Standards and IEC61508

Prof. Chris Johnson,
School of Computing Science, University of Glasgow.
johnson@dcs.gla.ac.uk
http://www.dcs.gla.ac.uk/~johnson

University of Glasgow

Introduction

- Limitations of Safety Culture.
- The Need for Standards.
- The IEC 61508 Case Study.

University of Glasgow

Limitations of Safety Culture

- Cannot rely on safety culture.
- Standards enforce rules of conduct:
  - They support and are supported by safety culture;
  - Documentation open to external inspection and audit.
- But Standards do not ensure safety:
  - ‘a good standard can still lead to a bad system’;
  - Were all the processes followed?
  - Were the staff trained and motivated?
  - Was there a sufficient budget and managerial support?

University of Glasgow

Dijkstra – Process versus Product…

Testing can prove the presence of errors, but not their absence.

University of Glasgow

Examples

- MIL STD 882D:
  - US Military Risk Assessment;
  - Extensive sections on software.
- IEC 61508:
  - Aimed for programmable systems;
  - Across the process industries.
- DO-178B:
  - Aviation software standard;
  - Will be covered later in the course.

University of Glasgow

IEC 61508

- 7 parts, 400 pages:

1. General requirements;
2. Requirements for electrical/electronic/programmable electronic safety-related systems (hardware).
3. Software requirements
4. Definitions and abbreviations.
5. Methods for determining safety integrity levels.
6. Guidelines for the application of 1 and 2.
7. Techniques and measures.

Ack: Felix Redmill

University of Glasgow

IEC 61508

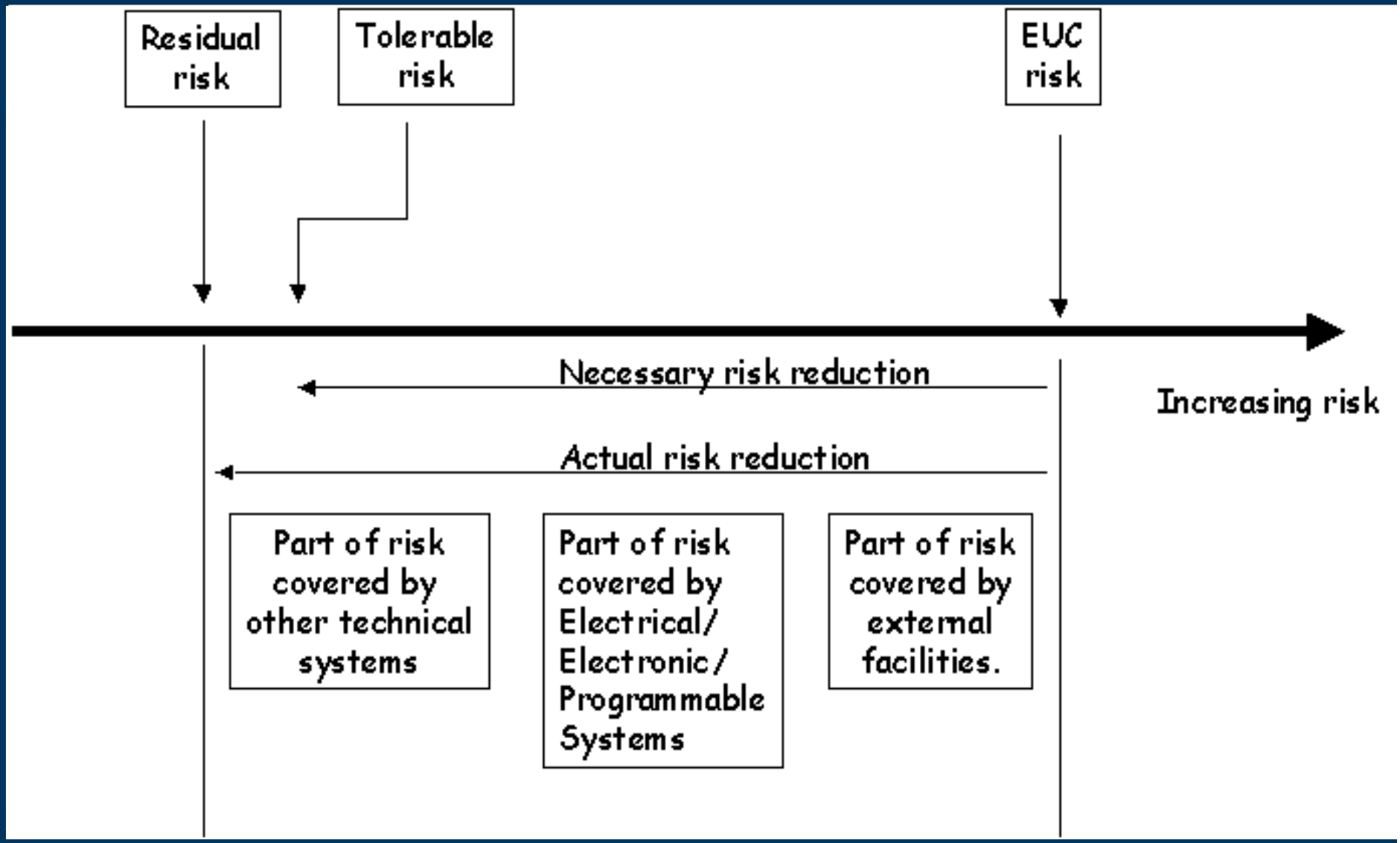
- Zero safety is impossible (cf Perrow).
- Must understand the risks.
- And reduce unacceptable risks.
- And DEMONSTRATE this reduction.
- Implies high level of documentation.

IEC 61508 (Definitions)

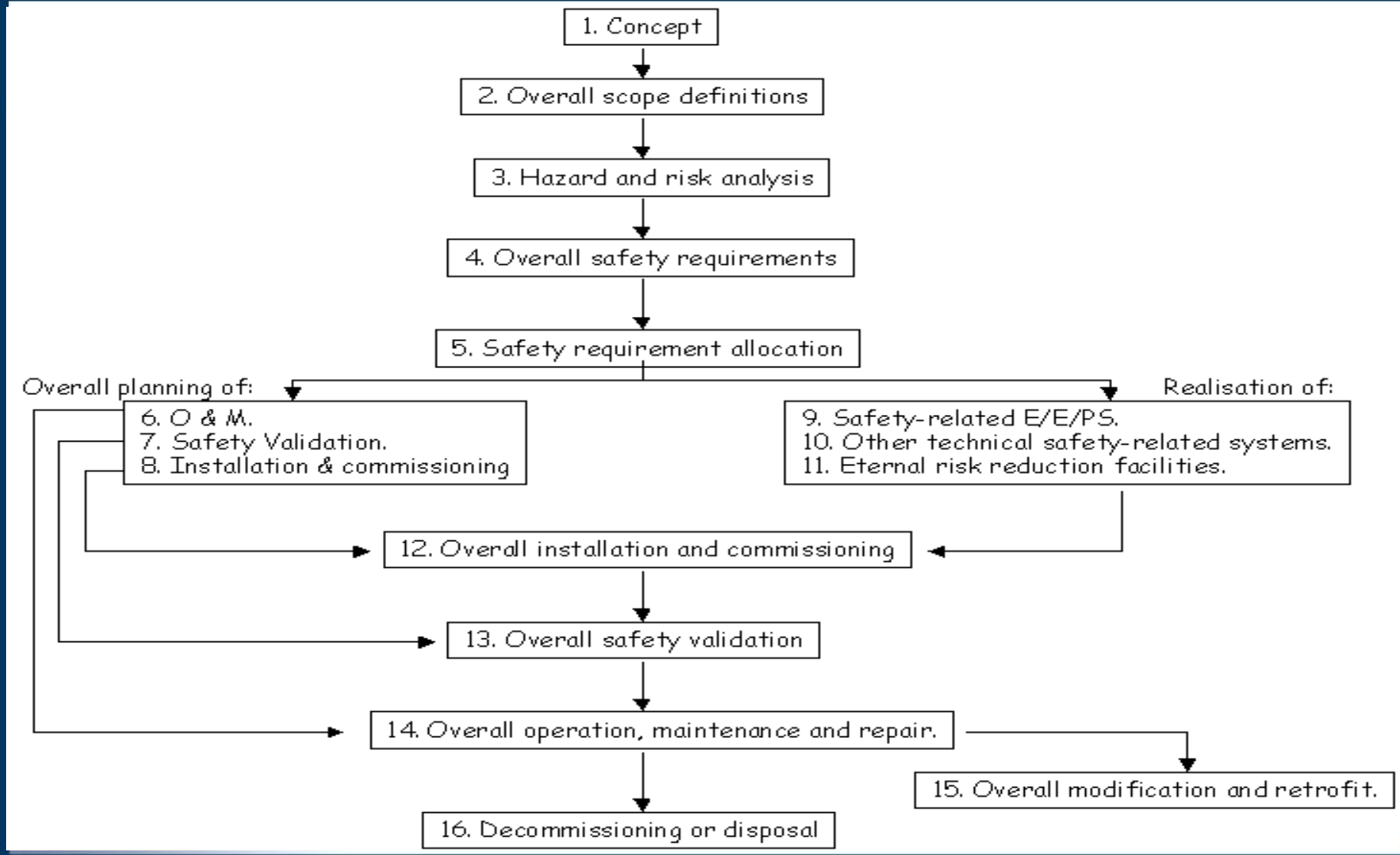
- Equipment Under control (EUC) [3.2.3]: equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.
- EUC risk [3.2.4]: risk arising from the EUC or its interaction with the EUC control system (risk associated with functional safety) [it should be assessed independently of countermeasures to reduce it].
- Tolerable risk [3.1.6]: risk which is accepted in a context based on the current values of society.

University of Glasgow

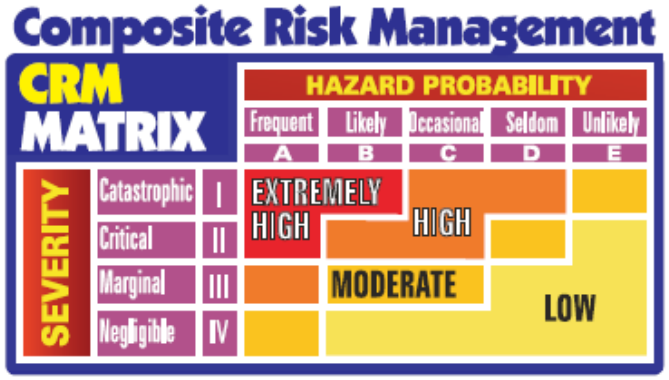
IEC 61508: Risk Reduction



IEC61508: Lifecycle Model



Hazard Identification



- Risk = hazard frequency x cost.
- But numerous paths to hazard
- Deduce frequency of random events
- Human error and software ‘bugs‘?

Hazard Identification

- [1:7.4.2.7] Estimate EUC risk of all hazards.
- [1:7.4.2.8] Quantitative or qualitative techniques.
- [1:7.4.2.12] Must be documented & maintained.
- User must choose the method.

Risk = Frequency x Consequence

Category	Meaning	Occurrences per operational hour
Frequent	Many times in a systems lifetime	> 10^{-3}
Probable	Several times in a systems lifetime	10^{-3} to 10^{-4}
Occasional	Once in a systems lifetime	10^{-4} to 10^{-5}
Remote	Unlikely in a systems lifetime	10^{-5} to 10^{-6}
Improbable	Very unlikely to occur	10^{-6} to 10^{-7}
Incredible	Cannot believe that it could occur	< 10^{-7}

- Can we trust low probabilities?
  - "it has never happened here…"

Risk = Frequency x Consequence

Category	Meaning
Catastrophic	Multiple deaths
Critical	A single death, and/or multiple severe injuries or severe occupational illnesses
Marginal	A single severe injury or occupational illness and/or multiple minor injuries or minor occupational illnesses
Negligible	At most a single minor injury or minor occupational illness.

- Consequences can be subjective?
  - "it could have been worse?"

University of Glasgow

IEC 61508 Risk Classes

- Class I: Intolerable under any circumstance.
- Class II: Undesirable and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained.
- Class III: Tolerable if the cost of risk reduction would exceed the improvement gained.
- Class IV: Negligible.
- As Low As Reasonably Practicable?

University of Glasgow

Safety Integrity Levels: The Key Idea…

- Risk analysis guides risk reduction.
  - By the allocation of development resources.
- A Class 1 (Intolerable) risk usually
  - requires software coded to SIL4 (highest) level.
- A Class 2 (Undesirable) risk might
  - Require software coded to SIL2/3 levels.
- Higher SILs require more resources…

University of Glasgow

IEC 61508 Definitions: SILs

- Safety-integrity [3.5.2]: probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

- Safety integrity level [3.5.6]: discrete level (one out of a possible four) for specifying the safety integrity requirements... where SIL 4 has the highest level of safety integrity and SIL 1 the lowest.

University of Glasgow

Safety Integrity Levels

- Using a recommended process for a particular SIL doesn't guarantee that your systems meets the reliability requirement of that SIL.

- Circular argument...
  - Cant measure software failure rate.
  - So use a recommended process...
  - Can we measure success of process?

University of Glasgow

Documentation

- [1:5.2] Requirements documentation should be:
  - sufficiently informative;
  - available;
  - accurate and concise;
  - easy to understand;
  - fit for purpose.
- [1:6.2.1 d] Management specifies `the ways in which information is to be structured and the extent to which information is to be documented'
- All activities to be documented & documents maintained.

University of Glasgow

Open Issues

- How do you:
  - demonstrate conformance?
  - ensure independent reviews?
  - control costs of following standard?
- Projects drowning in a sea of paper:
  - Teams afraid to make changes…
- Empirical evidence on benefits of standards?

University of Glasgow

Conclusions

- Safety culture not enough.
- Standards offer guidance.
- IEC 61508 case study.
- Is this enough?
  - Process versus product approaches…
  - On-going debate, standards will change...

University of Glasgow

Any Questions…