SIS Life cycle Management for Major Hazards Installations

Sujith Panikkar

TŰV Rheinland FS Expert, Senior Consultant – Functional Safety & Security

Director – APAC Consulting, HIMA Asia Pacific Pte. Ltd., Singapore

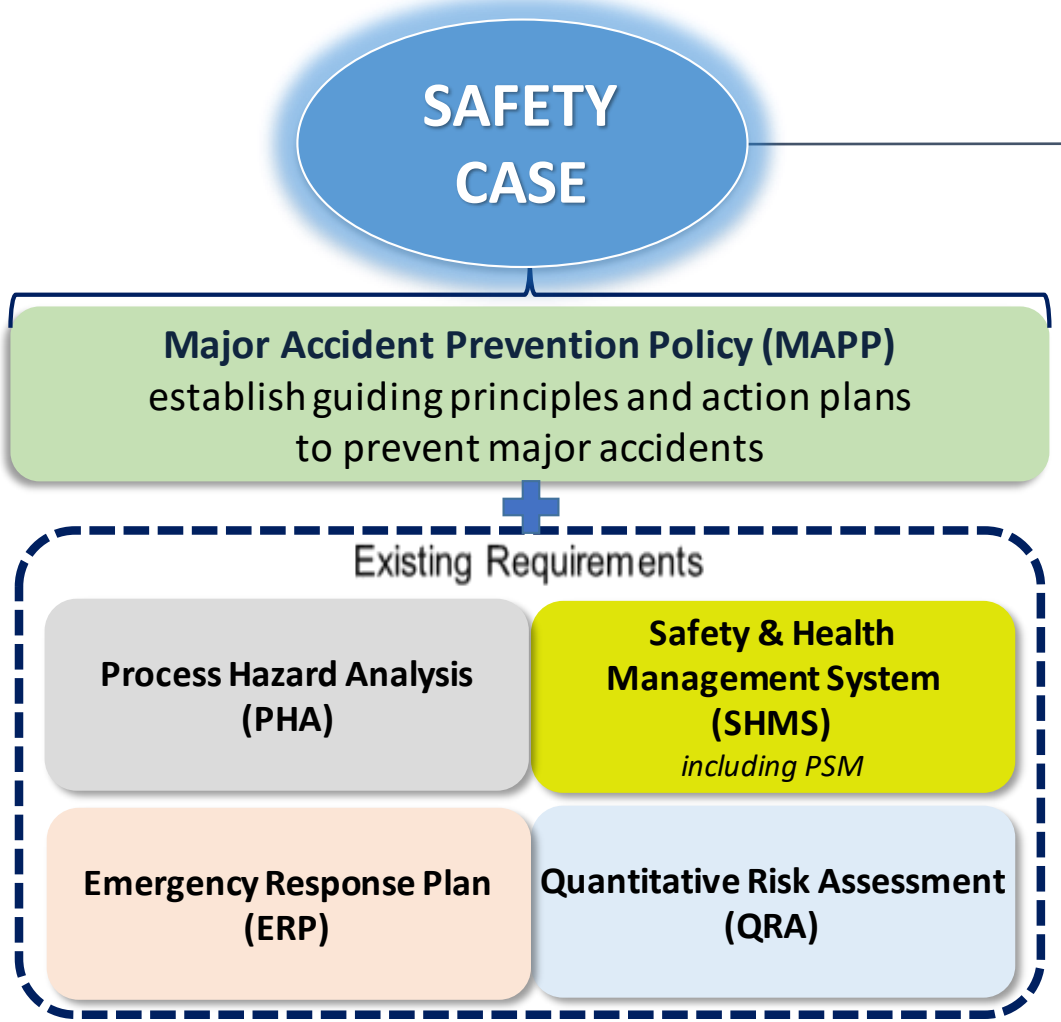
Safety Case Symposium 2018 Singapore

Agenda

1. Requirements from Singapore Safety Case Regulation
2. Basis: SIS Safety Lifecycle : IEC 61511
3. SIS Lifecycle Management & Requirements from IEC 61511
4. Benefits for MHIs

Singapore Safety Case: Safety Instrumented Systems

Safety Case Overview



Major Hazards Dept (MHD)
Single front, jointly regulated by MOM, NEA & SCDF

- A single consolidated Safety Case
- **ALARP demonstration**
- Integrate & demonstrate robustness of all SHE protocols to regulators
- Sharing of domino information with neighbouring plants
- Reviewed once every 5 years

** ALARP: As Low As Reasonably Practicable*

Source: MOM public presentations on WSH(MHI) Regulations

Safety Case: Main Components

- Descriptive info of MHI
- Major Accident Prevention Policy (MAPP)
- Safety Management System (SMS) description
- Risk assessment, including predictive aspects & identification of Major Accident Scenarios (MASs) along with domino effects
- Emergency Response Plan (ERP)
- ALARP demonstration for selected MASs

- Technical aspects of a Safety Case, including controls (prevention and mitigation measures) to prevent MASs from occurring
  - Process safety
  - Mechanical
  - Electrical, controls and instrumentation (EC&I)
  - Human factors

*SC contains all info required to **demonstrate** that the MHI can be **operated safely**.*

Source: MOM public presentations

Safety Case Technical Aspects*: Safety Control Systems

- The safety case shall show that the MHIs have examined the costs and benefits of automating the system and justified the suitability of the adopted approach.
- Safety Control Systems: MHIs shall describe the principles of how safety-related control systems have been designed to ensure safety and reliability.
- A control system or device is deemed to be safety critical if it provides functions which significantly reduce the risk of a hazard, and in combination with other risk reduction measures, reduces the overall risk to an ALARP level.

- Includes protective systems such as
  - Emergency shutdown systems
  - Trips and interlocks
- Evidence shall be provided in the safety case to show that the **complete system (from sensor to final element, including software and the human interface) has been considered (e.g. Safety Integrity Level).** This may include the use of accepted good practice, codes and standards

** Refer: MOM Safety Case Technical Guide*

Safety Case Technical Aspects*: Safety Control Systems

- MHIs shall describe how the design of safety related control systems have accounted for :
  - safe operating limits and their relation to the set points for safety functions
  - selection of appropriate measurement instrumentation
  - inspection and maintenance requirements, including the provision of facilities for carrying out proof testing
  - operating conditions, including start-up and shutdown and unusual operating conditions
  - independence and separation from other systems
  - environmental considerations, including requirements to operate in flammable atmospheres,
  - Consideration of electromagnetic interference
  - appropriate application of redundancy, diversity, separation and segregation to safeguard against the risks of common cause failure. This shall include hardware, software and human interfaces
  - shut-off requirements for valves and how their performance will be affected by the presence of corrosive or erosive conditions

Also requirements in IEC 61511!

** Refer:*
MOM Safety Case Technical Guide,
Safety Case Assessment Guide

Safety Regulations: Singapore

- QRA guidelines published by SG government : http://www.nea.gov.sg/docs/default-source/anti-pollution-radiation-protection/central-building-planning/qra-technical-guidance_final.pdf
- Safety Case regime; requires evidence by end user during regulatory audits

Modifier	Description	Comments
Detection and shut-down system	Probability of failure on demand of system which detects a loss of containment (e.g. pressure loss, gas detection etc) and operates shutdown valve(s) which will isolate the release or much reduce the quantity released.	Should be justified with reference to intention to provide system with suitable IEC61508/ 61511 safety integrity level (SIL) for entire system including detection, logic, field wiring or equivalent, actuators and valves. Extensive evidence and SIL2 rating required for lower end of range. Lower probabilities may be possible for SIL3 but better solution is often multiple diverse systems at SIL2 or SIL1. It should be noted that SIL 3 is very onerous to design in practice and will require suitable maintenance and inspection frequencies to maintain the level of risk reduction. Suitable SIL report will be required when available to justify SIL assumed. Shut down system should not normally rely on manual isolation. Manual isolation may be acceptable with

Singapore Safety Case Assessment Guide

7.1.1.4	**The safety case shall show how safety-related control systems have been designed to ensure safety and reliability.**	**To meet this criterion, the safety case shall describe:** a) the standards applied to the design of instrumented safety systems, including: (i) process safety systems; (ii) machinery safety systems (e.g. where machines are used in the manufacture of chemicals or explosives); b) the general approach to functional safety management; c) how it has been assured that persons involved in the design of safety instrumented systems (SIS) are competent to carry out the activities for which they are accountable; d) how current relevant good practice (e.g. IEC 61511) has been applied as far as reasonably practicable to systems designed before its publication;
		Content provided in the safety case to assist demonstration could include: a) sample safety requirements specification (SRS); b) sample SIL assessment record (e.g. PFD calculation and fault tolerance assessment); c) sample record of competence for an individual involved in the design of SIS or in the review of SIS against relevant good practice.

SIS Safety Life cycle

Basis: SIS Safety Life cycle

International Standards:

- IEC 61511: 2016 : Functional safety –
  Safety instrumented systems for the process industry

- IEC 61508: 2010: Functional safety of electrical/electronic/
  programmable electronic safety-related systems

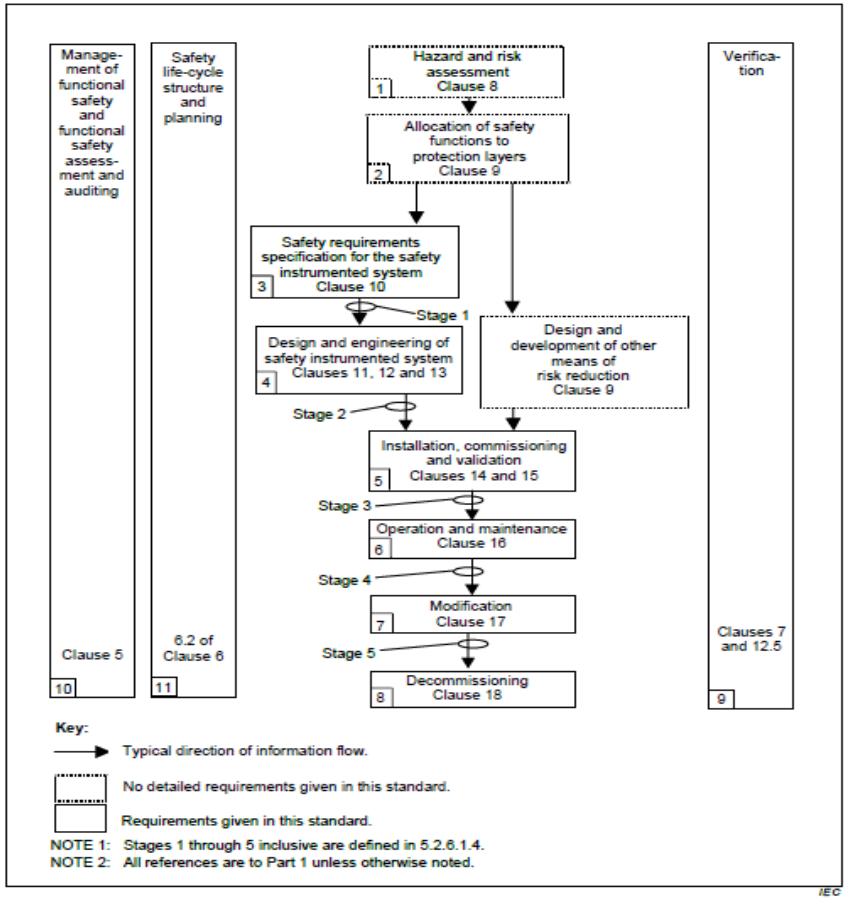
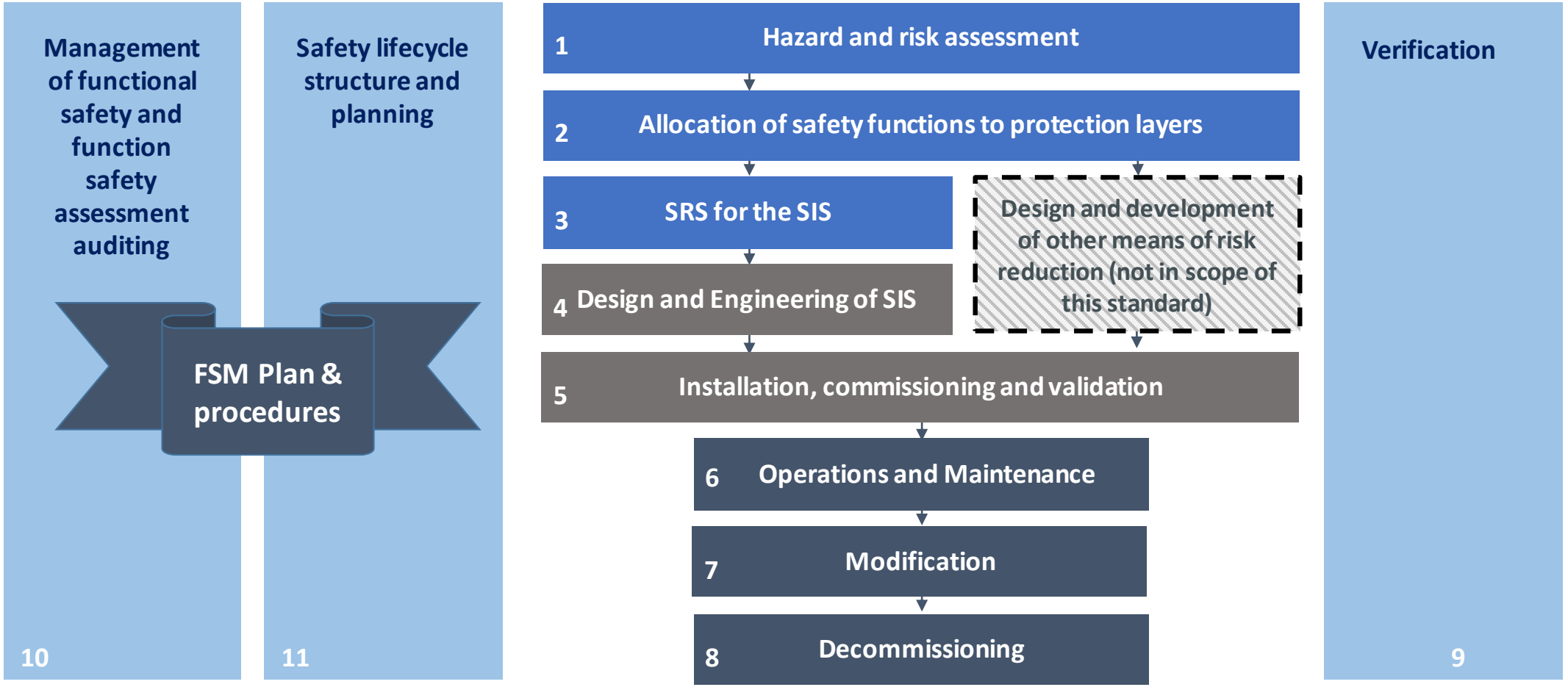


Fig. Safety Lifecycle as per IEC 61511

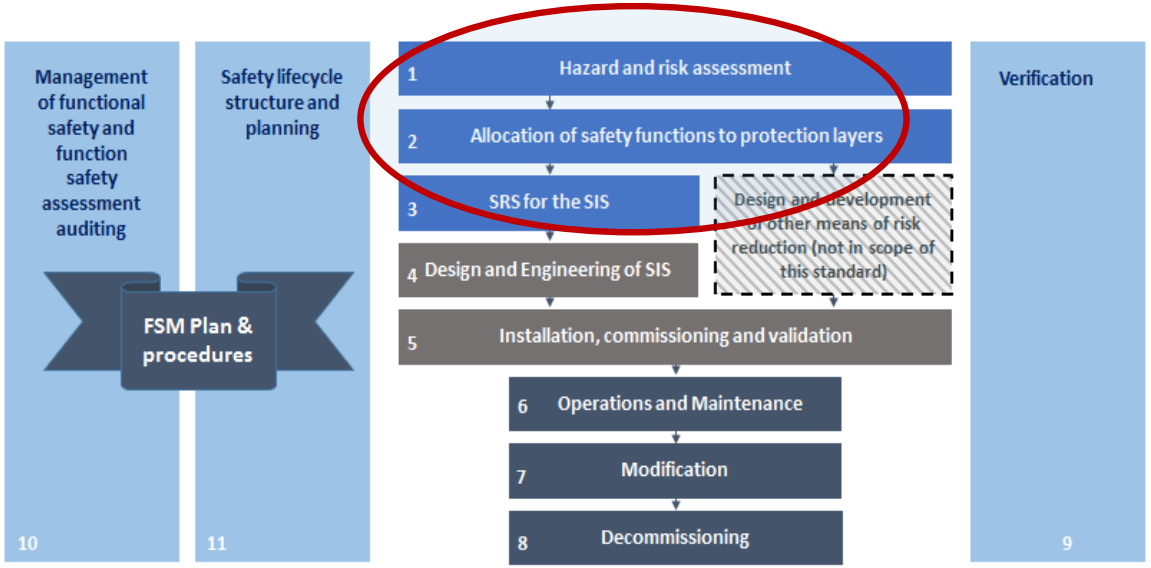
IEC 61511 Life cycle



SIS Life cycle management activities
&
Requirements from IEC 61511

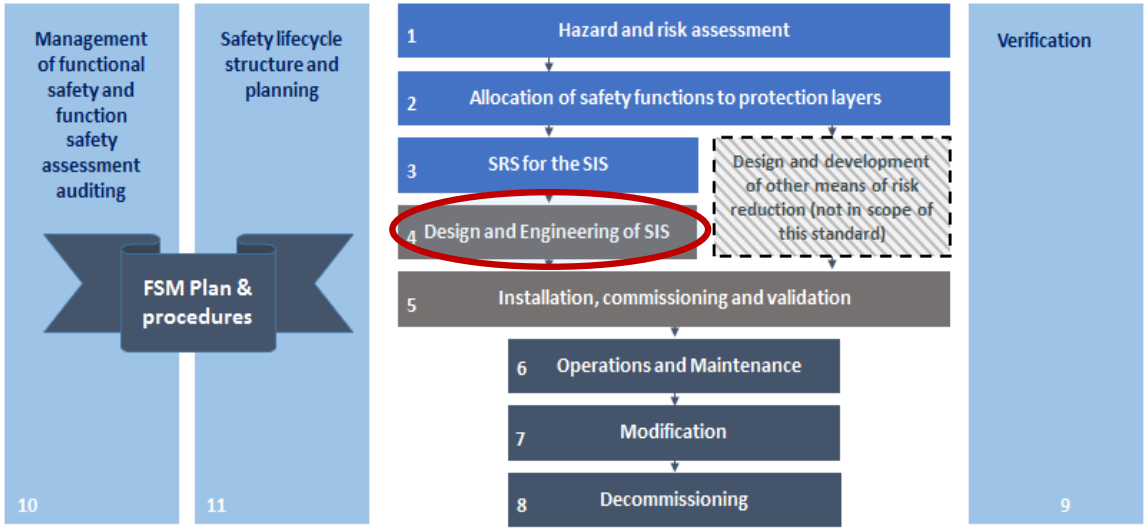
SIS in the Analysis Phase: Key activities

- Perform Hazard and Risk Analysis >> Identify Safety Functions
- Perform cyber-security risk analysis (Ref :IEC 62443/ ISA 99)
- SIL Classification >> Determine SIL targets for SIFs
- SRS documentation

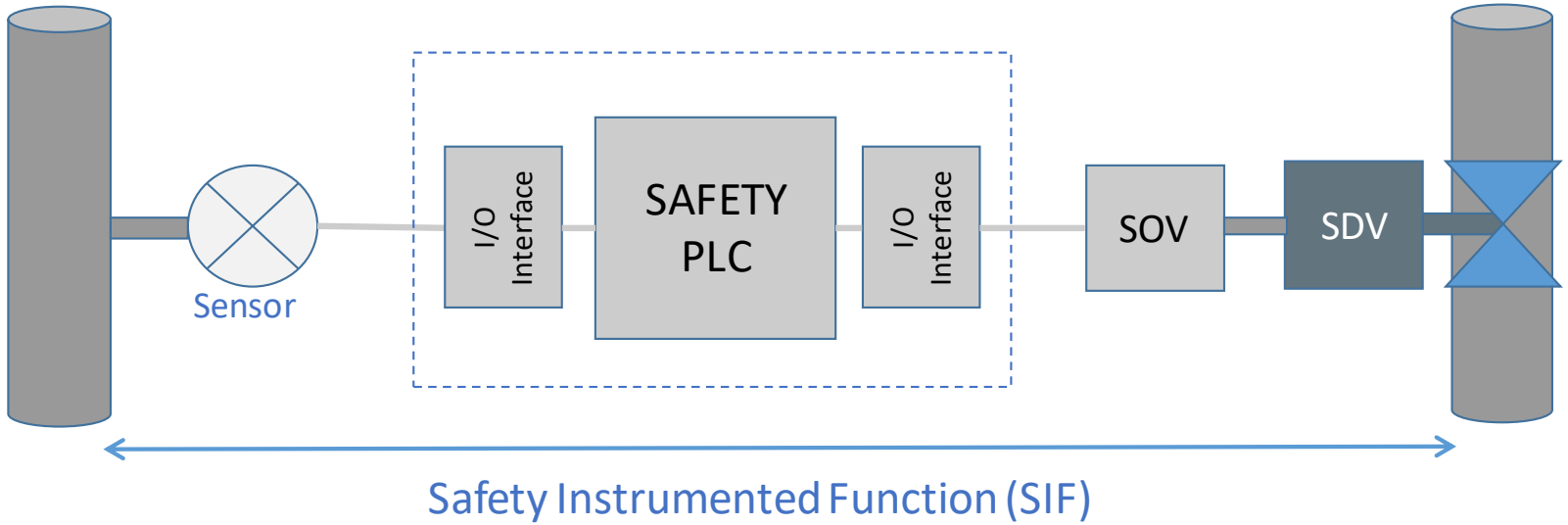


SIS in the Realization Phase: Key activities

- Design documents reviewed & approved
- Verification steps
- Consider and implement cybersecurity measures
- Integration & testing
- FAT records for SIS equipment
- Plannning for :
  - Installation
  - Operation & Maintenance
  - SIS validation



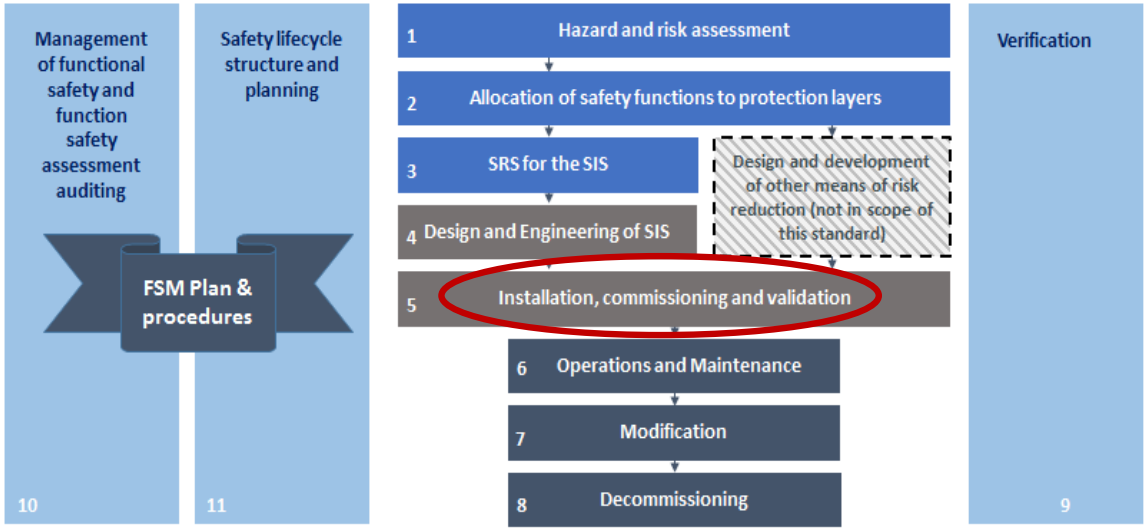
Calculations for Safety



- **To claim SIL achievement:**
  - Calculate PFDavg for the SIF loop in acc. with standards requirement
  - Check & confirm hardware fault tolerance (HFT) in acc. with standards
  - Systematic capability according to the claimed SIL target

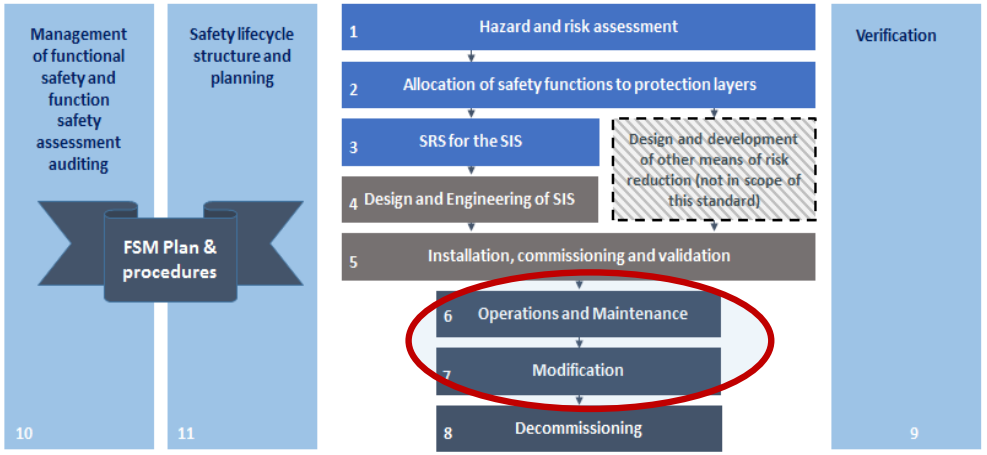
Install, Commission & Validate the SIS

- Install & commission the SIS according to plan and procedures
- Prior to introduction of hazards, perform SIS Validation



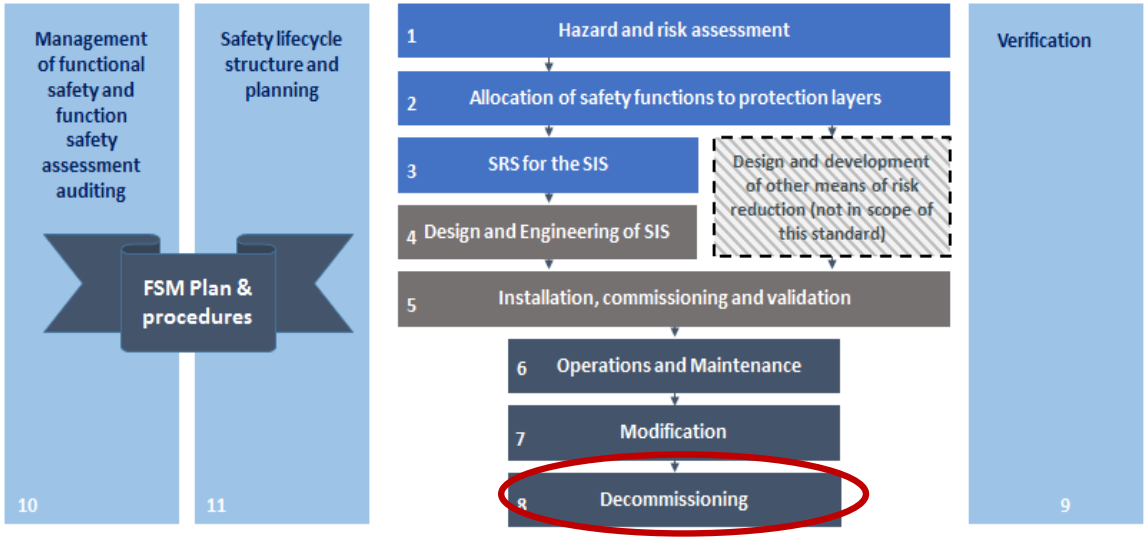
Management of SIS in the Operation Phase

- SIS Overrides/ bypasses management
- Proof Testing & Data Analysis
  - Analysis of demand rates vs. HAZOP assumptions
  - Analysis of failures vs. Initial assumptions
- SIS Modifications
  - Change Management/
  - Impact analysis
- SIS Management & Reports
- Also, manage Cybersecurity of the installation (Ref :IEC 62443/ ISA 99)



Decommissioning

- Procedures to ensure safety prior to de-commissioning any SIS from active service
- Required SIFs remain operational during de-commissioning
- Impact analysis



Competence Management

- Competence management is a mandatory requirement

5.2.2.3 A procedure shall be in place to manage competence of all those involved in the SIS life cycle. Periodic assessments shall be carried out to document the competence of individuals against the activities they are performing and on change of an individual within a role.

Functional Safety Assessments

- FSA is mandatory:
  - prior to start-up
  - periodically during operations & maintenance
  - prior to SIS modifications
- FSA shall cover all phases

5.2.6.1.5 Prior to the hazards being present the FSA team shall undertake functional safety assessment(s) and shall confirm:

5.2.6.1.10 A FSA shall also be carried out periodically during the operations and maintenance phase to ensure that maintenance and operation are being carried out according to the assumptions made during design and that the requirements within IEC 61511 for safety management and verification are being met.

5.2.6.1.9 In cases where a FSA is carried out on a modification the assessment shall consider the impact analysis carried out on the proposed modification and confirm that the modification work performed is in compliance with the requirements of IEC 61511.

Functional Safety Audits

- Functional Safety Audits are to be carried out by an independent person on the organization:

5.2.6.2.3 Functional safety audit shall be performed by an independent person not undertaking work on the SIS to be audited. Procedures shall be defined and executed for auditing compliance with requirements including:

- the frequency of the functional safety audit activities;
- the degree of independence between the persons, departments, organizations or other units carrying out the work and those carrying out the functional safety auditing activities;
- the recording and follow-up activities.

5.2.6.2.2 All procedures identified as necessary resulting from all safety life-cycle activities shall be subject to safety audit.

Benefits for MHIs

Benefits for MHIs

- Regulatory compliance
  - Helps comply to Singapore Safety Case regulation
- Demonstration for insurance and regulatory audits
  - Effectiveness of SIS management in the operations phase
  - “How many hours in the last 12 months were safety functions defeated?
- IEC 61511 ed2 Standards perspective:
  - End users have responsibility to manage their SIS installations operations and modifications
- Proactive approach to managing safety
- Optimise CAPEX by “right sizing“ SIS design
- OPEX improvements: Optimising “costs of safety“
  - Preventing Safety incidents by better Safety Management Systems & Tools
  - Proof Testing & Safety management in the operation phase
- Risk Insurance costs

Thank you very much for your kind attention!

Email: Sujith.Panikkar@hima.com

Safety Case Symposium 2018 Singapore

www.SafetyCaseSymposium.com