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

Exemplos de Acidentes

- Automatização do "London Ambulance Service" (1992)
- Fracasso dos Mísseis "Patriot" (1991)
- Acidente com Airbus A-320 em Habsheim (1988)
- Problemas mais recentes
- Lições Retiradas

Automatização do "London Ambulance Service"

- O "London Ambulance Service" (LAS)
  - Sistema de ambulâncias, cobrindo uma área de 250km2 para servir 7-12 milhões de potenciais utilizadores;
  - Trata diariamente 5000 pacientes, 2000-2500 chamadas telefónicas, das quais 1300-1600 de emergência;

Automatização do "London Ambulance Service"

- Automatização do LAS
  - No centro do LAS está um centro de despacho responsável pelo atendimento de chamadas, localização de ambulâncias, despacho da ambulância que melhor possa servir cada paciente e monitorização do seu estado ("a caminho", "no local", "em direcção ao hospital", "livre", etc.
- Caso de estudo
  - Transformou-se num caso de estudo acerca de "como não conceber, desenvolver ou implementar um sistema crítico em termos de segurança";

Automatização do "London Ambulance Service"

- Arranque do LAS
  - Dia de arranque: 26/10/1992, 07:00h;
    O centro de comando foi modificado para receber um novo sistema "paperless", colocando o sistema anterior inoperacional;
  - O sistema automatizado estava baseado num AVLS ("Automatic Vehicle Location System") para identificar ambulâncias, para efectuar alocação de recursos e para comunicar com os MDT ("Mobile Data Terminals") dos veículos;

Automatização do "London Ambulance Service"

- Arranque do LAS
  - As tripulações foram informadas para manterem um tráfego de voz reduzido com a central.
  - 10:00h.
    O numero de chamadas aumenta e o sistema começa a ter dificuldades. O AVLS não consegue manter actualizada a posição e o status das ambulâncias e começa a despachar incorrectamente (e mesmo a despachar múltiplas ambulâncias para o mesmo local);

Automatização do "London Ambulance Service"

- Arranque do LAS
  - Notificações de excepção começam a ser geradas em cascata. A dificuldade de resposta a um grande numero de excepções pela parte dos operadores, leva a que as mais antigas deixem de estar visíveis nos terminais, provocando a geração de um numero crescente de mensagens de excepção;
  - O aumento inerente da lentidão do sistema, leva a que os pacientes coloquem chamadas suplementares nas filas de espera, aumentando ainda mais a sua lentidão.

Automatização do "London Ambulance Service"

- Frustração
  - Sob pressão, as tripulações deixaram de informar o centro de despacho acerca do seu status (via MDT).
  - A aparente falta de recursos para alocar, sobrecarregou a execução do software de alocação de recursos, aumentando ainda mais o atraso do sistema;
  - As tripulações das ambulâncias acostumadas a atrasos de alguns minutos na resposta a chamadas de paciente, começam a responder com várias horas de atraso.

Automatização do "London Ambulance Service"

- 2 casos tiveram ampla repercussão na imprensa:
  - Uma pessoa cuja mãe tivera um ataque de coração ao inicio da tarde, decidiu levá-la de taxi para o hospital após 6h de espera. Às 2:00AM recebeu uma chamada telefónica, a perguntar se ainda precisava de assistência.
  - Uma ambulância respondendo a uma chamada colocada 8h antes, verificou que o corpo tinha acabado de ser retirado por uma agência funerária...

Automatização do "London Ambulance Service"

- Após o colapso inicial...
  - O despacho do LAS passou a semi-manual, com as chamadas atendidas e impressas automaticamente.
  - A selecção passou a ser efectuada manualmente em conjunto com a estação mais próxima do incidente, e enviada para o MDT da ambulância seleccionada.

Automatização do "London Ambulance Service"

- Após o colapso inicial...
  - Este sistema funcionou razoavelmente até às 2:00 de 4/11 (9 dias após o arranque), começando então a ficar mais lento, até parar;
  - A re-inicialização dos computadores não resolveu o problema. O servidor de backup não pode ser utilizado pois não tinha sido totalmente implementado, nem testado em modo semi-manual;
  - Em consequência as chamadas deixaram de poder ser impressas, e deixou de haver comunicação com os MDTs.

Automatização do "London Ambulance Service"

- Após o colapso inicial...
  - Os operadores passaram a sistema manual, garantindo que todas as chamadas gravadas em fita magnética foram atendidas, com a mobilização das ambulâncias efectuada via rádio e telefone.

Automatização do "London Ambulance Service"

- O que correu mal?
  - "*On 26 and 27 October 1992 the computer system itself did not fail in a technical sense. Response times did on occasions become unacceptable, but overall the system did what it had been designed to do.*"

    Relatório da comissão de inquérito, 1993.

Automatização do "London Ambulance Service"

- O que de facto correu mal
  - No arranque do sistema, o software estava incompleto, não tinha sido ajustado, nem tinha sido completamente testado (nomeadamente sob cenários com a carga adequada).
  - O sistema de backup estava inoperacional, e o sistema anterior (baseado em papel) tinha sido abandonado.
  - Nestas condições, restringir a utilização do rádio e depender unicamente de um sistema automático foi correr um risco desmesurado.

Automatização do "London Ambulance Service"

- O que de facto correu mal
  - Os factores humanos foram totalmente negligenciados:
    - » mudança súbita na configuração do local de trabalho;
    - » fim absoluto do habitual sistema de backup "em papel";
    - » fim da comunicação informal com as tripulações e as estações locais;

  levaram a que os operadores se sentissem fora do sistema, sem poderem influenciar a sua evolução.

Automatização do "London Ambulance Service"

- O que de facto correu mal
  - A concepção do sistema falhou, porque foi considerado que a informação sobre a localização e o status de cada ambulância estaria sempre disponível;
    - » existiam problemas com as rotinas de comunicação e as interfaces eram fracas;
  - O sistema era pouco fiável, havia bloqueios frequentes com recurso habitual à sua re-inicialização.

Automatização do "London Ambulance Service"

- O que de facto correu mal
  - A interface com o operador era muito fraca:
    - » impossível identificar chamadas repetidas;
    - » impossível prioritizar mensagens urgentes;
    - » quando o écran ficava cheio de mensagens, as mais antigas desapareciam;
    - » erros no software de alocação de recursos;
  - Tempos de resposta lentos para certas operações baseadas em interfaces gráficas.

Automatização do "London Ambulance Service"

- O que de facto correu mal
  - O crash de 4/11 foi devido a um erro de manutenção.
  - Uma rotina de teste que efectuava uma alocação de memória cada vez que uma ambulância era seleccionada, foi esquecida no sistema.
  - Ao fim de 3 semanas, a capacidade de memória esgotou, levando à paragem do sistema.

Automatização do "London Ambulance Service"

- Principais conclusões
  - Uma das principais causas do colapso foi a pressão política para ter o sistema a funcionar pelo menor preço e no mais curto espaço de tempo possível;
  - Infelizmente, a Comissão de Inquérito não fez nenhuma avaliação detalhada do custo final associado ao colapso do sistema.

Automatização do "London Ambulance Service"

- Recomendação da Comissão de Inquérito
  - "The development of a strategy for the future of Computer Aided Dispatch (CAD) within the London Ambulance System (LAS) must involve a full process of consultation between management, staff, trade union representatives and the Service's information technology advisers […]"
  - "What is certain is that the next CAD system must be made to fit the Service's current or future organisational structure and agreed operational procedures. This was not the case with the current CAD."

Exemplos de Acidentes

- Automatização do "London Ambulance Service" (1992)
- Fracasso dos Mísseis "Patriot" (1991)
- Acidente com Airbus A-320 em Habsheim (1988)
- Problemas mais recentes
- Lições Retiradas

Fracasso dos Mísseis "Patriot"

- Cenário: Guerra do Golfo, 1991;
  - Em 25/2/1991 um míssil Scud passou através das defesas anti-míssil Patriot, provocando a morte ou ferimentos a 28 e 98 soldados, respectivamente.
  - A avaria que levou a este acidente está documentada, e tem uma explicação simples: concepção deficiente do sistema de controlo.

Fracasso dos Mísseis "Patriot"

- Descrição do sistema
  - O sistema de controlo de um míssil Patriot examina em contínuo o céu para detectar eventuais alvos. Caso algo seja detectado, estreita a "zona de detecção" em torno do objecto detectado para identificação.
  - Em seguida, caso seja identificado um alvo, deve-o seguir com precisão.

Fracasso dos Mísseis "Patriot"

- Descrição do sistema
  - Patriot software measured time in increments of 0.1s second.
  - The decimal value 0.1 cannot be exactly represented in binary as it is a recurring fraction.
  - The Patriot used 24-bit arithmetic to represent time.
  - The longer a Patriot missile is in operation (booted up) the greater the accumulated time error becomes.

Fracasso dos Mísseis "Patriot"

- O que correu mal...
  - O sistema foi concebido para funcionar durante no máximo algumas horas, antes de ser transportado para uma nova localização (cenário de guerra Europeu).
  - No Golfo, o sistema estava em funcionamento contínuo há mais de 100h, provocando uma perda de precisão dos cálculos efectuados (erro acumulado de 0.34s).
  - A Scud flies at over 1,600 m/s and covers over 500 m in this time.
  - Devido a esta perda de precisão, a "zona de detecção" desviou-se do alvo. Em consequência, o míssil Scud atravessou o sistema anti-mísseis.

Fracasso dos Mísseis "Patriot"

- Razões técnicas
  - O cálculo da localização do míssil era efectuada com base nos valores de velocidade e de tempo (inteiros).
  - A precisão dos cálculos estava limitada pelas conversões inteiros/reais e pelo facto de os registos serem unicamente de 24 bits.
  - Em consequência, a precisão da "zona de detecção" era inversamente proporcional à velocidade do míssil e ao tempo de funcionamento do sistema.

Fracasso dos Mísseis "Patriot"

- Conclusões
  - Este acidente pode ser interpretado como consequência de um erro de programação, visto ter sido provado que a especificação funcional dos requisitos estava correcta.
  - A modificação das condições de operação (ambiente) colocou em evidência um modo de avaria crítico, que anteriormente não se tinha manifestado.

Fracasso dos Mísseis "Patriot"

- Conclusões
  - Falhas conhecidas (como a que causou o desvio da zona e detecção) e procedimentos de "desenrasca" (como a necessária re-inicialização periódica) devem estar devidamente documentados.

Exemplos de Acidentes

- Automatização do "London Ambulance Service" (1992)
- Fracasso dos Mísseis "Patriot" (1991)
- Acidente com Airbus A-320 em Habsheim (1988)
- Problemas mais recentes
- Lições Retiradas

Acidente com Airbus A-320 em Habsheim

- Principais características de sistemas "Civilian-FBW"
  - A320-100 foi o primeiro avião comercial a implementar um sistema "Fly-by-Wire" (FBW)
  - As principais características do FBW no A320-100 são:
    - » Facilidade no treino de pilotagem (interface de pilotagem idênticas em diferentes tipos de Airbus)
    - » Simplicidade na manutenção, devido à modularidade do sistema de controlo, que permite a troca simples de qualquer dos sistemas computacionais de bordo;

Acidente com Airbus A-320 em Habsheim

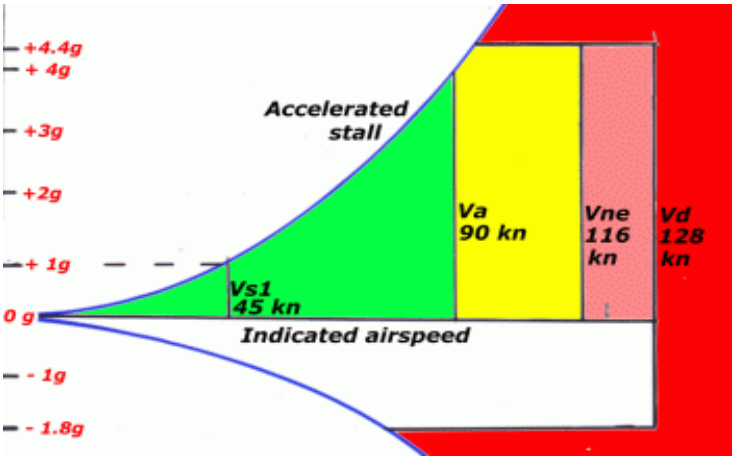
  - As principais características do FBW no A320-100 são:
    - » Implementação de algoritmos de controlo avançados, para a obtenção de "*neutral static stability*", ou seja, a tendência de manter o perfil de voo ("*attitude*") quando os pilotos libertam os comandos;
    - » Devido ao facto de o sistema de controlo ser maioritariamente definido em software, permite a sua fácil revisão para inclusão de novos requisitos resultantes da experiência operacional.

Acidente com Airbus A-320 em Habsheim

- As principais características do FBW no A320-100 são:
  - » Sistema de detecção e monitorização de falhas que armazena e disponibiliza dados sobre todas as avarias no final de cada voo;
  - » Segurança reforçada contra erros acidentais de pilotagem, através da definição de "*flight envelopes*". Este sistema impede velocidades superiores ou inferiores a limites pré-estabelecidos (mesmo no caso de descidas abruptas), diminuindo o risco de avarias estruturais;

The Flight Envelope

For a light aircraft from http://www.auf.asn.au/groundschool



The envelope defines the aircraft's safe area of operation.

The boundaries of the flight envelope are the aerodynamic stall and structural damage.

Alan Clements

The A320 Cockpit

Alan Clements

The sidestick gives a very uncluttered layout.

The sidestick provides a demand input to the computer. The computer controls the flying surfaces according to a set of algorithms.

One pilot can lockout the other pilot's sidestick.

Special problems of the A320 fly-by-wire system

Acidente com Airbus A-320 em Habsheim

- Acidente de Habsheim
  - Em 26/6/1988, um Airbus A320-100 teve um acidente em Habsheim, Mulhouse, França, durante um voo de demonstração;
  - Estava previsto efectuar uma primeira passagem "lenta" a 30m de altitude e 25º de inclinação *("near stall")*, e em seguida, efectuar uma 2ª passagem "rápida" a 30 m de altitude;
  - A 2ª passagem não foi efectuada, devido ao facto de o avião não ter conseguido subir no final da 1ª passagem.

Acidente com Airbus A-320 em Habsheim

» Como resultado do acidente (e do fogo que deflagrou), morreram 4 dos 130 passageiros (34 feridos). Dos 6 membros da tripulação, 4 ficaram feridos.

Acidente com Airbus A-320 em Habsheim

- O que correu mal (conclusão da Comissão de Inquérito):
  - Altitude de voo inferior à dos obstáculos existentes;
  - Velocidade demasiado reduzida (para maximizar angulo de ataque), com motores em estado "*idle*";
  - Aceleração tardia.

    "*Too low, too slow, too late*"
  - Conclusão: Erro Humano, visto ter sido apurado que o avião se encontrava em correcto estado de funcionamento.

Acidente com Airbus A-320 em Habsheim

- O que correu mal (conclusões do piloto Michel Asseline)
  - As sequências de treino efectuadas e as garantias do construtor, levaram a tripulação a um estado de sobre-confiança acerca da manobrabilidade do aparelho;
    - » Por exemplo, os manuais de voo garantiam que o voo a elevados graus de inclinação eram seguros. Os pilotos poderiam colocar o "*flight stick*" na posição extrema, que o software de controlo garantiria a não ultrapassagem do "*flight envelope*" seguro.
  - A especificação das altitudes correctas de passagem (30m / 100m) não foi incluída no plano de voo.

Acidente com Airbus A-320 em Habsheim

- O que correu mal (conclusões do piloto Michel Asseline)
  - A tripulação não compareceu na reunião de segurança (comparência obrigatória), devido a erro da Air France;
    - » Nesta reunião teriam tido conhecimento das limitações impostas ao voo de demonstração.
  - O dossier de voo (efectuado pelos serviços de segurança) foi entregue tardiamente à tripulação. Como resultado, esta só soube que havia árvores no final da pista com 10-15m de altura quando estavam em pleno voo...

Acidente com Airbus A-320 em Habsheim

- O que correu mal (conclusões do piloto Michel Asseline)
  - O piloto pensava estar a voar a 30m de altitude, quando se encontrava a voar unicamente a 10m de altitude. Duas razões foram apuradas para este facto:
    - » O aeroporto de Habsheim sendo menor que os aeroportos tradicionais, falseou as referências visuais do piloto;
    - » O altímetro utilizado pelo piloto apresentava um erro de 25m. A Air France argumenta que o piloto não efectuou a sua correcta calibração, enquanto que o piloto suspeita de uma falha no software de comunicação entre sistemas (conforme relatado noutros casos).

Acidente com Airbus A-320 em Habsheim

- O que correu mal (análise posterior)
  - Através da análise do acidente, parece claro que este não se deveu a uma avaria no software, no sentido de "ocorrência de falha de software que tenha provocado um desvio do comportamento especificado".
    - » No entanto este ponto não foi devidamente clarificado, devido a uma clara obstrução da Air France à completa análise das causas do acidente.

Acidente com Airbus A-320 em Habsheim

- O que correu mal (análise posterior)
  - O que parece claro é que os requisitos para os sistemas embarcados foram inadequadamente especificados, para o caso de o avião ser operado em condições limite.
  - Adicionalmente, o sistema de controlo tem um impacto severo na forma de pilotagem. A sobre-confiança e a dependência do piloto no sistema de controlo foram uma causa clara para o acidente.

Acidente com Airbus A-320 em Habsheim

- O que correu mal (análise posterior)
  - É possível o construtor defender que "todos os sistemas tiveram um desempenho conforme o especificado".
  - No entanto, através da análise das sequências de diversos acidentes, fica evidente que a forma como se comportaram os sistemas computacionais embarcados teve um impacto evidente em cada um dos acidentes.

Exemplos de Acidentes

- Automatização do "London Ambulance Service" (1992)
- Fracasso dos Mísseis "Patriot" (1991)
- Acidente com Airbus A-320 em Habsheim (1988)
- Problemas mais recentes
- Lições Retiradas

Problemas recentes

- Infraestruturas Críticas
  - Múltiplos blackouts devido a falhas de software de redes públicas de transporte de energia têm sido reportados;
  - Ataques do tipo "inserted trap doors" e "trojan horses" aos sistemas computacionais de controlo têm sido detetados;

Problemas recentes

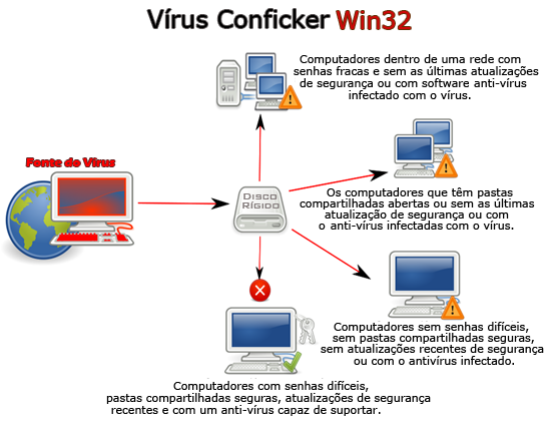
- Infraestruturas Críticas
  - A capacidade de deteção e diagnóstico de ataques a estas infraestruturas é muito reduzida;
  - É fundamental a proteção contra ataques à integridade e à segurança dos sistemas de informação que suportam as infraestruturas críticas (energia; telecom.; etc.).

Problemas recentes

- "Malware"
  - A existência / disseminação incontrolável de "malware" tem como consequência uma crescente "falta de confiança" nos sistemas de informação / redes que suportam os sistemas críticos

Problemas recentes

- "Malware"
  - Por exemplo, várias gerações do malware Conficker reapareceram em 2009, explorando "unpatched operating systems";



Problemas recentes

- Sistemas de votação eletrónicos
  - Dificuldades evidentes de "accountability"

Exemplos de Acidentes

- Automatização do "London Ambulance Service" (1992)
- Fracasso dos Mísseis "Patriot" (1991)
- Acidente com Airbus A-320 em Habsheim (1988)
- Problemas mais recentes
- Lições Retiradas

Principais Lições Retiradas

- The question is not, "Do computers cause errors?" but, "Do computers cause more or less errors than people alone"?

Principais Lições Retiradas

- Será que estas são "verdades absolutas"?
  - The computer apparently provides a solutions to all our problems.
  - The computer is accurate (error free) and reliable. Given the same data and same program it always achieves the same result.
  - The computer never gets distracted or gets tired.

Principais Lições Retiradas

- Acidentes Controlados por Computador
  - The theme of this lecture is the danger of computers inducing errors into systems.
  - These errors are often caused by a failure of the human-computer interface.
  - Consequently, these errors can also be regarded as a failure of the designers to anticipate problems.
  - Many of these problems are not new, unusual, or radical. They are the problems of everyday life – but with more serious consequences.

Principais Lições Retiradas

- O software avaria
  - Um sistema avaria quando o serviço prestado não está em conformidade com a especificação.
  - A avaria pode ser devida à activação de uma falha de concepção (falha latente). Se esta falha reside no software, então o software avaria.

Principais Lições Retiradas

- Contra argumentos (o software não avaria…):
  - O código fonte tem a sua própria especificação, logo "o serviço prestado está de acordo com a especificação"…
  - Errado, porque:
    - » O código objecto pode não ser uma transformação correcta do código fonte (avaria no compilador)
    - » O código fonte do software pode não implementar o requerido por uma especificação de nível superior (exemplo de avaria nos mísseis Patriot)

Principais Lições Retiradas

- O software é uma abstracção, que não funciona por si próprio, logo não pode avariar
  - No entanto, quando implementado num sistema deixa de ser uma abstracção, e passa a fazer parte de um sistema com uma implementação física (exemplo de avaria por deficiente alocação de memória no LAS)

Principais Lições Retiradas

- O software não se desgasta
  - Correcto, mas irrelevante. Isto só significa que as causas de uma avaria no software diferem das causas de uma avaria no hardware

Principais Lições Retiradas

- O software é sempre parte integrante de um sistema mais vasto
  - A avaliação de desempenho do software deve ser efectuada para o ambiente de execução pretendido
  - A verificação do software deve ser efectuada durante as fases de especificação e programação
  - A validação do software deve ser efectuada em operação.

Principais Lições Retiradas

- As falhas de concepção podem ser introduzidas em diferentes níveis
  - Quando os requisitos escritos não estão em conformidade com os requisitos "reais".
    - » Estes requisitos são por vezes expressos de uma forma implícita ou informal.
      "*It's just what I asked for, but not what I want*".
  - Quando a especificação não está em conformidade com os requisitos escritos

Principais Lições Retiradas

- As falhas de concepção podem ser introduzidas em diferentes níveis
  - Quando o código fonte não está em conformidade com os requisitos
    - » Ex.: avaria devida ao cálculo de janela nos mísseis Patriot
  - Quando o código máquina não está de acordo com o código fonte
    - » Ex.: devido a avaria ou documentação insuficiente de compilador

Principais Lições Retiradas

- A especificação errada de requisitos é uma das maiores causas de acidentes
  - O sistema pode ter sido adequadamente verificado (garantia de conformidade com a especificação) mas inadequadamente validado (garantia de conformidade com os requisitos)
  - "*The software is behaving to specification, but its behavior causes sufficient problems for the user for it to count as failure*"

Principais Lições Retiradas

- Falhas de concepção singulares raramente são a causa de um acidente
  - Na maior parte dos casos, em sistemas complexos, os acidentes ocorrem quando múltiplas avarias interagem de uma forma não expectável;

Principais Lições Retiradas

- Falhas de concepção singulares raramente são a causa de um acidente
  - No caso particular do software, as falhas nem sempre podem ser localizadas num simples módulo. Por exemplo,
    - » no caso de deficiências na especificação de requisitos;
    - » no caso de desempenho inadequado do sistema (por exemplo, no colapso do LAS);
    - » ou no caso de interacções complexas entre múltiplas interfaces.

Principais Lições Retiradas

- O operador é parte do sistema
  - Sempre que um erro humano possa provocar acidentes, este facto deve ser tomado em consideração na avaliação da segurança do sistema
  - Exemplo:
    - » Inicialmente vários dos acidentes dos Airbus foram atribuídos a erros humanos;
    - » Posteriormente foram detectadas insuficiências graves a nível da concepção das interfaces homem-máquina.

Principais Lições Retiradas

- O erro humano é inevitável
  - A concepção de um sistema deve garantir a máxima robustez contra erros humanos e fornecer um ambiente de trabalho para o operador que minimize a probabilidade de erro
  - O erro humano é frequentemente uma desculpa para uma fraca concepção

Principais Lições Retiradas

- O erro do operador é habitualmente uma desculpa para uma deficiente concepção
  - "*...technically, nothing at all failed...*"
  - A intenção é, por vezes, culpar o operador, por forma a ilibar o fabricante/fornecedor do sistema;
  - No entanto, é sempre pertinente analisar cuidadosamente a razão pela qual o operador errou...

Principais Lições Retiradas

- Maior complexidade do sistema implica normalmente a sua menor fiabilidade
  - A interacção (acoplamento) entre diferentes modos de funcionamento de vários sistemas significa que, por vezes, é extraordinariamente difícil analisar a possibilidade de ocorrência de situações perigosas;
  - A utilização de sistemas computacionais tende a incrementar a complexidade dos sistemas e o acoplamento entre os seus diferentes modos de funcionamento.

Principais Lições Retiradas

- Precaução ilimitada
  - Foi já diversas vezes demonstrado que o software não pode ser quantitativamente certificado para o nível de integridade requerido pela maior parte dos sistemas de segurança crítica;
  - Logo, a regra óbvia será: "*never let software be a single point of failure*".

Principais Lições Retiradas

- Conclusões
  - Por razões comerciais (vantagens competitivas), meios computacionais serão cada vez mais utilizados para suportar aplicações críticas.
  - Em consequência, um investimento elevado deve ser colocado na melhoria progressiva da sua confiança no funcionamento.

Principais Lições Retiradas

- Conclusões
  - A análise da ocorrência de acidentes e a compreensão das suas causas devem ser o primeiro passo para a melhoria da confiança no funcionamento de sistemas críticos.
  - Para tal torna-se necessária a existência de uma investigação independente, capaz de gerar relatórios credíveis acerca das causas reais dos acidentes.