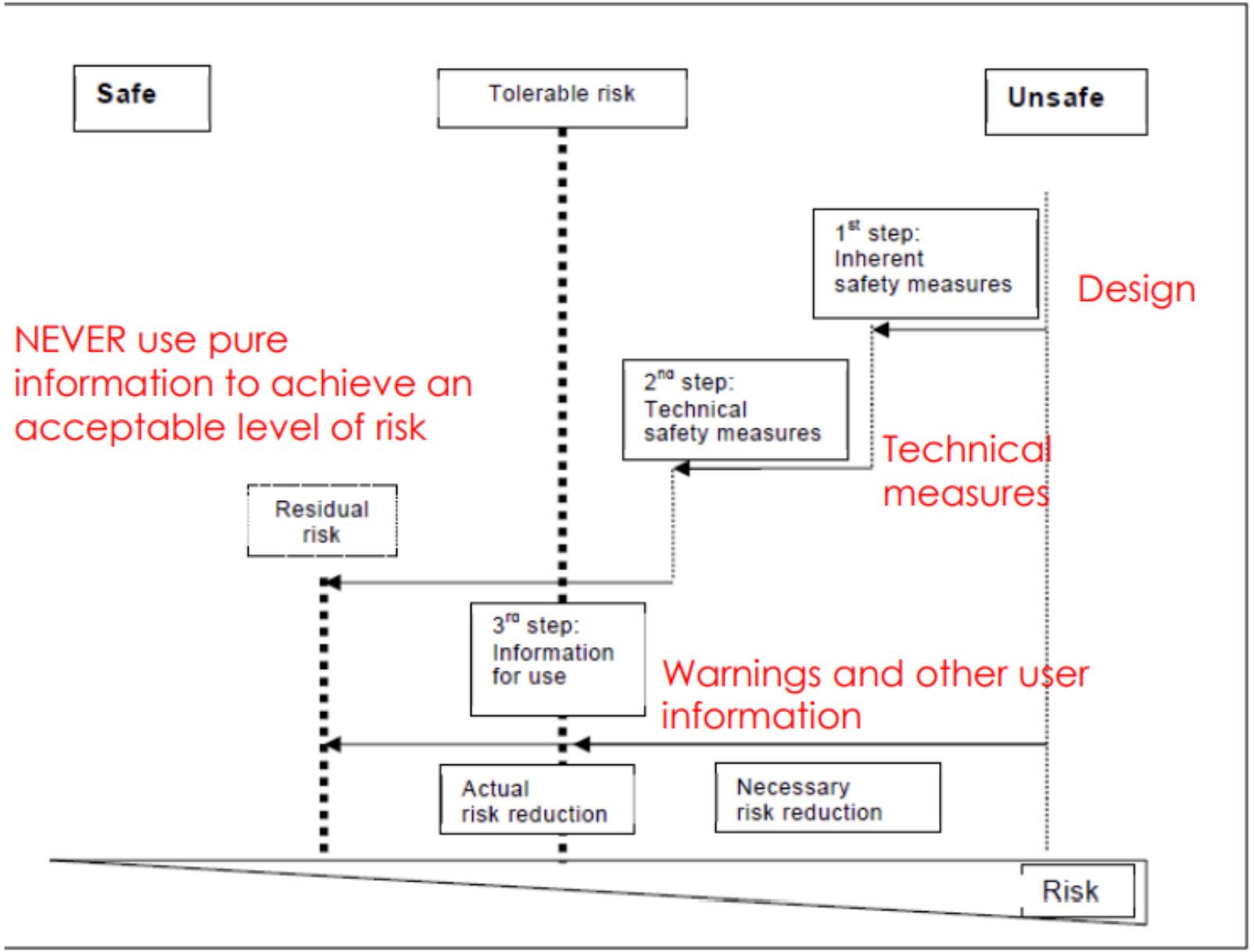

DTU


Safe
Tolerable risk
Unsafe
1st step: Inherent safety measures
Design
NEVER use pure information to achieve an acceptable level of risk
2nd step: Technical safety measures
Technical measures
Residual risk
3rd step: Information for use
Warnings and other user information
Actual risk reduction
Necessary risk reduction
Risk

Agenda

- Accident-Causation Theories
- Safety consideration in life cycle of system
- Human-machine Interaction and “Trust"
- Functional safety and its standards
- Risk and Risk Criteria
- Barrier theories
- Exercise

Accident-Causation Theories

Man crushed to death by robot in South Korea

8 November 2023

Share Save

Emily Atkinson
BBC News

A man has been crushed to death by a robot in South Korea after it failed to differentiate him from the boxes of food it was handling, reports say.

Accident-Causation Theories

- The most widely known theories of accident causation:

-Domino theory

-Human factors theory

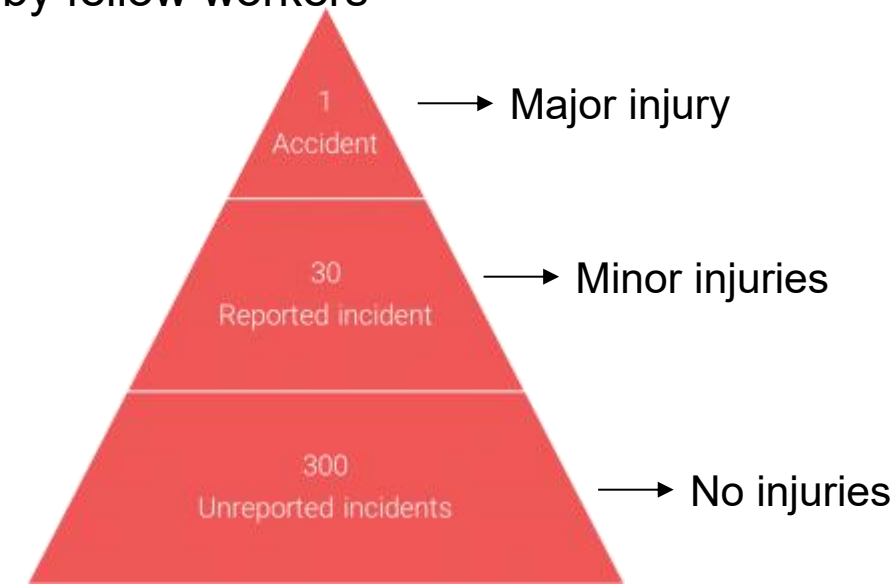
Domino Theory by Herbert.W. Heinrich

- In the late 1920's studying reports of 75,000 workplace accidents, he concluded the following:

-88% of accidents are caused by unsafe acts committed by fellow workers

-10% of accidents are caused by unsafe conditions

-2% of accidents are unavoidable



- It laid foundation for Axioms of Industrial Safety

Reference. Heinrich, H. W., and E. R. Granniss. Industrial Accident Prevention : McGraw-Hill, 1959, pp. 480 s.

Axioms of Industrial Safety

Injuries result from a completed series of factors, one of which is the accident itself.

An accident can occur only as the result of an unsafe act by a person and/or a physical or mechanical hazard.

Most accidents are the result of unsafe behavior by people.

An unsafe act by a person or an unsafe condition does not always immediately result in an accident/injury.

Reasons why people commit unsafe acts can serve as helpful guides in selecting corrective actions.

Severity of an accident is largely fortuitous, and the accident that caused it is largely preventable.

The best accident prevention techniques are analogous with the best quality and productivity techniques.

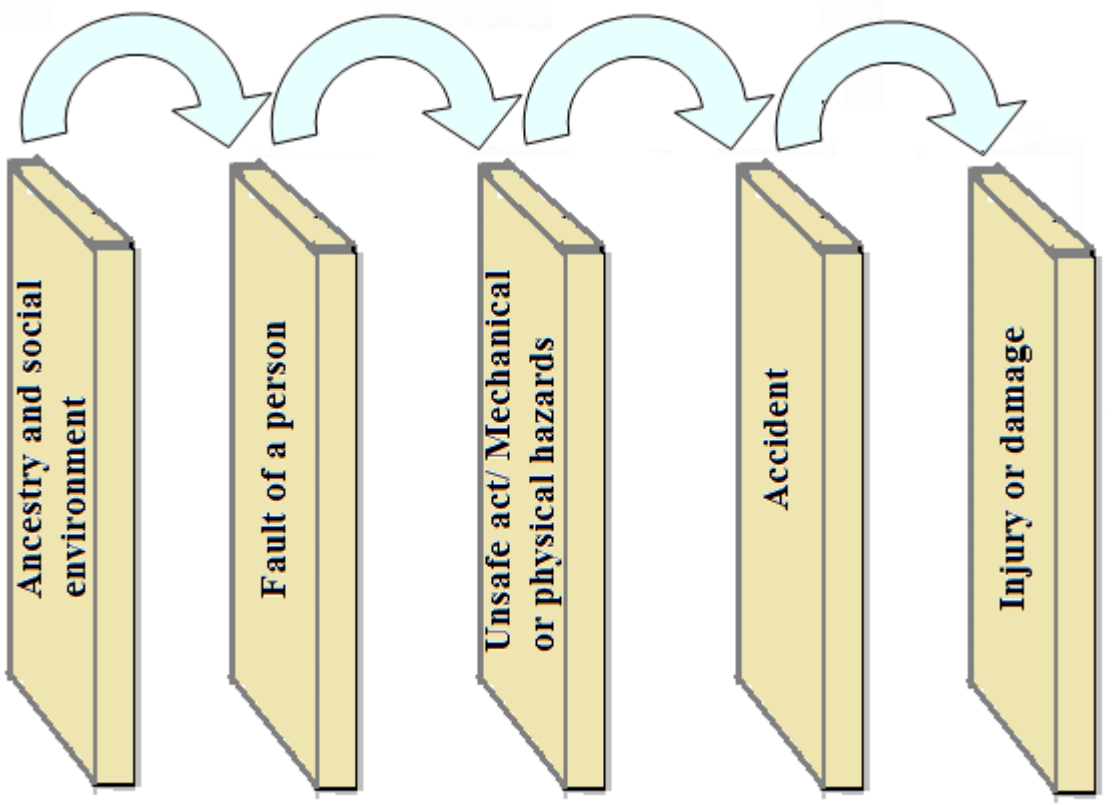
Management should assume responsibility for safety because it is in the best position to get results.

The supervisor is the key person in the prevention of industrial accidents.

Direct costs of an accident (for example, compensations, liability claims, medical costs, and hospital expenses), there are also hidden or indirect

Domino theory by Herbert.W. Heinrich

Five factors in sequence leading to an accident



It provided the foundation for accident prevention measures aimed at preventing unsafe acts or unsafe conditions.

Domino theory-example

- A construction company is a distributor of lumber, pipe and concrete products.
- Warehouse personnel load most of the orders by hand therefore they are required to wear personal protective gear.
- Management observed increases in minor injuries among personnel during summer months. However, during the last summer, they suffered from the serious back injuries of two workers.

Domino Theory-example

- Investigation revealed a series of events and a central causal behavior which created a domino effect.

-Personal protection gear becomes uncomfortable due to hot weather and loaders take it off.

-This situation increases the number of minor injuries, but management does not pay attention due to the nature of injuries. Therefore, it was probably inevitable to suffer from more serious injuries.

Domino Theory-example

- Solution:
- Removing the causal factor-the failure of warehouse personnel to use their personal protective gear during summer months.
- Forming a committee.

Committee's recommendations:

1. Provide all warehouse personnel with training on the importance and proper use of personal protection.
2. Require warehouse supervisors to monitor the use of personal protection gear more closely.
3. Establish a company policy that contains specific and progressive disciplinary measures for failure to use required personal protection gear.
4. Implement several heat reduction measures to make warehouses cooler.

Human Factors Theory

By Ferrell

- Attributes accidents to a chain of events ultimately caused by human error.

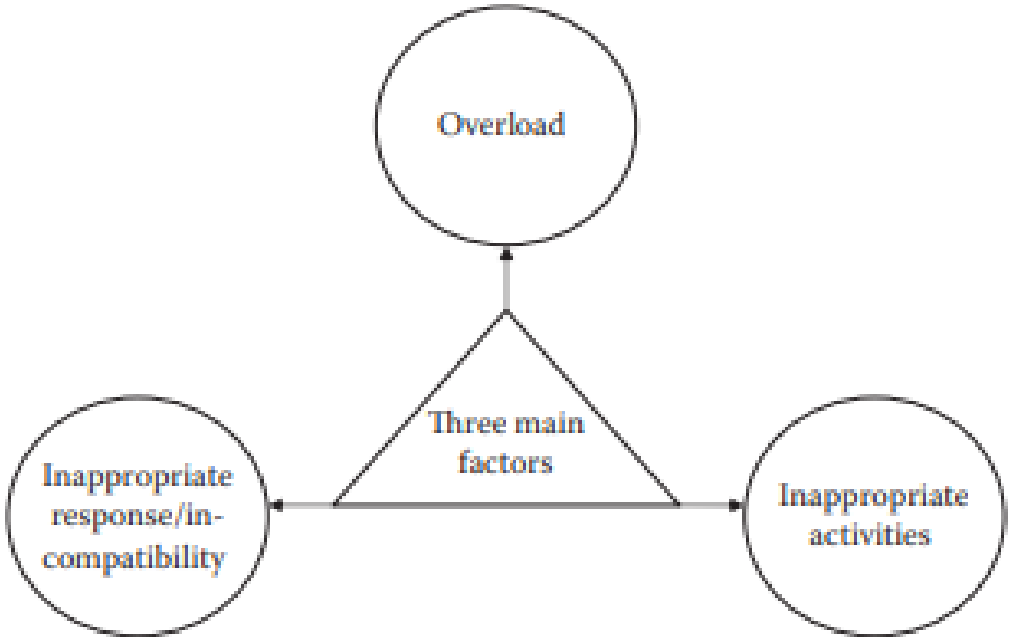
- Consists of three broad factors that lead to human error:
- Overload
- Inappropriate Response or Incompatibility
- Inappropriate Activities

Human Factors Theory

An imbalance between the capacity of an individual at any time and the load he/she is carrying in a given state

How a person responds to a given situation can cause or prevent an accident: e.g.,

- A person completely disregards the specified safety procedures
- A person removes a safeguard from a machine for increasing output
- A person detects a hazardous condition, but takes no corrective action



Inappropriate activities undertaken due to human error, poor judgment about the degree of risk invovled in a given task and subsequently acting on that misjudgment.

Examples:

-A person who undertakes a task that he/she does not know how to do.

Human Factors Theory-Example

- A construction company see rapid growth in sales which overwhelmed company's work force.
- New teams of carbinet makers and installers hired.
- Authorized unlimited overtime.
- Numbers of accidents and injuries increased.

Human Factors Theory-Example

- According to Human Factors Theory, possible causes in the three categories:

-Overload:

- Employees working beyond their personal limits and beyond their capacities.
- Stress, insufficient training and fatigue

- Inappropriate response:
- Cerpenters removing the safegaruds to speed up construction.

-Inappropriate activities:

- Assigning employees to duties for which they are not fully trained.

Safety consideration in life cycle of system

Safety consideration in life cycle of system

- Safety starts at the design stage; it can be assured in two ways:

-inherent safety

-safety that is engineered

Inherent safety

- Where the idea comes from?

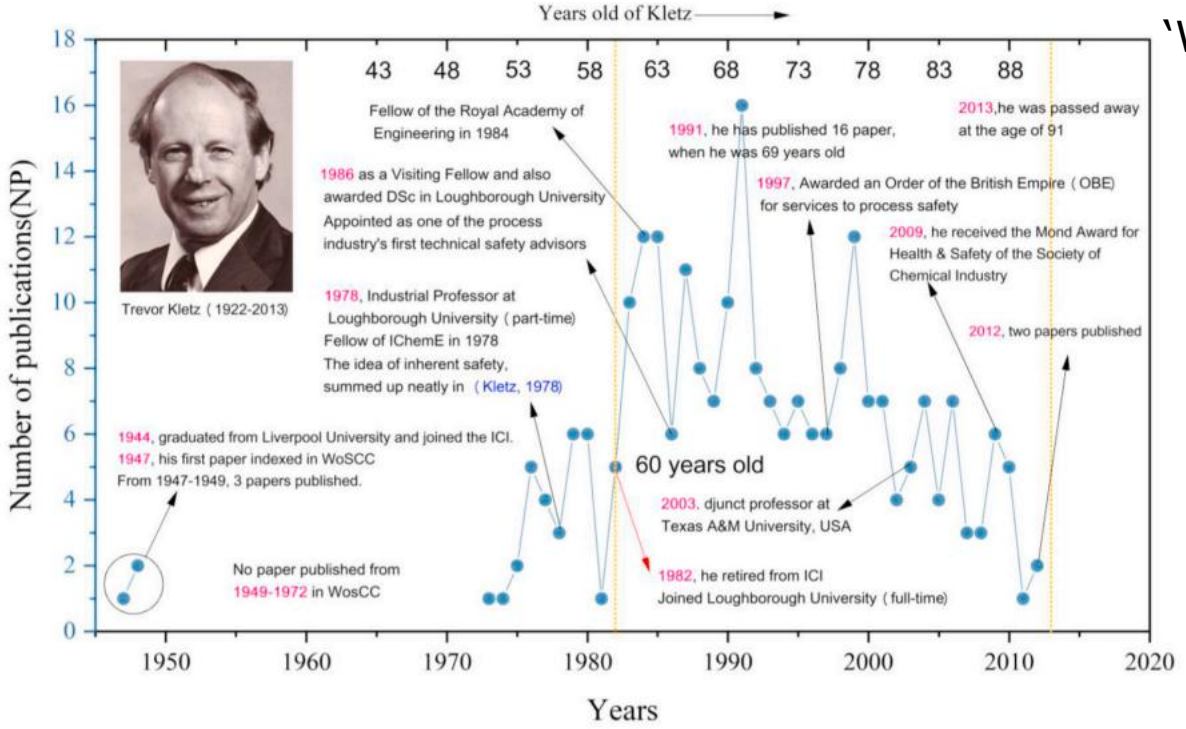


Fig. 3. Evolution trend of Dr. Kletz's published research articles in context of key events in his career

Li, Jie, et al. "Trevor Kletz's Scholarly Legacy: A Co-Citation Analysis." Journal of Loss Prevention in the Process Industries, vol. 66, Elsevier Ltd, 2020, p. 104166, doi:10.1016/j.jlp.2020.104166.

'What You Don't Have, Can't Leak' (Kletz, 1978)

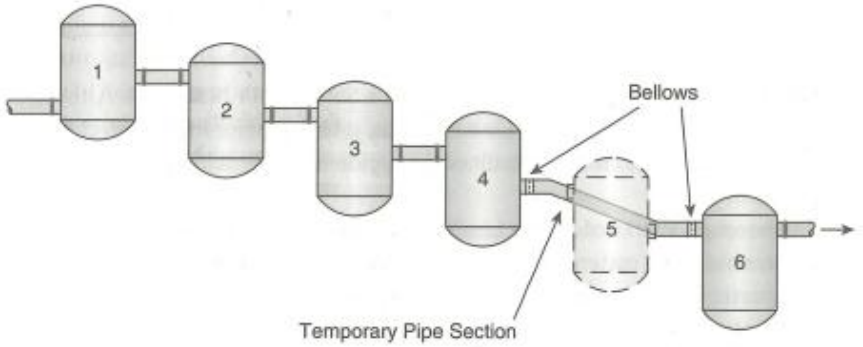


Figure 1-10 A failure of a temporary pipe section replacing reactor 5 caused the Flixborough accident.

Inherent safety

- This is the best way of ensuring safety, because it does not have to reply on the correct functioning of safety devices.

- Inherent safety includes:

-reducing the inventories of hazardous materials or, if possible, replacing them by less hazardous materials (Minimize and Substitute)

-the use of alternative process routes involving lower pressures or more moderate temperatures (Moderate)

-designing processes to be less complicated and therefore less prone to failure (Simplify)

Table 1-20 Inherently Safer Design Strategies

Type	Example applications
Minimize (intensification)	Replace a large batch reactor with a smaller continuous reactor. Reduce storage inventory of raw materials. Improve management and control to reduce inventory of hazardous intermediate chemicals. Reduce process hold-up.
Substitute (substitution)	Use mechanical pump seals instead of packing. Use a welded pipe rather than a flanged pipe. Use solvents that are less hazardous. Use chemicals with higher flash point temperatures, boiling points, and other less hazardous properties. Use water as a heat transfer fluid instead of hot oil.
Moderate (attenuation and limitation of effects)	Reduce process temperatures and pressure. Use a vacuum to reduce the boiling-point temperature. Refrigerate storage vessels to reduce the vapor pressure of liquids. Dissolve hazardous material in a nonhazardous solvent. Operate at conditions where reactor runaway is not possible. Locate control rooms remotely from the process to reduce impacts of accidents. Provide adequate separation distance from process units to reduce impacts of accidents. Provide barriers to reduce impacts of explosions. Provide water curtains to reduce downwind concentrations.
Simplify (simplification and error tolerance)	Reduce piping lengths, valves, and fittings. Simplify piping systems and improve ability to follow the pipes within them. Design equipment layout for easy and safe operation and maintenance. Select equipment that requires less maintenance. Select equipment with higher reliability. Label process equipment—including pipelines—for easy identification and understanding. Design control panels and displays that are easy to comprehend. Design alarm systems to provide the operators with critical information.

Crowl, Daniel A., and Joseph F. Louvar. 2011. Chemical Process Safety : Fundamentals with Applications. Prentice Hall.

Inherent safe design measures for robotics applications

1. Minimize (reduce hazard magnitude)

Reduce the *amount of energy, force, speed, or mass* involved so even failures are less dangerous.

Examples in robotics

- Use **lightweight robot arms** instead of heavy industrial manipulators
- Limit **speed, torque, and force** to the minimum needed for the task
- Reduce **payload mass** and end-effector inertia
- Minimize **stored energy** (low-pressure pneumatics, low-voltage systems)
- Shorten robot reach and workspace to only what's necessary

Inherent safe design measures for robotics applications

2. Substitute (replace the hazard)

Replace hazardous technologies, components, or processes with safer ones.

Examples in robotics

- Electric actuators instead of hydraulic systems (no high-pressure fluid leaks)
- Rounded, compliant grippers instead of sharp mechanical tools
- Vision-based inspection instead of human presence in hazardous areas
- Low-voltage DC power instead of high-voltage supplies
- Software-defined safety zones instead of hard physical intrusion risks

Inherent safe design measures for robotics applications

3. Moderate (attenuate severity)

If hazards can’t be eliminated, reduce their impact or consequences.

Examples in robotics

- Speed and separation monitoring (robot slows as humans approach)
- Force and torque limiting to avoid injury on contact
- Soft or padded robot surfaces
- Compliant joints and series elastic actuators
- Operating robots at lower temperatures (no hot surfaces)
- Safe stop modes instead of abrupt emergency stops that could create secondary hazards

Inherent safe design measures for robotics applications

4. Simplify (reduce complexity and error)

Design systems that are easy to understand, operate, and maintain—fewer mistakes, fewer failures.

Examples in robotics

- Simple, intuitive human–machine interfaces (HMI)
- Clear visual indicators of robot state (idle, moving, fault, safe)
- Reduced wiring, fewer sensors where possible
- Modular robot cells with standardized components
- Clear labeling of robot work envelopes and safety zones
- Straightforward recovery procedures after faults

Inherent safety to robotics

ISO 12100:2010, section 6.2 inherently safe design measure: protective measure which either eliminates hazards or reduces the risks associated with hazards by changing the design or operating characteristics of the machine without the use of guards or protective devices.

prEN ISO 12100: 2025 on the way.

SO 10218–1:2025,

ISO 10218-2: 2025

[Safety Connection | New ISO 10218:2025: Industrial Robots]

Engineered safety

- ISO 12100: Guard and protective device (3.27 and 3.28)
- Process system: Passive and active

Guard: physical barrier, designed as part of the machine to provide protection

Passive: minimize the hazard through process and equipment design features without the active functioning of any device

Active: requires an active response, engineering controls

It is not sufficient and certainly not cost effective to carry out the only safety review once the design is complete and then depends on the safety devices.

Safety in Operation

- Operating instructions play a particularly important part in the safe operation of process plant or a robot.

- They should contain information on all hazards likely to be encountered in the operation of the plant or robotics system and full details of what to do in the event of abnormal conditions developing.

- Major hazards in operation are due to:

-process hazards

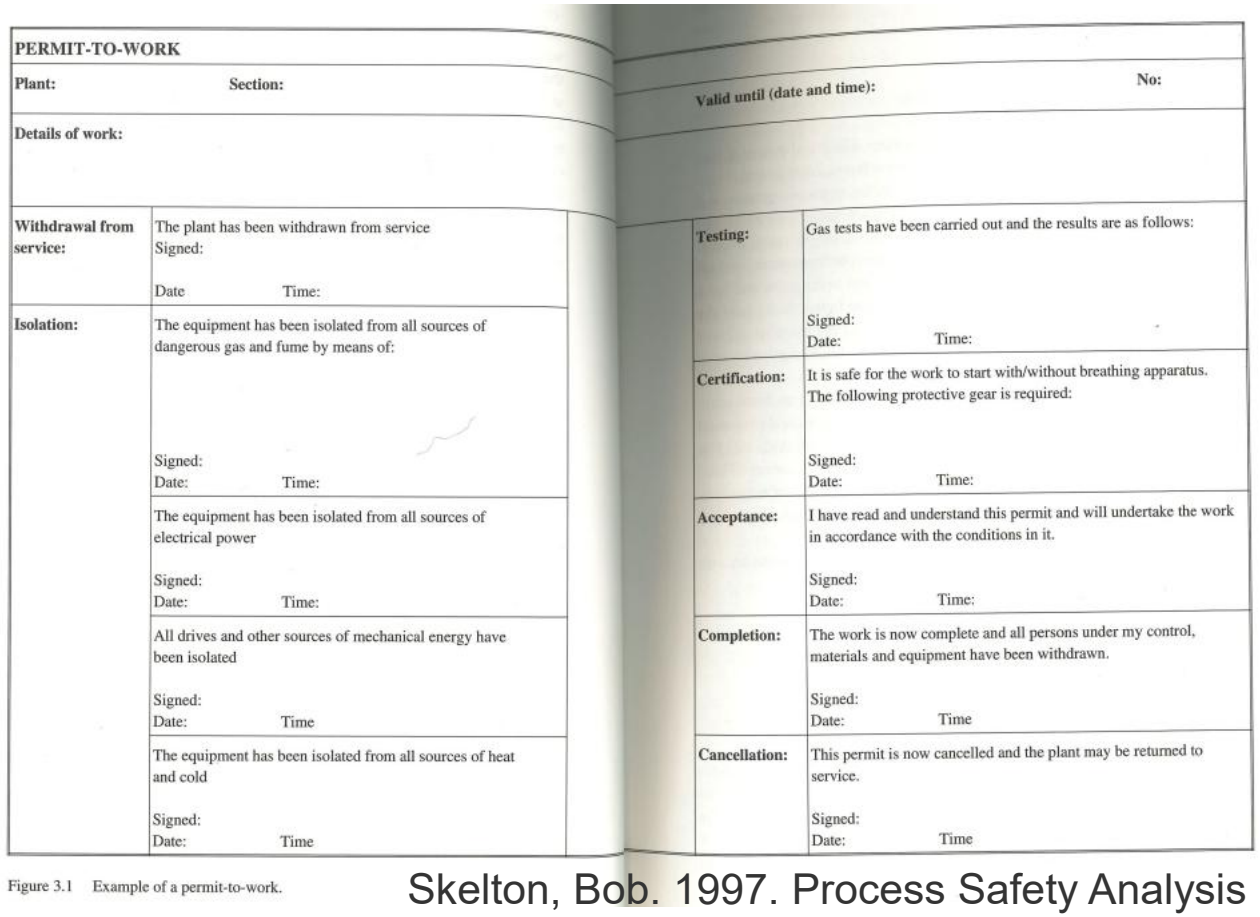
-machine guards

-safe access

-electrical safety

Safety in Maintenance

- Accidents to maintenance personnel
- Accidents resulting from improper maintenance procedures

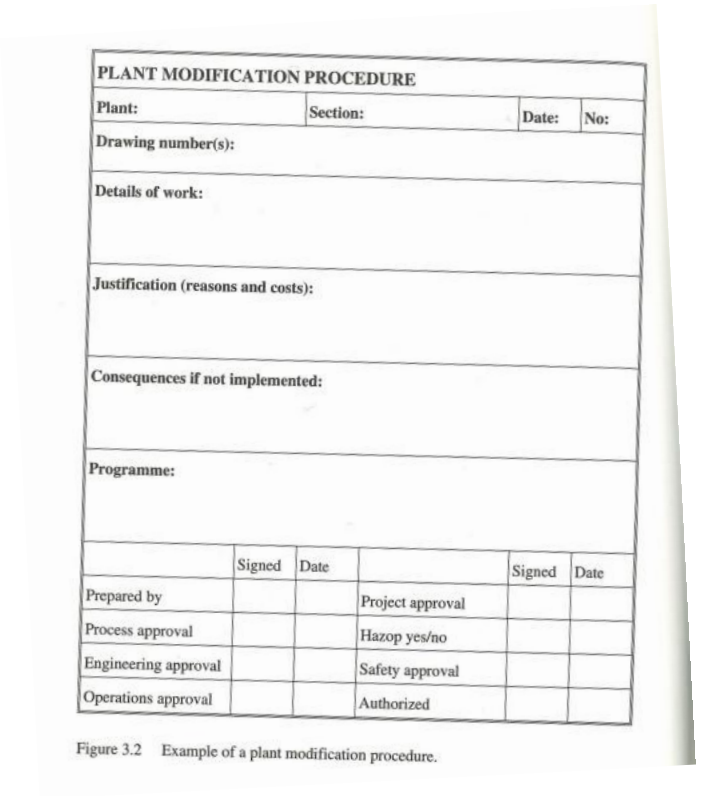


PERMIT-TO-WORK

Plant:	**Section:**
Details of work:	
Withdrawal from service:	The plant has been withdrawn from service Signed: Date Time:
Isolation:	The equipment has been isolated from all sources of dangerous gas and fume by means of: Signed: Date: Time:
	The equipment has been isolated from all sources of electrical power Signed: Date: Time:
	All drives and other sources of mechanical energy have been isolated Signed: Date: Time
	The equipment has been isolated from all sources of heat and cold Signed: Date: Time

Valid until (date and time):	**No:**
Testing:	Gas tests have been carried out and the results are as follows: Signed: Date: Time:
Certification:	It is safe for the work to start with/without breathing apparatus. The following protective gear is required: Signed: Date: Time:
Acceptance:	I have read and understand this permit and will undertake the work in accordance with the conditions in it. Signed: Date: Time:
Completion:	The work is now complete and all persons under my control, materials and equipment have been withdrawn. Signed: Date: Time
Cancellation:	This permit is now cancelled and the plant may be returned to service. Signed: Date: Time

Figure 3.1 Example of a permit-to-work.



PLANT MODIFICATION PROCEDURE

Plant:	**Section:**	**Date:**	**No:**
Drawing number(s):			
Details of work:			
Justification (reasons and costs):			
Consequences if not implemented:			
Programme:			

	Signed	Date		Signed	Date
Prepared by			Project approval		
Process approval			Hazop yes/no		
Engineering approval			Safety approval		
Operations approval			Authorized		

Figure 3.2 Example of a plant modification procedure.

Skelton, Bob. 1997. Process Safety Analysis : an Introduction. Inst. of Chemical Engineers.

Human-machine (robot) Interaction and "Trust"

Agenda

- Human machine (Robot) Interaction
- Automation and Human Factors
- Ethical Issues in HMI or HRI

Human machine (robot) interaction (MHI or HRI)

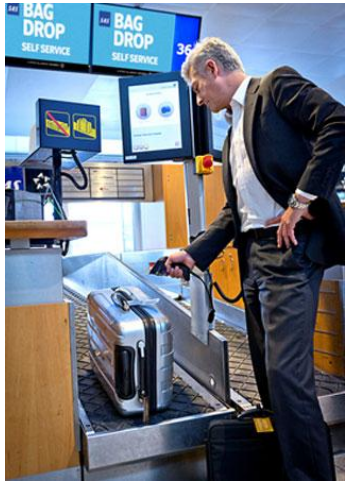
- Interactive system: combination of hardware and/or software and/or services and/or people that users interact with in order to achieve specific goals.

- Example: Check-in

-Self-Service Check-in

-Check-in counters

-Online check-in



HRI

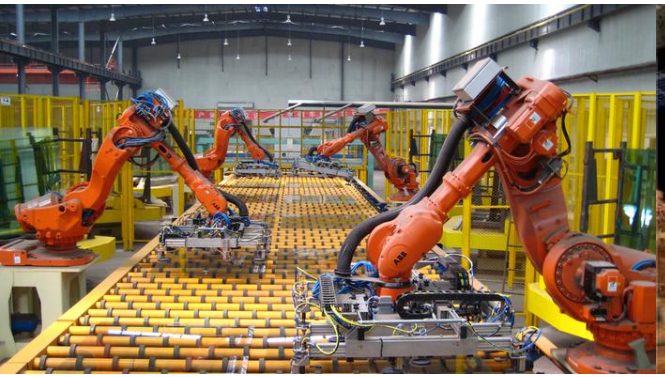
- Four application areas:

-*Telerobots:* Human supervisory control of robots in performance of routine tasks.

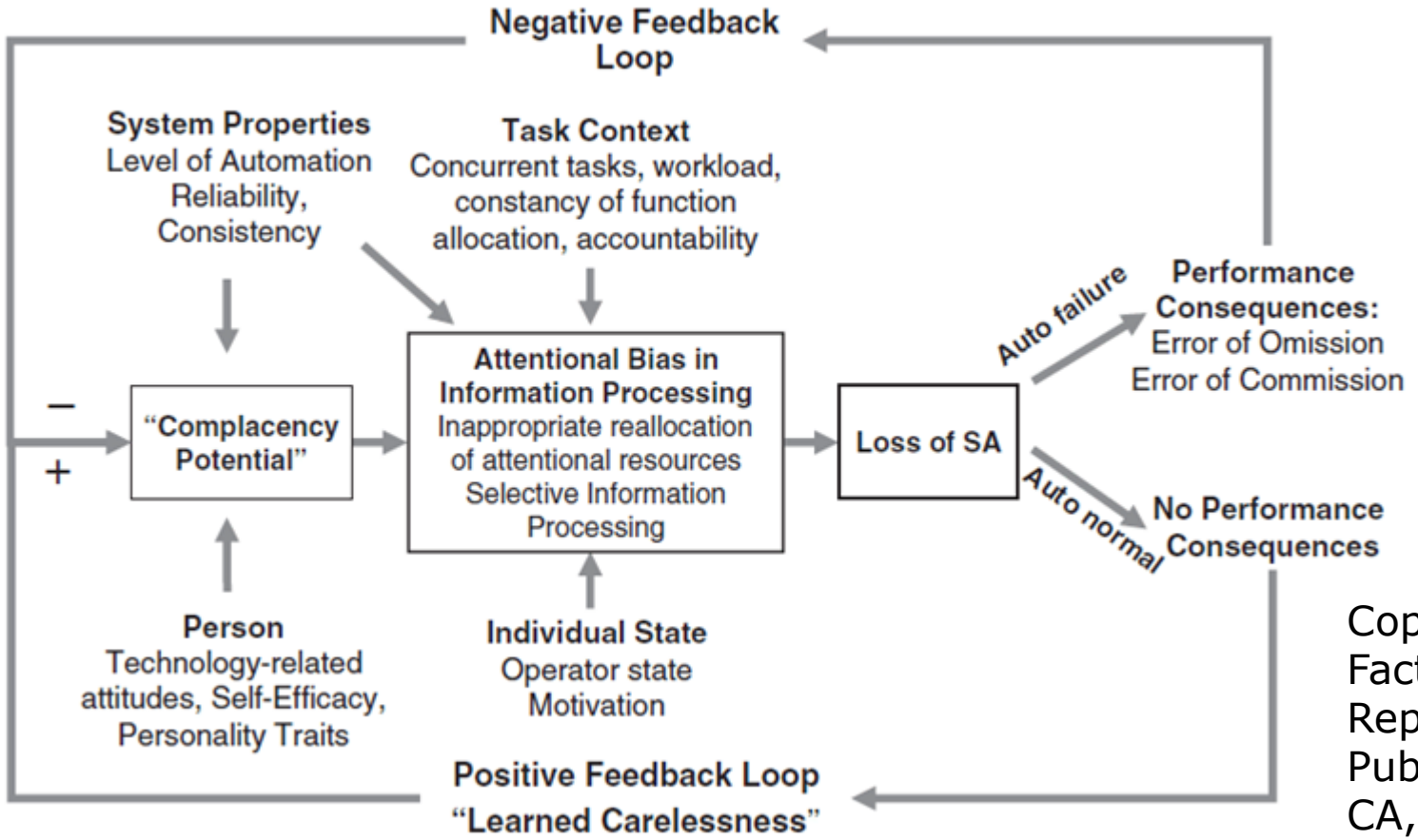
-*Teleoperators*: Remote control of space, airborne, terrestrial, and undersea vehicles for nonroutine tasks in hazardous or inaccessible environments.

-Automated vehicles in which a human is a passenger, including automated highway and rail vehicles and commercial aircraft.

-Human–robot social interaction, including robot devices to provide entertainment, teaching, comfort, and assistance for children and elderly, autistic, and handicapped persons.



Automation and Human Factors



Ethical issues in HMI or HRI

- HitchBOT

- hitchBOT was a Canadian hitchhiking robot created by professors David Harris Smith of McMaster University and Frauke Zeller of Ryerson University in 2013. It gained international attention for successfully hitchhiking across Canada, Germany and the Netherlands, **relying purely kindness of strangers**, but in 2015 its attempt to hitchhike across the United States ended when it was stripped and decapitated in Philadelphia, Pennsylvania.

Ethical issues in HMI or HRI

- On July 2, 1994, USAir Flight 1016 was scheduled to land in the Douglas International Airport in Charlotte, NC. Upon nearing the airport, the plane experienced inclement weather and was affected by wind shear (a sudden change in wind velocity that can destabilize an aircraft). On the ground, a wind shear alert system installed at the airport issued a total of three warnings to the air traffic controller. But due to **a lack of trust** in the alert system, the air traffic controller transmitted only one of the alarms that was, unfortunately, never received by the plane. Unaware of the presence of wind shear, the aircrew failed to react appropriately and the plane crashed, killing 37 people.

Ethical issues in HMI or HRI

- Georgia Institute of Technology in Atlanta

A study showed that people willingly ignored the emergency exit sign to follow an evacuation robot taking a wrong turn during a (simulated but realistic) fire emergency.

A total of 26 of the 30 participants chose to follow the robot during the emergency. Of the remaining four, two were thrown out of the study for unrelated reasons, and the other two never left the room.

These examples drive home a key message: miscalibrated trust can lead to misuse of robots and sometimes accidents in the end.

IEC 63303:2024 based on a US document, ANSI/ISA-101.01, HMIs for process automation systems

- Abstract

- IEC 63303:2024 defines general structures and functions of HMI systems.
  An HMI life cycle example for HMI systems is included.
  This document specifies requirements and recommendations for activities in each stage of the life cycle including designing, using, and maintaining the HMI system.
  It also provides requirements and recommendations for functions and performance of HMI systems.
  The requirements and recommendations in this document are applicable to any controlled process using an HMI to interface to a control system. There can be differences in implementation to meet the specific needs based on the application and controlled process type.

HMI life cycle model

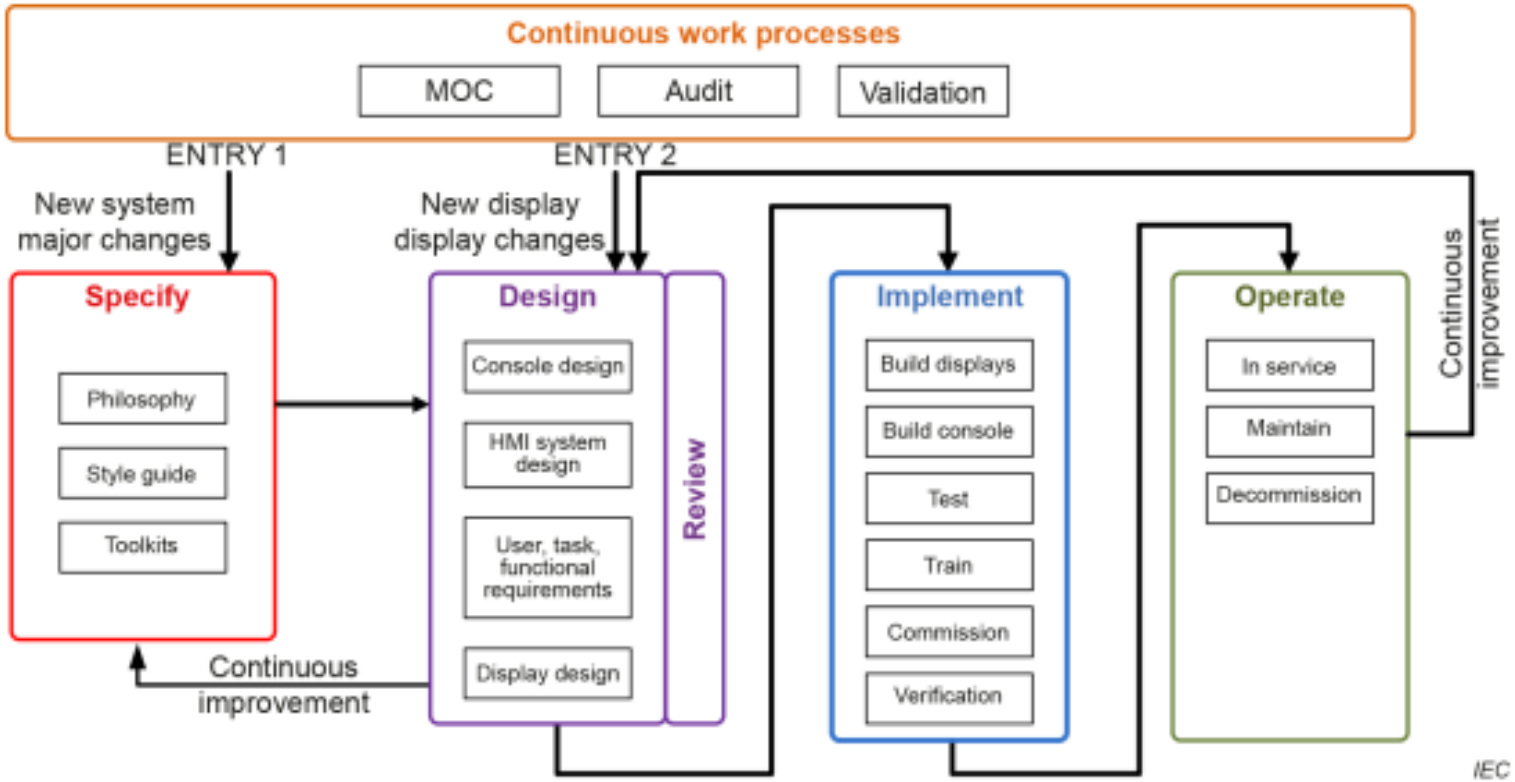
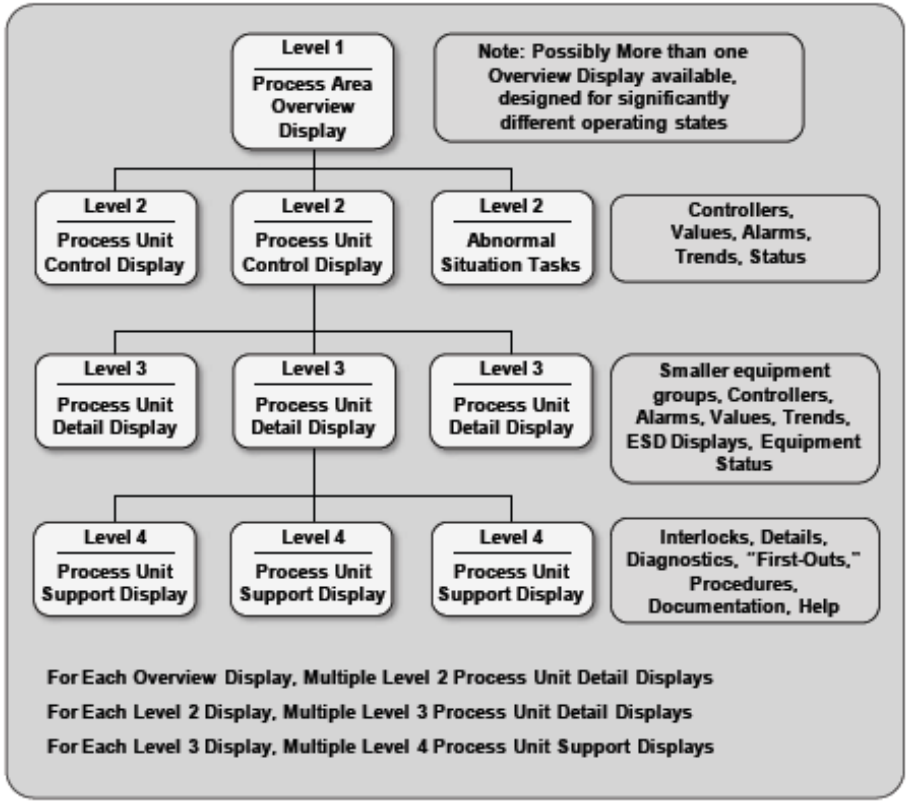
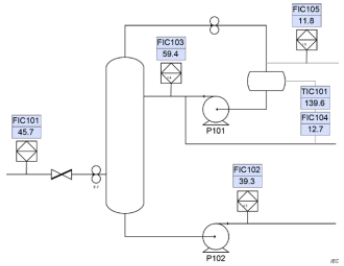


Figure 1 – Example of HMI life cycle

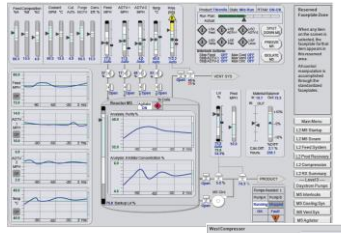
Display hierarchy



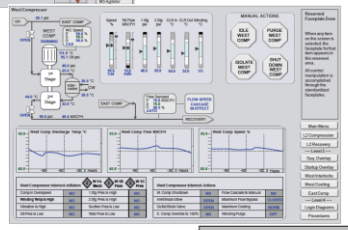
- Level 1: broadest scope, while level 4: the most focused scope



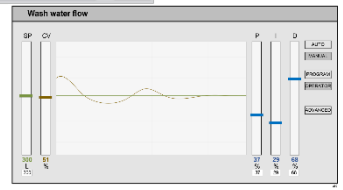
Level 1



Level 2



Level 3



Level 4

HMI example

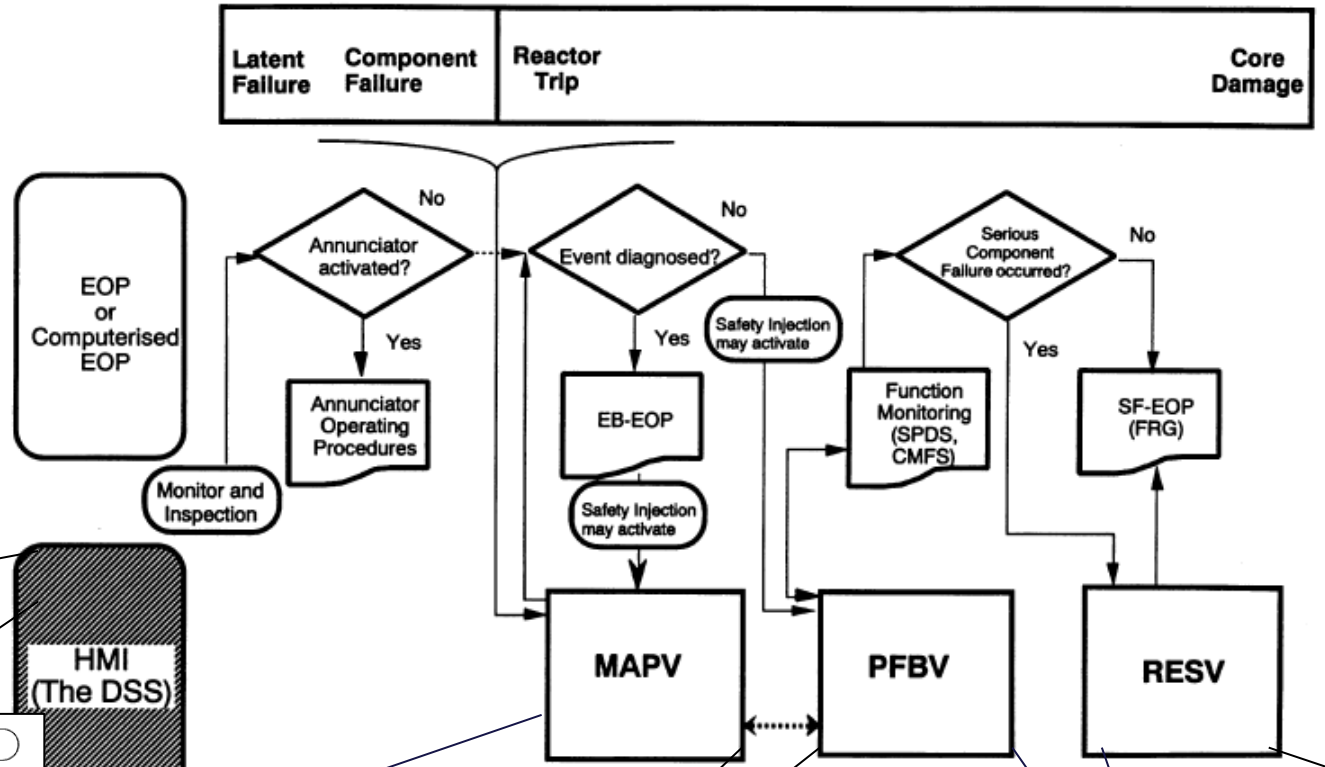


Fig. 11. Navigation considering the combined use of EOP and DSS.

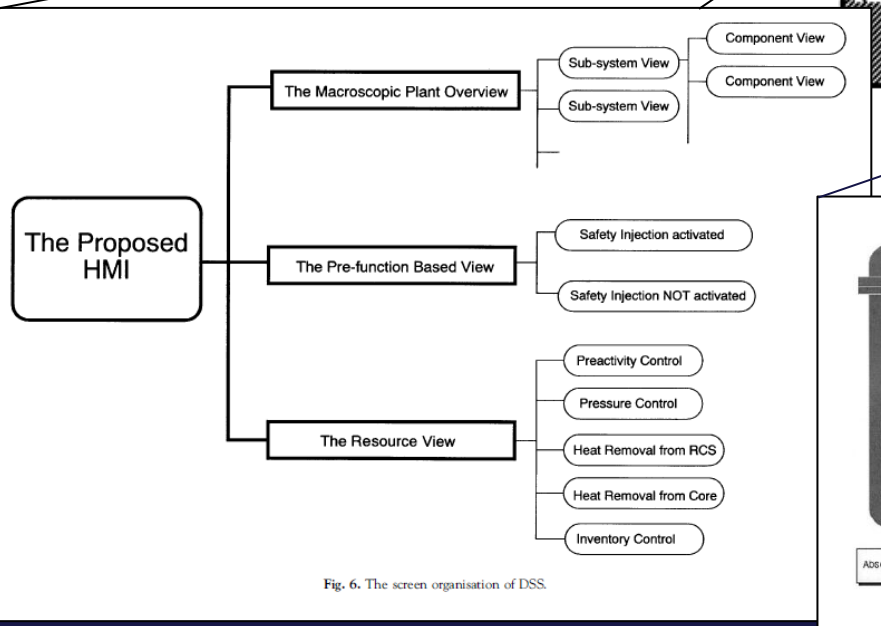


Fig. 6. The screen organisation of DSS.

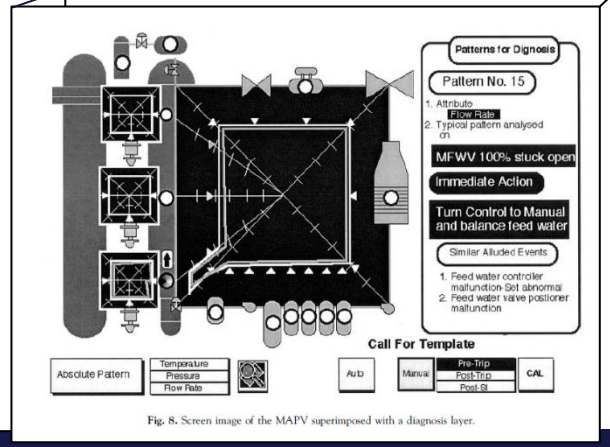


Fig. 8. Screen image of the MAPV superimposed with a diagnosis layer.

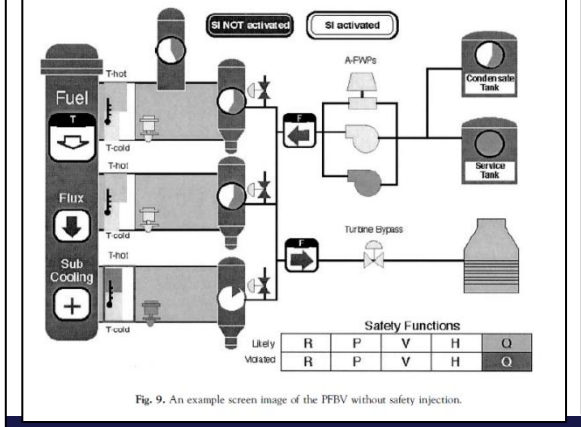


Fig. 9. An example screen image of the PFBV without safety injection.

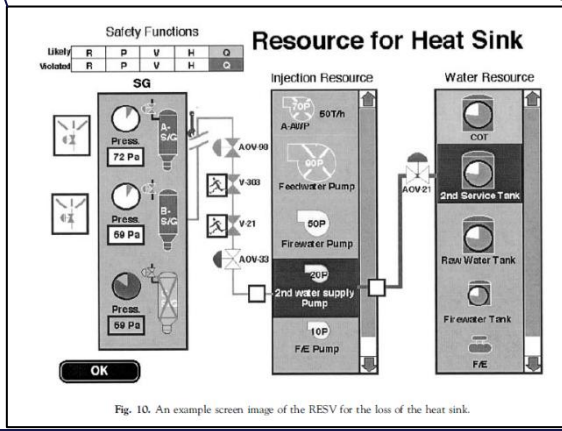


Fig. 10. An example screen image of the RESV for the loss of the heat sink.

Functional safety and its standards

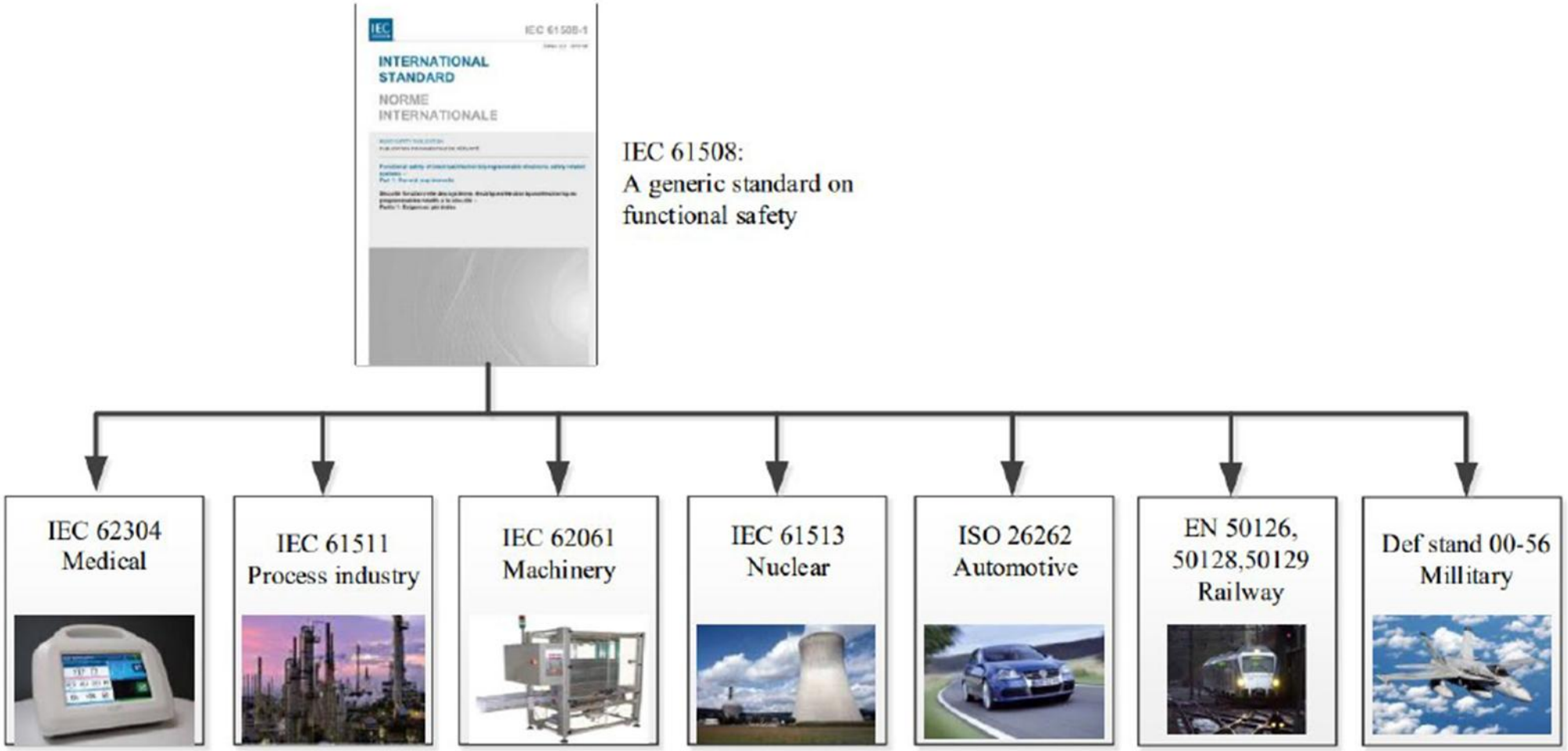


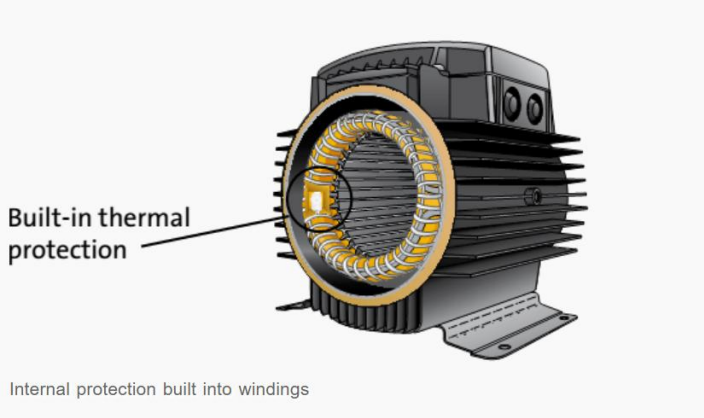
Figure by Mary Ann Lundteigen

Functional safety and its standards

- IEC61508-Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)

Regulate mechanical safety according to functions and reliability from around the year 2000.

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



Internal protection built into windings

Two types of requirements

- Two types of requirements are necessary to achieve functional safety:

-safety function requirements (what the function does) and

-safety integrity requirements (the likelihood of a safety function being performed satisfactorily).

These two requirements are called functional safety requirements specification.

- Any system, implemented in any technology, which carries out safety functions is a safety-related system. IEC 61508 is concerned with functional safety, achieved by safety-related systems that are primarily implemented in electrical and/or electronic and/or programmable electronic (E/E/PE) technologies, i.e. E/E/PE safety-related systems.

- In order to ensure that safety is achieved, both hazard analysis and risk assessment are necessary.

Safety Integrity Levels

- IEC 61508 specifies 4 levels of safety performance for a safety function. These are called safety integrity levels.
- Safety integrity level (SIL1) is the lowest level of safety integrity and SIL4 is the highest level.

Example of functional safety

- Consider a machine with a rotating blade that is protected by a hinged solid cover. The blade is accessed for routine cleaning by lifting the cover. The cover is interlocked so that whenever it is lifted an electrical circuit de-energieses the motor and applies a brake.

- Hazard analysis:

It should not be possible to lift the hinged cover more than 5 mm without the brake activating and stopping the blade.

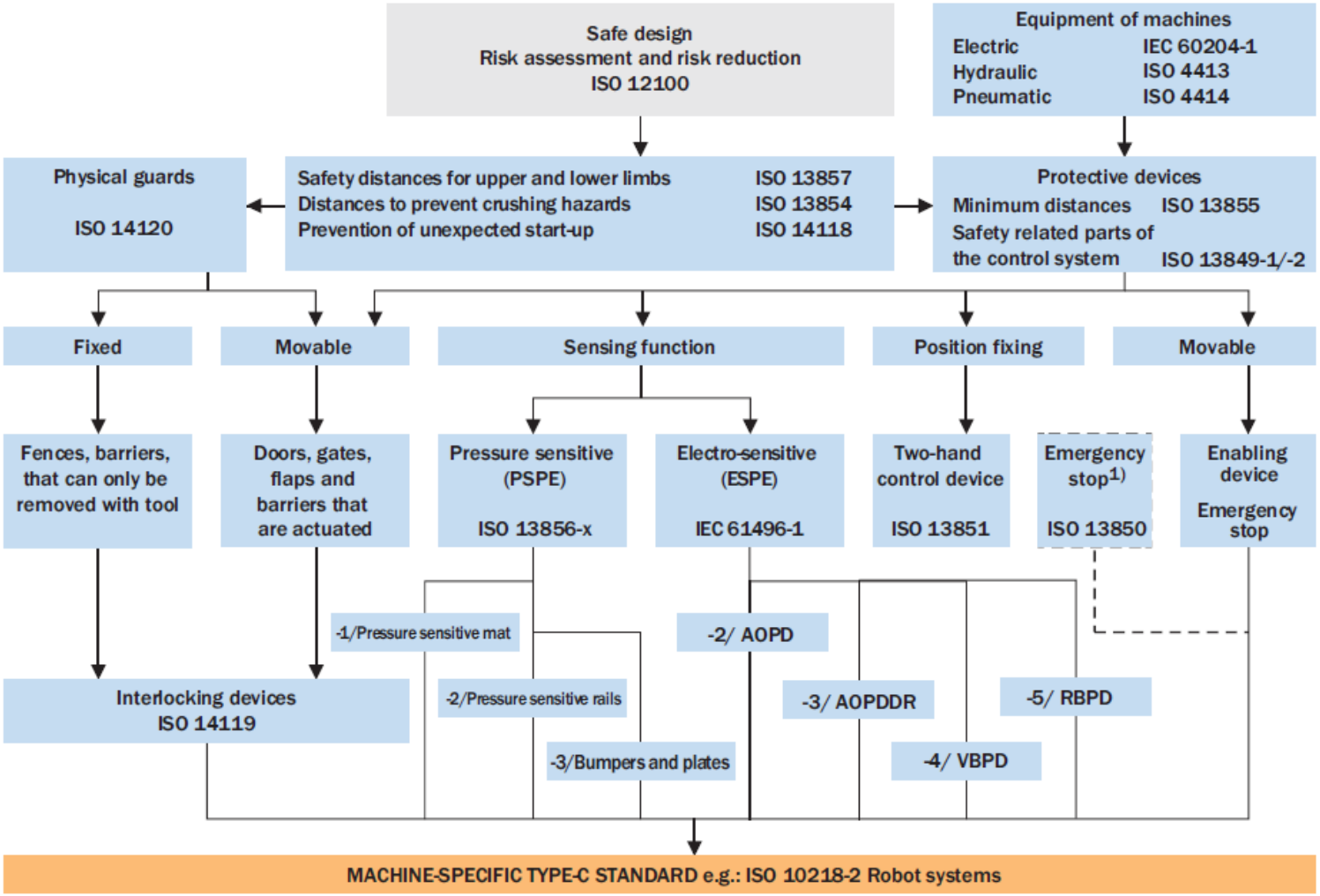
The time for the blade to stop shall be 1s or less.

- Risk assessment:

The safety integrity level of this safety function shall be SIL2.

- The safety-related system of this system includes the guard interlock switch, the eletricial circuit, contactors, the motor and the brake.

Overview of protective devices, physical guards and associated standards



1) Emergency stop is a safety measure but it is not a protective device!
AOPD Active optoelectronic protective device
AOPDDR Active optoelectronic protective device responsive to diffuse reflection
VBPD Vision based protective device
RBPD Radar based protective device

Type-A standard
Type-B standard
Type-C standard

Risk and Risk Criteria

Risk

- Risk: combination of the probability of occurrence of harm and the severity of that harm.

Harm: physical injury or damage to the health of people or damage to property or the environment.

- Risk receptors:

-personnel

-Environment

-Financial

-Equipment/Property Damage

-Business Interruption

-Business Liability

-Company Image

-Lost Market Share

Risk Categories

- Individual risk

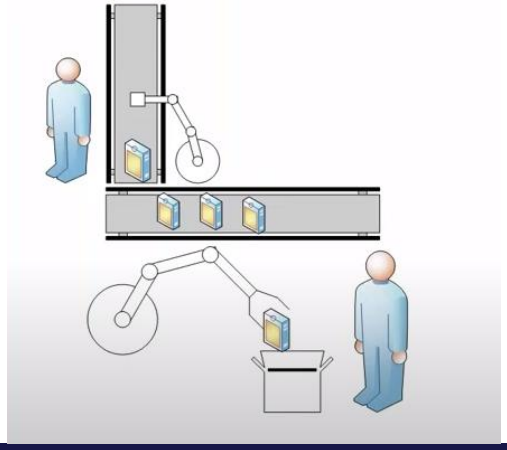
This is the risk, usually of an immediate consequence, to individual members of the general public from an untoward event. Such a risk is both person-and location-specific and can be defined as:

Risk=(frequency of event) × (casualty probability) × (fractional exposure)

The casualty probability is the probability of the untoward event causing a fatality

The fractional exposure is the fraction of time for which a person is likely to be present at the location in question.

Fatal accident rate (FAR)



Risk Categories

- Societal risk

This arises where multiple fatalities are likely to arise from single event. Such events are called societal because they are likely to provoke a socio-political response with long-term detriment including, for example, contamination of the environment.

F/N curve: the frequency of events F causing N deaths

Risk reduction

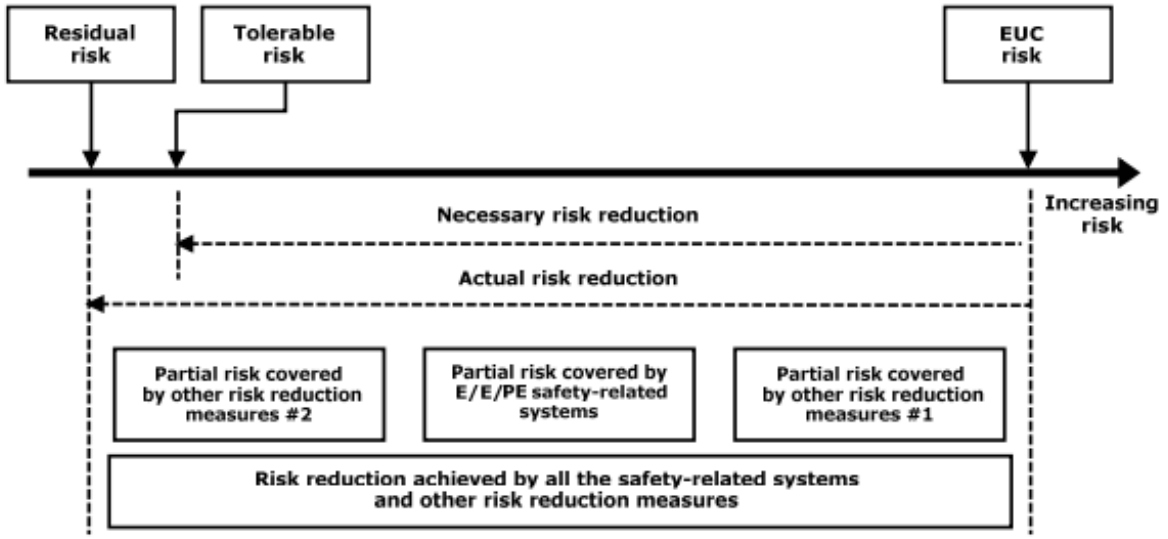
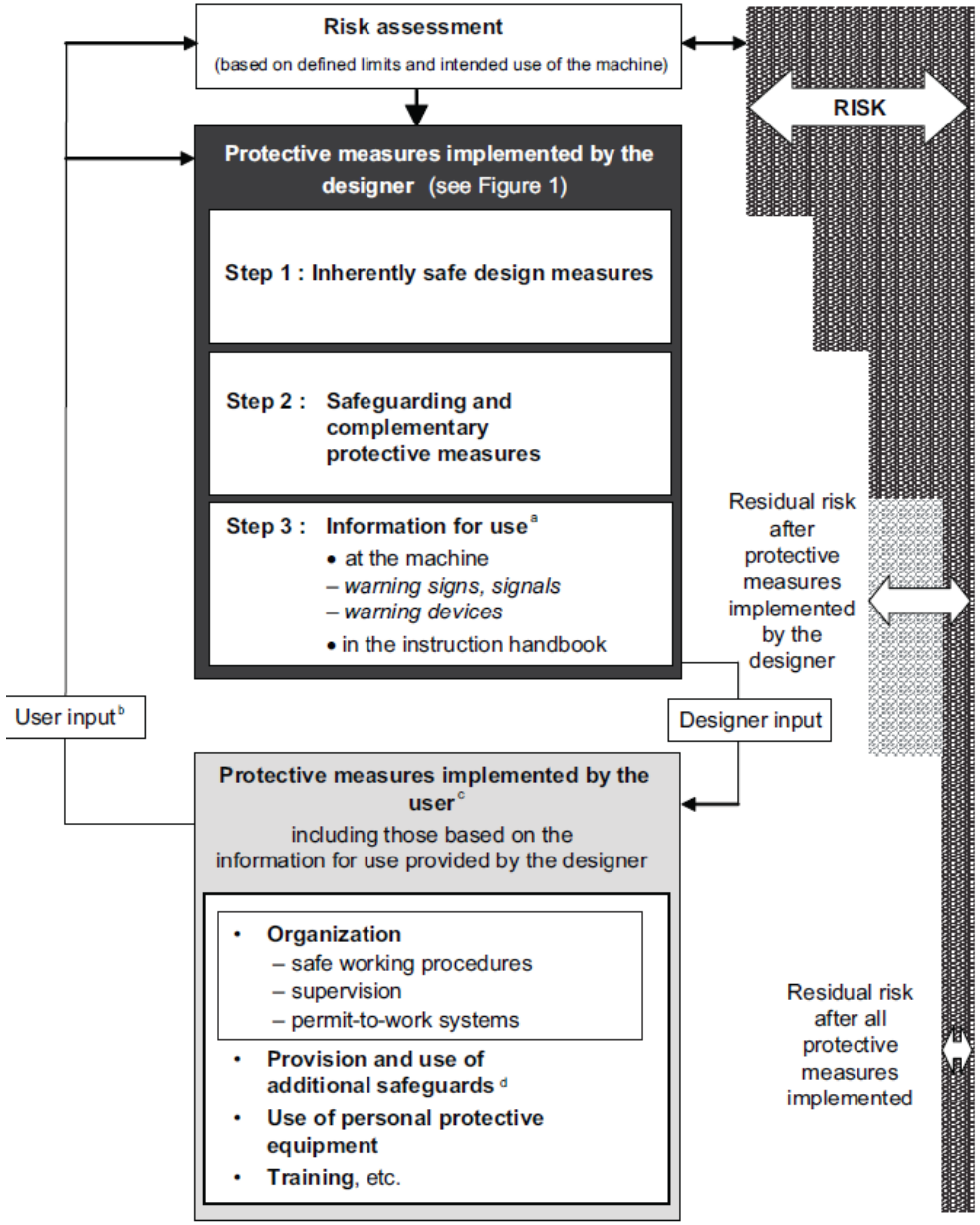


Figure A.1 – Risk reduction – general concepts (low demand mode of operation)

Source: IEC 61508-5

- **EUC(Equipment Under Control) risk**: the risk exisiting for the specified hazardous events for the EUC, the EUC control system and associated human factor issues: no designated safety protective features are considered in the determination of this risk
- **Tolerable risk**: the risk which is accepted in a given context based on the current values of society.
- **Residual risk**: remaining for the specified hazardous events for the EUC, the EUC control system, human factor issues but the addition of, E/E/PE safety-related systems and other risk reduction measures.



[a] Providing proper information for use is part of the designer's contribution to risk reduction, but the protective measures concerned are only effective when implemented by the user.

[b] The user input is that information received by the designer from either the user community, regarding the intended use of the machine in general, or from a specific user.

[c] There is no hierarchy between the various protective measures implemented by the user. These protective measures are outside the scope of this International Standard.

[d] These are protective measures required due to a specific process or processes not envisaged in the intended use of the machine or to specific conditions for installation that cannot be controlled by the designer.

Figure 2 — Risk reduction process from point of view of designer

ALARP

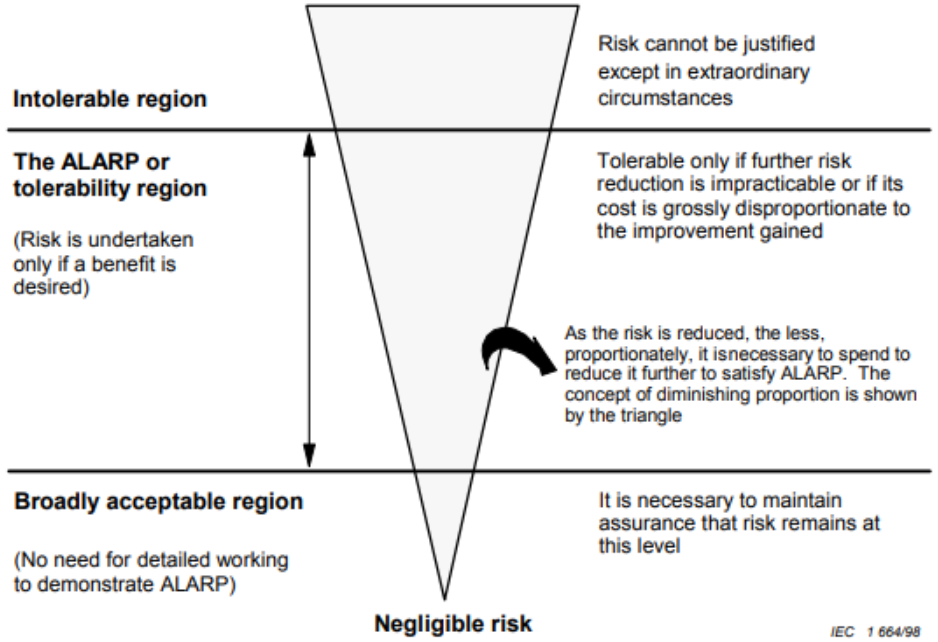


Figure C.1 – Tolerable risk and ALARP

Table C.1 – Example of risk classification of accidents

Frequency	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

NOTE 1 The actual population with risk classes I, II, III and IV will be sector dependent and will also depend upon what the actual frequencies are for frequent, probable, etc. Therefore, this table should be seen as an example of how such a table could be populated, rather than as a specification for future use.

NOTE 2 Determination of the safety integrity level from the frequencies in this table is outlined in Annex D.

Table C.2 – Interpretation of risk classes

Risk class	Interpretation
Class I	Intolerable risk
Class II	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
Class III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
Class IV	Negligible risk

Barrier theories

Agenda

- Barriers
- Perspectives on barriers
- Mechanisms of barriers

- How barriers can fail

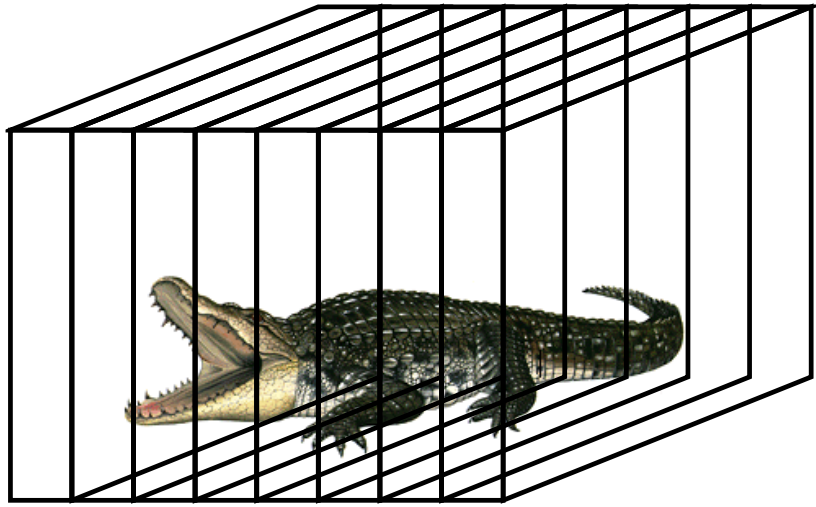
- Barriers in relation to robotics

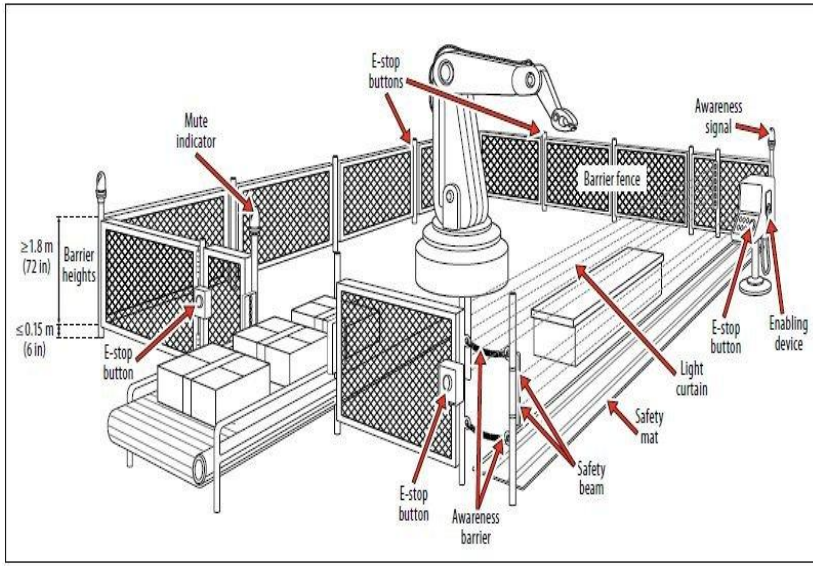
Barrier

- Barrier: Technical, operational and organisational elements which are intended individually or collectively to reduce possibility/ for a specific error, hazard or accident to occur, or which limit its harm/disadvantages.
- -quoted from *Principles for barrier management in the petroleum industry*

- Similar terms could be safety barriers, safeguard, layer of protection, defenses, defense-in-depth, risk reducing measures in different industries and applications.

- By searching the exact term of “safety barrier” as the keyword within paper topics, 28381 articles can be found (by December 7th, 2021) on the web of science, 23527 of which (82.9%) were published since 2010. It indicates increasing research interests in recent 10 years.





Perspectives on barriers

- Energy perspective: Gibson (1961) pioneered the development of the energy model, while Haddon (1980) developed the model further as he presented his ten strategies for accident prevention.

Energy Source	Barrier	Vulnerable Target
• Prevent build-up of energy • Reduce the amount of energy • Prevent uncontrolled release of energy • Modify rate or distribution of the released energy • Modify the qualities of the energy	• Separate in space and time, the victims from the energy being released • Separate the victims from the energy by physical barriers	• Make the vulnerable target more resistant to damage from the energy flow • Limit the development of damage • Rehabilitate the victims

Haddons 10 accident prevention strategies Haddon (1970, 1980)

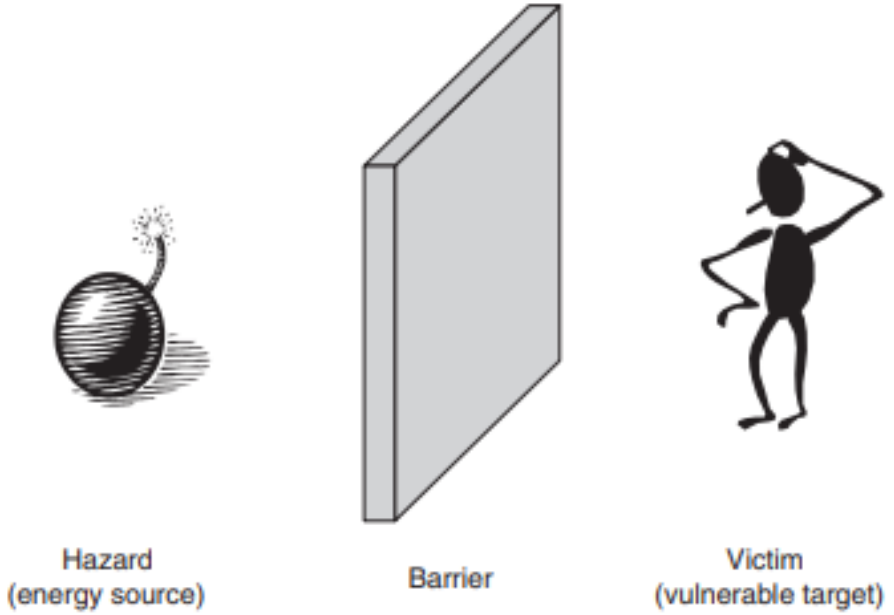


Fig. 1. The energy model (based on Haddon, 1980).

Example: Energy Barrier Analysis (EBA)

1. Sources of Potential Unwanted Energy (PUE) in: a. robot subsystems and overall system b. robot environment.
2. Means of reducing and controlling the levels of PUE from the source.
3. Means of blocking or controlling the transfer of PUE.
4. Means of properly warning the operator of the existence of PUE flow.

- RAHIMI, M. (1986). SYSTEMS SAFETY FOR ROBOTS - AN ENERGY BARRIER ANALYSIS. Journal of Occupational Accidents, 8(1-2), 127–138. https://doi.org/10.1016/0376-6349(86)90035-0

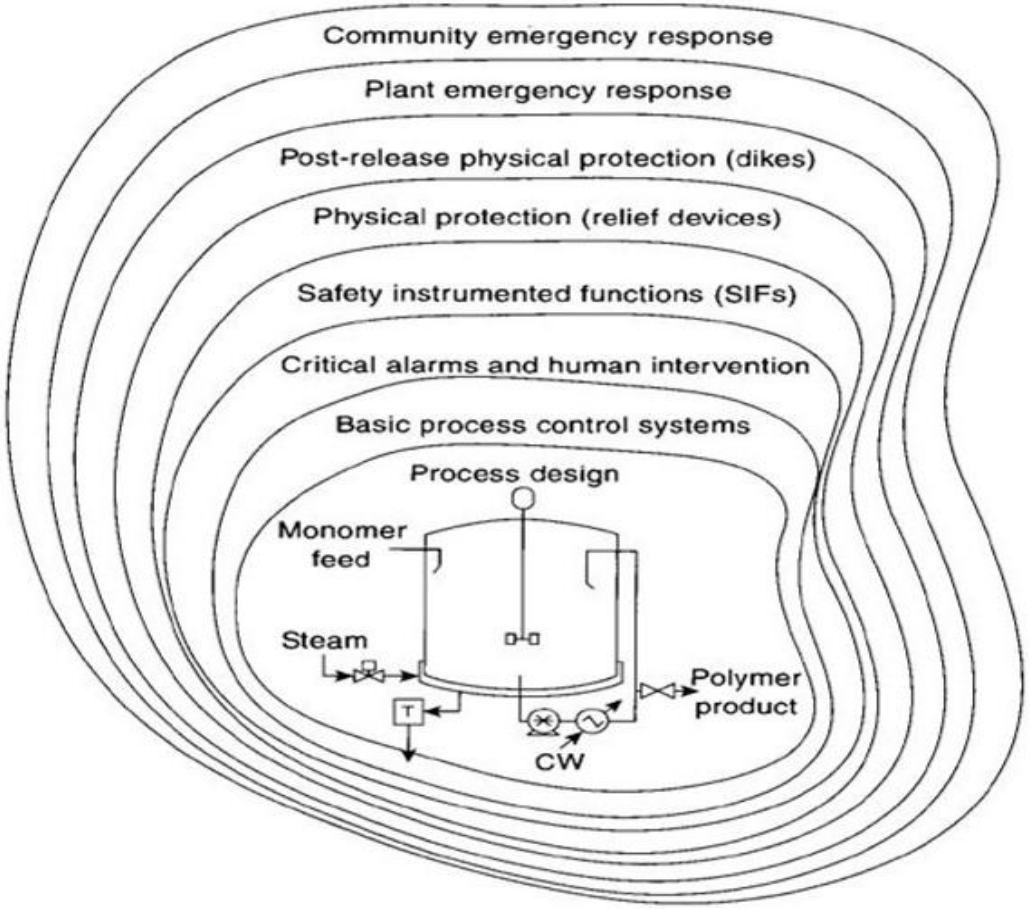
Perspectives on barriers

- Multiple lines of defence: defence-in-depth combines different types of barriers—from protection against the release of radioactive materials to event reporting and safety policies, the same principle applies to layer of protection.

Levels of Defense in Depth (IAEA, INSAG 10)

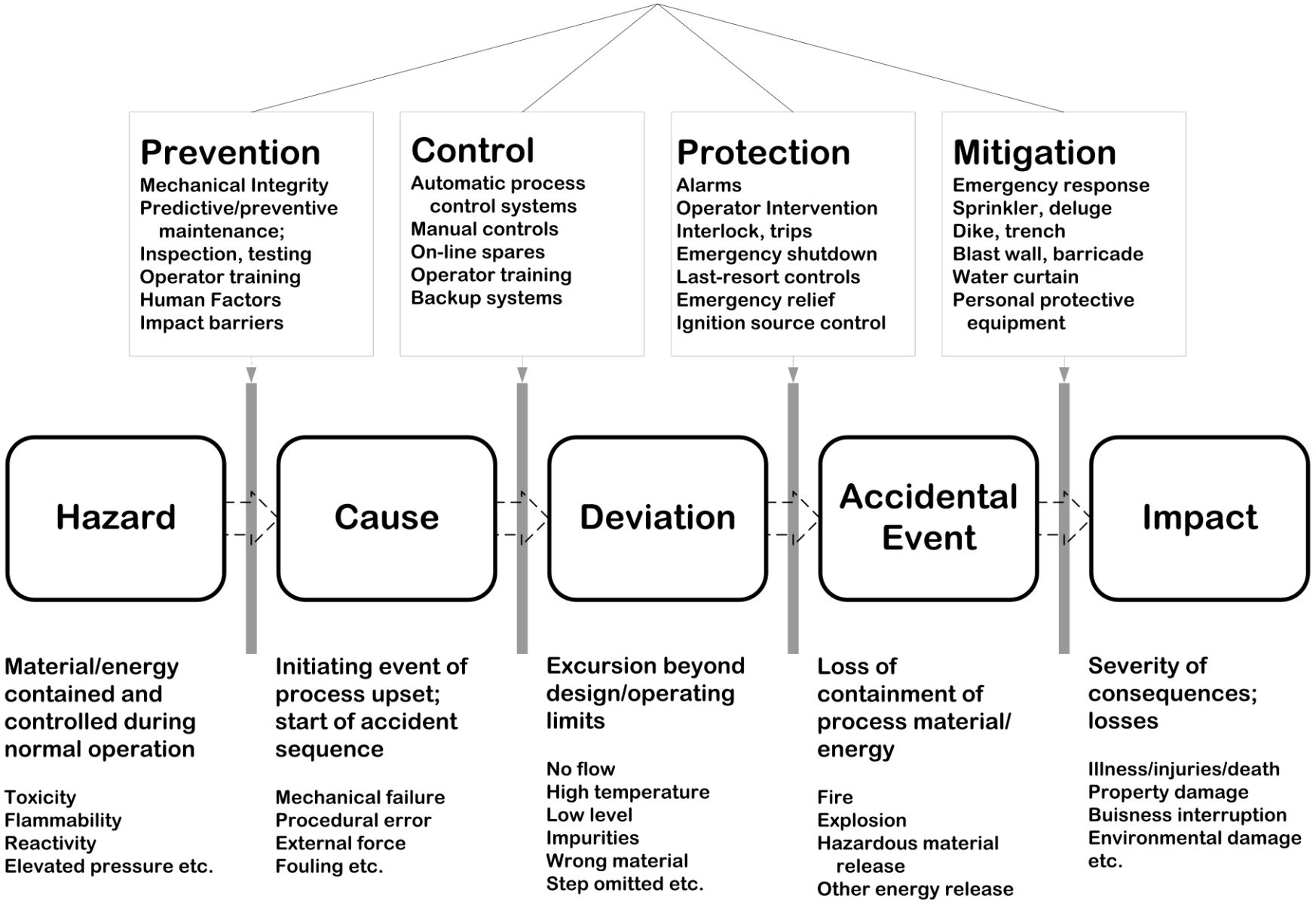
Levels of defense in depth	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high qualilty in construction and operatrion
Level 2	Control of abnormal operation and detection of failures	Control. Limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, icluding prevention of accident progression and mitigation of the consequences of severe accidents	Complementary emasures and accident management
Level 5	Mitigation of radiological consequqnces of significant releases of radioactive materials	Offsite emergency response

Layer of Protection



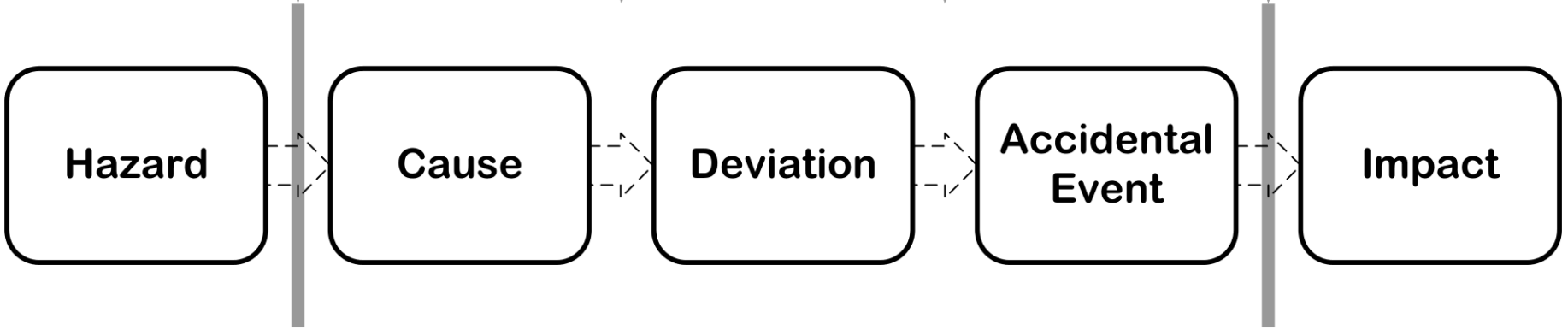
Center for Chemical Process Safety. (2015). Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis.

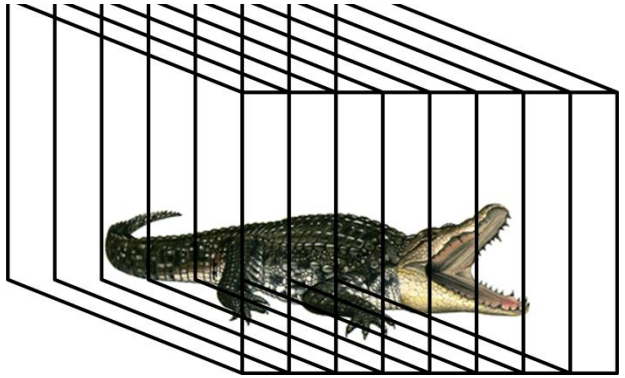
Levels of Defence

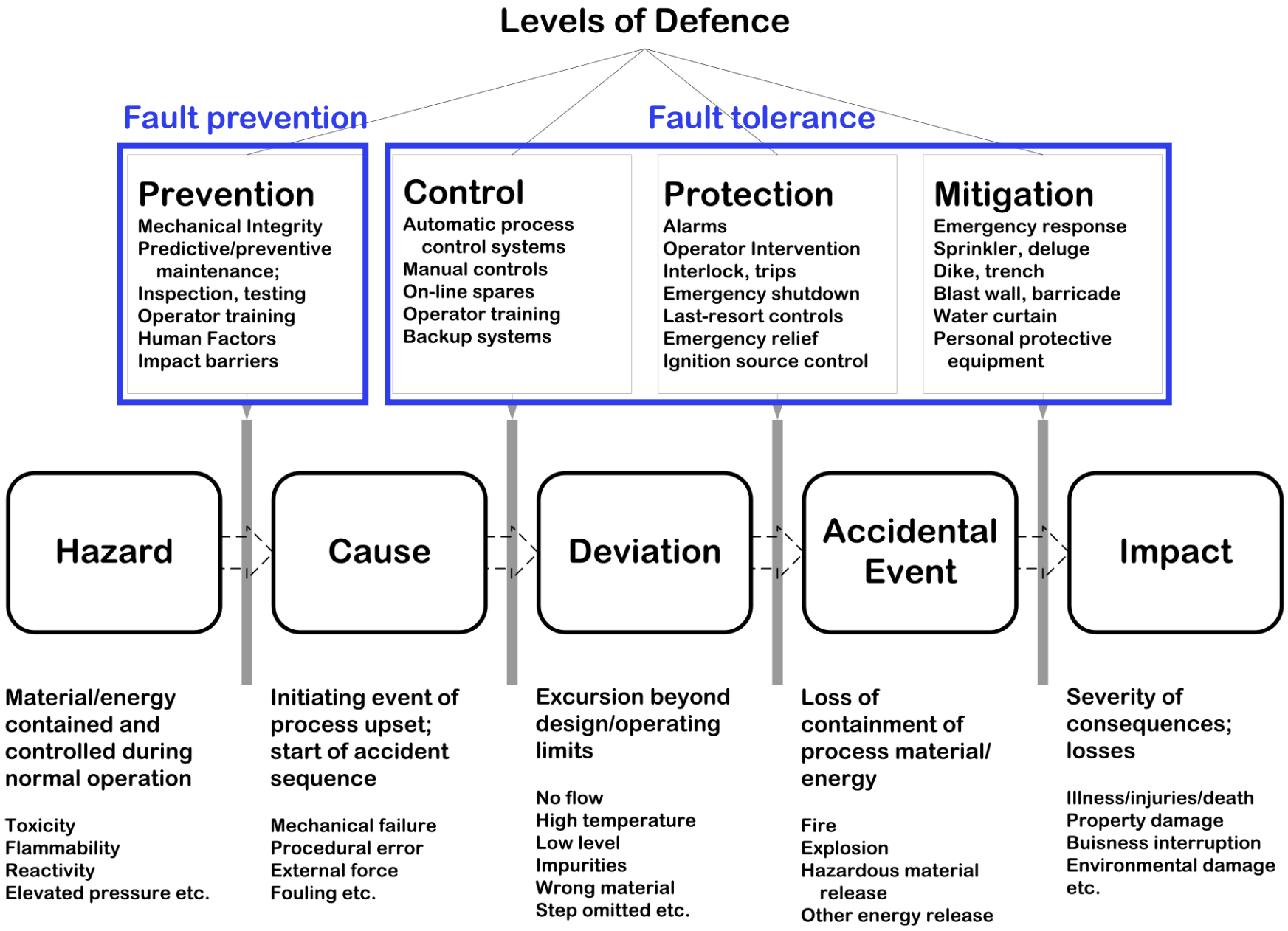


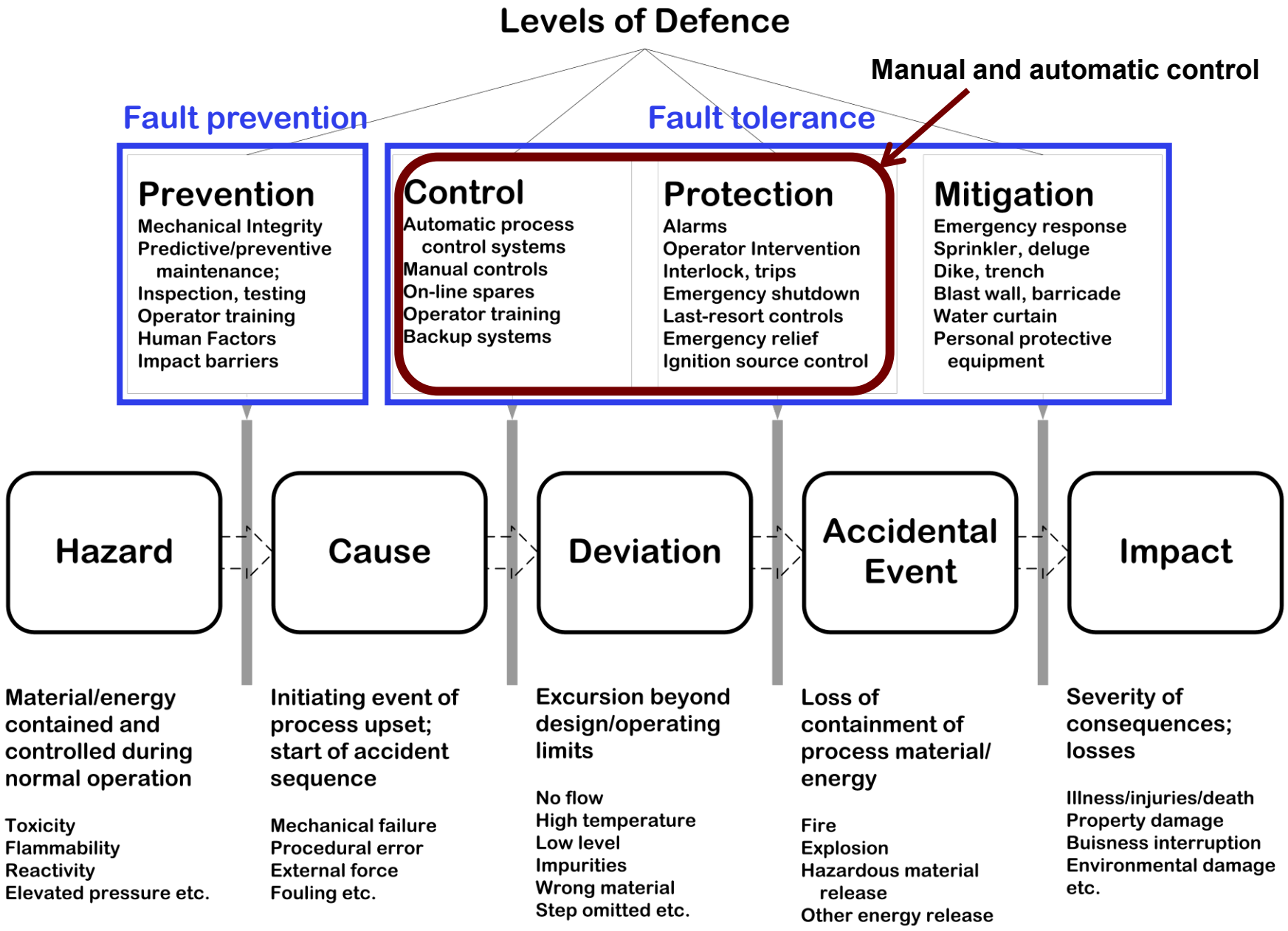
Prevention
Mechanical Integrity
Predictive/preventive maintenance;
Inspection, testing
Impact barrier

Mitigation
Personal protective equipment





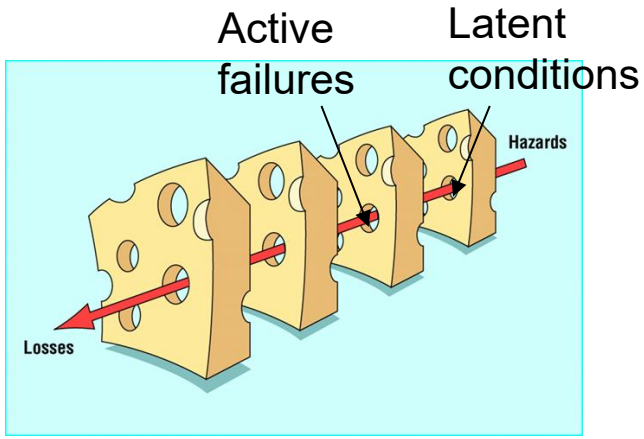

Levels of Defence
Fault prevention
Fault tolerance
Prevention
Mechanical Integrity
Predictive/preventive maintenance;
Inspection, testing
Operator training
Human Factors
Impact barriers
Control
Automatic process control systems
Manual controls
On-line spares
Operator training
Backup systems
Protection
Alarms
Operator Intervention
Interlock, trips
Emergency shutdown
Last-resort controls
Emergency relief
Ignition source control
Mitigation
Emergency response
Sprinkler, deluge
Dike, trench
Blast wall, barricade
Water curtain
Personal protective equipment
Hazard
Cause
Deviation
Accidental Event
Impact
Material/energy contained and controlled during normal operation
Toxicity
Flammability
Reactivity
Elevated pressure etc.
Initiating event of process upset; start of accident sequence
Mechanical failure
Procedural error
External force
Fouling etc.
Excursion beyond design/operating limits
No flow
High temperature
Low level
Impurities
Wrong material
Step omitted etc.
Loss of containment of process material/ energy
Fire
Explosion
Hazardous material release
Other energy release
Severity of consequences; losses
Illness/injuries/death
Property damage
Buisness interruption
Environmental damage
etc.


Levels of Defence
Manual and automatic control
Fault prevention
Fault tolerance
Prevention
Mechanical Integrity
Predictive/preventive maintenance;
Inspection, testing
Operator training
Human Factors
Impact barriers
Control
Automatic process control systems
Manual controls
On-line spares
Operator training
Backup systems
Protection
Alarms
Operator Intervention
Interlock, trips
Emergency shutdown
Last-resort controls
Emergency relief
Ignition source control
Mitigation
Emergency response
Sprinkler, deluge
Dike, trench
Blast wall, barricade
Water curtain
Personal protective equipment
Hazard
Cause
Deviation
Accidental Event
Impact
Material/energy contained and controlled during normal operation
Toxicity
Flammability
Reactivity
Elevated pressure etc.
Initiating event of process upset; start of accident sequence
Mechanical failure
Procedural error
External force
Fouling etc.
Excursion beyond design/operating limits
No flow
High temperature
Low level
Impurities
Wrong material
Step omitted etc.
Loss of containment of process material/ energy
Fire
Explosion
Hazardous material release
Other energy release
Severity of consequences; losses
Illness/injuries/death
Property damage
Buisness interruption
Environmental damage
etc.

Applying the design principles for safety on process automation

	Process	Automation	Human Operators and organisation
Fault Prevention	Errors in process components are prevented by design	Errors in automation components are prevented by design	Human Errors are prevented by operator training
Fault Tolerance	Process errors are compensated by redundancy (parallel pumps and pipes etc.)	Errors in automation elements are compensated by redundancy (e.g. parallel computers)	Human errors are compensated by redundancy in the organization

How barriers can fail



- *Active failures* are the unsafe acts committed by people who are in direct contact with the patient or system
- *Latent conditions* are the inevitable “resident pathogens” within the system. They arise from decisions made by designers, builders, procedure writers, and top level management.

Barriers in relation to robotics

- Barrier analysis in relation to robotics was traced back to 1986. Numerous safety devices are designed and adapted to produce safer operation of industrial robots.

- What are typical safeguards for robot systems?

https://www.youtube.com/watch?v=GtNKX4kpC18

- However, a few preliminary robot accident data analyses indicate that the traditional machine safety solutions such as fences, enclosures, and/or guards do not seem to be effective methods of preventing robot accidents.

-quoted from *System safety for robots: an energy barrier analysis*

Reasons:

➢ Robot accidents may occur during the periods of teaching, testing, or maintenance of robots. During such phases of operation, the workers have already disabled the traditional safety devices in order to enter into the robot work envelope.

➢ New hazards raised by cobots, the work envelop is dynamic changing.

Barriers in relation to robotics

- Therefore, robot functional safety is increasingly demanding, and new standards are in place to guide and regulate safety systems design and integration.

End-of-Arm-Safeguard (EOAS)

Certifications and standards:

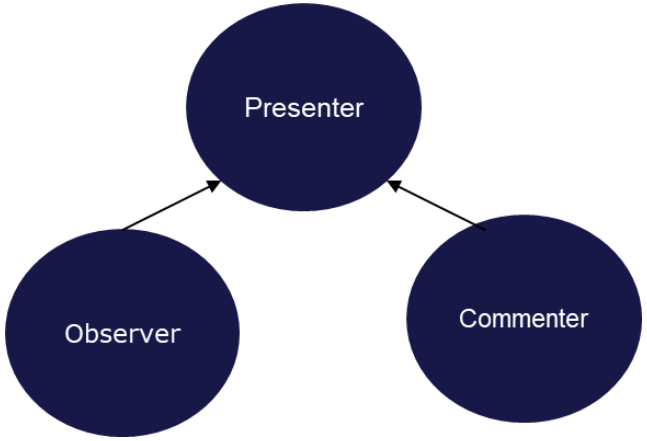
- Cat. 2, PL c device according to ISO 13849-1
- To be used in combination with a safe UR cobot (e-series) – power and force limited robot, PL d device according to ISO 10218

Sick Safety: sBot Speed Package

Certifications and standards:

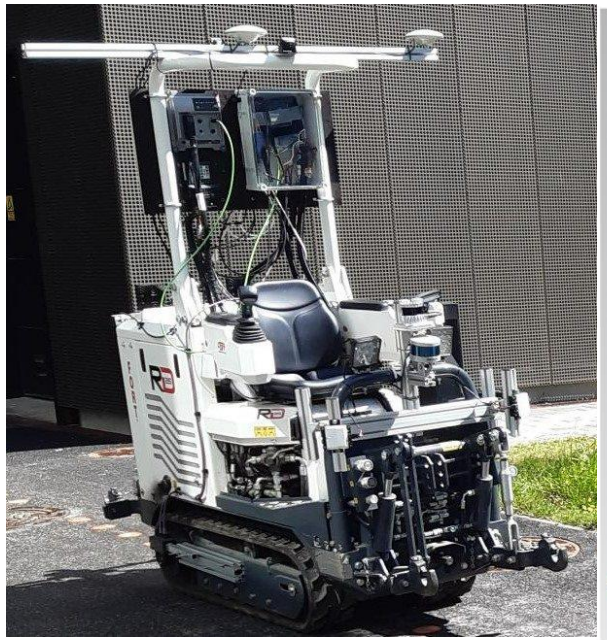
- IEC 61508: 2010, EN 62061: 2005 + AC2010,2013,2015, EN ISO 13849-1, ISO 10218-2, IP65 (IEC 60529)

Grouping

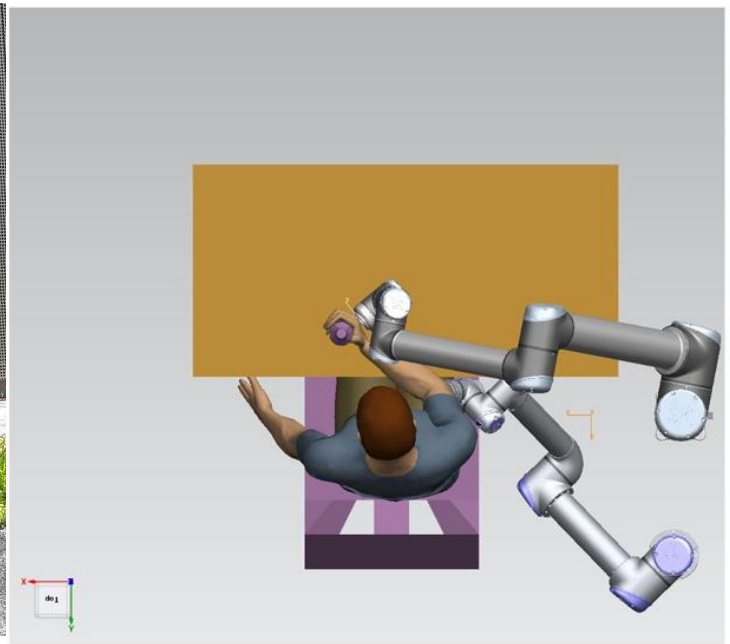


Each group is composed of 4 persons. Each group selects one robot.

MiR 500
(Manufacturing)



Fort RD 25
(Agriculture)



Reharob 3.0
(Healthcare)

Pick and place
(Slaughter house)

Exercise

Each group answers the following 3 questions in 8-10 minutes presentation :

- What EU regulations and directives do you identify for the robot?
- What standards do you identify for the robot, and why do you think they are relevant for the robot?
- Identify hazards for the robot and use standards from Groups A, B, and C under machinery regulation (choose at least one standard from each group) to illustrate how the standards can help with reduce risks associated with the identified hazard.

PRESENTER ROLE

Each group must clearly answer all three questions. Presentation Structure (8–10 minutes)

OBSERVER ROLE

- Observers **listen, evaluate, and prepare feedback**.
- **During the Presentation**
- Observers should check and take notes on:
- ☐ Are **all 3 questions** answered?
  ☐ Are EU directives **relevant and justified**?
  ☐ Are standards **clearly explained**, not just listed?
  ☐ Is at least **one hazard** clearly identified?
  ☐ Are **Group A, B, and C standards** used?
  ☐ Is the link between **hazard and risk reduction** clear?
- **After the Presentation**
- Observers prepare:
- **One strength** of the presentation
- **One unclear or missing point**
- **One improvement suggestion**
- 📌 Observers do **not** ask questions.

COMMENTER ROLE

Commenters **engage actively** with the presenters.

After the Presentation

Commenters must:

- Ask **1–2 focused questions**
- Add **one constructive comment**
- ⚠️ Be respectful, concise, and technical.