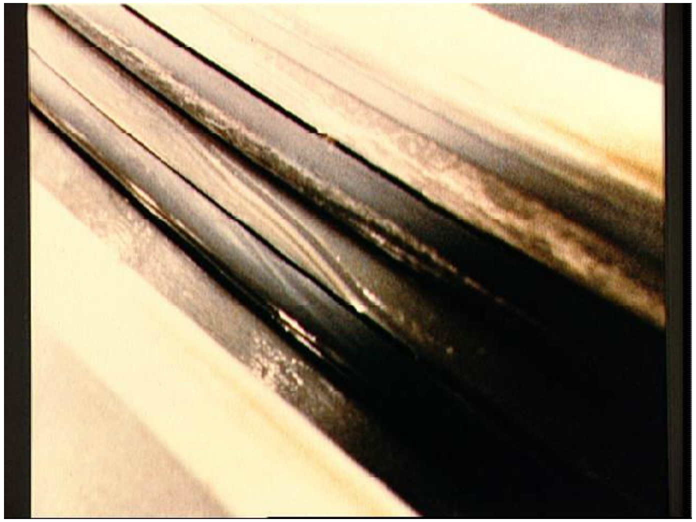
Industrial Automation
Automation Industrielle
Industrielle Automation



Safety analysis and standards

Analyse de sécurité et normes
Sicherheitsanalyse und Normen

Dr. Jean-Charles Tournier

Material initially prepared by Pr. Dr. H. Kirrmann

“To design systems that work correctly we often need to understand and correct how they can go wrong”

Dan Golding, NASA Administrator, 2000

Overview Dependability Analysis

1. Qualitative Evaluation
   - Failure Mode and Effects Analysis (FMEA)
   - Fault Tree Analysis (FTA)

2. Dependability Standards and Certification
   - Standardization Agencies
   - Standards

FMEA

FAILURE MODE AND EFFECT ANALYSIS

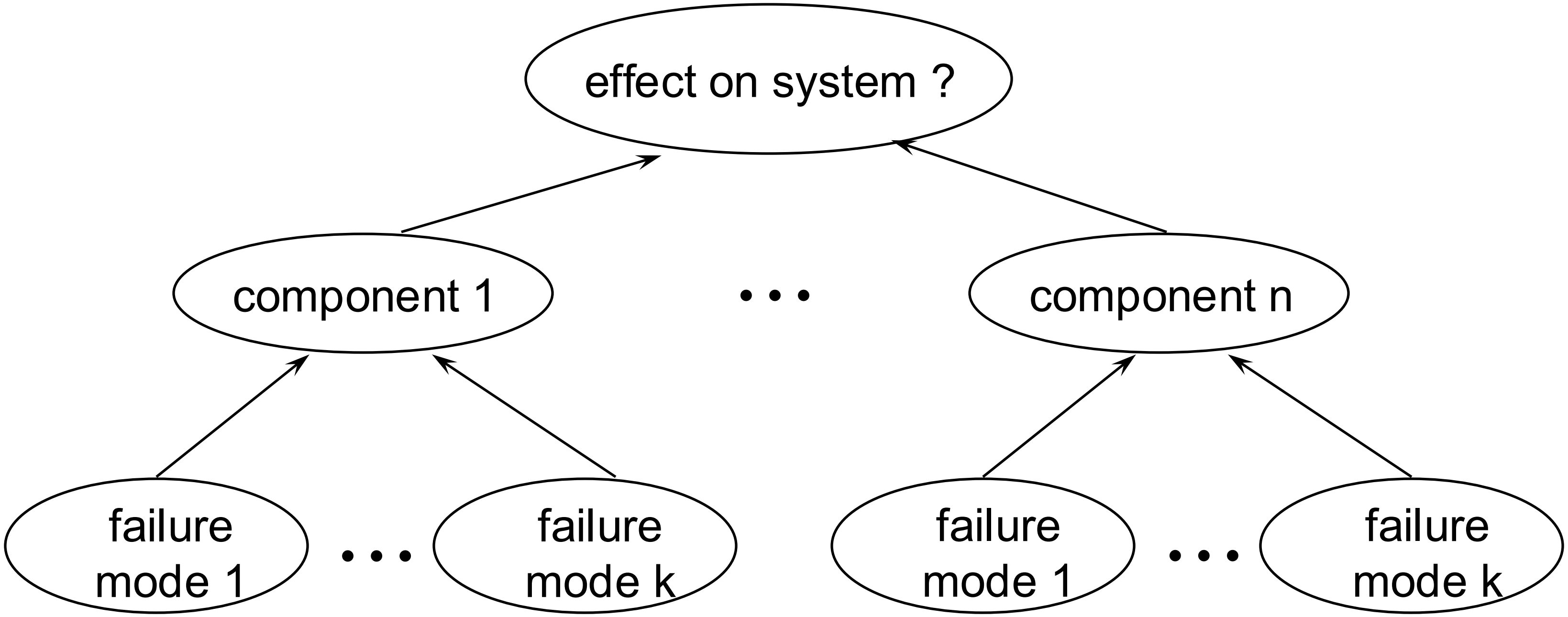
Origin of FMEA

- 1949 Military instruction MIL-P-1629
- 1963 NASA: Apollo project
- 1965 Aerospace & Aeronautics
- 1975 Nuclear industry
- 1978 Automotive industry (Ford)
- 1980 Standardization in Germany (DIN 25 448 Failure Effect Analysis)
- 1986 Further application in the automotive industry
- 1990 Application to electronic and software development
- 1996 Enhancement of the System FMEA (VDA-band 4.2)
- 2006 Further enhancement of the FMEA (VDA-band 4)

- ISO/TS 16949 (automotive industry)
  - the FMEA is mandatory as risk analysis method (not just recommended)

Failure Mode and Effects Analysis (FMEA)

Analysis method to identify component failures which have significant consequences affecting the system operation in the application considered.
→ identify faults (component failures) that lead to system failures.



FMEA is inductive (bottom-up)

FMEA: Purpose (overall)

There are different reasons why an FMEA can be performed:

- Evaluation of effects and sequences of events caused by each identified item failure mode
  (→ **get to know the system better**)

- Determination of the significance or criticality of each failure mode as to the system's correct function or performance and the impact on the availability and/or safety of the related process
  (→ **identify weak spots**)

- Classification of identified failure modes according to their detectability, diagnosability, testability, item replaceability and operating provisions (tests, repair, maintenance, logistics etc.)
  (→ **take the necessary precautions**)

- Estimation of measures of the significance and probability of failure
  (→ **demonstrate level of availability**/safety to user or certification agency)

FMEA: Critical decisions

Depending on the exact purpose of the analysis, several decisions have to be made:

- **For what purpose is it performed** (find weak spots ¦ demonstrate safety to certification agency, demonstrate safety ¦ compute availability)
- **When is the analysis performed** (e.g. before ¦ after detailed design)?
- **What is the system** (highest level considered), where are the boundaries to the external world (that is assumed fault-free)?
- **Which components are analyzed** (lowest level considered)?
- **Which failure modes are considered** (electrical, mechanical, hydraulic, design faults, human/operation errors)?
- **Are secondary and higher-order effects considered** (i.e. one fault causing a second fault which then causes a system failure etc.)?
- **By whom is the analysis performed** (designer, who knows system best ¦ third party, which is unbiased and brings in an independent view)?

FMEA and FMECA

FMEA only provides qualitative analysis (cause effect chain).

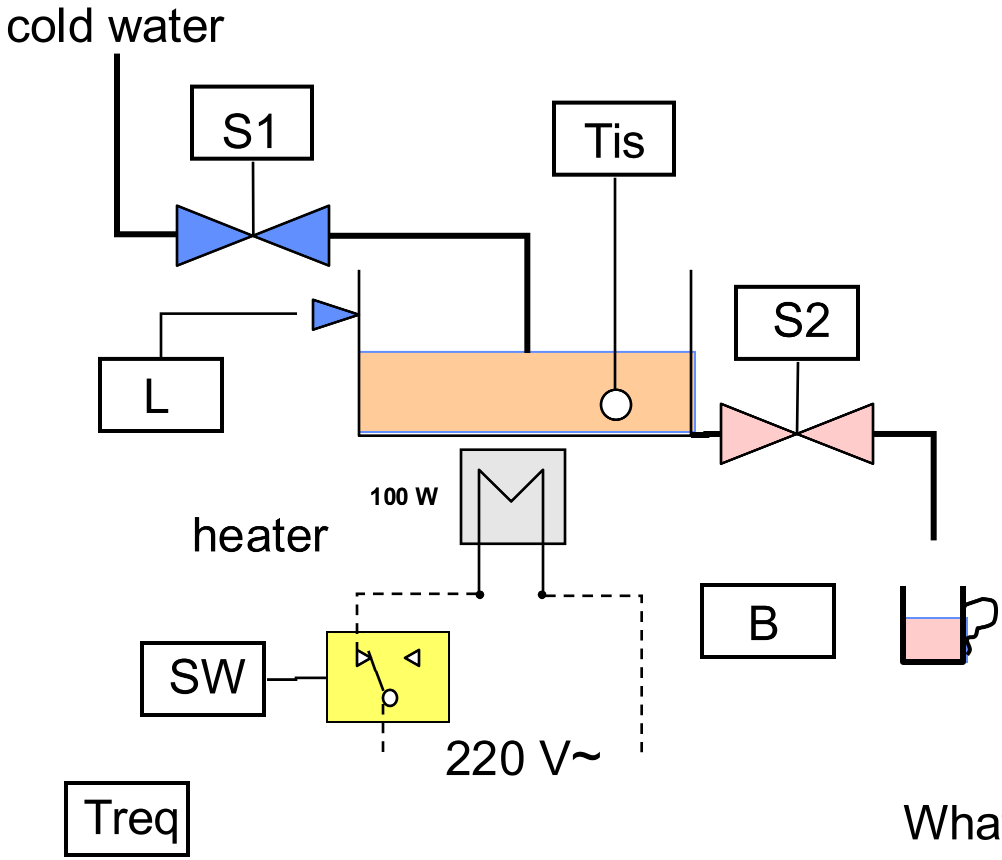
FMECA (failure mode, effects and criticality analysis) also provides (limited) quantitative information.

- each basic failure mode is assigned a failure probability and a failure criticality
- if based on the result of the FMECA the system is to be improved (to make it more dependable) the failure modes with the highest probability leading to failures with the highest criticality are considered first.

Coffee machine example:

- If a coffee machine is damaged, this is more critical than if the coffee machine is OK and no coffee can be produced temporarily
- If the water has to be refilled every 20 cups and the coffee has to be refilled every 2 cups, the failure mode “coffee bean container too low” is more probable than “water tank too low”.

Example: tea dispenser



The controller fills the tank up to the high water mark given by sensor L.
it then heats the liquid until the desired temperature Treq (entered by a potentiometer).
When the user presses the button, it opens the exit valve and fills a volume of water given by the aperture time.

What is the consequence of the failure of each of these elements:
-on the availability ?
-on the safety ? (flooding, burning….)

FMEA: Tea dispenser example

component	failure mode	effect on system
inlet valve	closed	no production
	open	flooding
outlet valve	closed	no production
	open	flooding
temperature sensor	stuck on high	cold water
	stuck on low	burning
button	closed	flooding
	open	no production
level indicator	stuck on high	burning
	stuck on low	flooding

………

Criticality Grid

Criticality levels

I				
II				
III				
IV				
	very low	low	medium	high

Probability of failure

Failure Criticalities

I: Any event which could cause degradation of system performance function(s) resulting in negligible damage to either system or environment and no damage to life

II: Any event which degrades system performance function(s) without appreciable damage to either system, environment or lives

III: Any event which could potentially cause the loss of primary system function(s) resulting in significant damage to the system or its environment and negligible hazards to life

IV: Any event which could potentially cause the loss of primary system function(s) resulting in significant damage to the system or its environment and causes the loss of life

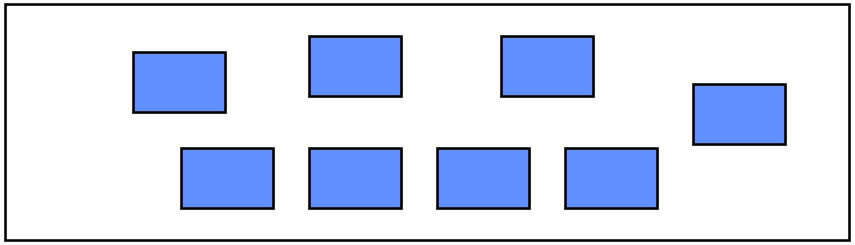
FMEA/FMECA: Result

Depending on the result of the FMEA/FMECA, it may be necessary to:

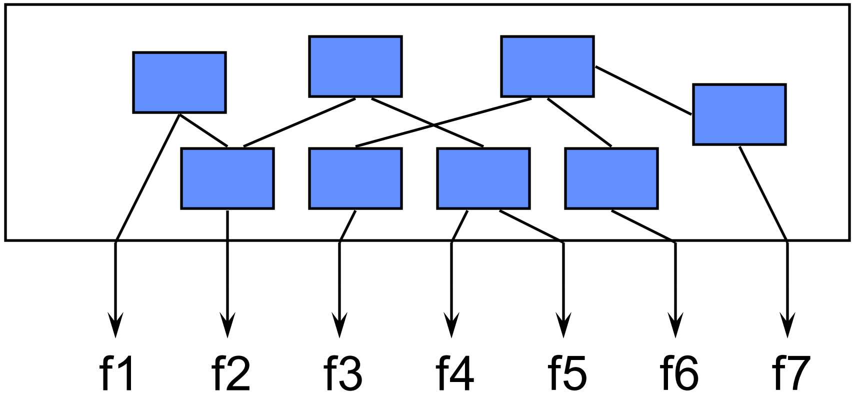
- change design, introduce redundancy, reconfiguration, recovery etc.
- introduce tests, diagnoses, preventive maintenance
- focus quality assurance, inspections etc. on key areas
- select alternative materials, components
- change operating conditions (e.g. duty cycles to anticipate/avoid wear-out)
- adapt operating procedures (e.g. allowed temperature range)
- perform design reviews
- monitor problem areas during testing, check-out and use
- exclude liability for identified problem areas

FMEA: Steps (1)

1) Break down the system into components.



2) Identify the functional structure of the system and how the components contribute to functions.



FMEA: Steps (2)

3) Define failure modes of each component

- new components: refer to similar already used components
- commonly used components: base on experience and measurements
- complex components: break down in subcomponents and derive failure mode of component by FMEA on known subcomponents
- other: use common sense, deduce possible failures from functions and physical parameters typical of the component operation

4) Perform analysis for each failure mode of each component and record results in table:

component name/ID	function	failure mode	failure cause	failure effect		failure detection	other provision	remark
				local	global			

Example (Generic) Failure Modes

- fails to remain (in position)
- fails to open
- fails to close
- fails if open
- fails if closed
- restricted flow
- fails out of tolerance (high)
- fails out of tolerance (low)
- inadvertent operation
- intermittent operation
- premature operation
- delayed operation
- false actuation
- fails to stop
- fails to start
- fails to switch
- erroneous input (increased)
- erroneous input (decreased)
- erroneous output (increased)
- erroneous output (decreased)
- loss of input
- loss of output
- erroneous indication
- leakage

Other FMEA Table Entries

Failure cause: Why is it that the component fails in this specific way?
To identify failure causes is important to
- estimate probability of occurrence
- uncover secondary effects
- devise corrective actions

Local failure effect: Effect on the system element under consideration (e.g. on the output of the analyzed component). In certain instances there may not be a local effect beyond the failure mode itself.

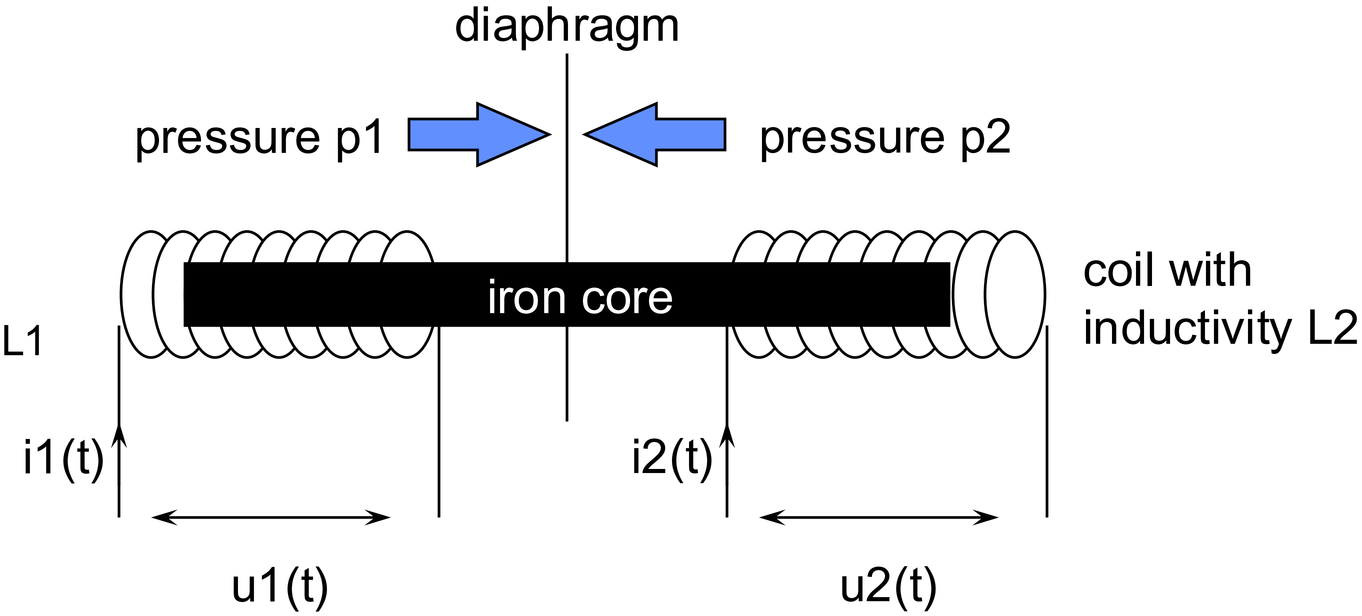
Global failure effect: Effect on the highest considered system level. The end effect might be the result of multiple failures occurring as a consequence of each other.

Failure detection: Methods to detect the component failure that should be used.

Other provisions: Design features might be introduced that prevent or reduce the effect of the failure mode (e.g. redundancy, alarm devices, operating restrictions).

Example: Differential Pressure Transmitter (1)

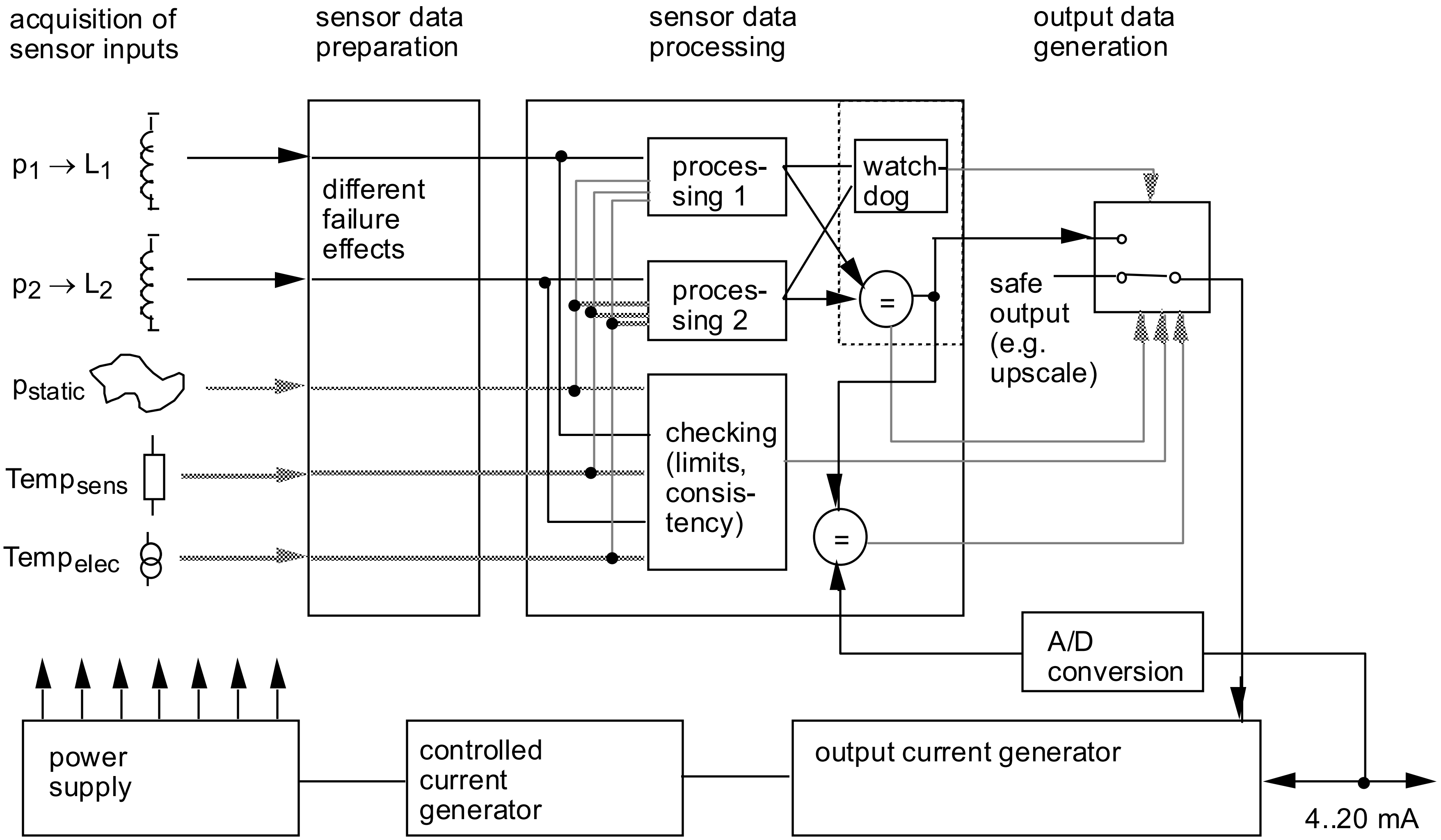
Functionality: Measure difference in pressures p1 – p2.



p1 – p2 = f1 (inductivity L1, temperature T, static pressure p)

p1 – p2 = f2 (inductivity L2, temperature T, static pressure p)

Example: Differential Pressure Transmitter (2)



FMEA for Pressure Transmitter

ID-Nr	Function	Failure Mode	Local Effect	Detection Mechanism	Failure Handling	Global Effect	Comments
1.1.1	p1 measurement	out of fail-safe accuracy range	pressure input via L1 wrong	limit check and consistency check (comparison with p2) in software of sensor data processing	go to safe state	output driven to up/downscale	diaphragm failure (both p1 and p2 wrong) detected by comparison with pstatic, requires that separate sensor is used for pstatic
1.1.2		wrong but within fail-safe accuracy range	pressure input via L1 slightly wrong	consistency check (comp. with p2), detection of small failures not guaranteed (allowed difference p1-p2)	not applicable (n/a)	output value slightly wrong, but within fail-safe accuracy range	
1.2.1	p2 measurement	out of fail-safe accuracy range	pressure input via L2 wrong	limit check and consistency check (comparison with p1) in software of sensor data processing	go to safe state	output driven to up/downscale	
1.2.2		wrong but within fail-safe accuracy range	pressure input via L2 slightly wrong	consistency check (comp. with p1), detection of small failures not guaranteed (allowed difference p1-p2)	n/a	output value slightly wrong, but within fail-safe accuracy range	

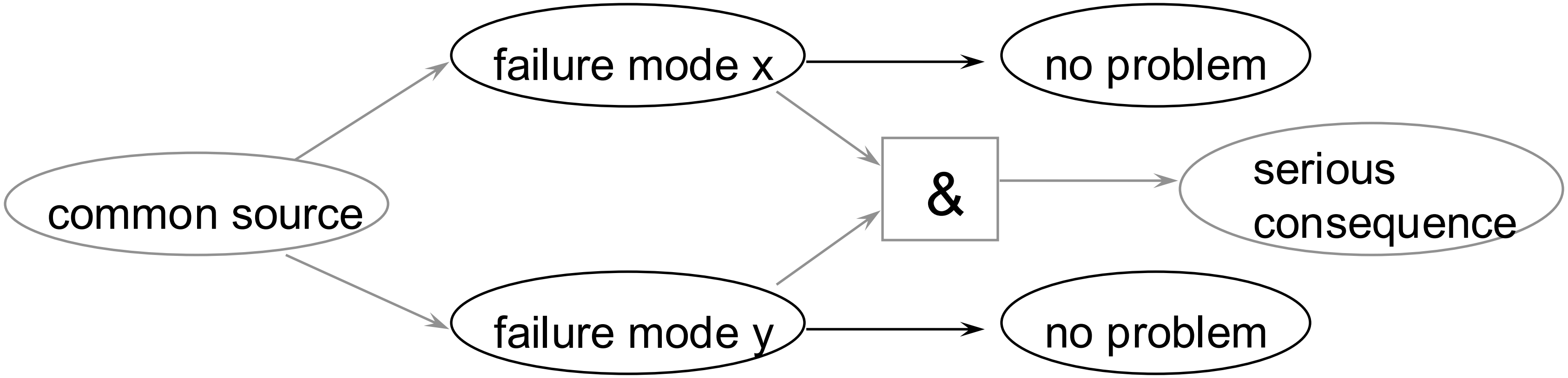
continue on your own ...

FMEA Limits

- Only as good as the team (experience, knowledge)
- Time consuming
- Might miss a failure mode (or component)
- Regular update is necessary to include new potential failure modes
- Most efficient in early design stages

Common Mode Failures (CMF)

In FMEA all failures are analyzed independent of each other.
Common mode failures are related failures that can occur due to a single source such as design error, wrong operation conditions, human error etc.



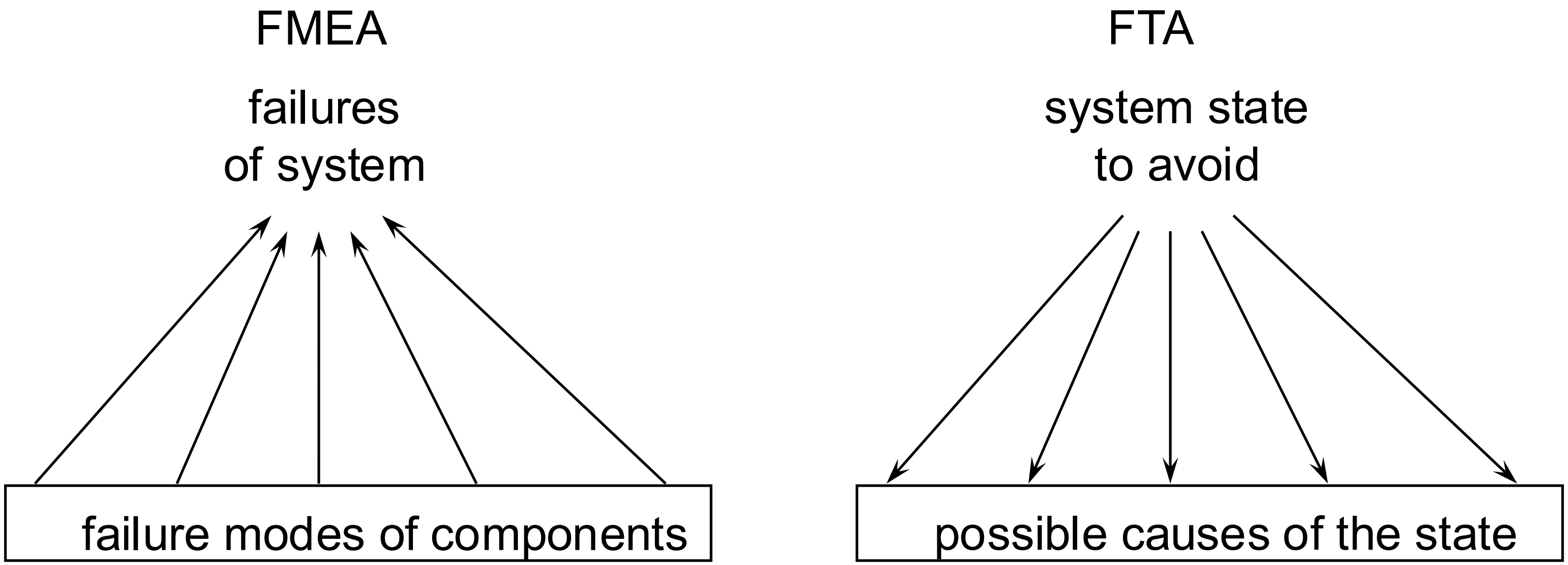
Example:
Failure of power supply common to redundant units causes both redundant units to fail at the same time.

FTA

FAULT TREE ANALYSIS

Fault Tree Analysis (FTA)

In contrast to FMEA (which is inductive, bottom-up), **FTA is deductive** (top-down).



The main problem with both FMEA and FTA is to not forget anything important.

Doing both FMEA and FTA helps to become more complete (2 different views).

FMEA vs. FTA

- FMEA considers all single component failures and evaluates their effects on the system

- FTA identifies combinations of conditions and component failures which lead to a single system failure.

History of FTA

- 1961 FTA developed by H.A. Watson (Bell Labs) for the US Airforce
- 1966 Boeing starts applying FTA
- 1970s FTA also used in the nuclear industry
    - Fault Tree Handbook (US Nuclear Regulatory Commission)
- 1980s FTA adopted by chemical and software (safety) industries
- 1990s FTA adopted by robotics and software industries

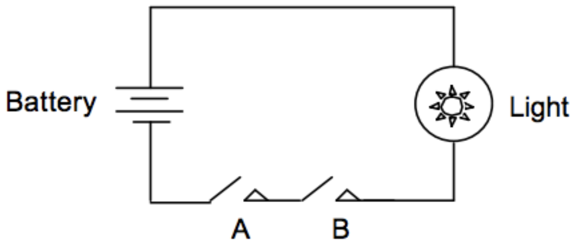
Fault Tree

- Begin fault analysis by identifying possible failures
  - In operation mode
  - In maintenance mode

- Fault Tree Graph
  - Nodes are failures
  - Edges are relationship among nodes by logical descriptor (AND, OR, NOT)

FTA Simple Example

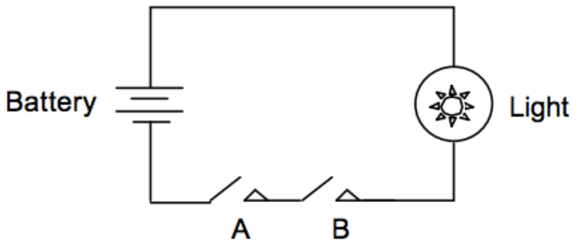
System



System undesired event: Light Fails Off

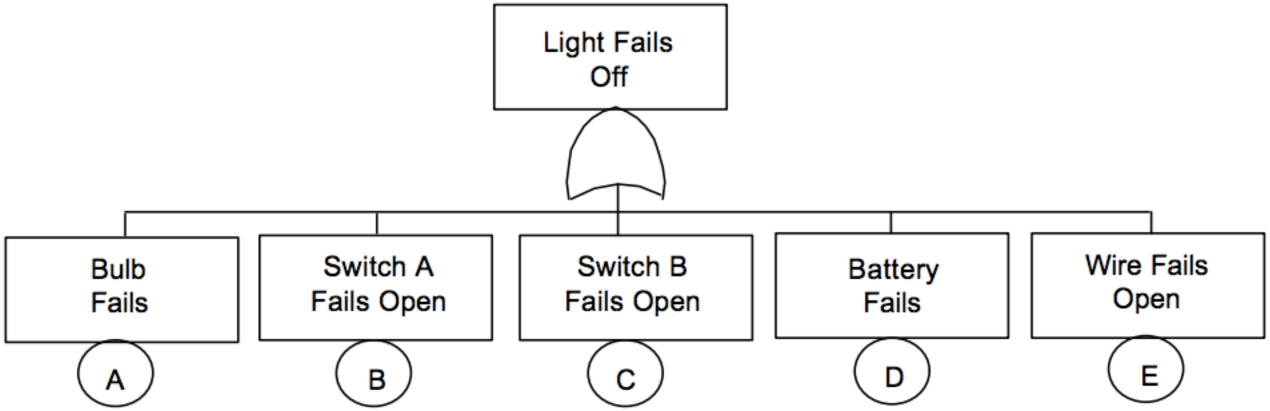
FTA Simple Example

System



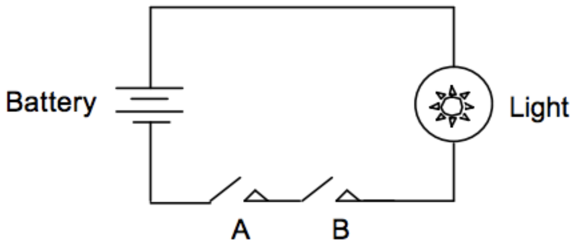
System undesired event: Light Fails Off

FTA



FTA Simple Example

System



System undesired event: Other faults? E.g. light fails on…

FTA

FTA Application - Rational

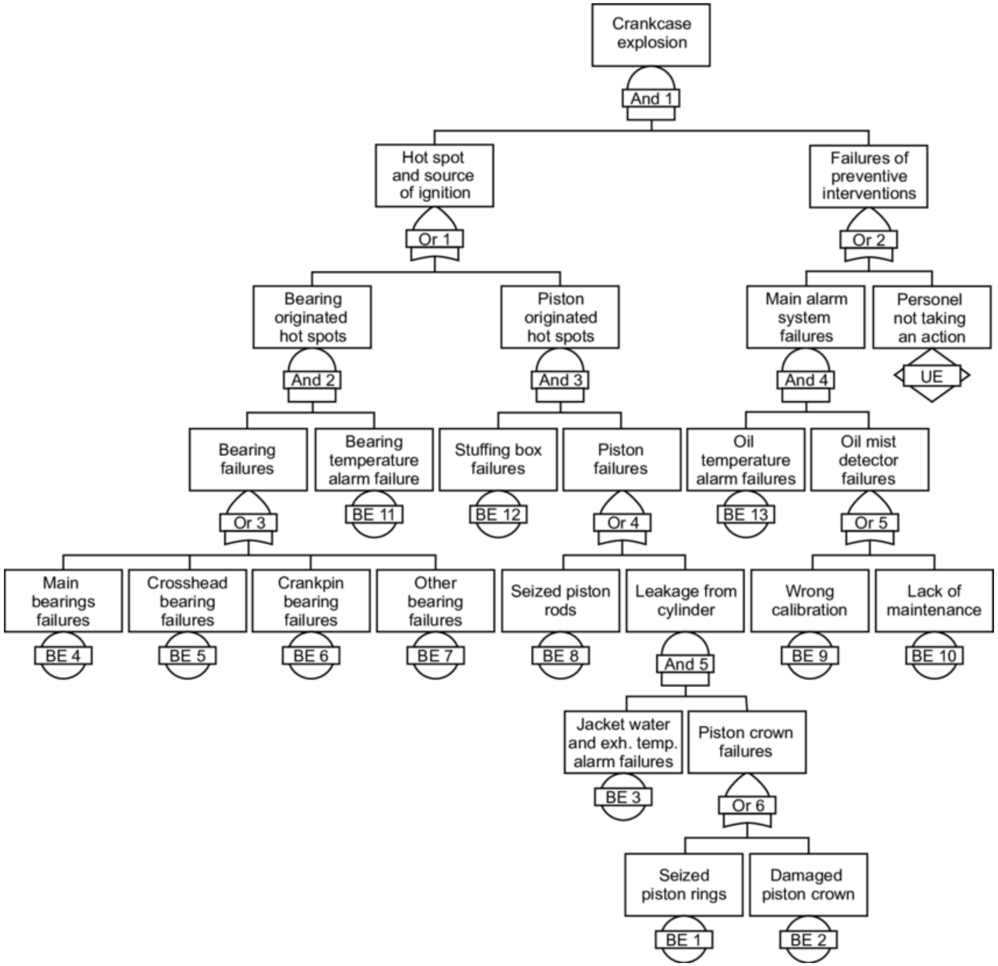
- Root Cause Analysis
  - Identify all relevant events and conditions leading to an undesired event
  - Determine parallel and sequential event combinations
  - Model divers/complex event interrelationships involved
- Risk Assessment
  - Calculate the probability of an undesired event (level of risk)
  - Identify safety critical components
  - Measure effect of design changes
- Design Safety Assessment
  - Demonstrate compliance with requirements
  - Shows where safety requirements are needed
  - Identify and evaluate potential design defects/weak links
  - Determine common mode of failure

FTA Applications

- FTA is not for every hazard
  - Usually only for safety critical hazards

- E.g.
  - Evaluate inadvertent arming and release of a weapon
  - Calculate the probability of a nuclear power plant accident
  - Evaluate an industrial robot going astray
  - Calculate the probability of a nuclear plant safety device being unavailable when needed
  - Evaluate the accidental operation and crash of a railroad car
  - Evaluate spacecraft failure
  - Evaluate the recent accidents of autonomous cars (root cause analysis)
    - Google car, Telsa
    - http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0184952

FTA Example
Root Causes of Explosions in Marine Engine Crankcases


Crankcase explosion
And 1
Hot spot and source of ignition
Failures of preventive interventions
Or 1
Or 2
Bearing originated hot spots
Piston originated hot spots
Main alarm system failures
Personel not taking an action
And 2
And 3
And 4
UE
Bearing failures
Bearing temperature alarm failure
Stuffing box failures
Piston failures
Oil temperature alarm failures
Oil mist detector failures
BE 11
BE 12
BE 13
Or 3
Or 4
Or 5
Main bearings failures
Crosshead bearing failures
Crankpin bearing failures
Other bearing failures
Seized piston rods
Leakage from cylinder
Wrong calibration
Lack of maintenance
BE 4
BE 5
BE 6
BE 7
BE 8
And 5
BE 9
BE 10
Jacket water and exh. temp. alarm failures
Piston crown failures
BE 3
Or 6
Seized piston rings
Damaged piston crown
BE 1
BE 2

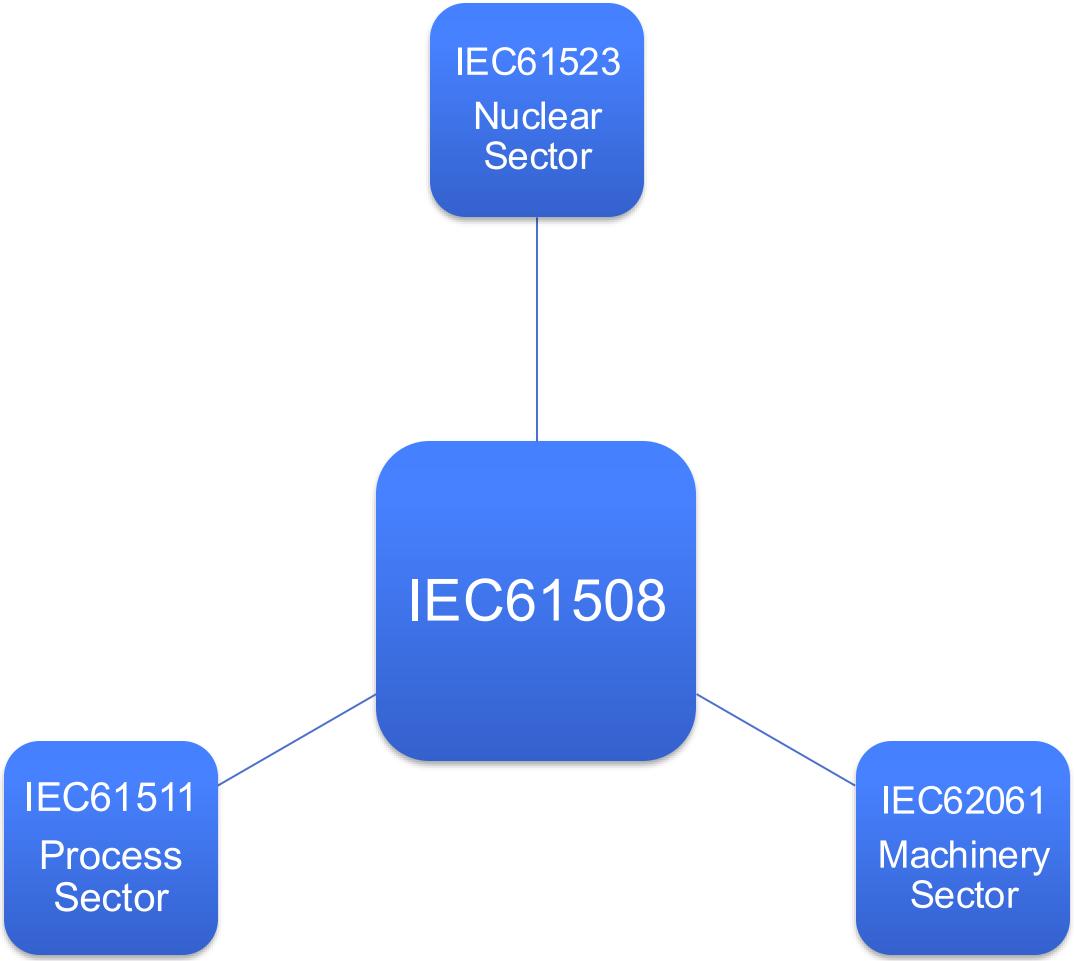
D. Wiaterek et al., Comparison of selected models useful in ranking the root causes of explosions in marine engine crankcases, 2022

SAFETY STANDARDS

Safety Issues

- How to demonstrate that a plant operation is “safe”?
- How to demonstrate that the equipment is “safe”?
- How to demonstrate that the safety and protective systems protect against hazards?
- => By demonstrating the compliance with Industry Safety Standards
  - IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems

Applications Sector Standards



IEC61523
Nuclear Sector

IEC61508

IEC61511
Process Sector

IEC62061
Machinery Sector

Standards for safety

IEC 60300	Dependability management
IEC 60204	Safety of machinery
IEC 61508 (VDE 0801)	Functional safety of E/E/PES safety related systems – International standard (7 parts)
IEC 61511	Functional safety of E/E/PES safety related systems – Functional safety: safety instrumented systems for the process industry sector
IEC 61784-	Safety communication in field busses
IEC 62061	Safety of machinery - functional safety –Electrical, electronic and programmable electronic control systems
ISO/IEC 13849 (EN 954)	Safety of machinery – Safety-related parts of control systems
IEC 62278	RAMS in railways
IEC 62279	system issues on the widest scale
EN 50126 (VDE 0115)	Railways applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) – general guidelines
EN 50129	Railways applications - Safety-related electronic systems for signaling
EN 50128	Railways applications - Software for railway control and protection systems
EN 50159	Requirements for safety-related communication in closed/open transmission systems
(VDE 0116)	Elektrische Ausrüstung von Feuerungsanlagen
IEC 880	Software for computers in the safety systems of nuclear power stations

Functional Safety Standard – IEC61508

- Generic Standard supported by many sectors
  - Industry best practice standard to reduce the risk of hazardous event to a tolerable level

- Guidance on use of Electrical, Electronic and Programmable Electronic System which perform safety functions

- Consider the entire safety critical loop
  - Safety Instrumented Function (SIF) implemented by a Safety Instrumented System (SIS)

- SIS is responsible for the operation safety and ensuring the emergency stop within the limits considered as safe, whenever the operation exceeds such limits
  - SIS is a set of devices and software that perform one or more Safety Instrumented Functions (SIFs)
  - Detect dangerous situations and automatically take action to prevent accidents.
  - Think of it as an emergency control system

- Comprehensive approach involving concepts of **Safety Lifecyle** and all elements of protective system

- Risk-based approach leading to determination of Safety Integrity Level (**SIL**)
  - Each SIF has a stated Safety Integrity Level (SIL) that is related to the probability that the SIF will NOT work when challenged (when needed)

SIL, SIS and SIF Example

SIS

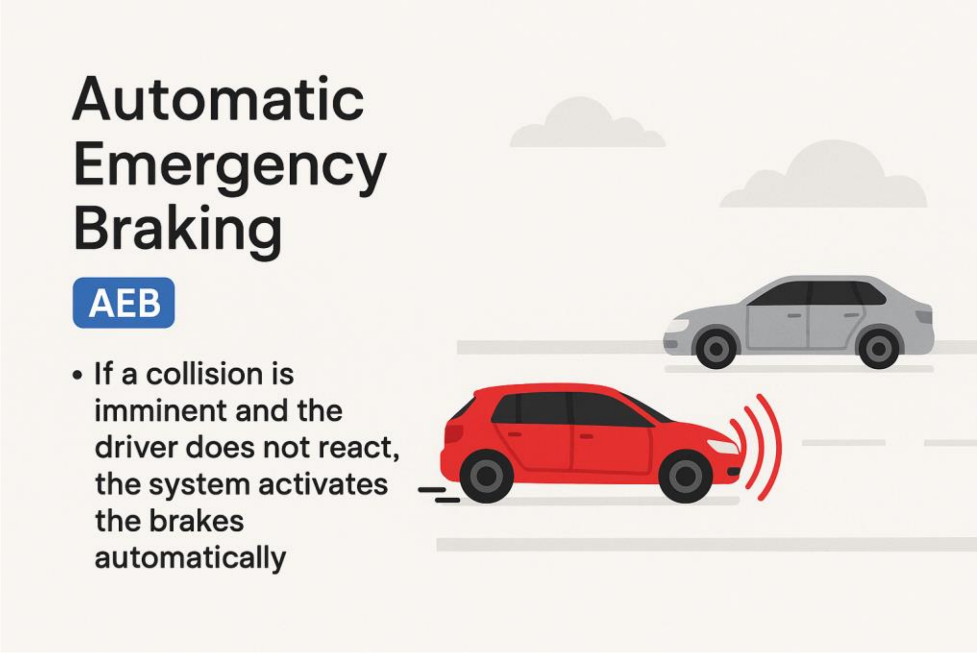
- The whole emergency braking system, including sensors, control logic, and brakes

SIF

- The specific function: “If an obstacle is detected and the driver doesn't react, apply the brakes.”

SIL

- How reliable the SIF function is

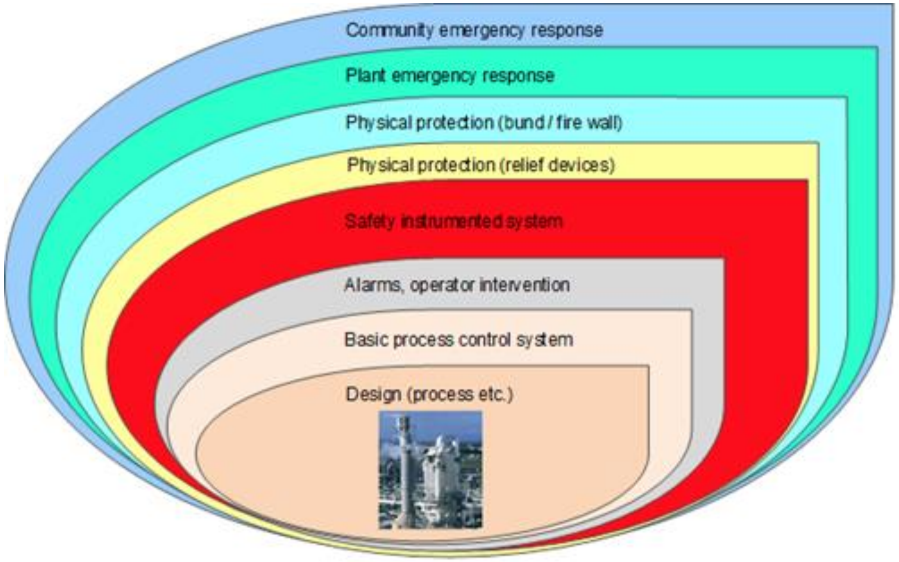


Automatic Emergency Braking

AEB

- If a collision is imminent and the driver does not react, the system activates the brakes automatically

Layers of Protection of a Plant


Community emergency response
Plant emergency response
Physical protection (bund / fire wall)
Physical protection (relief devices)
Safety instrumented system
Alarms, operator intervention
Basic process control system
Design (process etc.)

- Safety Instrumented System is the highest automated protection layer.
- Upper layers are passive or not automated

Safety Integrity Level

- SIL level is applicable to SIF (safety instrumented function)
- SIL is a discrete performance measurement
- Indicates the range of maximum acceptable probability of failure of a SIF
    - Either Probability of failure per demand
    - Or Probability of failure per hour

IEC standard 61508 for safety-related systems

Specifies four safety integrity levels, or SILs (with specified max. failure rates):

safety integrity level	control systems [per hour]	protection systems [per operation]
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$

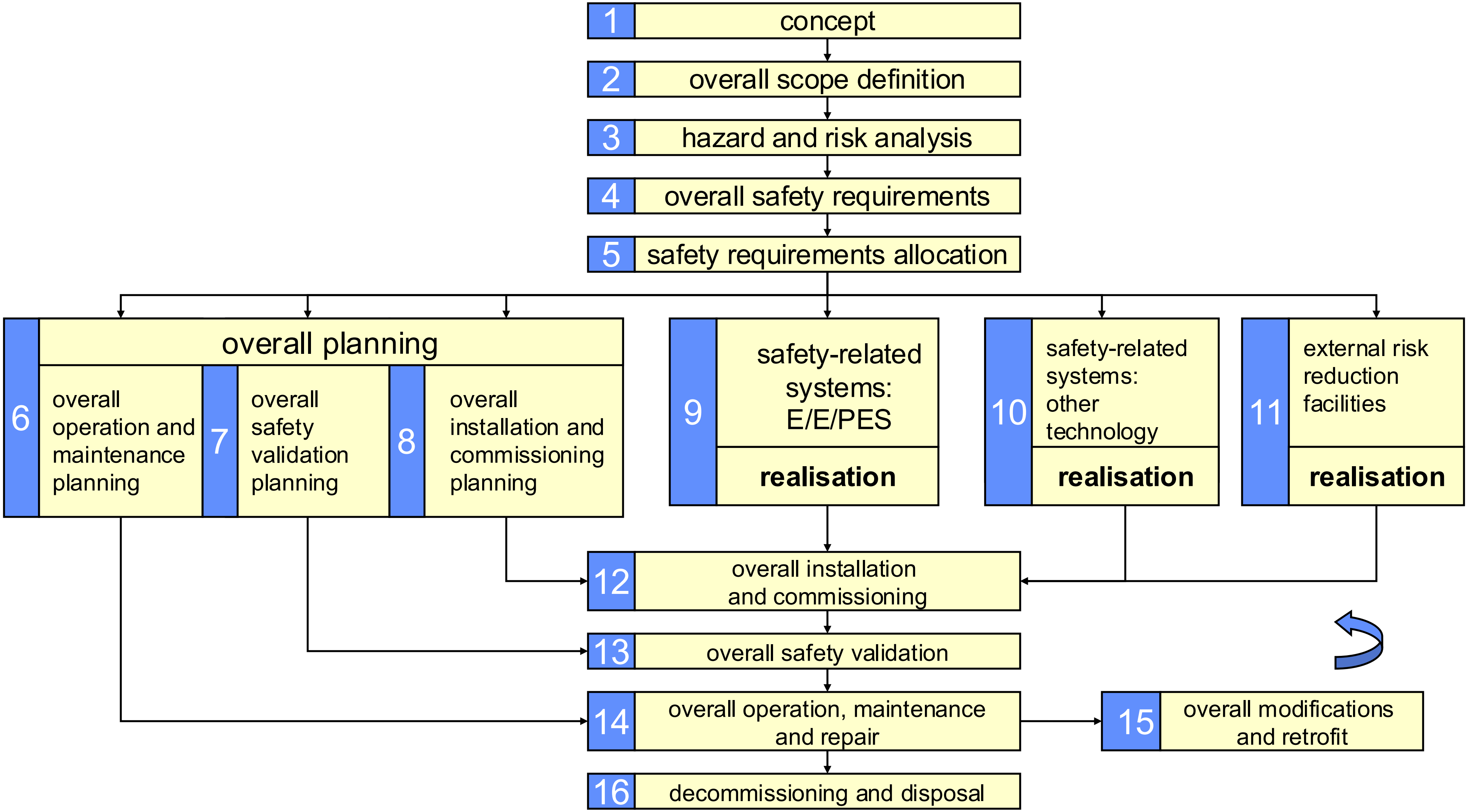
most safety-critical systems
(e.g. railway signalling)

< 1 failure every 10 000 years

1 failure every 100 000 operations

For each of the safety integrity levels it specifies requirements.

Cradle-to-grave reliability (IEC 61508)


1 concept
2 overall scope definition
3 hazard and risk analysis
4 overall safety requirements
5 safety requirements allocation
overall planning
6 overall operation and maintenance planning
7 overall safety validation planning
8 overall installation and commissioning planning
9 safety-related systems: E/E/PES
realisation
10 safety-related systems: other technology
realisation
11 external risk reduction facilities
realisation
12 overall installation and commissioning
13 overall safety validation
14 overall operation, maintenance and repair
15 overall modifications and retrofit
16 decommissioning and disposal

Methods for SIL Determination

- IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems)
  - Risk Graph
  - Hazardous event severity matrix

- IEC 61511 (Functional safety - Safety instrumented systems for the process industry sector)
  - Safety Layer Matrix
  - Risk Graph
  - Layer of Protection Analysis (LOPA)

Risk Graph

Extent of Damage

Ca = Minor Injury

Cb = Lost time injury

Cc = Major Injury

Cd = On-site fatality

Ce = Multiple on-site fatalities or one off-site fatality

Proportion of Time of Exposure to Hazard

Fa = Low (< 0.1)

Fb = High (> 0.1)

Mitigating Factors

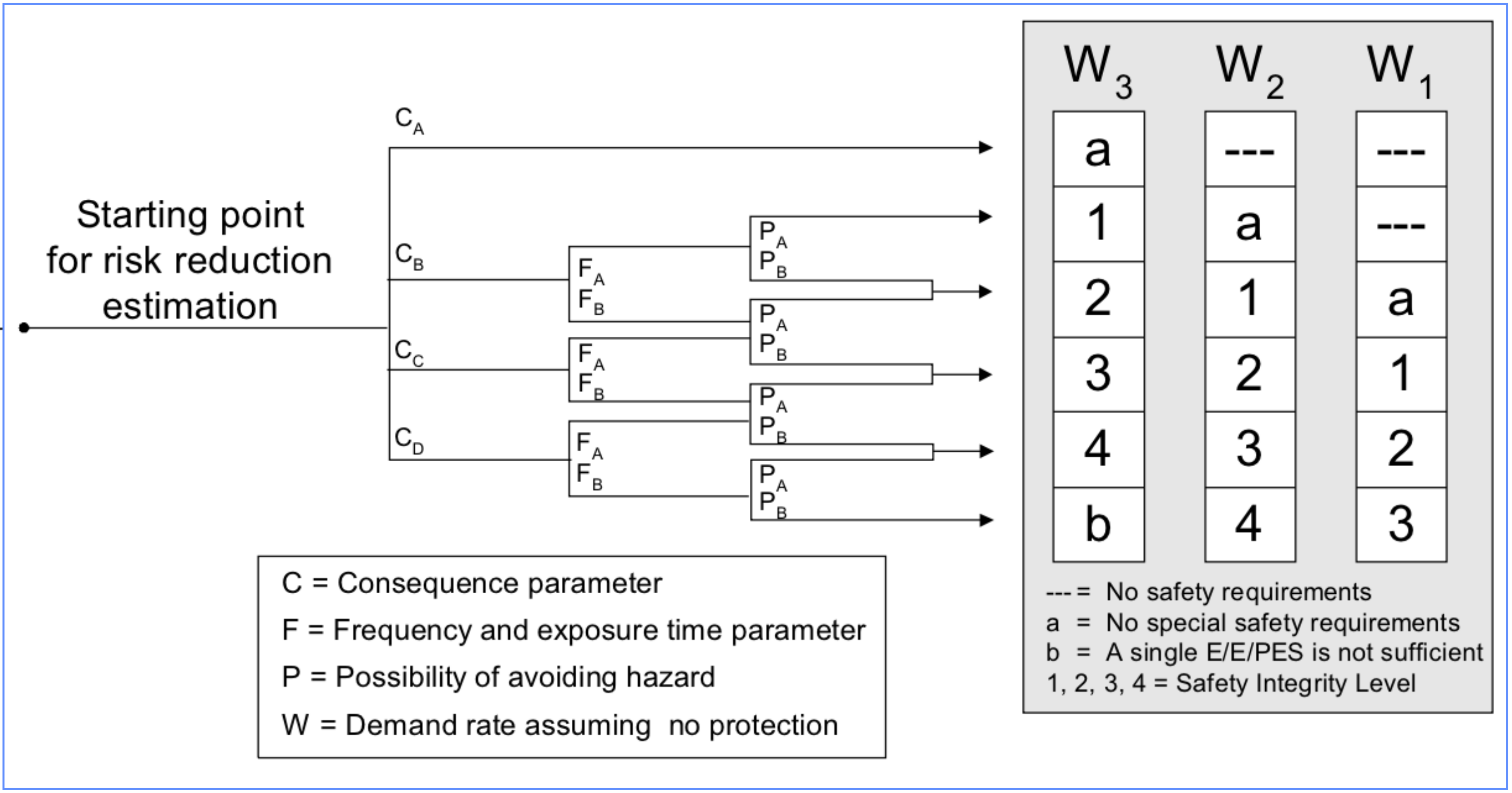
Pa = Good Chance of Avoiding Consequences (> 90%)

Pb = Poor Chance of Avoiding Consequences (< 10%)

Prob or Freq of Hazardous Event

W1 = Very Low (F < 0.01 / YR)

W2 = Low (F > 0.01 / YR)



W_3	W_2	W_1
a	---	---
1	a	---
2	1	a
3	2	1
4	3	2
b	4	3

--- = No safety requirements
a = No special safety requirements
b = A single E/E/PES is not sufficient
1, 2, 3, 4 = Safety Integrity Level

C = Consequence parameter
F = Frequency and exposure time parameter
P = Possibility of avoiding hazard
W = Demand rate assuming no protection

Summary/Questions

- What is FMEA
- What is FMECA
- What is FTA
- What is SIS, SIF and SIL
- How many SIL levels exist? Which level certifies less failure?
- Cite an example of SIL determination