Saving Lives with Safety Interlocks

Nicholas P. Sands, CAP, PE

DuPont Laureate

DuPont Water & Protection Global Engineering

Outline

- Safety Moment
- Interlocks and Safety Interlocks
- Safety Interlock Life Cycle
- Challenges
- Summary

Nicholas P. Sands – DuPont – Automation Engineer R25A

34 YEARS WITH DUPONT
- Currently living in Dallas, Texas
- Worked at several sites and businesses

DUPONT ROLES
- DuPont Laureate
- Process Control Leader
- PSM Competency Team
- SIS SME
- AM SME

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

ISA/IEC STANDARDS+
- Co-editor *Guide to the Automation Body of Knowledge* (ed3)
- ANSI USNC SC65A
- ISA past VP of Standards and Practices
- ISA18 (AM) past co-Chair and co-director, lead editor
- ISA84 (SIS) past co-Director
- ISA101 (HMI) past co-Director
- IEC 62682 (AM) lead editor
- IEC MT61511 (SIS) member

Safety Moment

Formosa Plastics, Illiopolis, Illinois, 2004

- Operator bypassed a safety interlock to clean a poly vinyl chloride (PVC) reactor, but the reactor was pressurized and full of material.
- Vinyl chloride mixture was released, ignited and exploded
- 5 workers were fatally injured, and 3 workers were severely injured
- There was a history of operators mistakenly bypassing valves on pressurized reactors

Image from CSB

Interlocks

Interlock

- to connect so that the motion or operation of any part is constrained by another

Interlocks help keep us safe by preventing us from making easy mistakes

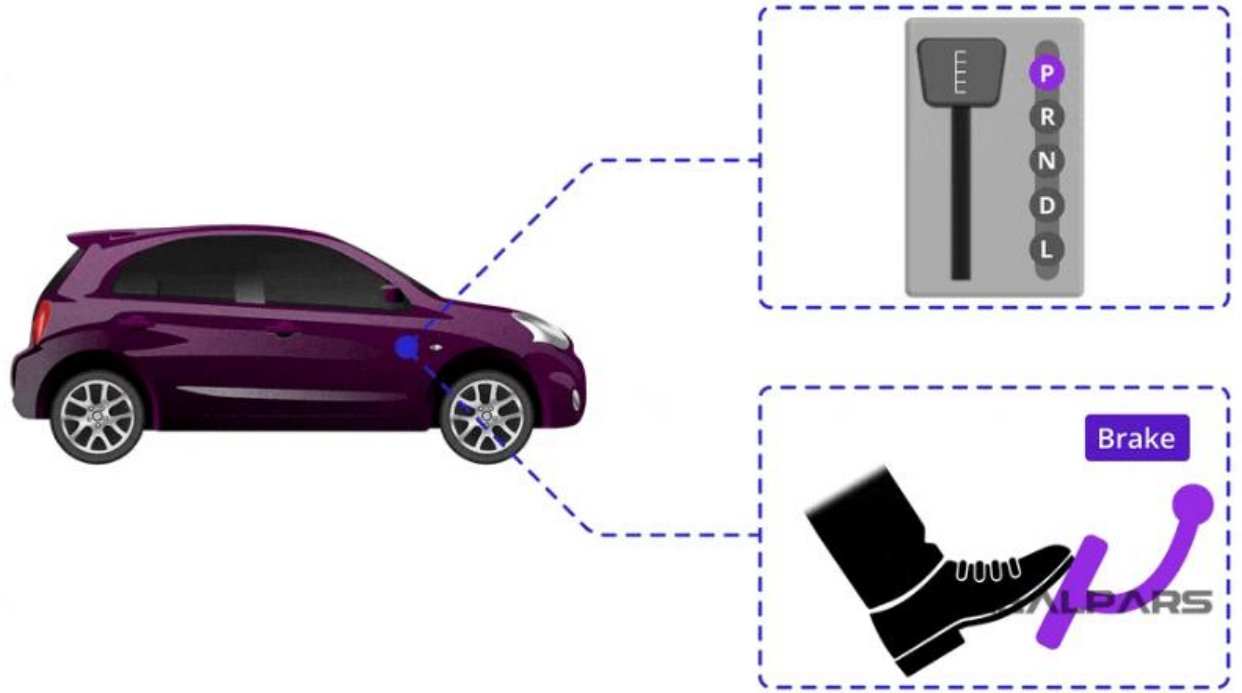
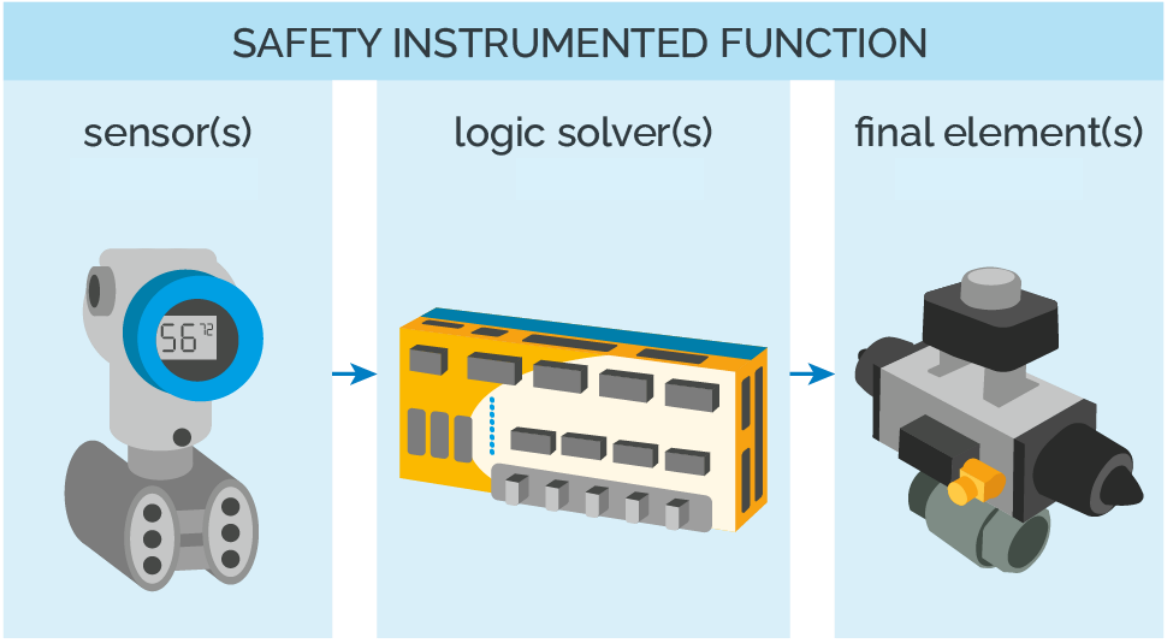


Image from REAL PARS

Safety Interlocks (Safety Instrumented Functions)

Safety Instrumented function (SIF)

- function to be implemented by one or more protection layers in a safety instrumented system, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event

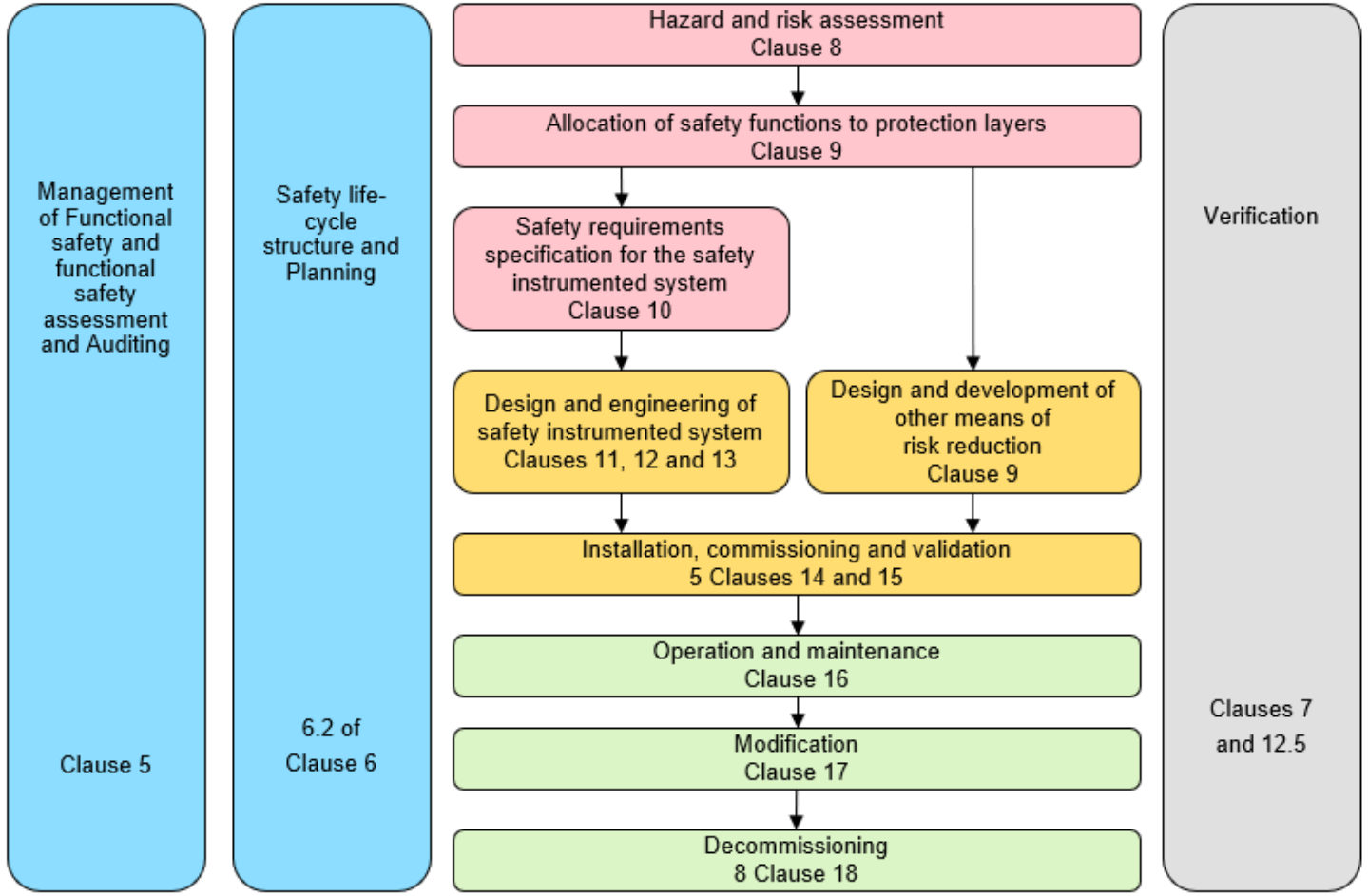


Safety interlocks are special types of interlocks in process safety, with many requirements and much documentation

Safety Instrumented System Life Cycle

ISA/IEC 61511 SIS Life Cycle

- Captures all the activities
- Phases include:
  - Verification
    - Review of deliverables during each phase
  - Life cycle structure and planning
    - Organization and planning for each activity



ISA – International Society of Automation
IEC – International Electrotechnical Commission

Safety Interlock Selection

Safety interlocks protect against process hazards

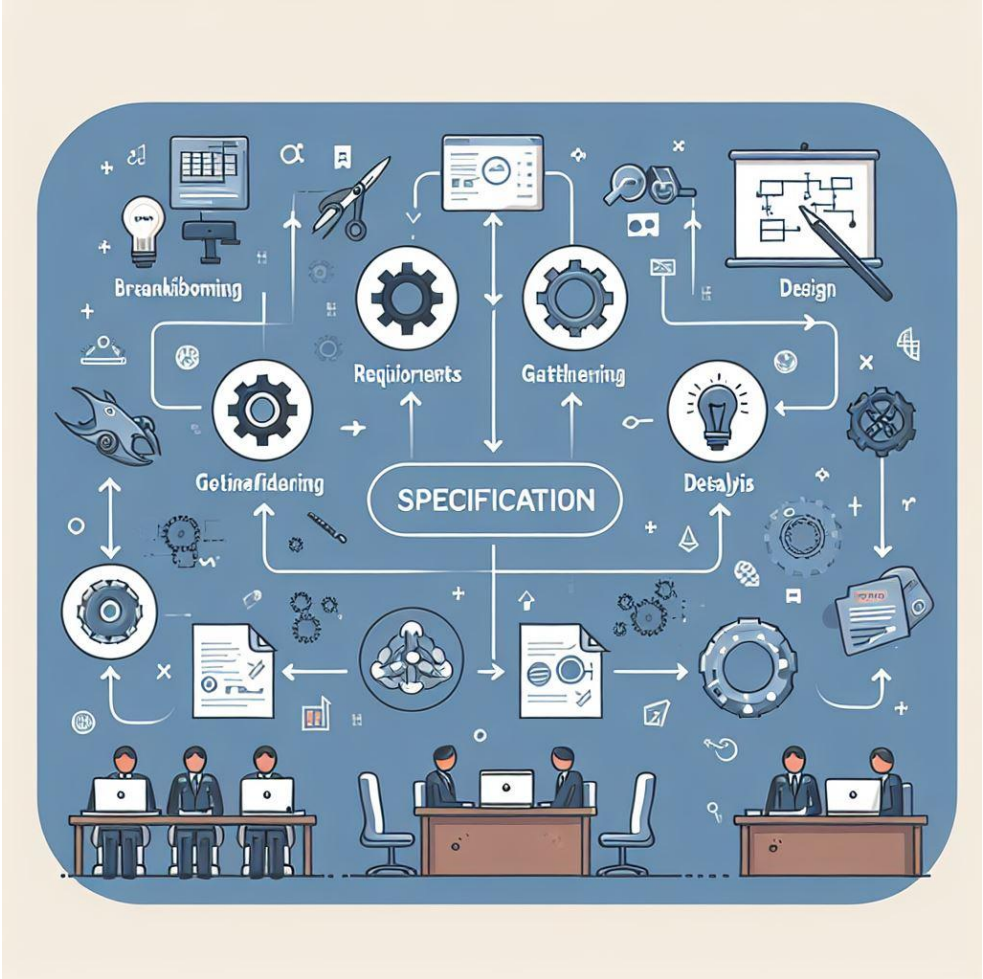
- Hazard and Risk Assessment
  - Identify process hazards and the existing protections
    - Process Hazard Analysis (PHA)
- Allocation of safety functions
  - Assigning risk reduction to safety interlocks and other protection layers
    - Risk Reduction Factor (RRF) >10
    - Probability of Failure on Demand (PFD) < 0.1
    - RRF = 1 / PFD

AI generated

Safety Interlock Specification

Safety Requirements Specification (SRS)

- The functional requirements for a safety interlock
  - ~25 requirements including:
  - Functional requirements
  - Safety Integrity Level (SIL)
  - Process safety time
  - Response time
  - Security requirements



AI generated

Safety Interlock Design

Safety interlock design

- Meets all requirements, including
  - Functional requirements
  - SIL requirement
    - Calculated RRF or PFD
    - Calculations use device failure rates
- Follows design rules
  - Independent of the (basic) process control system (BPCS)

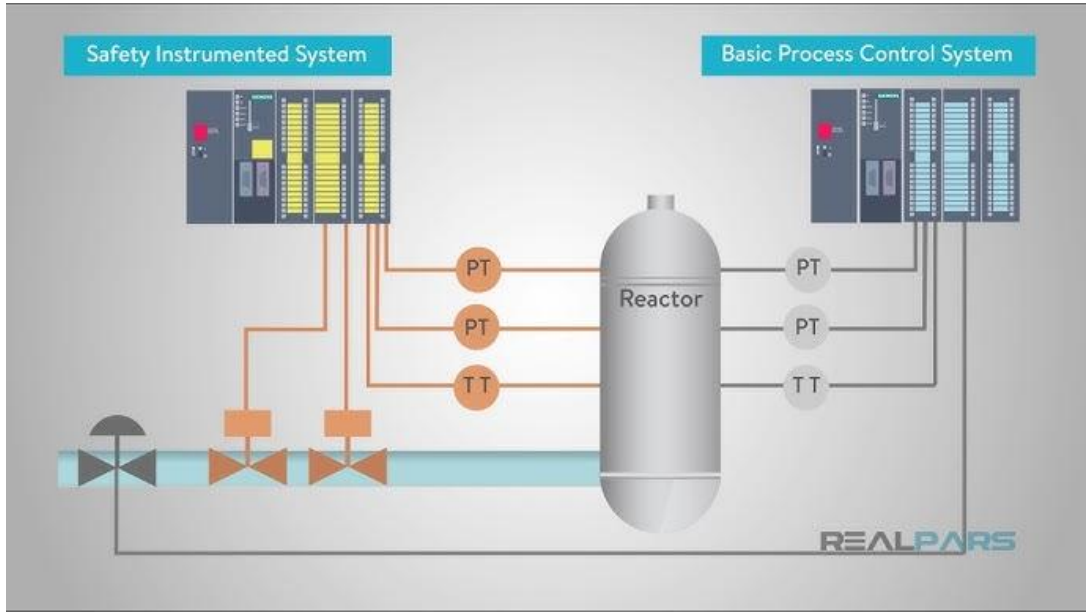


Image from REAL PARS

Safety Instrument System Validation

Safety Instrumented System (SIS)

- SIS is a set of safety interlocks

Installation and validation

- Validation is proving all requirements are met
  - Validation is very detailed and thoroughly documented

AI generated

Safety Interlock Operation and Maintenance

Operations and Maintenance:

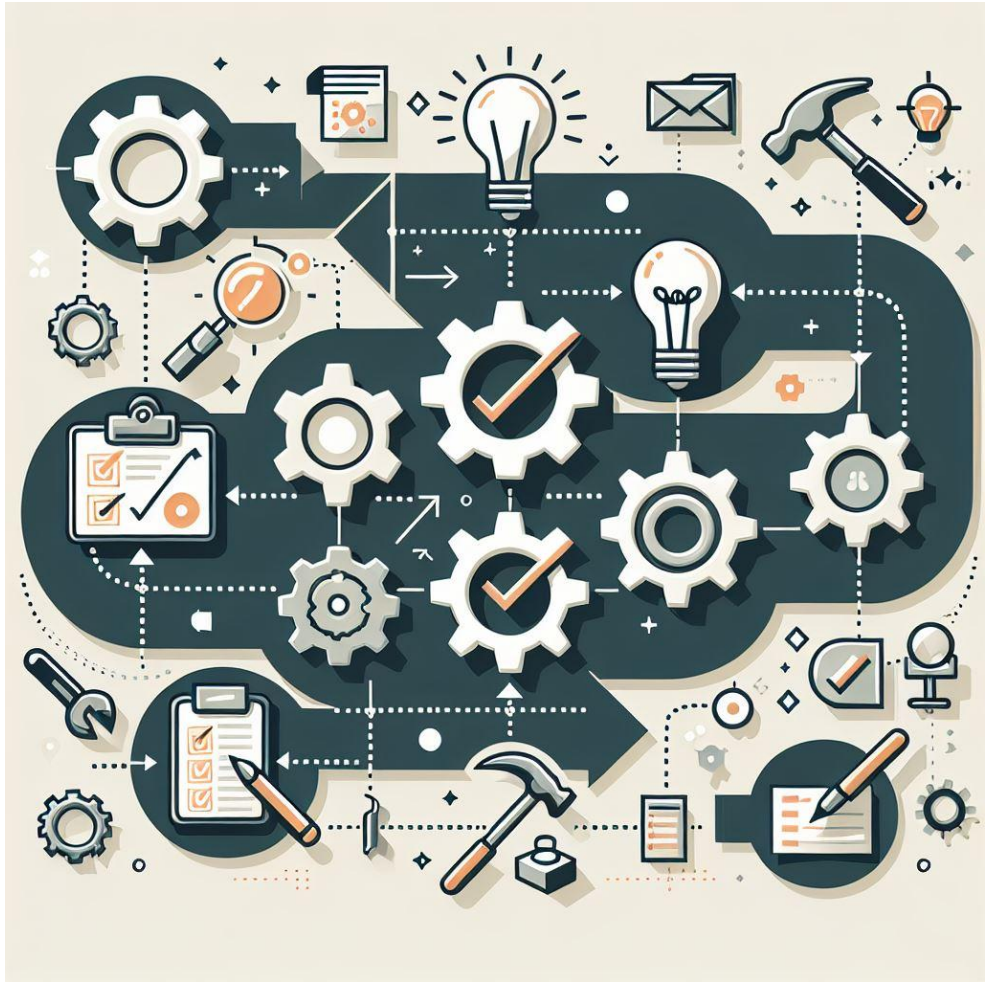
- Personnel trained on the safety interlock functions
- Operators trained to respond to demands and failures
- Maintenance trained on testing
- Tests completed periodically
- Demands and failures recorded

AI generated

Safety Interlock Management of Change

Management of Change (MOC)

- Update documentation
  - SRS
  - Design
  - Training
  - Test procedures
- Includes removal

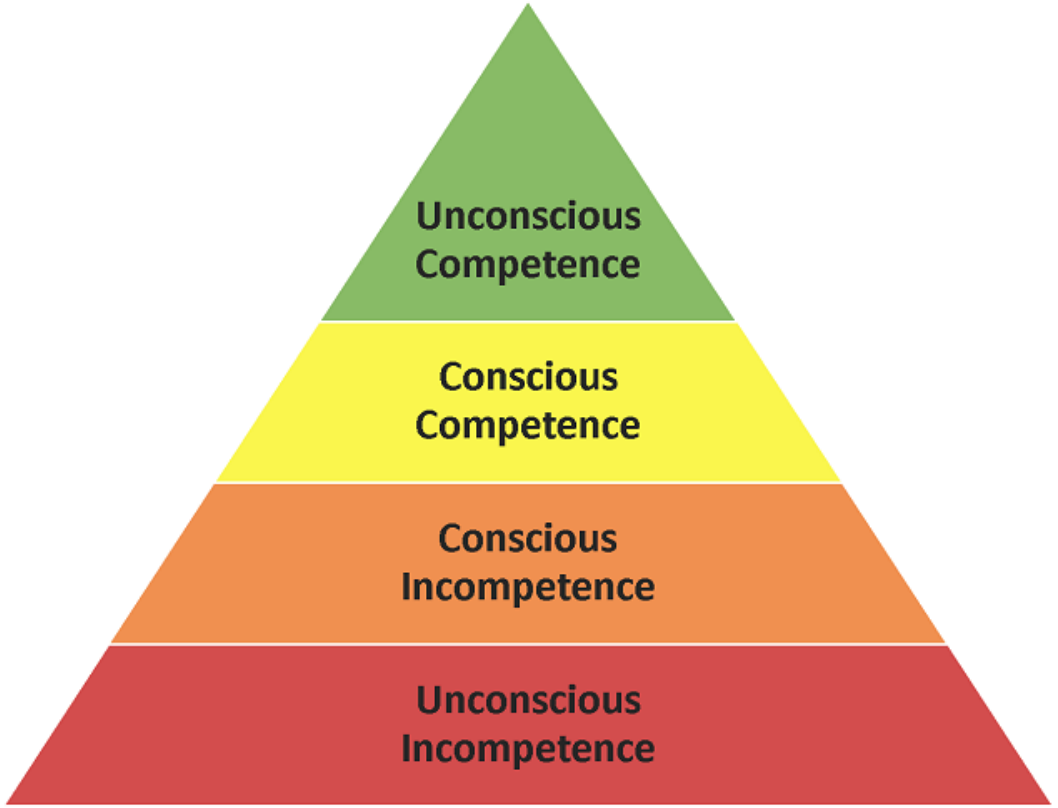


AI generated

Management of Safety Instrumented Systems

Management system elements

- Competency
  - Training and knowledge
- Functional Safety Assessments (FSAs)
  - At different phases
- Audits
- Performance evaluations



Challenges

- Standards
  - Changes
  - Misalignment
  - Interpretation
- Competency
  - Change in personnel
  - Deep competency
- Leadership support
  - Changes
  - Other safety needs
- Upgrading systems
  - End of useful life

AI generated

Coming Soon…

ANSI/ISA-84.91.03 Functional Safety: Low Integrity Protection Layers

- Applies to interlocks in the BPCS
- Does not apply to alarms
- Requirements similar to SIS, but less onerous
- Potentially significant new work
- Will be available for ANSI public comment soon

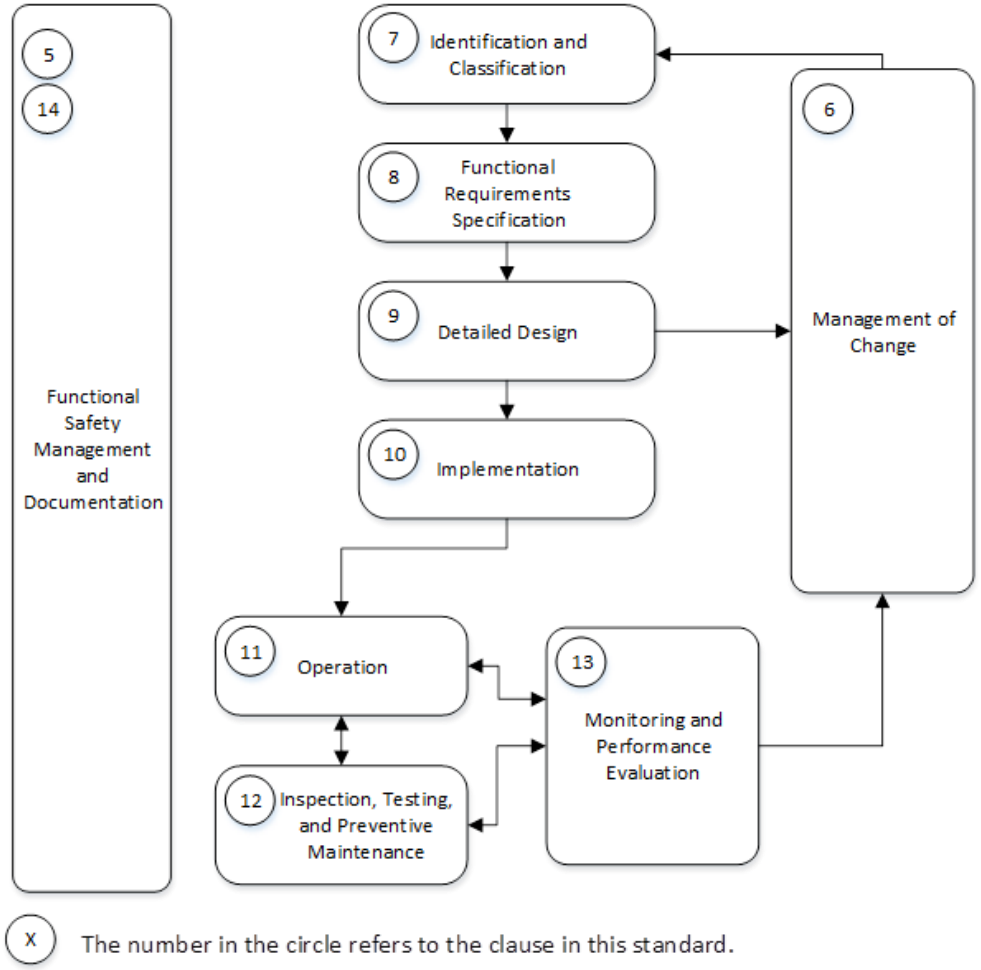


Figure 1. Example of LI-PL Lifecycle

Summary

- SIS life cycle organizes the important requirements for SIS
- Applies from creation to removal

- Management
- Planning
- Specification
- Validation
- Maintenance
- Assessments
- Competency
- Evaluation
- Design
- Operation
- MOC
- Audits