Practical and Robust Implementation of the IEC Functional Safety Standards

Abstract

- The release and adoption of IEC 61508 and IEC 61511 has created new requirements for all organizations involved with equipment used in safety related systems. As these functional safety standards are applied more broadly across industry and referenced more frequently as examples of best practice by industry and product standards the importance of meeting them is increasing. The requirements of the standards are new to many end users, EPCs, and manufacturers of valve, actuator, and other devices used in the final element which can result in effort invested in areas that do not guarantee compliance or increased safety reliability.
- This presentation will review the functional safety standards along with the steps necessary to meet them. IEC 61508 will be examined including the Safety Lifecycle, keys documentation necessary, and information that is supplied to end users. IEC 61511 will be reviewed to examine the impact of the information supplied by manufacturers. Examples from both the manufacturer and end user viewpoint will be provided to illustrate common pitfalls as well as best practices.

Chris O'Brien

Chris O'Brien is a Partner with Exida Consulting. He has over 25 years experience in the design, manufacturing and marketing of process automation, reserve power systems, and safety related equipment. He focuses on supporting new and existing customers with their implementation of the IEC 61508 and IEC 61511 functional safety standards as well as reliability analysis for mechanical devices.

He was formerly Vice President of the Power Systems Business Unit of C&D Technologies, a business that specialized in the design and implementation of high reliability back up power systems. Prior to that, he was with Moore Products/Siemens Energy and Automation where he held several positions including General Manager of the Instrumentation Division.

Chris is the author of Final Elements and the IEC 61508 and IEC 61511 Functional Safety Standards and has been awarded 5 patents, including a patent of the industry's first safety rated pressure transmitter. He has a Bachelors of Mechanical Engineering from Villanova University.

Topics

- The Functional Safety Standards
- What are Customers Doing?
- Critical Issues
- Importance of Data Integrity
- Product Certification
- Roles and Responsibilities

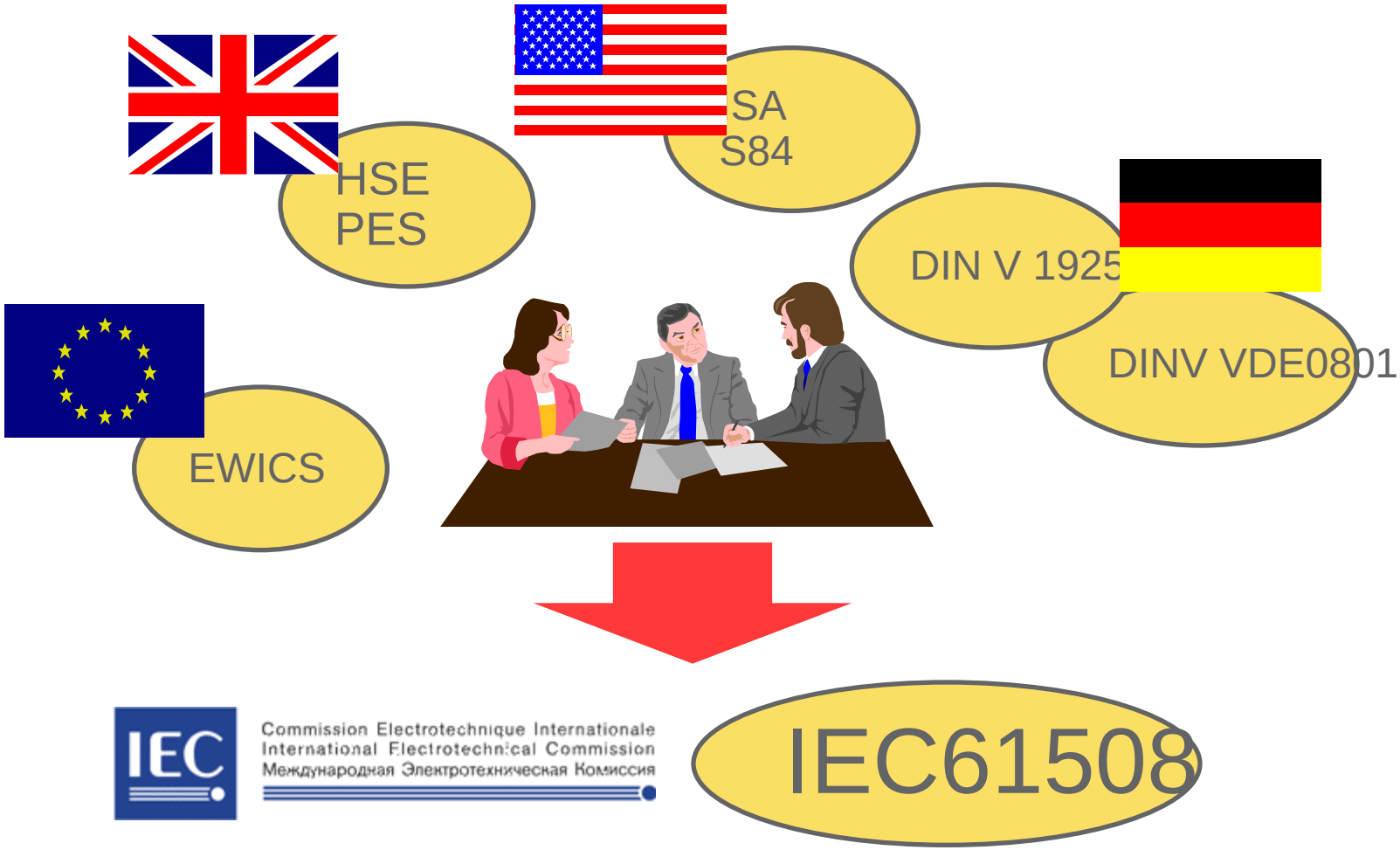
The Functional Safety Standards

- What is Functional Safety?
- Scope of IEC 61508
- How the standard apply to Mechanical Devices?
- What does the standard address?
  - Safety Lifecycle
  - Systemic Faults
  - Random Faults

IEC/EN 61508 – Functional Safety

Functional Safety Goal – The automatic safety function will perform the intended function correctly or the system will fail in a predictable (safe) manner.

IEC/EN 61508 – Consensus Standard



IEC 61508 – Summary

- Applies to “Automatic Protection Systems” – E/E/PE
- Provides measures of protection against random hardware failures and “systematic” design failures
- Can be applied to PROJECT level work – bespoke (turnkey) systems
- Can be applied to PRODUCT level work – off the shelf products applied in many applications

IEC
Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

IEC 61508 Standard

- Targets **Suppliers**
  - Requirements for suppliers of process control and instrumentation for component / element or sub-system safety
  - End Users should seek suppliers with products certified to this standard by a reputable certifying agency

IEC 61508 Enforcement

- In some countries, the standard has been accepted by governments with the force of law
- In most situations, the standard typically is cited as best practice
  - Often required by end-user customers as part of project contracts
- When accidents happen, the standard can be cited in civil cases as a commonly accepted standard of performance

IEC/EN 61508 – E/E/PE

IEC 61508 states it was written for E/E/PE based systems.

E – electrical

E – electronic

PE – programmable electronic

Therefore not applicable for mechanical products??

Just Google It

Safety Critical Mechanical Devices Must be Included

A4) How does IEC 61058 apply where E/E/PE technology makes up only a small part of the safety-related system?

IEC 61508 is applicable to any safety-related system that contains an E/E/PE device.

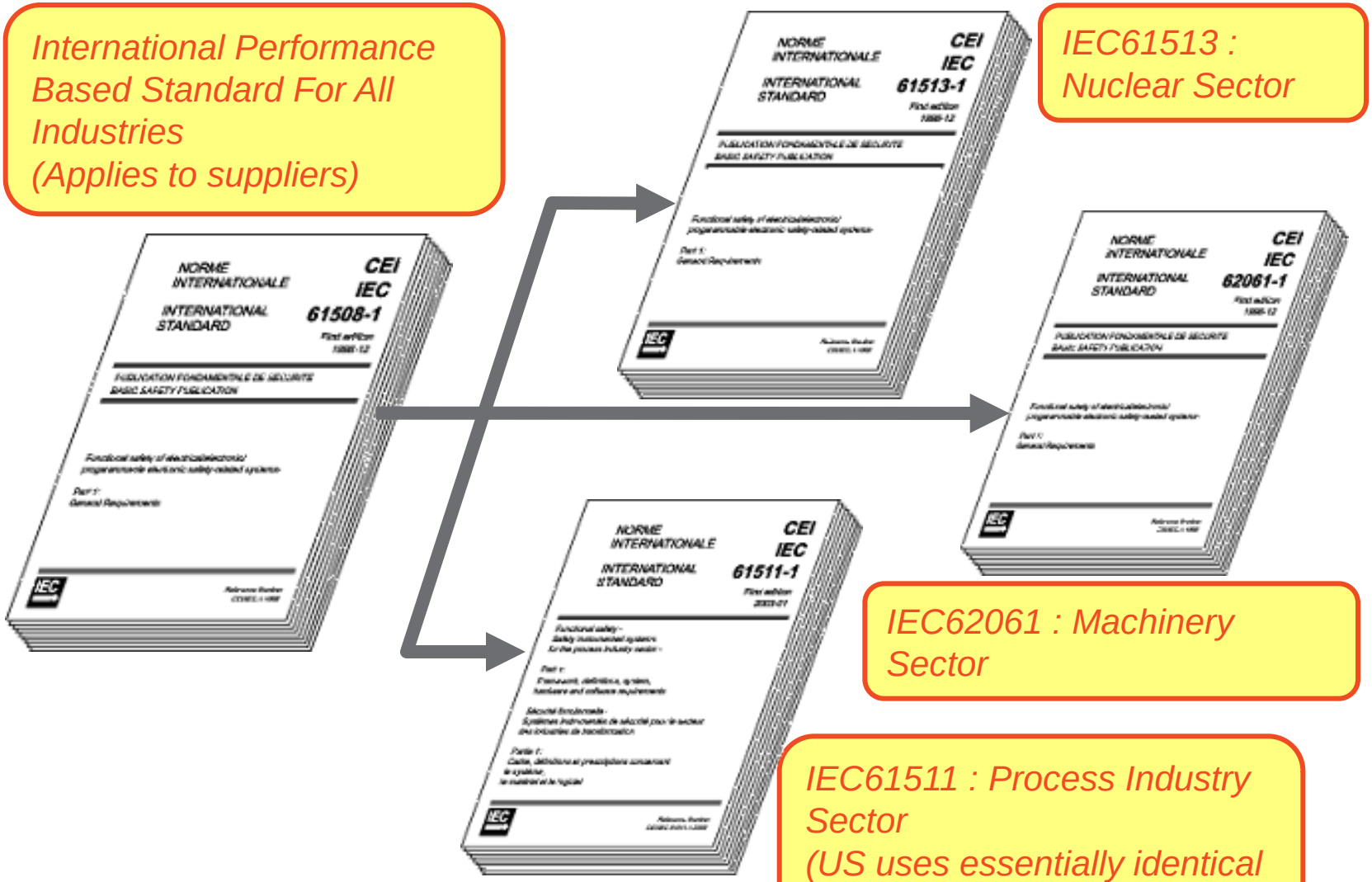
This applicability is appropriate because many requirements, particularly in IEC 61508-1, are not technology specific. Indeed, early development phases (such as initial concept, overall scope definition, hazard and risk analysis and specifying the overall safety requirements) may take place before the implementation technology has been decided.

Even during later phases such as realisation, specific functional safety requirements apply directly to non-E/E/PE devices, such as mechanical components, as well as E/E/PE devices. For example, the requirements for hardware reliability and fault tolerance in IEC 61508-2 directly relate to the properties of all components in the E/E/PE safety-related system, whether or not they include E/E/PE technology.

For low complexity E/E/PE safety-related systems, it is possible to comply with IEC 61508 while not meeting every requirement of the standard.

The Standards

International Performance Based Standard For All Industries (Applies to suppliers)



IEC61513 : Nuclear Sector

IEC62061 : Machinery Sector

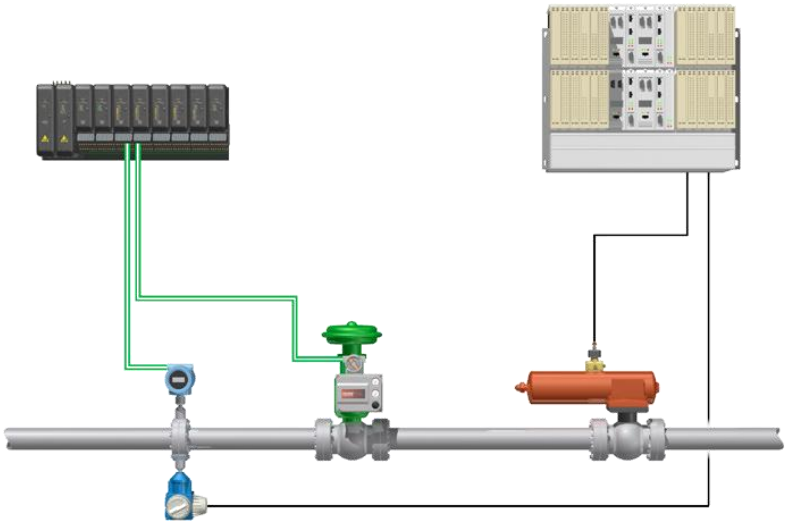
IEC61511 : Process Industry Sector (US uses essentially identical ISA 84.00.01-2004)

What are Customers Doing?

- IEC 61511
- Why is there a need?
- Safety Instrumented Systems
- Safety Instrumented Functions
- The Safety Lifecycle

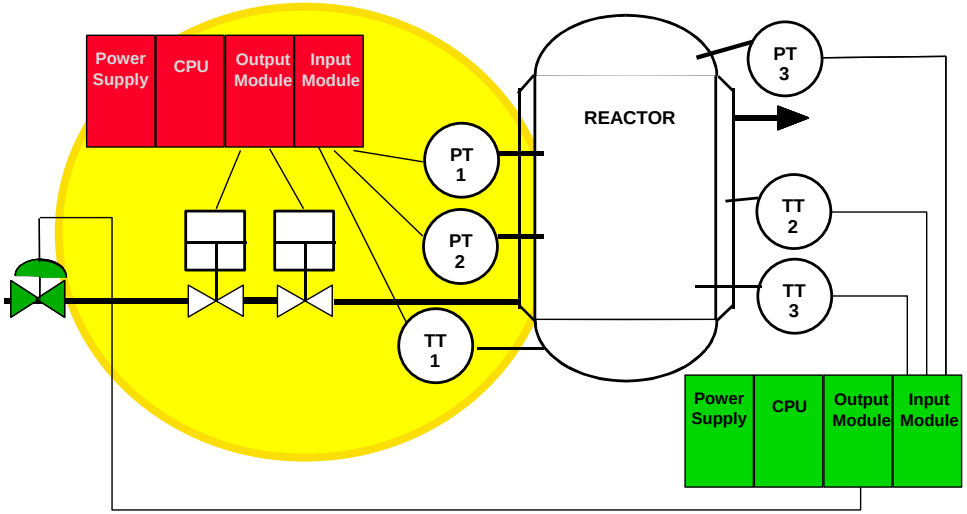
IEC 61511 Standard

- 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
  - Independent Functional Safety Assessments
- 3 sections
  - Requirements
  - Guidelines
  - SIL Selection



Why is There a Need?

Safety Instrumented System Definition



IEC 61511 defines a Safety Instrumented System (SIS) as:

"instrumented system used to implement one or more safety instrumented functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s)." *IEC 61511 Part 1 : 3.2.72*

Safety Instrumented System Functional Definition

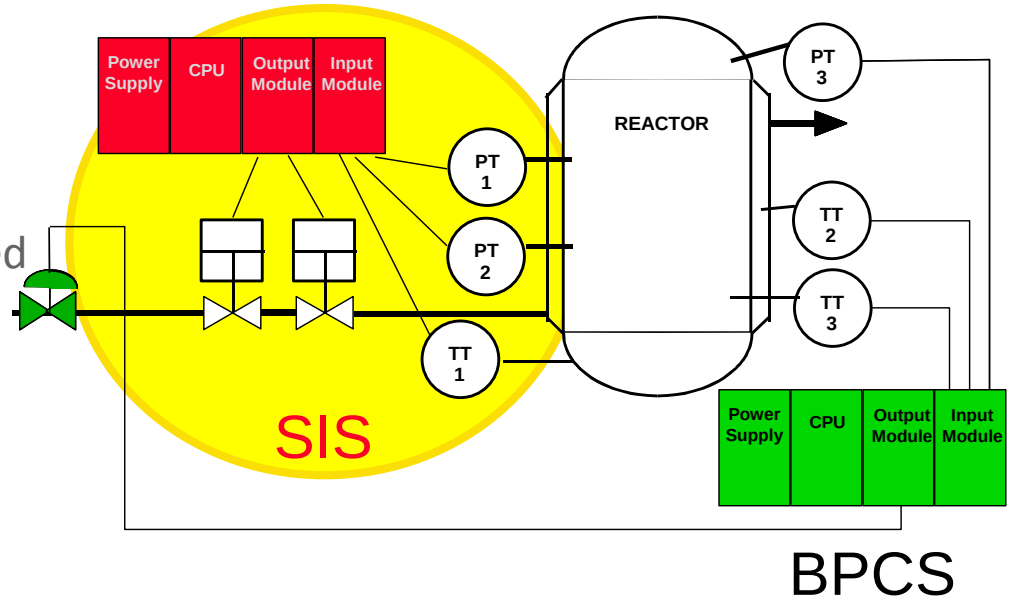
Practitioners often prefer a more functional definition of SIS such as:

"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;

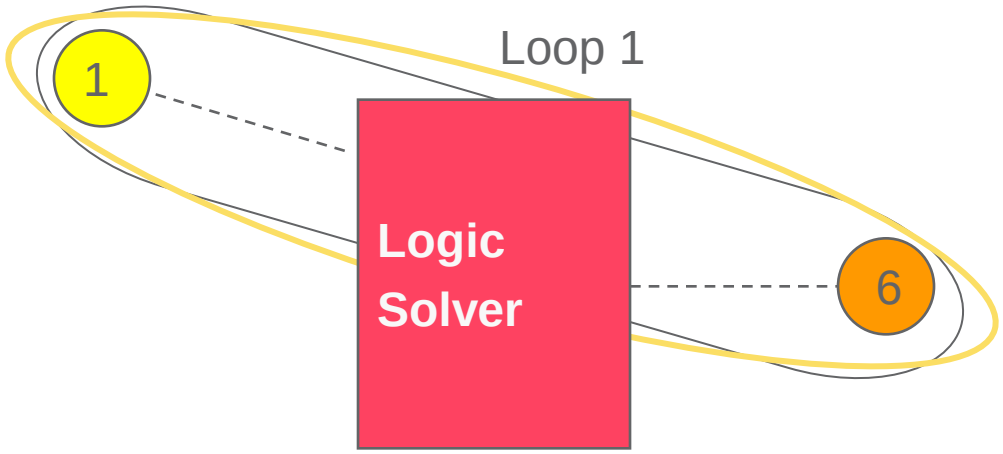
2. Permit a process to move forward in a safe manner when specified conditions allow (permissive functions);

3. Taking action to mitigate the consequences of an industrial hazard."



* BPCS: Basic Process Control System

Safety Instrumented Function (SIF)



"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

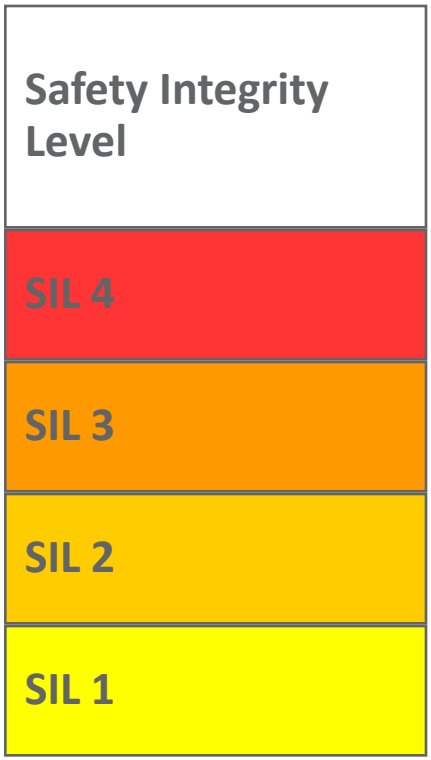
Safety Instrumented Function Examples

- On detecting high temperature, prevent column rupture by shutting off steam flow to the reboiler
- 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

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

What is SIL

SIL: Safety Integrity Level

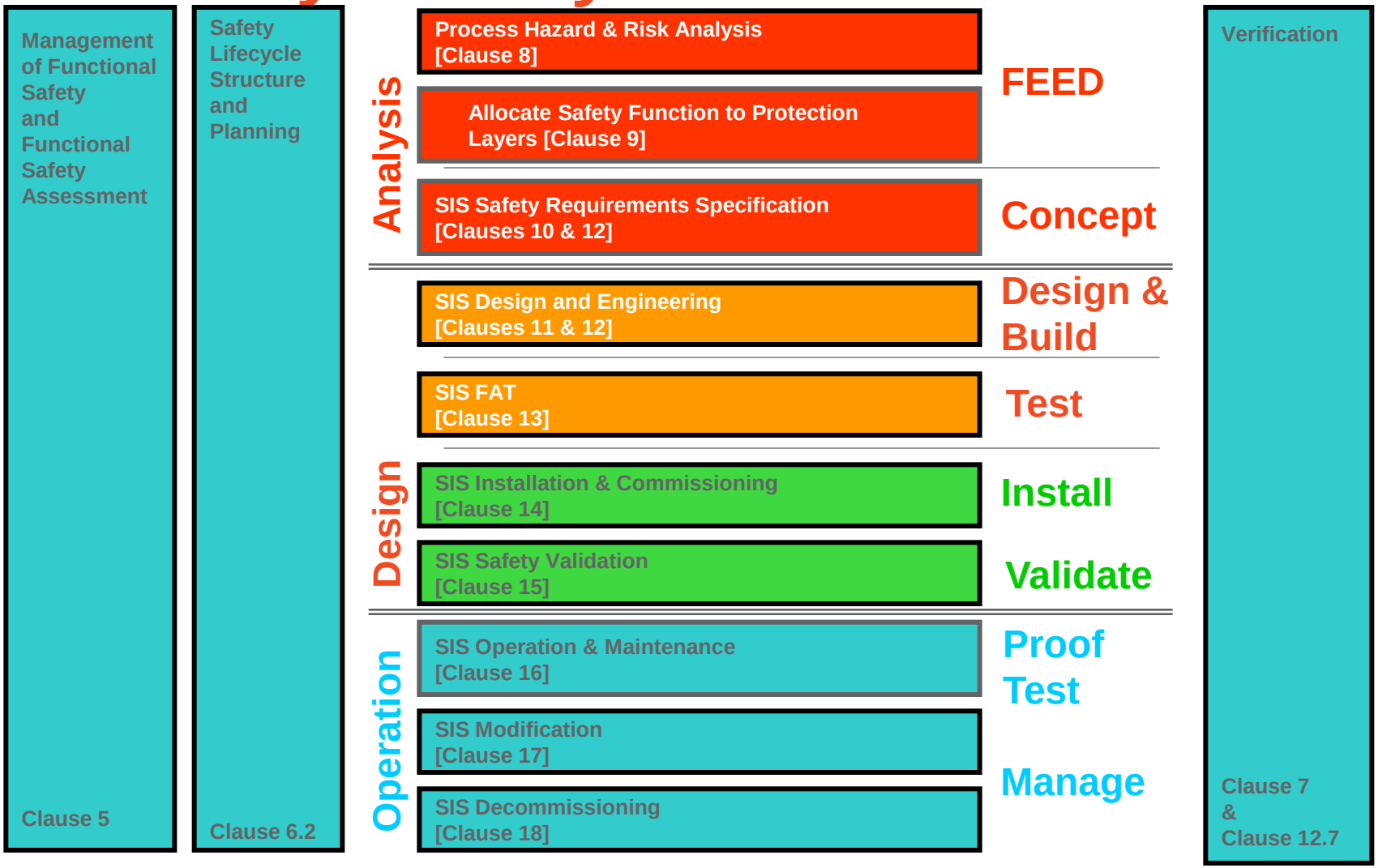


"Discrete level (one out of four) for specifying the safety integrity requirements of the ***safety instrumented functions*** to be allocated to the safety instrumented systems. SIL 4 has the highest safety integrity and SIL 1 the lowest."

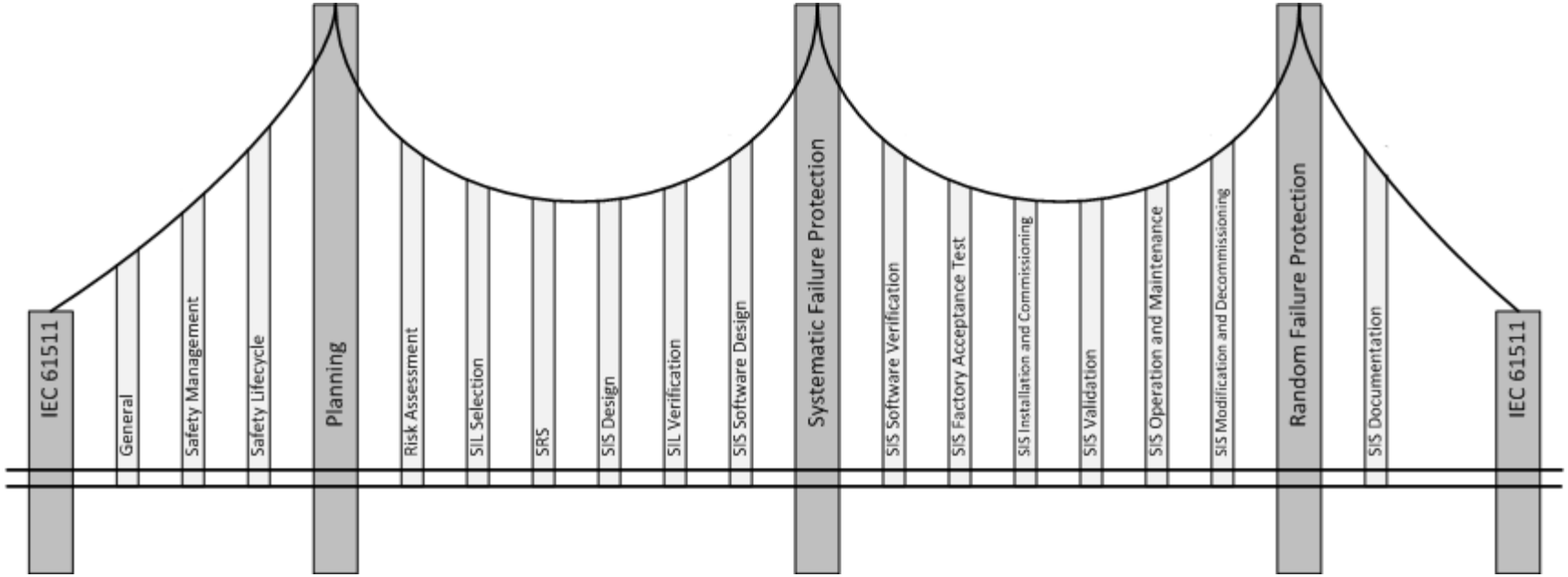
IEC 61511 Part 1 : 3.2.74

How well the SIF performs its job of managing risk

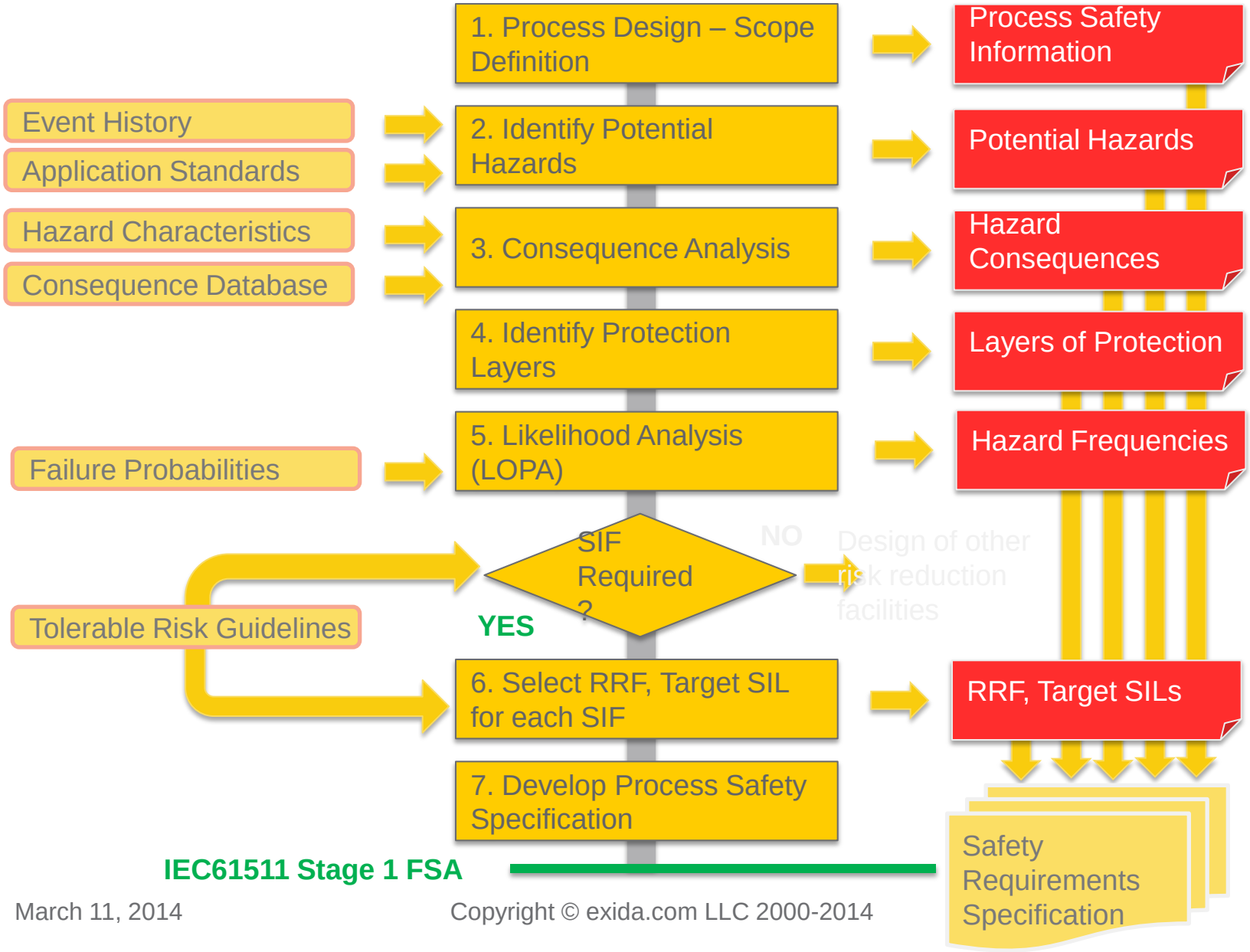
Safety Lifecycle – IEC 61511



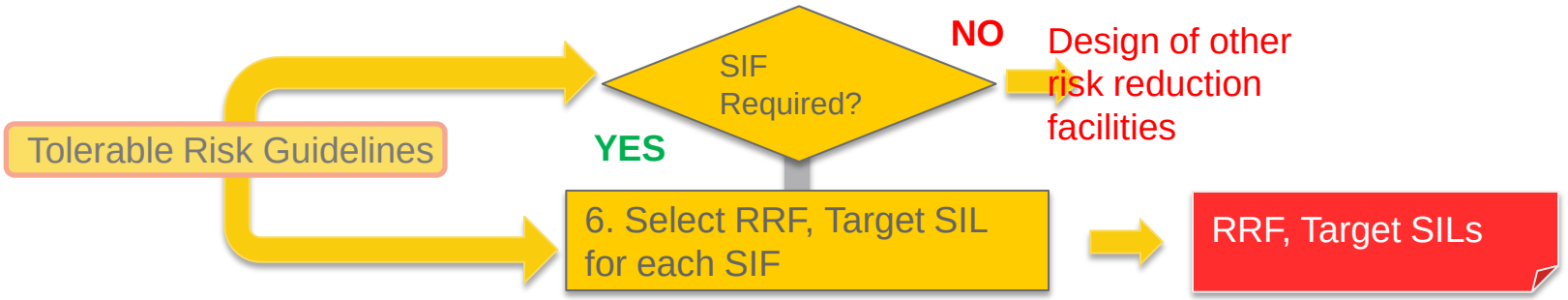
Bridge to Safety



Analysis Phase



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

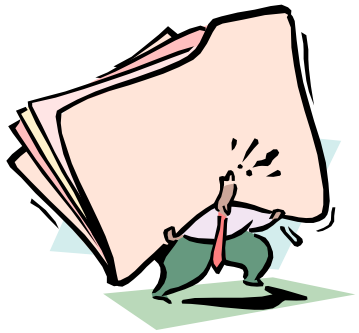
IEC61511
ISA84.01

Safety Requirements Specification

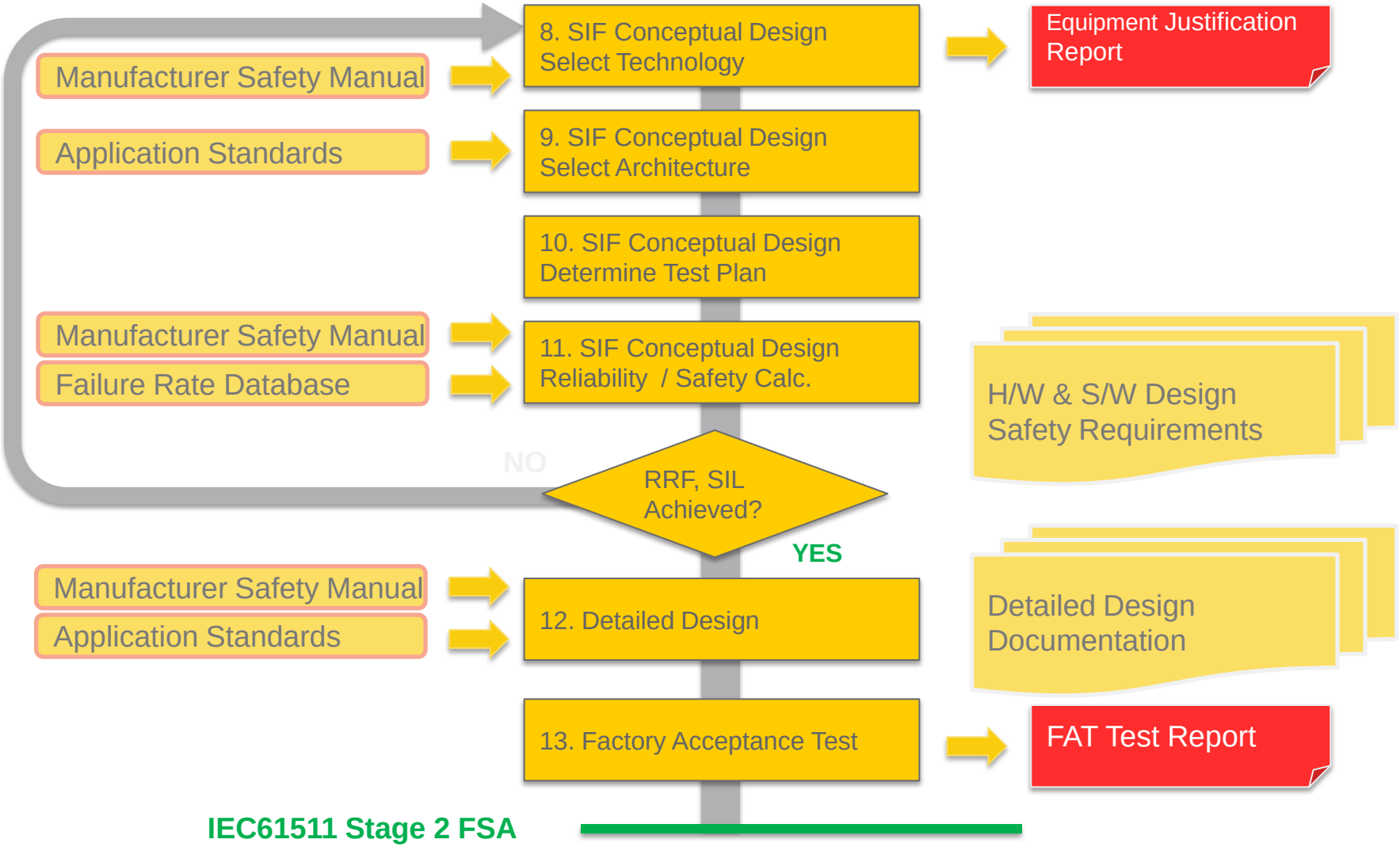
7. Develop Process Safety Specification

Safety Requirements Specification

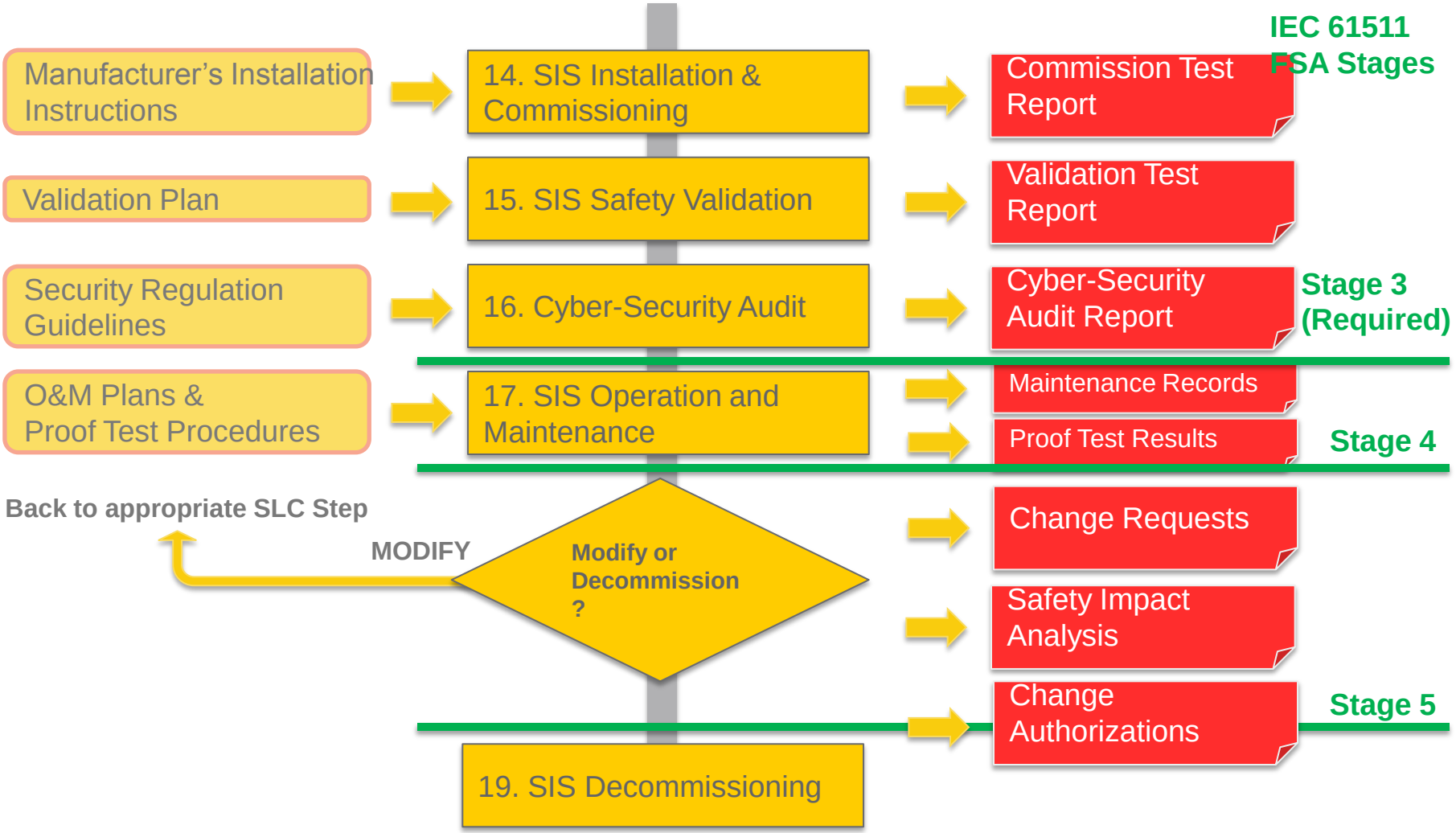
- Objective
  - Specify all requirements of SIS needed for detailed engineering and process safety information purposes
- Tasks
  - Identify and describe safety instrumented functions
  - Document SIL
  - Document action taken – Logic, Cause and Effect Diagram, etc.
  - Document associated parameters – timing, maintenance/bypass requirements, etc.



Design Phase



Operation and Maintenance Phase



Critical Issues

- Defines user project requirements well
- SIL Verification
- Proven-in-Use or IEC 61508 for ALL EQUIPMENT
- Requirements management

Defines user project requirements well

- Safety Lifecycle
- Strength against random failures
- Strength against systemic failure

SIF Verification Task

Safety Requirements Specification:
Safety Requirements including SIL target

Manufacturer Safety Manual

Failure Rate Database

11. SIF Conceptual Design
Reliability / Safety Calc.

PFDavg, RRF
MTTFS,
SIL achieved

Select Technology




- **Objective**
  - Choose the right equipment for the purpose - all criteria used for 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

Equipment Selection

IEC 61511, Functional Safety for the Process Industries, requires that equipment used in safety instrumented systems be chosen based on either **IEC 61508 assessment** (parts 2 and 3) to the appropriate SIL level or **justification based on "prior use" criteria** (IEC 61511-1, 11.5.3)

Select Architecture

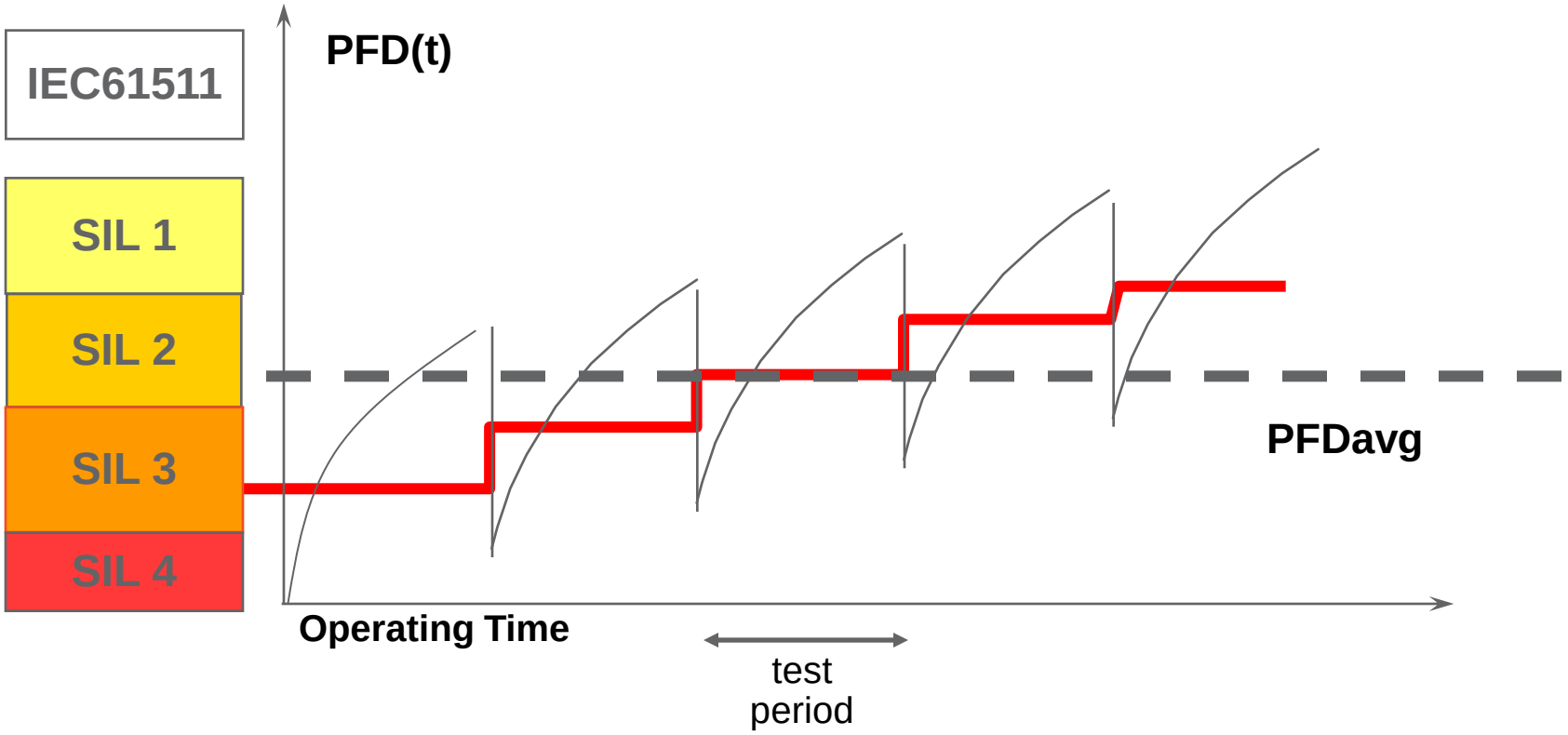
- Objective
  - Choose type of redundancy if needed
- Tasks
  - Choose architecture
  - Obtain reliability and safety data for the architecture

Establish Proof Test Frequency - Options

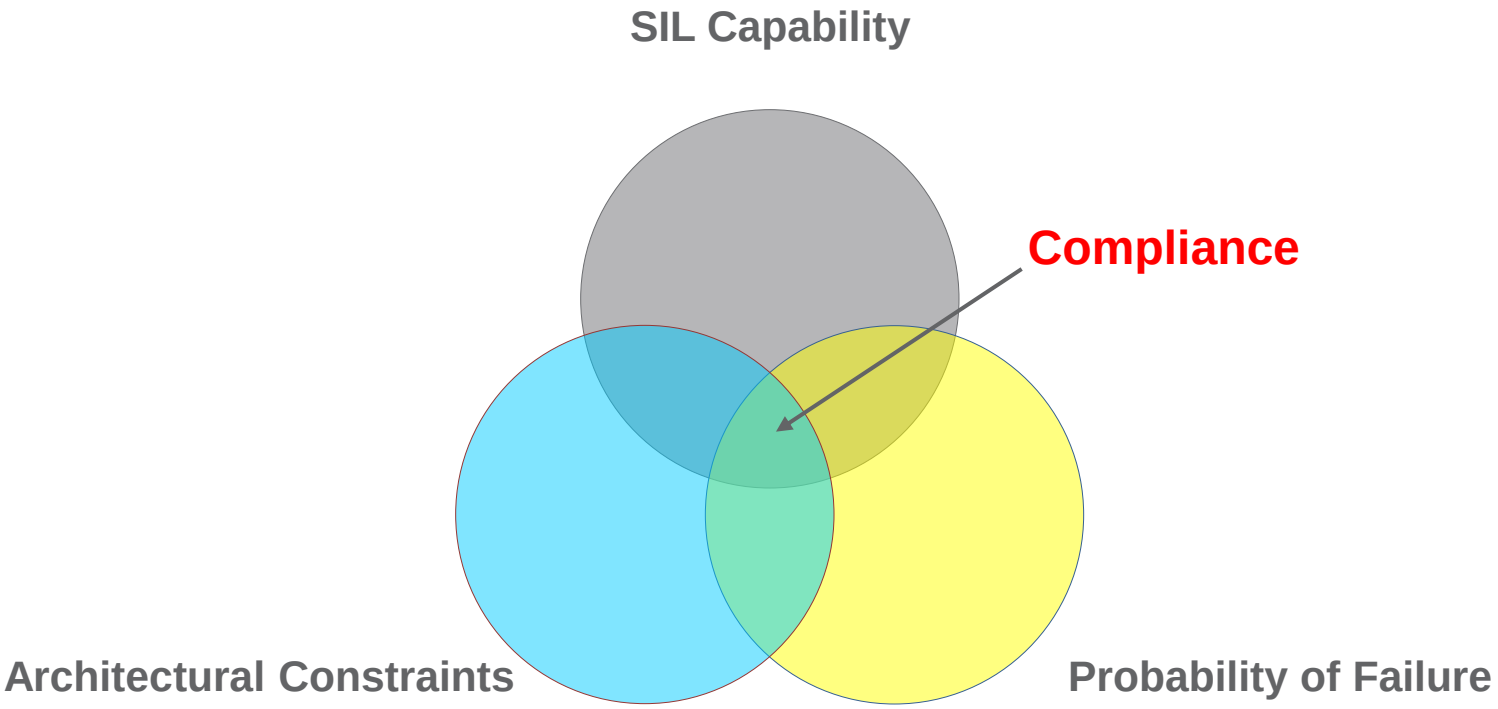
- In general the testing can include:
  - Automatic testing which is built into the SIS
  - Off-line testing, which is done manually while the process is not in operation
  - On-line testing, which is done manually while the process is in operation

Effects of Incomplete Testing

Because of incomplete testing the PFD never returns to its original value and the risk reduction can be significantly lower.



Compliance Requirements

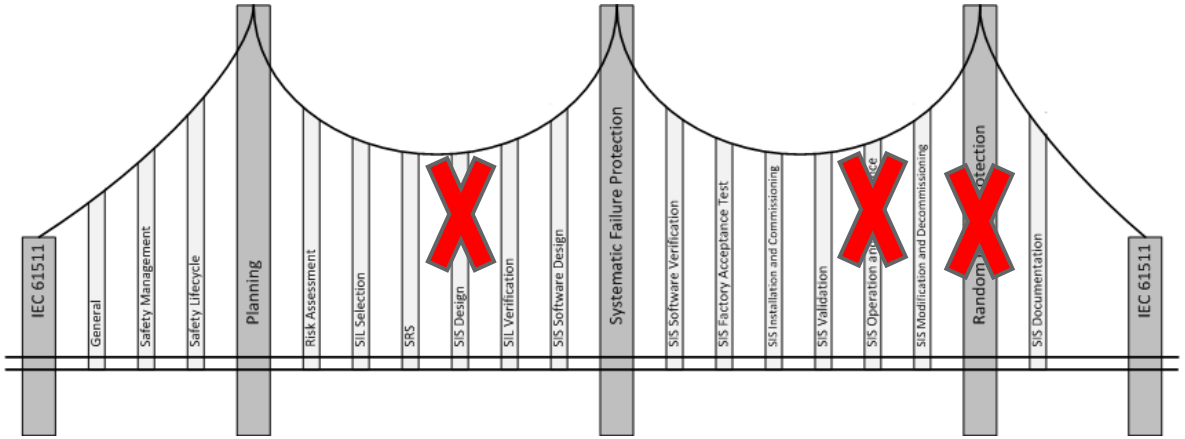


Importance of Data Integrity

- Why does it matter?
- Comparison of data sources
- Impact of “too good to be true” data
- Product Stewardship
- Legal Responsibility

Effect of Bad Data

- Optimistic data leads to unsafe designs
  - Insufficient redundancy
  - Insufficient testing
- Required risk reduction will not be reached



BAD Data

- Merriam-Webster defines BAD:
  - Failing to reach an acceptable standard: POOR < a *bad* repair job >

- exida defines BAD data as:
  - Data that leads to unrealistic, often dangerous, designs.

Risk Varies With Use

Use	Statement	Risk
Marketing Brochure	“We make very high quality stuff, it never fails!”	LOW: Reputation may suffer from exaggerated claims
Safety Reliability Calculations	“Look the math shows you don’t need redundancy and never need to test the function.”	VERY HIGH: Potential loss of life due to under-designed safety functions.

What are Some Companies Missing?

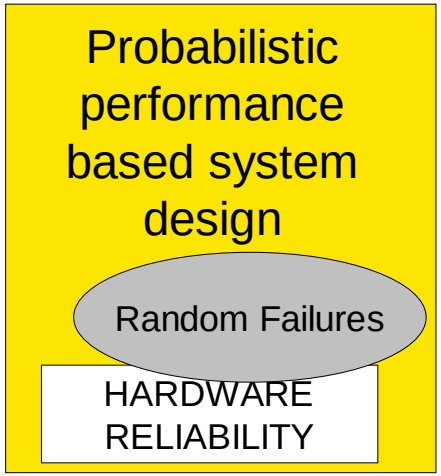
- One of the premises of IEC 61508 and IEC 61511 is that automated protection systems with diagnostics and periodic testing can provide higher safety reliability than typical control functions.
- The standards outline the steps that must take place to claim this higher safety reliability.
- However these steps are only valid if appropriate (GOOD) data is used.

Failure Rate Data Models

- Industry Databases
  - NOT Application Specific
  - NOT Product Specific
- Manufacturer FMEDA, Field Failure Study
  - Product Specific
  - NOT Application Specific
- Detail Field Failure Study – Application model
  - Product Specific
  - Application Specific

Mechanical Cycle Testing

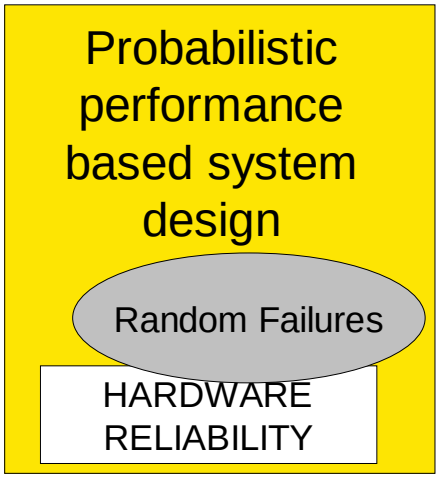
Cycle Testing is useful for estimating failure rates when the dominant mechanical failure rates are due to (premature) wear-out of components. This occurs in applications with frequent dynamic movement, lubrication and mechanical loading. **Testing must be done until at least 10% of the population has failed.**



This method is NOT APPLICABLE to static applications such as demand mode safety systems as it does not account for failure modes like sticktion, cold welding, corrosion, etc.

Field Failure Studies

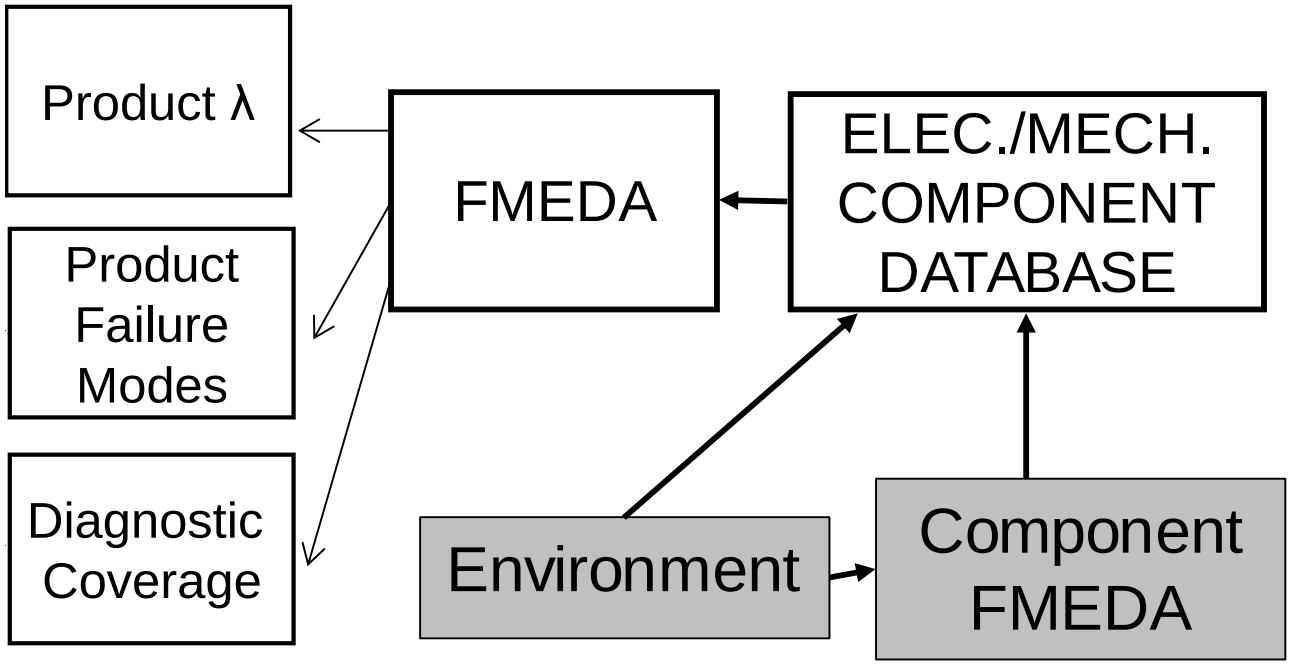
Field failure studies with sufficient information represent a rich opportunity to obtain failure rate and failure mode information about a product in a specific application.

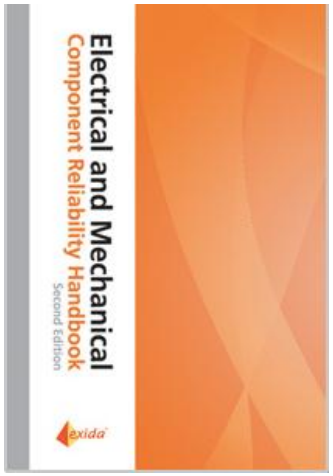


- A problem is insufficient information. However, even limited information is useful.
- Manufacturer's warranty studies are particularly bad as many failures are classified as "not a failure" and not counted.

FMEDA Based Failure Model

A predictive failure rate / failure mode model for some components can be constructed from a hierarchical set of FMEDAs. The component database is the repository of the data.





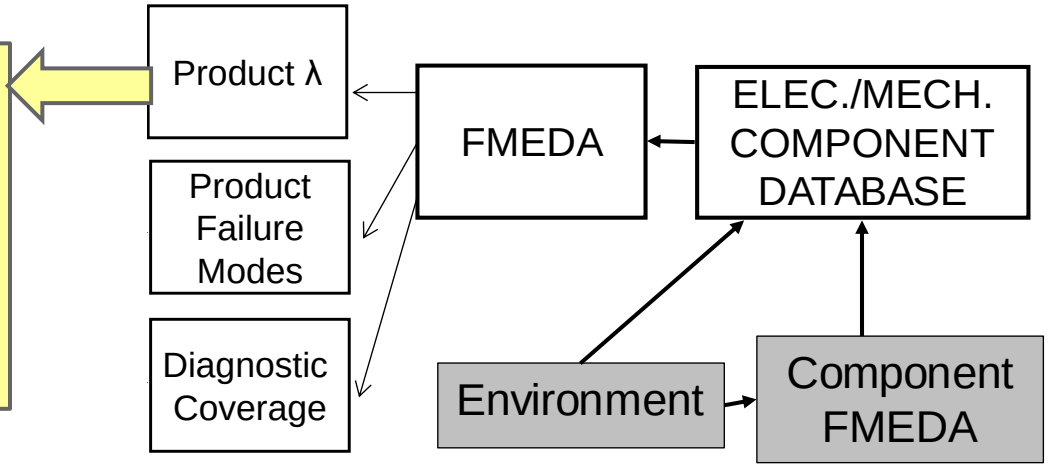
FMEDA = Validated Results

Proven In Use Study

-Performed for all assessments

FMEDA = 88 FITS

PIU = 57 FITS



Classified Failures		
	Data	**Comment**
Number of Failures	69	failures reported
Total Operating Hours	2.43E+09	# devices x # years x 8760 hours/year
% Reported Failures	50%	mix of expensive and inexpensive devices, warranty period
Estimate Actual Failures	138	
Point Estimate - Failure Rate	5.67E-08	
Complexity Factor	1	new versus old design if applicable
Estimate New Actual Failures	138	estimated failures of new design
New Point Estimate - Failure Rate	5.67E-08	per hour
Confidence Interval	0.7	IEC 61508, Part 2, 7.4.7.9
Upper Confidence Limit failure rate	5.93E-08	per hour
Lower Confidence Limit MTTF	1923.6	years

Use Care with High Demand Certifications

TÜV Rheinland Energie und Umwelt GmbH
Test Laboratory for Energy Appliances

TÜVRheinland®
Precisely Right.

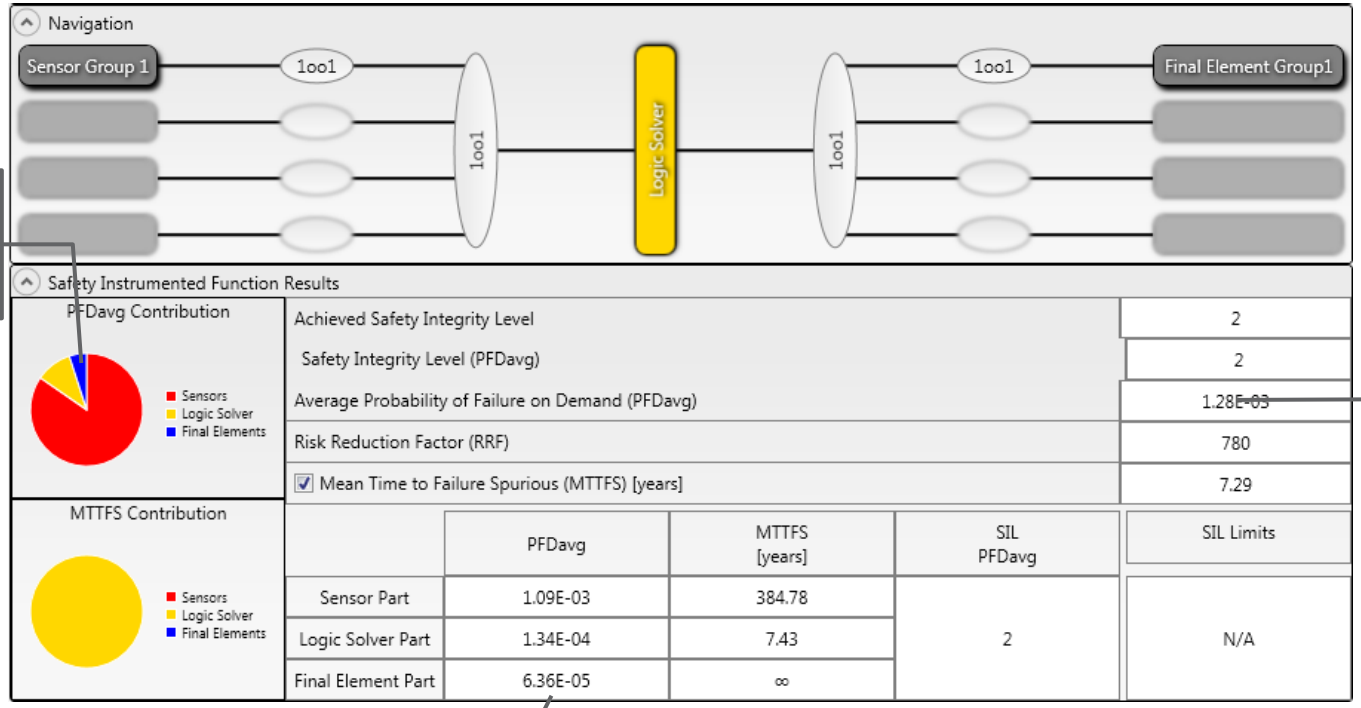
Some certifications are based on failure data derived from "cycle testing" or other methods that require frequent movement of electro-mechanical products. This assessment is not valid for typical low demand process applications.

OEM has Product Stewardship Responsibilities. Don't supply high demand data for low demand applications!

3. Summary of the technical safety characteristics

Probability of dangerous failure on demand	PFD_{spec}	Failure/demand	7,48E-06
Testinterval	Ti	y	1
Confidence niveau	1-α	%	90
Safe failure fraction	SFF	%	90
Hardware fault tolerance	HFT	[-]	0
Diagnostic coverage	DC	%	0
Type of sub system	IEC 61508-2, 7.4.4.1.2		Type A
Mode of Operation	IEC 61508-4, 3.5.16		Low Demand Mode
Assumed demands per year	f_{np}	demand/y	10
Interval for closing test		y	1
Derived Values			
Demand/hour	f_{np}	demand/h	1,14E-03
Meantime between demands		h	8,76E+02
Dangerous failure rate	λ_D	1/h	8,54E-09
		FIT	8,54
MTBF dangerous failures	$MTBF_D$	h	1,17E+08
		y	13368,98
Safe failure rate	λ_S	1/h	7,68E-08
		FIT	76,85
Total failure rate	$\lambda_S + \lambda_D$		8,54E-08
		FIT	85,39
MTBF total		h	1,17E+07
MTBF total		y	1336,90
Dangerous detected	λ_{DD}	1/h	0,00E+00
Dangerous undetected	λ_{DU}	1/h	8,54E-09
Safe detected	λ_{SD}	1/h	0,00E+00
Safe undetected	λ_{SU}	1/h	7,68E-08
Average probability of failure on demand	**PFD_{avg}**	**Failure/demand**	**3,74E-05**

Optimistic Data

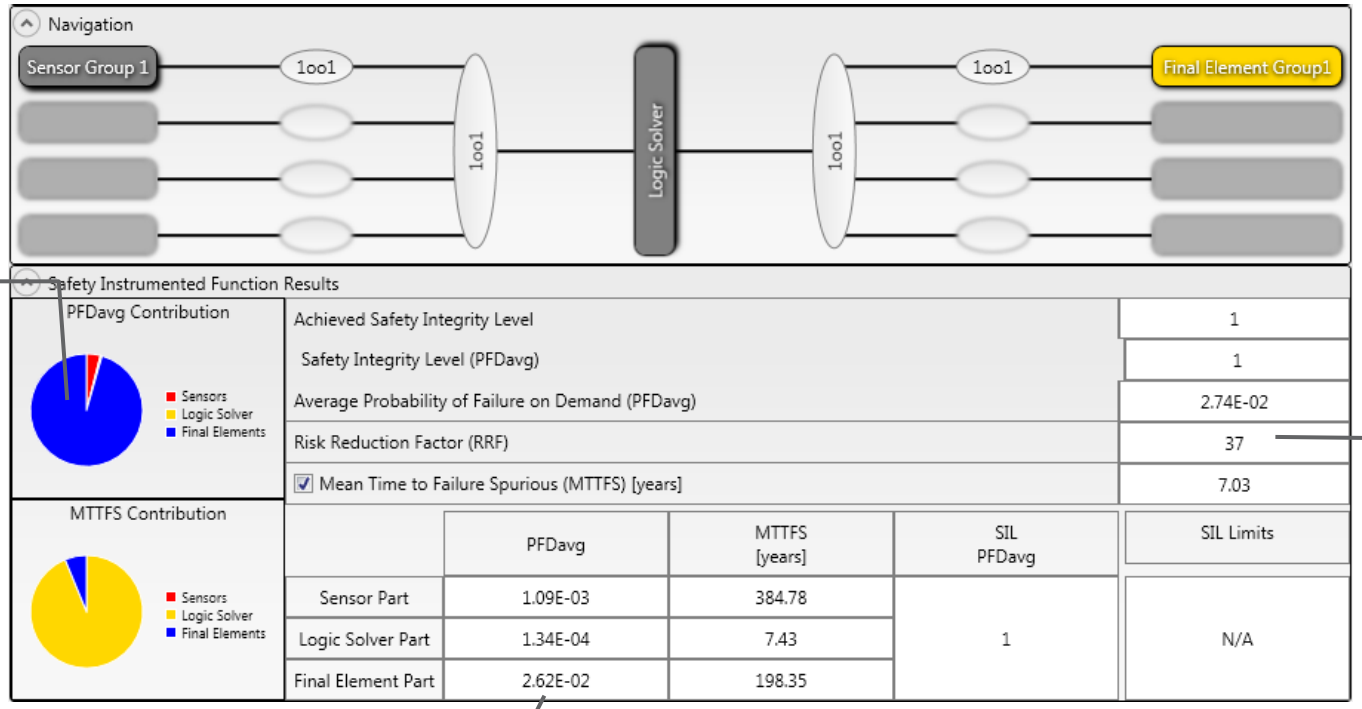


Final Element is only 5% of total

12.1 FITS
9458 years MTTF

Function
"achieves" SIL 2
n**o diagnostics or**
redundancy

Realistic Data



Final Element main **contributor**

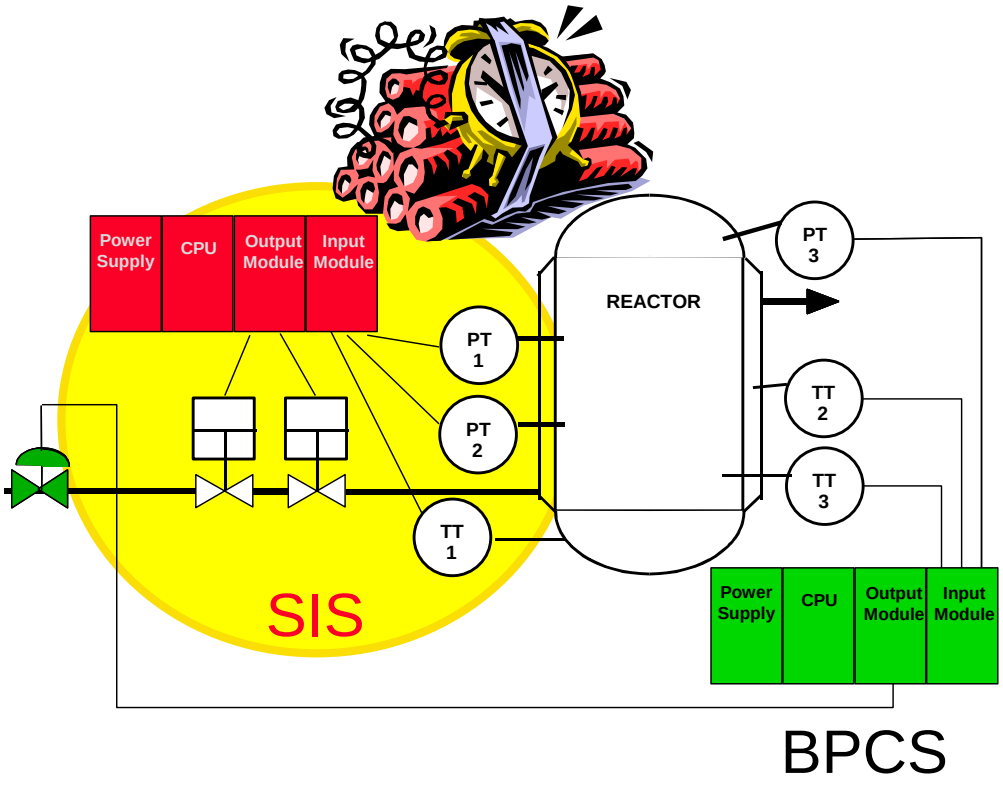
1311 FITS
87 years MTTF

Improve reliability by implementing **diagnostics**

Optimistic = Unsafe

"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."



Legal Responsibility

- Design Engineer – demonstrating reasonable level of expertise and judgment?
- EPC – Providing adequate training and controls?
- OEM – Supplying application appropriate information?
- Asset Owner – Implementing and maintaining an acceptable PSM program?

The Courts Will Decide

2 BP workers indicted on manslaughter counts in Deepwater Horizon oil spill

Published November 15, 2012 / Associated Press

Print
Email
Share
Like 34
Tweet 7
Share

RELATED VIDEO

NEW ORLEANS – Two men who worked for BP during the 2010 oil spill disaster have been charged with manslaughter and a with lying to federal investigators, according to indictments m public Thursday, hours after BP announced it was paying $4. billion in a settlement with the U.S. government over the disa

A federal indictment unsealed in New Orleans claims BP wel leaders Robert Kaluza and Donald Vidrine acted negligently their supervision of key safety tests performed on the Deepw Horizon drilling rig before the explosion killed 11 workers in A 2010. The indictment says Kaluza and Vidrine failed to phone engineers onshore to alert them of problems in the drilling operation.

Buncefield verdict to renew focus on oil safety

The conclusion of a Buncefield prosecution this week comes at a difficult time for the oil industry

Terry Macalister
The Guardian, Sunday 6 June 2010 12.45 EDT

Smoke rises from the fire at the Buncefield fuel depot on December 11, 2005 in Hemel Hemstead Photograph: Peter Macdiarmid/Getty Images

Recent News

EDN NETWORK

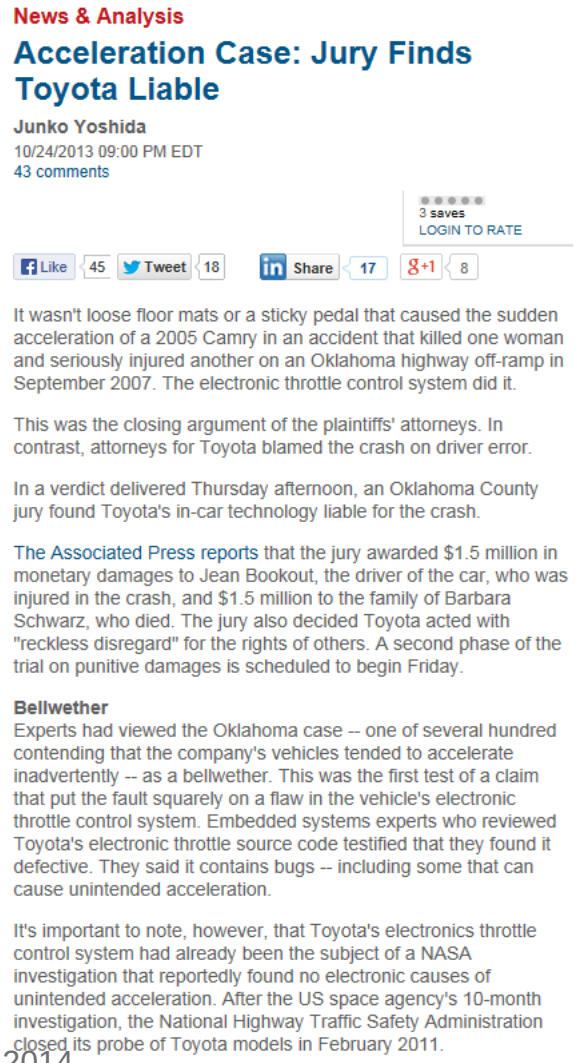
About Us • Subscribe to Newsletters

DESIGN CENTERS ▾ TOOLS & LEARNING ▾ COMMUNITY ▾

Home > Automotive Design Center > How To Article

Toyota's killer firmware: Bad design and its consequences

Michael Dunn - October 28, 2013



News & Analysis

Acceleration Case: Jury Finds Toyota Liable

Junko Yoshida

10/24/2013 09:00 PM EDT

43 comments

3 saves

LOGIN TO RATE

Like 45 Tweet 18 Share 17 +1 8

It wasn't loose floor mats or a sticky pedal that caused the sudden acceleration of a 2005 Camry in an accident that killed one woman and seriously injured another on an Oklahoma highway off-ramp in September 2007. The electronic throttle control system did it.

This was the closing argument of the plaintiffs' attorneys. In contrast, attorneys for Toyota blamed the crash on driver error.

In a verdict delivered Thursday afternoon, an Oklahoma County jury found Toyota's in-car technology liable for the crash.

The Associated Press reports that the jury awarded $1.5 million in monetary damages to Jean Bookout, the driver of the car, who was injured in the crash, and $1.5 million to the family of Barbara Schwarz, who died. The jury also decided Toyota acted with "reckless disregard" for the rights of others. A second phase of the trial on punitive damages is scheduled to begin Friday.

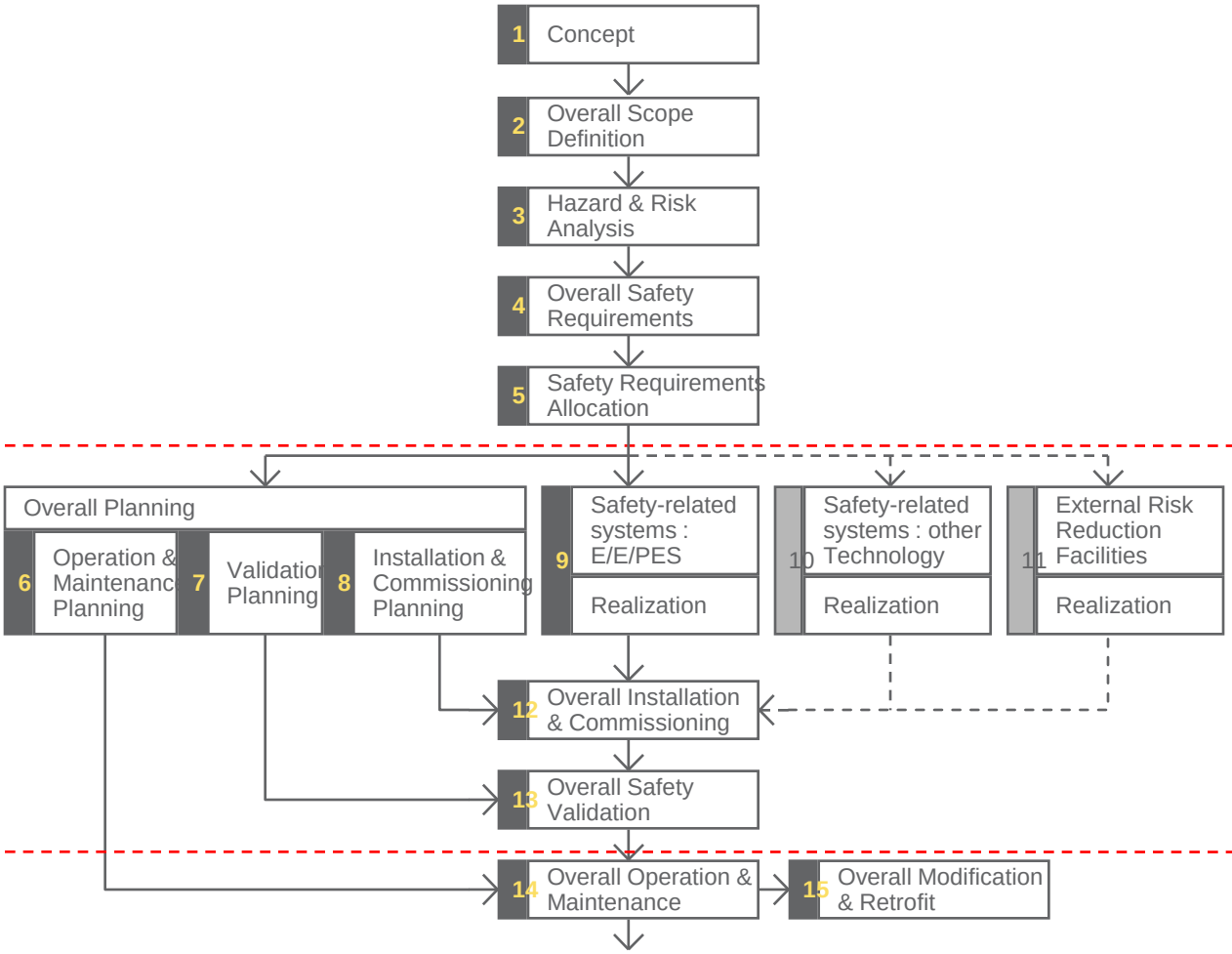
Bellwether

Experts had viewed the Oklahoma case -- one of several hundred contending that the company's vehicles tended to accelerate inadvertently -- as a bellwether. This was the first test of a claim that put the fault squarely on a flaw in the vehicle's electronic throttle control system. Embedded systems experts who reviewed Toyota's electronic throttle source code testified that they found it defective. They said it contains bugs -- including some that can cause unintended acceleration.

It's important to note, however, that Toyota's electronics throttle control system had already been the subject of a NASA investigation that reportedly found no electronic causes of unintended acceleration. After the US space agency's 10-month investigation, the National Highway Traffic Safety Administration closed its probe of Toyota models in February 2011.

Product Certification

Safety Lifecycle – IEC 61508



"ANALYSIS" Phase

"REALIZATION" Phase

"OPERATION" Phase

IEC 61508 – Fundamental Concepts

IEC61508 Safety Life Cycle – detailed engineering process

Systematic Faults – Design Mistakes

Probabilistic performance based system design

Random Failures

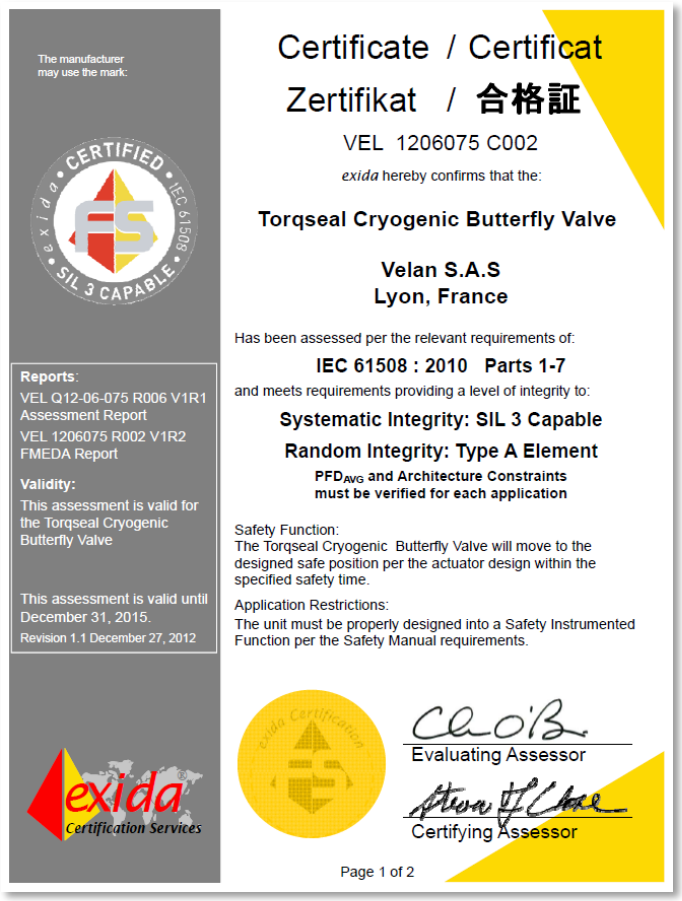
IEC 61508 Certification Milestones

1. Hardware - meet PFD_{AVG} expectations for target SIL via:
   - Low failure rates, fail-safe design
   - High diagnostic coverage
2. Hardware - Meet SFF requirement for target SIL.
3. Software - Meet software process requirements for target SIL, systematic fault avoidance
4. Product - Meet design process requirements for target SIL, systematic fault avoidance
5. Produce Safety Manual for User

What does it mean for product development?

- Need a documented lifecycle for safety
- Need requirements for safety-related functions
- Need a safety-related validation plan
- Need a defined architecture
- Need a qualified set of tools including language compiler fit for the purpose
- Need a coding standard and documented description of other means utilized to qualify set of tools
- Need to follow the coding standard
- Need to verify compliance to coding standard, design requirements and other means

Product Level - IEC 61508 Full Certification



The manufacturer may use the mark:

exida CERTIFIED IEC 61508 SIL 3 CAPABLE

Reports:
VEL Q12-06-075 R006 V1R1 Assessment Report
VEL 1206075 R002 V1R2 FMEDA Report

Validity:
This assessment is valid for the Torqseal Cryogenic Butterfly Valve

This assessment is valid until December 31, 2015.
Revision 1.1 December 27, 2012

exida Certification Services

Certificate / Certificat
Zertifikat / 合格証

VEL 1206075 C002

exida hereby confirms that the:

Torqseal Cryogenic Butterfly Valve

Velan S.A.S
Lyon, France

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Integrity: SIL 3 Capable

Random Integrity: Type A Element

PFD_{AVG} and Architecture Constraints must be verified for each application

Safety Function:
The Torqseal Cryogenic Butterfly Valve will move to the designed safe position per the actuator design within the specified safety time.

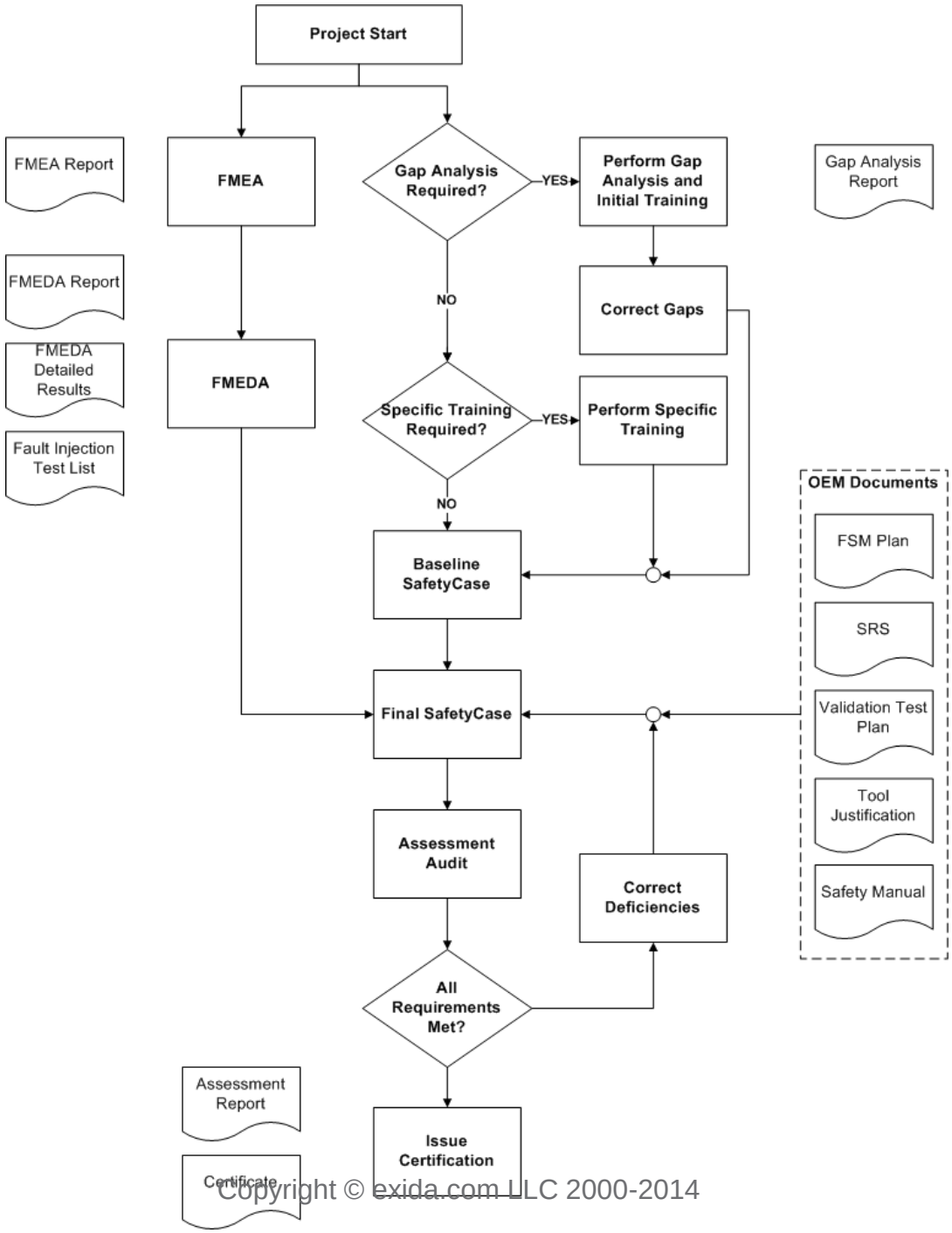
Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Evaluating Assessor

Certifying Assessor

Page 1 of 2

- The end result of the certification process is a certificate listing the SIL level for which a product is qualified and the standards that were used for the certification.
- A good certification assessment will demonstrate high design quality for hardware, software and high manufacturing quality.
- A good certification assessment will check to see that proper end user documentation is provided – “The Safety Manual”

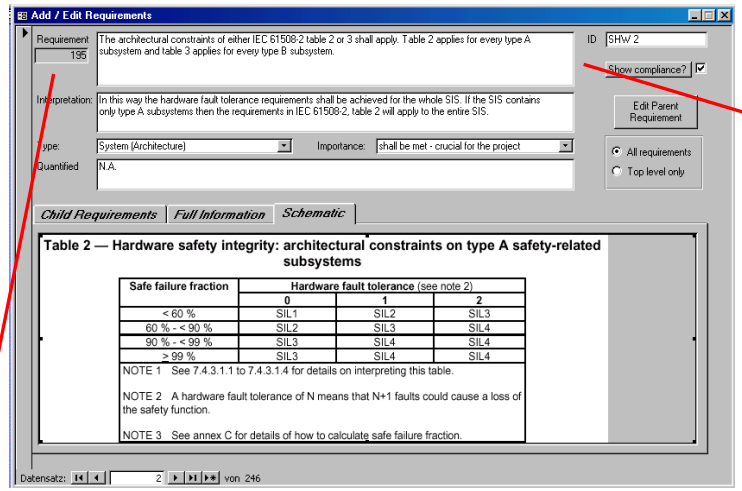


Typical Project Documents

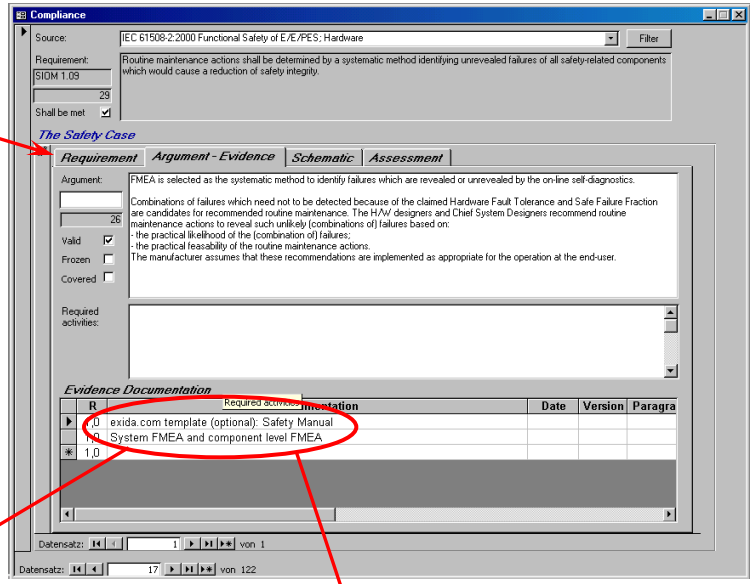
Category	P/R	**Preferred Document**
FSM	1R	List of procedures
FSM	2P	Functional Safety Management Procedure
DSN	3P	Development Process
SRS	4R	Safety Requirements Specification
DSN	5R	Requirements review MOM/record
DSN	6R	FSM Plan
DSN	7R	List of applicable agency standards
DSN	8R	Design Review MOM/record
DSN	9R	Gate Review and signoffs record
FSP	10R	Verification Plan
FSP	11R	Verification Results
DSN	12R	FMEDA
INT	13R	Integration test plan
INT	14R	Intergration test results
FSP	15R	Validation Test Plan
FSP	16R	Validation Test Plan Review MOM/record
FSP	17R	Validation test results
OM	18R	IOM manual
OM	19R	Safety Manual
OM	20R	Safety Manual review minutes/signoff
FSM	21P	Part Qualification Procedure
FSM	22P	Manufacturer qualification procedure
FSM	23P	Quality Management System Documentation Change Procedure
FSM	24P	Control of Design Documents
FSM	25P	Modification Procedure/Engineering Change Procedure
FSM	26P	Design Change Impact analysis
FSM	27P	Non-Conformance Reporting procedure
FSM	28P	Corrective Action Procedure
FSM	29P	Preventive Action Procedure
FSM	30P	Internal Audit Procedure
FSP	31P	Meeting minutes / Action Item list Tracking procedure
FSM	32R	Job descriptions /Competency Levels
FSM	33P	Training Procedure
FSM	34R	Training Record
FSM	35R	Training Matrix
FSM	36R	IEC 61508 training record
FSP	37P	Test equipment calibration procedure
FSM	38P	Customer notification procedure for safety releted products
FSM	39R	ISO Cert
FSP	40R	Other applicable certs

exida Safety Case Database

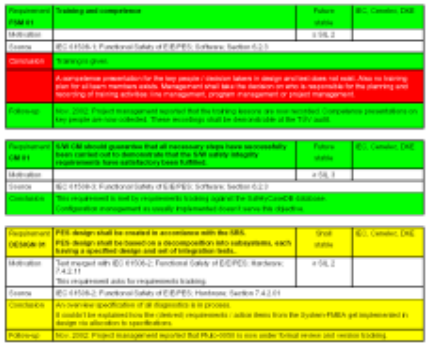
Requirements

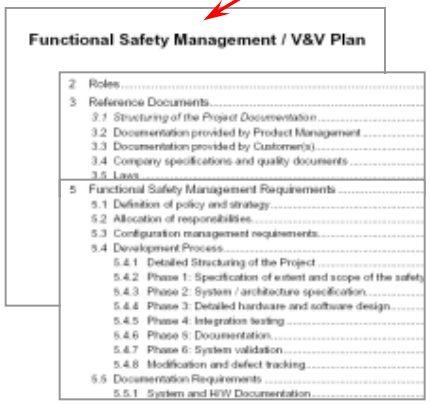


Arguments – Assessment



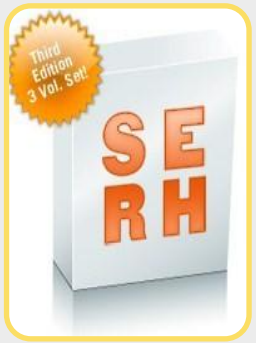
Audit Lists





Evidence

Main Product / Service Categories



Consulting

Process Safety (IEC 61511)

Control System Security (ISA S99)

Product Certification

Functional Safety (IEC 61508)

Functional Security

Security Lifecycle

Cyber-Security (ISASecure)

Training

Process Safety

Control System Security

Onsite

Offsite

Web

Engineering Tools

exSILentia

(PHAX HAZOP

SILAlarm

SIL Selection

LOPA

SRS

SIL Verification

Proof Tests)

Safety Case

FMEDA

SCA

Reference Materials

Databases

Tutorials

Textbooks

Reference Books

Market Studies

Professional Certification

CFSE

CFSP

Control System Security Expert (CSSE)

www.cfse.org

excellence in dependable automation