Industrial Embedded Systems
- Design for Harsh Environment -

Dr. Alexander Walsch
alexander.walsch@ge.com

WS 2011/12

Technical University Munich (TUM)

Agenda

Today:

Safety

Recap:

- Requirements Analysis (Definition, Specification)
- Reliability, availability, maintainability

From Reliability to Safety

- Reliability has been defined as the probability of system function survival.
  “deliver a specified functionality under specified condition for a specified period of time”
- Requirements analysis usually dictates to deliver very reliable systems. We defined the MTBF as a metric for reliability.
- But: there are circumstances where either continuous delivery or failure could lead to severe consequences for people, assets or the environment.
- Safety is about analyzing these circumstances, detecting them in a reliable way, and executing a defined method such that the system is free from not acceptable risk of being dangerous.

Motivation

- In recent considerations (reliability) we have not considered systematic failures.
- Therac 25 (1985-87, N. America) radiation therapy machine: severe radiation overdose caused by software failure
- Ariane 5 (1996) software exception causes self-destruct
- Links
  - http://en.wikipedia.org/wiki/List_of_software_bugs
  - http://catless.ncl.ac.uk/Risks
  - http://www.csl.sri.com/users/neumann/illustrative.html
  - http://wwwzenger.informatik.tu-muenchen.de/persons/huckle/bugse.html
  - http://page.mi.fu-berlin.de/prechelt/swt2/node36.html

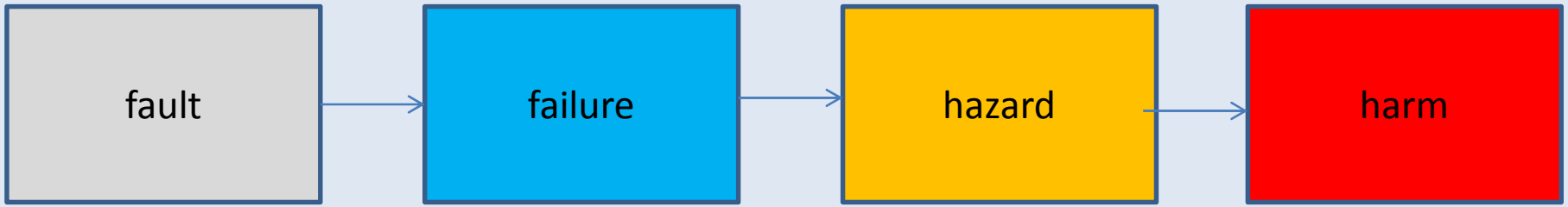
Hazards and Harm

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
[ISO/IEC Guide 51:1990 (modified)]

Hazard

potential source of harm. Hazard is a system state resulting from a failure.
[Guide 51 ISO/IEC:1990]



Risk

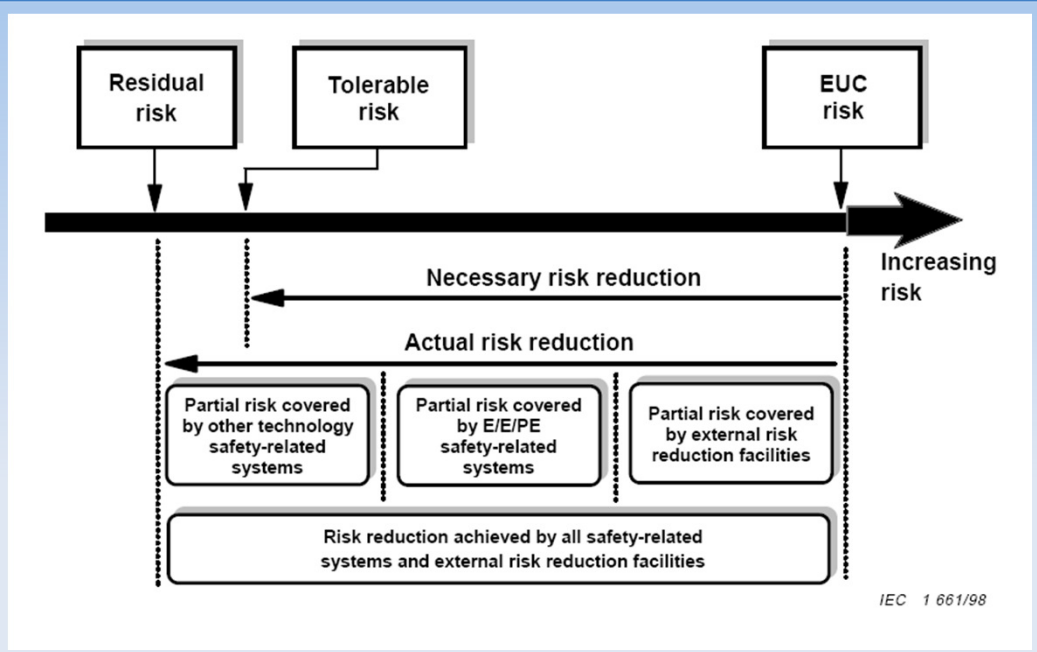
Risk
a measure of the probability and consequence of a specified hazardous event

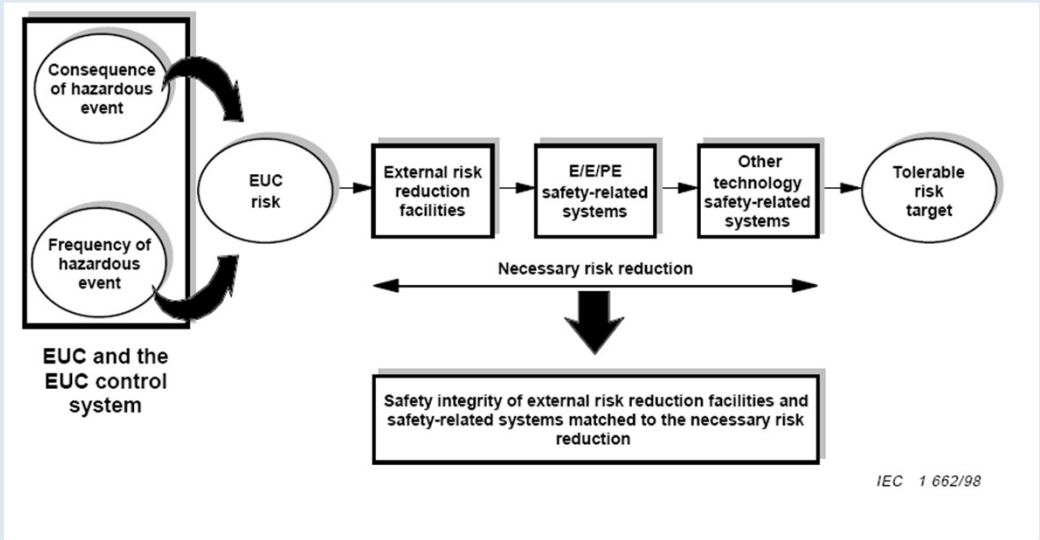
Tolerable Risk
determined on a societal basis and involves consideration of societal and political factors (the tolerable risk for running nuclear power plant changed recently – but not the probability of failure!)

Residual Risk
risk remaining after protective measures have been taken

Risk assessment is necessary to phrase the missing safety requirements for the requirements specification.

Risk and Risk Reduction (IEC61508)





EUC (from IEC61508):
System under control
E/E/PE (from IEC61508):
Electrical/electronic/programmable electronic system

Source:
IEC61508

Quantitative Risk Assessment Overview

Risk = Probability x Consequence

Maximum tolerable risk of fatality	*Individual risk (per annum)*
Employee	10^{-4}
Public	10^{-5}
Broadly acceptable risk (previously referred to as 'Negligible' (Employee and public))	10^{-6}

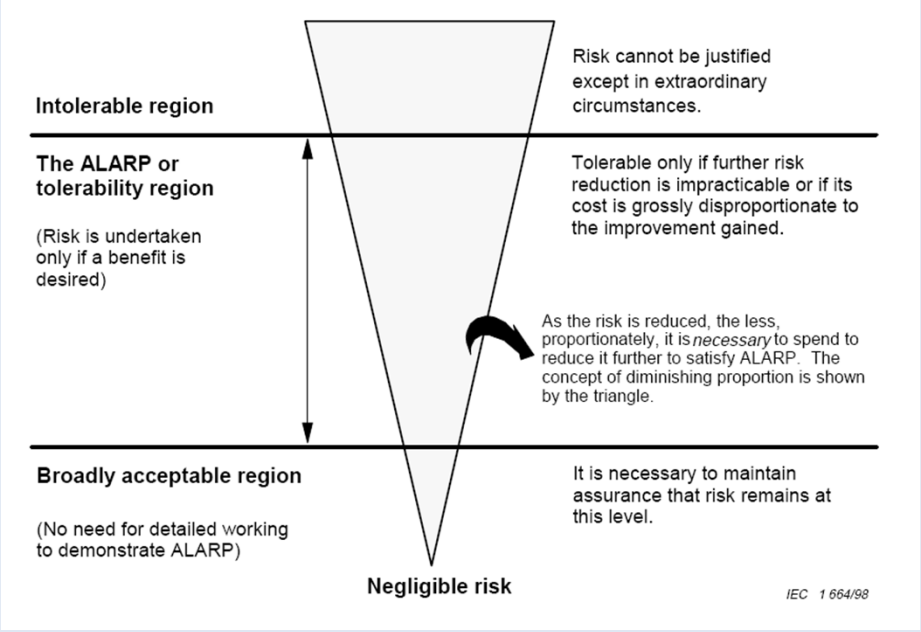
Catastrophic
Critical
Marginal
Negligible

Source:
Smith, Functional Safety

What are the hazards (state of the system)?, What is the frequency of occurrence (rate, probability)?, What are the consequences (harm)?

Tolerable Risk - ALARP

- ALARP-Prinzip: „As Low As Reasonably Practicable“
  - the risk is so great that it must be refused altogether, or
  - the risk is, or has been made, so small as to be insignificant, or
  - the risk falls between the two states specified in a) and b) above and has been reduced to the lowest practicable level, bearing in mind the benefits resulting from its acceptance and taking into account the costs of any further reduction.



Source: IEC61508

Example

The maximum tolerated fatality (harm) rate (one person dies) of a system has been decided to be 10^{-5} pa (ALARP, discussions). 10^{-2} of the hazards under investiogation leed to harm. From an independent assessment we know that the system as built today (no additional risk reduction) fails at 2×10^{-1} pa.

(a) Do we need an additional safety system?

(b) What quality (failure rate, etc.) must an additional safety system have if mandatory?

Quantitative Risk Assessment

Tolerated risk:

Risk = C x F; C = consequence, F = failure rate

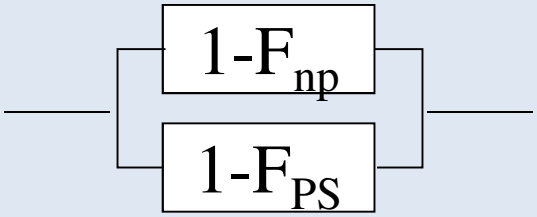
F = Risk/C = 10^{-5} pa/10^{-2} = 10^{-3} pa (tolerated failure rate)

(a) yes, we need an additional risk reduction since the failure rate of 10^{-3} pa is less than what we can achieve currently (2 x 10^{-1} pa)

(b) To minimize the risk the failure rate of an improved system must be addressed. Failure rate reduction can be achieved my means of redundancy (last lecture).

Quantitative Risk Assessment – Ctd.

In reliability calculations we looked at „survival“ of a function. Now, in risk calculations, we look at failure of a function.
But: $R = 1 - F$
All calculations from last lecture can be reused. Instead of reliability we look into failure. However, the failure rate for the not-protected (F_{np}) system and the protection system (F_{ps}) are different. Reliability diagrams can be used calculate the failure rate of the protected system (F_{PS}).

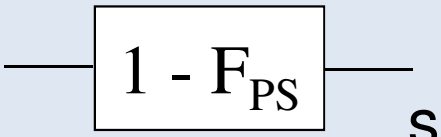


from $R_P = 1 - (1-R_{ps})(1-R_{np})$

$R_p = 1 - F_{ps} \times F_{np}$
$F_p = F_{ps} \times F_{np} \rightarrow F_{ps} = F_p/F_{np} = 10^{-3}\ pa/2 \times 10^{-1}\ pa = 5 \times 10^{-3}$ (PFD)

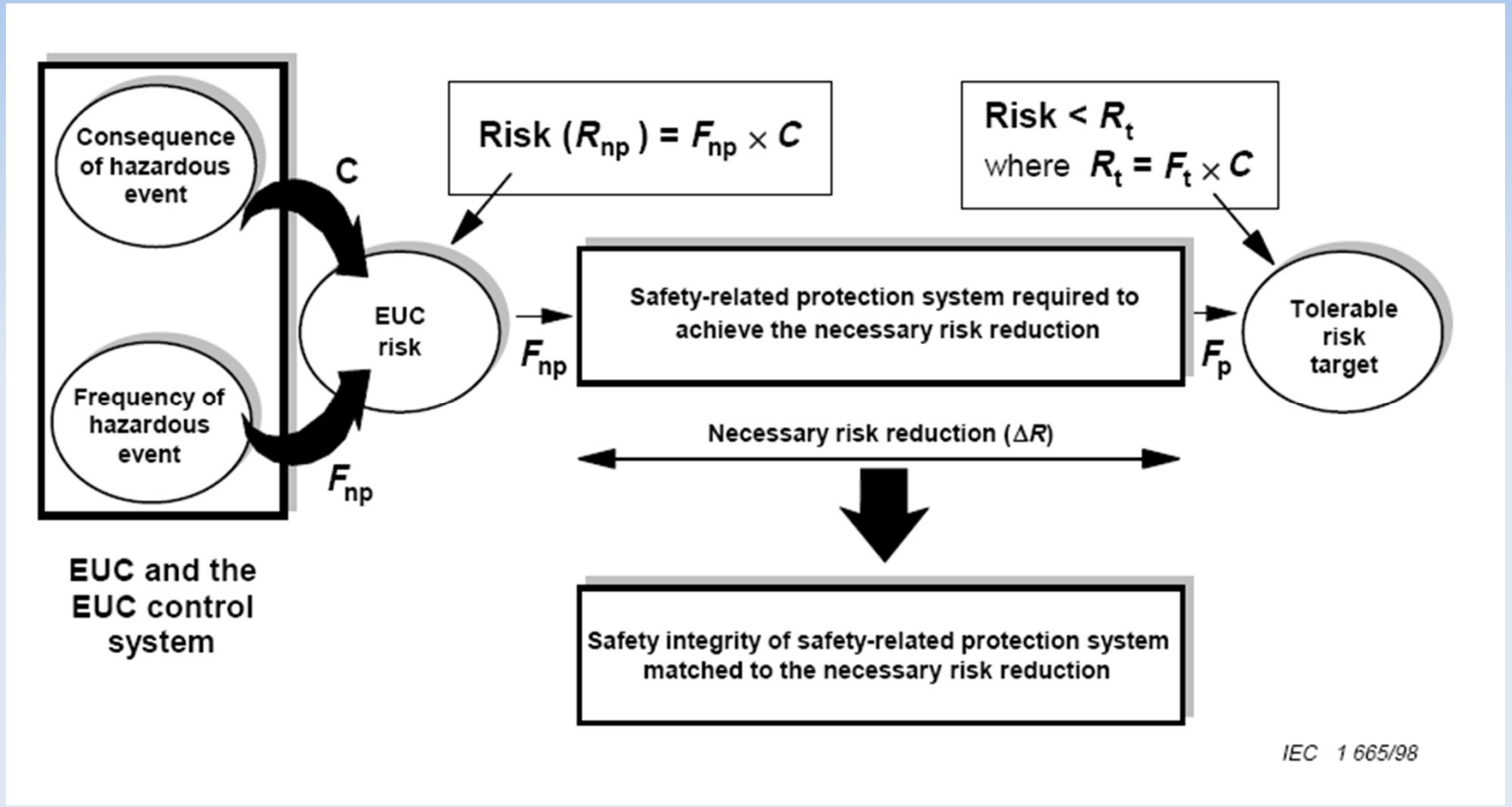
Quantitative Risk Assessment – Ctd.

- In the previous slide we have been looking at a system in full active redundancy configuration (not protected system having some kind of insufficient safety function and a protection system running in parallel).
- Most highly integrated systems combine the protection system and the not-protected system on one physical entity (processor). Therefore, it must be modelled in series reliability configuration. The not-protected system is not modelled in the reliability diagram since it does not have a protection function.



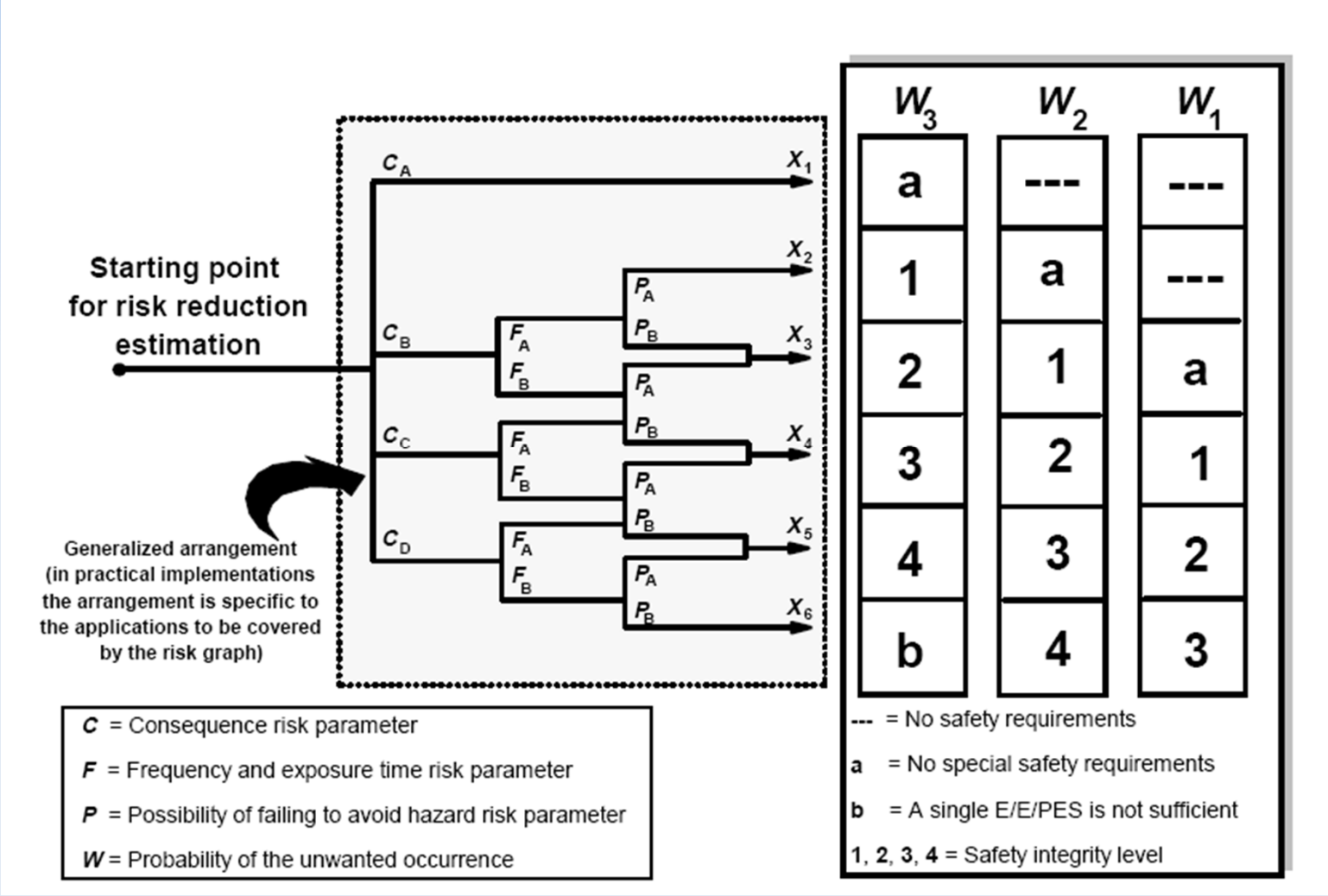
such probabilities are commonly expressed as rates

Quantitative Risk Assessment – Ctd.



Source:
IEC61508

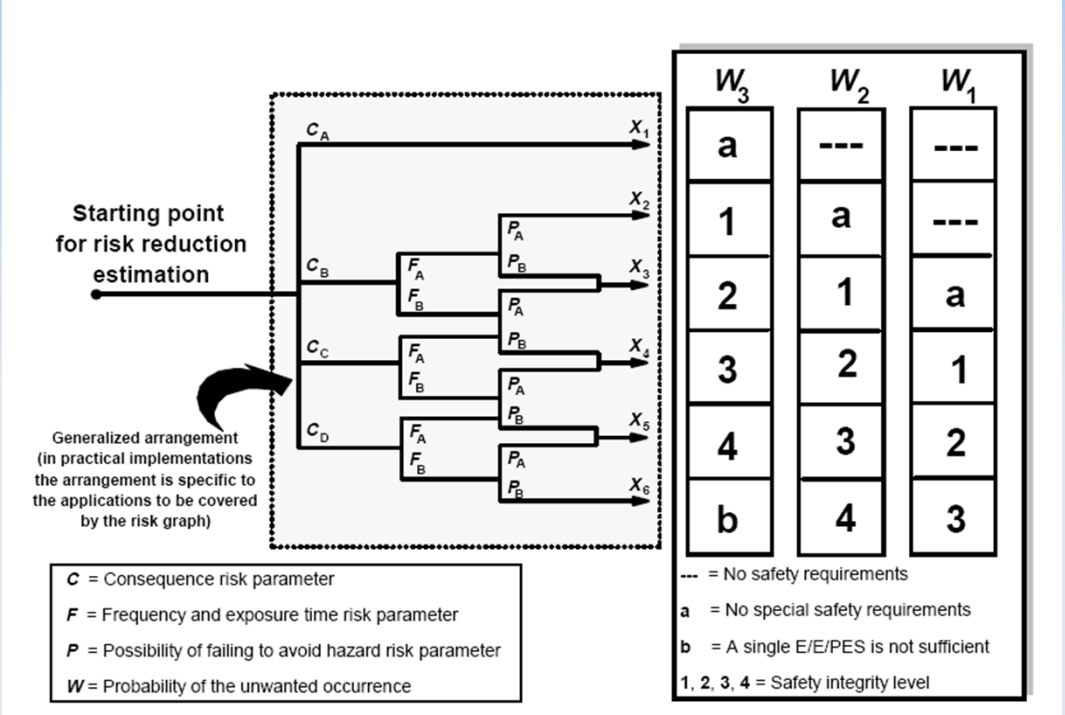
Qualtitative Risk Assessment



Source: IEC61508

Qualtitative Risk Assessment Example

The maximum tolerated fatality (harm) rate (one person dies) of a system has been decided to be 10^{-5} pa (ALARP, discussions). 10^{-2} of the hazards under investiogation leed to harm. From an independent assessment we know that the system as built today (no additional risk reduction) fails at 2×10^{-1} pa.



Source: IEC61508

(a) Do we need an additional safety system?

(b) What quality (failure rate, etc.) must an additional safety system have if mandatory?

Published Tolerated Risk

- Probability for nuclear meltdown: $< 10^{-5}$ pa (IAEA)
- Probability of larger amounts of radiation in case of an accident: $<< 10^{-6}$ pa (IAEA)
- Civil aviation:
  - Catastrophic event: $< 10^{-9}$ ph
  - Dangerous event: $< 10^{-7}$ ph
  - Other important flight operations: $< 10^{-5}$ ph
- Railway interlocking systems (Deutsche Bahn): $< 10^{-9}$ per setting

Safety and Functional Safety

Safety
is the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly as a result of damage to property or to the environment

Functional safety
is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs

According to IEC61508: Part of the overall safety relating to the equipment and its associated control system which depends on the correct functioning of electrical, electronic and programmable electronic safety-related systems……".

Overall Safety = Non-functional Safety + Functional Safety

Safety-critical and Safety-related Systems

- The term ‘safety-related’ applies to any hardwired or programmable system where a failure, singly or in combination with other failures/errors, could lead to death, injury or environmental damage.
- ‘Safety-critical’ has tended to be used where failure alone, of the equipment in question, leads to a fatality or increase in risk to exposed people.
- ‘Safety-related’ has a wider context in that it includes equipment in which a single failure is not necessarily critical whereas coincident failure of some other item leads to the hazardous consequences.
  -> we will use the term safety-related here

Safety Assessment

- Establish a risk target:
  - Formal hazard identification, HAZOP
  - Set a maximum tolerable risk
  - Carry out a quantified risk assessment
  - Maximum tolerable risk
  - Risk reduction: ALARP
  - Outcome: hazardous states, maximum tolerable failure probability
- Identify the safety function
  - What are the failure modes leading to the hazardous event
  - Identification of protection
  - Outcome: What needs to be done to reduce the risk?

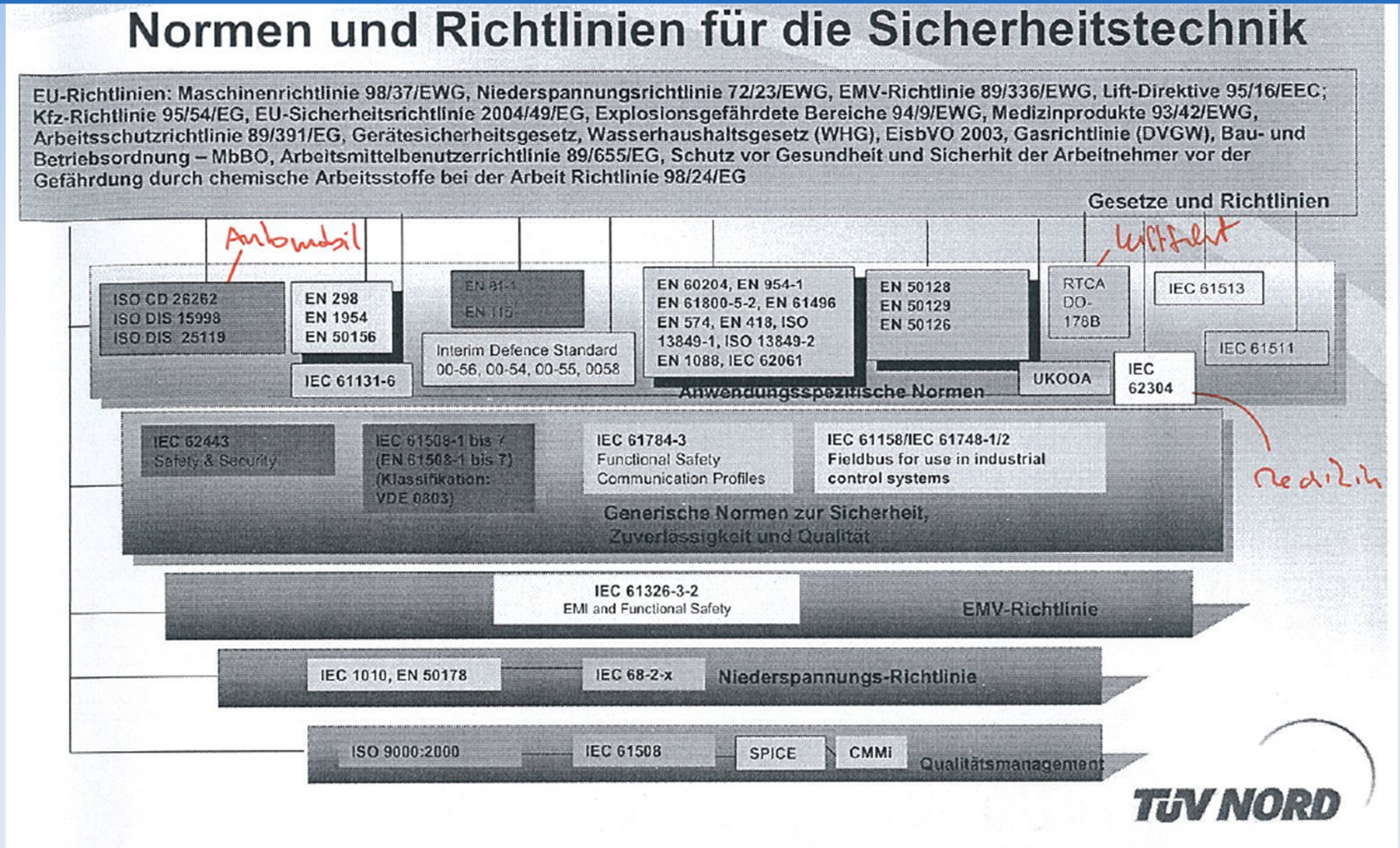
Safety Assessment – Ctd.

- Safety function integrity:
  - Numerical methods
  - Risk graphs
  - Outcome: Probability of failure of the safety function (target SIL)
  - Note: the actual SIL will be compared to the target SIL in later steps of the design process (FMEDA, Markov Chain Analysis)
- Add safety function and integrity level to the requirements specification
  - Safety-related systems usually need a separate safety documentation

Safety Standards

- Today more and more the devices and products dedicated to the safety of machinery incorporate complex and programmable electronic systems.
- Due to the complexity of the programmable electronic systems it is in practice difficult to determine the behavior of such safety device in the case of a fault.
- Therefore the standard IEC/EN 61508 with the title “Functional safety of electrical/electronic/ programmable electronic safety-related systems” provides a new approach by considering the reliability of safety functions.
- It is a basic safety standard for the industry and in the process sectors.

Safety Standards Ctd.



Safety Function and Safety Integrity Level (SIL)

Safety Function

function to be implemented by an electrical/electronic/programmable electronic safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the equipment under control (EUC), in respect of a specific hazardous event (from IEC61508)

Safety Integrity

probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time (from IEC61508)

- The higher the level of safety integrity of the safety-related systems, the lower the probability that the safety-related systems will fail to carry out the required safety functions.
- There are four levels of safety integrity for systems.

Safety Integrity Level (SIL)

IEC 61508 considers two modes of operation:
high demand or continuous mode – where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof check frequency; or
low demand mode – where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency

SIL	High demand	Low demand
4	$10^{-9} \leq$ PFH $\leq 10^{-8}$	$10^{-5} \leq$ PFD $\leq 10^{-4}$
3	$10^{-8} \leq$ PFH $\leq 10^{-7}$	$10^{-4} \leq$ PFD $\leq 10^{-3}$
2	$10^{-7} \leq$ PFH $\leq 10^{-6}$	$10^{-3} \leq$ PFD $\leq 10^{-2}$
1	$10^{-6} \leq$ PFH $\leq 10^{-5}$	$10^{-2} \leq$ PFD $\leq 10^{-1}$

Source:
IEC61508

Safety Assessment in Requirements Analysis

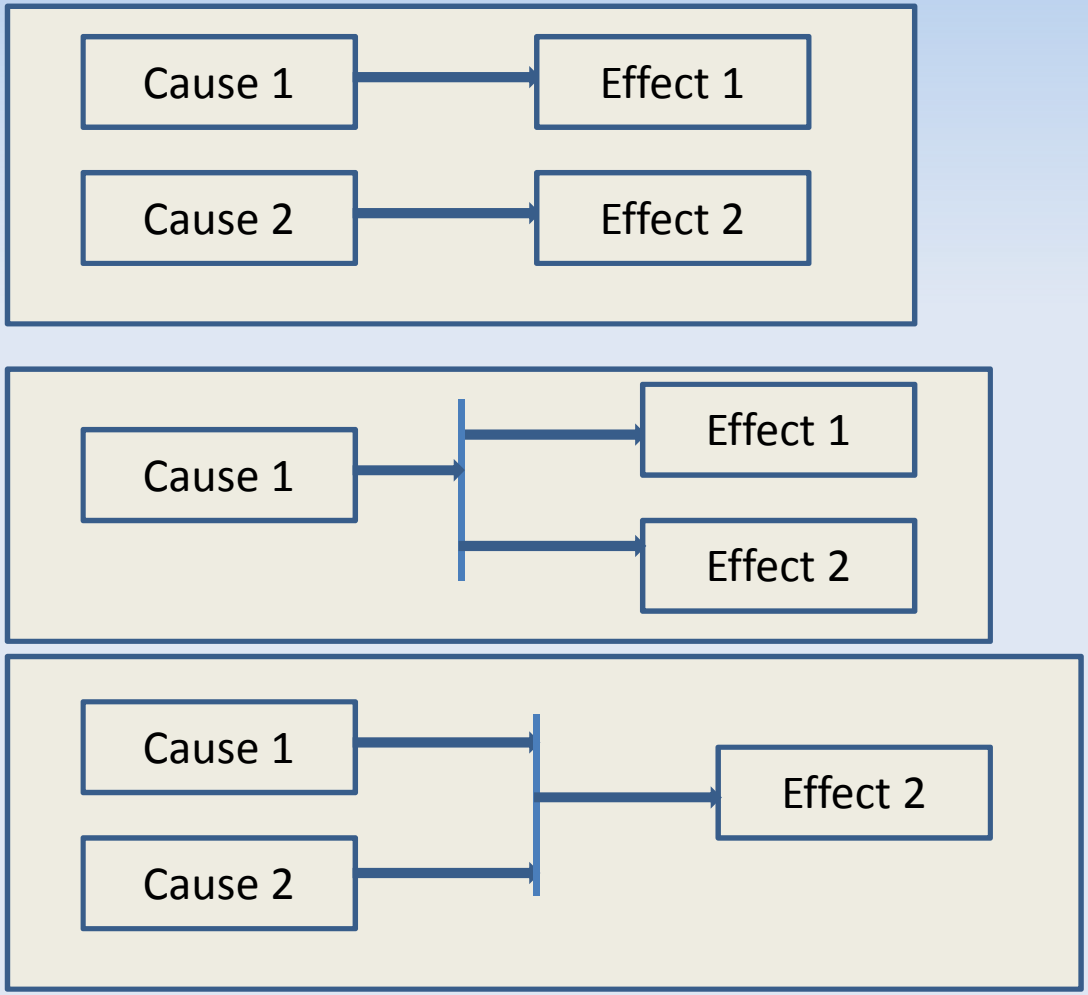
- Safety Function – identify failure modes (what shall we do?)
  - Block level FMEA
  - FTA
- Safety Integrity (how well shall we do this?)
  - Qualitative Methods
  - Quantitative Methods (Risk assessment, Reliability Block Diagrams)
  - Marketing (competitor analysis)

Failure Modes and Effect Analysis (FMEA)

- Block level in requirements analysis
  - Also: design FMEA (later) and process FMEA
- What are the failure modes and what is the effect:
  - System failure (e.g. power, communication, timeliness, erroneous) mode assessment
  - Plan how to prevent the failures
- How does it work?
  - Identify potential failure modes and rate the severity (team activity)
  - Evaluate objectively the probability of occurrence of causes and the ability to detect the cause when it occurs
  - Rank deficiencies
  - Focus on eliminating product concerns and help prevent problems from occurring

FMEA Ctd.

- Link cause to an effect (one to one, one to many, many to one)



FMEA Ctd.

- FMEA tools
  - Spreadsheet, proprietary (e.g. Reliasoft)
- Risk ratings: 1 (best) to 10 (worst)
  - Severity (SEV) – how significant is the impact to the customer
  - Occurance (OCC) – likelihood of occurance
  - Detection (DET) – how likely will the current system detect the failure mode
- Risk Priority Number (RPN)
  - A numerical calculation of the relative risk of a particular failure mode
  - RPN = SEV x OCC x DET
  - Used to place priority

FMEA Ctd.

- Example: IC Packaging

Function	Failure	Effect	Si	Classification	Cause	Oi	Control (Prevention)	Control (Detection)	Di	RPNi
Solder mask for the chip.	Oxidation.	Bad solder wettability.	4		Storage.	4		Nitrogen Storage.	7	112
								Incoming Insp.		
	Contamination.	Bad solder wettability.	4		Packing. Handling by vendor.	4		Vacuum pack.	7	112
								Incoming Insp.		
	Dimensions too big or too small.	Solder mask does not fit in jig.	1		Stamping defect.	2		Stamping tool control.	9	18
								Incoming Insp.		
	Coplanarity.	Flow characteristics of solder.	4		Packing transport.	4		Suitable packing.	7	112
								Incoming Insp.		
Wire Bonding Surface	Surface structure.	Bad adhesion of bonds.	7		Sintering failure.	1		Process control at vendor.	8	56
								Incoming Insp.		
	Coplanarity.	Bad adhesion. Deformed bonds.	7		Packing. Transport	2		Suitable packing.	8	112
								Incoming Insp.		
External electrical contact.	Oxidation.	Bad weldability.	7		Packing & Storage.	1		Storage.	9	63
					Breakage during forming.	1		Process control in sintering.	9	63

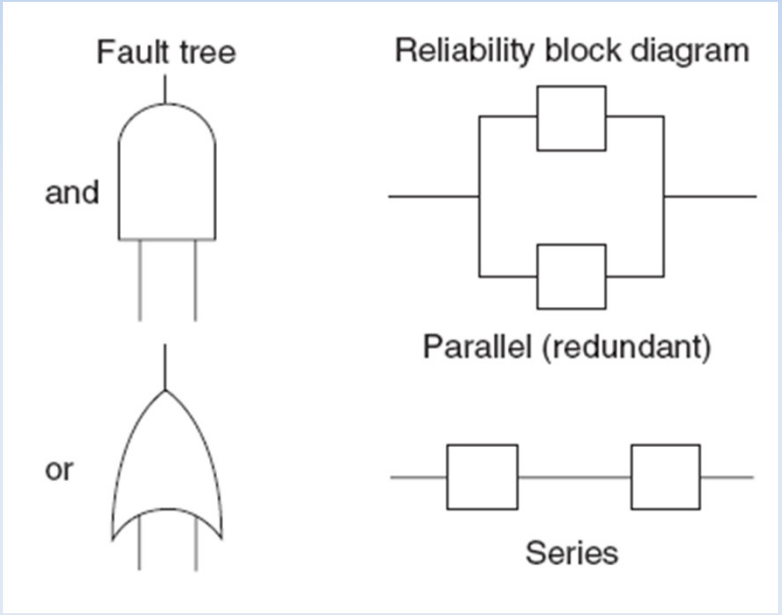
Fault Tree Analysis (FTA)

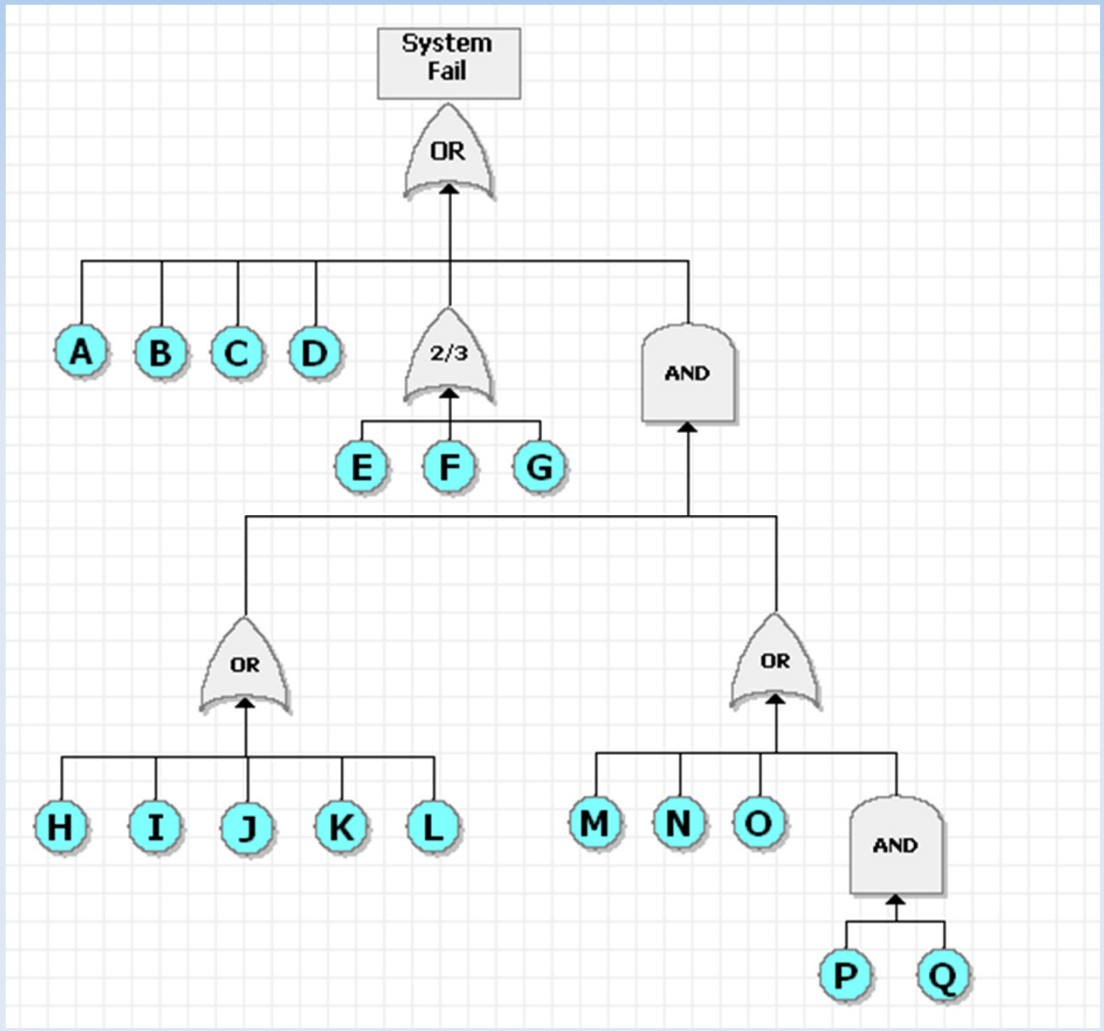
- Top event is hazardous event or a failure mode
- Devide system into components
- Look into combinations of faults
- Tree like structure
- Paths of Failure vs. paths of survival (in RBD)

Outcome:

- Root cause event (external, internal) that (in combination) will lead to top event
- Good system understanding

FTA Ctd.





Source:
Smith, Functional Safety

Safety Systems Overview
- Terminology from IEC 61508 -

EUC: Equipment under control (machinery, plant e.g.)

EUC control: machinery control or plant level control (DCS), e.g.

S: sensor

A: actuator

A safety function can run on a dedicated separate system or be part of the control system (or both)