Industrial Embedded Systems
- Design for Harsh Environment -

Dr. Alexander Walsch
alexander.walsch@ge.com

IN2244

Part V - Safety

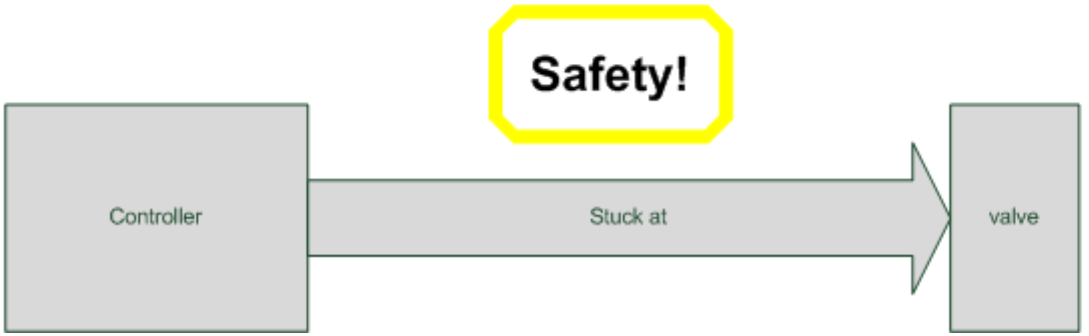
WS 2014/15

Technische Universität München

From Reliability to Safety

- The same failure mode of a function will have different consequences at the system level.
- A valve is controlled. The valve control function fails at ‚stuck at' failure mode and so the valve can not be opened.

Delivery valve does not open (stuck at failure mode). The process can not be excuted correctly and the product is degraded. The customer is annoyed and a downtime is necessary to clean up the mess.



Pressure relief valve does not open (stuck at failure mode). The reactor explodes and people die.

From Reliability to Safety II

- However, we need to seperate functions which are critical because their failure means reduced availability from those that mean loss of lives or severe danger. The latter is of public interest, the former more of a performance gain.
- Safety is about
  - Assessing the risk of those failures (similar to reliability) and the tolerated risk → setting a target risk reduction
  - Proposing risk reduction based on computer architecture, design, V+V and processes (different to reliability since not every architecture might be allowed)
  - Realizing a proposed system based on the proposed architecture and showing (proving) that the actual designed-in risk reduction meets the target risk reduction

Motivation

- Functional safety is concerned with the risk reduction of a specific (computer implemented) function.
- 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

Hazard

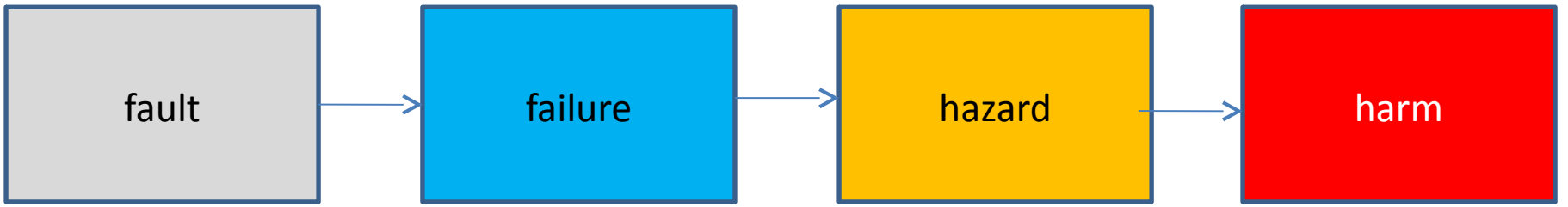
potential source of harm. Hazard is a system state resulting from a failure.

[Guide 51 ISO/IEC:1990]

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)]

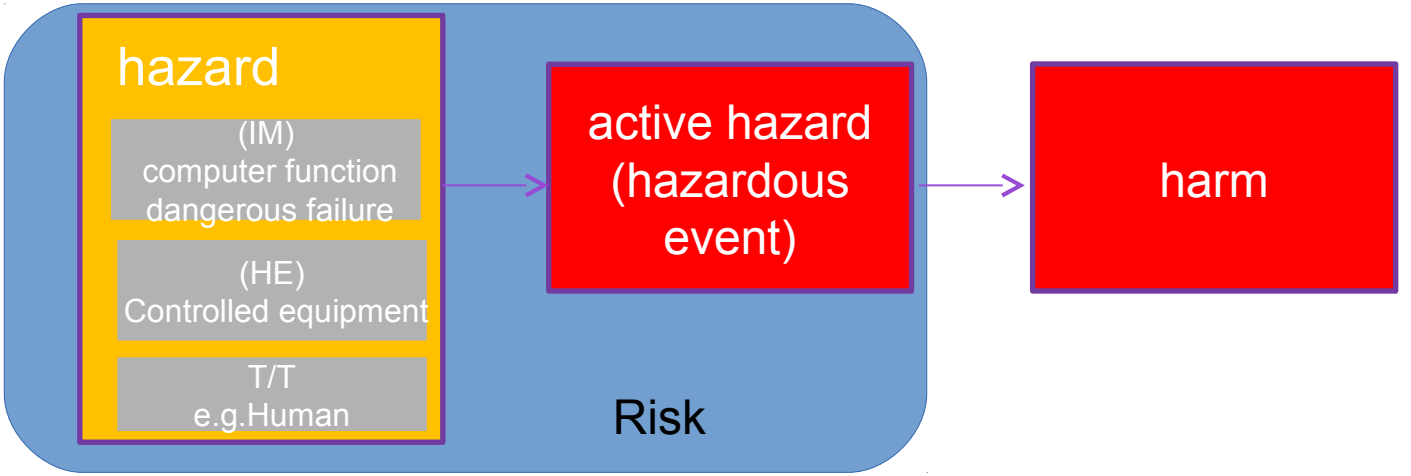


Hazards and Harm II

- Hazard is a widely used term and means „dangerous state of a system whichis controlled by a computer“ to us. Hazard may cause harm by the occurance of
  - a mishap (e.g. MIL-STD-882D)
  - an accident
  - a hazardous event
- We will use the term harm and hazardous event here but different domains, standards or best practices might use different terms which all refer to a similar situation: a hazard is there (property of the system) → the hazard can be activated → a hazardous event may happen → the hazardous event may cause harm.

Hazards

- Hazards can be active or inactive (but they are always there if not designed out). Hazard activation depends on the interdependence of
  - Initiating Mechanism (IM) – e.g. a computer function that fails
  - Hazardous Element (HE) – e.g. a system that stores electrical energy
  - Target and Threat (T/T) – e.g. a human working close to the system
- If either one is not present the hazard can not be activated.



Risk

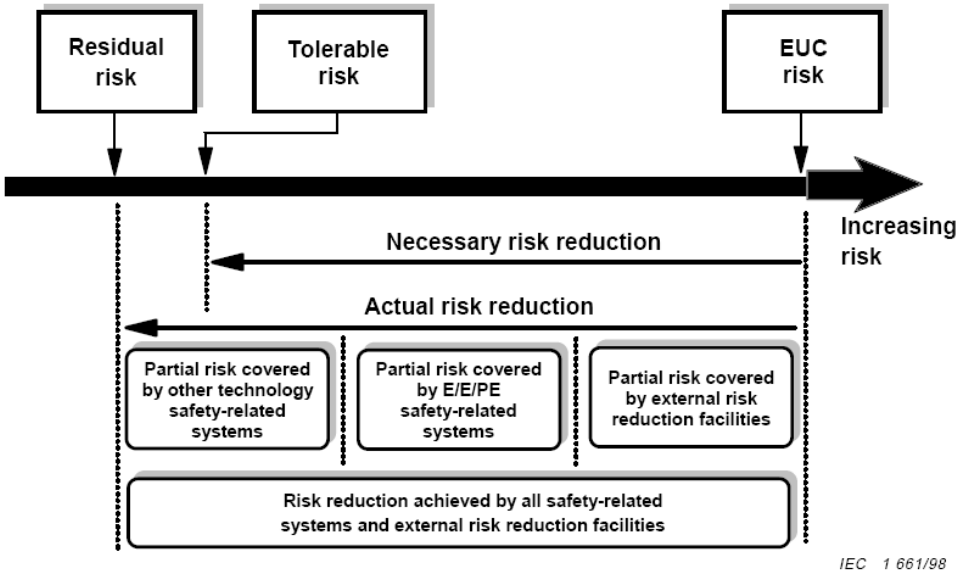
Risk
a measure of the probability and consequence (harm) of a specified hazardous event

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

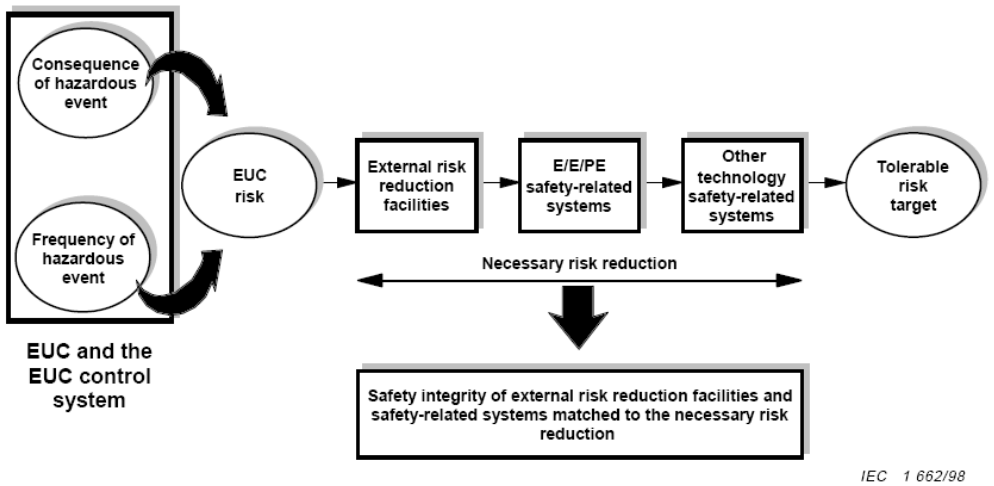
Risk assessment is necessary to phrase the missing safety requirements for the requirements specification.

Risk and Risk Reduction (IEC61508)



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

How to reduce risk?



Source:
IEC61508

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 (computer controlled 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 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.

Software Safety and Reliability Standards

- General/Industrial: IEC 61508 – Safety Integrity Level (SIL 1-4)
- Automotive: ISO CD 26262 – Automotive Safety Integrity Level (ASIL A-D)
- Aviation: DO178B(C) – Design Assurance Level (DAL E-A)
- Rail: EN 50126/50128/50129 – Safety Integrity Level (SIL 1- 4)
- Healthcare: IEC 62304 (Class A-C)

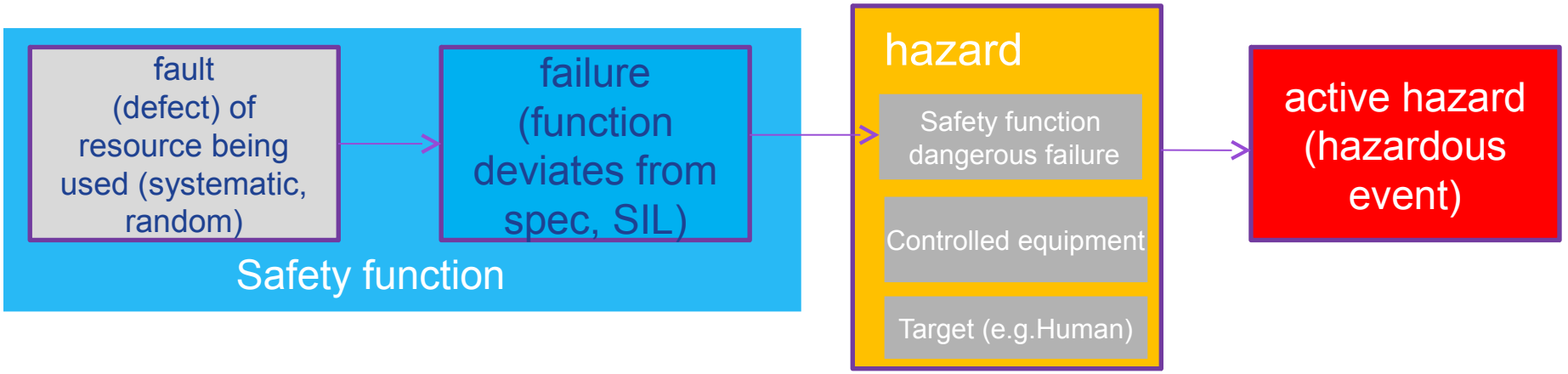
Safety Function and Safety Integrity Level (SIL)

Safety Function

function to be implemented on a controller which is intended to achieve or maintain a safe state in respect of a specific hazardous event (IEC61508 uses hazardous event)

Safety Integrity

probability that a required safety function is satisfactorily performed under all the stated conditions within a stated period of time



Safety Integrity Level (SIL)

IEC 61508 considers two modes of safety function operation:

high demand or continous mode
the frequency of demands (safety function requests) is greater than one per year or greater than twice the proof check frequency (test interval – system considered as new afterwards)

Think of a safety function that calculates a specific result on a microprocessor (on failure of the safety function a wrong result is communicated immediately which may activate the hazard)

low demand mode
the frequency of demands no greater than one per year and no greater than twice the proof test frequency

Think of a safety function requested on a specific event only (e.g. a sensor input). The failure of the safety function has no immediate impact on hazard activation.

Safety Integrity Level (SIL) II

- Probability of failure per hour – PFH (rate since hazard may be active immediately after failure)
- Probability of failure on demand – PFD (dimension less since hazardous state is measured against number of demands)

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

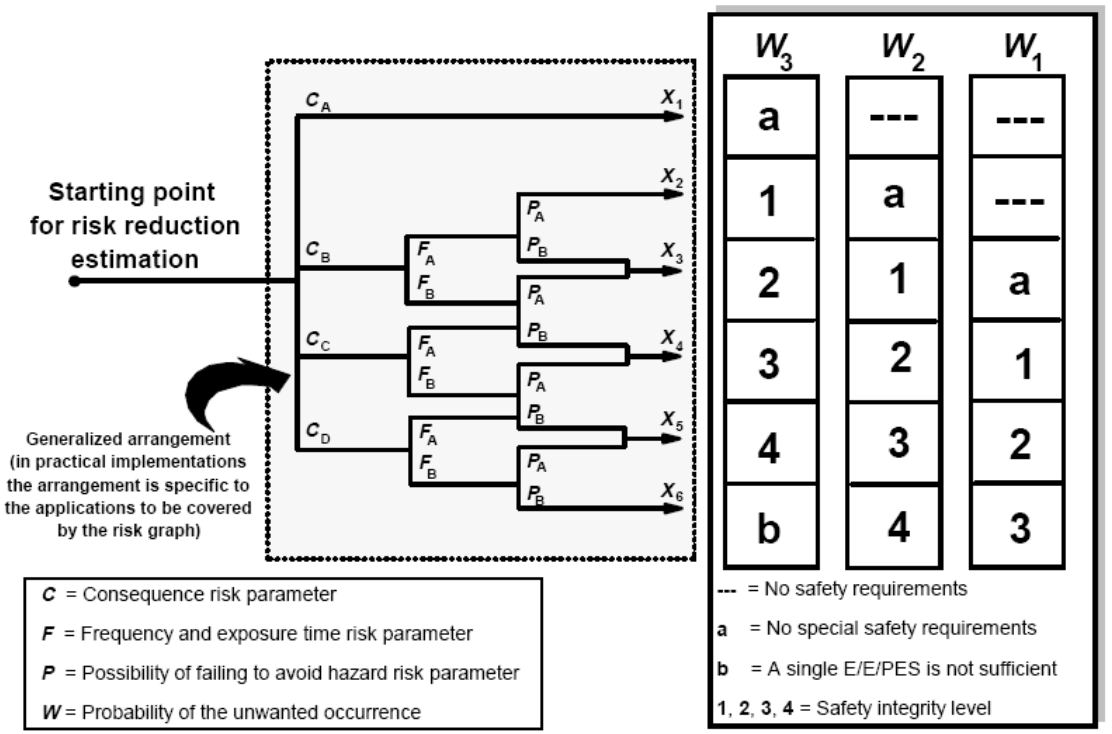
Source: IEC61508

Safety Assessment in Requirements Analysis

- Identify failure modes as in reliability analysis to get safety function
  - What are the hazards?
  - FTA – do system level to discover root causes of hazardous failures
  - Link those root causes (events) to function failure modes and their effects (FMEA)
  - The safety function is that function which may activate a hazard on failure (malfunction or not executed)
- Safety Integrity
  - Quality of the safety function (SIL)
  - Derived with qualitative Methods (PHA, FMEA), Quantitative Methods (Risk assessment and risk reduction), Marketing (competitor analysis)
- Response time
  - Every safety function comes with a real-time performance requirement

Qualititative Risk Assessment
- Risk Graph for a specific Hazardous Event -

Risk parameter		Classification	Comments
Consequence (*C*)	C_1	Minor injury	1 The classification system has been developed to deal with injury and death to people. Other classification schemes would need to be developed for environmental or material damage.
	C_2	Serious permanent injury to one or more persons; death to one person	
	C_3	Death to several people	2 For the interpretation of C_1, C_2, C_3 and C_4, the consequences of the accident and normal healing shall be taken into account.
	C_4	Very many people killed	
Frequency of, and exposure time in, the hazardous zone (*F*)	F_1	Rare to more often exposure in the hazardous zone	3 See comment 1 above.
	F_2	Frequent to permanent exposure in the hazardous zone	
Possibility of avoiding the hazardous event (*P*)	P_1	Possible under certain conditions	4 This parameter takes into account – operation of a process (supervised (i.e. operated by skilled or unskilled persons) or unsupervised); – rate of development of the hazardous event (for example suddenly, quickly or slowly); – ease of recognition of danger (for example seen immediately, detected by technical measures or detected without technical measures); – avoidance of hazardous event (for example escape routes possible, not possible or possible under certain conditions); – actual safety experience (such experience may exist with an identical EUC or a similar EUC or may not exist).
	P_2	Almost impossible	
Probability of the unwanted occurrence (*W*)	W_1	A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely	5 The purpose of the *W* factor is to estimate the frequency of the unwanted occurrence taking place without the addition of any safety-related systems (E/E/PE or other technology) but including any external risk reduction facilities.
	W_2	A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely	6 If little or no experience exists of the EUC, or the EUC control system, or of a similar EUC and EUC control system, the estimation of the *W* factor may be made by calculation. In such an event a worst case prediction shall be made.
	W_3	A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely	



Source:
IEC61508

Quantitative Risk Assessment

Risk = Probability x Consequence

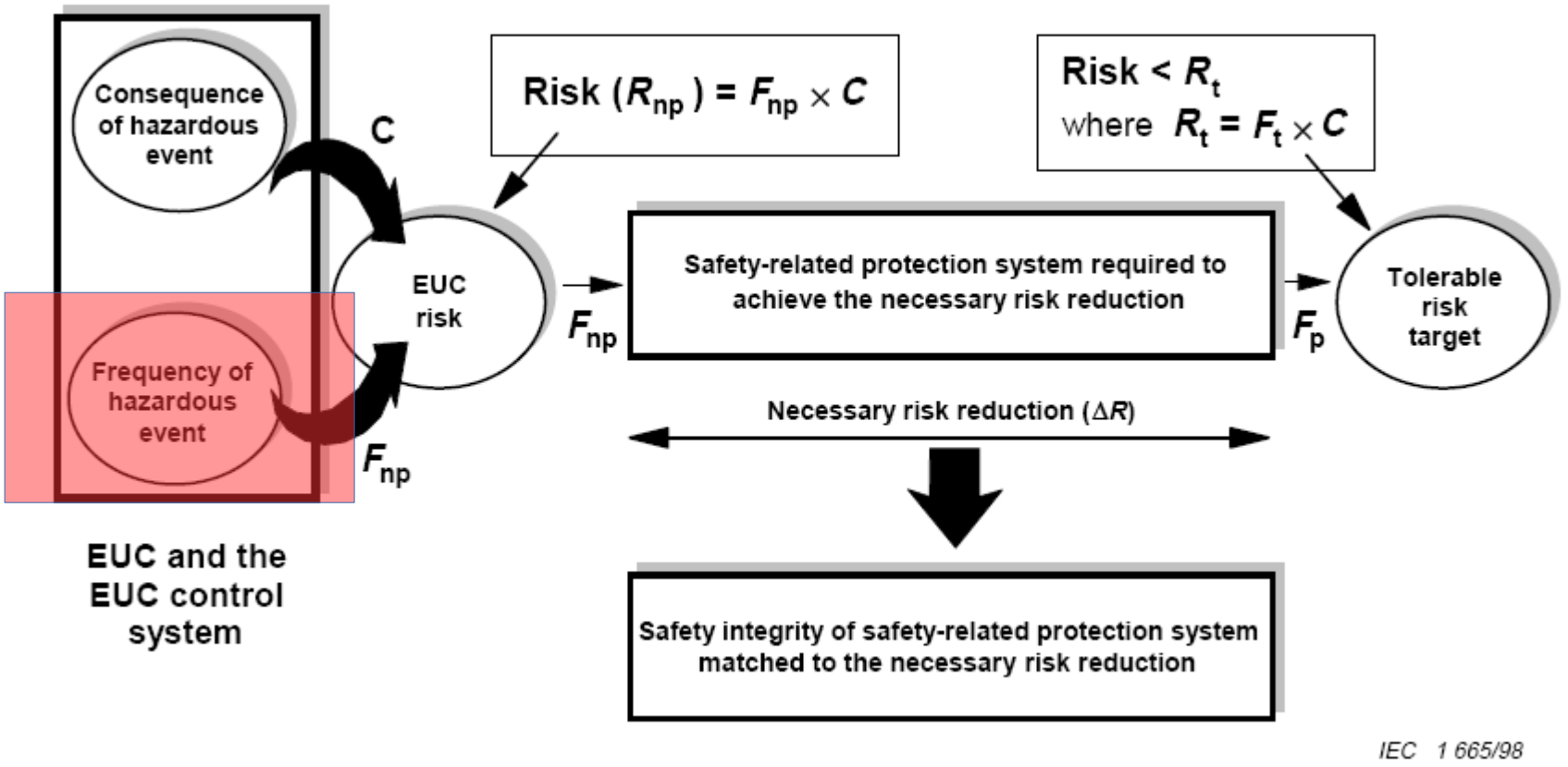
Maximum tolerable risk of fatality	*Individual risk (per annum)*
Employee	10^{-4}
Public	10^{-5}
Broadly acceptable risk (previously referred to as 'Negligible' (Employee and public))	10^{-6}

Catastrophic
Critical
Marginal
Negligible

Source:
Smith, Functional Safety

What is the frequency of the hazardous event (rate, probability)?, what are the consequences (harm)?

Quantitative Risk Assessment II
- from IEC61508 -



Source:
IEC61508

Quantitative Risk Assessment
- Example -

The maximum tolerated risk of an overpressure condition to result in an explosion is 10^{-5} pa (society, discussions).
10^{-2} of the overpressure conditions under investigation lead to an explosion.

From an FTA we know that the system as built today fails at 2×10^{-1} pa. A failure is due to a failure in the pressure control function.

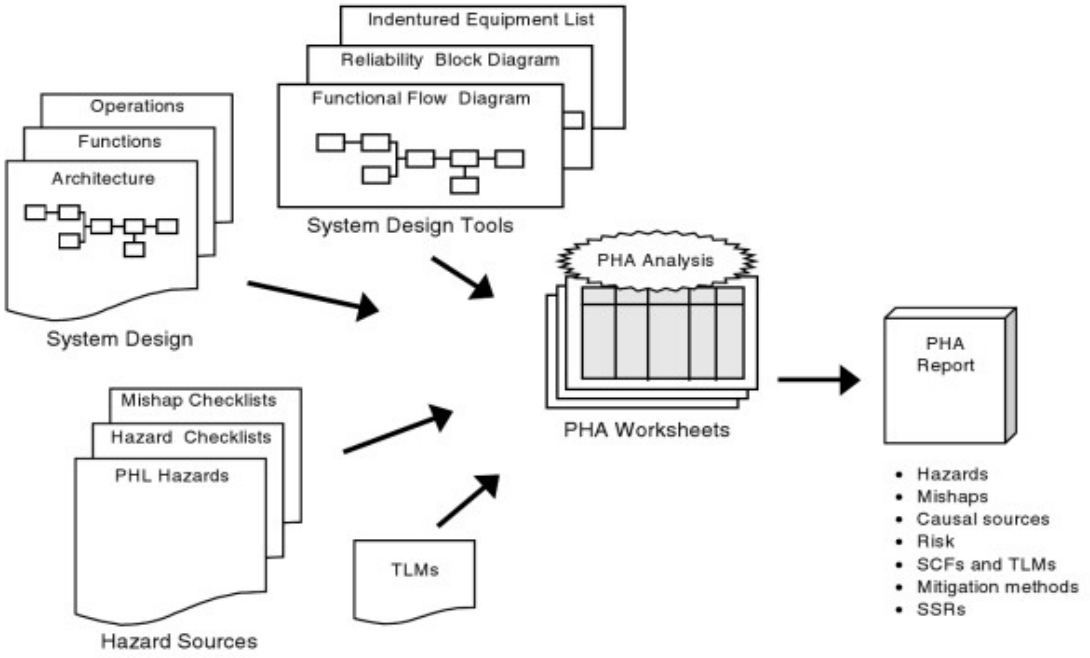
(a) Do we need additional protection?

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

Quantitative Risk Assessment Example
- see Whiteboard -

Preliminary Hazard Analyis (PHA)

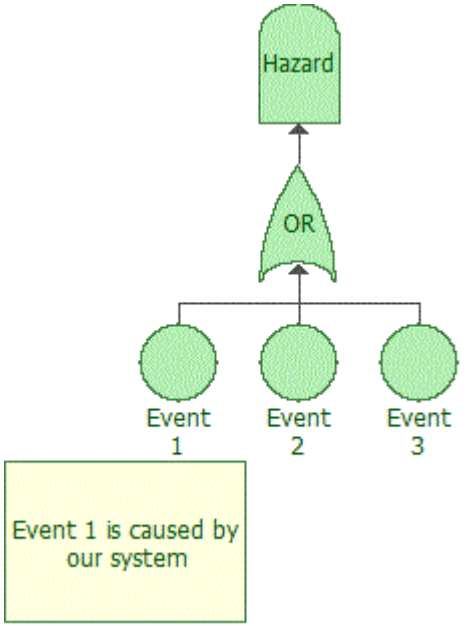
- PHA evaluates a design at a preliminary level. The design does not exist yet.
- Input: design knowledge, hazard knowledge, preliminary hazard list, system hazardous events
- Output: hazards, hazardous events, causes, safety functions, mitigation methods, safety requirements



Source:
Ericsson II, Hazard Analysis for System Safety

Methods in PHA

- FTA helps do discover events that could activate hazards in application system
- Event in FTA is linked to failure mode(s) of our system functions
- Isolate failure modes and identify the safety function



Methods in PHA

- Spreadsheet approach
- Team activity

Severity	Probability
I. Catastrophic	A. Frequent
II. Critical	B. Probable
III. Marginal	C. Occasional
IV. Negligible	D. Remote
	E. Improbable

Subsystem: **Preliminary Hazard Analysis** Last Update:

Number	System Item	Hazard	Causes	Effects	Project Phase(s)	Risk IMRI	Risk Value	Risk Cat.	Recommended Action	Risk FMRI	Risk Value	Risk Cat.	Comments

Order of Precedence

1. Eliminate hazard through design selection.
2. Incorporate safety devices.
3. Provide warning devices.
4. Develop procedures and training.

Preliminary Hazard Analyis (PHA)
- What to look for (not complete) -

- Hazardous components (e.g. energy sources, fuels, propellants, explosives, pressure systems, …)
- Subsystem interfaces (signals, voltages, timing, human interaction, …)
- Environmental constraints (vibration, shock, extreme temperatures, EMI)
- Undesired states (e.g. failure to safe state)
- Malfunctions
- Software errors (programming errors, omissions, design errors)
- System life cycle (not only operational...)
- Human error

Software Hazard Analysis Guideline

- Software Hazard Analysis guideline (what can go wrong) prepared by Lawrence Berkeley Livermore Lab (LBLL)
- Quality = requirement category in figure
- Document available online

Quality	Description of Quality
Accuracy	The term *accuracy* denotes the degree of freedom from error of sensor and operator input, the degree of exactness possessed by an approximation or measurement, and the degree of freedom of actuator output from error.
Capacity	The terms *capacity* denotes the ability of the software system to achieve its objectives within the hardware constraints imposed by the computing system being used. The main factors of capacity are Execution Capacity (timing) and Storage Capacity (sizing). These refer, respectively, to the availability of sufficient processing time and memory resources to satisfy the software requirements.
Functionality	The term *functionality* denotes the operations which must be carried out by the software. Functions generally transform input information into output information in order to affect the reactor operation. Inputs may be obtained from sensors, operators, other equipment or other software as appropriate. Outputs may be directed to actuators, operators, other equipment or other software as appropriate.
Reliability	The term *reliability* denotes the degree to which a software system or component operates without failure. This definition does not consider the consequences of failure, only the existence of failure. Reliability requirements may be derived from the general system reliability requirements by imposing reliability requirements on the software components of the application system which are sufficient to meet the overall system reliability requirements.
Robustness	The term *robustness* denotes the ability of a software system or component to function correctly in the presence of invalid inputs or stressful environmental conditions. This includes the ability to function correctly despite some violation of the assumptions in its specification.
Safety	The term *safety* is used here to denote those properties and characteristics of the software system that directly affect or interact with system safety considerations. The other qualities discussed in this table are important contributors to the overall safety of the software-controlled protection system, but are primarily concerned with the internal operation of the software. This quality is primarily concerned with the affect of the software on system hazards and the measures taken to control those hazards.
Security	The term *security* denotes the ability to prevent unauthorized, undesired and unsafe intrusions. Security is a safety concern in so far as such intrusions can affect the safety-related functions of the software.

Source:
Software Safety Hazard Analysis, J. Lawrence, LBLL

Preliminary Hazard Analyis (PHA)
- Safety Integrity and Response Time -

- Response time: depends on application → fault response time
- SIL: could feed hazardous event into qualitative analysis, quantitative more difficult