

Engenharia de Software

10 - Sistemas Confiáveis e de Segurança

Prof. Msc. Francisco de Assis de Souza Rodrigues

UniFAP
CENTRO UNIVERSITÁRIO PARAÍSO

"Todos os teus filhos serão ensinados pelo Senhor, e grande será a paz de teus filhos." **Isaías 54:13**

Aprender é também uma bênção espiritual. Buscar conhecimento com humildade traz paz e crescimento.

🎯 Objetivos

- **Definir Dependabilidade:** Compreender o conceito abrangente de dependabilidade e por que ele é crucial para todos os sistemas de software, especialmente em contextos críticos.
- **Identificar as Dimensões:** Distinguir as cinco principais dimensões da dependabilidade (Disponibilidade, Confiabilidade, Segurança (Safety), Segurança da Informação (Security), e Resiliência).
- **Analisar o Contexto Sociotécnico:** Entender que os sistemas devem ser considerados como entidades sociotécnicas, e não apenas como hardware e software.

UniFAP

🎯 Objetivos

- **Aplicar Estratégias Fundamentais:** Reconhecer o papel da redundância e da diversidade como mecanismos essenciais para construir sistemas confiáveis.
- **Reconhecer a Importância dos Processos:** Entender como a adoção de processos de desenvolvimento confiáveis e repetíveis é essencial para minimizar defeitos

UniFAP

Estrutura e Conteúdo da Aula

Introdução à Dependabilidade e Suas Propriedades

Dependabilidade:

O termo dependabilidade foi proposto para cobrir atributos de sistema relacionados à disponibilidade, confiabilidade, segurança (safety) e segurança da informação (security). É o grau de confiança que o usuário tem no sistema.

Por que a Dependabilidade é Crucial (Foco SI/ADS):

- A falha de sistemas computacionais críticos pode levar a grandes perdas econômicas.
- Pode provocar danos físicos ou ameaças à vida humana (em sistemas críticos).
- Sistemas não confiáveis podem causar perda de informação.

UniFAP

Estrutura e Conteúdo da Aula

Introdução à Dependabilidade e Suas Propriedades

As 5 Dimensões da Dependabilidade

Propriedade	Descrição
Disponibilidade	Capacidade de prestar serviços **quando solicitados**
Confiabilidade	Capacidade de prestar serviços **conforme especificado**
Segurança (*Safety*)	Capacidade de operar **sem falhas catastróficas**
Segurança da Informação (*Security*)	Capacidade de se proteger contra **intrusão acidental ou deliberada**
Resiliência	Capacidade de **resistir e se recuperar de eventos danosos**

UniFAP

Estrutura e Conteúdo da Aula

Introdução à Dependabilidade e Suas Propriedades

Nota:

Sistemas críticos (como uma bomba de insulina) são muito caros para serem desenvolvidos, pois as falhas devem ser raras e devem incluir mecanismos de recuperação. O custo para obter melhorias na dependabilidade aumenta exponencialmente à medida que se busca um nível de confiança mais alto.

Sistemas Sociotécnicos e Gestão de Risco

O software nunca está isolado; ele é sempre parte de um sistema mais amplo.

O Conceito de Sistemas Sociotécnicos

Um sistema confiável deve ser visto holisticamente, considerando todos os seus componentes interconectados:

1. Hardware (onde o software é executado).
2. Software (a aplicação em si).
3. Pessoas (usuários e operadores).
4. Processos Organizacionais (os processos de negócio nos quais o software é utilizado).

Insight: Se o hardware, o software e os processos operacionais forem projetados separadamente, é mais provável que os erros ocorram nas interfaces entre as diferentes partes do sistema.

UniFAP

Sistemas Sociotécnicos e Gestão de Risco

Regulamentação e Certificação:

Em sistemas críticos, é essencial seguir regulamentação e conformidade. Para obter a certificação de reguladores (como em aviões ou reatores nucleares), é necessário produzir um caso de segurança (safety case) extenso, demonstrando que as regras e normas foram seguidas.

UniFAP

Redundância, Diversidade e Processos Confiáveis

Redundância e Diversidade:

Como as falhas são inevitáveis, os sistemas devem ser projetados para que falhas de componentes individuais não levem a uma falha geral.

- **Redundância:** Significa ter uma capacidade extra (por exemplo, servidores replicados) para garantir que o sistema continue a operar.
- **Diversidade:** Significa que o mesmo tipo de funcionalidade é fornecido de diferentes maneiras (usando diferentes tecnologias ou implementações) para evitar que uma vulnerabilidade comum seja explorada.

UniFAP

Redundância, Diversidade e Processos Confiáveis

Processos Confiáveis:

O uso de processos de software confiáveis leva a um software que contenha poucos erros.

Atributos de Processos Confiáveis:

- **Padronizado:** A qualidade do software é garantida ao se utilizar um processo de desenvolvimento padronizado.
- **Repetível:** O processo não se baseia no julgamento individual e pode ser repetido com diferentes membros da equipe.
- **Diverso:** O processo deve incluir atividades de verificação e validação redundantes e diversas (como inspeções e testes, agindo em conjunto).

UniFAP

Redundância, Diversidade e Processos Confiáveis

Atividades Chave em Processos Confiáveis:

1. Revisões de requisitos para consistência e completude.
2. Gerenciamento de requisitos e de mudanças.
3. Inspeções de projeto e de programa.
4. Análise estática (checagens automatizadas no código-fonte).
5. Planejamento e gerenciamento de testes.

UniFAP

Redundância, Diversidade e Processos Confiáveis
Métodos Formais

São abordagens matemáticas para o desenvolvimento de software.

- Permitem a definição de um modelo formal do software que pode ser analisado para procurar erros e inconsistências.
- Podem ser usados para provar que um programa é consistente com o seu modelo.
- Têm sido usados principalmente no desenvolvimento de sistemas críticos que têm requisitos rigorosos de segurança (safety), confiabilidade ou segurança da informação (security).
- Técnicas como Verificação de Modelos (Model Checking) analisam exaustivamente a especificação para verificar se as propriedades de segurança são válidas.
- **Benefício:** Usuários relatam menos erros no software entregue, sendo essenciais para a certificação de reguladores.

UniFAP

Atividade

Uma empresa está desenvolvendo um novo aplicativo móvel interativo para agendamento de consultas médicas (não um sistema crítico, mas lida com dados pessoais). Eles têm um orçamento apertado.

Questão: Quais das cinco dimensões de dependabilidade (Disponibilidade, Confiabilidade, Segurança, Segurança da Informação, Resiliência) devem receber o maior investimento no projeto? Justifique por que as outras dimensões podem receber um investimento "Médio/Baixo", aceitando falhas ocasionais para manter o custo razoável.

UniFAP


UniFAP

Bibliografia

SOMMERVILLE, Ian. Engenharia de software. 10. ed. São Paulo, SP: Pearson, 2018. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 15 ago 2025.

https://plataforma.bvirtual.com.br/Acervo/Publicacao/168127



Referências

CHATGPT. Expansão conceitual sobre integração entre COBIT, ITIL e PMBOK. OpenAI, 2025. Disponível em: https://chat.openai.com/. Acesso em: 11 ago. 2025.


OBRIGADO
Arigato
Spasibo
Obrigado
Dankon
Maake
Multumesc
Ua Tsaug Rau Koj
Mochchakkeram
Kiitos
Merci
Raibh Maith Agat
Chokrane
Grazie
Terma Kasih
Asante
Mamana
Kia Ora
THANK YOU
Jusparxar
Welalin
Spasibo
Arigato

UniFAP