Safety Case Symposium 2018
Singapore
Mar 14 - 15, 2018

Safety Case Plus: Safety Case Regime in context of Functional Safety acc. IEC 61511

Dr. Thorsten Gantevoort
Head of Certification Body, TUV Rheinland

The occupier of a major hazard installation or deemed major hazard installation must take all measures necessary to **reduce the risk** of major accidents to **as low as is reasonably practicable** and to limit the consequences of major accidents.

WORKPLACE SAFETY AND HEALTH ACT

Agenda Overview

Safety Case Regime Lifecycle in context of Functional Safety acc. IEC 61511

Introduction / Overview IEC 61511

IEC 61511 Lifecycle

Introduction / Overview Safety Case

Safety Case Regime

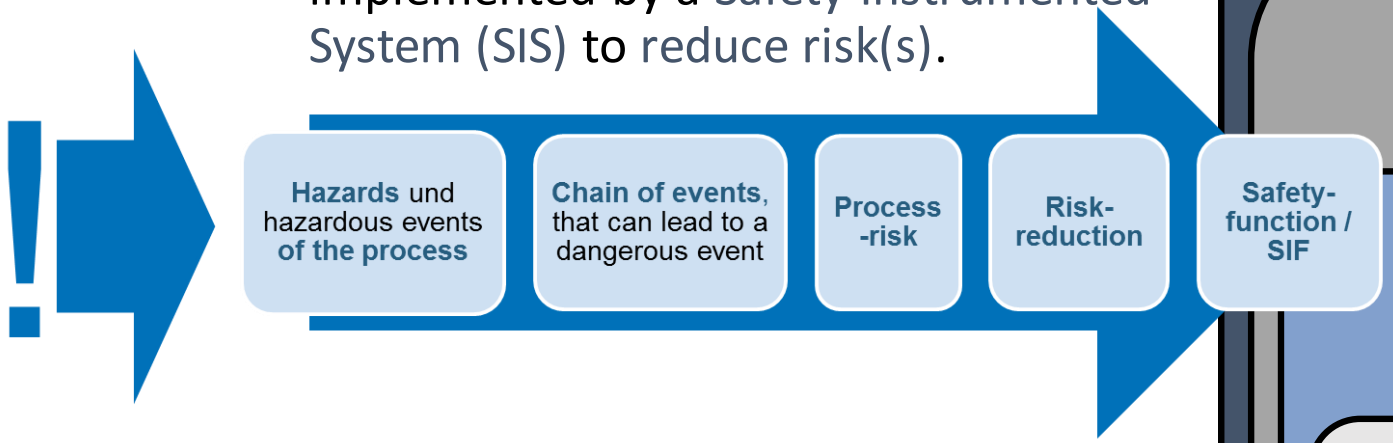
Safety Case Lifecycle in context of Functional Safety

IEC 61511

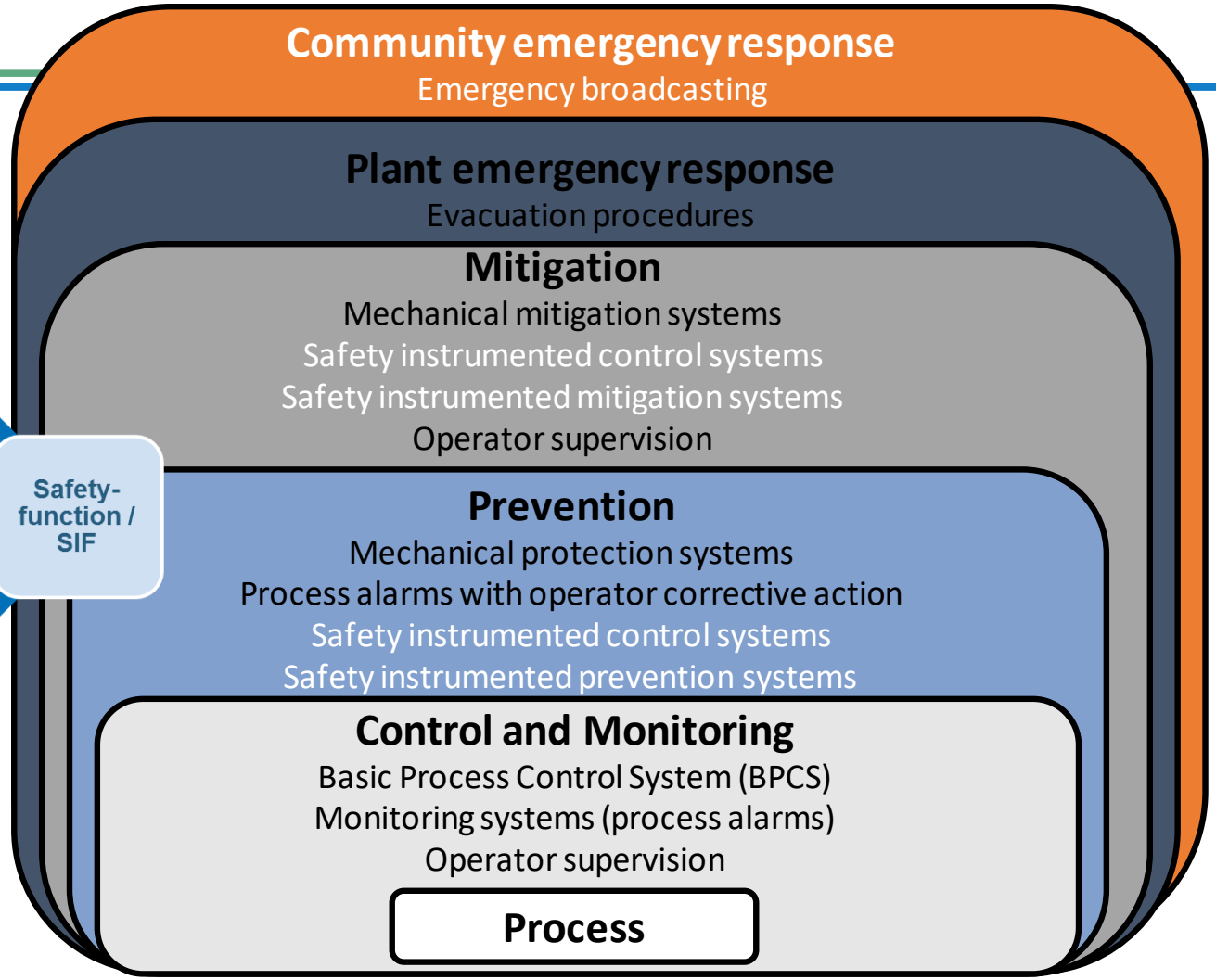
Introduction

Functional Safety

- A Safety Instrumented Function (SIF) is implemented by a Safety Instrumented System (SIS) to reduce risk(s).



IEC 61511: If risk reduction claimed for a [EC&I] protection layer is > 10, then it shall be designed and managed to the requirements within the IEC 61511 series.



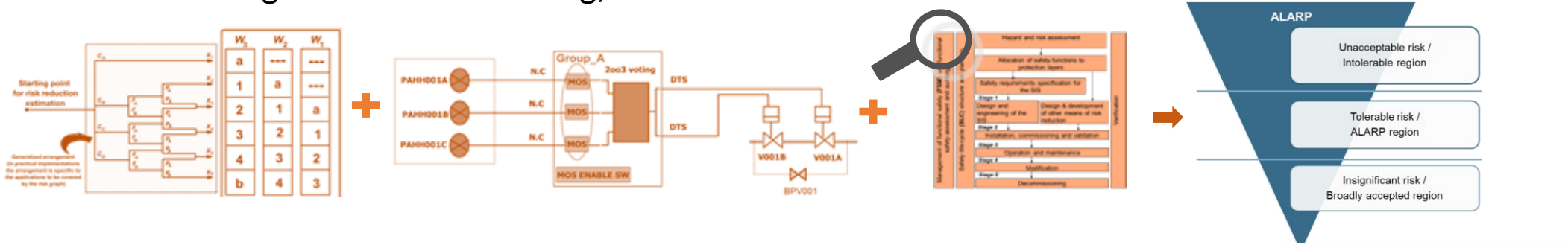
Typical protection layers and risk reduction means

IEC 61511

Overview

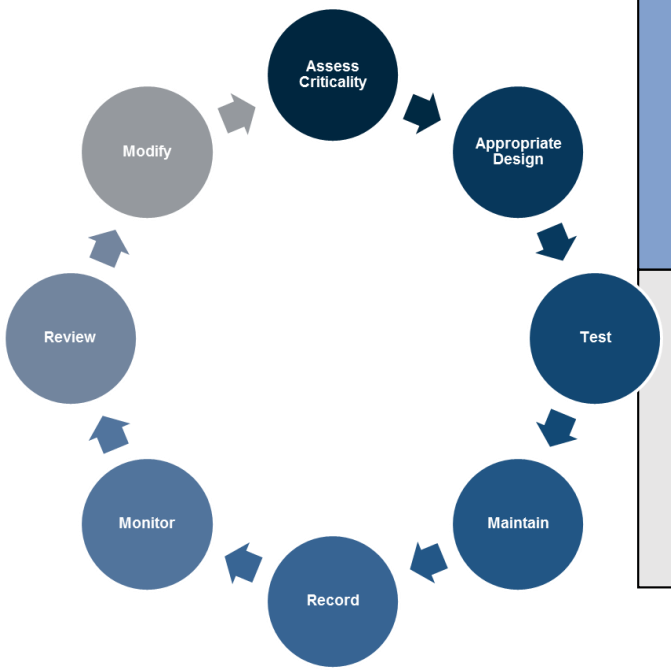
IEC 61511

- Addresses the application of Safety Instrumented Systems (SISs) performing Safety Instrumented Functions (SIFs) in the process industries, which are based on the use of electrical/electronic/programmable electronic technology
- Applies to a wide variety of industries within the process sector for example, chemicals, oil and gas, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation
- Addresses a Process Hazard and Risk Assessment (H&RA) to be carried out to enable the specification for SIS
- Has two concepts which are fundamental to its application: SIS safety lifecycle (SLC) and safety integrity levels (SILs)
- Addresses all SIS safety lifecycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;



IEC 61511

Safety Lifecycle (SLC) & FSM



Analysis & Concept

Design & Realization

Operation & Performance Monitoring & Modification

Management of functional safety **(FSM)** and functional safety assessment and auditing

Safety Lifecycle **(SLC)** structure and planning

Hazard and risk assessment

Allocation of safety functions to protection layers

Safety requirements specification for the SIS

Stage 1

Design and engineering of the SIS

Design & development of other means of risk reduction

Stage 2

Installation, commissioning and validation

Stage 3

Operation and maintenance

Stage 4

Modification

Stage 5

Decommissioning

Verification

Safety Lifecycle

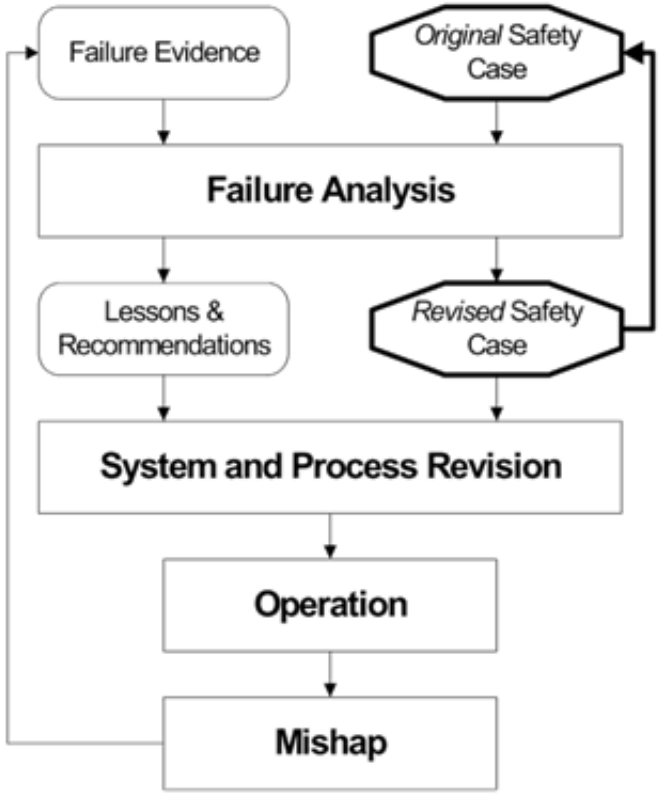
EN 61511 and others

EN 61511

- For all SLC phases, safety planning shall take place to:
  - ensure that the SIS safety requirements are achieved;
  - ensure proper installation and commissioning of the SIS;
  - ensure the safety integrity of the SIF after installation;
  - maintain the safety integrity during operation (e.g. proof testing, failure analysis);
  - manage the process hazards during maintenance activities on the SIS.
- Upon modification pertaining to an earlier lifecycle phase, then that earlier phase and the subsequent phases shall be re-examined, altered as required and re-verified.
- Security risk assessment shall be carried out […]
  - […] consideration of various phases such as design, implementation, commissioning, operation, and maintenance;

! Functional Safety & Cyber Security → Cyber Safety

Safety-Case Lifecycle



Enhanced Safety-Case Lifecycle
Source: FAILURE ANALYSIS AND THE SAFETY-CASE LIFECYCLE by William S. Greenwell, Elisabeth A. Strunk, and John C. Knight, 20[illegible]

Lifecycle for Functional Safety & Cyber Security (Cyber Safety)

Functional Safety
IEC 61508

Cyber Security
IEC 62443

1	Concept
2	Overall scope definition
	Hazard and risk analysis / 3 / **Risk and Threat analysis**
4	Overall safety & security requirements
5	Overall safety & security requirements allocation
9	Specification of E/E/PE System
10	Realization of E/E/PES Systems
12	Overall installation and commissioning
13	Overall validation
14	Overall operation, maintenance and repair
16	Decommissioning

→ Safety Integrity Level (SIL) 1 – 4

Probability of a dangerous failure in:	
SIL 1	≈ 10 years
SIL 2	≈ 100 years
SIL 3	≈ 1,000 years
SIL 4	≈ 10,000 years

→ Security Level (SL) 1 – 4

SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means
SL 3	Protection against intentional violation using sophisticated means
SL 4	Protection against intentional violation using sophisticated means with extended resources

(Functional) Safety Management

EN 61511 and others

EN 61511

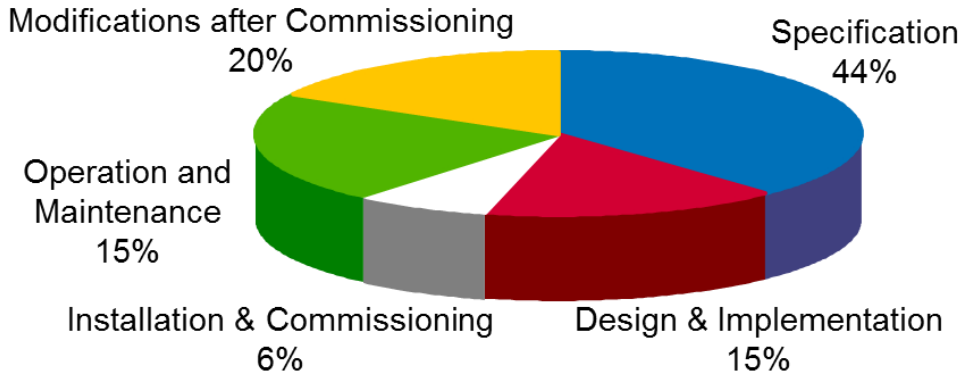
- For all SLC phases, safety planning shall take place to define the activities, criteria, techniques, measures, procedures and responsible organization/people […] post-incident and post-accident activities…
- Procedures shall be implemented to ensure prompt follow-up and satisfactorily resolution of recommendations arising from
  - hazard analysis and risk assessment;
  - assessment and auditing activities;
  - verification activities;
  - validation activities;
  - post-incident and post-accident activities.

SEVESO-II (III)-Directive

The safety management system should include the part of the general management system which includes the organizational structure, responsibilities, practices, procedures, processes and resources for determining and implementing the major accident prevention policy.

Singapore WORKPLACE SAFETY AND HEALTH ACT

The important elements of SHMS are:
Roles and Responsibilities, Resources, Personal Performance, Worker Participation, External Organization, Information Gathering, Internal Communication, Priorities for Improvement, Procedures, Management of Change, Active / Reactive Monitoring […]



Safety Case

Overview

A Case

- Safety Case essentially is a case, which makes a statement based on evidence through argument.

A tool

- Safety case, under Singapore's WSH(MHI) regulations, is also a regulatory tool. MHI is required to develop its safety case, and demonstrate it to the MHD and convince them that the strategy for managing safety is satisfactory, through the adoption of ALARP principle.

A set of live documents

- It also can be viewed as a set of documents, which demonstrate that the MHI are designed, constructed, commissioned, operated and decommissioned in such a way that the risks to personnel, the public and the environment are minimized, for the use of both regulators and operators.

Safety Case

Safety Case Regime

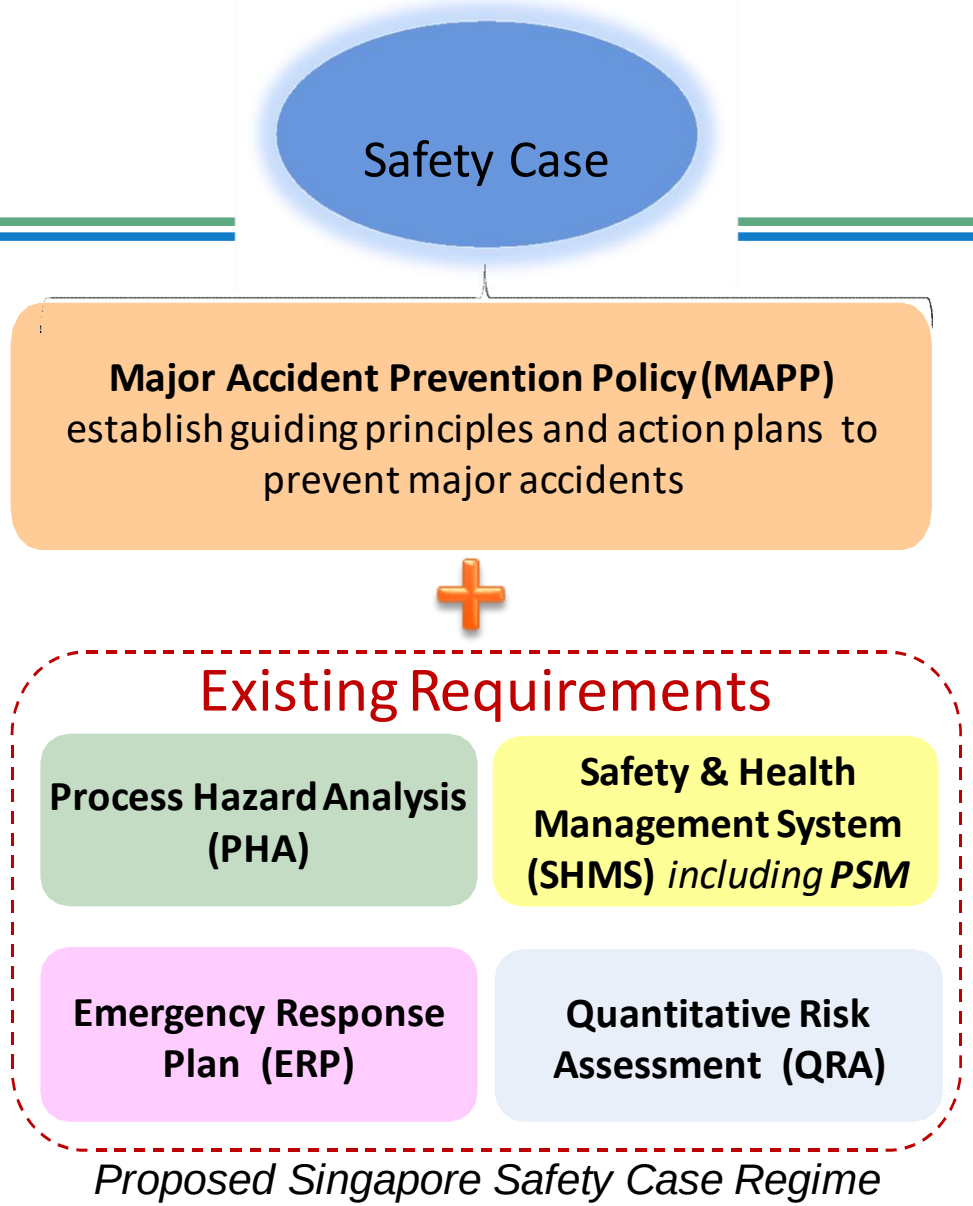
- **Core Feature of WSH(MHI) Regulation:**
- Safety Case Regime is the core feature of the WSH (MHI) Regulations. It allows flexibility for MHIs to tailor their risk mitigating measures, enabling MHIs to address their risk in a more holistic manner.
- Under the Safety Case Regime, MHIs are expected to:

1. Take on greater responsibilities.
2. Proactively identify and manage Safety Health and Environment (SHE) risks through integration of all SHE protocols.
3. Demonstrate to regulators that their risks are as low as reasonably practicable.

! Functional Safety in the sense of WSH(MHI) Regulation: … is concerned with the management, design, installation, operation, maintenance and modification of instrumented process safety systems that reduce the risk of a major accident. Such systems include: process control systems; safety instrumented systems; alarm systems.

Safety Case

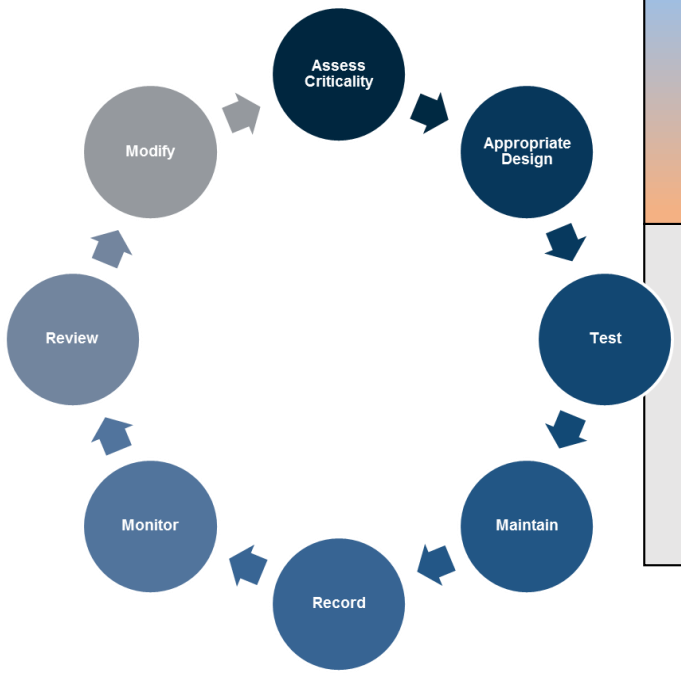
Safety Management



Proposed Singapore Safety Case Regime

Safety Case

Safety Case Lifecycle



Analysis & Concept

Design & Realization

Operation & Performance Monitoring & Modification

Safety Management with safety assessment and auditing

Attend pre-receipt meeting *

*Alignment of approach to develop safety case**

Act on safety case conclusions*

*Risk controls of safety case are implemented. Action items in Proposed Intervention Priorities & Intervention Plan are completed**

Assessment

Operation and maintenance

Review safety case*

Assessment

Decommissioning

* Ministry of Manpower: Preparing for safety case

Safety Case Lifecycle in context of Functional Safety

IEC 61511 as aid for Safety Case compliance

Safety Case Requirements	IEC 61511	
Management of safety as risk based approach	FSM	☑
Implement a lifecycle approach	SLC	☑
Identification of (major) hazard / risks; scenarios, triggers and probability; assessment of the severity of the consequences	PH&RA	☑
Implement measures of protection and intervention to limit the consequences	SIS / SIF	☑
Implement measure to monitor the "safety performance"	FSM	☑
Update / modify depending on lessons learned	FSM	☑

! The main emphasis of the IEC 61511 is concerned with the identification of hazards and reducing the associated risks from a level that is intolerable to a residual risk that is tolerable or 'as low as reasonably practicable' (ALARP).

Safety Case Lifecycle in context of Cyber Security

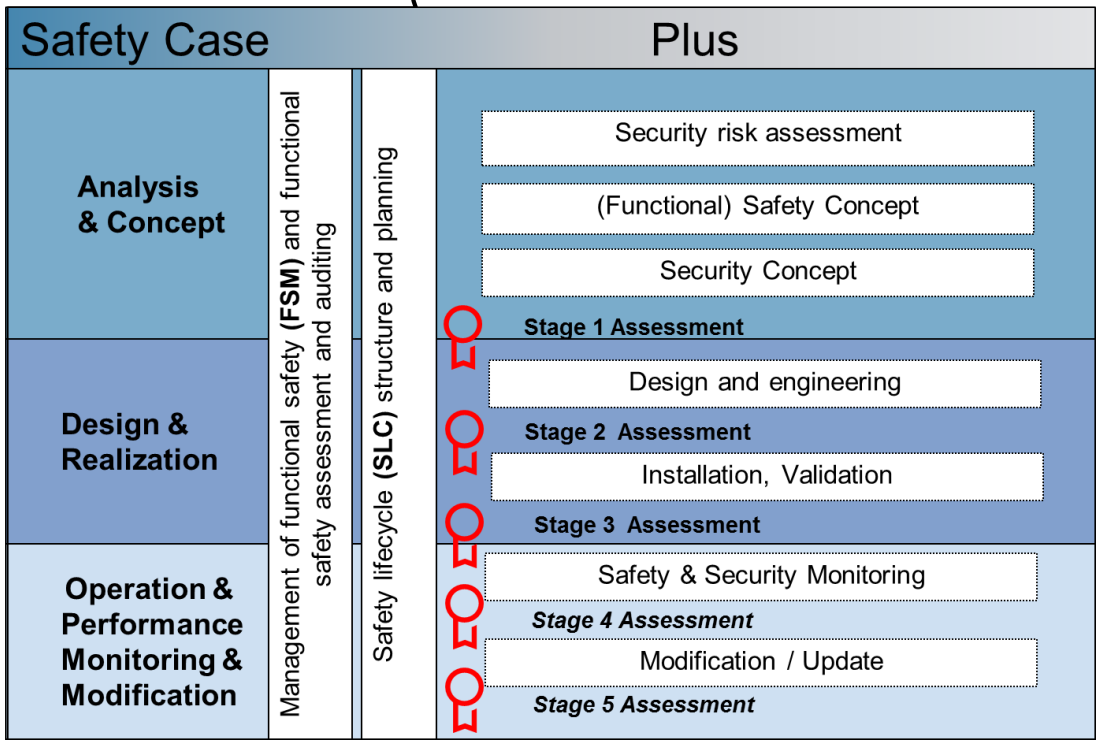
IEC 62443 as aid for Safety Case compliance

	Cyber Safety	
Safety Case Requirements	**IEC 62443**	IEC 61511
Management of security as risk based approach	CSMS	FSM
Implement a lifecycle approach	Sec-LC	SLC
Identification of (major) hazard / risks; scenarios, triggers and probability; assessment of the severity of the consequences	Risk Assessment	PH&RA
Implement measures of protection and intervention to limit the consequences	Risk Mitigation Ctrl	SIS / SIF
Implement measure to monitor the “safety performance”	Sec Performance	FSM
Update / modify depending on lessons learned	CSMS	FSM

Safety Case Plus in context of IEC 61511

Summary

- SIS play a significant role in overall risk reduction framework
- IEC 61511 requires a (safety) managed lifecycle framework
- Thus compliant SIS will provide assurance that Safety Case requirements are met
- The whole lifecycle needs controls (assessments) and management, as integral part of a safety management system,
- Keeping records throughout the entire lifecycle is essential for maintaining and demonstrating integrity



! IEC 61511 has become the established good practice for Functional Safety and sets the foundational requirements for Cyber Security, all based on a lifecycle approach → Safety Case Plus covers all these aspects, including Cyber Safety

Thank you

Questions?

Safety Case Symposium 2018
Singapore
www.SafetyCaseSymposium.com