SIL Awareness

Introduction to Safety Life-cycle IEC-61508 and IEC-61511

Today's Objective

- Do you aware of the requirements of IEC 61508/61511 compliance for the trips & alarms installed within your facilities/asset?

- The course will provide you with a clear understanding of the Best Practice requirements for SIS operating as part of your plant's layers of protection

Today's Objective

This short course is designed to give you an appreciation of the following

- A brief introduction to the IEC 61508 / 61511 standards and the guidance for operating, maintaining and managing Safety Instrumented Systems (SIS)
- An introduction to risk and the concept of Safety Integrity Level (SIL)
- An overview of designing a Safety Instrumented Function
- The importance of testing and maintaining Safety
- The need for documentation and records to support the operational basis of safety

Today's Objective

- IEC 61508 - "Functional Safety: Safety Related Systems" released in 2005
- IEC 61511 - "Functional Safety: Safety Instrumented Systems for the Process Industry Sector" Published in 2003
- ISA 84.01-2003 - "Functional Safety: Safety Instrumented Systems for the Process Industry Sector" Identical to IEC 61511 with inclusion of grandfather clause published in October 2003.

Today's Objective

- What is the SLC..? IEC 61508..? IEC 61511..? SIS..? SIF..? SIL..?
- What can happen? – Identify the Risk
- How bad can it be? – Assess the Risk
- What to do about it? – Reduce the Risk
- How well did we reduce? – Verify solution

Today's Objective

How Safe Do I Need to Be?

The global importance of SIL (Safety Integrity Levels) has grown substantially in the oil/gas, petrochemical and other process industries, however, for many end-users, systems integrators, and product vendors; SIL is still a somewhat ambiguous concept that often is misinterpreted and incorrectly implemented.

Today's Objective

Safety-related system;

A control-system or devices are deemed to be safety related if it provides functions which significantly reduce the risk of a hazard, and in combination with other risk reduction measures, reduces the overall risk to a tolerable level, or if it is required to function to maintain or achieve a-safe-state for the equipment under control (EUC).

Problems with the use of SIL

There are several problems inherently for the implementation of Safety Integrity Levels [SIL]. These can be summarized as follows...

- Poor harmonization of definition across the different standards bodies which utilize SIL
- Process-oriented metrics for derivation of SIL
- Estimation of SIL based on reliability estimates
- System complexity, particularly in software systems, making SIL estimation difficult to impossible

Section-1

Overview

Functional Safety Management

Functional Safety Management

Objectives;

- Specify management and technical activities during the Safety Lifecycle to achieve and maintain Functional Safety
- Specify responsibilities of persons and organizations
- Extend an existing and monitored quality system
  - Plan, execute, measure and improve

61508 and 61511 Versions of FSM

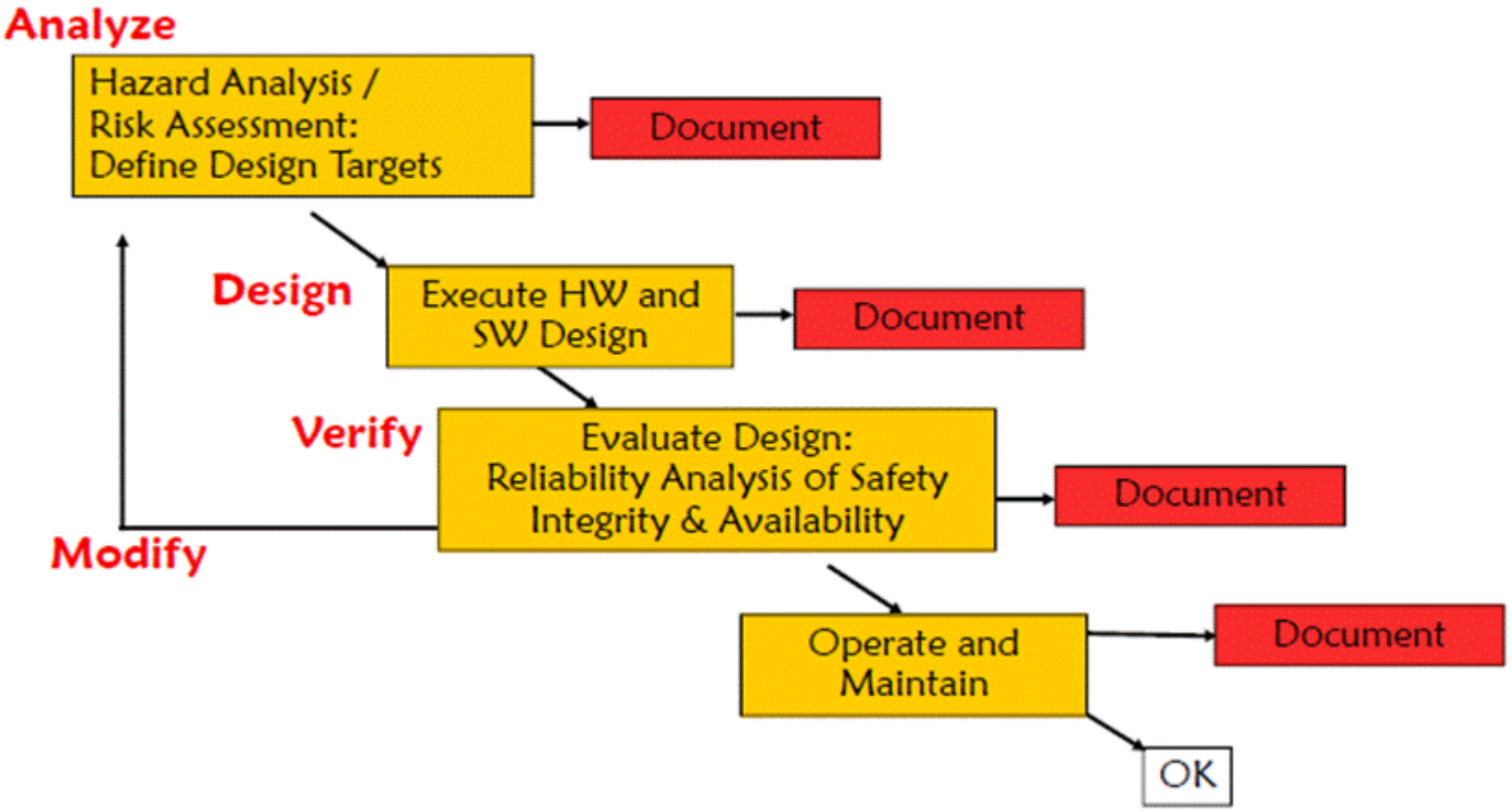
- Since FSM focuses on procedures, the standards provide a good reference
- 61508 covers everything including safety system hardware and software development
  - Part 1 Clause 6 lays out details of FSM
  - Broad coverage can make application challenging
- 61511 focuses on the process owners and safety system users
  - Part 1 Clause 5 lays out details of FSM
  - Narrower coverage makes application more manageable

Key Issues

- Functional Safety Management
  - Safety Planning – create a FSM Plan
  - Roles and Responsibilities
  - Personnel Competency
  - Documentation, Documentation Control
  - Functional Safety Verification and Assessment
  - Documented Processes

A FSM Plan describes

The Safety Lifecycle for the Project



Components of a FSM Plan

- Steps and sequence of work activities
  - Roles and responsibilities
  - Personnel competency
  - Documentation structure
  - Verification tasks for each step

- Safety Requirements Specification development plan
- Design guidelines and methods
- Verification and Validation plans
- Operation and maintenance guidelines
- Management of Change procedures
- Functional safety assessment plan

Roles and Responsibilities

- Must be clearly delineated and communicated
- Each phase of SLC and its associated activities
- One of the specifically noted primary objectives of functional safety management

Personnel Competency

- Ensure that staff “involved in any of the overall or software SLC activities are competent”
- Addressed specifically in Annex A, IEC61508
- Training, experience, and qualifications should all be assessed and documented
  - System engineering knowledge
  - Safety engineering knowledge
  - Legal and regulatory requirements knowledge
  - More critical for novel systems or high SIL requirements

Personnel competency

Certified Functional Safety Expert (CFSE) Program

- Operated by the CFSE Governing Board
  - To improve the skills and formally establish the competency of those engaged in the practice of safety system application in the process and manufacturing industries

- Certification audited by *Exida* Certification

Personnel competency

Certified Functional Safety Expert (CFSE) Program

- Types of Exams
  - Application – Process Industries
  - Application – Machine Industries
  - Developer – Software
  - Developer - Hardware

Personnel competency

Certified Functional Safety Expert (CFSE) Program

- Resources Available:
  - On-line Training
  - Study Guide
  - Reference Books

Certified Functional Safety Expert
Application Engineering-Process
Study Guide

exida

Documentation Objectives

- What needs to be documented?
- Any information to effectively perform:
  - Each phase of the safety lifecycle
  - Management of functional safety
  - Verification and Validation
  - Functional Safety Assessment

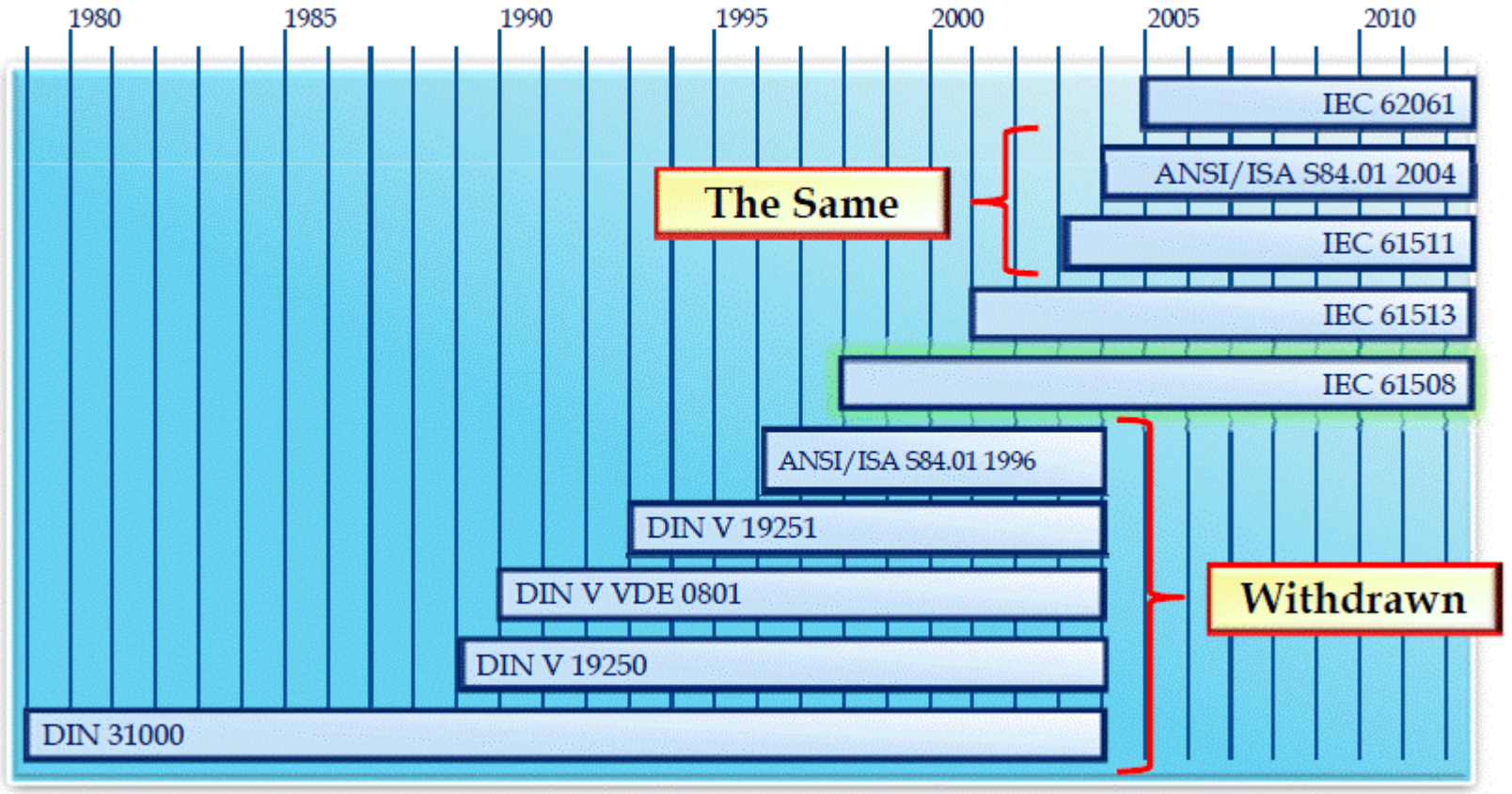
IEC 61511 Functional Safety Assessment

- Does the safety system meet spec and actually achieve functional safety (freedom from unacceptable risk)
- Independent team; one competent senior person not involved in the design as a minimum
- Should be performed after the stages below and MUST be done at least at stage 3
  - Stage 1 – After hazard and risk assessment and safety requirements specification
  - Stage 2 – After SIS design
  - Stage 3 – After commissioning and validation (before the hazard is present)
  - Stage 4 – After experience in operation and maintenance
  - Stage 5 – After modification

Section -2

Overview Safety Standards

Safety Standards

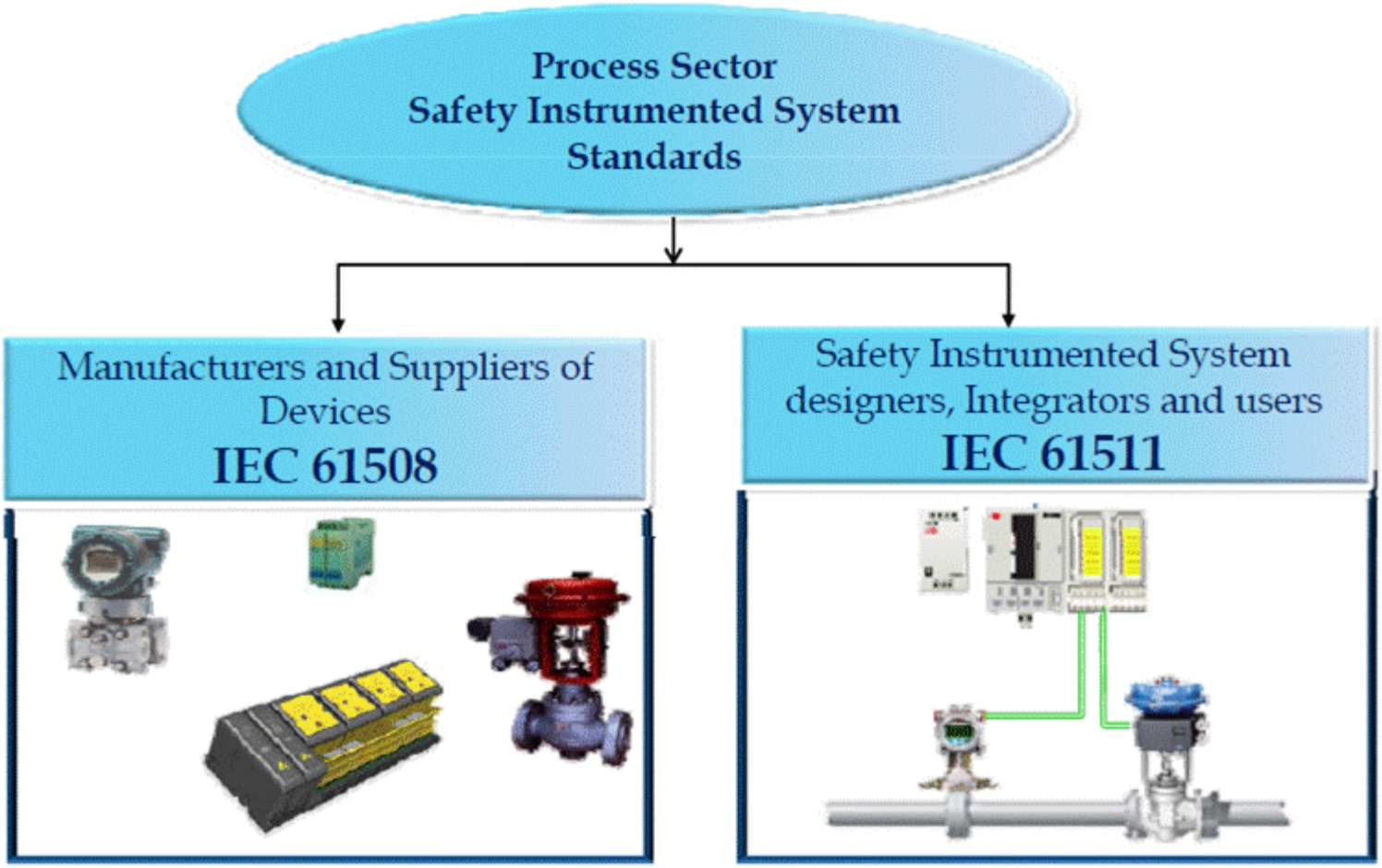


Global Standards

Global Standards for Functional Safety

Global Standards

Relationship IEC-61508 & 61511



IEC - 61508

- Targets Suppliers;
- Requirements for suppliers of process control and instrumentation for component / subsystem Safety
- End Users seek suppliers with products certified to this standard by reputable certifying agency

IEC - 61511

- Targets End Users, Engineering Contractors and Integrators in process industries
- Covers the entire SIS Life Cycle
  - Risk Analysis
  - Performance based design
  - Operations and Maintenance
- Performance NOT Prescriptive End user applications
  - Not typically certified
  - Independent Functional Safety Assessment
- 3 sections
  - Requirements
  - Guidelines
  - SIL Selection

Key Aspects of IEC 61511

- Safety Integrity Levels (SIL)
  - Reliable Hardware with predictable failure rates

> Random Failure

- Safety Lifecycle
  - Safety Management with controlled and systematic processes

> Systematic Failure

Standards and Practices

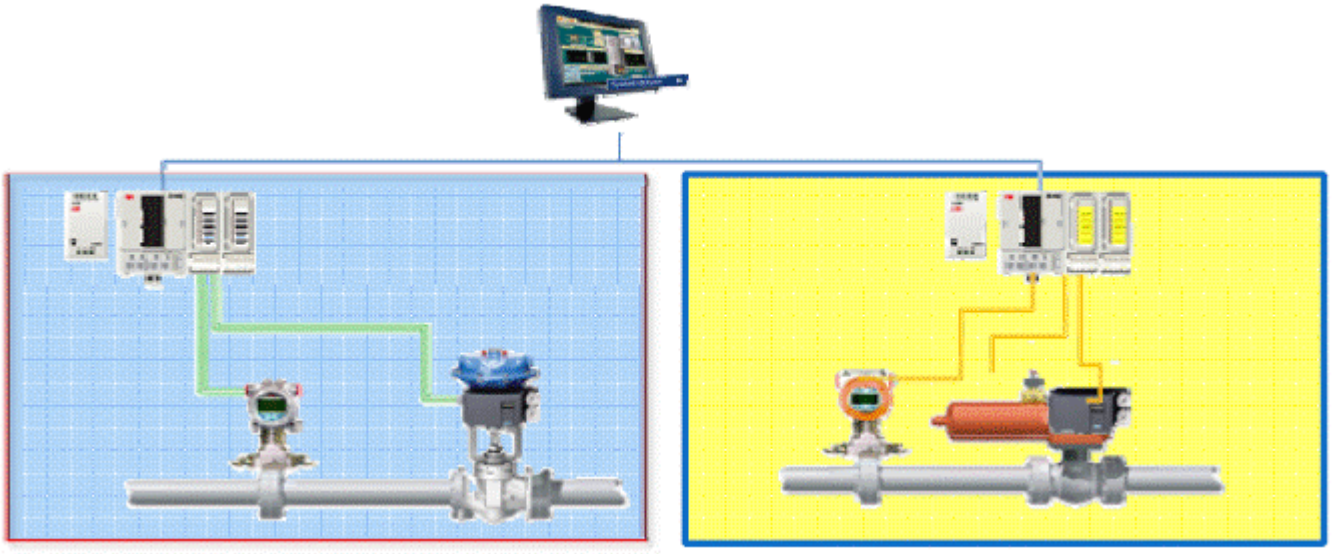
- Safety Instrumented Systems (General)
  - DIN V 19250
  - DIN VDE 0801 – Principles for Computers in Safety Related Applications
  - EN 292 – Safety of Machinery
  - EN 60240 – Safety of Machinery – Electrical Equipment of Machines
  - IEC 62061 – Safety of Machinery
- General Engineering and Management
  - ISO 9000 – Quality Management and Quality Assurance Standards
  - NFPA 70 – National Electrical Code
  - IEC 61131 – Programmable Controllers
  - UL 508 – Industrial Control Units
- Hazard and Risk Assessment
  - API RP 752 – Recommended Practice for Management of Hazards Associated with Locations of Process Buildings
  - IEC 60300 – Dependability Management
  - EN 1050 – Safety of Machinery – Principles of Risk Assessment

Standards and Practices

- Application Specific – Alarm Management
  - ISA 18.1 – Annunciator Sequence and Specifications
- Application Specific – Offshore Production
  - API RP 14-C – Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms
- Application Specific – Burner Management
  - NFPA 8501 – Standard for Single Burner Boiler Operation
  - NFPA 8502 – Standard for the Prevention of Explosions/Implosions in Multiple Burner Boilers
  - API RP 556 – Recommended Practice for Instrumentation and Control Manuals for Refinery Service – Fired Heaters and Steam Generators
  - DIN VDE 0116 – Electrical Equipment for Furnaces
  - FM 7605 – Programmable Logic Controller Based Burner Management Systems
  - UL 372 – Burner Control Units

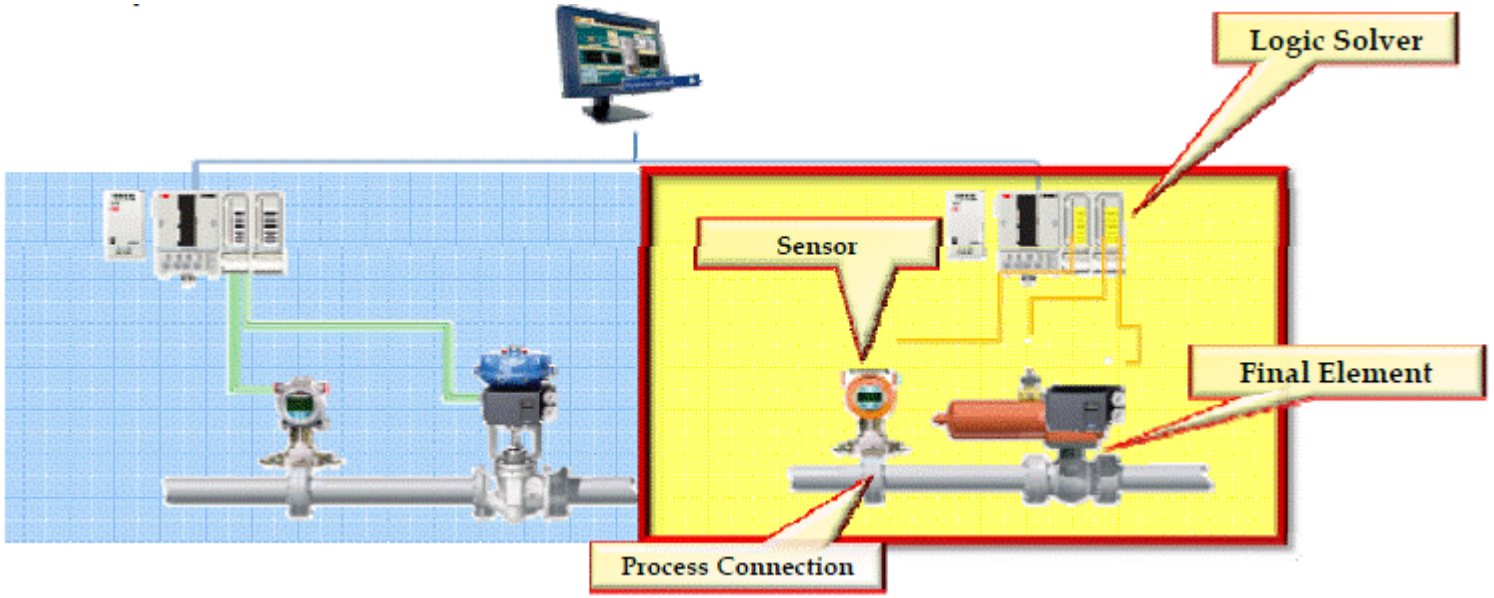
Definition: BPCS

- In the IEC Standards, a DCS is termed as “BPCS”
  - Basic Process Control System
  - A BPCS operates under dynamic conditions with outputs constantly being adjusted to for control



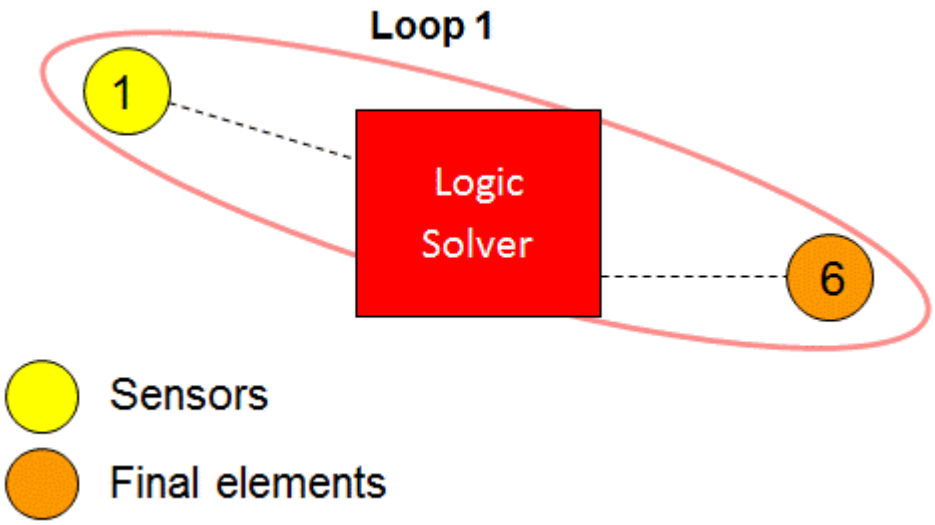
Definition: SIS

- Safety Instrumented System: “From Pipe to Pipe”
  - A SIS is a set of components executing Safety Instrumented Functions (SIF)
  - A SIS is typically Passive and takes action when a dangerous condition is detected and mitigate the consequences, automatically takes the process to a safe state



Definition: SIF

- Safety Instrumented Function:

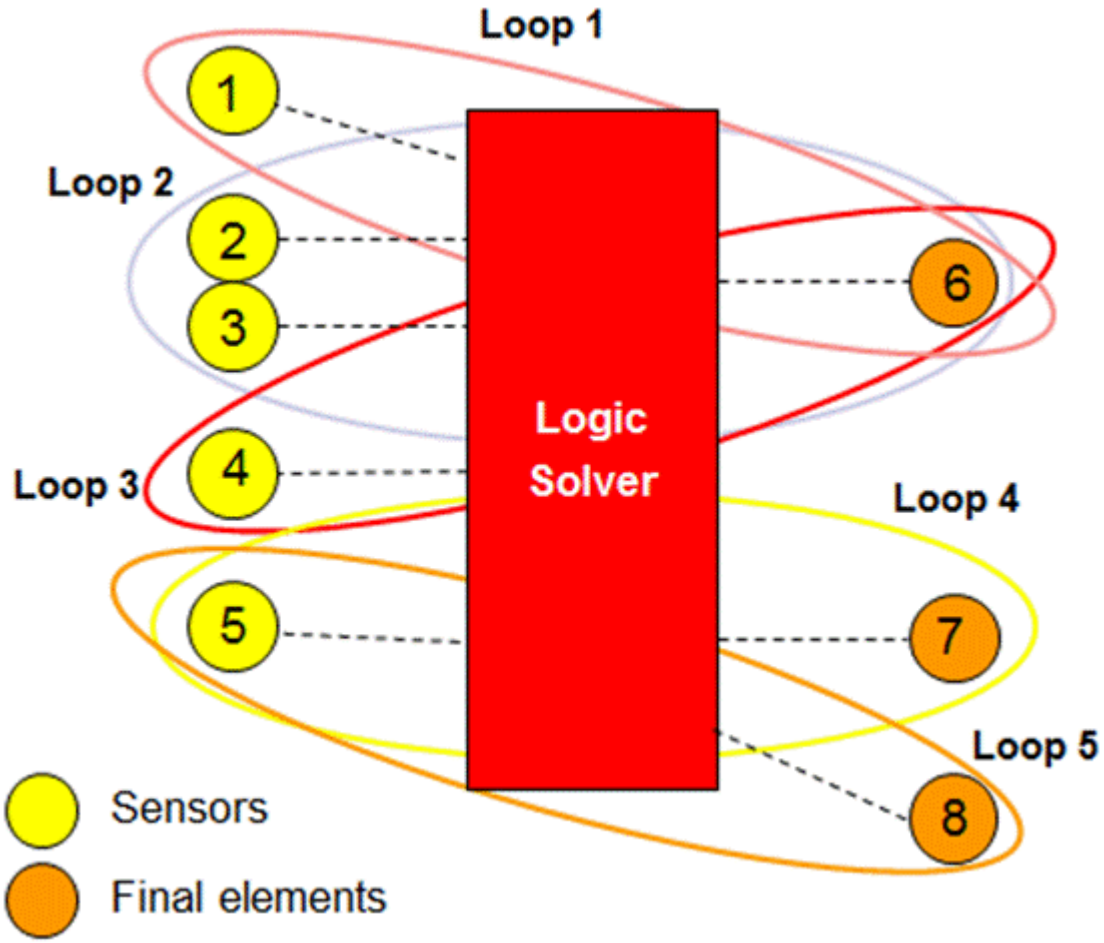


"Safety function with a specified SIL which is necessary to achieve functional safety and which can be either a safety instrumented *protection function or* a safety instrumented *control function.*"

IEC 61511 Part 1 (3.2.71)

Definition: SIF

- Safety Instrumented Function:



Definition: SIF

- Specific *single set of actions and the corresponding* equipment needed to identify a *single hazard and act to* bring the system to a safe state.
- Different from a SIS, which can encompass multiple functions and act in multiple ways to prevent multiple harmful outcomes. One SIS may have multiple SIF with different individual SIL, so it is incorrect and ambiguous to define a SIL for an entire safety instrumented system

Definition: SIF

Safety Instrumented Function, example:

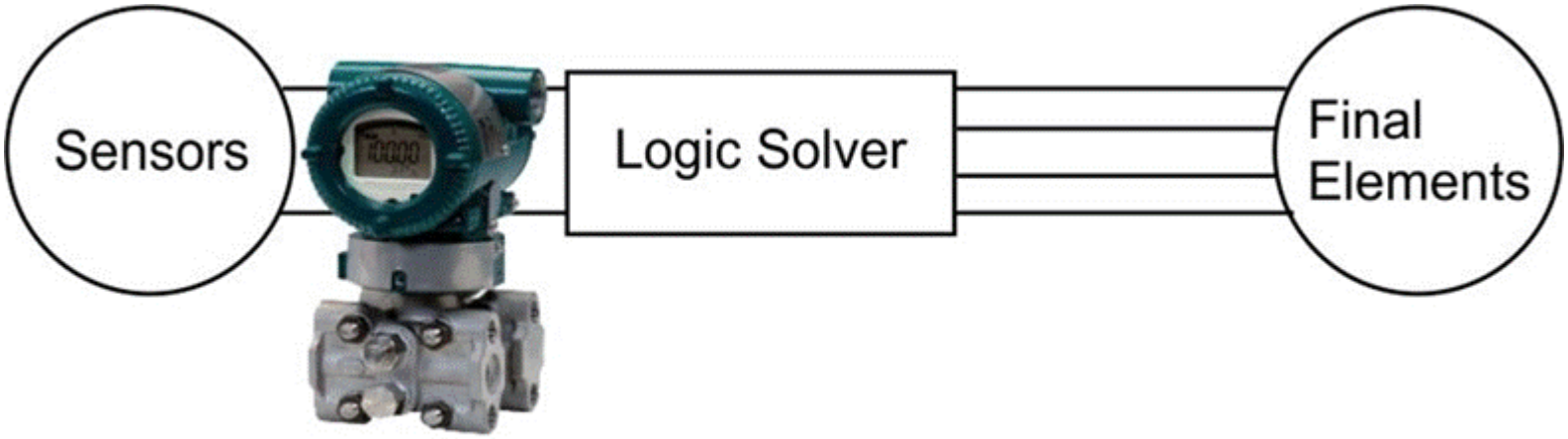
- On detecting high temperature, prevent column rupture by shutting off steam flow to re-boiler
- On detecting high pressure, prevent tank rupture by opening valve to relief system
- On detecting high level, open drain valve to direct excess liquid to waste sump to reduce environmental damage
- On detecting a fire, issue alarms to minimize damage and possible injury

(This last item is not a complete SIF since it does not achieve a safe state. The final actions must be included)

Definition: SIF

SIF – Sensor;

Like a control system, a safety system has sensors. In the process industries sensors measure process parameters including pressure, temperature, flow, level, gas concentrations and other measurements. In the machine industries sensors measure human proximity, operator intrusion into a dangerous zone and other protective parameters.



Definition: SIF

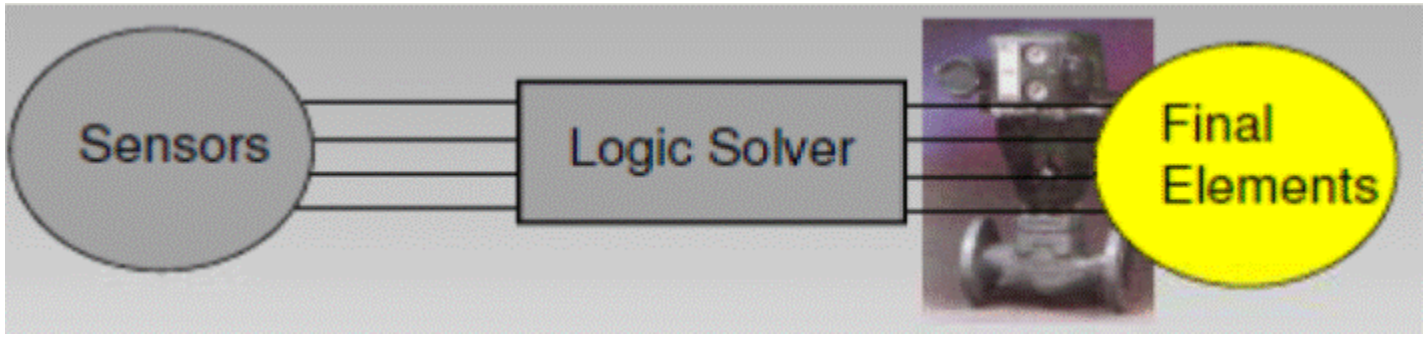
SIF – Logic Solver;

A safety system also has a logic solver, typically a controller, that reads signals from the sensors and execute preprogrammed actions to prevent or mitigate a process hazard. The controller does this by sending signals to final elements

Definition: SIF

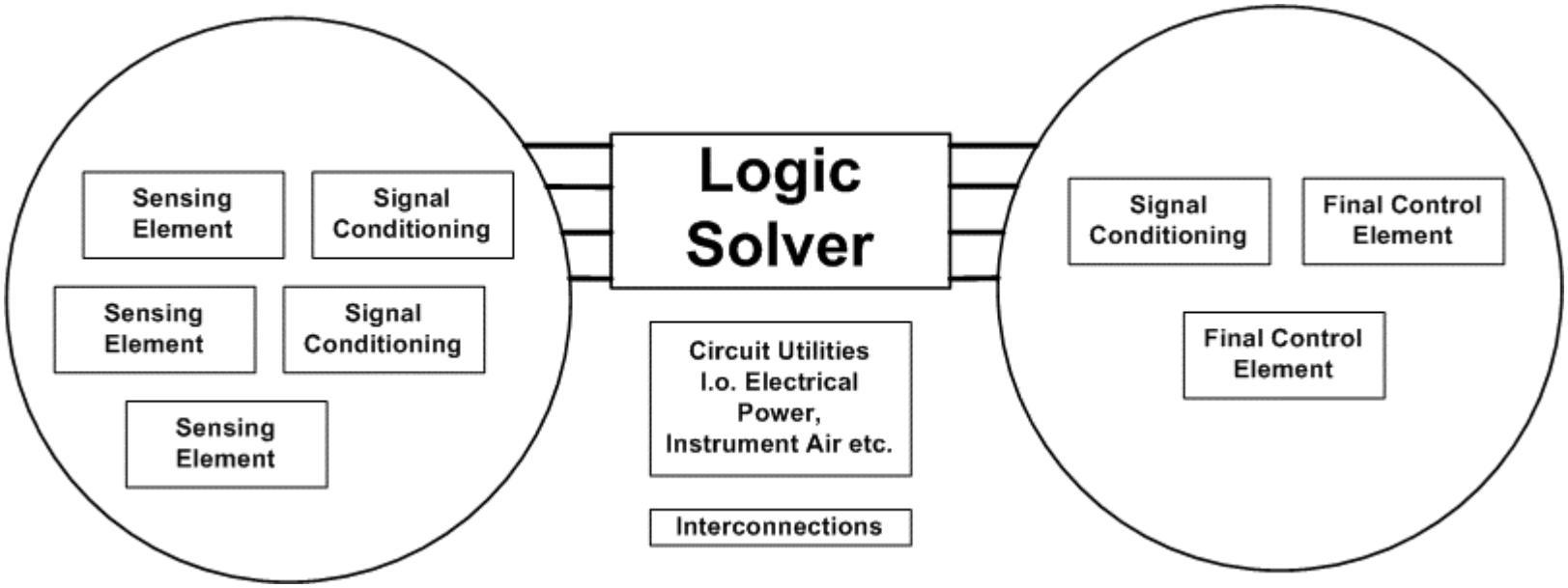
SIF – Final Element;

The final element in a SIF is what acts to bring about the safe state. This is often a remote actuated valve in the process industries while in machine safety it could likely be a clutch/brake assembly.



Definition: SIF

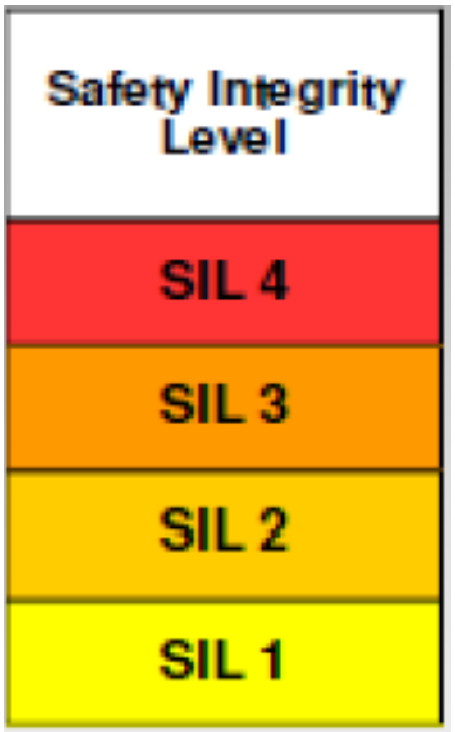
SIF – Implementation;



The actual implementation of any single safety instrumented function may include multiple sensors, signal conditioning modules, multiple final elements and dedicated circuit utilities like electrical power or instrument air

Definition: SIL

Safety Instrumented Level:



"Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. SIL 4 has the highest safety integrity and SIL 1 the lowest."

IEC 61511 Part 1 (3.2.74)

How well the SIF performs its job of managing risk

Section – 3

SAFETY LIFECYCLE [SLC]

What is SLC [Safety Lifecycle]

Safety life-cycle (SLC) is an engineering process designed to optimize the design of the SIS and to increase safety.

Objectives;

- A Safer Plant;
- Decrease Engineering, Operations & Maintenance Costs; and
- Increased Process Up-Time

What is SLC [Safety Lifecycle]

A complete safety life-cycle can be categorized into three major phases:

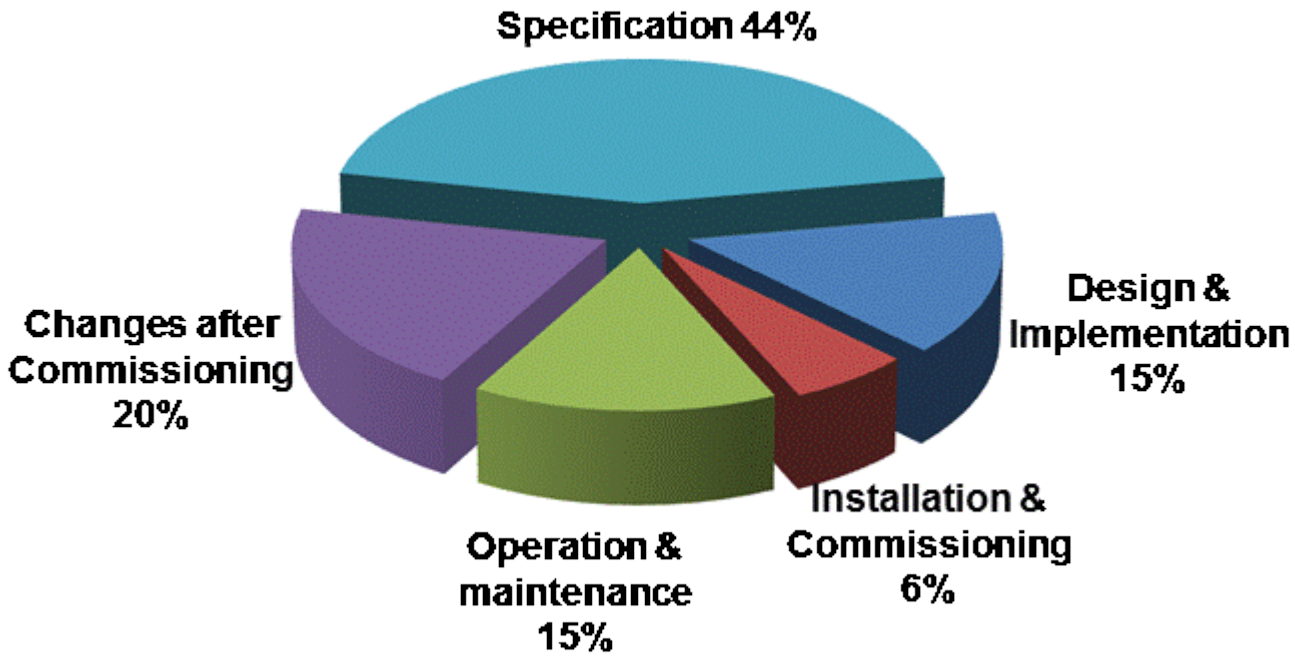
- Analysis phase → How safe do we need to be..?
- Realization phase → how good the safety can be achieved, and
- Operation Phase → how to sustain the safety..?

SLC [Safety Lifecycle]

- Accidents involving control / SIS
- Safety Lifecycle Objectives
- IEC 61508 and IEC 61511 (ISA 84.01) versions of the Safety Lifecycle
- Analysis Phase
- Realization Phase
- Operation Phase
- Personnel Competency

Accidents involving control / SIS

HSE study of accident causes involving control systems



"Out of Control: Why Control Systems go Wrong and How to Prevent Failure," U.K.: Sheffield, Heath and Safety Executive, 1995 (Ed 2, 2003)

Accidents involving control / SIS

Recent Accident History Driving Full SLC;

Buncefield (UK)

- Oil storage depot explosion on 11 December 2005
- 40 people injured
- Cost estimated close to £1 Billion ($1.6 Billion)

  "The safety systems in place to shut off the supply of petrol to the tank to prevent overfilling failed to operate."

Recommendation 11*: We recommend that the regulatory regime for major hazard sites should ensure *proper assessment of safety integrity levels (SILs) through the development of appropriate standards and guidance for determining SILs.*

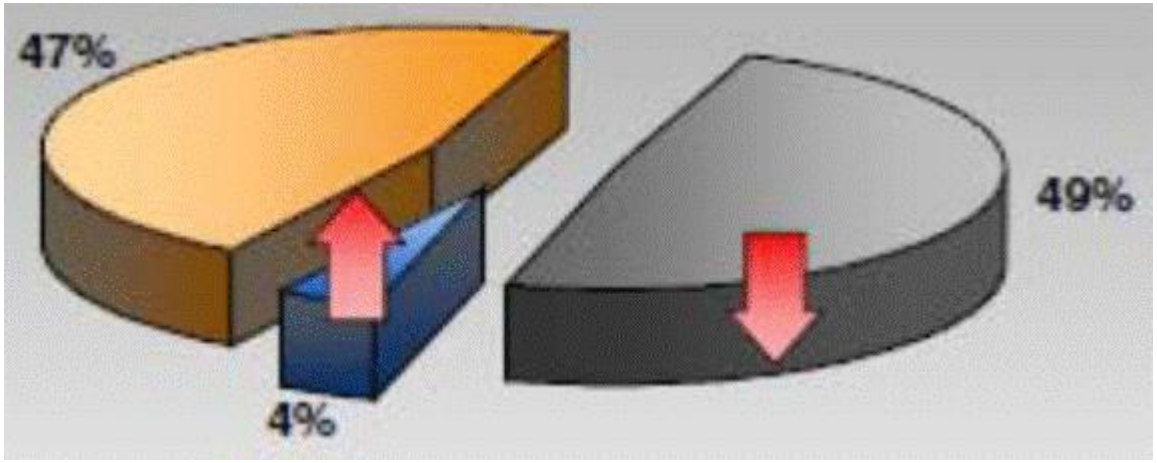
* Reference: The Buncefield Incident, 11 December 2005 – The final report of the Major Accident Investigation Board (Volume 1), 2008

SLC - Objectives

- Build safer systems that do not experience as many of the problems of the past
- Build more cost effective systems that match design with risk
- Eliminate “weak link” designs that cost much but provide little
- Provide a global framework for consistent designs

SLC – Practical Result

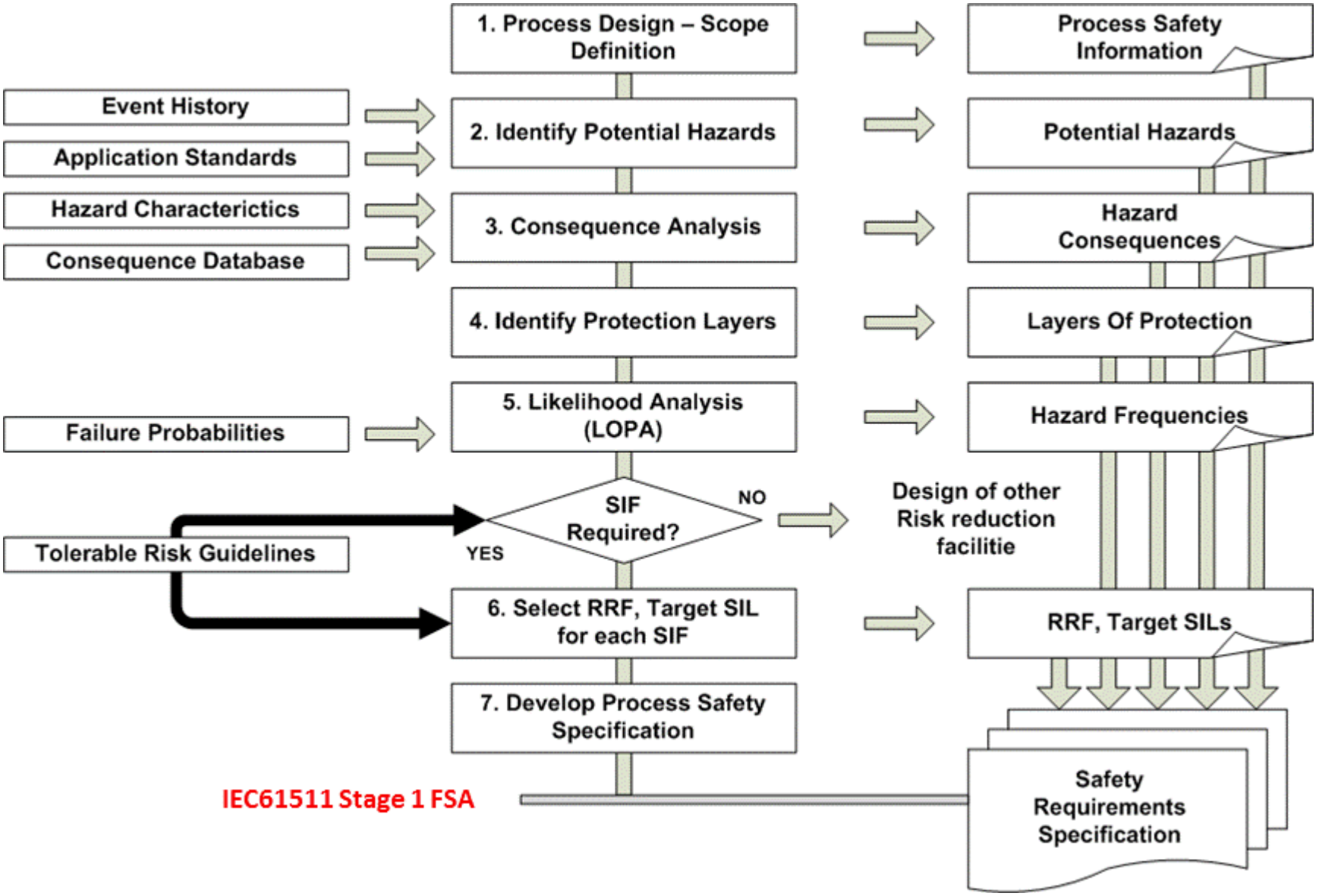
Refinery: Hydrogen Manufacturing Unit



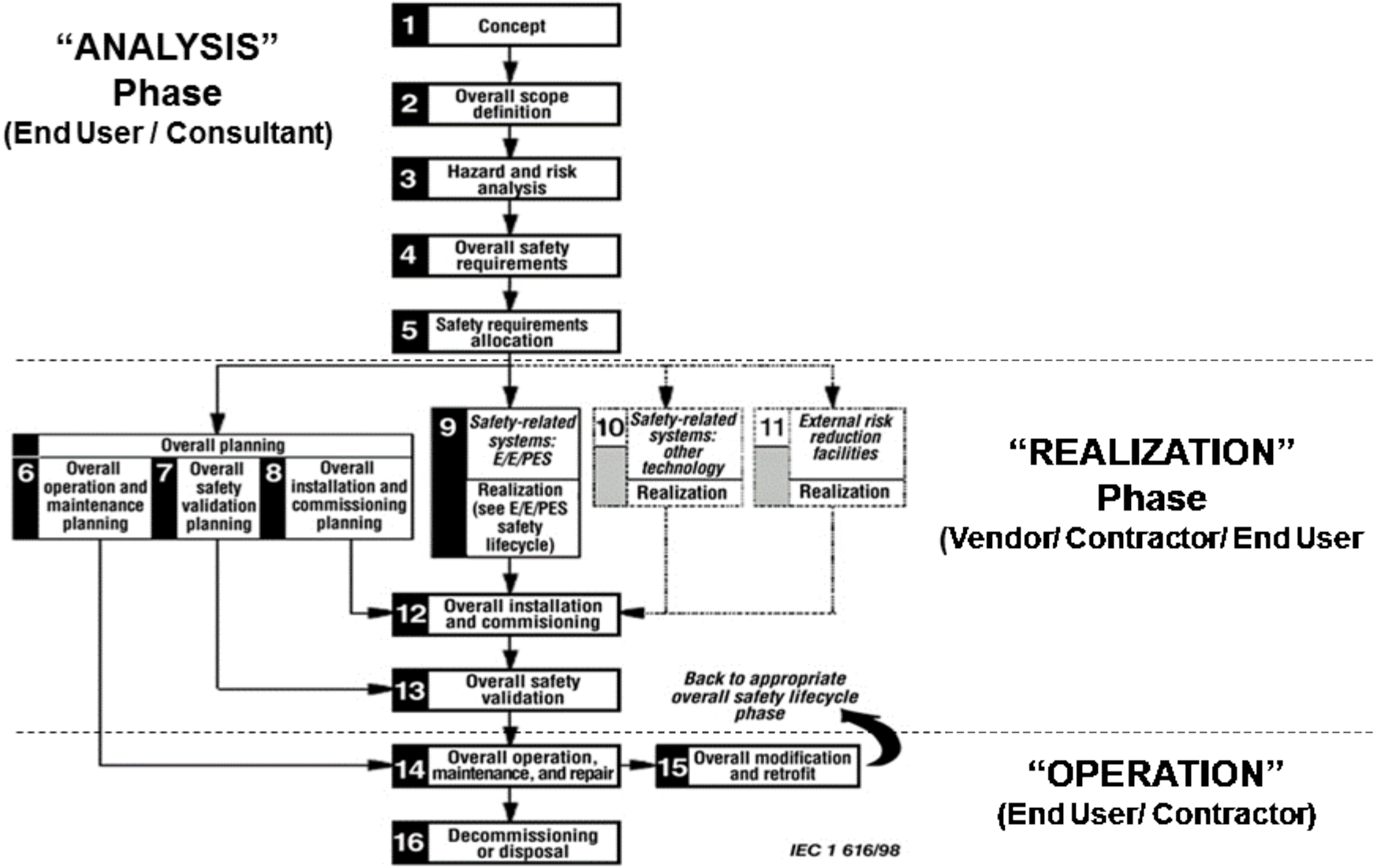
Source

- 49%: Safety Functions were over-engineered
- 4%: Safety Functions were under-engineered (unsafe)
- 47%: No change

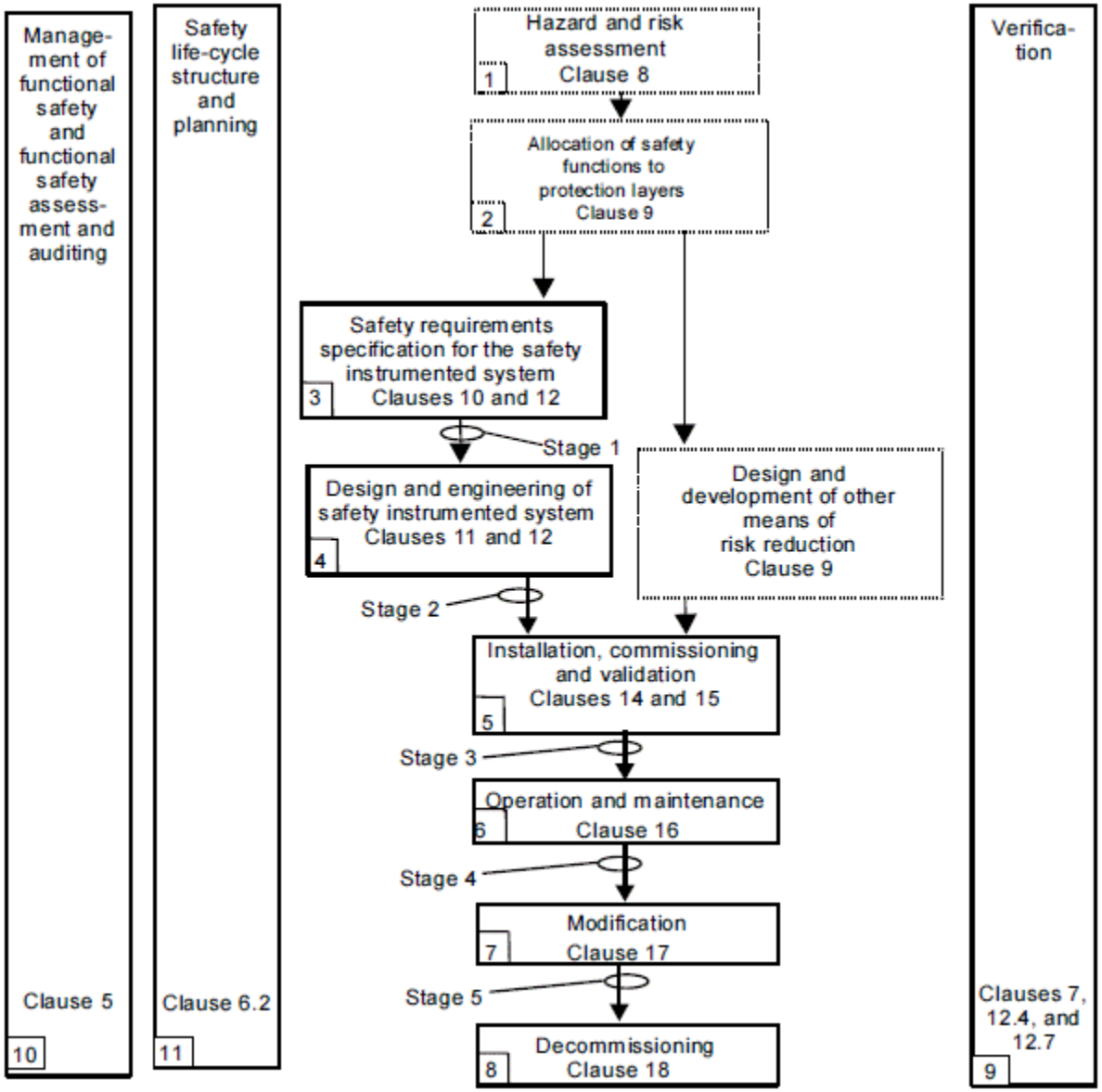
“Analysis” Information Flow Detail;



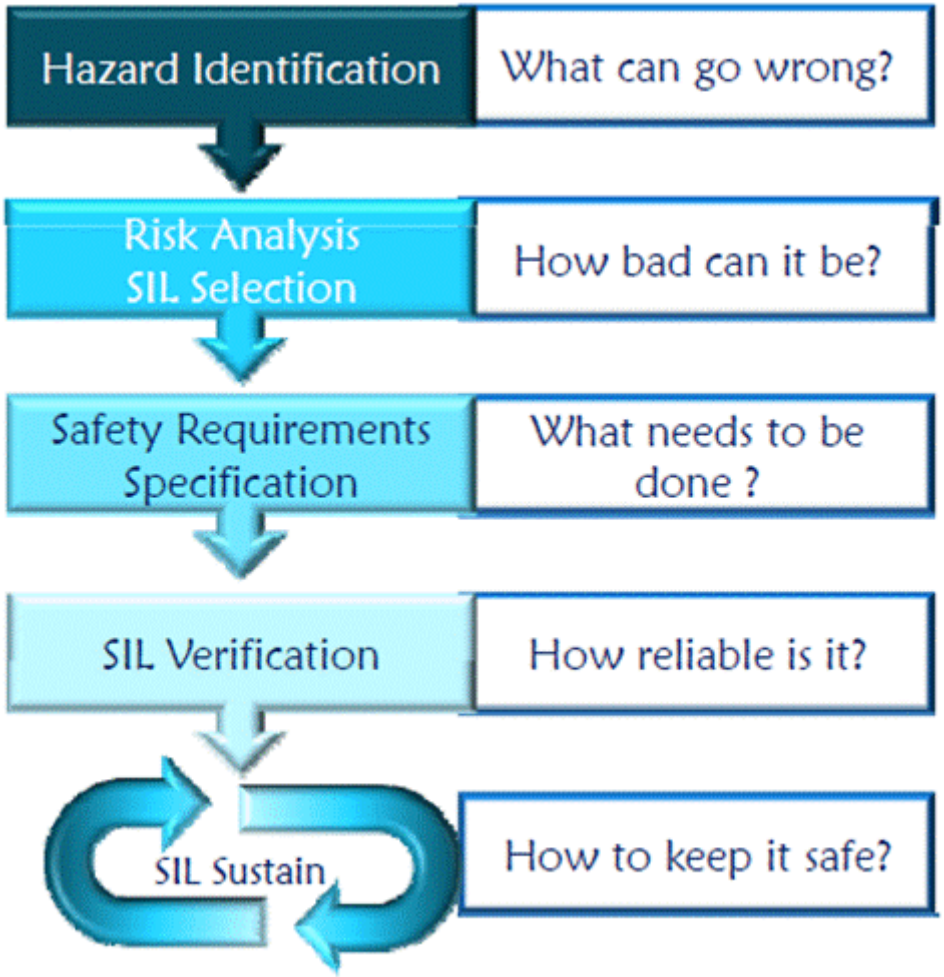
SLC [Safety Lifecycle]



SLC [Safety Lifecycle]



SLC [Safety Lifecycle]



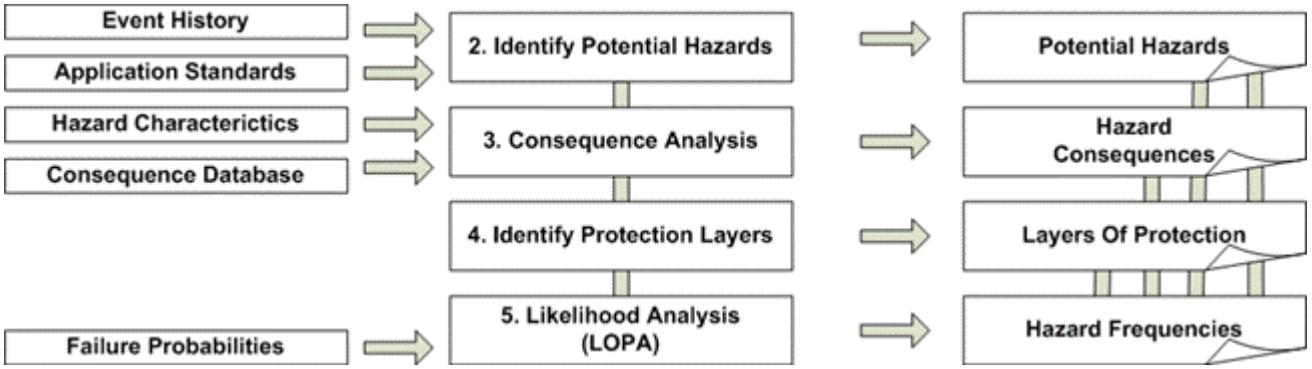
Section - 3.1

SAFETY LIFECYCLE [SLC]
Analysis Phase

Objective:

To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety instrumented functions required to achieve the necessary risk reduction

SLC – Hazard Analysis Focus



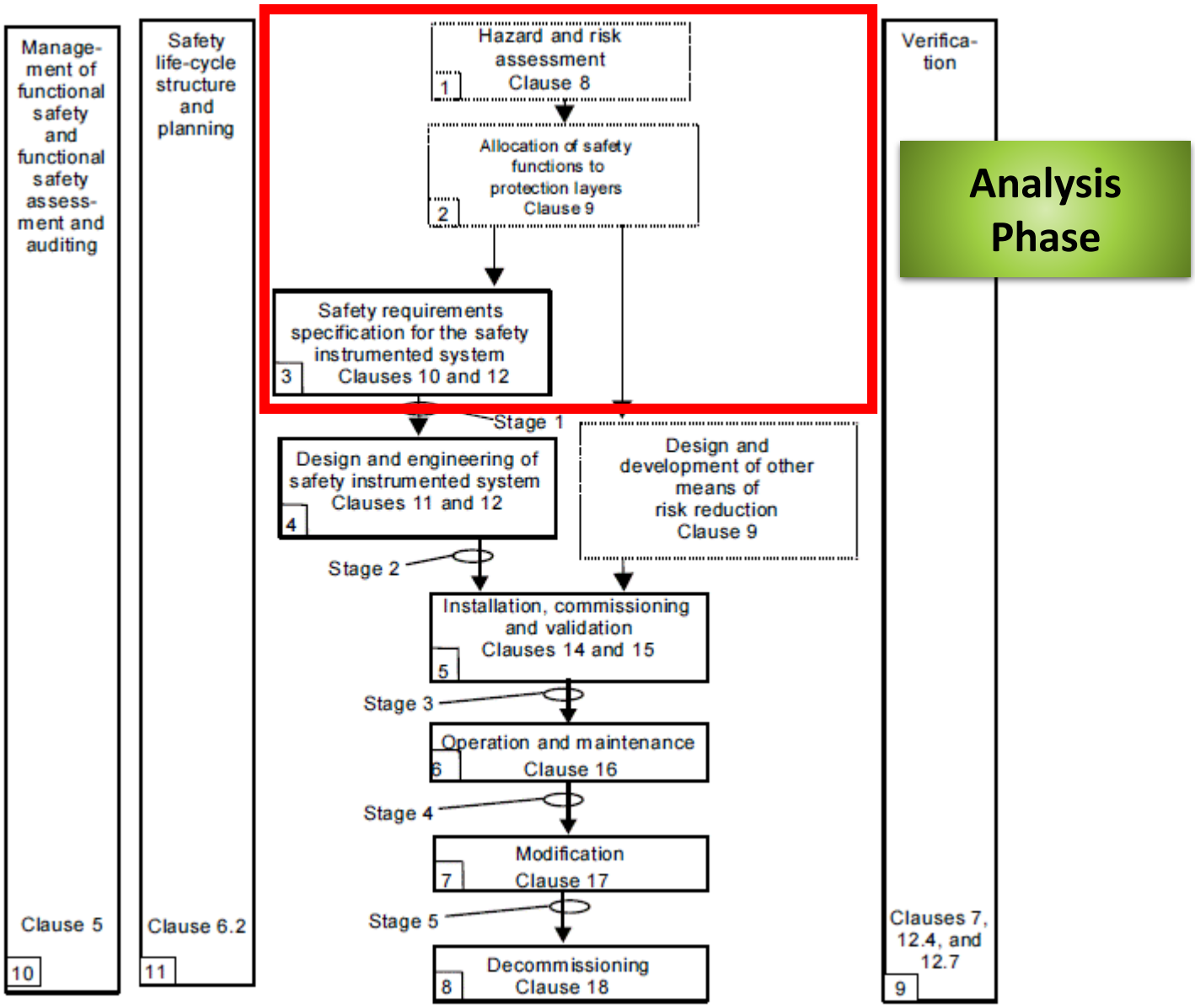
Objectives;

Identify process hazards, estimate their risks and decide if the risk is tolerable

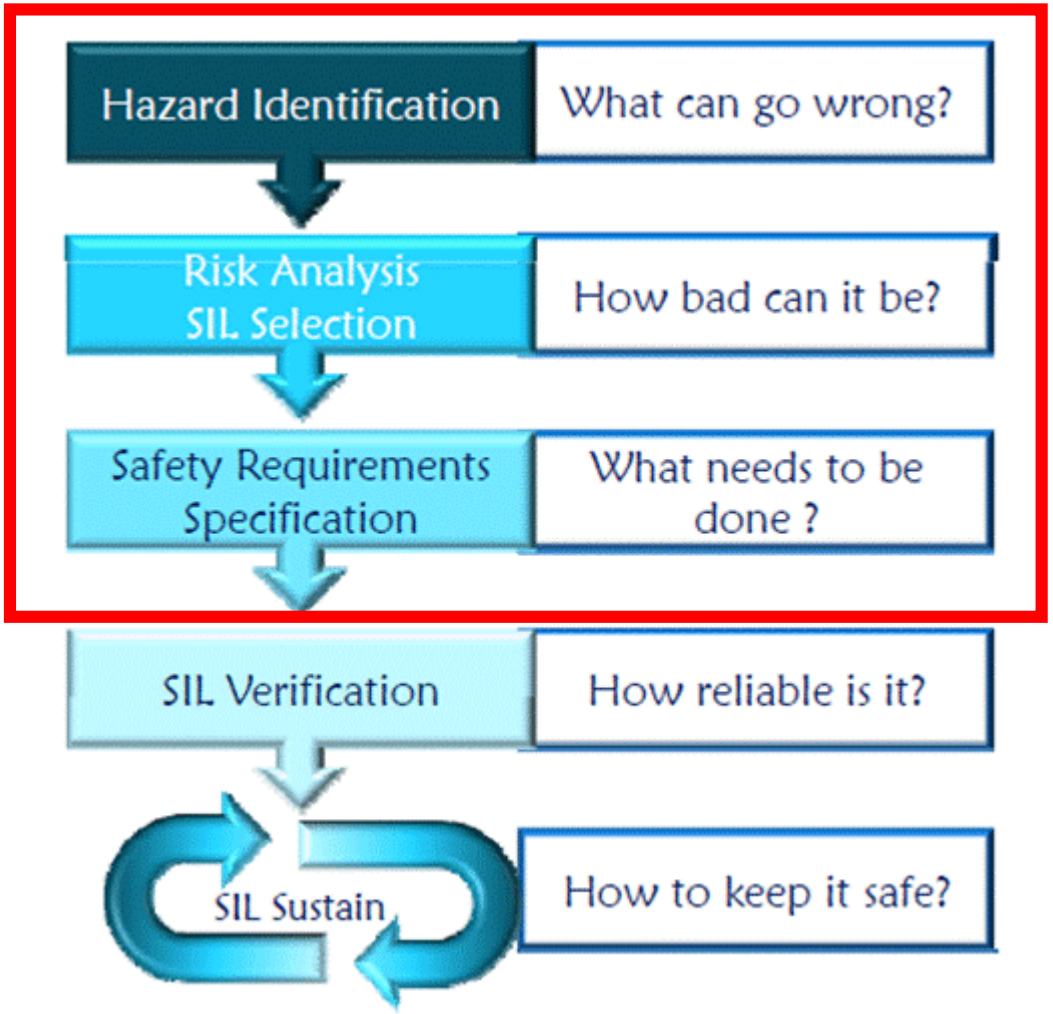
Tasks

- Hazard Identification (e.g., HAZOP)
- Analysis of Likelihood and Consequence
- Consideration of non-SIS Layers of Protection

SLC – Analysis Phase



SLC – Analysis Phase

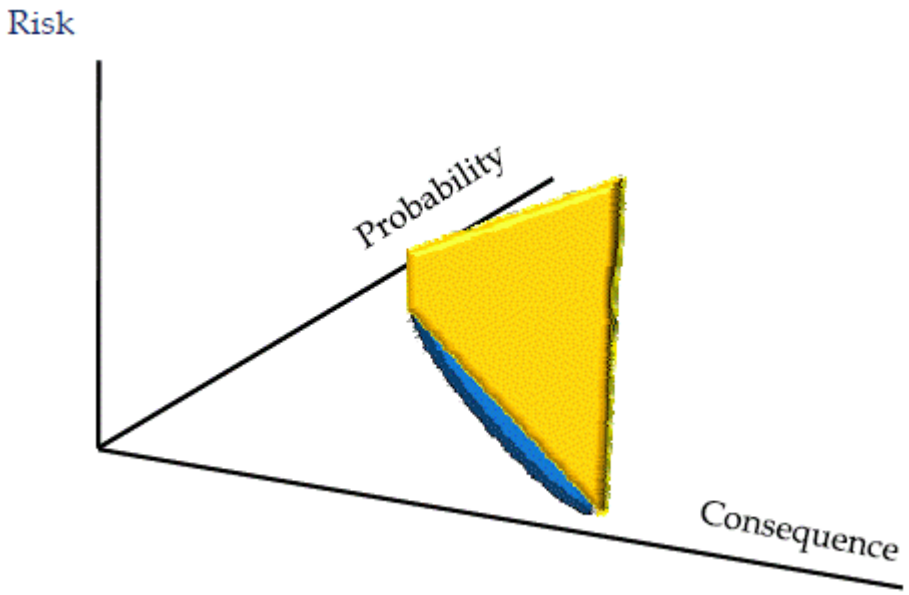


Analysis Phase

Risk Analysis Phase

f (risk) → {Si, Li, Ci}; for all i, where

Si = Scenario (accidental event) no. I
Li = The likelihood (probability or frequency) of Si
Ci = The potential consequences of Si



Risk Analysis Phase

Probability vs Frequency;

Probability;

The probability that a specific event will occur in a specified context (p = probability)

$$0.0 \leq p \leq 1.0 \text{ or } 0\% \leq p \leq 100\%$$

Frequency;

The number of events per time unit (e.g., per year)

(f –frequency) → f = 5 *events per year*

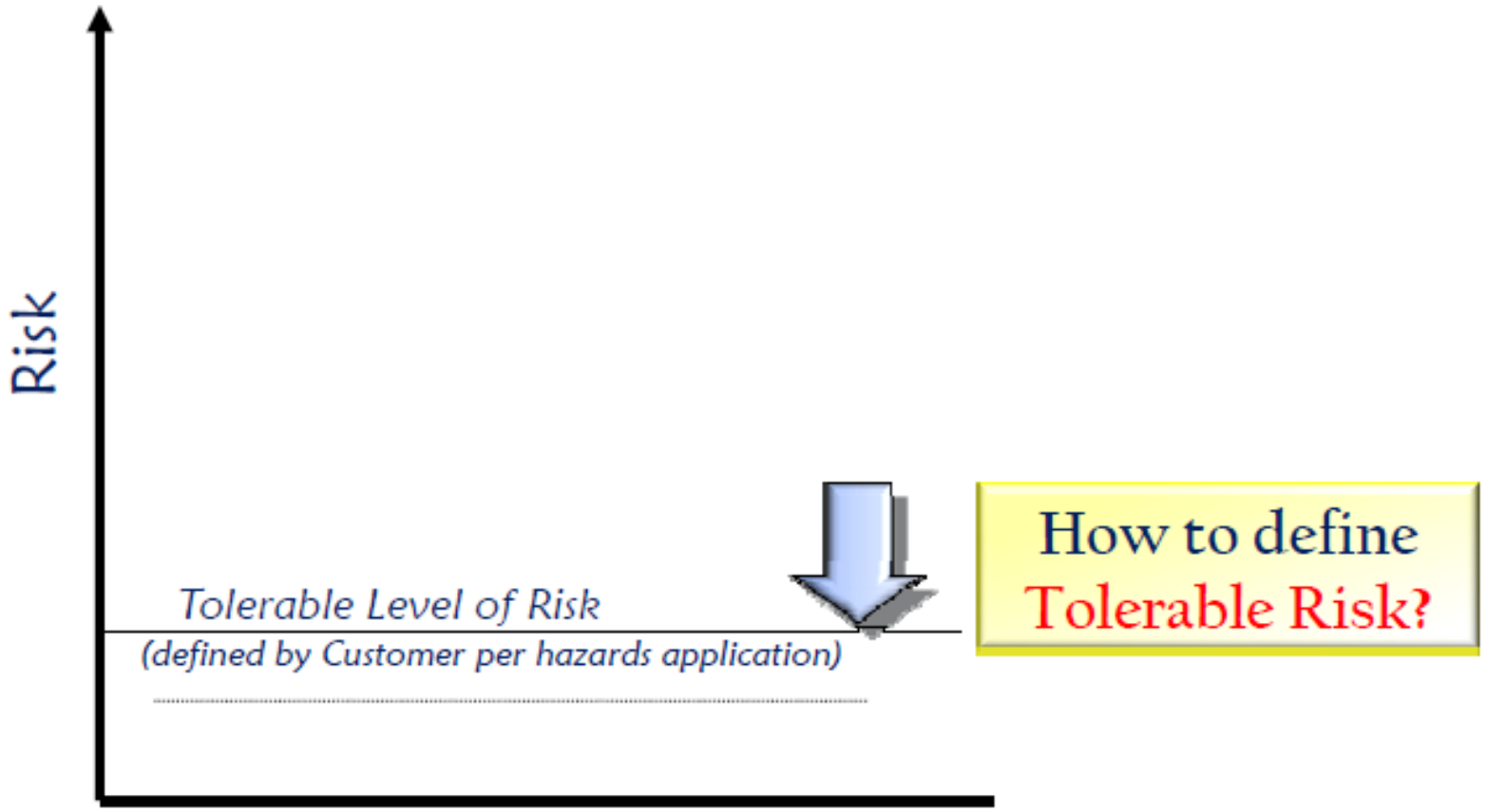
Risk Analysis Phase

Consequence Categories;

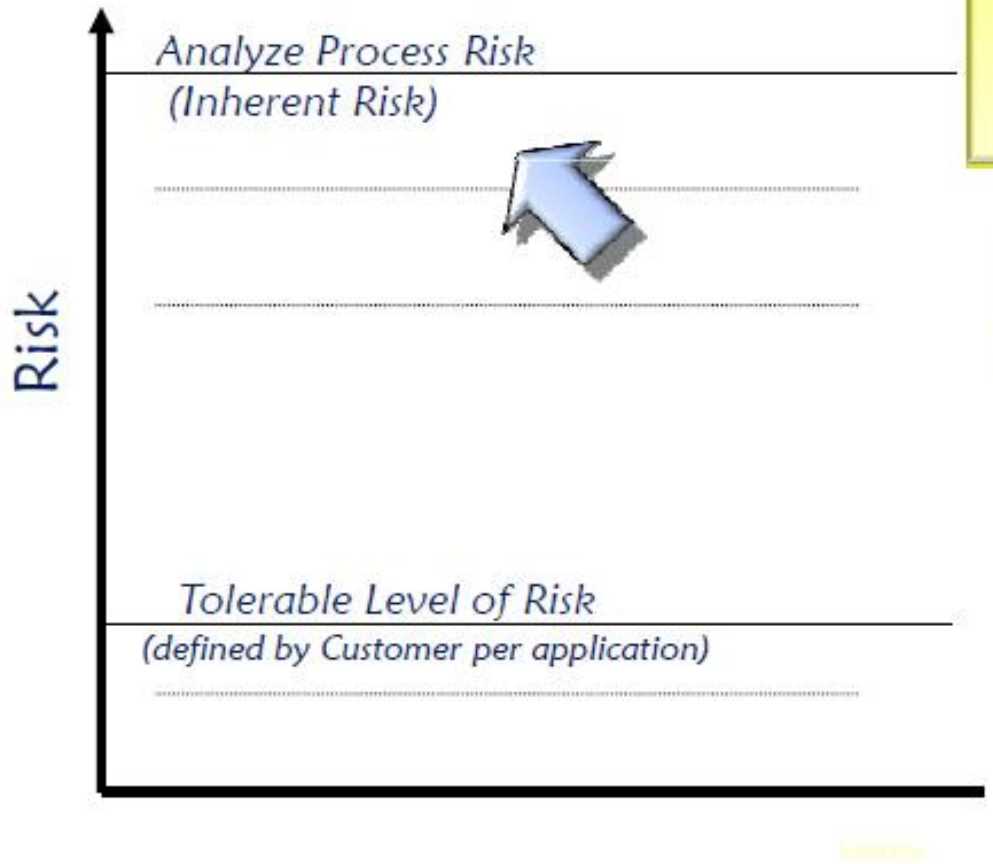
The consequences of an accident may be classified in different categories, as

- Personnel consequences
  - ✓Fatalities
  - ✓Impairment
- Environmental damage
- Economic loss
  - ✓Damage to material assets
  - ✓Production/service loss
- Information “loss”
- Image (i.e., damage to reputation)

Risk Analysis



SLC– Analysis Phase



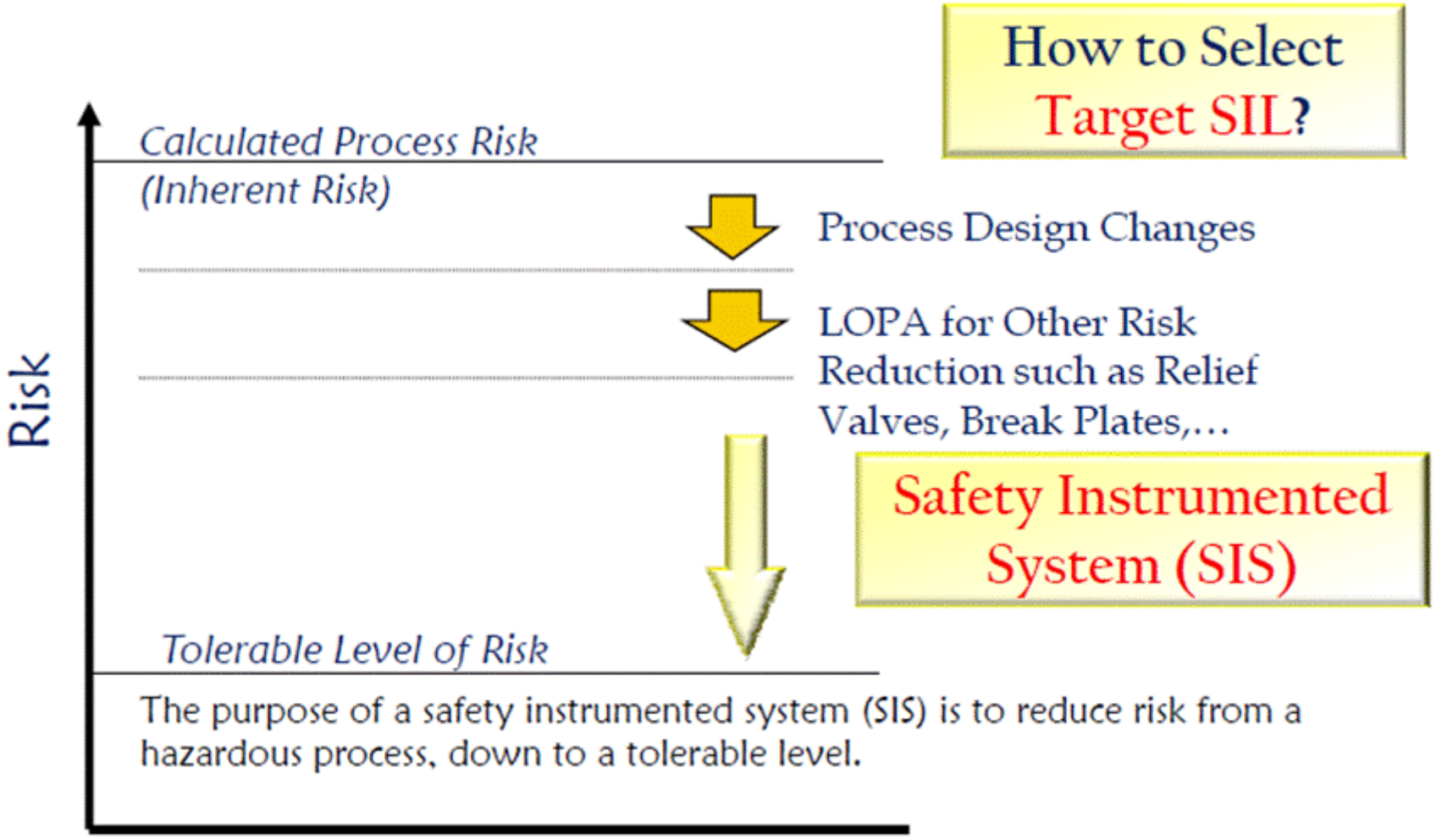
Analyze
Process Risk
(PHA/ HAZOP)

Typical PHA – HAZOP Report

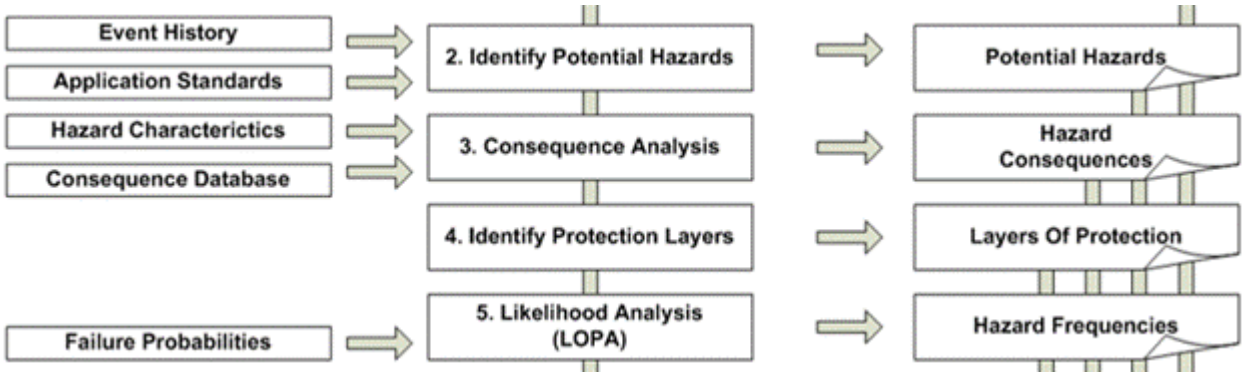
Node: Warm End Cryogenic Heat Exchanger
Parameter: Temperature

Deviation	Cause	Consequence	Safeguards	Recommendation	Action
Too low	Flow imbalance between streams	Potential brittle fracture of downstream piping and fire	Alarms, Process shut off, Indep. PLC Low T shut off	Should Indep. PLC low T shut off be an SIS?	J. Jones
	Weather extreme	Potential brittle fracture of downstream piping and fire	PLC Low T shut off	Same as above and verify likelihood of weather extreme	J. Jones
Too high	Flow imbalance between streams	Potential compressor damage	Flow alarms and Process shut off	Verify if compressor will be damaged	S. Smith

SLC– Analysis Phase



Layer of Protection Analysis

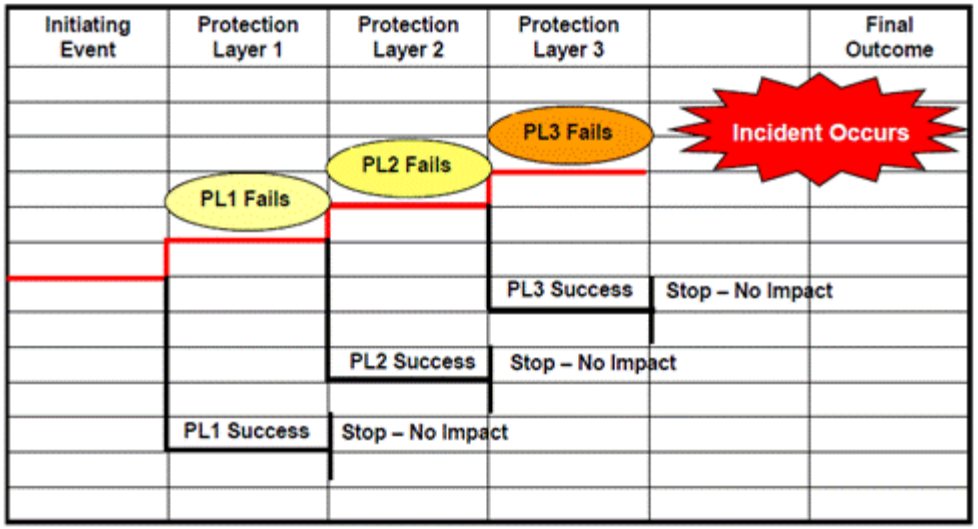


Objective

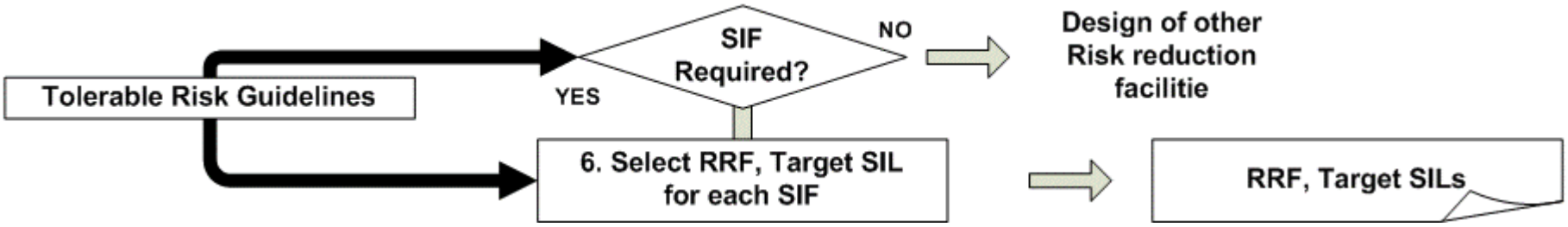
- Assess likelihood based on all protection layers

Tasks

- Identify Layers of Protection
- Use qualitative or quantitative
- methods



Safety Integrity Level Selection



Objective

- Specify the required risk reduction, or difference between existing and tolerable risk levels – in terms of SIL

Tasks

- Compare process risk against tolerable risk
- Use decision guidelines to select required risk reduction
- Document selection process

IEC-61511
ISA-84.01

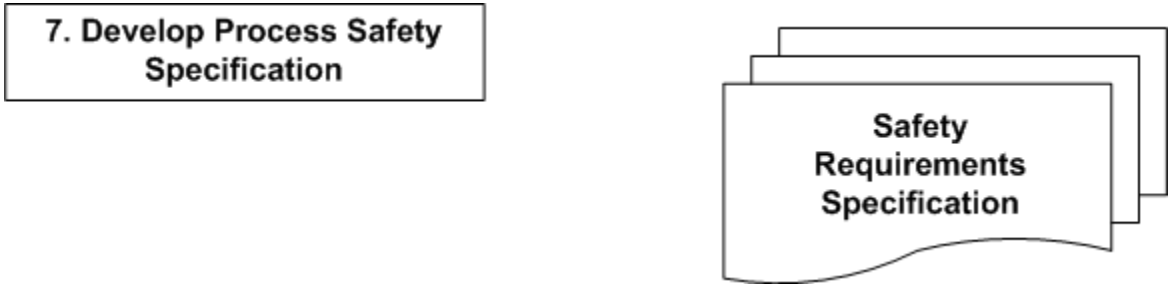
Safety Integrity Level	Average Probability of failure on demand	Risk Reduction Factor
SIL 4	1E-04 to 1E-05	10,000 to 100,000
SIL 3	1E-03 to 1E-04	1,000 to 10,000
SIL 2	1E-02 to 1E-03	100 to 1,000
SIL 1	1E-01 to 1E-02	10 to 100

SLC– Analysis Phase

DEMAND MODE

Safety Integrity Level	Average Probability of failure on demand	Risk Reduction Factor
SIL 4	1E-04 to 1E-05	10,000 to 100,000
SIL 3	1E-03 to 1E-04	1,000 to 10,000
SIL 2	1E-02 to 1E-03	100 to 1,000
SIL 1	1E-01 to 1E-02	10 to 100

Safety Requirements Specification



Objective

- Specify all requirements of SIS needed for detailed engineering and process safety information purposes

Tasks

- Identify and describe safety instrumented functions
- Document SIL
- Document action taken- Logic, Cause and Effect Diagram, etc.
- Document associated parameters -timing, maintenance/bypass requirements, etc.

Safety Requirement Specification (SRS)

2 types of requirements;

- Functional Requirements
  - ✓ Description of the functions of the SIF
  - ✓ Safe State

How it functions?

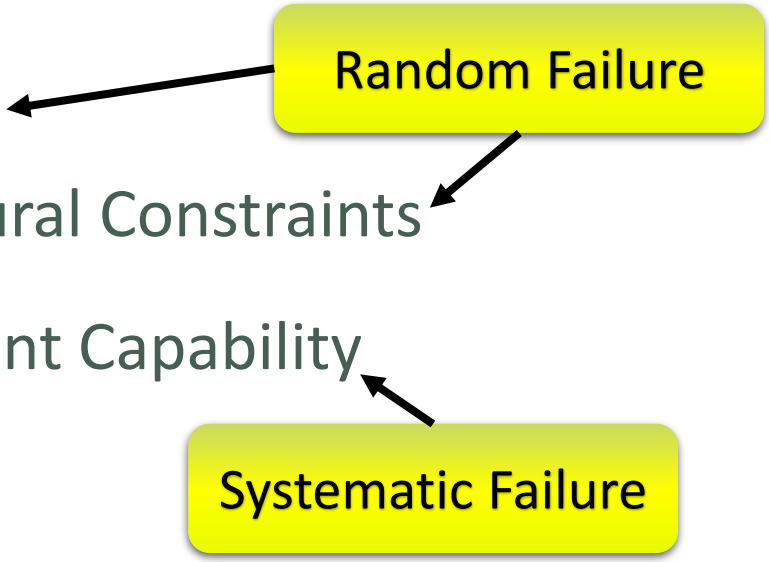
- Integrity Requirements
  - ✓ Risk reduction
  - ✓ Reliability requirements

How well it functions?

How to Meet the Target SIL (= Achieved SIL)

The achieved SIL is the minimum of:

1. SIL PFD: SIL based on PFDavg
2. SILac: SIL based on Architectural Constraints
3. SILcap: SIL based on Equipment Capability



Will be discussed further on section SIL verification

SLC– Analysis Phase

Summary of Analysis phase;

- Identify and estimate potential hazards and risks,
- Evaluate, if tolerable risk is within industry, corporate or regulatory standards,
- Check available layers of protection,
- If tolerable risk is still out of the limit, then allow use of a Safety Instrumented System (SIS) with an assigned Safety Integrity Level (SIL),
- Document the above into the Safety Requirement Specifications (SRS).

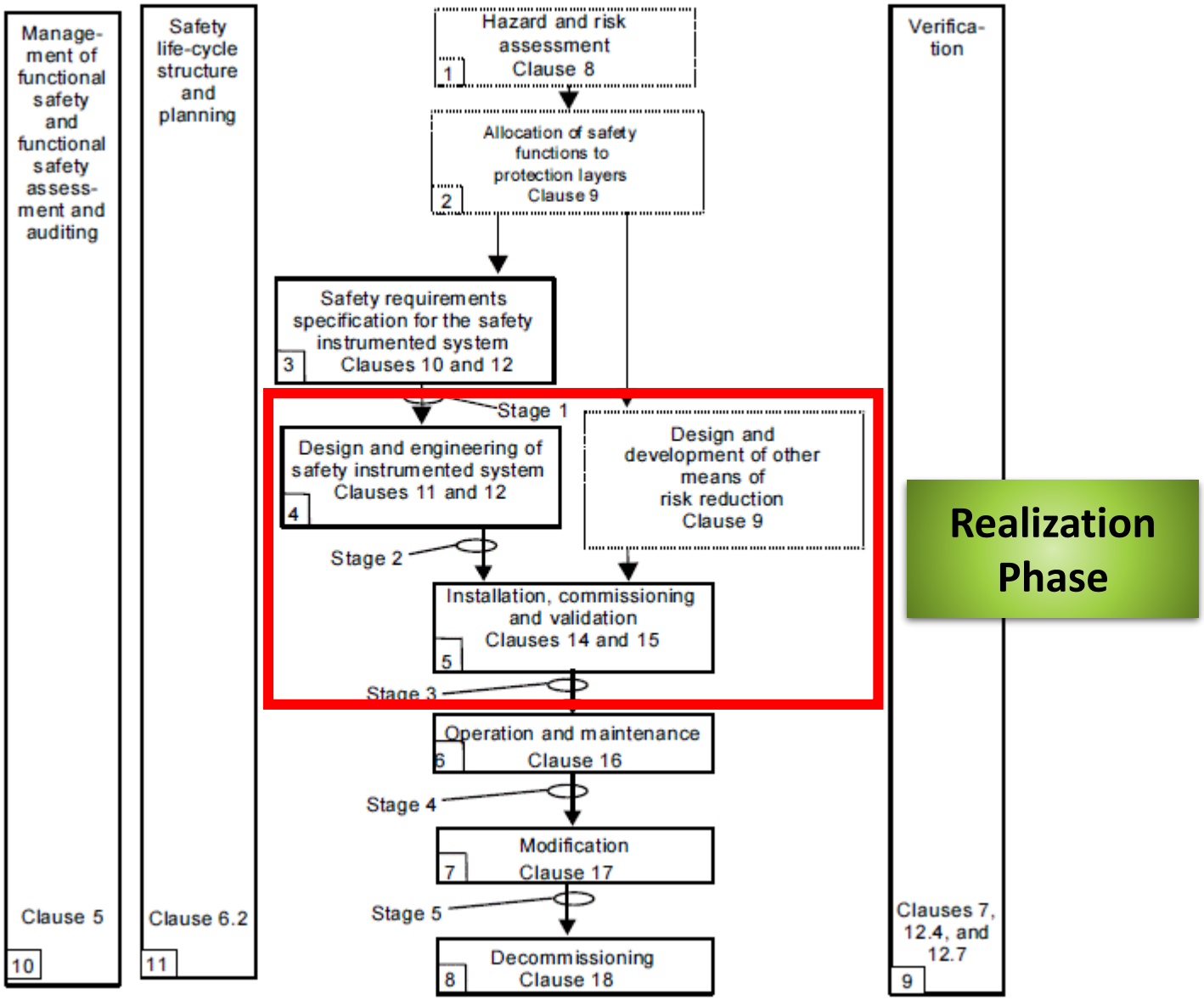
Section - 3.2

SAFETY LIFECYCLE [SLC]
Realization Phase

Objective:

- To integrate and test the SIS.
- To validate that the SIS meets, in all respects the requirements for safety in terms of the required safety instrumented functions and the required safety integrity

SLC– Realization Phase

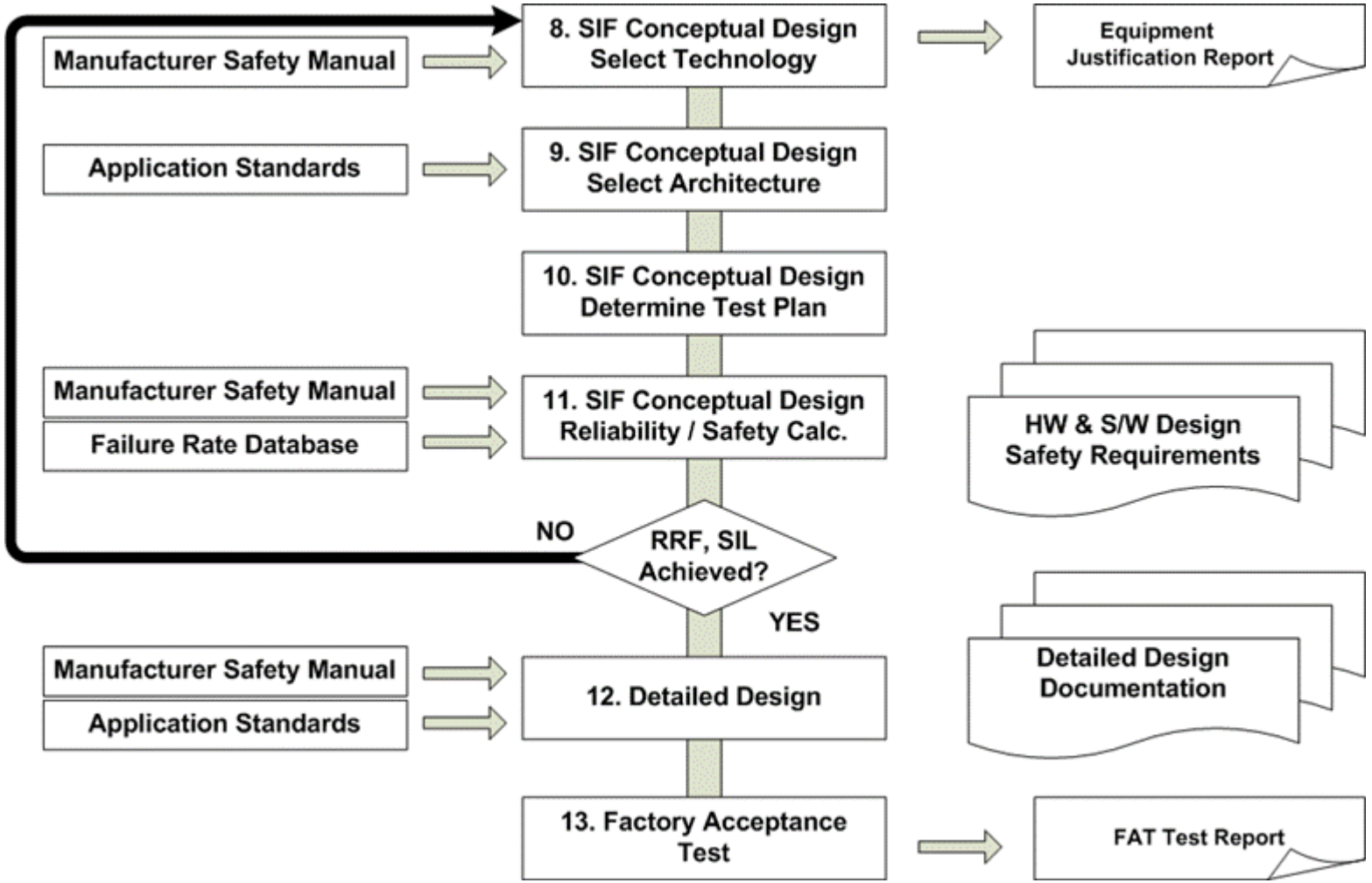


SLC– Realization Phase

Realization Phase

SLC– Realization Phase

Information Detail



SLC– Realization Phase

Realization Phase covered following actions;

Develop a conceptual design for technology, architecture, periodic test interval, reliability, safety evaluation.

Develop a detailed design for installation planning, commissioning, start up acceptance testing, and design verification.

The final part of realization phase is planning and executing the system's installation, commissioning and validation. Once these tasks are finished, the SIS should be fully functional at the SIL selected to achieve a tolerable level of risk. With this, the realization phase is complete

SLC– Realization Phase

Develop a conceptual design for;

- technology,
- architecture,
- periodic test interval,
- reliability, and
- safety evaluation.

Develop a detailed design for;

- installation planning,
- commissioning
- start-up acceptance testing, and
- design verification.

SLC– Realization Phase

Select Technology;



Objective

Choose the right equipment for the purpose - all criteria used or process control still apply

Tasks

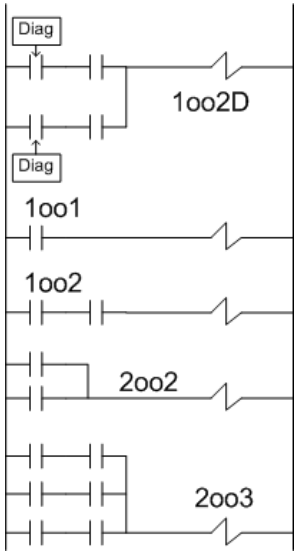
- Choose equipment
- Obtain reliability and safety data for the equipment
- Obtain Safety Manual for any safety certified equipment or equipment making a SIL capability claim

SLC– Realization Phase

Select Architecture;

Objective

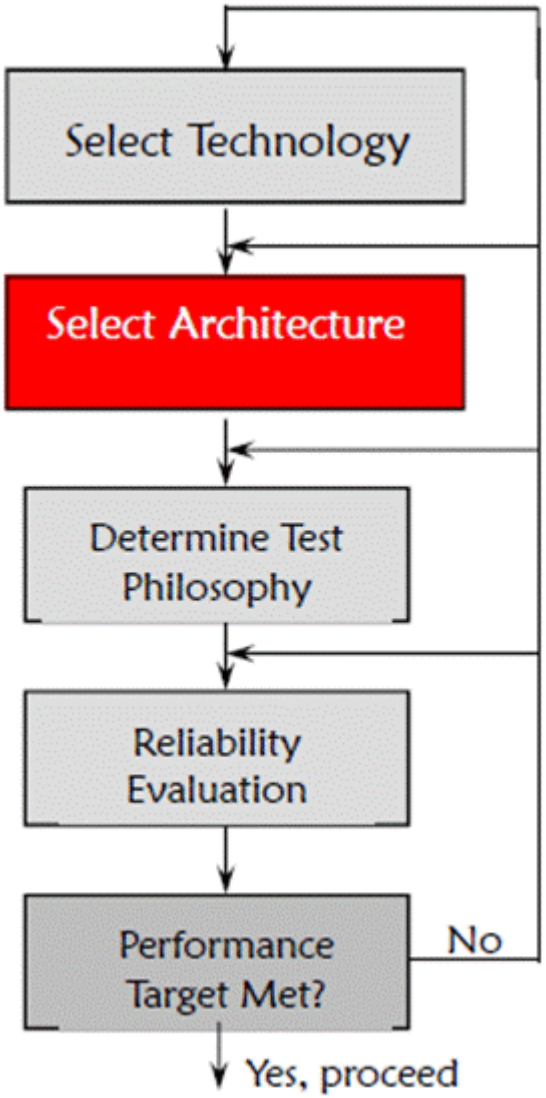
- Choose type of redundancy if needed



Tasks

- Choose architecture
- Obtain reliability and safety data for the architecture

Basic Architectures



How much?
What kind of redundancy?

1oo1
1oo2
2oo3
1oo1D
1oo2D

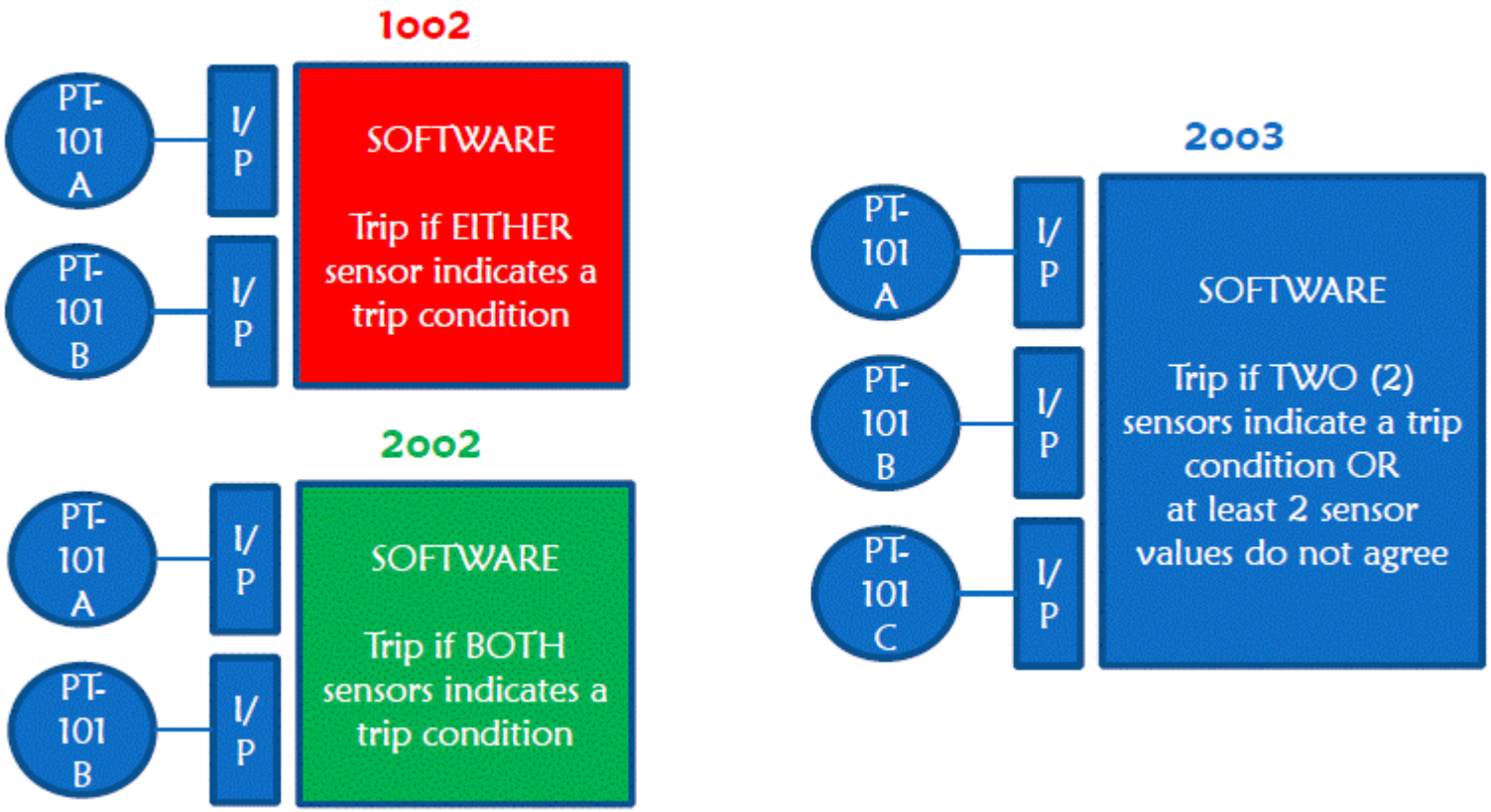
Basic Architectures

Simplified Equations;

Voting	Average probability of failure on demand (PFD_{avg})	Spurious trip rate (STR)
1oo1	$\lambda_d * T/2$	λ_s
1oo2	$\frac{(\lambda_d)^2 * T^2}{3}$	$2\lambda_s$
2oo2	$\lambda_d * T$	$\frac{2\lambda_s^2}{3\lambda_s + 2/T}$
2oo3	$(\lambda_d)^2 * T^2$	$\frac{6\lambda_s^2}{5\lambda_s + 2/T}$

Voting for Sensors

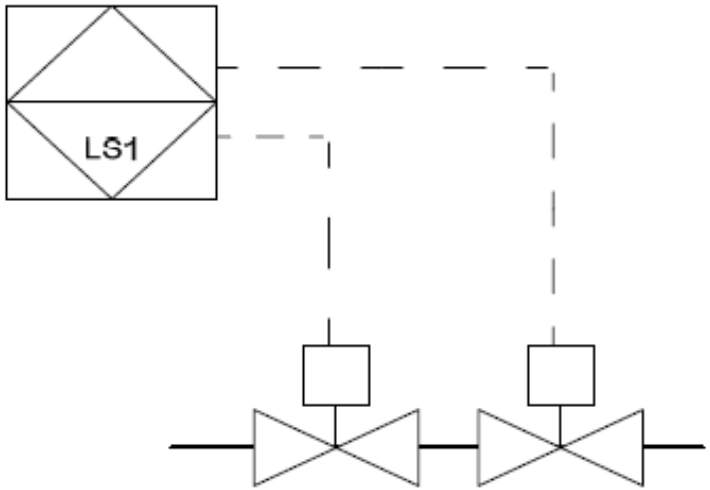
Field equipment; Sensor



Voting for Final Elements

Field equipment; Final Elements

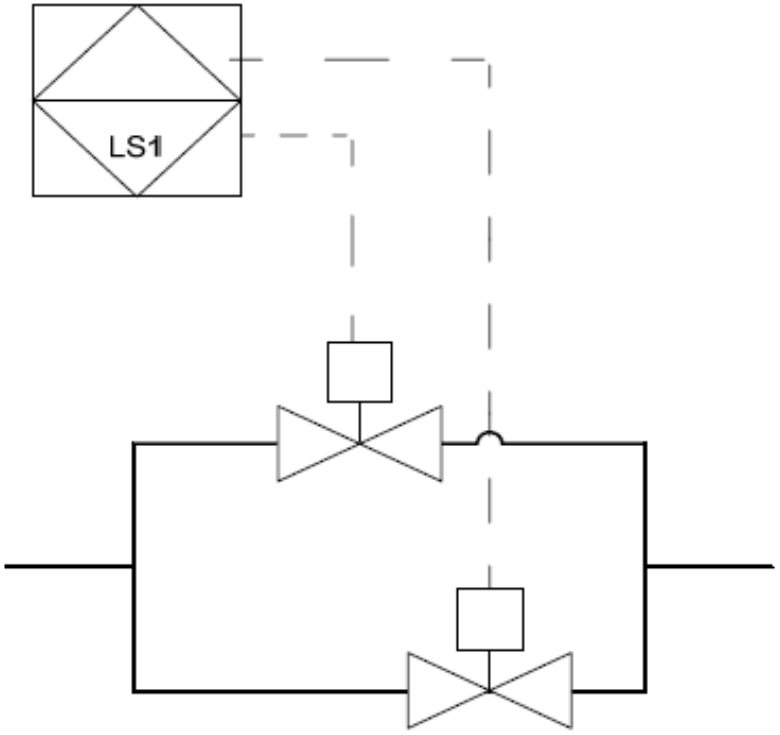
Trip both outputs on indicated trip



SOV

1oo2 = Valves in series on pipe

Trip both outputs on indicated trip



SOV

2oo2 = Valves in parallel on pipe

Hardware Fault Tolerance

Architecture	Hardware Fault Tolerance
1oo1	0
1oo1D	0
1oo2	1
2oo2	0
2oo3	1
2oo2D	0
1oo2D	1
1oo3	2

TYPE B

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	Not allowed	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

NOTE A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function

Hardware Fault Tolerance

For Programmable Electronic Systems (Type B)

Maximum SIL Allowed				
	Safe Failure Fraction			
Architecture	0 - <60%	60 - <90%	90 - <99%	99%+
1oo1	Not Allowed	SIL 1	SIL 2	SIL 3
1oo1D	Not Allowed	SIL 1	SIL 2	SIL 3
1oo2	SIL 1	SIL 2	SIL 3	SIL 4
2oo2	Not Allowed	SIL 1	SIL 2	SIL 3
2oo3	SIL 1	SIL 2	SIL 3	SIL 4
2oo2D	Not Allowed	SIL 1	SIL 2	SIL 3
1oo2D	SIL 1	SIL 2	SIL 3	SIL 4
1oo3	SIL 2	SIL 3	SIL 4	SIL 4

IEC 61511 HFT Table

PE logic solvers

SIL	Minimum Hardware Fault Tolerance		
	SFF < 60%	SFF 60% to 90%	SFF > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (see IEC 61508)		

Almost identical to IEC 61508 Type B table

– IEC 61508 specifies 4 levels of SFF

– IEC 61511 does not specify SIL 4

IEC 61511 HFT Table

Field Equipment

SIL	Minimum Hardware Fault Tolerance
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

- No Type A vs Type B
- No SFF
- Identical to IEC 61508 Type B table for SFF 60-90% and Type A table for SFF 0-60%

IEC 61511 HFT Table

Field Equipment;

Increase minimum HFT by one if the dominant failure mode is not to the safe state or dangerous failures are not detected

Reduce minimum HFT by one if

- The hardware of the device is selected on the basis of prior use; and
- The device allows adjustment of process-related parameters only, for example, measuring range, upscale or downscale failure direction; and
- The adjustment of the process-related parameters of the device is protected, for example, jumper, password; and
- The function has a requirement of less than 4.

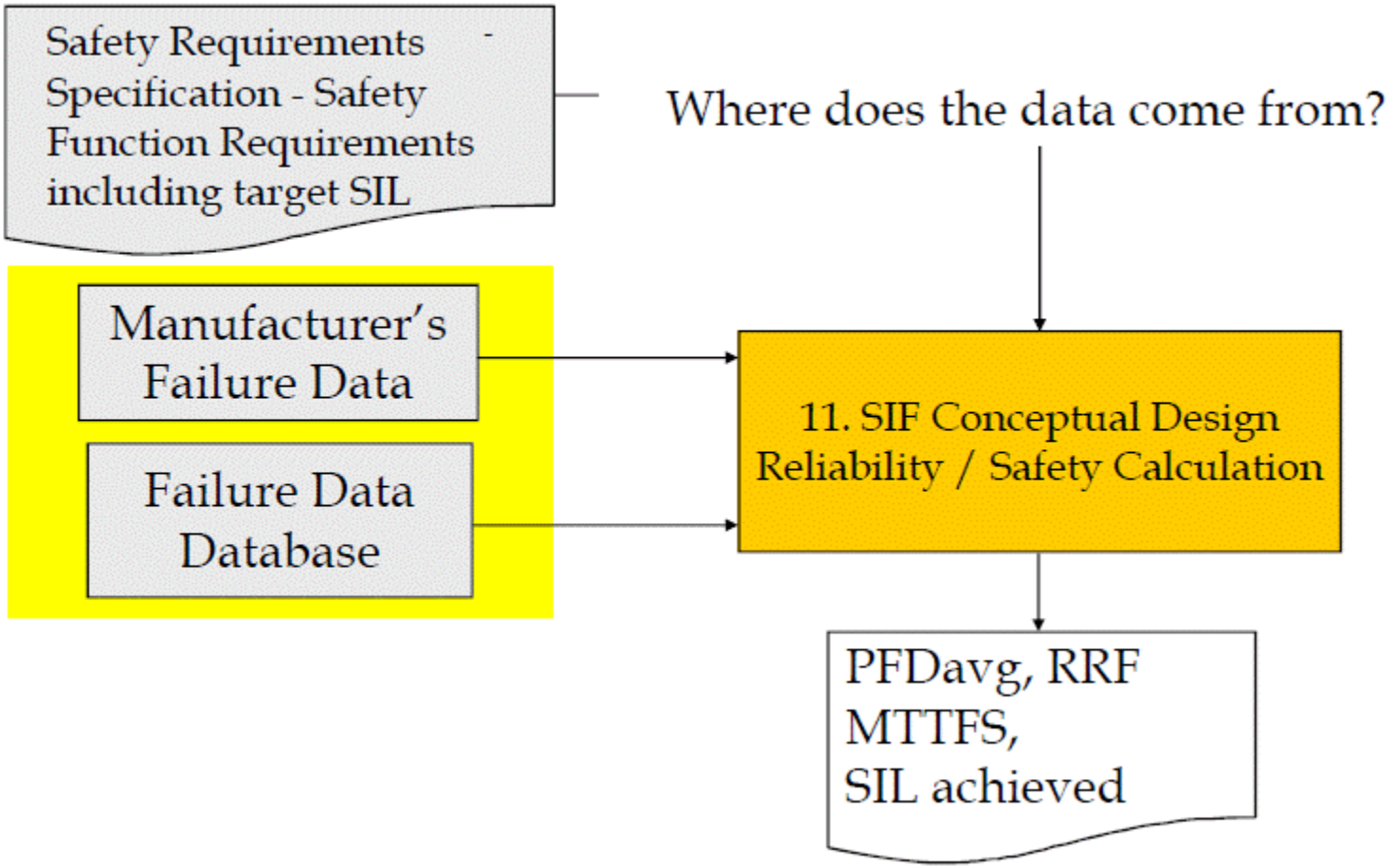
HFT Table Field Equipment

IEC 61508 HFT charts may be used instead of 61511 charts – recommended

They are clear and more flexible

Verification

SIF Verification Task



Failure Rate Data Models

1. Industry Databases – NOT Application Specific, NOT Product Specific
2. Manufacturer FMEDA, Field Failure Study – Product Specific, NOT Application Specific
3. Detail Field Failure Study – Application model. Product Specific. Application Specific

Failure Rate Data Handbook

1. Industry Databases – NOT Application Specific, NOT Product Specific

2. Manufacturer FMEDA, Field Failure Study – Product Specific, NOT Application Specific

Safety Integrity Levels

DEMAND MODE

Safety Integrity Level	Average Probability of failure on demand	Risk Reduction Factor
SIL 4	1E-04 to 1E-05	10,000 to 100,000
SIL 3	1E-03 to 1E-04	1,000 to 10,000
SIL 2	1E-02 to 1E-03	100 to 1,000
SIL 1	1E-01 to 1E-02	10 to 100

SIL Design Verification

Three Requirements for SIL Design Verification;

- Low Demand Mode - PFDavg
  - ✓ Manages risk from random failures
- Hardware Fault Tolerance
  - ✓ Meets standard requirements
- Systematic Integrity
  - ✓ Proven in use / 61508 compliant equipment
  - ✓ Manages risk from systematic failures

Putting the Function Together

- Overall function PFDavg ≈

PFDavg Sensor(s) +

PFDavg Logic Solver +

PFDavg Final Element(s)

- Overall function Spurious Trip Rate (STR) ≈

STR Sensor(s) +

STR Logic Solver+

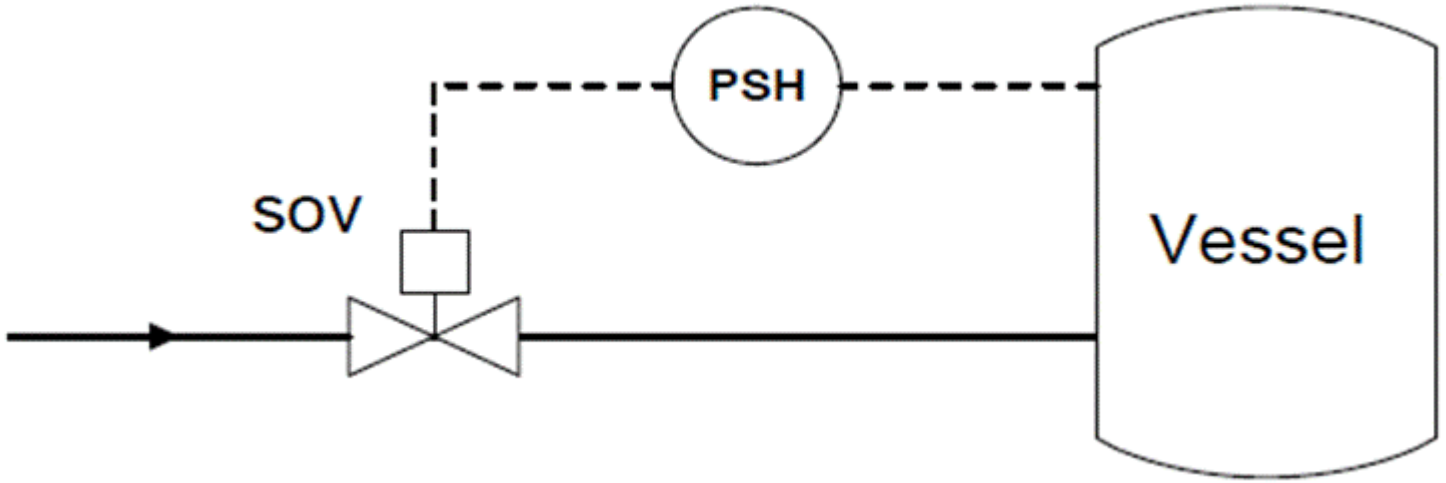
STR Final Element(s)

Example - 1:

High Pressure Protection Loop
Pressure Switch + Solenoid

	Lambda D (λ^D)
Solenoid	???
Pressure switch	???

No Diagnostics, Test Interval – 1 year, SIL2 required



SIF Verification Example

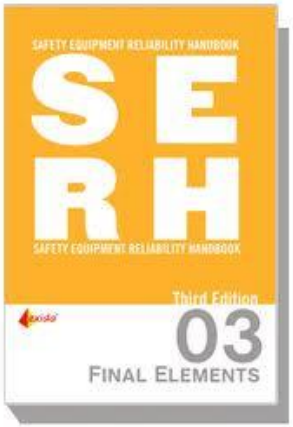
SERH Data

EQUIPMENT ITEM	Generic DP/ Pressure Switch		ITEM NO. 1.6.1
GENERAL INFORMATION			
MANUFACTURER	Generic Equipment		
MODEL	~~~		
MEASUREMENT TYPE	Pressure		
ANALOG / DIGITAL	Digital	HARDWARE FAULT TOLERANCE	0
ARCHITECTURE TYPE	A	CERTIFIED FOR USE UP TO SIL	N/A
ASSESSMENT	N/A	BY N/A	
DATA SOURCE	exida Comprehensive Analysis		
REMARKS	None		

FAILURE RATE DATA	PER 10^9 HOURS [FITS]	
FAIL LOW		
FAIL HIGH		
FAIL DETECTED		
FAIL DANGEROUS DETECTED		
FAIL DANGEROUS UNDETECTED	3600	
FAIL SAFE DETECTED		
FAIL SAFE UNDETECTED	2400	
FAIL ANNUNCIATION DETECTED		
FAIL ANNUNCIATION UNDETECTED		
FAIL NO EFFECT		
SFF [%]	40.0	

Lambda DU (λ^{DU})

SIF Verification Example



EQUIPMENT ITEM	Generic 3-way Solenoid		ITEM NO. 6.1.2
GENERAL INFORMATION			
MANUFACTURER	Generic Equipment		
MODEL	~~~		
INTERFACE TYPE	Solenoid, 3-way		
ANALOG / DIGITAL	Digital	HARDWARE FAULT TOLERANCE	0
ARCHITECTURE TYPE	A	CERTIFIED FOR USE UP TO SIL	N/A
ASSESSMENT	N/A	BY	N/A
DATA SOURCE	exida Comprehensive Analysis		
REMARKS	None		

FAILURE RATE DATA	PER 10^9 HOURS [FITS]		
	NORMAL	PVST	
FAIL DANGEROUS DETECTED		579	
FAIL DANGEROUS UNDETECTED	585	6	
FAIL SAFE DETECTED		1010	
FAIL SAFE UNDETECTED	1010		
FAIL ANNUNCIATION DETECTED			
FAIL ANNUNCIATION UNDETECTED			
FAIL NO EFFECT	500	500	
SFF [%]	72.1	99.7	

Lambda DU (λ^{DU})

SIF Verification Example

Example 1: High Pressure Protection Loop. Pressure Switch+Solenoid

Demand Mode

	Lambda DU (λ^{DU})
Solenoid	0.585 x 10-6 failures per hour
Pressure switch	3.6 x 10-6 failures per hour

No Diagnostics, Test Interval – 1 year, SIL2 requirement

PFDavg = $\lambda^{DU} * \left(\frac{TI}{2}\right)$

PFDavg = (0.000004185* 8760) / 2

PFDavg = 0.01833

RRF = 1/PFDavg = 54.5 → SIL 1

Use simplified equation for first pass. Assuming perfect proof testing very optimistic!

SIF Verification Example

Example 1: High Pressure Protection Loop. Pressure Switch+Solenoid

Proof Test: Operations has said that it is not practical to change the process pressure or isolate the pressure switch. Therefore the proof test will open the pressure switch wire once a year and check to see if the solenoid will de-energize The pressure switch will be inspected for corrosion and dirt and cleaned if necessary.

How good is this? What coverage?

Estimate of Test Effectiveness:

Pressure Switch – 20%
Solenoid – 95%

SIF Verification Example - PFDavg

Example 1: High Pressure Protection Loop. Pressure Switch+Solenoid

PFDavg = $C_{PT} * \lambda^D * \left(\frac{TI}{2}\right) + (1 - C_{PT}) * \lambda^D * \frac{LT}{2}$

C_{PT} = Effectiveness of proof test, 0 – 100%

LT = Operational Lifetime of plant

The process unit will be operated for 6 years then shutdown for complete overhaul. During the overhaul, solenoid and pressure switch will be replaced with new units

Therefore LT = 6 years

Note: This “simplified equation” is not as simple as before but gives reasonable results

SIF Verification Example - PFDavg

Example 1: High Pressure Protection Loop. Pressure Switch+Solenoid

PFDavg = $C_{PT} * \lambda^D * \left(\frac{TI}{2}\right) + (1 - C_{PT}) * \lambda^D * \frac{LT}{2}$

= 0.2 * 0.0000036 * 8760/2 + (1 – 0.2) * 0.0000036 * 6 * 8760/2

+ 0.95 * 0.000000585 * 8760/2 + (1 – 0.95) * 0.000000585 * 6 * 8760/2

= 0.082

RRF = 12 → LOW SIL 1

SIF Verification Example

SFF: Safe Failure Fraction

$$SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}}$$

SFF is defined as the ratio of the average rate of safe failures plus dangerous detected failures of the subsystem to the total average failure rate of the subsystem

$$SFF = 1 - \frac{\lambda^{DU}}{\lambda}$$

SIF Verification Example

Example 1: High Pressure Protection Loop. Pressure Switch+Solenoid

1. Pressure Switch - Solenoid

	Lambda DU (λ^{DU})	**Lambda S(λ^{S})**	**SFF**
Solenoid	0.585 x 10^{-6} f/hr	1.010 x 10^{-6} f/hr	72.1%
Pressure switch	3.6 x 10^{-6} f/hr	2.4 x 10^{-6} f/hr	40%

Limiting sub-system is sensor – pressure switch.

SIF Verification Example - SFF

Example 1: High Pressure Protection Loop. Pressure Switch+Solenoid

1. Pressure Switch - Solenoid

TYPE A Subsystem **Demand Mode**

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

NOTE A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function

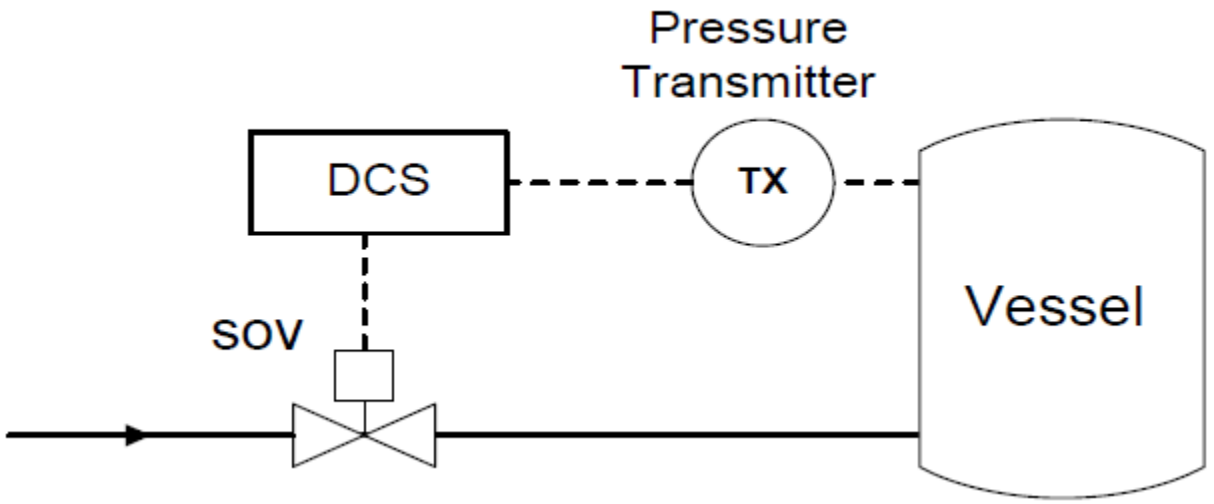
Example 2:

High Pressure Protection Loop Transmitter - DCS - Solenoid

1. Verify that the DCS was not being used as a “Layer of Protection.”
2. Verify that any DCS failure would not be an “initiating event” for a hazard

If either of these are possible, then one cannot use the DCS in a safety instrumented function

Prior Use justification documentation REQUIRED



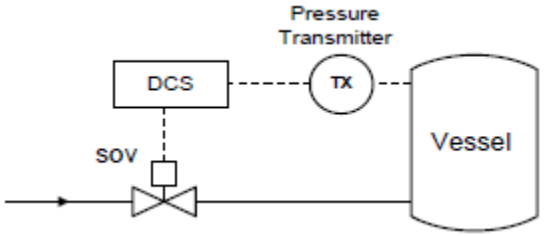
Example 2:

High Pressure Protection Loop Transmitter - DCS - Solenoid

Equipment Item	Rosemount 3051C			Item No.	1.6.16
GENERAL INFORMATION					
Manufacturer	Rosemount Inc.				
Model	3051C, Rev. 178				
Measurement Type	Pressure				
Analog / Digital	Analog	Hardware Fault Tolerance	0		
Architecture Type	B	Certified for use up to SIL	N/A		
Assessment	FMEDA	By	exida		
Data Source	FMEDA by exida				
Remarks	None				

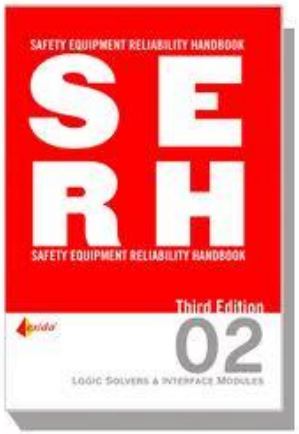
FAILURE RATE DATA	Per 10^9 hours [FITs]	
Fail Low	215	
Fail High	48	
Fail Detected	57	
Fail Dangerous Detected		
Fail Dangerous Undetected	98	
Fail Safe Detected		
Fail Safe Undetected		
Fail Annunciation Detected		
Fail Annunciation Undetected	7	
Fail No Effect	118	
SFF [%]	82.0	

Prior Use justification documentation REQUIRED



Example 2:

High Pressure Protection Loop Transmitter - DCS - Solenoid



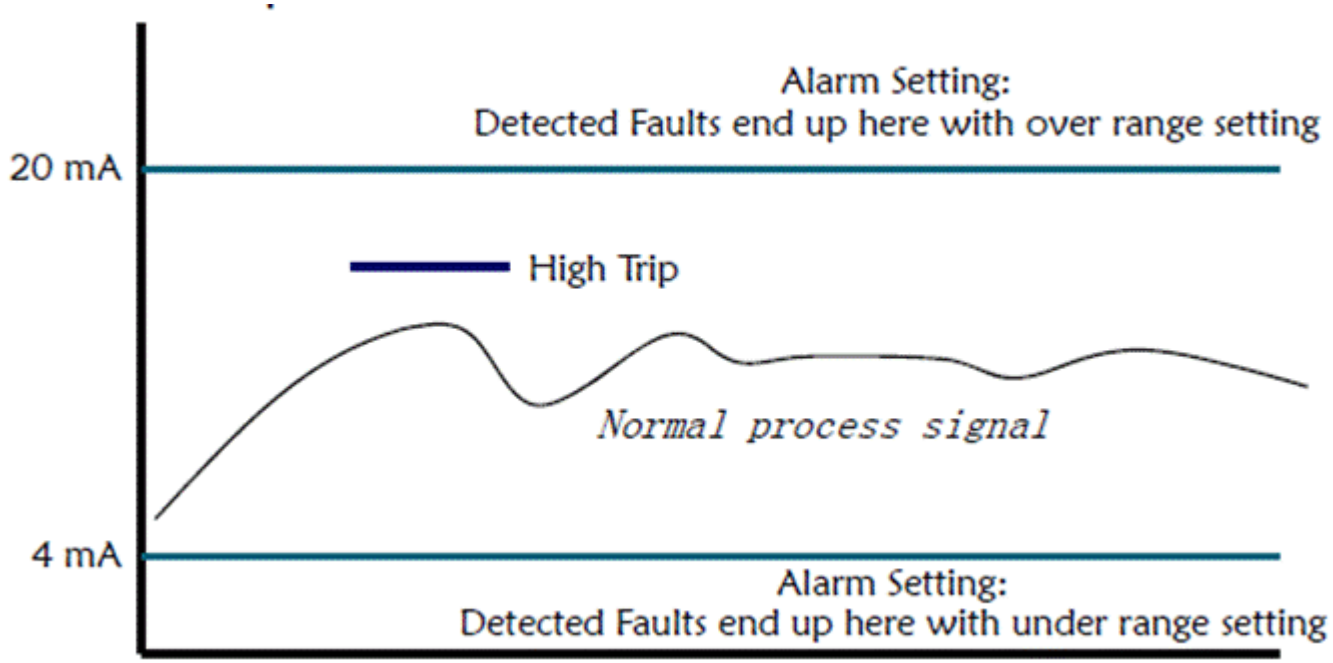
Prior Use justification documentation REQUIRED

EQUIPMENT ITEM	General Purpose PLC			ITEM NO.	4.1.1
GENERAL INFORMATION					
MANUFACTURER	Generic Equipment				
MODEL	~~~				
LOGIC SOLVER TYPE	PLC	BETA FACTOR [%]		N/A	
CONFIGURATION	1oo1	HARDWARE FAULT TOLERANCE		0	
ARCHITECTURE TYPE	B	CERTIFIED FOR USE UP TO SIL		N/A	
ASSESSMENT	N/A	BY	N/A		
DATA SOURCE	exida Comprehensive Analysis				
REMARKS	None				

FAILURE RATE DATA		PER 10^9 HOURS [FITS]						
	MODEL #	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	λ^{AD}	λ^{AU}	λ^{NE}
MAIN PROCESSOR	N/A	4500	500	3500	1500			
POWER SUPPLY	N/A	4513	238	238	13			
ANALOG IN MODULE	N/A (16)	850	150	750	250			
ANALOG IN CHANNEL		25	25	13	38			
DIGITAL IN MODULE	N/A (16)	425	75	375	125			
DIGITAL IN CHANNEL		50	50	25	75			
ANALOG OUT MODULE	N/A (16)	850	150	750	250			
ANALOG OUT CHANNEL		125	125	63	188			
DIGITAL OUT LOW MODULE	N/A (16)	425	75	375	125			
DIGITAL OUT LOW CHANNEL		50	50	25	75			
DIGITAL OUT HIGH MODULE	N/A (16)	425	75	375	125			
DIGITAL OUT HIGH CHANNEL		100	100	50	150			

Trip Setting

Alarm Setting Diagnostic Filtering



Diagnostic Filtering:

- Detection of over range / under range (invalid) signals
- Detection of rate of change (indication of internal transmitter error) – also called input filtering

Example 2:

High Pressure Protection Loop Transmitter - DCS - Solenoid

If we assume “clean service” on the pressure transmitter – no plugged impulse line problem then:

Lambda DU transmitter = 98 FITS (1 failure per 109 hours)

The SIF in the DCS Logic Solver has one analog input, all common circuitry and one digital output

Lambda DU DCS =		(1 * 38)	One Analog Input Channel
	+	250	Analog Module Common
	+	1500	Main Processor
	+	13	Power Supply
	+	125	Digital Output Module Common
	+	(1 * 150)	One Digital Output High Current Channel
	=	2076 FITS	

SIF Verification Example

PFDavg

Example 2 High Pressure Protection Loop. Transmitter - DCS - Solenoid

	Lambda DU (λ^{DU})
Transmitter	98 x 10-9 failures per hour
Logic Solver	2076 x 10-9 failures per hour
Solenoid	0.585 x 10-6 failures per hour

PFDavg = $\lambda^{DU} * \left(\frac{TI}{2}\right)$

PFDavg = (0.000002759* 8760) / 2

PFDavg = 0.012

RRF = 1/PFDavg = 83 → SIL 1

Use simplified equation for first pass. Assuming perfect proof testing very optimistic!

SIF Verification Example

SFF

Transmitter SFF is 82%, smart device therefore Type B. Still limited to SIL 1

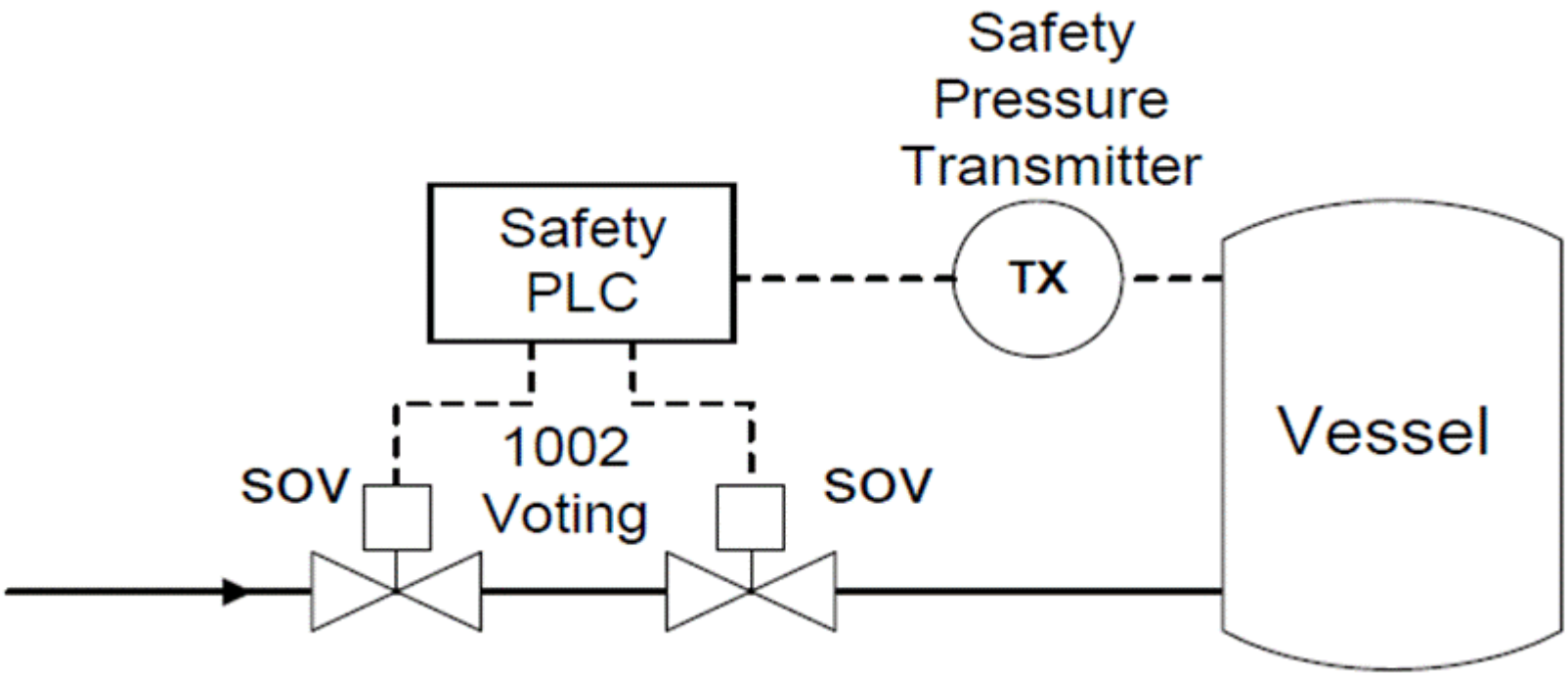
TYPE B Subsystem — **Demand Mode**

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	Not allowed	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

NOTE A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function

Example - 3:

Safety Transmitter +Safety PLC+1oo2 Solenoid



Example - 3:

Safety Transmitter +Safety PLC+1oo2 Solenoid

Equipment Item	Rosemount 3051S SIS		Item No.	1.6.18
General Information				
Manufacturer	Rosemount Inc.			
Model	3051S SIS, 3051S_C / 3051S_T			
Measurement Type	Pressure			
Analog / Digital	Analog	Hardware Fault Tolerance	0	
Architecture Type	B	Certified for use up to SIL	2 / 3	
Assessment	IEC 61508 Certification	By	exida / RWTUV Systems GmbH	
Data Source	FMEDA by exida			
Remarks	None			

Failure Rate Data	Per 10^9 hours [FITs]		
	Coplanar version	In-Line version	
Fail Low	277	280	
Fail High	62	59	
Fail Detected	500	470	
Fail Dangerous Detected			
Fail Dangerous Undetected	73	68	
Fail Safe Detected			
Fail Safe Undetected			
Fail Annunciation Detected			
Fail Annunciation Undetected	39	31	
Fail No Effect	409	437	
SFF [%]	94.6	94.9	

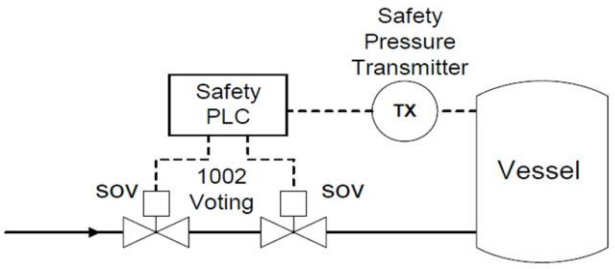
exida.com®
excellence in dependable automation

Failure Modes, Effects and Diagnostic Analysis

Project:
3051S SIS Pressure Transmitter,
with Safety Feature Board, Software Revision 3.0

Customer:
Rosemount Inc.
Chanhassen, MN
USA

Contract No.: Ros 02/11-07 R2
Report No.: Ros 02/11-07 R001
Version V2, Revision R4, August 27, 2007
William M. Goble – John C. Grebe



Justification via IEC 61508 Certification

Example - 3:

Safety Transmitter +Safety PLC+1oo2 Solenoid

EQUIPMENT ITEM	Emerson DeltaV SIS Redundant SLS		ITEM NO. 4.1.10
GENERAL INFORMATION			
MANUFACTURER	Fisher-Rosemount Systems		
MODEL	DeltaV SIS Redundant SLS		
LOGIC SOLVER TYPE	PLC	BETA FACTOR [%]	2
CONFIGURATION	2oo2D	HARDWARE FAULT TOLERANCE	0
ARCHITECTURE TYPE	B	CERTIFIED FOR USE UP TO SIL	3
ASSESSMENT	IEC 61508 Certification	BY	exida / RWTÜV Systems GmbH
DATA SOURCE	FMEDA by exida		
REMARKS	None		

FAILURE RATE DATA		PER 10^9 HOURS [FITS]						
	MODEL #	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	λ^{AD}	λ^{AU}	λ^{NE}
MAIN PROCESSOR	SLS1508	1099	15	1298	6	1052	203	689
ANALOG IN CHANNEL		29	0	23	0.008	8	14	41
DIGITAL IN CHANNEL		13	27	13	0	8	11	46
ANALOG OUT CHANNEL		29	0	18	0.008	8	14	41
DIGITAL OUT CHANNEL		20	0	12	0	5	4	14
COMMON FAILURES								
MAIN PROCESSOR	SLS1508		38					
ANALOG IN CHANNEL			12	3				2
DIGITAL IN CHANNEL			12	3				2
ANALOG OUT CHANNEL			23	3				2
DIGITAL OUT CHANNEL			16	0				0


exida

Certificate / Certificat
Zertifikat / 認証
FRS 060530 C001

DeltaV SIS

Emerson Process Management
Fisher Rosemount Systems, Inc.
Austin, TX USA

Has been assessed per the relevant requirements of:
IEC 61508 Parts 1, 2, 3
NFPA 72

Reports:
FRS 04-09-22 R001 FMEDA Report V2 R1
FRS 06-05-30 R001 Assessment Report V1 R2
FRS 03-02-15 R003 V3 R1 Markov Model Report

Validity:
This assessment is valid for the DeltaV SIS safety logic solver.

This assessment is valid until May 1 2010.

And meets requirements providing a level of integrity to:
Systematic Integrity: SIL 3 Capable
Random Integrity for Type B device: SIL 3 @ HFT=0

Safety Function:
The DeltaV SIS will perform the configured safety logic and execute the automatic diagnostics in the specified time period.

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

Product Assessor
Auditor

exida Certification Services

Justification via IEC 61508 Certification

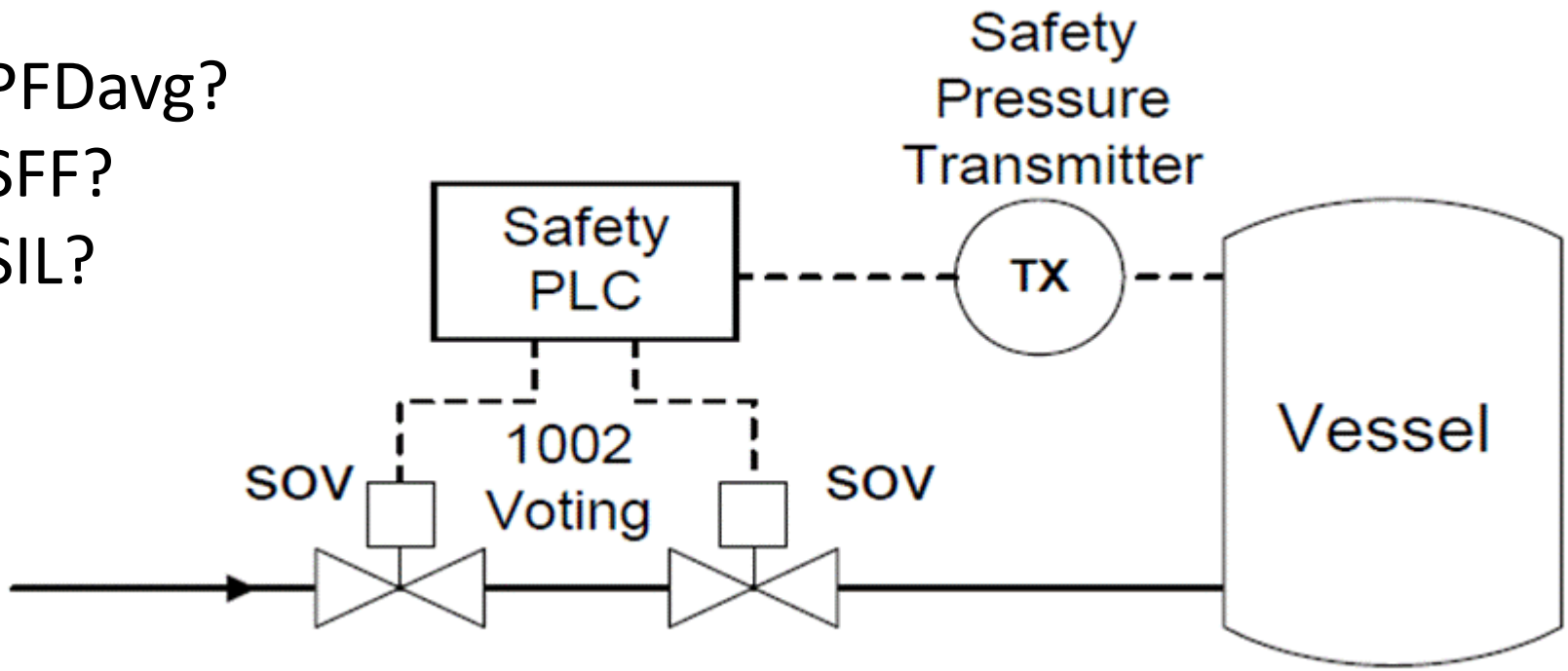
Example - 3:

Safety Transmitter +Safety PLC+1oo2 Solenoid

PFDavg?

SFF?

SIL?



SIF Verification

The achieved SIL is the minimum of;

- SIL based on PFDavg (SILpfd)
- SIL based on Architectural Constraints (SILac)
- SIL based on Equipment Capability (SILcap)

Majority of cases SILpfd and SILac will be identical

Users need to select IEC 61508 certified equipment or justify the use of specific equipment based on Prior Use arguments

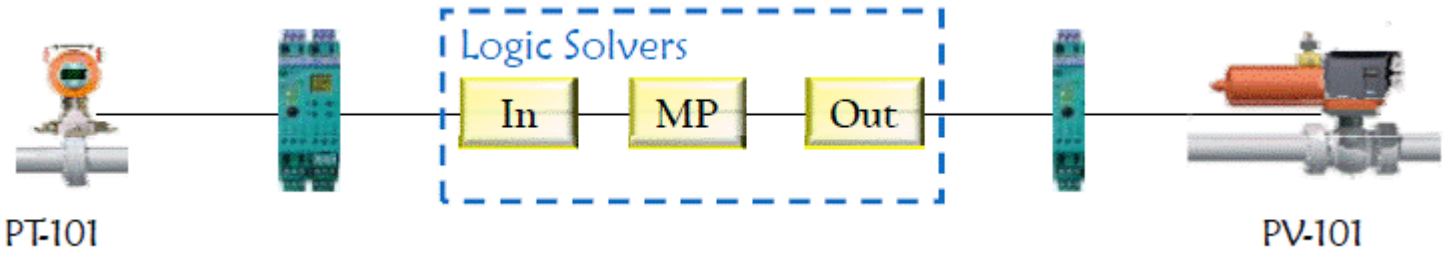
Rule 1: Comply to PFDavg

SIL based on PFDavg (SILpfd)

The PFD for the total SIF =

PFDsensor + PFDmux + PFDinput + PFDmp + PFDOutput + PFDrelay + PFDfe + PFDprocess-connection

PFDavg = $\lambda^{DU} * \left(\frac{TI}{2}\right)$



SLC– Realization Phase

Maximum Probability of Failure

PFDavg (low demand mode applications)

SAFETY INTEGRITY LEVEL	LOW DEMAND MODE OF OPERATION (AVERAGE PROBABILITY OF FAILURE TO PERFORM ITS DESIGN FUNCTION ON DEMAND)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

PFH (high or continuous demand mode applications)

SAFETY INTEGRITY LEVEL	HIGH OR CONTINUOUS DEMAND MODE OF OPERATION
4	$\geq 10^{-5}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-5}$

SLC– Realization Phase

SIL based on Architectural Constraints (SILac)

SFF of Device [See FMEDA]

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	not allowed	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.

NOTE 2 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.

NOTE 3 See annex C for details of how to calculate safe failure fraction.

Rule 2: Comply to Architectural Constraints

SFF and Hardware Fault Tolerance

82,5%

...Defines The Required Architecture

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	[illegible]	[illegible]	[illegible]
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL 3	SIL 4	SIL 4

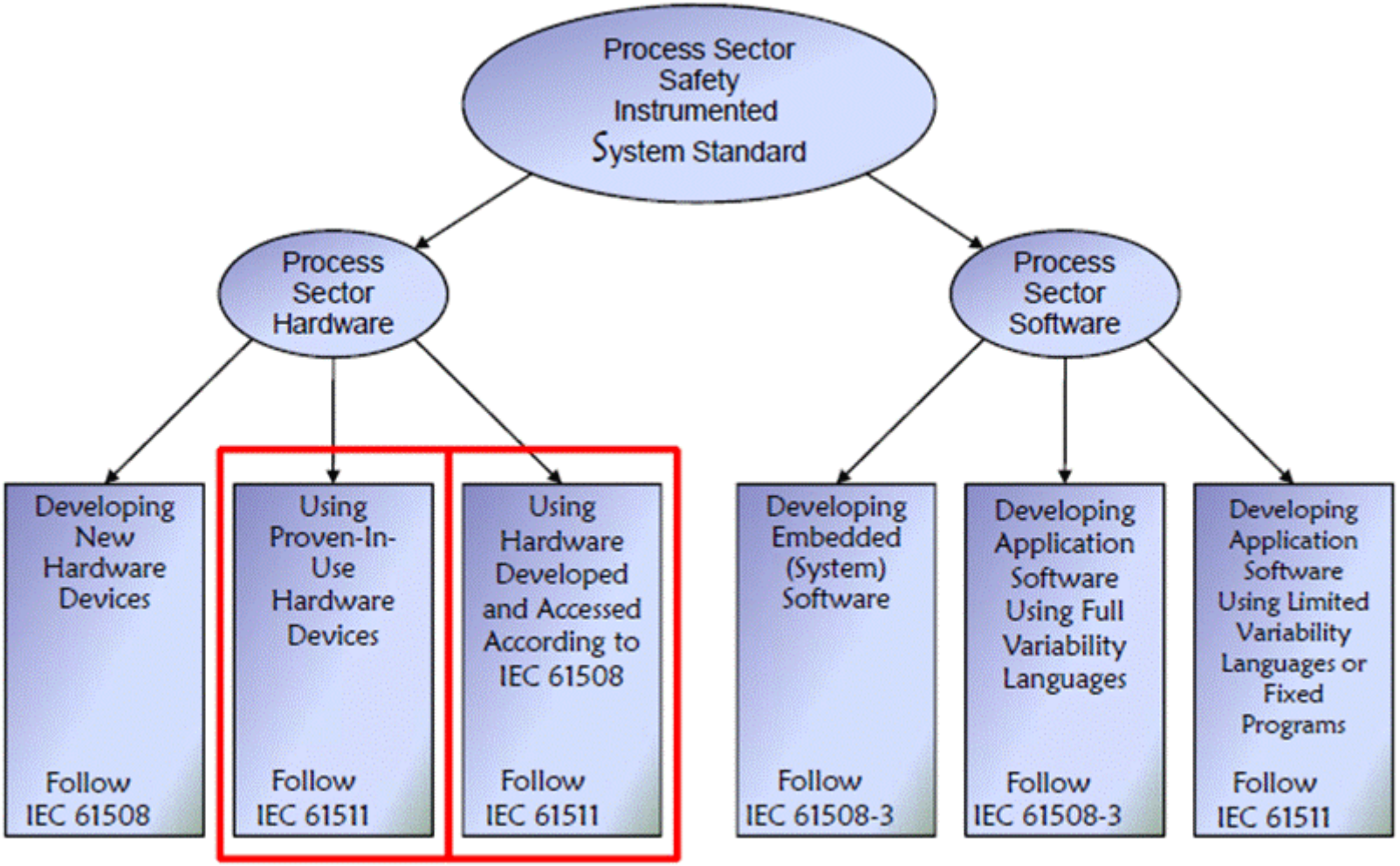
NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.

NOTE 2 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.

NOTE 3 See annex C for details of how to calculate safe failure fraction.

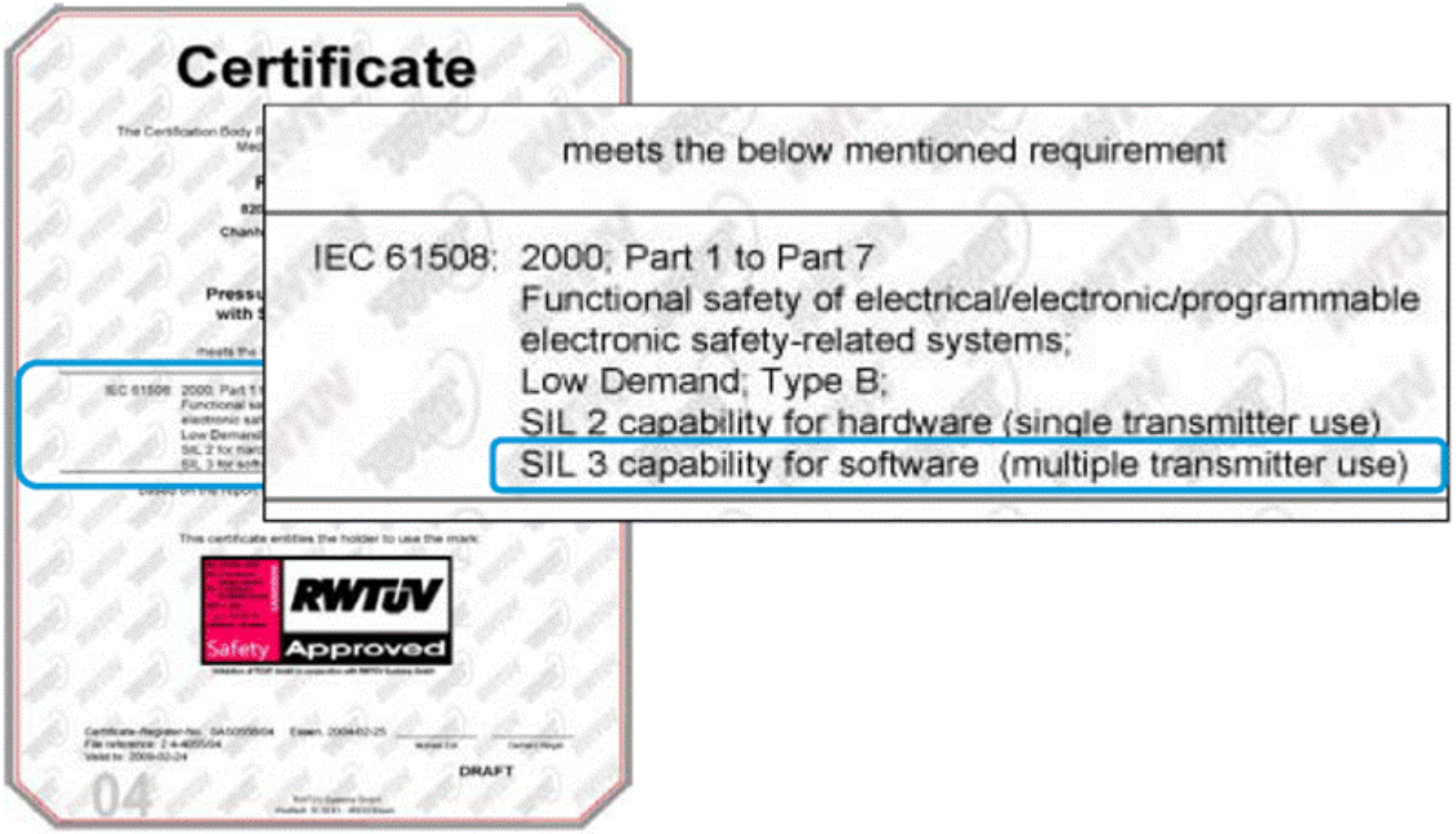
SLC– Realization Phase

Equipment SIL Capability



SLC– Realization Phase

Equipment SIL Capability



SLC– Realization Phase

Summary Realization phase;

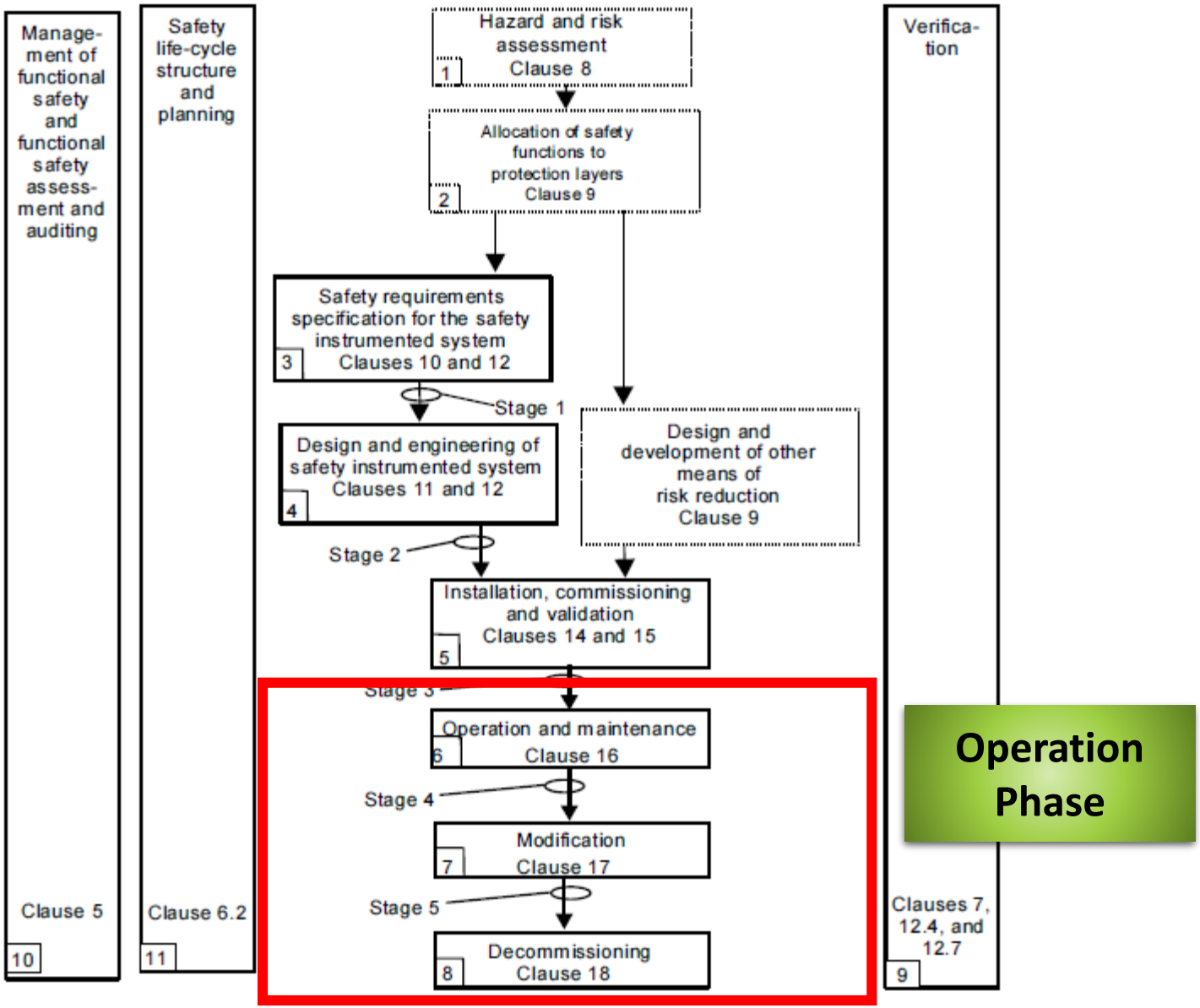
- Develop a conceptual design (for technology, architecture, periodic test interval, reliability, safety evaluation),
- Develop a detailed design for installation planning, commissioning, start up acceptance testing, and design verification.

Section - 3.3

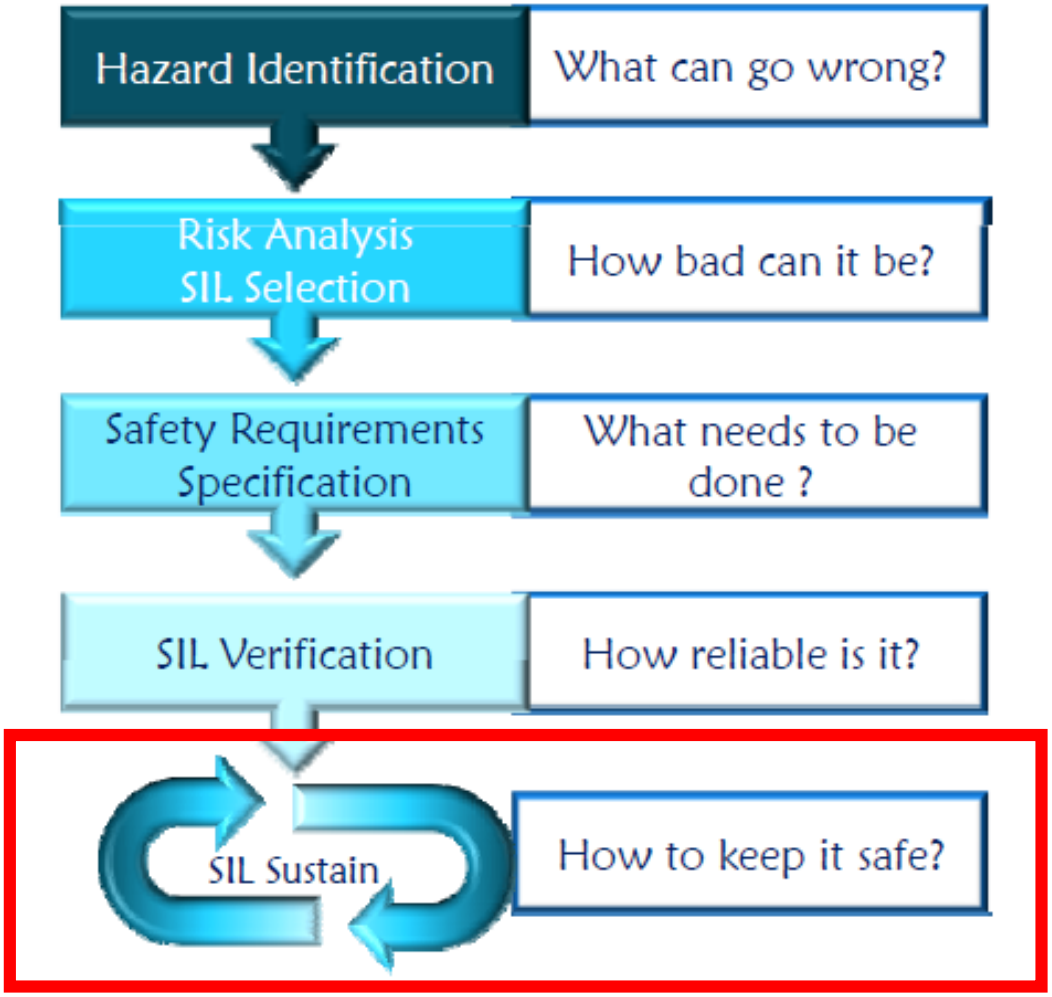
SAFETY LIFECYCLE [SLC]
Operations Phase

It begins at start up of plant and continues until the Safety Instrumented System [SIS] is decommissioned or redeployed. The most significant part of Operations phase is the maintenance and testing of the SIS.

SLC– Operations Phase



SLC– Operations Phase



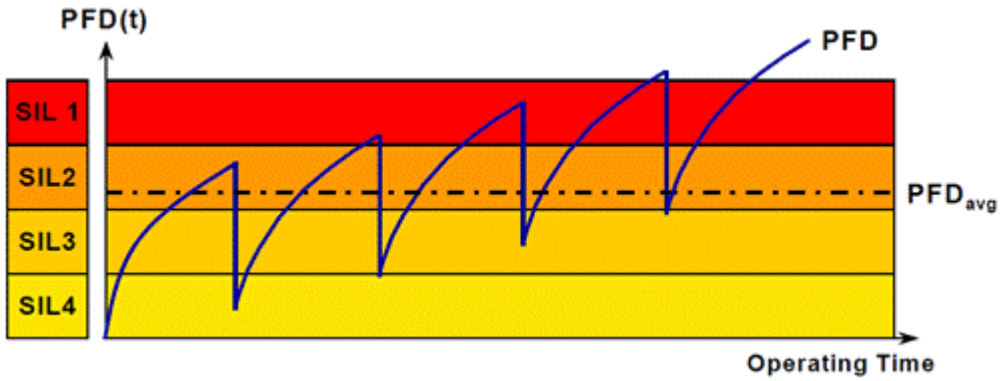
Operation Phase

SLC– Operations Phase

- Maintenance Planning
- Manufacturer‘s Maintenance Data
- Periodic Inspection Testing / Records

How to maintain a SIL?

- Functional Safety is based on achieving a SIL
  - SIL is based on average PFDavg in *low demand* systems
- Equipment Performance degrades with time
  - PFDavg increases with time
- Regular testing is needed to detect & repair failures
  - PFDavg sustained
- Equipment restored to ‘as new’ equivalent?



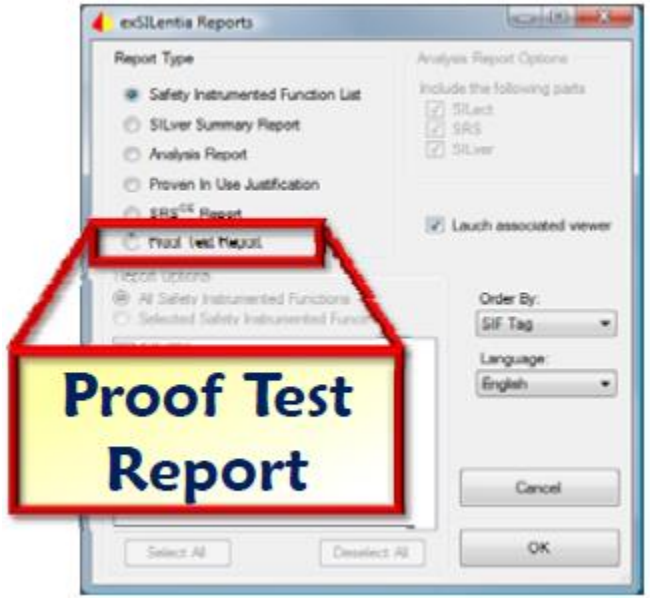
Periodic Proof Testing

A proof test detects failures not detected by automatic diagnostics

The maximum proof test interval will be published in the certificate

Tasks

- ✓Verify operation of field instruments
- ✓Validate logic and operation
- ✓Document results of all periodic testing



Modification and De-Commissioning

- Periodically review hazards and take corrective action if necessary
  - ✓Review incidents
  - ✓Review Facility Change Notices or Management of Change (MOC) documents

Update SIS according to the appropriate safety lifecycle step

Maintenance Planning

- All tests required to verify proper operation of Safety Instrumented Function must be planned
- Proper periodic test interval that was calculated during SIF verification must be documented as part of the plan
- Online? Offline? Bypass Procedures?
- Proof test procedures must be at least as effective as planned during the SIF verification

Proof Test?

The purpose of the Proof test is to verify that safety instrumented works properly. It is often assumed that if it works properly it has not failed.

Procedure:

Block valve from closing.

1. Move input signal above trip point
2. Verify that valve attempted to close
3. Move input signal back to normal below trip point
4. Remove valve block

Assume 100% Diagnostic coverage ??

100% Coverage?

100% coverage is not likely due to intermittent faults and not exercising all functionality.

Transmitter failures

Logic Solver Failures

Final Elements Failures

What are the DUs? What are the dangerous failures not detected by any automatic diagnostics?

Assume 100% Diagnostic coverage ??

Proof Test

~~The purpose of the Proof test is to verify that safety instrumented works properly. It is assumed that if it works properly it has not failed.~~

The purpose of the Proof test is to detect any failures not detected by automatic on-line diagnostics – dangerous failures, diagnostic failures, parametric failures and to detect unauthorized program changes

Safety Manual

- Products intended for SIF applications are supplied with a “Safety Manual”
- The “safety manual” may be part of another document
- The Safety Manual contains important restrictions on how the product must be used in order to maintain safety
  - Environmental restrictions
  - Design restrictions
  - Periodic Inspection / Test requirements
  - Failure rate / failure mode data

Safety Manual : Test Content

From Rosemount 3051S, Safety:
Safety Manual : Test Content
Proof Test 1 – 65%
Proof Test 2 – 98%
Why bother with proof test 1?

OPERATION AND MAINTENANCE

Proof Test

The following proof tests are recommended. Proof test results and corrective actions taken must be documented at *www.emersonprocess.com/rosemount/safety/certtechdocumentation.htm* in the event that an error is found in the safety functionality.

Use "HART Fast Key Sequence" on page S-4 to perform a Loop Test, Analog Output Trim, or Sensor Trim.

Proof Test 1

Conducting an analog output Loop Test satisfies the proof test requirements and will detect more than 50% of DU failures not detected by the 3051S automatic diagnostics.

Required Tools: HART host/communicator and mA meter.

1. On HART host/communicator enter the Fast Key Sequence 1, 2, 2.
2. Select "4 Other."
3. Enter the milliampere value representing a high alarm state.
4. Check the reference meter to verify the mA output corresponds to the entered value.
5. Enter the milliampere value representing a low alarm state.
6. Check the reference meter to verify the mA output corresponds to the entered value.
7. Document the test results per your requirements.

Proof Test 2

This proof test, when combined with Proof Test 1, will detect over 99% of DU failures not detected by the 3051S automatic diagnostics.

Required Tools: HART host/communicator and pressure calibration equipment.

1. Perform a minimum two point sensor calibration check using the 4-20mA range points as the calibration points.
2. Check the reference mA meter to verify the mA output corresponds to the pressure input value.
3. If necessary, use one of the "Trim" procedures available in the 3051S reference manual to calibrate.
4. Document the test results per your requirements.

NOTE
The user determines the proof-test requirements for impulse piping.

Safety Manual : Test Content

From Rosemount 3051S, Safety:

Proof Test 1 – 65%

Proof Test 2 – 98%

Why bother with proof test 1?

Because the time interval between the more expensive PROOF TEST 2 can extended several years!!

Strategic Proof Test

The purpose of the Proof test is to detect any failures not detected by automatic on-line diagnostics and program changes.

Strategic Proof Test

1. We can design proof test procedures that are easier to perform, cost less and are more likely to actually get done.
2. By understanding the actual DU/AU failures in our instruments we can significantly improve our test coverage as well as lower cost.
3. We can detect program changes via tools built into most products.

Effective Testing Techniques

Analog Sensors : Force process variable between –10% and 110% of scale. This tests transmitter, power supplies and wiring resistance. Inspect for corrosion on terminal strips and loose wiring. Inspect (or perform cleanout) for plugged impulse lines.

Discrete Sensors : Force process variable over full scale and inspect for proper movement of mechanisms as well as switch closure at the proper point. Inspect for corrosion on terminal strips or switch mechanical components.

Effective Testing Techniques

Solenoids : Check for speed of response and sound level during a full cycle of air pressure. Inspect for corrosion and clogged air inlets

Pneumatic Actuators : Inspect for air consumption rates and clogged air inlets. During a partial stroke check for speed of response and pressure curve During a full stroke check for speed of curve. response, pressure curve and abnormal response when seating. When valve is closed, check for leakage.

Safety Manual

Mechanical Integrity

The safety manual will often include specific tests and inspections that must be done on a periodic basis. For example:

“The window of the flame detector must be inspected to ensure that it is clean and clear. The maintenance schedule must be established based on plant conditions”.

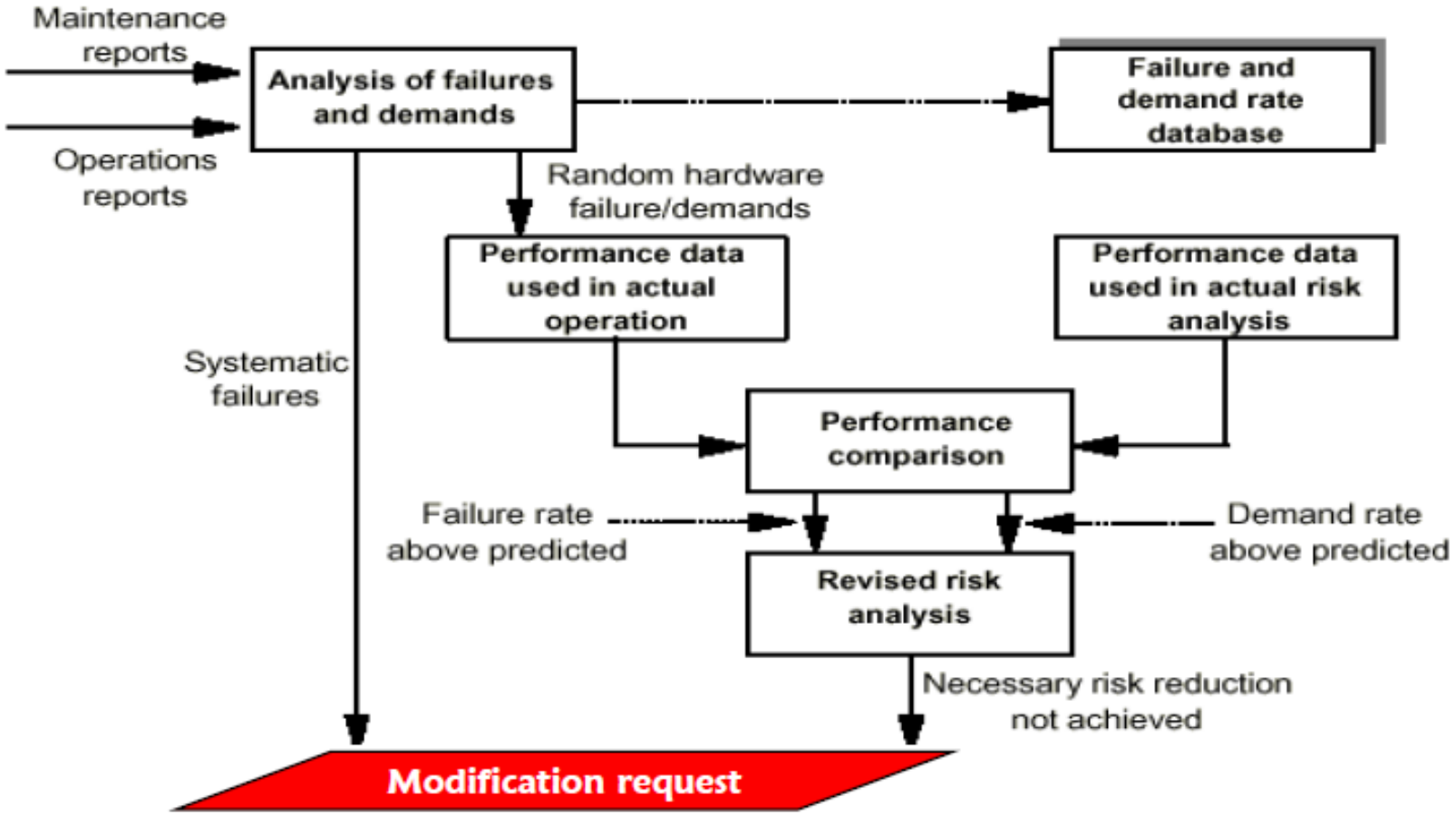
The designer must estimate plant conditions and add periodic inspection to the mechanical integrity procedures

Periodic Test & Inspection Records

- Actual Testing must be documented:
  - Test details
  - Personnel, date
  - Bypass authorization
  - Tests performed
  - Results
  - System restored

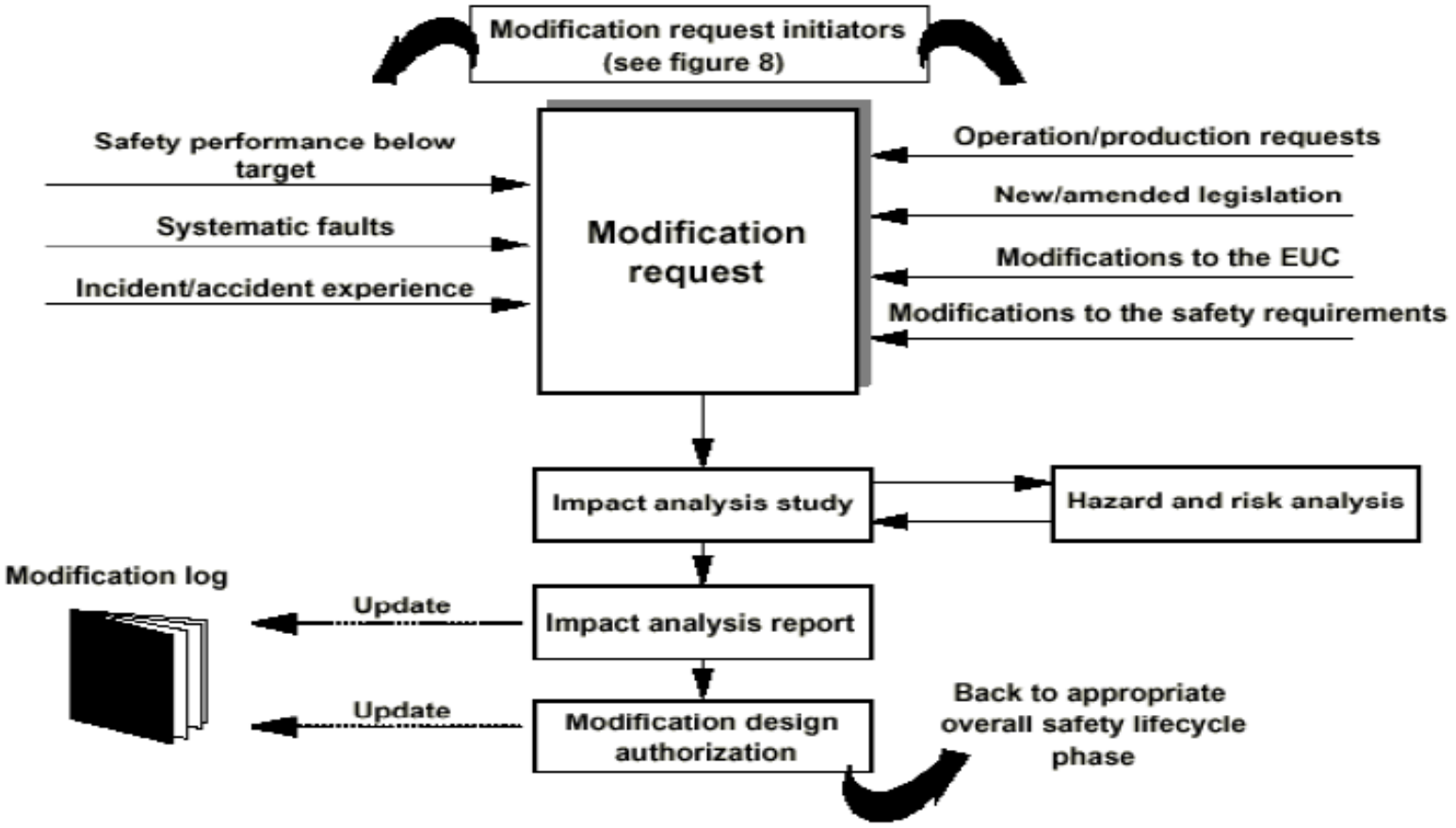
Management of Change

Before Modification Request;



Management of Change

After Modification Request,



SLC– Operations Phase

In short the operation phase of the Safety Life Cycle begins with a validation of the design. Following check-list has to be used prior to start-up;

- Does the system actually solve the problems identified during the hazard analysis?
- Have all necessary design steps been carried out successfully?
- Has the design met the target SIL for each Safety Instrumented Function?
- Have the maintenance procedures been created and verified?
- Is there a management of change procedure in place?
- Are operators and maintenance personnel qualified and properly trained?

If the answers to these questions are acceptable, the process can proceed with startup and operation.

Section - 3.4

SAFETY LIFECYCLE [SLC]
Benefits
and
Impact on Field Devices

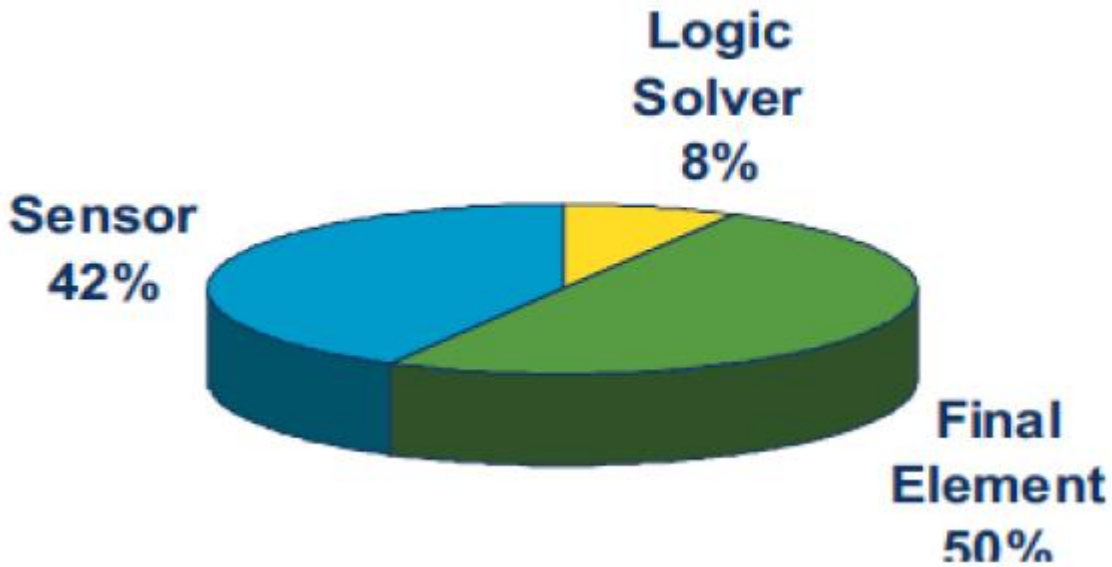
SLC– Benefit

Safety Life Cycle implantation provides a safer plant with low systematic errors. It decreases the cost of engineering and increases process up-time.

It considerably lowers operations and maintenance cost by selecting the right technology equipment with correct implementation, as well as providing proper guidelines for operation, maintenance, modifications and decommissioning. This will not only reduce plant risk, but it will also provide overall design consistency

SLC– Impact on Field Devices

Recent study reports from OREDA (Offshore Reliability Data Handbook) that 92% of all SIS failures occur in field devices such as final control elements and sensors



SLC– Impact on Field Devices

Following to OREDA study, a number of measures, listed below, can be used to minimize the number of dangerous failures relate to sensor component of SIF loop;

Use measurements that are as direct as possible. (Correct technology)

Control isolation or bleed valves to prevent uncoupling from the process between proof tests. (Installation and maintenance)

Use good engineering practice and well proven techniques for process connections and sample lines in order to prevent blockage, sensing delays, etc. (Correct specifications)

Use analogue devices (transmitters) rather than digital (switches). (Better design equipment selection)

Use appropriate measures to protect the process connections and sensors against effects of the process such as vibration, corrosion, and erosion. (Operation and maintenance)

Monitor the protective system process variable measurement (PV) and compare it against the equivalent control system PV, either by the operator or the control system. (Design, specification and operation)

Ensure integrity of process connections and sensors for containment, such as sample or impulse lines. Instrument pockets are often a weak link in process containment measures. (Better maintenance and modification plan)

SLC– Impact on Field Devices

Other matters that should also be considered for dangerous failures of final control elements of SIF loop can be minimized by a number of measures such as;

Valves should be properly selected, including correct sizing for actuator thrust requirement with additional safety cushion as per guidelines. It should never be assumed that a control valve can satisfactorily perform isolation functions without proper design and selection; (Specifications)

Process fluid and physical process condition should be properly considered for selecting suitable valve type and style. (Specifications)

Proper metallurgical selection of the valve body, trim material, linkages, etc. (Technical requirement)

Environmental conditions should be taken into account for minimizing stem blockage, corrosion, dust protection, etc. (Outside environmental Conditions)

Actuators may also include microprocessor-based Digital Valve Controllers (i.e., smart positioners) with configurable travel, stroking speed, pause time, etc. It is normally reasonably practicable for the Demand signal to act directly upon the final control element. (Predictive Maintenance)

SLC– Impact on Field Devices

Following to OREDA study, Dangerous failures of final control elements of SIF loop can be minimized by a number of measures such as;

Use of ‘fail-safe’ principles so that the actuator takes up the Safe state on loss of signal or power (electricity, air etc.); e.g. use of a spring return actuator; (De-Energize to trip) {Proper Specifications during SRS}

Provision for uninterruptible power or reservoir supplies of sufficient capacity for essential power; (Energize to Trip) {Proper Specifications during SRS}

Failure detection and performance monitoring (valve travel diagnostics, limit switches, time to operate, torque, etc.) during operation; (On-line Testing & Diagnostics) {Operation and Maintenance}

Exercising actuators or performing partial stroke shutoff simulation during normal operation in order to reveal undetected failures or degradation in performance Note that performance. this is not proof testing but it may reduce the probability of failure by improved diagnostic coverage; (Partial Stroke Test) {Testing and inspection}

Overrating of equipment; (Safety factor) {Design and Specification}

Section - 4

Safety Integrity Level [SIL] Study using Engineering Tools exSILentia®v-3.0

Section - 4.1

SIL Selection [SILect] – Tolerable Risk;

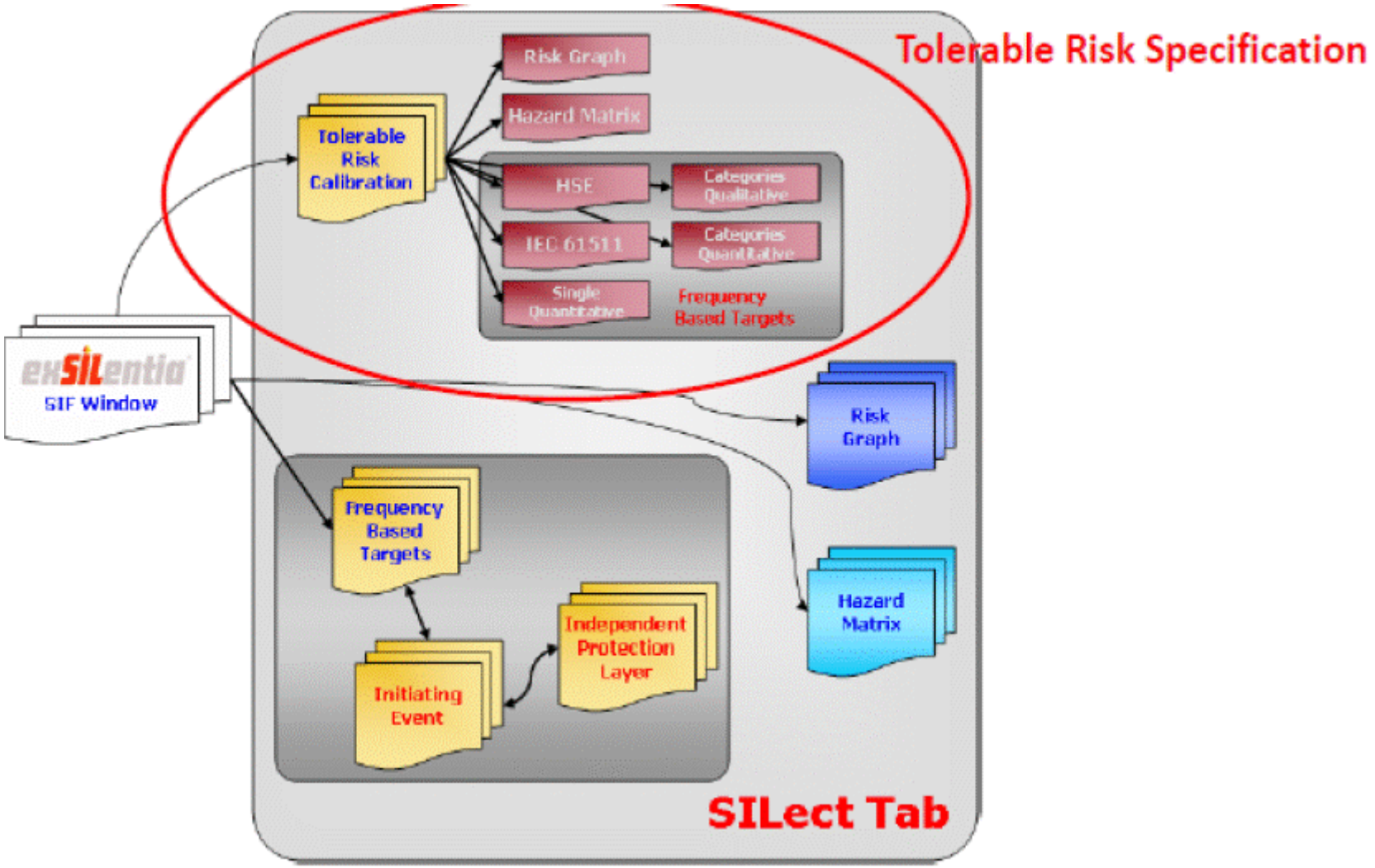
SILect Structure

Why Specify Tolerable Risk?

Specify Tolerable Risk for different SIL Selection Methods

- Risk Graph
- Hazard Matrix
- Frequency Based Targets (LOPA)

SILect Structure



Tolerable Risk

Why do I need to specify my Tolerable Risk Level? Otherwise you cannot determine what is your Required Risk Reduction [RRF] should be;

No Tolerable Risk Specified

$$RRF = \frac{\text{Unmitigated Risk}}{\text{Tolerable Risk}}$$

$$RRF = \frac{\text{Unmitigated Risk}}{???}$$

If “NO” Tolerable Risk

I cannot tolerate any Risk

- Tolerable Risk of “0” would lead to a required risk reduction of ∞
- Do not build or operate your plant

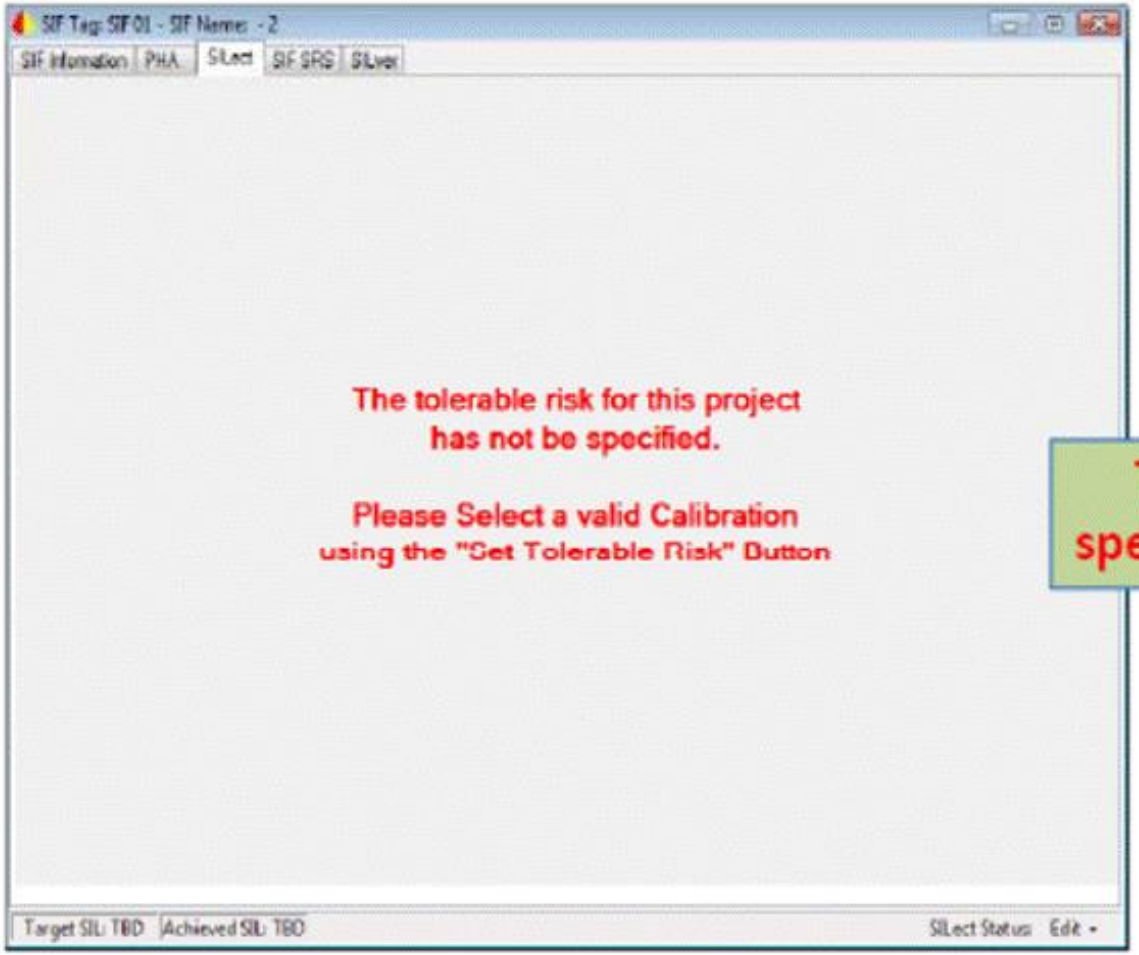
$$RRF = \frac{\text{Unmitigated Risk}}{\text{Tolerable Risk}}$$

Tolerable Risk = 0

$$RRF = \frac{\text{Unmitigated Risk}}{0} = \infty$$

Tolerable Risk

SILect Requires Tolerable Risk Specification



Tolerable Risk needs to be specified only once for a project

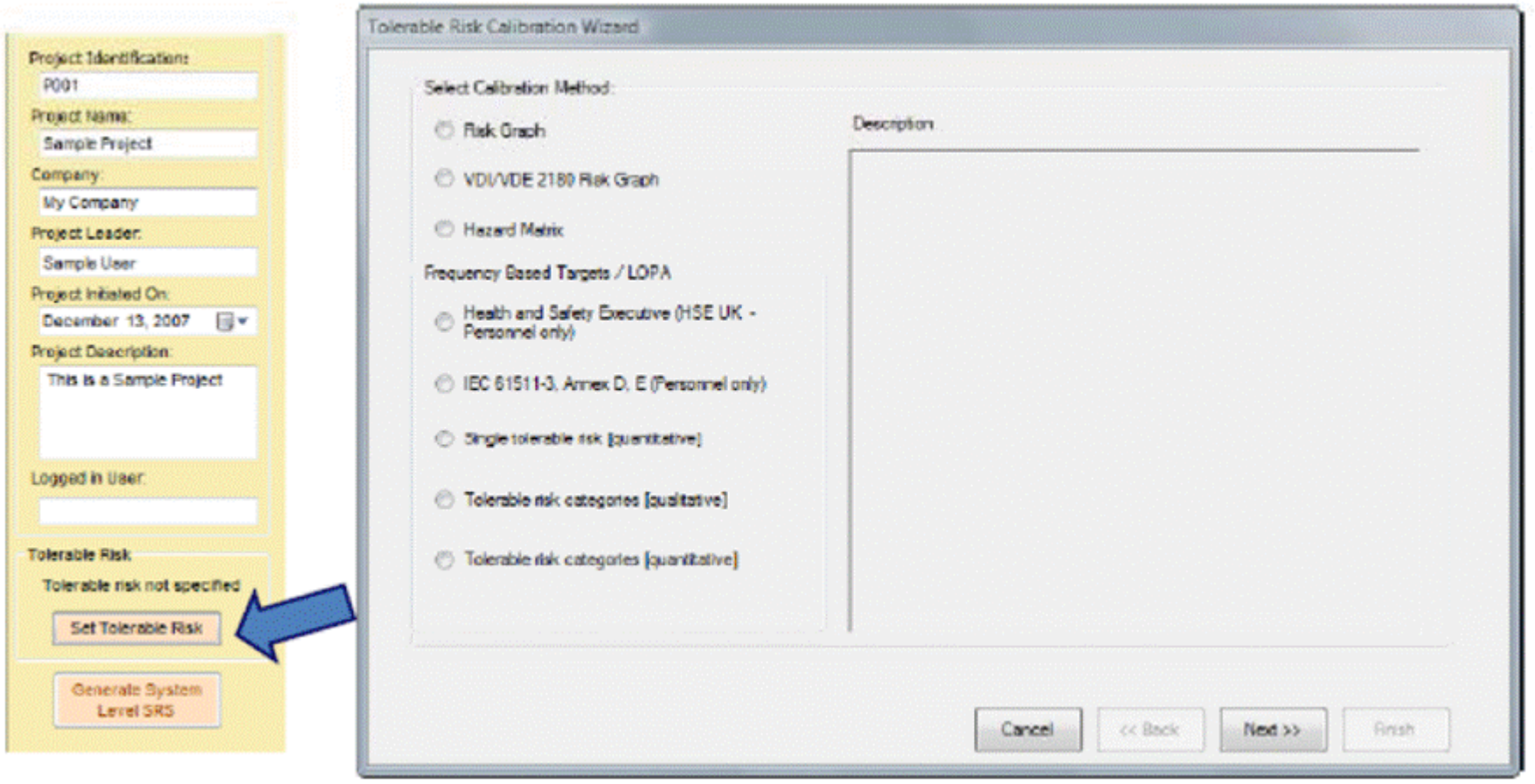
Risk Receptors

SILect allows consideration of three risk receptors (irrespective of SIL selection method)

- Personnel
- Environment
- Assets (Equipment / Monetary)
- User Defined / Custom

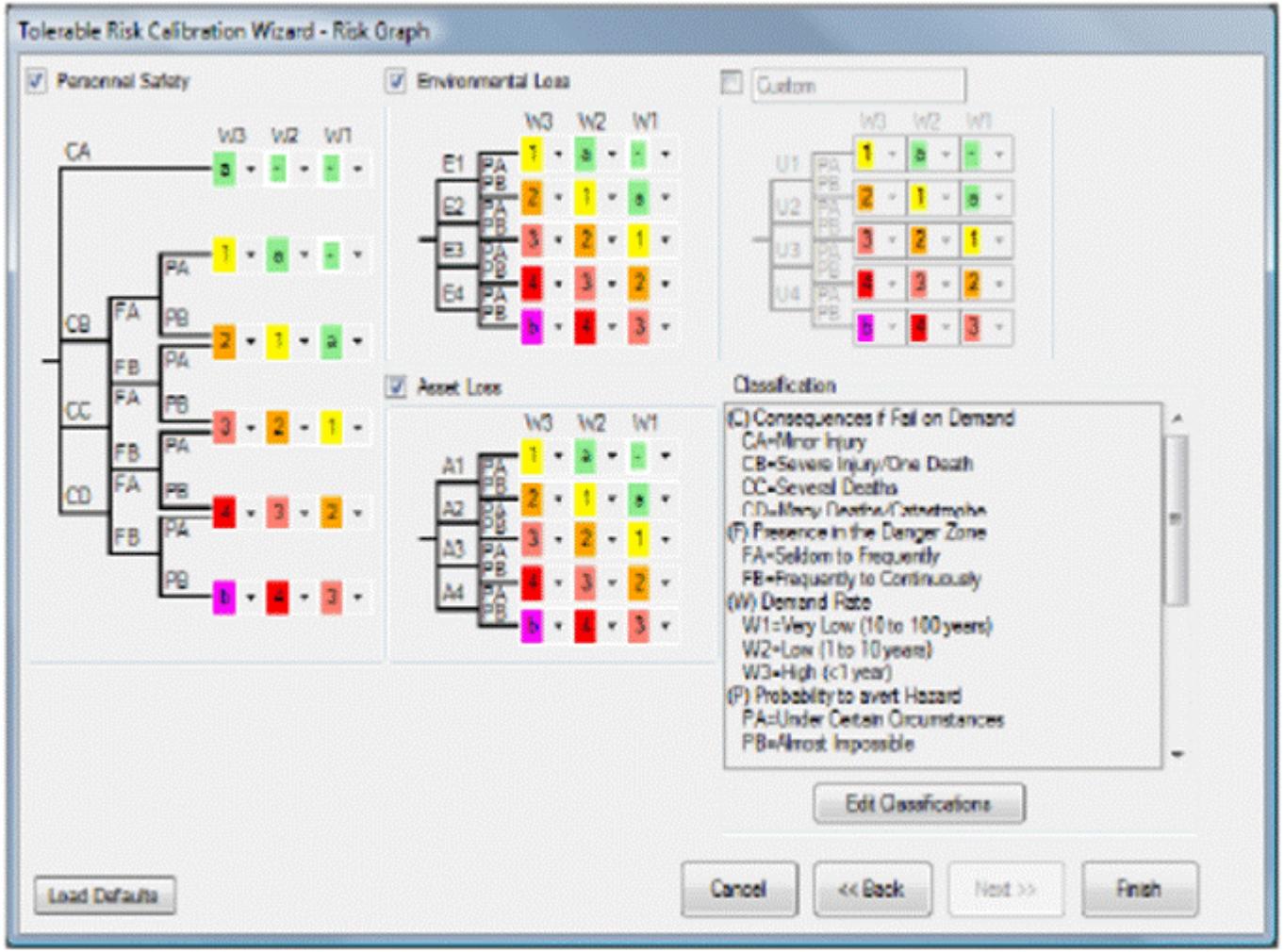
Tolerable Risk

Tolerable Risk Calibration Wizard



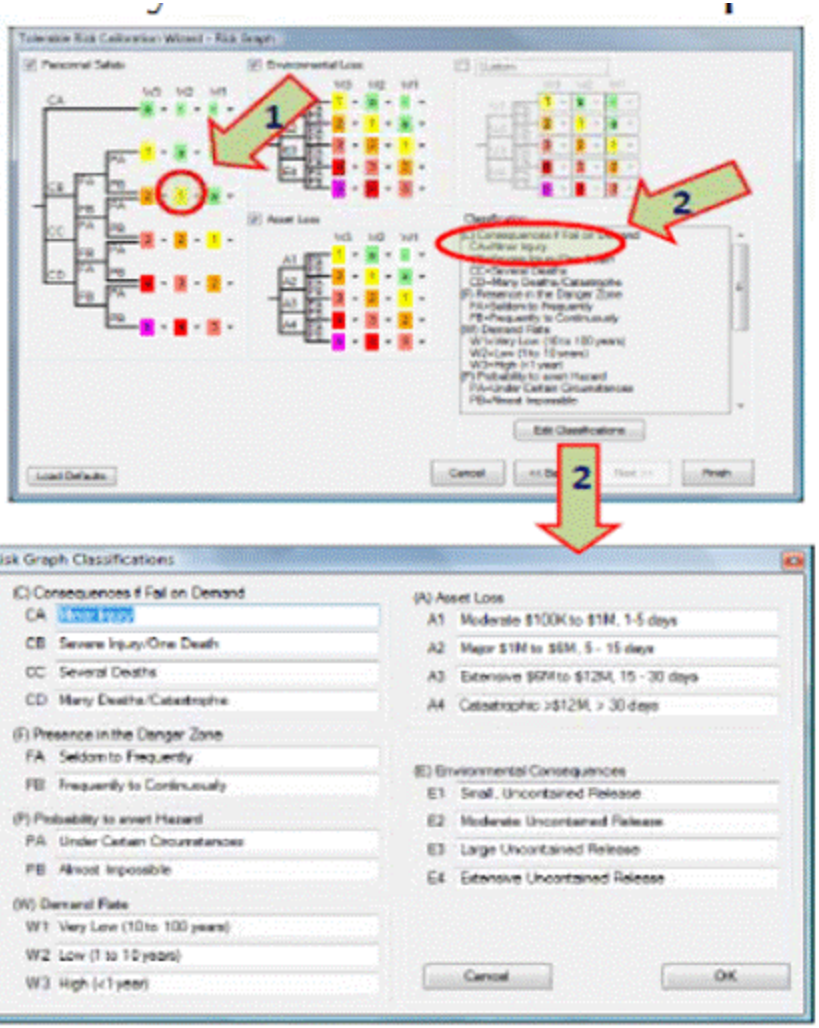
Tolerable Risk

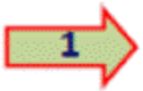
Risk Graph Calibration Wizard

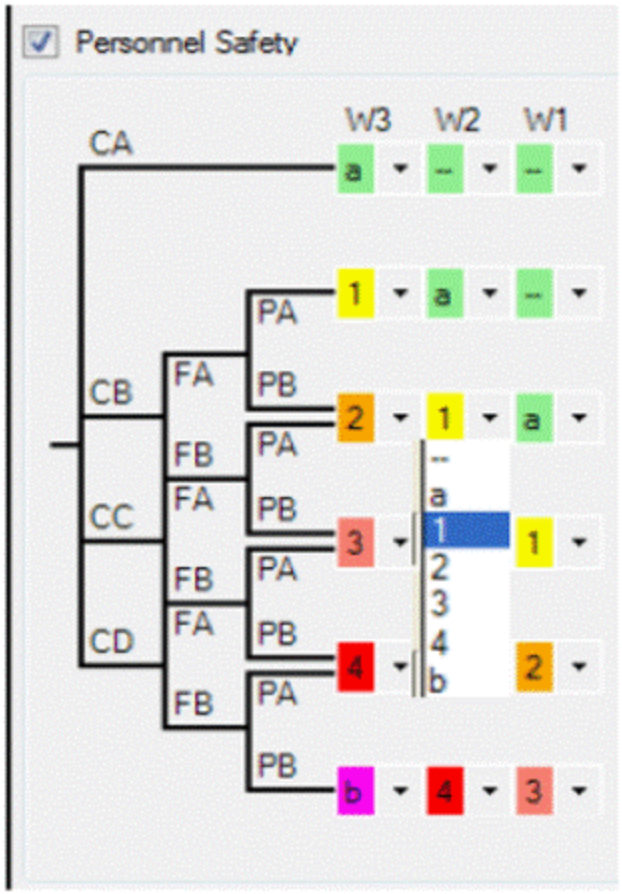


Tolerable Risk

Modify Parameter Descriptions

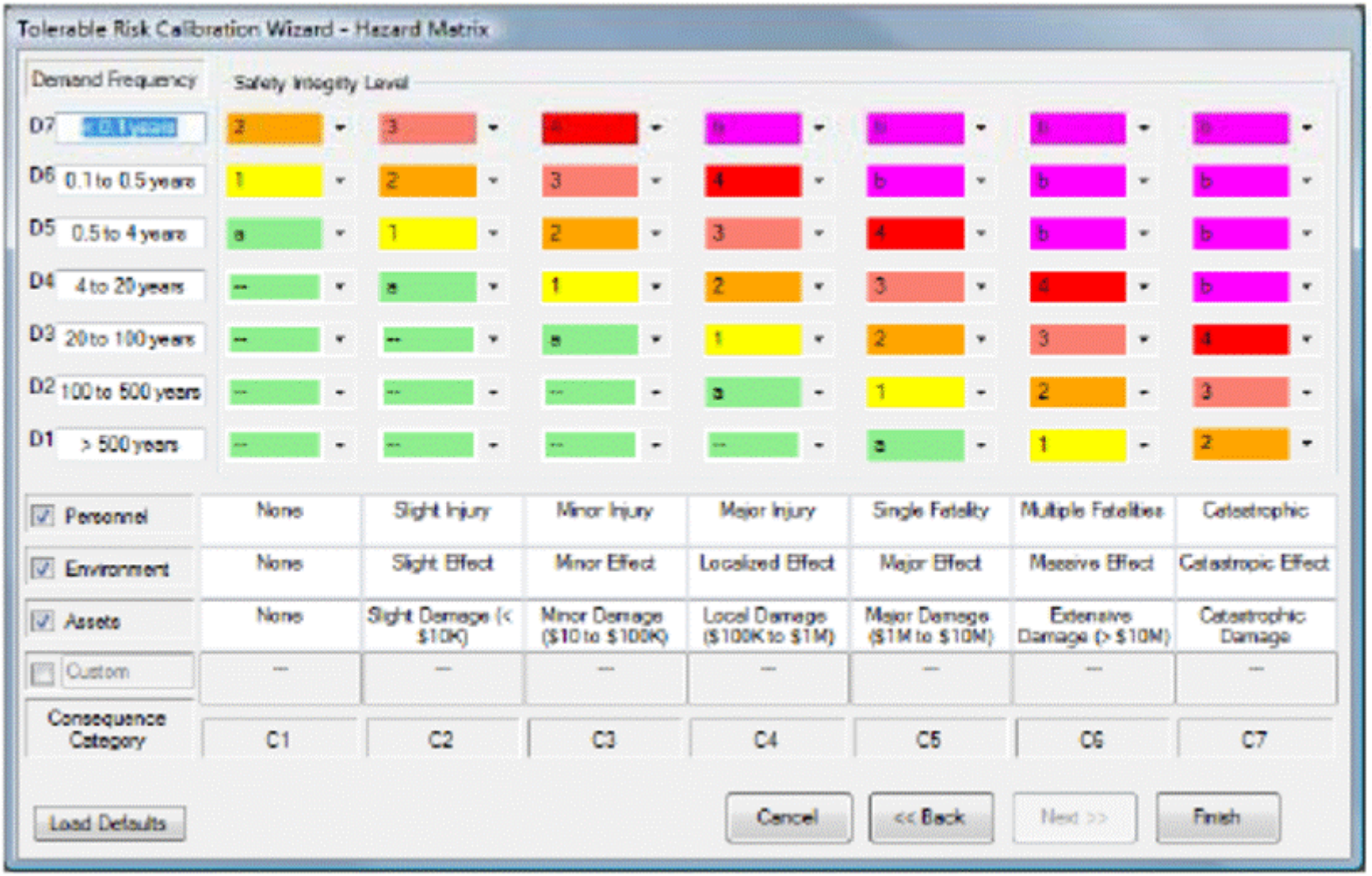






Tolerable Risk

Hazards Matrix Calibration Wizard



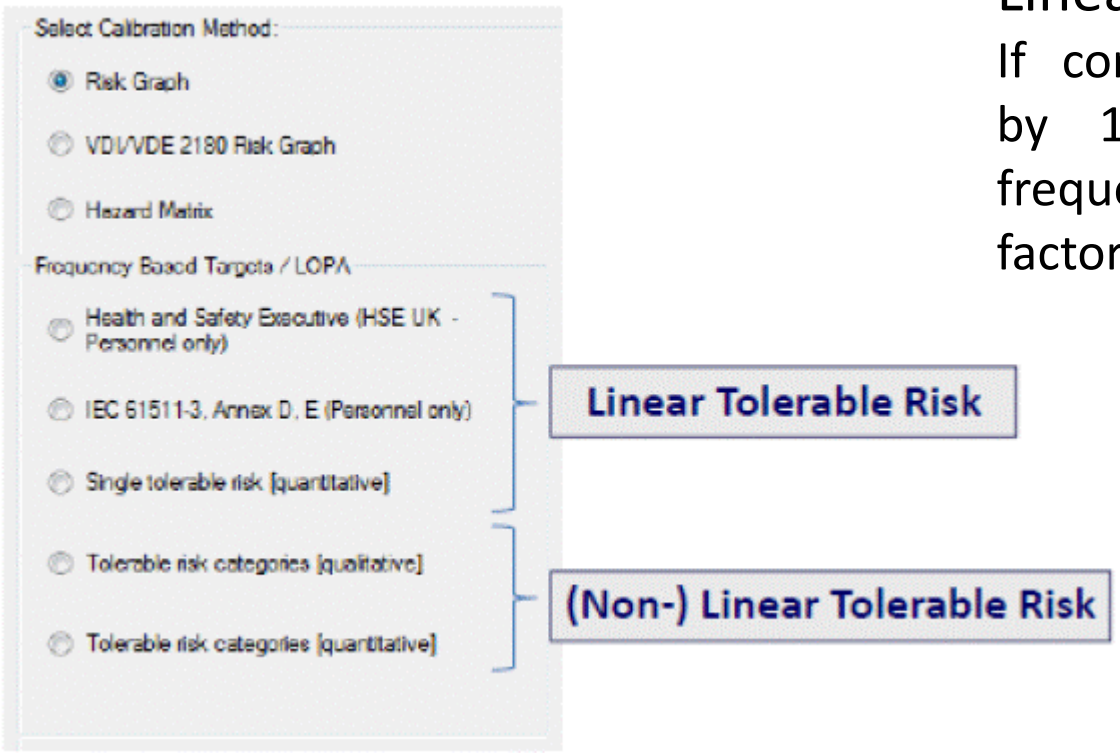
Tolerable Risk

Modify Parameter Descriptions

Slight Injury	Minor Injury	Major Injury	Single Fatility	Multiple Fatalities
Slight Effect	Minor Effect	Localized Effect	Major Effect	Massive Effect
Slight Damage (< $10K)	Minor Damage ($10 to $100K)	Local Damage ($100K to $1M)	Major Damage ($1M to $10M)	Extensive Damage (> $10M)
C1	C2	C3	C4	C5

Tolerable Risk

Frequency Based Target [LOPA]



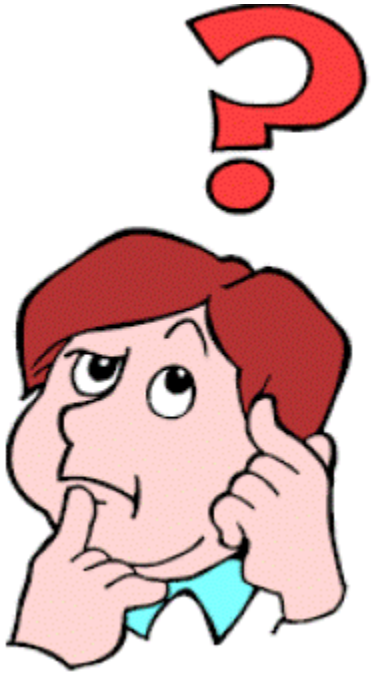
- Linear
  If consequence increases by 10 factor, tolerable frequency will decrease by factor 10

- (Non-) Linear
  - ✓ Tolerable risk specified for different category
  - ✓ Can be non-linear, e.g. if consequence increases by 10 factor, tolerable frequency could decrease by 100

SIL Selection with SILect

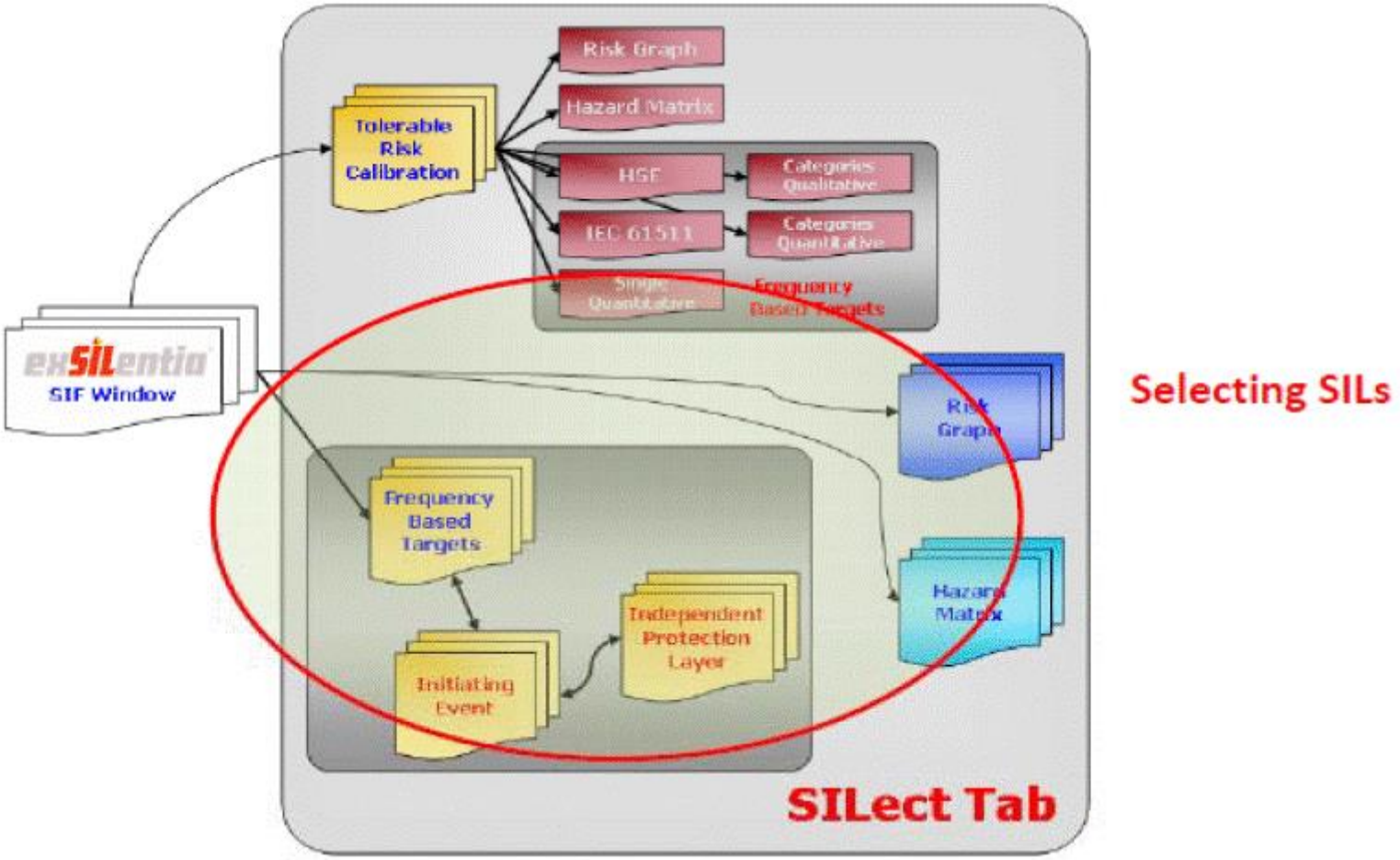
Perform SIL selection with different SIL Selection Methods;

- Risk Graph
- Hazard Matrix
- Frequency Based Targets (LOPA)
- Independent Protection Layers
- IPL Reuse



SIL Selection with SILect

SILect Structure;

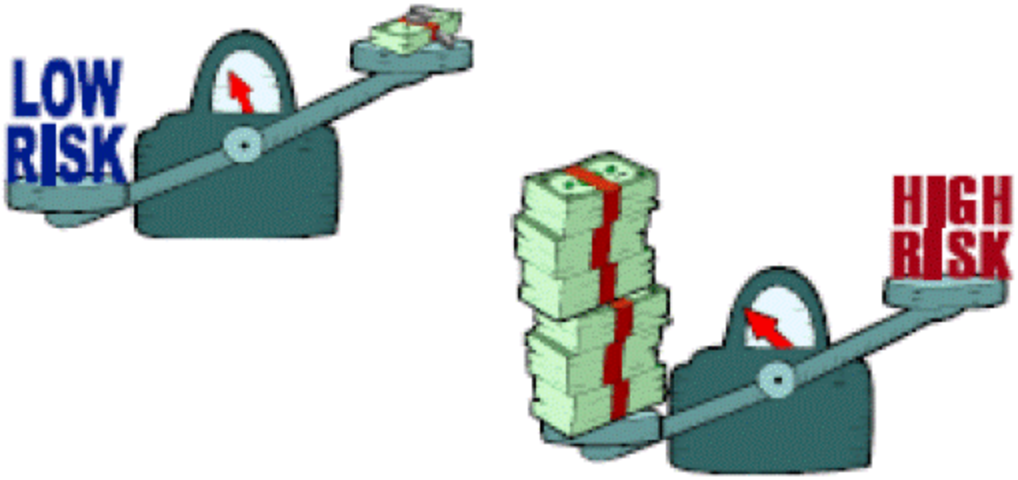


Selecting SIL

After the tolerable risk has been specified deriving target SILs is “trivial”

Specify Hazard Unmitigated Risk

- Consequence
- Likelihood



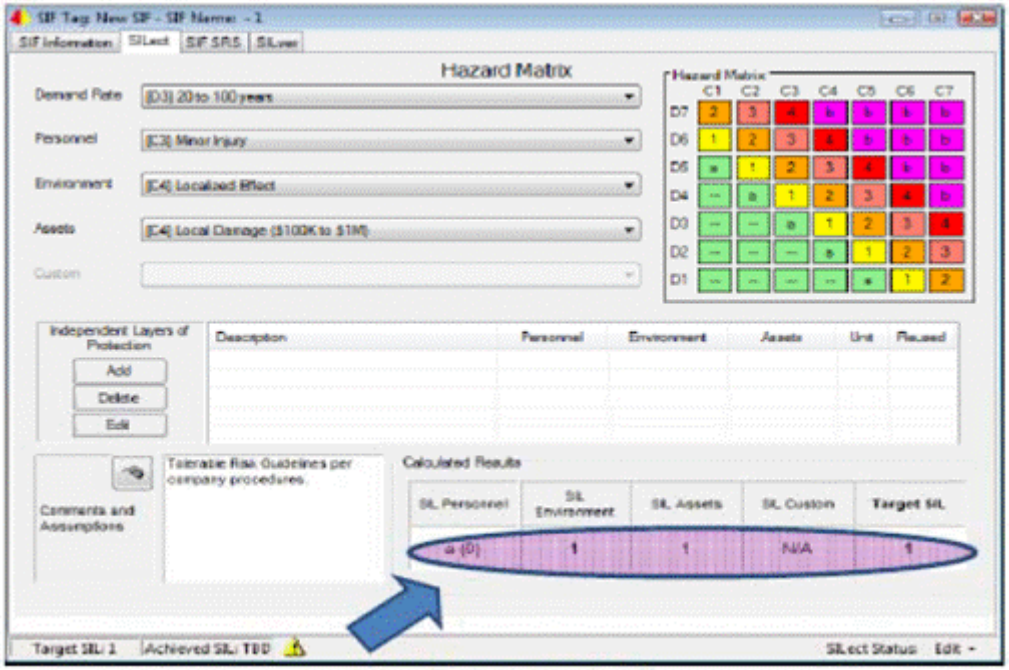
Hazards Matrix

Select Demand Rate

Select Consequences: Health & Safety, Environmental, Assets, and User Defined / Custom

Add any IPL's as per risk graph example

Document all assumptions



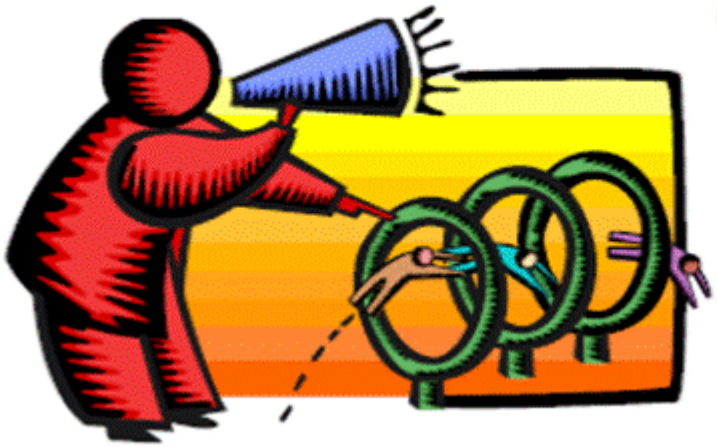
Resulting Target SIL

Section - 4.2

SIF Safety Requirements Specification [SIF-SRS];
Position SRS in Safety Lifecycle

SIF SRS tool

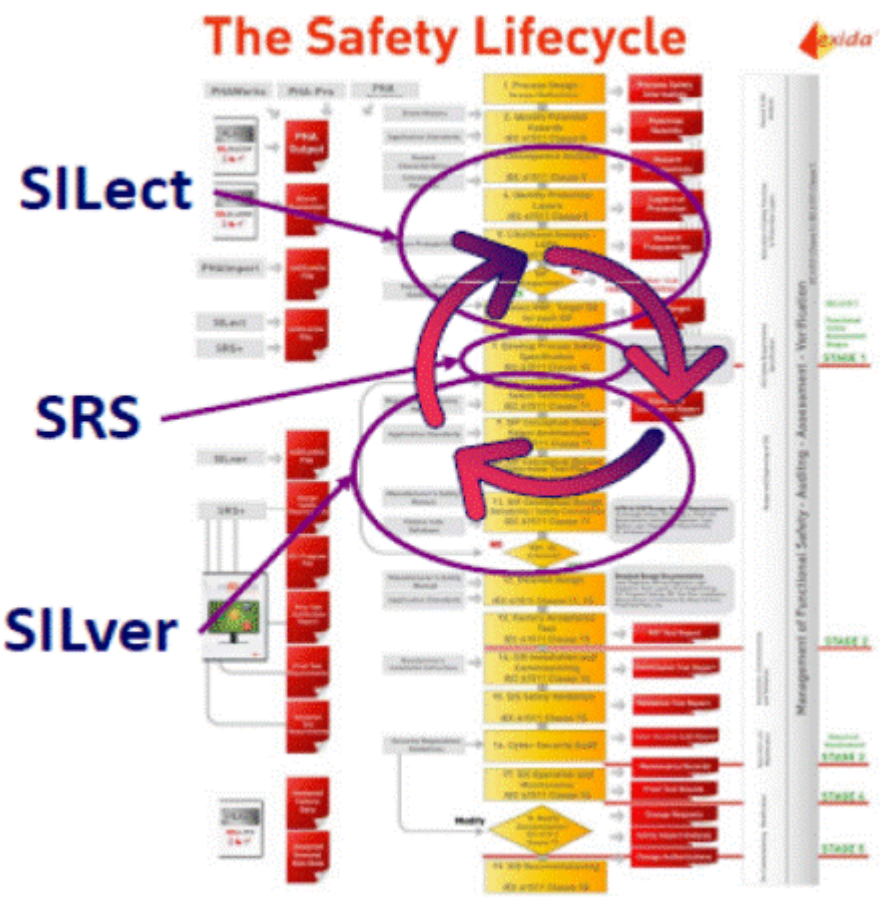
SRSC&E Plug-in (optional)



Business demands
Vs.
SIF requirements

SIF - SRS

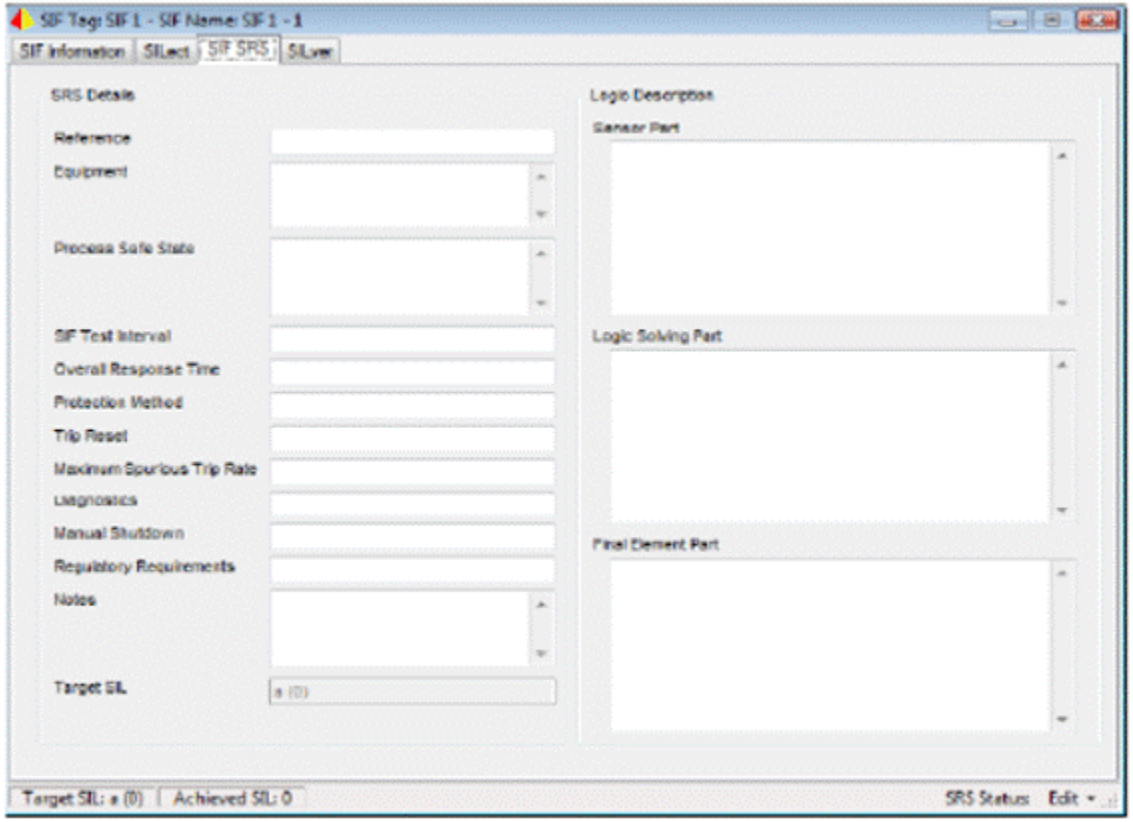
Position SRS in Safety Lifecycle



- Functional Safety Standards show “straight-line” lifecycle
- SRS is used as input to both Conceptual Design and Detailed Design
- During Conceptual Design Detailed Design aspects will be determined
- Creation of SRS will need to be an iterative process

SIF - SRS

SIF SRS tool



- Text template for SIF specific requirements
- Tool orientation is “straight-line” lifecycle
- Some requirements should however be specified by conceptual design

SIF - SRS

SRS$^{C\&E}$

Create System Level SRS

- Cover more than just SIF requirements through SRS document with detailed template

Create Process SRS documenting process requirements

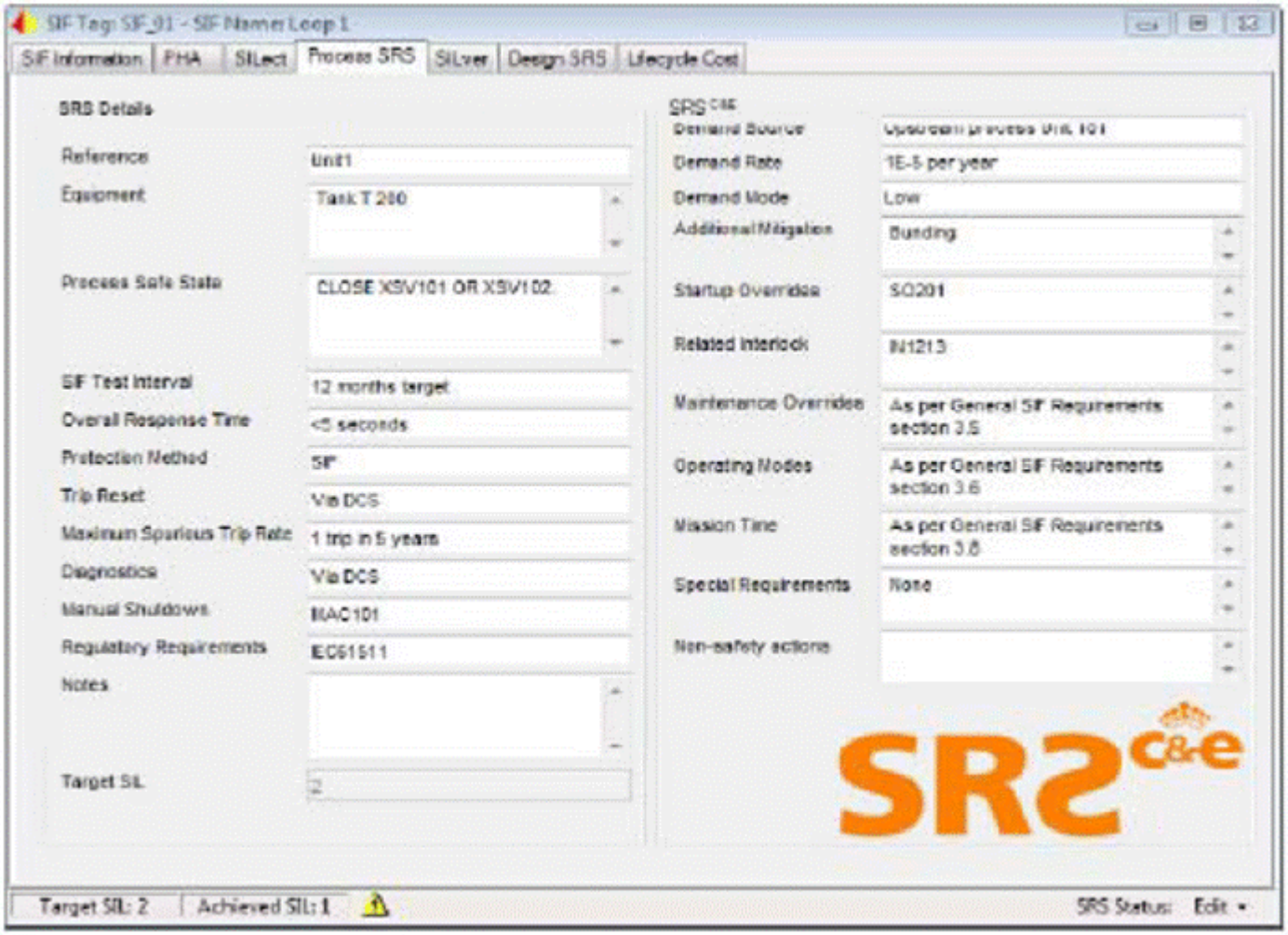
- Input to conceptual design

Created Design SRS documenting detailed design requirements based on conceptual design

- SILver selections will feed Design SRS
  - o Listing of selected diagnostics, e.g. PVST, external comparison
  - o Selected configurations will be represented in C&E matrix
  - o Safe state description based on selected Final Element action

SIF - SRS

SRS$^{C\&E}$ Process SRS



Section - 4.3

SIL verification with SILver

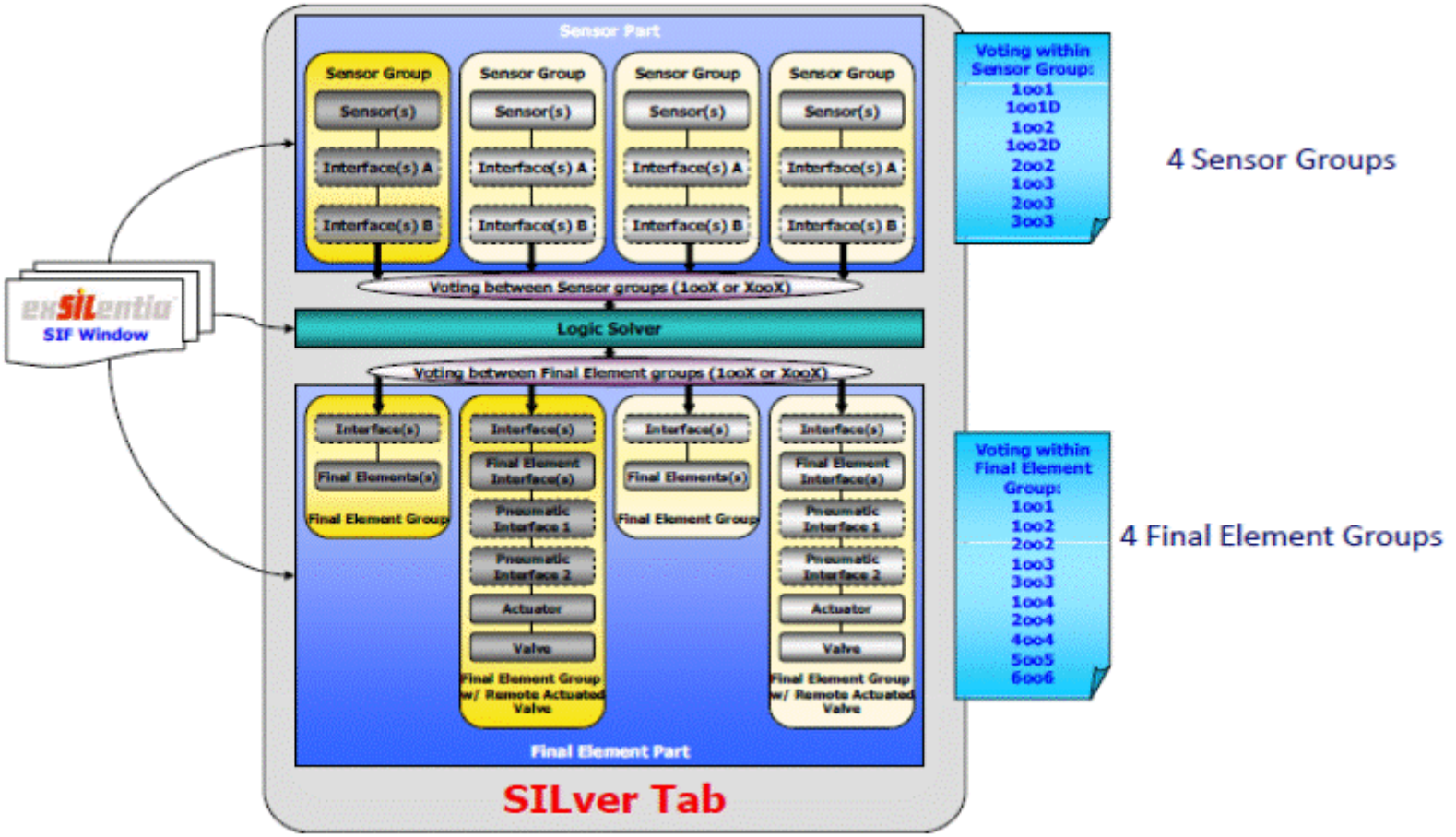
SILver Structure

How to approach a SIL verification

Example SIF SIL verification

SIL verification

SILver Structure;



SIL verification

Think in Block Diagrams;

Only include components part of the Safety Function (no auxiliary functions)

Include all components part of the Safety Function (pipe-to-pipe)

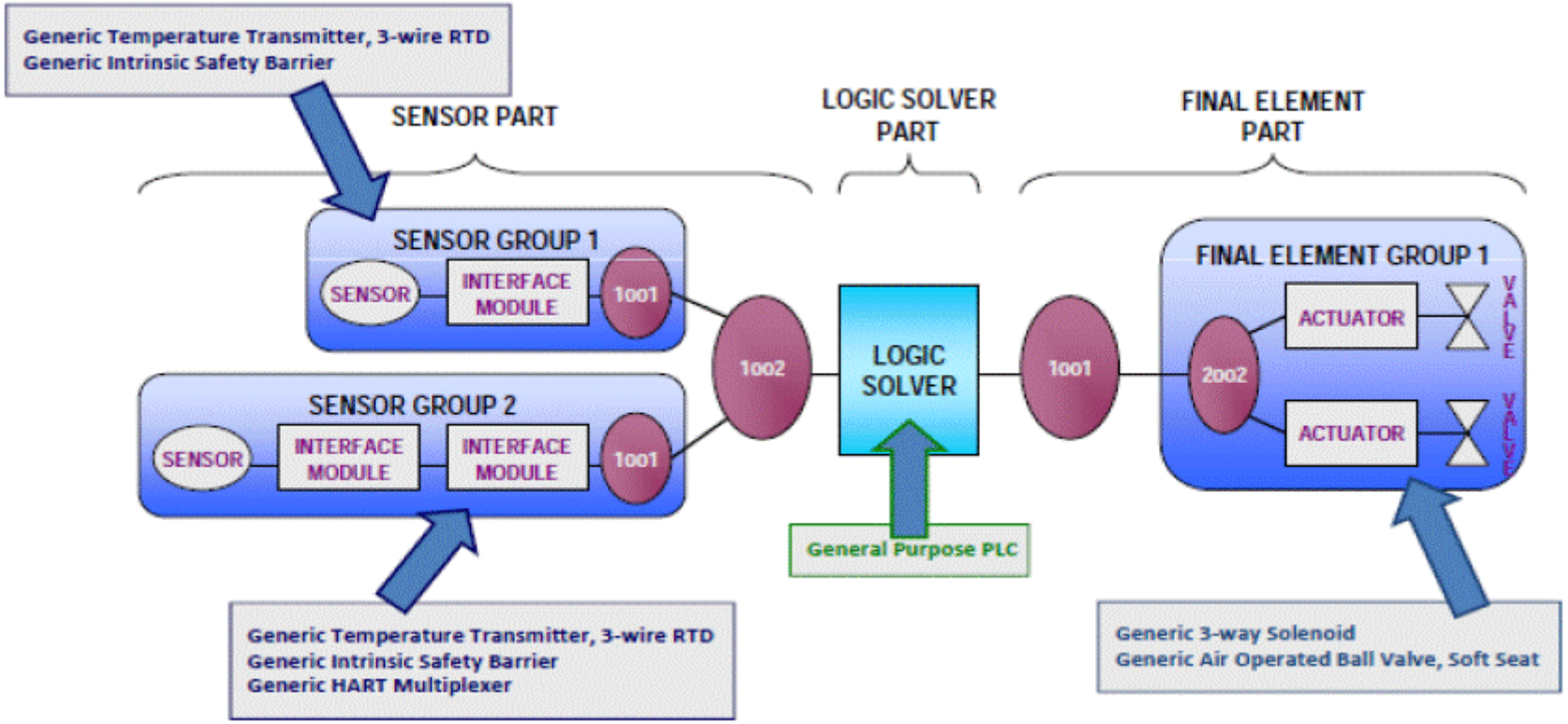
As in any reliability modeling, divide the “problem” into smaller bits

Make the smaller bits fit the SILver structure, through

- Groups
- Voting
- Diversity

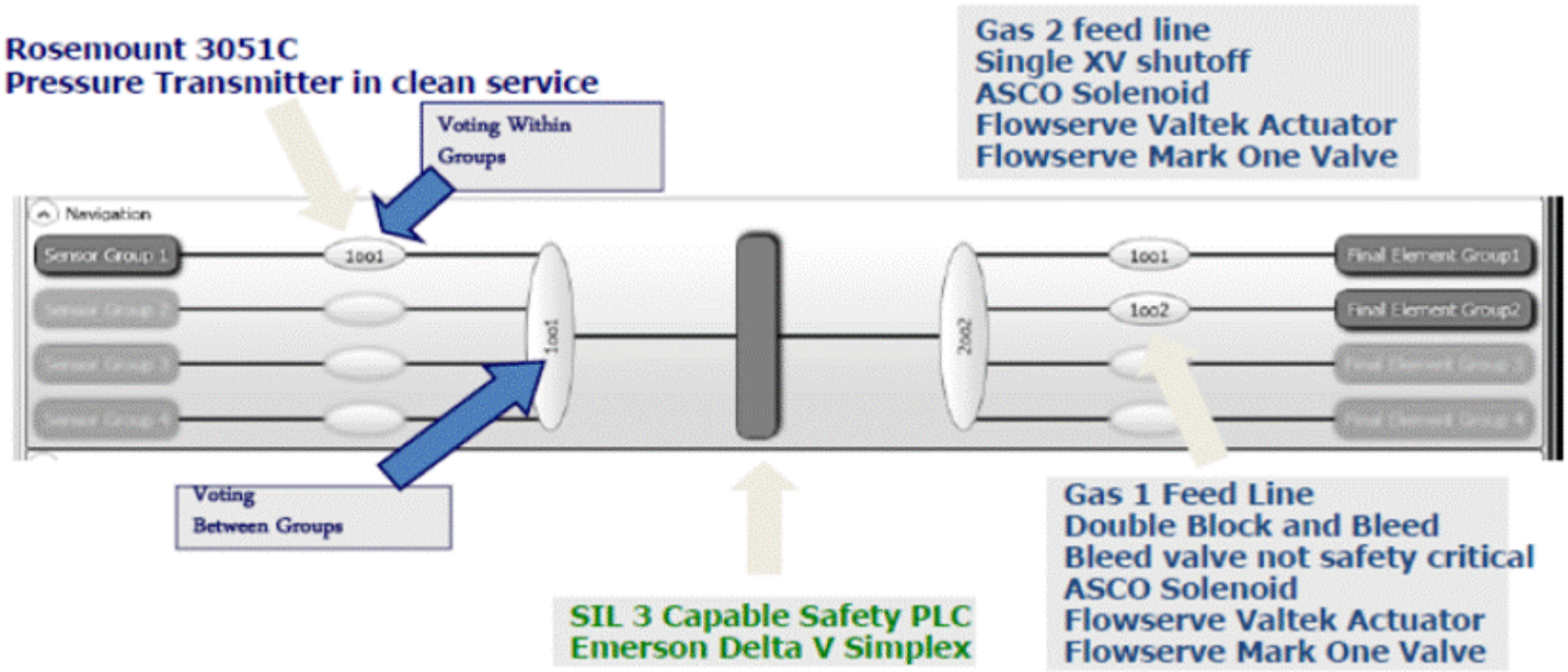
SIL verification

Example SIF;



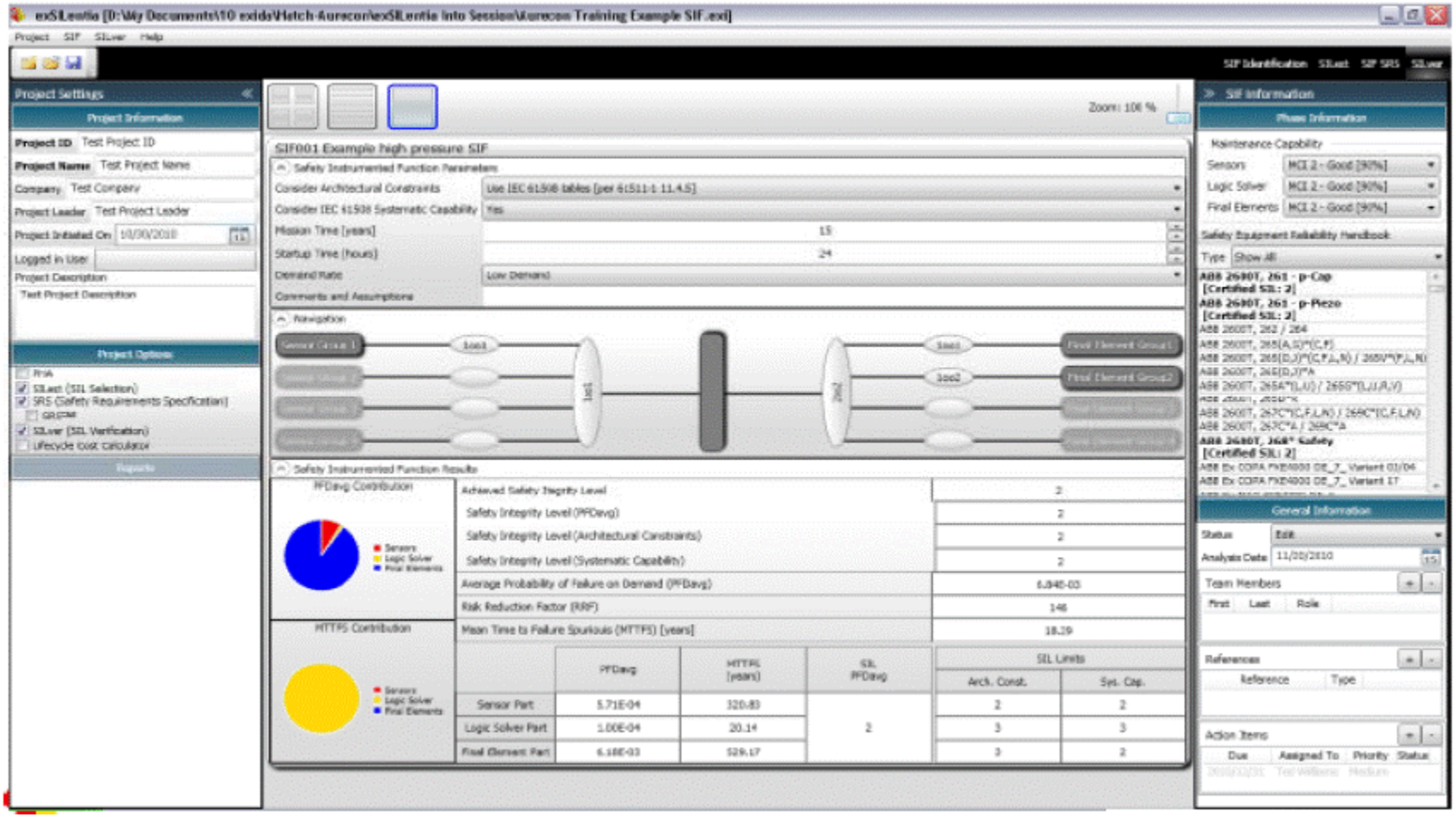
SIL verification

Example SIF;



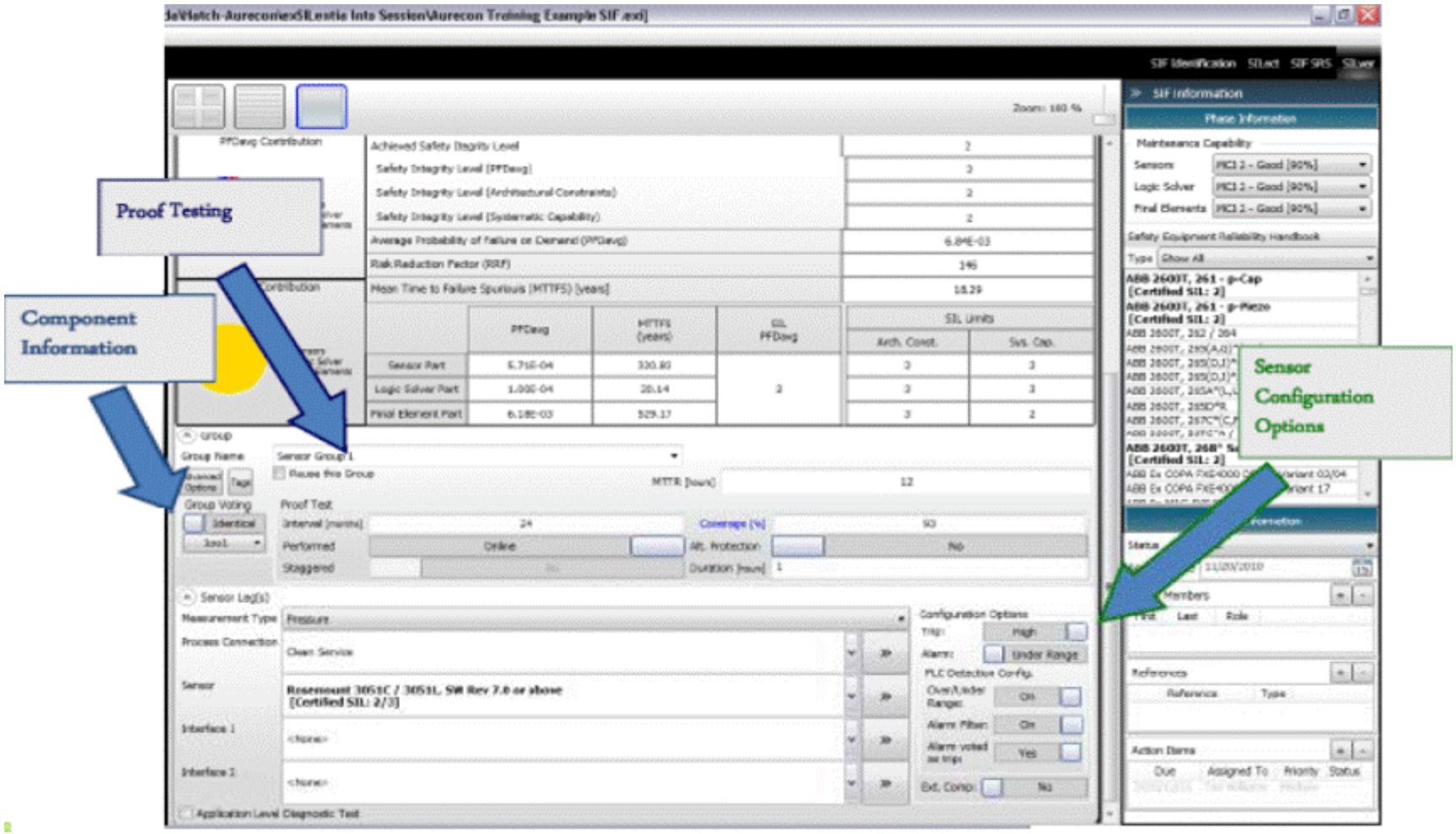
SIL verification

SILver in exSILentia® v-3.0;



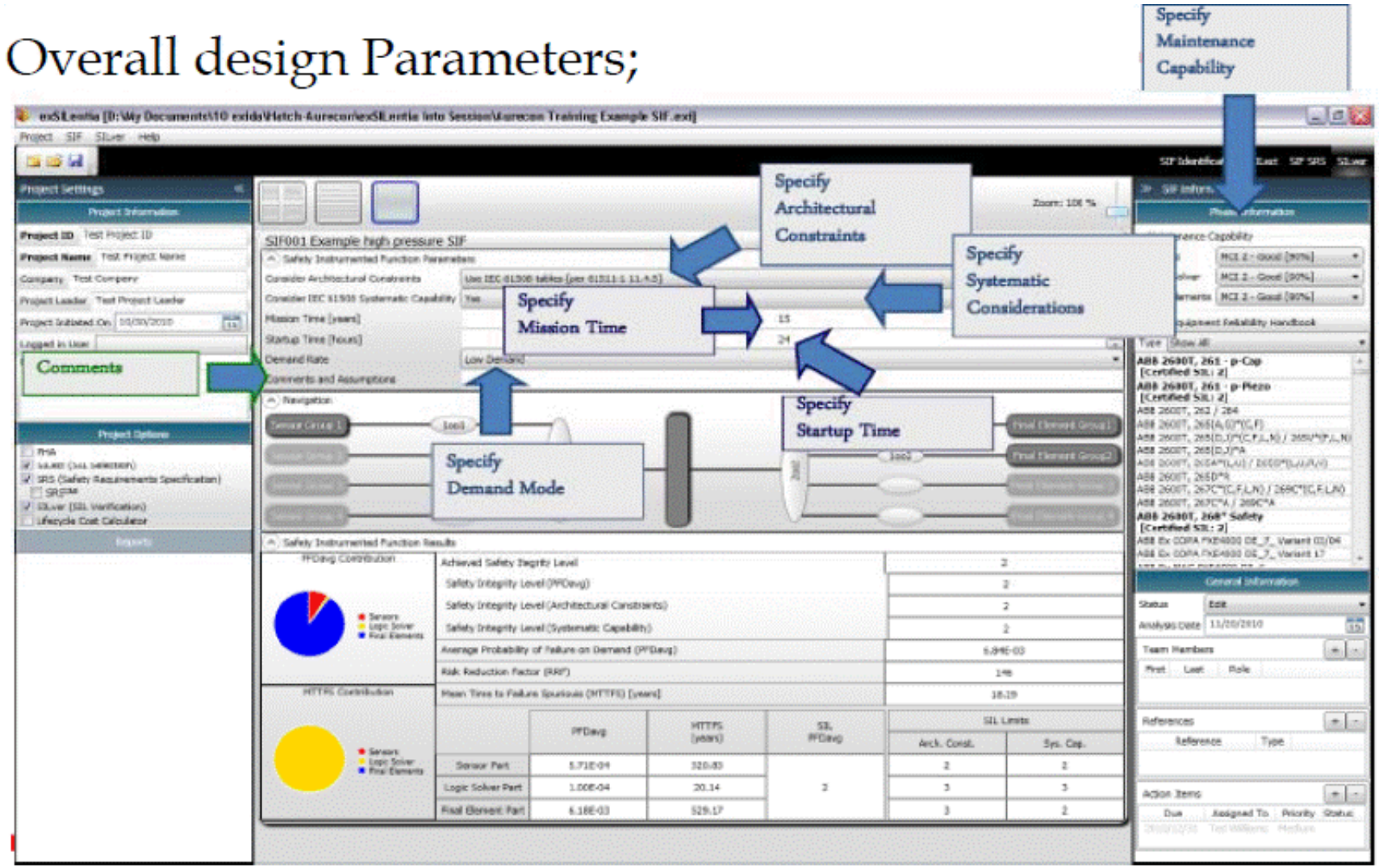
SIL verification

Sensor Part Specification;



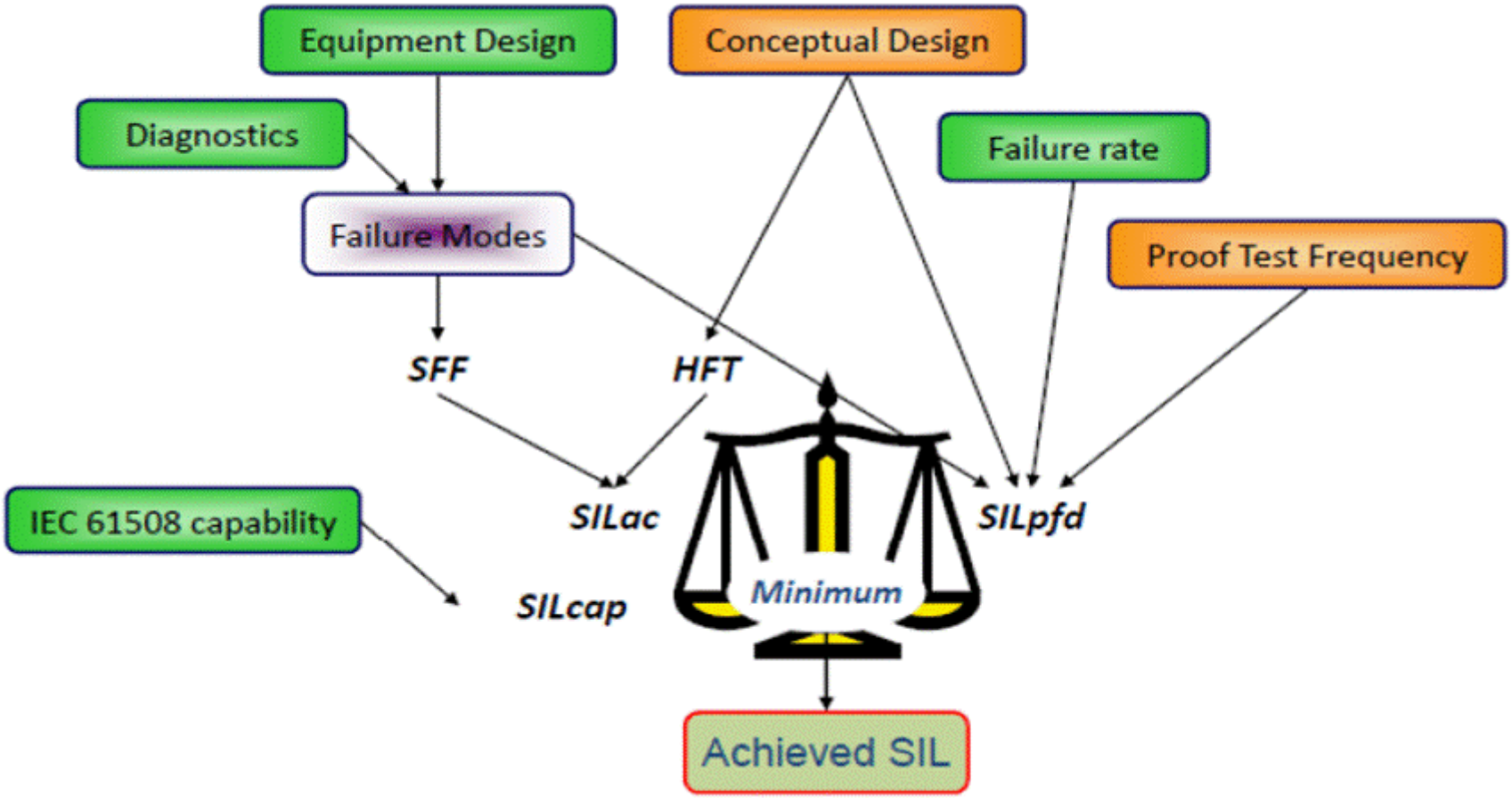
SIL verification

Overall design Parameters;



SIL verification

Achieved SIL;



SIL verification

The achieved SIL is the minimum of

- SIL based on PFDavg (SILpfd)
- SIL based on Architectural Constraints (SILac)
- SIL based on equipment Capability (SILcap)

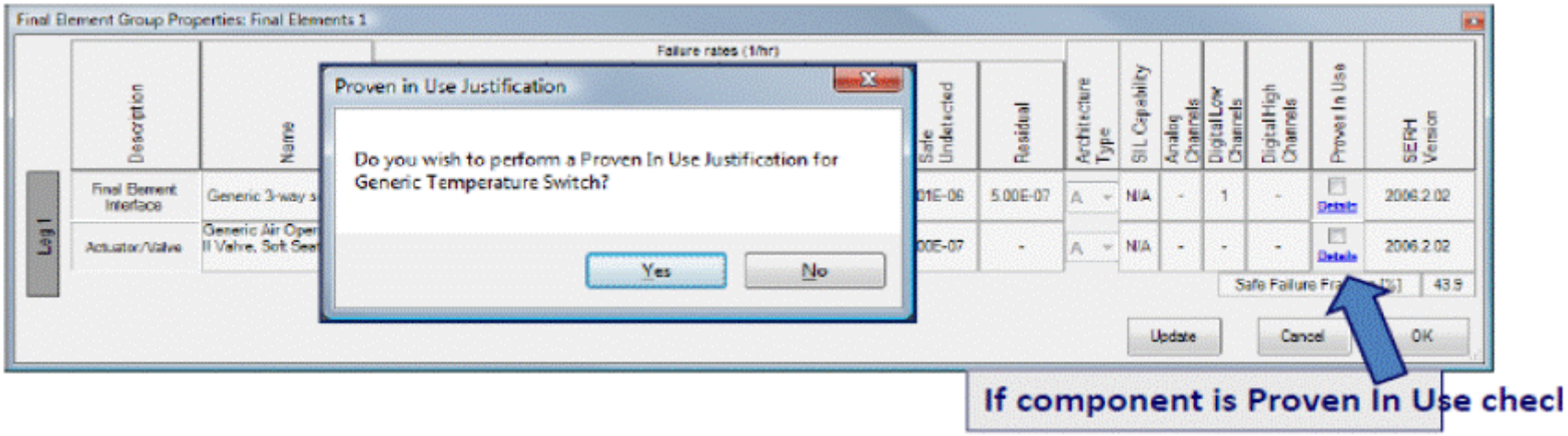
Majority of cases SILpfd and SILac will be identical

Users need to select IEC 61508 certified equipment or justify the use of specific equipment based on Prior Use arguments

No SIL Capability

If an equipment item has no SIL Capability, i.e. not IEC 61508 certified, the , user must justify the use of that equipment item

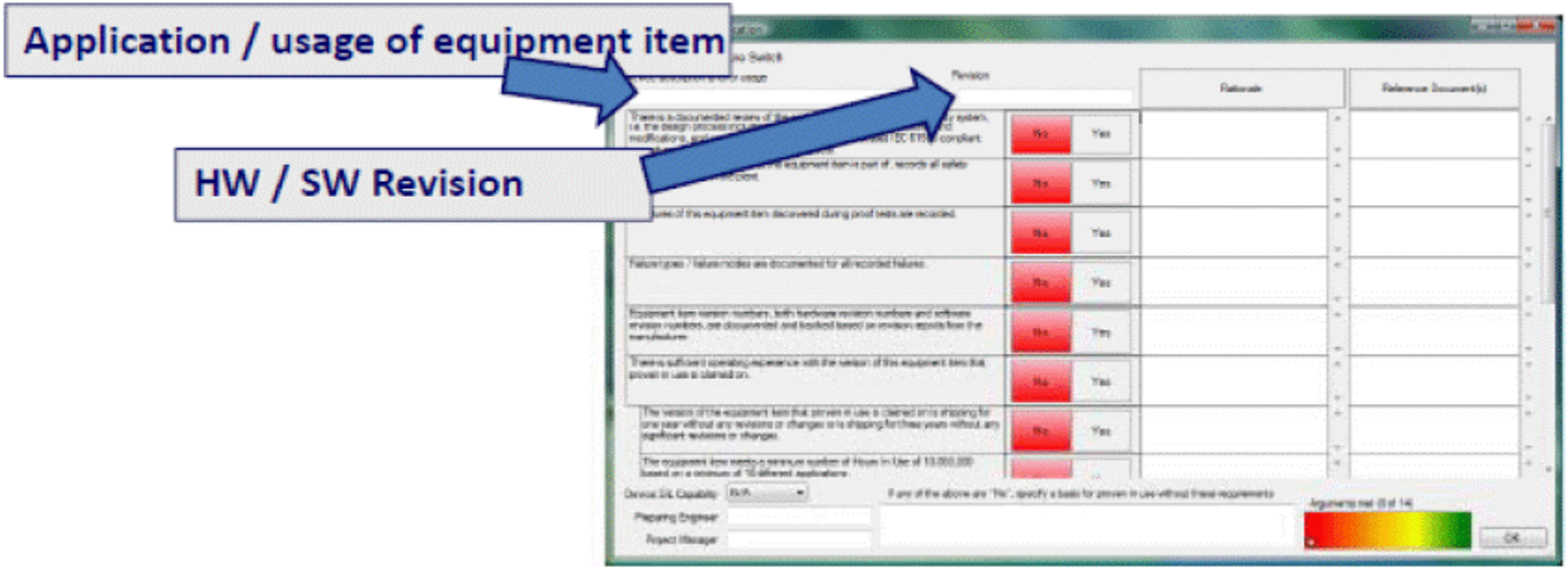
Equipment item Prior-Use / Proven-In-Use [PIU] Justification



PIU Justification

Proven In Use Justification wizard allows documentation of rationale and reference per claim

Proven In use Justification is application specific and component revision specific



THANK YOU