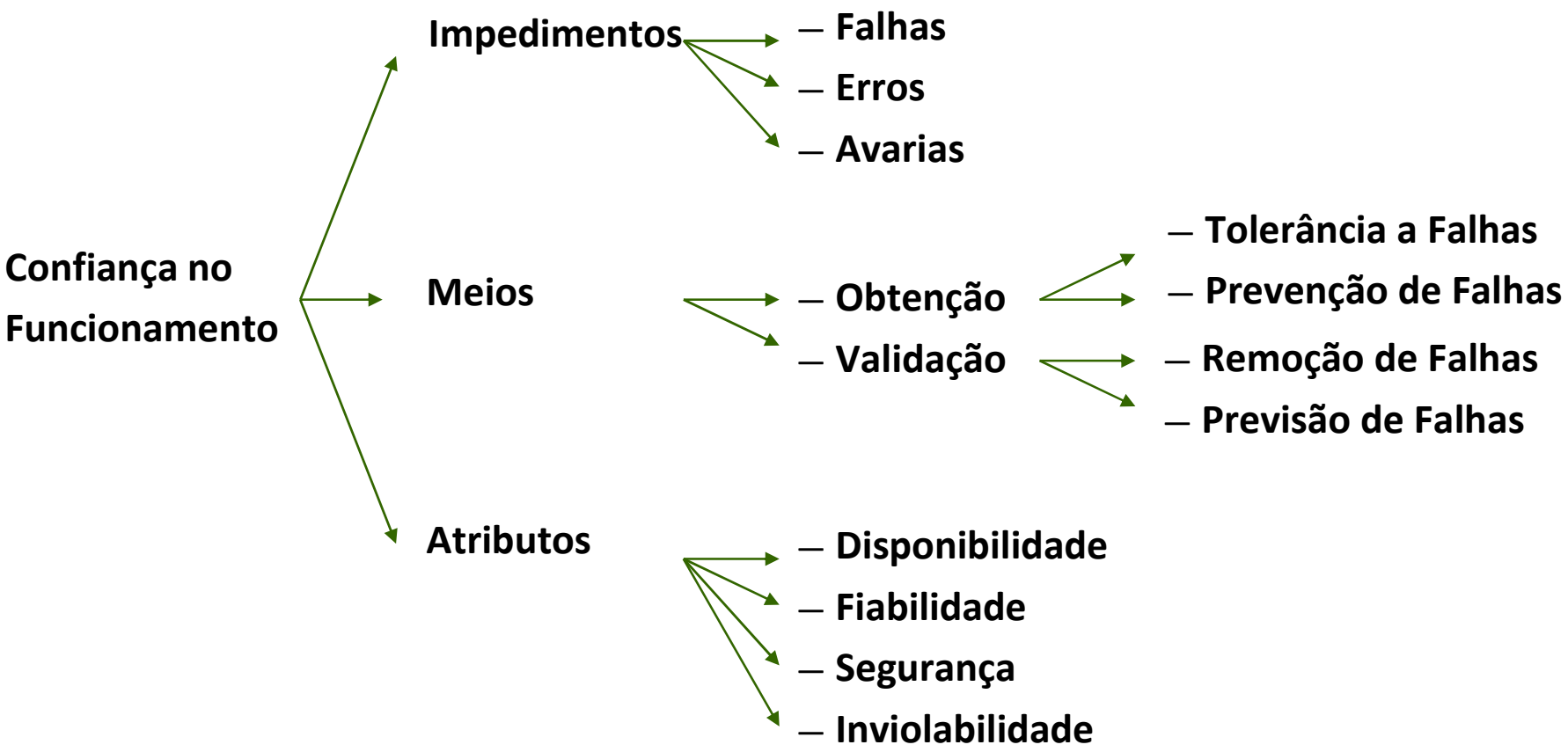
Tolerância a Falhas

Introdução

Conceitos básicos: confiança no funcionamento



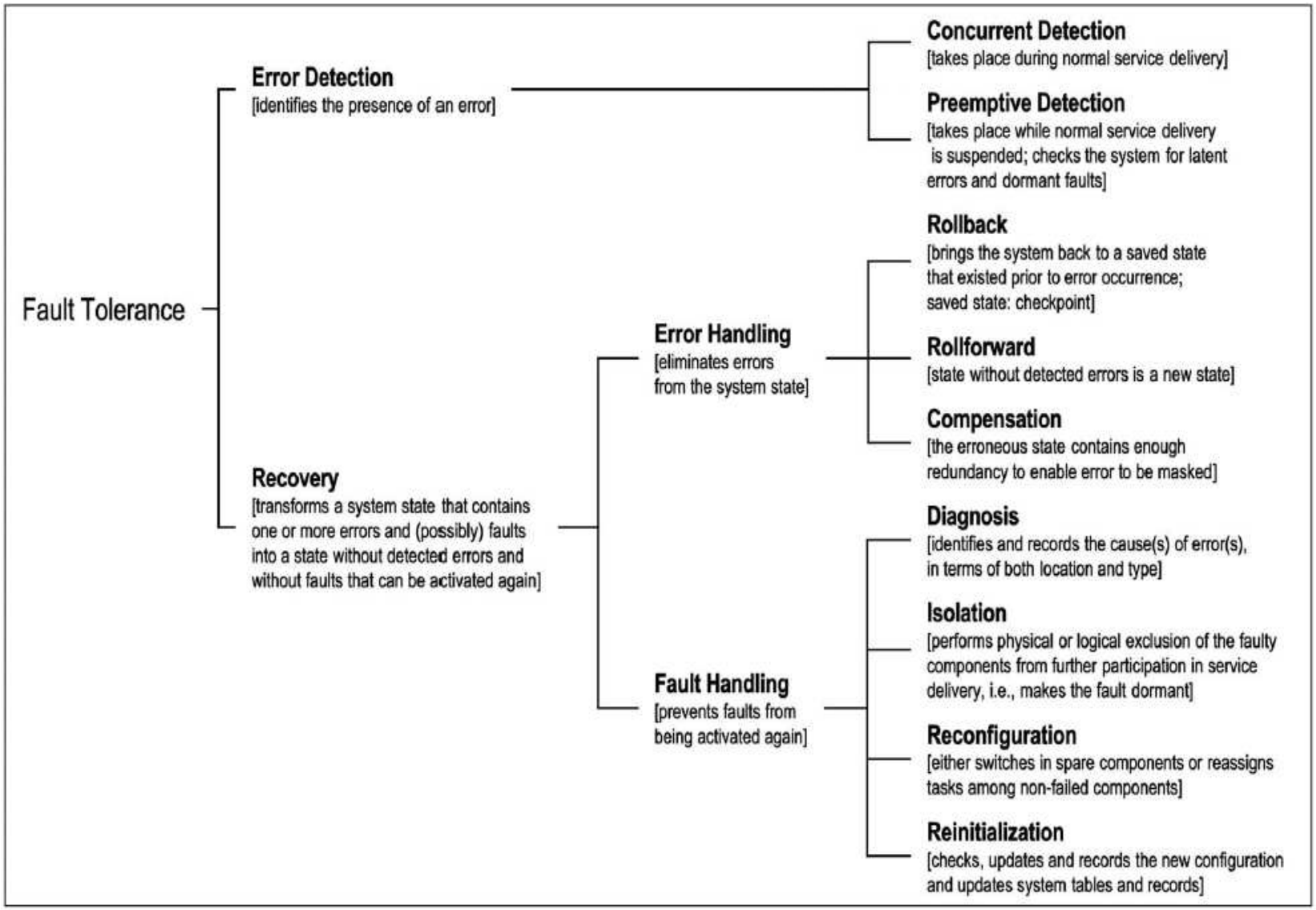
Conceitos Básicos de Tolerância a Falhas

FEUP
Universidade do Porto
Faculdade de Engenharia

- Dependência entre os meios para a Obtenção e a Validação da Confiança no Funcionamento:
  - Prevenção de falhas
  - Tolerância a falhas
  - Remoção de falhas
  - Previsão de falhas

Tolerância a falhas: visão geral

FEUP
Universidade do Porto
Faculdade de Engenharia



Conceitos Básicos de Tolerância a Falhas

FEUP
Universidade do Porto
Faculdade de Engenharia

- Etapas da tolerância a falhas:

1. O Processamento de Erros visa eliminar os erros de um sistema computacional, se possível antes da ocorrência de uma avaria
2. O Tratamento de Falhas destina-se a impedir a reactivação das falhas.

Conceitos Básicos de Tolerância a Falhas

FEUP
Universidade do Porto
Faculdade de Engenharia

Processamento de Erros

1. Detecção de erros:
   - permite que o estado erróneo seja identificado como tal
   - Quando se recorre à recuperação de erros, o estado erróneo necessita de ser identificado com sendo erróneo, antes de ser substituído.
2. Diagnóstico de erros:
   - permite a avaliação dos danos causados pelo erro detectado, ou por erros propagados antes da detecção
3. Recuperação de erros:
   - onde um estado erróneo é substituído por um estado livre de erros (para trás, para a frente, compensação).

Conceitos Básicos de Tolerância a Falhas

FEUP
Universidade do Porto
Faculdade de Engenharia

- Recuperação de erros:
  - Recuperação para trás
    - Consiste em fazer o sistema voltar a um estado pelo qual o sistema já passou anteriormente, antes da ocorrência do erro;
    - Envolve a definição de pontos de recuperação, para os quais o estado do processo pode posteriormente ser restaurado.
  - Recuperação para a frente
    - Consiste em procurar um novo estado a partir do qual o sistema possa funcionar (frequentemente em modo degradado).
  - Compensação
    - Onde o estado erróneo contém redundância suficiente para permitir que o serviço(s) prestado a partir de um estado erróneo esteja contudo isento de erros.

Conceitos Básicos de Tolerância a Falhas

FEUP
Universidade do Porto
Faculdade de Engenharia

Tratamento de Falhas

- Primeiro passo ⇨ Diagnóstico das falhas
  - determinação da causa(s) do erro(s), tanto em termos de localização como em termos de natureza.

- Segundo passo ⇨ Desactivação de falhas
  - Prevenir que a(s) falha(s) sejam de novo activadas, tornando-a(s) passiva(s).
  - Por exemplo, removendo o componente considerado como defeituoso de execuções seguintes.

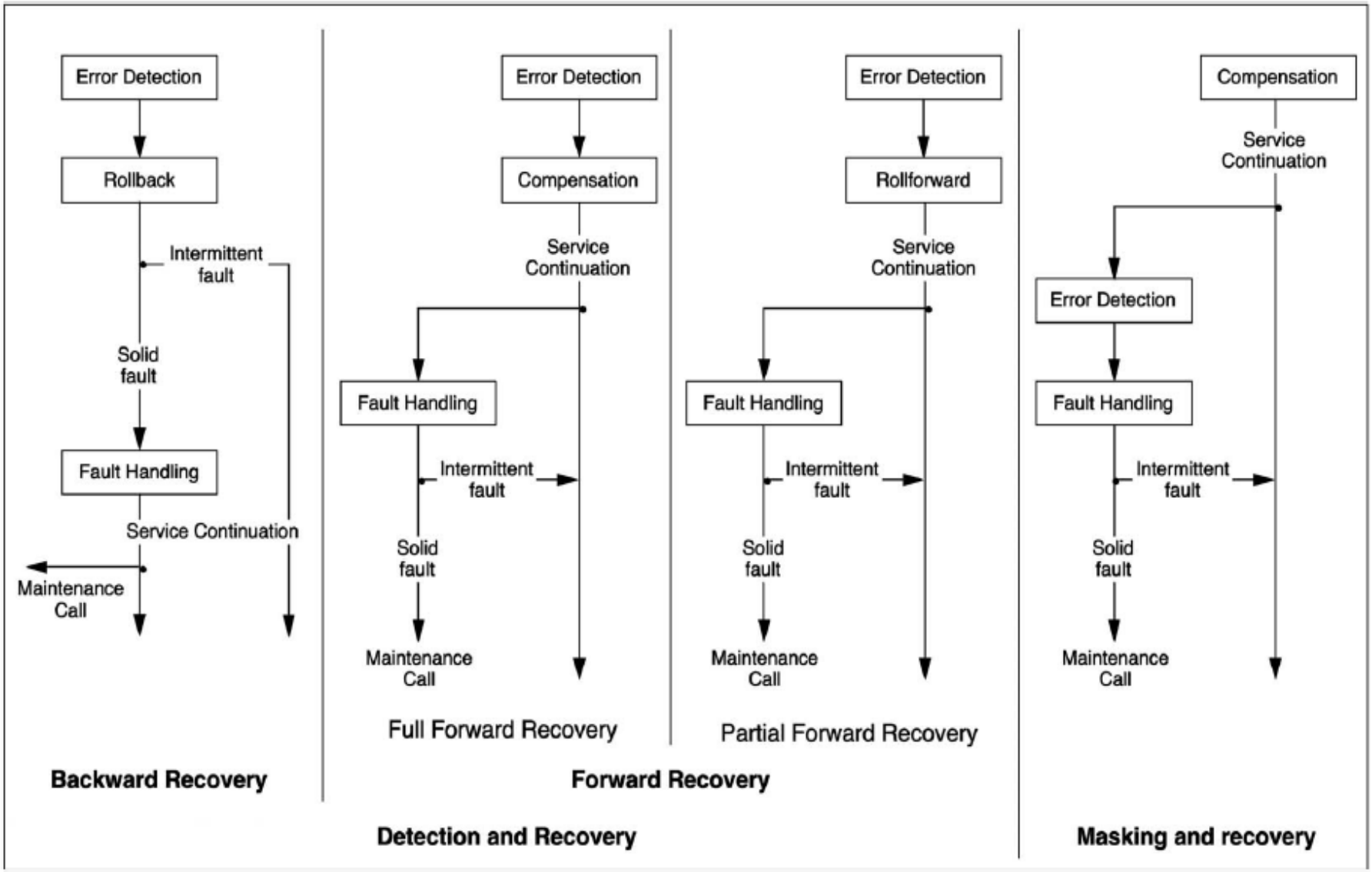
FEUP
Universidade do Porto
Faculdade de Engenharia

Cobertura da Tolerância a Falhas

- As classes de falhas que podem ser toleradas dependem das hipóteses de falhas que são consideradas na fase de concepção.
  - Um exemplo poderá ser considerar a tolerância a falhas físicas e a tolerância a falhas de concepção.

- Esta Cobertura nunca é total devido a:
  - falhas de concepção afectando os mecanismos de tolerância a falhas no que respeita às hipóteses de falhas efectuadas durante a concepção (falta de cobertura da manipulação de falhas e erros);
  - hipóteses de falhas que diferem das falhas que realmente acontecem durante a operação do sistema (falta de cobertura dos modos de falha).

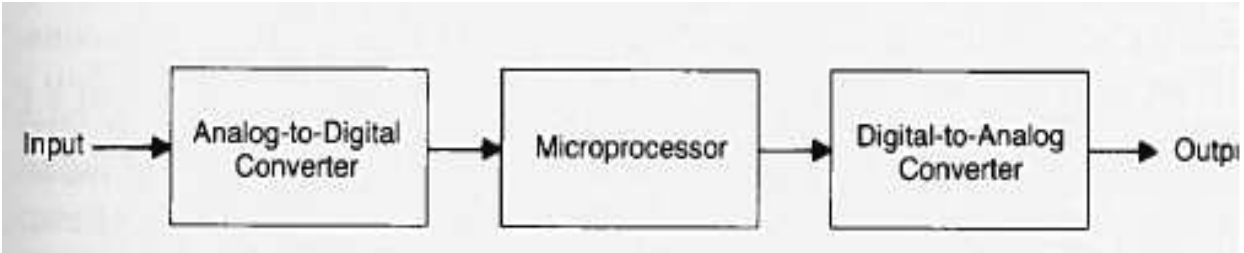
Tolerância a falhas: resumo das técnicas



Exemplos

FEUP
Universidade do Porto
Faculdade de Engenharia

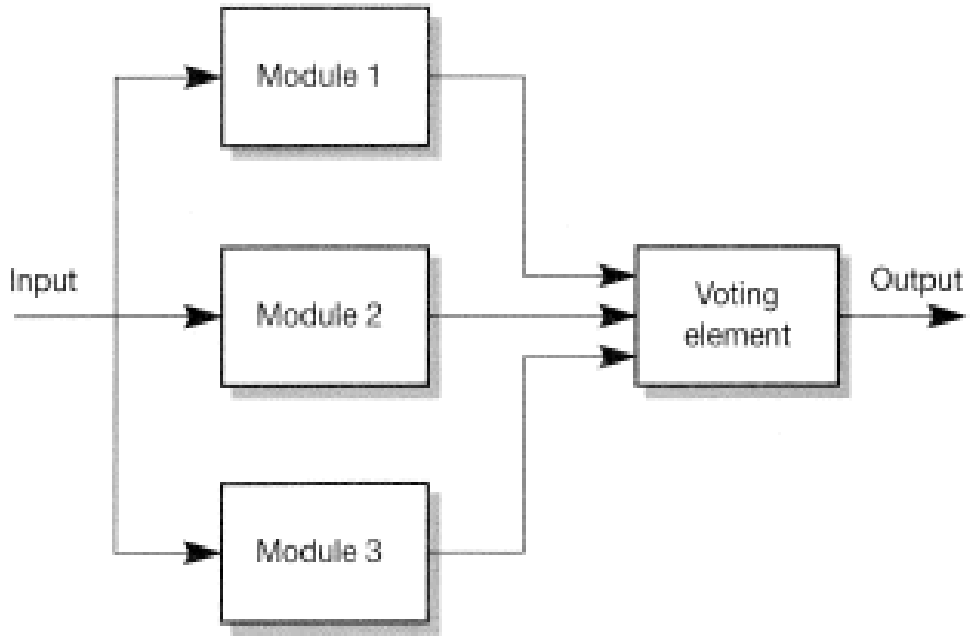
- Sistema de aquisição de dados
  - Teste de *overflow* dos dados adquiridos
  - Execução dupla (em instantes diferentes) das tarefas
  - Armazenamento de dados (na memória) utilizando um bit extra de paridade



Exemplos

FEUP
Universidade do Porto
Faculdade de Engenharia

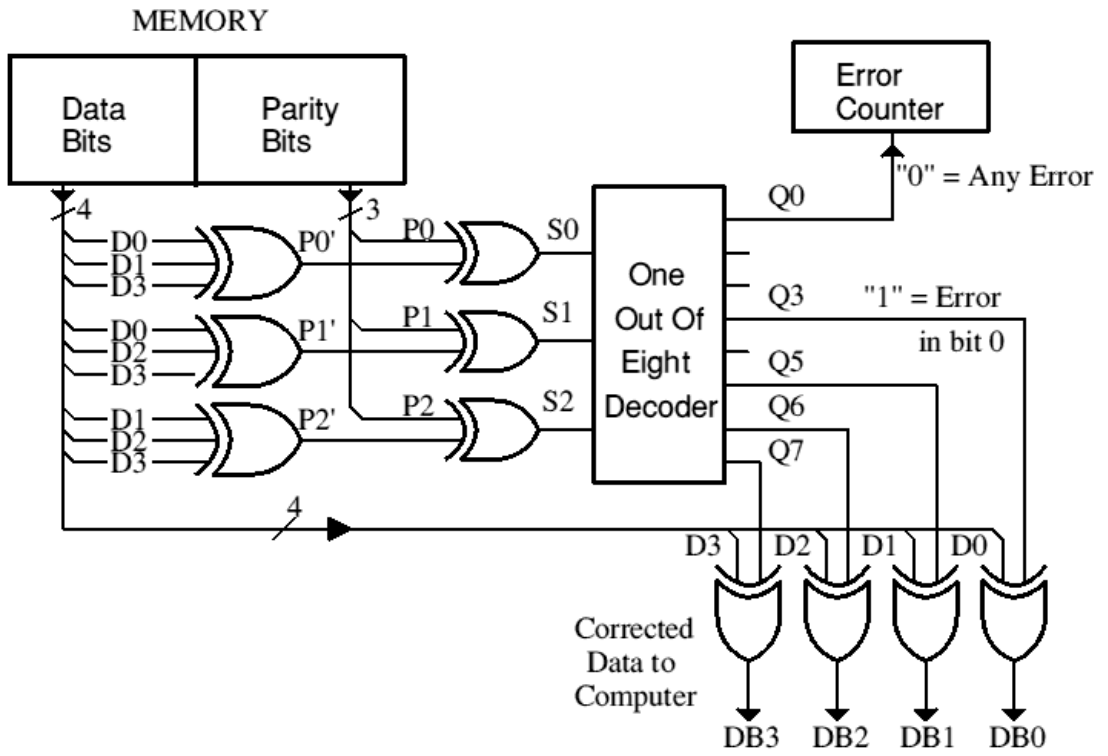
- Redundância de Hardware
  - Utilização de módulos de hardware suplementares;
  - Exemplo: Arquitectura TMR ("Triple Modular Redundancy").



Exemplos

Redundância de Informação

- Utilização de informação suplementar, destinada a detectar ou tolerar falhas;
  - Exemplo, códigos de CRC, bits de paridade, “checksums”.

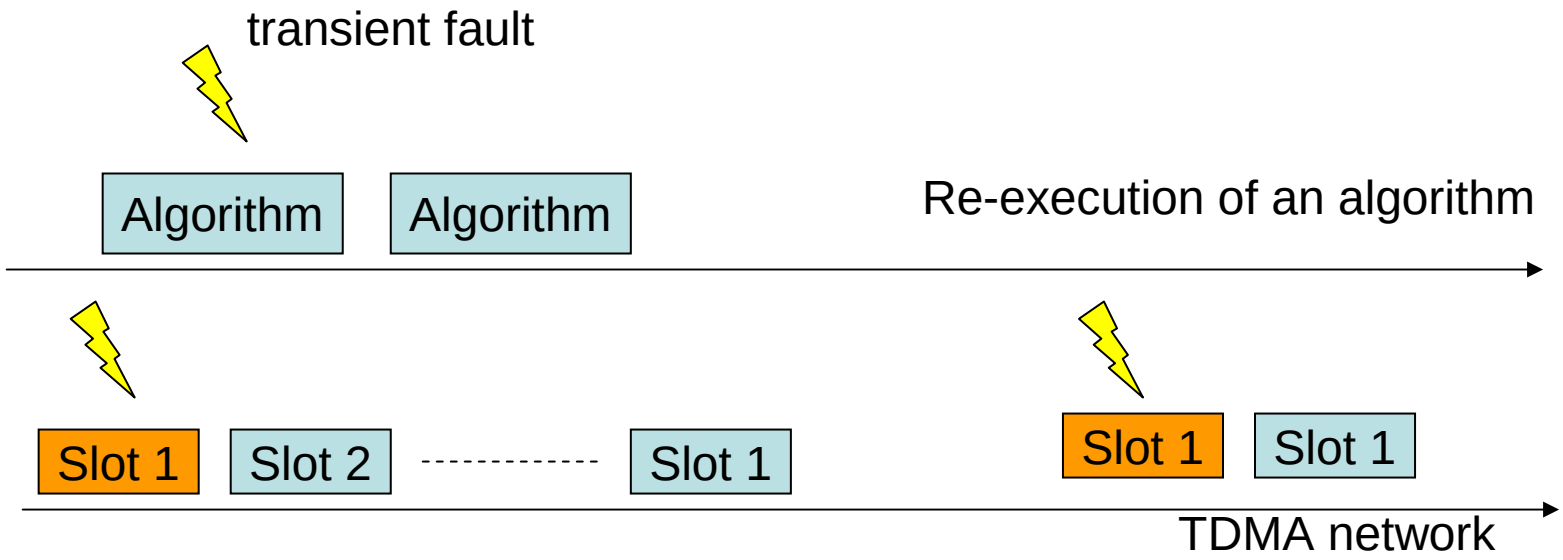


Exemplos

FEUP
Universidade do Porto
Faculdade de Engenharia

Redundância Temporal

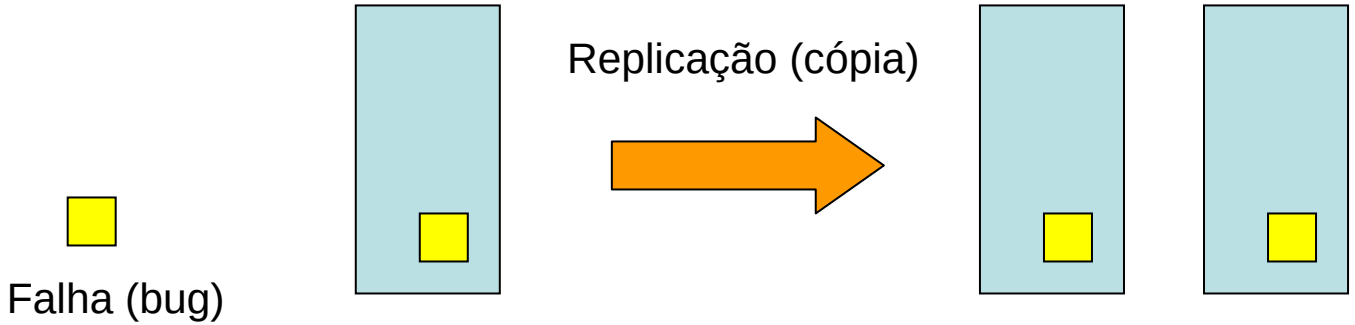
- Utilização de "tempo", para além do requerido para implementar uma dada função, destinada a detectar ou tolerar falhas;
- Pode ser implementada sob a forma de:
  - repetição de cálculos e comparação de resultados;
  - repetição de envio de mensagens e comparação de valores.



Exemplos

FEUP
Universidade do Porto
Faculdade de Engenharia

- Redundância de Software
  - Utilização de módulos de software suplementares, para além dos que seriam necessários no caso de um funcionamento sem falhas.
- Replicar o SW nem sempre é uma boa abordagem…



- Erros de concepção e implementação estão presentes em todas as cópias
- Solução: diversidade+ redundância

Bibliografia

FEUP
Universidade do Porto
Faculdade de Engenharia

- "Safety-Critical Computer Systems", Neil Storey, Addison Wesley, 1996
  - Capítulo 6
- Documentação de apoio nos conteúdos da disciplina