Lifecycle of Safety Instrumented Systems

Nicholas P Sands, CAP, P.E.
Senior Technology Fellow
DuPont

Nicholas P. Sands – Automation Engineer – Water and Protection R22B

32 YEARS WITH DUPONT

- Currently working on Tyvek Line 8 in Luxembourg
- Currently living in Dallas, Texas
- Worked at several sites and businesses

CREDENTIALS

- BS ChE from Virginia Tech
- Certified Automation Professional
- Professional Engineer
- International Society of Automation (ISA) Fellow
- Process Automation Hall of Fame

DUPONT ROLES

- Senior Manufacturing Technology Fellow
- Tyvek Process Control Technology Leader
- Global Alarm Management Leader
- A&PC CoC Competency Workstream Leader
- PSM Competency Core Team
- PS&A Strategist
- SIS Technology Team
- AM Technology Team

DUPONT BEST STANDARDS & PRACTICES

- Safety Interlock Training
- S27A Interlock Bypassing and Alarm Suppression
- Automation Competency Assessment
- Alarm Management
- Safety Requirements Specification
- Functional Safety Assessment
- Safety Alarm Design
- Human Machine Interface
- SIS Audit Protocol
- SIS Device SIL Evaluation Process
- SIS Projects
- SIS Performance Evaluation

ISA/IEC STANDARDS+

- Co-editor *Guide to the Automation Body of Knowledge* (ed3)
- ISA VP of Professional development (2009-2011)
- ISA VP of Standards and Practices (2015-2016)
- Co-Chair of ISA18 on AM (2003-2022)
- Co-Director of ISA18 on AM, lead editor for ANSI/ISA-18.2
- Co-Director of ISA84 on SIS
- Co-Director of ISA101 on HMI
- Secretary of IEC62682 committee on AM, lead editor
- Member of others: MT61511, ISA105, ISA108…

Agenda

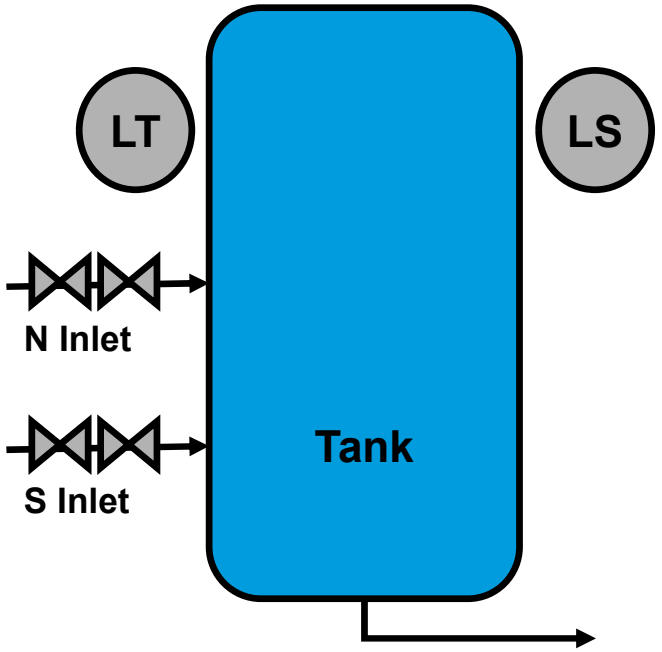
- Safety Moment
- SIF Standards and History
- SIS Safety Lifecycle Stages
- Discussion

Disclaimer:

- This is a high-level overview of the SIS lifecycle for discussion and not a comprehensive guide. There are more details in the standard. Only competent resources should execute SIS tasks.

Safety Moment – Failed Periodic Proof Test

- A SIF failed a periodic proof test. The test procedure was modified and the SIF re-tested and failed to function properly.
- The safety logic was modified and the SIF re-tested and functioned properly.
- Investigation showed several revisions marked on the test procedure, including bypassing of another SIF and a change to the type of test.
- Investigation of past tests showed that similar revisions had been marked, but the procedure was not updated, and the issue not previously investigated.
- The investigation concluded the logic had not been installed prior to this test.



SIS Standards and History

10/11/2022

Abbreviations

BPCS - Basic Process Control System

- A part of the control system (DCS, PLC) that does not include SIFs

ESD – Emergency Shutdown System

- A manually activated shutdown
- A type of IPL

IPL - Independent Protection Layer

- This training is limited to instrumented IPLs
- An alarm or interlock evaluated as protection against a hazardous consequence

PFD – Probability of Failure on Demand

- Calculation of the average failure rate of a safety instrumented function

SIF - Safety Instrumented Function

- Safety interlock
- A type of IPL

SIL - Safety Integrity Level

- A classification of SIF availability

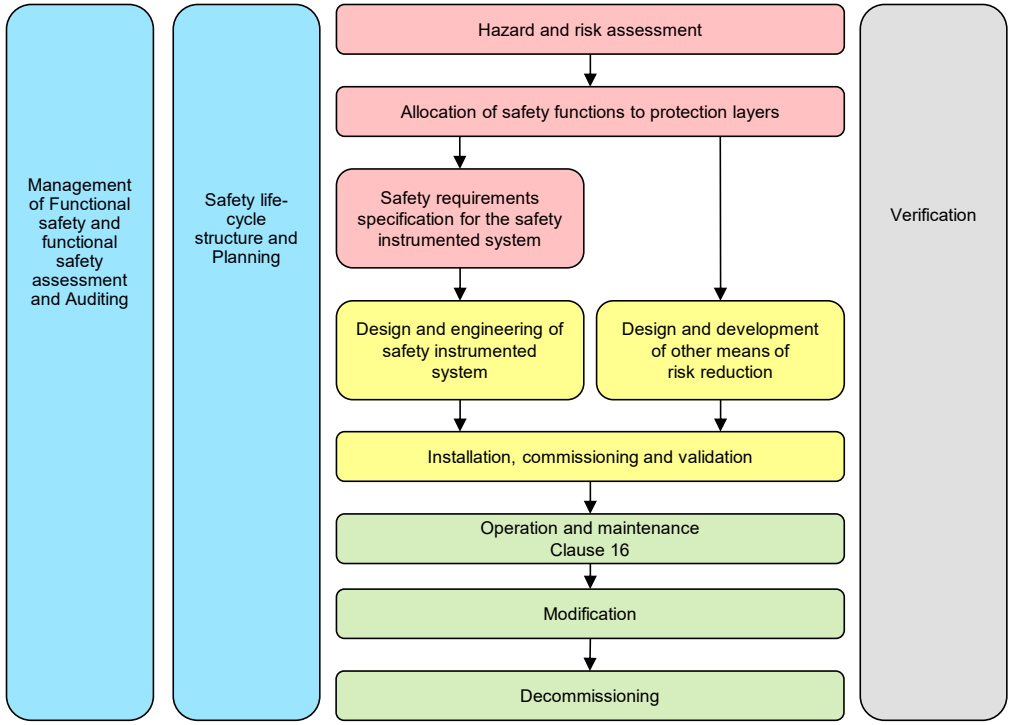
SIS - Safety Instrumented System

- A system that includes SIFs

Safety Instrumented System Scope

Safety Instrumented Systems (SIS) lifecycle activities:

- Planning
- Specification
- Design
- Validation
- Operation
- Maintenance
- Management of Change (MOC)



SIS and PSM Standards

PLC introduced
- Evaluated for safety

Relays for SIS

ISA-84-1996
First SIS standard

IEC61511
SIS standard

IEC61511 ed2
SIS standard

…	1970			1984	1990	1996		2003	2010		2018	…

PHA

OSHA PSM

LOPA

CCPS

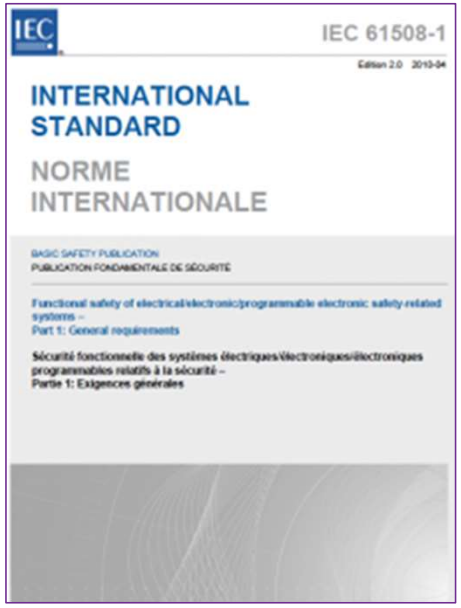
BP Texas City

Bhopal

SIS Standards

IEC61508

- Umbrella for safety standards
- Standard for device certification
- Ed2 - 2010



IEC61511

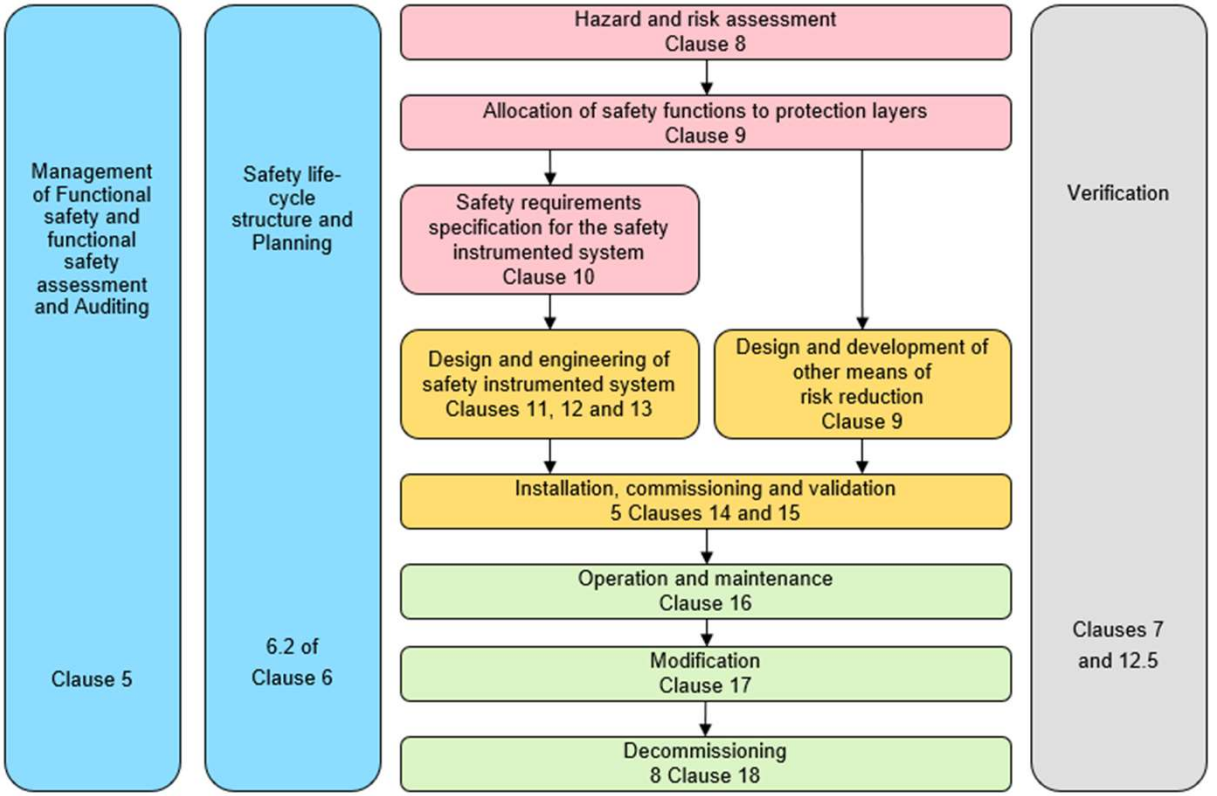
- SIS standard for process industry
- Ed2 - 2018

SIS Safety Lifecycle

10/11/2022

Safety Instrumented System Lifecycle

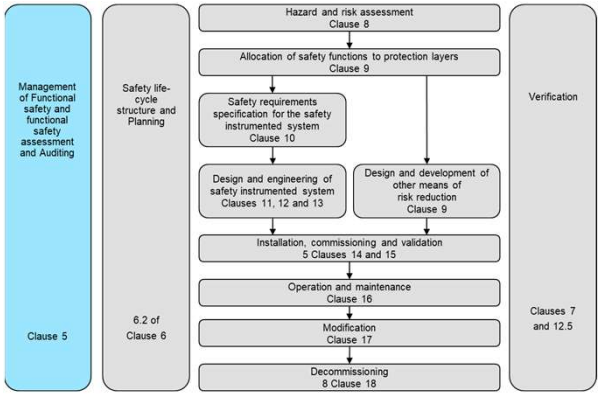
- Requirements are grouped.
- Stages are between the groupings.
- The lifecycle is used to organize the activities
- This is helpful for:
  - Standards
  - Work processes
  - Roles
  - Training
  - Alignment to projects



Management, Assessment and Audit

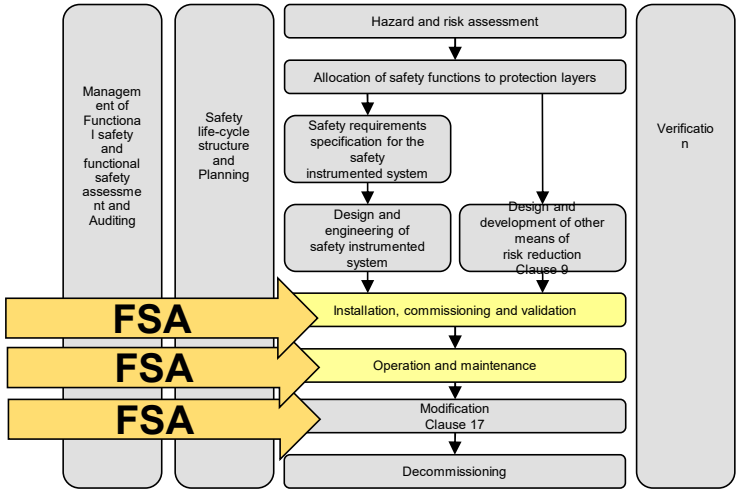
Key Requirements include:

- The policy and strategy for achieving functional safety shall be identified together with the methods for evaluating their achievement and shall be communicated within the organization. [Management requirement]
- Persons, departments or organizations involved in safety life-cycle activities shall be competent to carry out the activities for which they are accountable. [Competency requirement]
- The stages in the safety life-cycle at which the functional safety assessment activities are to be carried out shall be identified during safety planning. [FSA requirement]
- Functional safety audit shall be performed by an independent person not undertaking work on the SIS to be audited. [Audit requirement]
- Procedures shall be implemented to evaluate the performance of the SIS against its safety requirements. [Performance evaluation requirement]



Functional Safety Assessment and Audit Requirement

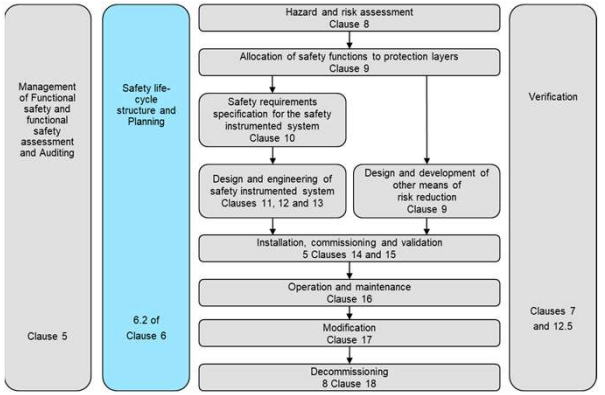
- FSA Requirement:
  - Project FSA: FSA required for a <u>new</u> SIF/SIS prior to introduction of the hazard.
  - Modification FSA: FSA required for any <u>modifications</u> of SIF/SIS (including components) prior to introduction of the hazard.
  - Periodic FSA (aka SIS Audit): Required periodically throughout the life of the SIF/SIS
  - FSAs are conducted by an independent senior competent person:
    - Project: Independent of the project
    - Others: Independent of the support and operations team of the SIF/SIS



Lifecycle and Planning

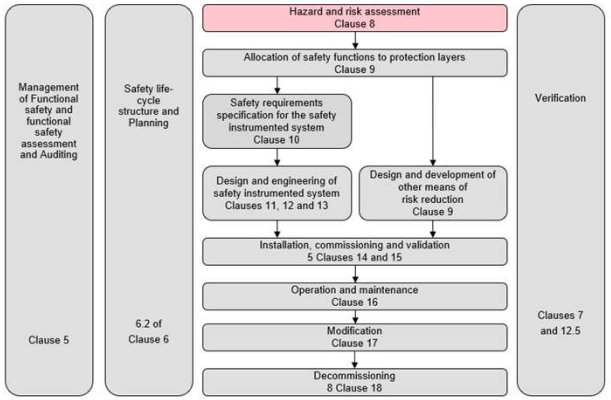
Key requirements include:

- A safety life-cycle incorporating the requirements of ANSI/ISA/IEC 61511 shall be defined during safety planning.
- For all safety life-cycle phases, safety planning shall take place to define the criteria, techniques, measures and procedures to ensure that the SIS safety requirements are achieved for all relevant modes of the process. [Planning requirement]



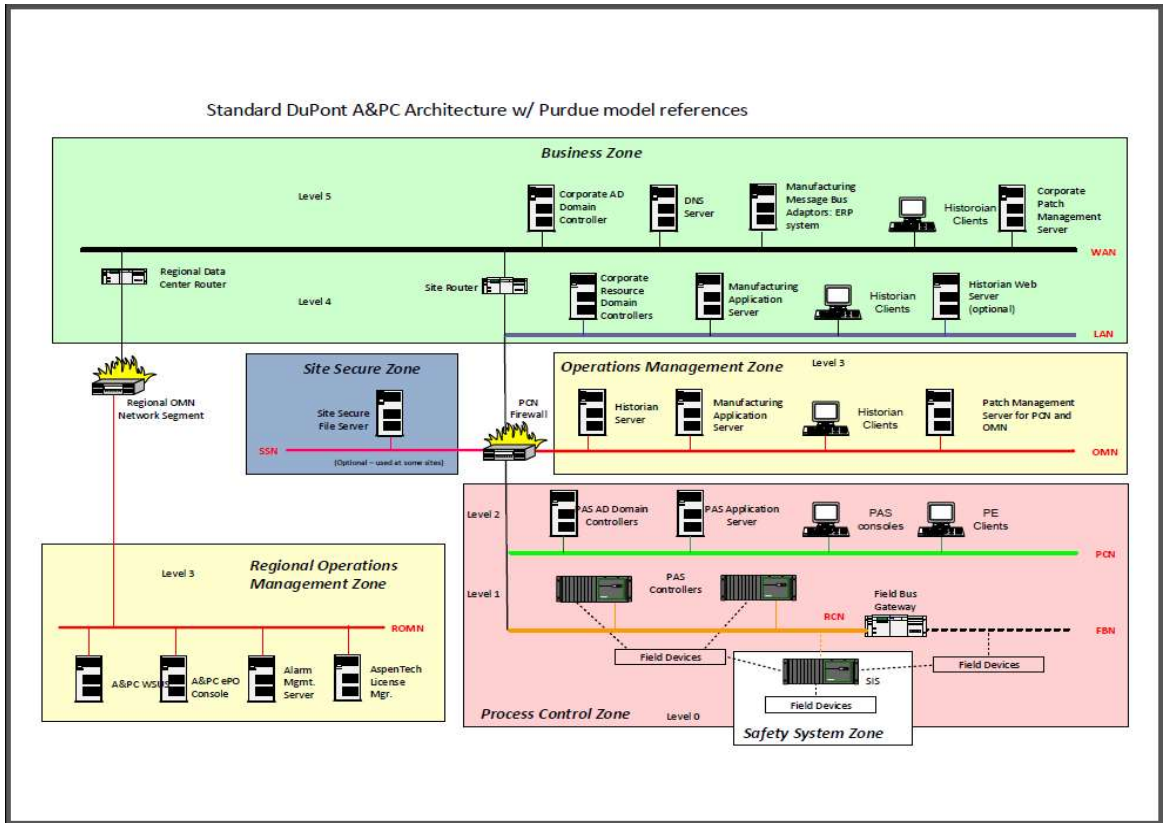
Hazard and Risk Assessment

- The potential need for SIFs and IPLs is determined using a risk assessment methodology during the Process Hazards Analysis (PHA). [Risk assessment requirement]
- A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. [Cyber-security requirement]



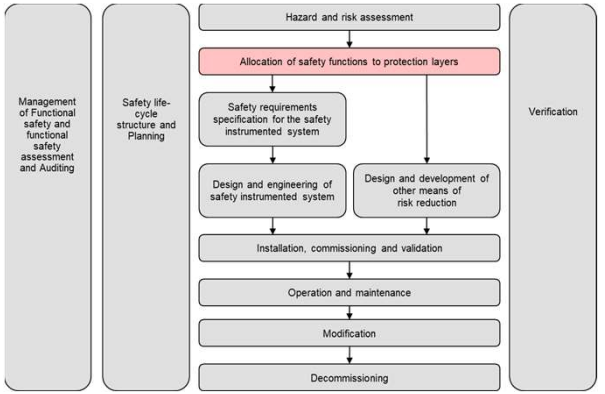
Cyber Security Assessment

- Cyber-security requirement
  - Security is performed in layers
  - General purpose network layer is covered by ISO2700x
  - Process control network layer is covered by IEC62443



Allocation of Safety Layers

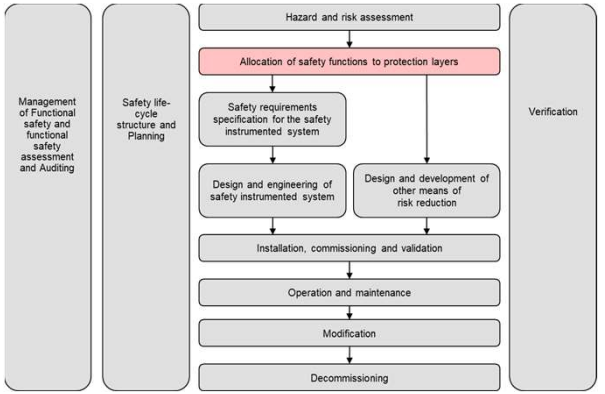
- The need for SIFs and IPLs is clearly defined following risk assessment, including:
  - The allocation of safety functions required to achieve the necessary risk reduction to specific protection layers
  - The allocation of risk reduction to each SIF.
- The SIFs are described in terms of the functional needs of the process requirements, and in terms of the risk reduction requirements (RRF or PFD or SIL). [Risk reduction requirement]



SIL	RRF	PFD
1	10-100	0.1-0,01
2	100-1000	0.01-0.001
3	1000-1000	0.001-0.0001

Allocation Limits

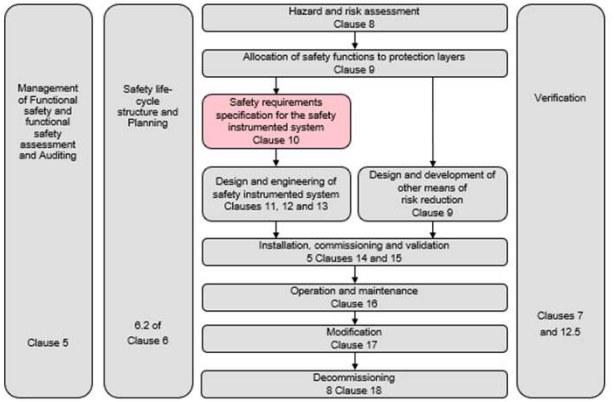
- Each BPCS protection layer shall be independent and separate from the initiating source and from each other to the extent that the claimed risk reduction of each BPCS protection layer is not compromised. [Independence requirement]
  - Limit of two BPCS credits per scenario
  - BPCS protection layers must be independent of each other



Safety Requirements Specification (SRS)

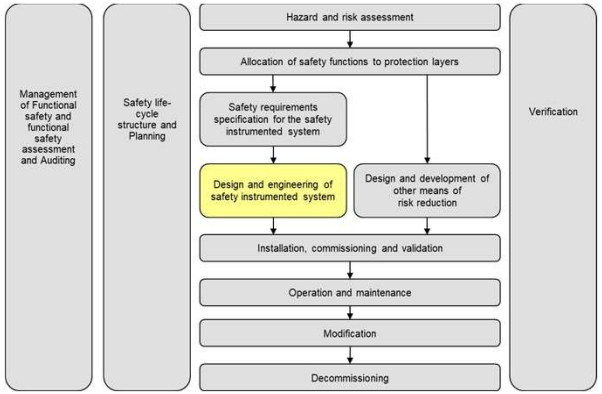
The requirements for each SIF are documented as part of the design. [SRS requirement]

- SRS includes a list of requirements:
  - Description
  - Devices, safe states, accuracies,
  - Sources of demands, spurious trip rates
  - Response times
  - Mode (low demand, high demand, continuous)
  - Manual shutdown
  - Interfaces to other systems
  - Bypass requirements
  - …



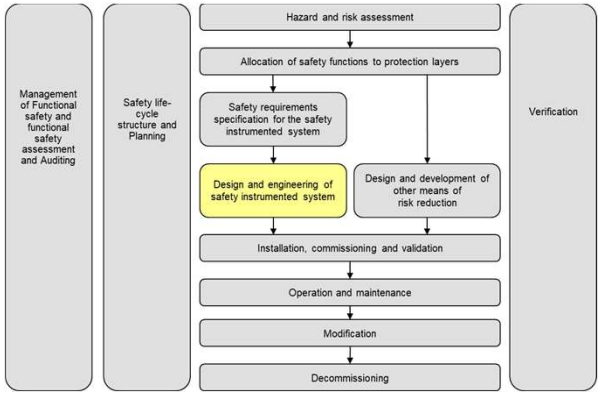
Design and Engineering

- The SIS is designed in detail and SIS devices are selected.
  - meet IEC61511 requirements (including architectural constraints)
  - be in accordance with the SIS SRS
- Probability of Failure on Demand (PFD) calculations are done to verify the integrity of each SIF. [RRF verification requirement]
- SIS application (software) is designed and shall match the SRS and its intended purpose.
- This stage includes Factory Acceptance Testing (FAT)



PFD Requirement

- Probability of Failure on Demand (PFD) calculations are done to verify the integrity of each SIF.
  - Required to use qualified tools or calculation method to determine the PFD
  - Is a function of testing intervals
  - The reliability data used when quantifying the effect of random failures shall be credible, traceable, documented and justified. [Reliability data requirement]



Reliability Data Requirement

- Device SIL Evaluation for SIS:
- Documented basis for failure rate data based on:
  - SIL certification data or
  - Proven-In-Use data.

exida CERTIFICATION

The manufacturer may use the mark:

CERTIFIED • IEC 61508 • SIL 3 CAPABLE •

Report:
ASC Q1301001 R001 V1R2
Assessment Report

Valid until February 28, 2016
Revision 1.1 March 21, 2013

ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

Certificate / Certificat
Zertifikat / 合格証

ASC 1301001 C001

exida hereby confirms that the:

Series 8314 Solenoid Valves

ASCO
Florham Park, NJ - USA

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A Element

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

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

Safety Function:
The Valve will move to the designed safe position when de-energized / energized within the specified safety time.

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

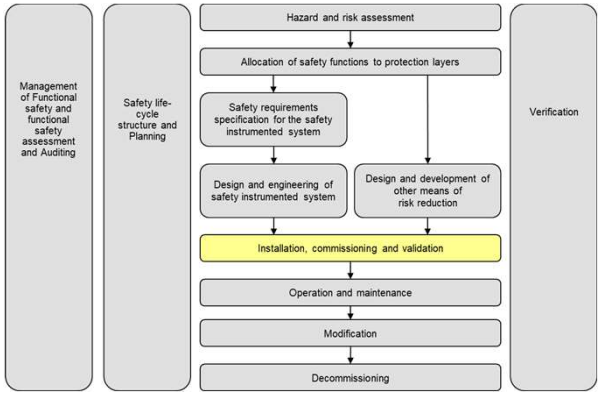
Evaluating Assessor

Certifying Assessor

Page 1 of 2

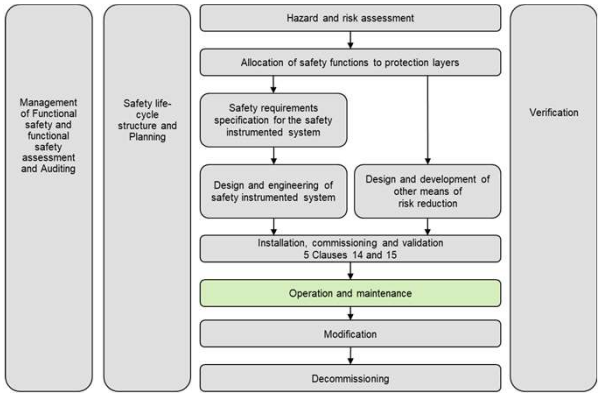
Installation, Commissioning and Validation

- Begins with Validation Planning:
  - shall define all activities and equipment required for validation.
- Installation: All SIS devices shall be properly installed according to the design and installation plan(s).
  - Changes from the issued design need to be approved by qualified personnel.
- Commissioning: The SIS shall be commissioned in accordance with planning in preparation for the final system validation.
  - Site Acceptance Testing (SAT) may be part of this
- Validation: The validation of the SIS and its associated SIF(s) shall be carried out in accordance with the SIS validation planning [Validation requirement].



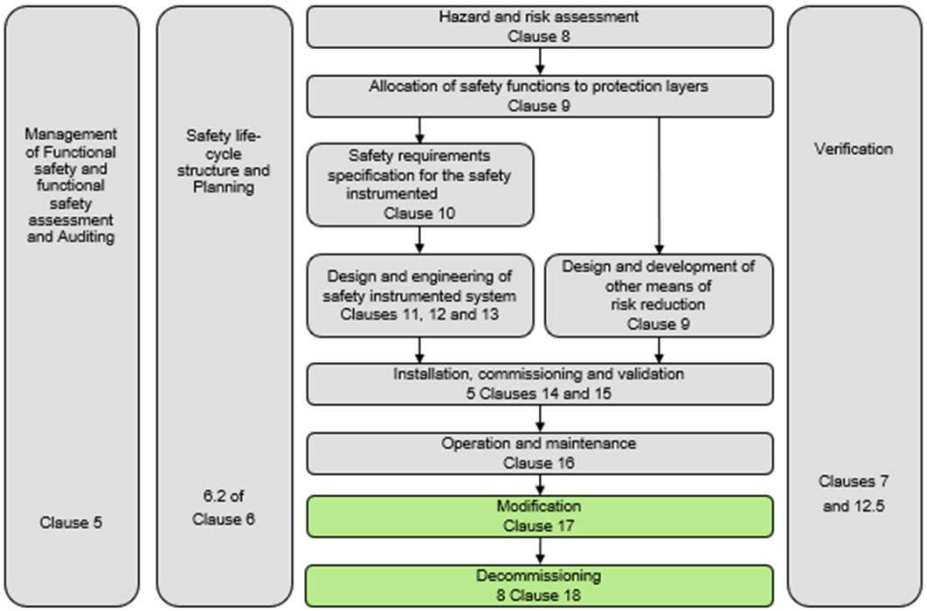
Operation and Maintenance

- Operations and maintenance procedures are developed
- Operations and maintenance personnel are trained
  - All personnel are required to be trained on the SIS task(s) they perform (including Operators, Maintenance, Technical, and Management)
- SIFs demands are recorded and analyzed. [Demand tracking requirement]
- Incidents are investigated
  - on true demands, on test failures, on other failures (especially dangerous failure while running)
- SIF bypasses (whether intentional or not)
- SIFs should have periodic proof tests. [Proof test requirement]



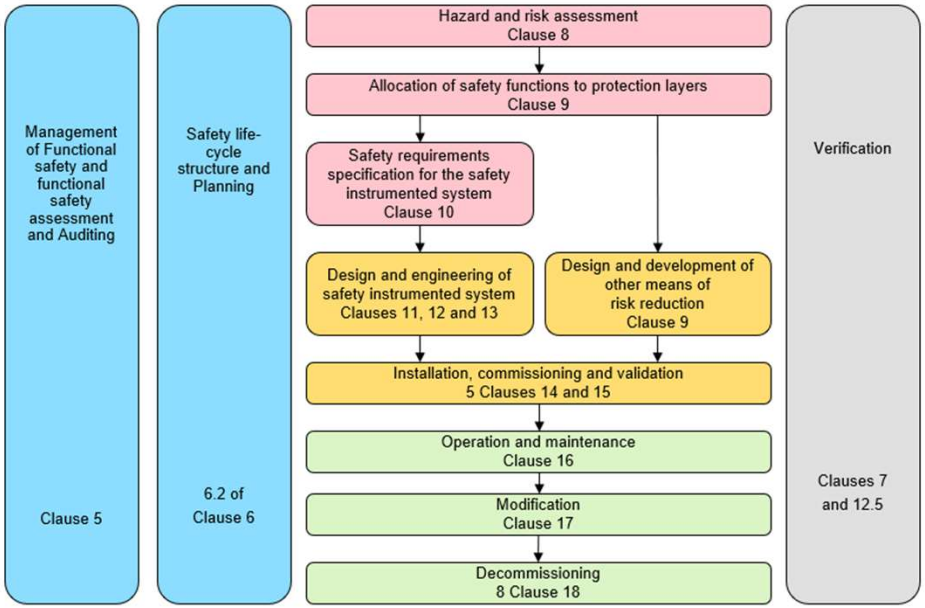
Modification and Decommissioning

- SIS changes follow the MOC procedure.
  - SIFs may be decommissioned.
  - MOC includes the lifecycle activities required for the change.
    - Includes potential impact on other SIFs in the SIS
    - Includes FSA



Summary

- SIS Lifecycle organizes the important requirements for SIF's/SIS's
- Applies cradle-to-grave
- All the activities are required for successful risk reduction
  - Management
  - Planning
  - Specification
  - Validation
  - Maintenance
  - Assessments
  - Competency
  - Evaluation
  - Design
  - Operation
  - Management of Change (MOC)
  - Audits



Questions?


Thank
you!