



**An Update on Process Safety
Standards: ISA 84-2004 & IEC 61511**

Houston, TX, +1-832-439-3793

Sellersville, PA, +1-215-453-1720

Munich, Germany +49-89-4900-0547

www.exida.com



Introduction

➤ Curt Miller

exida's newest partner, has recently opened a branch in Houston to support the Gulf, and has over 13 years of professional experience working with safety systems and sales with several large corporations in the Gulf Region including Honeywell, Exxon, and Siemens. He most recently spent 6 years developing automation markets as a Sr. Engineer for Siemens Energy & Automation originally in New Orleans and then in Austin, TX in early 2003. Mr. Miller is a graduate of Texas A&M University with a B.S. in Chemical Engineering and is currently the ISA - Bluebonnet (Austin & San Antonio) President.





network of excellence in dependable automation

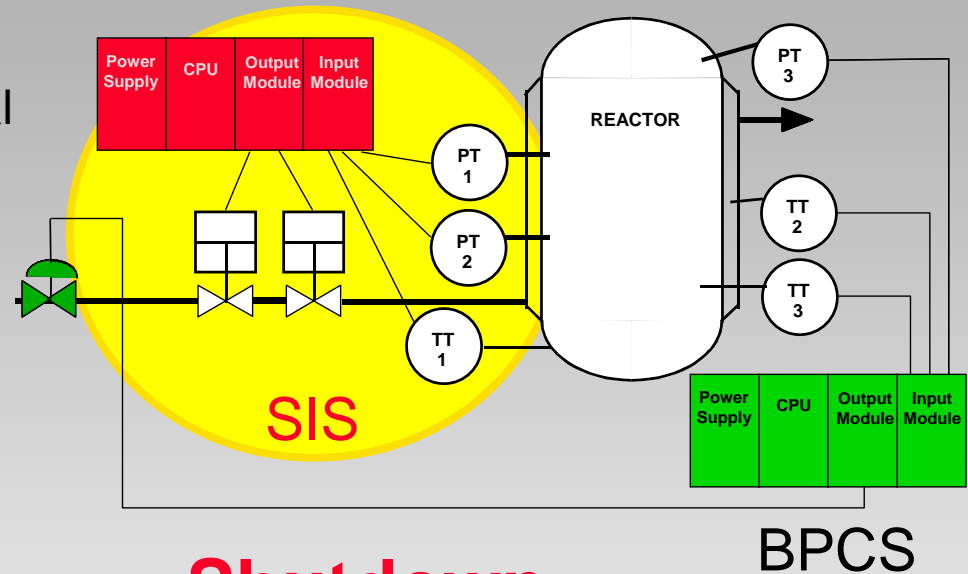


Safety Instrumented System Functional Definition

Practitioners often prefer a functional definition of SIS such as:

“A SIS is defined as a system composed of sensors, logic solvers and final elements designed for the purpose of:

1. Automatically taking an industrial process to a safe state when specified conditions are violated;
2. Permit a process to move forward in a safe manner when specified conditions allow (permissive functions); or
3. Taking action to mitigate the consequences of an industrial hazard.”



Shutdown

Permissive

Mitigation

Most Influential Documents

- DIN VDE 0801; Functional Safety for Automation Equipment, 1992
- AIChE CCPS; **Guidelines for Safe Automation of Chemical Processes, 1993**
- ANSI/ISA84.01; **Application of Safety Instrumented Systems for the Process Industries, 1996**
- **IEC 61508; Functional Safety - Safety Related Systems, 1998/2000**



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

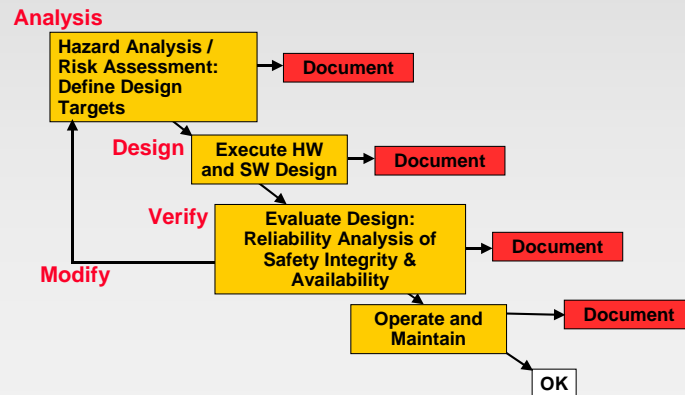
Safety Evolution

- 2000's

Safety Equipment – Transmitters, PLCs, Valves



- IEC61511
- Better Diagnostics
- Safety Lifecycle Process



IEC61508 and derivatives

IEC 61508 - Functional Safety, “Umbrella Standard” - 1998/2000

IEC (EN) 61511 – Process industry application oriented standard, 2003

ISA84.01-2004 (61511+)

Passed ANSI September 2004

1. Performance based not PERSCRIPTIVE

2. Use of a Safety Lifecycle engineering process



84.01-1996 versus 84.00.01-2004

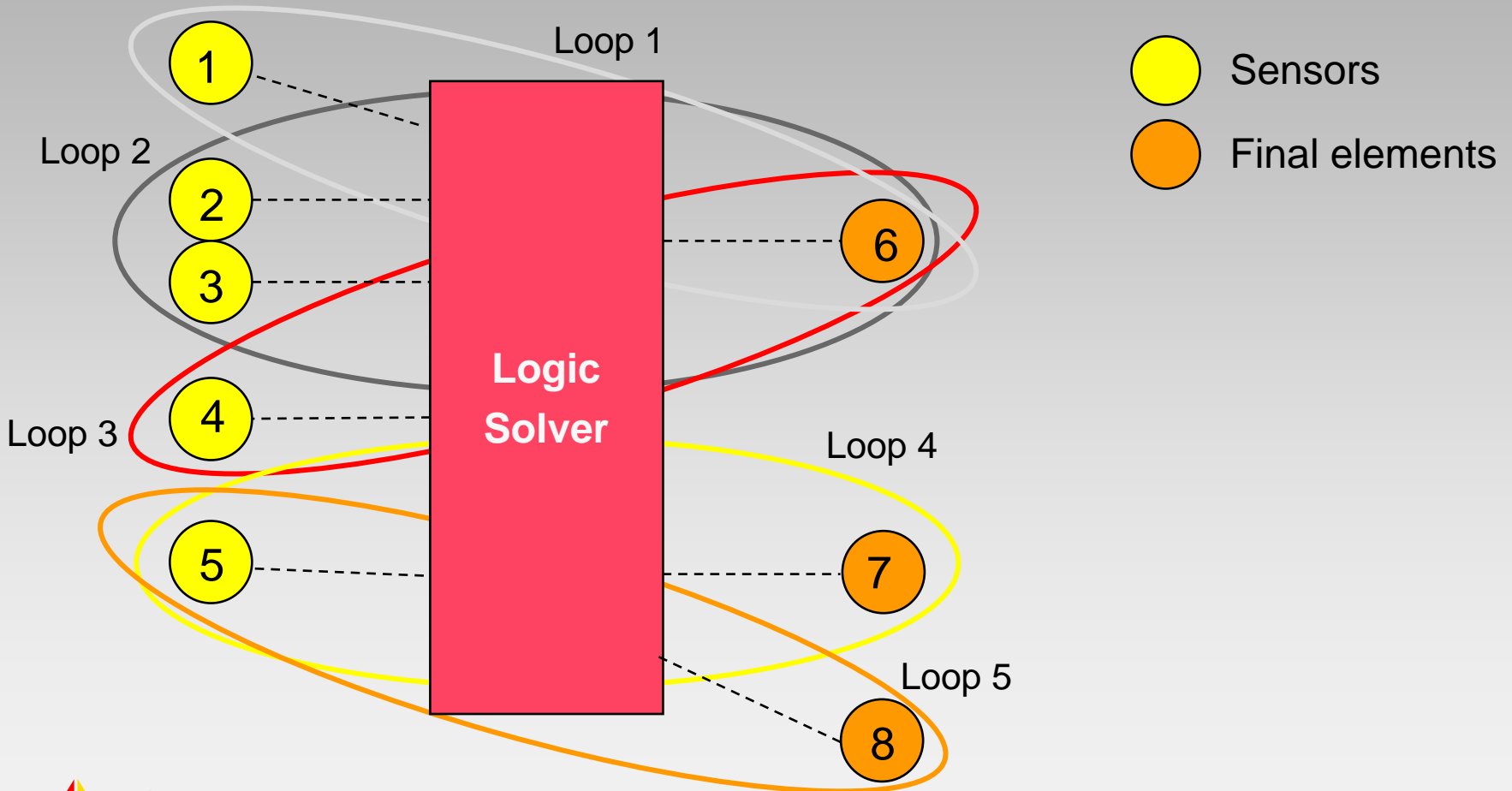
Passed ANSI September 2004

New standard has:

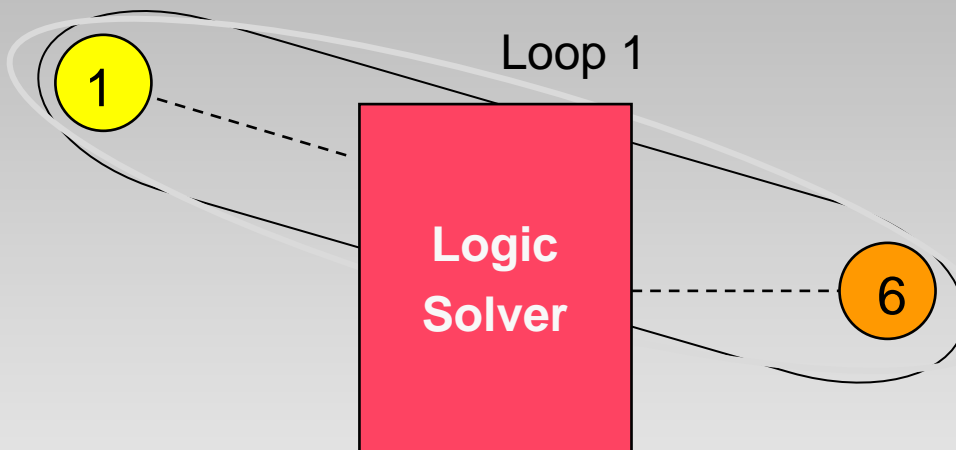
1. More detail, better explanation
2. Requirements for “Functional Safety Management”
 - Documented Personnel Competency
 - Documented Engineering Procedures for SIS Design
3. Instrument selection requirements
 - IEC 61508 Certified Equipment or “Proven In Use”
4. Minimum levels of redundancy
5. Requirement for probabilistic calculations to verify designs





Terms - Safety Instrumented System



Term - Safety Instrumented Function (SIF)



-  Sensors
-  Final elements

A safety instrumented function is defined as a “Function to be implemented by a SIS which is intended to achieve or maintain a safe state for the process with respect to a specific hazardous event.”

Safety Instrumented Function Examples

- Prevent vessel rupture by supplying emergency coolant to reduce extreme temperature
- Prevent vessel rupture by opening valve to relieve excessive pressure
- Direct escaping liquid to waste handling system to prevent environmental damage
- Issue fire alarms to minimize damage and possible injury

Certified Functional Safety Expert

ANSI/ISA 84.00.01-2004 Personnel Competency

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

-IEC 61511, Part 1, Paragraph 5.2.2.2

“...ensuring that applicable parties involved in any of the overall E/E/PE or software safety lifecycle activities are competent to carry out activities for which they are accountable.”

-IEC 61508, Part 1, Paragraph 6.2.1 (h)

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 TÜV



Certified Functional Safety Expert (CFSE) Program

- Types of Exams

- Application – Process Industries: IEC 61511

- Application – Machine Industries

- Developer – Software

- Developer - Hardware



Certified Functional Safety Expert (CFSE) Program

Certified Functional Safety Expert
Application Engineering- Process
Study Guide
2nd Edition



Resources Available:

- On-line Training
- Onsite Training
- Study Guide
- Reference Books



Documented Engineering Procedures - Safety Life Cycle

Analysis

Conceptual Process Design
Identify Potential Risks
Consequence Analysis
Layer of Protection Analysis
Develop Non-SIS Layers

**How much safety
do I need?**

Realization

Select SIS Technology
Select SIS Architecture
Determine Test Frequency

**How much safety
do I have
with my design?**

Yes

Modify?

No

Operation

Startup
Operation
Maintenance
Periodic Proof Tests
Modifications
Decommissioning

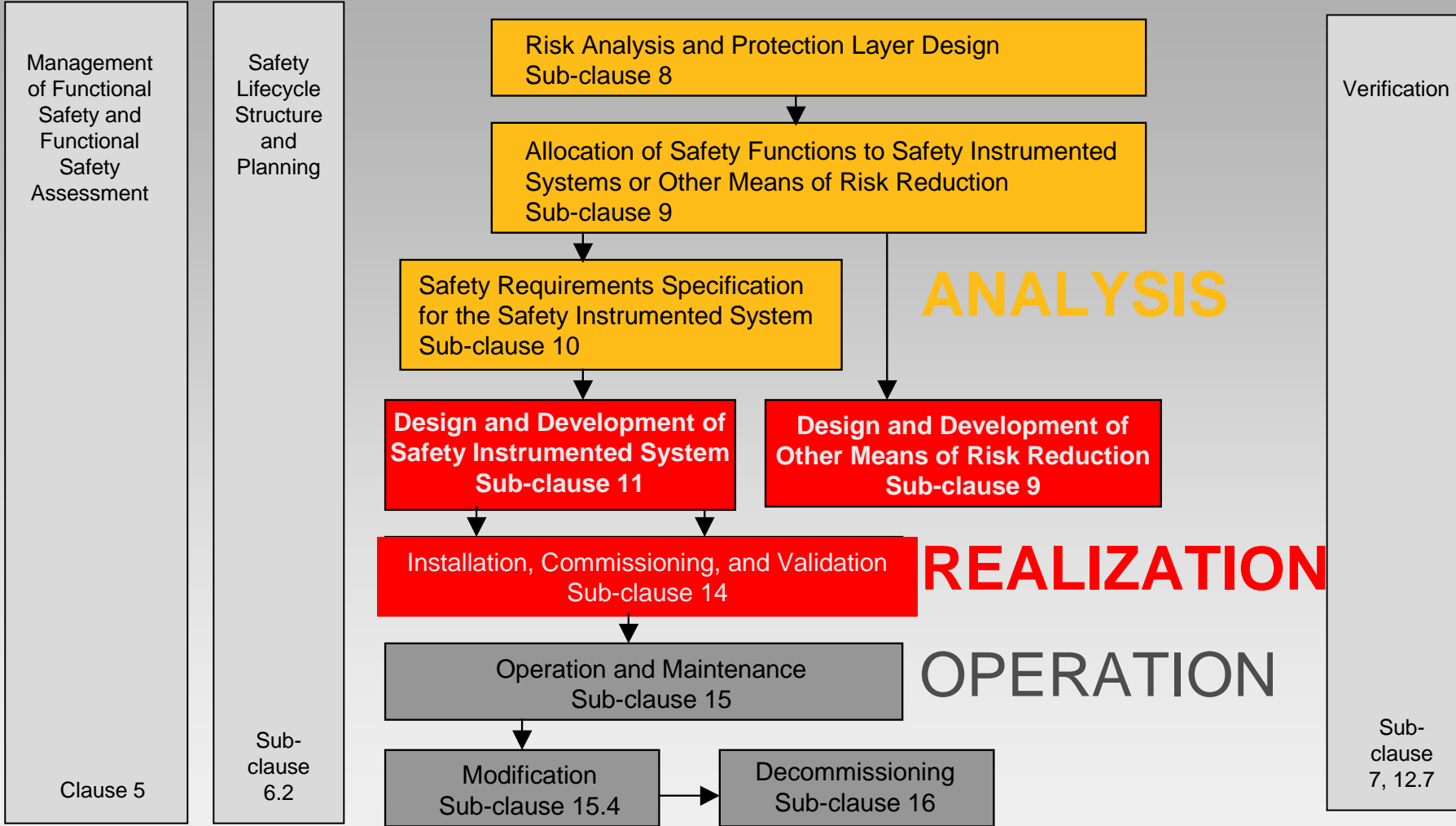
**How will I keep
it safe?**

Yes

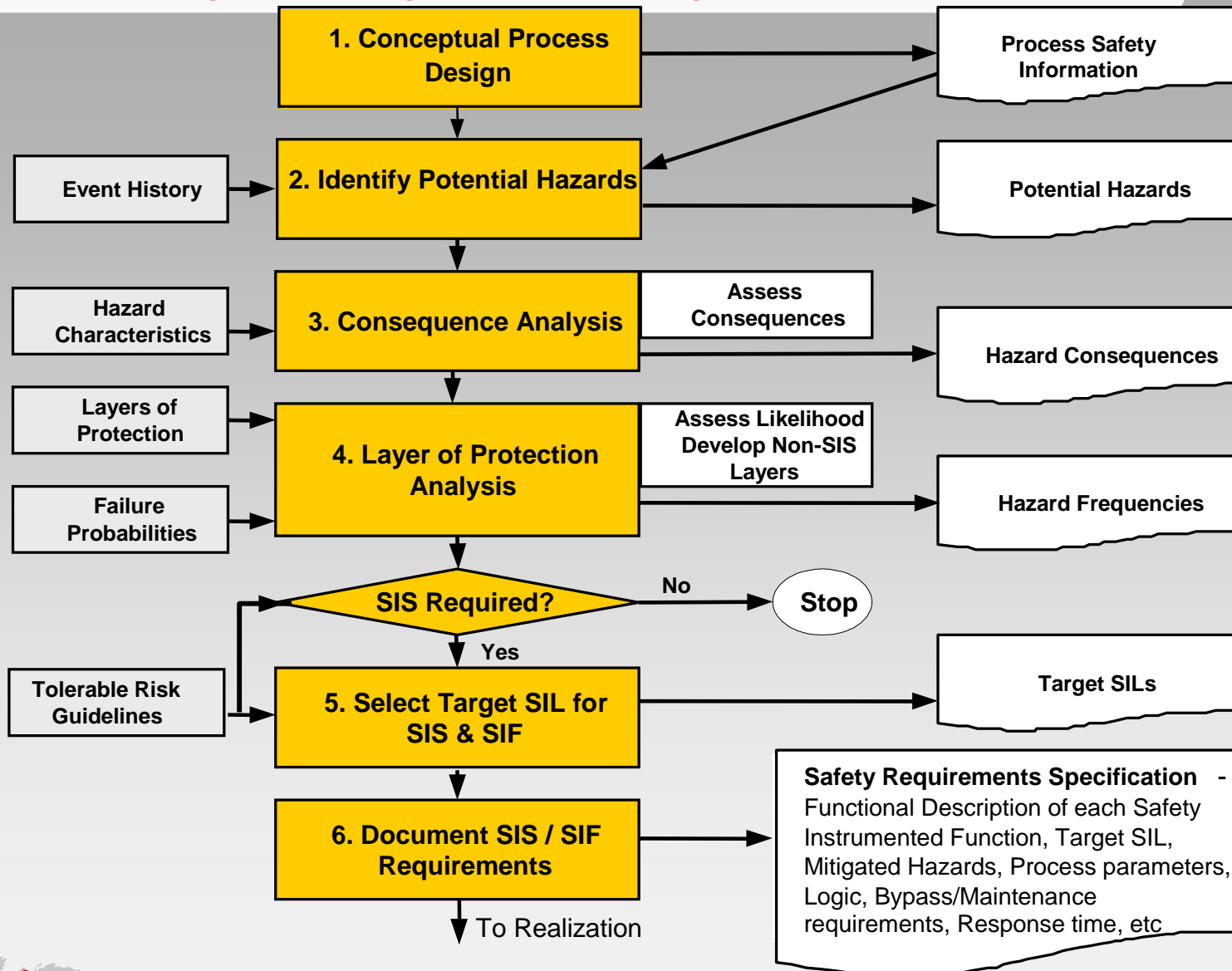
Modify?

No

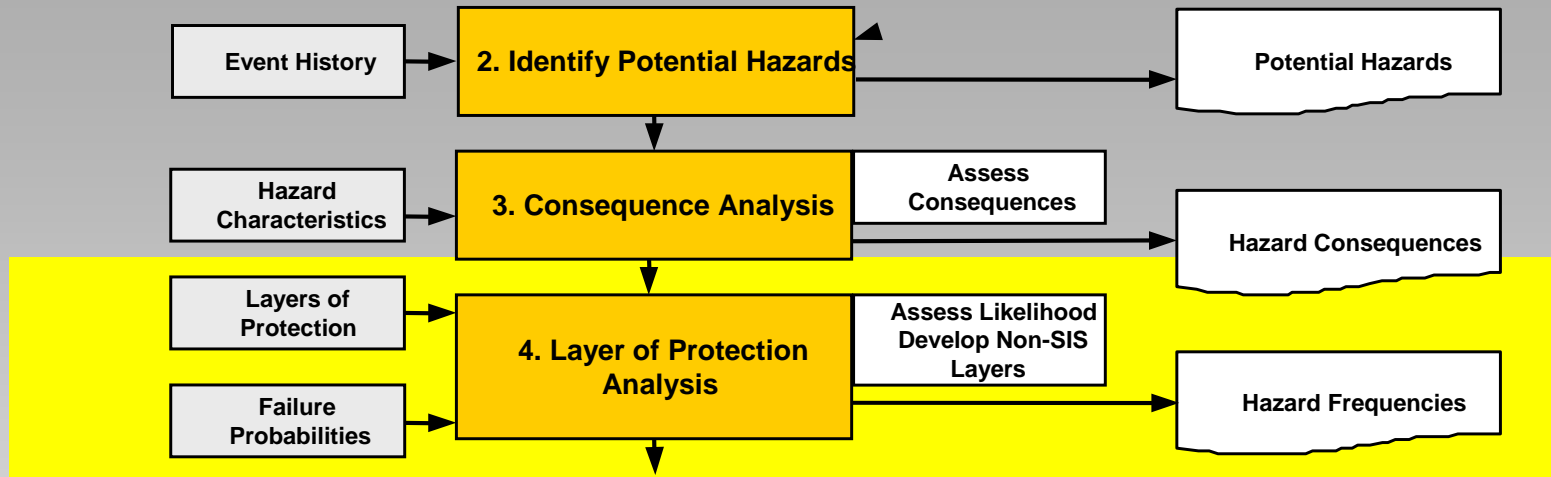
IEC 61511 Safety Life Cycle



Safety Lifecycle "Analysis" Phase



Layer of Protection Analysis



•Objective

Assess likelihood based on all protection layers.

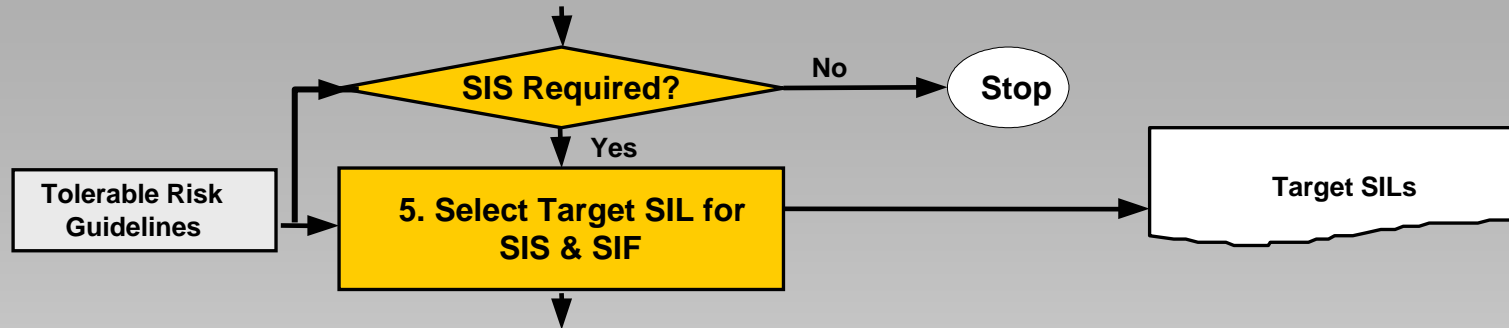
•Tasks

Identify Layers of Protection

Use qualitative or quantitative methods

Initiating Event	Protection Layer 1	Protection layer 2	Protection Layer 3		Final Outcome
			PL3 Fails		Accident Occurs
	PL1 Fails	PL2 Fails			
Init Event			PL3 success	No Impact Stop	
		PL2 Success	No Impact Stop		
	PL1 Success	No Impact Stop			

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

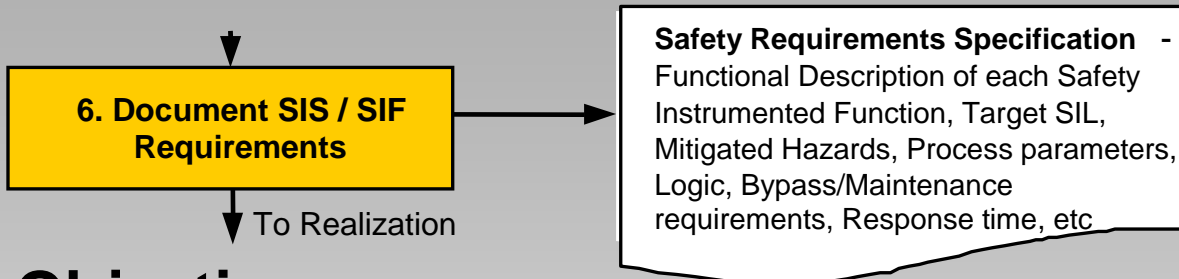
Safety Integrity Level	Risk Reduction Factor
SIL 4	100000 to 10000
SIL 3	10000 to 1000
SIL 2	1000 to 100
SIL 1	100 to 10

Old ISA84.01

SLC Engineering Software Tools - LOPA Analysis

		SIF: High Pressure Loop 43 Logged in as: William Goble	
Home : Applications : SILect : Initiating Event			
<input type="button" value="Delete this Initiating Event"/>			
Initiating Event Details			
Initiating Event	<input type="text" value="Pump failure"/>		
Initiating Likelihood (1/year)	<input type="text" value="0.05"/>		
Enabling Condition	<input type="text" value="None"/>		
Enabling Condition (probability [-])	<input type="text" value="1"/>		
<input type="button" value="Add Independent Protection Layer"/>			
Independent Protection Layers			
IPL Description	Probability of Failure on Demand		
	Personnel	Environment	Equipment
Pump failure diagnostic	0.2	0.2	0.2
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

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.

SRS Documentation Software Tools

General Information

Project Identification: Example 11/24/2004

Project Name: Example Project

Company: exida

Project Leader: Curt Miller

Project Initiated On: 11/24/2004

Project Description: This is my first project. It will be used to demonstrate the functionality of the Project Manager and associated tools.

SIF Safety Requirements Specification - SIF SRS

SIF	Safety Function 01	Service
Reference	Meeting Minutes 8/6/04	Large Flow through the supply line will close supply line valve
Required SIL	2	
Test Interval	2 year	
Response Time	4 seconds	
Method	De-energize to trip	
Reset Type	Manual required	Safe State
Spurious Trip Rate Req's	MTTFS>10 years	Flow to the tank farm is stopped by closing the supply line valve
Diagnostics	None additional	
Manual Shutdown	Through Handswitch 3HS-004	
Regulatory Requirements	See company procedure	
Notes	None	

Logic Description

Sensor Part	Logic Solving Part	Final Element Part
If either the vessel pressure transmitter or the supply line flow transmitter indicate trip, the SIF should trip. In addition, Handswitch 3HS-004 will cause a trip	A generic SIL 3 certified PLC will be used as the logic solver for the SIF	Single shutoff valve stops the flow to the tank farm

Select Technology



- **Objective**
 - Choose the right equipment for the purpose. All criteria used for process control still applies.
- **Tasks**
 - Choose equipment: **IEC 61508 Certification or “Proven In Use”**
 - Obtain reliability and safety data for the equipment
 - Obtain Safety Manual for any safety certified equipment

Safety Assessment for Products

- FMEDA – manufacturer provides failure rate and failure mode data
- Proven In Use – manufacturer provides modification history, field performance data
- IEC 61508 Certification – manufacturer has third party assessors certify that a product meets all requirements of 61508.



Safety Assessment Limitations

- FMEDA – manufacturer provides failure rate and failure mode data
 - **DOES NOT INCLUDE PROCESS CONNECTIONS!**
- Proven In Use – manufacturer provides modification history, field performance data
 - **MANUFACTURER P.I.U. INFO IS JUST A START, THEY DO NOT USE THE EQUIPMENT.**



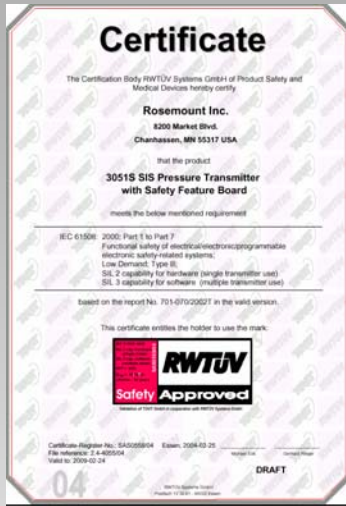
Assessment Criteria	FMEDA only	FMEDA / exida	Prior Use / IEC 61511	exida Proven In Use Criteria	IEC 61508 Certification
Detail analysis of hardware failure modes	X	X		X	X
Detail Analysis of hardware diagnostic capability	X	X		X	X
Analysis of hardware useful life		X		X	X
Analysis of proof test effectiveness		X		X	X
Assessment of operational hours based on manufactured units			X	X	X
Assessment of Configuration Management system per requirements of IEC 61508			X	X	X
Assessment of Field Failure Return System - field failures corrected				X	X
Assessment of Field Failure Return System - notification to users of safety issues				X	X
Assessment of design revision history - few revisions based on design faults				X	X
Assessment of hardware design process					X
Assessment of hardware testing techniques					X
Assessment of software requirements					X
Assessment of software criticality					X
Assessment of software design techniques					X
Verification of Safety Manual per IEC 61508					X
Assessment of software testing techniques					X
Assessment of product testing techniques including environmental testing					X
Assessment of manufacturing process					X

RANDOM

SYSTEMATIC



IEC 61508 Full Certification Enough?



- NO!
- Equipment must match intended application
- Equipment “restrictions” must be followed
- Process connections must be included

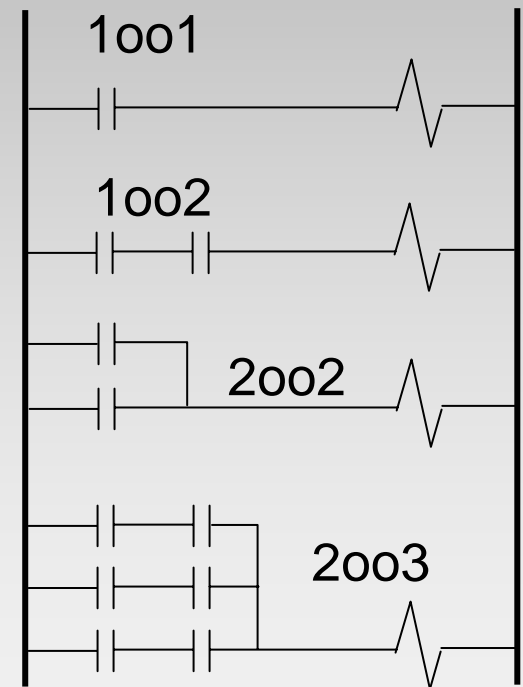
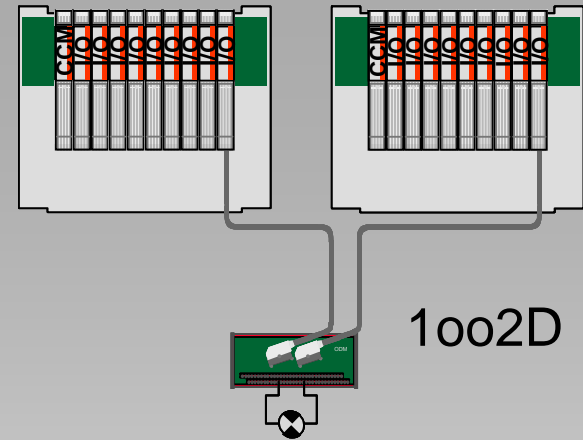
Manufacturer's Safety Manual



- Usage Requirements-Restrictions
- Environmental Limits
- Optional Settings
- Failure Rate Data
- Useful Life Data
- Common Cause Beta Estimate
- Inspection and Test Procedures

Select Architecture

- **Objective**
 - Choose type of redundancy if needed.
- **Tasks**
 - Choose architecture
 - Obtain reliability and safety data for the architecture

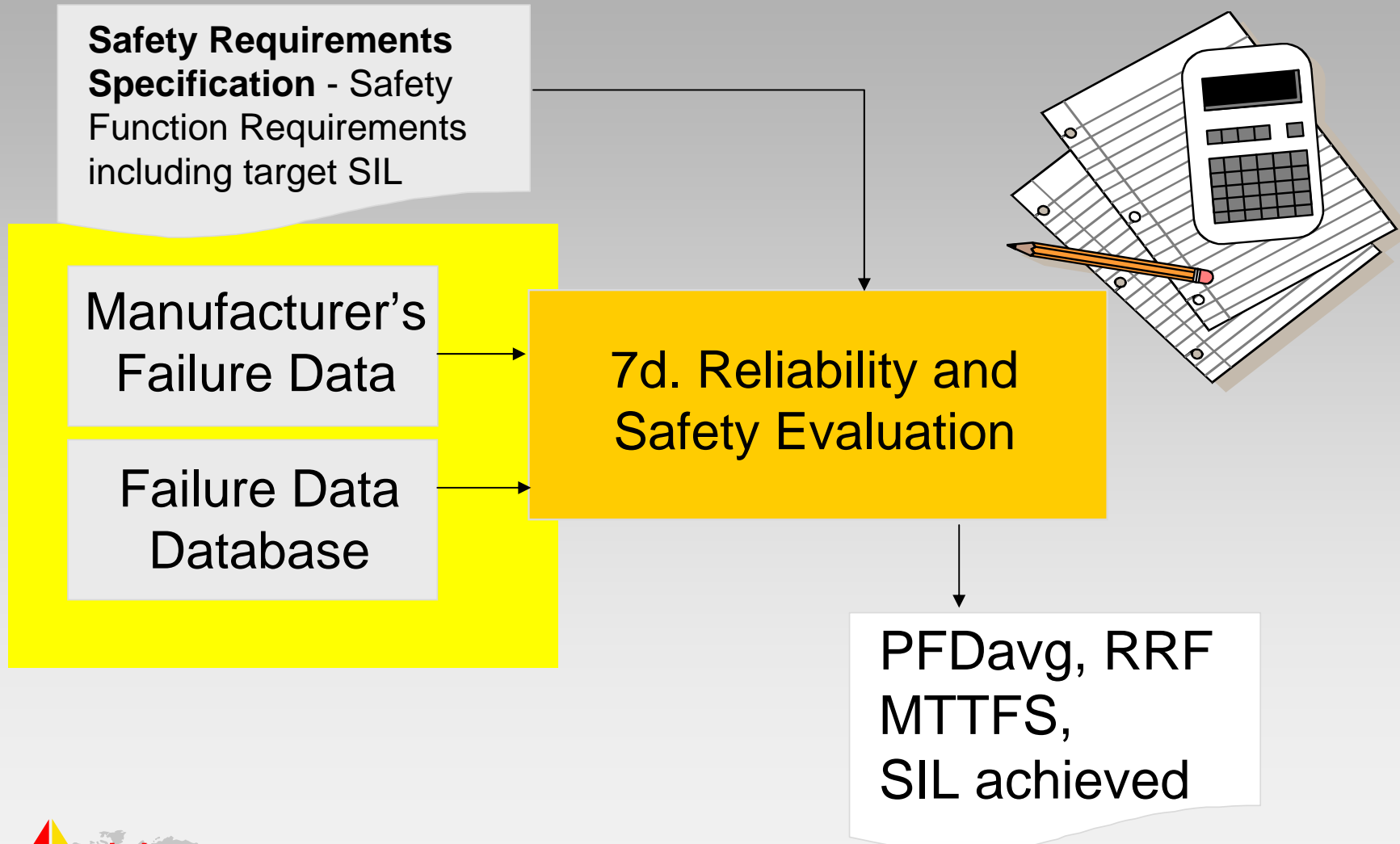


Establish Proof Test Frequency - Options

In general the testing can consist of:

- Automatic testing which is built into the SIS
- Automatic testing from external system
- Off-line testing, which is done manually while the process is not in operation.
- On-line testing, which is done manually while the process is in operation.

SIF Verification Task

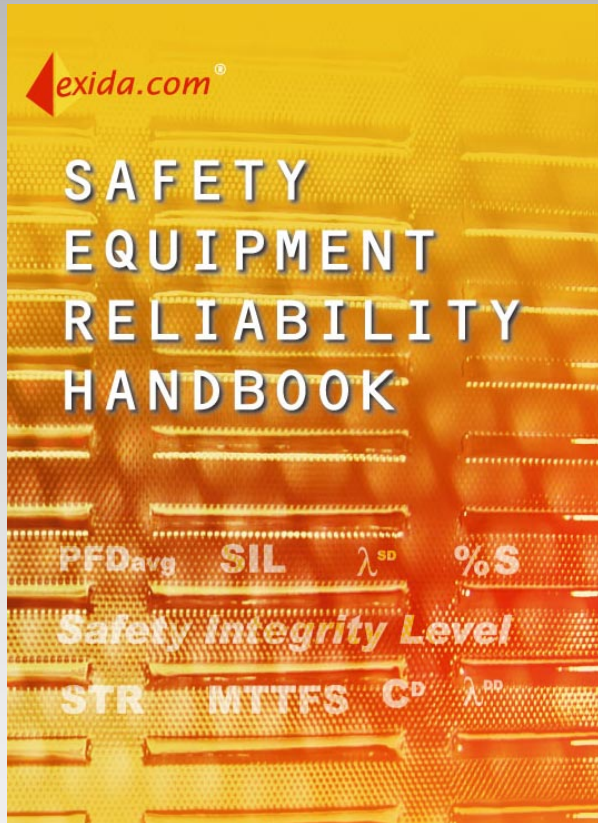


Failure Rate Data Models

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

SIL

NEW

Safety Integrity Level	Probability of failure on demand (Demand mode of operation)	Risk Reduction Factor
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	100000 to 10000
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	10000 to 1000
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	1000 to 100
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	100 to 10

IEC61508 Safe Failure Fraction

TYPE B

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	Not Allowed	SIL1	SIL2
60 % < 90 %	SIL1	SIL2	SIL3
90 % < 99 %	SIL2	SIL3	SIL4
< 99 %	SIL3	SIL4	SIL4



SIL Verification Tool

Sensor Part Information

Sensor Group(s)	Edit
(1) Sensor Group 1	Details
(2) Sensor Group 2	Details
PFDavg Sensor Part:	3.44E-05
MTTFS Sensor Part (years):	35.31

Logic Solver Part Information

Logic Solver	Edit
(1) Example PLC	Details
PFDavg Logic Solver Part	3.32E-02
MTTFS Logic Solver Part (years)	3.83

Final Element Part Information

Final Element Group(s)	Edit
(1) Final Element Group	Details
PFDavg Final Element Part:	7.07E-03
MTTFS Final Element Part (years):	2668.95

SIF Performance Metrics

Safety Instrumented Function	Preview
Average Probability of Failure on Demand (PFDavg)	4.01E-02
Safety Integrity Level	1
Safety Integrity Level (Architectural Constraints)	0
Risk Reduction Factor	25
MTTFS (years)	3.45



SIF Design Options

If the SIF verification shows that the SIL level has not been achieved by the proposed design a number of options are available to the designer:

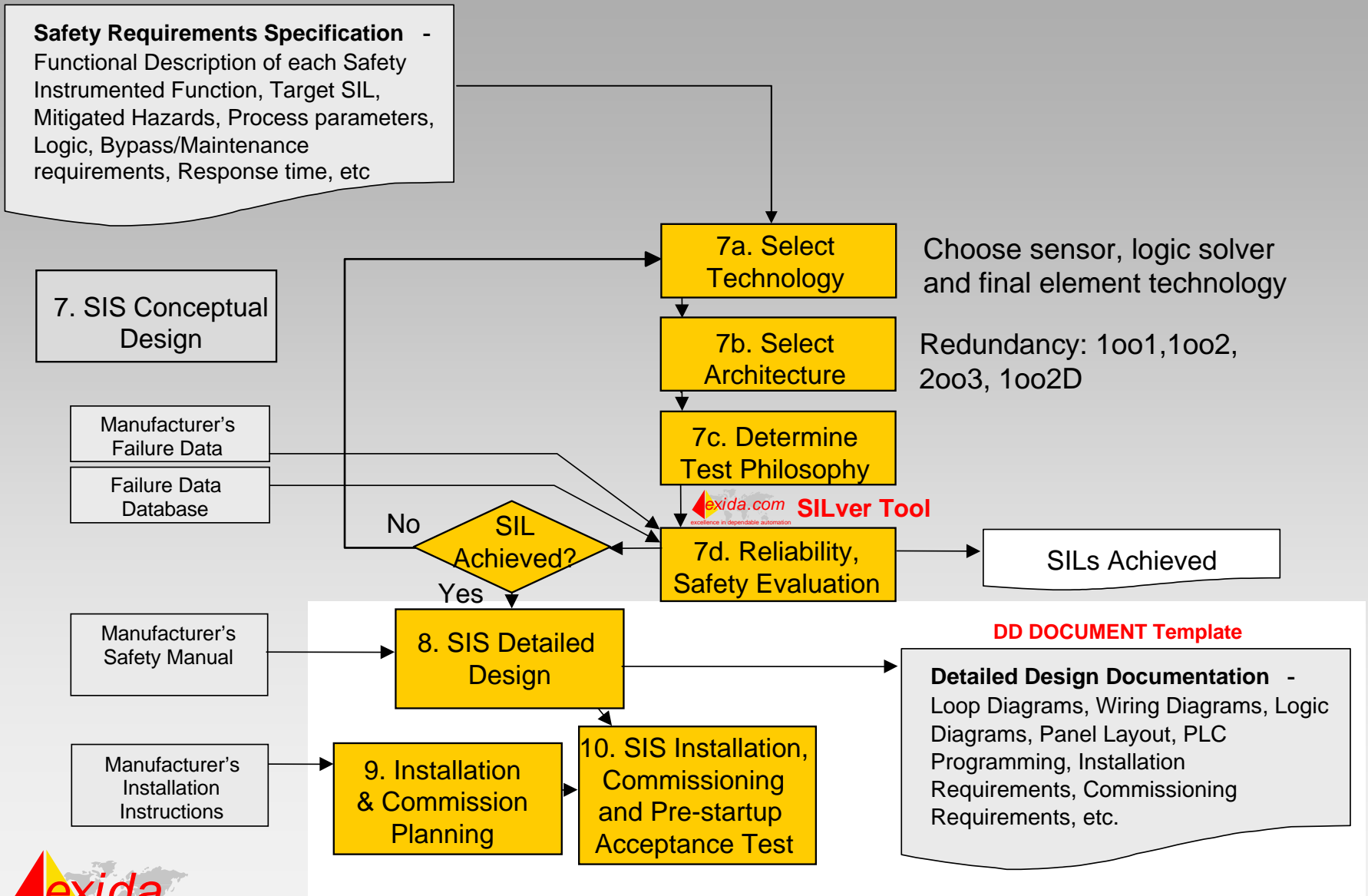
1. Re-evaluate the SIL requirement by adding other layers of protection, etc.
2. Reduce the proof test interval – this may involve provisions for on-line testing.
3. Choose equipment with better safety ratings – lower dangerous failure rate or better diagnostics.
4. Change the architecture by adding more redundancy.

Safety Requirements Specification - Safety Function Requirements including target SIL

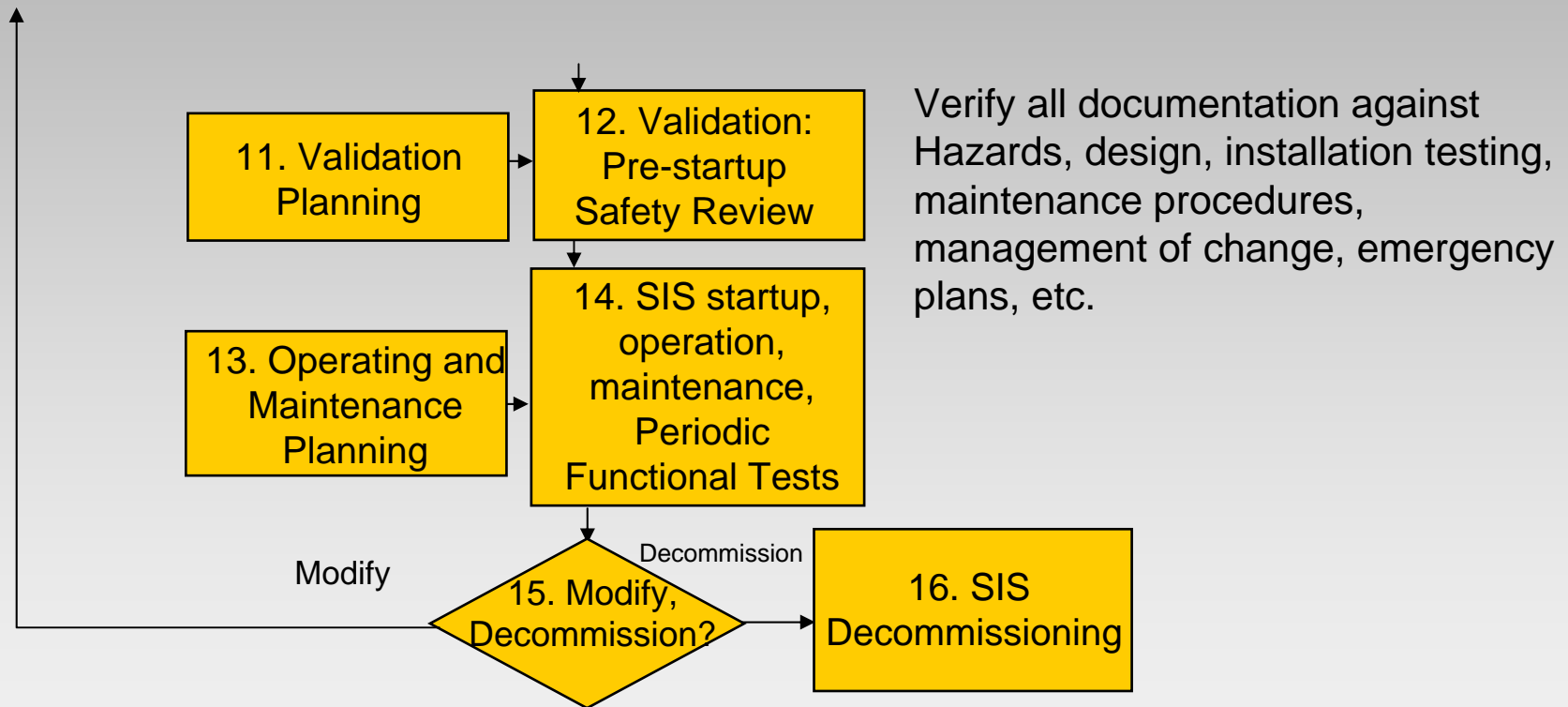
7d. Reliability and Safety Evaluation

PFDavg, RRF
MTTFS,
SIL achieved

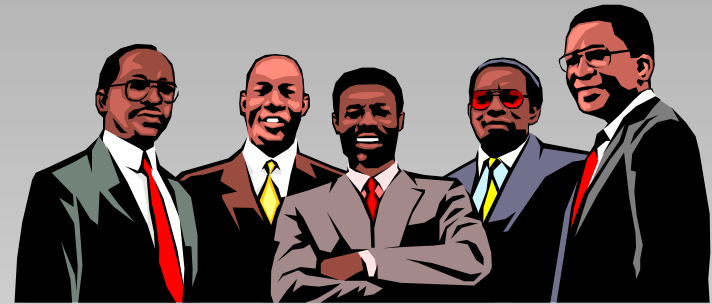
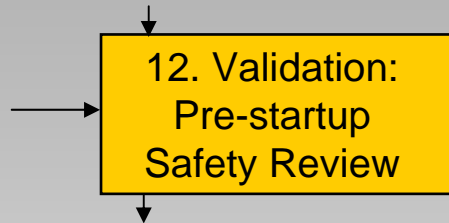
Safety Lifecycle “Realization” Phase



Safety Lifecycle “Operation” Phase



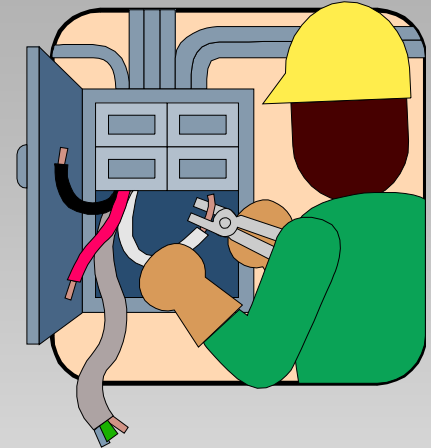
Validation / Pre-Startup Acceptance Test (PSAT)



- Objectives
 - Verify that the SIS functions according to design requirements.
- Tasks
 - Verify operation of field instruments
 - Validate logic and operation
 - Verify SIL of installed equipment
 - Produce required documentation – Certifications if required

Periodic Proof Testing

14. SIS startup,
operation,
maintenance,
Periodic
Functional Tests



- **Objectives**
 - Verify that the SIS continues to function according to design requirements.
- **Tasks**
 - Verify operation of field instruments
 - Validate logic and operation
 - Document results of all periodic testing

Safety Life Cycle

Analysis

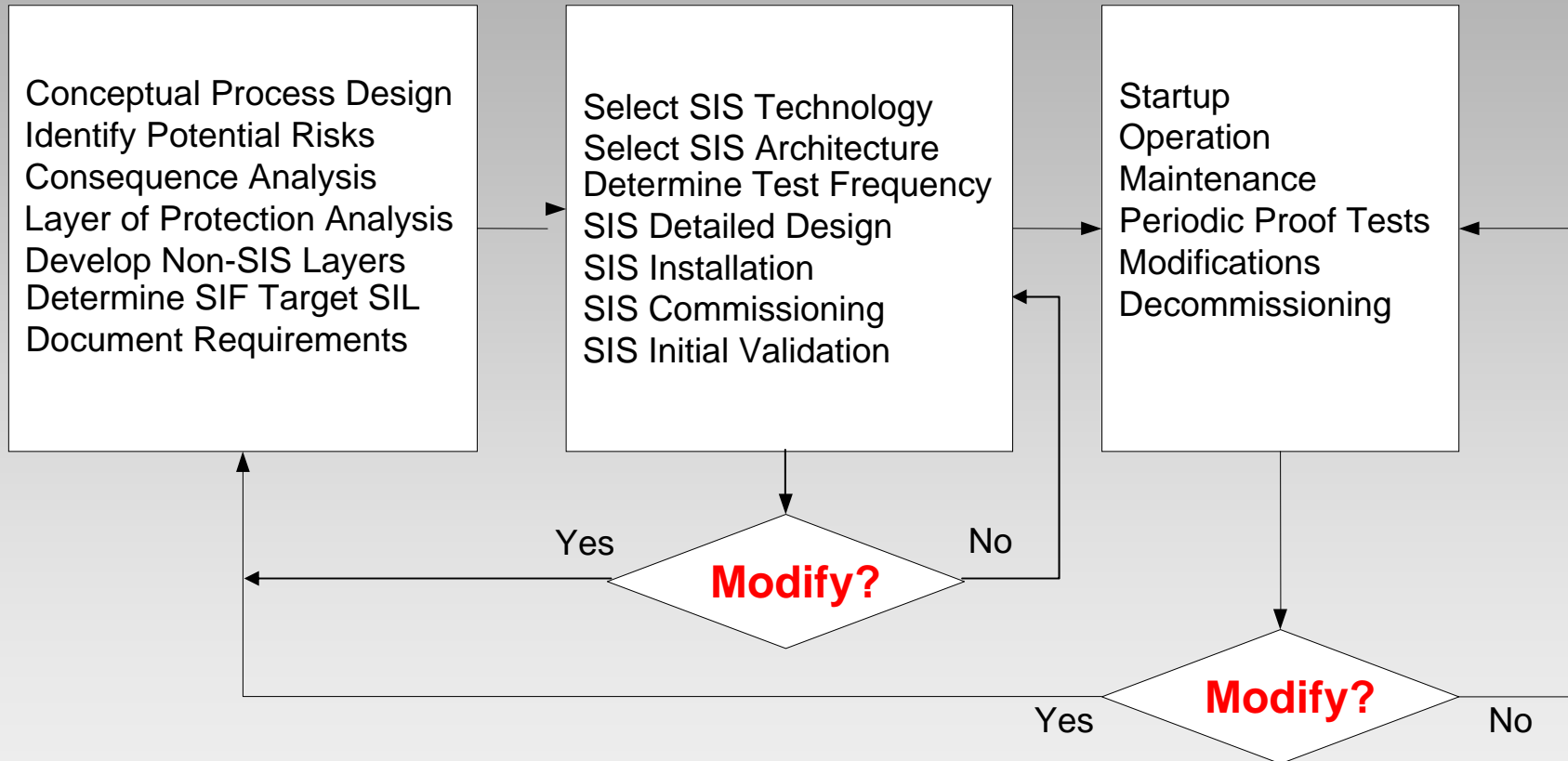
Conceptual Process Design
Identify Potential Risks
Consequence Analysis
Layer of Protection Analysis
Develop Non-SIS Layers
Determine SIF Target SIL
Document Requirements

Realization

Select SIS Technology
Select SIS Architecture
Determine Test Frequency
SIS Detailed Design
SIS Installation
SIS Commissioning
SIS Initial Validation

Operation

Startup
Operation
Maintenance
Periodic Proof Tests
Modifications
Decommissioning

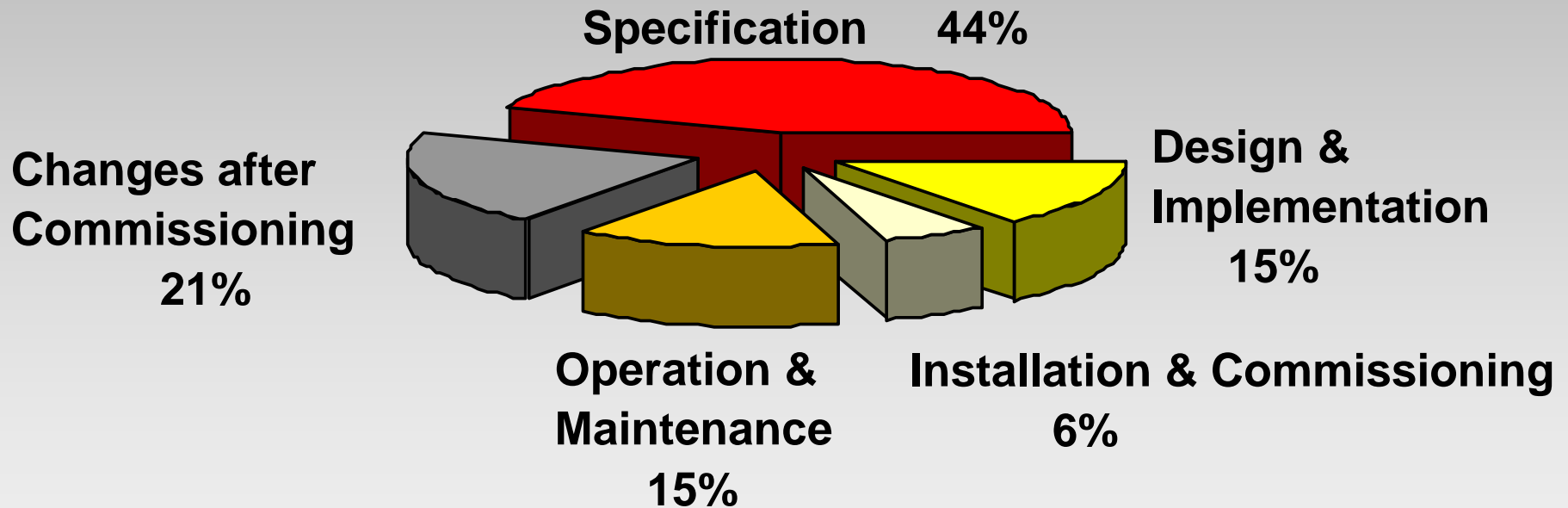


Safety Lifecycle Objectives

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

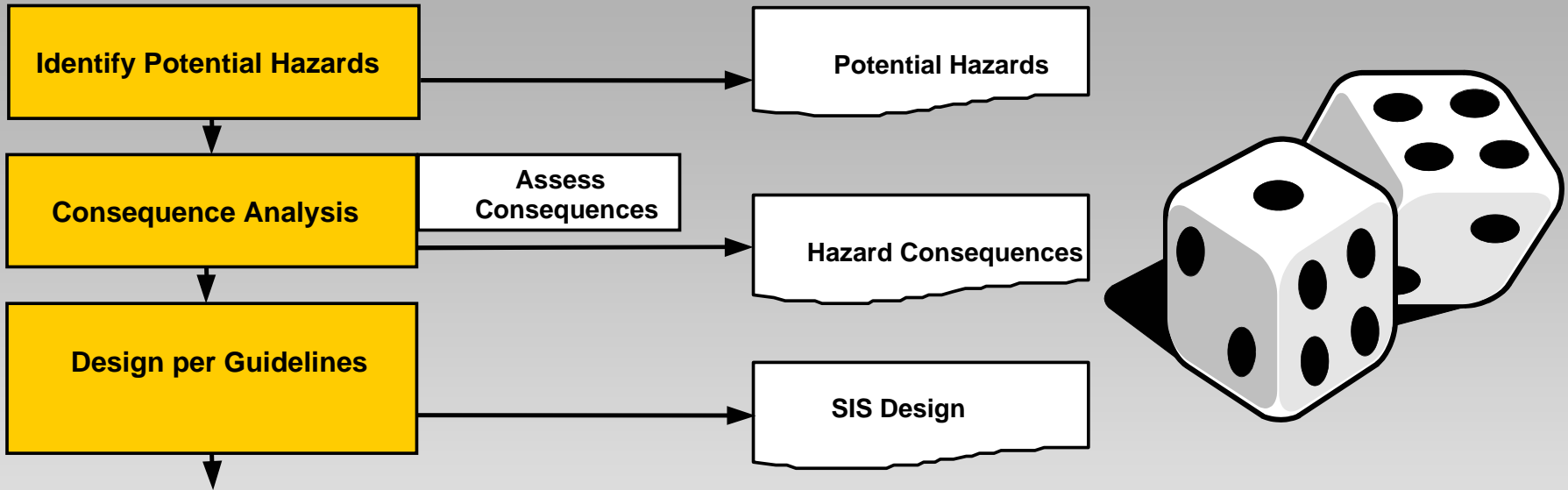
Do not continue problems of the past

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

Match design with risk – optimize

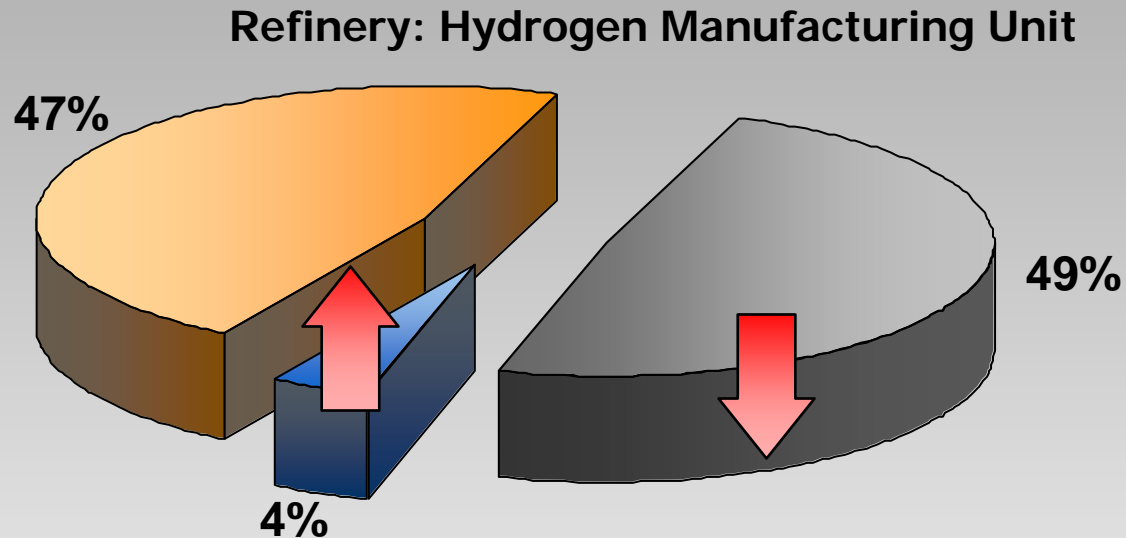


Safety Instrumented Functions

Practical results of a SLC



Source



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

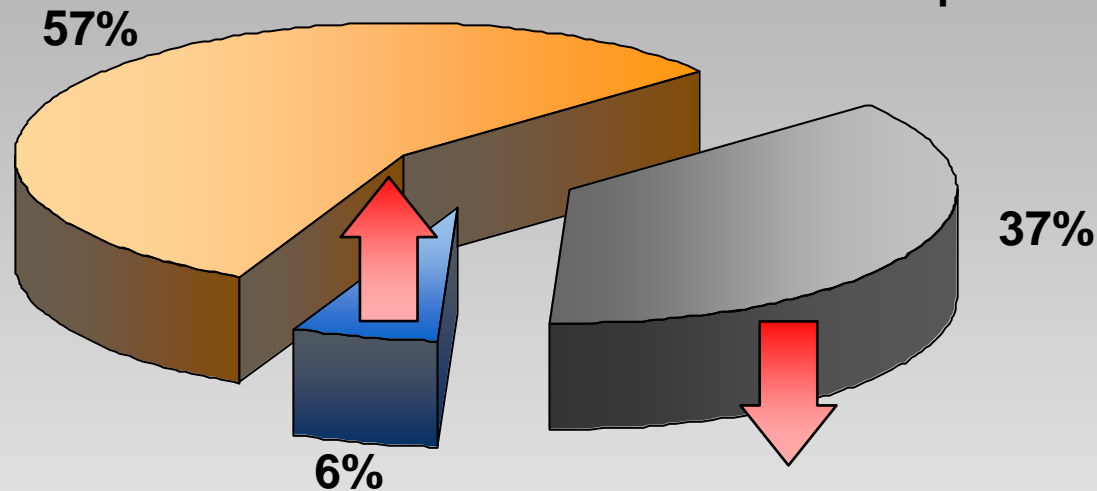
Safety Instrumented Functions

Practical results of SLC

Total of 5319 loops are considered.
At 7 different plants

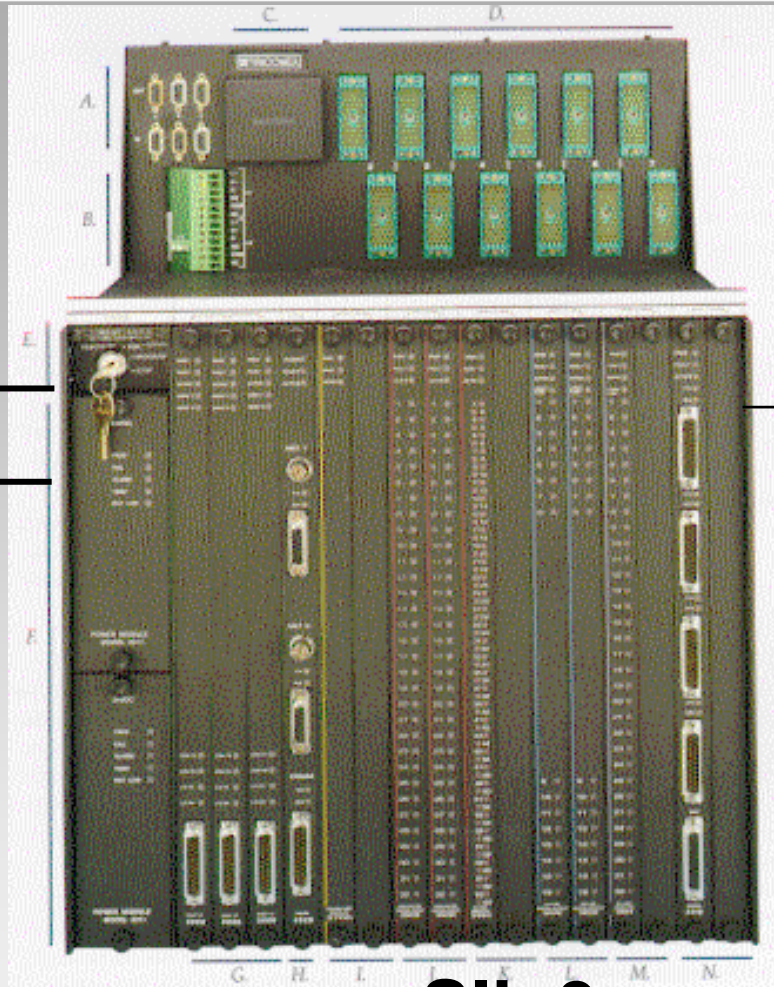


Source NAM



- 37%: Safety Functions were over-engineered
- 6%: Safety Functions were under-engineered (unsafe)
- 57%: No change

Eliminate “Weak Link” designs



**Pressure
Switch –
SIL ?**

Solenoid Control Valve

SIL ?

SIL 3

Common Global Standards

**Plant
Upgrade**

**Gas
Pipeline**

**Offshore
Platform**

**Offshore
Platform**

**Chemical
Plant**

FPSO



Higher Safety – Optimal Cost

IEC 61508 - Functional Safety, “Umbrella Standard” - 2000

IEC (EN) 61511 – Process industry application oriented standard, 2003

ISA84.01-2004 (61511+)

Passed ANSI September 2004



- 1. Performance based not PERSCRIPTIVE**
- 2. Use of a Safety Lifecycle engineering process**



excellence in dependable automation

www.exida.com

