Universidade do Porto
FEUP Faculdade de Engenharia

Sistemas Críticos

Paulo Portugal, Francisco Vasques

{pportugal, vasques}@fe.up.pt

Universidade do Porto
FEUP Faculdade de Engenharia

Sistemas de Segurança Crítica

- Objetivos da Disciplina
  - Abrir os horizontes dos Engenheiros Informáticos para os Sistemas de Segurança Crítica;
    - » *"Security"*: ... não ocorrência de avarias intencionais;
    - » *"Safety"*: ...não ocorrência de avarias acidentais;
    - » *"Safety-Critical System"*: quando uma *avaria* pode ter consequências catastróficas...

Universidade do Porto FEUP Faculdade de Engenharia

Sistemas de Segurança Crítica

- Objetivos da Disciplina
  - Abordar noções ligadas à Segurança, fundamentais para desenvolvimento de Sistemas de Segurança Crítica.
    - » *"Security": ...* não ocorrência de avarias intencionais;
    - » *"Safety"*: ...não ocorrência de avarias acidentais;
    - » *"Safety-Critical System":* quando uma *avaria* pode ter consequências catastróficas...

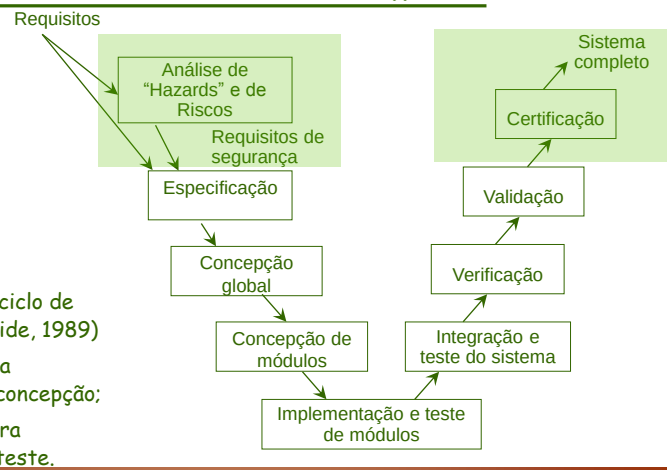
Universidade do Porto FEUP Faculdade de Engenharia

Sistemas de Segurança Crítica

- Objetivos da Disciplina
  - Abordar noções ligadas metodologias e técnicas para garantir Tolerância a Falhas ao nível das aplicações.
    - » *"Security": ...* não ocorrência de avarias intencionais;
    - » *"Safety"*: ...não ocorrência de avarias acidentais;
    - » *"Safety-Critical System":* quando uma *avaria* pode ter consequências catastróficas...

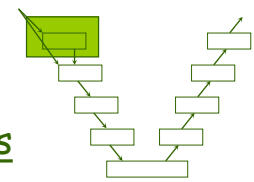
Sistemas de Segurança Crítica

- Noção de ciclo de vida de desenvolvimento:

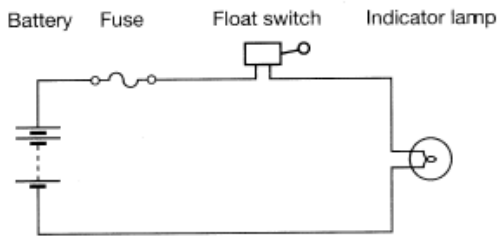


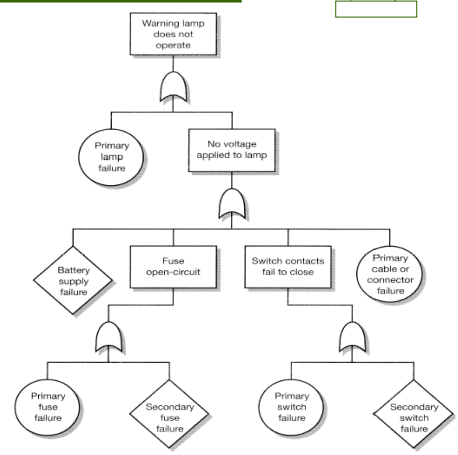
- Exemplo: Modelo de ciclo de vida em V (Starts guide, 1989)
  - » "Top-Down" para actividades de concepção;
  - » "Bottom-Up" para actividades de teste.

Sistemas de Segurança Crítica

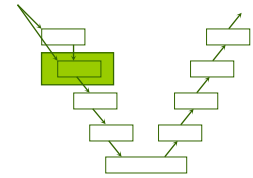


- Técnicas de Análise de *Hazards* e Riscos
  - FMEA/FMECA
  - HAZOP
  - FTA





Sistemas de Segurança Crítica

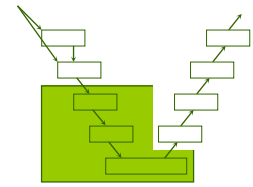


- Especificação
  - definição do SIL do sistema
    SIL -> Nível de Integridade de Segurança
  - definição de um conjunto de medidas a tomar para garantir a segurança do sistema.

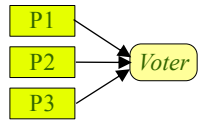
Table A.1 – SIL-table

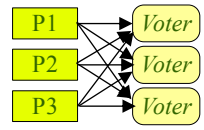
Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

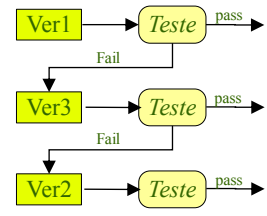
Sistemas de Segurança Crítica



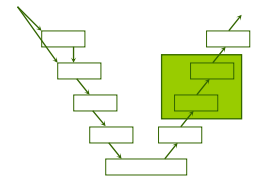
- Concepção e Implementação





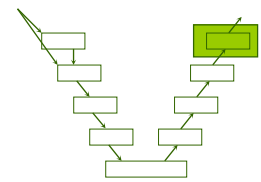


Sistemas de Segurança Crítica



- Técnicas de Verificação e Validação
  - O sistema pode ter sido adequadamente verificado (garantia de conformidade com a especificação)...
  - mas inadequadamente validado (garantia de conformidade com os requisitos).

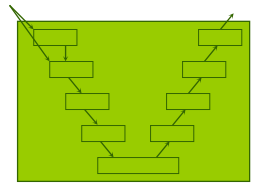
Sistemas de Segurança Crítica



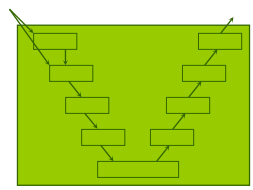
- Certificação
  - É necessário que uma entidade externa certifique que todo o sistema crítico foi concebido e desenvolvido através da utilização de procedimentos seguros.

Sistemas de Segurança Crítica

- Âmbito da Segurança
  - A garantia da segurança de um sistema não está unicamente ligada ao hardware e/ou software utilizados, envolvendo todos os aspectos ligados ao ciclo de vida do sistema, desde a sua concepção, até à sua instalação, utilização e manutenção.

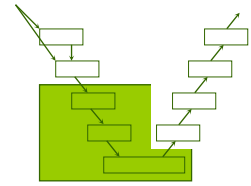


Programa



- Introdução aos Sistemas Críticos.
  - Taxonomia.
  - Apresentação de casos de estudo.
  - Critérios de segurança.

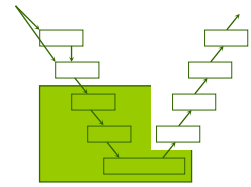
Programa



Tolerância a falhas

- Técnicas de tolerância a falhas em hardware
  - Redundância de hardware: estática, dinâmica e híbrida
  - Redundância temporal
  - Redundância de informação

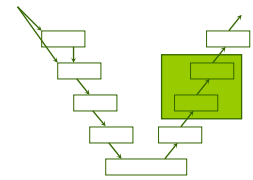
Programa



Tolerância a falhas

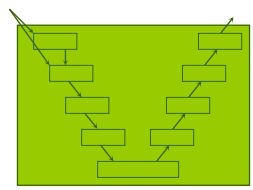
- Tolerância a Falhas em software:
  - Recuperação para trás vs Recuperação para a frente
  - Diversidade de Conceção/Implementação
  - Diversidade de Dados
  - Diversidade Temporal
  - Formas de Adjudicação de Resultados

Programa



- Verificação e validação:
  - Modelação da confiança no funcionamento: conceitos básicos;
  - Técnicas de modelação: blocos de fiabilidade e árvores de falhas
  - Fiabilidade do Software: conceitos, modelos, estimação de parâmetros
  - Modelação de arquiteturas HW/SW.

Programa



- Desenvolvimento de Sistemas Críticos
  - Análise de situações perigosas ("hazards")
  - Análise de risco.
  - Prevenção de falhas
  - Gestão de qualidade para Sistemas Críticos

Bibliografia

- Safety Critical Computer Systems
  Neil Storey, Addison-Wesley
- Software Safety and Reliability
  Debra S. Herrmann, IEEE Computer Society
- Software Fault Tolerance – Techniques and Implementation
  Laura L. Pullum, Artech House

Saídas Profissionais

OMNIDEA Lda.

SKYSOFT PORTUGAL

activespace technologies

Critical

Vulcano SOLUÇÕES DE ÁGUA QUENTE

esa

CERN

Avaliação

- Exame Final – 50%
- Trabalho – 50%