Especificação de Sistemas Críticos

Objetivos

- Explicar como os requisitos de confiabilidade podem ser identificados por meio da análise de riscos enfrentados pelos sistemas críticos
- Explicar como os requisitos de segurança são gerados a partir da análise de riscos do sistema
- Explicar a derivação dos requisitos de proteção
- Descrever as métricas usadas para especificação de confiabilidade

Tópicos cobertos

- Especificação dirigida a riscos
- Especificação de segurança
- Especificação de proteção
- Especificação de confiabilidade de software

Requisitos de confiança

- Requisitos funcionais: são gerados para definir os recursos de verificação e de recuperação de erros e proteção contra falhas de sistema.
- Requisitos não funcionais: são gerados para definir a confiabilidade e a disponibilidade necessaria ao sistema.
- Requisitos de exclusão: são os que definem os estados e as condições que não devem surgir.

Especificação dirigida a riscos

- A especificação de sistemas críticos deve ser dirigida a riscos.
- Essa abordagem foi amplamente usada em sistemas críticos de segurança e de proteção.
- O objetivo do processo de especificação é compreender os riscos (segurança, proteção, etc.) enfrentados pelo sistema e definir requisitos que reduzam esses riscos.

Estágios da análise baseada em riscos

- Identificação de riscos
  - Identificar os riscos potenciais que podem surgir.
- Análise e classificação de riscos
  - Avaliar a severidade de cada risco.
- Decomposição de riscos
  - Decompor os riscos para descobrir suas causas potenciais de origem.
- Avaliação de redução de riscos
  - Definir como cada risco deve ser eliminado ou reduzido quando o sistema é projetado.

Especificação dirigida a riscos

Figura 9.1 Especificação dirigida a riscos.

Identificação de riscos

- Identificar os riscos enfrentados pelo sistema crítico.
- Em sistemas críticos de segurança, os riscos são os perigos que podem levar a acidentes.
- Em sistemas críticos de segurança, os riscos são os ataques potenciais sobre o sistema.
- Na identificação de riscos, você deve identificar as classes de risco e as posições dos riscos nessas classes
  - Falha de serviço;
  - Riscos elétricos.

Riscos da bomba de insulina

- Dose excessiva de insulina (falha de serviço).
- Dose insuficiente de insulina (falha de serviço).
- Falha de energia devido ao desgaste da bateria (elétrico).
- Interferência elétrica com outros equipamentos médicos (elétrico)
- Mau contato de sensor e atuador (físico)
- Partes do equipamento quebradas no corpo (físico).
- Infecção causada por introdução de equipamento (biológico).
- Reação alérgica aos materiais ou à insulina (biológico).

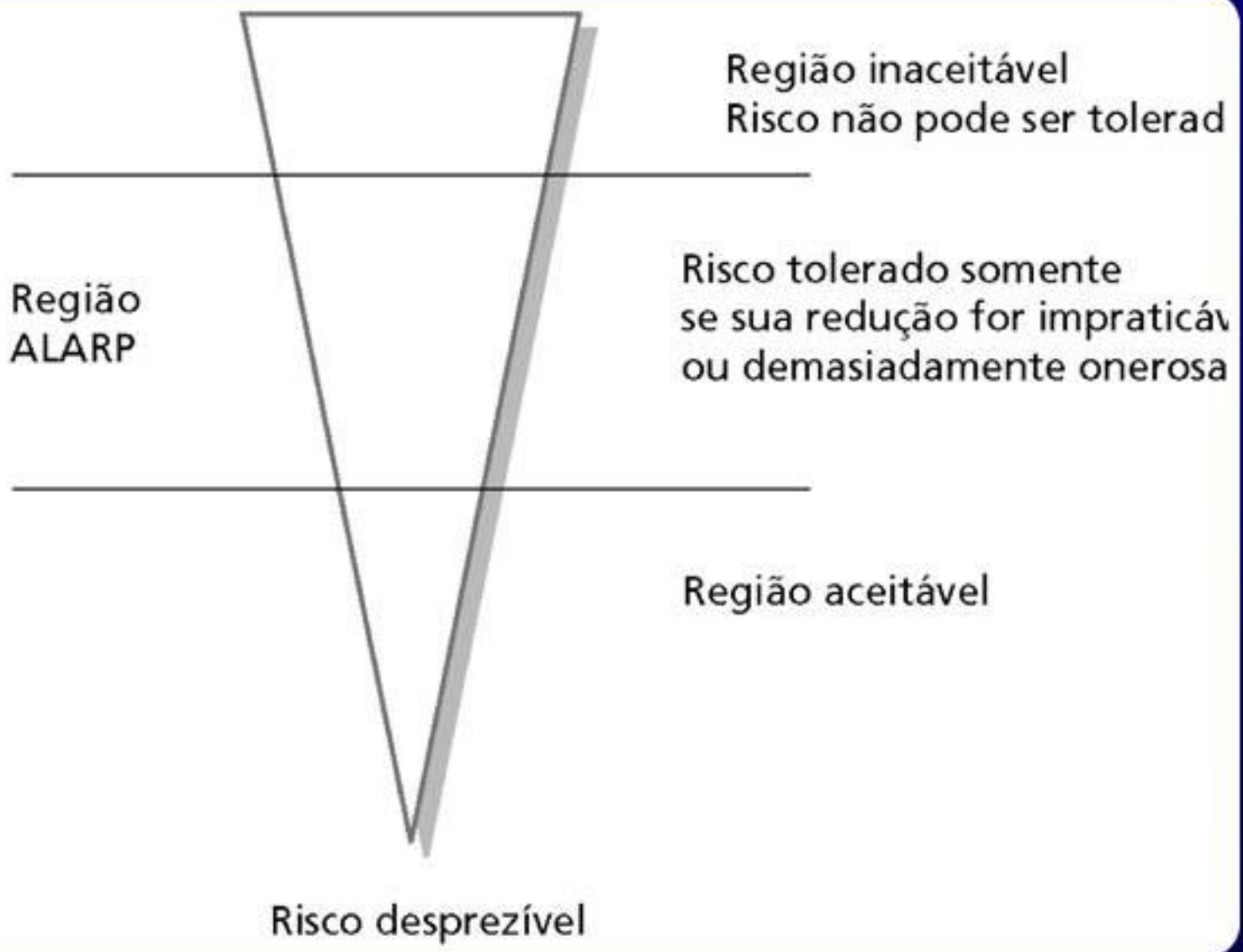
Análise e classificação de riscos

- O processo é relacionado com o entendimento da probabilidade de ocorrência de um risco e as conseqüências potenciais, se um acidente ou incidente ocorrer.
- Os riscos podem ser classificados como:
  - Intolerável. Nunca deve surgir ou resultar em um acidente.
  - Tão baixo quanto razoavelmente prático (ALARP). Deve minimizar a possibilidade de um risco dadas as restrições como custo e prazo.
  - Aceitável. As conseqüêncas do risco são aceitáveis, e custos extras não devem ser incorridos para reduzir a probabilidade de perigo.

Níveis de risco

Figura 9.2

Níveis de risco.



Aceitabilidade social de riscos

- A aceitabilidade de um risco é determinado pelas considerações humana, social e política.
- Na maioria das sociedades, os limites entre as regiões são movidas para cima com o tempo, isto é, a sociedade é menos propensa a aceitar riscos
  - Por exemplo, os custos de limpeza de poluição podem ser menores que os custos de prevenção, mas isso pode não ser socialmente aceitável.
- A avaliação de riscos é subjetiva
  - Os riscos são identificados como provável, improvável, etc. Isso depende de quem está realizando a avaliação.

Avaliação de riscos

- Estima a probablidade e a severidade do risco
- Normalmente, não é possível fazer isso de forma precisa e, assim, os valores relativos são usados como 'improvável', 'rara', 'muito alta', etc.
- O objetivo deve ser excluir os riscos cujas ocorrências são prováveis, ou aqueles que têm alta severidade.

Avaliação de riscos
Bomba de insulina

Tabela 9.1 Análise de riscos de perigos identificados em uma bomba de insulina

Perigo identificado	Probabilidade do perigo	Gravidade do perigo	Risco estimado	Nível de aceitação
1. Dose excessiva de insulina	Média	Alta	Alto	Intolerável
2. Dose insuficiente de insulina	Média	Baixa	Baixo	Aceitável
3. Falha de energia	Alta	Baixa	Baixo	Aceitável
4. Equipamento ajustado incorretamente	Alta	Alta	Alto	Intolerável
5. Quebra do equipamento durante o uso no paciente	Baixa	Alta	Médio	ALARP
6. Equipamento causa infecção	Média	Média	Médio	ALARP
7. Interferência elétrica	Baixa	Alta	Médio	ALARP
8. Reação alérgica	Baixa	Baixa	Baixo	Aceitável

Decomposição de riscos

- Está relacionada com a descoberta das causas da origem dos riscos em um sistema particular.
- Essas técnicas foram derivadas, principalmente, de sistemas críticos de segurança, e podem ser:
  - Técnicas indutivas *bottom-up*. Iniciam com uma falha de sistema proposta e avaliam os perigos que poderiam ocorrer a partir dessa falha;
  - Técnicas dedutivas *top-down*. Iniciam com um perigo e deduzem-se quais poderiam ser as causas.

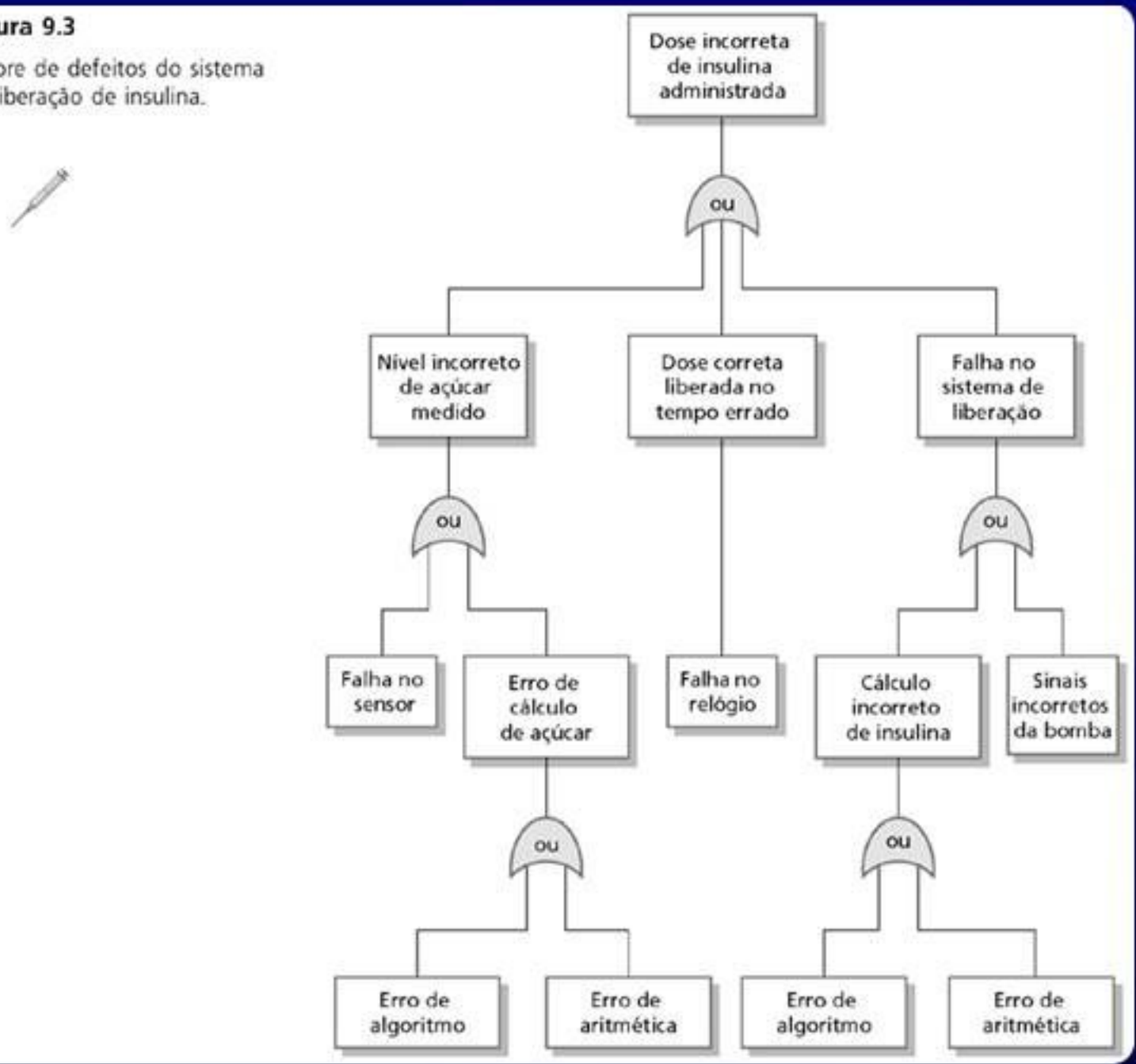
Análise de árvore de defeitos

- É uma técnica dedutiva *top-down.*
- Coloca o risco ou perigo na raiz da árvore e idenfica os estados de sistema que poderiam levar a esse perigo.
- Onde apropriado, ligar esses estados por meio dos símbolos ‘e’ ou ‘ou’.
- A meta deve ser minimizar o número de causas isoladas de falha de sistema.

Árvore de defeitos de bomba de insulina

Figura 9.3

Árvore de defeitos do sistema de liberação de insulina.



Avaliação de redução de riscos

- O objetivo desse processo é identificar requisitos de confiança que especificam como os riscos deveriam ser gerenciados e assegurar que acidentes/incidentes não ocorram.
- Estratégias de redução de riscos
  - Prevenção de riscos;
  - Detecção e remoção de riscos;
  - Limitação de danos.

Uso estratégico

- Em sistemas críticos, normalmente são usadas uma mistura de estratégias.
- Em um sistema de controle de planta química, o sistema incluirá sensores para detectar e corrigir excesso de pressão no reator.
- Contudo, incluirá também um sistema de proteção independente que abre uma válvula de alívio caso seja detectado algum perigo de alta pressão.

Riscos de software
Bomba de insulina

- Erros de aritmética
  - Um cálculo causa *overflow* ou *underflow* do valor de uma variável;
  - Incluir talvez um tratador de exceção para cada tipo de erro aritmético.
- Erros de algoritmo
  - Comparar a dose a ser liberada com a dose anterior ou doses máximas seguras. Reduzir a dose caso seja muito alta.

Requisitos de segurança
Bomba de insulina

Quadro 9.1 Exemplos de requisitos de segurança para uma bomba de insulina

RS1:	O sistema não deve fornecer uma dose única de insulina maior do que a dose máxima especificada para um usuário do sistema.
RS2:	O sistema não deve fornecer uma dose diária cumulativa de insulina maior do que a dose máxima especificada para um usuário do sistema.
RS3:	O sistema deve incluir um recurso de diagnóstico de hardware executado pelo menos quatro vezes por hora.
RS4:	O sistema incluirá um manipulador de exceções para todas as exceções identificadas na Tabela 3.
RS5:	Um alarme audível será emitido quando qualquer anomalia de hardware ou software for descoberta e uma mensagem de diagnóstico, conforme definida na Tabela 4, deverá ser exibida.
RS6:	No caso de acionamento do alarme, o fornecimento de insulina será suspenso até que o usuário reinicie o sistema e desative o alarme.

Especificação de segurança

- Os requisitos de segurança de um sistema devem ser especificados separadamente.
- Esses requisitos devem ser, conforme discutidos anteriormente, baseados na análise de possíveis perigos e riscos.
- Os requisitos de segurança se aplicam geralmente ao sistema como um todo, ao invés de serem aplicados a subsistemas individuais. Em termos de engenharia de sistemas, a segurança de um sistema é uma propriedade emergente.

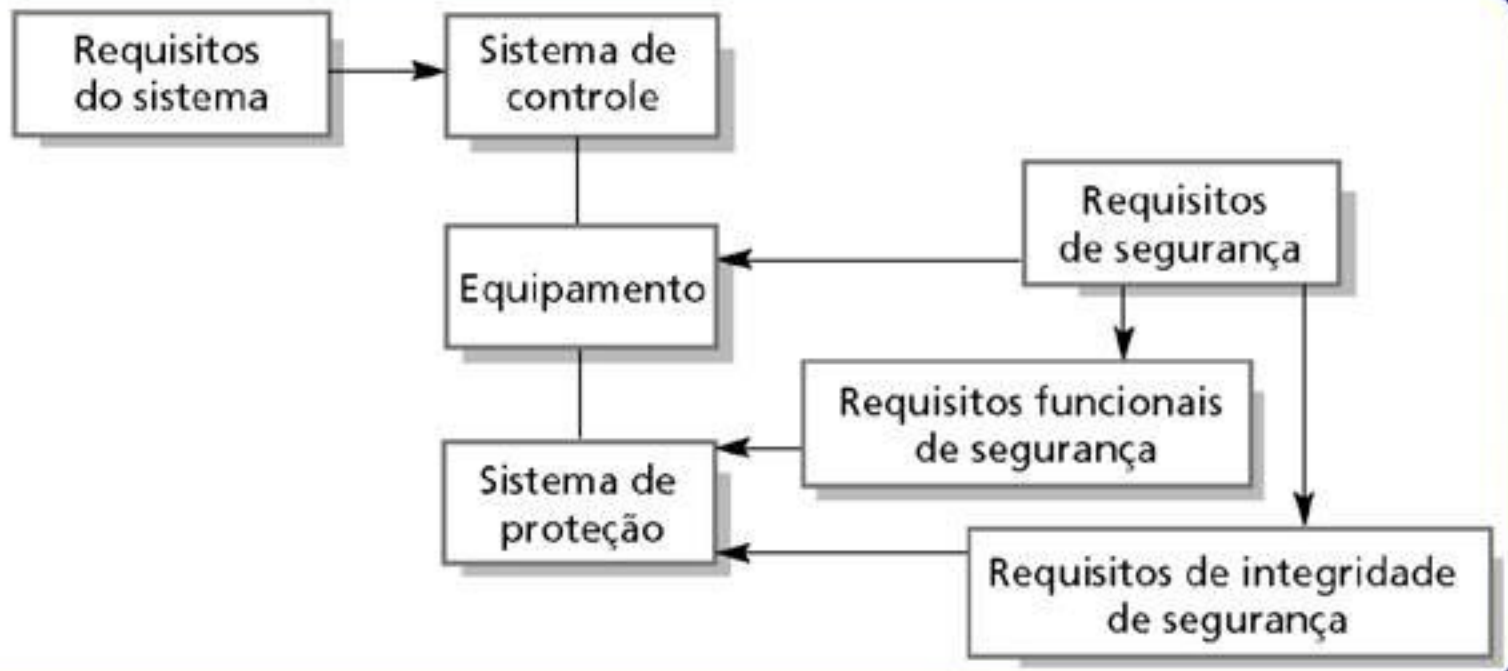
IEC 61508

- É um padrão internacional para gerencimento de segurança, que foi especificamente projetado para sistemas de proteção – não é aplicável a todos os sistemas críticos de segurança.
- Incorpora um modelo do ciclo de vida de segurança e cobre todos os aspectos de gerenciamento de segurança, desde a definição de escopo até a desativação de sistema.

Requisitos de segurança de sistema de controle

Figura 9.4

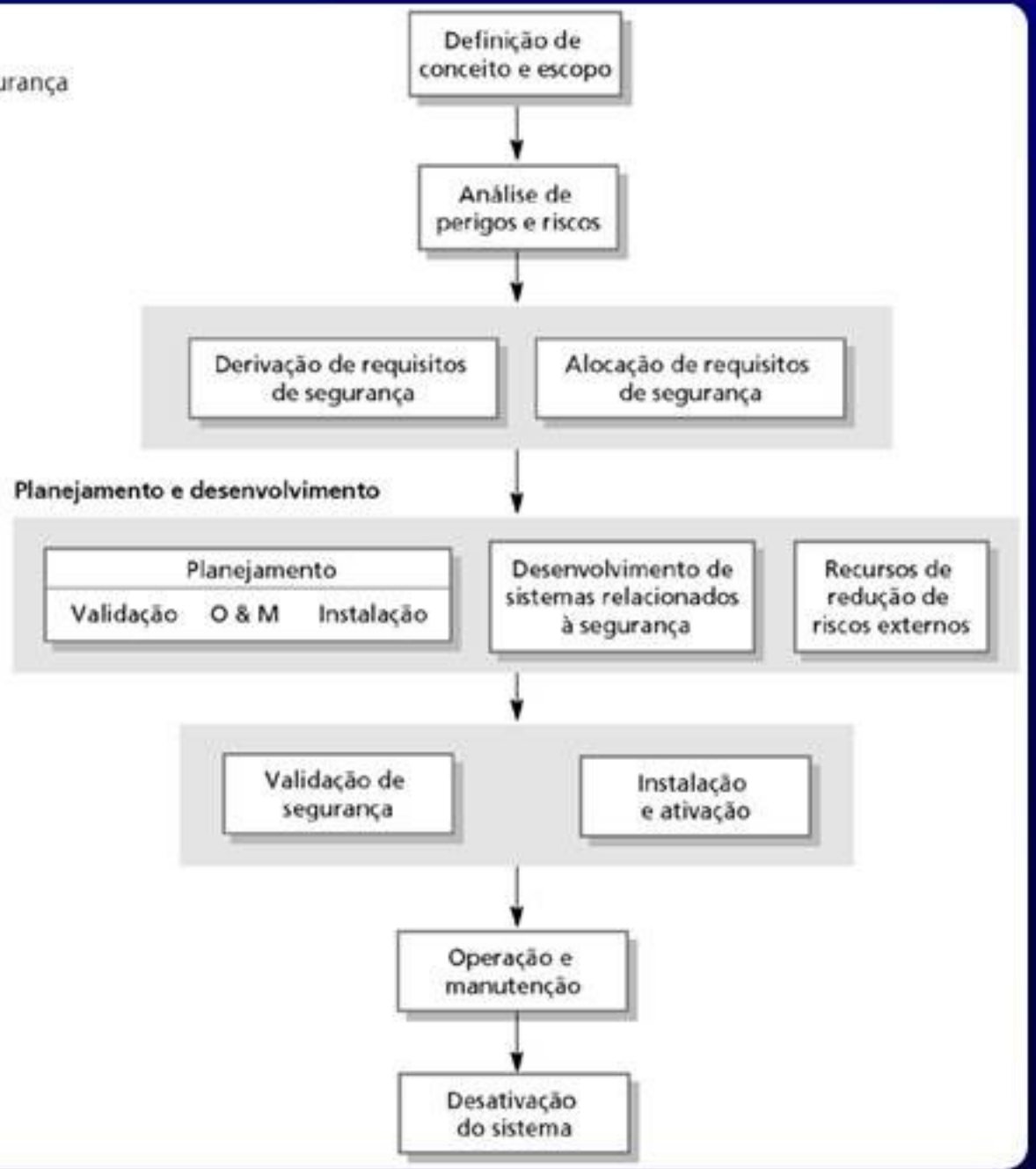
Requisitos de segurança de sistema de controle.



O ciclo de vida de segurança

Figura 9.5

Ciclo de vida de segurança do IEC 61508.



Requisitos de segurança

- Requisitos funcionais de segurança
  - Esses requisitos definem as funções de segurança do sistema de proteção, isto é, definem como o sistema deve fornecer proteção.
- Requisitos de integridade de segurança
  - Esses requisitos definem a confiabilidade e a disponibilidade do sistema de proteção. São baseados no uso esperado e classificados por meio de um nível de integridade de segurança de 1 a 4.

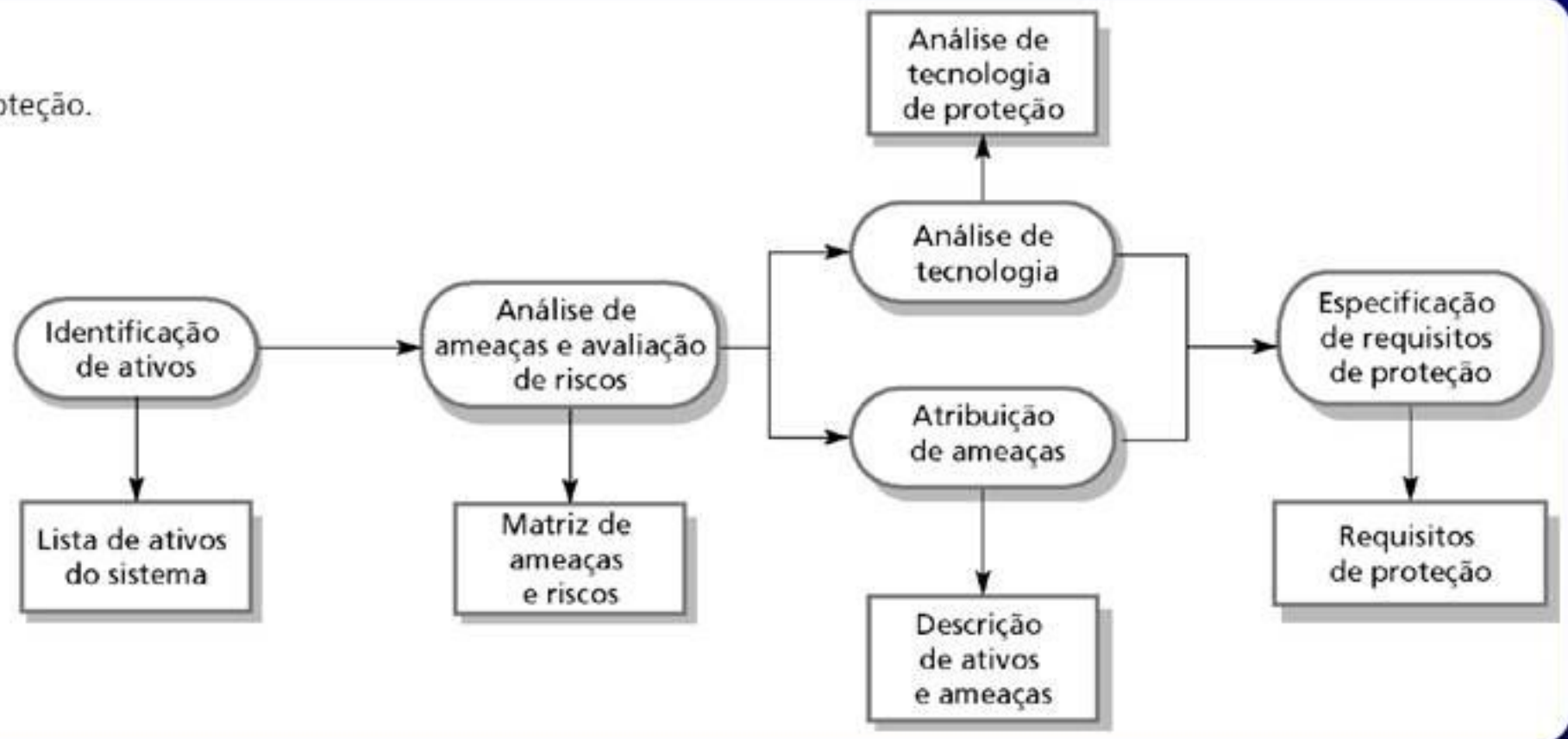
Especificação de proteção

- Possui algumas semelhanças com a especificação de segurança
  - Não é possível especificar os requisitos de proteção quantitativamente;
  - Os requisitos são mais freqüentemente do tipo 'não deve' que do tipo 'deve'.
- Diferenças
  - Não há noção bem definida de um ciclo de vida de proteção para gerenciamento; Não há padrões;
  - Ameaças genéricas ao invés de perigos específicos de sistema;
  - Tecnologia madura de proteção (criptografia, etc.). Contudo, existem problemas co sua transferência para uso geral;
  - O domínio de um fornecedor único (Microsoft) significa que um grande número de sistemas pode ser afetado pela falha de proteção.

O processo de especificação de proteção

Figura 9.6

Especificação de proteção.



Estágios na especificação de proteção

- Identificação e avaliação de ativos
  - Os ativos (dados e programas) e seus níveis necessários de proteção são identificados. A proteção necessária depende do valor do ativo, de tal modo que um arquivo com senhas (digamos) tem mais valor que um conjunto de páginas *Web* públicas.
- Análise de ameaças e avaliação de riscos
  - Possíveis ameaças de proteção são identificadas, e os riscos associados a cada uma dessas ameaças são estimados.
- Atribuição de ameaças
  - Ameaças identificadas são relacionadas aos ativos, de modo que, para cada ativo identificado, exista uma lista de ameaças associada.

Estágios na especificação de proteção

- Análise de tecnologia
  - As tecnologias de proteção disponíveis e sua aplicabilidade em relação às ameaças identificadas são avaliadas.
- Especificação de requisitos de proteção
  - Os requisitos de proteção são especificados. Quando apropriado, serão identificadas explicitamente as tecnologias de proteção que podem ser usadas para proteção contra diferentes ameaças ao sistema.

Tipos de requisitos de proteção

- Requisitos de identificação.
- Requisitos de autenticação.
- Requisitos de autorização.
- Requisitos de imunidade.
- Requisitos de integridade.
- Requisitos de detecção de intrusão.
- Requisitos de não rejeição.
- Requisitos de privacidade.
- Requsitos de auditoria de proteção.
- Requisitos de proteção de manutenção de sistema.

Requisitos de proteção do LIBSY

Quadro 9.2 Alguns requisitos de proteção do sistema LIBSYS

RP1:	Todos os usuários do sistema devem ser identificados por meio de seu número de cartão de biblioteca e senha pessoal.
RP2:	Os privilégios dos usuários devem ser atribuídos de acordo com sua classe (estudante, pessoal, pessoal de biblioteca).
RP3:	Antes da execução de qualquer comando, o LIBSYS deve verificar se o usuário tem privilégios suficientes para acessar e executar esse comando.
RP4:	Quando um usuário pedir um documento, a solicitação do pedido deverá ser registrada. Os dados de registro mantidos incluirão a hora do pedido, a identificação do usuário e os artigos pedidos.
RP5:	Todos os dados do sistema devem ser gravados uma vez por dia, e os back-ups, armazenados em uma área de repositório protegida, fora do local do sistema.
RP6:	Não deve ser permitido que os usuários efetuem mais de um login simultâneo no LIBSYS.

Especificação de confiabilidade de software

- Confiabilidade de hardware
  - Qual é probabilidade de um componente de hardware falhar e quanto tempo levaria para reparar esse componente?
- Confiabilidade de software
  - Qual é a probabilidade que um componente de software produzir uma saída incorreta? As falhas de software são diferentes das falhas de hardware, pois o software não se desgasta. Ele pode continuar em operação mesmo depois de produzir um resulado incorreto.
- Confiabilidade de operador
  - Qual é a probabilidade de o operador de um sistema cometer um erro?

Requisitos funcionais de confiabilidade

- Uma faixa predefinida de todos os valores que são inseridos pelo operador será definida, e o sistema verificará se todas as entradas do operador estão dentro desta faixa.
- O sistema, quando iniciado, verificará todos os discos por blocos defeituosos.
- O sistema deve usar programação em N-versões para implementar o sistema de controle de freios.
- O sistema deve ser implementado em um subconjunto seguro da linguagem Ada e verificado usando a análise estática.

Especificação não funcional de confiabilidade

- O nível necessário de confiabilidade de sistema deve ser expresso quantitativamente.
- Confiabilidade é um atributo dinâmico do sistema – as especificações de confiabilidade relacionadas ao código fonte são significativas.
  - Não mais do que N defeitos/1000 linhas;
  - Isao é útil somente para uma análise de processo de pós-entrega, onde você está tentando avaliar quão boas são as suas técnicas de desenvolvimento.
- Uma métrica de confiabilidade apropriada deve ser escolhida para especificar a confiabilidade global do sistema.

Métricas de confiabilidade

- Métricas de confiabilidade são unidades de medição da confiabilidade do sistema.
- A confiabilidade de sistema é medida pela contagem do número de falhas operacionais e, quando apropriado, relacionando-o às demandas feitas ao sistema e ao tempo em que o sistema esteve operacional.
- Um programa de medição a longo prazo é necessário para avaliar a confiabilidade dos sistemas críticos.

Métricas de confiabilidade

Tabela 9.2 Métricas de confiabilidade

Métrica	Explicação
POFOD Probabilidade de falha sob demanda	A probabilidade de que o sistema falhará quando for feita uma solicitação de serviço. Uma POFOD de 0,001 significa que uma entre mil solicitações de serviços pode resultar em falha.
ROCOF Taxa de ocorrência de falhas	A freqüência com que um comportamento inesperado pode ocorrer. Uma ROCOF de 2/100 significa que é provável que ocorram duas falhas em cada 100 unidades operacionais de tempo. Essa métrica é, às vezes, chamada de intensidade de falhas.
MTTF Tempo médio para falhar	O tempo médio entre as falhas observadas no sistema. Um MTTF de 500 significa que se pode esperar uma falha a cada 500 unidades de tempo.
AVAIL Disponibilidade	A probabilidade de que o sistema esteja disponível para uso em um dado tempo. Uma disponibilidade de 0,998 significa que o sistema provavelmente estará disponível em 998 de cada 1.000 unidades de tempo.

Probabilidade de falha sob demanda (POFOD)

- É a probabilidade que o sistema falhará quando uma solicitação de serviço for feita. É útil quando as demandas de serviços são intermitentes e, relativamente, pouco freqüentes.
- É apropriado para sistemas de proteção onde os serviços são demandados ocacionalmente, e onde existem sérias conseqüências caso o serviço não seja prestado.
- É relevante para muitos sistemas críticos de segurança, com exceção dos componentes de gerenciamento
  - Sistema de desligamento de emergência em uma planta química.

Taxa de ocorrência de falhas (ROCOF)

- Reflete a taxa de ocorrência de falhas no sistema.
- Um ROCOF de 0.002 significa que 2 falhas são prováveis em cada 1000 unidades de tempo de operação, por exemplo, 2 falhas por 1000 horas de operação.
- É relevante para sistemas operacionas e sistemas de processamento de transações, onde o sistema tem de processar um grande número de solicitações similares que são relativamente freqüentes
  - Sistema de processamento de cartões de crédito e sistema de reservas de vôo.

Tempo médio para falha (MTTF)

- É a medida de tempo entre as falhas observadas do sistema. É a recíproca do ROCOF para sistemas estáveis.
- MTTF de 500 significa que o tempo médio entre falhas é de 500 unidades de tempo.
- Relevante para sistemas com transações longas, isto é, onde o processamento de sistema leva um longo temo. MTTF deve ser maior que o tempo de transação
  - Sistemas de projeto auxiliado por computador, onde um projetista trabalhará em um projeto por várias horas e sistemas de processamento de texto.

Disponibilidade (AVAL)

- É a medida da fração de tempo que o sistema está disponível para o uso.
- Leva em conta o tempo de reparo e o de reinício.
- Disponibilidade de 0.998 significa que o software está disponível para 998 das 1.000 unidades de tempo.
- É relevante para sistemas *non-stop* e processamento contínuo
  - Sistemas de comutação telefônica e sistemas de sinalização ferroviária.

Especificação de requisitos não funcionais

- As medições de confiabilidade NÃO levam em conta as conseqüências das falhas.
- Os defeitos transientes podem não ter conseqüências reais, mas outros defeitos podem causar perda ou corrupção de dados e perda do serviço de sistema.
- Pode ser necessário identificar as classes de falhas diferentes e usar diferentes métricas para cada uma delas. A especificação de confiabilidade deve ser estruturada.

Conseqüências de falhas

- Ao especificar a confibilidade, não é somente o número de falhas de sistema que importa, mas as conseqüências dessas falhas.
- Falhas que têm sérias conseqüências são claramente mais danosas que aquelas onde o reparo e a recuperação são diretos.
- Em alguns casos, portanto, especificações de confiabilidade diferentes para tipos diferentes de falhas podem ser definidas.

Classificação de falhas

Tabela 9.3 Classificação de falhas

Tipo de falha	Descrição
Transitória	Ocorre apenas com determinadas entradas.
Permanente	Ocorre com todas as entradas.
Recuperável	O sistema pode se recuperar sem intervenção do operador.
Irrecuperável	A intervenção do operador é necessária para a recuperação da falha.
Não de corrompimento	A falha não corrompe o estado ou os dados do sistema.
De corrompimento	A falha corrompe o estado ou os dados do sistema.

Passos para uma especificação de confiabilidade

- Para cada subsistema, analise as conseqüências das possíveis falhas do sistema.
- A partir da análise de falhas do sistema, divida as falhas em classes apropriadas.
- Para cada classe de falha identificada, defina a confiabilidade usando uma métrica apropriada. Métricas diferentes podem ser usadas para requisitos de confiabilidade diferentes.
- Identificar requisitos funcionais de confiabilidade para reduzir as chances de falhas críticas.

Sistema auto-atendimento de banco (ATM)

- Cada máquina na rede é usada 300 vezes por dia
- O banco tem 1.000 máquinas
- O tempo de vida da release do software é de 2 anos
- Cada máquina trata aproximadamente 100.000 transações
- Cerca de 300.000 transações de banco de dados no total por dia

Especificação de confiabilidade de um sistema de caixa eletrônico

Tabela 9.4 Especificação de confiabilidade de um caixa eletrônico

Tipo de falha	Exemplo	Métrica de confiabilidade
Permanente, não de corrompimento	O sistema falha ao operar com qualquer cartão inserido. O software deve ser reiniciado para corrigir a falha.	ROCOF 1 ocorrência em 1.000 dias.
Transitória, não de corrompimento	Os dados da faixa magnética não podem ser lidos em um cartão sem danos inserido.	ROCOF 1 ocorrência em 1.000 transações.
Transitória, de corrompimento	Um padrão de transações na rede causa o corrompimento do banco de dados.	Não quantificável! Nunca deve ocorrer no tempo de vida do sistema.

Validação da especificação

- É impossível validar empiricamente especificações de confiabilidade muito altas.
- Nenhuma corrupção de banco de dados significa POFOD menor do que 1 em 200 milhões.
- Se uma transação leva 1 segundo, então a simulação de transações de um dia leva 3,5 dias.
- Levaria mais tempo que o tempo de vida do sistema para testá-lo pela confiabilidade.

Pontos-chave

- A análise de riscos é a base para identificar os requisitos de confiabilidade de sistema.
- A análise de riscos está relacionado à avaliação das chances de um risco ocorrer e à classificação dos riscos de acordo com sua severidade.
- Os requisitos de proteção devem identificar os ativos e definir como devem ser protegidos.
- Os requisitos de confiabilidade podem ser definidos quantitativamente.

Pontos-chave

- As métricas de confiabilidade incluem POFOD, ROCOF, MTTF e AVAL.
- Especificações não funcionais de confiabilidade podem levar a requisitos funcionais de sistema para reduzir falhas ou lidar com sua ocorrência.