University of Bielefeld
Faculty of Technology

RVS
Rechnernetze und Verteilte Systeme

CAUSALIS

The Concepts of IEC 61508

An Overview and Analysis

Prof. Peter B. Ladkin PhD
ladkin@rvs.uni-bielefeld.de

Motivation: Clear Concepts

- Concepts must be clear in order to enable easy and uniform use in engineering
- If concepts are unclear, then
  - reasoning is not easily seen to be (in)correct
  - mistakes are harder to detect

- There are various concepts of risk and hazard
- Which are effective for engineering purposes, and which are not?
  - Which are effective in which domains, and which not?

Motivation: Effective Methods

- Effective methods have three characteristics
  - They „work“
    - They are applicable to the domain of interest
    - They enable passable assessments of risk and safety-critical failure
    - They can be used within an engineering organisation
  - We know why they work
    - Good arguments exist concerning applicability and correctness
  - We have independent means to check the results

- Summary: good engineering means knowing what methods are applicable, where, why and how.

Basic Concepts of System Safety

- Basic ontological concepts
  - system, environment, boundary, objects, fluents, state, state change, event, behavior, near and far behaviors, necessary causal factor
    plus
- Accident
  - Likelihood, Severity
- Hazard
  - Likelihood, Consequences
- Risk

Basic Concepts in de Moivre, Leveson, IEC 61508

De Moivre

- Abraham de Moivre, De Mensura Sortis, 1711
  - in the Philosophical Transactions of the Royal Society
  - „The Risk of losing any sum is the reverse of Expectation; and the true measure of it is, the product of the Sum adventured multiplied by the Probability of the Loss.“
  - Severity: „the Sum adventured“

De Moivre: Risk

- *Risk*: expected value of loss
  - Σ p(Cx).S(Cx)
    - Cx: a loss event
    - S(Cx): the severity of the loss event
- *Accident*: here, the loss event
- *Hazard*: ??

Leveson: Safeware definitions (1)

- *Accident*: „an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss.“
- *Hazard*: „a state or set of conditions of a system ... that, together with other conditions in the environment of the system ..., will lead inevitably to an accident“
  - defined with respect to the environment
  - what constitutes a hazard depends on the boundary of the system

Leveson: Safeware definitions (2)

- *Hazard* (cont'd)
  - *Severity* (or *damage*): „the worst possible accident that could result from the hazard given the environment in its most unfavorable state“
  - *Likelihood* of occurence
  - *Hazard level*: „combination of severity and likelihood of occurrence“
- *Risk:* „the hazard level combined with (1) the likelihood of the hazard leading to an accident ... and (2) hazard exposure or duration“
- *Safety*: „freedom from accidents or losses“

Interpretation of Safeware definitions

- Accident
  - an unwanted event
- Hazard
  - a system state, which in combination with the most unfortunate environment state, results inevitably in (is a sufficient causal factor of) an accident
- Severity
  - Level of loss (on a ratio scale)
- Risk
  - Σ p(H).p(Cx | H).S(Cx)
    - Cx: an accident that results from/through H
    - S(Cx): the severity of the accident Cx

Hazard: Variant Definitions

- Leveson: system state
  - A commercial aircraft encounters thunderstorm turbulence which causes loss of control and breakup
    - When the environment contains such turbulence, and the aircraft is flying, then an accident is inevitable
    - It follows that flying states of the aircraft are hazard states
- Environment state
  - In this example, as in the game of golf or of real tennis, the „hazard“ is more intuitively an environmental state
- Global State (Jackson 1995; Simpson & Stoker 2002)
- IEC 61508: „potential source of harm“
  - seems to allow system+environment state (*global state*)
  - but then, it seems to allow lots of things

Comparison of Safeware and De Moivre Risk

- How do Σ p(H).p(Cx | H).S(Cx) and Σ p(Cx).S(Cx) compare?
  - H1, H1, ... ,Hk a collection of mutually exclusive hazards such that each accident happens through one of them
  - Then by a basic calculation in conditional probability p(Cx) = Σ p(Hi).p(Cx | Hi)
  - Thus p(Cx).S(Cx) = Σ p(Hi).p(Cx | Hi).S(Cx)
  - And summing over all Cx yields the result

  - (Repeat): H1, H1, ... ,Hk *a collection of mutually exclusive hazards such that each accident happens through one of them*
  - Without this assumption, the sums may not be the same

IEC 61508: Definitions (1)

- Harm
  - „physical injury or damage to the health of people either directly, or indirectly as a result of damage to property or to the environment“
- Hazard
  - „potential source of harm“
- Hazardous event
  - „hazardous situation which results in harm“
- Hazardous situation
  - „circumstance in which a person is exposed to hazard(s)“

IEC 61508: Definitions (2)

- Risk
  - „combination of the probability of occurrence of harm and the severity of that harm“
- Tolerable Risk
  - „risk which is acceptable in a given context based on the current values of society“
- Safety
  - „freedom from unacceptable risk“

Comments on IEC 61508 definitions (1)

- There is no definition of accident
  - „hazardous event“ comes close, but is a „situation“
- Harm is limited to personal injury
  - but US aviation regs (14 CFR 830 §830.2) allow an accident to be significant aircraft damage alone
  - similarly with USAF Class A mishaps (the severest sort)
- Definition of hazard is unclear
  - Basic question: is it a state or an event?
  - What is a „source“?
  - What is a „potential source“?
  - Potential source of harm? Source of potential harm?

Comments on IEC 61508 definitions (2)

- Risk
  - how does one combine probability of harm with severity of harm?
    - One can „combine“ in an arbitrary number of ways
  - If severity is quantitative, does/can „combine“ mean „multiply“?
  - If so, then risk is defined here to be a multiplication
  - In de Moivre & Leveson, it is a sum

Risk in IEC 61508: Clear?

- It is certain I shall suffer some degree of harm while using my bicycle (from a trivial scratch from a part once a month, to falling off once a decade, to being run over)
  - The probability of harm is 1
- Severity is variable from trivial to catastrophic
- Which „severity“ do I use? Call it S
- How do I „combine“ S with 1?
- It cannot mean the actual harm that will in fact occur, since that would render the concept unusable for calculation in advance, as IEC 61508 requires during system development („EUC risk“, „tolerable risk“, „residual risk“)

Comments on IEC 61508 definitions (3)

- Good definitions (good programs) define terms (variables) before they use them (Def-use test, used a lot in static analysis of programs)
- Usable definitions try to
  - be precise
  - reduce or eliminate ambiguity
  - limit the number of undefined concepts
  - be clear to the intended interpreters

- My opinion: IEC 61508 does not do well on these criteria, similar to many (but by no means all) engineering standards

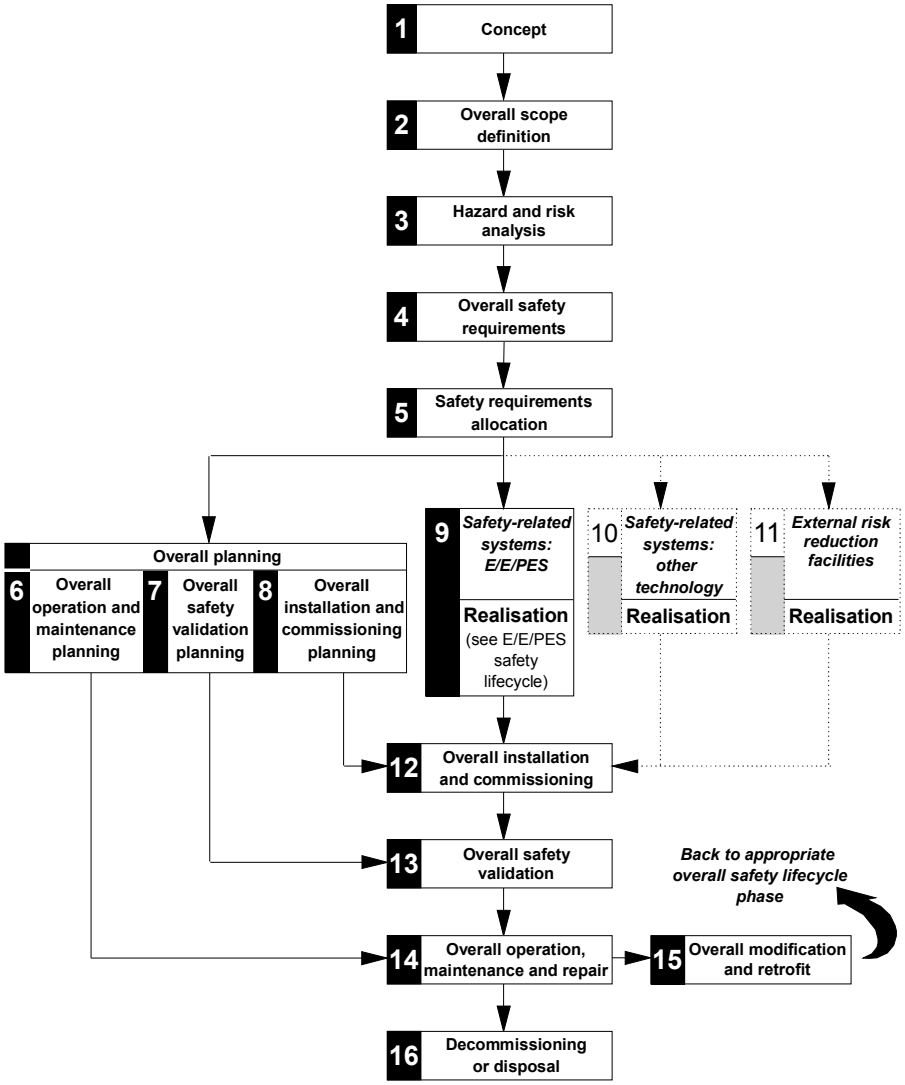
Fundamental Concepts of IEC 61508

- System Lifecycle
- Fuctional Safety
- Risk and Risk Reduction
- System Subdivision
- Safety Integrity Level (SIL)
- As Low As Reasonably Practicable (ALARP)

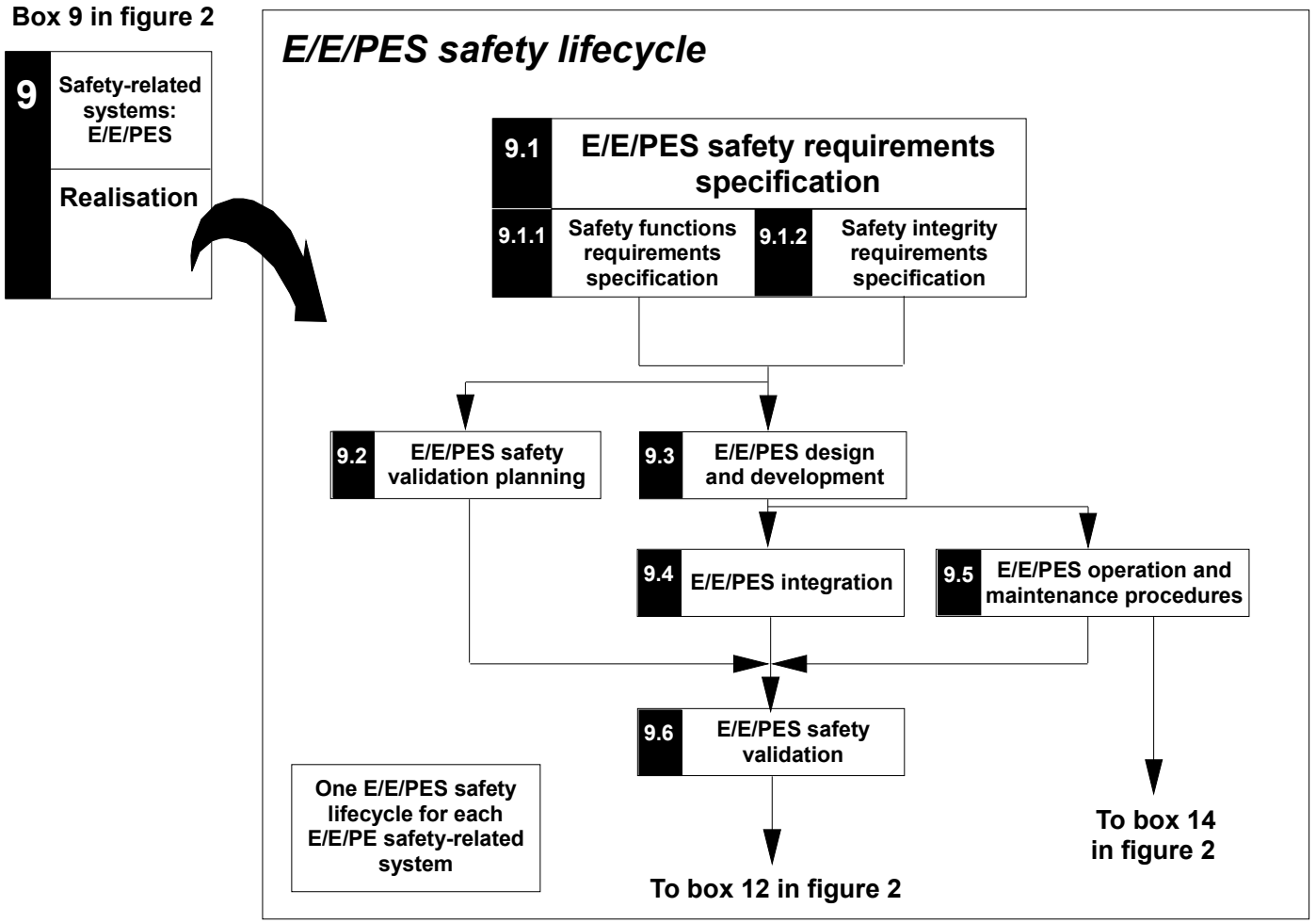
Concepts 1: System Lifecycle

- The System Life Cycle Model
  - Detailed
  - The safety task list follows the model

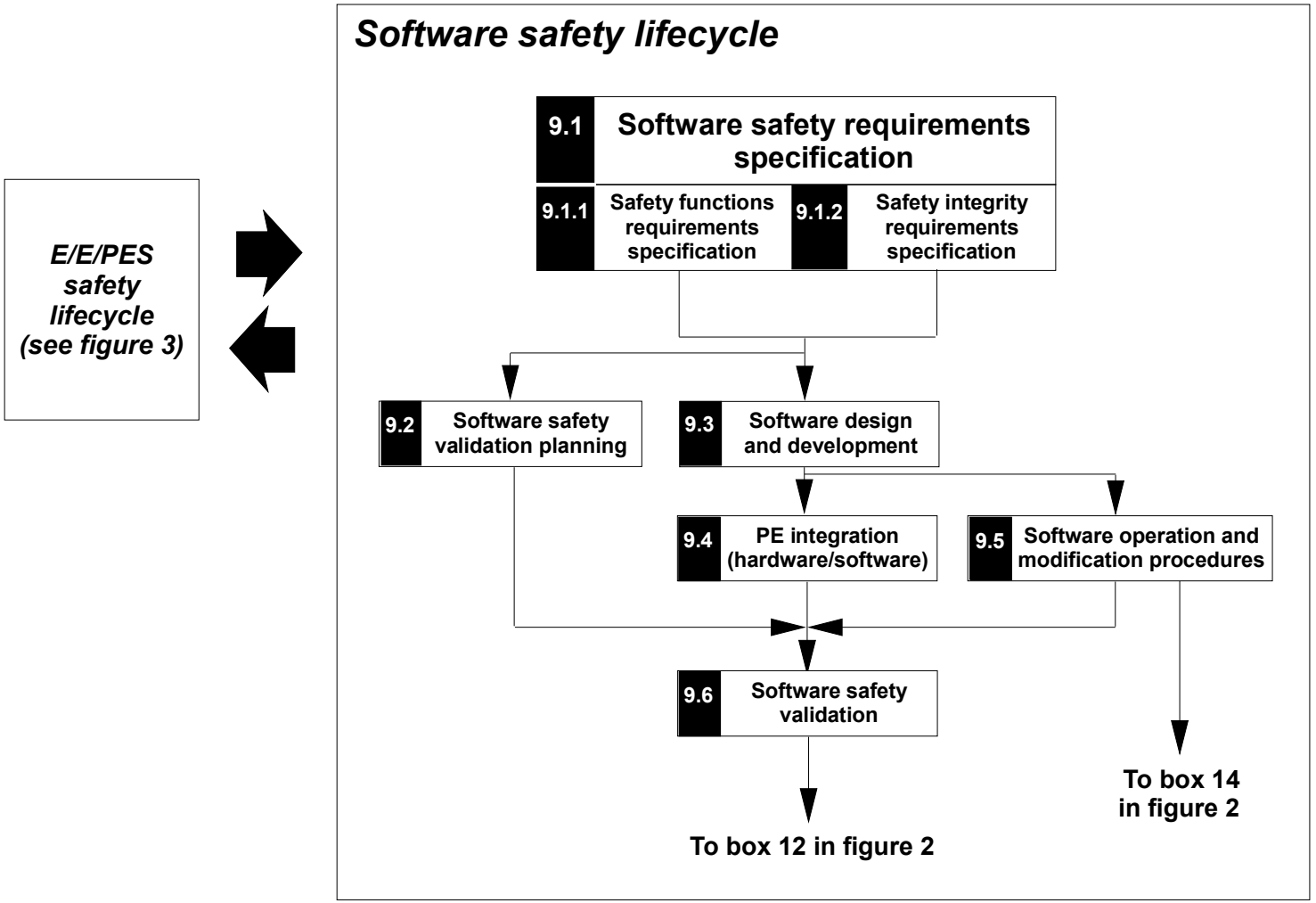
The IEC 61508 Safety Lifecycle



The E/E/PES (Sub)system Safety Lifecycle



The SW Safety Lifecycle



The Lifecycle

- One needs a lifecycle model
- The 61508 lifecycle model is as good as any and more detailed than most
- However, there is no guidance on how to fit it to a typical system development lifecycle

A Typical Development Lifecycle

- Requirements
  - Elicitation, Analysis, Specification
- Design Specification
- Coding
  - Code development, Testing
- Implementation
  - Integration, Integration-Testing
- „Maintenance“
  - Further development according to new requirements, Modification through error correction and failure correction
- Decommissioning

Comparison of Lifecycle Models

- We need to harmonise the IEC 61508 lifecycle model and the typical system development lifecycle model used in a firm
  - presumed to be straightforward, but how do we know? Who has done it?
- There are three sorts of different requirements in IEC 61508 (Fenton/Neil, 1998)
  - For the final product (the SC system)
  - For documentation
    - Specifications at the various levels
    - Analysis and reporting documents, e.g. the Safety Case
  - For resources
    - checks and sign-offs to be conducted by qualified personnel

Concepts 2: Functional Safety

- Functional Safety
  - Safety prophylaxis restricts itself to *safety functions*
  - Safety functions are actions, that are „intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event“
  - Recall that a hazardous event results in harm. If harm is to be avoided by means of the safety function, then the function should inhibit the specific hazardous events which are precursors of the harm

- Remember: not all major safety issues are functional!

Concepts 3: Risk & its Reduction

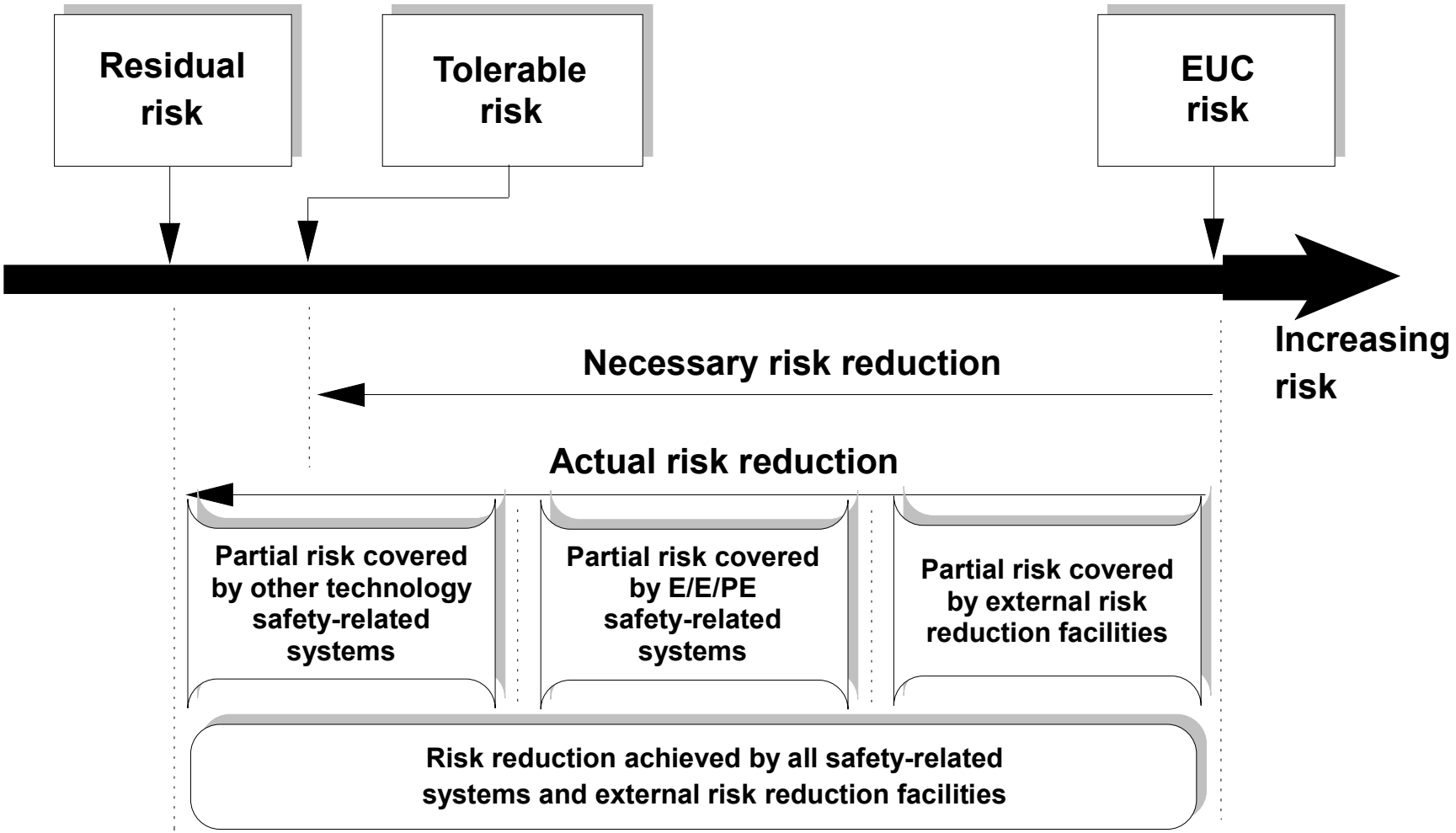
- Risk Reduction
  - There is no such thing as „Zero Risk“
  - The Safety Functions (SF) are concerned with *risk reduction*
    - There is an *EUC risk*: „risk arising from the EUC or its interaction with the EUC control system [EUCCS]“
    - There is a *tolerable risk*
    - There is a *residual risk*: „risk remaining after protective measures have been taken“
    - Developers must assess the EUC risk and the tolerable risk (to calculate the required *safety integrity level*, SIL) as well as the residual risk, which must be *as low as reasonably practicable* (ALARP)

Concepts 4: System Subdivision

- Three-way classification of (sub)system types
  - Equipment under control (EUC)
  - EUC control system (EUCCS)
  - Safety-Related System (SRS)
  - The EUCCS can be classified as an SRS or not (but the criterion, in clause 7.5.2.4, is a logical tautology!!)

- Safety-Related System
  - An SRS is „a designated [sub]system that
    - implements the required safety functions ..... and
    - is intended to achieve [in possible combination with others] the necessary safety integrity for the required safety functions“

Risk Reduction



Issues: Risk Reduction

- Risk Reduction must be calculated
  - on the basis of particular statistics
    - Risk of EUC/EUCCS without SRSs
    - Risk of EUC/EUCCS + SRSs
    - Acceptable Risk (socially derived)
  - The statistics don't always exist!
    - How often do they exist? There is some scepticism (Fowler 2000)

Concepts 5: SIL

- Safety Integrity Level (SIL)
  - Each SRS is assigned a SIL, which represents the probability that the SRS fulfils its safety function(s)
  - That is, the SIL of an SRS represents objectively the reliability of its safety function(s) (a *product requirement*)
  - The SIL is assigned according to the required risk reduction (from EUC risk at least to the tolerable risk)
  - A quantitative difference is made between
    - Continuous-operation (high-demand) functions
    - Low-demand functions (known elsewhere as on-demand functions)
  - Development of an SRS with a designated SIL requires a certain development process (*a process requirement*)

SILs, continued

- SIL (cont'd)
  - I shall ignore the difference between low-demand and high-demand modes
  - Four levels of increasing reliability (SIL 1 – SIL 4)
    - Implicitly five, with SIL 0, about which nothing is said
    - Each level requires a reliability of
      10^(-(n+1)) to 10^(-n) dangerous failures per hour/per demand
    - Highest recognised level ist n=8 (SIL 4, continuous mode)

SIL Table: High-Demand/Continuous Mode

Safety integrity level	**High demand or 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 $< 10^{-5}$

Issues with SILs

- The distinction between low-demand and high-demand modes may well disappear in the next release of 61508 (Simon Brown, 2005)
- A SIL is valid for a *particular SF-component* in a *particular system+environment* given a (socially-determined) *particular tolerable risk*
  - However, organisations such as the TÜVs are starting to „certify“ components independent of specific application
  - There is a real danger that a SIL will be seen as a property of the component, which it is not (Redmill 2000, Hamilton-Rees, 1999)

Issues with SILs (Martyn Thomas)

- SILs are unhelpful to software developers
  - SIL 1 target failure rates are already beyond practical verification (Littlewood-Strigini 1993, Butler-Finelli 1993)
  - SILs 1-4 subdivide a problem space in which there is no sensible distinction to be made amongst applicable development and assurance methods
  - For many recommended methods, there is little or no evidence that they reduce failure rates
  - There is increasing evidence that those methods which do reduce failure rates also save money: they should be used at any SIL

Issues with SILs (Martyn Thomas)

- SILs set developers impossible targets
  - so the focus shifts from providing adequate safety (product) to fulfilling the recommendations of the standard (process)
  - But there is little correlation between process properties and safety
- Focus shift from product to process does not help safety
- (Note: There are concepts of SIL in other standards which suffer from only some of these problems. PBL)

Issues with SILs

- Highest SIL requirement:
  - Less than one dangerous failure every 10^8 op-hours
  - (But more than one dangerous failure every 10^9 op-hours!! Daft.)

- The combinatorics doesn't work out for
  - Commercial aviation (which requires lower failure rates for certain critical subsystems, and the general history suggests this can be achieved)
  - The automobile industry (which has a real requirement of SRS reliability of up to 10^10 op-hours per failure!!)

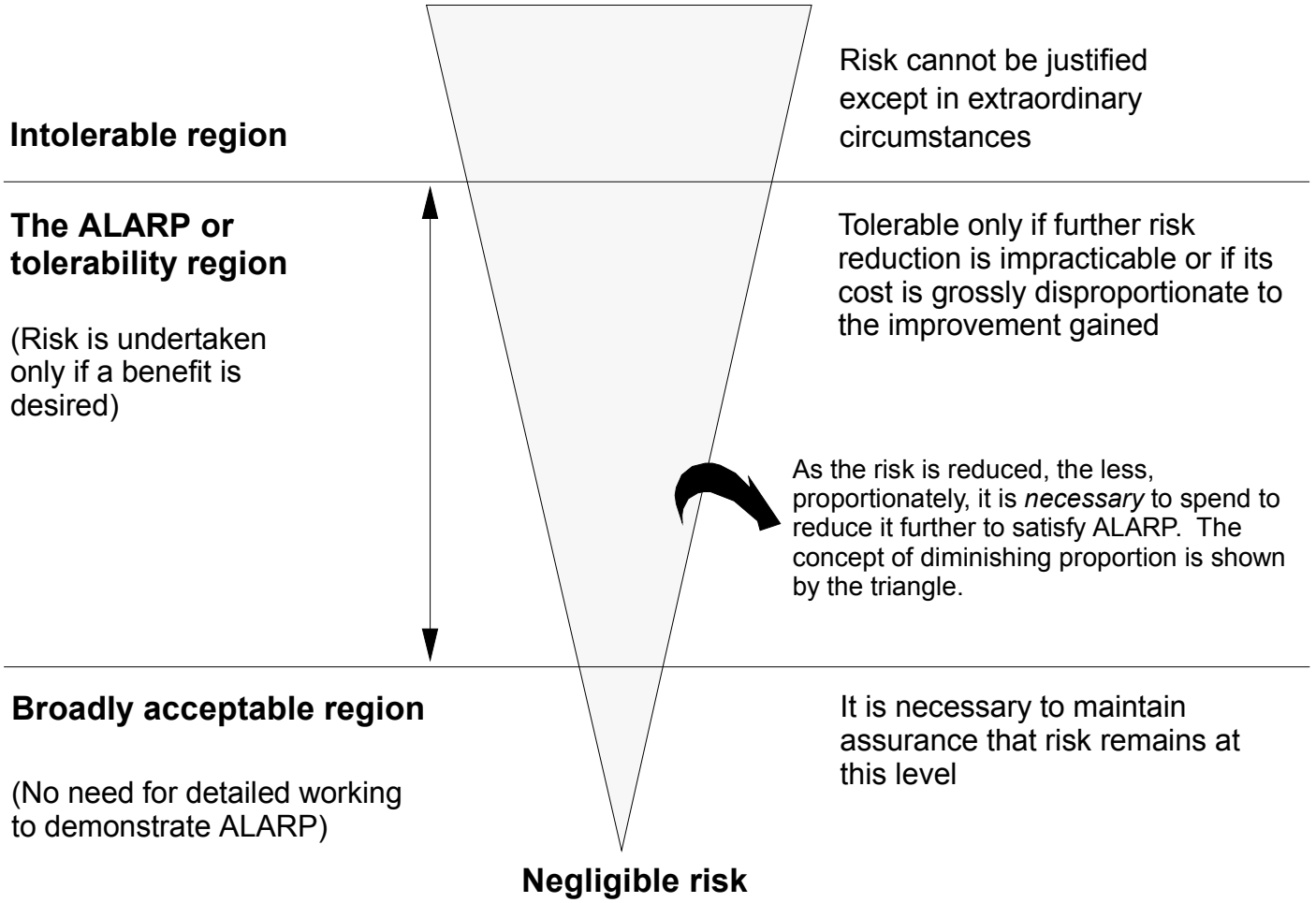
Concepts 6: ALARP

- The ALARP Principle
  - To calculate the required risk reduction, one must use the As Low As Reasonably Practicable (ALARP) principle
  - Origins: English law
    - Lord Asquith, 1949
    - significantly reinforced: Lord Cullen (1989), Piper Alpha oil platform fire investigation
  - Risks are classified into three:
    - Acceptable: so low that it can for all practical purposes be ignored
    - Intolerable: so high as to be unacceptable in all circumstances
    - The ALARP region: the region between acceptable and intolerable, in which the system developer is required to reduce the risk to be „as low as reasonably practicable“

ALARP

- ALARP (cont'd)
  - In legal cases, the UK HSE regards the ALARP principle as having been fulfilled if a developer is able to establish that a system was developed in accordance with IEC 61508 (Mark Bowell, UK HSE, mailing-list comment, 2004)
  - So it seems as if IEC 61508 requires ALARP, but to conform with ALARP one needs only to do everything else
  - Logically, this makes ALARP redundant!!
- It would help to resolve this confusion

The ALARP Principle



Tolerable Risk Target: Quantitative Risk Classification Matrix (RCM) Example

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

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

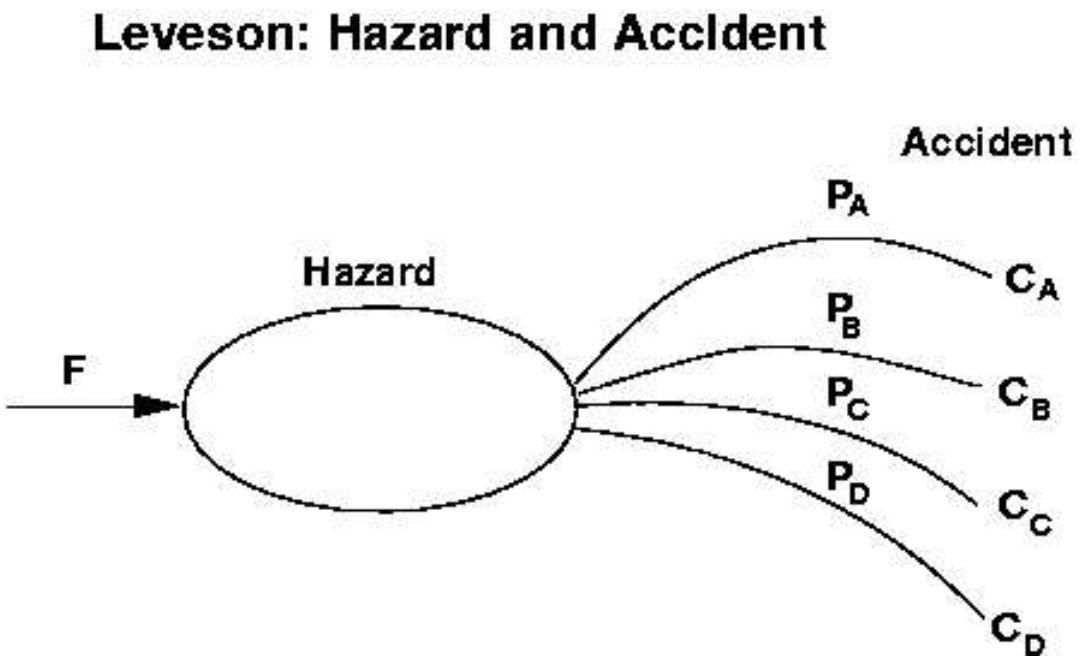
Issues: ALARP and Risk Classes

- Risk Classes I and IV fit with ALARP
- Risk Classes II and III don't obviously fit with ALARP
  - In the region in which Risk Classes II and III apply, one is required to use the ALARP risk-reduction principle
  - ALARP requires in both cases that:
    risk shall be reduced so far as reasonably practicable
  - ALARP does not (obviously) say:
    - Risk reduction may cease when cost is grossly disporportional to benefits. No RCA is implied
    - As risk is reduced, the less it is necessary proportionately to spend to reduce it further
    - But both of these claims are in the IEC 61508 explanatory diagram!

Issues: Relation between SIL and ALARP (Redmill, 2000)

- A SIL is an a priori requirement
  - It is assigned in the Safety-Requirements-Analysis task
- ALARP is a dynamic requirement
  - It will be assigned and handled in the Design task
- It is thereby possible that in a particular case ALARP would require a further reduction in risk beyond that set by the SIL

Leveson et al.: Accident Concepts

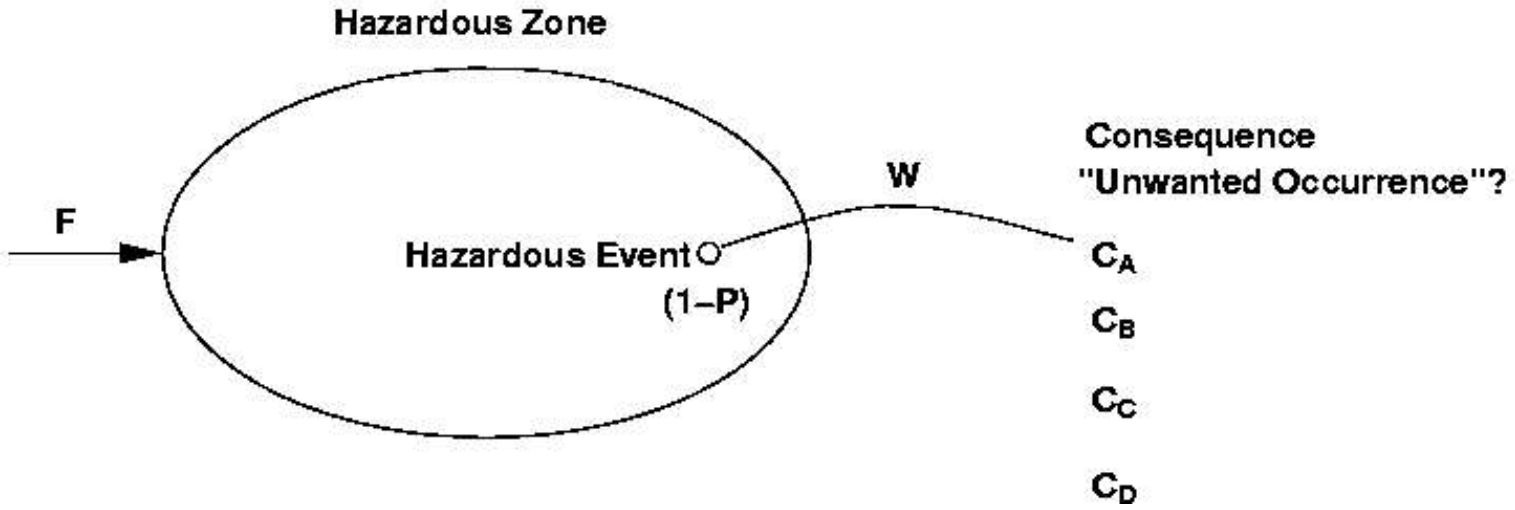


Difficult Example

- There is an example in which the Leveson-Risk does not equal the expected level of loss (Ladkin 1997)
  - Not every accident sequence passes through a hazard state
  - There is a stochastic dependence amongst the possible accident sequences

IEC 61508 Part 5: How to Have an Accident

IEC 61508: Hazardous Zone, Hazardous Event, Consequence, "Unwanted Occurence"



IEC 61508: Accident

- IEC 61508 understands Hazardous Event as:
  - something that can come to pass, independently of the severity of its harmful consequences
  - a „situation“, which in turn is a „circumstance“
- It seems similar to the concept of an accident (which however is an event), but in which the severity is abstracted away
  - Maybe an „accident type“?
  - Let's forget the „situation“/“circumstance“ imprecision
- The concepts appear to be interdefinable, given the basic ontology (Ladkin, 2004)

Advantage of the IEC 61508 Refinement

- The refinement of accidents into hazardous events and explicit severity may well be appropriate for, say, process control. Example:
  - A pressure vessel breaches (event type, encompassing many event types from leaks to explosions)
  - Severity:
    - Is the breach small or large?
    - Was nearby equipment heavily damaged, lightly damaged, or not at all?
    - Were nearby people injured? Severely injured? Were some killed?
    - And how many of those people were there?

Summary of Major IEC 61508 Concepts

- Lifecycle: helpful but a very particular model. Not clear how it fits with traditional lifecycle models
- Safety Functions/SRSs: a restricted concept
- Risk Reduction: generally a good idea, but application is restricted both in suitability to the application domain and statistically
- 3 system-types: restricted, sometimes misleading concept
- SIL: restricted and misleading
- ALARP: in principle strong, in practice weak. It strains against proven techniques such as Risk Matrix classification. A legal principle whose technical translation is not yet clear.

The End

Thanks for listening!