**ABNT-Associação Brasileira de Normas Técnicas**

Sede:
Rio de Janeiro
Av. Treze de Maio, 13 - 28º andar
CEP 20003-900 - Caixa Postal 1680
Rio de Janeiro - RJ
Tel.: PABX (21) 210-3122
Fax: (21) 220-1762/220-6436
Endereço Telegráfico:
NORMATÉCNICA



JUL 1998 | NBR 14153

# Segurança de máquinas - Partes de sistemas de comando relacionadas à segurança - Princípios gerais para projeto

Origem: Projeto 04:016.01-023:1997
CB-04 - Comitê Brasileiro de Máquinas e Equipamentos Mecânicos
CE-04:016.01 - Comissão de Estudo de Máquinas Injetoras de Plástico
NBR 14153 - Safety of machinery - Safety related parts of control systems - General principles for design
Descriptors: Control systems. Safety of machines. Machine control
Esta Norma foi baseada na EN 954-1:1996
Válida a partir de 01.09.1998

Palavras-chave: Sistema de comando. Segurança de máquina. Comando de máquina | 23 páginas

## Sumário



## Prefácio

A ABNT - Associação Brasileira de Normas Técnicas - é o Fórum Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (CB) e dos Organismos de Normalização Setorial (ONS), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

Os Projetos de Norma Brasileira, elaborados no âmbito dos CB e ONS, circulam para Votação Nacional entre os associados da ABNT e demais interessados.

Esta Norma contém os anexos A, B, C, D e E, de caráter informativo.

Usou-se como texto de referência para este trabalho a EN 954-1:1994 - “Safety of machinery - Safety related parts of control systems - Part 1: General principles for design”.

## Introdução

Partes de sistemas de comando de máquinas têm, freqüentemente, a atribuição de prover segurança; essas são chamadas as partes relacionadas à segurança. Essas partes podem consistir de *hardware* e *software* e desempenham as funções de segurança de sistemas de comando. Podem ser parte integrante ou separada do sistema de comando.

O desempenho, com relação à ocorrência de defeitos, de uma parte de um sistema de comando, relacionada à segurança, é dividido, nesta Norma, em cinco categorias (B, 1, 2, 3 e 4), que devem ser usadas como pontos de referência. Não é objetivo a utilização dessas categorias, em qualquer ordem de hierarquia, com respeito a requisitos de segurança.

As categorias podem ser aplicadas para:

- comandos para todo tipo de máquinas, desde simples máquinas (por exemplo, pequenas máquinas

para a cozinha) até complexas instalações de manufatura (por exemplo, máquinas de embalagem, máquinas de impressão, prensas, etc.);

- sistemas de comando de equipamentos de proteção, por exemplo, dispositivos de comando a duas mãos, dispositivos de intertravamento, dispositivos de proteção eletrossensitivos, por exemplo, barreiras foto-elétricas, e plataformas sensíveis à pressão.

A categoria selecionada dependerá da máquina e da extensão a que os meios de comando são utilizados para medidas de proteção.

Na seleção de uma categoria e no projeto de uma parte de um sistema de comando, relacionada à segurança, o projetista deverá declarar, ao menos, as seguintes informações, relativas à parte relacionada à segurança:

- a(s) categoria(s) selecionada(s);

- a característica funcional e a exata finalidade da parte na(s) medida(s) de segurança;

- os limites exatos (ver 3.1);

- todos os defeitos relevantes à segurança considerados;

- aqueles defeitos relevantes à segurança não considerados pela exclusão de defeitos e as medidas empregadas para permitir sua exclusão;

- os parâmetros relevantes à confiabilidade, tais como condições ambiente;

- a(s) tecnologia(s) aplicada(s).

O uso das categorias, como pontos de referência e essa declaração nos princípios de projeto, tem o objetivo de permitir a utilização flexível desta Norma e proporcionar uma base clara, sobre a qual o projeto e o desempenho de qualquer aplicação da parte de um sistema de comando (e a máquina), relacionada à segurança, possam ser avaliados, por exemplo, por terceiros, em ensaios internos ou em laboratórios independentes.

## 1 Objetivo

Esta Norma especifica os requisitos de segurança e estabelece um guia sobre os princípios para o projeto (ver EN 292-1) de partes de sistemas de comando relacionadas à segurança. Para essas partes, especifica categorias e descreve as características de suas funções de segurança. Isso inclui sistemas programáveis para todos os tipos de máquinas e dispositivos de proteção relacionados. Esta Norma se aplica a todas as partes de sistemas de comando relacionadas à segurança, independentemente do tipo de energia aplicado, por exemplo, elétrica, hidráulica, pneumática, mecânica. Esta Norma não especifica que funções de segurança e que categorias devem ser aplicadas em um caso particular.

Esta Norma abrange todas as aplicações de máquinas, para uso profissional ou não profissional. Também, onde apropriado, esta Norma pode ser aplicada às partes de sistemas de comando relacionadas à segurança, utilizadas em outras aplicações técnicas.

## 2 Referências normativas

As normas relacionadas a seguir contêm disposições que, ao serem citadas neste texto, constituem prescrições para esta Norma. As edições indicadas estavam em vigor no momento desta publicação. Como toda norma está sujeita à revisão, recomenda-se àqueles que realizam acordos com base nesta que verifiquem a conveniência de se usarem as edições mais recentes das normas citadas a seguir. A ABNT possui a informação das normas em vigor em um dado momento.

NBR 13759:1996 - Segurança de máquinas - Equipamentos de parada de emergência, aspectos funcionais - Princípios para projeto

NBR 14009:1997 - Segurança de máquinas - Princípios para apreciação de riscos

EN 292-1:1991 Safety of machinery - Basic concepts, general principles for design - Part 1: Basic terminology, methodology.

EN 292-2:1991 - Safety of machinery - Basic concepts, general principles for design - Part 2: Technical principles and specifications.

EN 457:1992 - Safety of machinery - Auditory danger signals - General requirements, design and testing

EN 614-1:1995 - Safety of machinery - Ergonomic design principles - Part 1: Treminology and general principles

EN 775:1992 - Manipulating industrial robots - Safety

EN 842:1996 - Safety of machinery - Visual danger signals - General requirements, design and testing

EN 981:1996 - Safety of machinery - System of danger and non-danger signals with sound and light

EN 982:1996 - Safety of machinery - Safety requeriments for fluid power systems an components - Hydraulics

EN 983:1996 - Safety of machinery - Safety requeriments for fluid power systems an components - Pneumatics

EN 1037:1995 - Safety of machinery - Prevention of unexpected start-up

EN 60204 -1:1992 - Electrical equipment of machines - Part 1: General requeriments

EN 60335-1:1994 Safety of household and similar electric appliances - Part 1: General requirements

IEC 50(191):1990 - International Eletrotechnical Vocabulary, Chapter 191: Dependability and quality of service

## 3 Definições

Para os efeitos desta Norma, aplicam-se às definições das EN 292-1 e IEC 50(191) e as seguintes:

**3.1 parte de sistema de comando relacionada à segurança:** Parte ou subparte de sistema de comando, que responde a sinais de entrada do equipamento sob comando (e/ou de um operador) e gera sinais de saída relacionados com segurança. As partes combinadas de um sistema de comando relacionadas à segurança começam no ponto em que os sinais relacionados à segurança são gerados e findam na saída dos elementos de controle de potência (ver também EN 292-1). Isto também inclui sistemas de monitoração.

**3.2 categoria:** Classificação das partes de um sistema de comando relacionadas à segurança, com respeito à sua resistência a defeitos e seu subseqüente comportamento na condição de defeito, que é alcançada pelos arranjos estruturais das partes e/ou por sua confiabilidade.

**3.3 segurança de sistemas de comando:** Habilidade de desenvolver sua(s) função(ões) para um dado período, de acordo com sua categoria especificada, baseada em seu comportamento no caso de defeito(s).

**3.4 defeito:** Estado de um item caracterizado pela inabilidade de desenvolver a função requerida, excluindo a inabilidade durante manutenções preventivas ou outras ações planejadas, ou devido à perda de recursos externos.

NOTA - Um defeito é, freqüentemente, o resultado de uma falha do próprio item, porém pode existir sem falha prévia.

**3.6 falha:** Término da habilidade de um item em desenvolver uma função requerida.

NOTAS

1 Após a falha o item tem um defeito.

2 Falha é um evento, distintamente de defeito, que é um estado.

3 Esse conceito, como definido, não se aplica a item constituído apenas por *software*.

4 Na prática, os termos defeito e falha são freqüentemente usados como sinônimos.

**3.7 função segurança de sinais de comando:** Função iniciada por um sinal de entrada e processada pelas partes do sistema de comando, relacionadas à segurança, para permitir à máquina (como um sistema) alcançar um estado seguro.

**3.8 pausa:** Suspensão temporária automática da(s) função(ões) de segurança, por partes do sistema de comando, relacionadas à segurança.

**3.9 rearme manual:** Função com que as partes de um sistema de comando relacionadas à segurança recuperam, manualmente, suas funções de segurança, antes do reinício de operação da máquina.

## 4 Considerações gerais

### 4.1 Objetivos de segurança no projeto

As partes de um sistema de comando relacionadas à segurança, que proporcionam as funções de segurança, devem ser projetadas e construídas de tal forma que os princípios da NBR 14009 sejam integralmente considerados:

- durante toda a utilização prevista e utilização incorreta previsível;

- na ocorrência de defeitos;

- quando erros humanos previsíveis forem cometidos durante a utilização planejada da máquina como um todo.

### 4.2 Estratégia geral para projeto

Dos princípios para a apreciação de riscos na máquina (ver NBR 14009), o projetista deve decidir sobre a contribuição à redução do risco, que precisa ser suprida por cada parte das partes do sistema de comando relacionadas à segurança (ver anexo B). Esta contribuição não cobre a totalidade dos riscos da máquina sob comando; por exemplo, não é considerado o risco total de uma prensa mecânica ou uma máquina de lavar, porém a parte do risco reduzida pela aplicação de funções de seguranças particulares. Exemplos de tais funções são a função de parada iniciada pela utilização de um dispositivo de proteção eletrossensitivo em uma prensa ou a função de bloqueio de uma porta de máquina de lavar.

O principal objetivo é que o projetista assegure que as partes de um sistema de comando relacionadas à segurança produzam sinais de saída que atinjam os objetivos de redução de riscos da NBR 14009. Isto não é sempre possível, mas o projetista deve, em tais casos, gerar outras medidas de segurança. A hierarquia para a estratégia na redução do risco é dada na EN 292-1.

A categoria e outras características (por exemplo, posição física de partes, isolação), selecionadas pelo projetista para as partes relacionadas à segurança, dependem da contribuição feita à redução do risco, por essas partes, pelo projeto e tecnologia (ver Introdução). O projetista deve declarar:

- que categoria(s) está sendo usada como ponto de referência para o projeto;

- os pontos exatos em que as partes relacionadas à segurança têm início e fim;

- a análise lógica do projeto (por exemplo, os defeitos considerados e os excluídos) para alcançar aquela(s) categoria(s).

Quanto mais a redução do risco depender das partes de sistema de comando relacionadas à segurança, maior precisa ser a habilidade dessas partes para resistir a defeitos. Essa habilidade - entendendo-se que a função requerida é cumprida - pode ser parcialmente quantificada por valores de confiabilidade e por uma estrutura resistente a defeitos. Ambos, confiabilidade e estrutura, contribuem para essa habilidade das partes relacionadas à segurança em resistir a defeitos. Uma resistência especificada a defeitos pode ser atingida pela definição de níveis de confiabilidade de componentes e/ou com estruturas melhoradas para as partes relacionadas à segurança. A contribuição da confiabilidade e da estrutura pode variar com a tecnologia aplicada. Por exemplo, é possível, em uma tecnologia, para um único canal de partes relacionadas à segurança de alta confiabilidade, prover a mesma ou maior resistência a defeitos, que em uma estrutura tolerante a defeitos, de menor confiabilidade em uma tecnologia diferente

NOTA - Quanto maior a resistência a defeitos das partes relacionadas à segurança, menor a probabilidade que esta parte falhe no cumprimento de suas funções de segurança.

Confiabilidade e segurança não são o mesmo (ver anexo D). Por exemplo, é possível que a segurança de um sistema com componentes de baixa confiabilidade seja em uma estrutura redundante, maior que a segurança de um sistema com uma estrutura mais simples, porém com componentes de maior confiabilidade. Esse conceito é importante porque, em algumas aplicações, a segurança requer a mais alta prioridade, independentemente da confiabilidade alcançada, por exemplo, quando as conseqüências de uma falha são sempre sérias e normalmente irreversíveis. Em tais aplicações, uma estrutura de detecção de defeito (tolerância de defeito de um ciclo), que proporciona a segurança requerida após um, dois ou mais defeitos, deve ser prevista de acordo com a apreciação do risco.

Esta Norma não requer o cálculo de valores de confiabilidade para estruturas complexas, onde a segurança é predominantemente obtida pela melhoria da estrutura do sistema. Para estruturas simples (por exemplo, canal único), onde a confiabilidade do componente é importante para a segurança, o cálculo dos valores de confiabilidade é um indicador útil da contribuição à redução do risco global, pela parte relacionada à segurança.

No caso de aplicações de riscos menores, medidas para evitar defeitos podem ser apropriadas. Para aplicações de riscos maiores, a melhoria da estrutura das partes de sistemas de comando relacionadas à segurança pode proporcionar medidas para evitar, detectar ou tolerar defeitos. Medidas práticas incluem redundância, diversidade, monitoração (ver também EN 292-2 e EN 60204-1).

O comportamento atingido para resistência a defeitos, pelas partes de sistemas de comando relacionadas à segurança, é função de vários parâmetros, incluindo, por exemplo:

- confiabilidade com relação ao desempenho das funções de segurança;

- estrutura (ou arquitetura) do sistema de comando;

- qualidade da documentação relacionada à segurança;

- qualidade da especificação;

- projeto, construção e manutenção;

- qualidade e exatidão do *software*;

- amplitude dos ensaios funcionais;

- características de operação da máquina ou parte da máquina sob comando.

Esses parâmetros podem ser agrupados sob três características principais:

- confiabilidade de *hardware* - o nível de confiabilidade dos componentes para evitar defeitos;

- estrutura do sistema - o arranjo dos componentes na parte de um sistema de comando relacionada à segurança, para evitar, tolerar ou detectar defeitos;

- aspectos qualitativos, não quantificáveis, que afetam o comportamento da parte de um sistema de comando relacionada à segurança.

**4.3 Processo para a seleção e projeto de medidas de segurança**

Este item especifica um processo para a seleção das medidas de segurança a serem implementadas e, então, para o projeto de partes de sistemas de comando relacionadas à segurança. É importante que as interfaces entre as partes relacionadas à segurança e aquelas não relacionadas à segurança do sistema de comando e todas as outras partes da máquina sejam identificadas. Então, a contribuição à redução do risco pode ser especificada dentro da apreciação do risco da máquina, de acordo com a NBR 14009.

Por haver muitas maneiras de redução dos riscos de uma máquina e por haver muitas formas de projeto para as partes de sistemas de comando relacionadas à segurança, este processo é interativo. Decisões e/ou hipóteses feitas em qualquer passo do procedimento podem afetar decisões e/ou hipóteses feitas em algum passo anterior. Esse aspecto pode ser checado pela volta através do procedimento, a qualquer etapa. Tal checagem na etapa de validação é essencial para assegurar que o desempenho de segurança atingido é o mesmo daquele definido na especificação.

O processo é ilustrado na figura 1. Aspectos importantes que devem ser considerados durante o processo de projeto são dados como quesitos no anexo A, para auxílio ao projetista. Esses quesitos ilustram a filosofia a ser seguida no projeto de partes relacionadas à segurança. Nem todos os quesitos são válidos a todas as aplicações. Algumas aplicações requerem quesitos adicionais.

Passo 1: Análise do perigo e apreciação de riscos:

- identificar os perigos presentes à máquina durante todos os modos de operação e a cada estágio da vida da máquina, pelo seguimento do guia da EN 292-1 e NBR 14009;

- avaliar os riscos provenientes daqueles perigos e decidir sobre a apropriada redução de risco para essa aplicação, de acordo com as EN 292-1 e NBR 14009.

Passo 2: Decisão das medidas para redução do risco:

- definir medidas de projeto na máquina e/ou a aplicação de proteções para levar à redução do risco. Partes do sistema de comando que contribuem como parte integral das medidas de projeto ou no comando de proteções devem ser consideradas como partes do sistema de comando relacionadas à segurança.

Passo 3: Especificação dos requisitos de segurança para as partes de sistemas de comando relacionadas à segurança:

- especificar as funções de segurança (ver seção 5) a serem cumpridas no sistema de comando. A tabela 1 lista a fonte de referência das funções de segurança mais comuns e as características que devem ser incluídas se uma particular função de segurança for selecionada;

- especificar como a segurança deve ser atingida e selecionar a(s) categoria(s) para cada parte e combinações de partes, dentro das partes de sistemas de comando relacionadas à segurança (ver seção 6).

Passo 4: Projeto:

- projetar as partes de sistemas de comando relacionadas à segurança de acordo com as especificações desenvolvidas no passo 3, e a estratégia geral de projeto em 4.2. Listar os aspectos de projeto incluídos que proporcionam a base lógica de projeto para a(s) categoria(s) alcançadas;

- verificar o projeto a cada estágio, para assegurar que as partes relacionadas à segurança preencham os requisitos do estágio anterior no contexto da(s) função(ões) e categoria(s) especificada(s).

Passo 5: Validação:

- validar as funções e categoria(s) de segurança alcançadas no projeto com relação às especificações do passo 3. Reprojetar, se necessário (ver seção 8);

- quando a eletrônica programável for usada no projeto de partes de sistemas de comando relacionadas à segurança, outros procedimentos detalhados são necessários (ver 8.4.2).

NOTAS

1 Atualmente acredita-se que é difícil determinar, com algum grau de exatidão, situações em que um perigo significante pode ocorrer em conseqüência do mau funcionamento do sistema de comando, que a confiança da operação correta de um canal isolado de um equipamento eletrônico programável possa ser assegurada. Durante o tempo em que essa situação possa ser resolvida, não é aconselhável confiar na operação correta de um dispositivo de tal canal isolado (de acordo com a EN 60 204-1).

2 Também será necessário validar a parte do sistema de comando relacionada à segurança, em conjunto com todo o sistema de comando e como parte da máquina. Os requisitos para tal validação não fazem parte desta Norma, porém devem ser especificados pelo construtor da máquina ou em normas apropriadas do tipo C.

**4.4 Princípios para o projeto ergonômico**

A interface entre pessoas e as partes de sistemas de comando relacionadas à segurança devem ser projetadas e instaladas de tal forma que ninguém seja posto em perigo durante toda utilização planejada e mau uso previsível da máquina (ver também EN 292-2, EN 614-1 e EN 60204-1).

Princípios ergonômicos devem ser aplicados de tal forma que o sistema de comando e a máquina, incluindo as partes relacionadas à segurança, sejam de fácil utilização e de tal forma que o operador não seja levado a agir de maneira perigosa. Os requisitos de segurança para observação dos princípios ergonômicos dados em 3.6 da EN 292-2:1991devem ser aplicados.

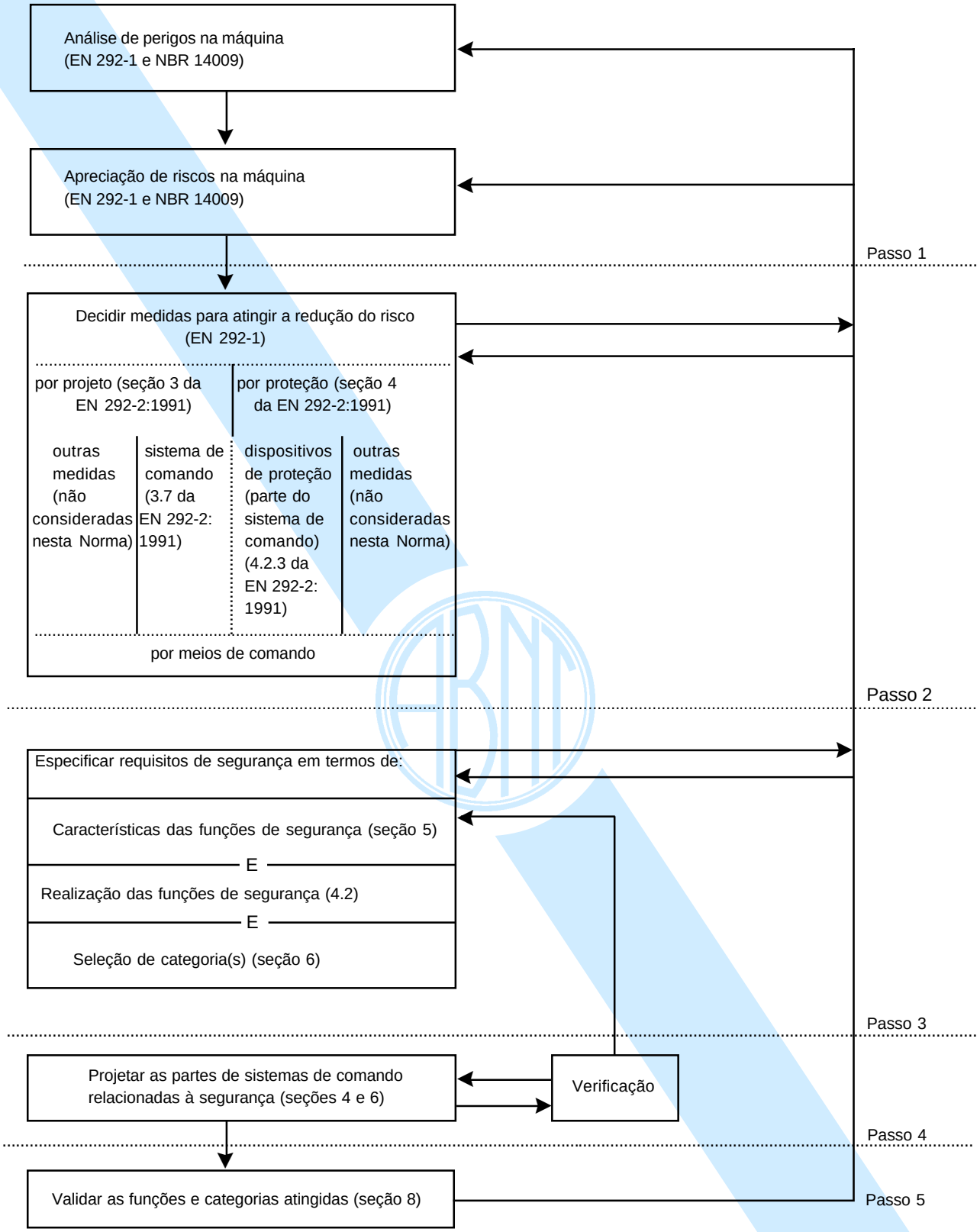



**Figura 1 - Processo interativo para o projeto de partes de sistemas de comando relacionadas à segurança**

**Tabela 1 - Lista de algumas normas que especificam requisitos para características de funções de segurança**

| Características de funções de segurança | NBR 14153 | EN 292-1 | EN 292-2 | EN 292-2:1991 anexo A | Outras normas | Informações adicionais[1)] |
|---|---|---|---|---|---|---|
| Definições | 3 | X | | | EN 60204-1 | EN 60335-1 |
| Princípios de projeto | 4.2 | | X | X | EN 60204-1 | EN 60335-1<br>EN 775 |
| Princípios ergonômicos | 4.4 | X | X | X | EN 60204-1 | EN 775 |
| Funções de parada | 5.2 | | X | X | EN 60204-1 | EN 60335-1 |
| Função parada de emergência | 5.3 | | X | X | NBR 13579<br>EN 60204-1 | EN 775 |
| Rearme manual | 5.4 | | | X | EN 60204-1 | EN 775 |
| Partida e reinício | 5.5 | | X | X | EN 60204-1 | EN 775 |
| Tempo de resposta | 5.6 | | | | | |
| Parâmetros relacionados à segurança | 5.7 | | X | | EN 60204-1 | EN 775<br>EN 60335-1 |
| Função de comando local | 5.8 | | X | | | EN 775 |
| Pausa | 5.9 | | | | | |
| Suspensão manual de funções de segurança | 5.10 | | X | | EN 60204-1 | EN 775 |
| Flutuações, falta e restauração de fontes de energia | 5.11 | | X | | EN 60204-1 | |
| Sistemas eletrônicos programáveis | | | X | | EN 60204-1 | |
| Partida inesperada | | | X | X | EN 1037<br>EN 60204-1 | |
| Indicações e alarmes | | | X | X | EN 457, EN 842,<br>EN 981,<br>EN 60204-1 | |
| Liberação e salvamento de pessoas presas | | | X | X | | |
| Equipamento elétrico | | X | | X | EN 60204-1 | |
| Abastecimento elétrico | | | | X | EN 60204-1 | |
| Outras fontes de energia | | | | X | EN 982<br>EN 983 | |

**Tabela 1** (conclusão)

| Características de funções de segurança | NBR 14153 | EN 292-1 | EN 292-2 | EN 292-2:1991 anexo A | Outras normas | Informações adicionais[1)] |
|---|---|---|---|---|---|---|
| Proteções e coberturas | | | | | EN 60204-1 | |
| Equipamento pneumático e hidráulico | | | X | X | EN 982<br>EN 983 | |
| Isolação e dissipação de energia | | | X | X | EN 1037<br>EN 60204-1 | |
| Meio ambiente físico e condições de operação | | | X | | EN 60204-1 | EN 775 |
| Modos de comando e seleção do modo | | | X | X | EN 60204-1 | EN 775 |
| Interfaces/ conexões | | | | X | EN 60204-1 | |
| Interação entre diferentes partes de sistemas de comando relacionadas à segurança | | | X | | EN 60204-1 | |
| Interface homem - máquina | | | X | X | EN 60204-1 | |

[1)] As referências dessa coluna devem ser consideradas como um auxílio ao projetista, e não como parte dos requisitos desta Norma.

## 5 Características das funções de segurança

### 5.1 Generalidades

Este item apresenta uma lista de funções típicas de segurança (ver EN 292-1), que podem ser supridas pelas partes de sistemas de comando relacionadas à segurança. O projetista (ou o elaborador de normas do tipo C) deve incluir as funções de segurança dessa lista, necessárias para alcançar as medidas de segurança requeridas do sistema de comando, para a aplicação específica.

A tabela 1 lista funções típicas de segurança e algumas de suas características. Ela faz referência a detalhes das características que são claramente definidas nas referências normativas. O projetista (ou o elaborador de normas do tipo C) deve assegurar que os requisitos de todas essas normas sejam cumpridos para as funções de segurança selecionadas. Requisitos adicionais detalhados também são citados neste item para algumas características. Estes devem ser incluídos.

Onde necessário, as características devem ser adaptadas para utilização com diferentes fontes de energia.

### 5.2 Função parada

Em adição aos requisitos das referências dadas na tabela 1, deve ser aplicado também o seguinte:

- uma função de parada iniciada por um dispositivo de proteção deve, tão rápido quanto necessário, após sua atuação, colocar a máquina em condição segura. Esse tipo de parada deve ter prioridade sobre uma parada por razões operacionais;

- quando um grupo de máquinas trabalha em conjunto, de forma coordenada, meios devem existir para sinalizar ao comando supervisor e/ou às outras máquinas que tal função de parada existe.

NOTA - Esse tipo de parada pode causar problemas operacionais e dificultar o reinício de operação, por exemplo, em solda a arco. Em algumas aplicações, essa função pode ser combinada com uma parada para razões operacionais, para reduzir o incentivo à manipulação da função de segurança.

**5.3 Função parada de emergência**

Em adição aos requisitos das referências dadas na tabela 1, deve ser aplicado também o seguinte:

- quando um grupo de máquinas trabalha de forma coordenada, as partes relacionadas à segurança devem ter meios de sinalizar uma função de parada de emergência a todas as partes do sistema coordenado;

- onde seções do sistema coordenado são claramente separadas, por exemplo, proteções ou localização física, não é sempre necessário aplicar a parada de emergência a todo o sistema, mas apenas a seções particulares, identificadas pela apreciação dos riscos.

Após a efetivação de uma parada de emergência para uma seção, um perigo não deve estar presente nas interfaces dessa seção com as outras seções.

**5.4 Rearme manual**

Em adição aos requisitos das referências dadas na tabela 1, deve ser aplicado também o seguinte:

- após o início de um comando de parada por um dispositivo de proteção, a condição de parada deve ser mantida até a atuação manual do dispositivo de rearme e até que uma condição segura de operação exista;

- o restabelecimento da função segura pelo rearme do dispositivo de proteção cancela o comando de parada. Se indicado pela apreciação do risco, o cancelamento do comando de parada deve ser confirmado por uma ação manual, separada e deliberada (rearme manual).

A função rearme manual:

- deve ser atuada através de um dispositivo separado, manualmente operado, em conjunto com as partes do sistema de comando relacionadas à segurança;

- somente pode ser efetivado se todas as funções de segurança e dispositivos de proteção estiverem operando. Se isso não for possível, o rearme não deve estar disponível;

- não deve, por si só, iniciar movimento ou uma situação perigosa;

- deve ser de ação deliberada;

- deve preparar o sistema de comando para a aceitação de um comando de partida separado;

- deve somente ser aceito pela atuação do atuador de sua posição liberada (desligado).

A categoria das partes relacionadas à segurança, que atuam o rearme manual, deve ser selecionada de tal forma que a inclusão do rearme manual não diminua a segurança requerida da função de segurança relevante.

O atuador para rearme deve estar situado fora da área de perigo e em posição segura, de onde se tenha boa visibilidade para a verificação da inexistência de pessoas na zona de perigo.

**5.5 Partida e reinício**

Em adição aos requisitos das referências dadas na tabela 1, deve ser aplicado também o seguinte:

- o reinício do movimento deve ocorrer automaticamente, apenas se uma situação de perigo não puder existir. Em particular, para proteções de controle, ver EN 292-2.

Esses requisitos de partida e reinício de movimento também devem se aplicar a máquinas que podem ser controladas remotamente.

**5.6 Tempo de resposta**

Em adição aos requisitos das referências dadas na tabela 1, deve ser aplicado também o seguinte:

- o projetista ou o fabricante deve declarar o tempo de resposta, quando a apreciação do risco da parte do sistema de comando relacionada à segurança indicar que isso é necessário (ver também seção 10).

NOTA - O tempo de resposta do sistema de comando é parte do tempo total de resposta da máquina. O tempo de resposta total necessário da máquina pode influenciar o projeto da parte relacionada à segurança, por exemplo, a necessidade de aplicar um sistema de freio.

**5.7 Parâmetros relacionados à segurança**

Em adição aos requisitos das referências dadas na tabela 1, deve ser aplicado também o seguinte:

- quando parâmetros relacionados à segurança (por exemplo, posição, velocidade, temperatura, pressão) desviam dos limites preestabelecidos, o sistema de comando deve iniciar medidas apropriadas (por exemplo, atuação da função parada, sinal de alarme, advertência);

- se erros na entrada manual de dados, relacionados à segurança, em sistemas eletrônicos programáveis, podem levar a situações de perigo, devem ser previstos sistemas de checagem de dados no sistema relacionado à segurança (por exemplo, checagem de limites, formato e /ou entrada de valores lógicos).

**5.8 Função de comando local**

Quando uma máquina é comandada no local (por exemplo, por dispositivos de comando portáteis, pendentes), os seguintes requisitos também devem ser aplicados, em adição àqueles das referências dadas na tabela 1:

- os meios para seleção do comando local devem estar situados fora da zona de perigo;

- não deve ser possível iniciar condições perigosas fora da zona do comando local;

- a comutação entre comando local e externo (por exemplo, remoto) não deve criar uma situação de perigo.

**5.9 Pausa**

A pausa não deve resultar na exposição de qualquer pessoa a uma situação de perigo.

Durante uma pausa, condições seguras devem ser asseguradas por outros meios.

Ao final da pausa, todas as funções de segurança das partes relacionadas à segurança do sistema de comando devem ser restabelecidas.

A categoria das partes relacionadas à segurança que são responsáveis pela função pausa devem ser selecionadas, de tal forma que a inclusão da função pausa não diminua a segurança requerida das funções relevantes de segurança.

NOTA - Em algumas aplicações um sinal indicador de pausa é necessário.

**5.10 Suspensão manual de funções de segurança**

Se for necessária a suspensão manual de funções de segurança (por exemplo, para configuração, ajustes, manutenção, reparos), os seguintes requisitos também devem ser aplicados, em adição aos requisitos das referências citadas na tabela 1:

- meios efetivos e seguros para impedir a suspensão manual nos modos de operação em que isso não for permitido;

- restabelecimento das funções de segurança das partes relacionadas à segurança dos sistemas de comando, antes que se possa continuar a operação normal;

- a parte relacionada à segurança do sistema de comando responsável pela suspensão manual deve ser selecionada, de tal forma que os princípios da NBR 14009 sejam integralmente considerados.

NOTA - Em algumas aplicações um sinal adicional de suspensão manual é necessário.

**5.11 Flutuação, falta e retorno das fontes de alimentação**

Em adição aos requisitos das referências dadas na tabela 1, deve também ser aplicado o seguinte:

- quando ocorrem flutuações no nível de energia, além dos limites considerados no projeto, incluindo o corte do fornecimento de energia, as partes relacionadas à segurança de sistemas de comando devem continuar a fornecer, ou iniciar, sinais de saída, que habilitarão outras partes do sistema da máquina a manter um estado seguro.

## 6 Categorias

**6.1 Generalidades**

As partes relacionadas à segurança de sistemas de comando devem estar de acordo com os requisitos de uma ou mais das cinco categorias especificadas em 6.2. Essas categorias não objetivam sua aplicação em uma seqüência ou hierarquia definidas, com relação aos requisitos de segurança.

As categorias determinam o comportamento requerido, das partes relacionadas à segurança de sistemas de comando, com relação à sua resistência a falhas, baseado na estratégia descrita em 4.2.

A categoria B é a categoria básica. A ocorrência de um defeito pode levar a perda da função de segurança. Na categoria 1, uma maior resistência a defeitos é alcançada predominantemente pela seleção e aplicação de componentes. Nas categorias 2, 3 e 4, um desempenho melhorado, com relação à função de segurança especificada, é alcançado predominantemente pela melhoria da estrutura da parte relacionada à segurança do sistema de comando. Na categoria 2 isso é conseguido pela checagem periódica de que a função de segurança especificada esta sendo cumprida. Nas categorias 3 e 4 isso é conseguido pela garantia de que um defeito isolado não levará à perda da função de segurança. Na categoria 4 e, sempre que razoavelmente praticável, na categoria 3, tais defeitos serão detectados. Na categoria 4 a resistência ao acúmulo de defeitos será especificada.

A comparação direta do comportamento de resistência a defeitos entre categorias apenas pode ser feita se for alterado um parâmetro por vez. Categorias mais altas apenas podem ser interpretadas como proporcionando uma maior resistência a defeitos em circunstâncias comparáveis (por exemplo, quando usando tecnologia similar, componentes de confiabilidade comparável, regimes similares de manutenção e aplicações comparáveis).

A tabela 2 oferece uma visão das categorias das partes de sistemas de comando relacionadas à segurança, os requisitos e o comportamento do sistema no caso de defeitos.

Quando se consideram as causas de falhas em alguns componentes, é possível a exclusão de alguns defeitos (ver seção 7).

**6.2 Especificação das categorias**

**6.2.1 Categoria B**

As partes de sistemas de comando relacionadas à segurança, como mínimo, devem ser projetadas, construídas, selecionadas, montadas e combinadas, de acordo com as normas relevantes, usando os princípios básicos de segurança para a aplicação específica, de tal forma que resistam a:

- fadiga operacional prevista, como, por exemplo, a confiabilidade com respeito à capacidade e freqüência de comutação;

- influência do material processado ou utilizado no processo, como, por exemplo, detergentes em máquinas de lavar;

- outras influências externas relevantes, como, por exemplo, vibrações mecânicas, campos externos, distúrbios ou interrupção do fornecimento de energia.

NOTAS

1 Não são aplicadas medidas especiais para segurança para as partes integrantes da categoria B.

2 Quando um defeito ocorre, ele pode levar à perda da função de segurança. Para atender aos requisitos do anexo A da EN 292-2:1991, medidas adicionais, que não são proporcionadas pelas partes relacionadas à segurança de sistemas de comando, podem ser necessárias.

**6.2.2 Categoria 1**

Devem ser aplicados os requisitos da categoria B e os desta subseção.

As partes de sistemas de comando relacionadas à segurança, de categoria 1, devem ser projetadas e construídas utilizando-se componentes bem ensaiados e princípios de segurança comprovados.

Um componente bem ensaiado para uma aplicação relacionada à segurança é aquele que tem sido:

- largamente empregado no passado, com resultados satisfatórios em aplicações similares, ou

- construído e verificado utilizando-se princípios que demonstrem sua adequação e confiabilidade para aplicações relacionadas à segurança.

Em alguns componentes bem ensaiados, certos defeitos podem também ser excluídos, em razão de ser conhecida a incidência de defeitos e esta ser muito baixa.

A decisão de se aceitar um componente particular como bem ensaiado pode depender de sua aplicação.

NOTAS

1 Ao nível de componentes eletrônicos isolados, normalmente não é possível o enquadramento na categoria 1. Princípios de segurança comprovados são, por exemplo:

- impedimento de certos defeitos, como, por exemplo, impedimento de curtos-circuitos por isolação;

- redução da probabilidade de defeitos, como, por exemplo, superdimensionamento ou uma baixa solicitação de componentes;

- pela orientação do modo de defeitos, como, por exemplo, pela garantia da abertura de um circuito, quando isso é vital para remover a energia no evento de defeitos;

- detecção precoce de defeitos;

- restringindo as conseqüências de um defeito, como, por exemplo, aterrando o equipamento.

Princípios de segurança e componentes de desenvolvimento recente podem ser considerados como equivalentes a “princípios comprovados e componentes bem ensaiados”, se estes atendem às condições acima mencionadas.

2 A probabilidade de uma falha na categoria 1 é menor que na categoria B. Conseqüentemente a perda da função de segurança é menos provável.

3 Quando um defeito ocorre ele pode levar à perda da função de segurança. Para atender aos requisitos do anexo A da EN 292-2:1991, medidas adicionais, que não são proporcionadas pelas partes relacionadas à segurança de sistemas de comando, podem ser necessárias.

**6.2.3 Categoria 2**

Devem ser aplicados os requisitos da categoria B, o uso de princípios de segurança comprovados e os requisitos desta subseção.

As partes de sistemas de comando relacionadas à segurança, de categoria 2, devem ser projetadas de tal forma que sejam verificadas em intervalos adequados pelo sistema de comando da máquina. A verificação das funções de segurança deve ser efetuada:

- na partida da máquina e antes do início de qualquer situação de perigo, e

- periodicamente durante a operação, se a avaliação do risco e o tipo de operação mostrarem que isso é necessário.

O início dessa verificação pode ser automático ou manual. Qualquer verificação da(s) função(ões) de segurança deve:

- permitir a operação se nenhum defeito foi constatado, ou

- gerar um sinal de saída, que inicia uma ação apropriada do comando, se um defeito foi constatado. Sempre que possível, esse sinal deve comandar um estado seguro. Quando não for possível comandar um estado seguro, como, por exemplo, fusão de contatos no dispositivo final de comutação, a saída deve gerar um aviso do perigo.

A verificação por si só não deve levar a uma situação de perigo. O equipamento de verificação pode ser parte integrante, ou não, da parte(s) relacionada(s) à segurança, que processa(m) a função de segurança.

Após a detecção de um defeito, o estado seguro deve ser mantido até que o defeito tenha sido sanado.

NOTAS

1 Em alguns casos a categoria 2 não é aplicável, em razão de não ser possível a verificação a todos os componentes, como, por exemplo, pressostatos ou sensores de temperatura.

2 Em geral, a categoria 2 pode ser alcançada com técnicas eletrônicas, como, por exemplo, em equipamento de proteção e sistemas específicos de comando.

3 O comportamento de sistema de categoria 2 permite que:

- a ocorrência de um defeito leve à perda da função de segurança entre as verificações;

- a perda da função de segurança é detectada pela verificação.

**6.2.4 Categoria 3**

Devem ser aplicados os requisitos da categoria B, o uso de princípios comprovados de segurança e os requisitos desta subseção.

Partes relacionadas à segurança de sistemas de comando de categoria 3 devem ser projetadas de tal forma que um defeito isolado, em qualquer dessas partes, não leve à perda das funções de segurança. Defeitos de modos comuns devem ser considerados, quando a probalidade da ocorrência de tal defeito for significante. Sem-

pre que, razoavelmente praticável, o defeito isolado deve ser detectado durante ou antes da próxima solicitação da função de segurança.

NOTAS

1 Este requisito de detecção do defeito isolado não significa que todos os defeitos serão detectados. Conseqüentemente, o acúmulo de defeitos não detectados pode levar a um sinal de saída indesejado e a uma situação de perigo na máquina. Exemplos típicos de medidas utilizadas para a detecção de defeitos são os movimento conectados de relés de contato ou a monitoração de saídas elétricas redundantes.

2 Se necessário, em razão da tecnologia e aplicação, os elaboradores de normas do tipo C devem fornecer maiores detalhes sobre a detecção de defeitos.

3 O comportamento de sistema de categoria 3 permite que:

- quando o defeito isolado ocorre, a função de segurança sempre é cumprida;

- alguns, mas não todos, defeitos sejam detectados;

- o acúmulo de defeitos não detectados leve à perda da função de segurança.

4 “Sempre que razoavelmente praticável” significa que as medidas necessárias para à detecção de defeitos e o âmbito em que são implementadas depende, principalmente, da conseqüência de um defeito e da probabilidade da ocorrência desse defeito, dentro dessa aplicação. A tecnologia aplicada irá influenciar as possibilidades da implementação da detecção de defeitos.

**6.2.5 Categoria 4**

Devem ser aplicados os requisitos da categoria B, o uso de princípios comprovados de segurança e os requisitos desta subseção.

Partes de sistemas de comando relacionadas à segurança, de categoria 4, devem ser projetadas de tal forma que:

- uma falha isolada em qualquer dessas partes relacionadas à segurança não leve à perda das funções de segurança, e

- a falha isolada é detectada antes ou durante a próxima atuação sobre a função de segurança, como, por exemplo, imediatamente, ao ligar o comando, ao final do ciclo de operação da máquina. Se essa detecção não for possível, o acúmulo de defeitos não deve levar à perda das funções de segurança.

Se a detecção de certos defeitos não for possível ao menos durante a verificação seguinte à ocorrência do defeito, por razões de tecnologia ou engenharia de circuitos, a ocorrência de defeitos posteriores deve ser admitida. Nessa situação, o acúmulo de defeitos não deve levar à perda das funções de segurança.

A revisão de defeitos pode ser suspensa, quando a probabilidade de ocorrência de defeitos posteriores, for considerada como sendo suficientemente baixa. Nesse caso, o número de defeitos, em combinação, que precisam ser levados em consideração, dependerá da tecnologia, estrutura e aplicação, mas deve ser suficiente para atingir o critério de detecção.

NOTAS

1 Na prática, o número de defeitos; que precisam ser considerados variará consideravelmente; por exemplo, no caso de circuitos complexos de microprocessadores, um grande número de defeitos pode existir, porém em um circuito eletroidráulico, a consideração de três (ou mesmo dois) defeitos pode ser suficiente.

Essa revisão de defeitos pode ser limitada a dois defeitos em combinação, quando:

- a taxa de defeitos de componentes for baixa, e

- os defeitos em combinação são bastante independentes uns dos outros, e

- a interrupção da função de segurança ocorre somente quando os defeitos aparecem em uma certa ordem.

Se defeitos posteriores ocorrerem como resultado do primeiro defeito isolado, o primeiro e todos os defeitos conseqüentes devem ser considerados como defeitos isolados.

Defeitos de modo comum devem ser levados em consideração, por exemplo, utilizando diversidade, procedimentos especiais para identificar tais defeitos.

2 No caso de estruturas de circuitos complexos (por exemplo, microprocessadores, redundâncias completas), a revisão de defeitos é geralmente executada em nível estrutural, isto é, baseado em grupos de montagem.

3 O comportamento de sistema de categoria 4 permite que:

- quando os defeitos ocorrerem, a função de segurança seja sempre processada;

- os defeitos serão detectados a tempo de impedir a perda da função de segurança.

**Tabela 2 - Resumo dos requisitos por categorias (para requisitos plenos, ver seção 6)**

| Categoria[1)] | Resumo de requisitos | Comportamento do sistema[2)] | Princípios para atingir a segurança |
|---|---|---|---|
| B (ver 6.2.1) | Partes de sistemas de comando, relacionadas à segurança e/ou seus equipamentos de proteção, bem como seus componentes, devem ser projetados, construídos, selecionados, montados e combinados de acordo com as normas relevantes, de tal forma que resistam às influências esperadas | A ocorrência de um defeito pode levar à perda da função de segurança | Principalmente caracterizado pela seleção de componentes |
| 1 (ver 6.2.2) | Os requisitos de B se aplicam<br>Princípios comprovados e componentes de segurança bem testados devem ser utilizados | A ocorrência de um defeito pode levar à perda da função de segurança, porém a probabilidade de ocorrência é menor que para a categoria B | |
| 2 (ver 6.2.3) | Os requisitos de B e a utilização de princípios de segurança comprovados se aplicam<br><br>A função de segurança deve ser verificada em intervalos adequados pelo sistema de comando da máquina | - A ocorrência de um defeito pode levar à perda da função de segurança entre as verificações<br><br>- A perda da função de segurança é detectada pela verificação | Principalmente caracterizado pela estrutura |
| 3 (ver 6.2.4) | Os requisitos de B e a utilização de princípios de segurança comprovados se aplicam<br><br>As partes relacionadas à segurança devem ser projetadas de tal forma que:<br><br>- um defeito isolado em qualquer dessas partes não leve à perda da função de segurança, e<br><br>- sempre que razoavelmente praticável, o defeito isolado seja detectado | - Quando um defeito isolado ocorre, a função de segurança é sempre cumprida<br><br>- Alguns defeitos, porém não todos, serão detectados<br><br>- O acúmulo de defeitos não detectados pode levar à perda da função de segurança | Principalmente caracterizado pela estrutura |
| 4 (ver 6.2.5) | Os requisitos de B e a utilização de princípios de segurança comprovados se aplicam<br><br>As partes relacionadas à segurança devem ser projetadas de tal forma que:<br><br>- um defeito isolado em qualquer dessas partes não leve à perda da função de segurança, e<br><br>- o defeito isolado seja detectado durante ou antes da próxima demanda da função de segurança. Se isso não for possível, o acúmulo de defeitos não pode levar à perda das funções de segurança | - Quando os defeitos ocorrem, a função de segurança é sempre cumprida<br><br>- Os defeitos serão detectados a tempo de impedir a perda das funções de segurança | Principalmente caracterizado pela estrutura |

[1)] As categorias não objetivam sua aplicação em uma seqüência ou hierarquia definidas, com relação aos requisitos de segurança.

[2)] A apreciação dos riscos indicará se a perda total ou parcial da(s) função(ões) de segurança, conseqüente de defeitos, é aceitável.

**6.3 Seleção e combinação de partes relacionadas à segurança de diferentes categorias**

As funções de segurança (ver 3.6 e seção 5) são especificadas pelo procedimento descrito em 4.3 (figura 1, passo 3). Categorias de acordo com 6.2 devem ser selecionadas para todas as partes do sistema de comando relacionadas à segurança. O projeto e a seleção de partes relacionadas à segurança do sistema de comando devem ser feitos de acordo com as seções 4 e 5. Uma função de segurança isolada pode ser processada por uma ou mais partes relacionadas à segurança. De forma similar, várias funções de segurança podem ser processadas por uma ou mais partes relacionadas à segurança. Na prática pode ser necessário implementar uma ou mais funções de segurança para atingir a redução do risco.

Quando uma função de segurança é processada por várias partes relacionadas à segurança, como, por exemplo, sensores, unidade de comando, elementos de controle de potência, essas partes podem ser de uma categoria e/ou de diferentes categorias em combinação.

Quando partes relacionadas à segurança de mesma ou diferentes categorias são usadas em combinação para atender a uma função de segurança, uma análise da combinação deve ser incluída na validação geral requerida no passo 5 de 4.3. Essa análise é mais simples se as categorias de algumas ou de todas as partes relacionadas à segurança já forem conhecidas.

A seleção de uma categoria para uma parte específica relacionada à segurança do sistema de comando depende principalmente de:

- redução de risco a ser atingida pela função de segurança, para a qual a parte contribui;

- probabilidade de ocorrência de defeito(s) nessa parte;

- aumento de risco, no caso de defeito(s) nessa parte;

- possibilidades de evitar defeito(s) nessa parte;

- tecnologia aplicada.

Informação adicional para a seleção de categorias é dada no anexo A.

## 7 Consideração de defeitos

### 7.1 Generalidades

De acordo com a categoria requerida, as partes relacionadas à segurança devem ser selecionadas como função de suas habilidades em resistir a defeitos (ver 4.2). Para avaliar sua habilidade em resistir a defeitos, os vários modos de falhas devem ser considerados. Certos defeitos também podem ser excluídos (ver 7.2).

O anexo C lista alguns dos defeitos e falhas significantes para as várias tecnologias. A lista de defeitos relacionada no anexo C não é exclusiva e, se necessário, defeitos adicionais devem ser considerados e listados. Em tais casos, o método de validação deve também ser claramente elaborado.

De maneira geral, o seguinte critério de defeitos deve ser levado em consideração:

- se, como conseqüência de um defeito, outros componentes falham, o primeiro defeito e os defeitos seguintes devem ser considerados como um defeito isolado;

- defeitos de modo comum são considerados como defeito isolado;

- não é considerada a ocorrência simultânea de dois defeitos independentes.

Para informações detalhadas, ver EN 982 e EN 983.

### 7.2 Exclusão de defeitos

É impraticável a avaliação das partes de sistemas de comando relacionadas à segurança, sem assumir que certos defeitos podem ser excluídos. Os defeitos que podem ser excluídos são um compromisso entre os requisitos técnicos para segurança e as possibilidades teóricas de ocorrência. Isso é influenciado pelo projeto, dimensionamento, instalação e arranjo dos componentes nas partes relacionadas à segurança. O projetista deve declarar, justificar e listar todas as exclusões de defeitos relevantes.

A exclusão de defeitos pode ser baseada em:

- improbabilidade de ocorrência de certos defeitos;

- experiência técnica genérica, que pode ser considerada independentemente da aplicação em questão;

- requisitos técnicos conseqüentes da aplicação e o risco específico sob consideração.

## 8 Validação

### 8.1 Generalidades

Esta seção explica os requisitos do passo 5 na seção 4.

A finalidade da validação é a determinação do nível de conformidade da especificação das partes relacionadas à segurança do sistema de comando, com referência aos requisitos de segurança especificados para a máquina. A validação consiste na execução de ensaios e aplicação de análises, de acordo com o plano de validação (ver 8.2).

O projeto das partes relacionadas à segurança do sistema de comando deve ser validado. A validação deve demonstrar que as partes relacionadas à segurança atingem:

- todos os requisitos da categoria específica (ver seção 6), e

- as características de segurança especificadas para a parte, como definido nos princípios de projeto.

A validação das partes relacionadas à segurança de sistemas de comando deve conter os seguintes elementos:

- seleção da estratégia de validação (um plano de validação);

- gerenciamento e execução de atividades de validação (especificação de ensaios, procedimentos de ensaios, procedimentos de análises);

- documentação (relatórios auditáveis de todas as atividades de validação e decisões).

**8.2 Plano de validação**

O plano de validação deve identificar os requisitos para a efetivação de todos os estágios do processo de validação. O plano deve ser desenvolvido em paralelo ao projeto da parte relacionada à segurança do sistema de comando ou pode ser especificado em normas relevantes do tipo C. O plano deve incluir uma descrição de todos os requisitos para:

a) validação por análise;

b) validação por ensaios, incluindo:

1) ensaio da função de segurança especificada;

2) ensaio da categoria especificada;

3) ensaio do dimensionamento e conformidade a parâmetros ambientais.

**8.3 Validação por análise**

Em geral, análises são necessárias para validar o alcance da redução do risco. Exemplos de ferramentas de análise incluem lista de defeitos (ver seção 7), árvore de análise de defeitos, modo de falhas e análise de efeitos, análise crítica e lista de verificação para defeitos sistemáticos.

**8.4 Validação por ensaio**

**8.4.1 Ensaio das funções de segurança especificadas**

Um passo importante é o ensaio das funções de segurança (das partes relacionadas à segurança de sistemas de comando), para completa conformidade com suas características especificadas. É importante a verificação, quanto a erros e particularmente por omissões, quando da formulação da especificação e durante o desenvolvimento da máquina.

O propósito do ensaio das funções de segurança é para assegurar que os sinais de saída relacionados à segurança estão corretos e logicamente dependentes dos sinais de entrada. Os ensaios devem abranger todas as condições normais e as anormais previsíveis na simulação estática e dinâmica, como necessário da apreciação de riscos, para validar o sistema.

**8.4.2 Ensaio das categorias especificadas**

As categorias baseiam-se sobre o comportamento no evento de um defeito. O ensaio deve demonstrar que esse requisito é atendido. Os procedimentos de ensaio devem ser escolhidos baseados em dois critérios: tecnologia e complexidade do sistema de comando. Principalmente, os seguintes métodos se aplicam:

- uma verificação teórica e uma análise do comportamento dos diagramas de circuitos;

- ensaios práticos do circuito atual e simulação de defeitos dos componentes atuais, particularmente em áreas de dúvidas, do comportamento identificado durante a verificação e análise teórica;

- uma simulação do comportamento do sistema, por exemplo, por meio do *hardware* e/ou modelos de *software*.

Em algumas aplicações, quando as partes relacionadas à segurança de sistemas de comando forem conectadas de forma complexa, é usualmente necessário dividir as partes relacionadas à segurança conectadas em vários subsistemas funcionais e submeter exclusivamente as interfaces aos ensaios de simulação de defeitos.

Um guia para avaliação de sistemas eletrônicos programáveis é dado no anexo E.

**8.4.3 Ensaio de dimensionamento e conformidade com parâmetros ambientais**

Esses ensaios devem demonstrar que o desempenho especificado no projeto é alcançado em todos os modos de operação e condições ambientais especificadas. Os ensaios devem incluir, por exemplo, ensaio da estrutura mecânica, tensão nominal, temperatura, umidade, vibração, impacto, compatibilidade eletromagnética e influência dos materiais processados.

**8.5 Relatório de validação**

Na conclusão do processo de validação, um relatório de validação sobre segurança deve ser elaborado, resumindo os ensaios e análises, indicando quais foram integralmente executados, incluindo seus resultados. O relatório deve identificar especificamente:

- todos os itens ensaiados;

- pessoal responsável pelos ensaios;

- equipamento de ensaio (incluindo detalhes de calibração) e ferramentas de simulação;

- análises e ensaios executados;

- problemas encontrados e como foram resolvidos.

Os resultados devem ser documentados e arquivados em forma auditável.

NOTA - A conformidade com 8.5 ajudará o fabricante na atualização do arquivo técnico da construção, com respeito às partes relacionadas à segurança de sistemas de comando.

## 9 Manutenção

Manutenção preventiva ou corretiva é usualmente necessária para manter o desempenho especificado das partes relacionadas à segurança. Com o tempo, o desvio do desempenho especificado pode levar à deterioração da segurança ou a situações de perigo. Para identificar tais desvios, inspeções manuais periódicas são, algumas vezes, necessárias.

As condições para a manutenção de partes relacionadas à segurança de sistemas de comando devem seguir os princípios da EN 292-2. Todas as informações para manutenção devem obedecer à EN 292-2.

## 10 Informações para utilização

A EN 292-2 e outros documentos relevantes (por exemplo, a EN 60204-1) devem ser aplicados. Em particular, as informações importantes para o uso seguro das partes relacionadas à segurança do sistema de comando devem ser fornecidas ao usuário. Isso inclui, mas não é limitado a:

- limites da(s) categoria(s) selecionada(s) das partes relacionadas à segurança, incluindo qualquer exclusão de defeito;

NOTA - Quando a exclusão de defeitos é essencial na manutenção da(s) categoria(s) selecionada(s) e no desempenho da segurança, informação apropriada (por exemplo, modificação, manutenção e reparo) será necessária para assegurar a continuada justificativa da exclusão de defeito.

- efeitos dos desvios do desempenho especificado sobre as funções de segurança;

- descrição clara da interface entre as partes relacionadas à segurança do sistema de comando e dispositivos de proteção;

- tempo de resposta;

- limites de operação (incluindo condições ambientais);

- indicação e alarmes;

- pausa e suspensão das funções de segurança;

- modos de comando;

- manutenção (ver seção 9);

- listas de verificação para manutenção;

- facilidade de acesso e substituição de partes internas;

- meios para fácil e segura eliminação de problemas.

Sempre que se fornecerem informações sobre as categorias de partes relacionadas à segurança do sistema de comando, devem ser referendadas da seguinte forma:

- NBR 14153 Categoria B;

- NBR 14153 Categoria 1;

- NBR 14153 Categoria 2;

- NBR 14153 Categoria 3;

- NBR 14153 Categoria 4.

**/ANEXO A**

## **Anexo A** (informativo)
## Questionário para o processo de projeto

Esse anexo lista alguns aspectos importantes que devem ser considerados durante o processo de projeto (ver 4.3).

### A.1 Que reação é necessária da parte relacionada à segurança do sistema de comando, quando um defeito ocorre?

a) Não é necessária qualquer ação especial.

b) Reação de segurança é necessária dentro de um certo tempo.

c) Reação de segurança é imediatamente necessária.

### A.2 Em que parte(s) relacionada(s) à segurança de sistemas de comando os defeitos devem ser admitidos?

a) Somente naquelas partes em que (por experiência) os defeitos ocorrem com relativa freqüência, como, por exemplo, nos sensores e cabeamento periférico.

b) Em partes auxiliares.

c) Em todas as partes relacionadas à segurança.

### A.3 Foram considerados os defeitos sistemáticos e os ocasionais?

### A.4 Que defeitos devem ser admitidos nos componentes das partes relacionadas à segurança do sistema de comando?

a) Defeitos apenas nos componentes que não foram bem ensaiados.

NOTA - “Bem ensaiados” não no sentido de confiabilidade, mas sob o ponto de vista de segurança (ver 6.2.2).

b) Defeitos em todos os componentes.

### A.5 Foi selecionada a correta categoria de referência com respeito aos requisitos para a detecção de defeitos?

a) Requisitos normais para a detecção de defeitos.

NOTA - Isso significa que todos os defeitos que podem ser detectados com métodos relativamente simples devem ser detectados.

b) Requisitos severos para a detecção de defeitos.

NOTA - Isso significa que técnicas devem ser empregadas para possibilitar a detecção da maioria dos defeitos. Se isso não for razoavelmente praticável, a combinação de defeitos deve ser admitida (acúmulo de defeitos - ver 6.2.5).

### A.6 Qual deve ser a ação seguinte do sistema de comando, se um defeito foi constatado?

a) A máquina deve ser levada a um estado predeterminado, conforme requerido pela avaliação de riscos.

b) A operação posterior da máquina pode ser permitida até o reparo do defeito.

c) A indicação do(s) defeito(s) é suficiente (por exemplo, sinal de advertência por unidade visual).

### A.7 O que é necessário para atingir os requisitos de manutenção?

a) Fornecimento de informações sobre os efeitos de desvios das especificações de projeto.

b) Indicação automática da necessidade de manutenção.

c) Fixação da freqüência de manutenção.

d) Informação da vida de componentes.

e) Fornecimento de meios de diagnose e pontos de ensaio.

f) Precauções especiais para segurança durante a manutenção.

### A.8 Que métodos devem ser empregados para a detecção de defeitos?

a) Detecção automática de defeitos, na medida em que for necessário.

b) Detecção manual de defeitos, por exemplo, por inspeção periódica.

c) Por mais de um método.

### A.9 A redução de risco foi atingida?

a) Pode a redução do risco ser atingida mais facilmente com uma diferente combinação de medidas de redução do risco?

b) Verificar se as medidas implementadas:

- não reduzem a habilidade da máquina em desenvolver sua função;

- não geram perigos ou problemas novos ou inesperados.

c) As soluções são válidas para todas as condições de operação e para todos os procedimentos?

d) Essas soluções são compatíveis com cada uma das outras?

e) A especificação de segurança está correta?

**A.10 Foram considerados princípios ergonômicos?**

a) As partes relacionadas à segurança do sistema de comando, incluindo os dispositivos de proteção, oferecem facilidade de uso?

b) O acesso ao sistema de comando é fácil e seguro?

c) Foi dada prioridade aos sinais de advertência (por exemplo realçados)?

**A.11 Foram as relações entre segurança, confiabilidade, disponibilidade e ergonomia otimizadas, de tal forma que as medidas de segurança sejam mantidas durante a vida do sistema e não incentivem a usuários a anulação das funções de segurança?**

**/ANEXO B**

## **Anexo B** (informativo)
## Guia para a seleção de categorias

### B.1 Generalidades

Este anexo descreve um método simplificado baseado na NBR 14009 (particularmente com relação à simplificação dos elementos de risco) para seleção de categorias apropriadas como ponto de referência para o projeto das diversas partes relacionadas à segurança de sistemas de comando.

O guia deste anexo deve ser considerado como parte da apreciação do risco dada na NBR 14009 e não como um substituto para a mesma.

É importante que o projeto de partes relacionadas à segurança de sistema de comando, incluindo a seleção de categorias, como descrito na seção 4, seja baseado na apreciação dos riscos, utilizando seus princípios dados na NBR 14009, e seja parte da apreciação do risco total da máquina.

A quantificação do risco é usualmente muito difícil ou impossível e este método apenas diz respeito à contribuição para a redução do risco, feita pelas partes relacionadas à segurança de sistemas de comando. Este método fornece apenas uma estimativa da redução do risco e tem a intenção de orientar o projetista e o elaborador de normas a escolher a categoria, baseado em seu comportamento, no caso de um defeito. Entretanto, isso é apenas um aspecto e outras influências também irão contribuir para a avaliação de que a adequada segurança tenha sido atingida. Isso inclui, por exemplo, confiabilidade de componentes, tecnologia aplicada, aplicação particular, as quais podem indicar um desvio da categoria, antecipadamente escolhida.

O método é como segue:

A severidade do ferimento (representada por *S*) é relativamente fácil de ser estimada (por exemplo, laceração, amputação, fatalidade).

Para a freqüência da ocorrência, parâmetros auxiliares são usados para melhorar a estimativa. Esses parâmetros são:

- freqüência e tempo de exposição ao perigo (*F*);

- possibilidade de evitar o perigo (*P*).

A experiência tem mostrado que esses parâmetros podem ser combinados, como mostrado na figura B.1, para fornecer uma graduação do risco, de baixo a alto. É enfatizado que isso é um processo qualitativo, que fornece apenas uma estimativa do risco.

Na figura B.1, a categoria preferencial é indicada por um círculo maior totalmente cheio. Em algumas aplicações o projetista, ou o elaborador de normas do tipo C, pode desviar para outra categoria, indicada por um círculo totalmente preenchido menor, ou um círculo maior, vazio. Outras, diferentes das categorias preferenciais, podem ser utilizadas (ver 6.3), porém o comportamento pretendido do sistema na ocorrência de defeitos deve ser mantido. As razões para o desvio devem ser expostas. Essas razões para a seleção de outra categoria com relação à preferencial podem ser a aplicação de outra tecnologia, como, por exemplo, componentes hidráulicos ou eletromecânicos bem ensaiados (categoria 1), em combinação com sistemas elétricos ou eletrônicos (categoria 3 ou 4). Quando categorias indicadas com um círculo pequeno na figura B.1 forem selecionadas, medidas adicionais podem ser necessárias, como, por exemplo:

- superdimensionamento ou aplicação de técnicas, que levem à exclusão de defeitos;

- utilização de monitoração dinâmica.

Por exemplo, uma estimativa de risco, com um parâmetro S1 (ver B.2.1), determina uma categoria da parte relacionada à segurança do sistema de comando como categoria 1. Em algumas aplicações, o projetista ou o elaborador de normas do tipo C pode escolher a categoria B pela utilização de outras medidas de proteção.

### B.2 Guia para a seleção dos parâmetros *S*, *F* e *P* para a estimativa do risco

#### B.2.1 Severidade do ferimento *S1* e *S2*

Na estimativa do risco proveniente de um defeito na parte relacionada à segurança de um sistema de comando, apenas ferimentos leves (normalmente reversíveis) e ferimento sérios (normalmente irreversíveis, incluindo a morte) são considerados.

Para tomar uma decisão, as conseqüências usuais de acidentes e processos normais de cura devem ser levadas em consideração na determinação de *S1* e *S2*, por exemplo, contusões e/ou lacerações, sem complicações devem ser classificadas como *S1*, enquanto que uma amputação ou morte deve ser classificada como *S2*.

#### B.2.2 Freqüência e/ou tempo de exposição ao perigo *F1* e *F2*

Um período de tempo geralmente válido para a escolha do parâmetro *F1* ou *F2* não pode ser especificado. Entre-tanto, a seguinte explicação pode ajudar a tomar a decisão correta, em caso de dúvida.

*F2* deve ser selecionado, se a pessoa estiver, freqüentemente ou continuadamente, exposta ao perigo. É irrelevante se a mesma pessoa ou pessoas diferentes estiverem expostas ao perigo em sucessivas ocasiões, como, por exemplo, para a utilização de elevadores.

O período de exposição ao perigo deve ser avaliado com base no valor médio observado, com relação ao período total de utilização do equipamento. Por exemplo, se for necessário acessar regularmente as ferramentas da máquina durante sua operação cíclica, para a alimentação e movimentação de peças, *F2* deve ser selecionado. Se o acesso somente for necessário de tempo em tempo, pode-se selecionar *F1*.

**B.2.3 Possibilidade de evitar o perigo *P***

Quando um perigo aparece, é importante saber se ele pode ser reconhecido e quando pode ser evitado, antes de levar a um acidente. Por exemplo, uma importante consideração é se o perigo pode ser diretamente identificado por suas características físicas ou por meios técnicos, por exemplo, indicadores. Outro aspecto importante que influencia a seleção do parâmetro *P* inclui, por exemplo:

- operação com ou sem supervisão;

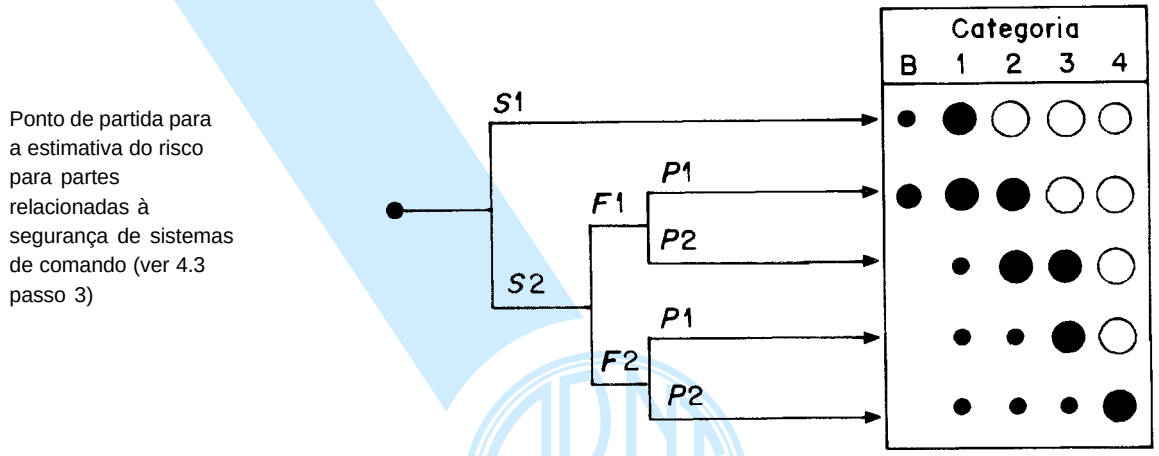
- operação por especialistas ou por não profissionais;

- velocidade com que o perigo aparece, por exemplo, rapidamente ou lentamente;

- possibilidades de se evitar o perigo, por exemplo, por fuga ou por intervenção de terceiros;

- experiências práticas de segurança relativas ao processo.

Quando uma situação de perigo ocorre, *P1* deve apenas ser selecionado se houver uma chance real de se evitar um acidente ou reduzir significativamente o seu efeito. *P2* deve ser selecionado se praticamente não houver chance de se evitar o perigo.




***S* Severidade do ferimento**

*S1* Ferimento leve (normalmente reversível)

*S2* Ferimento sério (normalmente irreversível) incluindo morte

***F* Freqüência e/ou tempo de exposição ao perigo**

*F1* Raro a relativamente freqüente e/ou baixo tempo de exposição

*F2* Freqüente a contínuo e/ou tempo de exposição longo

***P* Possibilidade de evitar o perigo**

*P1* Possível sob condições específicas

*P2* Quase nunca possível

**B, 1 a 4 Categorias para partes relacionadas à segurança de sistemas de comando**

● Categorias preferenciais para pontos de referência (ver 4.2)

● Categorias possíveis que requerem medidas adicionais (ver B.1)

○ Medidas que podem ser superdimensionadas para o risco relevante

**Figura B.1 - Seleção possível de categorias**

/ANEXO C

## **Anexo C** (informativo)
## Lista de alguns dos defeitos e falhas significantes para várias tecnologias

### C.1 Componentes eletroeletrônicos

Alguns defeitos e falhas a considerar são:

- curto-circuito ou circuito aberto, por exemplo, falta de terra (curto-circuito para o condutor de proteção ou para uma parte condutiva), circuito aberto de qualquer condutor;

- curto-circuito ou circuito aberto, ocorrendo em componentes isolados, como, por exemplo, em interruptores, equipamento de controle e regulagem, atuadores da máquina, relés;

- não desacionamento ou não acionamento de elementos eletromagnéticos, como, por exemplo, contatores, relés, solenóides;

- não partida ou não parada de motores, como, por exemplo, servomotores;

- bloqueio mecânico de elementos móveis, soltura ou desmontagem de elementos, como, por exemplo, chaves de posição;

- desvio, além da tolerância de valores para elementos analógicos, como, por exemplo, resistores, capacitores, transistores;

- oscilação (instabilidade) de sinais de saída em componentes integrados;

- perda total ou parcial de função (pior caso), em componentes integrados complexos, como, por exemplo, microprocessadores, sistemas eletrônicos programáveis, aplicações de circuitos integrados específicos.

### C.2 Componentes hidráulicos e pneumáticos

Alguns defeitos e falhas a considerar são:

- não comutação ou comutação incompleta do elemento móvel, como, por exemplo, engripamento de pistão de válvula;

- desvio de posição de controle original do elemento móvel, como, por exemplo, em válvulas direcionais de controle;

- vazamento e modificação do volume do fluxo de vazamento, como, por exemplo, em válvulas direcionais de controle;

- características de controle instáveis em servoválvulas ou válvulas proporcionais;

- perda de pressão ou rompimento de linhas, como, por exemplo, mangueiras, tubos ou em suas conexões;

- obstrução do elemento filtrante (em particular causado por substâncias sólidas);

- pressão e/ou volume de fluxo anormais, como, por exemplo, em bombas hidráulicas, motores hidráulicos, compressores, cilindros;

- falha ou modificação anormal das características dos sinais de entrada ou saída em sensores, como, por exemplo, pressostatos.

### C.3 Componentes mecânicos

Alguns defeitos e falhas a considerar são:

- quebra de molas;

- engripamento ou endurecimento de componentes móveis de guias;

- soltura de fixações, por exemplo, em vibração;

- desgaste, por exemplo, em roldanas, fechos, rolamentos;

- desalinhamento de peças;

- influências ambientais, como, por exemplo, corrosão, temperatura.

**/ANEXO D**

## **Anexo D** (informativo)
## **Relação entre segurança, confiabilidade e disponibilidade para máquinas**

Os conceitos de segurança, confiabilidade e disponibilidade podem ser descritos da seguinte forma:

- Segurança de uma máquina é sua habilidade em desempenhar sua função, ser transportada, instalada, ajustada, sofrer manutenção, ser desmontada e desativada de suas condições de utilização previstas, especificadas em seu manual de instruções (e, em alguns casos, durante um determinado período de tempo, indicado no manual de instruções), sem causar ferimentos ou danos à saúde (ver EN 292-1).

- Confiabilidade é a habilidade da máquina ou componentes, ou equipamentos, em desempenhar uma determinada função, sem falhas, sob condições especificadas para um dado período de tempo (ver EN 292-1)

- Disponibilidade é a habilidade de um item estar no estado adequado para desempenhar uma determinada função, sob condições determinadas, em um dado instante ou em um intervalo de tempo, assumindo-se que os recursos externos necessários são fornecidos (ver IEC 50(191).

A segurança abrange as causas e conseqüências de possíveis acidentes (ferimentos ou danos à saúde). Requisitos de segurança estão relacionados a conceber um sistema que não cause acidentes. Os requisitos de segurança asseguram que o sistema não alcançará um estado de perigo ou inseguro, quando um evento pode causar um acidente. Os requisitos de segurança devem indicar quais as ações a serem tomadas, se um evento imprevisto no ambiente levar a um estado inseguro.

Do ponto de vista de segurança não importa se o sistema não cumpre sua finalidade, contanto que os requisitos de segurança não sejam violados. Por outro lado, é possível que o sistema seja altamente confiável, mas inseguro; por exemplo, um sistema com *software* formalmente verificado, porém onde uma situação relacionada à segurança não foi adequadamente especificada.

A disponibilidade influencia a segurança. A disponibilidade de um sistema implica que a confiabilidade relacionada à segurança é desempenhada; caso contrário, o dispositivo de proteção pode ser desativado.

O projetista tem a responsabilidade de decidir, para cada aplicação, a relação entre disponibilidade, confiabilidade e segurança, para assegurar que a redução do risco seja alcançada.

**/ANEXO E**

## **Anexo E** (informativo)
## **Bibliografia**

Segue abaixo uma relação de publicações que fornece informações adicionais sobre partes relacionadas à segurança de sistema de comando.

### E.1 Publicações sobre sistemas eletrônicos programáveis

- EN 61000-4-1 - Eletromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 1: Overview of immunity tests - Basic EMC publication (IEC 1000-4-1 : 1992)

- IEC 1508 - Functional safety: safety-related systems (provisonal title)

- DIN V VDE 0801 - Principles for computers in safety related computer systems, January 1990

- HSE Guidelines - Programmable Eletronic Systems in Safety Related Applications Part 1 (ISBN 0 11 883906 6) and Part 2 (ISBN 0 11 883906 3)

- Personal Safety in Microprocessor Control Systems (CECR - 184, Elektronikcentralen, Denmark)

### E.2 Outras publicações

- IEC 68 Basic environmental testing procedures