

Segurança funcional

Integridade de segurança

Taisy Weber

?



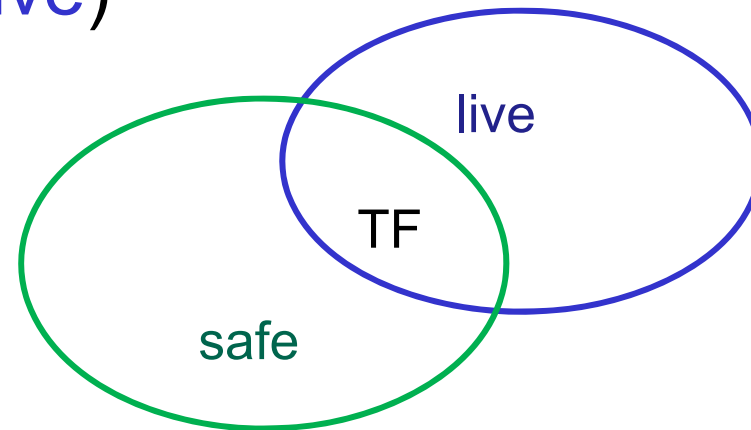
safety

não relacionado a **security**

- garantia de que uma “coisa ruim” jamais vai acontecer
 - por exemplo: elevador despencar
- não garante que um **coisa boa** possa acontecer (vivacidade – liveness)
 - por exemplo: elevador se movimentar

safety

- sistema tolerante a falhas deve ser seguro (**safe**) e vivaz (**live**)



- termo “safety”
 - enfatizado também em outras áreas da computação (eng. software, especificação formal)
 - muito usado na área de controle de processos

safety versus dependabilidade

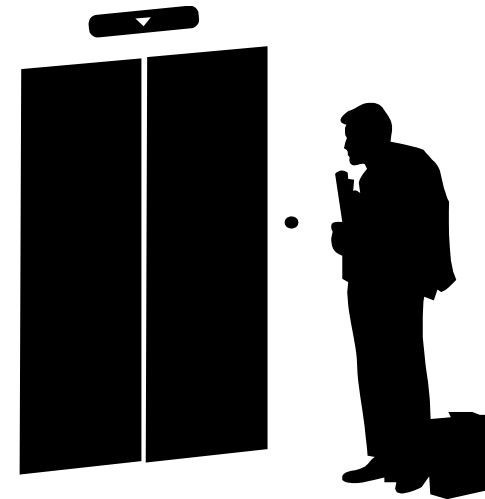
- safety é um **atributo** de dependabilidade
 - aparece frequentemente com a medida da capacidade *fail-safe* do sistema
 - relacionado a *detecção de falhas*

um sistema seguro não apresenta defeito:
ou está fornecendo as saídas corretas ou está
em um estado seguro

a medida numérica (probabilidade)
indica o quão próximo o sistema está
do ideal

fail-safe versus fail-operate

- muitos sistemas reais são *fail-safe*
 - ou seja, possuem um estado **não operacional** seguro e fácil de alcançar em caso de falha interna
- exemplos
 - elevador
 - sinais de trânsito
 - máquina de corte
 - escadas rolantes



fail-safe versus fail-operate

- **mas** muitos outros sistemas reais não podem parar em caso de falha
 - aviões no ar
 - processos contínuos que não podem ser subitamente interrompidos
- são chamados *fail-operate*
 - ou seja, tolerantes a falhas



sistemas críticos

- sistemas críticos exigem segurança
 - são denominados *safety-critical*
- money-critical
 - prejuízos a propriedade
 - ou a economia
- life-critical
 - prejuízos a vida humana
 - ou ao ambiente do qual dependemos

exemplo: acidentes ambientais

problemas podem ser graves quando computadores sujeitos a apresentar defeitos são usados no controle desses sistemas

exemplos de sistemas críticos

- controle do espaço aéreo
- controle de usinas nucleares
- controle de segurança em plataformas de petróleo

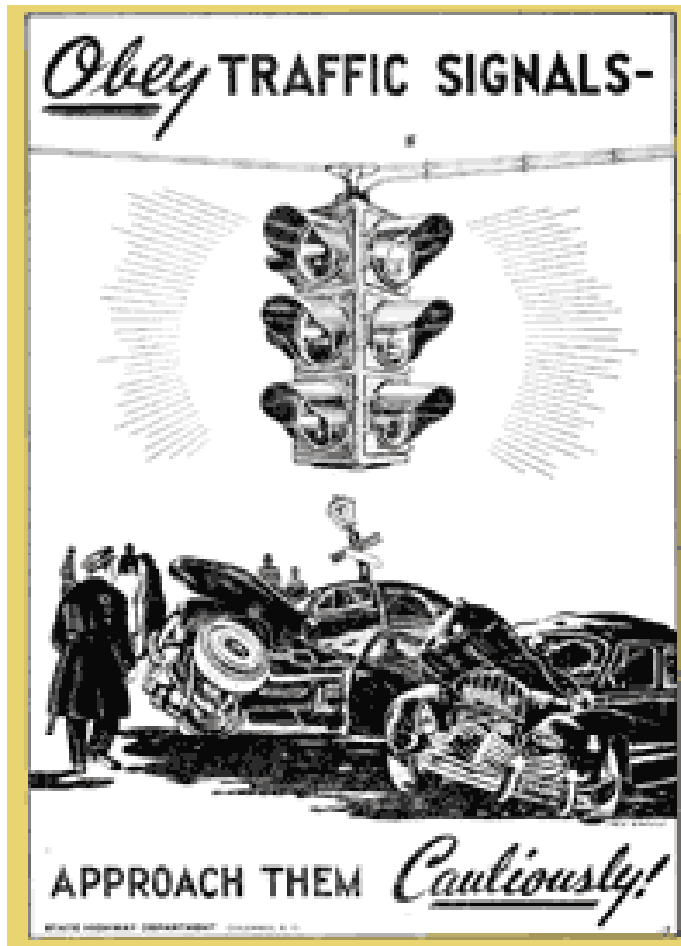


exemplos de sistemas críticos

- controle de vazamento de gases tóxicos
- controle de processos químicos
- sistemas de suporte de vida em hospitais



exemplos de sistemas críticos



- controle de transporte terrestre (trens, metrô subterrâneo e de superfície)
- sistemas embarcados (ex: automóveis)
- controle de robôs

fracassos

- causas de projetos mal sucedidos
 - conhecimento incompleto do que torna um sistema seguro
 - desconhecimento do sistema geral onde o controlador ou computador vai atuar
 - ignorância dos pontos de defeito críticos (*single-points-of-failure*) do sistema
- impossível sistema perfeito
 - falhas são inevitáveis
 - mas os riscos podem ser reduzidos consideravelmente

hazards e riscos

- *hazards* ameaça, perigo
 - fonte potencial de perigo
 - análise de hazards e estimativa dos riscos
- riscos
 - danos ao negócio, a pessoas, à propriedade
 - riscos:
 - inaceitáveis
 - aceitáveis (ou toleráveis)

hazards e riscos

Exemplos de riscos:

acidentes em estradas	100	cpm
dirigir um carro	150	cpm
queda de aviões	0.02	cpm
mordida de inseto ou cobra	0.1	cpm
fumar 20 cigarros por dia	5000	cpm

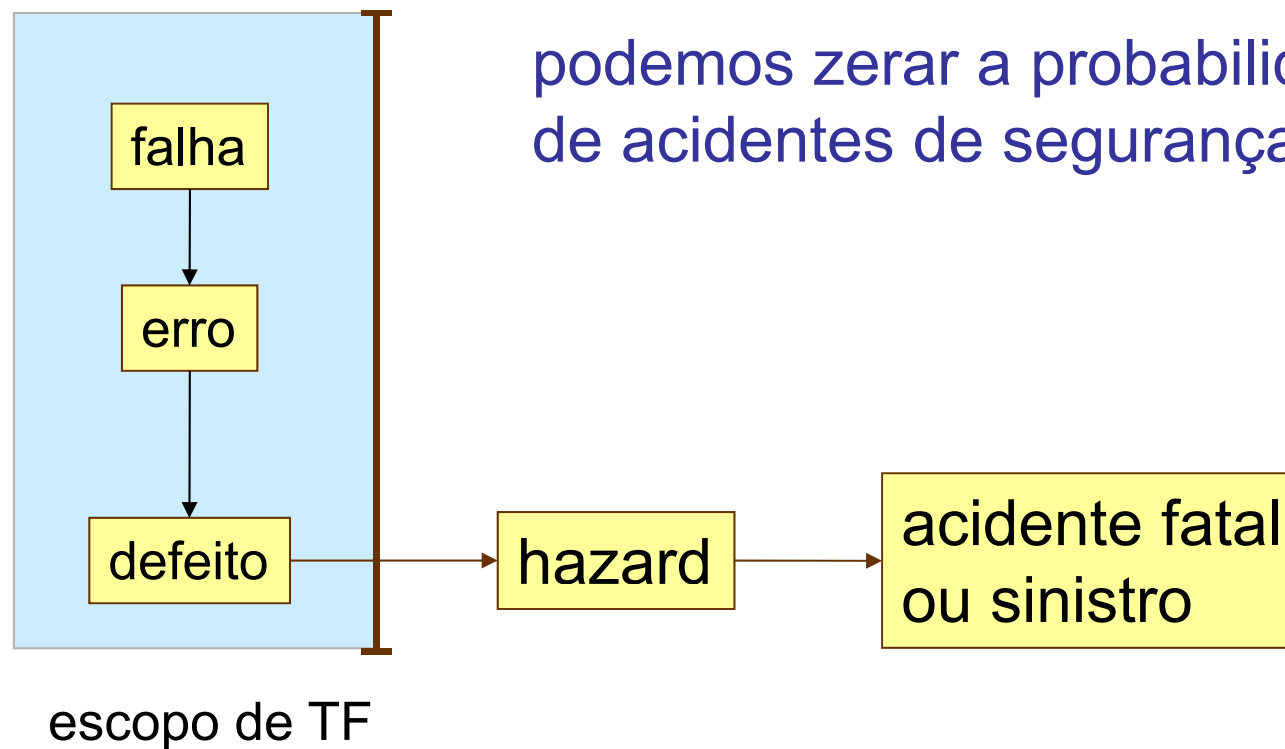
cpm - chances por
milhão por ano

hazards

- ameaça, perigo (*hazard*)
- definida como alguma condição real ou potencial que pode causar
 - ferimento, doença, ou morte de pessoas;
 - danos a (ou perda de) um sistema, um equipamento ou uma propriedade;
 - danos ao ambiente



hazards x falhas



elementos associados ao risco

estimativa de risco

- risco de que?
 - consequência ou severidade
- quanto provável é o risco?
 - frequência ou probabilidade de ocorrência por unidade de tempo
 - probabilidade de ser morto por raio é 10^{-7} por ano;
 - probabilidade de um avião cair durante aterrissagem devido a defeito nos instrumentos é $< 10^{-7}$ por aterrissagem.

riscos baixos são frequentemente ignorados;
riscos a longo prazo são frequentemente ignorados

elementos associados ao risco

- exemplo:
 - defeito de uma válvula química pode resultar em uma explosão que pode matar 10 pessoas,
 - se esse componente falhar **uma vez a cada 10.000 anos**, qual o **risco** associado a esse componente?
- solução:
 - **taxa de defeito** da válvula é 0,0001 defeitos por ano.
 - então, o risco de uma fatalidade é $10 \times 0,0001 = 0.001$ mortes por ano.

pergunta: é aceitável ou não?
a resposta não é técnica

risco

- risco aceitável
 - deve fazer parte da especificação do sistema
 - variação de 10^{-2} a 10^{-10} incidentes por hora
 - geralmente definido por leis ou órgãos reguladores no interesse da população
- normas
 - **várias** normas estabelecem padrões de segurança para diferentes setores
 - médico-cirúrgico
 - nuclear
 - transportes, ...



<http://www.iec.ch/>

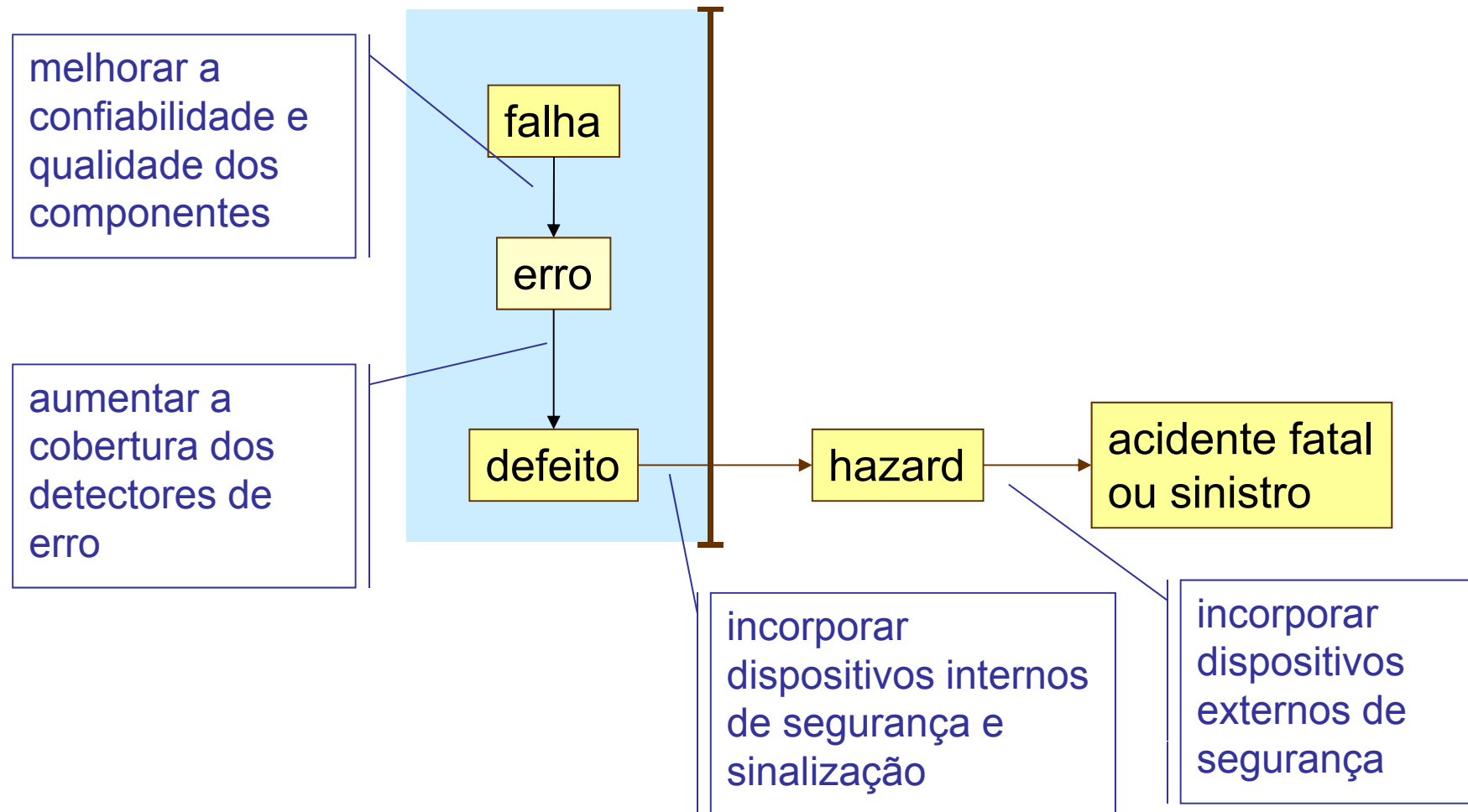
normas de segurança

- exemplos:
 - IEC 61508 (industrial)
 - Mil-Std-882D (militar)
- normas relacionadas
 - IEC 61511 (process industry)
 - IEC 62061 (machinery control systems),
 - IEC 61513 (nuclear power plants),
 - IEC 60601 (medical equipment),
 - ISO/CD 26262 (automotive systems)



<http://www.iec.ch/>

redução de risco



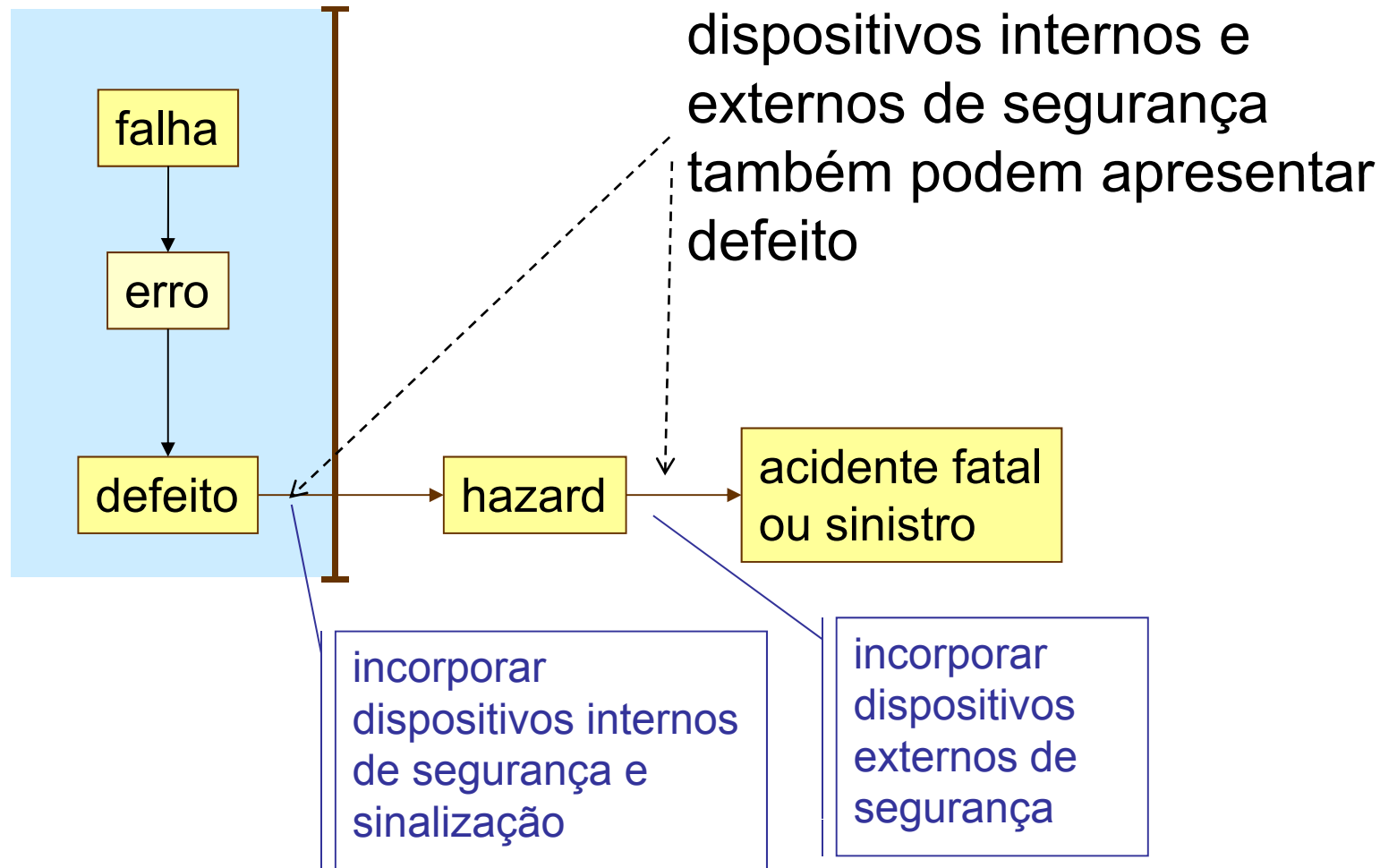
confiabilidade e safety



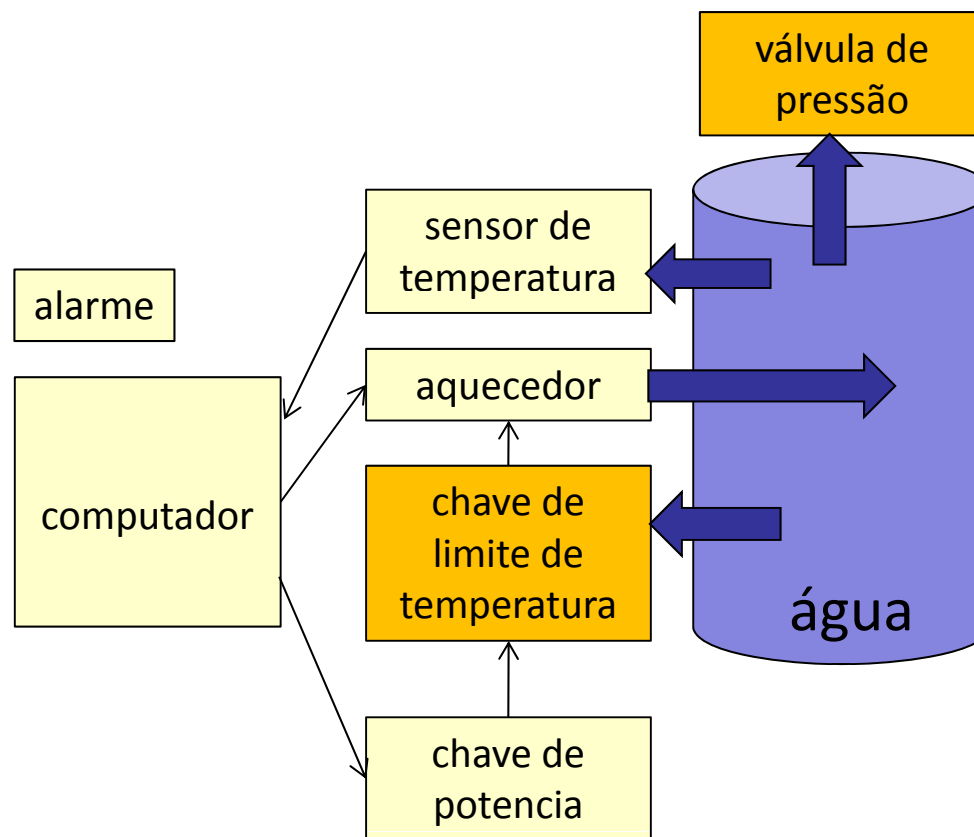
componente altamente
confiável
implementando função
de segurança

"Larry here is one of our most reliable men.
He's in charge of safety!"

dispositivos de segurança



exemplo



hazards:
sobreaquecimento da água
e explosão do tanque

defeitos:
devidos a falhas no sensor,
no aquecedor, no
computador, no software,
no operador

dispositivos de segurança

- devem ser construídos com componentes confiáveis
 - baixa taxa de defeito
- devem possuir baixa probabilidade de falha
 - se forem dispositivos eletrônicos programáveis, devem ser **tolerantes a falhas**
 - um defeito em um dispositivo de segurança não deve provocar dano ao ambiente ou usuários
- devem também ser seguros
 - provar sua **integridade de segurança**

norma de segurança?



- norma para segurança funcional

- independente do domínio da aplicação
- equipamentos elétricos, eletrônicos e eletrônicos programáveis

E/E/PE *electrical/electronic/ programmable electronic*

- **sugere** ou **impõe** técnicas, estratégias e métodos para o projeto de sistemas seguros
- usada em aplicações críticas (principalmente sistemas de segurança, mas pode ser usada em sistemas de controle)
- permite **certificação** por organizações internacionais

safety e segurança funcional

- safety (no contexto da norma IEC)
 - sistemas livres de riscos inaceitáveis envolvendo prejuízos físicos ou danos à saúde de pessoas resultantes direta ou indiretamente de danos a propriedades ou ao ambiente

obs: ênfase nos riscos inaceitáveis

- *segurança funcional (functional safety)*
 - é parte da segurança global de um sistema
 - depende do sistema ou equipamento operar corretamente em resposta a suas entradas

essa definição não implica em estado seguro

segurança funcional x fail safe

- a norma considera o conceito de *fail-safe* inadequado para sistemas computacionais complexos
 - *fail-safe* só indicado para sistemas de baixa complexidade com modo de defeito bem definido
 - a norma visa um escopo maior de sistemas (fail-operate)
 - *fail-operate* = tolerante a falhas

na prática os estados seguros precisam ser identificados e defeitos seguros separados de perigosos

IEC 61508: objetivos

- permitir usar a tecnologia para aumentar segurança sem prejudicar desenvolvimento futuro,
 - aproveitamento do potencial da tecnologia E/E/PE para melhorar a segurança e aspectos econômicos
 - desenvolvimento tecnológico considerando segurança global
- estabelecer **padrão genérico**,
- prover meios para **usuários e reguladores** terem confiança em controladores computacionais
- abordagem flexível e baseada em **risco presumido**

IEC 61508: abordagem

- dois conceitos fundamentais
 - ciclo de vida de segurança (SLC)
 - análise probabilística de falhas para quantificar nível de integridade de segurança (SIL)
- ciclo de vida
 - reduzir ou eliminar defeitos devido a erros sistemáticos
- cálculo de SIL
 - determinação de probabilidade de defeitos randômicos

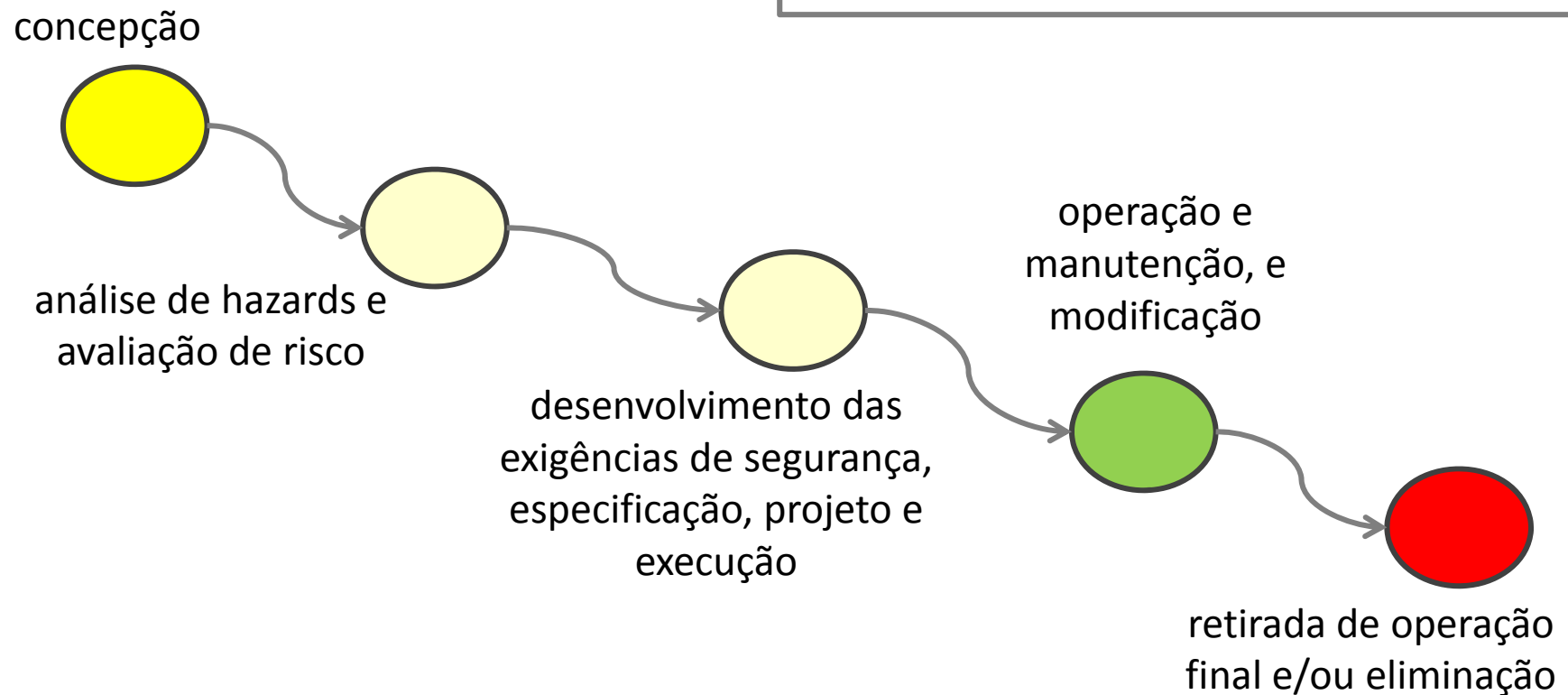
IEC 61508: ciclo de vida

- modelagem do ciclo de vida
 - a norma cobre todas as atividades do ciclo de vida de safety:
 - concepção,
 - análise de hazard e avaliação de risco,
 - desenvolvimento das exigências de segurança, especificação, projeto e execução, operação e manutenção, e também modificação,
 - retirada de operação final e/ou eliminação.
- compreende aspectos do sistema e de mecanismos de tratamento de falhas

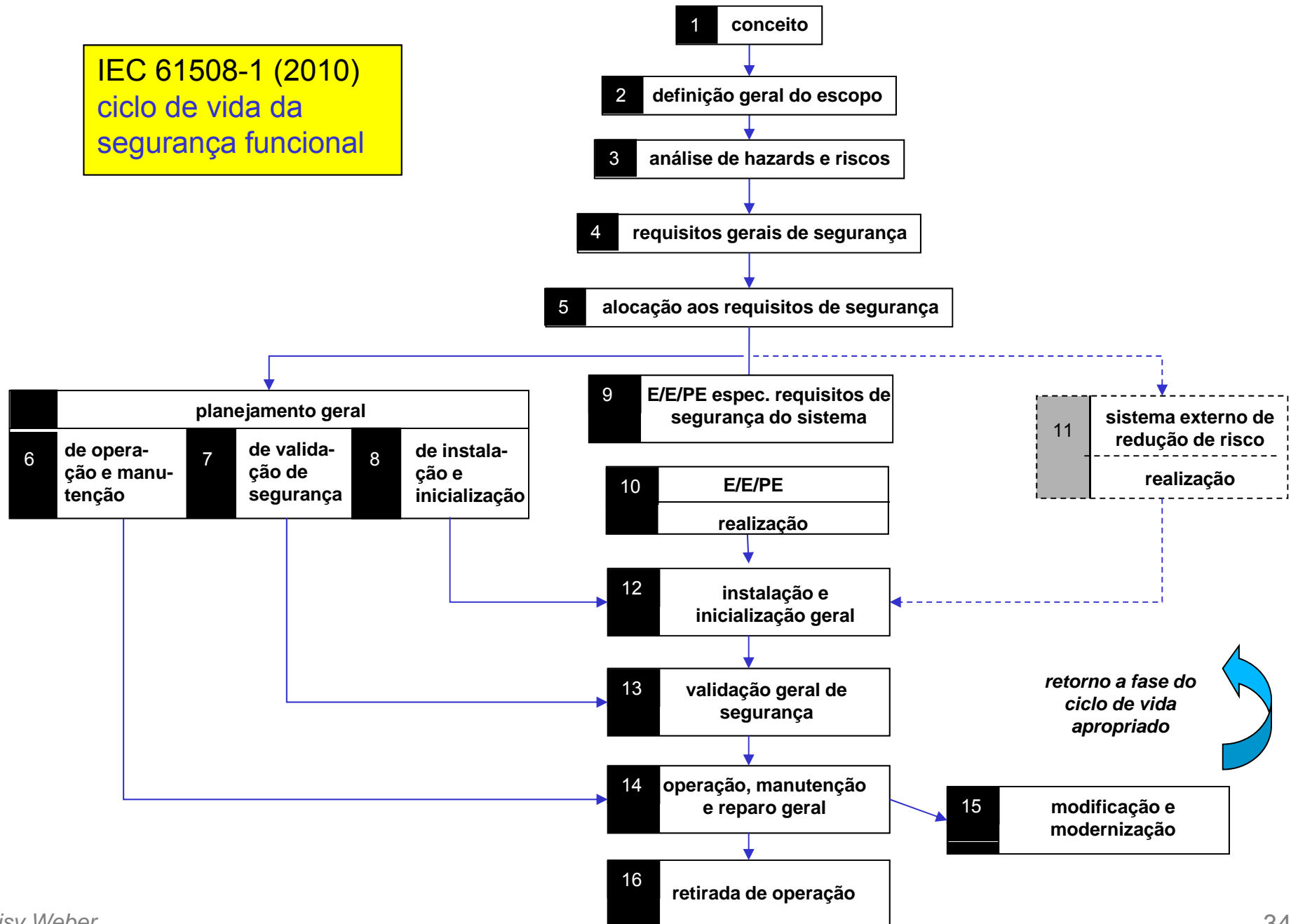
IEC 61508: características

- modelagem do ciclo de vida de safety

compreende aspectos do sistema e de mecanismos de [tratamento de falhas](#)



IEC 61508-1 (2010)
ciclo de vida da
segurança funcional

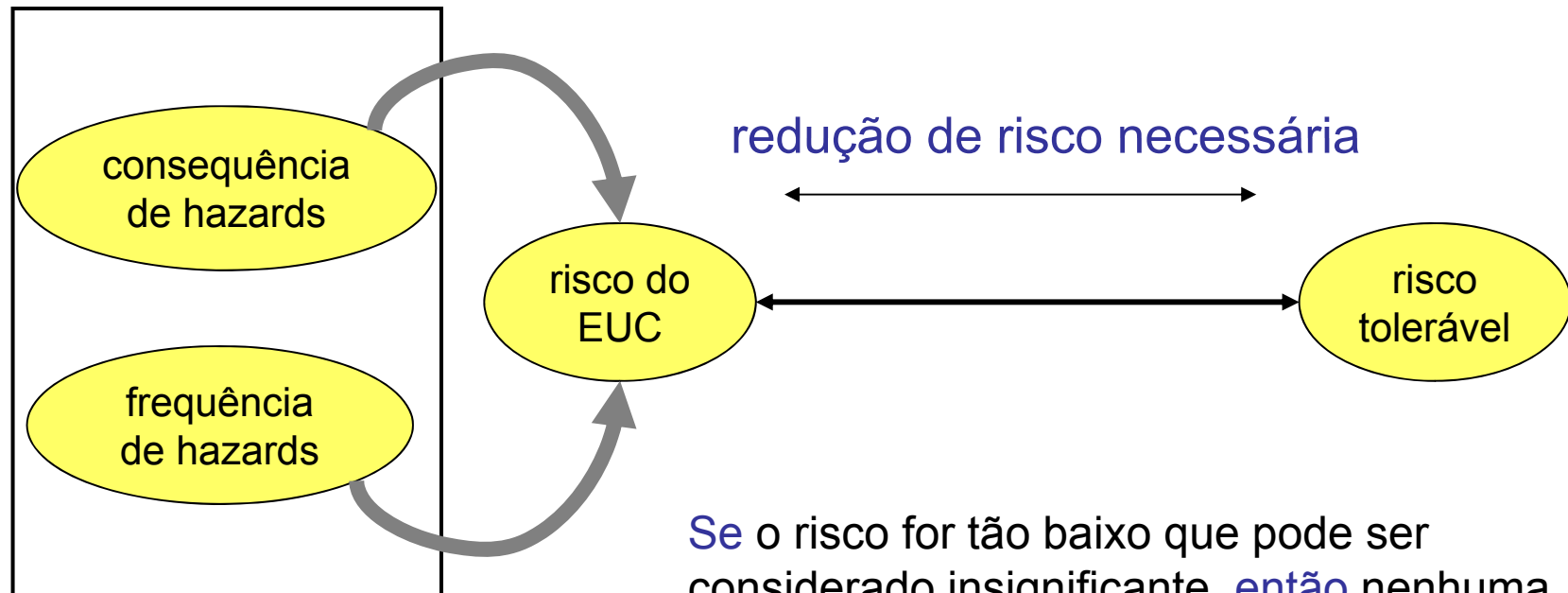


IEC 61508: características

- prevenção e controle de defeitos
 - exigências para impedir defeitos
 - evitar a introdução de falhas - prevenção
 - exigências para controlar defeitos
 - garantir segurança mesmo quando falhas estão presentes
- técnicas e medidas
 - a norma especifica as técnicas e as medidas que são necessárias para conseguir a integridade de segurança requerida

tolerância a falhas

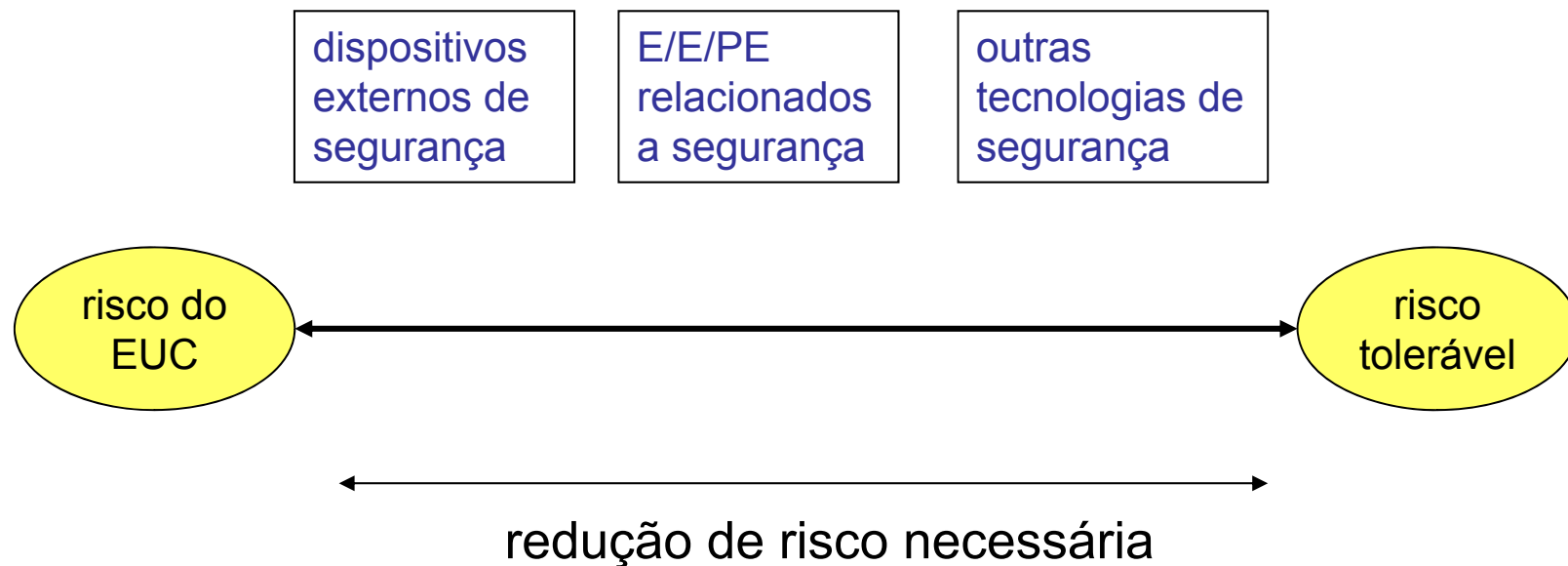
IEC 61508 – redução de risco



EUC (equipamento sob controle) e controle do EUC

Se o risco for tão baixo que pode ser considerado insignificante, **então** nenhuma ação adicional é requerida
Se não for o caso, **então** características de segurança devem ser incorporadas no projeto para reduzir o risco a um nível tolerável para a aplicação.

IEC 61508 – redução de risco



sistemas relacionados a segurança

na literatura técnica: **SIS** – sistemas instrumentados de segurança

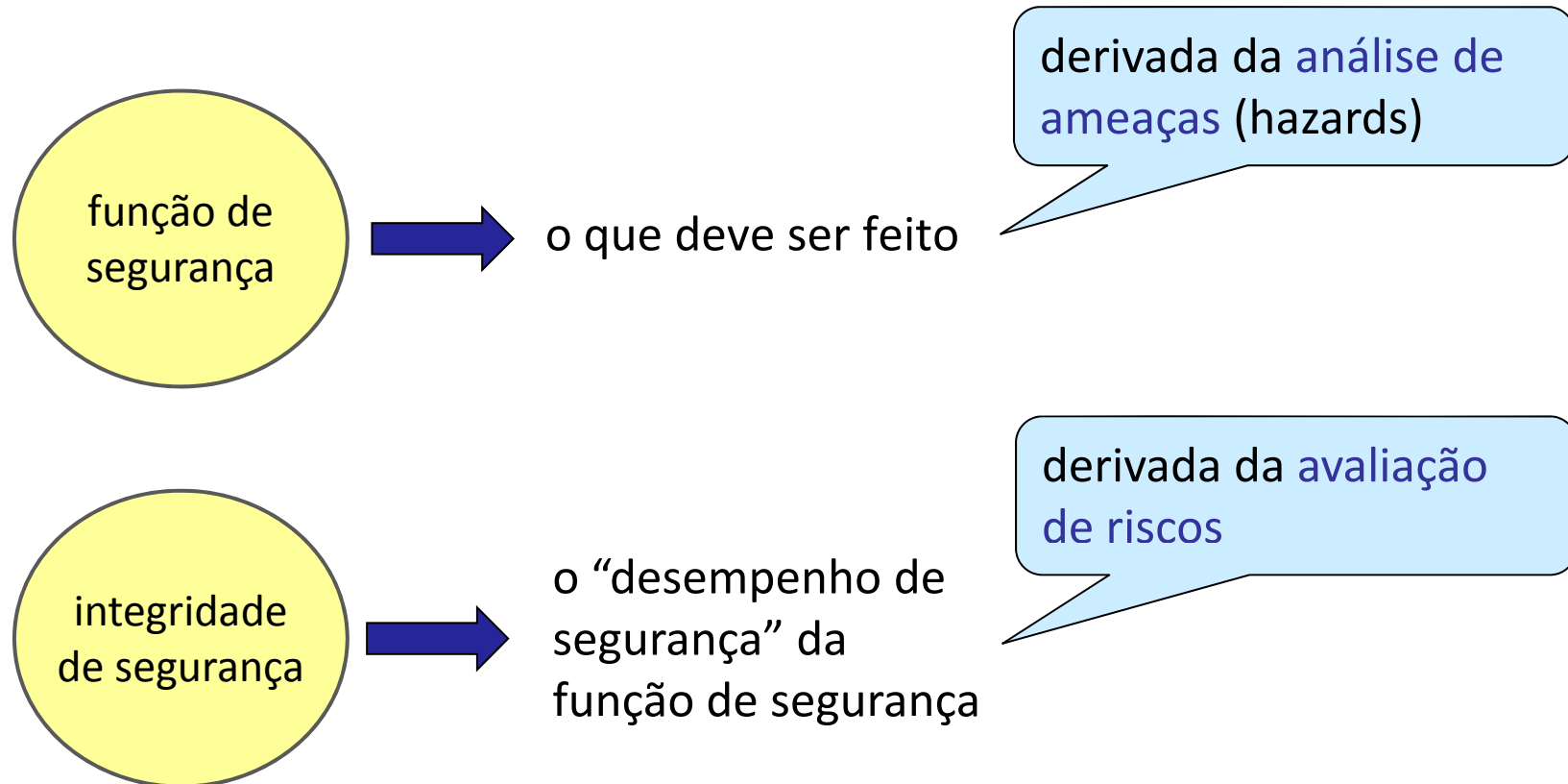
- aplicados para garantir que os riscos serão mantidos em um nível aceitável
- executam funções de segurança
- qualquer sistema que realiza funções de segurança é um SIS
 - pode estar integrado a equipamentos ou sistemas de controle (**interno**)
 - pode estar separado deles
 - dispositivo **externo** de segurança

funções de segurança

- requisitos para as funções de segurança
 - o que a função de segurança efetivamente deve realizar
 - derivados da **análise de ameaças** (hazards)
- integridade de segurança
 - relacionado a **probabilidade** que a função de segurança seja executada satisfatoriamente (sob condições definidas e durante um dados período de tempo)
 - requisitos derivados da **estimativa de riscos**

o conceito de **integridade** aparece também na literatura como a capacidade de detecção de falhas de um sistema

funções de segurança vs integridade



Exemplo

- função de segurança
 - para prevenir a ruptura de um reservatório X sob pressão, a válvula Y deve abrir em 2 segundos quando a pressão no reservatório alcançar 2.6 bar
- integridade de segurança
 - a integridade de segurança da função de segurança deve ser SIL 2

Bell, R.: *Introduction to IEC 61508*. In Proc. of the 10th Australian Workshop on Safety Critical Systems and Software, 3-12. (2006)

funções de segurança

- funções de segurança executadas por sistemas eletrônicos programáveis

CLPs e computadores

- alta complexidade
 - falhas e erros que levam a defeitos
 - impossível determinar com precisão o modo de defeito
 - impossível teste exaustivo
- desafio:
 - projetar sistemas que previnem defeitos ou controlam falhas (ou erros) quando eles aparecem

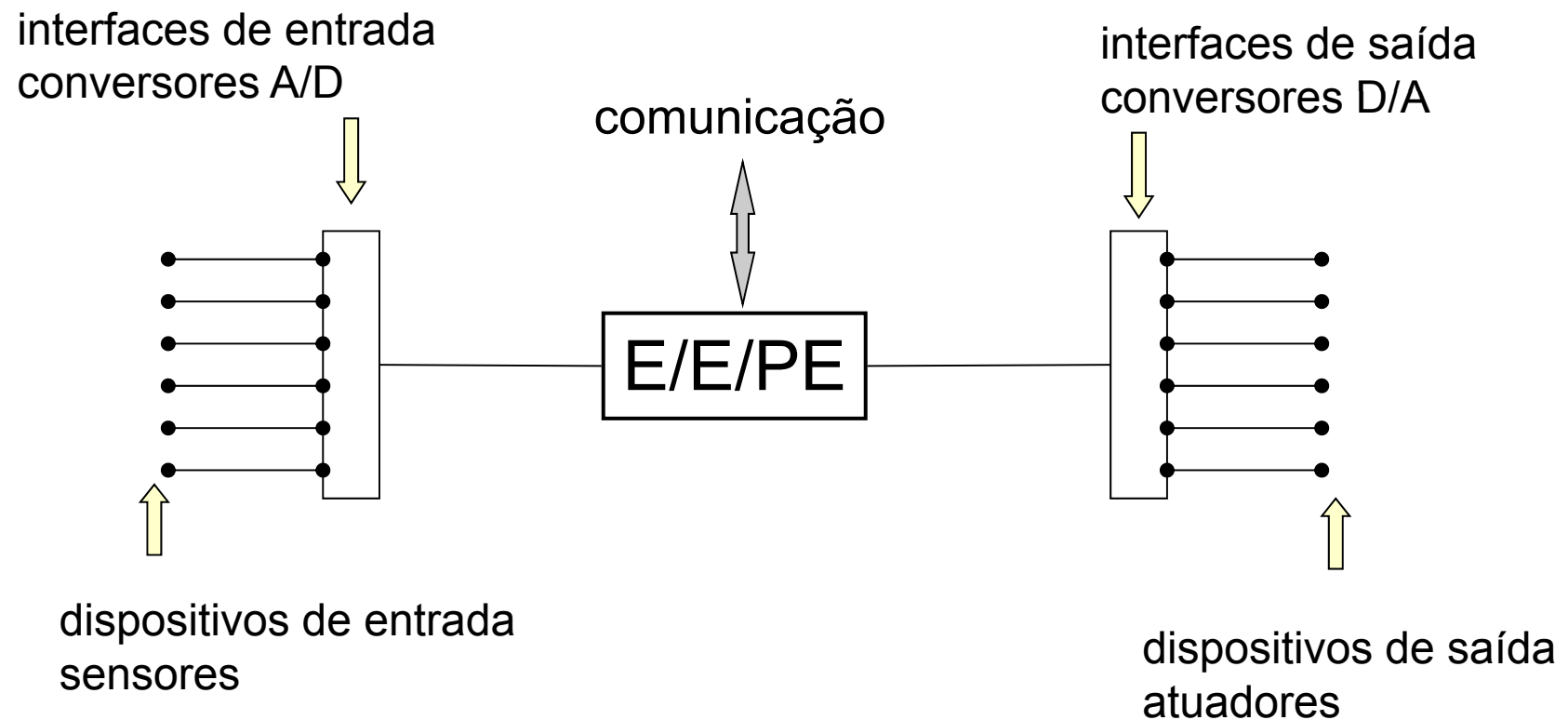
aqui entra-se na área de dependabilidade

exemplos de sistemas E/E/PE relacionados a segurança

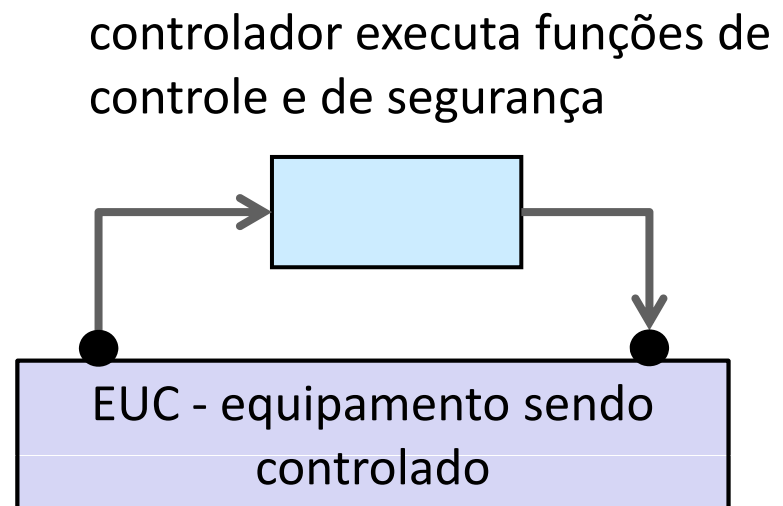
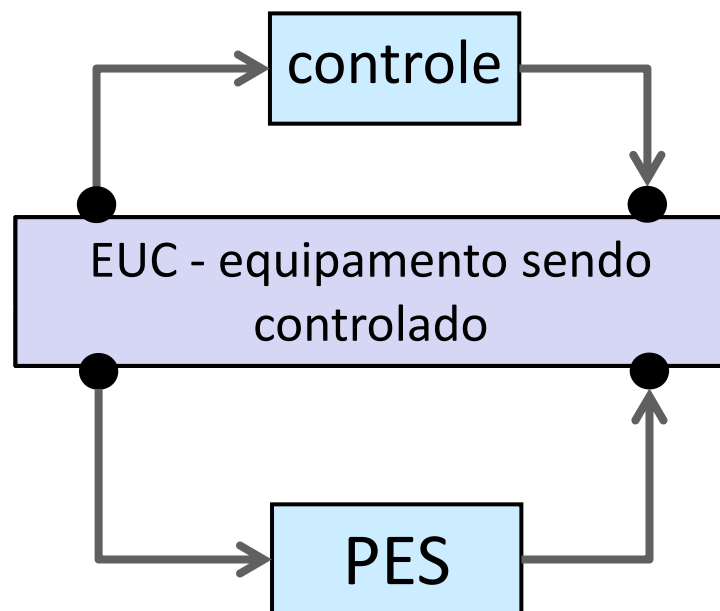
- sistemas de emergência (shut-down) em uma planta de processamento químico;
- indicador de segurança de carga em guindastes;
- sistema de sinalização em ferrovias;
- sistema de proteção e parada de emergência em máquinas e equipamentos ;
- sistemas de controle de exposição a doses de radiação (radioterapia médica);
- luzes de indicação de um automóvel, freio anti-bloqueante e sistemas de gerência de motor;
- monitoração remota, operação ou programação de uma planta através da rede.

PES

programmable electronic system (PES)



arquiteturas de sistemas de segurança



causa de defeitos

- especificação incorreta
 - do sistema, do hardware ou do software;
 - omissões na especificação dos requisitos de *safety*;
- defeitos de hardware **randômicos**;
- defeitos de hardware **sistemáticos**
- erros de software (qualquer tipo de bug);
- causas comuns de defeitos;
- erros humanos;
- influências do ambiente:
 - eletromagnéticas, temperatura, mecânicas, atmosféricas
- distúrbios na fonte de alimentação:
 - falta de energia, tensões reduzidas, reconexão de fonte.

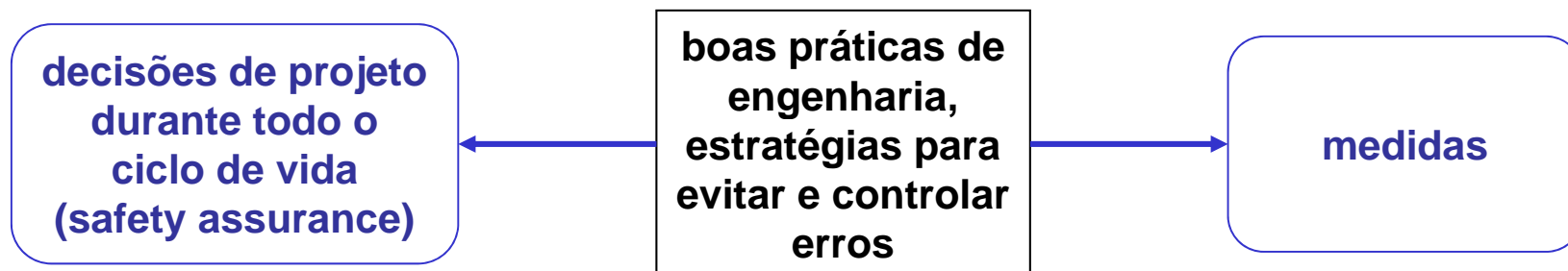
tipos de defeitos

defeitos de hardware **randômicos**

Reliability, Availability &
Maintainability



defeitos **sistemáticos** (incluindo erros de software)



SIL - Safety integrity levels

- IEC 61508 especifica 4 níveis de integridade de segurança para uma função de segurança.
 - safety integrity level 1 (SIL1) é o menor
 - safety integrity level 4 (SIL4) é o maior
- IEC 61508 detalha os requisitos necessários para alcançar cada nível.

os requisitos são mais rigorosos nos níveis mais altos de integridade para garantir menor probabilidade de defeitos perigosos

hardware vs software

- hardware

$$PFH_{G,1001} = \lambda_{DU}$$

- quantitativo

- taxa de defeitos de cada componente, forma de conexão no sistema, cobertura de falhas dos mecanismos de detecção, falhas correlacionadas (causa comum), taxa de reparo, ..

- qualitativo (para evitar introduzir falhas)

- ciclo de vida do projeto de hardware
 - conjunto de regras e recomendações
 - tabelas com técnicas
 - indicação de técnica **não recomendada**, **recomendada** e **altamente recomendada** para cada nível de SIL

NR, R, HR

hardware vs software

- software (qualitativo)
 - ciclo de vida do software
 - conjunto de regras e recomendações
 - tabelas com técnicas
 - indicação de técnica não recomendada, recomendada e altamente recomendada para cada nível de SIL

NR, R, HR

não são usadas fórmulas para cálculo de confiabilidade de software (falhas não são consideradas randômicas)

taxa de defeitos e SIL na norma IEC

- relaciona **taxas de defeitos** a níveis de integridade **derivados de medidas como FIT, MTTF**
- estabelece limites mínimos para taxas de defeito
 - baixa demanda - *probabilidade média de falhar* ao realizar função prevista sob demanda
 - por exemplo: PFD de 10^{-5}
 - significa 1 vez a cada 100000 vezes
 - alta demanda ou **modo de operação contínua** - *probabilidade de um defeito perigoso* por hora
 - PFH : 10^{-9}

baixa demanda



probabilidade de falhar
ao realizar função
prevista sob demanda

por exemplo: PFD de 10^{-5}
significa 1 vez a cada 100000 vezes

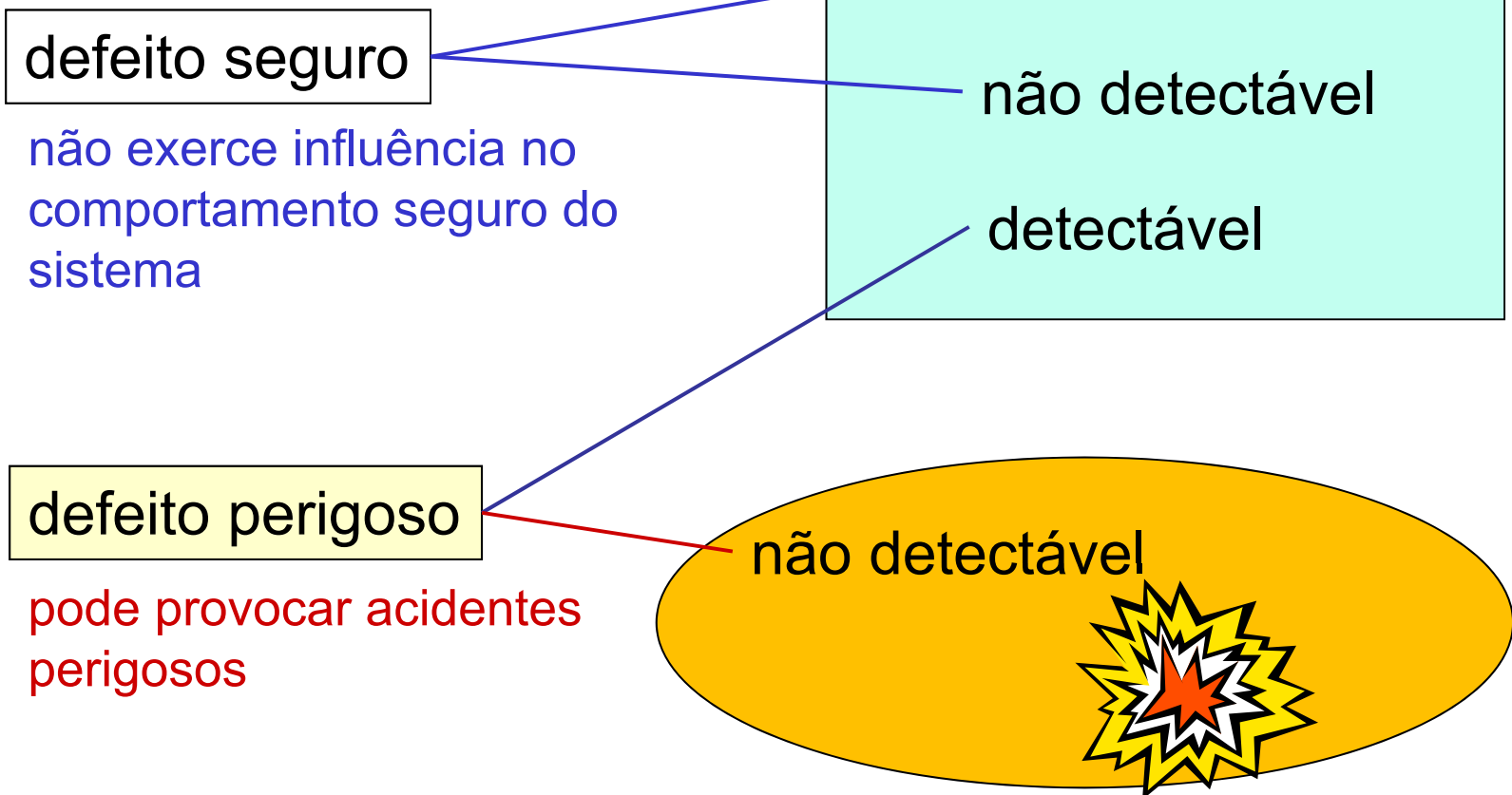
tabela SIL

baixa demanda -
probabilidade média de falhar ao realizar função prevista sob demanda

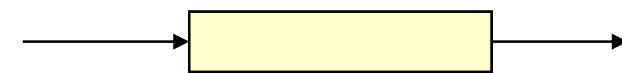
alta demanda ou modo de operação contínua -
probabilidade de um defeito perigoso por hora

modo de operação		
SIL	baixa demanda PFD	alta demanda PFH
4	$\geq 10^{-5}$ a $< 10^{-4}$	$\geq 10^{-9}$ a $< 10^{-8}$
3	$\geq 10^{-4}$ a $< 10^{-3}$	$\geq 10^{-8}$ a $< 10^{-7}$
2	$\geq 10^{-3}$ a $< 10^{-2}$	$\geq 10^{-7}$ a $< 10^{-6}$
1	$\geq 10^{-2}$ a $< 10^{-1}$	$\geq 10^{-6}$ a $< 10^{-5}$

defeitos

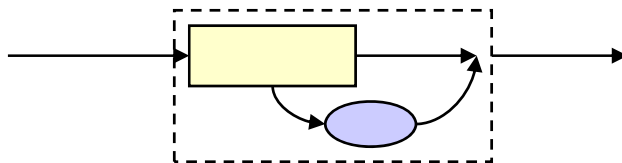


Arquiteturas MooN



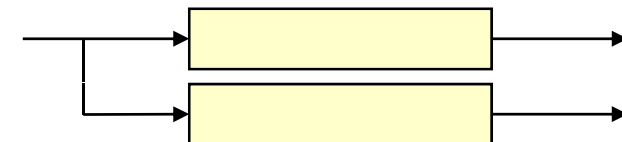
1oo1

componentes
confiáveis e em
pequeno número



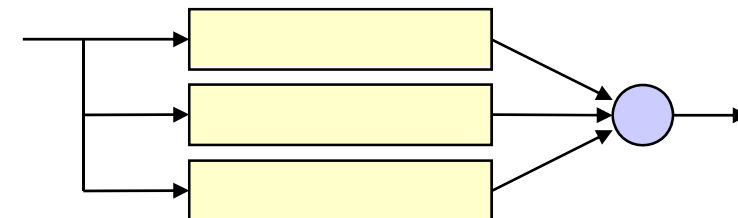
1oo1D

diagnóstico exige circuitos
extras ou algoritmos extras



1oo2

ideal para fail-safe



2oo3

ideal para períodos
curtos de missão

É possível alcançar alta integridade de segurança sem
necessidade de canais redundantes. Qual o segredo?

PFH para 1001

$$PFH_{G,1001} = \lambda_{DU}$$

λ_{DU} : λ devido a defeitos perigosos não detectáveis

PFH - probabilidade média de defeito por hora

onde se obtém λ ?

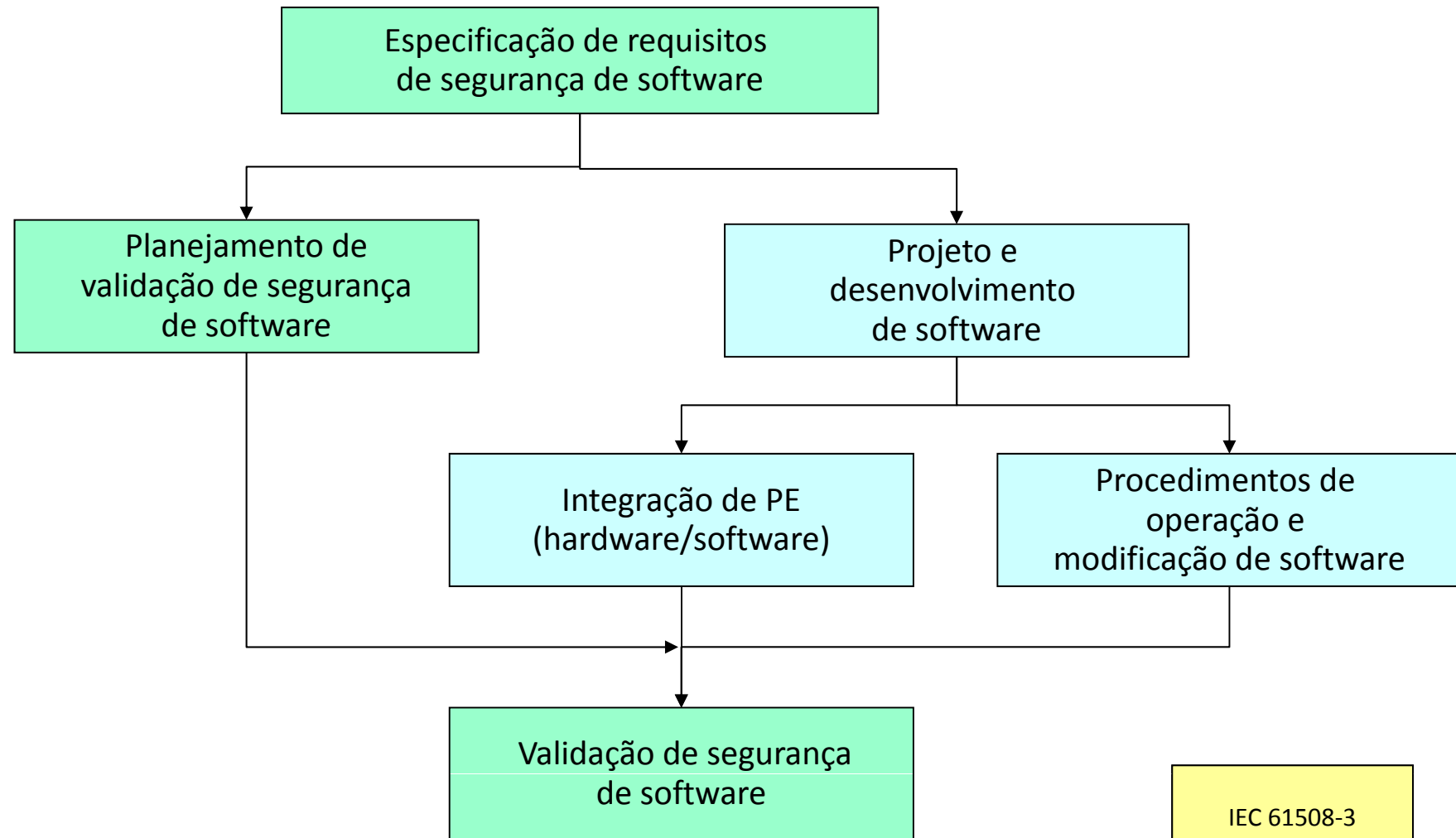
especificação de cada componente de hardware usando base de dados de componentes

causa comum: defeitos correlacionados

- importante nos sistemas 1oo2 ou 2oo3
 - causa comum - falhas que afetam canais redundantes
 - β - fator (peso) para defeitos perigosos não-detectáveis
 - β_D - fator para defeitos perigosos detectáveis

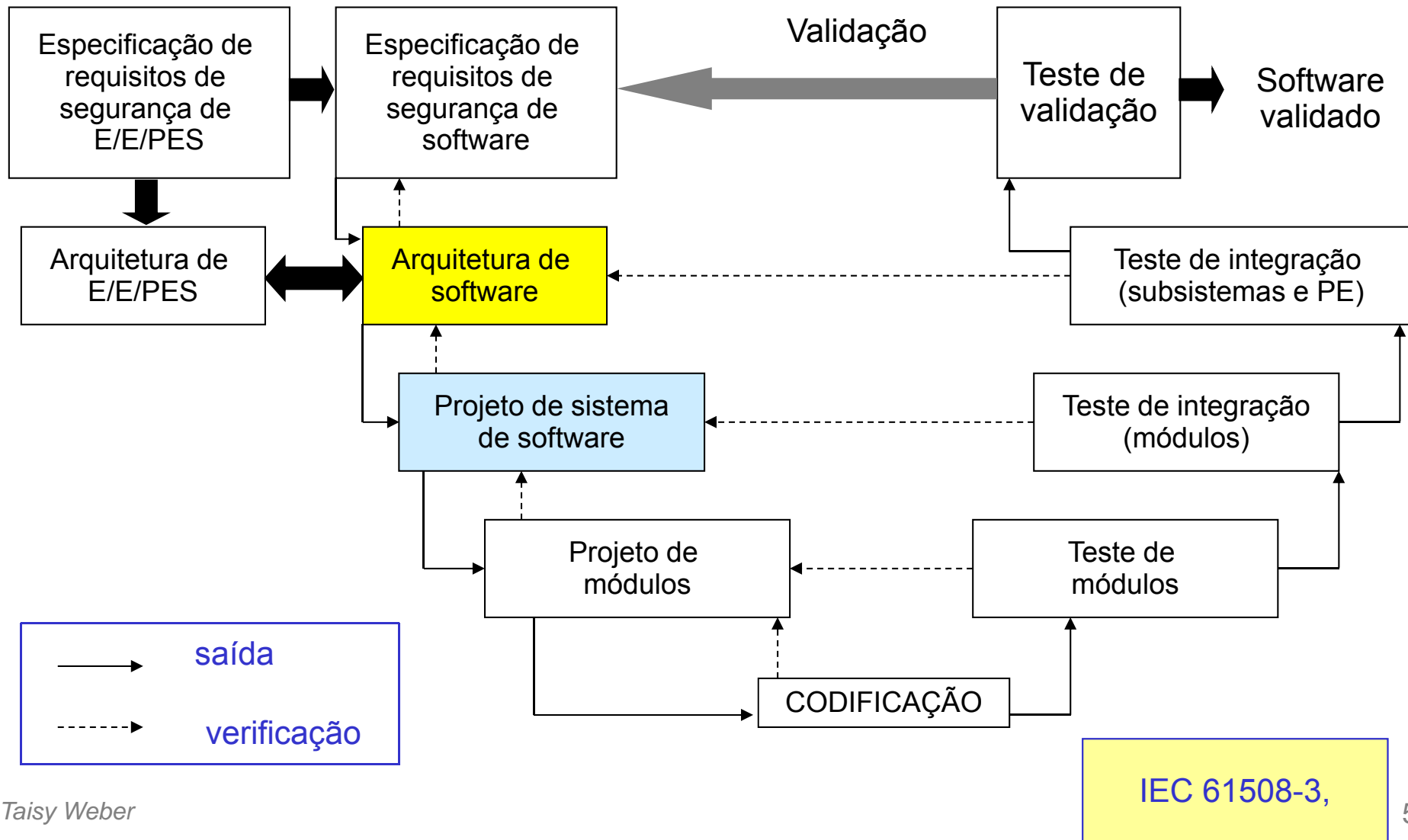
para sistemas 1oo2 ou 2oo3 o cálculo do λ_{DU} é mais complicado do que o cálculo de 1oo1 pois envolve β e esquemas série paralelo de composição de taxa de defeitos

Ciclo de vida de segurança de software



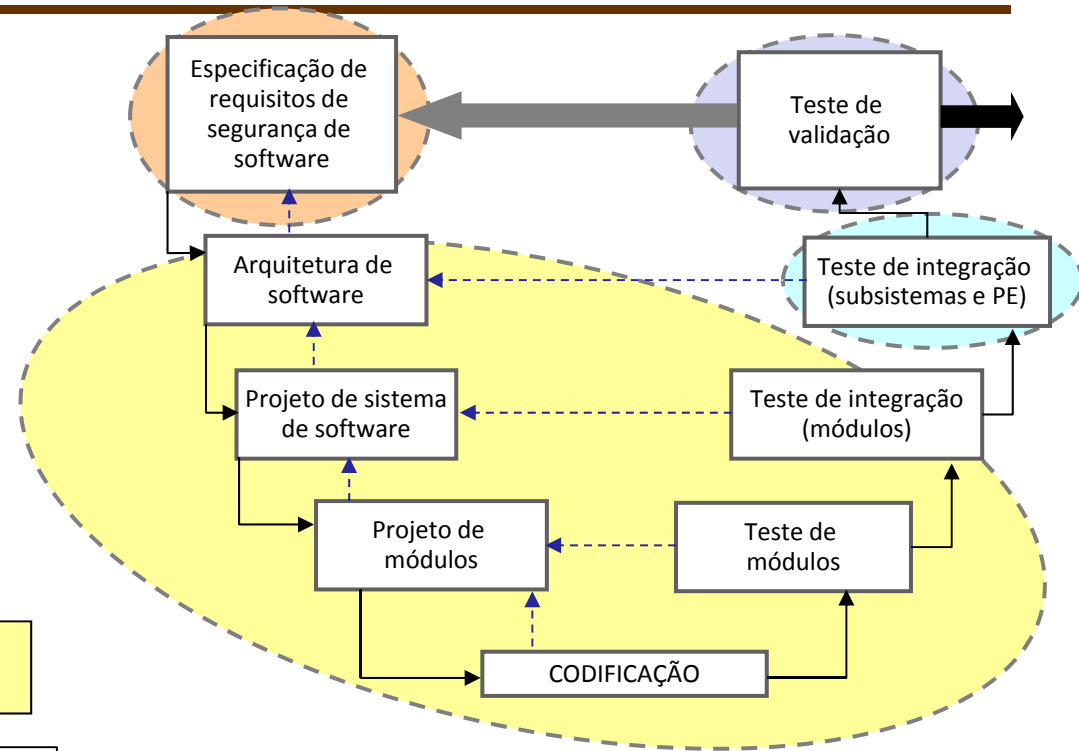
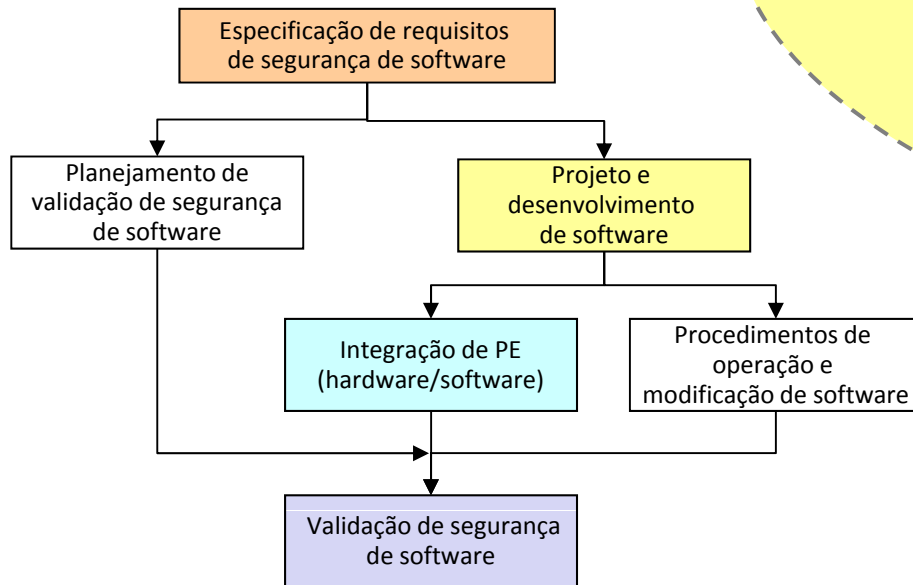
IEC 61508-3

modelo em V: software



Relação entre os modelos

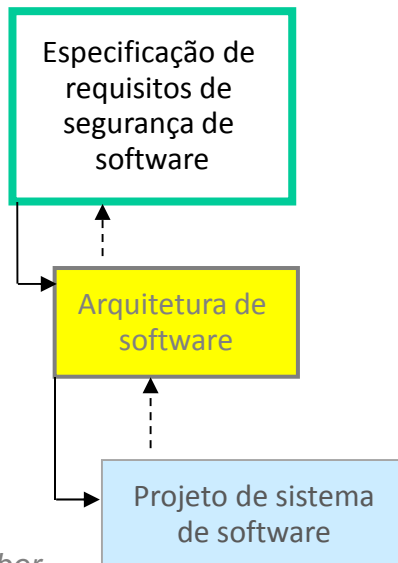
ciclo de vida de software



modelo V

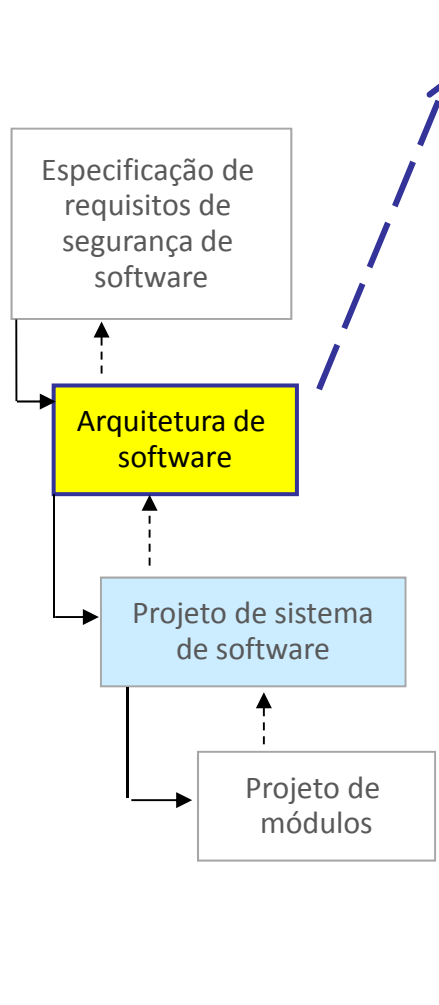
Nova tabela A.1 (IEC61508-3 2010)

Technique/Measure *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1a	Semi-formal methods	Table B.7	R	R	HR	HR
1b	Formal methods	B.2.2, C.2.4	---	R	R	HR
2	Forward traceability between the system safety requirements and the software safety requirements	C.2.11	R	R	HR	HR
3	Backward traceability between the safety requirements and the perceived safety needs	C.2.11	R	R	HR	HR
4	Computer-aided specification tools to support appropriate techniques/measures above	B.2.4	R	R	HR	HR



traceability foi introduzida na versão de 2010

exemplo de tabela: A.2 - arquitetura





		1	2	3	4
1	Fault detection and diagnosis	---	R	HR	HR
2	Error detecting and correcting codes	R	R	R	HR
3a	Failure assertion programming	R	R	R	HR
3b	Safety bag techniques	---	R	R	R
3c	Diverse programming	R	R	R	HR
3d	Recovery block	R	R	R	R
3e	Backward recovery	R	R	R	R
3f	Forward recovery	R	R	R	R
3g	Re-try fault recovery mechanisms	R	R	R	HR
3h	Memorising executed cases	---	R	R	HR
4	Graceful degradation	R	R	HR	HR
5	Artificial intelligence - fault correction	---	NR	NR	NR
6	Dynamic reconfiguration	---	NR	NR	NR
7a	Structured methods including for example, JSD, MASCOT, SADT and Yourdon.	HR	HR	HR	HR
7b	Semi-formal methods	R	R	HR	HR
7c	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	---	R	R	HR

Nova A.2

Technique/Measure *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
	Architecture and design feature					
1	Fault detection	C.3.1	---	R	HR	HR
2	Error detecting codes	C.3.2	R	R	R	HR
3a	Failure assertion programming	C.3.3	R	R	R	HR
3b	Diverse monitor techniques (with independence between the monitor and the monitored function in the same computer)	C.3.4	---	R	R	----
3c	Diverse monitor techniques (with separation between the monitor computer and the monitored computer)	C.3.4	---	R	R	HR
3d	Diverse redundancy, implementing the same software safety requirements specification	C.3.5	---	---	---	R
3e	Functionally diverse redundancy, implementing different software safety requirements specification	C.3.5	---	---	R	HR
3f	Backward recovery	C.3.6	R	R	---	NR
3g	Stateless software design (or limited state design)	C.2.12	---	---	R	HR
4a	Re-try fault recovery mechanisms	C.3.7	R	R	---	---
4b	Graceful degradation	C.3.8	R	R	HR	HR

Arquitetura de software

Nova A.2

5	Artificial intelligence - fault correction 	C.3.9	---	NR	NR	NR
6	Dynamic reconfiguration 	C.3.10	---	NR	NR	NR
7	Modular approach	Table B.9	HR	HR	HR	HR
8	Use of trusted/verified software elements (if available)	C.2.10	R	HR	HR	HR
9	Forward traceability between the software safety requirements specification and software architecture	C.2.11	R	R	HR	HR
10	Backward traceability between the software safety requirements specification and software architecture	C.2.11	R	R	HR	HR
11a	Structured diagrammatic methods **	C.2.1	HR	HR	HR	HR
11b	Semi-formal methods **	Table B.7	R	R	HR	HR
11c	Formal design and refinement methods **	B.2.2, C.2.4	---	R	R	HR
11d	Automatic software generation	C.4.6	R	R	R	R
12	Computer-aided specification and design tools	B.2.4	R	R	HR	HR

Arquitetura de
software

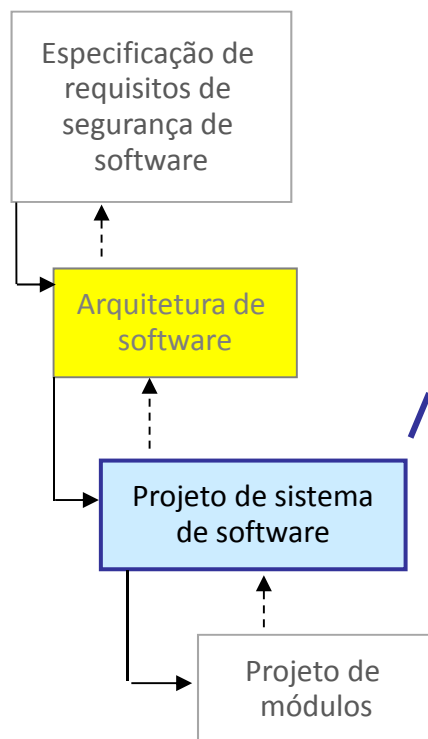
Nova A.2

13a	Cyclic behaviour, with guaranteed maximum cycle time	C.3.11	R	HR	HR	HR
13b	Time-triggered architecture	C.3.11	R	HR	HR	HR
13c	Event-driven, with guaranteed maximum response time	C.3.11	R	HR	HR	-
14	Static resource allocation	C.2.6.3	-	R	HR	HR
15	Static synchronisation of access to shared resources	C.2.6.3	-	-	R	HR

os itens 13 só se aplicam para sistemas com requisitos de temporização de segurança

Arquitetura de
software

exemplo de tabela: projeto de software



		1	2	3	4
1	Suitable programming language	HR	HR	HR	HR
2	Strongly typed programming language	HR	HR	HR	HR
3	Language subset	---	---	HR	HR
4a	Certificated tools	R	HR	HR	HR
4b	Tools: increased confidence from use	HR	HR	HR	HR
5a	Certificated translator	R	HR	HR	HR
5b	Translator: increased confidence from use	HR	HR	HR	HR
6	Library of trusted/verified software modules and components	R	HR	HR	HR

documentos IEC

2550,-

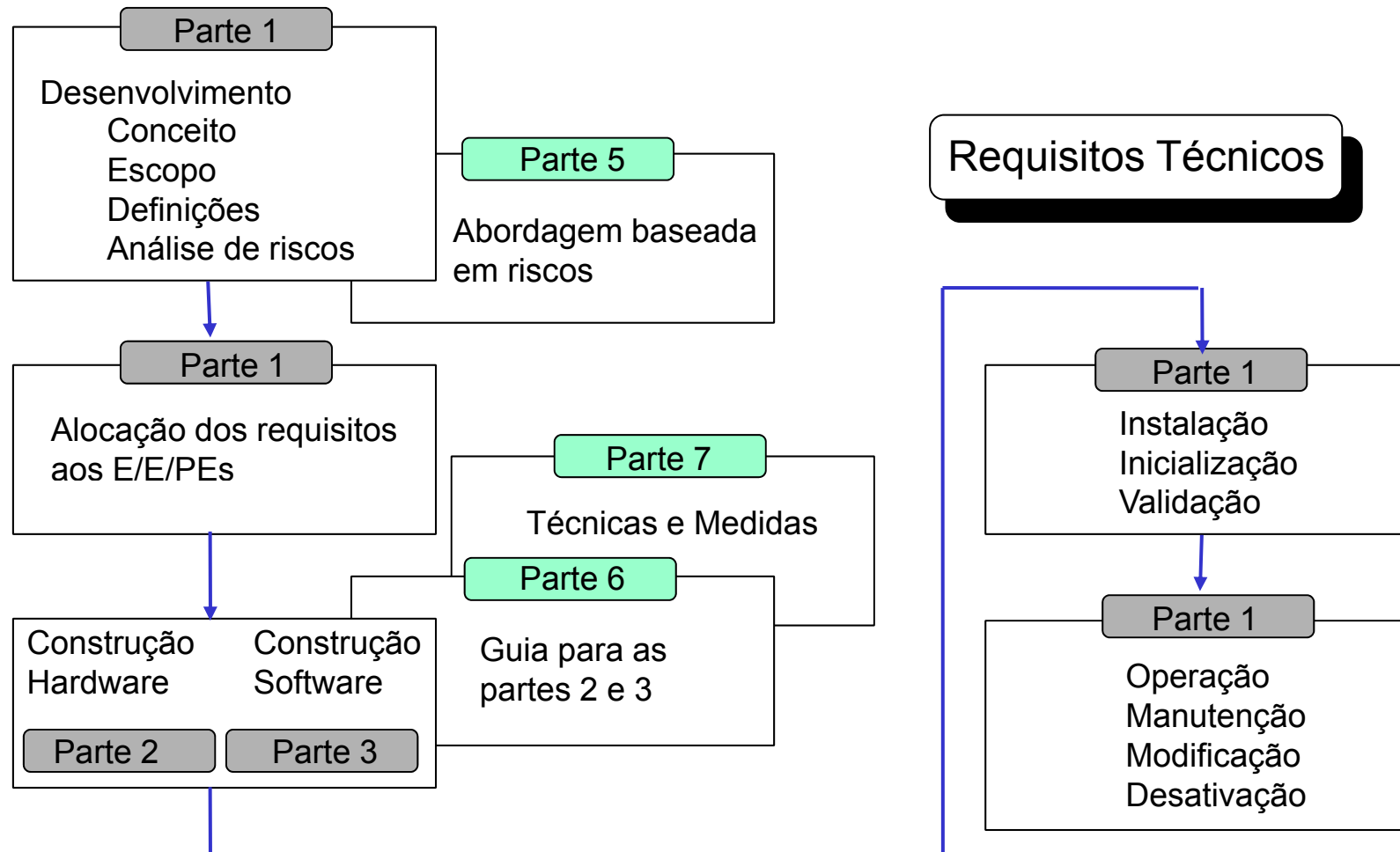
- IEC 61508-0 - Functional safety and IEC 61508
- IEC 61508-1 - General requirements
- IEC 61508-2 - Requirements for electrical/electronic/
programmable electronic safety-related systems
- IEC 61508-3 - Software requirements
- IEC 61508-4 - Definitions and abbreviations
- IEC 61508-5 - Examples of methods for the determination of safety integrity
levels
- IEC 61508-6 - Guidelines on the application of IEC 61508-2 and IEC 61508-3
- IEC 61508-7 - Overview of measures and techniques

<http://www.iec.ch/functionalsafety/standards/>

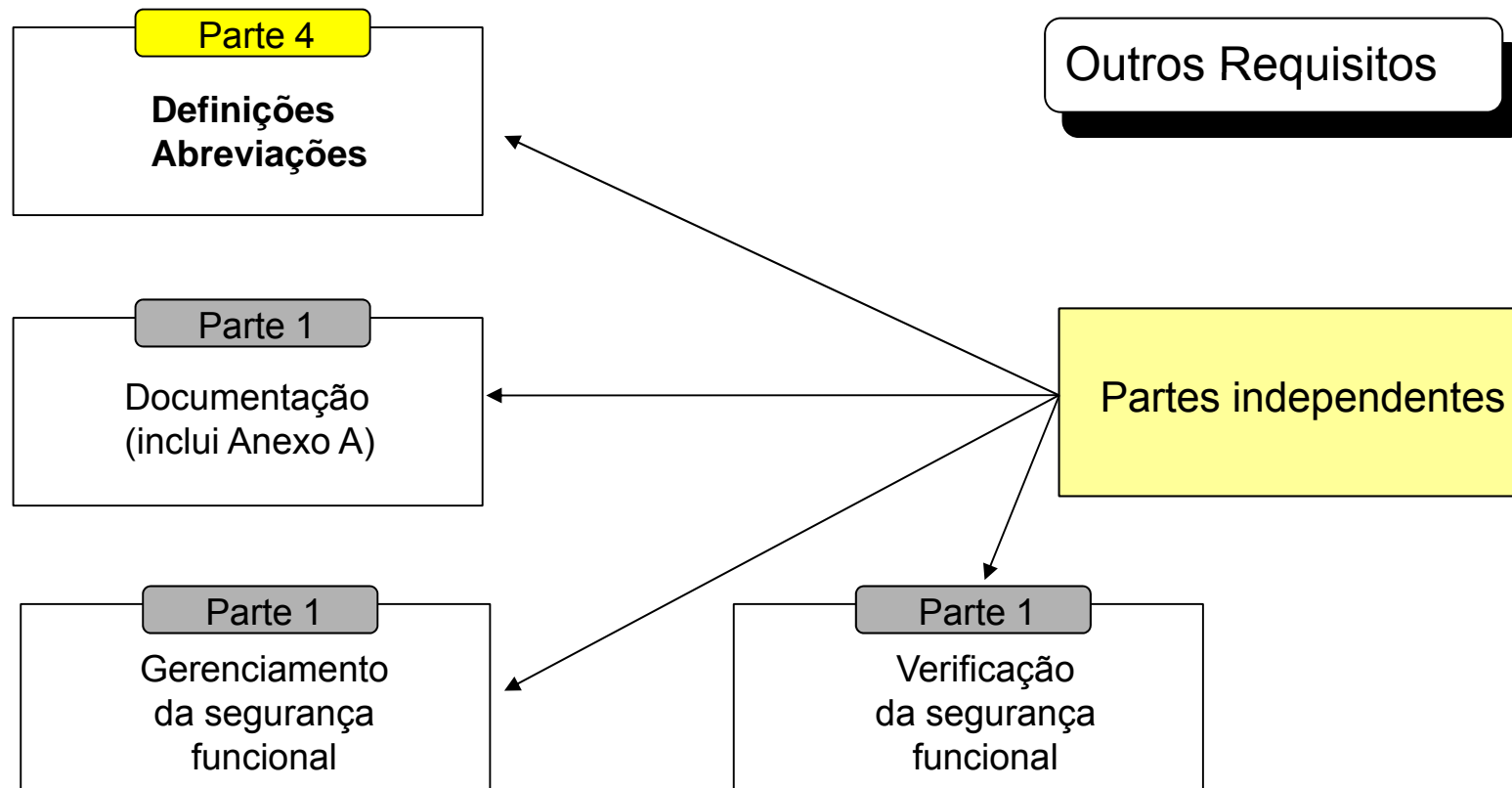


exceto a parte zero, de 2005, todas as demais são de 98 a 2000 e foram revisadas em abril de 2010

IEC 61508



IEC 61508



tolerância a falhas e safety (norma)

- conceitos da área de dependabilidade não se tornaram obsoletos com a norma
 - falha, erro e defeito
 - confiabilidade e suas medidas
 - modelagem de confiabilidade
 - teste e validação
- os termos e técnicas usuais na área de tolerância a falhas continuam aplicáveis
 - as diferenças são apenas relativas a área de aplicação (segurança crítica)
 - dano, perigo, risco

bibliografia

- *Functional safety and IEC 61508: A basic guide*
 - November 2002 (IEC web site)
- Dunn, William R. *Designing Safety-Critical Computer Systems*. Computer, 2003
- Bell, R.: *Introduction to IEC 61508*. In Proc. of the 10th Australian Workshop on Safety Critical Systems and Software, 3-12. (2006)

Abreviaturas

- E/E/PE Electrical/electronic/programmable electronic
- E/E/PES Electrical/electronic/programmable electronic system
- EUC Equipment under control
- PES Programmable electronic system
- PLC Programmable logic controller
- SIL Safety integrity level