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

- 2. Análise da Ocorrência de Situações Perigosas ("*Hazard Analysis*")
- 3. Análise do Risco ("*Risk Analysis*")

Análise da Ocorrência de Situações Perigosas

- Tópicos a abordar:
  - Análise de Modos de Avaria e Efeitos ("*Failure Modes and Effects Analysis*" - *FMEA*)
  - Análise de Modos de Avaria, Efeitos e Criticalidade ("*Failure Modes, Effects and Criticality Analysis*" - *FMECA*)
  - Estudos de Operabilidade e de Situações Perigosas ("*Hazard and Operability Studies*" - *HAZOP*)
  - Análise por Árvore de Falhas ("*Fault Tree Analysis*" - *FTA*)
  - Análise da Ocorrência de Situações Perigosas ao longo do Ciclo de Vida de Desenvolvimento

Análise da Ocorrência de Situações Perigosas

- Avaliação Qualitativa
  - 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).

Análise de Modos de Avaria e Efeitos - FMEA

- Metodologia FMEA
  - Selecciona cada um dos componentes (ou funções) do sistema, e determina quais os seus modos de avaria;
  - Considerando individualmente cada modo de avaria, "segue" os seus efeitos para determinar as suas consequências.
    - » Pressupostos ⇨ modos de avaria de cada componente;
    - » Análise ⇨ consequências de cada avaria individual.

Universidade do Porto FEUP Faculdade de Engenharia

Análise de Modos de Avaria e Efeitos - FMEA

- Metodologia FMEA
  - Esta metodologia pode ser aplicada quer ao nível dos componentes de hardware, quer de uma forma modular (blocos funcionais).

Análise de Modos de Avaria e Efeitos - FMEA

- Vantagens / Desvantagens
  - Pontos fortes
    - » Detecção dos casos em que uma simples avaria pode resultar numa situação perigosa;
    - » Pode ser aplicada em diferentes níveis do sistema, e com diferentes níveis de detalhe;
    - » Fomenta o espírito de equipa e o conhecimento detalhado do sistema pelos membros da equipa que efectua a análise.

Análise de Modos de Avaria e Efeitos - FMEA

- Vantagens / Desvantagens
  - Pontos fracos
    - » Não consideração da avaria simultânea de múltiplos componentes;
    - » Como existem modos de avaria que não resultam em situações perigosas, a análise exaustiva desses casos é desnecessária.

Análise de Modos de Avaria e Efeitos - FMEA

- Exemplo

  [Storey, 96]

FMEA for a microswitch

Ref No.	Unit	Failure mode	Possible cause	Local effects	System effects	Remedial action
1	Tool guard switch	Open-circuit contacts	(a) faulty component (b) excessive current (c) extreme temperature	Failure to detect tool guard in place	Prevents use of machine – system fails safe	Select switch for high reliability and low probability of dangerous failure Rigid quality control on switch procurement
2		Short-circuit contacts	(a) faulty component (b) excessive current	System incorrectly senses guard to be closed	Allows machine to be used when guard is absent – dangerous failure	Modify software to detect switch failure and take appropriate action
3		Excessive switch-bounce	(a) ageing effects (b) prolonged high currents	Slight delay in sensing state of guard	Negligible	Ensure hardware design prevents excessive current through switch

Análise de Modos de Avaria, Efeitos e Criticalidade - FMECA

- Metodologia FMECA
  - Extensão da metodologia FMEA para consideração da importância das avarias de cada um dos componente do sistema;
    - » Considera as consequências de cada avaria, e a sua probabilidade ou frequência de ocorrência.
  - Introduz análise quantitativa básica;

Análise de Modos de Avaria, Efeitos e Criticalidade - FMECA

- Metodologia FMECA
  - Objectivo
    - » identificar quais os subsistemas onde as avarias têm o maior impacto.
    - » focalizar a análise da ocorrência de situações perigosas nos subsistemas onde as avarias têm o maior impacto (e assim evitar análises detalhadas de subsistemas onde as avarias têm impacto reduzido).

Estudos de Operabilidade e de Situações Perigosas - *HAZOP*

- Metodologia HAZOP
  - Desenvolvida no âmbito da industria química (ICI, 60s). Utiliza uma série de "palavras chave" para investigar os efeitos de desvios das condições normais de operação, durante cada fase de funcionamento do sistema;
    - Exemplo: "O que aconteceria se..."
  - Uma análise HAZOP é baseada numa investigação rigorosa e sistemática de cada potencial desvio identificado.

Estudos de Operabilidade e de Situações Perigosas - *HAZOP*

- Metodologia HAZOP
  - Os estudos de HAZOP são tipicamente conduzidos por equipas multidisciplinares de 6-8 engenheiros.
  - Partindo de uma especificação básica do sistema, a equipa investiga o efeito de potenciais desvios no funcionamento normal do sistema;
  - Para cada desvio, é colocada uma série de questões: "porquê? "quais as consequências"?

Estudos de Operabilidade e de Situações Perigosas - *HAZOP*

- Metodologia HAZOP
  - Para cada potencial situação perigosa identificada, é colocada uma série de questões extra: "quando"? "em que situação"? "que correcções devem ser efectuadas"?
  - O objectivo de uma análise HAZOP é o de avaliar prioridades, por forma a identificar as áreas críticas que justificam investigação suplementar.

Estudos de Operabilidade e de Situações Perigosas - *HAZOP*

- Exemplo [Storey, 96]

Guide word	*Chemical plant*	*Computer-based system*
No	No part of the intended result is achieved	No data or control signal exchanged
More	A quantitative increase in the physical quantity	A signal magnitude or a data rate is too high
Less	A quantitative decrease in the physical quantity	A signal magnitude or a data rate is too low
As well as	The intended activity occurs, but with additional results	Redundant data sent in addition to intended value
Part of	Only part of the intended activity occurs	Incomplete data transmitted
Reverse	The opposite of what was intended occurs, for example reverse flow within a pipe	Polarity of magnitude changes reversed
Other than	No part of the intended activity occurs, and something else happens instead	Data complete but incorrect

Estudos de Operabilidade e de Situações Perigosas - *HAZOP*

- Exemplo [Storey, 96]

Attribute	*Guide word*	*Possible meaning*
Data flow	More	More data is passed than expected
	Less	Less data is passed than expected
Data rate	More	The data rate is too high
	Less	The data rate is too low
Data value	More	The data value is too high
	Less	The data value is too low
Repetition time	More	The time between output updates is too high
	Less	The time between output updates is too low
Response time	More	The response time is longer than required
	Less	The response time is shorter than required

Estudos de Operabilidade e de Situações Perigosas - *HAZOP*

- Exemplo

[Storey, 96]

Item	Inter-connection	Attribute	Guide word	Cause	Consequence	Recommendation
1	Sensor supply line	Supply voltage	No	PSU, regulator or cable fault	Lack of sensor signal detected and system shuts down	
2			More	Regulator fault	Possible damage to sensor	Consider overvoltage protection
3			Less	PSU or regulator fault	Incorrect temperature reading	Include voltage monitoring
4		Sensor current	More	Sensor fault	Incorrect temperature reading, possible loading of supply	Monitor supply current
5			Less	Sensor fault	Incorrect temperature reading	As above
6	Sensor output	Voltage	No	PSU, sensor or cable fault	Lack of sensor signal detected and system shuts down	
7			More	Sensor fault	Temperature reading too high – results in decrease in plant efficiency	Consider use of duplicate sensor
8			Less	Sensor mounted incorrectly or sensor failure	Temperature reading too low – could result in overheating and possible plant failure	As above

Análise por Árvore de Falhas - FTA

- Metodologia FTA
  - Metodologia gráfica: construção de uma árvore a partir de cada Situação Perigosa identificada ("*Top Event*") e análise das suas possíveis causas;
    - » Caso exista informação anterior fidedigna sobre o funcionamento do sistema, podem ser utilizados como origem da árvore Acidentes (ou Incidentes) anteriores;
    - » Alternativamente, a informação de entrada pode ser obtida através de uma análise FMEA ou HAZOP.

Análise por Árvore de Falhas - FTA

- Vantagens
  - Particularmente eficaz para demonstrar os efeitos de variações de parâmetros ou de valores "fora da escala" sobre a segurança do sistema.
  - O facto de se analisarem unicamente cadeias de acontecimentos que garantidamente levam à ocorrência de situações perigosas, reduz o espaço de análise necessário.

Análise por Árvore de Falhas - FTA

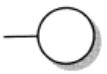
- Notação específica
  - Uma falha primária no sistema ocorre quando, em condições normais (segundo a especificação) de funcionamento, um seu componente avaria;
  - Uma falha secundária no sistema ocorre quando um seu componente avaria devido a terem sido excedidas as suas condições normais de funcionamento;
  - Uma falha de comando ocorre quando um componente reage (responde) em circunstâncias inesperadas.

Análise por Árvore de Falhas - FTA

- Notação

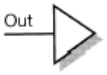
[Storey, 96]

Fault event resulting from other events



Basic event, taken as an input

Fault event not fully traced to its source. It is taken as an input but its causes may be unknown

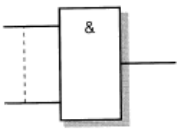


The triangle symbol is used to link trees. The 'in' symbol indicates an input from another tree (on another sheet). The 'out' symbol appears in place of the 'top event' and indicates that this point forms the input to another tree

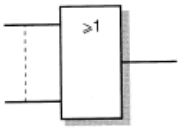
Análise por Árvore de Falhas - FTA

- Notação

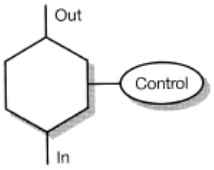
[Storey, 96]



The output event occurs if ALL the inputs occur



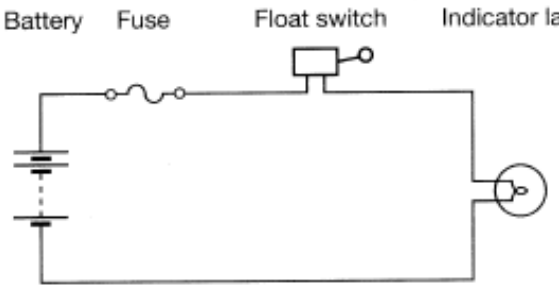
The output event occurs if ANY of the inputs occur, either alone or in combination



The control condition determines whether the input event appears at the output

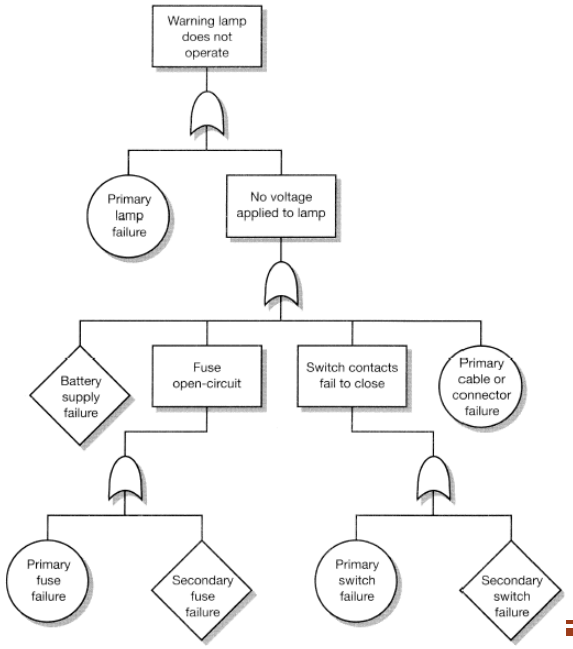
Análise por Árvore de Falhas - FTA

- Exemplo [Storey, 96]
  - » "*Top event*": lâmpada não indica "nível baixo de óleo"



Análise por Árvore de Falhc - FTA

- Exemplo [Storey, 96]



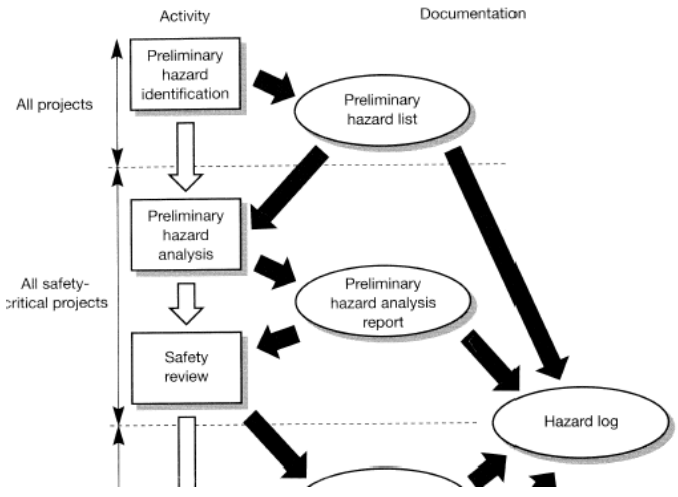
Análise da Ocorrência de Situações Perigosas ao longo do Ciclo de Vida de Desenvolvimento

- Pressuposto
  - A Análise da Ocorrência de Situações Perigosas deve ser efectuada não só durante a primeira fase do ciclo de vida (como parte da avaliação dos requisitos de segurança), mas sim ao longo de todo o ciclo de vida de desenvolvimento;
  - Porquê?
    - » Porque esta análise deve ser efectuada não só considerando as características do sistema global, mas também os detalhes de concepção / implementação.

Análise da Ocorrência de Situações Perigosas ao longo do Ciclo de Vida de Desenvolvimento

- Exemplo

[Storey, 96]



Análise da Ocorrência de Situações Perigosas ao longo do Ciclo de Vida de Desenvolvimento

- Identificação Preliminar de potenciais Situações Perigosas (PHI)
  - Identificação preliminar de "*hazards*" potenciais;
  - Criação da "*Preliminary Hazard List* - PHL";
  - A PHL será um documento de entrada para as fases subsequentes do ciclo de vida.
    - » A existência desta lista prova que foi efectuada a identificação preliminar de "*hazards*";

Análise da Ocorrência de Situações Perigosas ao longo do Ciclo de Vida de Desenvolvimento

- Análise Preliminar de Situações Perigosas (PHA)
  - Análise preliminar para avaliação da criticalidade dos diversos subsistemas;
  - Criação do "*Hazard Log*", para registo de questões relevantes para a segurança do sistema;
  - Primeira tentativa de classificação dos requisitos de integridade de segurança, para cada função relevante do sistema;

Análise da Ocorrência de Situações Perigosas ao longo do Ciclo de Vida de Desenvolvimento

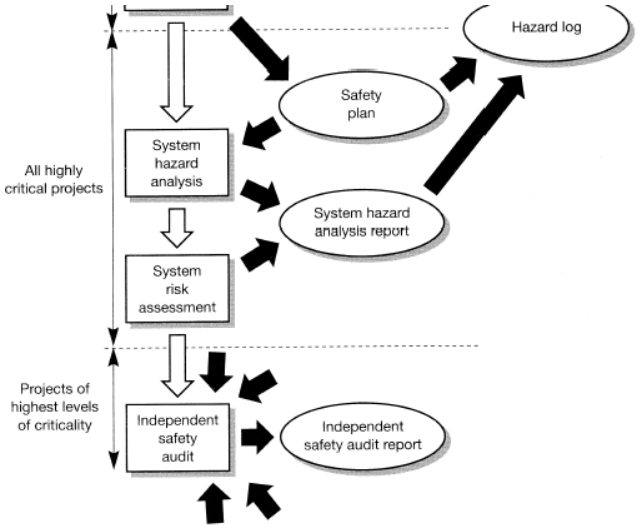
- Análise Preliminar de Situações Perigosas (PHA)
  - Criação do "Preliminary Hazard Report", com:
    - » Descrição breve do sistema e do seu ambiente;
    - » Descrição breve das funções do sistema e das suas implicações em termos de segurança;
    - » Os Objectivos de Segurança do sistema;
    - » Justificação do Risco e dos SIL atribuídos;
    - » Definição das taxas de avaria e dos níveis de Segurança;
    - » Referência a todas as fontes de documentação utilizadas.

Análise da Ocorrência de Situações Perigosas ao longo do Ciclo de Vida de Desenvolvimento

- Revisão da Segurança ("*Safety Review*")
  - Efectuada ao longo de todo o ciclo de vida de desenvolvimento;
  - Após a PHA, a Revisão da Segurança pretende validar os Níveis de Integridade da Segurança (SILs) atribuídos.

Análise da Ocorrência de Situações Perigosas ao longo do Ciclo de Vida de Desenvolvimento

- Exemplo
  [Storey, 96]



Análise da Ocorrência de Situações Perigosas ao longo do Ciclo de Vida de Desenvolvimento

- Plano da Segurança ("*Safety Plan*")
  - Planeamento da segurança;
  - Planeamento das acções de controlo;
  - Atribuição de responsabilidades ao pessoal envolvido.

Sistemas Computacionais de Segurança Crítica

- 2. Análise da Ocorrência de Situações Perigosas ("*Hazard Analysis*")
- 3. Análise do Risco ("*Risk Analysis*")

Análise do Risco ("*Risk Analysis*")

- Tópicos a abordar:
  - Considerações sobre o Risco
  - Considerações sobre a classificação do Risco
  - Considerações sobre a tolerabilidade do Risco
  - Níveis de Integridade da Segurança

Considerações sobre o Risco

- Definições
  - Um Acidente é um evento ou uma sequência de eventos que tem como consequência a morte ou o ferimento de pessoas, ou 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.

Considerações sobre o Risco

- Avaliação Quantitativa
  - A relevância de uma determinada Situação Perigosa está relacionada com os Acidentes que daí podem resultar.
  - Dois factores devem ser considerados:
    - » as potenciais consequências de um acidente resultante;
    - » a frequência (ou probabilidade) de ocorrência do referido acidente.

Considerações sobre o Risco

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

Sobre a Classificação do Risco

- Avaliação Quantitativa
  - O resultado do processo de análise do Risco é a sua classificação numa de várias classes, em função da criticalidade e da probabilidade de ocorrência de cada situação perigosa específica

Sobre a Classificação do Risco [IEC 61508]

Risk classification of accidents

Frequency	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

- Classe I - Risco intolerável
- Classes II e III - Risco ALARP
- Classe IV - Risco tolerável

Sobre a Classificação do Risco [IEC 61508]

Interpretation of risk classes

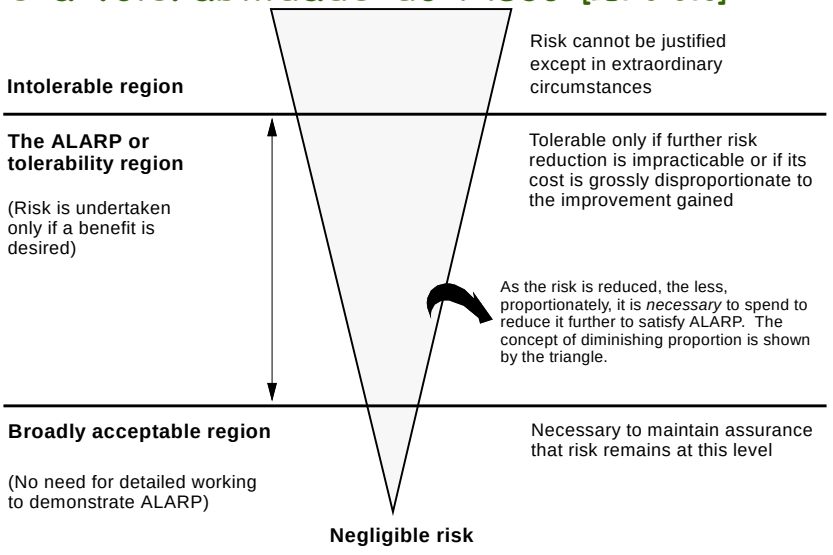
Risk class	Interpretation
Class I	Intolerable risk
Class II	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
Class III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
Class IV	Negligible risk

- Classe I - Risco intolerável
- Classes II e III - Risco ALARP
- Classe IV - Risco tolerável

Sobre a tolerabilidade do Risco [IEC 61508]

- Risco inaceitável, que nunca poderá ser justificável excepto em circunstâncias excepcionais;
- Risco aceitável, quando pode ser negligenciado.
- Risco tolerável - ALARP ("*As Low As Reasonably Practicable*"), quando o custo da sua redução ultrapassa largamente o benefício decorrente dessa redução;
  - Um Risco na gama ALARP, caso seja de fácil redução nunca poderá ser considerado tolerável.
  - Em sistemas de Integridade Elevada, cabe à entidade de certificação determinar se um determinado Risco terá ou não que ser reduzido.

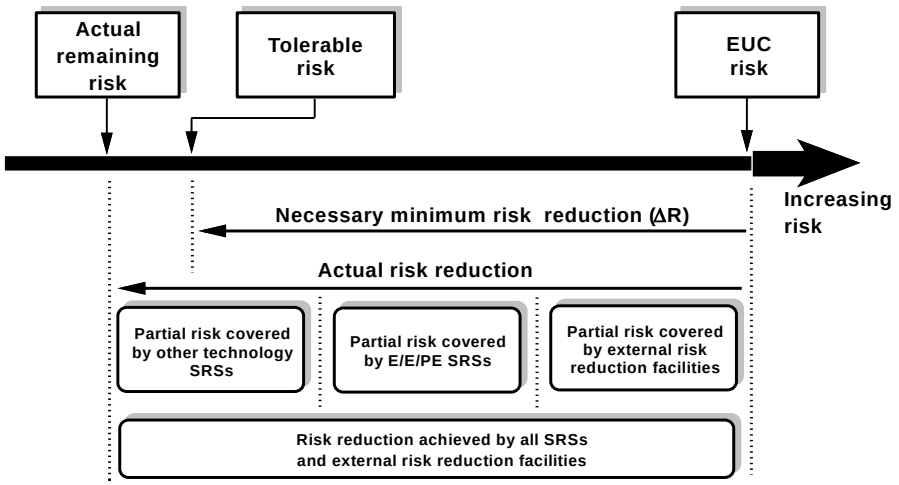
Sobre a tolerabilidade do Risco [IEC 61508]



Sobre a tolerabilidade do Risco [IEC 61508]

- Gestão do Risco
  - A gestão do processo de desenvolvimento de um Sistema de Segurança Crítica pode ser vista como a gestão de um processo de Redução de Risco.
  - Terminologia
    - » EUC - "*Equipment Under Control*"
    - » SRS - "*Safety Related System*"
    - » ΔR - "Risk Reduction"

Sobre a tolerabilidade do Risco [IEC 61508]



Níveis de Integridade da Segurança

- Níveis de Integridade da Segurança
  - Relacionados com o nível de Redução de Risco exigível:
    - » Caso seja necessária uma elevada Redução do Risco (potencial de Risco elevado), os mecanismos de redução do risco devem ser de elevado nível de confiança.
    - » Caso a necessidade de Redução de Risco seja baixa, esses mecanismos poderão ser mais simples.

Níveis de Integridade da Segurança

- Níveis de Integridade da Segurança
  - Diferentes tipos de requisitos de Segurança, levaram à definição de Níveis de Integridade da Segurança (SIL).
- Definição
  - *"Safety Integrity is the probability of a safety-related system satisfactorily performing the required safety functions, under all the stated conditions, within a stated period of time."* [IEC 61508]

Níveis de Integridade da Segurança

- Níveis de Integridade da Segurança
  - Apesar de ser possível exprimir quantitativamente a Integridade da Segurança, é prática habitual atribuír a cada sistema relacionado com a Segurança um Nível de Integridade da Segurança (de entre 4 níveis).
  - Estes vários níveis têm associados requisitos numéricos, tais como as gamas de "avarias por ano", ou "probabilidade de avaria durante um acidente".

Níveis de Integridade da Segurança

- Exemplo [IEC 61508]

Safety integrity level	**Low demand mode of operation** (Average probability of failure to performs its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

  - Para sistemas a operarem em "*demand mode operation*", a medida da integridade da Segurança relevante é a probabilidade de não conformidade com a especificação (avaria) da função, quando esta é pedida (ex: relevante para "*shut-down systems*").

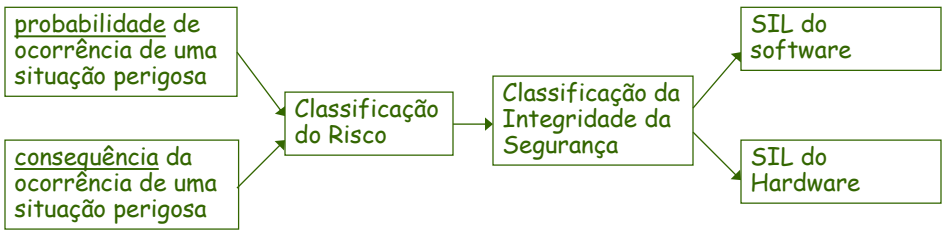
Níveis de Integridade da Segurança

- Exemplo [IEC 61508]

Safety integrity level	High demand/continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

  - Para sistemas a operarem em "*continuous / high demand mode operation*", a medida da integridade da Segurança relevante é a probabilidade de avaria por hora (1 ano = 8760 horas).

Níveis de Integridade da Segurança



» Um Nível da Integridade da Segurança (SIL) é atríbuido ao software para definir a importância da exactidão dos módulos de software.

» O nível seleccionado determina os métodos de desenvolv. e de teste a utilizar ao longo do ciclo de vida.

Níveis de Integridade da Segurança

- A atribuição dos SIL a um sistema está relacionada com o nível de Risco do sistema.
  - Não esquecer que:
    - » Risco é a medida combinada da probabilidade de ocorrência de uma situação perigosa e das suas consequências;
    - » Integridade da Segurança é a medida da probabilidade de um sistema de Segurança desempenhar correctamente as suas tarefas, para as condições e durante um período de tempo especificados.

Níveis de Integridade da Segurança

- Atribuição dos SIL
  - Os vários standards de Segurança definem gamas de taxas de avaria alvo para cada Nível de Integridade da Segurança.
  - A atribuição dos SIL é efectuada em função dessas taxas de avaria alvo (definidas para cada nível), e das taxas de avaria máxima toleráveis resultantes da Análise do Risco.

Níveis de Integridade da Segurança

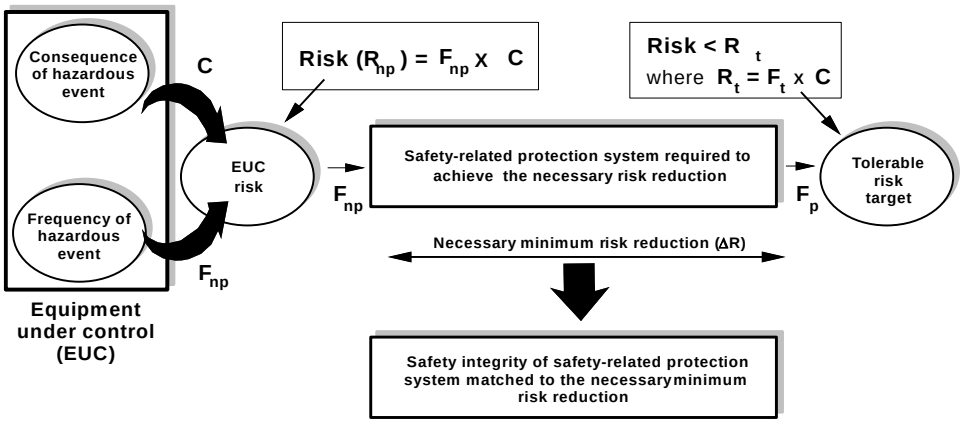
- Determinação Quantitativa dos SIL [IEC 61508]
  - 1. Determinar o Risco Tolerável (em termos numéricos)
    - Ex.: uma determinada consequência especificada não deve ocorrer com uma frequência superior a uma vez em 10^4 anos (F_t)
  - 2. Determinar o Risco do equipamento sob Controlo (EUC)
    - Determinar a frequência (F_{np}) associada ao Risco do EUC através da análise de taxas de avaria para situações similares, ou através de métodos de previsão adequados.
    - Determinar a consequência da ocorrência da situação perigosa em análise (C)

Níveis de Integridade da Segurança

- Determinação dos SIL [IEC 61508]
  - 3. Verificar se é necessária efectuar uma Redução de Risco (ΔR) suplementar.
  - 4. Caso seja necessário efectuar essa redução, determinar a probabilidade máxima de avaria "*low demand*" requerida para o sistema de protecção: $PFD_{avg}=(F_t/F_{np})=\Delta R$
    - Considerando que a consequência da ocorrência da situação perigosa (C) em análise se mantém constante
  - 5. O SIL pode ser obtido através da tabela adequada.

Níveis de Integridade da Segurança

- Determinação dos SIL [IEC 61508]



Níveis de Integridade da Segurança

- Atribuição do SIL
  - Após ter sido atribuído o SIL a um sistema, a sua concepção e o seu método de desenvolvimento devem garantir que o SIL definido é realizado.
  - Os standards relacionados com a Segurança garantem, para cada SIL, um conjunto de procedimentos que responde à questão anterior.