com exclusão de falha no intertravamento da lingueta. A exclusão de falha elimina a consideração da falha dos contatos com a abertura do intertravamento da lingueta. A exclusão de falha deve ser tecnicamente justificada e documentada. A velocidade do atuador, seu alinhamento, os batentes mecânicos e um cabeçote de operação seguro devem ser considerados na justificativa.

Se o projetista do sistema de segurança preferir usar o intertravamento da lingueta, mas não se sentir confortável com o uso de exclusão de falhas nos intertravamentos, então, dois intertravamentos da lingueta podem ser usados para atender à categoria 4. O relé de segurança de monitoração deve ser dimensionado para atender à categoria 4 e os dois contatores de saída, usando os contatos ligados mecanicamente, devem ser monitorados.

A diversidade pode ser aplicada para reduzir ainda mais a probabilidade de perda da função de segurança devido às falhas de modo comum ou causa comum, uma das chaves de intertravamento da lingueta pode ser convertida para o modo negativo. Uma chave funcionando em modo negativo é aceitável desde que uma segunda chave use contatos de ação de abertura direta. O diagrama a seguir mostra um exemplo desta abordagem diversificada. Com esta abordagem, o MSR deve ser projetado para aceitar entradas normalmente abertas e normalmente fechadas.



Categoria 4 com vários intertravamentos de lingueta redundantes

Classificações de componentes e sistemas

As categorias podem ser usadas como parte das classificações do componente de segurança (dispositivo), bem como as classificações do sistema. Isso gera uma certa confusão que pode ser esclarecida através da compreensão dos componentes e suas capacidades. Ao estudar os exemplos anteriores vemos que o componente assim como uma chave de intertravamento classificada na categoria 1 pode ser usada por si só, em um sistema de categoria 1, e pode ser utilizada num sistema de categoria 2, se a monitoração da função adicional for fornecida. Isto também

pode formar parte de um sistema de categoria 3 ou 4 se dois dos componentes forem usados em conjunto com uma função de diagnóstico fornecida por um relé de segurança de monitoração.

Alguns componentes, como o relé de segurança de monitoração e os controladores de segurança programáveis, têm os seus próprios diagnósticos internos e verificam-se para garantir o desempenho adequado. Assim, eles podem ser classificados como componentes de segurança para atender às categorias 2, 3 ou 4 sem quaisquer medidas adicionais.

Considerações e exclusões de falha

A análise de segurança exige uma extensa análise de falhas e é necessária uma compreensão completa do desempenho do sistema de segurança na presença de falhas. Os ISO 13849-1 e ISO 13849-2 fornecem detalhes sobre considerações e exclusões de falhas.

Se uma falha resultar em uma falha de um componente subsequente, a primeira falha e todas as falhas subsequentes deverão ser consideradas uma falha.

Se duas ou mais falhas ocorrem como resultado de uma única causa, as falhas devem ser considerados uma única falha. Isto é conhecido como uma falha de causa comum.

A ocorrência de duas ou mais falhas ao mesmo tempo é considerada altamente improvável e não é considerada na análise. Há uma suposição básica de que uma única falha pode ocorrer entre as exigências colocadas sobre a função de segurança, desde que o períodos entre o uso da função não sejam excessivamente longos.

Exclusões de falhas

O EN 954-1, e as mais recentes EN ISO 13849-1 e IEC 62061, permitem o uso de exclusões de falhas ao determinar um sistema de classificação de segurança se puder ser demonstrado que a ocorrência da falha é extremamente improvável. É importante que as situações onde as exclusões de falhas forem usadas sejam devidamente fundamentadas e válidas pela vida útil esperada do sistema de segurança. Quanto maior o nível de risco protegido pelo sistema de segurança, mais rigorosa a justificativa exigida para a exclusão de falha. Isto sempre causou certa confusão sobre quando certos tipos de exclusão de falha podem ou não ser usados. Como já vimos neste capítulo, os padrões mais recentes e documentos de orientação esclareceram alguns aspectos desta questão.

Em geral, quando PLe ou SIL3 são especificados para uma função de segurança a ser implementada por um sistema de segurança, não é normal basear-se apenas nas exclusões de falha para a obtenção deste nível de desempenho. Isso depende da tecnologia usada e do ambiente operacional pretendido. Portanto, é essencial que o projetista tenha cuidado adicional sobre o uso de exclusões de falhas na medida

em que PL ou SIL aumentam. Por exemplo, as exclusões de falhas não são aplicáveis aos aspectos mecânicos das chaves de posição eletromecânicas e chaves manualmente operadas (por exemplo, um dispositivo de parada de emergência) para obter um sistema PLe ou SIL3. As exclusões de falha que podem ser aplicadas às condições específicas de falhas mecânicas (por exemplo, o desgaste/corrosão, fratura) estão descritas na Tabela A.4 do ISO 13849-2. Portanto, um sistema de intertravamento de proteção que deva alcançar PLe ou SIL3 precisará incorporar uma tolerância mínima a falhas de 1 (por exemplo, duas chaves de posição mecânica convencionais), para alcançar este nível de desempenho, uma vez que normalmente não é justificável excluir falhas de atuadores de comutação quebrados. No entanto, pode ser aceitável excluir falhas, como curto-circuito de fiação dentro de um painel de controle designado de acordo com os padrões relevantes.

Mais informações sobre o uso de exclusões de falhas serão fornecidas na próxima revisão do padrão EN ISO 13849-2.

Categorias de parada de acordo com IEC/EN 60204-1 e NFPA 79

É tanto infeliz quanto confuso que o termo “Categoria” em relação aos sistemas de controle relacionados à segurança tenha dois significados diferentes. Até agora discutimos as categorias que foram originadas no EN 954-1. Elas são uma classificação do desempenho de um sistema de segurança sob condições de falhas.

Há também uma classificação conhecida como “Categorias de parada” que se originou no IEC/EN 60204-1 e NFPA 79. Existem três categorias de parada.

A categoria de parada 0 requer a remoção imediata da energia dos atuadores. Isso às vezes é considerado como uma parada descontrolada porque, em algumas circunstâncias, o movimento pode levar algum tempo para cessar, já que o motor pode ficar livre para parar por inércia.

A categoria de parada 1 requer que a energia seja retida para aplicar a frenagem até que a parada seja atingida e então o atuador seja desligado.

A categoria de parada 2 permite que a energia não seja removida do atuador.

Observe que somente as categorias de parada 0 ou 1 podem ser usadas como paradas de emergência. A escolha de qual das duas categorias utilizar deve ser ditada por uma avaliação de risco.

Todos os exemplos de circuitos mostrados até agora neste capítulo usaram uma categoria de parada 0. Uma categoria de parada 1 é atingida com uma saída com atraso de tempo para uma remoção final de energia. Uma proteção intertravada com trava frequentemente acompanha um sistema de parada de categoria 1. Isto mantém a proteção trancada e fechada até que a máquina atinja um estado seguro (ou seja, parado).

Parar uma máquina sem levar em consideração o controlador programável pode afetar o rearme e resultar em danos graves à ferramenta e à máquina. Um CLP padrão (inseguro) não pode ser responsável sozinho por uma tarefa relacionada a uma parada de segurança; portanto, outras abordagens precisam ser consideradas.

Duas soluções possíveis são dadas abaixo:

1. Relé de segurança com comando de supressão de atraso de tempo

É usado um relé de segurança com saídas de ação imediata e de ação com retardo. As saídas de atuação imediata estão ligadas às entradas no dispositivo programável (por exemplo, CLP) e as saídas com ação com atraso são ligadas ao contator. Quando a chave de proteção de intertravamento é acionada, as saídas imediatas no relé de segurança são chaveadas. Isso sinaliza o sistema programável para realizar uma parada corretamente sequenciada. Após um tempo curto, porém suficiente, ter transcorrido para permitir este processo, a saída com atraso do relé de segurança é chaveada e isola o contator principal.

Observação: Quaisquer cálculos para determinar o tempo de parada total devem levar o período do atraso de saída do relé de segurança em conta. Isto é particularmente importante ao usar este fator para determinar o posicionamento dos dispositivos de acordo com o cálculo da distância segura.

2. CLPs de segurança

As funções de tempo e lógica requeridas podem ser convenientemente implementadas através do uso de um CLP (de segurança) com um nível de integridade de segurança apropriado. Na prática, isto seria alcançado pelo uso de um CLP de segurança como o SmartGuard ou GuardLogix.

Requisitos dos EUA para sistemas de controle

Nos EUA, os requisitos para os sistemas de controle relacionados à segurança podem ser encontrados em vários padrões diferentes, mas dois documentos destacam-se: ANSI B11.TR3 e ANSI R15.06. O relatório técnico ANSI B11.TR3 estabelece quatro níveis caracterizados pela quantidade prevista de redução do risco que cada um pode oferecer. Os requisitos para cada nível seguem:

Redução de risco no grau mais baixo

No ANSI B11.TR3, as proteções que proporcionam menor grau de redução de risco incluem dispositivos elétricos, hidráulicos ou pneumáticos e sistemas de controle associados, utilizando uma configuração de canal único. Implícita nos requisitos está a exigência de utilização de dispositivos com classificação de segurança. Isto está estreitamente alinhado com a categoria 1 do ISO13849-1.

Redução de risco baixa/intermediária

As proteções no ANSI B11.TR3 que proporcionam redução de riscos baixa/intermediária incluem sistemas de controle com redundância que podem ser verificados manualmente para garantir o desempenho do sistema de segurança. Olhando para os requisitos puros, o sistema emprega redundância simples. O uso de uma função de verificação não é necessário. Sem a verificação, um dos componentes de segurança redundantes pode falhar e o sistema de segurança não perceber isso. Isso resultaria em um sistema de canal único. Este nível de redução de risco alinha-se melhor com a categoria 2, quando a verificação é usada.

Redução de risco alta/intermediária

As proteções proporcionando redução de risco alta/intermediária no ANSI B11.TR3 incluem sistemas de controle tendo redundância com autoverificação na inicialização para confirmar o desempenho do sistema de segurança. Para máquinas que são ligadas todos os dias, o autocontrole proporciona uma melhora significativa na integridade da segurança sobre o sistema puramente redundante. Para máquinas ligadas 24 horas por dia, a autoverificação é uma melhora marginal, na melhor das hipóteses. Empregar monitoração periódica do sistema de segurança alinha-se com as exigências da categoria 3.

Redução de risco no grau mais alto

ANSI B11.TR3 proporciona uma redução maior de risco através de sistemas de controle redundantes e com autoverificação contínua. A autoverificação deve verificar o desempenho do sistema de segurança. O desafio para o projetista do sistema de segurança é determinar o que é contínuo. Muitos sistemas de segurança efetuam os controles na inicialização e quando a demanda é colocada sobre o sistema de segurança.

Alguns componentes, por outro lado, realizam autoverificação contínua. Cortinas de luz, por exemplo, sequencialmente ligam e desligam seus LEDs. Se ocorrer uma falha, a cortina de luz desliga suas saídas antes que uma demanda seja colocada no sistema de segurança, já que ela verifica a si mesma continuamente. Os relés com base em microprocessador e os CLPs de segurança são outros componentes que executam autoverificação contínua.

O requisito do sistema de controle para autoverificação “contínua” não destina-se a limitar a seleção de componentes a cortinas de luz e unidade de lógica baseadas em microprocessador. A verificação deve ser feita na inicialização e depois de cada demanda ao sistema de segurança. Este nível de redução de risco destina-se ao alinhamento com a categoria de 4 do ISO13849-1.

Padrões para robôs: EUA e Canadá

Os padrões para robôs nos EUA (ANSI RIA R15.06) e Canadá (CSA Z434-03) são muito similares. Ambos têm quatro níveis, os quais são semelhantes às categorias do EN954-1:1996 e que são descritos abaixo.

Simples

Neste nível mais baixo, os sistemas de controle simples de segurança devem ser concebidos e construídos com circuitos aceitos de canal único; esses sistemas podem ser programáveis. No Canadá, este nível é ainda mais restrito para fins de sinalização e anúncio apenas. O desafio para o projetista do sistema de segurança é determinar o que é "aceito". O que é um circuito de canal único aceito? Para quem o sistema é aceitável? A categoria simples é a mais próxima da categoria B do EN954-1:1996.

Canal único

O próximo nível é um sistema de controle de segurança de um canal único que:

- É baseado em hardware ou é um dispositivo de software/firmware classificado para segurança;
- Inclui componentes classificados para segurança; e
- É usado de acordo com as recomendações dos fabricantes; e
- Utiliza projetos de circuitos comprovados.

Um exemplo de um projeto de circuito comprovado é um dispositivo de ruptura positiva eletromecânico de canal único que sinaliza uma parada em um estado sem corrente. Sendo um sistema de canal único, a falha de um único componente pode levar à perda da função de segurança. A categoria simples é a mais estreitamente alinhada com a categoria 1 do EN9541:1996.

Dispositivo de software/firmware classificado para segurança

Embora os sistemas baseados em hardware tenham sido o método preferido de fornecer segurança de robôs, os dispositivos de software/firmware estão se tornando uma opção popular devido à sua capacidade de lidar com sistemas complexos. Dispositivos de software/firmware (CLPs ou controladores de segurança) são permitidos, desde que sejam classificados para segurança. Esta classificação exige que a falha de um único componente relacionado à segurança ou firmware não conduza à perda da função de segurança. Quando a falha é detectada, a operação automática subsequente do robô é impedida até que a falha seja eliminada.

Para conseguir uma classificação de segurança, o dispositivo de software/firmware deve ser testado de acordo com um padrao aprovado por um laboratório aprovado. Nos EUA, a OSHA mantém uma lista de laboratórios reconhecidos nacionalmente (NRTL). No Canadá, o Standards Council of Canada (SCC) mantém uma lista similar.

Canal único com monitoração

Sistemas de controle de segurança de canal único com monitoração devem satisfazer os requisitos de um único canal; ter classificação de segurança e utilizar a verificação. A verificação da função de segurança deve ser feita na partida da máquina e periodicamente durante a operação. A verificação automática é preferível à verificação manual.

A operação de verificação permite a operação caso nenhuma falha tenha sido detectada ou gera um sinal de parada se for detectada uma falha. Deve ser fornecida uma advertência se um perigo permanecer após a cessação do movimento. Claro, a própria verificação não deve causar situações de risco. Após detectar a falha, o robô deve permanecer em estado seguro até que a falha seja corrigida. O canal único com monitoração está mais estreitamente alinhado com a categoria 2 do EN954-1:1996

Controle confiável

O maior nível de redução de risco nos padrões para robôs dos EUA e Canadá é alcançado por sistemas de controle relacionados à segurança que atendam os requisitos de controle confiável. Sistemas de controle relacionados à seguranca com o controle confiável são arquiteturas de canais duplos com monitoração. A função de parada do robô não deve ser evitada por nenhuma falha de um único componente, incluindo a função de monitoração.

A monitoração deve gerar um comando de parada após a detecção de uma falha. Se um perigo continuar após o término do movimento, deve ser emitido um sinal de advertência. O sistema de segurança deve permanecer em um estado seguro até que a falha seja corrigida. De preferência, a falha é detectada no momento em que ocorre. Se isto não puder ser alcançado, então a falha deve ser detectada na próxima demanda do sistema de segurança. As falhas de modo comum devem ser levadas em consideração se existe uma probabilidade significativa de tal falha ocorrer.

Os requisitos canadenses diferem dos americanos pela adição de dois requisitos adicionais. Primeiro, os sistemas de controle relacionados à segurança devem ser independentes dos sistemas normais de controle do programa. Segundo, o sistema de segurança não deve ser facilmente desligado ou contornado sem detecção.

Os sistemas de controle confiáveis alinham-se com as categorias 3 e 4 do EN 954-1:1996.

Comentários sobre o controle confiável

O aspecto mais fundamental de controle confiável é a tolerância a falhas únicas. Os requisitos definem como o sistema de segurança deve responder na presença de “uma falha única”, “qualquer falha única” ou “qualquer falha de um componente único”.

Três conceitos muito importantes devem ser considerados a respeito de falhas: (1) nem todas as falhas são detectadas, (2) adicionar a palavra “componente” levanta dúvidas sobre a fiação e (3) a fiação é uma parte integrante do sistema de segurança. Falhas na fiação podem resultar na perda de uma função de segurança.

A intenção da confiabilidade de controle é claramente o desempenho da função de segurança na presença de uma falha. Se a falha for detectada, então o sistema de segurança deve executar uma ação de segurança, fornecer notificação da falha e impedir a operação da máquina até que a falha seja corrigida. Se a falha não for detectada, a função de segurança ainda deve ser realizada sob demanda.

Exemplo de aplicação usando SISTEMA

Este exemplo de aplicação ilustrará como conectar, configurar e programar um PAC Compact GuardLogix e a E/S PointGuard para monitorar um sistema de segurança de duas zonas. Cada zona consiste em uma única chave de segurança de intertravamento que, quando acionada, sinaliza a remoção da energia de um par de contatores redundantes para essa zona. Isto é duplicado na segunda zona. Ambas as zonas também são protegidas por uma parada de emergência global que, em atuação, sinaliza o fechamento de ambas as zonas com segurança.

OBSERVAÇÃO: Este exemplo é apenas para fins ilustrativos. Devido às muitas variáveis e requisitos associados a qualquer instalação particular, a Rockwell Automation não assume a responsabilidade pelo uso real com base neste exemplo.

Recursos e benefícios

- O Compact GuardLogix permite que tanto as aplicações padrão como as de segurança sejam executadas em um único controlador.
- As E/S padrão e de segurança podem ser misturadas em um único adaptador Ethernet.
- O status de segurança e diagnóstico pode ser facilmente passado da aplicação de segurança para a aplicação padrão, para exibição em IHM e passada remotamente para dispositivos adicionais via Ethernet.
- A aplicação descrita aqui pode ser ampliada e incorporada em uma aplicação de cliente.

Descrição

Esta aplicação monitora duas zonas. Cada zona é protegida por um interruptor de segurança SensaGuard. Se qualquer dos portões estiver aberto, os contatores de saída serão desenergizados, desligando qualquer equipamento associado àquela zona. O reset é manual. Ambas as zonas também são protegidas por uma chave de parada de emergência global. Se a parada de emergência for acionada, ambos os conjuntos de contatores desenergizam-se.

Função de segurança

Cada interruptor de segurança SensaGuard está ligado a um par de entradas de segurança de um módulo 1734-IB8S (E/S POINTGuard). O módulo de E/S é conectado via segurança CIP em uma rede EtherNet/IP ao controlador de segurança Compact GuardLogix (1768- L43S). O código de segurança no processador de segurança monitora o estado das entradas de segurança, usando uma instrução de segurança pré-certificada chamada Parada de Entrada de Canal Duplo (DCS). O código de segurança é executado em paralelo com uma configuração de processador 1oo2. Quando todas as condições estão satisfeitas, o gate de segurança

está fechado, nenhuma falha detectada nos módulos de entrada, a parada de emergência global não está acionada e o botão de reset é pressionado, um segundo bloco de funções certificado chamado saída configurável redundante (CROUT) verifica o status dos dispositivos de controle finais, um par de contatores redundantes 100S. O controlador então emite um sinal de saída para o módulo 1734-OBS para LIGAR um par de saídas para energizar os contatores de segurança. A função de parada de emergência global também é monitorada por uma instrução DCS. Caso a parada de emergência global seja acionada, ela desativa ambas as zonas.

Lista de materiais

Este exemplo de aplicação usa esses componentes.

Código de catálogo	Descrição	Quantidade
440N-Z21SS2A	Chave SensaGuard Plástico sem contato RFP	2
800FM-G611MX10	Botão de reset 800F, metálico, com proteção, azul, R, montagem com trava metálica, 1 contato NA, padrão	4
100S-C09ZJ23C	Cód. cat. 100S-C - Contatores de segurança	2
1768-ENBT	Módulo ponte EtherNet/IP CompactLogix	1
1768-L43S	Processador CompactLogix L43, 2,0 MB de memória padrão, 0,5 MB de memória de segurança	1
1768-PA3	Fonte de alimentação, entrada de 120/240 Vca, 3,5 A em 24 Vcc	1
1769-ECR	Terminação/terminador direito	1
1734-AENT	Adaptador Ethernet 24 Vcc	1
1734-TB	Módulo base com terminais de parafuso IEC removíveis	4
1734-IB8S	Módulo de entrada de segurança	2
1734-OB8S	Módulo de saída de segurança	1
1783-US05T	Switch Ethernet não gerenciável Stratix 2000	1

Instalação e fiação

Para obter informações detalhadas sobre a instalação e fiação, consulte o manual fornecido com o produto ou faça o download em:
http://literature.rockwellautomation.com

Visão geral do sistema

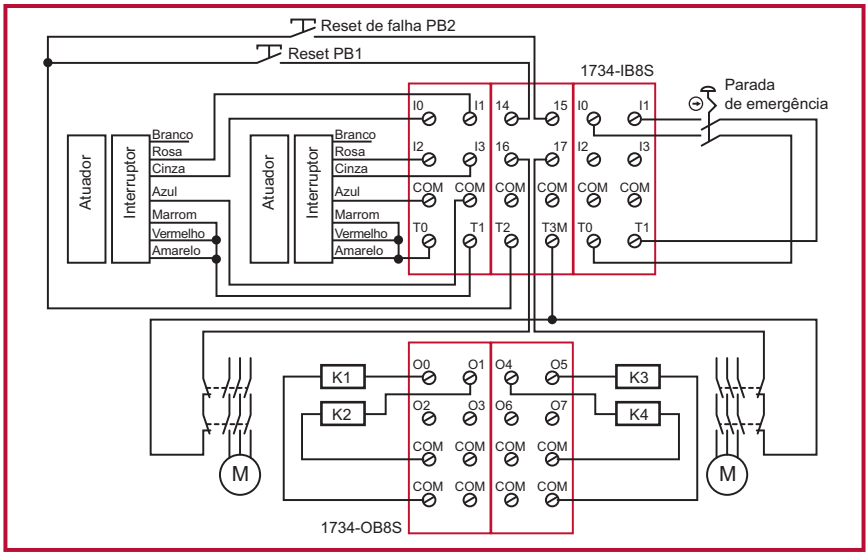
O módulo de entrada 1734-IB8S monitora as entradas de ambas as chaves SensaGuard.

O SensaGuard usa saídas OSSD que realizam testes periódicos das saídas. Assim, são as saídas OSSD que estão testando a integridade da fiação entre o interruptor SensaGuard e as entradas de segurança.

As saídas de teste de pulso estão configuradas como fontes de 24V.

O dispositivo de controle final é um par de contatores de segurança 100S, K1 e K2. Os contatores são controlados pelo módulo de saída de segurança 1734-OBS. Eles são ligados em uma configuração redundante e são testados na partida em busca de falhas. O teste de partida é conseguido por meio do monitoração do circuito de retorno para a entrada 2 (I2), antes de os contatores serem energizados. Isso é feito usando uma instrução de saída redundante configurável (CROUT). O sistema é reinicializado pelo botão momentâneo, PB1.

Fiação



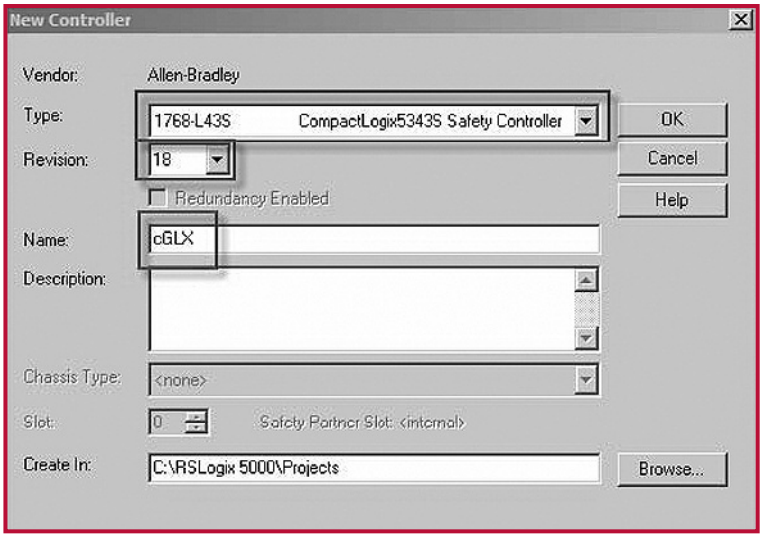
Configuração

O controlador Compact GuardLogix é configurado usando o RSLogix 5000, versão 18 ou posterior. Você deve criar um novo projeto e adicionar os módulos de E/S. Em seguida, configure os módulos de E/S para os tipos de entrada e saída corretos. Uma descrição detalhada de cada etapa vai além do escopo deste documento. Deduz-se que haja conhecimento do ambiente de programação RSLogix.

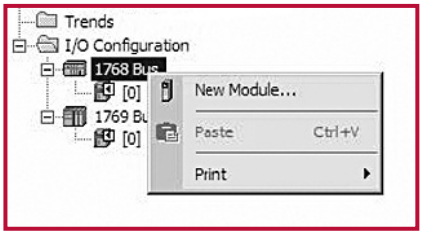
Configure o controlador e adicione módulos de E/S

Siga estes passos.

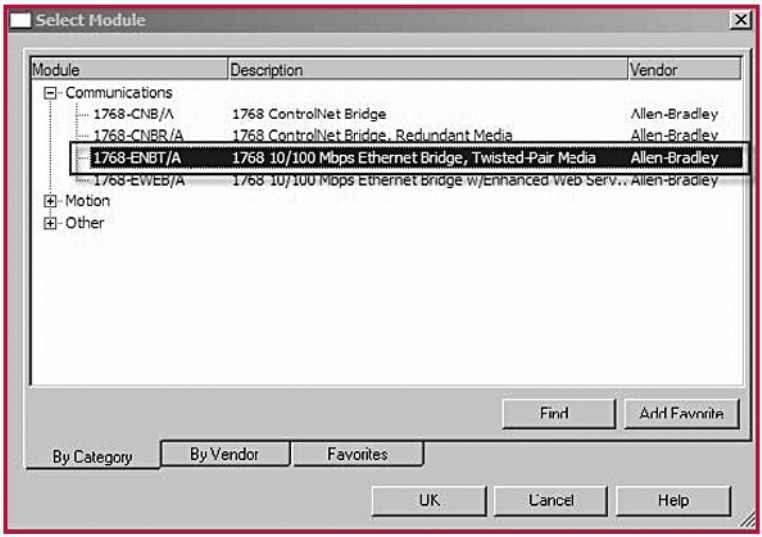
1. No software RSLogix 5000, crie um novo projeto.



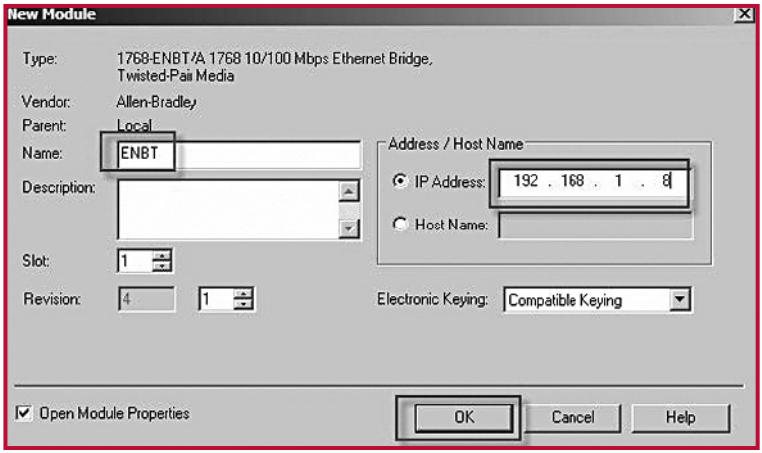
2. No Organizador do controlador, adicione o módulo 1768-ENBT para o barramento 1768.



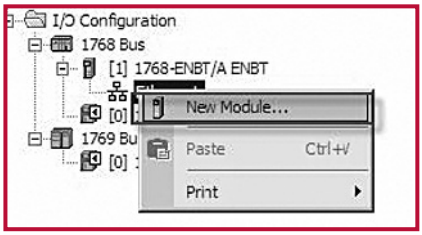
3. Selecione o módulo 1768-ENBT e clique em OK.



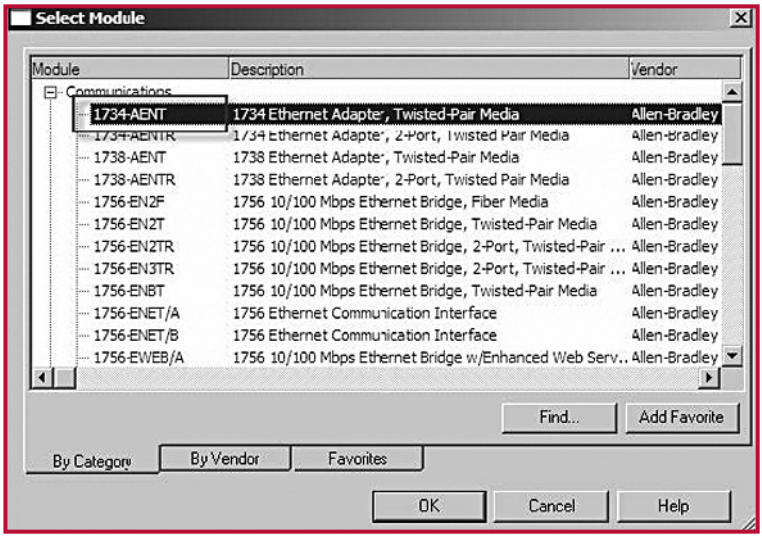
4. Nomeie o módulo, digite o seu endereço IP e clique em OK. Usamos 192.168.1.8 para este exemplo de aplicação. O seu pode ser diferente.



5. Adicione o adaptador 1734-AENT clicando com o botão direito do mouse no módulo 1768-ENBT no organizador do controlador e escolhendo “New Module”.

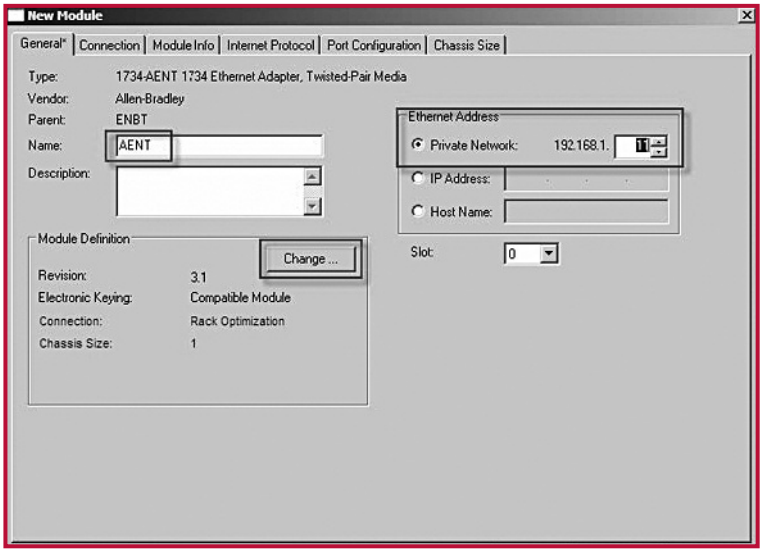


6. Selecione o adaptador 1734-AENT e clique em OK.



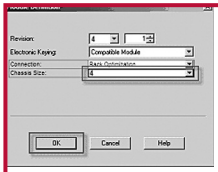
7. Nomeie o módulo, digite o seu endereço IP e clique em OK. Usamos 192.168.1.11 para este exemplo de aplicação. O seu pode ser diferente.

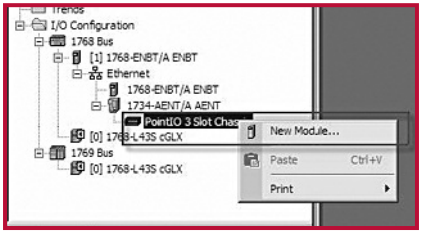
8. Clique em “Change”.



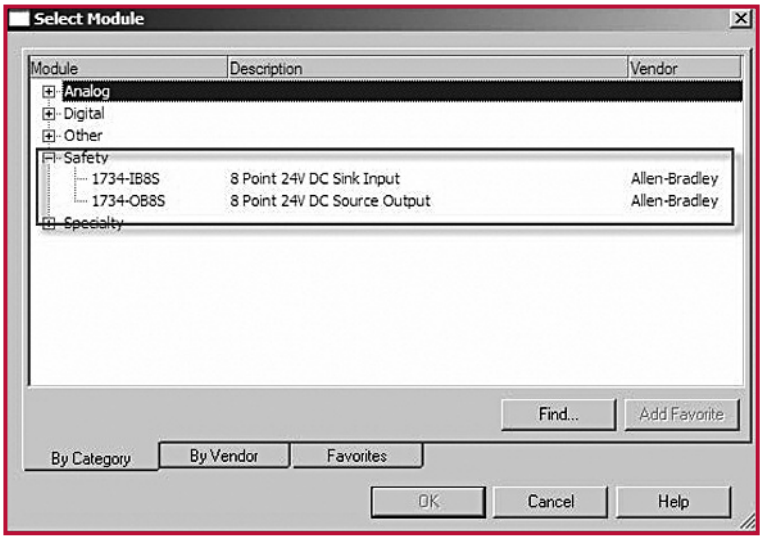
9. Defina o tamanho do chassi como 4 para o adaptador 1734-AENT e clique em OK. O tamanho do chassi é o número de módulos que serão inseridos no chassi. O adaptador 1734-AENT é considerado no slot 0, então para dois módulos de entrada e um módulo de saída, o tamanho do chassi é 4.

10. No organizador do controlador, clique com o botão direito do mouse no adaptador 1734-AENT e selecione “New Module”.

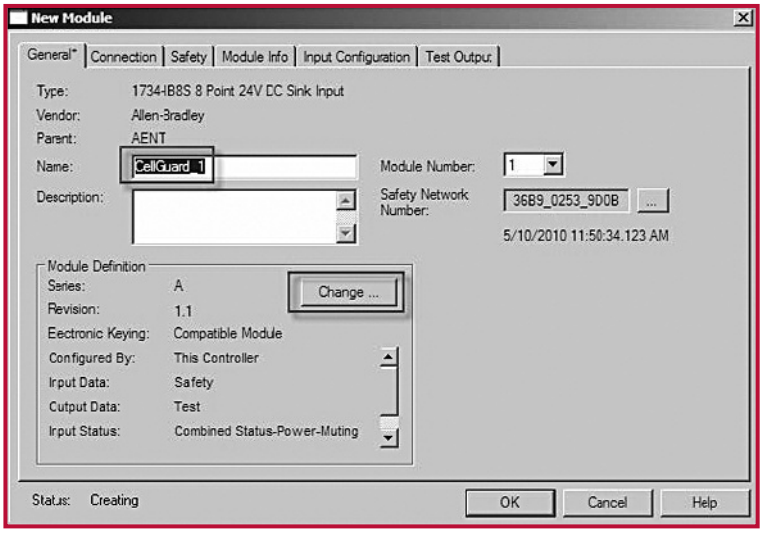




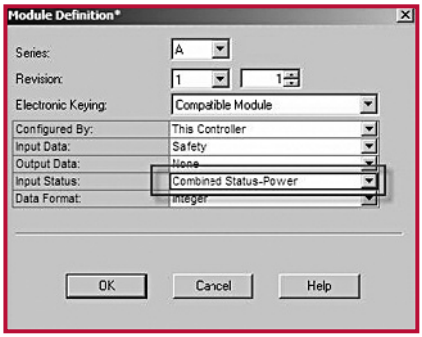
11. Expanda a “Safety”, selecione o módulo 1734-IB8S e clique em OK.



12. Na caixa de diálogo “New Module”, nomeie o dispositivo “CellGuard_1” e clique em “Change”.



13. Quando a caixa de diálogo “Module Definition” for aberta, altere o status da entrada para “Combined Status-Power” e clique em OK.



14. Feche a caixa de diálogo “Module Properties” clicando em OK.

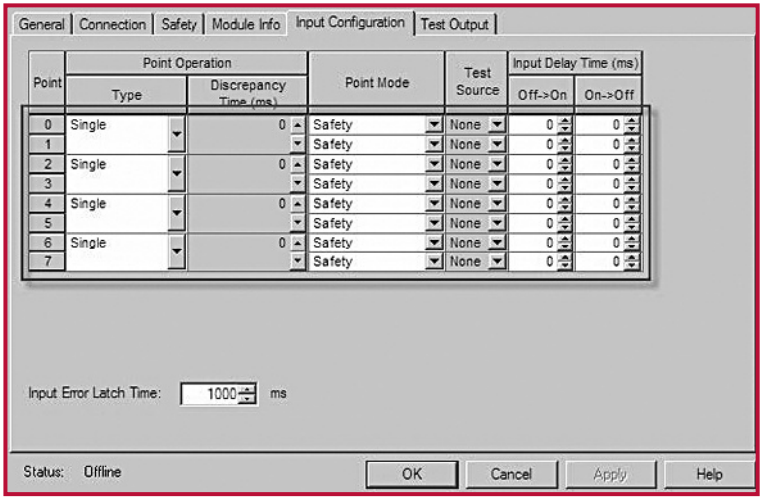
15. Repita os passos 10-14 para adicionar um segundo módulo de entrada de segurança 1734-IB8S e um módulo de saída de segurança 1734-OB8S.

Configurar os módulos de E/S

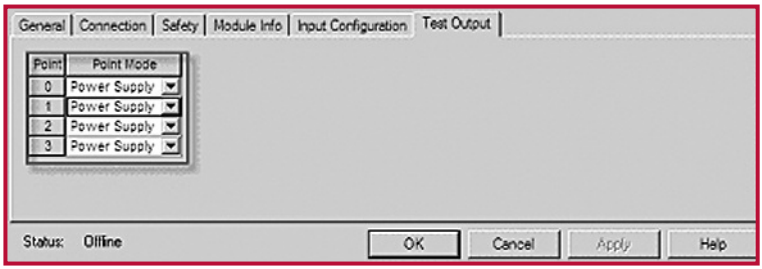
Siga estes passos para configurar os módulos de E/S POINT Guard.

1. No organizador do controlador, clique com o botão direito do mouse no módulo 1734-IB8S e escolha “Properties”.

2. Clique em “Input Configuration” e configure o módulo como mostrado.



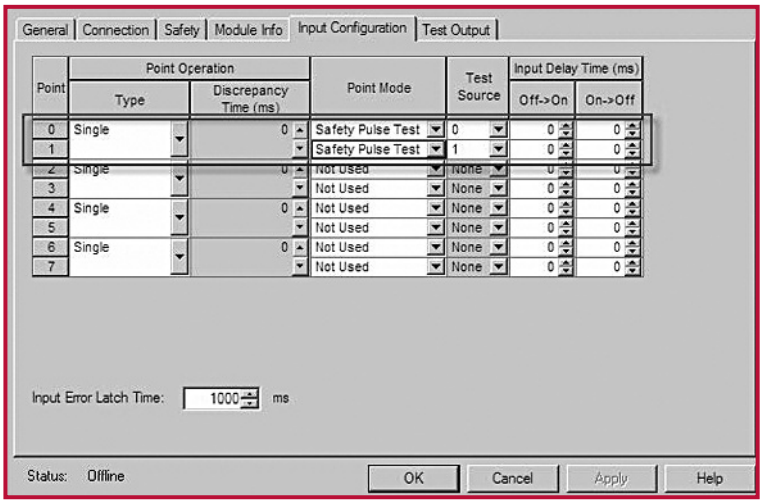
3. Clique em “Test Output” e configure o módulo como mostrado.



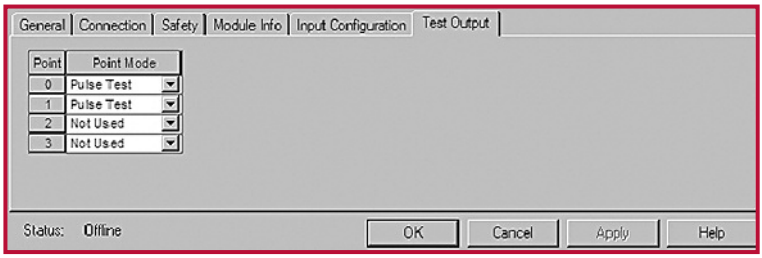
4. Clique em OK.

5. No organizador do controlador, clique com o botão direito do mouse no segundo módulo 1734-IB8S e escolha “Properties”.

6. Clique em “Input Configuration” e configure o módulo como mostrado.



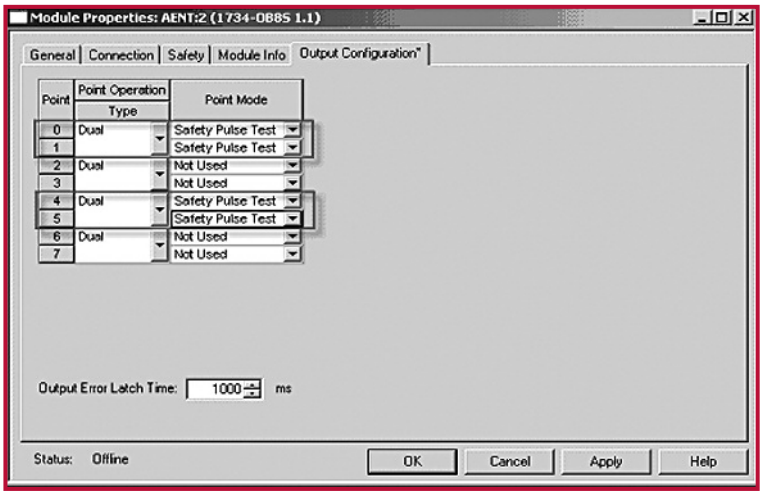
7. Clique em “Test Output” e configure o módulo como mostrado.



8. Clique em OK.

9. No organizador do controlador, clique com o botão direito do mouse no módulo 1734-OB8S e escolha “Properties”.

10. Clique em “Output Configuration” e configure o módulo como mostrado.

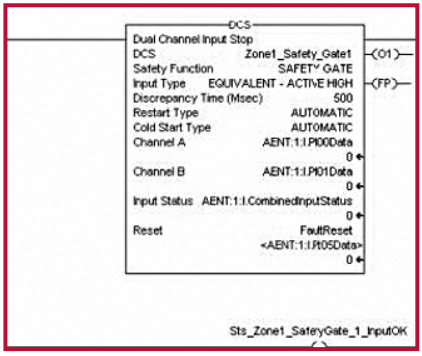


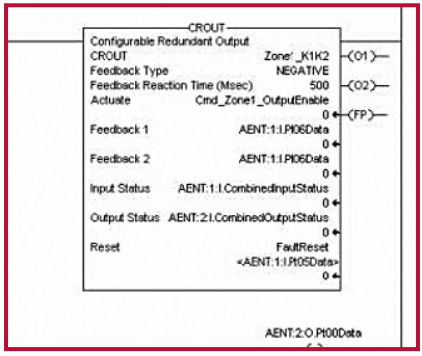
11. Clique em OK.

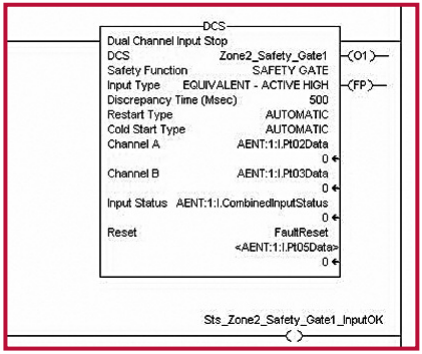
Programação

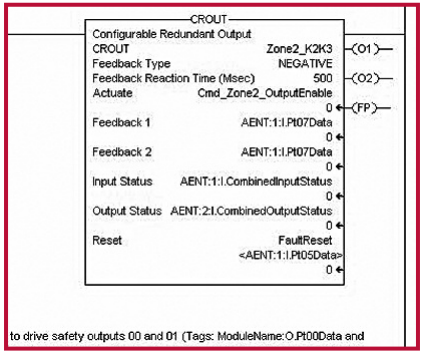
A instrução DCS monitora dispositivos de entrada dupla de segurança, cuja principal função é a de parar a máquina com segurança, por exemplo, uma parada de emergência, cortina de luz ou gate de segurança. Esta instrução só pode energizar a Saída 1 quando as duas entradas de segurança, Canal A e Canal B, estiverem no estado ativo, conforme determinado pelo parâmetro de tipo de entrada e as ações de redefinição corretas forem realizadas. A instrução DCS monitora os canais de entrada dupla para a consistência (Equivalent – Active High) e detecta e captura falhas quando a inconsistência for detectada por mais tempo do que a discrepância de tempo configurada (ms). A instrução CROUT controla e monitora as saídas redundantes. O tempo de reação para realimentação de saída é configurável. A instrução suporta sinais de realimentação positivos e negativos.

O código da aplicação de segurança na rotina de saída de segurança evita que as saídas reiniciem se o canal de entrada reinicia automaticamente, oferecendo funcionalidade anti-vinculante para o reset do circuito.



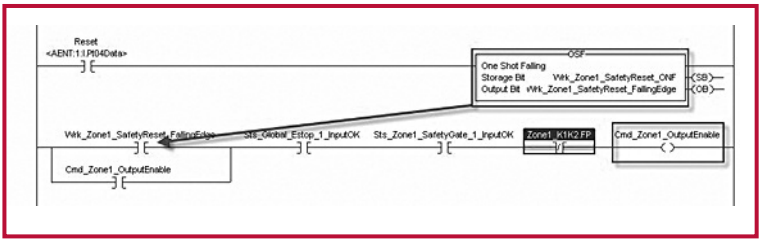






Reset de borda descendente

O EN ISO 13849-1 estabelece que as funções de reset de instrução devem ocorrer em sinais de borda descendentes. Para cumprir este requisito, adicione uma instrução de queda monoestável no código de reset, como mostrado abaixo.



Dados de desempenho

Quando configuradas corretamente, cada função de segurança pode conseguir uma classificação de segurança de PLe, CAT 4 de acordo com o EN ISO 13849.1 2008.

Os cálculos baseiam-se no funcionamento durante 360 dias por ano, 16 horas por dia, com atuação do gate de segurança uma vez por hora, em um total de 5.760 operações por ano. A função de parada de emergência global é testada uma vez por mês.

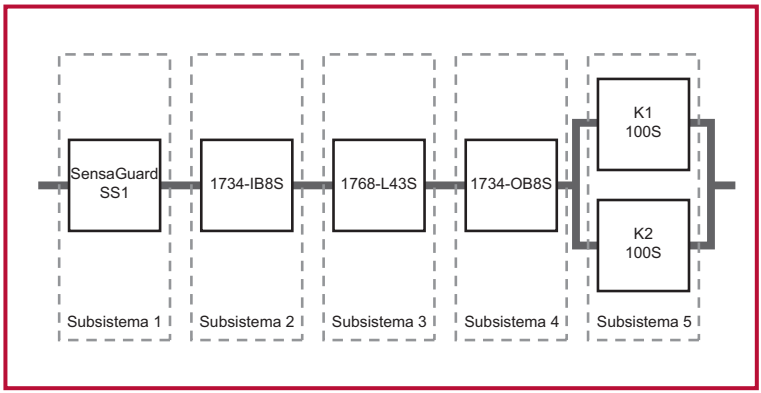
Safety Gate 1	
PLr	e
PL	e
PFH [1/h]	2.64E-8

Estop 1	
PLr	d
PL	e
PFH [1/h]	5E-8

Safety Gate 2	
PLr	e
PL	e
PFH [1/h]	2.64E-8

Exemplo de aplicação usando SISTEMA

Cada função do gate de segurança pode ser representada como se segue.



Interlock Switch: SensaGuard	
PL	e
PFH [1/h]	1.12E-9
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

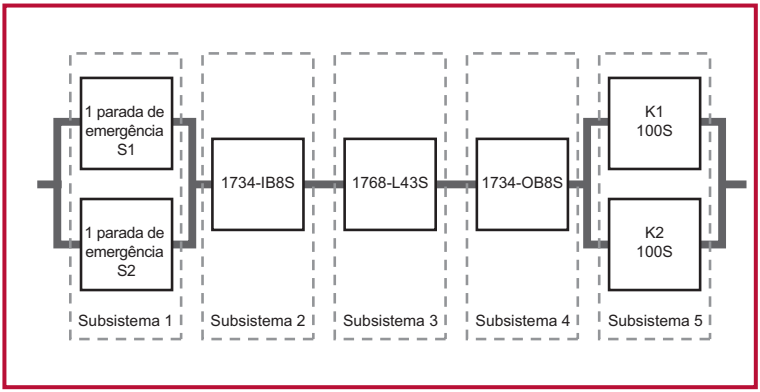
Safety I/O: 1734-IB8S	
PL	e
PFH [1/h]	2.25E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

Safety PLC: Compact GuardLogix 1768	
PL	e
PFH [1/h]	2.1E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

Safety I/O: 1734-OB8S	
PL	e
PFH [1/h]	2.29E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

Contactors	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

A função de parada de emergência pode ser representada como se segue.



SB Estop 1	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

SB Safety I/O: 1734-IB8S	
PL	e
PFH [1/h]	2.25E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety PLC: Compact GuardLogix 1768	
PL	e
PFH [1/h]	2.1E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety I/O: 1734-OB8S	
PL	e
PFH [1/h]	2.29E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Contactors	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

Pode fazer download deste exemplo, o arquivo de cálculo do SISTEMA e código do aplicativo RSLogix 5000 em:

www.discoverrockwellautomation.com

Para obter mais informações sobre os produtos utilizados neste exemplo, consulte a Literature Library da Rockwell Automation e pesquise pelos números de publicação destacados abaixo. Alternativamente, visite www.ab.com para obter características gerais de produtos.

O url da Literature Library é: **www.theautomationbookstore.com**

Recurso	Descrição
Manual do usuário dos controladores Compact GuardLogix. Publicação: **1768-UM002**	Fornece informação sobre a configuração, operação e manutenção dos controladores Compact GuardLogix
Manual de instalação e do usuario dos modulos de seguranca POINT Guard I/O Publicação: **1734-UM013**	Fornece informações sobre a instalação, a configuração e a operação dos módulos POINT Guard I/O
Manual de referencia de segurança dos sistemas de controlador GuardLogix Publicação: **1756-RM093**	Contém os requisitos detalhados para obter e manter classificações de segurança com o sistema de controlador GuardLogix.
Manual de referência do conjunto de instruções para aplicações de segurança do GuardLogix. Publicação: **1756-RM095**	Oferece informações detalhadas sobre o conjunto de instruções para aplicações de segurança do GuardLogix.
Guia de Inicio Rapido do kit de ferramentas acelerador de seguranca para sistemas GuardLogix. Publicação: **IASIMP-QS005**	Fornece um guia passo a passo para a utilização das ferramentas de projeto, programação e diagnóstico no kit de ferramentas acelerador para segurança.
Catálogo de produtos de segurança Publicação: **S117-CA001A**	Uma publicação abrangente que inclui produtos de segurança, exemplos de aprovação e informações úteis

A Rockwell Automation desenvolveu um conjunto de exemplos semelhantes que podem ser baixados na Literature Library. Acesse a Literature Library e realize uma busca por “SEGURANÇA EM” no campo de pesquisa, ajustando o menu suspenso para “Número da publicação”.

Cálculos SISTEMA e códigos de aplicações RSLogix 5000 estão disponíveis para algumas das aplicações e pode fazer download de:

www.discoverrockwellautomation.com

MTTFd para cada canal em anos	Probabilidade média de uma falha perigosa por hora (1/h) e nível de desempenho correspondente (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	$DC_{média}$ = nenhum		$DC_{média}$ = nenhum		$DC_{média}$ = baixo		$DC_{média}$ = médio		$DC_{média}$ = baixo		$DC_{média}$ = médio		$DC_{média}$ = alto	
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	A	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	A	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-5}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-5}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}31 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		

MTTFd para cada canal em anos	Probabilidade média de uma falha perigosa por hora (1/h) e nível de desempenho correspondente (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	$DC_{média}$ = nenhum		$DC_{média}$ = nenhum		$DC_{média}$ = baixo		$DC_{média}$ = médio		$DC_{média}$ = baixo		$DC_{média}$ = médio		$DC_{média}$ = alto	
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e