Equipment, Systems and Process: The role of Actuated Valves in Safety Instrumented Systems

Jacqueline Onditi
Pentair Actuation and Controls

IEC 61508 and IEC 61511

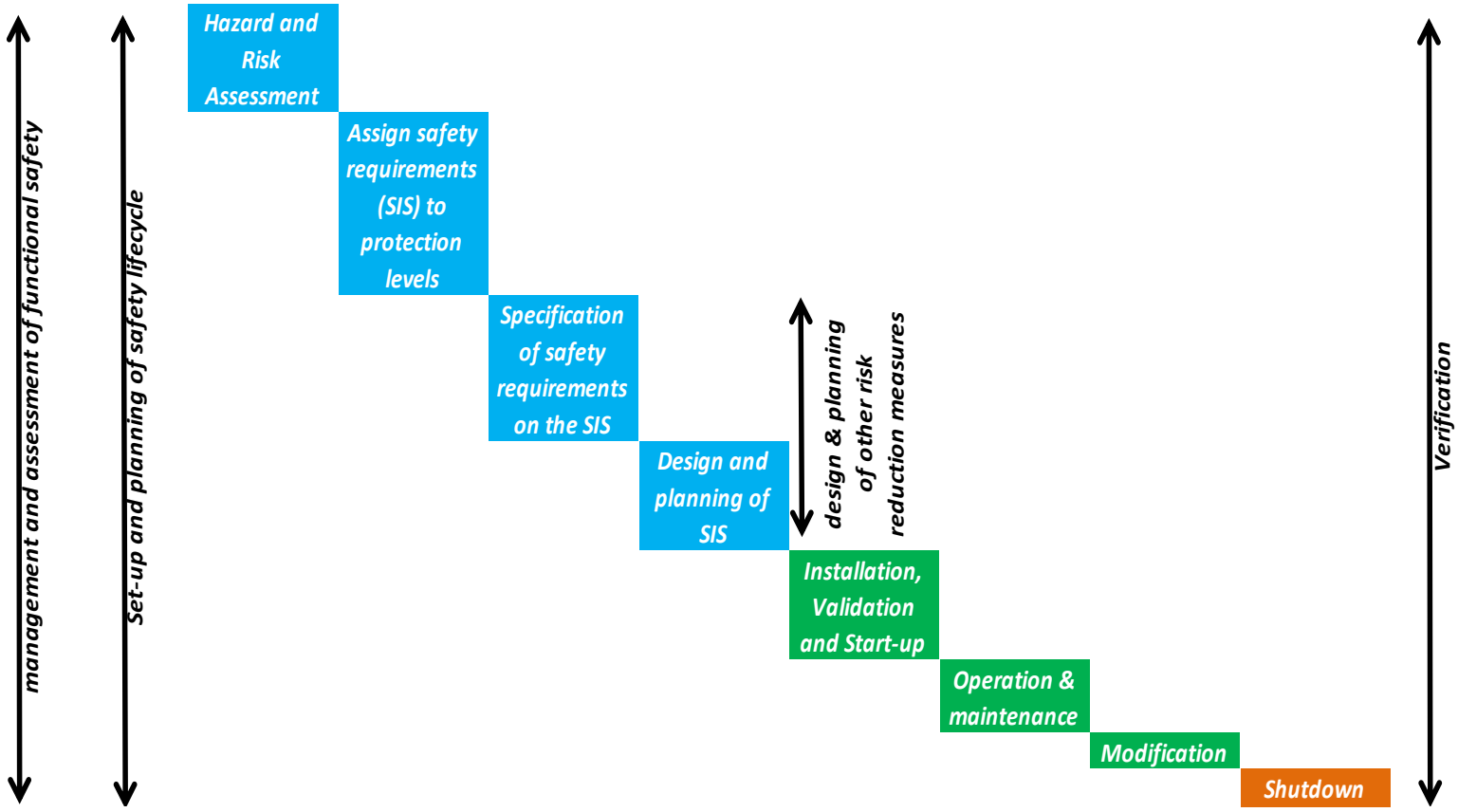
IEC 61508 «Standard for Functional Safety of Electrical / Electronic / Programmable Electronic Safety related Systems»

- It is an equipment manufacturer standard.
- It defines the design and performance criteria necessary for equipment installed on safety systems that include an E/E/PE device.
- It is technology neutral.
- It is based on reduction of risk according to the principle of «ALARP»
- It is structured to be applied in conjuction with sector specific functional safety standard.

IEC 61511 «Functional Safety – Safety Instrumented Systems for the Process Sector»

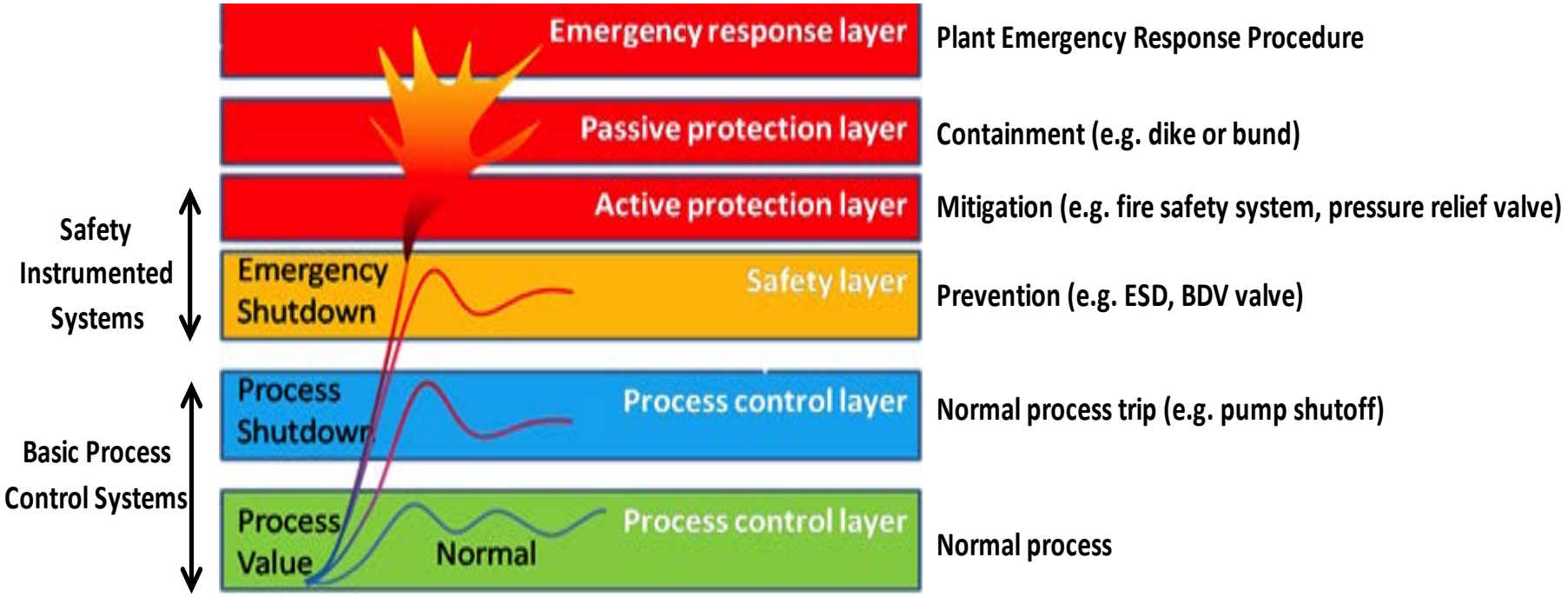
- It is a process systems standard.
- It defines the criteria and performance necessary for safety systems installed in the process sector.
- It integrates equipment covered by IEC 61508 into the wider concept of Safety Instrumented Systems.

Safety Lifecyle and Functional Safety Management System



Safety Systems need to be considered within the Safety Life Cycle, defined as “an engineering process that includes **all the necessary steps** to achieve the required functional safety”

Safety Systems



Safety-related systems are meant to protect industrial processes where harm may occur in case of failure. Their purpose is to bring the plant to a safe state in case of a malfunction in normal process.

Functional safety refers to an **active system** where safety equipment has to function correctly to prevent the hazardous incident.

Actuated valves in a Safety Instrumented Function

A process will have a Safety Instrumented System (SIS) composed of one or more of Safety Instrumented Functions (SIF) each classified according to a Safety Integrity Level (SIL).

For example, on hydrocarbon storage tanks, several valve functions can be incorporated into the Safety Instrumented System:

- ESD on inlet line (emergency close)
- ESD on outlet line (emergency close)
- BDV on overflow line (emergency open)
- Venting (emergency open)

Each SIS loop is a Safety Instrumented Function – SIF. In each case, there are 3 main elements involved in the SIF:

Equipment Selection Criteria

Compatible with ambient, Compatible with process, Adequate performance.

Have you selected the right Valve?

- Type of service
- Size & pressure rating
- Fluid medium
- Materials
- …

Have you selected the right Actuator?

- Motive power supply
- Suitable torque
- Operating speed
- Operating frequency
- Fail action
- …

Have you selected the right Controls?

- Size / Flow rate
- Power supply
- Functionality
- Materials
- …

System Architecture

And that's not all. Even after correct selection of all the correct equipment, this needs to be correctly integrated into the overall safety sytem.

System architecture must consider aspects such as process layout, eventual redundancy requirements, safeguards against suprious trips, verification and maintenance of the equipment and system SIL ratings…

Probability of Failure on Demand

SIL stands for Safety Integrity Level. It is essentially a measure of the system performance in terms of availability – or Probability of Failure on Demand (PFD). SIL applies to the SIF as a whole because a failure of any component will compromise the safety function.

However the performance of each element (Probability of Failure on Demand – PFD) is analyzed separately when determining the safety performance of the SIF.

The element is defined as suitable for use in a SIL application when it presents third-party certified functional safety data in accordance to IEC 61508.

SAFETY INTEGRITY LEVEL ***(low demand mode)***	**RISK REDUCTION FACTOR**	**PROBABILITY OF FAILURE ON DEMAND**
SIL 1	FROM 1/10 TO 1/100	10^{-1} TO 10^{-2}
SIL 2	FROM 1/100 TO 1/1000	10^{-2} TO 10^{-3}
SIL 3	FROM 1/1,000 TO 1/10,000	10^{-3} TO 10^{-4}
SIL 4	FROM 1/10,000 TO 1/100,000	10^{-4} TO 10^{-5}

Probability of Failure on Demand

PFD values for single devices are defined as an average over a set period of time (PFDavg)

PFDavg values on single devices are determined by:

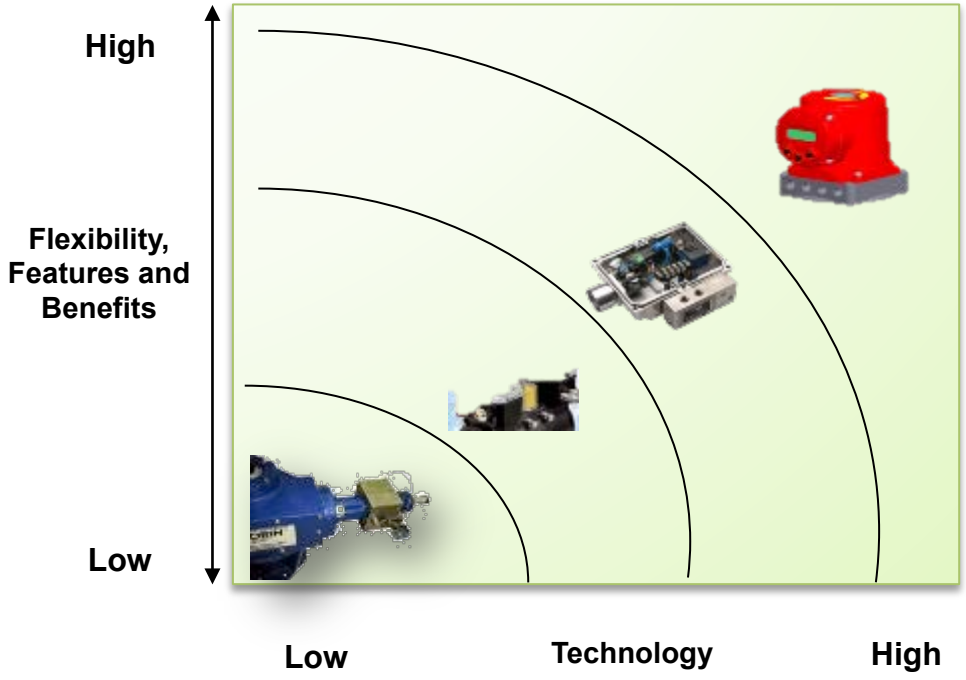
- Demand mode: frequency of demand: low, high or continuous.
- Failure rates: calculated by FMEDA methodology, or by combination of FMEDA and Prove-in-Use statistics
- Diagnostic coverage: The number of dangerous failures detected by automatic test procedures in relation to the total number of dangerous failures. A test interval must be specified on the PFD calculation and respect of the test interval is essential to maintain the SIL level of the SIF.

Diagnostic Coverage: Partial Stroke Testing

There are a number of different techniques available for partial stroke testing and the selection of the most appropriate technique depends on the specifics of the application.

The most common techniques are:

1. **Mechanical Jammers**. Lowest cost, low coverage, device unavailable for safe action if required.
2. **Electro-Pneumatic Positioners.** Higher cost, partial coverage, device availability if required
3. **Electronic Position Transmitters**. Higher cost, good coverage, device availability.
4. **Smart devices.** Higher cost, good coverage, additional features benefit predictive maintenance and asset managment.



Wait a minute…

What about Hazop? LoPA? HFT? SFF? CCF? 1oo2? 2oo3? λ?

IEC 61508 & 61511. Safety is more than just a list of acronyms!

QUESTIONS?