

Process Safety Management (PSM) Webinar

Safety Instrumented System

Process Safety & Engineering Committee, SCIC



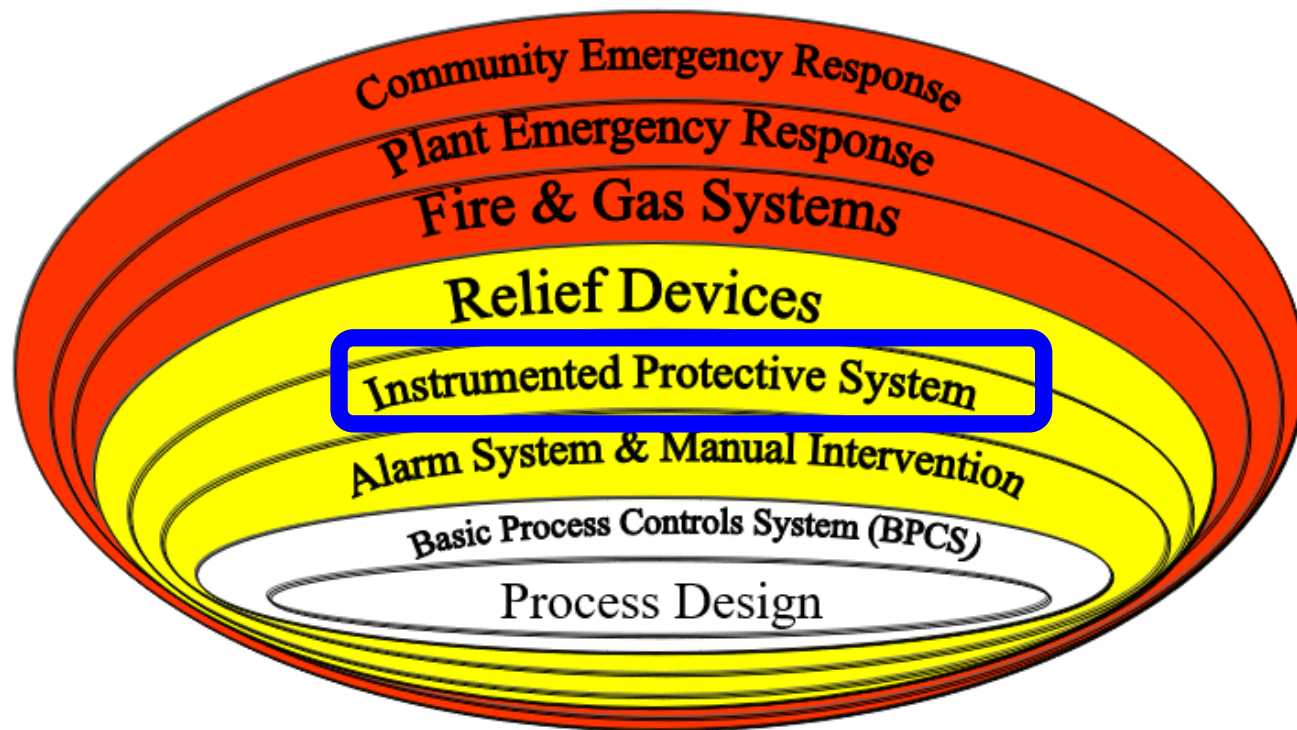
Contents

- 1 **Layers Of Protection**
- 2 **Instrumented Protective System**
- 3 **Buncefield Terminal Fire & Explosion**
- 4 **SIS: Safety Instrumented System**
- 5 **Key SIS Definitions**
- 6 **International Safety System Standard - IEC 61511**
- 7 **Summary**



Layers Of Protection

- Layers Of Protection installed for **safe operation** of chemical facilities
- Today's discussion on **Instrumented Protective System**



Instrumented Protective System

- Also known **Emergency Shutdown System (ESD), Plant Shutdown System (PSD), Interlocks** in different organisations
- Protective system responds to an **initiating event** and brings the process or equipment to its **safe state**.
- Protection system may consist of a component, group of components, or system that reduces risk by **preventing** or **mitigating** the consequences of a hazard
- Systems may be either **manually** or **automatically** initiated.
- Hazards are typically assessed by a **Risk Analysis** and can be primarily **Health, Safety, Environment (HSE), Operational, or Equipment protection** based risks.



Features Of Instrumented Protective System

Instrumented Protective System designed to ensure:

- **Personnel, Environment or Equipment**, are not impacted by process conditions that **exceeds Plant Operating Envelope** or **Critical Operating Parameters**
- **Plant Operating envelopes** set by Health, Safety, Environment (HSE), Operational or Equipment protection-based risks

Achieved By:

Bringing plant/ equipment into safe state by removing the energy sources (Chemical, Pressure, Heat, Electrical etc.)



Features Of Instrumented Protective System

- Failure action of shutdown systems is **Fail-Safe**
- Separation from the **Basic Process Control System (BPCS), Process Alarms** to ensure it responds on failures or loss of BPCS
- **Independent power supply source with backup** to ensure safe shutdown
- **Auto initiated** or activated **manually by trip switch (pushbutton)** on DCS console, in control room, or in field
- **Shutdown system logic** remains in its **protective state** after trip until **manually reset**
- Each **protective function** typically consist of following elements:
 - Process **Sensor (Pressure, Temperature, Flow, Vibration, Analyser.....)**
 - **Logic Controller (Relay, PLC etc.)**
 - **Final Element (On/ Off Valve (ESV), Motor drives**
 - **Auxiliary Systems** (Rack Panel, Cabling, Junction Boxes etc.)



**How Reliable Is Instrumented
Protective System Installed At
Your Facility?**

**Will It Work on All Demands
From The Process System?**

**You Think it will work or You
Know it will work!**

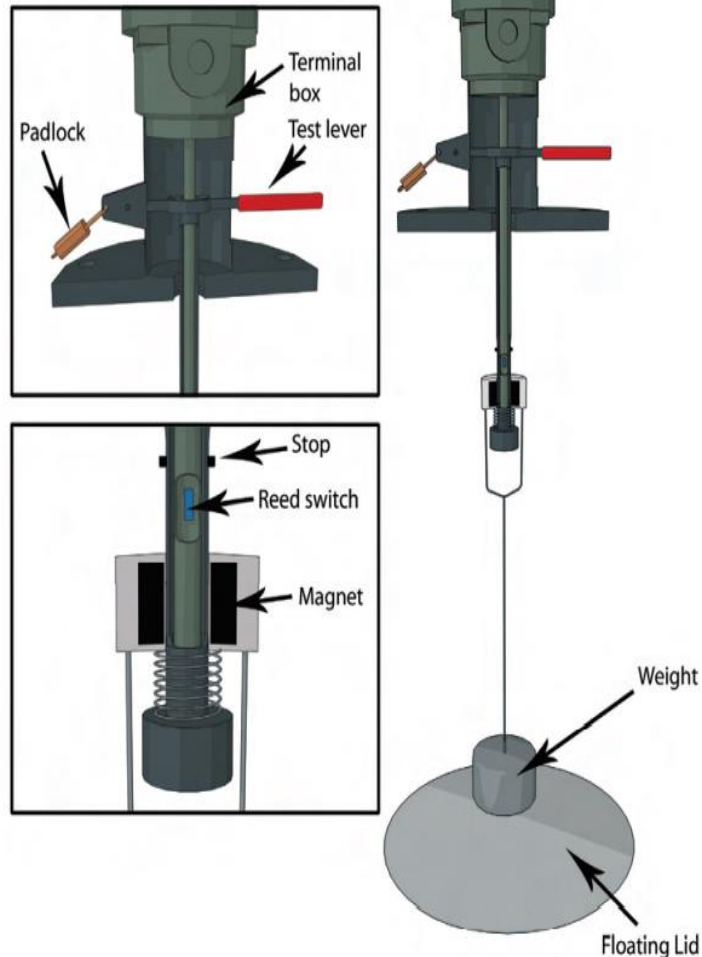


Buncefield Terminal Fire & Explosion

- Massive vapour cloud explosion at Buncefield Fuel depot near Hemel Hempstead, UK on 11 December 2005.
- Explosion caused by an **overflow from storage tank 912** resulting in the release of over 300 tons of petrol.
- **Vapour cloud** spread over an area of 80,000m², which **ignited and exploded**.
- Considerable damage caused in the vicinity of the explosion, **43 people injured**



Root Cause Of Buncefield Terminal Fire & Explosion



- **Instrumented Level gauge** for monitoring the tank level and an **Independent High-Level switch (IHLS)** designed to shut down operations automatically were **inoperable**.
- Tank 912 was fitted with a new IHLS on 1 July 2004.
- IHLS was designed so that some of its functionality could be routinely tested.
- Contractor who installed and operators did not fully understand the way new switch worked, or the crucial role played by a padlock, the switch was left effectively inoperable after the test

Ref: UK HSE COMAH: Buncefield: Why did it happen?



Other Industry Accidents Attributed To Faulty Instrumentation

- CAPECO Terminal Fire/ Explosion 2009
- BP Texas City Fire Explosion 2005
- Clapham Junction Train Crash 1988
- Three Mile Island Nuclear Facility 1979
- Others.....

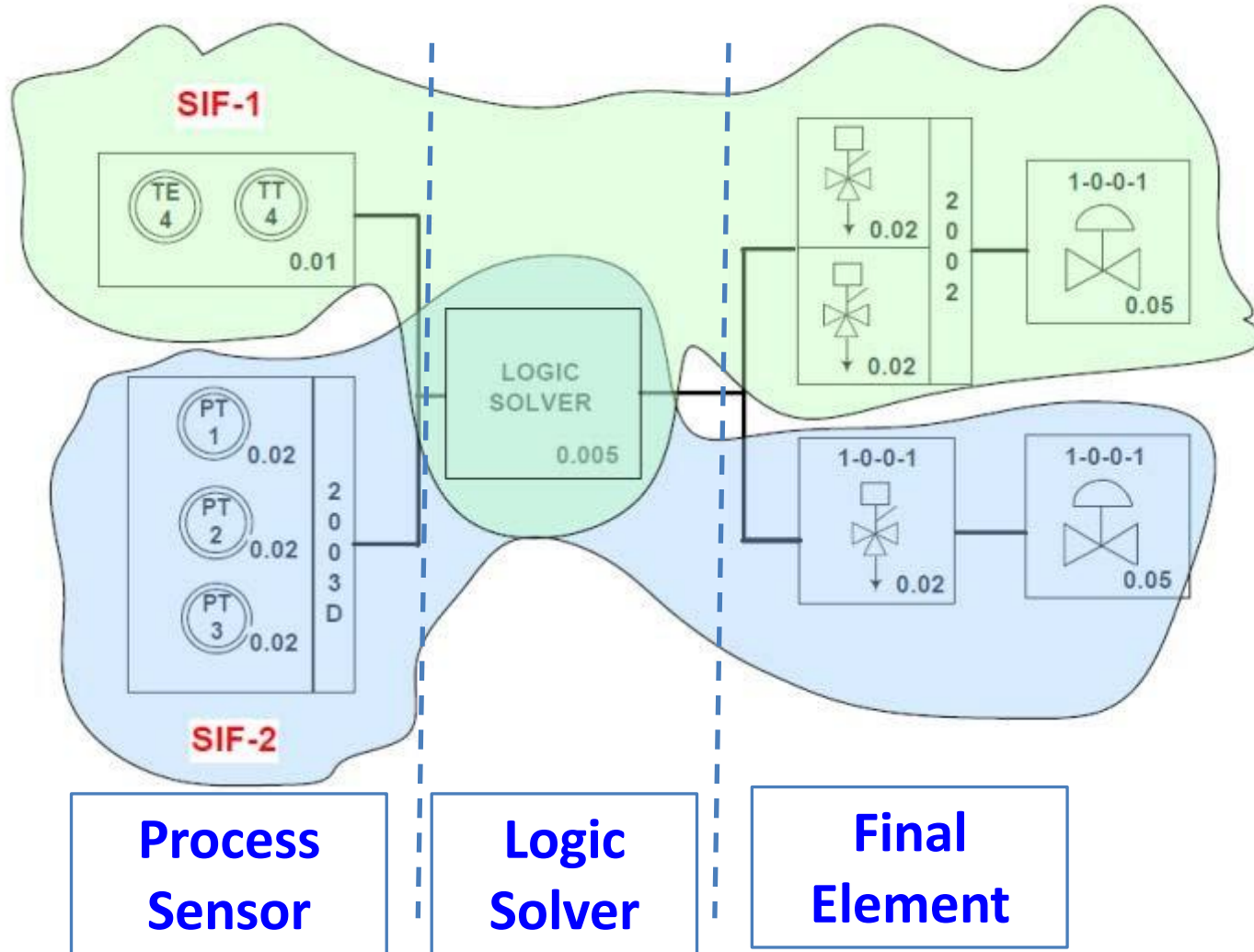


SIS: Safety Instrumented System

- Instrumented Protective System designed, installed & maintained (full lifecycle) to meet **specified performance standards** are known as **Safety Instrumented System (SIS)**
- SIS is a subset of an **Instrumented Protective System** installed for prevention or mitigation of a safety hazard
- Key features of Instrumented Protective System retained in SIS
- **Risk based performance standard** defined by International Standard IEC-61511
- Individual Protective Function to **prevent/ mitigate specific risk scenario** is known as **Safety Instrumented Function (SIF)**



Safety Instrumented Function



Safety Instrumented System (SIS) ensures Design, Installation, Maintenance Regime (full lifecycle) of Instrumented Protective System to meet the expected demand from the process & bring the plant/equipment to safe state every time

Think >>> Know



Risk based approach with higher risk plant requires more stringent design, installation and maintenance regime



Key SIS Definitions:

- **Probability of Failure on Demand (PFD)**: A value that indicates the **probability of a protective system failing** to respond to an initiating event
- **Availability**: “Availability” represents the statistical probability that the protective system is **operational** and can **respond properly** to an initiating event at any instant in time
- **Availability** = 1-PFD
- **Risk Reduction Factor (RRF)**: Indicate the **Probability of Failure on Demand for a protective system**. RRF is inverse of the required PFD.
 - For example, a required PFD value of .001 would equal a risk reduction factor of 1,000, meaning that the protective system would fail during a dangerous scenario about once every 1000 demands



Key SIS Definitions:


Safety Integrity Level:

- **SIL** is a **numerical** means of quantifying the full lifecycle requirements of a **Safety Instrumented Function** to match the risk imposed by the process.
- SIL of an SIF is a means of quantifying the **relative reduction** in risk associated with the correct operation of that SIF
- **PDF (RRF) calculation** done for the **SIF configuration** and meet **SIL requirement**
- SIL implies a **numeric designation of PFD or RRF**, as per table below:

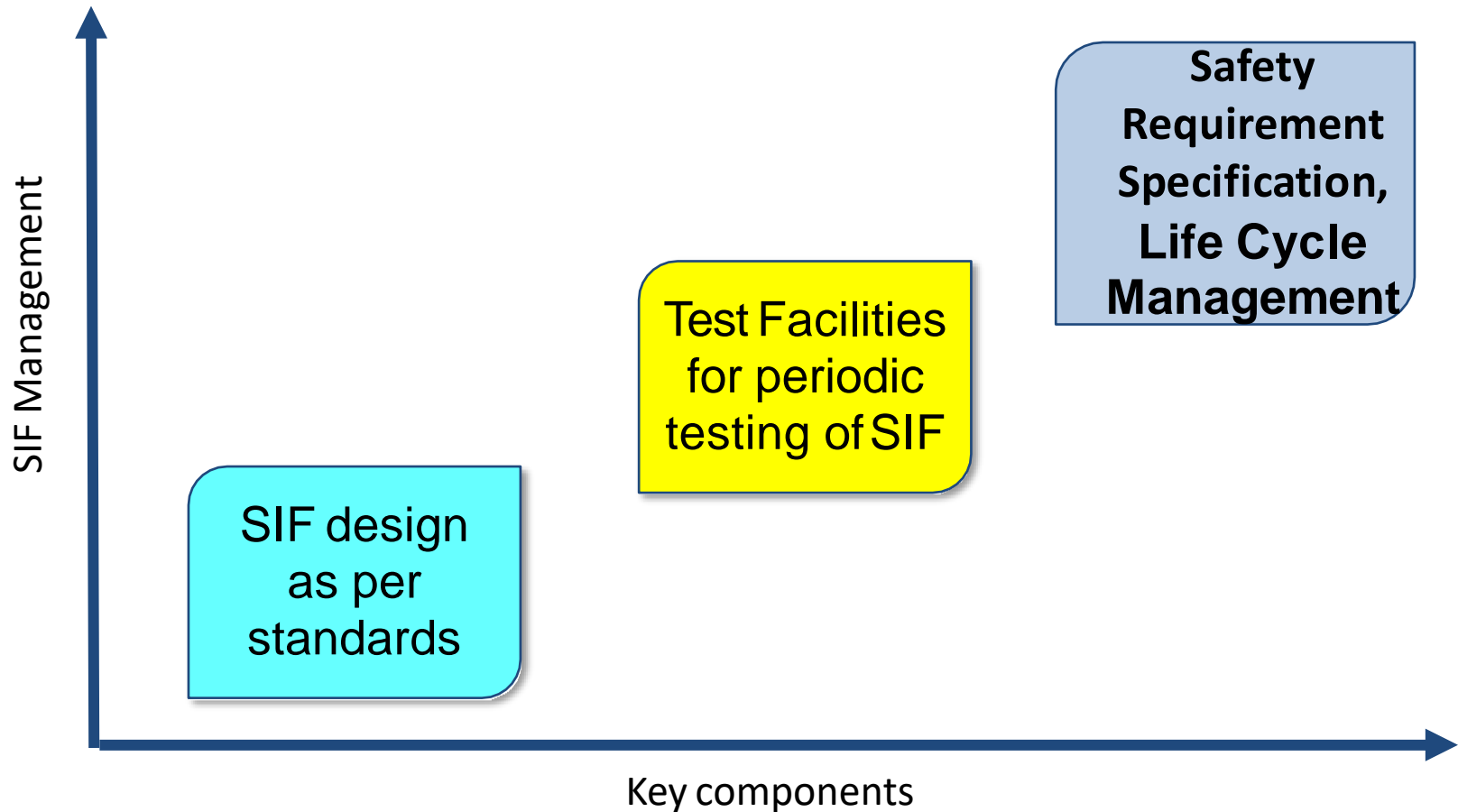
Safety Integrity Level (SIL)	PFD Range	Availability
1	$<10^{-1}$ to $\geq 10^{-2}$	$>90.00\%$ to $\leq 99.00\%$
2	$<10^{-2}$ to $\geq 10^{-3}$	$>99.00\%$ to $\leq 99.90\%$
3	$<10^{-3}$ to $\geq 10^{-4}$	$>99.90\%$ to $\leq 99.99\%$
4	$<10^{-4}$ to $\geq 10^{-5}$	$>99.99\%$ to $\leq 99.999\%$



SIS Application

Parameter	SIL NR	SIL 1	SIL 2	SIL 3	SIL 4
RRF	<10	10 ~ 99	100 ~ 999	100 ~ 9999	>10,000, <100,000
Availability (% of Demands)	< 90	90 ~ 99	99 ~ 99.9	99.9 ~ 99.99	>99.999
Architecture	Simple	Increasing Complexity 			Highly Complex
SIF Components	Non SIL certified Instruments	Suitable SIL certified instruments including Logic Solver, Sensors, Final Elements			
Typical Application (based on LOPA Analysis)	Equipment, Operational risk	Low HSE Risk,	Medium HSE Risk	Catastrophic Consequences	
Application In	Chemical Industry			Rarely in chemical industry	Nuclear Industry
Typical % spread In Chemical Industry	Depending upon facility	~85 to 95%	~ 5 to 15%	Rare (redesign process)	Not installed in Chemical Industry

SIF Key Requirements

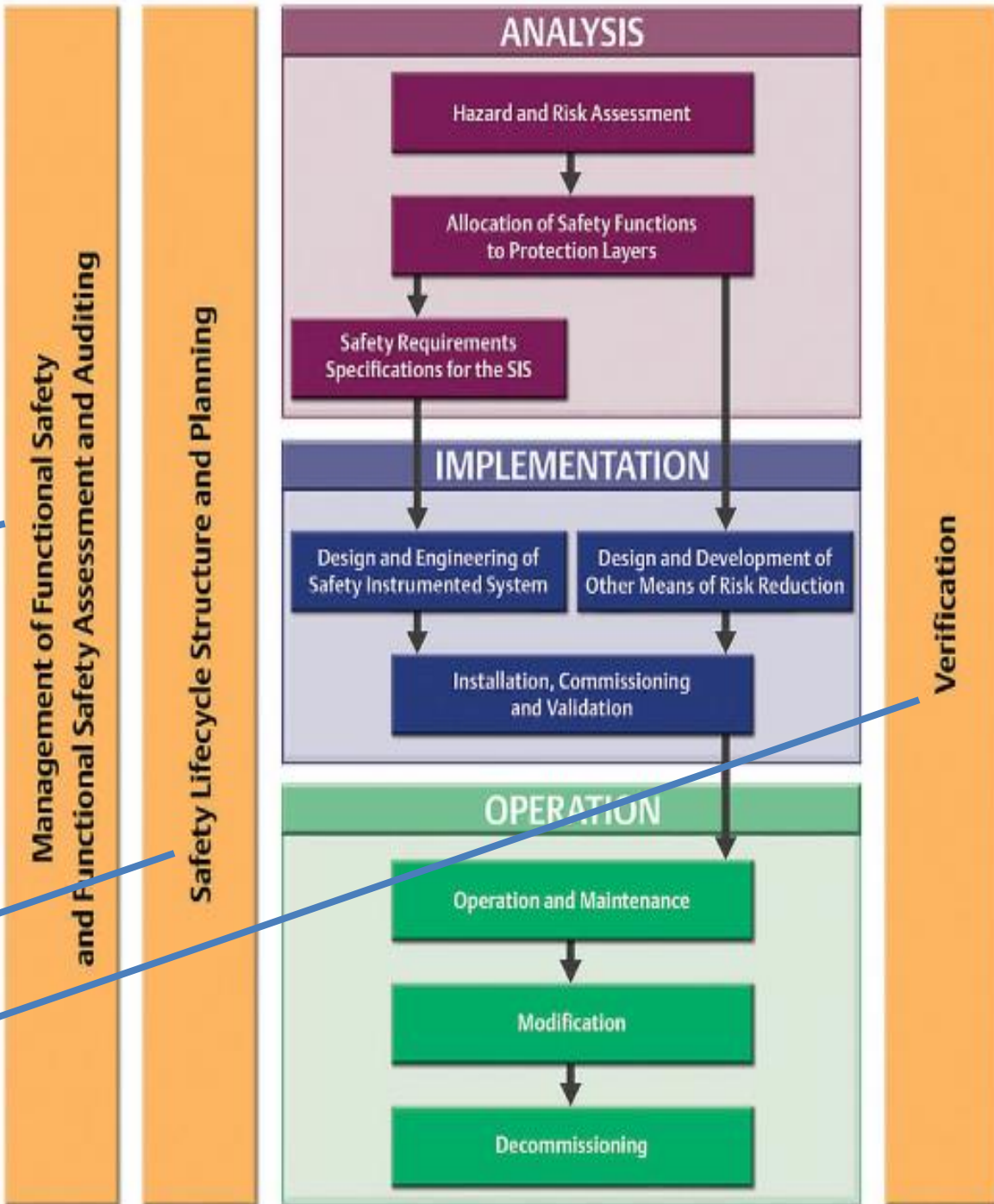


International Safety System Standard – IEC 61511 Requirement

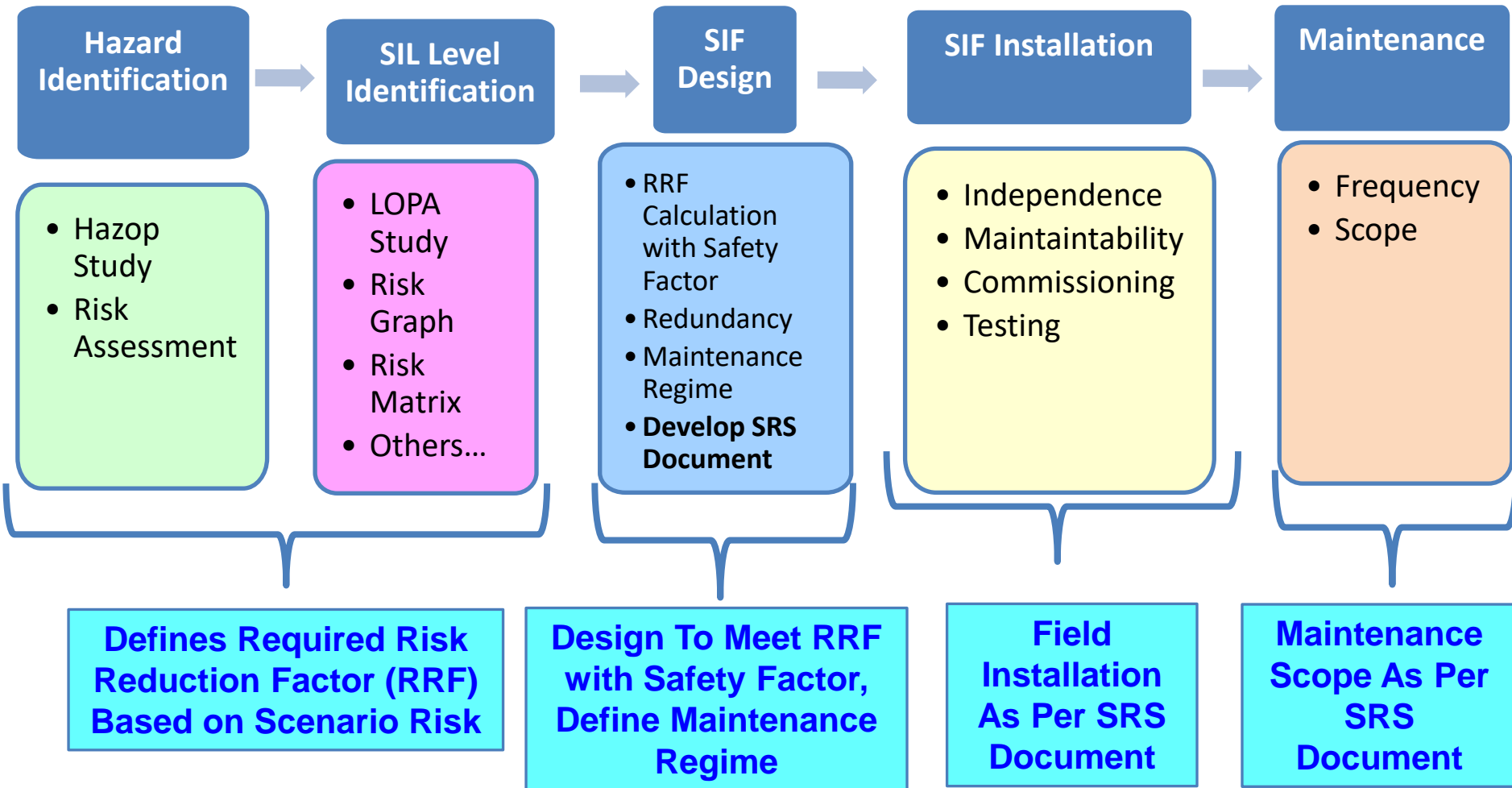
Management Of Functional Safety & Functional Safety Assessment & Audit

Safety Lifecycle Structure and Planning

Verification



SIS Lifecycle Process



Summary

- Upgrading existing interlocks to SIS provides a level of **assurance** that **Safety Instrumented Function** will work on process demand (risk based approach)
- Complete **lifecycle** consideration of SIF
- **Verification** at each stage of lifecycle to ensure identified requirements are properly met
- Risk based **optimized SIF design**
- **Optimized maintenance regime**

I Think >> I Know



Resources

- **IEC 61508: Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems**
 - Sets out the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required safety integrity level (SIL)
 - Basic or “umbrella” standard for Functional Safety.
- **IEC61511: Functional Safety for the Process Industry**
 - Is process industry derivative of the international standard for functional safety, IEC 61508
 - Performance based rather than prescriptive;
 - SIF design is based on risk analysis and providing the required risk reduction.

Thank You