



# 16<sup>th</sup> Chemical Process Safety Sharing (CPSS)

## Journey of Functional Safety in SCGC

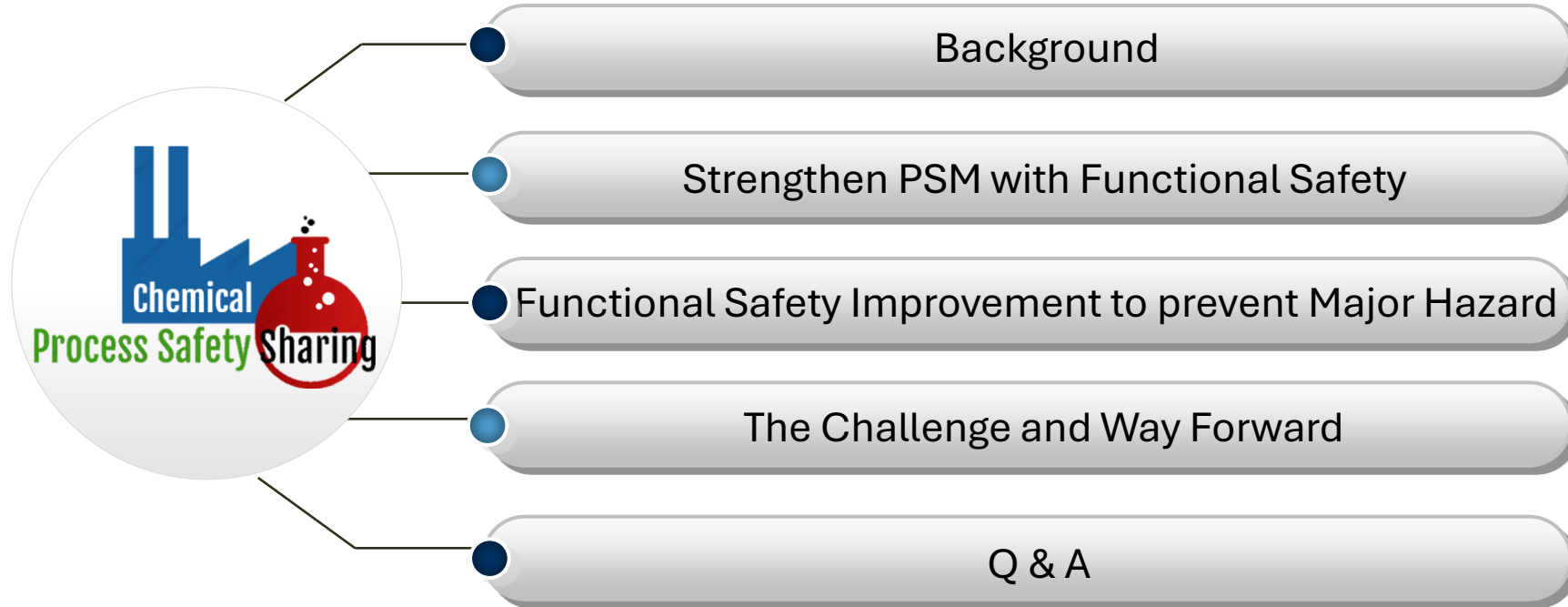


Vorachatra Sukwattanajaroon  
E-mail: [Vorachas@scg.com](mailto:Vorachas@scg.com)  
Company : SCG Chemicals





# Contents



16<sup>th</sup> Chemical Process Safety Sharing (CPSS)  
Sep 26<sup>th</sup>, 2025, BITEC BANGNA





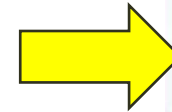
# Background



Lessons learnt from incidents take us to review & revisit what we did and find gaps to improve



**Strengthen PHA quality and ensure Major Hazard Incident Prevention with the effectiveness of interlock evaluation, design, operation and maintenance**



## Safety Reform

### 1 Process Safety Management

- Process Safety Design**  
ทบทวนการออกแบบระบบความปลอดภัยในกระบวนการผลิต
- Plant Aging Management**  
ทบทวนการตรวจสอบ ดูแล อุปกรณ์และเครื่องจักรให้มีสภาพที่สมบูรณ์
- Safe Operating Procedure**  
ทบทวนมาตรฐานการปฏิบัติงานและกิจกรรมที่มีความเสี่ยง เพื่อให้มั่นใจว่ามีมาตรการความปลอดภัยอย่างครอบคลุม
- Emergency Preparedness & Response**  
ทบทวนความรู้ ทรัพยากร แนวทางปฏิบัติ ทบทวนการตรวจสอบ ดูแล อุปกรณ์และเครื่องจักรให้มีสภาพที่สมบูรณ์
- High Risk Work Control**  
บ่งชี้อันตราย, กำหนดมาตรการการทำงาน และการควบคุมให้ปลอดภัย

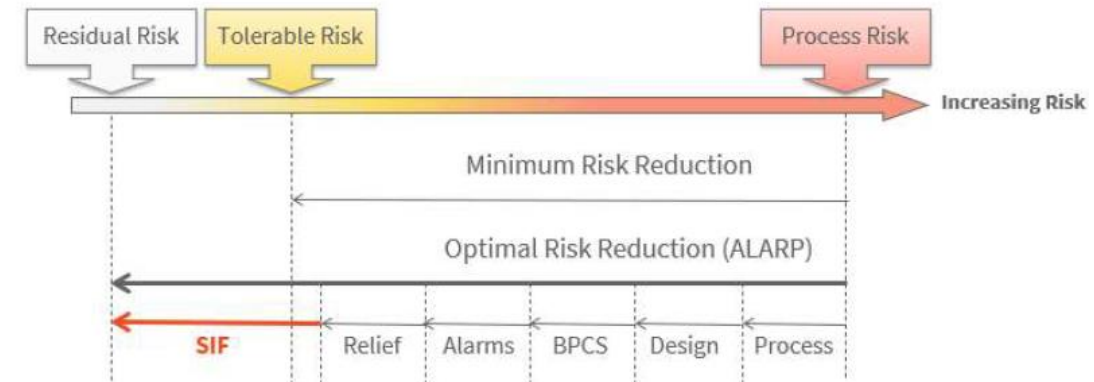
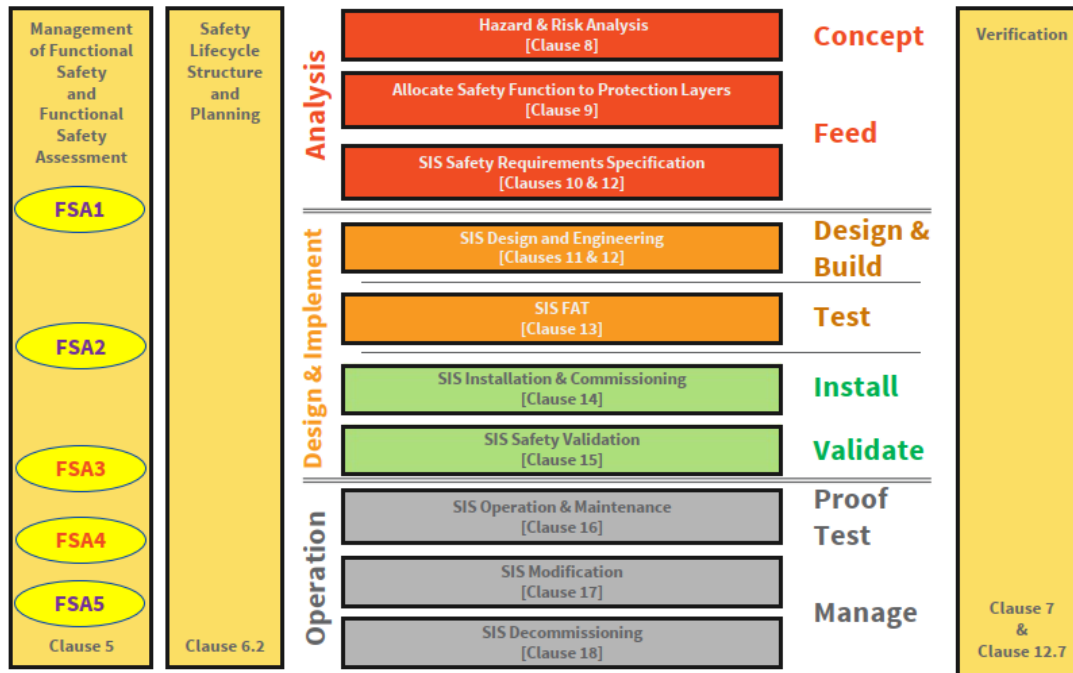


# Functional Safety



“Part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers” IEC 61511:2016 Part1

## IEC 61511 Safety Lifecycle



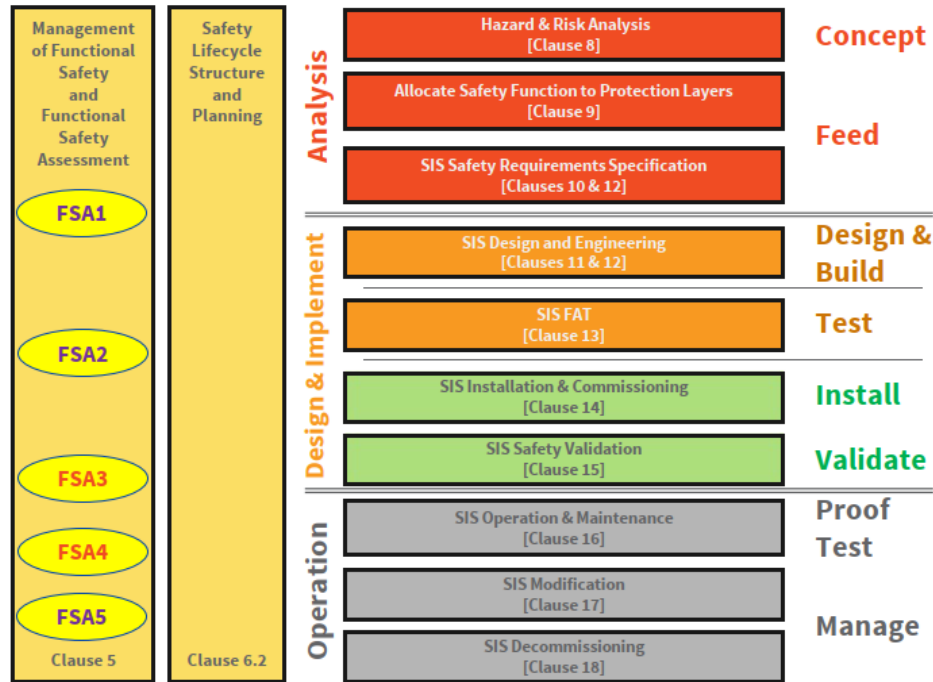


# Strengthen PSM with Functional Safety

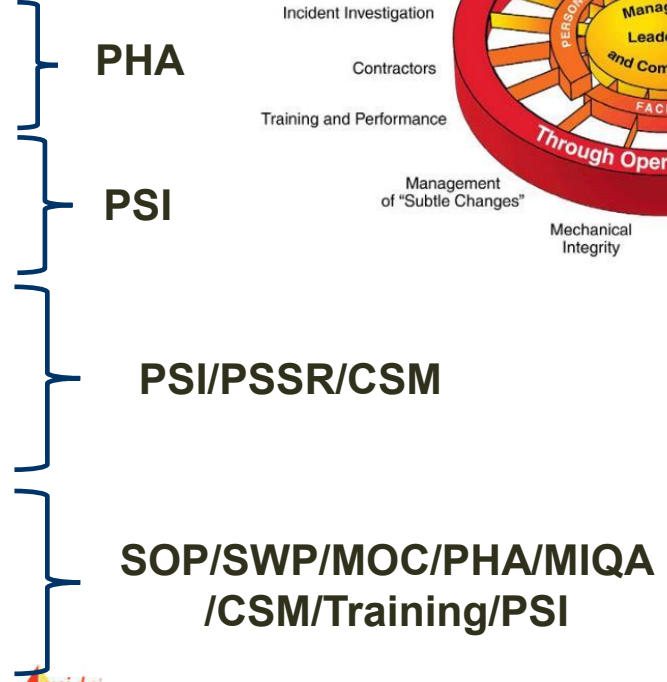


## Mapping PSM vs Safety Life Cycle (IEC 61511)

### IEC 61511 Safety Lifecycle



### Audit





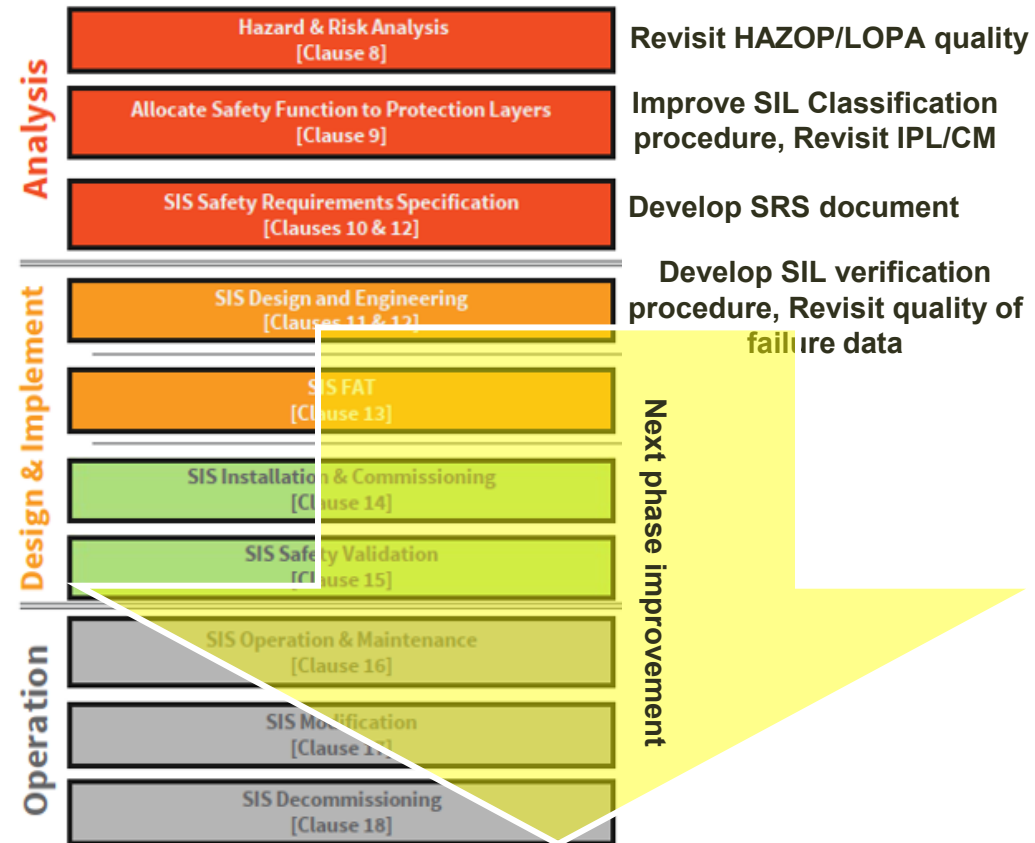
## Review existing PHA practice

### 10 Steps of PHA

- |   |   |
|---|---|
| <ol style="list-style-type: none"> <li>1. <b>Planning and Preparing</b></li> <li>2. <b>Hazards Identification</b></li> <li>3. <b>Consequence Analysis</b></li> <li>4. <b>Process Hazards Evaluation</b> <ul style="list-style-type: none"> <li>&gt; What If</li> <li>&gt; HAZOP / LOPA</li> </ul> </li> <li>5. <b>Other Considerations</b> <ul style="list-style-type: none"> <li>&gt; Human Factors</li> <li>&gt; Facility Siting</li> <li>&gt; Inherently Safer Process</li> <li>&gt; Interlock Evaluation</li> </ul> </li> </ol> | <ol style="list-style-type: none"> <li>6. <b>Risk Assessment</b></li> <li>7. <b>Recommendations</b></li> <li>8. <b>Documentation</b></li> <li>9. <b>Management Response</b></li> <li>10. <b>Communication and Tracking</b></li> </ol> |
|---|---|



## What we're improving







# Functional Safety Improvement to prevent Major Hazard



## Revisit HAZOP/LOPA, IPL quality

- Unreliable measuring devices e.g. level, temperature, pressure switches will not be IPL credited if no testing evidence.
- Review process design/calculation used in IPL (e.g. sizing PSV for which scenario)
- Review impacted from the consequence with process design (e.g. overpressure, cold temperature, surge against pipe class)
- Consider corrosion impact in case of prolong operation
- Encourage to record as note in worksheet in case of no cause identified, low consequence impact e.g. happen in short period.
- For alarm & operator response, ensure operator has enough time to take action.

# Functional Safety Improvement to prevent Major Hazard



## Develop Safety Requirement Specification (SRS) document

- Clearly identified the SIF design intent
- Visualize via Reliability Block Diagram
- Indicate the characteristic of SIF and its elements
- Indicate the characteristic of SIF and its elements
- Indicate necessary parameters of test to be used in SIL Verification
- Indicate the SIL target and SIL Verification result

**SIF Information**

Project/Plant: \_\_\_\_\_  
 Unit/Area: \_\_\_\_\_  
 SIF Tag Number: \_\_\_\_\_ Requested PFD: \_\_\_\_\_ Requested SIL: \_\_\_\_\_  
 P&ID Reference: \_\_\_\_\_  
 C&E Reference: \_\_\_\_\_  
 SIF Design Intent: \_\_\_\_\_  
 SIF Functional Description (Safe State Action): \_\_\_\_\_  
 Demand Source (Cause) of SIL Activation: \_\_\_\_\_  
 IF common cause failures exist among: \_\_\_\_\_  
 Demand Mode: \_\_\_\_\_  
 Consequence of SIF Failure: \_\_\_\_\_

**Interface between SIF and any other system**

Any process sharing between EPCS and SIF: YES or NO \_\_\_\_\_  
 Any logic colour sharing between EPCS and SIF: \_\_\_\_\_  
 Any final element sharing between EPCS and SIF: \_\_\_\_\_

**SIF Design Requirement**

Reliability Block Diagram (RBD): \_\_\_\_\_

**Sensor**

Type Number: \_\_\_\_\_  
 Number of sensors including enable, bypass, & compensation: \_\_\_\_\_  
 Architecture (No&M): \_\_\_\_\_  
 Disruption mode: \_\_\_\_\_  
 Application Related Effect: \_\_\_\_\_  
 Failure Effects: \_\_\_\_\_  
 Surrounding Environment Effects: \_\_\_\_\_  
 Sensor Failure Response: \_\_\_\_\_  
 Process Variable Response: \_\_\_\_\_  
 Logic Solver: \_\_\_\_\_  
 Type Number: \_\_\_\_\_  
 Top Model: \_\_\_\_\_  
 Input Channel: \_\_\_\_\_  
 Output Channel: \_\_\_\_\_  
 Final Element: \_\_\_\_\_  
 Type Number: \_\_\_\_\_  
 Number of Final Element: \_\_\_\_\_  
 Architecture (No&M): \_\_\_\_\_  
 Disruption mode: \_\_\_\_\_

**States to Trip** \_\_\_\_\_ **Failure Response (Exclude/Include)** \_\_\_\_\_ **Remote activation** \_\_\_\_\_

**Application Related Effect**

Normal  Unwanted Heat Soak  Impaired Soft Soak   
 Stagnant  Crystallizing  Polymerizing   
 Build-up of Layer or Trim Parts  Abrasion   
 Corrosion  Inertion  Slaking

**Surrounding Environment Effects**

Normal  High Humidity  High Vibration   
 High Temperature  Low  High Activity  Corrosive Environment

**For valve, Required Trip Setoff (Yes/No)**  **Actuator Architecture** \_\_\_\_\_ **Solenoid Architecture** \_\_\_\_\_

**Additional Information**

Miscellaneous for SIF: \_\_\_\_\_  
 Restarting SIF after a shutdown (local/remote/manual/automatic): \_\_\_\_\_  
 Specific requirements for starting up and restarting SIF: \_\_\_\_\_  
 Override function, if yes, how they are cleared? \_\_\_\_\_  
 Bypass requirement, if yes, how they are cleared? \_\_\_\_\_  
 Specific requirements for SIF to prevent a major accident (e.g. fire): \_\_\_\_\_  
 Concurrent safe state action of SIF avoiding a repetitive hazard? \_\_\_\_\_  
 Disruptive Combination of Output State of SIFs, if any, specify: \_\_\_\_\_

**Other Design Related Information**

Process Safety Time (sec): \_\_\_\_\_ **Maximum Allowable Response Time, MART (sec)** \_\_\_\_\_  
 SIF Loop Response Time (sec) = Sensor + Logic Solver + Final Element + Process Safety Time + MART  
 SIF Loop Response Time (sec) = Sensor + Logic Solver + Final Element + Process Safety Time + MART  
 Pre-Alarm Tag Number: \_\_\_\_\_ **Pre-Alarm Set Point** \_\_\_\_\_

**Summary of Inputs & Outputs**

Special Operation Mode: \_\_\_\_\_ **Maximum Response to Service Time (Mr)** \_\_\_\_\_  
 Mission Time (Yr): \_\_\_\_\_ **Start-up/Restart Time (Mr)** \_\_\_\_\_

Element Name	Proof Test		Partial Strain Test		Other Test		MTBF (Hours)	β <sup>n</sup>	PFD <sup>n</sup>	MTFR <sup>n</sup> (Years)
	Interval (Months)	Consp <sup>n</sup> (%)	Interval (Months)	Consp <sup>n</sup> (%)	Description	Interval (Months)				
Sensor										
Logic Solver										
Final Element										

**Notes:**  
 1) Time to Repair  
 2) Common Sense Failure  
 3) PFD<sup>n</sup> = Risk Reduction Factor (RRF)  
 4) SIL (Architectural Consistency)  
 5) SIL (Systematic Consistency)

**Achieved Safety Integrity Level (SIL) Rating**

SIL (PFD<sup>n</sup>) \_\_\_\_\_ **Risk Reduction Factor (RRF)** \_\_\_\_\_  
 SIL (Architectural Consistency) \_\_\_\_\_  
 SIL (Systematic Consistency) \_\_\_\_\_

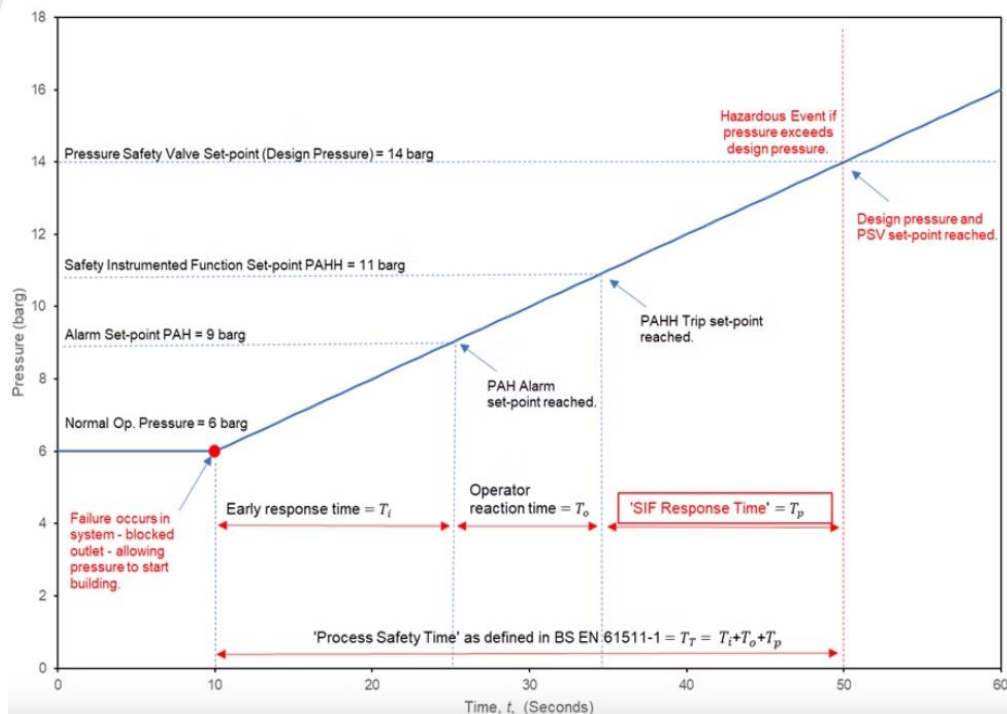
**Data prepared by:**

Rev	Date	Prepared by	Checked by	Approved by	Remark

# Functional Safety Improvement to prevent Major Hazard

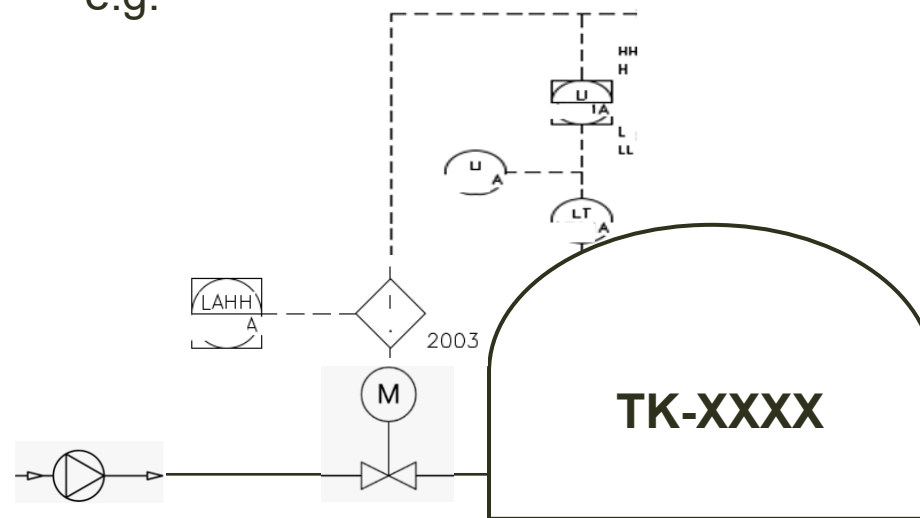
## Develop Safety Requirement Specification (SRS) document

- Assess SIF response time VS process safety time



<https://www.ors-consulting.com/difference-between-the-process-safety-time-and-the-sif-response-time>

e.g.



Change MOV to XV valve to reduce closure time in case of level high high



# Functional Safety Improvement to prevent Major Hazard

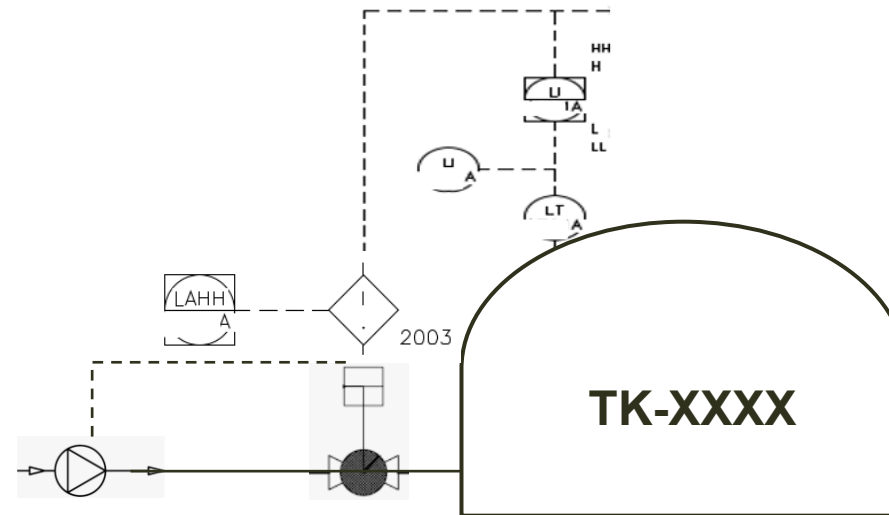


## Develop Safety Requirement Specification (SRS) document



- Review concurrent safe state hazard

Safe state function of SIF will not create a new hazard (collateral hazard)

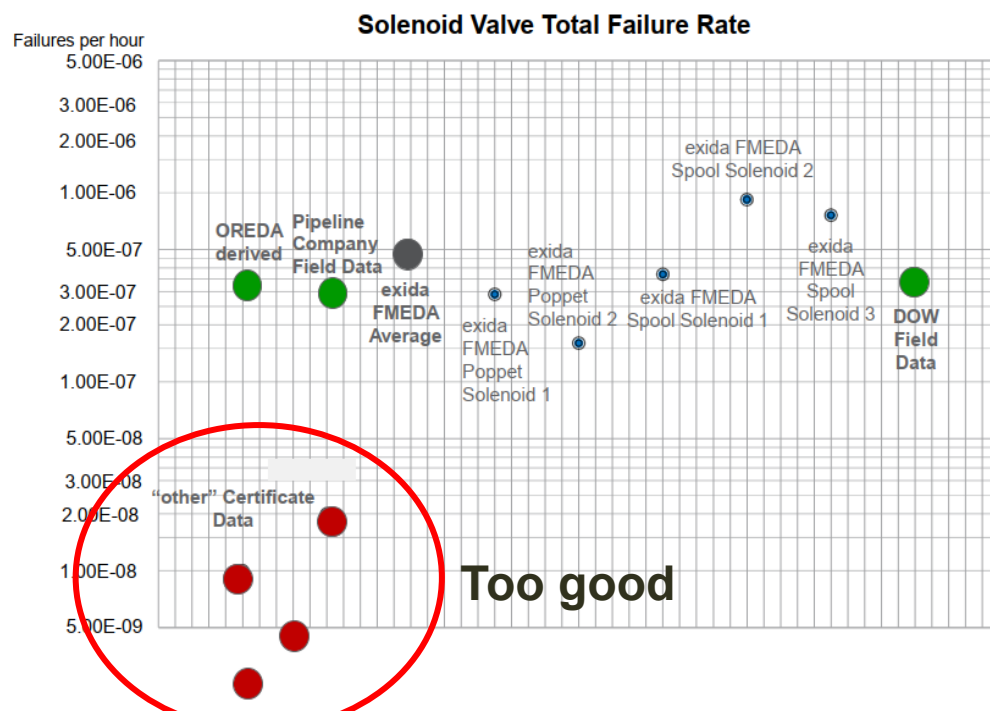


# Functional Safety Improvement to prevent Major Hazard



## Develop procedure to control SIL Verification quality

- Review & Screen failure rate data of hardware



[https://www.researchgate.net/figure/Solenoid-valve-total-failure-rate-DOW-Dow-chemical-field-data-FMEDA-failure-modes\\_fig5\\_351947208](https://www.researchgate.net/figure/Solenoid-valve-total-failure-rate-DOW-Dow-chemical-field-data-FMEDA-failure-modes_fig5_351947208)

## IEC 61508 Failure Rates in FIT\*

Application/Device/Configuration	$\lambda$ SD	$\lambda$ SU	$\lambda$ DD	$\lambda$ DU
Full Stroke, Clean Service	0	0	0	396
Tight Shut-Off, Clean Service	0	0	0	1185
Open on Trip, Clean Service	0	135	0	261
Full Stroke with PVST, Clean Service	0	0	131	265
Tight Shut-Off with PVST, Clean Service	0	0	131	1054
Open on Trip with PVST, Clean Service	134	1	131	130
Full Stroke, Severe Service	0	0	0	719
Tight Shut-Off, Severe Service	0	0	0	2244
Open on Trip, Severe Service	0	257	0	462
Full Stroke with PVST, Severe Service	0	0	226	493
Tight Shut-Off with PVST, Severe Service	0	0	226	2018
Open on Trip with PVST, Severe Service	254	2	226	236

PTI period ?

# Functional Safety Improvement to prevent Major Hazard



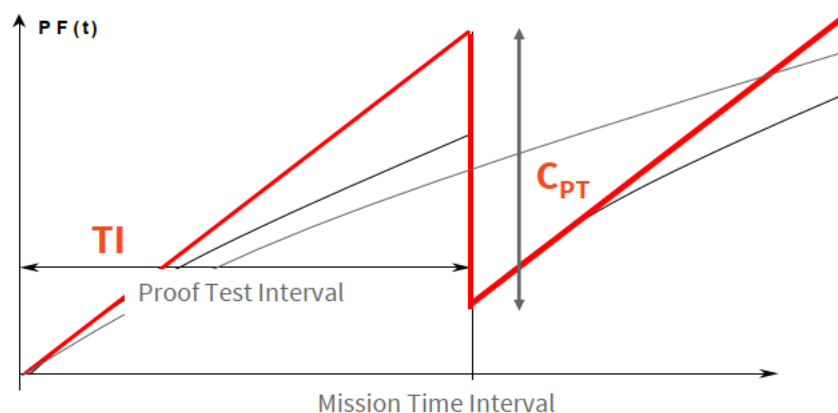
## Develop procedure to control SIL Verification quality

- How to claim % prove test coverage not too optimistic

Ensure to follow the proof test instruction in safety manual

If no data? How to define? Liaise with vendor/manufacture

e.g. Valve Overhaul and Full Test → PTC = 99% Is it reasonable?



## Safety Manual

### Device-Specific Values

Probability of Dangerous Failure on Demand	$PFD_{spec}$	2,12 E-04
Confidence Level	$1-\alpha$	95 %
Safe Failure Fraction <sup>(see note)</sup>	SFF	68 %
Hardware Fault Tolerance	HFT	0
Diagnostic Coverage	DC	0 %
Type of Sub System		Type A
Mode of Operation		Low Demand
Proof Test Coverage	PTC	85 %

## 5. Operation

### 5.1 Recommended proof test

The purpose of proof testing is to detect failures of the complete final element subsystem. Neles recommends the following proof test procedure:

- Conduct an initial visual inspection. Check that there are no unauthorized modifications to the SIS valve assembly. Verify that there is no observable deterioration in the SIS valve such as pneumatic leaks, visible damage, or impurities on the SIS valve.
- Bypass the SIS valve if full stroke could cause an unnecessary process shutdown.
- Perform the safety action (full stroke), preferably using the system. Verify that the SIS valve achieves safe position within the required time specified by the application. Verify also the shutoff tightness for tightness critical applications. Note that a tightness measurement might require removing the valve from the pipeline. If the valve must be removed from the pipeline, verify proper full stroke operation after re-installation.
- Restore the SIS valve to its normal position.
- Conduct a final visual inspection. Check that the SIS valve is in the normal position, and verify that all accessories are operating according to the specification for the SIS valve normal operation. Inspect visually that there is no observable deterioration of the SIS valve.
- Record all results and observations into the corresponding database with necessary audit trail information.
- Remove the SIS valve bypassing, if used.

# The Challenge and Way Forward



Human Errors & Mistake



Competency gaps

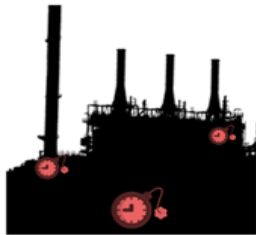


Lean Manpower

How AI tool assist and control quality of work



AILY



Unidentified Hidden risks

We sit on the uncertainty → random failure



Lack of linkage & integration

How to live monitoring interlock health check





Thank you for your attention

