Universidade do Porto
FEUP Faculdade de Engenharia

Sistemas Críticos

Francisco Vasques, Paulo Portugal

{vasques, pportugal}@fe.up.pt

Universidade do Porto
FEUP Faculdade de Engenharia

Sistemas Computacionais de Segurança Crítica

- 1. Introdução
  - Exemplos de Acidentes
  - Conceitos Básicos e Terminologia
  - Áreas Relacionadas

Conceitos Básicos e Terminologia

- Segurança
- Sistemas Computacionais e Segurança
- Definições de Base
- Falhas, Erros e Avarias
- Situações Perigosas e Risco
- Requisitos e Critérios de Segurança

Segurança

- Definição de Segurança.
  - Confiança no funcionamento relativamente à não ocorrência de avarias catastróficas (avarias que colocam em causa a vida humana ou o ambiente).
- O que é um Sistema de Segurança Crítica?
  - Um sistema de segurança crítica ("*safety-critical system*") é aquele no qual a segurança (não ocorrência de avarias catastróficas) é garantida, em tempo de concepção/ implementação .

Segurança

- Sobre a Segurança
  - A segurança de um sistema depende essencialmente de uma concepção/implementação segura, e não de adicionar "segurança" a um sistema já desenvolvido.
  - A segurança de um sistema equaciona o sistema como um todo, e não como um conjunto de subsistemas ou componentes.

Segurança

- Sobre a Segurança
  - A segurança de um sistema considera de uma forma sistemática a possibilidade de ocorrência de situações perigosas ("*hazards*"), e não unicamente a ocorrência de avarias ("*failures*").
  - A segurança de um sistema deve ser fundamentada através da análise de ocorrência de situações perigosas ("*hazard analysis*") e através da análise de risco ("*risk analysis*"), e não unicamente através da análise de experiências anteriores e da aplicação de standards.

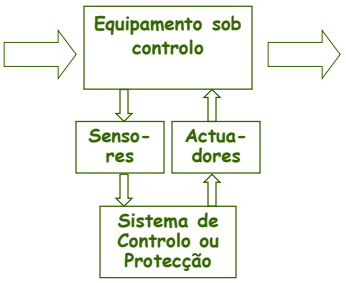
Segurança

- Sobre a Segurança
  - Segurança Primária: Inclui perigos causados directamente pelo próprio sistema. Por exemplo, no caso de hardware computacional, inclui perigo de electrocussão ou de simples choque eléctrico.

Segurança

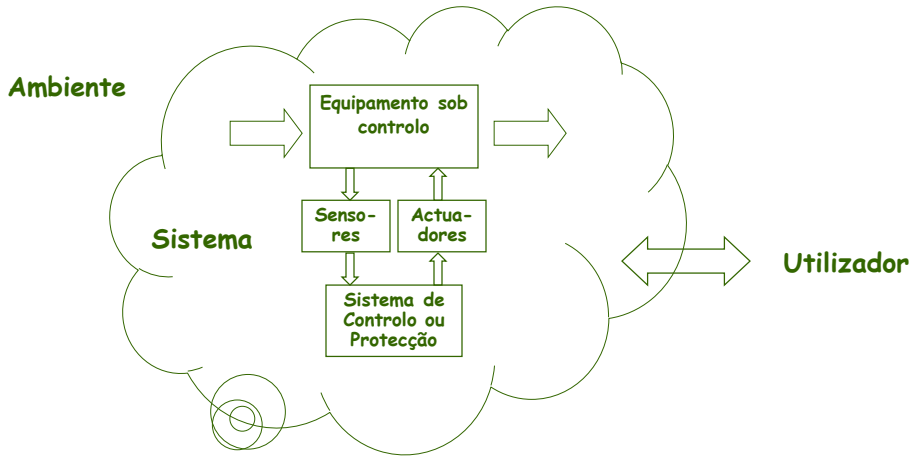
- Sobre a Segurança
  - Segurança Funcional: Diz respeito ao equipamento directamente controlado pelo sistema computacional e está relacionada com o correcto funcionamento do sistema computacional e do software.
  - Segurança Indirecta: Está relacionada com as consequências indirectas de uma avaria computacional ou com a produção de informação incorrecta.

Sistemas Computacionais e Segurança



- Sistema de Controlo.
  - Determina a forma de operação de um sistema (simples <-> complexo).
  - Caso especificado, também fornece funções de segurança (sistema de segurança crítica);
- Sistema de Protecção.
  - Utiliza sensores para detectar condições de falha e produz saídas tendentes a minorar (anular) os seus efeitos;
  - Caso especial: "*shutdown system*".

Sistemas Computacionais e Segurança



Sistemas Computacionais e Segurança

- Sistema, Ambiente, Utilizador
  - Um Sistema é uma entidade que interage ou interfere com outras entidades, i.e., com outros sistemas. Estes outros sistemas constituem o seu meio envolvente (Ambiente).
  - Um Utilizador de um sistema é aquela parte do ambiente que interage com o sistema considerado:
    - » o utilizador fornece entradas ao sistema e/ou recebe as suas saídas;
    - » o que o distingue do resto do meio envolvente é o facto de utilizar o serviço(s) prestado pelo sistema

Sistemas Computacionais e Segurança

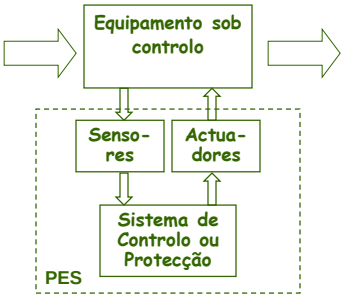
- Tendência:

  "Software is a pervasive Enabling technology"
  - » Actualmente, múltiplas funções de segurança crítica são já suportadas por sistemas computacionais;
  - » Os sistemas embarcados terão um papel dominante na nossa interacção com sistemas computacionais, mais cedo do que o esperado;
  - » O desenvolvimento de sistemas embarcados será brevemente um dos maiores clientes de tecnologia de segurança crítica (hardware/software/...)

Sistemas Computacionais e Segurança

- Gama de aplicação em Sistemas de Segurança Crítica:
  - Desde sofisticados sistemas aviónicos até controladores de máquinas de lavar; ou desde controladores para centrais nucleares até sistemas de ABS.
  - A utilização de microprocessadores mede-se na escala dos milhões de unidades para aplicações domésticas / aplicações no ramo automóvel ou na escala das unidades para sistemas dedicados, por exemplo na área do controlo industrial.

Sistemas Computacionais e Segurança



- "*Programmable Electronic Systems*" (PES)
  - Denominação tradicional para equipamento de controlo/ protecção baseado em sistema computacional, sob a forma de:
    - » Computadores convencionais;
    - » Micro-controladores
    - » Controladores Lógicos Programáveis (PLCs)

Definições de Base

- Confiança no funcionamento:
  - Propriedade que permite que um utilizador de um sistema computacional possa depositar uma confiança justificada no serviço que ele presta;
    - » Notar que um serviço, para ser bem sucedido, tem não só que produzir valores lógicos correctos (domínio do valor), mas também de os disponibilizar dentro de um determinado período de tempo (domínio do tempo).

Definições de Base

- Impedimentos à Confiança no Funcionamento
  - A Avaria de um sistema ocorre quando o serviço prestado deixa de estar conforme a especificação;
    - A definição de avaria foi posteriormente alargada para incluir comportamentos que, apesar de satisfazerem a especificação, sejam inaceitáveis para os utilizadores do sistema (falha na especificação).
  - Erro é um estado do sistema que pode levar a uma avaria.
  - A causa hipotética de um erro é uma Falha.

Definições de Base

- Meios para obtenção de confiança no funcionamento:
  - prevenção de falhas;
  - tolerância a falhas;
  - supressão de falhas;
  - previsão de falhas.
- Permitem:
  - fornecer a capacidade de prestar um serviço em que pode ser depositada confiança;
  - atingir confiança nesta capacidade.

Definições de Base

- Os atributos da confiança no funcionamento
  - permitem expressar as propriedades que se esperam do sistema;
  - permitem avaliar quantitativamente a qualidade do sistema que resulta dos impedimentos à sua confiança no funcionamento e dos meios utilizados para os ultrapassar.

Definições de Base

- Atributos da confiança no funcionamento:
  - relativamente à capacidade para estar pronto a utilizar, confiança no funcionamento significa disponibilidade;
  - no que respeita à continuidade do serviço prestado, confiança no funcionamento significa fiabilidade;
  - no que respeita à não ocorrência de avarias catastróficas, confiança no funcionamento significa segurança ("*safety*");
  - no que respeita à prevenção de acesso ou da manipulação de informação não autorizados, confiança no funcionamento significa inviolabilidade ("security").

Definições de Base

Falhas, Erros e Avarias

- Natureza das Falhas ("causa hipotética de um erro")
  - Falhas acidentais, que aparecem ou são criadas fortuitamente;
  - Falhas intencionais , que são criadas deliberadamente e de má fé.

Falhas, Erros e Avarias

- Origem das Falhas:
  - Causas Fenomenológicas:
    - » Falhas físicas , que se devem a fenómenos físicos adversos;
    - » Falhas humanas, que resultam de imperfeições humanas.

Falhas, Erros e Avarias

- Origem das Falhas:
  - Fronteiras do sistema:
    - » Falhas internas, que são aquelas partes do estado de um sistema que irão produzir um erro;
    - » Falhas externas, que resultam de interferência ou de interacção com o seu ambiente físico ou humano;

Falhas, Erros e Avarias

- Origem das Falhas:
  - Fase de criação:
    - » Falhas de concepção , que resultam de imperfeições
      - durante o desenvolvimento do sistema (da especificação dos requisitos até à implementação);
      - durante modificações subsequentes ao desenvolvimento;
      - durante o estabelecimento dos procedimentos para operar ou manter o sistema;
    - » Falhas de operação, que aparecem durante a exploração do sistema;

Falhas, Erros e Avarias

- Persistência temporal das falhas:
  - Falhas permanentes, quando a sua presença não está relacionada com condições pontuais, internas (actividade computacional) ou externas (meio envolvente);
  - Falhas transitórias, quando a sua presença se deve a tais condições pontuais e, consequentemente, estão presentes durante um tempo limitado .

Falhas, Erros e Avarias

- Discussão (sobre a origem das Falhas)
  - A ocorrência de uma falha num determinado sistema, é a consequência de uma avaria de um outro sistema que está a prestar um serviço ao sistema em consideração.
    - » este critério de classificação das falhas pode levar-nos, recursivamente, "muito para trás":
      - porque é que os programadores cometem erros?
      - porque é que os circuitos integrados avariam?
    - » a recursividade pára na causa que se pretende ser prevenida ou tolerada.

Falhas, Erros e Avarias

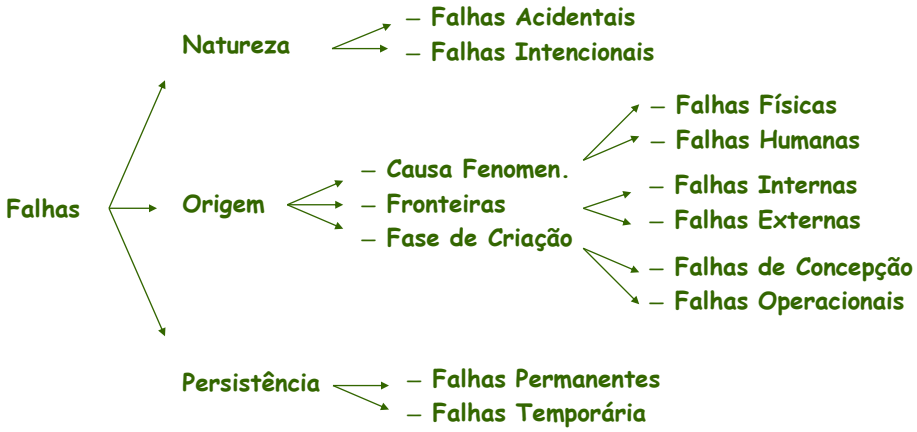
- Discussão (sobre Falhas)
  - Uma falha de concepção resulta de uma avaria de quem concebeu o sistema;
  - Uma falha física interna é devida a uma avaria num componente de hardware, que, por sua vez, é a consequência de um ou mais erros ao nível eléctrico ou electrónico.

Falhas, Erros e Avarias

- Discussão (sobre Falhas)
  - Uma falha externa física ou humana é uma falha de concepção: a incapacidade de prever todas as situações com que o sistema se vai deparar durante a sua vida operacional;
    - » no caso de EMI: será uma falha externa ou uma falha de concepção (ausência de uma blindagem adequada)?
    - » no caso de uma avaria causada por um operador que tecla um caracter desadequado: será uma falha de interacção ou uma falha de concepção (ausência de confirmação por parte do sistema)?

Falhas, Erros e Avarias

- Classes de Falhas



Falhas, Erros e Avarias

- Um Erro conduz ou não a uma avaria, dependendo de:
  - (1) Composição do sistema (tipo de redundância):
    - » redundância intencional, que se destina explicitamente a evitar que um erro conduza a uma falha;
    - » redundância involuntária que pode ter o mesmo resultado que a redundância intencional.

Falhas, Erros e Avarias

- Um Erro conduz ou não a uma avaria dependendo de:
  - (2) Actividade do sistema: um erro pode ser apagado antes de produzir estragos .

Falhas, Erros e Avarias

- Um Erro conduz ou não a uma avaria dependendo de:
  - (3) Definição de avaria do ponto de vista dos utilizadores: uma avaria para um dado utilizador, pode ser insignificante para outro (diferentes taxas de erro aceitáveis).

Falhas, Erros e Avarias

- O domínio de uma Avaria leva a distinguir:
  - Avarias de valor: o valor do serviço prestado não está de acordo com a especificação;
  - Avarias temporais: o tempo de prestação de um serviço não está de acordo com a especificação.

Falhas, Erros e Avarias

- Avarias por paragem ("*stopping failures*"):
  - » a actividade do sistema não é perceptível pelos utilizadores, passando a ser prestado um serviço de valor constante;
  - » Um sistema no qual as avarias são unicamente por paragem designa-se por Sistema Pára em caso de Avaria ("Fail-Stop")

Falhas, Erros e Avarias

- Avarias por omissão ("*ommission failure*")
  - » caso particular de avaria por paragem, no qual não é prestado qualquer serviço.
- Avaria por omissão persistente ("*crash failure*")
  - » Um sistema no qual as avarias são unicamente por omissão persistente designa-se por Sistema Silencioso em caso de Avaria ("*Fail-Silence*");

Falhas, Erros e Avarias

- Quando um sistema tem diversos utilizadores, distinguem-se em termos de percepção da avaria :
  - Avarias coerentes ("*Consistent Failures*"): todos os utilizadores do sistema têm a mesma percepção das avarias;
  - Avarias incoerentes ou Bizantinas ("*Byzantines Failures*"): os utilizadores do sistema poderão ter diferentes percepções de uma dada avaria.

Falhas, Erros e Avarias

- Em termos de consequências para o ambiente:
  - Avarias benignas, quando as suas consequências são da mesma ordem de grandeza (em termos de custos) do benefício proporcionado por um serviço correcto;

Falhas, Erros e Avarias

- Em termos de consequências para o ambiente:
  - Avarias catastróficas, quando as suas consequências são incomensuravelmente superiores ao benefício proporcionado por um serviço correcto.
    - » Um sistema no qual as avarias são unicamente avarias benignas designa-se por Sistema Seguro em caso de Avaria ("*Fail-Safe*");

Falhas, Erros e Avarias

- Cadeia "Falha → Erro → Avaria"
  - Uma falha torna-se activa quando produz um erro. Uma falha activa poderá ser:
    - » uma falha interna que estava previamente dormente e que foi activada pelo processo computacional;
    - » uma falha externa.
  - As falhas físicas apenas podem afectar directamente os componentes de hardware, enquanto que as falhas humanas podem afectar qualquer componente.

Falhas, Erros e Avarias

- Cadeia "Falha → Erro → Avaria"
  - Um erro está latente quando ainda não foi reconhecido com tal; um erro pode ser detectado por um mecanismo ou algoritmo de detecção.
  - Um erro pode propagar-se, o que geralmente acontece; ao propagar-se, um erro cria outro - novo - erro(s).
  - Uma avaria ocorre quando um erro "passa pela" interface utilizador-sistema e afecta o serviço prestado pelo sistema.

Falhas, Erros e Avarias

- Cadeia "Falha → Erro → Avaria"
  - A avaria de um componente resulta numa falha para o sistema que contem o componente;
  - Os modos de avaria do componente avariado são "tipos de falha" para os componente que com ele interagem.
- Estes mecanismos permitem completar a "cadeia fundamental":

… → avaria → falha → erro → avaria → falha → …

Falhas, Erros e Avarias

- Transições de estado "Falha → Erro → Avaria"

Falhas, Erros e Avarias

- Exemplos de cadeias "Falha → Erro → Avaria"
  - O resultado do erro de um programador é uma falha (dormente) no software escrito (instruções ou dados errados);
    - » Após a sua activação (ex.: invocação do componente onde a falha reside), a falha torna-se activa e produz um erro;
    - » Ocorrerá uma avaria se os dados erróneos afectarem o serviço prestado (em valor ou no tempo da sua prestação);

Falhas, Erros e Avarias

- Exemplos de cadeias "Falha → Erro → Avaria"
  - Uma perturbação electromagnética é uma falha;
    - » esta falha poderá causar directamente um erro;
    - » poderá provocar uma outra falha (interna); por exemplo alterando o valor de alguns bits da memória;
    - » estas falhas permanecerão dormentes até serem activadas (leitura daquele endereço de memória);
    - » a sequência erro-avaria desde a falha externa até à falha interna manifesta-se ao nível electrónico;

Falhas, Erros e Avarias

- Exemplos de cadeias "Falha → Erro → Avaria"
  - Uma interacção homem-máquina inadequada, quando executada por um operador durante a vida operacional de um sistema, é uma falha (do ponto de vista do sistema);
  - a alteração dos dados resultantes é um erro;
  - etc.

Falhas, Erros e Avarias

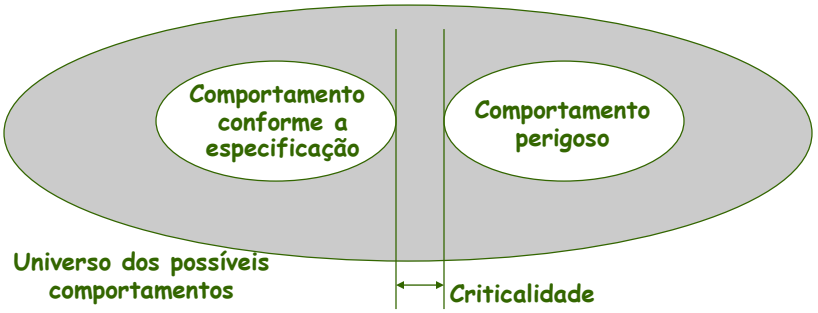
- Exemplos de cadeias "Falha → Erro → Avaria"
  - Um erro do editor de um manual de manutenção ou de utilização pode resultar numa falha no manual correspondente (directivas defeituosas);
  - Esta falha permanecerá dormente até que as referidas directivas não sejam aplicadas para fazer face a uma dada situação;
  - etc.

Situações Perigosas e Risco

- Segurança → Não existência de Acidentes?
  - Um Acidente é um evento ou uma sequência de eventos que tem como consequência:
    - » a morte ou o ferimento de pessoas;
    - » prejuízos ambientais ou materiais.
  - Um Incidente ("*Near Miss*") é um evento ou uma sequência de eventos inesperado(a) que não resulta em perdas, mas que noutras circunstâncias tem esse potencial.

Situações Perigosas e Risco

- Criticalidade
  - A criticalidade descreve "quão perto" se encontram entre si os modos de funcionamento correcto e perigoso;



Situações Perigosas e Risco

- Avaliação Qualitativa / Quantitativa
  - Uma Situação Perigosa ("*Hazard*") é uma situação na qual existe um perigo real ou potencial para a vida humana ou para o ambiente.
  - "*Hazard Analysis*": Identificação de cadeia(s) de acontecimentos conducentes à ocorrência de sit. perigosas
    - » Identificação sistemática de todas as possíveis ameaças contra a Segurança (Análise Qualitativa).

Situações Perigosas e Risco

- Análise da ocorrência de situações perigosas
  - As consequências de uma avaria podem não ser evidentes.
    - O controlador de uma máquina de lavar pode avariar por descontrolo de aquecimento, o que pode provocar um incêndio, com consequências catastróficas…
    - Apesar da reduzida probabilidade de ocorrência, as avarias em equipamentos domésticos são relevantes no contexto de segurança para a vida humana.
  - A análise qualitativa da ocorrência de situações perigosas pretende identificar possíveis ameaças contra a Segurança.

Situações Perigosas e Risco

- Avaliação Qualitativa / Quantitativa
  - Risco ("*Risk*") é a combinação da probabilidade de ocorrência de uma situação perigosa específica, e das sua consequências.
  - Análise de risco ("*Risk Analysis*"):
    - » Análise quantitativa do risco (probabilidade) associado a uma cadeia de acontecimentos na origem de uma situação perigosa específica.

Situações Perigosas e Risco

- Análise de risco ("*Risk Analysis*"):
  - Determina qual o nível de integridade apropriado para o sistema em questão;
  - Atribui um Nível de Integridade de Segurança ("*Safety Integrity Level*" - SIL) ao sistema;
    - » O SIL seleccionado define os métodos de concepção e de implementação que podem ser utilizados durante o ciclo de vida do sistema.

Requisitos e Critérios de Segurança

- Requisitos
  - A Segurança é uma propriedade do sistema. Logo, pode entrar em conflito com outros requisitos.
- Questão: Os aviões comerciais são seguros?
  - Raramente têm avarias catastróficas…
  - Quantas avarias catastróficas é necessário acontecerem para se considerar que são já em demasia?
- Questão: Os automóveis são seguros?
  - Têm avarias catastróficas frequentes…

Requisitos e Critérios de Segurança

Requisitos externos

- Requisitos Funcionais
  - Correcção ("*Correctness*")
  - Usabilidade
  - Credibilidade ("*Trustability*")
  - …
- Requisitos Não-Funcionais
  - Fiabilidade
  - Disponibilidade
  - Desempenho
  - Eficiência
  - …

Requisitos e Critérios de Segurança

Requisitos Internos

- Desenvolvimento
  - Compreensibilidade ("*Understandability*")
  - Testabilidade
  - Verificabilidade
  - ...
- Impacto noutros Projectos
  - Reusabilidade
- Manutenção
  - Recuperabilidade ("*Recoverability*")
  - Manutenibilidade
  - Portabilidade
  - ...

Requisitos e Critérios de Segurança

- Fiabilidade $R(t)$
  - Probabilidade de um componente, ou um sistema, funcionar correctamente durante um determinado período de tempo, e sob um determinado conjunto de condições de operação.
  - De uma forma quantitativa, $R(t)$ é a probabilidade de um sistema funcionar em conformidade com a sua especificação durante um período de duração t.

Requisitos e Critérios de Segurança

- Fiabilidade vs. Segurança
  - Fiabilidade e Segurança não são sinónimos. Por exemplo, num estado seguro em caso de avaria ("*failsafe state*"), o sistema está num estado seguro mas a fiabilidade é nula
    - durante um período de duração *t*, o sistema não está a funcionar em conformidade com a sua especificação.
  - Frequentemente, a Segurança tem que ser reduzida para permitir a satisfação de outros requisitos funcionais.

Requisitos e Critérios de Segurança

- Fiabilidade vs. Segurança (exemplo)
  - Sistema de sinalização ferroviária:
    - » semáforo vermelho ⇨ sistema num estado seguro
    - » sistema num estado seguro tem fiabilidade nula
    - ⇨ Fiabilidade ≠ Segurança

Requisitos e Critérios de Segurança

- Fiabilidade vs. Segurança (exemplo)
  - Sistema de controlo "*Fly-by-Wire*"
    - » num avião, após a decolagem não existem estados seguros (não-funcionais);
    - » Neste caso, Fiabilidade = Segurança
  - Frequentemente, existe um conflito entre Segurança e Fiabilidade

Requisitos e Critérios de Segurança

- Disponibilidade A
  - Probabilidade de um componente, ou um sistema, estar a funcionar correctamente em qualquer instante de tempo.
  - De uma forma quantitativa, A é a percentagem de tempo durante o qual o sistema está a funcionar em conformidade com a sua especificação.

Requisitos e Critérios de Segurança

- Fiabilidade vs. Disponibilidade (Exemplo)
  - Um sistema que avaria, em média, uma vez por hora, mas que re-arranca automaticamente em 10ms, é um sistema que é pouco fiável mas que tem uma grande disponibilidade.
  - Em aplicações de Automação Industrial, o sistema computacional tem que garantir uma elevada disponibilidade. A fiabilidade não tem o mesmo nível de importância.

Requisitos e Critérios de Segurança

- Operação Segura em caso de Avaria ("*Failsafe*")
  - Caso um estado seguro exista e seja alcançável, quaisquer que sejam as condições de operação, a concepção do sistema pode utilizar este estado para garantir uma Operação Segura em caso de Avaria ("*Failsafe*");
    - » Através de uma comutação para o estado seguro em caso de avaria seguida de incapacidade de recuperação.
  - Exemplo: Semáforo vermelho no caso de sinalização ferroviária.

Requisitos e Critérios de Segurança

- Integridade
  - Integridade de um Sistema ("*System Integrity*") é a capacidade de um sistema detectar falhas na sua própria operação e de informar o utilizador desse facto.
  - Integridade de Dados ("*Data Integrity*") é a capacidade de um sistema evitar a corrupção dos seus dados e de detectar, e possivelmente corrigir, erros que ocorram.
  - Recuperação do Sistema ("*System Recovery*") é a capacidade de um sistema detectar avarias e de retomar rapidamente no caso de falhas transitórias.

Requisitos e Critérios de Segurança

- Manutenibilidade
  - Manutenção designa o conjunto de procedimentos e operações a efectuar para manter um sistema, ou para o fazer regressar, às suas condições de operação especificadas.
  - Manutenibilidade representa a facilidade com que as acções de manutenção podem ser levadas a cabo.
    - » Problema: As acções de manutenção podem despoletar a ocorrência de avarias.

Requisitos e Critérios de Segurança

- Exemplos de requisitos
  - Telecomunicações
    - » Disponibilidade, Manutenibilidade.
  - Transportes.
    - » Fiabilidade, Disponibilidade, Segurança
  - Armamento
    - » Segurança.
  - Sistemas Nucleares
    - » Segurança.

Sistemas Computacionais de Segurança Crítica

- 1. Introdução
  - Exemplos de Acidentes
  - Conceitos Básicos e Terminologia
  - Áreas Relacionadas

Áreas Relacionadas

- Questão: Quais os sistemas que são de Segurança Crítica, e quais os que não o são?
- Como se relaciona a Segurança com:
  - » Inviolabilidade ("*Security*")?
  - » Sistemas de Elevada Integridade ("*High Integrity*")?

Áreas Relacionadas

- Segurança vs. Inviolabilidade
  - Segurança: Risco para a vida humana ou para o ambiente
  - Inviolabilidade: Risco para a privacidade (pessoal ou organizacional) ou para a segurança nacional.
    - » Em ambos os casos, a certificação não é ditada por questões económicas.

Áreas Relacionadas

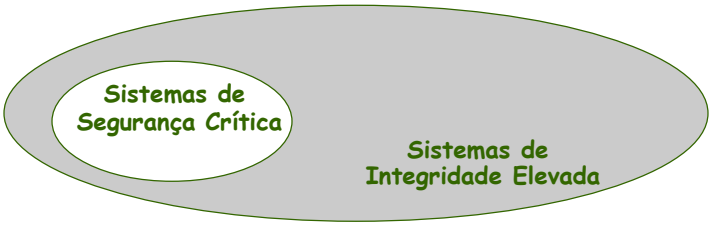
- Segurança vs. Inviolabilidade
  - Inviolabilidade
    - » Considera unicamente acções maliciosas
    - » Baseada na prevenção de acessos não autorizados
  - Segurança
    - » Considera também acções "bem intencionadas"
    - » Evita, de uma forma geral, as acções maliciosas

Áreas Relacionadas

- Segurança vs. Inviolabilidade
  - Quando um acesso não autorizado a um sistema pode resultar num acidente
    - ⇨ A Segurança também requer um pouco de Inviolabilidade!
  - Quando um acesso não autorizado pode ser considerado um acidente

Áreas Relacionadas

- Sistemas de Integridade Elevada
  - "High Integrity System: A system that must be trusted to work dependably and may result in unacceptable loss or harm otherwise. This includes Safety-Critical Systems and other critical systems."



Áreas Relacionadas

- Integridade Elevada vs. Segurança
  - Exemplo de Sistemas de Integridade Elevada que não são Sistemas de Segurança Crítica
    - » Sistemas de Comutação Telefónica
    - » Sistemas de Comunicação via Satélite
  - Comentário:
    - » No caso de avaria neste tipo de sistemas, existirão severas perdas económicas; no entanto, daqui não resultará risco para a vida humana, nem para o ambiente.

Conclusão

- "A fundamental conclusion is that, even if we are extremely cautious and lucky, we must still anticipate the occurrences of serious catastrophes in using computer systems in critical applications".

[Neumann, 95]