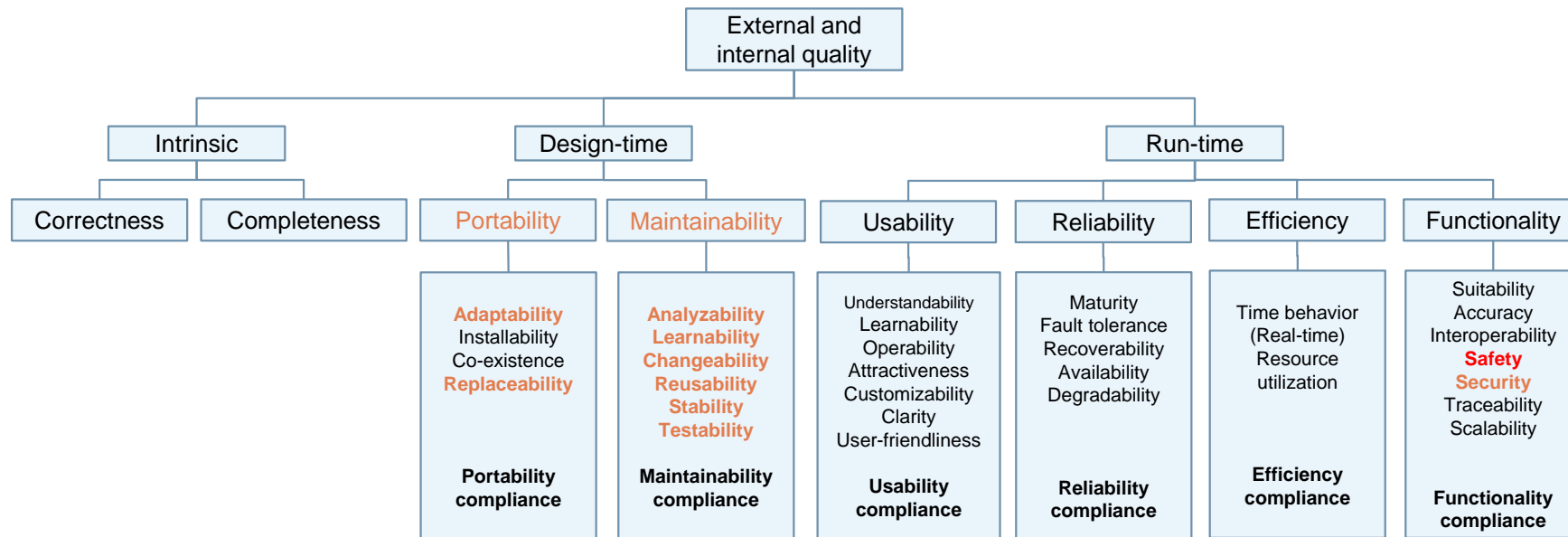


# Advanced Topics of Software Engineering (ASE)

## Chapter 2. From requirements to system design

Prof. Dr. Florian Matthes, Prof. Dr. Alexander Pretschner

Chair of Software Engineering for Business Information Systems (sebis)  
Faculty of Informatics  
Technische Universität München  
[www.matthes.in.tum.de](http://www.matthes.in.tum.de)



# From requirements to system design

2.1. Software architecture

2.2. Antipatterns in software engineering

2.3. Reuse

2.4. Testability

2.5. Safety

## **2.5.1. Terminology**

2.5.2. Risk

2.5.3. Faults, errors, and failures

2.5.4. Functional safety

2.5.5. Safety analyses using FMEA and FTA

2.6. Information security



How would you translate the term 'Sicherheit' into English?

# Safety vs security



# Intuitive notion of safety (1)

Most of us have a ***general idea of what safety is***

- Water is safe to drink
- Food is safe to eat
- A car is safe to drive

## Intuitive notion of safety (2)

- Water is safe to drink
- Food is safe to eat
  - We imply absence of harmful bacteria and other contaminants
  - Is water / food 100% free of these items?  
No. The levels of these items are below a certain threshold which has been determined to be 'safe'
- A car is safe to drive

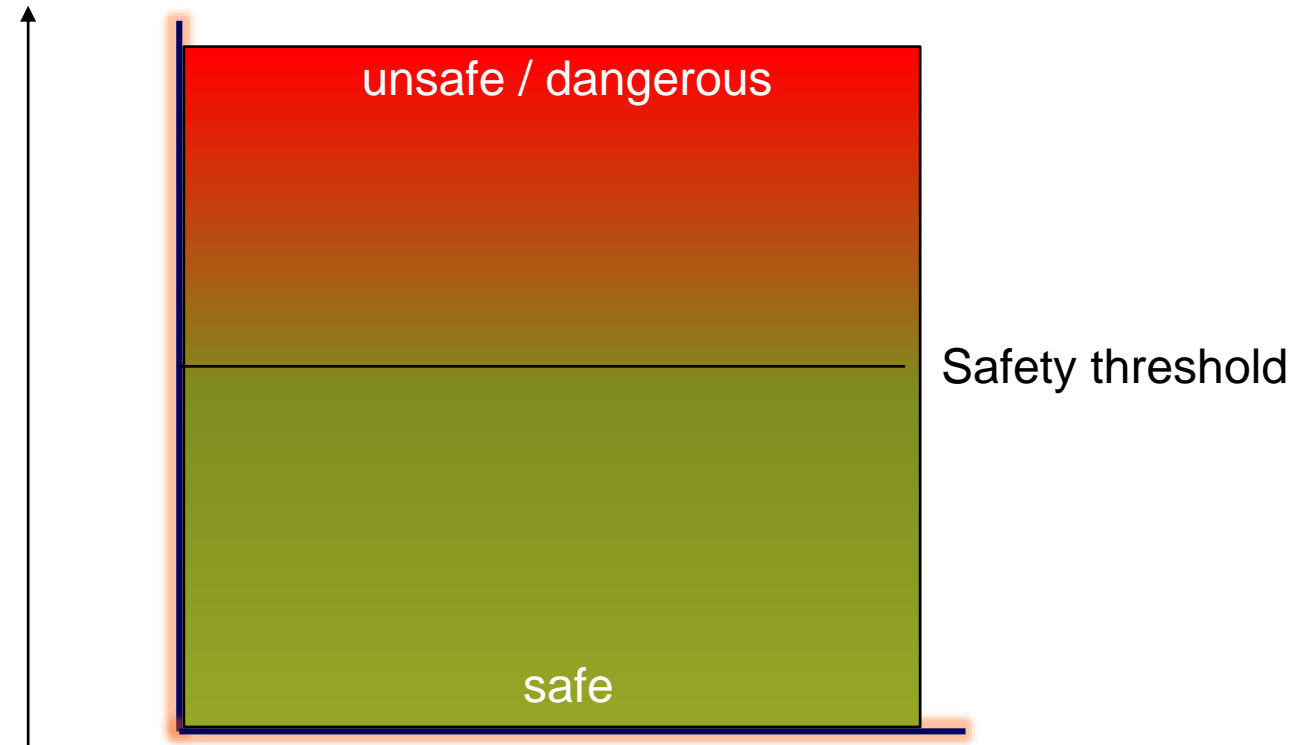
## Intuitive notion of safety (3)

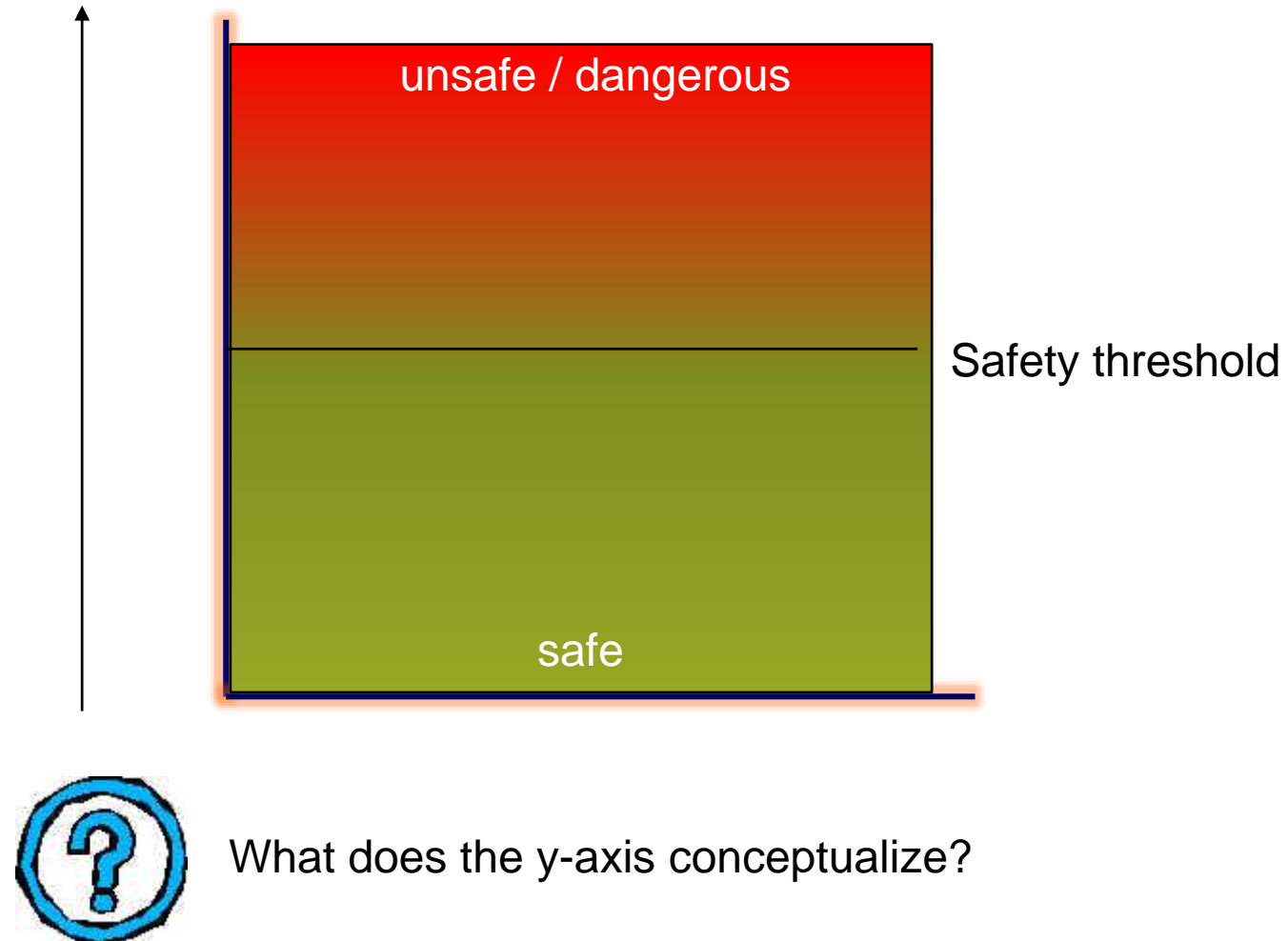
- Water is safe to drink
- Food is safe to eat
- A car is safe to drive
  - An automobile presents a somewhat different scenario.  
It contains electronic parts, mechanical parts, combustible energy sources...
  - This creates many opportunities for potential hazards.  
A multitude of factors must be evaluated before a car can be determined to be safe.
  - Is a car 100% safe?  
No. Again thresholds have been established for braking response, bumper impact resistance, engine fire containment, ...



- Concept of **safety thresholds**: established safety engineering principle
  - Not unique to software or electronic systems.
  - The idea that there are various thresholds above or below which a product is considered to be safe has been applied in microbiology, medicine, engineering for many years.

Goal: to determine how safe is 'safe enough' without over- or under- engineering a product





# From requirements to system design

2.1. Software architecture

2.2. Antipatterns in software engineering

2.3. Reuse

2.4. Testability

2.5. Safety

2.5.1. Terminology

**2.5.2. Risk**

2.5.3. Faults, errors, and failures

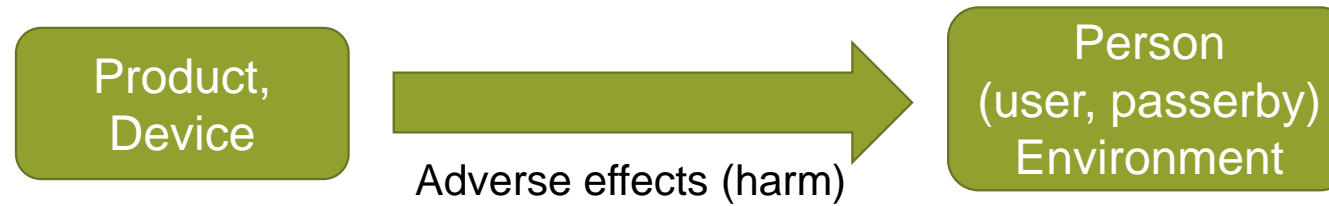
2.5.4. Functional safety

2.5.5. Safety analyses using FMEA and FTA

2.6. Information security

# Adverse effect / harm

 Schaden



What criteria could be used to quantify the adverse effects originating from a product / device?

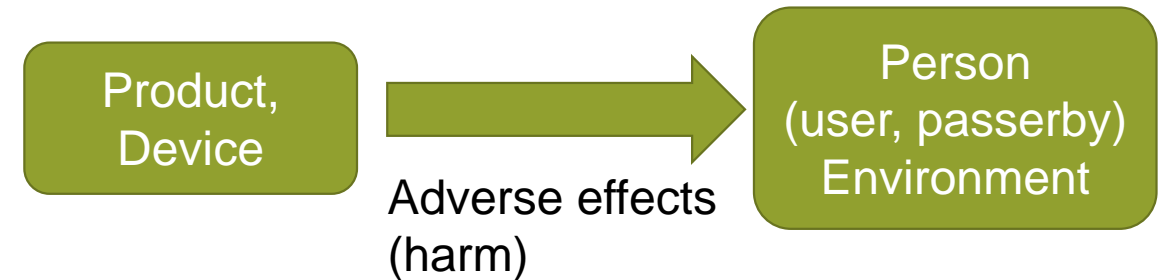
 Risiko

Measure comprising

- the ***probability of occurrence of adverse effects*** (harms) and
- their ***severity***

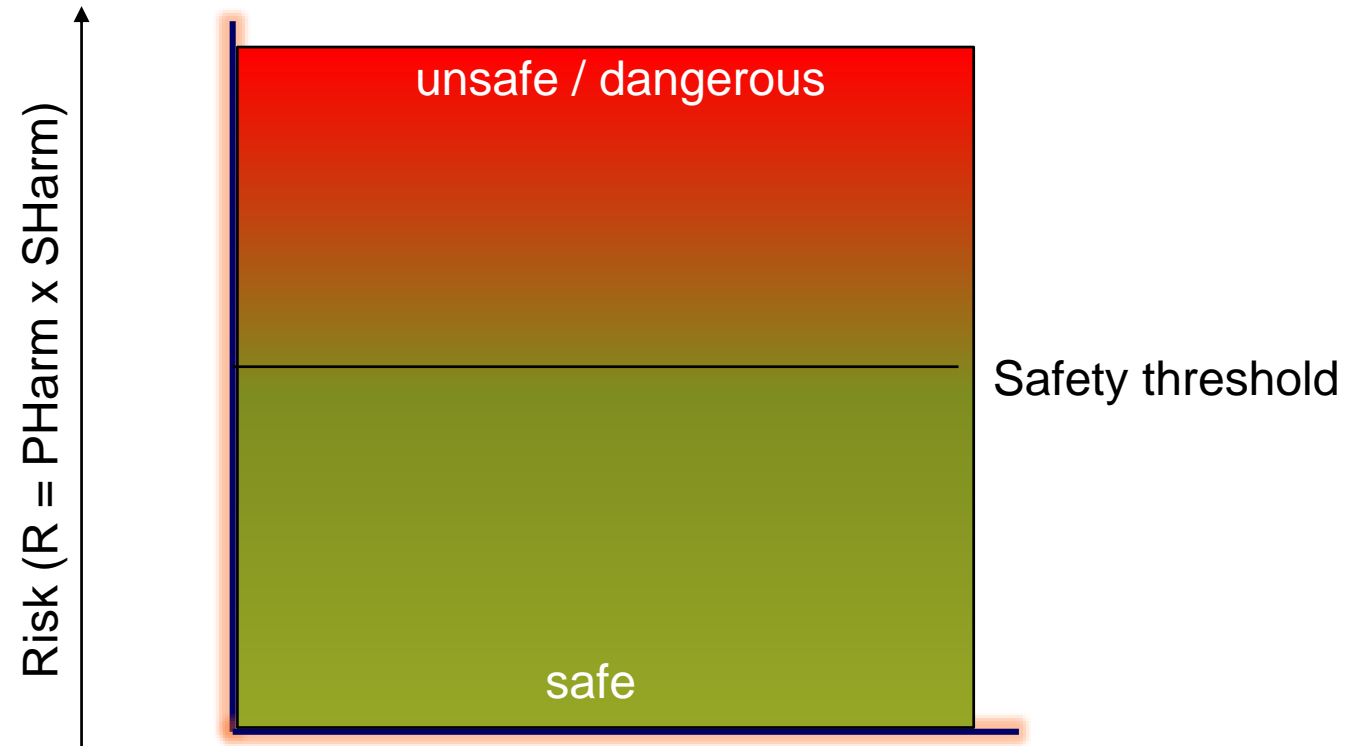
Dimensions of harm:

- Persons (users, passersby)
- Environment, equipment, property
- Liability, company/brand image



$$R = PHarm \times SHarm$$

[ISO 26262-1:2011]  
["Functional Safety". M. Conrad]  
["Introduction to IEC 61508." R. Faller, W. Goble, J. Keswick (2000)]



	IEC 61508	ISO 26262
Harm	Physical injury or damage to the health of people or damage to property or the environment	Physical injury or damage to the health of persons
Risk	Combination of the probability of occurrence of harm and the severity of that harm	Combination of the probability of occurrence of harm and the severity of that harm

① IEC 61508 and ISO 26262 are functional safety standards



- Fatality risk figures

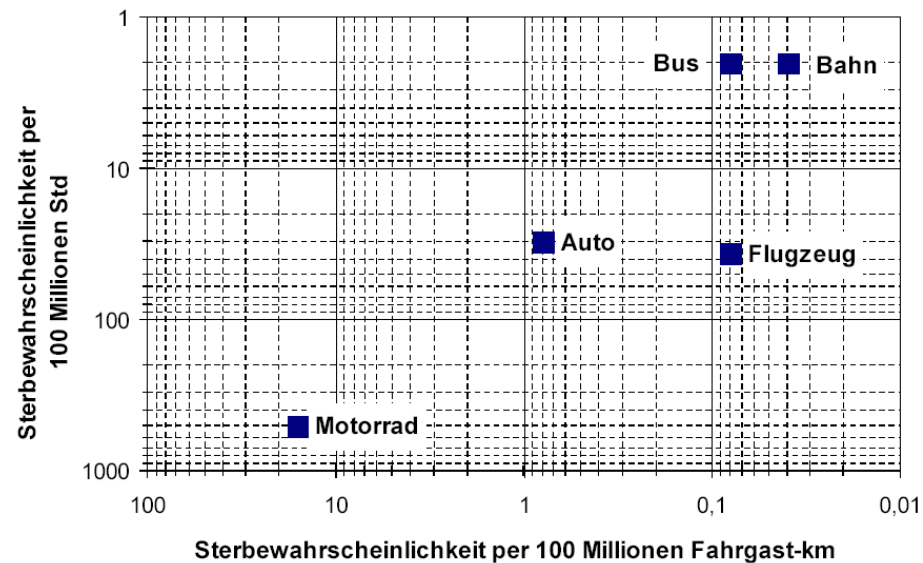
▪ Falling aircraft	$2.0 \cdot 10^{-8} / \text{yr}$	(0.02cpm)
▪ Lightning strike	$1.0 \cdot 10^{-7} / \text{yr}$	(0.1cpm)
▪ Insect / snake bite	$1.0 \cdot 10^{-7} / \text{yr}$	(0.1cpm)
▪ Work accident	$1.0 \cdot 10^{-5} / \text{yr}$	(10cpm)
▪ Road accident	$1.0 \cdot 10^{-4} / \text{yr}$	(100cpm)
▪ Car accident	$1.5 \cdot 10^{-4} / \text{yr}$	(150cpm)
▪ Smoking	$5.0 \cdot 10^{-3} / \text{yr}$	(5000cpm)

cpm ... chances per million of the population per year

# Risk figures

Verkehrsmittel	Sterbefälle pro 100 Millionen Stunden Reisezeit der Fahrgäste	Sterbefälle pro 100 Millionen Kilometer Reisewege der Fahrgäste
Motorrad	500	16
Auto	30	0,8
Bus	2	0,08
Flugzeug	36,5	0,08
Bahn	2	0,04

Quelle: SNCF






[\"Functional Safety\". M. Conrad]

[\"Neue und Herkömmliche Maße zur quantifizierung des Risikos im Eisenbahnverkehr.\" E. Schnieder (2004)]

[Lecture 'Software Engineering II.' H. Schlingloff (2006)]

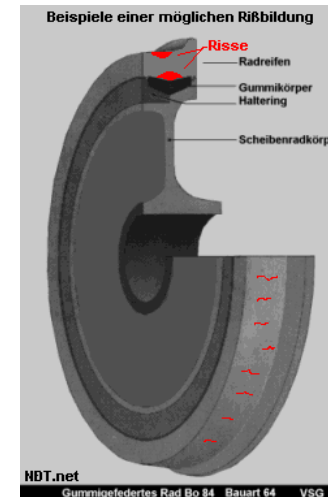
Tabelle 2.1: Verkehrsträger im Vergleich [SBS08]

	Luftfahrt	Automobiltechnik	Eisenbahntechnik
			
<b>Bewegung</b>	3-D (Raum)	2-D (Fläche)	1-D (Linie)
<b>Pilot / Fahrer</b>	i. d. R. 2 (Profis)	1 (Amateur v Profi)	1 (Profi [+ Sicherheitsfahr- schaltung (Sifa)])
<b>Wetter</b>	Allwetter, ohne Sicht	Allwetter, mit Sicht	Allwetter, ohne Sicht
<b>Phasen</b>	Start, Steig-, Reise, Sinkflug, Landung	Stadt, Autobahn, Landstraße, Parken	Bahnhof, freie Strecke
<b>Stückzahlen (in Europa)</b>	$10^3$ (Tendenz fallend)	$10^6$ (Tendenz steigend)	$10^3$ (Tendenz fallend)
<b>Kosten (Elektronik)</b>	ca. 10.000 €/kg	ca. 1.000 €/kg	ca. 1600 €/kg (z.B. PZB 90; 25000€/15kg)
<b>Frequenz der Modellwechsel</b>	ca. 20 Jahre	ca. 7 Jahre	ca. 40 Jahre
<b>Unfalluntersuchungen</b>	Sehr aufwändig aber meist gut dokumentiert	Wenig aufwändig	Sehr aufwändig, Dokumentation wird besser
<b>Instandhaltung, Reparatur</b>	Nur von zugelassenen Betrieben	Auch kleine „Klitschen“, jeder	auch kleine Werkstätte bei NE-Bahnen

# Risk and perception (1)

## Eschede train disaster

- June 3, 1998; Eschede, Lower Saxony, Germany
- World's deadliest high-speed train accident involving an ICE 1 train equipped with single-cast (monobloc) wheels.
- Accident cause: Single fatigue crack in one wheel which, when the wheel finally failed, caused the train to derail at a switch; one derailed car was thrown into the pylons of a roadway overpass which collapsed.
- 101 fatalities, 88 severe injuries



[\"Functional Safety\". M. Conrad]

[Lecture – \"Safety and reliability engineering\" S. Kowalewski (2007)]

## Risk and perception (2)

### Eschede train disaster

- 101 fatalities, 88 severe injuries
- The accident was the news headline for ~5.5 days
- Fatalities from road traffic in the same period: ~100
- How much media attention was given to these fatalities?

## Risk Perception

- Subjective judgment that people make about the characteristics and severity of a risk.

## Risk Aversion

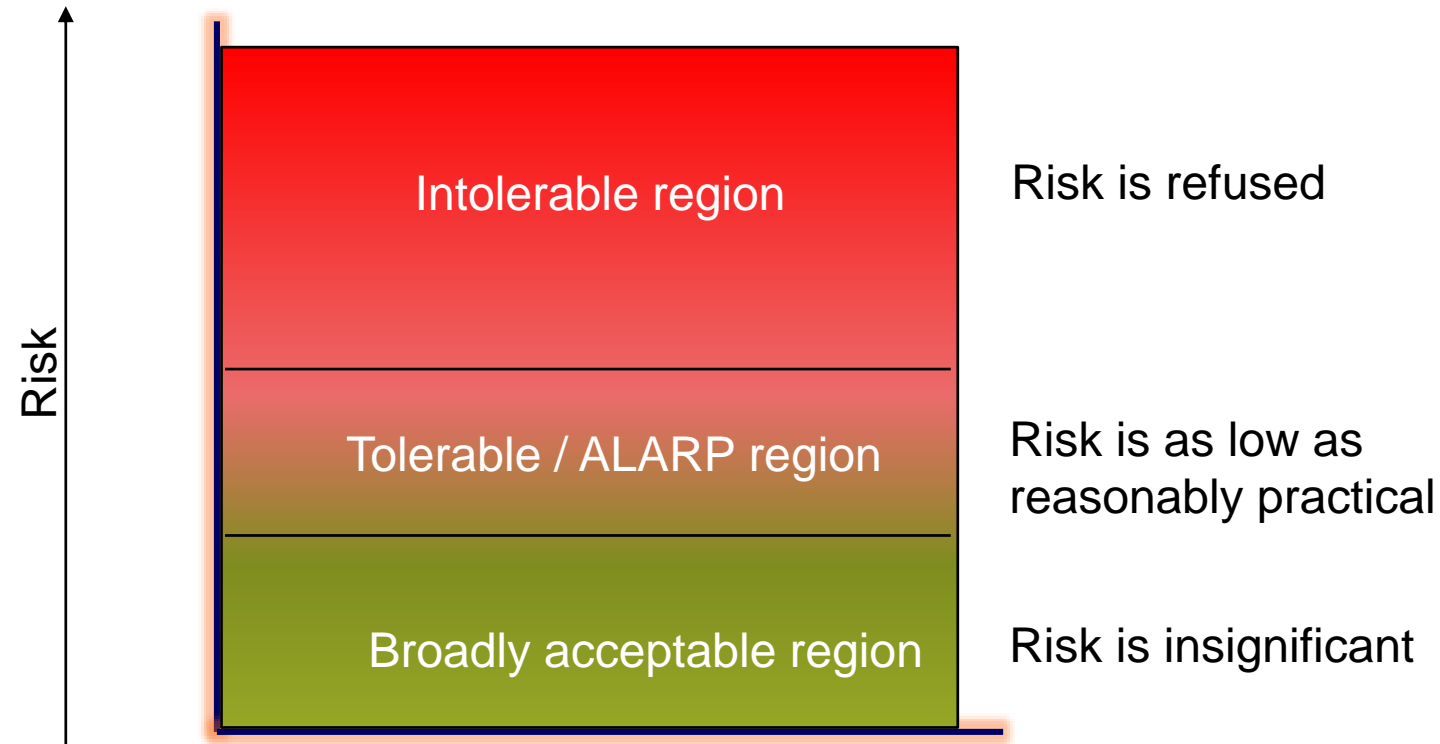
- Reluctance of people to accept a bargain with an uncertain payoff rather than another bargain with more certain, but possibly lower, expected payoff.

## Scale Aversion

- Tendency to want greater protection where consequences are high
  - A scale-averse person would prefer 100 deaths as the result of more frequent incidents in a 10-year period than a single event with 100 deaths in the same period.

["Functional Safety". M. Conrad]  
["Evidence or otherwise of scale aversion: public reactions to major disasters".  
Technical note 03, Environmental Resources Management Ltd. (2009)]

- ALARP (As Low As is Reasonably Practical)



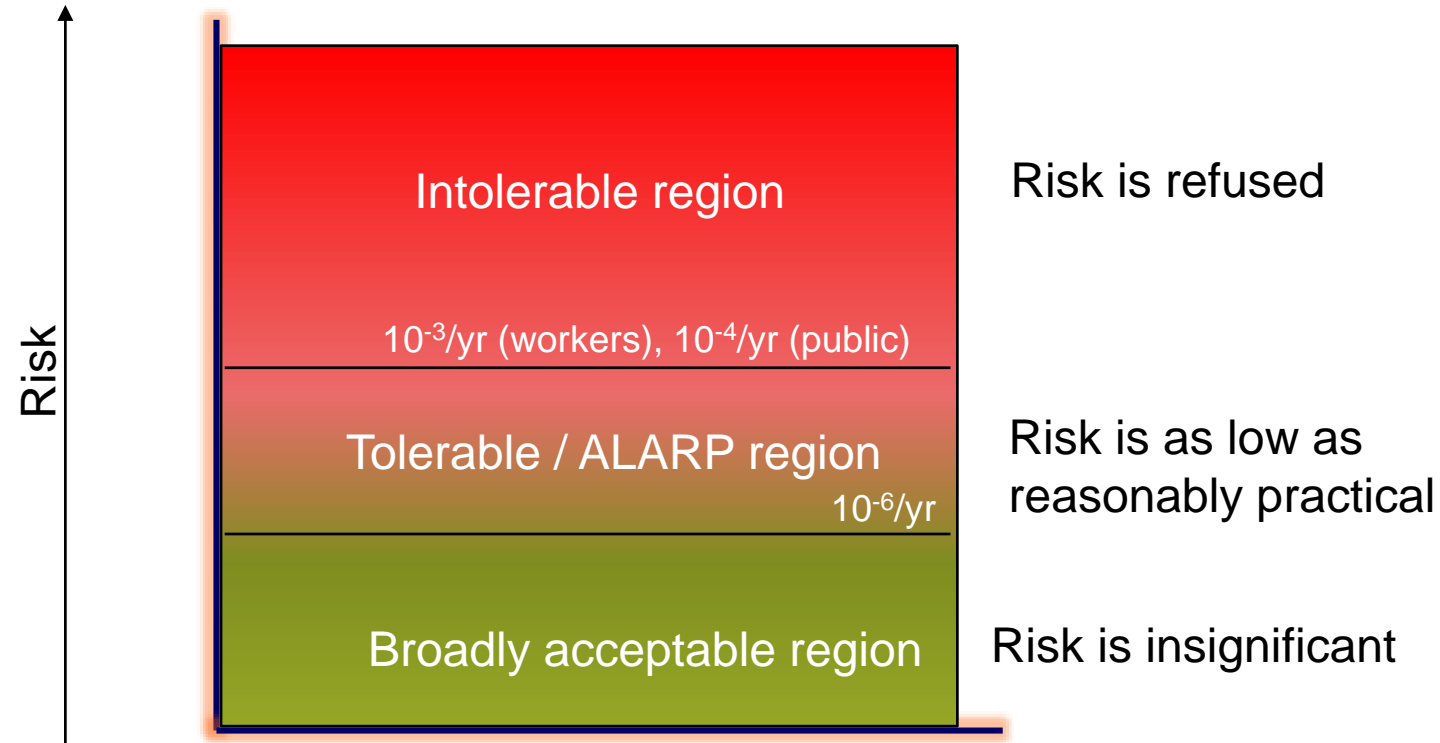
- Defines acceptable risk and influences selection of tools for risk reduction

[*"Functional Safety"*. M. Conrad]

[*"Introduction to IEC 61508"* R. Faller et al. (2000)]

[*"Functional safety for programmable electronics used in PPE: best practice recommendations."* Part 1: Introduction to functional safety. Safety Requirements, Inc., (2007)]

- ALARP example



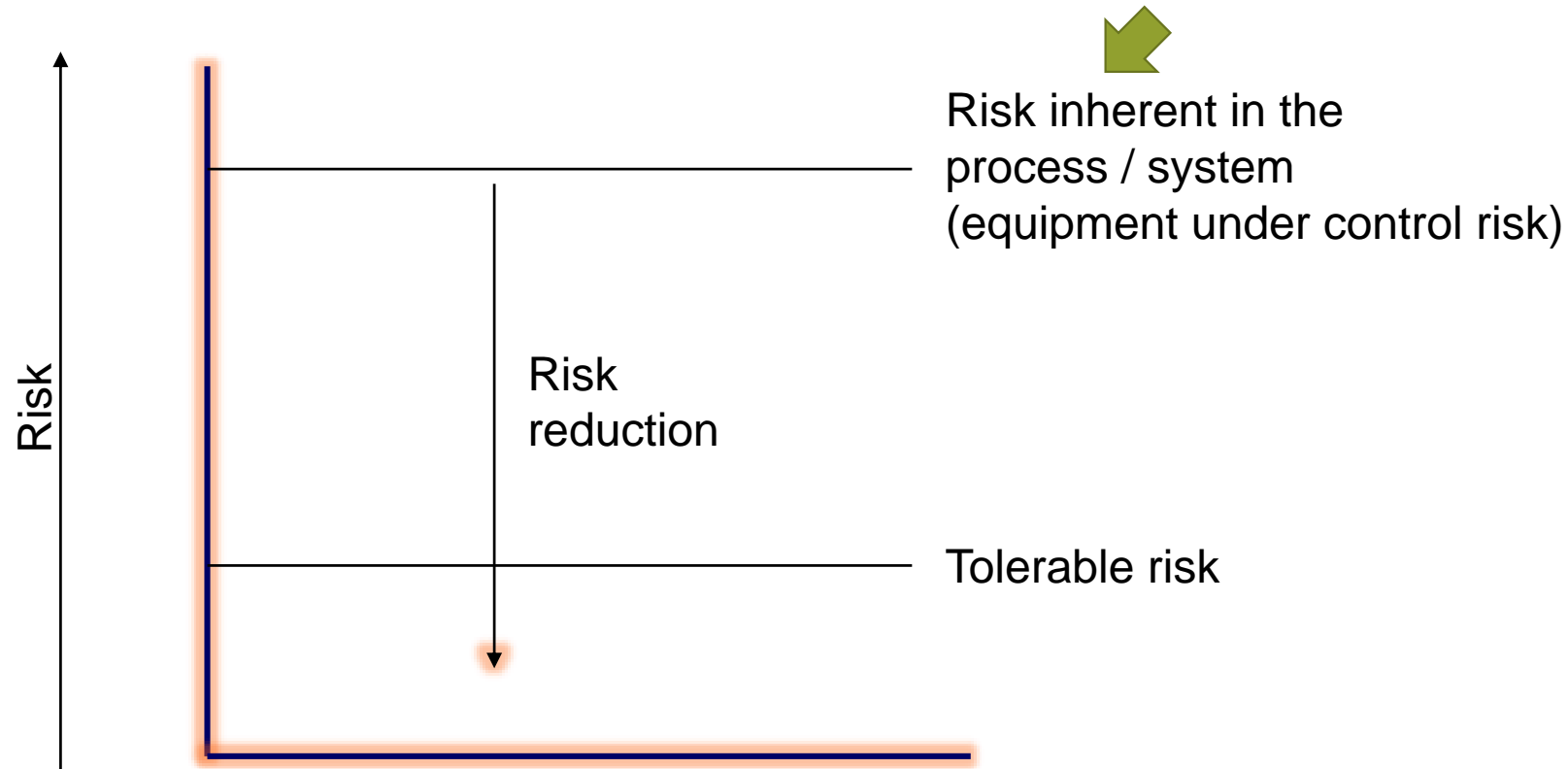
["Functional Safety". M. Conrad]

["Introduction to IEC 61508" R. Faller et al. (2000)]

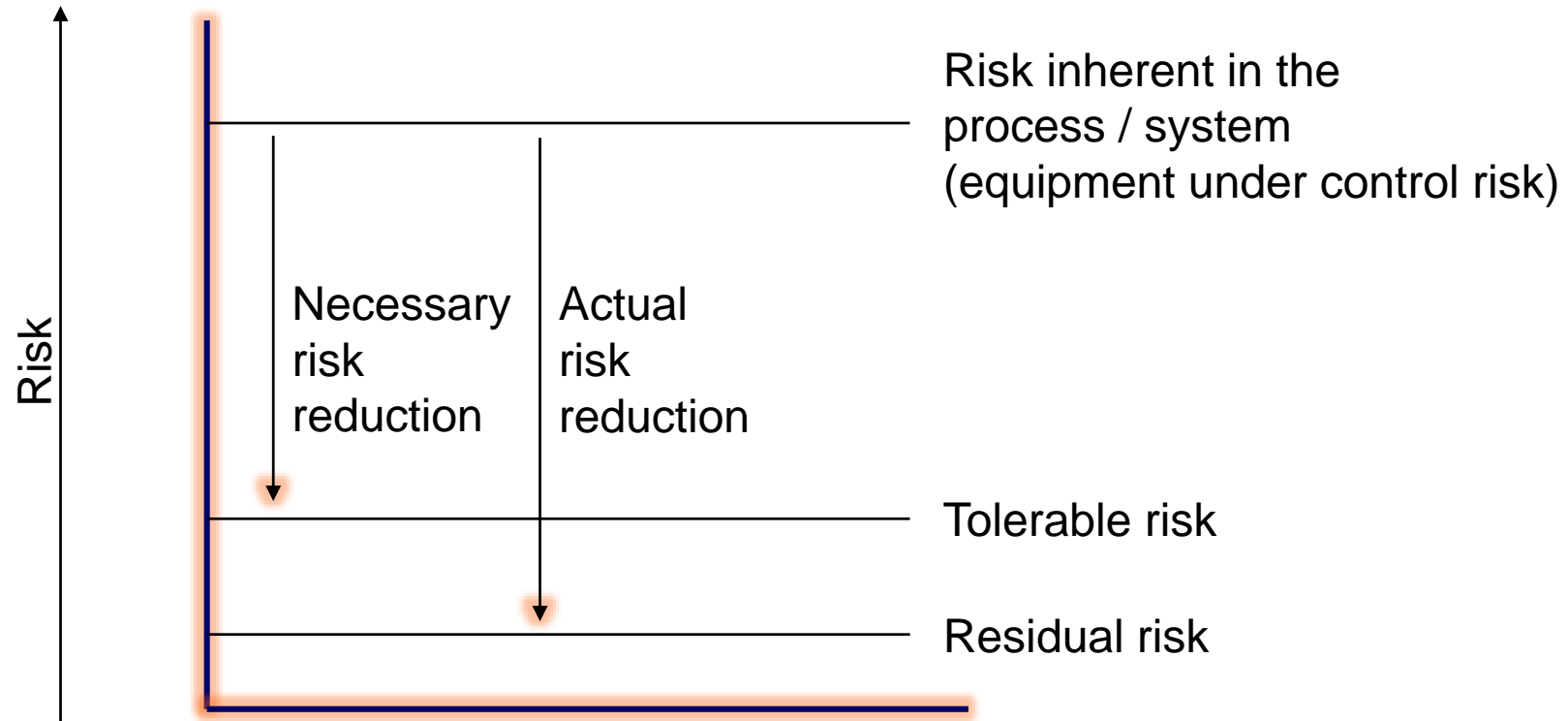
["Functional safety for programmable electronics used in PPE: best practice recommendations." Part 1: Introduction to functional safety. Safety Requirements, Inc., (2007)]



Operating a technical system without dedicated means to reduce its risk would typically exceed the tolerable risk



Goal: Reduce risk to a tolerable level by combining multiple methods / means



Goal: Reduce risk to a tolerable level by combining multiple methods/means (not to zero)

## Different means of risk reduction


Risk reduction  
through  
external  
measures



- Physical containment, guardrails

Risk reduction  
through  
electronics and  
software



Focus of  IEC 61508 and ISO 26262

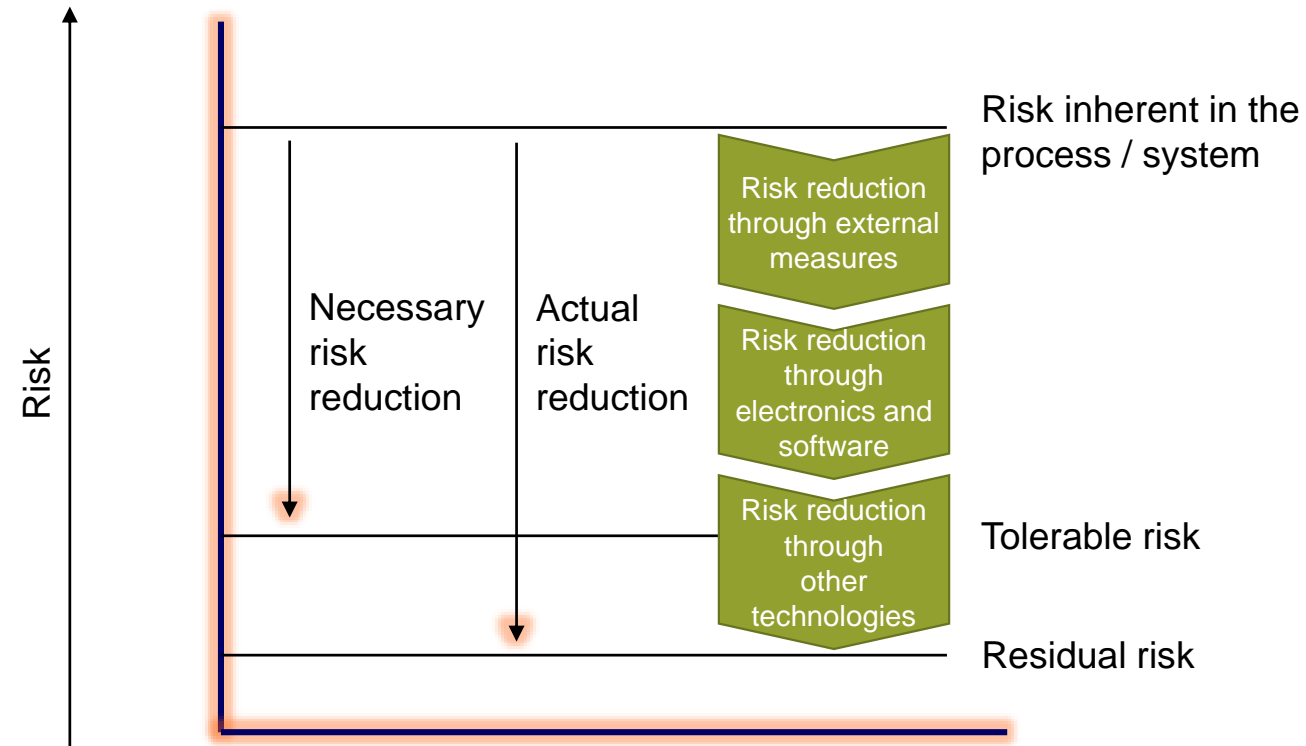
Risk reduction  
through  
other  
technologies



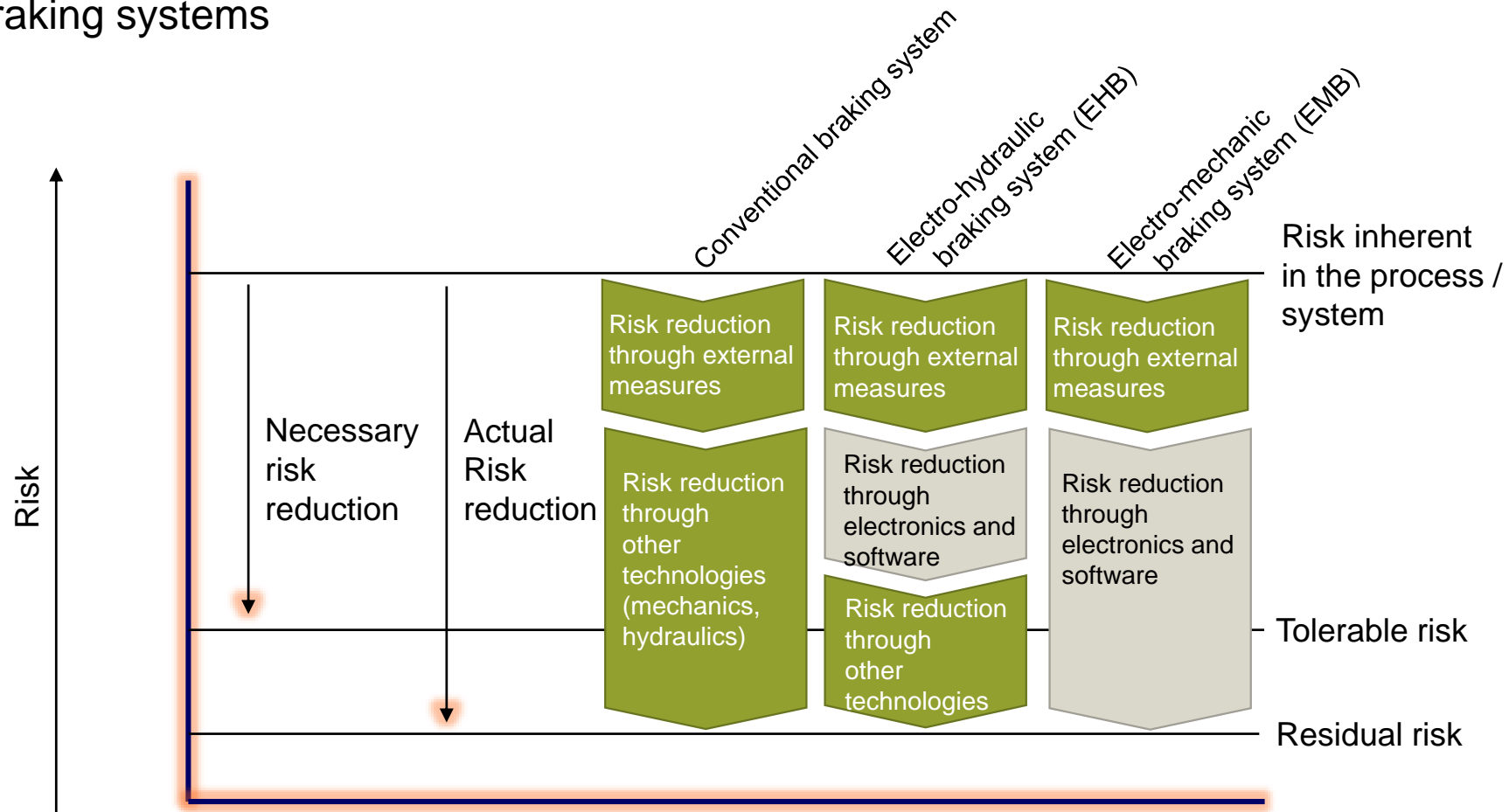
- Safety valves, hydraulic back-up

[ "Functional Safety". M. Conrad]  
[cf. intecs / ikv: ISO 26262 – Introduction and Overview. Training materials 2011, <http://www.tagesschau.de/inland/pkw-maut100.html>]

# Risk reduction

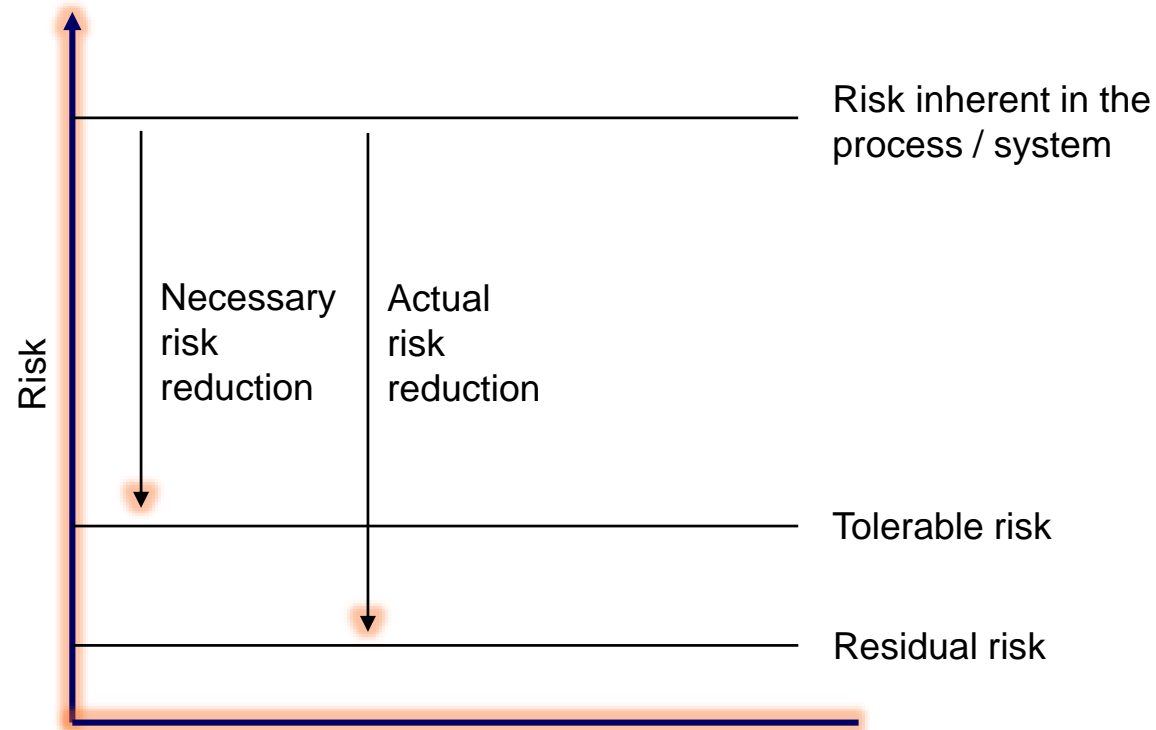


## Braking systems

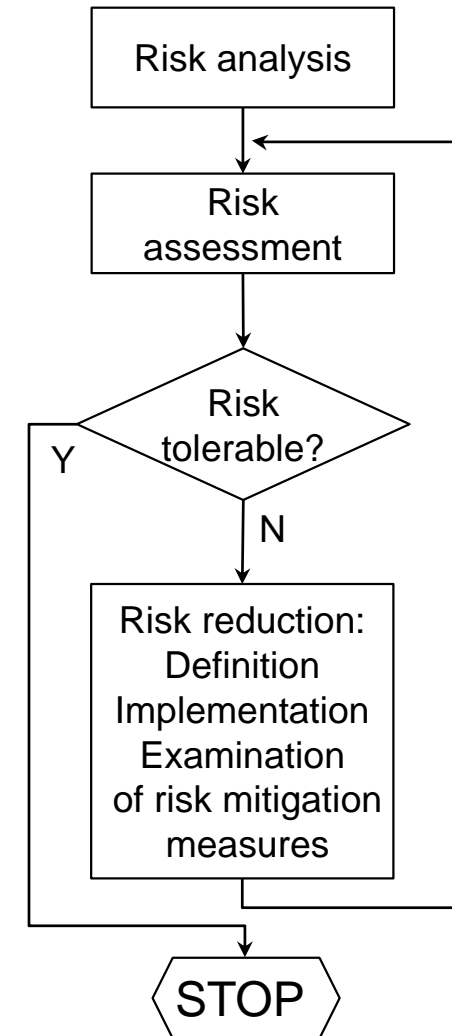


["Functional Safety". M. Conrad]

["Funktionale Sicherheit in der KFZ-Elektronik Fachseminar zur Interpretation der IEC 61508." M. Rau]



Iterative process



["Functional Safety". M. Conrad]  
[Lecture "Entwicklung und Test von verteilten, eingebetteten  
Systemen im Bereich Automotive." K. Dussa-Zieger, U. Hehn (2007)]



Considering the concepts discussed so far (harm, risk), how would you define safety ?





Considering the concepts discussed so far (harm, risk), how would you define safety ?

## Safety

Freedom from / absence of unacceptable / unreasonable risk



	IEC 61508	ISO 26262
Safety	Freedom from unacceptable risk	Absence of unreasonable risk

	IEC 61508	ISO 26262
Harm  Schaden	Physical injury or damage to the health of people or damage to property or the environment	Physical injury or damage to the health of persons
Risk  Risiko	Combination of the probability of occurrence of harm and the severity of that harm	Combination of the probability of occurrence of harm and the severity of that harm
Tolerable Risk	Risk which is accepted in a given context based on the current values of society	---
Unreasonable Risk	---	Risk judged to be unacceptable in a certain context according to valid societal moral concepts
Safety	Freedom from unacceptable risk	Absence of unreasonable risk

[IEC 61508-4:2010] [ISO 26262-1:2011] ["Functional Safety". M. Conrad]

Stakeholders:

- **Society, customers, lawmakers, regulatory bodies**
  - Have rising expectations regarding accident prevention as well as avoidance of injuries or damage to the health of persons
  - Demand risk reduction to a tolerable level
  
- **Manufactures, suppliers, dealers / distributors**
  - Want to satisfy expectations of customers and society
  - Fear loss of reputation caused by accidents / disasters
  - Prefer to avoid claims for damages and law suites



Gefahr,  
Gefährdung

## Hazard

- Potential source of harm

- A hazard is something that can cause harm, e.g. electricity, chemicals, working up a ladder, noise, a keyboard, a bully at work, stress, etc.
- A risk is the chance, high or low, that any hazard will actually cause somebody harm.



[["What is the difference between a 'hazard' and a 'risk'?"](#). Worksmart]

# From requirements to system design

2.1. Software architecture

2.2. Antipatterns in software engineering

2.3. Reuse

2.4. Testability

2.5. Safety

2.5.1. Terminology

2.5.2. Risk

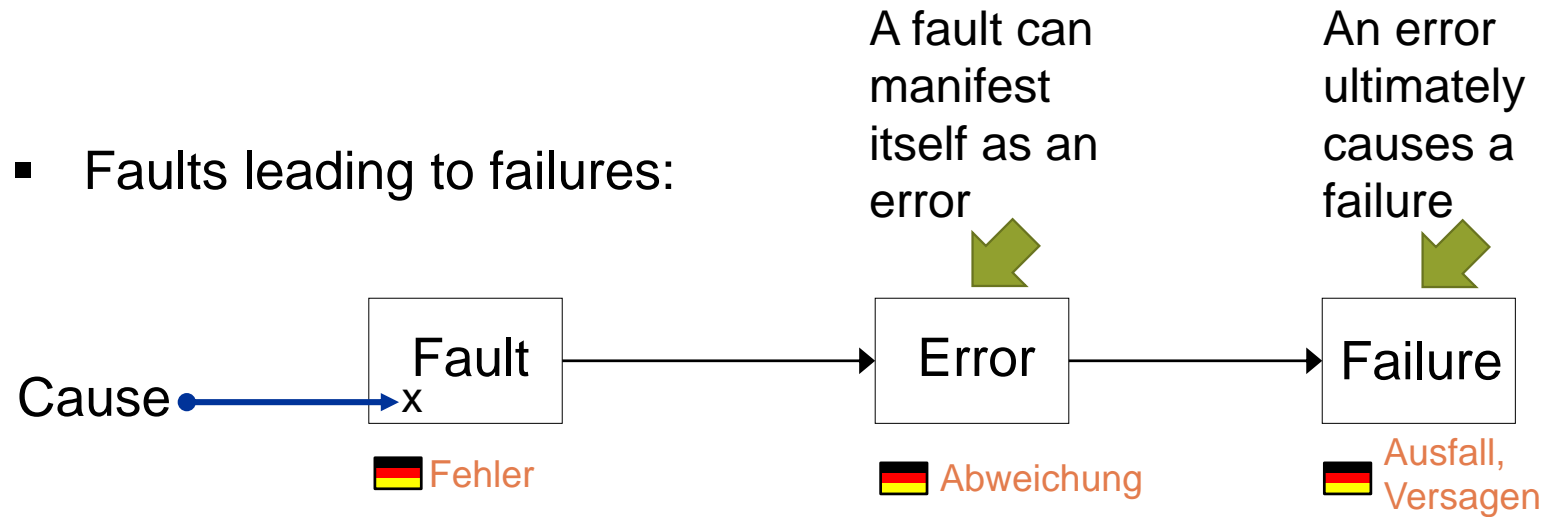
**2.5.3. Faults, errors, and failures**

2.5.4. Functional safety

2.5.5. Safety analyses using FMEA and FTA

2.6. Information security

- Faults leading to failures:



**Terms used differently in other contexts!**

## **Fehler**

**(en: fault)**

Nicht normale Bedingung, die eine Verminderung oder den Verlust der Fähigkeit einer Funktionseinheit verursachen kann, eine geforderte Funktion auszuführen.

## **Abweichung**


**(en: error)**


Nichtübereinstimmung zwischen Rechenergebnissen, beobachteten oder gemessenen Werten oder Beschaffenheiten und den betreffenden wahren, spezifizierten oder theoretisch richtigen Werten oder Beschaffenheiten.

## **Ausfall / Versagen**


**(en: failure)**

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen.





	IEC 61508	ISO 26262
Fault  Fehler	Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function	Abnormal condition that can cause an element or an item to fail

	IEC 61508	ISO 26262
<b>Error</b>  Abweichung	Discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition	Discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretically correct value or condition  NOTE An error can arise as a result of unforeseen operating conditions or due to a fault within the system, subsystem or component being considered.









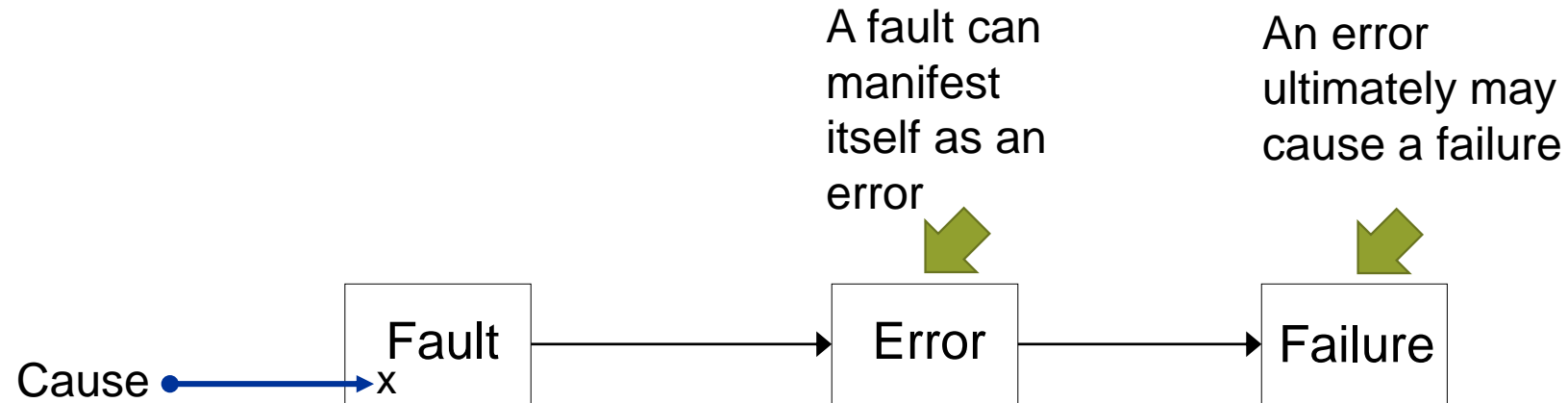
	IEC 61508	ISO 26262
<b>Failure</b>  Ausfall, Versagen	Termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required	Termination of the ability of an element, to perform a function as required  NOTE Incorrect specification is a source of failure.

## Aviation

- Bit flips due to cosmic rays, or a fire  
- As a consequence, incorrectly computed altitude of an airplane  
- As a consequence, crash of the airplane  

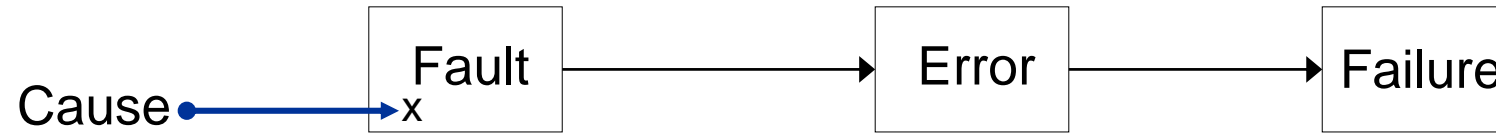
## Software testing: different terminology

- Wrong code  
  - Wrong state of the program (wrong w.r.t. a specification)  
  - Wrong output of the program (wrong w.r.t. a specification)  
- 
- **A fault will lead to an error**
  - **Errors need not lead to failures** because of
    - Masking (by chance, the error is corrected)
    - Special mechanisms like redundancy



- **Random issues**  
(typically, due to physical processes such as damage or fatigue)
- **Systematic issues**  
(typically, due to specification or design issues, or hardware wear-out)

# Random vs systematic issues



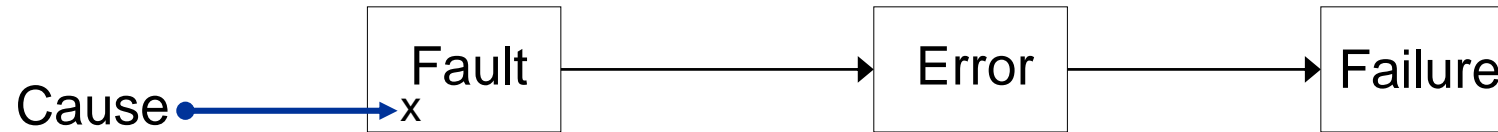
- Random issues
- Systematic issues



- Which type(s) of issue(s) can occur in hardware?
- Which type(s) of issue(s) can occur in software?

	Hardware	Software
Systematic issues		
Random issues		

# Random vs systematic issues



- Random HW issues
- Systematic HW issues
- Systematic SW issues

- Random HW faults
- Systematic HW faults
- Systematic SW faults

- Random HW failures
- Systematic HW failures
- Systematic SW failures

	Hardware	Software
Systematic issues	✓	✓
Random issues	✓	✗

### Failure

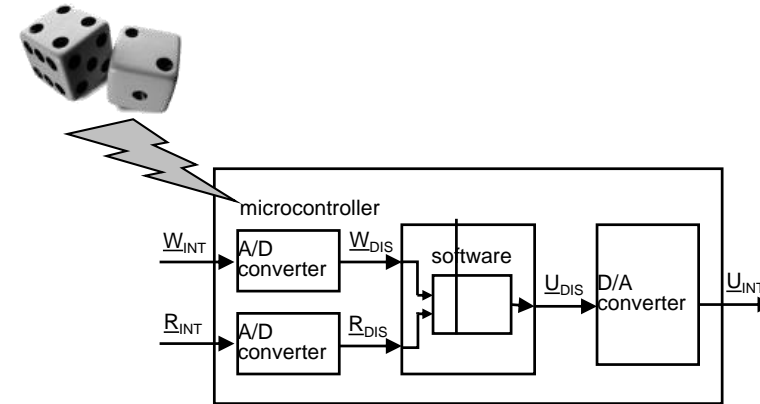
- Termination of the ability to perform a required function

### Random Failure (in hardware)

- Failure occurring at a random time during operation

### Systematic Failure (in hardware or software)

- Failure related in a deterministic way to a certain cause
- Can only be eliminated by a modification of the design, the manufacturing process, operational procedures, documentation etc.



# Random vs systematic failure

- **Random Failure**

- Results from hardware degradation
- Occurs at a random time
- Resulting system failure rates can be predicted with reasonable accuracy

- **Systematic Failure**

- Related in a deterministic way to a certain cause
- Can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation etc.
- Cannot be accurately predicted / statistically quantified

	IEC 61508	ISO 26262
Systematic failure	<p>Failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.</p> <p>NOTE Examples of causes of systematic failures include human error in</p> <ul style="list-style-type: none"><li>▪ the safety requirements specification;</li><li>▪ the design, manufacture, installation, operation of the hardware;</li><li>▪ the design, implementation, etc. of the software.</li></ul> <p>NOTE In this standard, failures in a safety-related system are categorized as random hardware failures or systematic failures.</p>	<p>Failure, related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.</p>



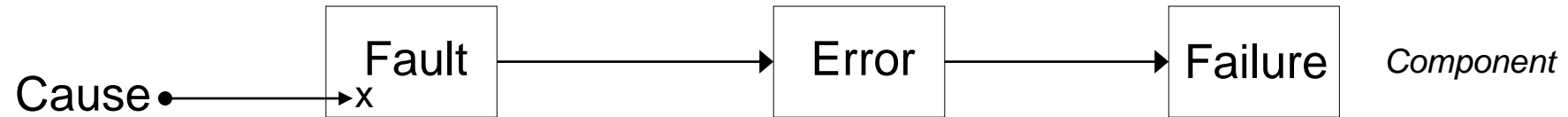
	IEC 61508	ISO 26262
Random failure	<p>Termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required.</p> <p>NOTE Performance of required functions necessarily excludes certain behavior, and some functions may be specified in terms of behavior to be avoided. The occurrence of such behavior is a failure.</p> <p>NOTE Failures are either random (in hardware) or systematic (in hardware or software).</p>	

	IEC 61508	ISO 26262
Random hardware failure	<p>Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.</p> <p>NOTE There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.</p> <p>...</p>	<p>Failure that can occur unpredictably during the lifetime of a hardware element and that follows a probability distribution.</p> <p>NOTE Random hardware failure rates can be predicted with reasonable accuracy.</p>

	IEC 61508	ISO 26262
Random hardware failure	<p>...</p> <p>NOTE A major distinguishing feature between random hardware failures and systematic failures, is that system failure rates, arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.</p>	

# How systems fail?

Example: Engine control unit (component level)



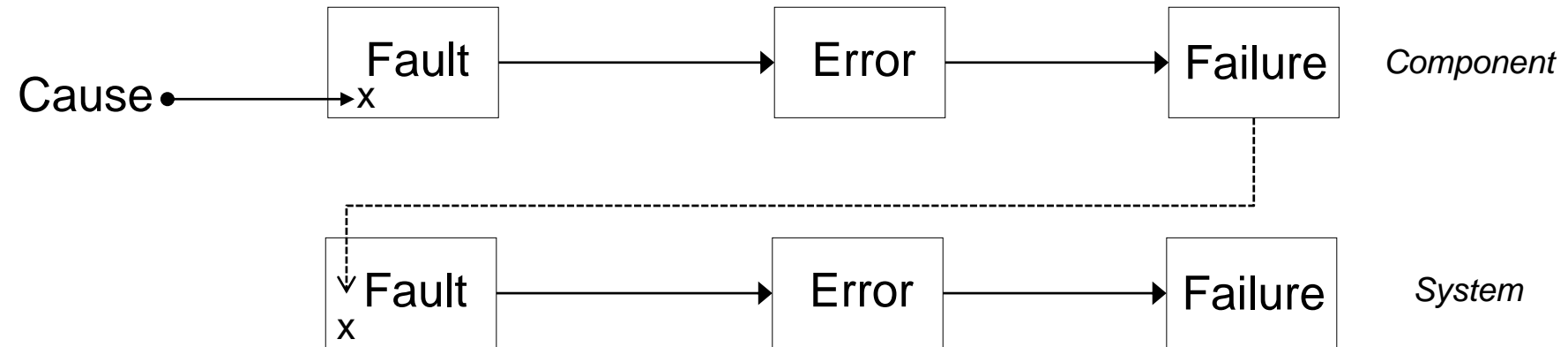
Random HW	Oxidation	Loss of electrical connection	Ignition coil intermittently wrongly without current
Systematic HW	Insufficient EMC protection of engine ECU w.r.t. wiper cable EMC susceptibility	Program sequence in engine ECU is disturbed	Engine ECU intermits operation when wiper is switched on
Systematic SW	Programming error at loop termination condition	Unwanted endless loop leading to watchdog reset	Engine ECU stops operation intermittently

EMC – Electromagnetic compatibility

[ISO/DIS 26262-10: 2009]  
["[Functional Safety](#)". M. Conrad]

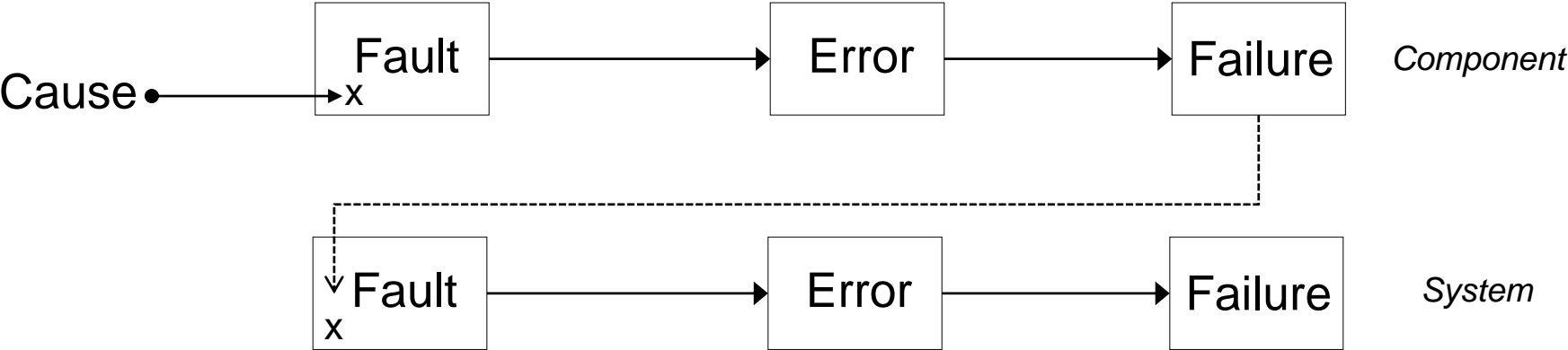
# How systems fail?

- Failures at the component level can represent faults at the system level



# How systems fail?

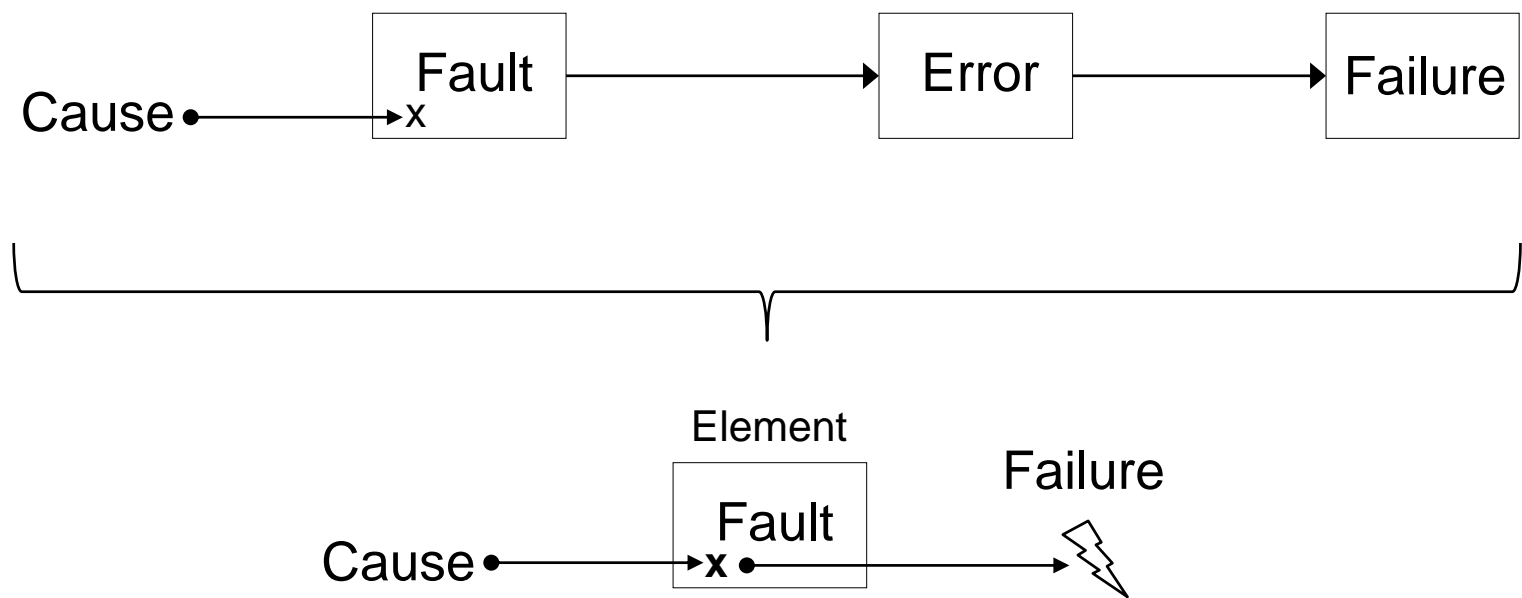
Example: Vehicle (system level)



Random HW	Ignition coil intermittently wrongly without current		
Systematic HW	Engine ECU intermits operation when wiper is switched on	Ignition interrupted by intermittence	Vehicle bucks
Systematic SW	Engine ECU stops operation intermittently		

# How systems fail?

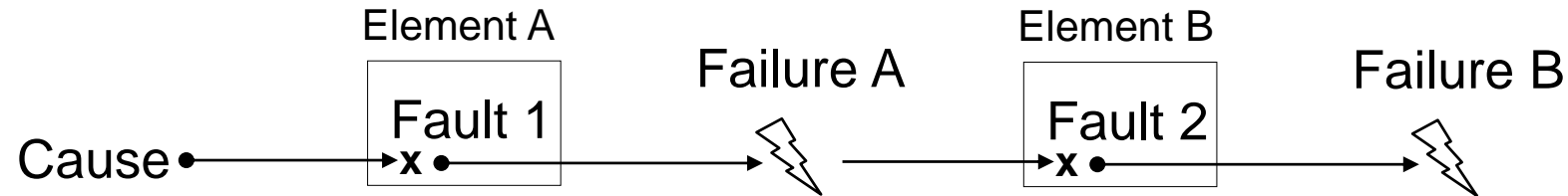
Abbreviated notation:



# How systems fail?

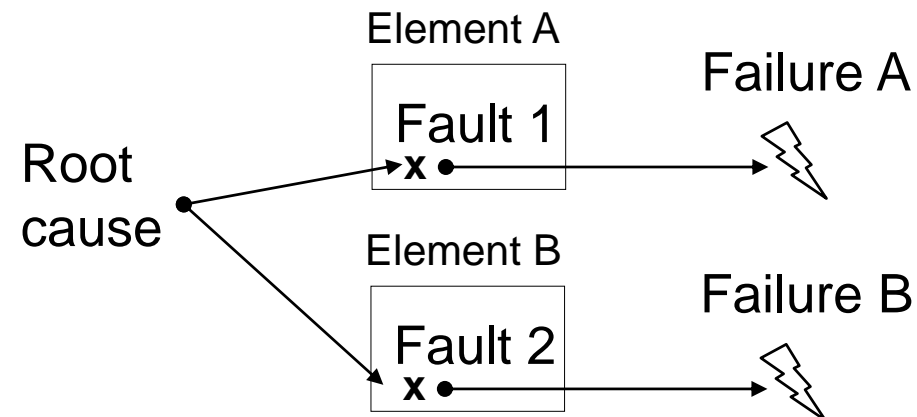
- **Cascading failure:**

Failure of an element causing another element of the same item to fail



- **Common cause failure (CCF):**

Failure of two or more elements resulting from a single specific event or root cause

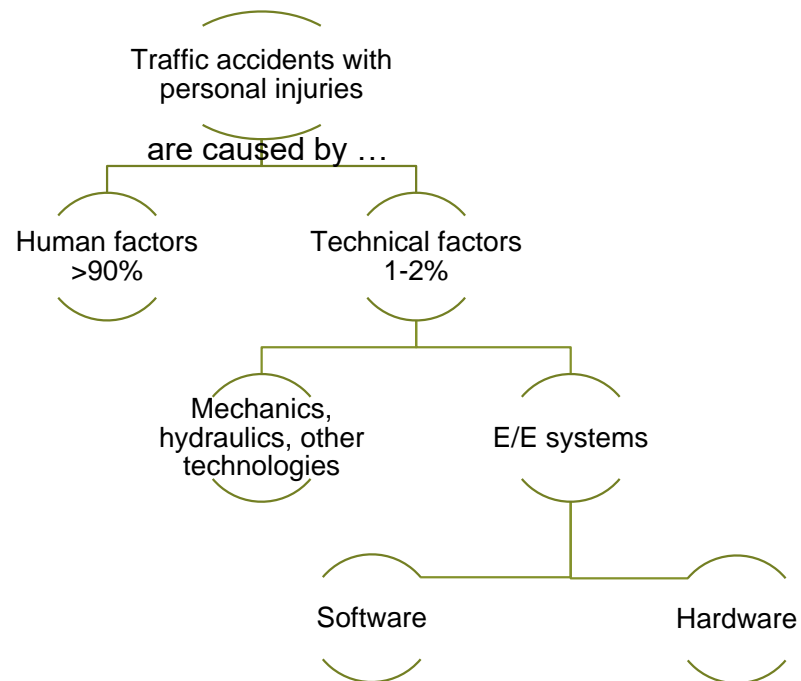




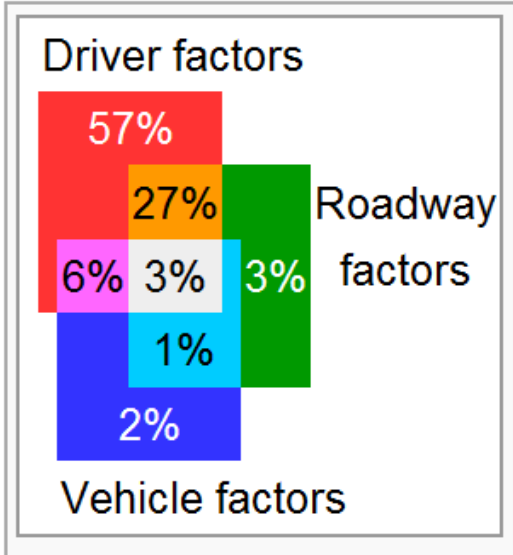


What percentage of traffic accidents with bodily injuries is caused by technical (vs. human) factors?





## Breakdown of British and American crash causes



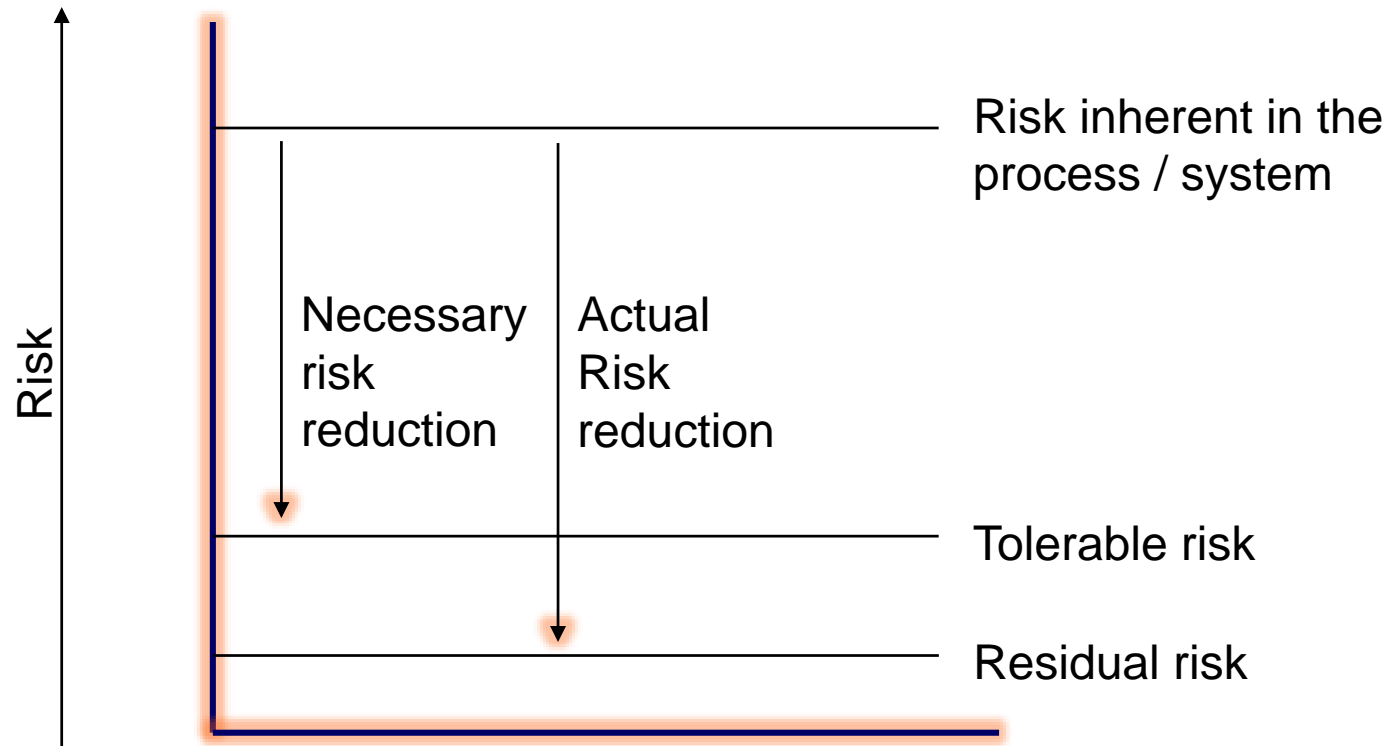
[["Functional Safety"](#). M. Conrad]

[DaimlerChrysler REI/AA (2005)]

[["Interactive Highway Safety Design Model: Accident Predictive Module."](#) Public Roads Magazine. H. Lum, and J. A. Reagan. (1995)]

# Recap

## Risk reduction



Goal: Reduce risk to a tolerable level (not to zero)

**Avoidance of systematic faults** during design, production, ...

- Use of techniques and procedures that aim to avoid the introduction of faults during any phase of the safety lifecycle

**Tolerance re. systematic faults** during operation

- Ability of a functional unit to continue to perform a required function in the presence of systematic faults or errors

**Tolerance re. random faults** during operation

- Ability of a functional unit to continue to perform a required function in the presence of random faults or errors

# From requirements to system design

2.1. Software architecture

2.2. Antipatterns in software engineering

2.3. Reuse

2.4. Testability

2.5. Safety

2.5.1. Terminology

2.5.2. Risk

2.5.3. Faults, errors, and failures

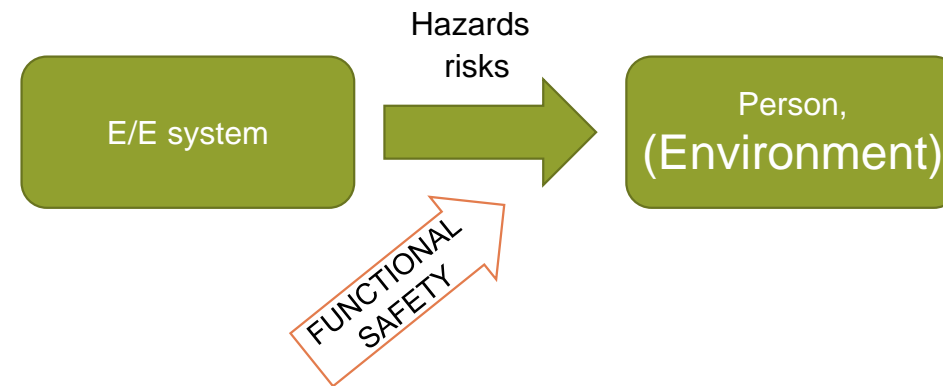
**2.5.4. Functional safety**

2.5.5. Safety analyses using FMEA and FTA


2.6. Information security

# Functional safety

- Functional safety focuses on the hazards and risks originating from the function of an (E/E) system.
  - It does not cover risks like fire or environmental pollution.



**Functional Safety:** Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems

	IEC 61508	ISO 26262
Safety	Freedom from unacceptable risk	Absence of unreasonable risk
Functional Safety	Part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures.	Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems. 

Equipment Under Control (EUC)

Electrical/Electronic/Programmable Electronic system (E/E/PE system)

Electrical and/or Electronic system (E/E system)

- Concept can be traced back to 1947.
- Manufacturer takes a systems approach by designing and building safety into the entire system from initial conceptualization to decommissioning.
- Concept applicable to safety of complex electronics and software-based systems.

"The primary concern of the safety life cycle is the management of hazards: their identification, evaluation, elimination, and control through analysis, design and management procedures."

[N. Leveson (1995)]

[["Functional Safety"](#). M. Conrad]

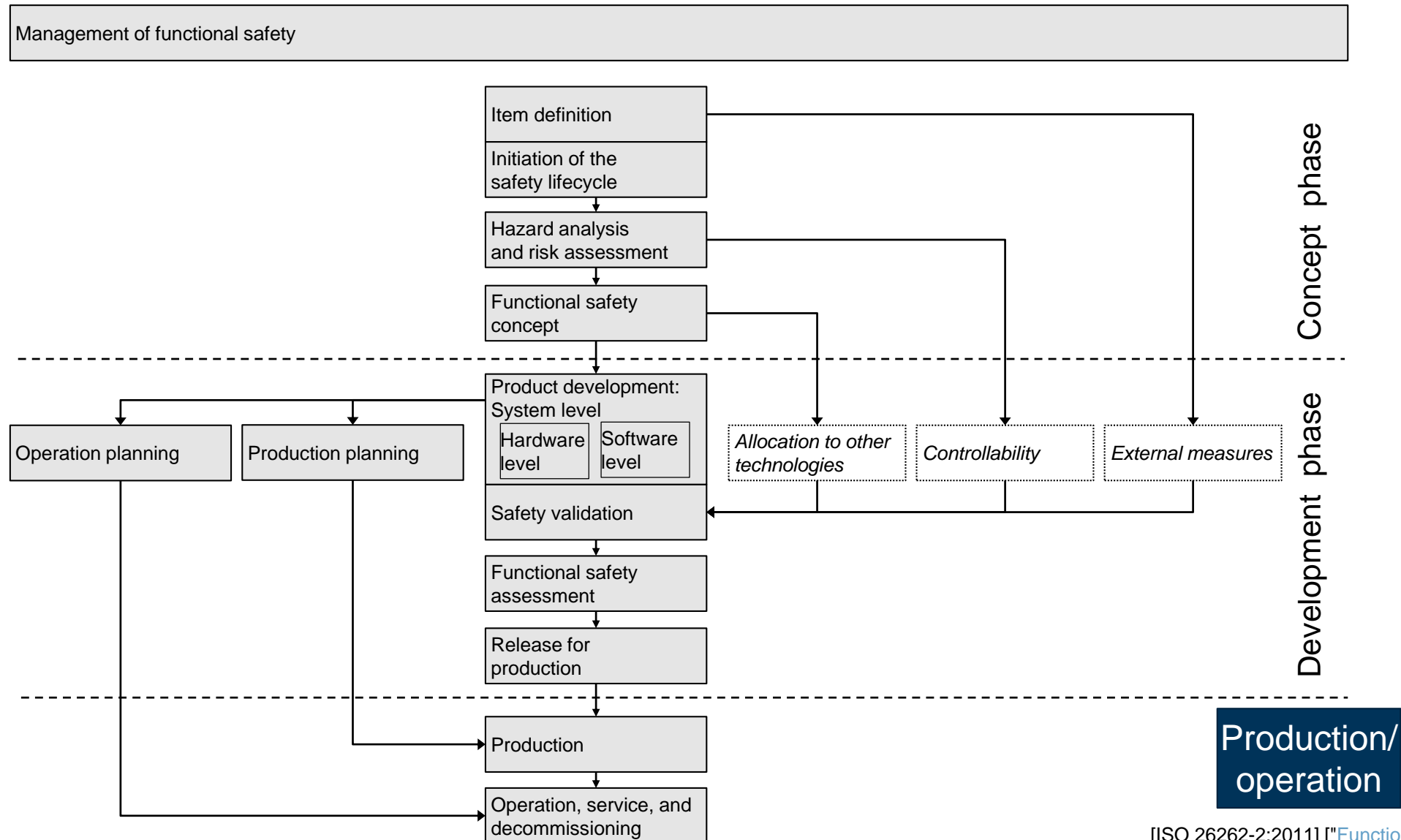
[["Functional safety for programmable electronics used in PPE: Best practice recommendations."](#) Part 1: Introduction to functional safety. Safety requirements, Inc., (2007)]



- It emphasizes:
  - Integration of safety into the design
  - Systematic hazard identification and analysis
  - Addressing the entire system in addition to the subsystems and components
  - Using protection layers for risk reduction
  - Qualitative and quantitative approaches
- To achieve functional safety, manufacturers construct and implement a safety lifecycle suitable for each application.

[["Functional Safety"](#). M. Conrad]  
["Functional safety for programmable electronics used in  
PPE: Best practice recommendations." Part 1: Introduction  
to functional safety. Safety requirements, Inc., (2007)]

# ISO 26262: Safety lifecycle model

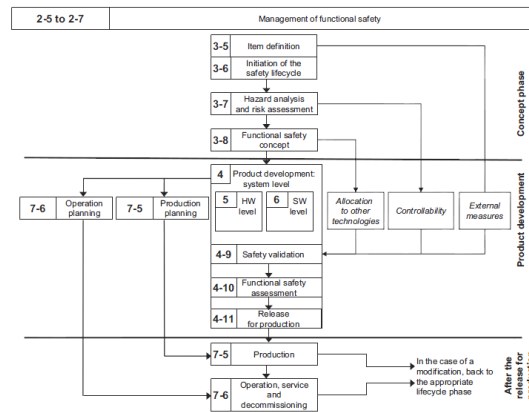


[ISO 26262-2:2011] [[Functional Safety](#)]. M. Conrad]

# Goals, requirements, specifications

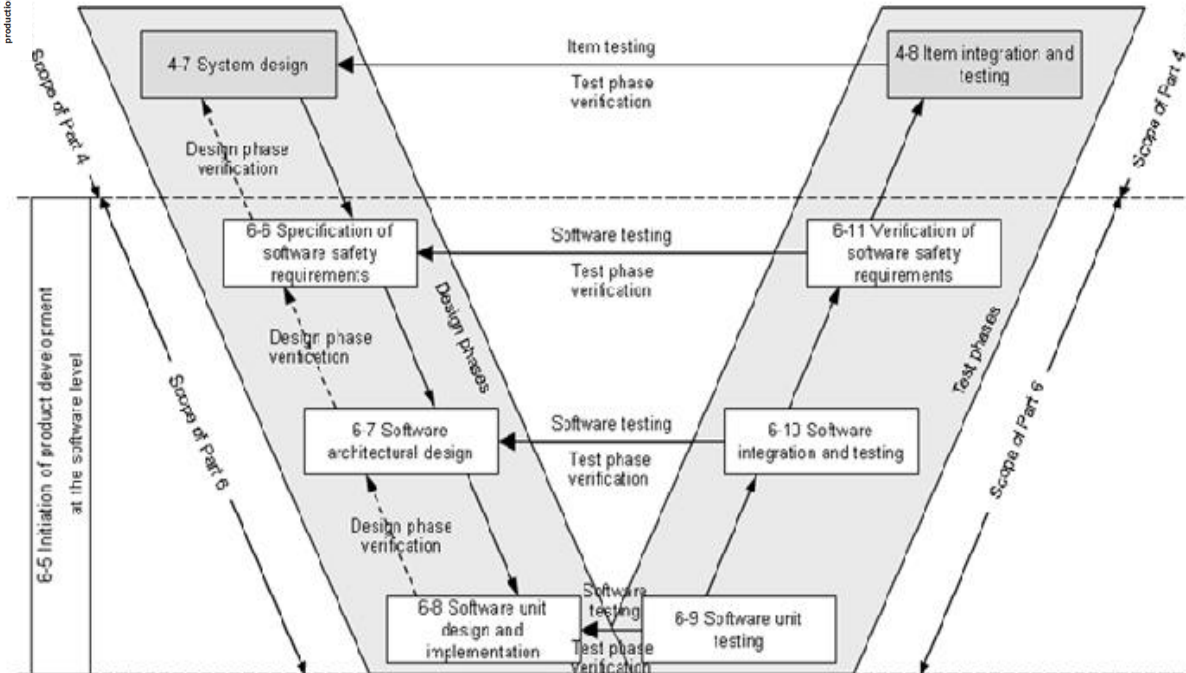
- *Hazard analysis and risk assessment* identify hazards that require risk reduction.
  - A safety goal is formulated for each hazardous event.
  - An Automotive Safety Integrity Level (ASIL) is associated with each safety goal.
- The *functional safety concept* is a statement of the functionality to achieve the safety goal.
  - Stated in the functional safety requirements
- The *technical safety concept* is a statement of how this functionality is implemented in hardware or software.
  - Stated in the technical safety requirements.
- Software safety requirements and hardware safety requirements state the specific safety requirements which will be implemented as part of the software and hardware designs

# ISO 26262: Software lifecycle model



**Objective:** Avoidance of systematic faults

- Generic description that provides guidance for the individual phases
- To be tailored when used in a specific project



ISO 26262 reference phase model for software development

	IEC 61508	ISO 26262
Lifecycle		Entirety of phases from concept through decommissioning of the item.
Software lifecycle	Activities occurring during a period of time that starts when software is conceived and ends when the software is permanently decommissioned.	---
Safety lifecycle	Necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems and other risk reduction measures are no longer available for use	---

	IEC 61508	ISO 26262
Phase	---	Stage in the safety lifecycle that is specified in a distinct part of ISO 26262

# Translation of safety terminology

Hazard	Gefahr / Gefährdung
Harm	Schaden
Risk	Risiko
Hazard analysis and risk assessment	Gefahren- und Risikoanalyse (GuR)
Fault	Fehler, Mangel
Error	Abweichung
Failure	Ausfall, Versagen
Safety	(Betriebs-)Sicherheit
Security	(Angriffs-)Sicherheit
Safety goal	Sicherheitsziel
Safety integrity level	Sicherheitsintegritätsstufe

# From requirements to system design

2.1. Software architecture

2.2. Antipatterns in software engineering

2.3. Reuse

2.4. Testability

2.5. Safety

2.5.1. Terminology

2.5.2. Risk

2.5.3. Faults, errors, and failures

2.5.4. Functional safety

**2.5.5. Safety analyses using FMEA and FTA**

2.6. Information security



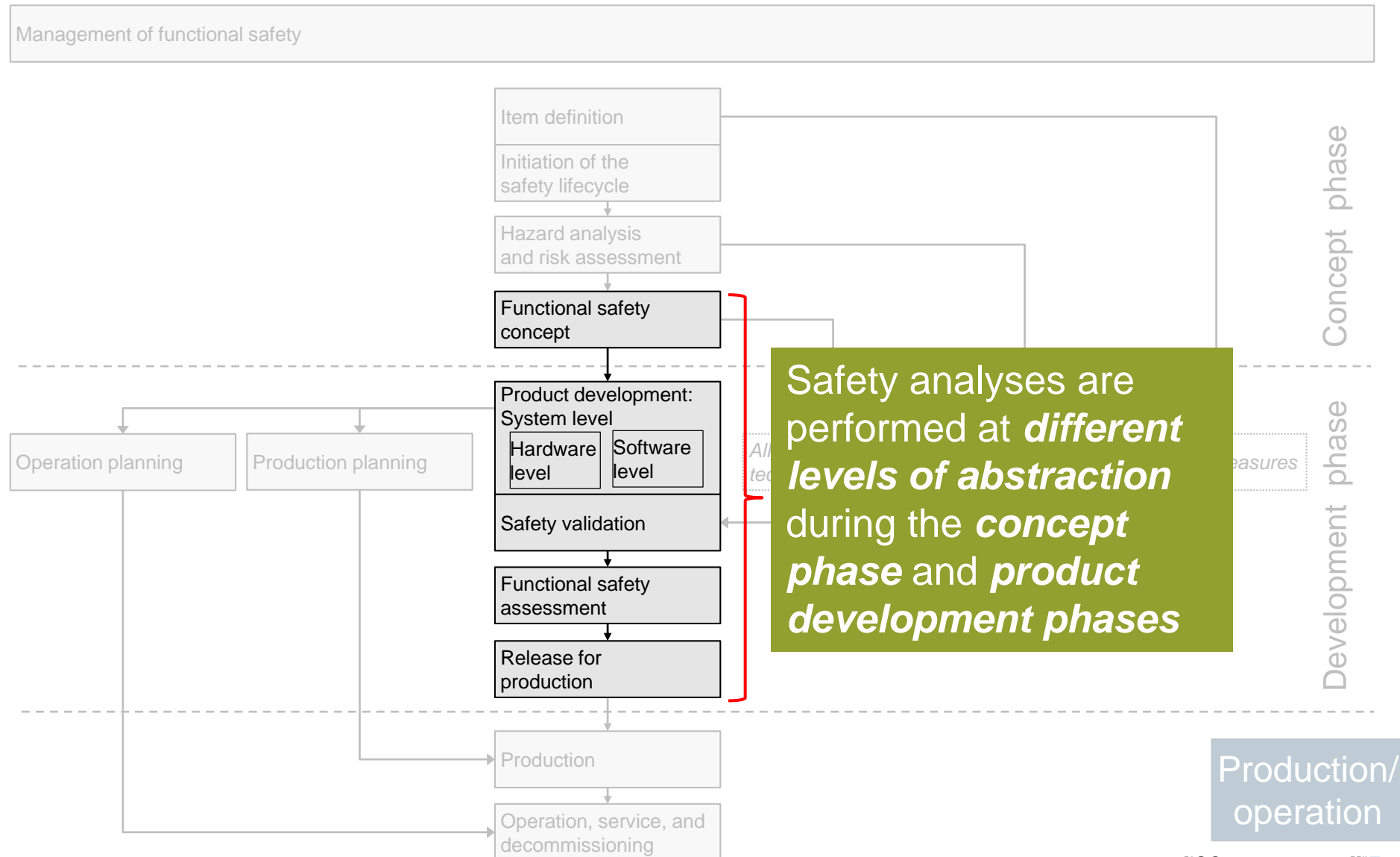
## Objectives

- Examine consequences of faults and failures on functions, behavior and design of items / elements.
- Provide information on conditions / causes that could lead to violation of a safety goal or safety requirement.
- Contribute to identification of new functional or non-functional hazards not previously identified during the hazard analysis and risk assessment.



- General scope
  - Validation of safety goals and safety concepts
  - Verification of safety concepts and safety requirements
  - Identification of conditions and causes, incl. faults and failures, that could lead to the violation of a safety goal or safety requirement
  - Identification of additional requirements for detection of faults or failures
  - Determination of required responses (actions/measures) to detected faults or failures
  - Identification of additional requirements for verifying that the safety goals or safety requirements are complied with, incl. safety-related vehicle testing

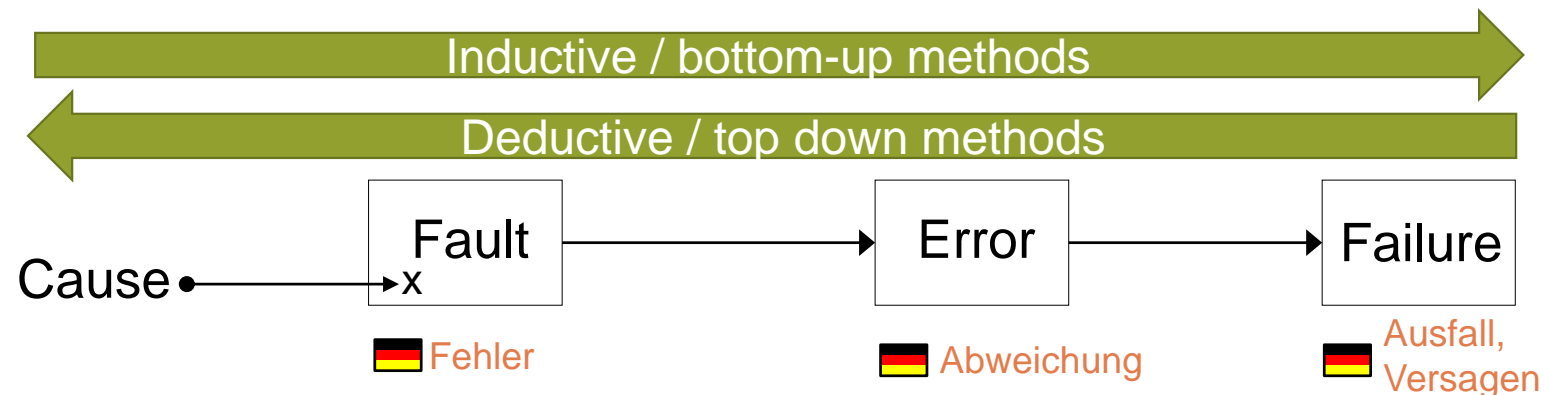
# Safety analyses in the automotive safety lifecycle



Qualitative analysis methods	vs.	Quantitative analysis methods
<ul style="list-style-type: none"> <li>Identify failures</li> <li>Do not predict frequency of failures</li> </ul>		<ul style="list-style-type: none"> <li>Complement qualitative analyses</li> <li>Predict the frequency of random hardware failures</li> <li>Used to verify hardware designs                             <ul style="list-style-type: none"> <li>Against targets for evaluation of hardware architectural metrics</li> <li>Evaluation of safety goal violations due to random hardware failures</li> </ul> </li> </ul>
Require knowledge: <ul style="list-style-type: none"> <li>Relevant fault types / fault models</li> </ul>		Required knowledge <ul style="list-style-type: none"> <li>Relevant fault types / fault models</li> <li>Quantitative failure rates of the hardware elements</li> </ul>
Examples: <ul style="list-style-type: none"> <li>Qualitative system, design, or process FMEA</li> <li>Qualitative FTA</li> <li>HAZOP</li> <li>Qualitative ETA</li> </ul>		Examples: <ul style="list-style-type: none"> <li>Quantitative FMEA</li> <li>Quantitative FTA</li> <li>Quantitative ETA</li> <li>Markov models</li> <li>Reliability block diagrams</li> </ul>

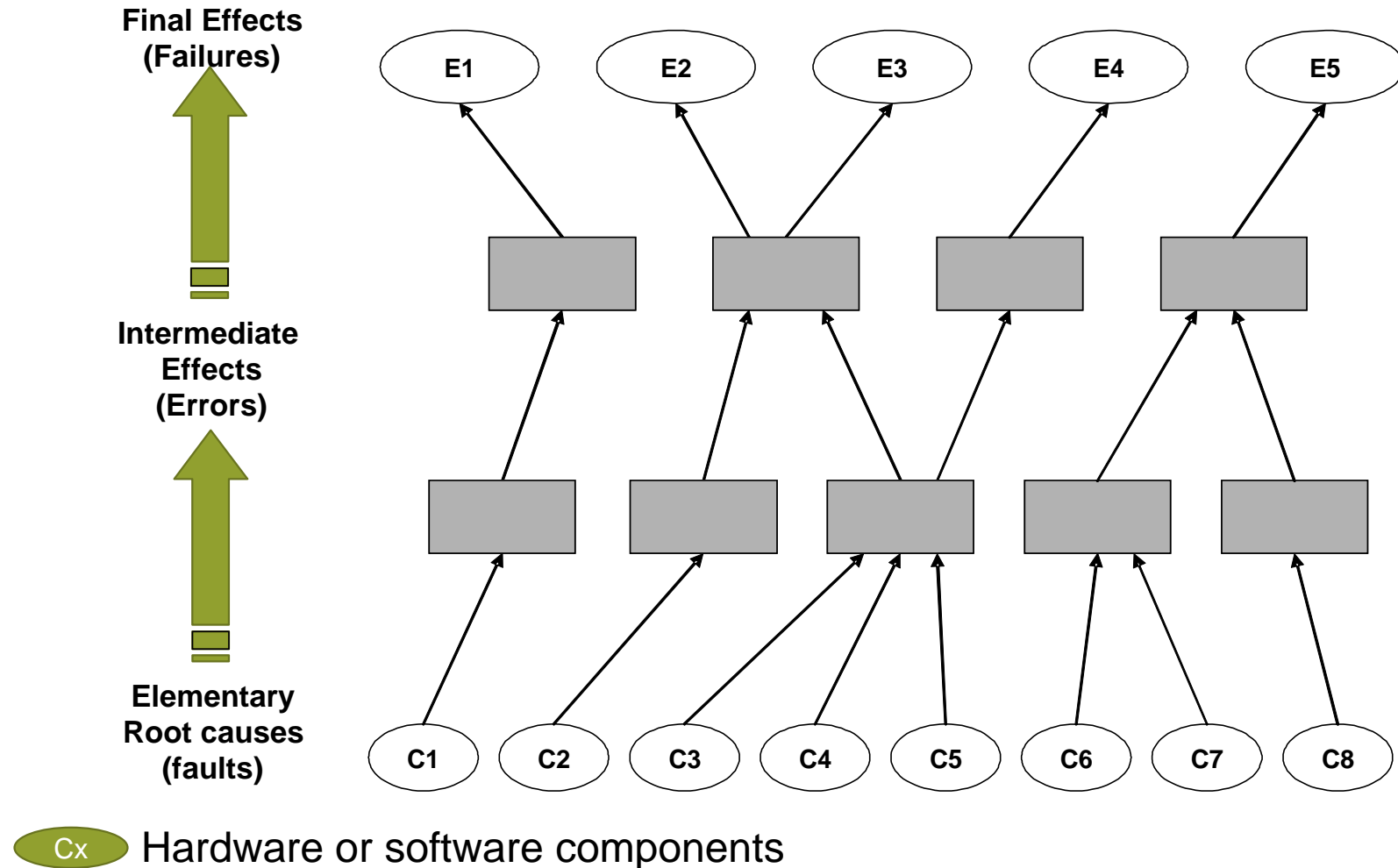
Alternative classification scheme:

Inductive Analysis Methods	vs.	Deductive Analysis Methods
<ul style="list-style-type: none"> <li>▪ Bottom-up methods</li> <li>▪ Start from known causes and forecast unknown effects</li> </ul>		<ul style="list-style-type: none"> <li>▪ Top-down methods</li> <li>▪ Start from known effects and analyze unknown causes</li> </ul>
<p>Examples:</p> <ul style="list-style-type: none"> <li>▪ System, design, or process FMEA</li> <li>▪ ETA</li> <li>▪ Markov modeling</li> </ul>		<p>Examples:</p> <ul style="list-style-type: none"> <li>▪ FTA</li> <li>▪ Reliability block diagrams</li> </ul>



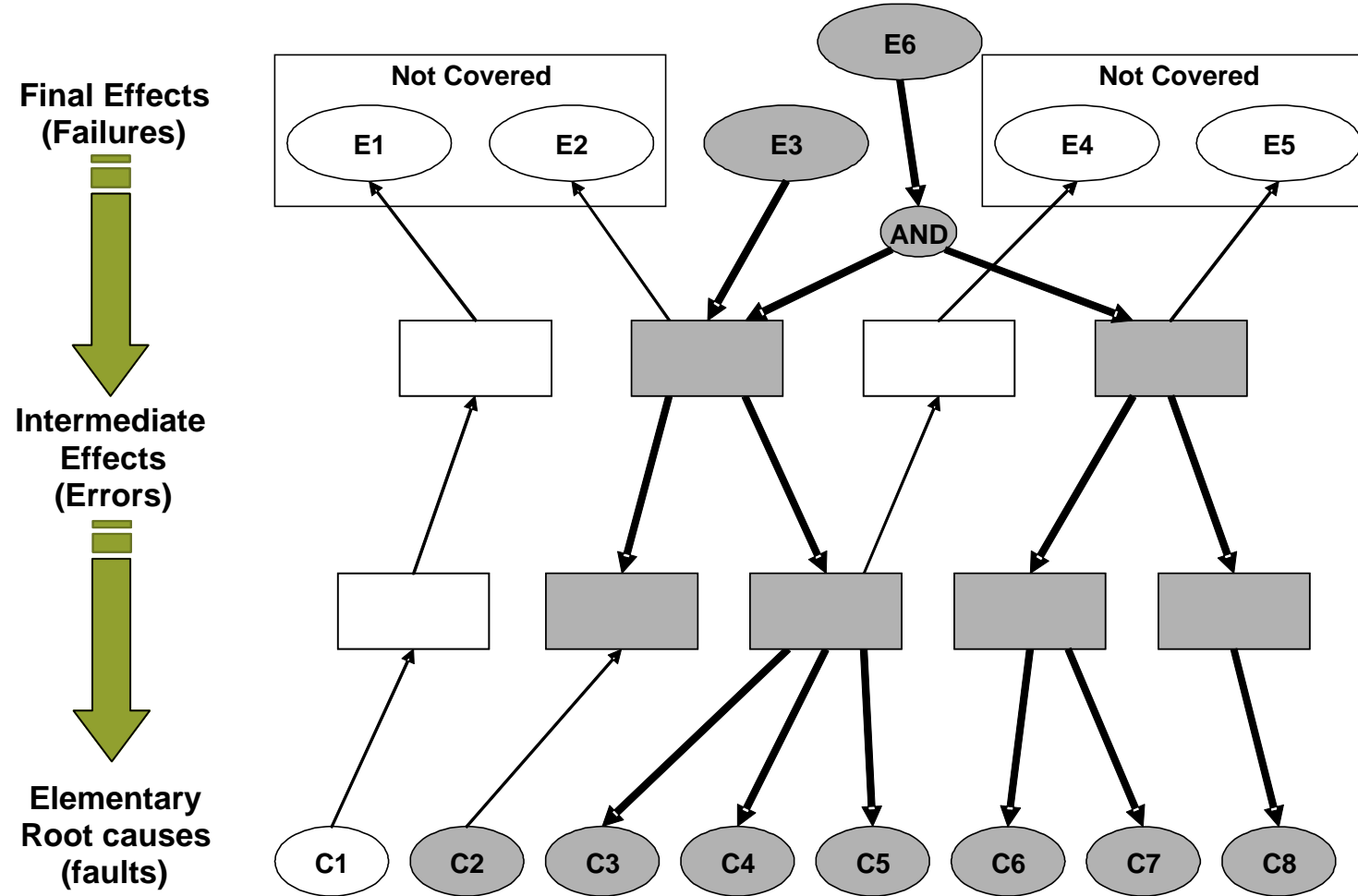
### Failure Mode and Effects Analysis (FMEA)

 Fehlermöglichkeits-  
und Einflussanalyse



### Fault Tree Analysis (FTA)

 Fehlerbaumanalyse



 Hardware or software components

- Inductive and deductive approaches are usually complementary
- FTA and FMEA can be combined to provide safety analysis with the right balance of top-down and bottom-up approaches



Heating, Ventilation, and Air Condition (HVAC) System

Project: Item: HVAC System				Date: Prepared by:				FMEA Number: Reference documents:				
Component / part, function	Failure mode	Failure effect(s)	S E V	Class	Cause(s)	O C C	Prevention measure(s)	Detection measure(s)	D E T	R E P N	Recommend ed action(s)	Responsibility, completion date

The HVAC system must defog windows and heat or cool cabin to 70 ° F in all operating conditions (-40 ° F to 100 ° F) within 3 to 5 minutes.

Heating, Ventilation, and Air Condition (HVAC) System

Project: Item: HVAC System			Date: Prepared by:			FMEA Number: Reference documents:						
Component / part, function	Failure mode	Failure effect(s)	S E V	Class	Cause(s)	O C C	Prevention measure(s)	Detection measure(s)	D E T	R E P N	Recommend ed action(s)	Responsibility, completion date

HVAC system,

The HVAC system must defog windows and heat or cool cabin to 70 ° F in all operating conditions (-40 ° F to 100 ° F) within 3 to 5 minutes or as specified in functional spec #\_\_\_\_\_ (rev. date \_\_\_\_\_)

- **Failure Mode**
  - Manner in which a component / part could potentially fail to meet design intent
- **Failure Effects**
  - Effects of the failure mode on the function as perceived by the customer
- **Causes**
  - Indication of a design weakness, the consequence of which is the failure mode
- **Detection / Prevention Measures** (Current Design Controls)
  - Activities which will assure the design adequacy for the failure cause/mechanism under consideration

### Heating, Ventilation, and Air Condition (HVAC) System

Project: Item: HVAC System			Date: Prepared by:			FMEA Number: Reference documents:						
Component / part, function	Failure mode	Failure effect(s)	S E V	Class	Cause(s)	O C C	Prevention measure(s)	Detection measure(s)	D E T	R E P N	Recommend ed action(s)	Responsibility, completion date

- HVAC system does not heat vehicle or defog windows
- HVAC system takes more than 5 minutes to heat vehicle
- HVAC system does not heat cabin to 70 degrees in below zero temperatures
- HVAC system cools cabin to 50 degrees
- HVAC system activates rear window defogger

### Heating, Ventilation, and Air Condition (HVAC) System

Project: Item: HVAC System			Date: Prepared by:			FMEA Number: Reference documents:						
Component / part, function	Failure mode	Failure effect(s)	S E V	Class	Cause(s)	O C C	Prevention measure(s)	Detection measure(s)	D E T	R E P N	Recommend ed action(s)	Responsibility, completion date

- Cannot see out of front window
- Air conditioner makes cab too cold
- Does not get warm enough
- Takes too long to heat up

### Heating, Ventilation, and Air Condition (HVAC) System

Project: Item: HVAC System			Date: Prepared by:			FMEA Number: Reference documents:						
Component / part, function	Failure mode	Failure effect(s)	S E V	Class	Cause(s)	O C C	Prevention measure(s)	Detection measure(s)	D E T	R E P N	Recommend ed action(s)	Responsibility, completion date

- Incorrect location of vents
- Incorrect routing of vent hoses (too close to heat source)
- Inadequate coolant capacity for application

Project: Item: HVAC System			Date: Prepared by:			FMEA Number: Reference documents:						
Component / part, function	Failure mode	Failure effect(s)	S E V	Class	Cause(s)	O C C U R R E N C E	Prevention measure(s)	Detection measure(s)	D E T E C T I O N	R E P A R E D	Recommend ed action(s)	Responsibility, completion date

#### Prevention measures

- Engineering specifications
- Historical data

#### Detection measures

- Functional testing
- General component durability

### **Severity (SEV)**

- Rates the severity of a potential failure effect (scale: 1...10)

### **Occurrence (OCC)**

- Rates the likelihood that the failure will occur (scale: 1...10)

### **Detection (DET)**

- Rates the likelihood that the problem will **not** be detected before it reaches the end-user/customer (scale: 1...10)

### **Risk Priority Number (RPN)**

- $RPN = SEV \times OCC \times DET$
- Used to prioritize concerns/actions  
(The greater the RPN value, the greater the concern)



RPN Calculation Method: Cause RPN = Severity x Occurrence x Detection    Failure RPN = Sum of Cause RPNs    Item RPN = Sum of Mode RPNs plus Sub-Item RPNs

Severity Rating Scale			Occurrence Rating Scale		
#	Description	Criteria	#	Description	Criteria
1	None	No discernible effect.	1	Remote: Failure is unlikely	<= 0.01 per thousand vehicles/items
2	Very Minor	Fit and finish/Squeak and rattle item does not conform. Defect noticed by discriminating customers (less than 25%).	2	Low: Relatively few failures	0.1 per thousand vehicles/items
3	Minor	Fit and finish/Squeak and rattle item does not conform. Defect noticed by 50% of customers.	3	Low: Relatively few failures	0.5 per thousand vehicles/items
4	Very Low	Fit and finish/Squeak and rattle item does not conform. Defect noticed by most customers (greater than 75%).	4	Moderate: Occasional failures	1 per thousand vehicles/items
5	Low	Vehicle/Item operable but Comfort/Convenience item(s) inoperable. Customer somewhat dissatisfied.	5	Moderate: Occasional failures	2 per thousand vehicles/items
6	Moderate	Vehicle/Item operable but Comfort/Convenience item(s) inoperable. Customer dissatisfied.	6	Moderate: Occasional failures	5 per thousand vehicles/items
7	High	Vehicle/Item operable but at a reduced level of performance. Customer very dissatisfied.	7	High: Frequent failures	10 per thousand vehicles/items
8	Very High	Vehicle/Item inoperable (loss of primary function).	8	High: Frequent failures	20 per thousand vehicles/items
9	Hazardous with warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning.	9	Very High: Persistent failures	50 per thousand vehicles/items
10	Hazardous without warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning.	10	Very High: Persistent failures	=> 100 per thousand vehicles/items

Detection Rating Scale		
#	Description	Criteria
1	Almost Certain	Design Control will almost certainly detect a potential cause/mechanism and subsequent failure mode.
2	Very High	Very High chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.
3	High	High chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.
4	Moderately High	Moderately High chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.
5	Moderate	Moderate chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.
6	Low	Low chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.
7	Very Low	Very Low chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.
8	Remote	Remote chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.
9	Very Remote	Very Remote chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.
10	Absolute Uncertainty	Design Control will not and/or cannot detect a potential cause/mechanism and subsequent failure mode; or there is no Design Control.

Example SEV, OCC, and DET rating scales

### Heating, Ventilation, and Air Condition (HVAC) System

Project:

Item: HVAC System

Date:

Prepared by:

FMEA Number:

Reference documents:

Component / part, function	Failure mode	Failure effect(s)	SEV	Class	Cause(s)	OCC	Prevention measure(s)	Detection measure(s)	DET	Recommended action(s)	Responsibility, completion date

- Cannot see out of front window: SEV 9
- Air conditioner makes cab too cold: SEV 5
- Does not get warm enough: SEV 5
- Takes too long to heat up: SEV 4

- Incorrect location of vents: OCC 3
- Incorrect routing of vent hoses (too close to heat source): OCC 6
- Inadequate coolant capacity for application: OCC 2

- Engineering specifications: No DET value
- Historical data: No DET value
- Functional testing: DET 3
- General vehicle durability: DET 5

### Heating, Ventilation, and Air Condition (HVAC) System

Project: Item: HVAC System			Date: Prepared by:			FMEA Number: Reference documents:						
Component / part, function	Failure mode	Failure effect(s)	S E V	Class	Cause(s)	O C C	Prevention measure(s)	Detection measure(s)	D E T	R P N	Recommend ed action(s)	Responsibility, completion date

- Cannot see out of front window: SEV 9
- Incorrect location of vents: OCC 2
- Functional testing: DET 3
- RPN:  $9 \times 2 \times 3 = 54$

# Example

## FMEA example of a front door at

[https://www.reliasoft.com/images/documents/xfmea\\_pfmea.pdf](https://www.reliasoft.com/images/documents/xfmea_pfmea.pdf)

System

1 - Automobile

Subsystem

2 - Body Closures

X Component

3 - Front Door L.H.

Model Year(s)/Program(s)

199X/Lion 4dr/Wagon

Core Team

T. Fender - Car Product Dev., C. Childers - Manufacturing, J. Ford - Assy Ops (Dalton, Fraser, Henley Assembly Plants)

FAILURE MODE AND EFFECTS ANALYSIS

Front Door L.H.

FMEA Number

1234

Page 4 of 9

Design Responsibility

Body Engineering

Prepared By

A. Tate - X8412 - Body Engr

FMEA Date (Orig.)

2/28/2003

(Rev)

3/3/2003

Item	Potential Failure Mode	Potential Effect(s) of Failure	SEV	CLASS	Potential Cause(s)/Mechanism(s) of Failure	Occur	Current Design Controls	Detect	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Action Results				
												Actions Taken	SEV	Occ	Detect	RPN
3 - Front Door L.H.																
<ul style="list-style-type: none"> <li>Ingress to and egress from vehicle.</li> <li>Occupant protection from weather, noise, and side impact.</li> <li>Support anchorage for door hardware including mirror, hinges, latch and window regulator.</li> <li>Provide proper surface for appearance items - paint and soft trim.</li> </ul>	Corroded interior lower door panels	Deteriorated life of door leading to: <ul style="list-style-type: none"> <li>Unsatisfactory appearance due to rust through paint over time.</li> <li>Impaired function of interior door hardware.</li> </ul>	7		Upper edge of protective wax application specified for inner door panels is too low.	6	Vehicle general durability test veh. T-118 T-109 T-301	7	294	Add laboratory accelerated corrosion testing.	A. Tate Body Engr - 2/25/2003	Based on test results (Test No. 1481) upper edge spec raised 125 mm.	7	2	2	28
			10		Insufficient wax thickness specified.	4	Vehicle general durability testing - as above.	7	196	Add laboratory accelerated corrosion testing.	A. Tate Body Engr - 3/28/2003	Test results (Test No. 1481) show specified thickness is adequate.	7	2	2	28
									Conduct Design of Experiments (DOE) on wax thickness.	A. Tate Body Engr - 3/28/2003	DOE shows 25% variation in specified thickness is acceptable.					
					Inappropriate wax formulation specified.	2	Physical and Chem Lab test - Report No. 1265.	2	28			7	2	2	28	
					Entrapped air prevents wax from entering corner edge access.	5	Design aid investigation with nonfunctioning spray head.	8	280	Add team evaluation using production spray equipment and specified wax.	Body Engr & Assy Ops - 3/28/2003	Based on test, addition vent holes will be provided in affected areas.	7	1	3	21
					Wax application plugs door drain holes.	3	Laboratory test using "worst case" wax application and hole size.	1	21			7	3	1	21	
					Insufficient room between panels for spray head access.	4	Drawing evaluation of spray head access.	4	112	Add team evaluation using design aid buck and spray head.	Body Engr & Assy Ops - 3/28/2003	Evaluation showed adequate access.	7	1	1	7

- FMEAs are system-level analyses
- Among other things, are used for drug production processes as well
- FMEAs can help establish (software) test goals
  - Write tests that try to provoke a failure mode
  - These test cases are "good" in that they provide evidence that a certain problem (likely) is not present; regardless of the failure that actually can be provoked.

Goal: identify all conditions that lead to a system failure (top level event)

- Developed at Bell Labs in the 1960s for missile launch control system
- DIN and IEC standards
- Aims at finding the sources of a system failure
- Quantitative and qualitative
- Deductive top-down method
- Graphical representation of causal relationships
- Used in nuclear/medical/aerospace industries

# Prerequisites

- Understand how the system works e.g., FMEA
- Done when design/architecture is available
- Facilitated discussions with different group members

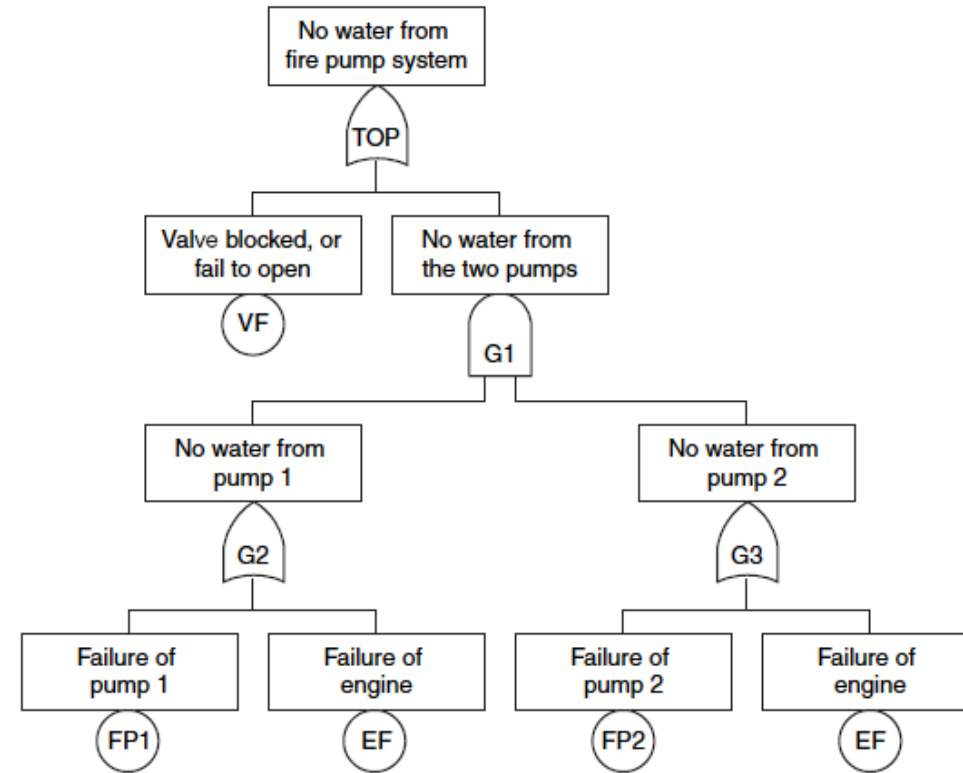
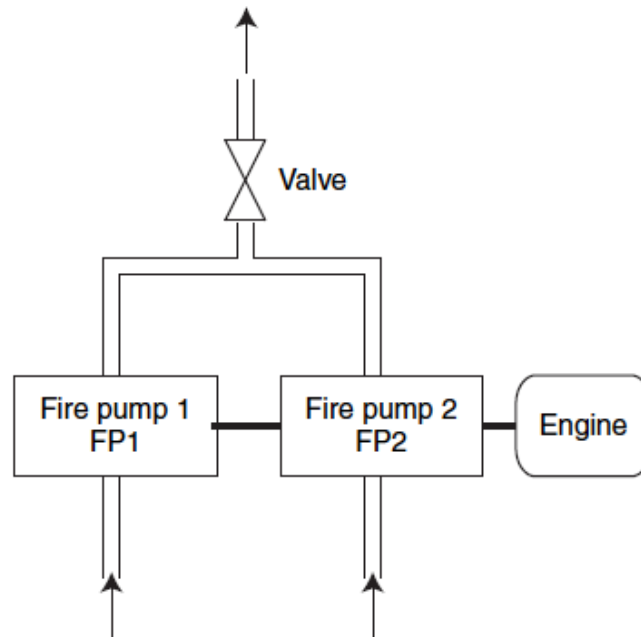
- Plan of the system and FMEA—if existing—taken as input
- Define system under scrutiny (its boundary)
- Determine undesired event(s) (top event)
  - Failure / malfunction
- Identify event or series of events that lead to the top level event
  - lower-level failures
- Apply recursively
  - Symbols used: AND/OR; possibly probabilities
  - Leaves: possible cause, e.g., a single component, environmental condition or functional characteristic, or interaction of a combination or plurality of any thereof
- Identify cut sets
  - Sets of events that, taken together, lead to the system failure



- Primary events
  - *Basic* events: no precursor; probabilistic
    - e.g., bits flipped by cosmic rays
  - *Undeveloped* events: no major effect on the system
    - e.g., indication lamp fails
  - *External* events: expected to happen; not a fault
- Intermediate events
  - Link primary or other intermediate events via AND/OR gates
- Expanded events
  - Need a separate fault tree to explain

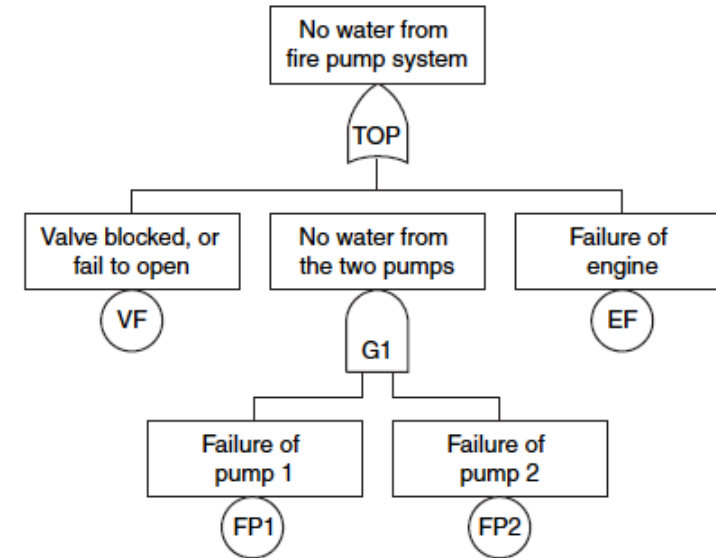
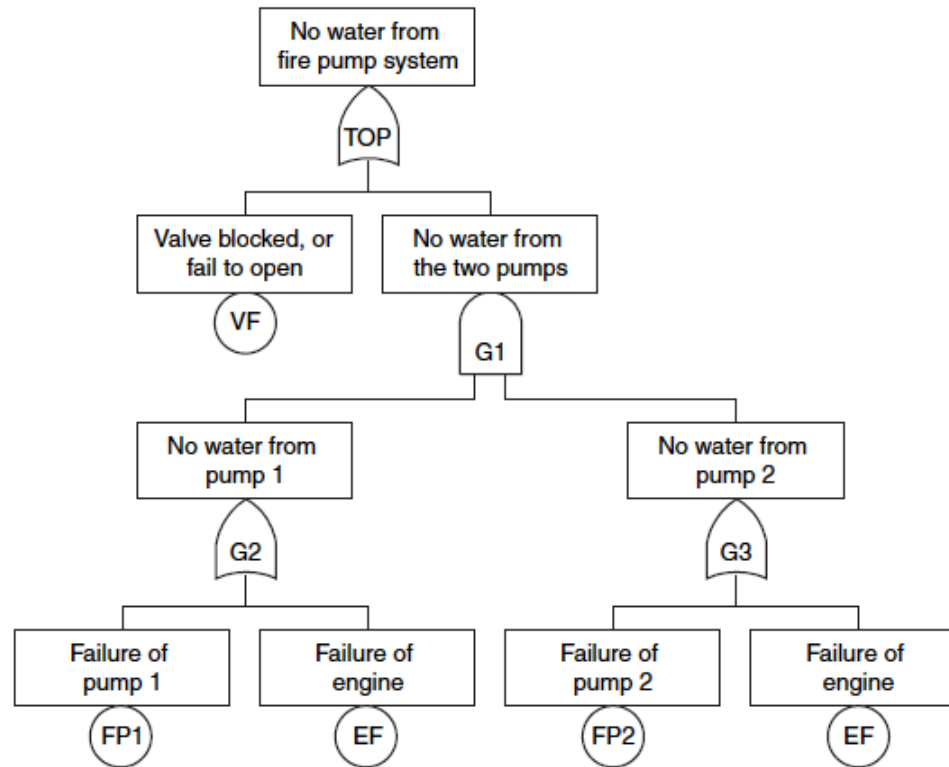
Different graphical symbols

# Example – Redundant fire pumps



["Fault Tree Analysis." M. Rausand (2004)  
<http://www.fmeainfocentre.com/presentations/fta.pdf>]

# Equivalent fault trees



["Fault Tree Analysis." M. Rausand (2004)  
<http://www.fmeainfocentre.com/presentations/fta.pdf>]

- Safety is not absolute but rather “good enough” safety!
- Basic idea is to think about what can go wrong and provide mitigations. Many real systems are (surprisingly?) safe in practice.
- System boundaries must be defined very early. This becomes more difficult in self-adaptive settings, or on the internet of things (solution: runtime monitoring).
- Software does not fail randomly but only systematically. This makes it very difficult to estimate fault/error/failure probabilities. (Think about recent Tesla hazard).
- FMEAs not very widespread for software. FTAs are, when recast as attack trees (information security).
- Standards put aside, how do these ideas integrate with agile development?

## Coming up...

2.1. Software architecture

2.2. Antipatterns in software engineering

2.3. Reuse

2.4. Testability

2.5. Safety

**2.6. Information security**