↗ Classificação dos falhas do sistema como um todo

Modelos de falha

- SDs devem ser tolerantes a falhas
- SDs admitem falhas parciais
  - ↳ Podem apresentar uma falha parcial sem comprometer todo o sistema.

⇨ Mecanismos de tolerância a falhas

- Redundância
- Isolamento
- Atualização

- É a replicação de um serviço e pode ser de
  - ↳ Informação: adiciona uma informação extra aos dados transmitidos.
  - ↳ Tempo: uma ação é realizada e então, caso seja detectada uma falta, a ação é realizada novamente.
  - ↳ Física: Equipamentos adicionais são inseridos para tolerar falhas de outros equipamentos.

↳ Redundância Tripla Modular

- Técnica de redundância projetada para circuitos, onde cada dispositivo é replicado 3 vezes, e cada estágio tem um receptor que recebe 3 entradas e agrega 1 saída.

⊛ se 2 ou 3 entradas são (=) → saída = entrada

se as 3 entradas são (≠) → saída indefinida

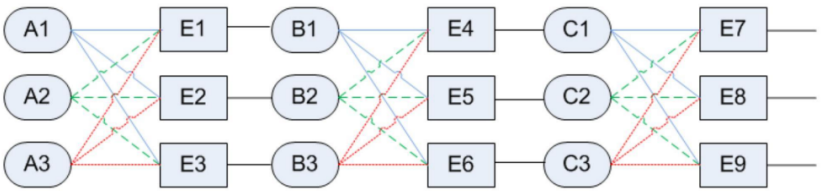


Figura: Redundância Tripla Modular (baseado em TANEMBAUM, 2007).

↳ Ou seja, em cada estágio, se um, e apenas um, dos dispositivos geradores de entrada falhar, a saída do dispositivo gerador ainda permanece correta.

Definições

→ **Confiabilidade (Reliability)**

• Propriedade que indica que o sistema executa continuamente sem falhas por um longo período.

→ **Disponibilidade (Availability)**

• É a medida dos instantes de tempo em que um sistema se mantém operacional.

→ **Safety (Integridade de dados)**

• Quando um sistema falha, mesmo que por um curto período, os dados não são comprometidos

→ **Security (Meios de Acesso)**

• Restrição de acesso aos dados

→ **Capacidade de manutenção**

• É a possibilidade de partes funcionais do sistema serem trocadas, adicionadas ou removidas sem comprometer o seu funcionamento.

* Um SD, deve ser capaz de se recuperar automaticamente de falhas

↳ Definições IEEE 610.12-1990

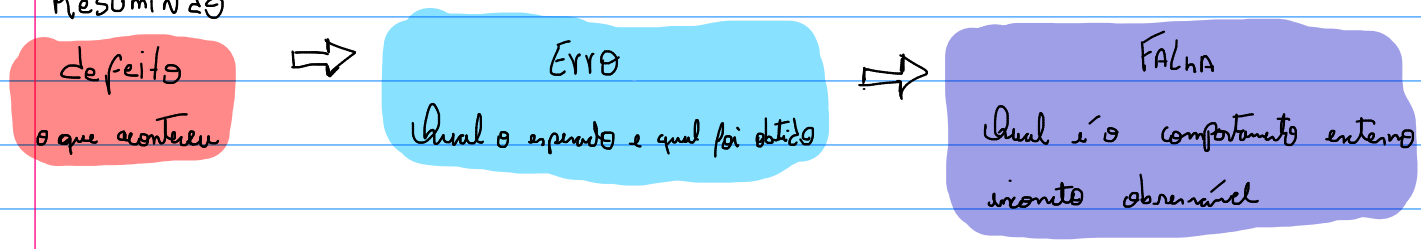
- Falha / defeito (estático)
  - Também conhecido como bug
  - É um defeito interno e estático no software

→ um defeito produz um erro

- Erro (Dinâmico)
  - É a diferença entre a saída esperada e a saída obtida
  - Estado interno incorreto
  - O erro é observado durante a execução do defeito

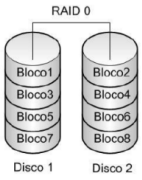
- Falha (Resultado final)
  - É a inabilidade do sistema de cumprir a sua função
  - Comportamento externo observável está incorreto

Resumindo



▷ Classificação de falhas

- Falha por Queda → O serviço é interrompido de maneira abrupta e inesperada.
- Falha por Omissão → O serviço não responde ou não recebe requisições
- Falha de temporização → O serviço demora muito para responder
- Falha de resposta → A resposta do serviço está errada
- Falha bizantina → A resposta do serviço é inesperada e não deveria ter sido produzida.
  (Arbitrárias)



Raid (Redudant Array of Independent Disks)

- É uma forma de armazenar dados em vários discos para obter redundância
- Para o SO, é um único disco
- Aumenta confiabilidade → Redundância e paridade de blocos
- Aumenta desempenho → Acesso simultâneo e distribuição (stripping) de dados em vários discos.

Modelos de Segurança

Metodologia AAA

- **Autenticação**
  - Validação das credenciais do usuário.
  - Usuários devem provar que são quem dizem ser.
  - Controle de quem acessa os recursos.

- **Autorização**
  - Atributos (papéis) para acessar os recursos.
  - Define quais são os privilégios de acesso aos recursos.
  - Quais recursos e quais operações o usuário pode realizar.

- **Registro**
  - Registro de quais recursos e operações foram realizados.
  - Logs para auditoria e contabilidade de métricas.
  - Proteção contra ações maliciosas.

Aspetos de Design

- Um fator chave para Tolerância a falhas é o agrupamento de falhas, pois pode ajudar a tratar a maior parte delas

Detecção de falhas

- O método mais simples de detecção de falhas é verificar se o host está ativo. (Similar ao ping)
  - Este processo está sujeito a falhas, pois um host malicioso poderia mascarar a resposta em uma rede não confiável.
  - Tempo de resposta alto em redes com muitos hosts.

ISO/IEC 27000

⇨ Ciclo de vida da gestão de segurança

1- Planejar

- Definir regras de acesso e definir os riscos
- Definir escopo das atividades
- Caso apareça uma coisa nova posteriormente é ignorada (manter o padrão)

2- Fazer

- Treinamento de pessoal e alocação de recursos de segurança.
- Criar e implementar um plano de gestão de riscos.

3- Verificar

- Monitorar a implementação regularmente
- Manter um resumo detalhado dos registros de acesso

4- Agir

- Realizar ações preventivas
- Continuar o processo de melhoria

⇨ Algumas Vulnerabilidades

- Vírus: Software embutido em outro e que executa código malicioso no host.
- Worm: Malware que executa cópias de si no host e distribui pela rede.
- Trojan: Software que parece legítimo, mas é direcionado para interferir em alguma aplicação
- Spyware: Software que coleta infos e manda para outro processo.
- Adware: Software que gera mensagens de anúncio