

# **Technical Process Safety Seminar**

**Applying Functional Safety and  
Reaction Safety for Safety Cases:  
Functional Safety and  
Safety Integrity Level**

Hello!



# Aravindhan Ramasamy

SIS/Automation Technical Specialist  
CIS Automation Pte. Ltd.

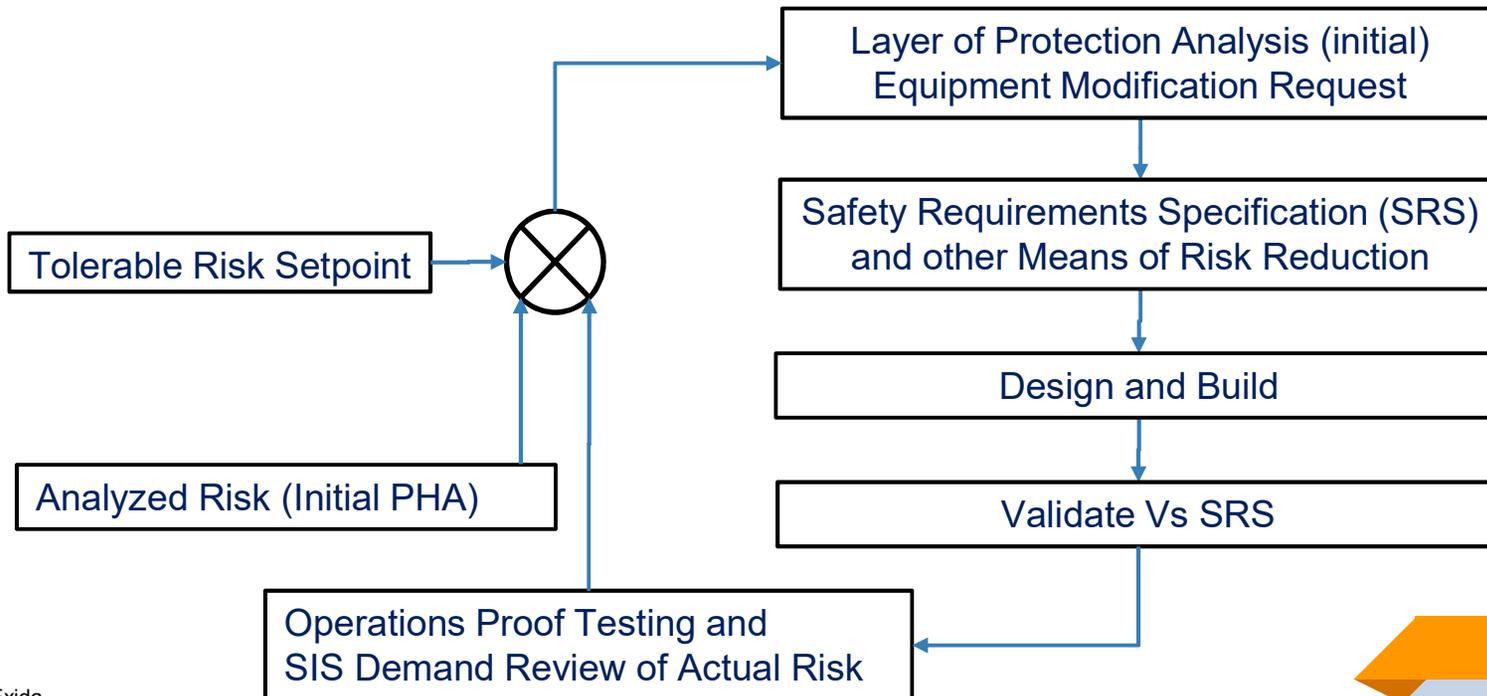
Organised by:

**IChemE** ADVANCING  
CHEMICAL  
ENGINEERING  
WORLDWIDE



# Functional Safety = Managing SIS Risk

Functional Safety means “*Freedom from Unacceptable Risk*”



Source: Exida



# Functional Safety on Local Context

## Singapore Safety Case Regime Regulation for MHI: Safety Case Assessment Guide

2.2. For the assessment of EC&I, the MHD would be covering on three priority topics:

- a) **Functional safety;**
- b) Explosive and/or flammable atmospheres; and
- c) Electrical power systems.

### **Functional Safety**

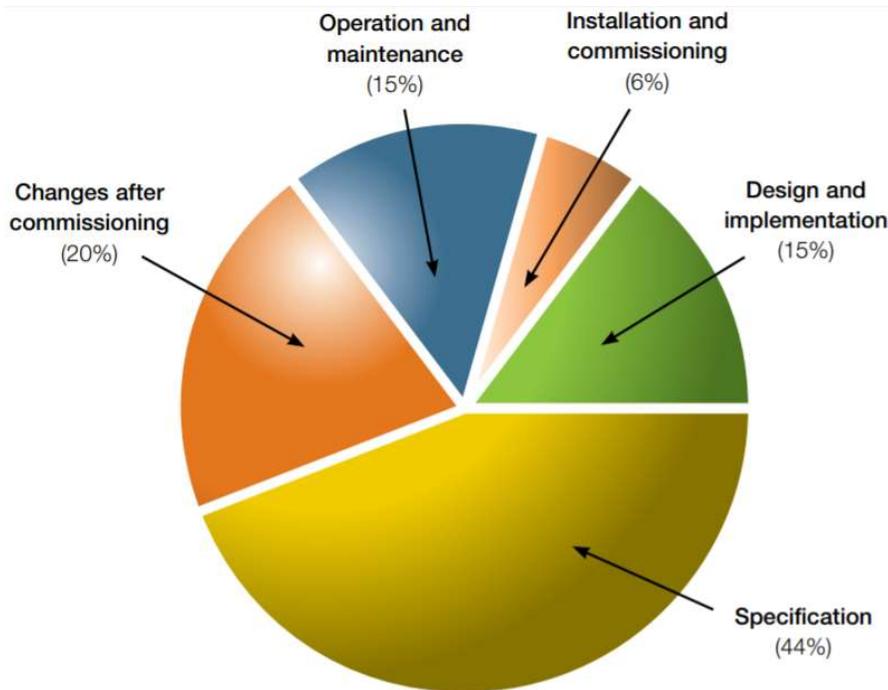
2.3. Functional safety is concerned with the management, design, installation, operation, maintenance and modification of instrumented process safety systems that reduce the risk of a major accident. Such systems include:

- process control systems;
- safety instrumented systems;
- alarm systems.

Source: <https://www.mom.gov.sg/~f/media/mom/documents/safety-health/mhi/safety-case-assessment-guide.pdf?la=en>



# Control System Accident Causes



A significant percentage of the problems were caused by poor specification, that is functionality that was missing or incorrect

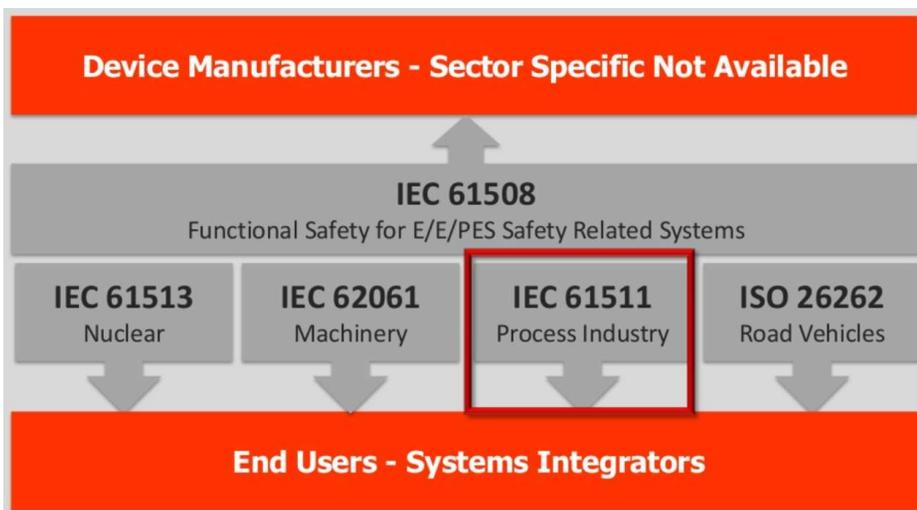
*How can a control system designer create an automatic protective function when that a designer does not know its performance requirements?*

Source: <http://www.hse.gov.uk/pubns/priced/hsg238.pdf>

# Standards for Process Standard

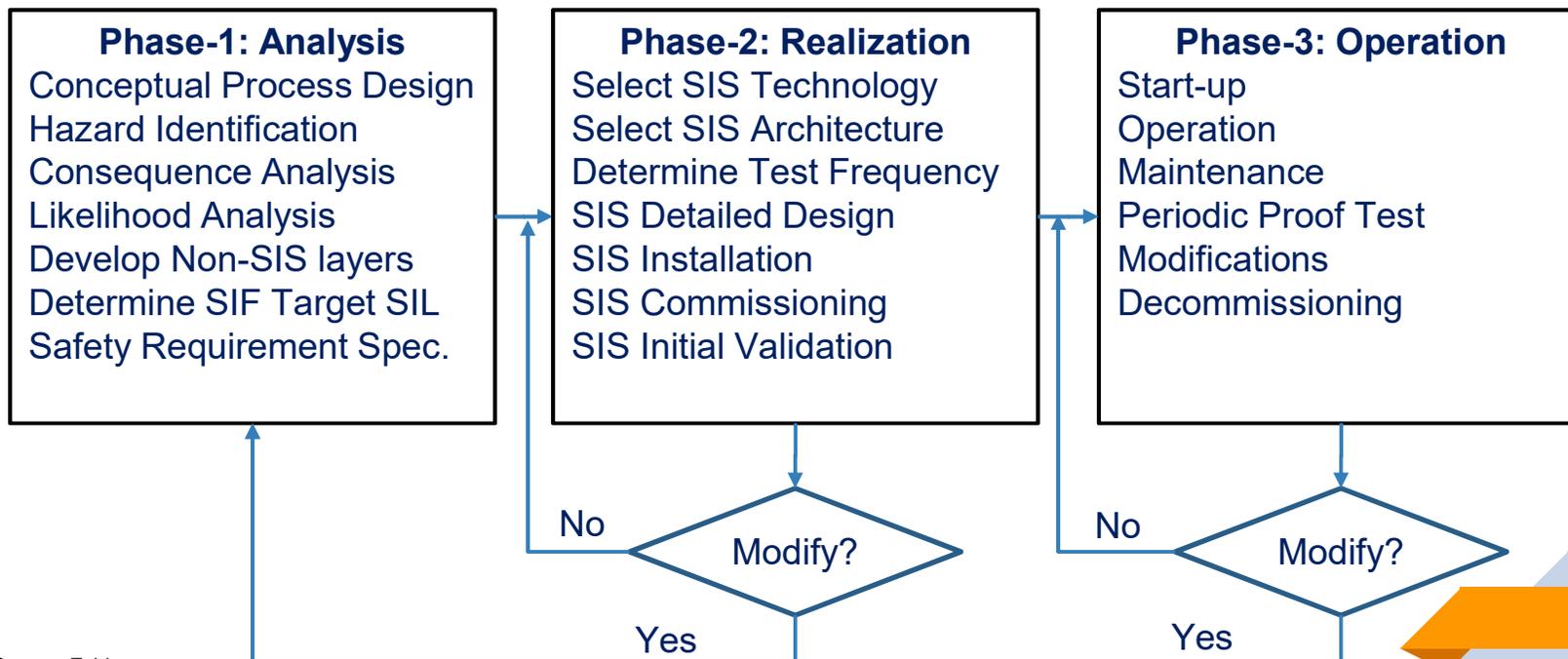
Singapore Safety Case Regime Regulation for MHI: Guideline for good practice.

- d) how current relevant good practice (e.g. IEC 61511) has been applied as far as reasonably practicable to systems designed before its publication;



# SIS Safety Lifecycle

## IEC 61511-1: 2016: Simplified Safety Lifecycle



Source: Exida

# Process Hazard Analysis (PHA)

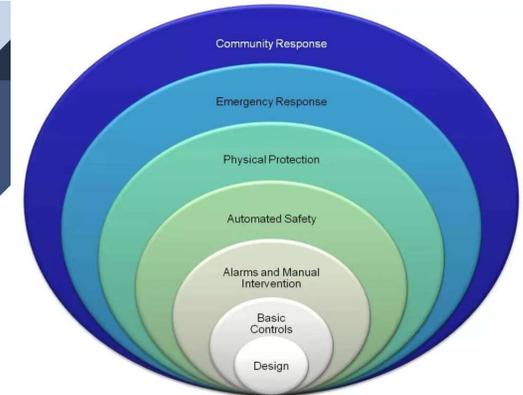
## Risk Prevention Options: Hindsight Vs Foresight

 **Hindsight:** Industrial experiences is easy to learn & implement.  
*Still, in almost every accident, Process Hazard Analysis (PHA) was found to be lacking. This relates to identifying the hazards and properly specifying the SIS, based on the risk reduction required to mitigate hazardous events.*

 **Foresight:** Much difficult to predict but required in preventing industrial accidents  
*Foresight is required especially with today's large, high risk, complicated highly hazardous process plants, can't be designed by trial and error. The risks are too great to learn that way. The risk must be prevented even they have never happened. This is the subject of 'system safety', which is achieved by incorporating PHA as part of process design.*

Evidences of PHA studies such as HAZOP, FMEA, PHR is a requirement in accordance with Singapore Safety Case Regime Regulation for MHI

# Allocation of Safety Functions for SIS



## SIS Design Options: Expensive Vs Optimal

☹️ **Expensive SIS Design:** *Over designing the Instrumentation based risk reduction is incorrect. Example:*

Quantity of SIS SIFs in a process plant	~ 250
Quantity of FGS SIFs in a process plant	~ 200

😊 **Optimal SIS Design:** *The primary objective should be the risks associated with a hazardous event must be prevented with something other than instrumentation (inherent safety design). This does not mean under designing the process or taking wrong/multiple credit for control system or other IPLs. Remaining unmitigated risk can be assigned to Instrumentation based risk reduction.*

For all safety functions assigned to instrumentation i.e. Safety Instrumented Functions (SIF), the level of performance required needs to be determined i.e. Safety Integrity Level (SIL).

Evidences of a SIL determination records (e.g. LOPA, risk graph output) is a requirement in accordance with Singapore Safety Case Regime Regulation for MHI



# Safety Instrumented Functions

## IEC 61511:2016: Clause 3.2.65:

“A function to be implemented by one or more protective layers, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event”

Examples:

- Close the outlet valve in a separation unit to prevent high pressure from propagating downstream, which might result in vessel rupture and explosion
- Cut off fuel flow in an industrial burner when fuel pressure is too low to sustain combustion, possibly resulting in flameout and explosion due to fuel buildup in the combustion chamber
- Open the coolant flow valve to prevent column rupture due to over temperature
- Close the valve if a high material level is detected to stop material flow into a tank, preventing spillage that could result in environmental damage.

SIL is not directly measure of process risk rather a measure of the SIF's performance required in order to control the risk to an accepted level.

# Safety Requirement Specification (SRS)

## SRS Options: Bad Vs Good

 **Bad SRS:** The experience shows that SRS is either not well understood or incomplete information managed throughout SIS lifecycle.

 **Good SRS:** A good SRS for SIS and for each SIF (also called as SIF data sheet) really helps to manage and maintain its SIF performance.

SRS consists of:

- *Functional* specification i.e. *what* the system should do?
- *Integrity* specification i.e. *how well* it should do it?

*Like any other instrument datasheet, SRS must include data sheets for each SIF.*

Evidences of a good SRS is a requirement in accordance with Singapore Safety Case Regime Regulation for MHI.

# SIS Design & Engineering

## SIS Design Options: Prescriptive Vs Performance

 **Prescriptive based SIS Design:** *May end-up with mostly over design. Constraint to comply with prescriptive based standard. Example: EN 746-2 for BMS applications. All SIF elements must be SIL 3 certified. In this case, BMS design is an expensive solution.*

- d) PLC based system in which all components comply with defined SIL 3/ PL e and with a defined SIL 3/ PL e of hard and software;

*The experience shows that most people want a simple “cookbook” of pre-planned solutions based on prescriptive standards, which do not account for new developments or technology and can be easily become outdated in general.*

 **Performance based SIS Design:** *Performance based standards (e.g. IEC 61511) do provide the freedom to select the technology and components for a specific solution. Example: SIL 3 certified elements are not required in a SIL 1 rated SIF.*

## SIS Installation, Validation & Comm.

### **IEC 61511:2016: Clause 15.2 SIS Validation, Validation & Commissioning**

*“To validate, through inspection and testing, that the installed and commissioned SIS achieve the requirements as stated in the SRS”*

 The experience shows that SIS installation activities being treated as same as any other control system (e.g. site acceptance test such as loop check).  
*Some of the SIS assumed performance requirements (e.g. SIF response time Vs SIF process safety time) can be only verified only upon site installation. Assumed IPL credited events being missed during validation*

 Upon installation, the SIF shall to be verified for its correct installation (e.g. no field bypass), function test of each SIF elements individually, validate SIF pipe to pipe for its correct function & confirming its response time, verify various assumed failure modes, validating IPLs

**The experience shows that SIF validation by validation by competent person reveals SIF functional gaps assumed during design Vs installation.**

## Managing SIS during plant O&M Phase

### IEC 61511-1: Clause 16.3.1.1: Periodic Proof Testing

*“Periodic proof tests shall be conducted using a written procedure to reveal undetected faults that prevent the SIS from operating in accordance with the SRS”*

 The experience shows that not all faults are self revealing by SIS elements. The O&M personnel are not confident to carryout the ‘proof test’ due to spurious trip concern. Plant authority’s power constraint of plant ‘availability’ takes priority over plant ‘reliability’ requirements assumed during SIS design stage. Lack of competent in understanding of SIS and its failure mode issues leads to mishandling of SIS elements

 Developing competency in SIS and well written & proven proof test procedures helps plant O&M personnel in operating & maintaining SIF, which would sustain the SIF design objectives definitely.

Evidences of SIS Proof test procedure and Proof test records are requirement in accordance with Singapore Safety Case Regime Regulation for MHI

## Managing SIS during plant O&M Phase

### IEC 61511-1: Clause 16.3.1.5: SIS Performance Monitoring

*“At some periodic interval, the frequency of testing shall be re-evaluated based on various factors including historical test data, plant experience and hardware degradation”*

-  Collecting real data related to the actual demand rate, failure rate and monitoring & analyzing SIS performance are not really practiced in operating plants.
-  Collection and analysis of failure data has many benefits including the potential to reduce maintenance costs if failures rates in operation are significantly lower than what were predicted during design. The experience shows that frequency of the proof test can be optimized based on plant real data such as demand and failure.
-  The experience shows that recent much matured plant specific analytical software functionality helps to optimize such efforts.

# Managing SIS during plant Modification

## IEC 61511-1: Clause 17.2: Analysis of Impact

Modifications in a plant due to design change is unavoidable. Such modification is subject to *“An analysis shall be carried out to determine the impact on functional safety as a result of the proposed modification”*

 To facilitate smooth plant operations i.e. to avoid ‘spurious trip’, some of the SIF elements are being bypassed either at field or at software without analysis of impact.

A change that may be considered minor by one individual (e.g. plant technician) may actually have a major impact to the overall process.

 Modification activity shall not begin until a Functional Safety Assessment (FSA) is completed and after proper authorization”.

# Functional Safety Assessment

## IEC 61511-1: Clause 5.2.6: Functional Safety Assessment (FSA)

*“Additional FSA activities can be introduced as new hazards are identified, after modification and at periodic intervals during operation”*

 During plant design & construction stage, the FSA at various stages are fulfilled by Contractors due to their contractual obligation. This means SIFs are designed & installed in accordance with requirements (perfect SIF).

 The experience shows that a well defined ‘Safety Lifecycle’ is not part of plant operation & maintenance phases. In the absence of Safety Lifecycle, the assumed operation & maintenance requirements (e.g. proof test, periodic FSA) of perfect designed SIF is in really question!!!

 The experience shows that the such periodic FSA helps to reveal the gap from design stage Vs operating stage, which would sustain the SIF design objectives definitely



# SIS Security Risk Assessment

## IEC 61511-1: Clause 8.2.4

*'A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS'.*

The SIS elements has ports for intended or unintended threat to control, alarm, spurious shutdown or prevent protective function dangerously. Example:

- HART enable transmitter without 'write' protection: Threat for sensing parameter modification
- Shared network between SIS and Control System: Threat for CPU parameter modification

*One of the recent incident is directly targeting a safety instrumented system (Triconex SIS) by modifying the SIS program via engineering workstation, the Triton malware caused operational disruption to a critical infrastructure facility in the Middle East. Source: Automation World*

The IEC 62443-3-3: Contains requirements for industrial automation and control systems, many of which are currently being assessed and certified to this standard.



# Management of Competency

## IEC 61511-1: Clause 5.2.2: Organization and Resources

*“Persons, departments or organizations involved in SIS safety life-cycle activities shall be competent to carry out the activities for which they are accountable.”*

While assessing competency, the functional safety experienced & trained personnel can be considered.

Alternatively, competency can be assessed in terms of a person’s qualifications, knowledge and experience on functional safety for the respective position and responsibility in line with requirements of IEC 61511.

Evidences of a competency management is a requirement in accordance with Singapore Safety Case Regime Regulation for MHI.

# SIS Element Design Issues

## Some of the SIS Design Constraints:

- Separation of Control System application Vs SIS application
- Separation of Control Network Vs SIS Network
- Segregation of Control Instruments and SIS Instruments
- Selection of Discrete Sensors Vs Smart Sensors
- Selection of Discrete Final Element Vs Smart Final Element
- Consideration of Redundancy i.e. 1ooN Vs 2ooN voting for SIS elements
- Selection of Similar technology Vs Diverse technology for SIS elements
- Consideration of de-energized to trip Vs Energized to trip
- Consideration of Independent Certified Elements Vs Manufacturer Declaration
- Consideration of Process Safety Time Vs Response Time
- Various credit for IPLs (alarm, control functions etc)

## SIS/SIF Modelling

### **IEC 61511:2016: Clause 11.9.2:**

In practice, most analysts/tools performing SIS/SIF modelling use either Fault Tree Model or Markov Model. These methods provide a clear way to express the reality of multiple system failure modes.

Often the models are created separately for each element of the SIF such as 'Sensor', 'Logic Solver' and 'Final Element' as these elements architecture are always in series in a SIF.

$$\text{PFD}_{\text{avg}} (\text{SIF}) = \text{PFD}_{\text{avg}} (\text{Sensor}) + \text{PFD}_{\text{avg}} (\text{Logic Solver}) + \text{PFD}_{\text{avg}} (\text{Final Element})$$

*A realistic level of detail that includes realistic component failure rates, component failure modes, effect of automatic diagnostic, common cause failures, proof test time & its effectiveness, repair time etc.,*

## Challenges in getting Failure Rate Data

### **IEC 61511:2016: Clause 11.9.3**

*“The reliability data used when quantifying the effect of random failures shall be credible, traceable, documented, justified and shall be based on field feedback from similar devices used in a similar operating environment”*

### **Failure Rate Estimation:**

Manufacturers' Field Return Data

Industry Database Consortium

Site Specific / Company Data Collection Systems

### **Failure Rate Estimation (e.g. FMEDA)**

Incomplete or missing safety manual. Missing realistic failure rate and failure mode data



## Equipment Failure Modes

### **IEC 61511:2016: Clause 3.2.18.1**

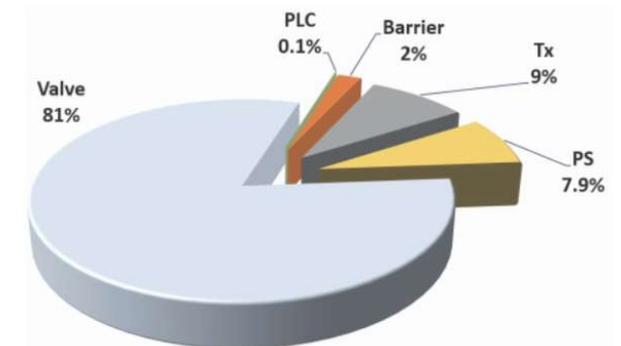
*“A failure mode may be defined by the function lost or the state transition that occurred”.*

A control system engineer’s first design priority is for a successful operation of all components for the life of the system. This makes sense in most systems because the failure mode is not relevant.

*In SIS, however, the failure mode is important. It makes a difference if the system experience a failure that causes a false trip i.e., “spurious trip” versus a failure that prevents automatic protection i.e., “fail dangerously”.*

# A Typical SIL Calculation (1001)

Sub-system	$\lambda_s$ per year	$\lambda_{DD}$ per year	$\lambda_{DU}$ per year	$\lambda$ per year = $1/MTBF$	MTBF (yrs)	MTBFs = $1/\lambda_s$ (yrs)	PFDavg 1001 = $\lambda_{DU}/2$	% of Total PFDavg	RRF = $1/PFDavg$	SFF	SIL Level
Tx	0.00800	0.0010	0.00080	0.00980	102	125	0.000400	9 %	-	91.8 %	SIL 2
Barrier	0.00159	0.0014	0.00019	0.00318	314	629	0.000095	2 %	-	94.0 %	SIL 3
PLC	0.00135	0.0001	0.00001	0.00146	685	741	0.000005	0.1 %	-	99.3 %	SIL 3
Valve	0.01370	0.0066	0.00720	0.02750	36	73	0.003602	81 %	-	73.8 %	SIL 2
Power Supply	0.00530	0.0000	0.00070	0.00600	167	189	0.000350	7.9 %	-	88.3 %	SIL 3
<b>Total (SIF)</b>	<b>0.02994</b>	<b>0.0091</b>	<b>0.00890</b>	<b>0.04794</b>	<b>21</b>	<b>33</b>	<b>0.004452</b>	<b>100 %</b>	<b>225</b>	<b>-</b>	<b>SIL 2</b>



Evidences of a SIL assessment records (PFD calculation and Fault tolerance assessment) is a requirement in accordance with Singapore Safety Case Regime Regulation for MHI.

**Thanks!**



**Any questions?**

You can find me at  
**[arvin@cisautomation.com.sg](mailto:arvin@cisautomation.com.sg)**