Delhi Section

Setting the Standard for Automatio

COLLATIVE CORRELATION O FUNCTIONAL SAFETY LIFE CYCL

M. ULAGANAT

McDermott International Pv

ISA-D: “Fertilizer , Food and Pharma Symposium-2019”

ABOUT THE PRESENTER

ISA D

Having 10 years of experience in field of Functional Safety involving Syste consulting, Engineering Software, Safety critical and High availability systems.

Involved in various stage of Functional Safety process and have executed Functional Safety projects in different regions.

Involved in upgradation of Failure data analysis associated with Product (Final Element accessories) based FMEDA certification.

Member of ISA committee.

EFNITIONS:

liability - Probability of a system to perform its intended functions satisfactorily, re by meeting the Design intent of System.

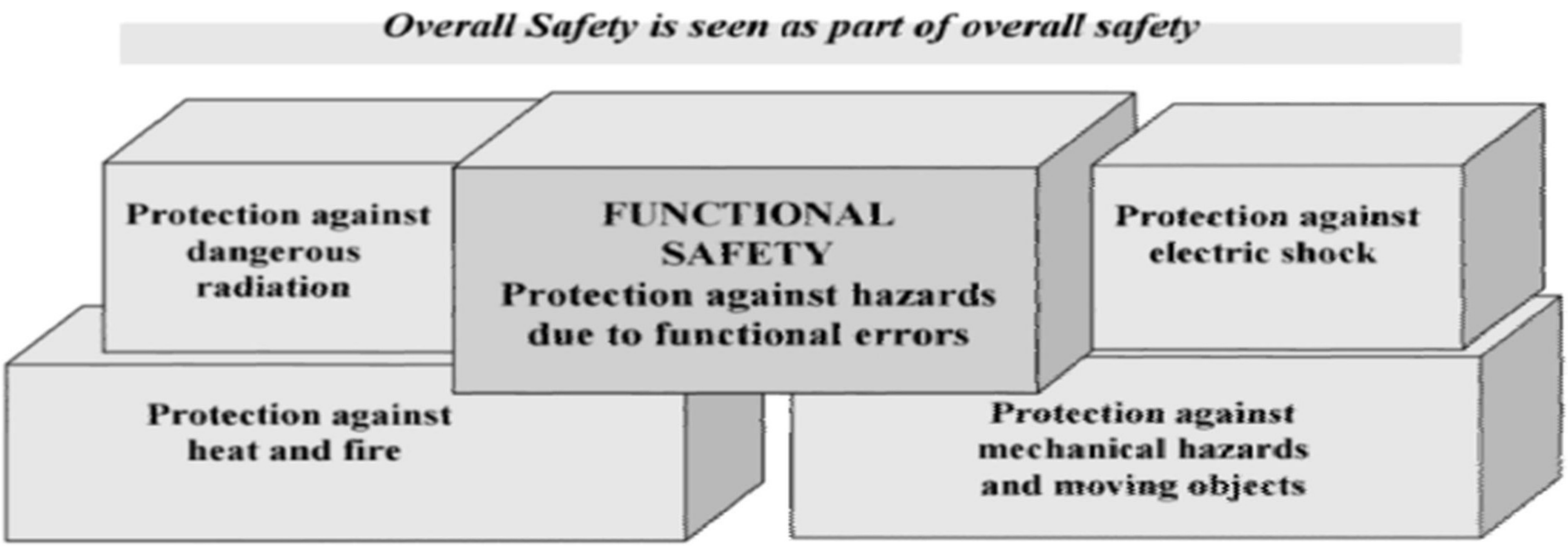
sk – Combination of probability of occurrence of a Hazard and severity of the zard, resulting in failure of system.

fety Instrumented Function – Specific single set of actions and the correspondin uipment needed to identify a single hazard and act to bring the system to safe stat

fety Instrumented System – Instrumented Systems used to implement one or re Safety Instrumented Functions. A SIS is composed of any combination of Sens Logic solver, Final element (s).

fety Integrity Level –Discrete level for specifying the probability of SIS satisfactor rforming SIF under all stated conditions and within stated time period.

FUNCTIONAL SAFETY:



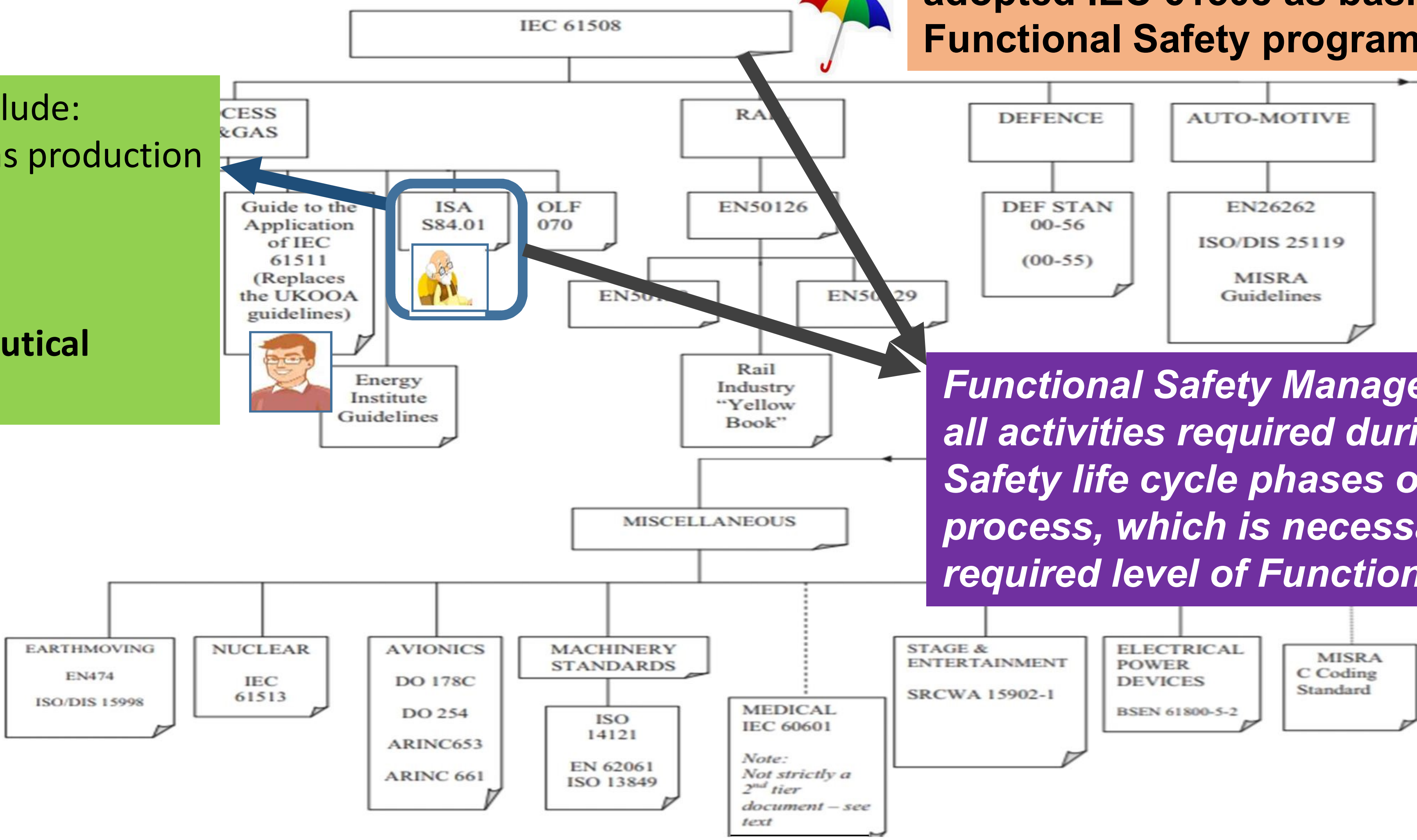
urpose of Functional Safety – Automatic Safety function to erform the intended function correctly or the system will fail a predictable (safe) manner.

STANDARDS:

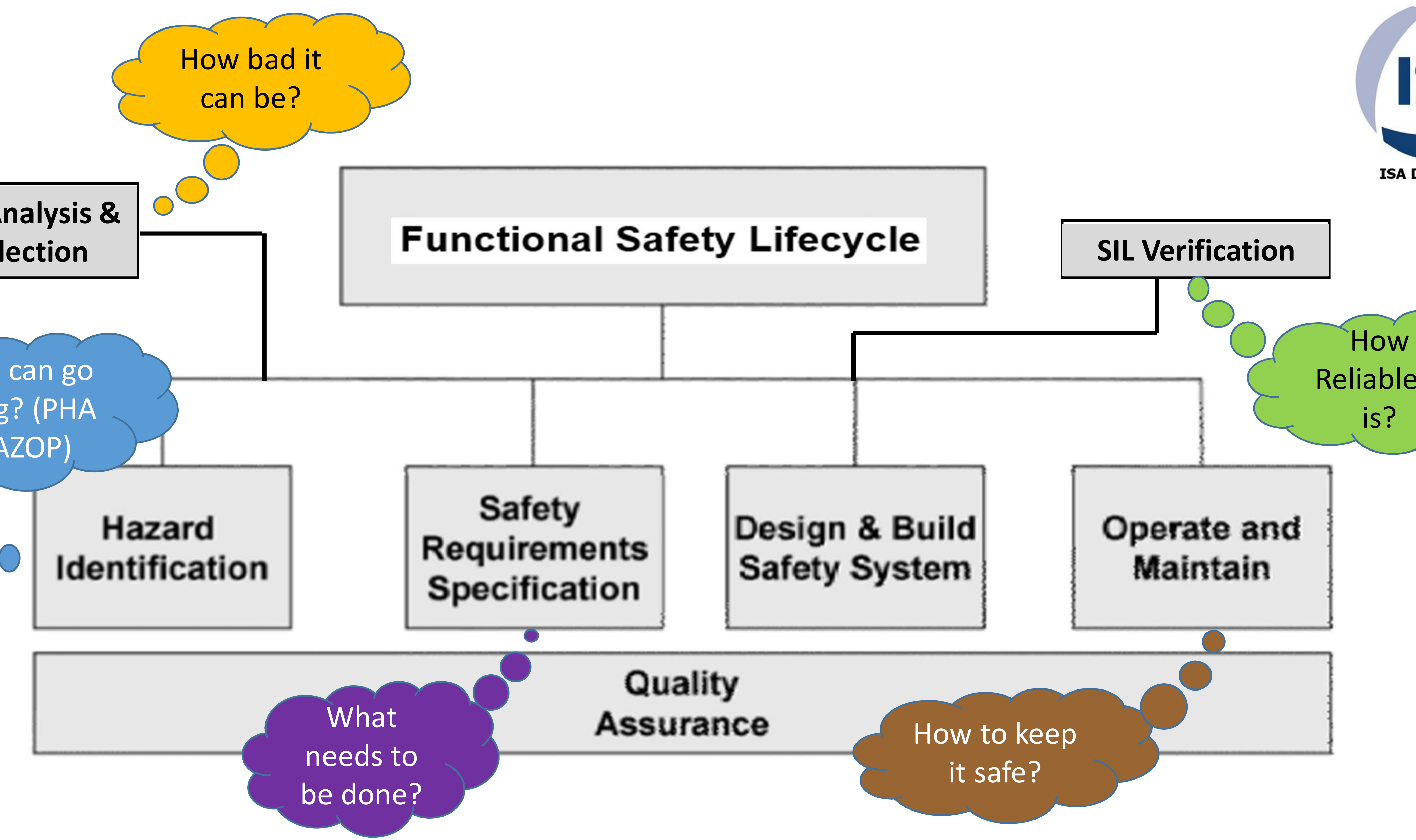
include:
l Gas production
g
cal

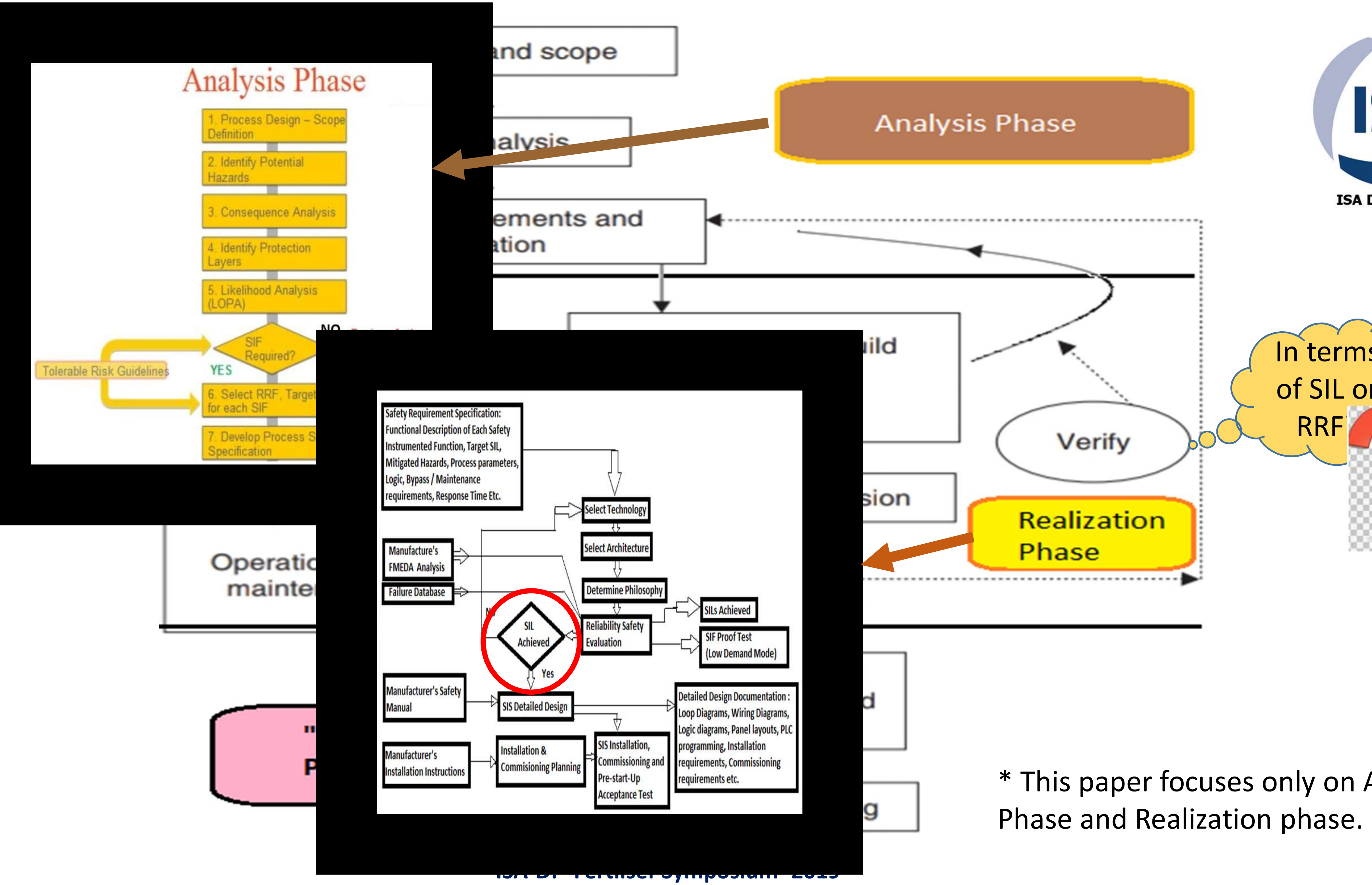
aceutical

Companies around the world adopted IEC 61508 as basis of Functional Safety programs.



Functional Safety Management governs all activities required during Functional Safety life cycle phases of a product / process, which is necessary in achievin required level of Functional Safety.


How bad it can be?
nalysis & lection
Functional Safety Lifecycle
SIL Verification
can go g? (PHA AZOP)
How Reliable is?
Hazard Identification
Safety Requirements Specification
Design & Build Safety System
Operate and Maintain
Quality Assurance
What needs to be done?
How to keep it safe?
ISA


Analysis Phase
1. Process Design – Scope Definition
2. Identify Potential Hazards
3. Consequence Analysis
4. Identify Protection Layers
5. Likelihood Analysis (LOPA)
SIF Required?
NO
YES
Tolerable Risk Guidelines
6. Select RRF, Target for each SIF
7. Develop Process S Specification
Analysis Phase
Realization Phase
Verify
In terms of SIL or RRF
Safety Requirement Specification: Functional Description of Each Safety Instrumented Function, Target SIL, Mitigated Hazards, Process parameters, Logic, Bypass / Maintenance requirements, Response Time Etc.
Select Technology
Select Architecture
Determine Philosophy
Manufacture's FMEDA Analysis
Failure Database
Reliability Safety Evaluation
SILs Achieved
SIF Proof Test (Low Demand Mode)
SIL Achieved
Yes
Manufacturer's Safety Manual
SIS Detailed Design
Detailed Design Documentation : Loop Diagrams, Wiring Diagrams, Logic diagrams, Panel layouts, PLC programming, Installation requirements, Commissioning requirements etc.
Manufacturer's Installation Instructions
Installation & Commisioning Planning
SIS Installation, Commissioning and Pre-start-Up Acceptance Test
* This paper focuses only on A
Phase and Realization phase.

SIL DETERMINATION METHODS

- Hazard Matrix
- Calibrated Risk Graph.
- Layer Of Protection Analysis (LOPA)
- Fault Tree Analysis
- Reliability Block diagrams.

SIL CLASSIFICATION TABLE

ISA 84.00.01

Safety Integrity Level	Risk Reduction Factor	PFD_{AVG} : Average
SIL 4	100,000 – 10,00	[illegible]
SIL 3	10,000 - 1,000	[illegible]
SIL 2	1,000 - 100	$>=10^{-3}$ to $<10^{-2}$
SIL 1	100 to 10	$>=10^{-2}$ to $<10^{-1}$

As per table, RRF / PFD avg is governing factor for SIL

ISA-D: “Fertliser Symposium -2019"

Layer Of Protection Analysis:

- LOPA is a process to evaluate risk with explicit risk tolerance fo specific consequences.

- LOPA is a semi-quantitative method, which ranks somewhere between Risk Graph method and Markov Analysis.

- LOPA method is solely dependent on values used for initiating event frequency and Independent Protection Layer (IPL).

- LOPA is order-of-magnitude method, however this only reflects tolerance of error, not tolerance of uncertainty.

LOPA – METHODOLGY

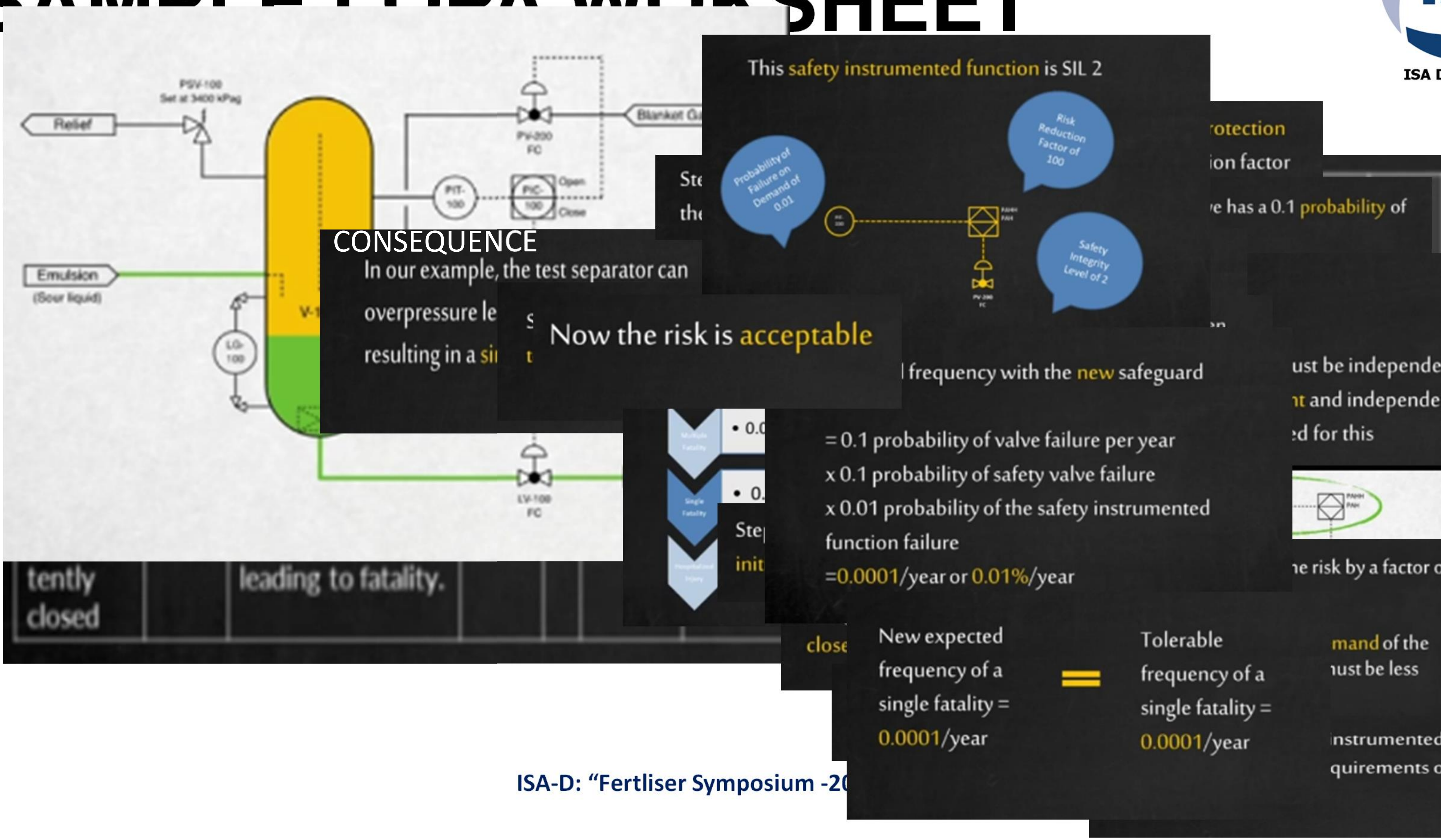
dentify initiating event (s) (IE) with potential to lead to defined Hazard scena

dentify Enabling conditions (EC), IPLs, Con
itiating event.

Multiply each IE by probability risk reduction
pply.

dd the resulting individual scenario frequencie rio
equency.

SAMPLE LOPA WOKSHEET



TYPICAL FMEDA CERTIFICATE

exida

The manufacturer may use the mark:

CERTIFIED • IEC 61508 • SIL 3 CAPABLE

sion 1.2 October 16, 2019
urveillance Audit Due
October 31, 2022

AF ANSI
ISO/IEC 17065
DUCT CERTIFICATION BODY
#1004

Certificate / Certificat
Zertifikat / 合格証

MEW 1901146 C006

exida hereby confirms that the:

Diaphragm Actuator
Model 2800, 3800, 3300 and 2900
MOTOYAMA ENG. WORKS, LTD
Ohira, Miyagi, Japan

Have been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 2_H Device

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Safety Function:
The Diaphragm Actuator will move to the designed safe position per the actuator design within the specified safety time.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

exida Certification

Evaluating Assessor

Kiyoshi Takai

Certifying Assessor

Page 1 of 2

Model 2800, 3800, 3300 and 2900

Diaphragm Actuator

Certificate / Certificat / Zertifikat / 合格証

MVG 1901146 C006

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 2_H Device

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Systematic Capability:
The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:
The SIL limit imposed by the Architectural Constraints must be met for each element. This device meets *exida* criteria for Route 2_H.

IEC 61508 Failure Rates in FIT*

2800, 3800, 3300 Direct Acting

Device	λSD	λSU	λDD	λDU
Spring Return	0	506	0	121
Spring Return with PVST	501	5	86	35

2800, 3800, 3300 Reverse Acting

Device	λSD	λSU	λDD	λDU
Spring Return	0	578	0	147
Spring Return with PVST	572	6	104	43

2900 Diaphragm Actuator

Device	λSD	λSU	λDD	λDU
Spring Return	0	506	0	160
Spring Return with PVST	501	5	122	38

* FIT = 1 failure / 10^9 hours
† PVST = Partial Valve Stroke Test of a final element Device

SIL Verification:
The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH/PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: MEW 1901146 R012 V1 R4 (or later)

Safety Manual: MSE-B9002B (or later)

exida

80 N Main St
Sellersville, PA 18960

T-109, V3R2

Page 2 of 2

ISA D

SIL Verification:

$$PFD_{SIF} = PFD_{PT} + PFD_{in} + PFD_{PLC} + PFD_{pw} + PFD_{out} + PFD_{sol} + PFD_{act} + PFD_{valve}$$

Element	PFD
Pressure transmitter	0.010518
PLC – input	0.004388
PLC – main processor	0.000051
PLC – power supply	0.000002
PLC – output	0.002194
Solenoid	0.010254
Actuator	0.005995
Valve	0.046975

$$PFD_{SIF} = 0.080376$$

1.3.2 Safety Requirements Specification

The key objective of writing the safety requirements specification is to make sure that the specification is complete and understandable. The safety requirements specification will be the primary input for the conceptual design of the Safety Instrumented Functions. If the specification is not complete the Safety Instrumented Functions may not be designed correctly and the achieved safety integrity may not be enough (under design) or too much (over design).

The IEC 61511 standard provides a clear list of issues to be addressed in the safety requirements specification. The use of a template or templates is highly suggested to assure completeness and for consistency purposes.

1.3.3 SIL Verification

The objective of calculating the Achieved Safety Integrity Level is to determine the amount of risk reduction a Safety Instrumented Function, in its conceptual design, provides. If the achieved Safety Integrity Level meets or exceeds the Target Safety Integrity Level the conceptual design can be passed on to the detail design phase where the Safety Instrumented Functions are implemented.

The functional safety standards reference various methods that can be used to perform the reliability analyses from which the Achieved SIL is obtained. The most popular reliability analysis techniques listed in an increasing order of accuracy are:

- Simplified equations
- Fault tree analysis
- Markov modeling

There have been many debates and publications [8], [9] on what technique should be used for the reliability analysis with regard to Safety Instrumented Functions especially since different techniques may yield different results. Detailed analysis has shown, however, that the different techniques are based on different assumptions, consequently leading to different results [10]. Therefore, the user of any of these techniques should be aware of the assumptions inherent to the technique.

Another key issue in the reliability calculations is the reliability data to be used in the SIL verification [11], [12]. Especially when comparing results from different calculations it is key that the data source used in the calculations is identical. Data sources may vary by orders of magnitude with respect to equipment failure rate data.

1.4 Market Drivers

The release and adoption of new functional safety standards provide a means for manufacturers of equipment to qualify them for safety applications. These provide a framework for both equipment vendors and end users to justify the use of standards equipment for safety. Many operating companies have also found that adopting a lifecycle approach as recommended by these functional safety standards has had the effect of reducing both capital and operational expenditure [13].

ISA D

MPACTS :

n SIL level i.e. between Target an

sibility of excluding Higher order

nce betw

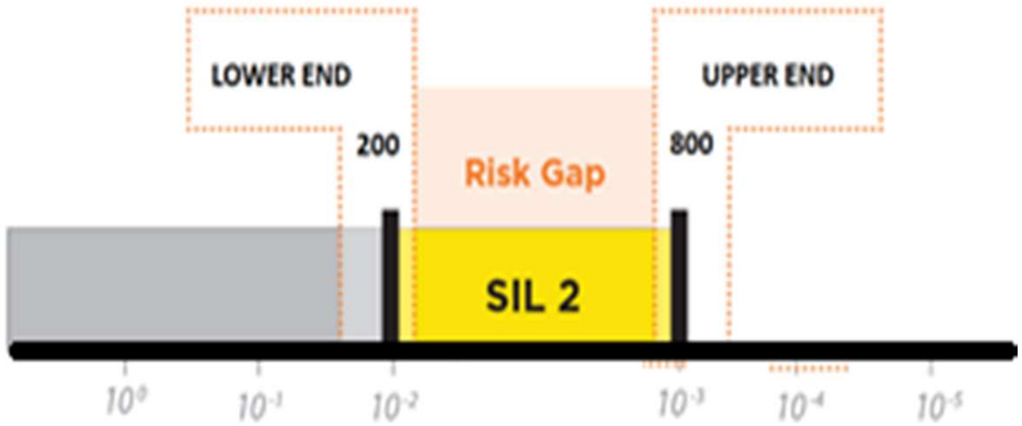
la

e

lerable

Design of SIF shall suffer because of existing uncertainties (mainly RRF) of SIL assessment process.

RECOMMENDATION:



SIL Level	RRF		PFDavg	
	Lower End	Upper End	Lower End	Upper End
SIL 1	NA			
SIL 2	200	800	5.00E-03	1.25E-03
SIL 3	2000	8000	5.00E-04	1.25E-04

ASON FOR CONSIDERING TOLERANCE IN WER END OR UPPER END

pe of technique employed in SIL determination and SIL verification.

lerance of error in LOPA due to Initiating event frequency estimates, Risk duction for each Protection layers, enabling conditions and conditional odifiers and true independence of each or those values from all of other mbers. Approximate % of error tolerance limits estimated is around +/- 30%

ta that are been collected for calculating Risk Tolerability criteria for plant vel data and FMEDA analysis, proven-in-use method for Product based rtification.

ONCLUSION

If No Explosion has been occurred in a Plant, doesn’t means Plant is Safe
Reliable”. Even though occurrence of such incidents may be rare, but it sho
not occur. Always it is better to safeguard a plant from future awaited
catastrophic events, if higher level of functional safety has been followed.

Thank You!

Any Questions?