Reliability and Safety Assessment in Offshore and Process Industries

PSAM 7 / ESREL ´04

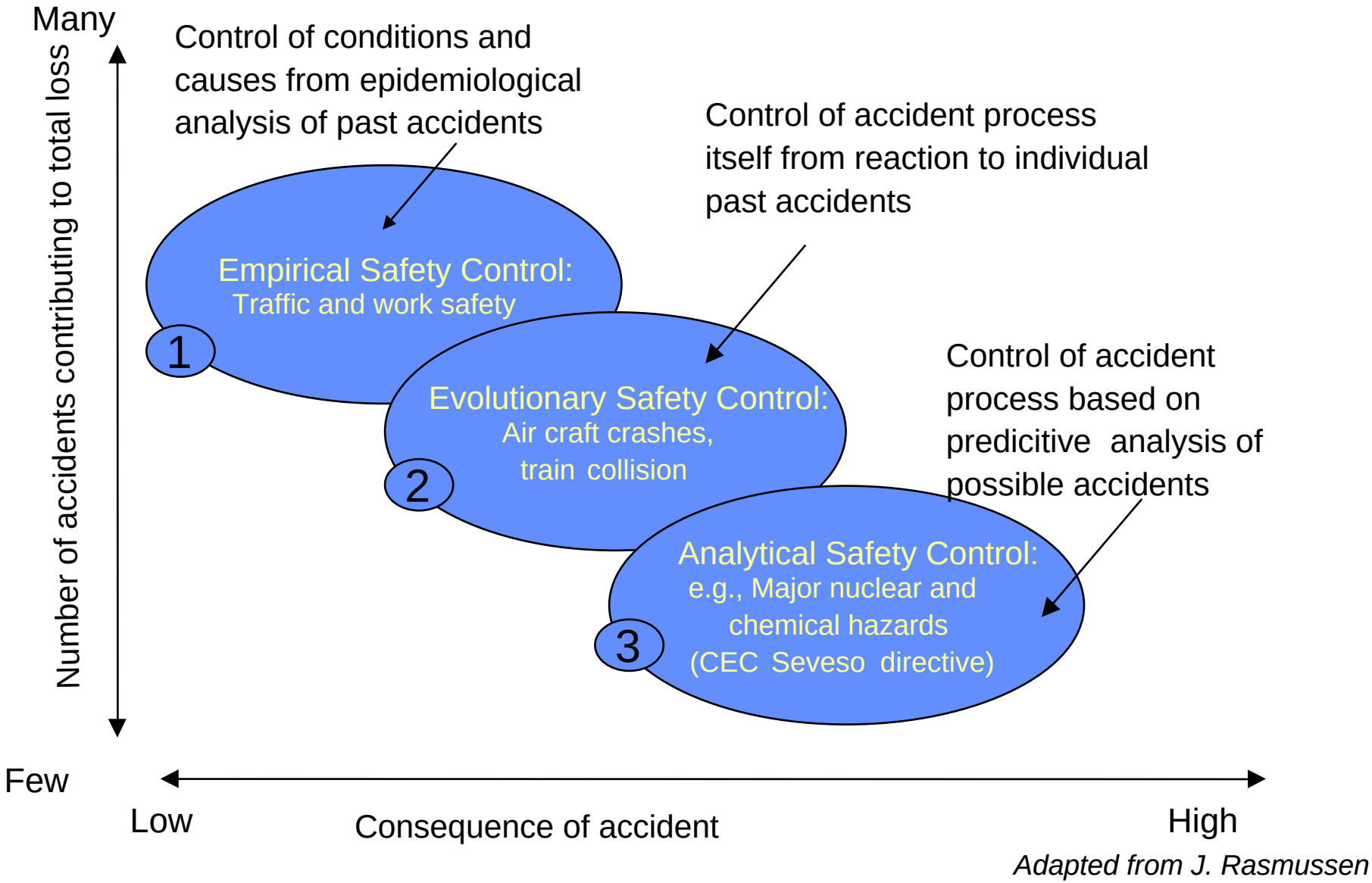
Berlin, Germany

Lars Bodsberg
SINTEF, Trondheim, Norway

”All models are wrong!
Some are useful.”

(G.E. Box)

Safety Management Principles



Adapted from J. Rasmussen


© Norsk Hydro

IEC 61508 and IEC 61511

- The International standard IEC 61508: *Functional safety of electrical/-electronic/programmable electronic (E/E/PE) safety-related systems“*
  (7 parts)
  - *Generic standard*

- The International standard IEC 61511: *Functional safety – Safety instrumented systems for the process industry sector (3 parts)*
  - *Sector specific standard*

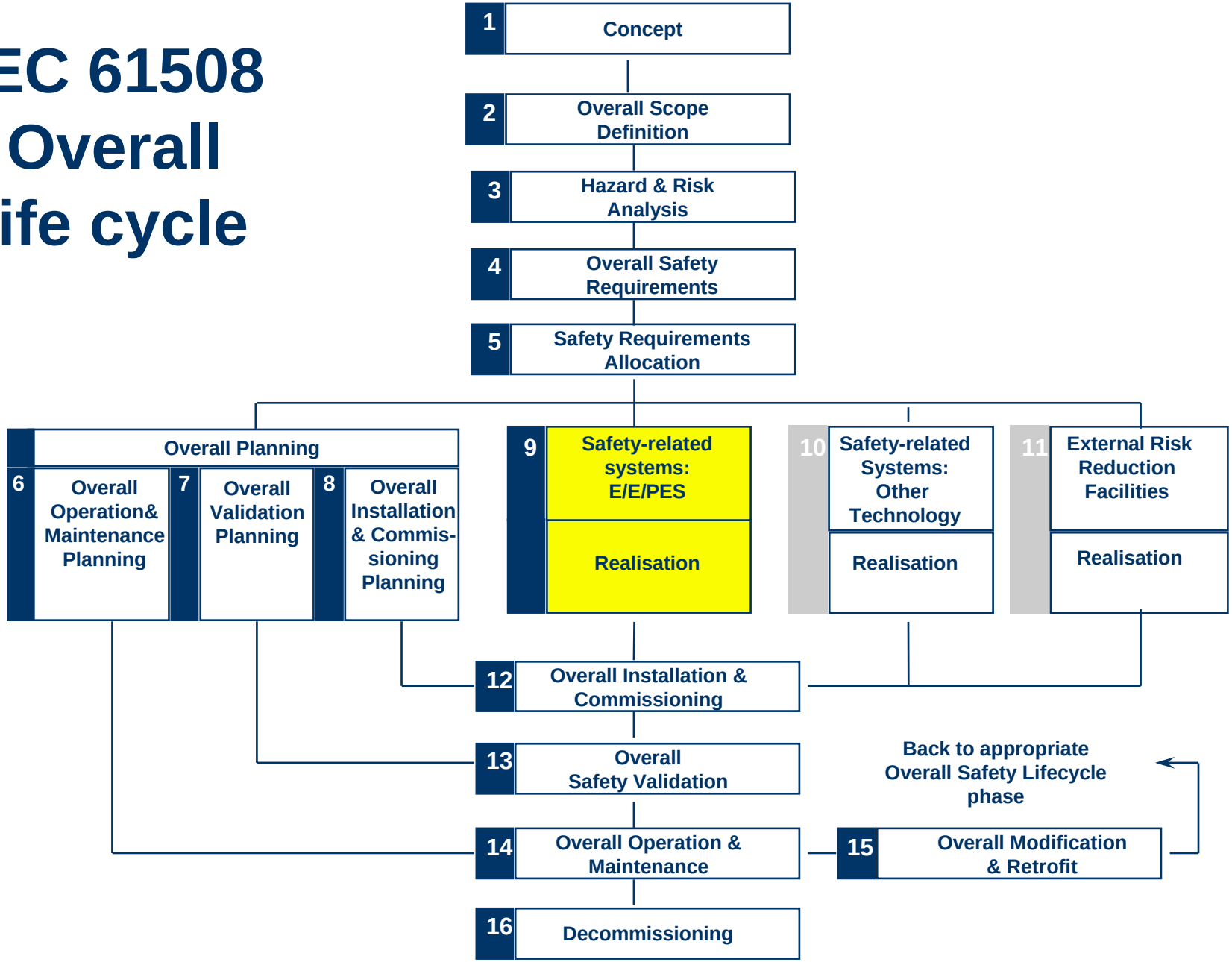
Widespread use of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry

- The Petroleum Safety Authority Norway recommends the use of IEC 61508
- The Norwegian Oil Industry Association (OLF) provides financial support to a joint industry project between operators and the various suppliers of services and equipment to establish a guideline
- Guideline published at: www.itk.ntnu.no/sil

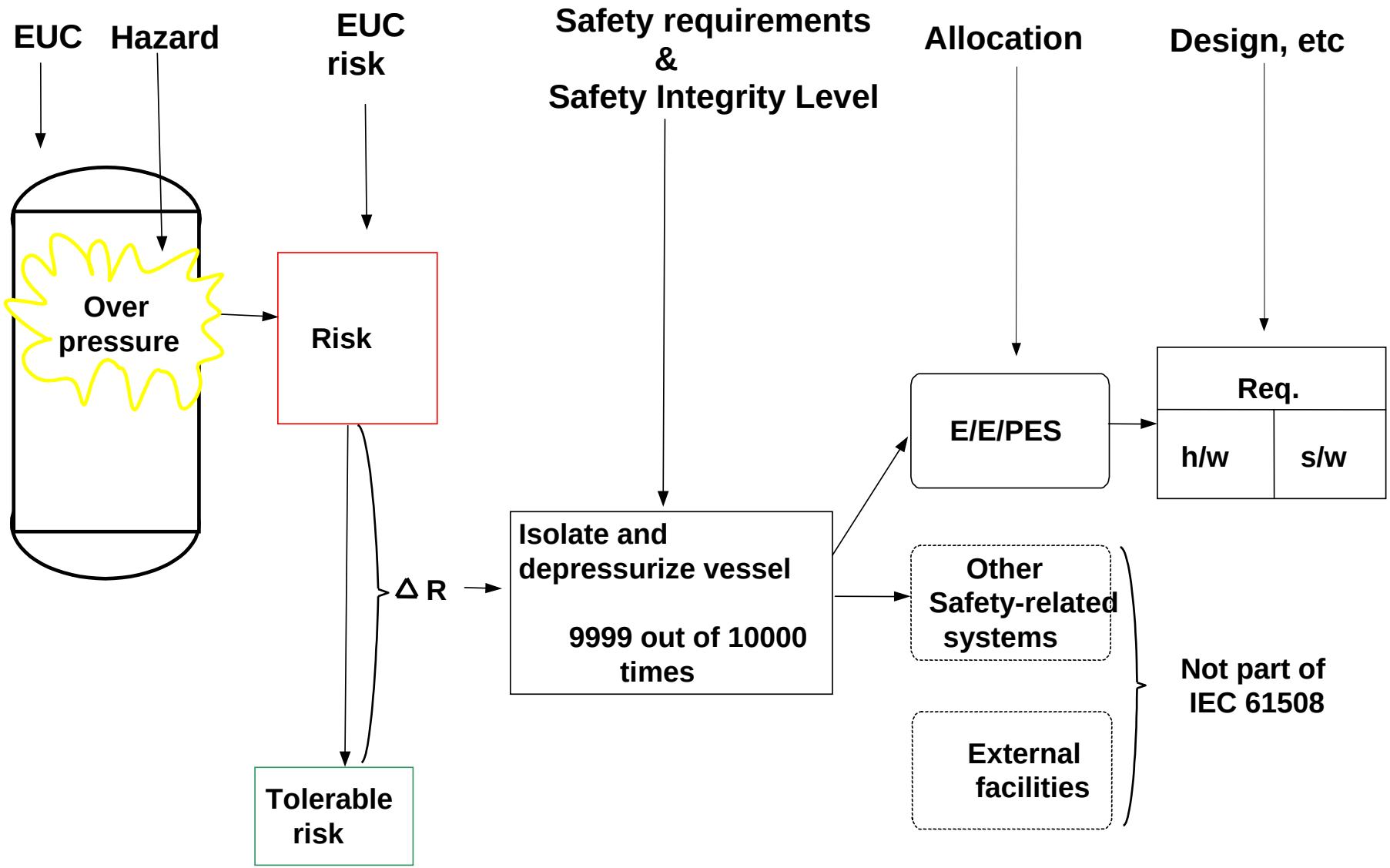
IEC 61508: *Functional safety of electrical/-electronic/programmable electronic (E/E/PE) safety-related systems“*

- Generic standard, i.e.:
  - Providing general framework, covering a wide range of complexity, hazards and risk potentials
  - Conceived with a rapidly developing technology in mind - framework sufficiently robust and comprehensive
- Major objective:
  - Facilitate development of sector specific standards
  - Provide consistency within and across application sectors
  - Provide a generic approach for all lifecycle activities
  - Provide qualitative and quantitative safety requirements to safety systems

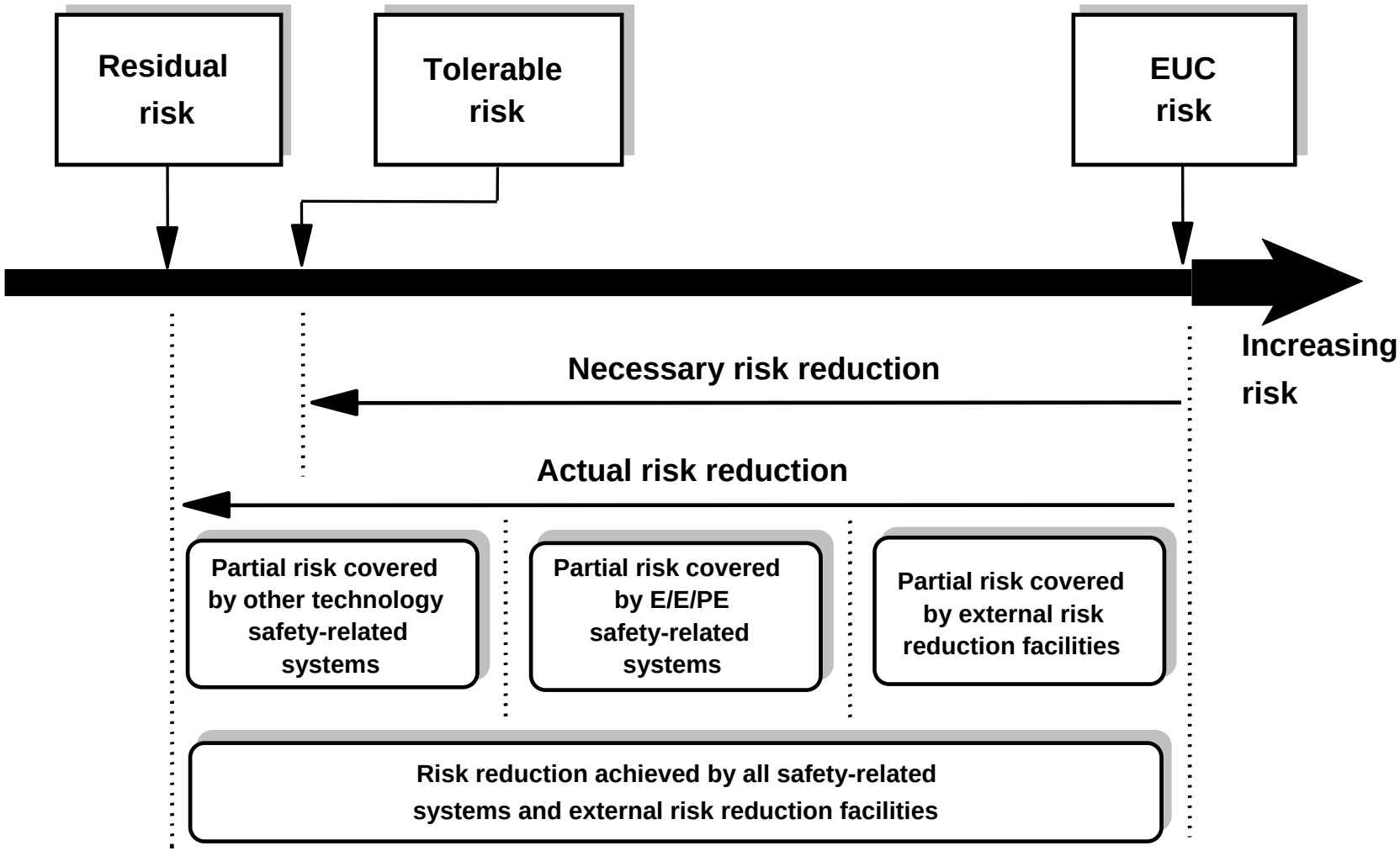
IEC 61508 Overall life cycle



Development of Safety System Requirements



Risk reduction in IEC 61508 - General concept



Source: IEC 61508

Safety Integrity Level - SIL

SAFETY INTEGRITY LEVEL - SIL	DEMAND MODE OF OPERATION (Probability of Failure on Demand - PFD)	CONTINUOUS/HIGH DEMAND MODE OF OPERATION (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

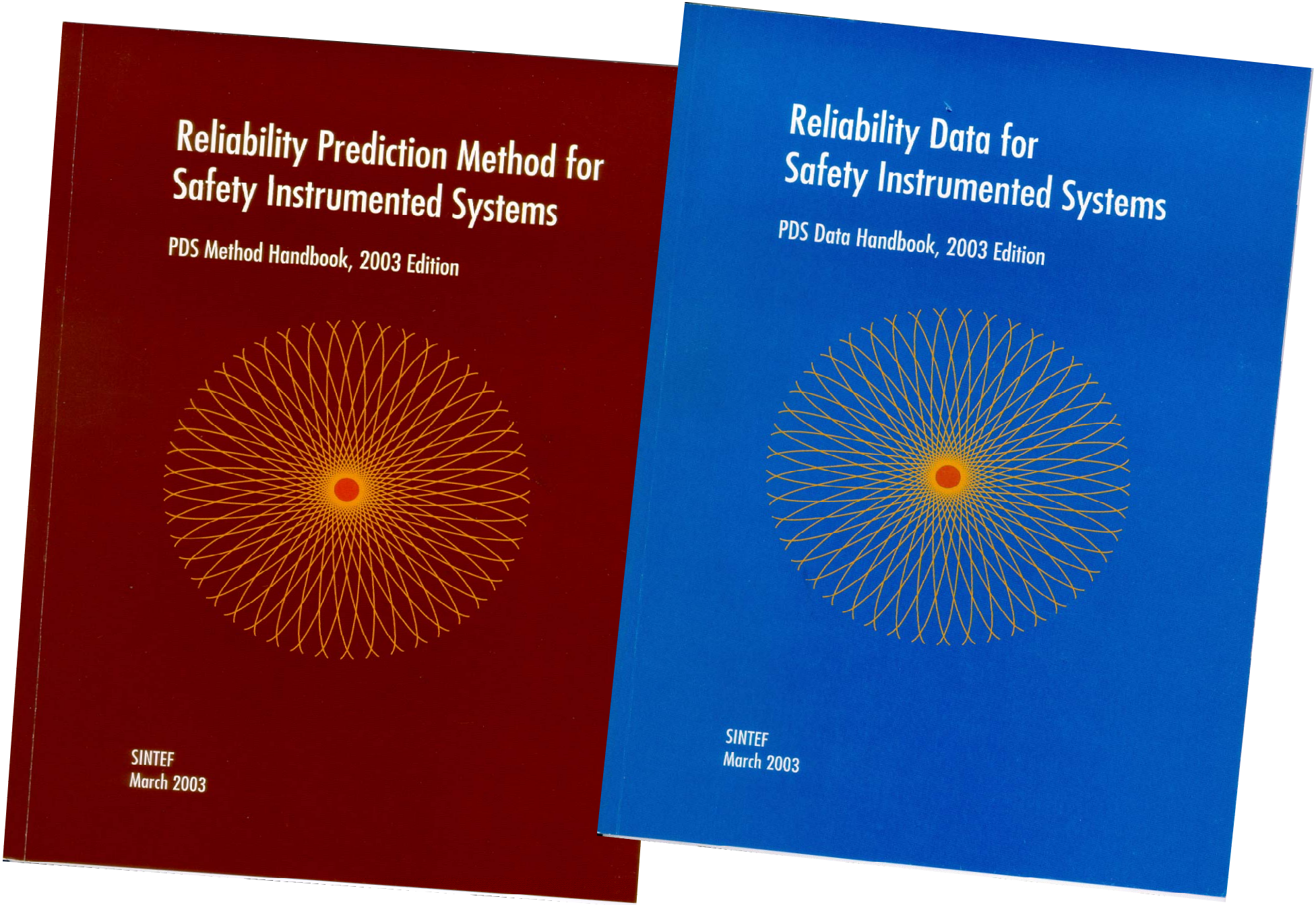
IEC 61508 implications on safety and reliability modelling

- The IEC 61508 standard sets out a risk-based approach for deciding the Safety Integrity Level (SIL) for systems performing safety functions
  - On-going R&D to improve QRAs in Norway.
- The IEC 61508 standard requires evaluation of reliability performance of the safety instrumented systems
  - The PDS method

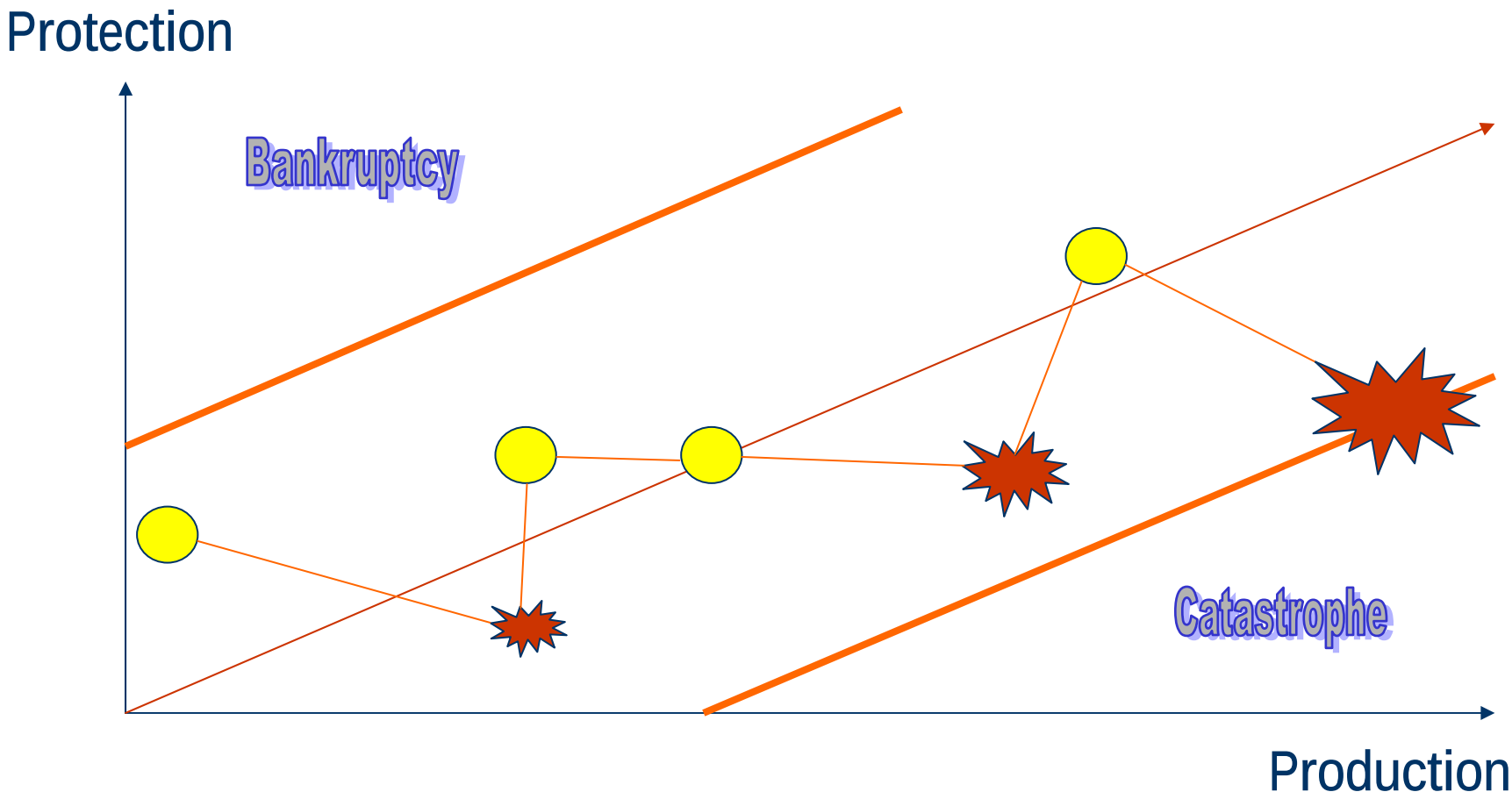
Comparison PRA vs. QRA

Topic	PRA	QRA
Initiating events	Root cause analysis of initiating events presented in fault trees. Identification of common cause initiators (CCIs). Predefined lists and handbooks.	No root cause analysis No CCI assessment Predefined categories of leakage Frequencies based on counting leakage point, or platform data.
Fault tree/ event tree analysis (system modeling)	Detailed modeling Support systems explicitly modeled. Link between event trees and fault trees. (Time-dependent models for living PSA).	Rough model Support systems not included Only partly use of fault trees No linking of event and fault trees.
Data and parameter estimation	Best estimates and confidence intervals. Classical and Bayesian framework. 'Weighted' plant-specific data	Best estimates Generic data and separate plant-specific data
Human reliability	Thorough analysis of important human actions (e.g. by THERP, SHARP, etc.).	Almost non-existing
Dependencies	Partly inherent in models Separate dependency analysis Regarded as crucial	Partly inherent in models No separate analysis
Uncertainty	Always included, at least qualitatively. Regarded as important	Absent
External events	Covers some external events Linked to the 'internal' event	Covers many external events Separate analysis (Limited modeling effort)
Results	Best estimate and uncertainty in short and long term fatalities. Cumulative distribution functions.	Single best estimate FAR-, and PLL-values

Reliability Assessment of Safety Instrumented Systems – the PDS Method

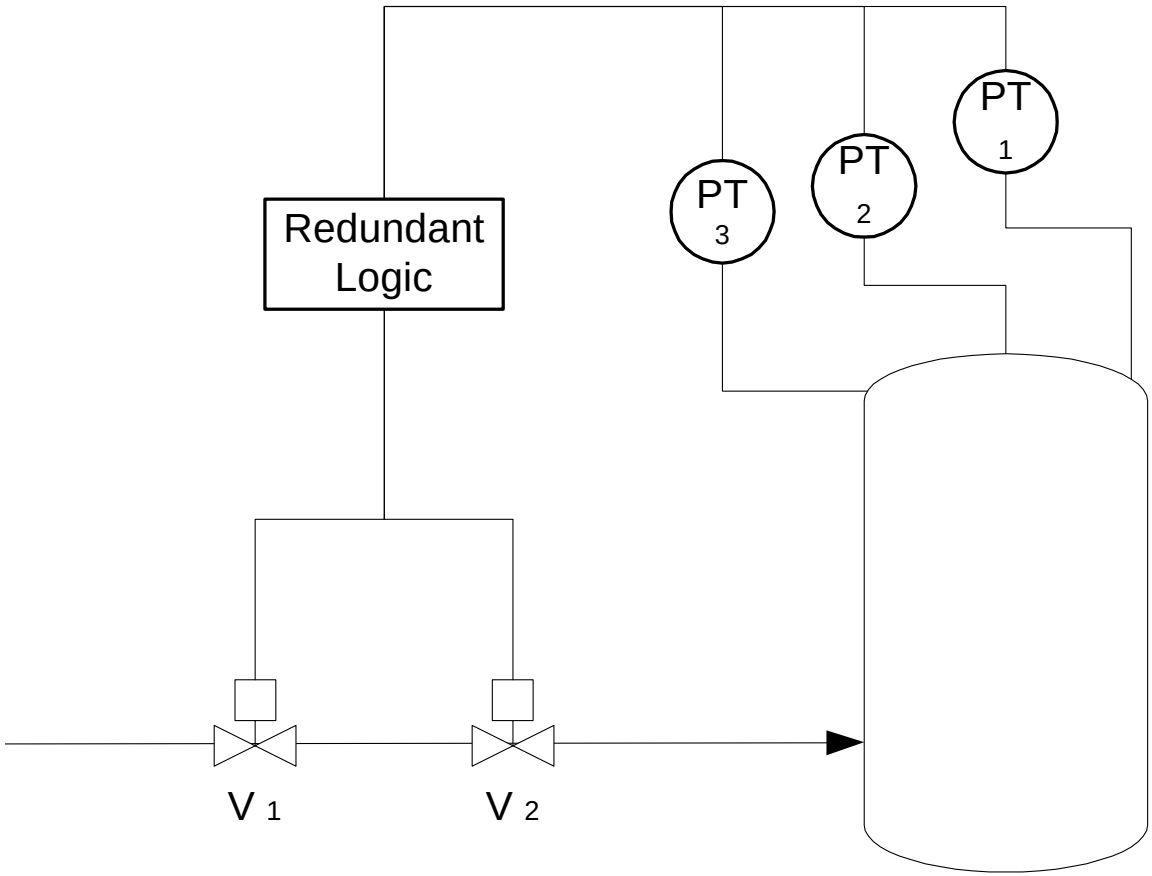

Reliability Prediction Method for Safety Instrumented Systems
PDS Method Handbook, 2003 Edition
SINTEF
March 2003
Reliability Data for Safety Instrumented Systems
PDS Data Handbook, 2003 Edition
SINTEF
March 2003

Balance between production and protection

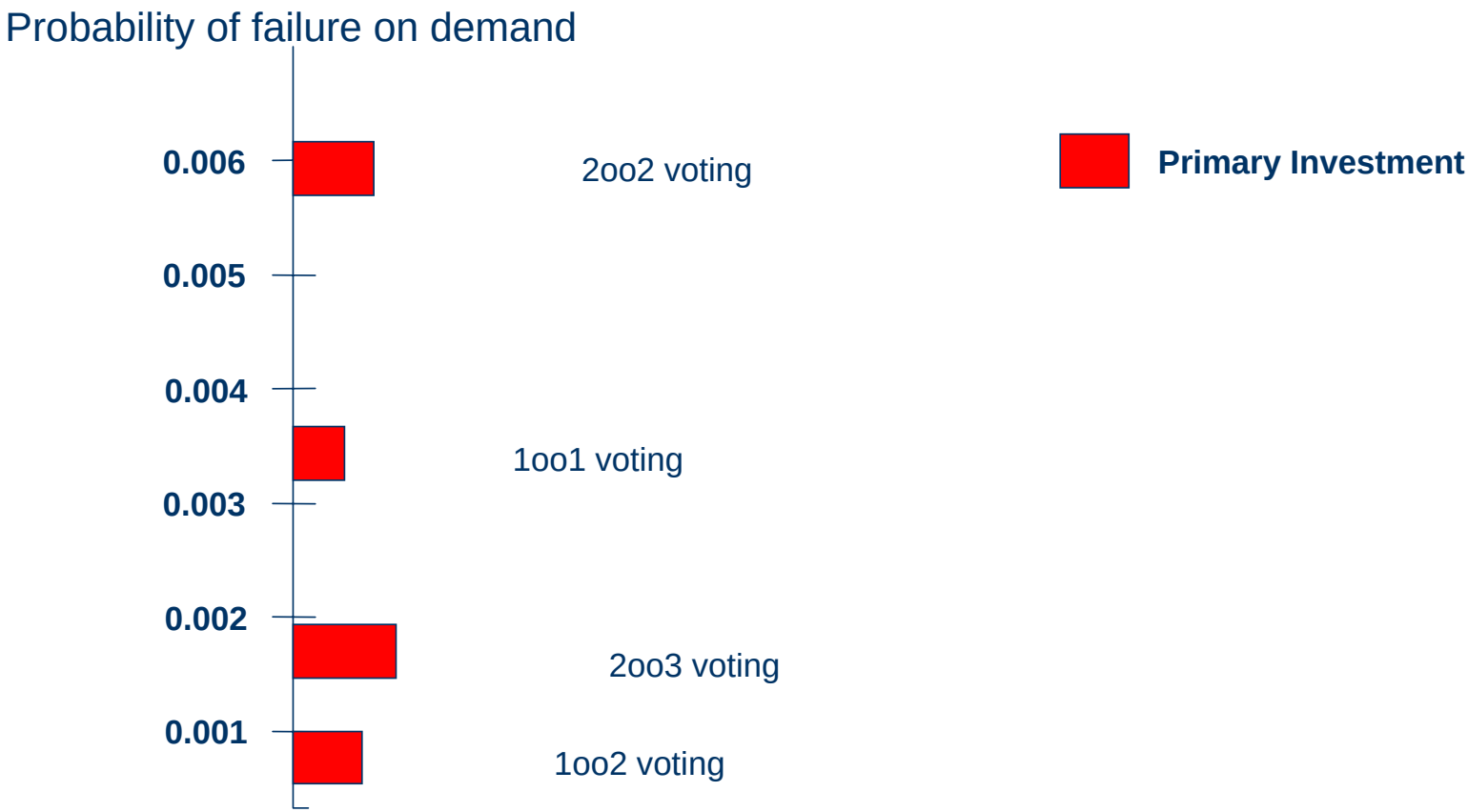


Reason (1998)

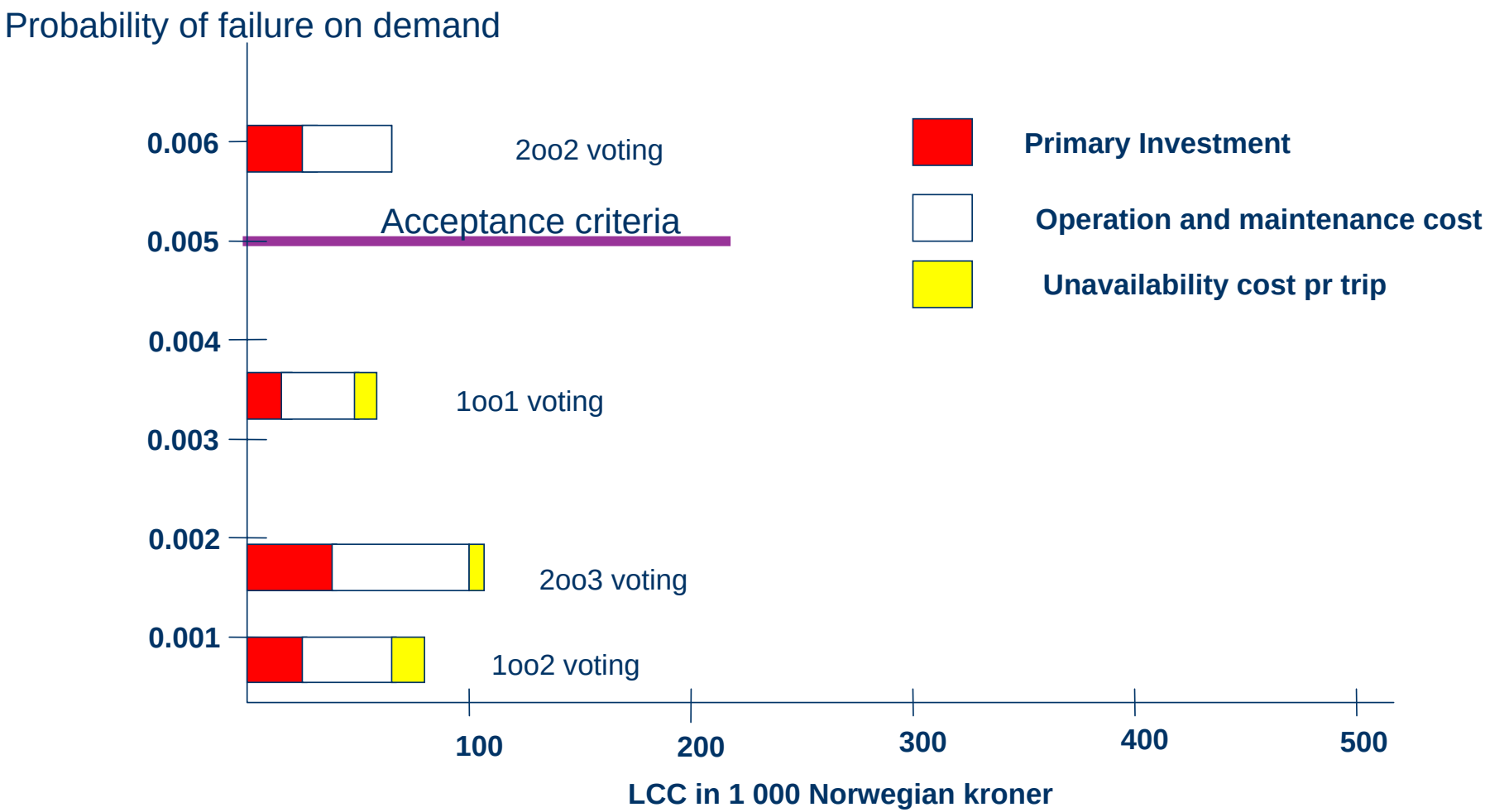
High Integrity Pressure Protection System (HIPPS)



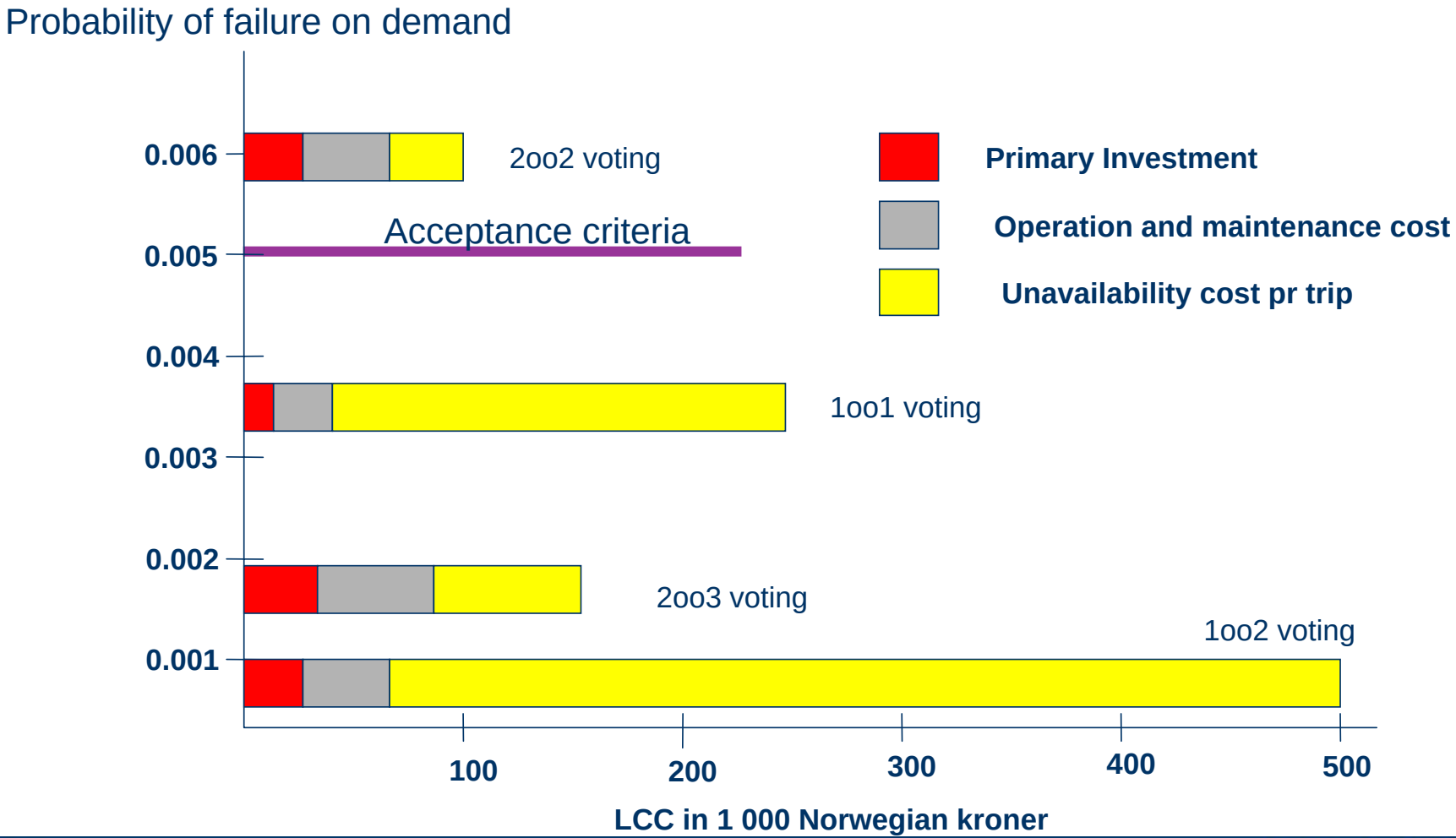
Safety performance – voting logic



Safety vs. LCC – Low Unavailability Cost pr Trip

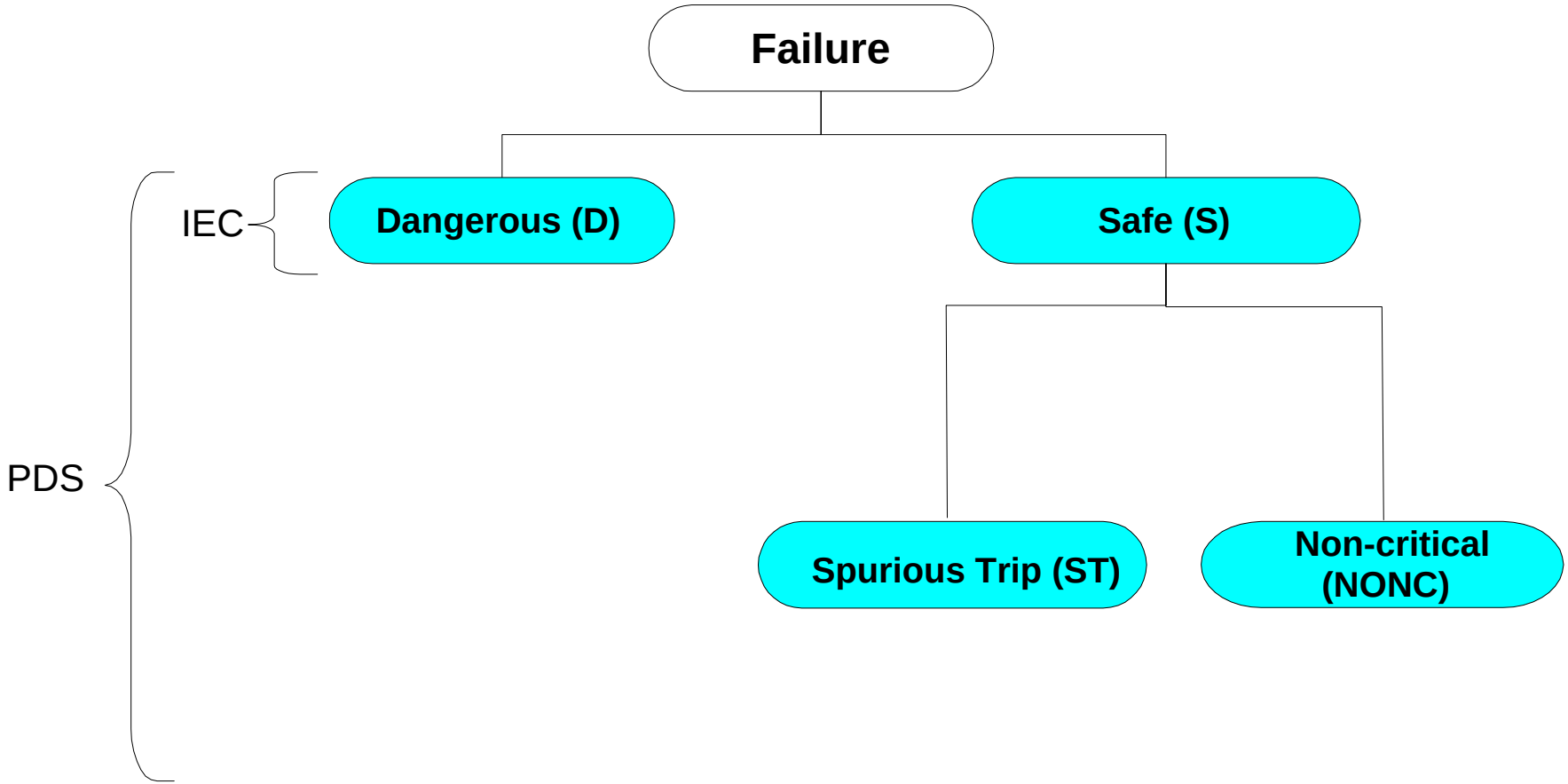


Safety vs. LCC – High Unavailability Cost pr Trip



Gareth Morgan

Failure *Mode* Classification in PDS and IEC

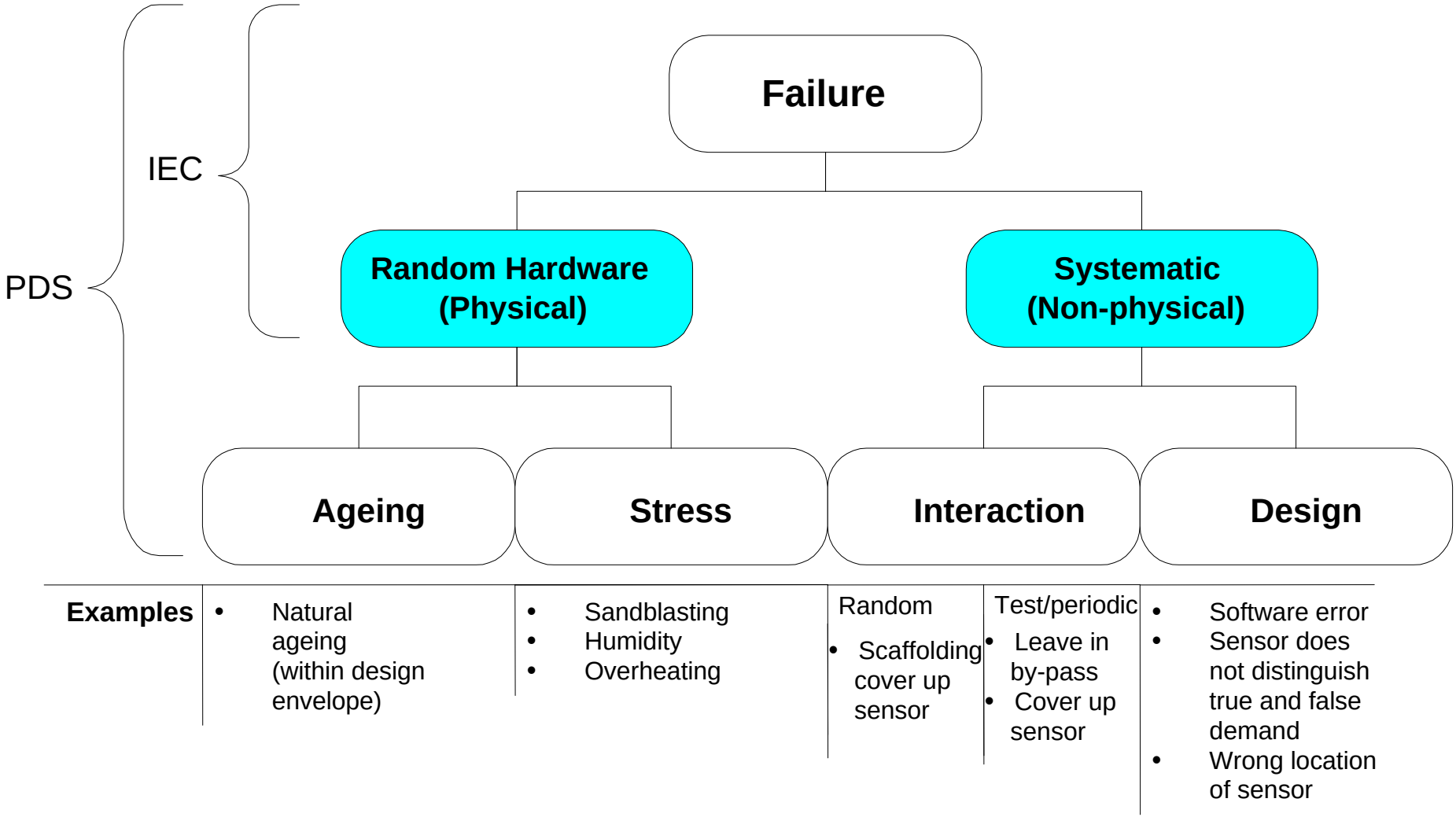


Main Failure Modes in PDS

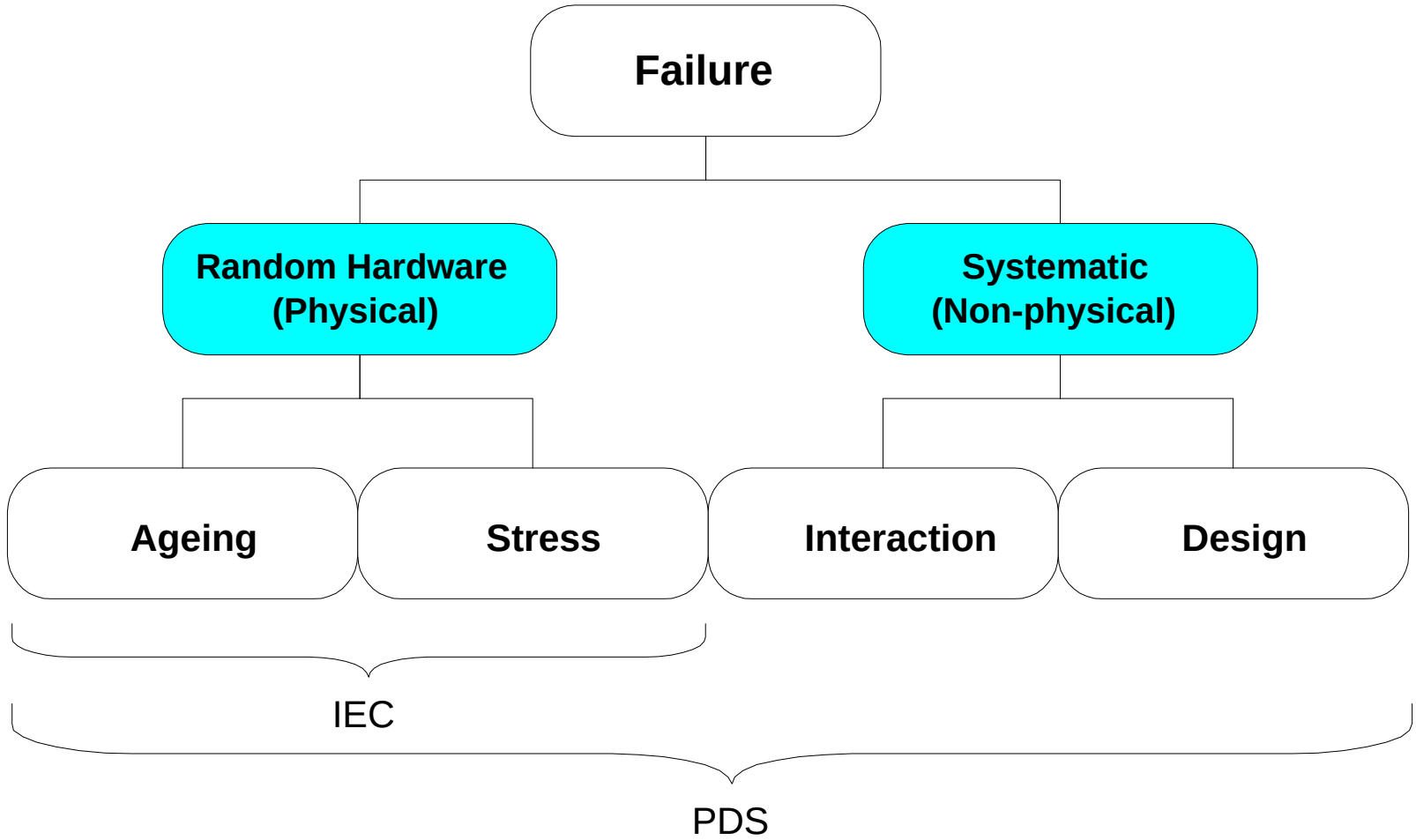
- Dangerous (D)
  - Safety system/module does not operate on demand
    (e.g. sensor stuck upon demand)
- Spurious Trip (ST)
  - Safety system/module operates without demand
    (e.g. sensor provides signal without demand)
- Non-Critical (NONC)
  - Main functions not affected
    (e.g. sensor imperfection which has no direct effect on control path)

✓ The IEC standard does not distinguish between *ST* and *NONC* failures; both are referred to as *Safe* failures

Failure *Cause* Classification in PDS and IEC



Loss of Safety Quantification in PDS and IEC

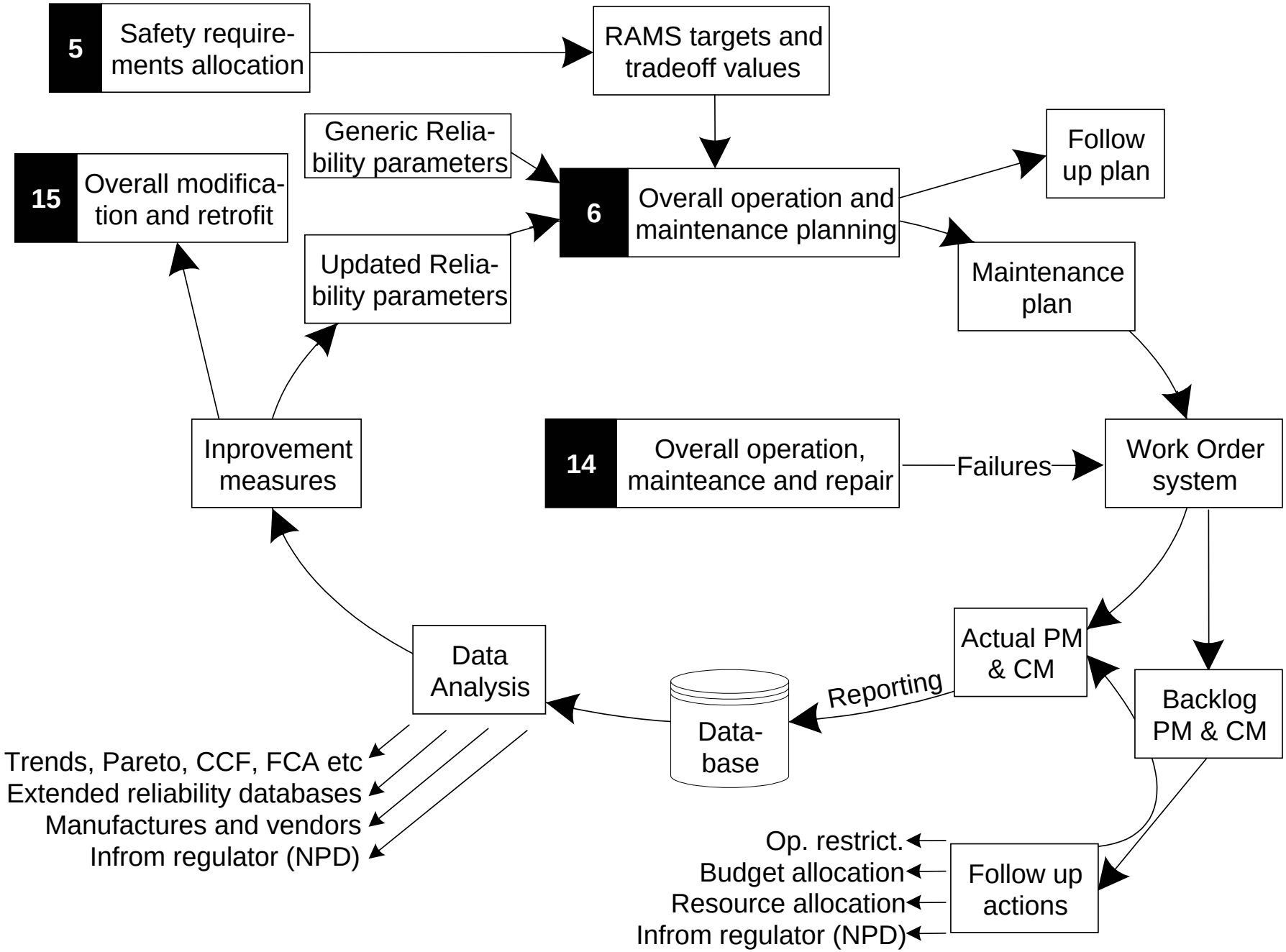


Reliability Performance Measures

- Loss of safety.
  - Critical Safety Unavailability (CSU):
    "The probability that the safety system will fail to automatically carry out a successful safety action on the occurrence of a hazardous/-accidental event"
  - *Probability of Failure on Demand (PFD):*
    That part of CSU which is caused by random hardware failures IEC
- Loss of production regularity.
  - Spurious Trip Rate (STR):
    "The mean number of spurious activations of the safety system per unit time"
- Maintenance activity.
  - *Mean Corrective Maintenance (MCM):*
    "The mean number of man-hours spent on CM per year"
  - *Mean Preventive Maintenance (MPM):*
    "The mean number of man-hours spent on PM per year"

Loss of Safety Calculations - Example

Component	PFD	PSF	CSU
	Random hardware	Systematic	Total
PT (1oo2)	$1.1 \cdot 10^{-5}$	$3.6 \cdot 10^{-5}$	$4.7 \cdot 10^{-5}$
Logic (1oo2)	$0.2 \cdot 10^{-5}$	$2.5 \cdot 10^{-5}$	$2.7 \cdot 10^{-5}$
V (1oo2)	$11.8 \cdot 10^{-5}$	$0.03 \cdot 10^{-5}$	$11.8 \cdot 10^{-5}$
Total	$13.1 \cdot 10^{-5}$	$6.1 \cdot 10^{-5}$	$19.2 \cdot 10^{-5}$


5
Safety require-ments allocation
RAMS targets and tradeoff values
Generic Relia-bility parameters
15
Overall modifica-tion and retrofit
6
Overall operation and maintenance planning
Follow up plan
Updated Relia-bility parameters
Maintenance plan
Inprovement measures
14
Overall operation, mainteance and repair
Failures
Work Order system
Actual PM & CM
Data Analysis
Reporting
Backlog PM & CM
Data-base
Trends, Pareto, CCF, FCA etc
Extended reliability databases
Manufactures and vendors
Infrom regulator (NPD)
Op. restrict.
Budget allocation
Resource allocation
Infrom regulator (NPD)
Follow up actions

Summary

- Risk-based approach adopted in Norwegian offshore production
- Widespread application of the IEC 61508 standard
- Requirements to safety functions can normally not be obtained directly from the Quantitative Risk Analysis (QRA) as it is performed today.
- Cooperation between regulatory authorites, industry and R&D to establish guideline document for IEC 61508
- Ongoing research to improve QRA
- Reliability analysis should support the balance between production and protection

IEC 61508 and 61511 – Lessons learned

- Provides good framework for design, implementation and operation of safety-related systems
- Sensible risk-based approach, however in an area, and at a level of detail, which is not yet very mature
- Difficult to apply for
  - systems involving several vendors
  - “global functions”

”All models are wrong!
Some are useful.”

(G.E. Box)

References

- **Reliability Prediction Method for Safety Instrumented Systems; PDS Method Handbook, 2003 Edition**
  Published by SINTEF (www.sintef.no/pds) and distributed by Sydvest (www.sydvest.com)

- **Reliability Data for Safety Instrumented Systems; PDS Data Handbook, 2003 Edition**
  Published by SINTEF (www.sintef.no/pds) and distributed by Sydvest (www.sydvest.com)

- **Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry**
  Published at www.itk.ntnu.no/sil

Lars Bodsberg
Ph.D - Research Director

SINTEF, Safety and Reliability
N-7465 Trondheim

Telephone: +47 73 59 27 58
Telefax: +47 73 59 28 96
http://www.sintef.no