exida

exida Academy

Functional Safety Management (FSM) for Managers…

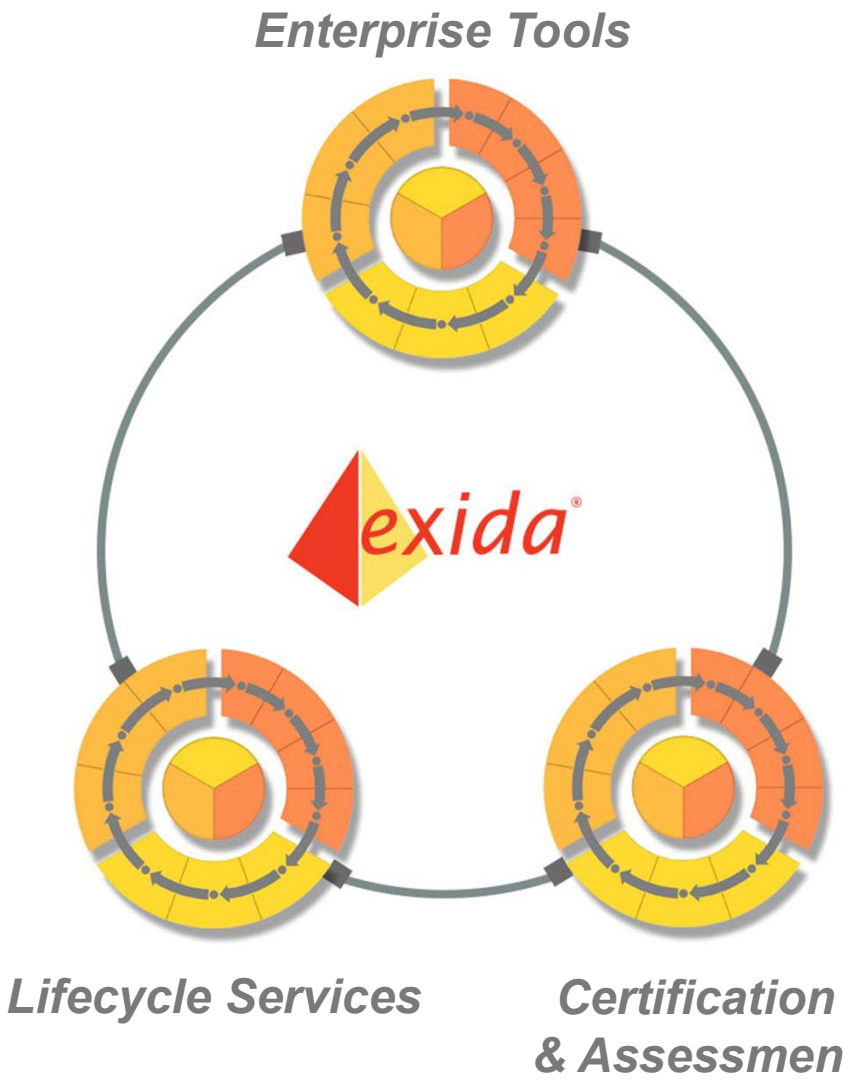
Instrumentation Experts Club
Automation India Week 2018

Sudhir Pai

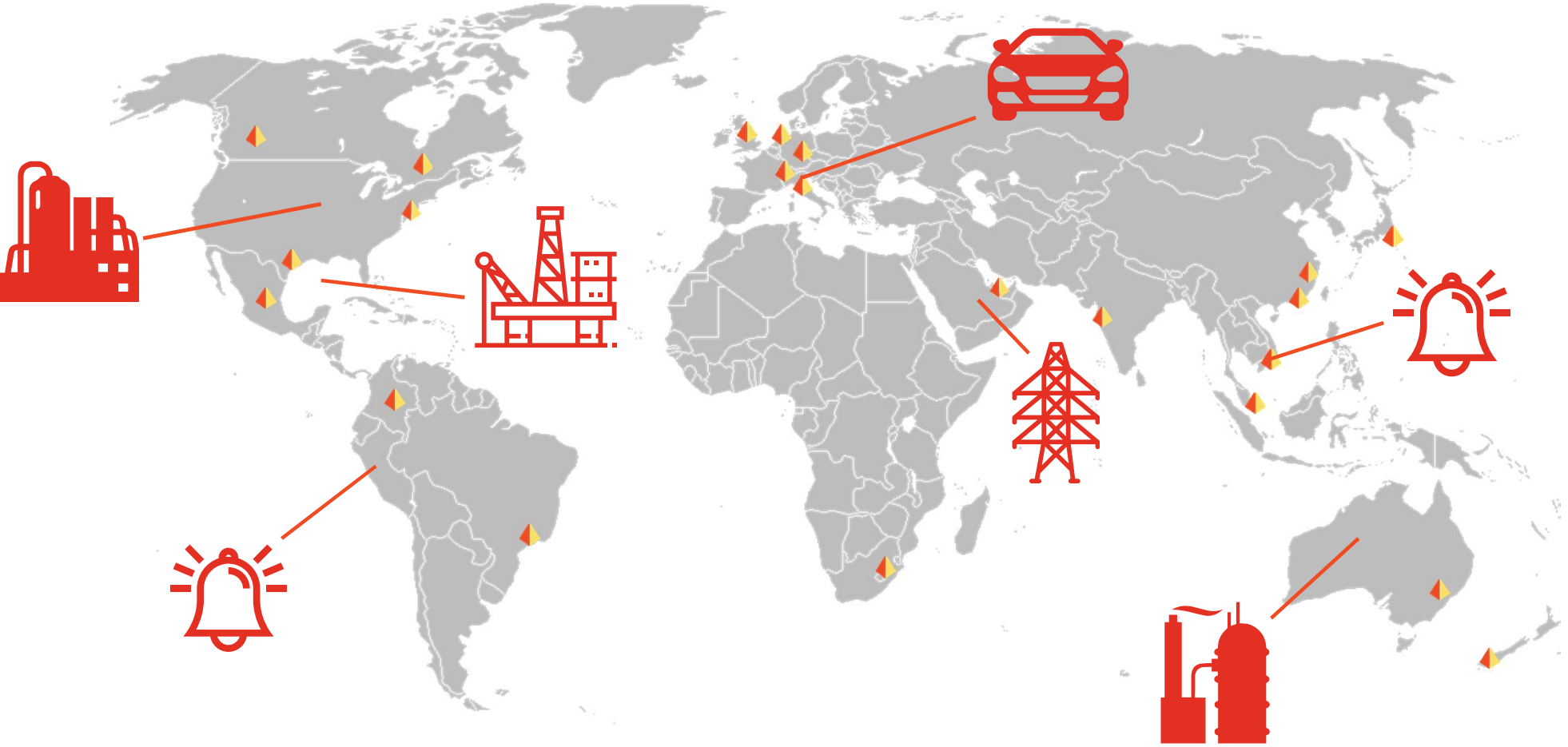
exida… A Customer Focused Company

exida helps customers achieve safe and reliable solutions through:

- Powerful lifecycle tools that efficiently deliver technically correct results.
- Thorough certification and assessment schemes that achieve compliance through a pragmatic approach.
- Comprehensive lifecycle services that deploy experts to solve your toughest problems.

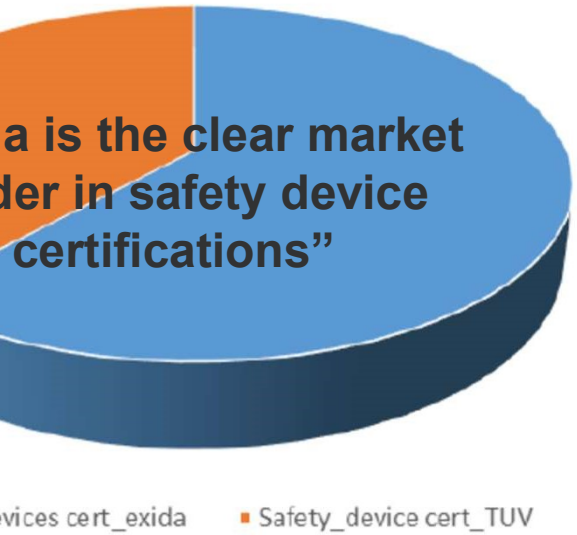


exida… Global Customer Focus



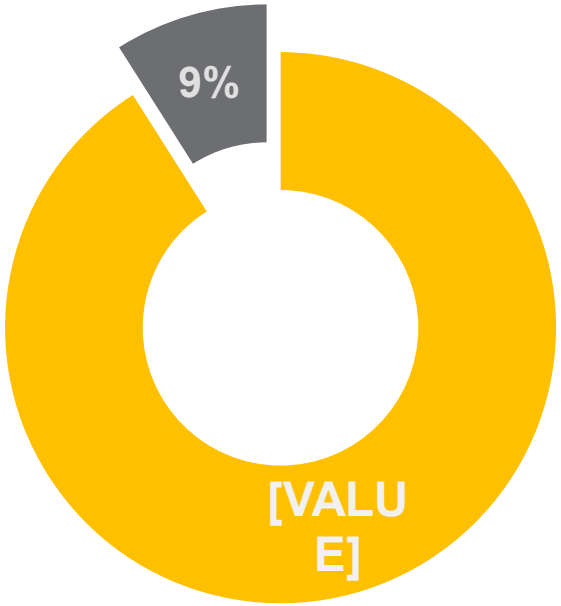
How do We Measure Success?

Market Share



ource: ARC Advisory Group, Nov. 2015

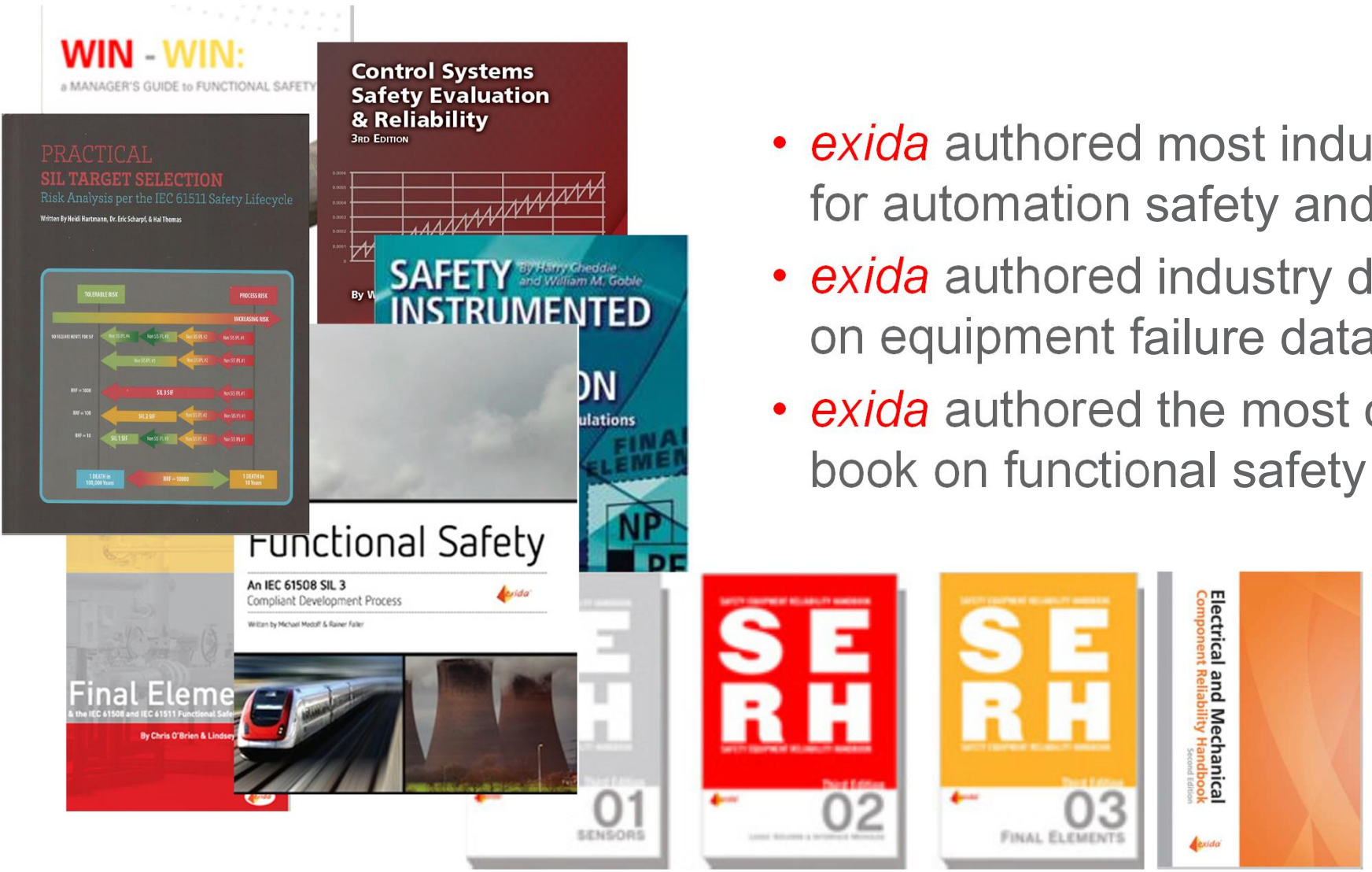
Employee Ownership



Key Statistics

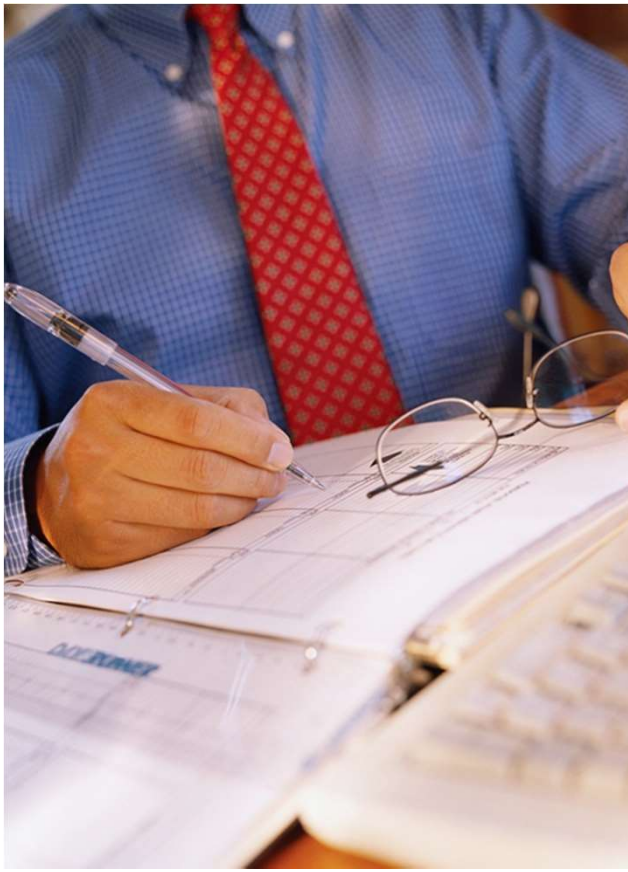
- Over 100 Global Exper
- Over 1000 Certification and Assessment Proje
- Over 500,000 SIFs Modeled

Reference Materials



- *exida* authored most industry referenc for automation safety and reliability
- *exida* authored industry data handbool on equipment failure data
- *exida* authored the most comprehensiv book on functional safety in the marke

FUNCTIONAL SAFETY MANAGEMENT (FSM) FOR MANAGERS



Introduction

Recent accidents have revealed deficiencies in Process Safety Manageme

- Poor safety culture
- Lack of mechanical integrity
- Poor maintenance & training

Management of Functional Safety is key to:

- Avoid and prevent systematic faults occurring
- Maintaining process safety
- Ensuring the integrity of SIS implementation

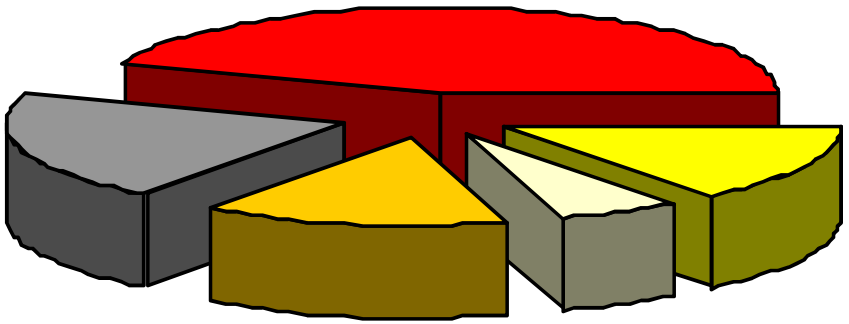
BP Texas City Refinery Explosion 2005

Industrial Accidents

nt	Country	Year	Fatalities	Injuries	Financial Impact
Transocean pwater	USA	2010	11		Overall estimate >50 Billion; BP may have to pay the entire $42 Billion cleanup bill, BP h estimated maximum possible fines could $20 Billion if gross negligence is demonstrated has paid out $7 Billion in claims, further claims estimated at 15 Billion
Bruno Pipeline losion	USA	2010	8	Many	Pacific Gas & Electric Co. has agreed to pay $70 Million to aid city of San Bruno's recov
s Alaska line Spill	USA	2010			$45 Million in lost production and about $13 Million in state revenue
ay Oil Refinery	Venezuela	2012	48	151	Property Damage estimated at $330 Million
t Fertilizer pany	USA	2013	15	260	Widespread community damage. Losses from the explosion are estimated to be around $230 million + federal disaster assistance is estimated to exceed $16 million
of Tanjin	China	2015	173	797	Cost to businesses estimated at $9 billion; Various courts in China handed jail sentence 49 government officials and company staff with a death sentence to Company chairman
etrol's Litvinov	Czech Republic	2015 2018	6		Over 10 months of production loss. Cost of repair stands at almost €152 Million and lost business profit at over €244 Million. Another incident with 6 deaths happened in 2018
ky oil refinery	USA	2018		36	Refinery isn't expected to reopen for at least 18 months. The fire and explosion resulted $27 million in damages and another $53 million in unspecified costs related to the incide

Industrial Accident Primary Causes

HSE study of accident causes involving control systems:



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

FOLLOWING BEST PRACTICE

FUNDAMENTAL FUNCTIONAL SAFETY REQUIREMENTS

What is Risk?

Risk is a measure of the ***LIKELIHOOD*** and ***CONSEQUENCE*** of an adverse effect *(i.e., How often can it happen and what will be the effects if it does?)*

- Risk receptors:
  - Personnel
  - Environment
  - Financial
  - Equipment/Property Damage
  - Business Interruption
  - Business Liability
  - Company Image
  - Lost Market Share

What is Functional Safety?

Functional Safety" is a set of rules and methods fo
the specification, design, and operation of safety
functions which are part of **Automatic Protection
Systems**.

Following Best Practice

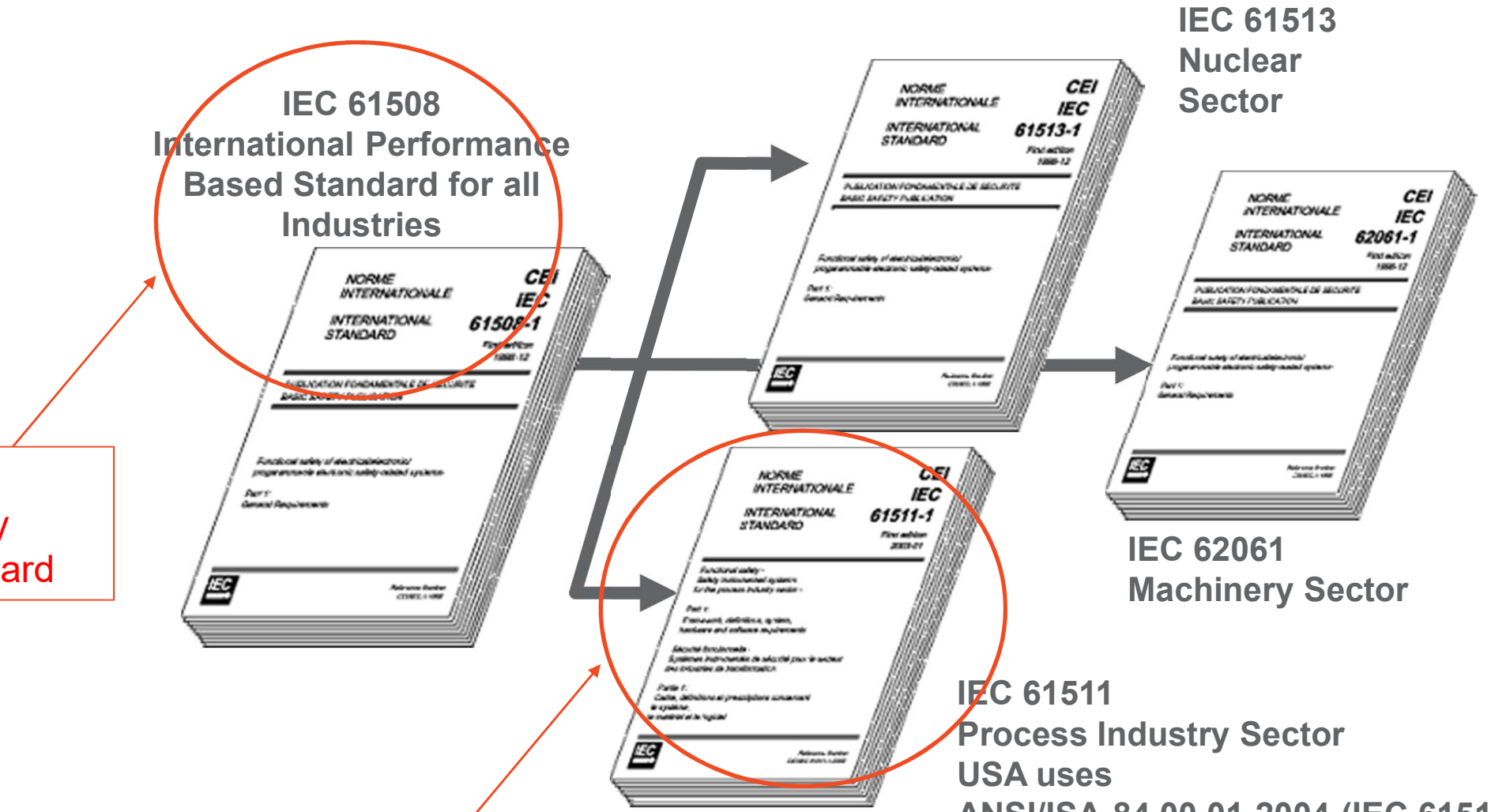
COMAH/OSHA CFR1910 requires operators of hazardous processes to follow best practice

IEC61511/S-84 is recognized as being RAGAGEP (Recognized and Generally Accepted Good Engineering Practice)

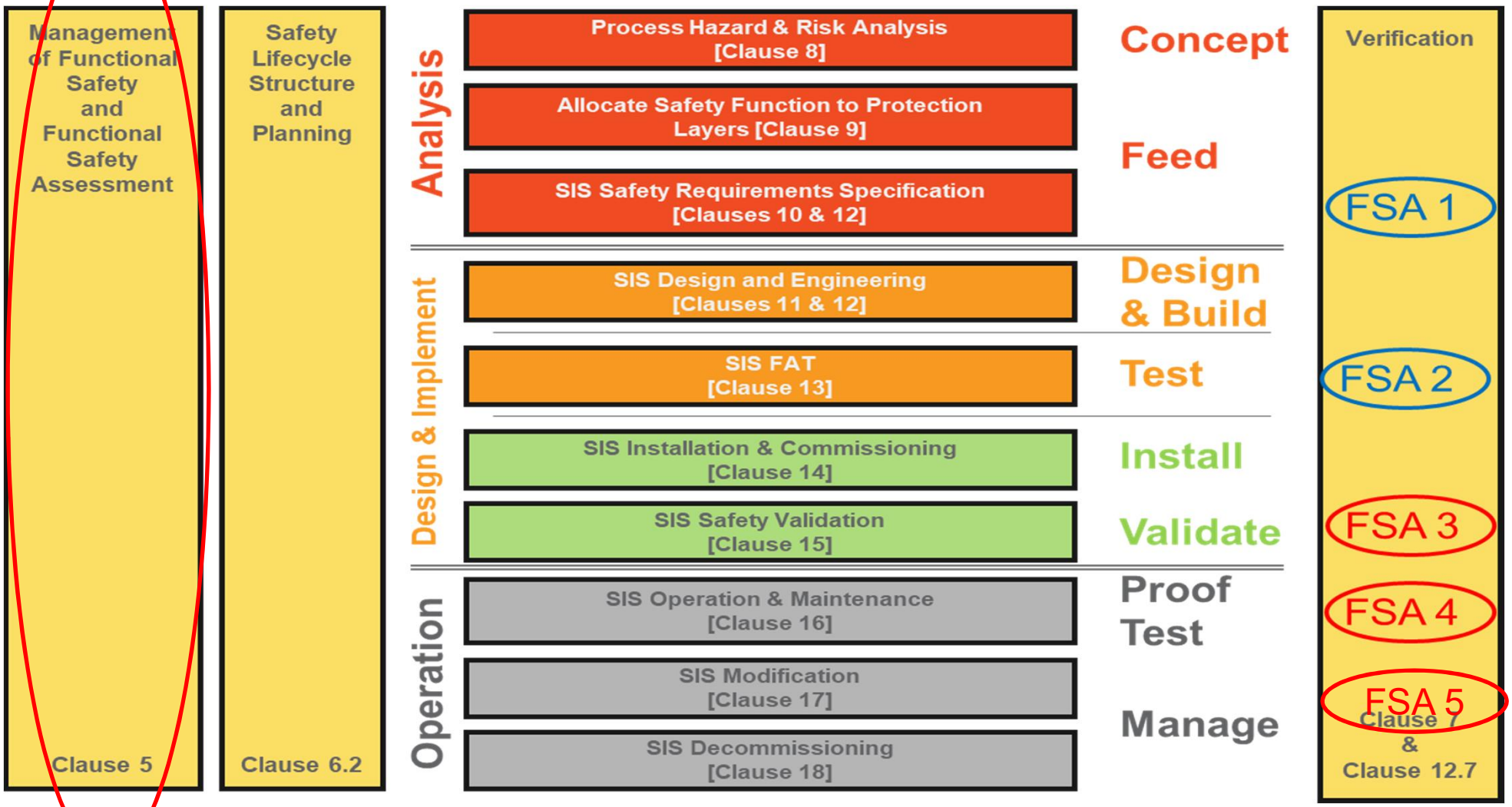
IEC61511 is a performance-based standard built around a Safety Lifecycle (SLC) to

- Ensure the problems of the past are not repeated
- Provide a consistent approach to identifying and mitigating risk
- Provide a means of achieving optimum design that balances risk reduction with performance
- Provide a means to consistently measure performance

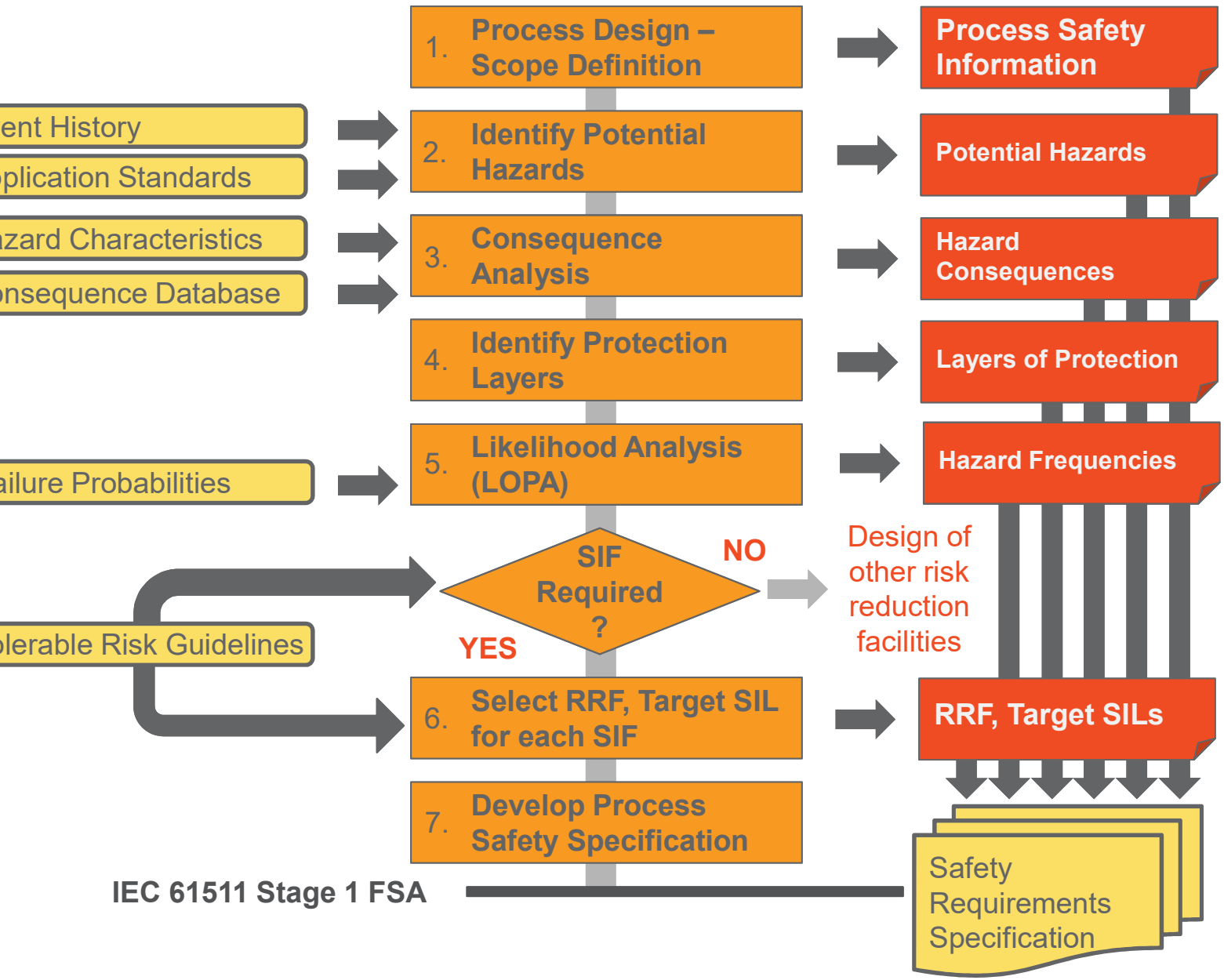
Current Functional Safety Standards



IEC 61511 Safety Lifecycle



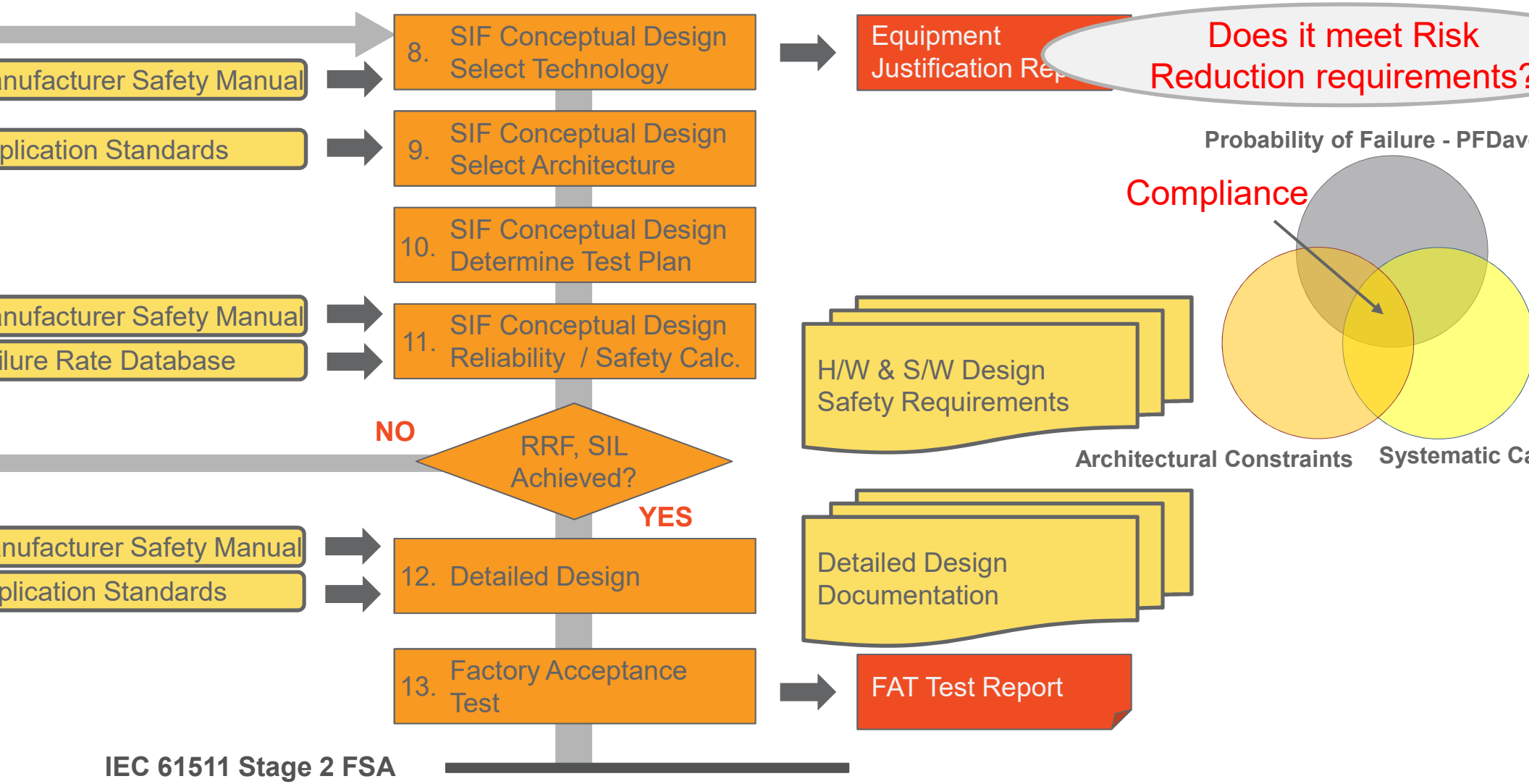
“Analysis” Information Flow



What is the Tolerable Risk?

Requirements from clause 10.3.2

“Realization” Information Flow



Manufacturer's Certificates

Manufacturer's IEC 61508 functional safety certificates should provide key pieces of information

1. Systematic Capability
2. Failure Rate Data
3. Architecture Constraint Type
4. Statement of Compliance
5. Accreditation Body

exida

ANSI Accredited Program

Certificate / Certificat

Zertifikat / 合格証

HON 1002038 C001

exida hereby confirms that the:

SmartLine ST 800 HART Pressure Transmitter

Honeywell International Inc.
Honeywell Field Products
Fort Washington, PA 19034 - USA

has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity for:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2 @ HFT=0; SIL 3 @ HFT = 1; Route 2H

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

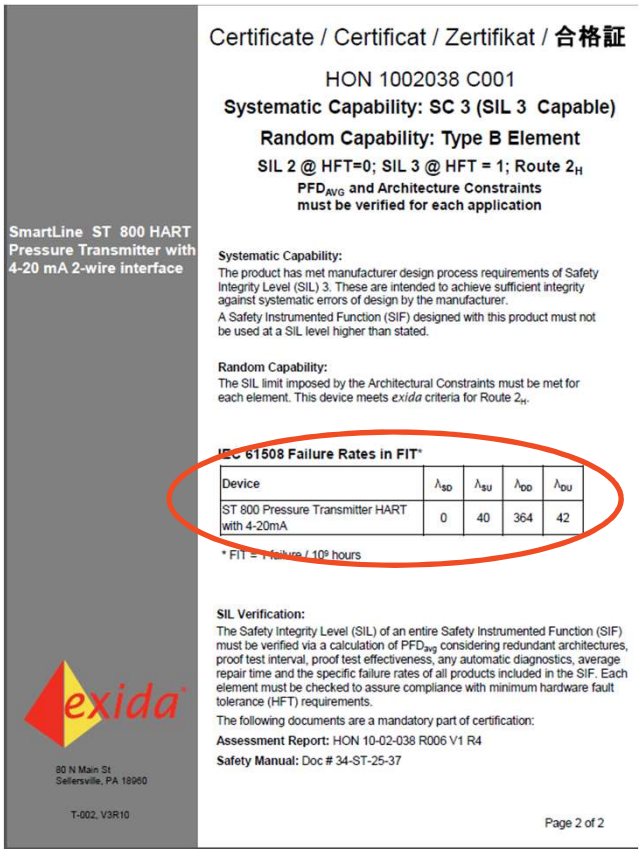
Safety Function:
The ST 800 HART Pressure Transmitter with 4-20 mA 2-wire interface will measure pressure within the stated safety accuracy.

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



SmartLine ST 800 HART Pressure Transmitter with 4-20 mA 2-wire interface

exida

80 N Main St
Sellersville, PA 18960

T-002, V3R10

Certificate / Certificat / Zertifikat / 合格証

HON 1002038 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2 @ HFT=0; SIL 3 @ HFT = 1; Route 2_H

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

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

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

IEC 61508 Failure Rates in FIT*

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
ST 800 Pressure Transmitter HART with 4-20mA	0	40	364	42

* FIT = 1 failure / 10^9 hours

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

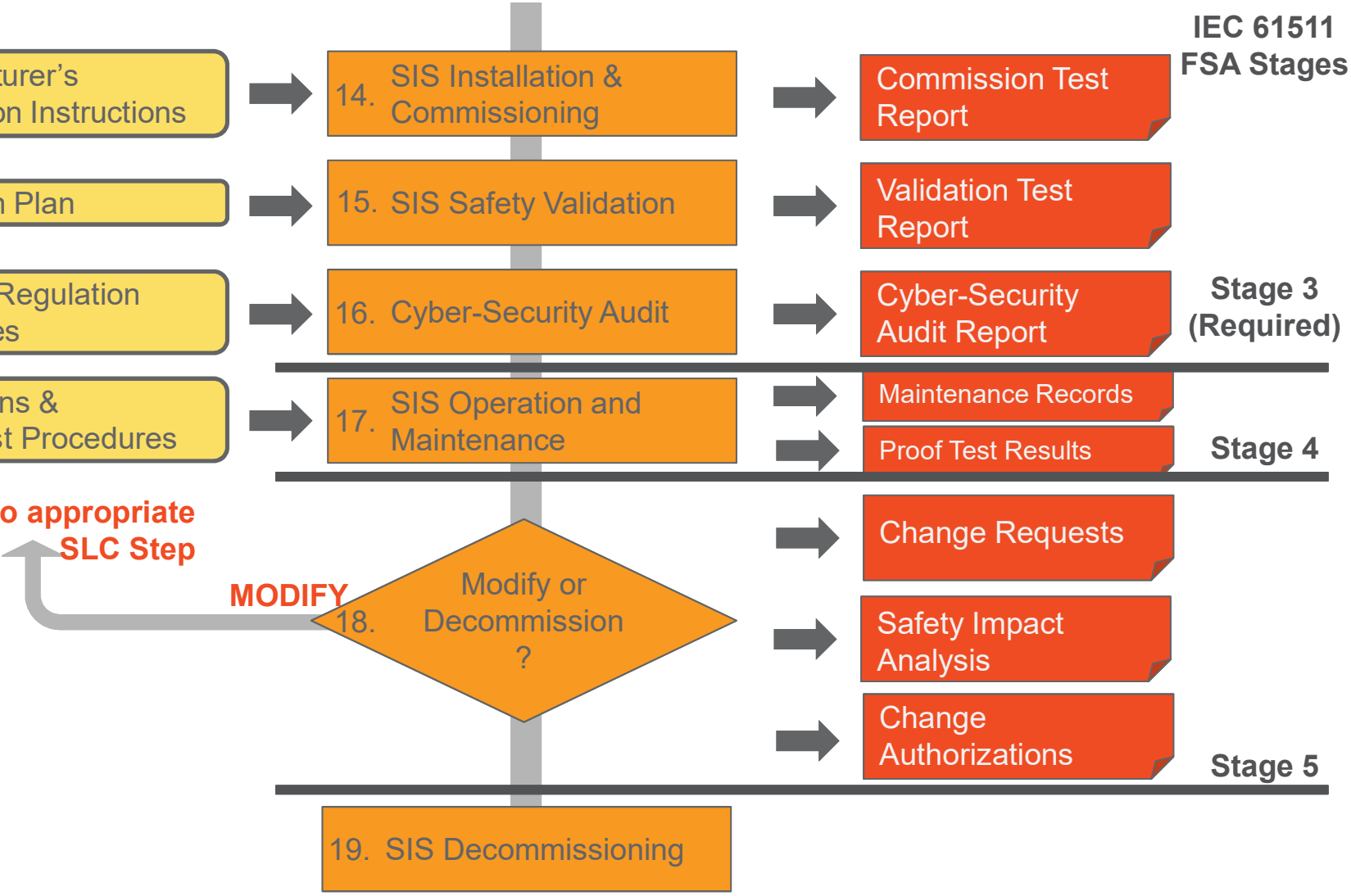
The following documents are a mandatory part of certification:

Assessment Report: HON 10-02-038 R006 V1 R4

Safety Manual: Doc # 34-ST-25-37

Page 2 of 2

“Operation” Phases Information Flow



- O&M planning
- Inspection & proof test planning / execution
- Equipment rep
- *End of life refurbishment and replaceme*
- **Failure event data collectio**
- Functional safe process auditin
- Modification approval and validation

IEC 61511 Now Includes Cyber Requirements for the SIS

The new version of IEC 61511 emphasizes the need for Cyber Assessment (Clause 8.2.4):

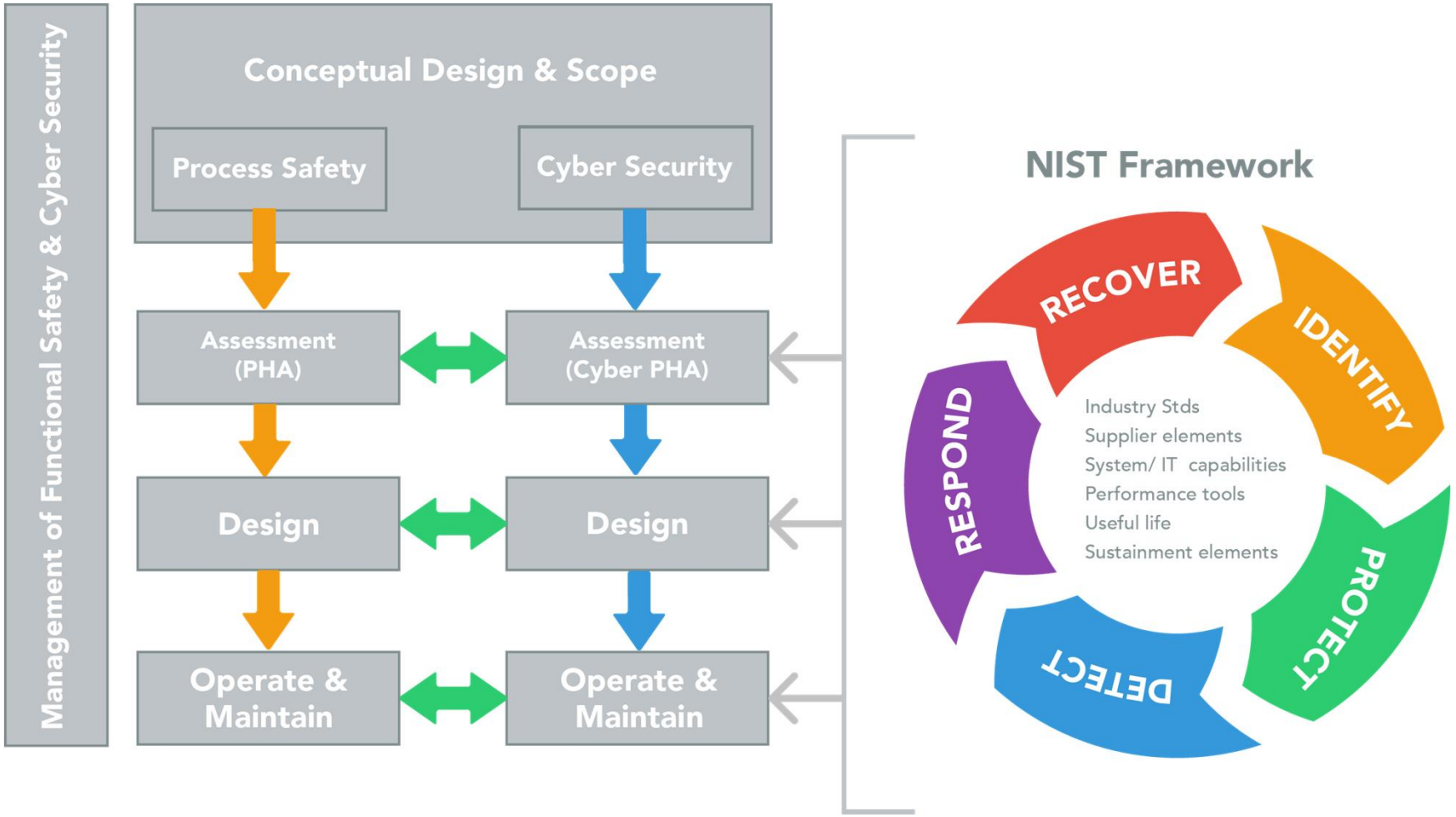
- Security Risk Assessments including a description of identified threats, the likelihood and potential consequences of a security event.
- Determination of requirements for additional risk reduction.
- Description of measures taken to reduce or remove threats.

Emphasizes the responsibility of the owner / operating company of the of the facility (Clause 8.2.4, Note 2).

Consequences of incomplete CSMS

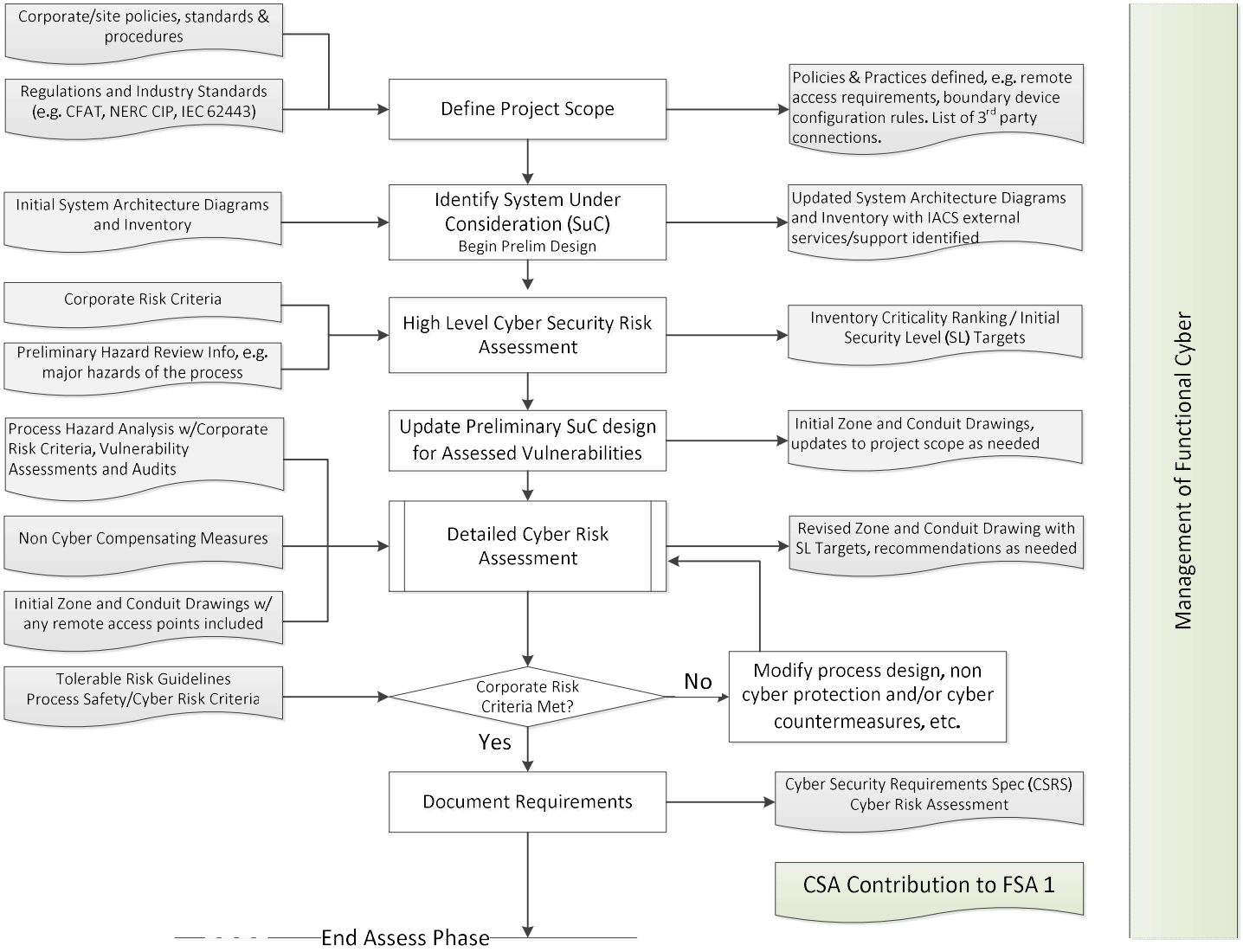
- ranian Nuclear Facility - STUXNET – direct failure of a process equipment
- Yahoo – 1 billion user accounts compromised
- LinkedIn – 160 million accounts compromised
- Target, Sony, Home Depot – retailers compromised
- Lockheed – F035 fighter jet program
- German Steel Mill – “spear phishing” success leads to attack on blast furnace control
- Ukrainian Power Grid – “KillDisk” virus attack bricked switching station in 2015, second attack a year later
- National Laboratories – disrupted communications
- Pentagon Files – compromised file content not released

Safety/Cybersecurity Integration



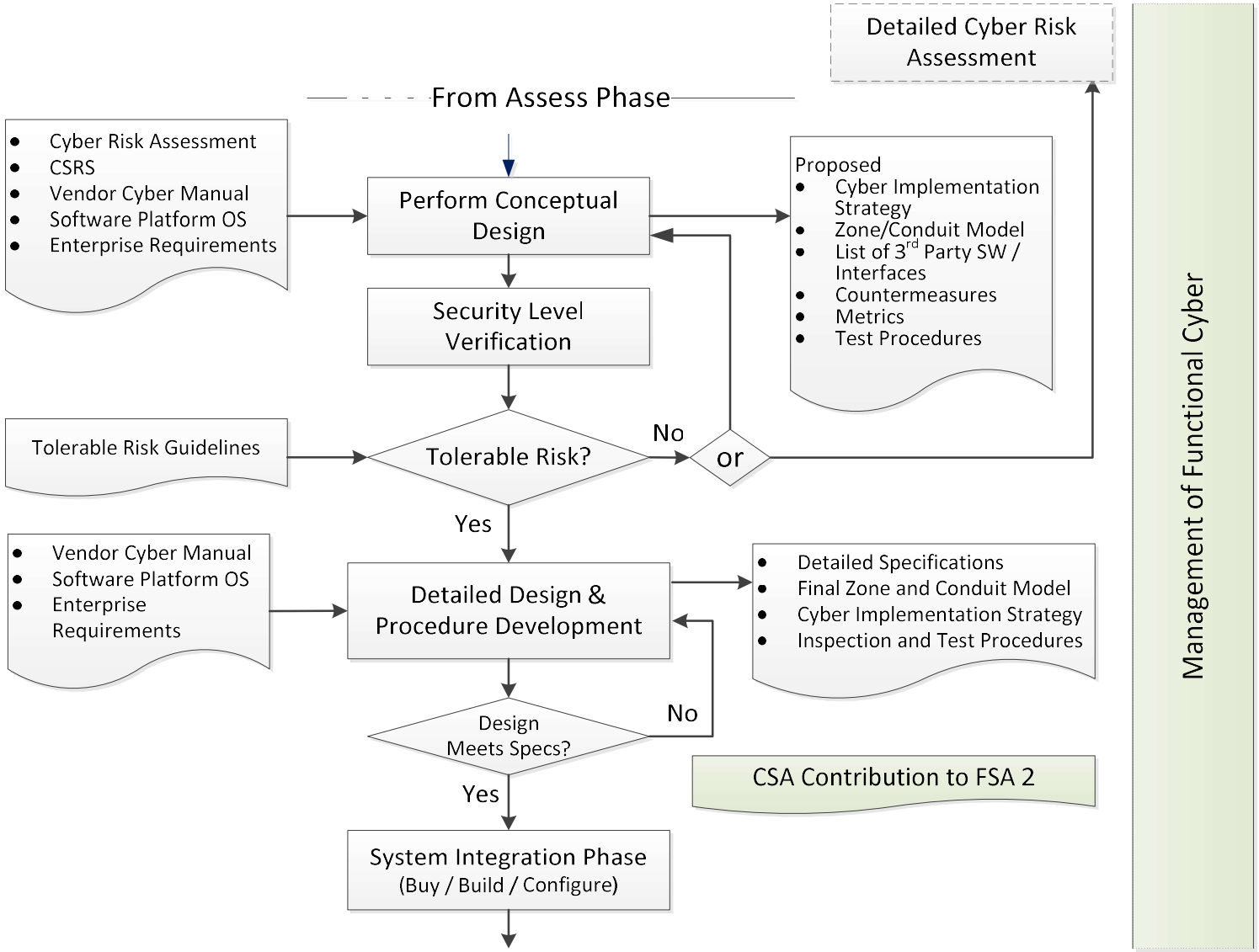
Cybersecurity Assessment Phase

Excerpted from ISA TR84.00.09



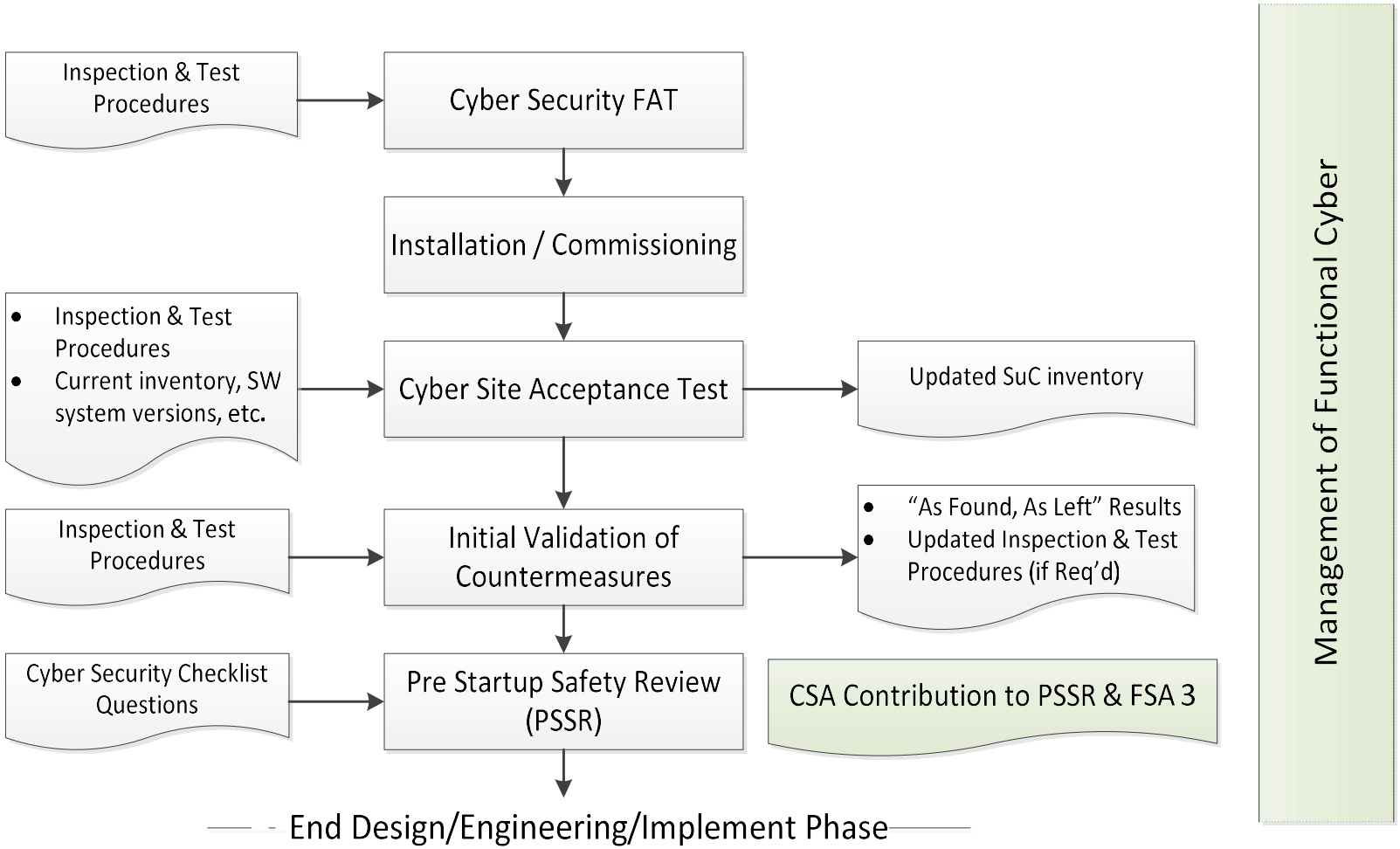
Design & Implement(1)

Excerpted from ISA TR84.00.09

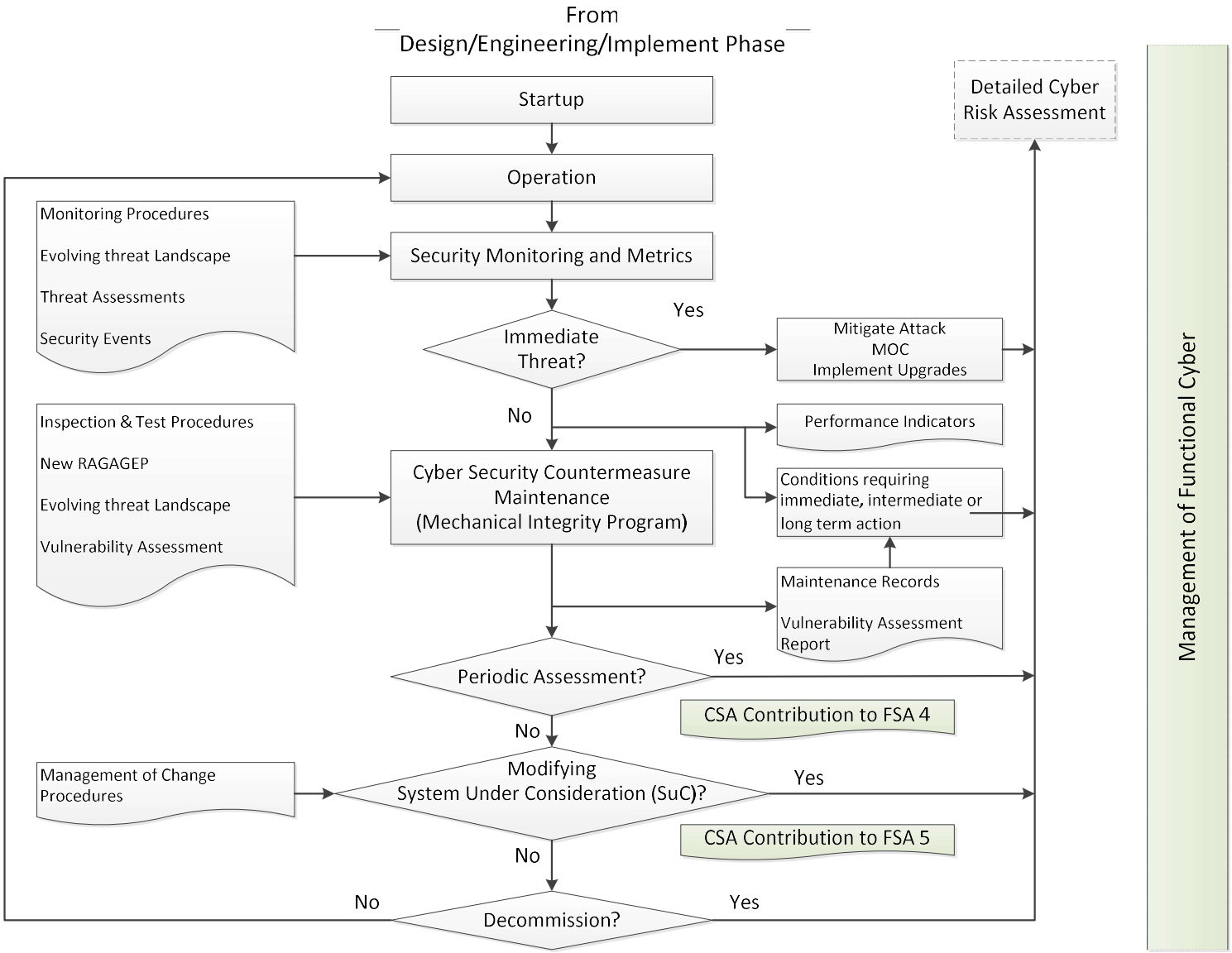


Design & Implement(2)

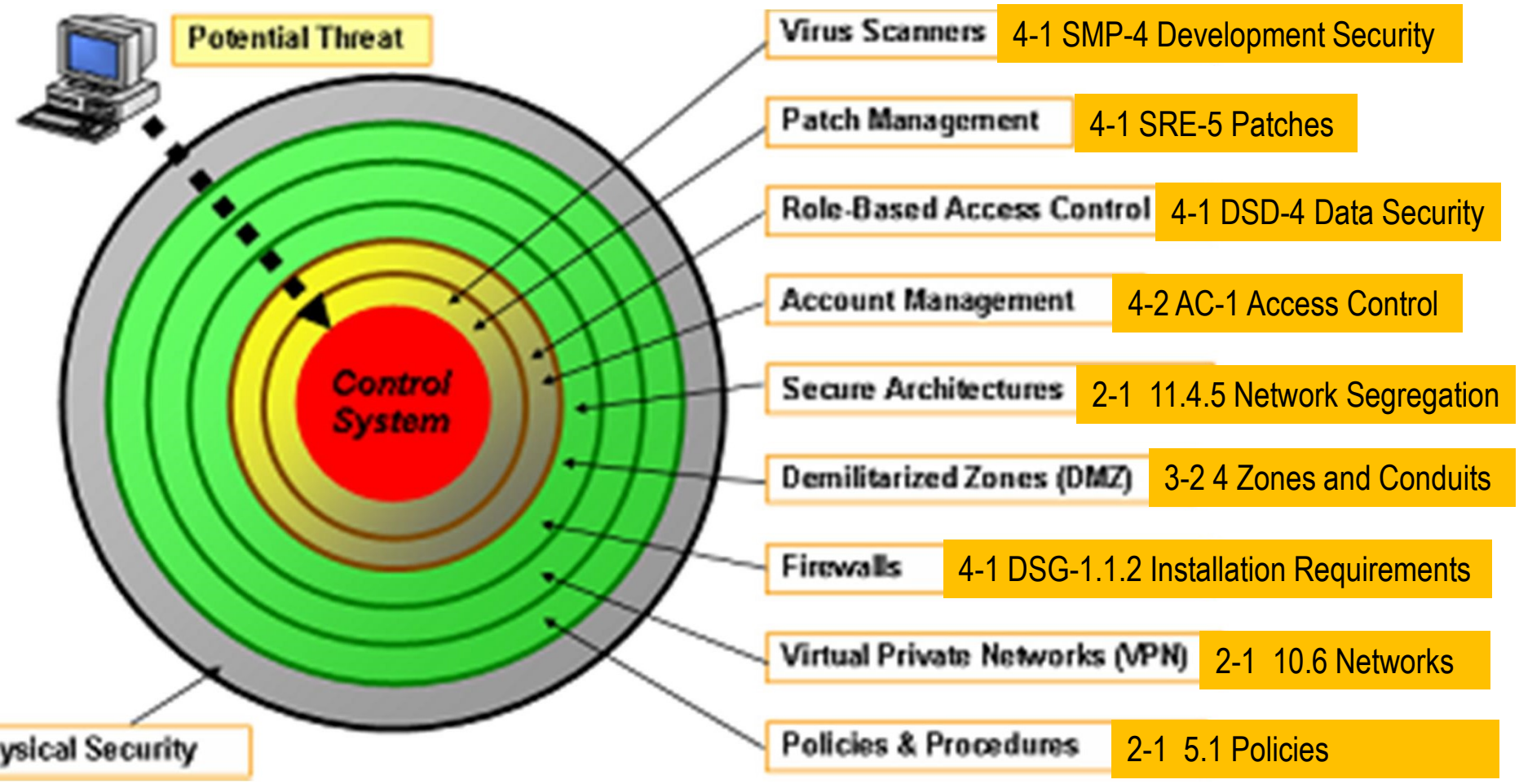
Excerpted from ISA TR84.00.09



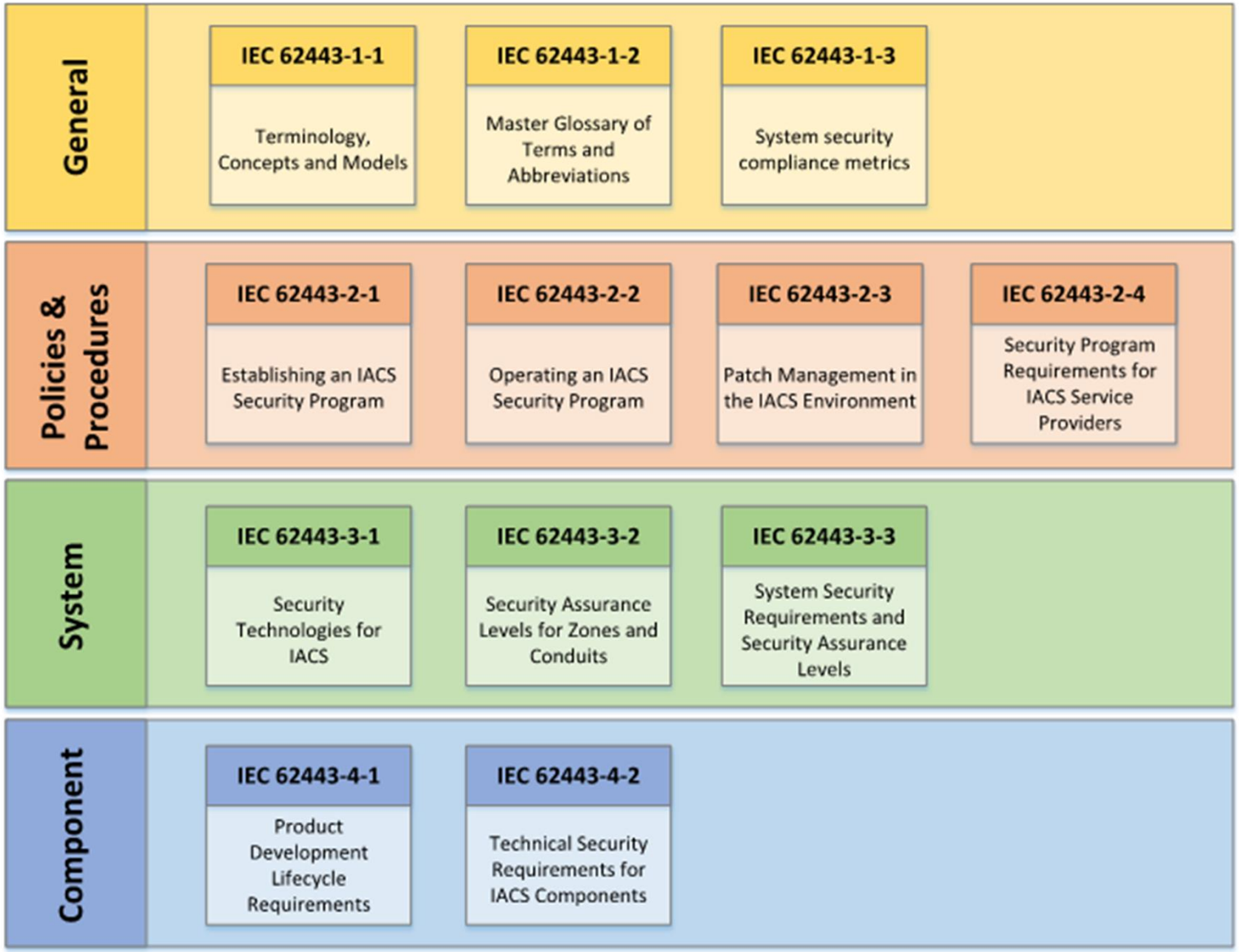
Operate & Maintain Excerpted from ISA TR84.00.09



Defense In Depth



IEC 62443 family of cyber standards



Functional Safety Management

Functional Safety Management is about

- **People**
- **Procedures**
- **Paperwork**

The 3 Ps!

Apply the same redundancy to these as for equipment to ensure systematic errors are:

- Rarely created
- Easily identified
- Promptly corrected

Functional Safety Management

Governs the entire Safety Lifecycle

Allocating lifecycle responsibilities

Specifying the activities of those with responsibilities (develop procedures)

Ensuring people are competent

Manage the risk of systematic faults to get an acceptable level of overall risk

So what does this mean for me as manager?

What Are Your Responsibilities?

Managers need to be able to demonstrate competence according to IEC61511:2016, in terms of having:

- knowledge of the legal and regulatory functional safety requirements
- understanding of the potential consequence of an event
- adequate management and leadership skills appropriate to their role in the SIS safety lifecycle activities

Managers need to read incident reports and to ensure leading and lagging indicators are being used to monitor SIS performance and risk

Managers need to understand the ramifications of cost-cutting, especially when it comes to process safety and/or mechanical integrity

Managers need to be trained in understanding what Process and Functiona Safety is all about – ignorance is no excuse

Functional Safety Management Objectives

Leverage quality programs already in place.

Specify management and technical activities during the Safety Lifecycle to achieve and maintain Functional Safety

Specify responsibilities of people, departments and organizations

How?

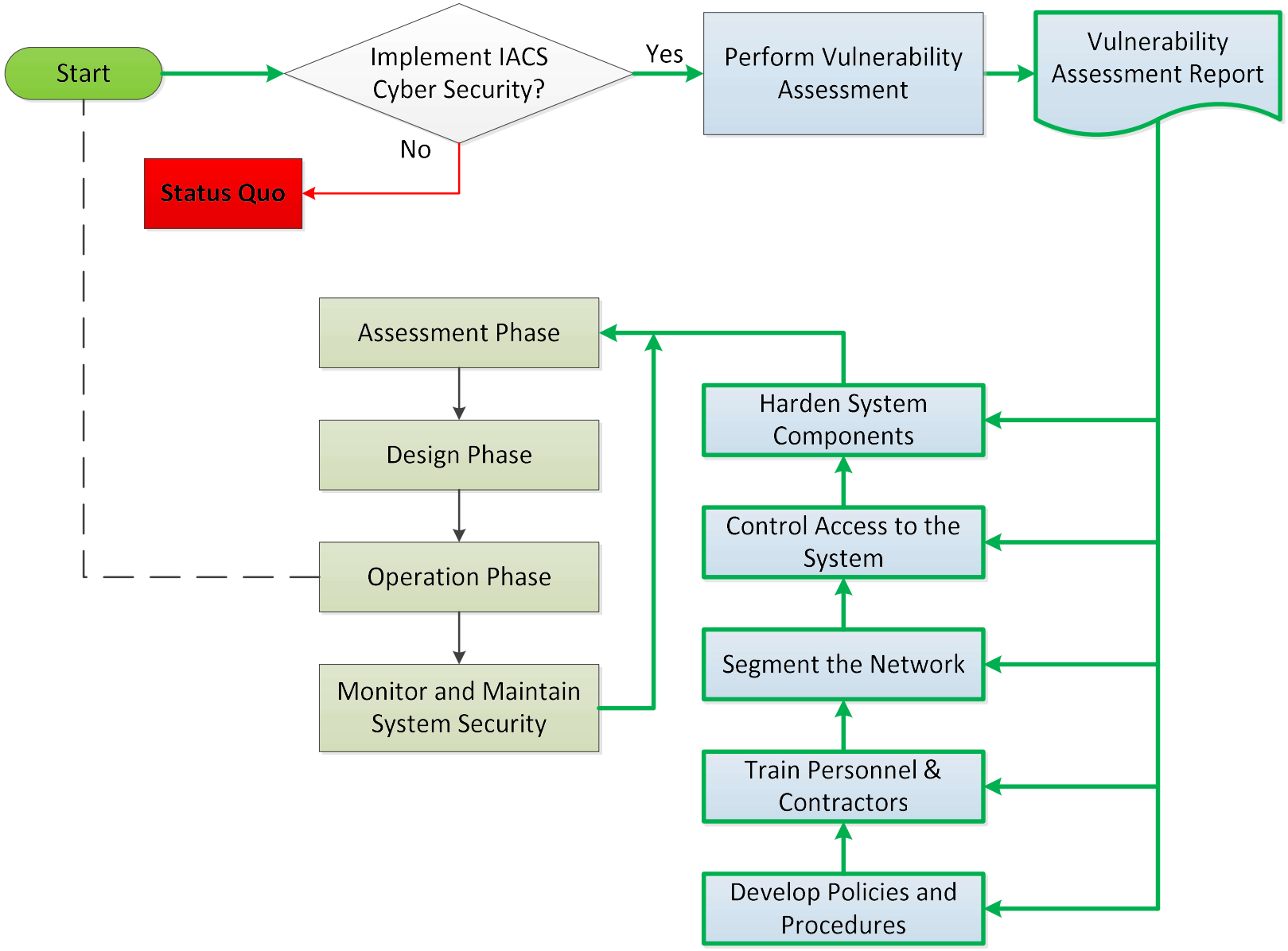
- Appoint one or more people to lead FS activity
- Extend an existing monitored quality system
- Develop FS-related procedures
- Plan, execute, audit and improve (conduct Functional Safety Audits)

How To Deal With Legacy Systems?

Legacy Systems

- Making sure Corporate Risk Guidelines exist
- Need to start by reconsidering PHA and LOPA; PHAs have to be revisited every 5 years under OSHA
- PHA needs to consider all hazards (especially if there have been incidents and/or near misses during the 5 year period)
- LOPA needs to consider highest consequence hazards and existing IPLS to asses further risk reduction
- Legacy systems can be made to be compliant by replacing non-certified with certified devices at end of useful life
- Mechanical integrity program needs to consider useful life, beyond which replacement/refurbishment is required
- Reverse engineering legacy systems to create an SRS is possible, if good documentation and test/maintenance records exist; if not then time consuming an costly

Entering Lifecycle as Brownfield Site

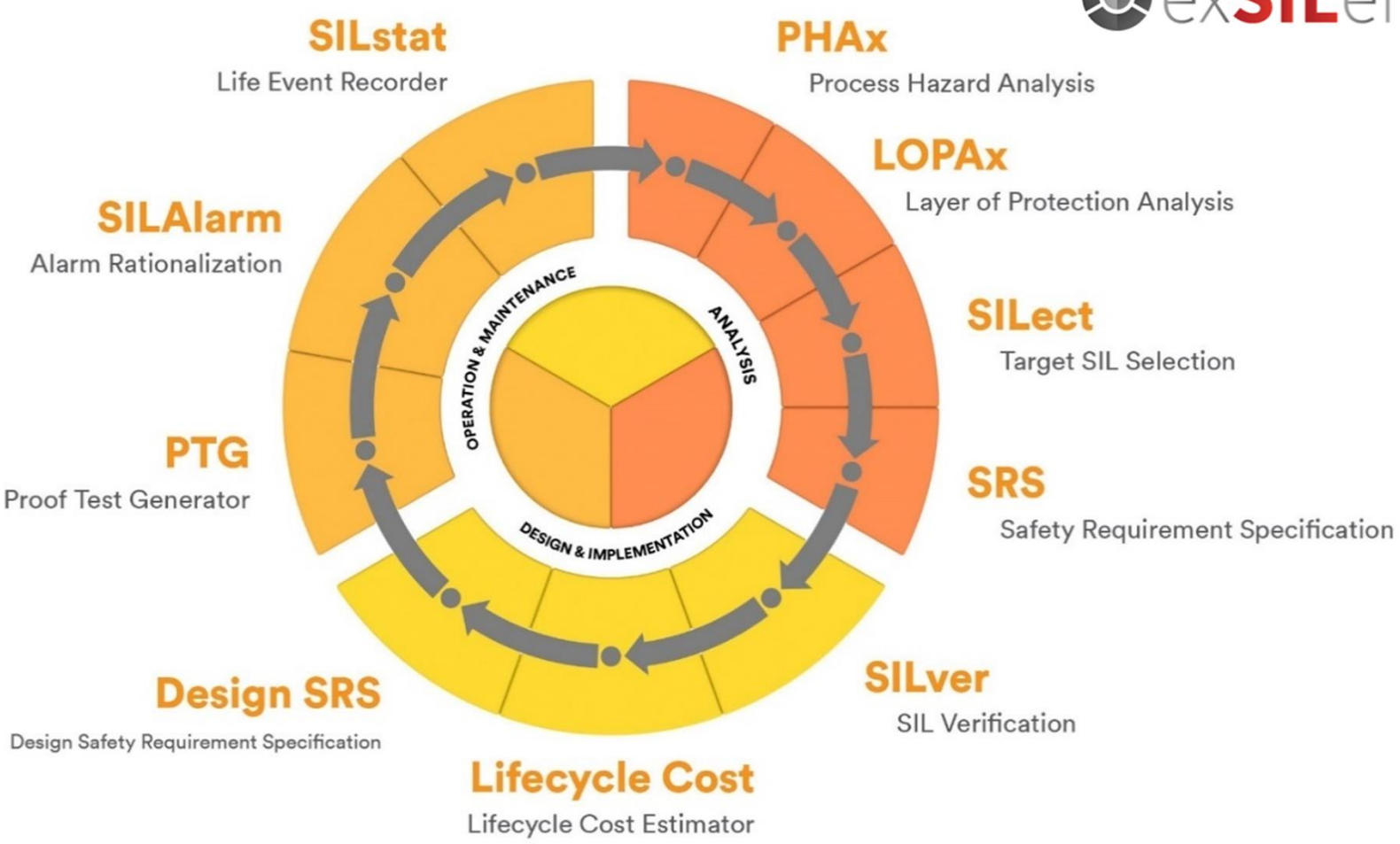


Summary

- IEC61511 defines that a Functional Safety Management System be put in place to manage the Safety Lifecycle activities
- Having the right Safety Culture is imperative; management has to understa and support FSM or it won't work
- People, Procedures and Processes must be covered by any FSM system t ensure protection against systematic errors
- Functional Safety Assessments and Functional Safety Audits are required t ensure that procedures and processes are being followed correctly to help safeguard against systematic errors
- Competency is a key part and maintaining a matrix is a good approach to plan training

Intelligent Lifecycle Integration

exSILentia CYBE



If You Think Safety's Expensive

Then Try an Accident!

Questions?

Sudhir Pai
Mob.: 9930250104
email: spai@exida.com