# Chapter 1

# Introduction

This document is basically a summary of chapter 1 in the textbook *Reliability of Safety-Critical Systems* by Marvin Rausand.

## 1.1 Safety-critical systems

Safety-critical systems are used in many products and application areas. The safety-critical systems that are considered in this book are technical systems and may, or may not, involve human operator actions. The scope is delimited to systems that are designed to perform one or more safety functions. A safety function is usually implemented to protect against a specific undesired event that can cause harm. The system that is protected by the safety-critical system is called equipment under control (EUC).

Examples of safety-critical systems that may be assessed by the models and methods described in this course include:

- Cars (e.g., airbag systems, brakes, steering, electronic stability program (ESP) systems)
- Process industry (e.g., emergency shutdown (ESD) systems, fire and gas systems, gas burner management systems)
- Railway transport (e.g., signalling systems, automatic train stop (ATS) systems)

Examples of equipments under control are:

- Persons (protected by the airbag in a car)
- Pipeline (protected by the HIPPS, i.e., HIgh Pressure Protection System)
- Train (protected by the ATS, i.e., Automatic Train Stop)

A safety function that is performed by a safety-critical system may be categorized as follows:

- *Safety control function.* A safety function that is a normal part of the operation of the EUC and/or integrated into the EUC control system (e.g., a railway signalling system, the braking system of a car).
- *Safety protective function.* A dedicated safety function that is separate from the EUC control system and is only activated when the safety function is demanded (e.g., the ESD system in a process plant, the airbag system in a car)

Many safety-critical systems are based on electrical, electronic, or programmable electronic (E/E/PE) technology. In this course we mainly consider safety-critical systems where E/E/PE technology plays an important role, often together with mechanical or other technology items. The important standard IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems **?** designates these systems by the term E/E/PE safety-related systems. In the process industry such systems are usually denoted safety-instrumented system (SIS).

Consider the process system in Figure 1.1. The process vessel in red is the equipment which should be kept under control, i.e., the EUC. Several safety and other control functions are implemented to make sure that the EUC is kept in a safe state.

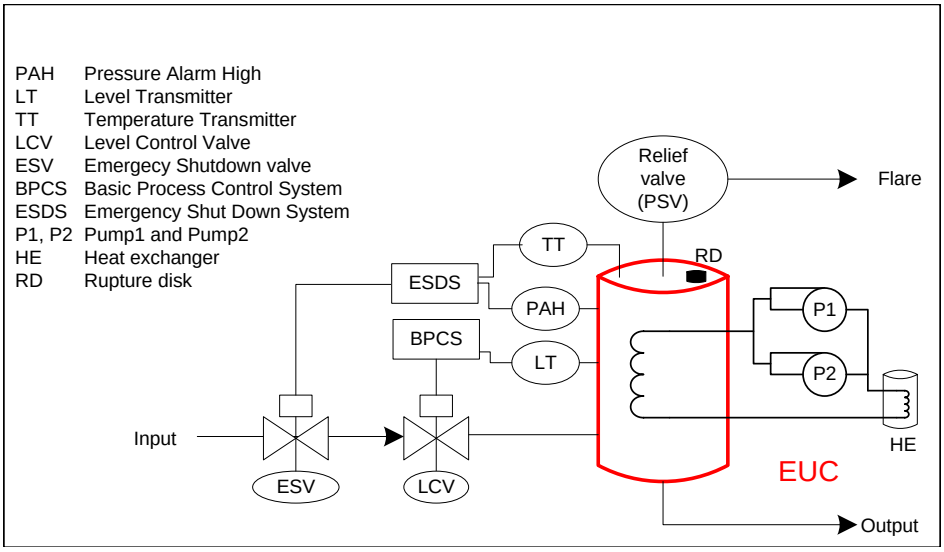


Figure 1.1: Equipment under control - Process system

## 1.2 Risk and risk management

Generally, risk management is defined (IEC 60300-3-9) as a "systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk". It will comprise (IEC definitions in parentheses):

- Risk assessment, that is:
  - Risk analysis ("Systematic use of available information to identify hazards and to estimate the risk to individuals or populations, property or the environment"), and
  - Risk evaluation ("Process in which judgements are made on the tolerability of the risk on the basis of risk analysis and taking into account factors such as socio-economic and environmental aspects")
- Risk reduction/control (Decision making, implementation and risk monitoring).

There exists no common definition of risk, but for instance IEC 60300-3-9 **?** defines risk as a "combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous events". Most definitions comprise the elements of probabilities and consequences. However, some as Klinke and Renn (2001) **?** suggest a very wide definition, stating: "Risk refers to the possibility that human actions or events lead to consequences that affect aspects of what humans value". So the total risk comprises the possibility of a number ("all") unwanted/hazardous events. It is part of the risk analysis to delimit which hazards to include.

A definition of risk that is appropriate for inclusion in risk analysis is to define risk as the combined answer to the following three questions:

- What can go wrong?
- Will it go wrong?
- And if so, what are the consequences?

These questions are motived by the famous article by Kaplan and Garrick **?**. Further, risk usually refers to threats in the future, involving a (high) degree of uncertainty. Therefore, risk is the combined answer of the above questions with corresponding uncertainties.

To make an operational definition of risk three elements are introduced: $< e, p, \mathbf{S} >$. $p$ is used as a uncertainty/probability measure of the occurrence of an event, say $e$. $\mathbf{S}$ represents the severity of the event. Note that $\mathbf{S}$ is a multidimensional random quantity, covering several dimensions like personnel safety, environmental impacts, material damages, project delays, extra costs, etc. Since there is more than one event to treat, $i$ is used as an index to run through all relevant events. An operational definition of risk is thus the set of all relevant triplets:

$$R = \left\{< e_i, p_i, \mathbf{S}_i >\right\} \tag{1.1}$$

## 1.3 Bow-tie diagram

The so-called bow-tie diagram is often used to illustrate causes leading up to what can go wrong, i.e., the Hazardous event, and what would be the consequences. Figure 1.2 illustrates this where also both preventive and mitigating barriers are illustrated.

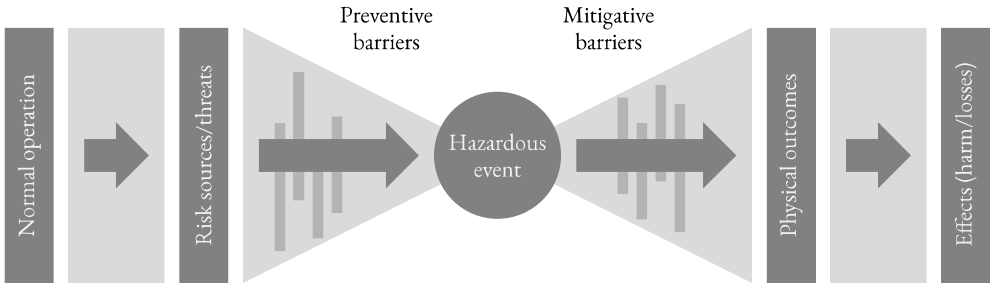


Figure 1.2: Bow-tie diagram illustrating consequences as chains of events (van der Meulen and Myhrvold, 2022)

In Figure 1.2 the "knot" is referred to as the "hazardous event", whereas the term "undesired" event is also frequently used to denote the "knot" in the bow-tie.

In risk analyses often fault tree analysis (FTA) is used to structure causes leading to the hazardous event, and event tree analysis (ETA) is used to structure what is happening after the hazardous event eventually occurs. Further the safety barriers in the bow-tie diagram is often analysed with FTA or reliability block diagram (RBD) analysis. In some cases also Markov analysis is used to analyse the safety barriers.

## 1.4 Safety barriers

Safety barrier is a common term in most risk analyses and is partly overlapping with our definition of a safety-critical system. A safety barrier system may be a technical system or some dedicated human and organizational effort. Safety barrier is therefore not the same concept as safety-critical system.

Safety barrier systems are also called defences, safeguards, countermeasures, or protection layers. A safety barrier system may perform one or more safety barrier functions and may usually be split into several safety barrier subsystems and elements.

## 1.5 Classification of Safety Barriers

Safety barriers may be classified according to whether they are active or passive, technical or human/organizational, how often they are demanded, and so on. We introduce briefly some of

these classifications.

### 1.5.1 Proactive Versus Reactive Safety Barriers

Proactive and reactive safety barriers are illustrated in the bow-tie diagram in Figure 1.1.

- *Proactive safety barrier.* A safety barrier that is installed to prevent one or more undesired events in the EUC from occurring. A proactive safety barrier is also called a frequency-reducing barrier because it should reduce the frequency of the undesired event(s). Proactive safety barriers are often referred to as preventive barriers as illustrated in Figure 1.2.
- *Reactive safety barrier.* A safety barrier that is installed to remove or mitigate the consequences of one or more undesired events in the EUC (if they should happen). A reactive safety barrier is also called a consequence-reducing barrier or a mitigating barrier.

### 1.5.2 Passive Versus Active Safety Barriers

Safety barriers may also be categorized as passive or active safety barriers:

- *Passive safety barrier.* A barrier whose safety function is always available as an inherent property of the EUC or workplace. Examples of passive safety barriers are fire walls, means for physical separation (e.g., fences, shields), housing used to protect equipment from gas or water intrusion, and so on.
- *Active safety barrier.* The safety function of an active safety barrier is not always available, but will be performed in response to certain events. An ESD system in a process plant is an active safety barrier and is only activated when a dangerous situation occurs.

### 1.5.3 Technical Versus Human/Organizational Safety Barriers

Safety barriers may also be classified according to their nature:

- *Technical safety barriers.* A technical safety barrier is a safety barrier where the bar-rier function is performed by a technical system. Technical safety barriers may partly be based on E/E/PE technology.
- *Human and organizational safety barriers.* A human barrier is a safety barrier where the barrier function is carried out by one or more persons, sometimes by using technical safety barrier elements. The term organizational safety barrier is used

### 1.5.4 Mode of Operation

Safety barriers may be categorized according to how often the barrier functions are demanded. We distinguish between

- *Demanded mode.* These safety barrier functions do not take active part in the control of the EUC and are only activated when a dangerous situation (i.e., a demand, undesired event) occurs. We often distinguish between
  - *Low-demand mode.* A safety barrier is said to operate in low-demand mode when its function is demanded no more often than once per year. The airbag system in an automobile is an example of a safety barrier operating in low-demand mode.
  - *High-demand mode.* A safety barrier is said to operate in high-demand mode when it is exposed to distinct demands that occur more often than once per year. A presence-sensing safeguarding device for a moving robot is (usually) an example of a safety barrier operating in high-demand mode.
- *Continuous mode.* A safety barrier is said to operate in continuous mode when its function is always crucial. In this case, the safety barrier is integrated with the EUC control system, and an undesired event will occur when the safety barrier fails. Examples of safety barriers operating in continuous mode are (i) fly-by-wire systems for flight control of aircrafts and (ii) dynamic positioning systems (DPS) for ships and offshore platforms.

## 1.6 Layers of Protection

In the process industry, safety barriers are often called layers of protection or protection layers and are sometimes visualized as in Figure 1.4, where the layers are drawn in the sequence they are activated.

Following this sequence, it is distinguished between:

a) Process design (by using inherently safe design principles).

b) Control, using basic control functions, alarms, and operator responses to keep the system in normal (steady) state.

c) Prevention, using safety-instrumented systems (SISs) and safety critical alarms to act upon deviations from normal state and thereby prevent an undesired event from occurring.

d) Mitigation, using SISs or functions implemented by other technologies, to mit-igate the consequences of the undesired event. Examples include the protection that is provided by pressure relief valves.

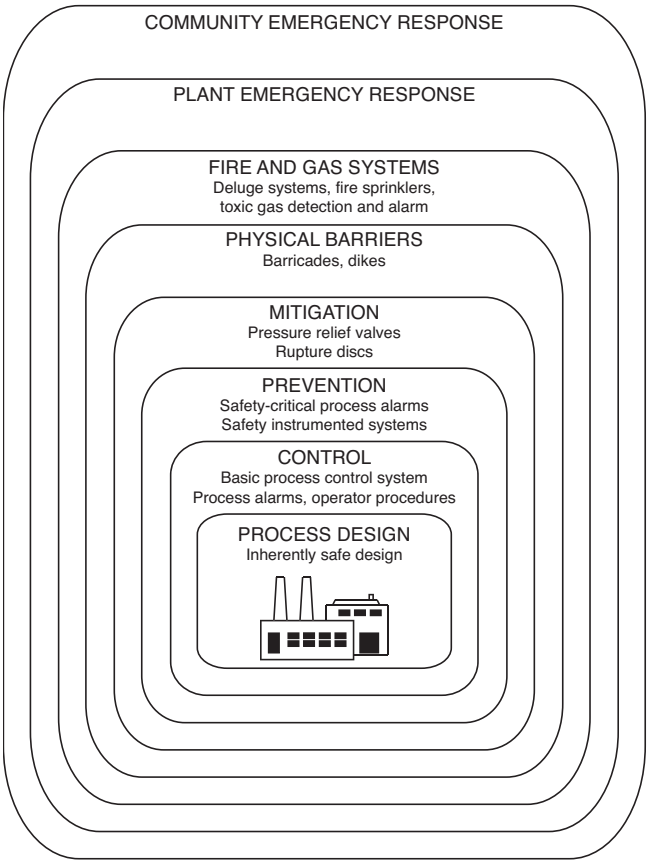


Figure 1.3: Protection layers for process plants (van der Meulen and Myhrvold, 2022; Rausand, 2014)

e) Physical protection, using permanent (and more robust) safety barriers to enhance the mitigation. Examples include the protection that is achieved by having dikes and barricades in place.

f) Fire and gas detection and distinguishing, as a third strategy to mitigate the con-sequences by avoiding ignition, and thereby an accident, in relation to explosive gases and mixtures.

g) Emergency response, using various means to limit the severity of the accident, locally as well as in the community. Examples include rescue procedures, mobilization of rescue teams, and use of emergency exits.

## 1.7 Safety Performance Criteria

A simplified demanded SIS or technical safety barrier is illustrated in Figure 1.3. The safety barrier is installed in an EUC to reduce the risk related to a specific type of demands that occurs with frequency $\lambda_{\text{de}}$. The objective of the safety barrier is to stop the demands or to reduce the

frequency or consequences of the demands. In most cases, the safety barrier is not 100% effective and some demands may pass the safety barrier and have negative effects on the EUC. The frequency of these negative effects is denoted $\lambda_{\text{eff}}$. If the safety barrier were not installed, all the demands would have negative effects. We may therefore use the relative reduction of the demand frequency as a measure of the risk-reduction performance of the safety barrier as

$$\text{Risk Reduction}_1 = \frac{\lambda_{\text{de}} - \lambda_{\text{eff}}}{\lambda_{\text{de}}} \tag{1.2}$$

Reactive safety barriers are installed in the EUC to remove or reduce the consequences of demands. The risk-reduction performance of these safety barriers can be assessed based on the relative reduction of the consequences obtained. Let $C_{\text{wo}}$ and $C_{\text{w}}$ be the assessed consequences of demands without and with the safety barrier, respectively. The risk-reduction obtained is then

$$\text{Risk Reduction}_2 = \frac{C_{\text{wo}} - C_{\text{w}}}{C_{\text{wo}}} \tag{1.3}$$

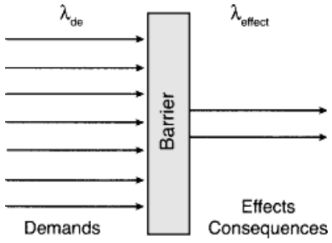


Figure 1.4: The risk-reduction of a safety barrierRausand (2014)

The main performance criteria for an active safety barrier are related to:

- *Functionality/effectiveness.* This criterion concerns how effectively the safety barrier can reduce the risk related to a specific demand, and also the safety barrier's ability to handle different situations and variants of the demand.
- *Reliability/availability.* An active safety barrier can never be completely reliable and available. The reliability and availability are therefore important performance measures.
- *Response time.* To reduce the risk, the safety barrier must often be activated quickly. Sometimes, a maximal response time is specified as part of the functional requirements.
- *Robustness.* The safety barrier must sometimes function in hazardous situations where it is exposed to external stresses. It is therefore important that the safety barrier is robust and not vulnerable to these stresses. This criterion is sometimes referred to as survivability.

## 1.8 Safety Instrumented Systems and Safety Instrumented Functions

A safety instrumented system (SIS) is an independent protection layer that is installed to mitigate the risk associated with the operation of a specified hazardous system, which is referred to as the equipment under control (EUC). An example of an EUC is a process vessel.

A SIS is composed of *sensors* often referred to as *input elements*, *logic solvers* and *actuating items* often referred to as *final elements*.

A safety instrumented function (SIF) is a function that is implemented by a SIS and that is intended to achieve or maintain a safe state for the EUC with respect to a specific process demand such as high pressure in the vessel.

A SIS has two main system functions:

1. When a predefined process demand occurs in the EUC; the deviation shall be detected by the SIS sensors, and the required actuating items shall be activated and fulfil their intended functions.

2. The SIS shall not be activated spuriously, that is, without the presence of a predefined process demand in the EUC.

A *demand* is defined as: An event or a condition that requires a SIF to be activated (i) to prevent an undesired event from occurring or (ii) to mitigate the consequences of an undesired event. In the process industry, a demand is also called a *process upset* or a *process deviation*.

A SIS consists of at least three subsystems:

- *Sensor subsystem* - detects a potential danger and produces an appropriate elec-trical signal that is sent to the logic solver. Examples of sensors are pressure transmitters, level transmitters, temperature gauges, and so on.

- *Logic solver subsystem* - detects the electrical signal exceeding a given threshold and sends a signal to the final elements. Logic solvers can be computers, programmable electronic controllers (PLCs), and relay circuits.

- *Final element subsystem* - performs the safety function. Examples of final ele-ments are shutdown valves, circuit breakers, motors, fans, and so on. The three subsystems must act in concert to detect the deviation (i.e., demand) and bring the EUC into a safe state.

In brief, a SIS shall *detect*, *react*, and *avert*. A sketch of a simple SIS that is used for pressure protection of a pipeline is shown in Figure 1.5. Three pressure transmitters monitor the pressure in the pipeline and send this information to the logic solver subsystem. The logic solver compares the received values with predefined set points and, when high pressure occurs, a signal is sent

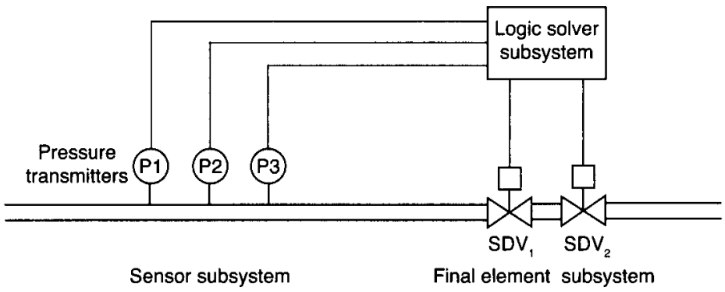


Figure 1.5: Sketch of a simple SIS used as pressure protection system in a pipeline Rausand (2014)

to the two shutdown valves (SDVs) to close the flow in the pipeline. Each subsystem can have one or more channels. The sensor subsystem in Figure 1.5 has three channels (i.e., pressure transmitters) and the final element subsystem has two channels (i.e., shutdown valves).

## 1.9 The Fail-Safe Principle

A SIS element can be designed according to two different principles:

- *Energize-to-trip*. The SIS element is de-energized during normal operation and need to be energized (e.g., by electricity, hydraulic pressure, pneumatic pressure) to perform its safety function (i.e., to trip). Loss of energy will, by this principle, prevent the element from performing its safety function.

- *De-energize-to-trip*. The SIS element is energized during normal operation and removal of the energy will cause a trip action. By this principle, loss of energy will cause a spurious (i.e., false) activation of the safety function. Many SIS elements are today designed according to the de-energize-to-trip principle. This principle is also a basis for the fail-safe principle.

☞ **Fail-safe**: A design property that causes a SIS element to go to a predetermined safe state in the event of a specific failure or malfunction.

The term 'fail-safe' will be extensively discussed in Chapter 11 of the Safety 4.0 textbook.

# Bibliography

Rausand, M. (2014). *Reliability of Safety-Critical Systems.* Wiley Series in Probability and Statistics. Wiley.

van der Meulen, M. and Myhrvold, T. (2022). *Demonstrating safety of software-dependant systems.* DNV AS.