Chapter 2.
Concepts and Requirements

Mary Ann Lundteigen Marvin Rausand

RAMS Group
Department of Mechanical and Industrial Engineering
NTNU

(Version 0.1)

NTNU – Trondheim
Norwegian University of
Science and Technology

Learning objectives

Key learning objectives from this chapter are to become familar with:

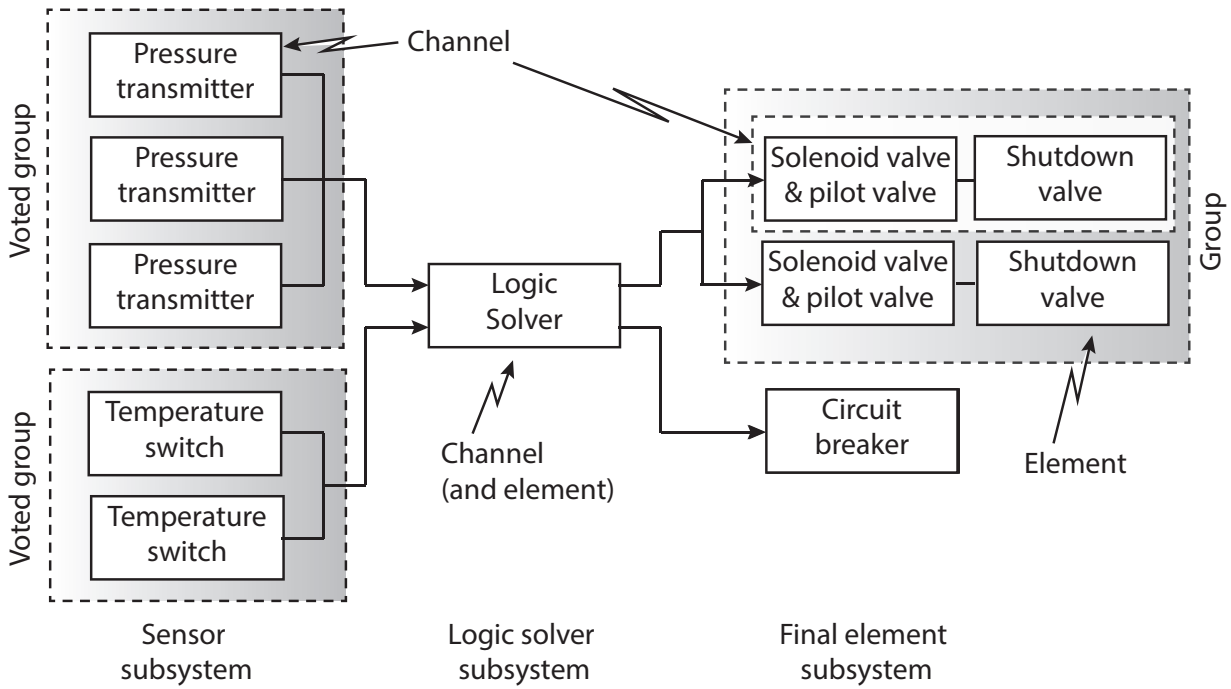
- Key terms and definitions
- The role of SIS in risk analysis
- The application of safety integrity level (SIL) as a measure of SIS performance
- Probabilistic measures used for SIS performance, such as PFD and PFH
- The safety lifecycle and its main phases

The slides build on Chapter 2 in **Reliability of Safety-Critical Systems: Theory and Applications**. DOI:10.1002/9781118776353.

Outline of Presentation

Subsystems, Groups, Channels, and Elements

The IEC 61508 standard distinguishes between *subsystem*, *groups*, *channel*, and *elements*. These terms are not used consistently in the IEC standards. In this chapter, the terms are defined as follows:



Redundancy

Redundancy is an important means to improve the reliability of SIS.

☞ Redundancy: The presence of more than one element to carry out the same function.

Redundancy ...

- ...provides *fault tolerance*
- ... increases the reliability
- ...adds complexity (that must be balanced against the benefits)

Redundancy may be classified as follows:

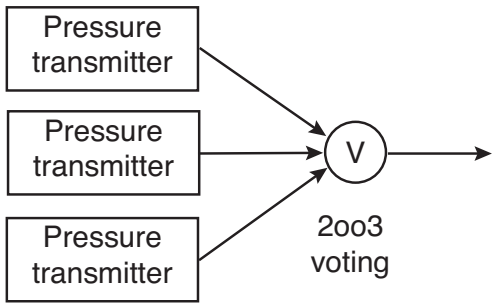
- Active redundancy
- Standby redundancy
- Hardware redundancy
- Software redundancy

Voting

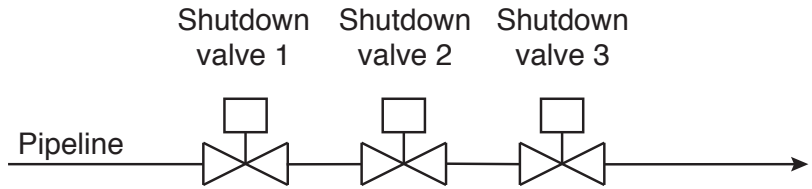
Voting specifies the impact of redundancy on the fault tolerance.

☞ *koon* voted structure: A structure of elements that is functioning when *k*-out-of-*n* channels are functioning, and which fails when (n-k+1) or more of its elements fail.

A 2oo3 structure of sensors:



A 1oo3 structure of valves:



Hardware Fault Tolerance

☞ Hardware fault tolerance (HFT): The ability of a subsystem to continue to perform a required function in the presence of hardware faults or errors.

HFT is given as digit numbers, as 1, 2, etc and calculated on the basis of voting.

Voting	HFT	Voting	HFT
1oo1	0	1oo$n$	n-1
1oo2	1	$k$oo$n$	n-k
1oo3	2		
2oo2	0		
2oo3	1		

Functional Safety Requirements

It does not help to add redundancy and highly reliable components if the **required safety functions have not been specified**...

☞ Functional safety requirements: The specified safety functions which are required to (i) ensure correct performance, i.e. to response adequately to the demand, and (ii) correct performance upon fault conditions.

Some aspects to consider:

- Response time (e.g. time available for responding before safety is lost)
- Range of conditions that represent demand (e.g. pressure range)
- Fault conditions to consider (e.g. loss of power, diagnostics alarms, wrong range of signal)

Safety Integrity Level (SIL)

In addition to having specified the required functional safety requirements, it is necessary to specify **how reliable the functions must be**.

IEC 61508 has introduced **safety integrity** and **safety integrity level (SIL)** as the two main measures of reliability. On the following slides, we will discuss:

- What do we mean by safety integrity?
- How do we distinguish safety integrity levels (SIL)?
- What does SIL imply for SIS?
- What is the difference between *the required* SIL, *the claimed* SIL, and *the achieved* SIL?

Definition of safety integrity

Safety integrity is a measure of reliability performance with respect to safety.

☞ Safety integrity: Probability of a SIS satisfactorily performing the specified SIF under all the stated conditions within a stated period of time.

[Adopted from IEC 61508]

Safety integrity can be interpreted as:

- **A measure of confidence** used in relation to a specific SIF: How much can we trust the safety function when needed?
- **A way to frame SIS design and use**: How should we design hardware devices, prepare test and validate software, and carry out design processes, installation, testing, and operation and maintenance?

Safety integrity levels (SIL)

Safety integrity is divided into four discrete *safety integrity levels* og SIL:

SIL	Description	Remark
SIL 1	The lowest level that is allowed while being defined as a safety-critical system.	Typical for process shutdown functions
SIL 2	The level that can be regarded as medium level.	Typical for process shutdown functions.
SIL 3	The highest SIL level used for low-demand systems in process industry sector and for machinery.	Applies to last in line protection functions, such as isolation of oil wells and protection against overpressurization of pipelines.
SIL 4	The highest SIL level. If used, it is often for high-demand/continously operated functions.	Railway signaling systems often have a SIL 4 requirement for critical functions

Remark: Process industry sector has adapted similar concept for assets protection (AIL) and environmental protection (EIL). Automotive sector applies what is called automotive SIL (ASIL), and distinguish between four levels: ASIL A, ASIL B, ASIL C, and ASIL D.

SIL and failure target measures

IEC 61508 standard suggests the following relationship between reliability measures for random hardware failures and SIL.

SIL	**PFD**$_{\text{avg}}$	**PFH** (per hour)
SIL 4	10^{-5} to 10^{-4}	10^{-9} to 10^{-8}
SIL 3	10^{-4} to 10^{-3}	10^{-8} to 10^{-7}
SIL 2	10^{-3} to 10^{-2}	10^{-7} to 10^{-6}
SIL 1	10^{-2} to 10^{-1}	10^{-6} to 10^{-5}

- PFD$_{avg}$: Average probability of failure on demand (due to dangerous failures)
- PFH: Average probability of having a dangerous failure per hour (or more precisely, failure frequency of dangerous failures)

Example: What does a SIL 2 requirement imply?

Assume that a SIF has a SIL 2 requirement.

SIL	**PFD**$_{\text{avg}}$	**PFH** (per hour)
SIL 4	10^{-5} to 10^{-4}	10^{-9} to 10^{-8}
SIL 3	10^{-4} to 10^{-3}	10^{-8} to 10^{-7}
SIL 2	10^{-3} to 10^{-2}	10^{-7} to 10^{-6}
SIL 1	10^{-2} to 10^{-1}	10^{-6} to 10^{-5}

- If operating in the low-demand, the SIF shall fail less often than once every 100 trials (demands or tests)
- If operating in the high-demand, the SIF shall fail less often than once per 100 years[1]

[1] Here, we assume for simplicity that 1 year $\approx$ 10 000 hours

Required SIL vs Claimed and Achieved SIL

It is important to note that SIL means different things depending on the context:

- **Required SIL ("SIL requirement"):** The SIL level that is required for a SIF on the basis of the risk analysis.
- **Claimed SIL:** The SIL that can be claimed or predicted for a specific SIF on the basis of design and results from analyses, checks, and tests *before* the system is installed.
- **Achieved (or actual/experienced) SIL:** The SIL that is claimed based on operational experience and failure reporting.

Safety lifecycle

The safety life cycle outlines a **sequential pathway** from initiation of a new system till it is installed and eventually removed.

☞ *Safety lifecycle.* An engineering process designed to manage the design and operation of safety-critical systems, in light of requirements in standards like IEC 61508 [Slightly modified version of definition from the textbook].

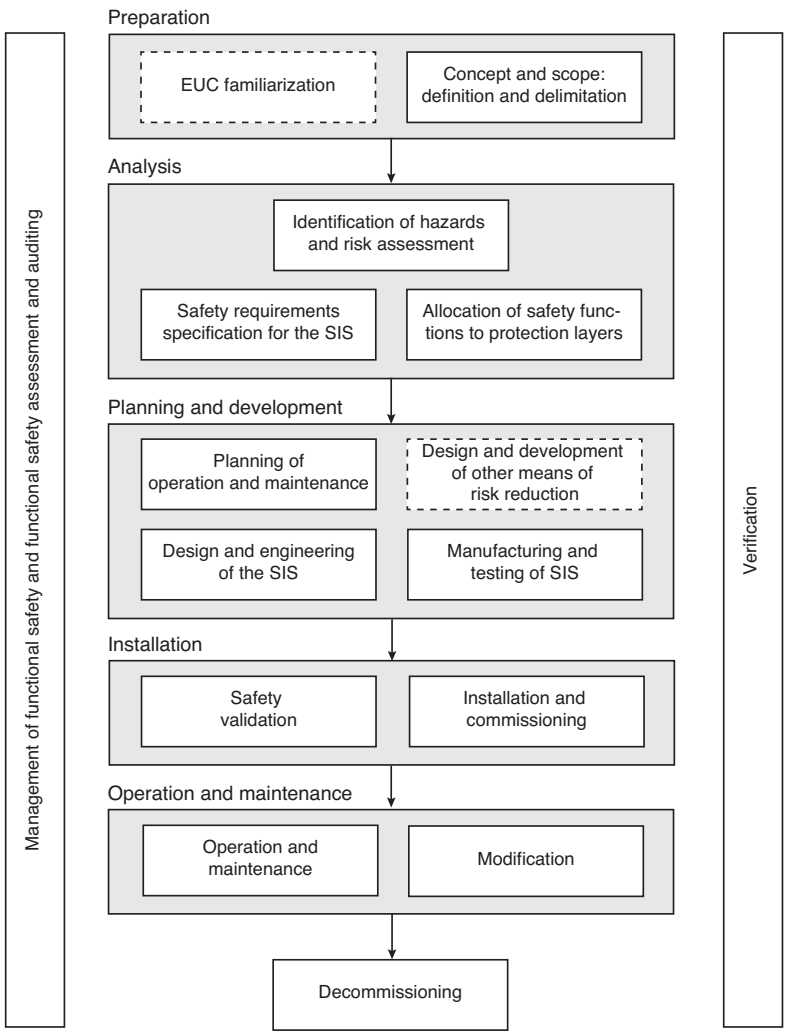
Safety lifecycle phases

IEC 61508 suggests the following life cycle phases to achieve the desired level of functional safety:

- Preparation (familiarization)
- Analysis (risk assessment and overall design specification)
- Implementation (realization of SIS, based on design specification)
- Operation (follow-up of SIS, including maintenance, modifications and eventually decommissioning)

Parallel phases:

- Planning, auditing, verification, and validation,++



Analysis Phases

The purpose of the analysis phases is to identify the needs for safety instrumented functions (SIFs), and how reliable they must be in order meet the given risk acceptance criteria.

Typical analyses and activities:

- Hazards and risk analyses: Identify the need for SIFs and the overall need for risk reduction
- SIL allocation:Allocation of functional safety requirements and overall risk reduction down to individual SIFs:
  - Layers of protection analysis (LOPA), mainly used in process industry
  - Risk graph (used many sectors)
  - Risk table (used in many sectors)
  - Minimum SIL requirements (Norwegian petroleum industry)
- Prepare of “first version” of safety requirement specification (SRS)
- Carry out audits, such as functional safety assessment (FSA)

Planning and Development Phases

The purpose of the planning and development phases is to build SIS according to SRS and to demonstrate and document compliance to requirements.

Planning and development phases include:

- Placing purchase orders and requesting compliance documentation such as SIlL certifications, safety analysis report (SAR) or safety manual from manufacturers)
- Developing/building hardware and software system architecture
- Application (software) program development
- Development of compliance reports
- Preparation of installation, commissioning, and site acceptance testing as preparation
- Preparation of and participation in factory acceptance tests, reporting and follow-up
- Preparation of all documentation and procedures for use in operation, maintenance, and management of modifications.
- Conducting audits, such as functional safety assessment (FSA)
- Training of people to be involved in operation and maintenance

Installation Phase

The purpose of the installation phases is to install SIS and demonstrate and document compliance to requirements.

Implementation phases include:

- Conducing installation and commissioning of all SIS-related systems according to specified procedures
- Carrying out reporting, tracking, and resolution of non-conformities
- Final preparation of all documentation and procedures for use in operation, maintenance, and management of modifications.
- Preparation of and conducting site acceptance test

Operation and Maintenance Phase

The purpose of the operation and maintenance phases is maintain compliance to requirements in SRS over the whole use life, typically 10-20 years

Typical activities in the operational phase are:

- Testing, and reporting and correction of failures
- Replacements of equipment as needed
- Management of bypasses/inhibits
- Analysis and verification of any modifications initiated due to (i) lack of adequate performance (SIL or otherwise), (ii) changes in operational or environmental conditions, (iii) new tie-ins/expansions of existing systems, including SIS.

SIL and Safety Lifecycle

Analysis phase:

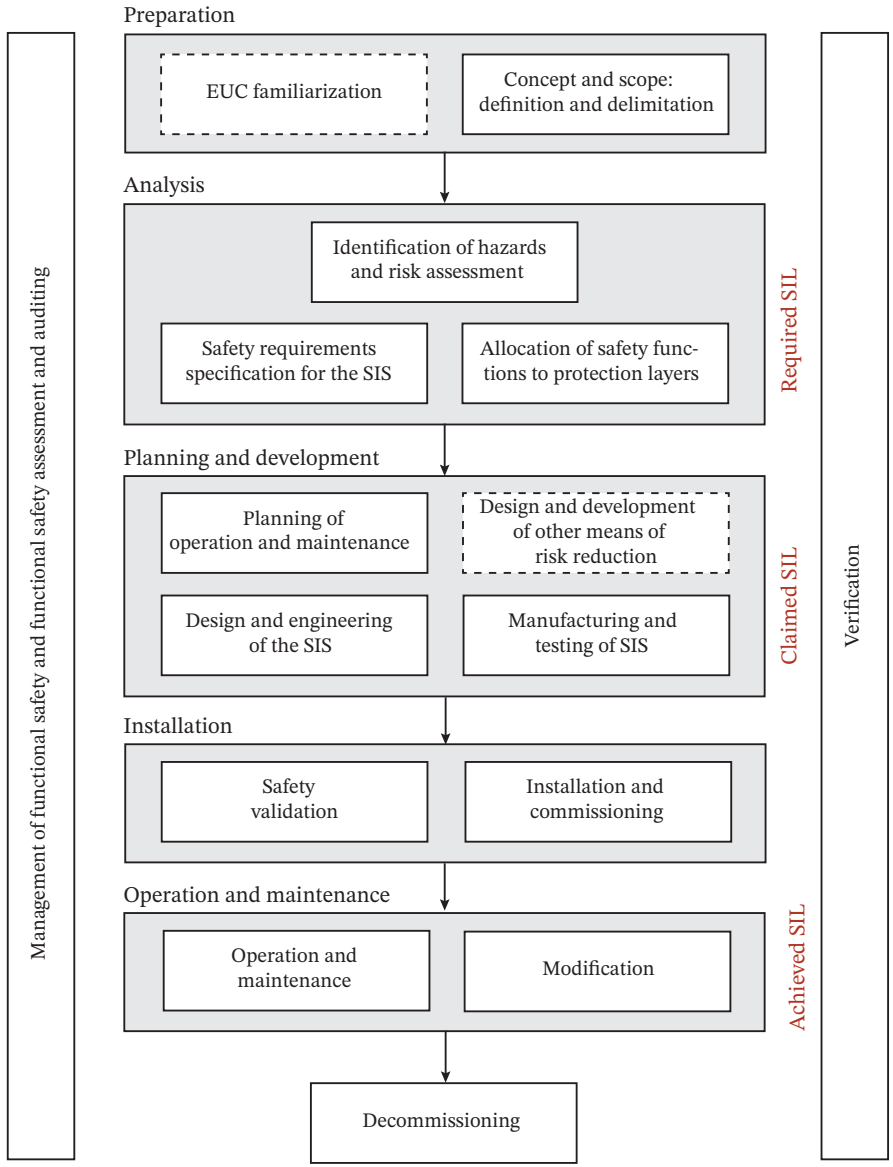
- Focuses on the specification of functional safety and the **required SIL**

Planning and development phase:

- Focuses on the demonstration of functional safety requirements and the **claimed SIL**

Operation and maintenance phase:

- Focuses on the demonstration of of functional safety requirements and the **achieved SIL**



Management of Functional Safety

Management of functional safety is a term used to cover everything you need to plan for and do according to requirements in the functional safety standards.

Typical management activities cover:

- Setting up plans, with all tasks as mandated by e.g. IEC 61508. Plans may be prepared to design phase, for installation phase, for operation phase etc.
- Keeping track of competence requirements and training needs of personnel
- Keeping procedures updated
- Carrying out audits and other assessments at regular intervals to verify compliance to regulatory and key standard requirements

All involved in SIS design and operation must have their own management of functional safety plans. This means:

- Manufacturers of safety products
- Engineering companies, building systems based on safety products
- End user, giving the premises for and being responsible for operation, maintenance and modifications

Safety Lifecycle

The safety lifecycle "means different things" for a manufacturer compared to an engineering company and end user

Manufacturer focuses on:

- Planning and development of new products for safety applications
- Collection of field experience from worldwide installations (based on reported failures, warranty claims, products received in workshop) to build own databases for reliability data

Engineering company focuses on:

- The integration of products for a particular application area and installation
- Taking responsibility for preparation, analysis, planning and development and installation phases on behalf of client (end user)

End user focuses on:

- The overall responsibility for all phases of their planned and existing SIS
- Initiation and giving premises for preparation phase for new SIS
- Operation, maintenance, and management of modifications, a set of tasks that will last for many years.
- Training of personnel involved in SIS-related work

How to Design According to SIL Requirement

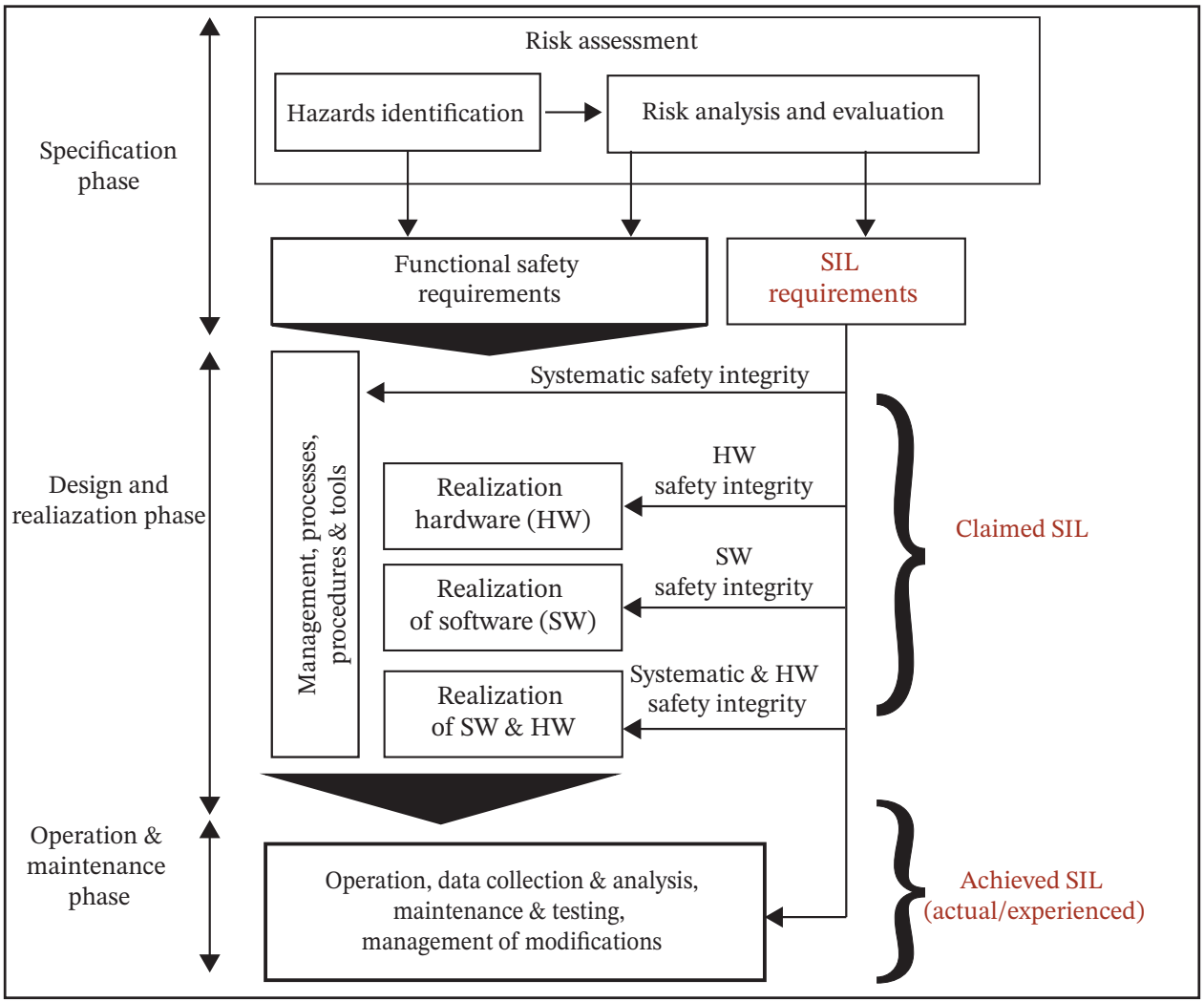
A SIL requirement is broken down into three main sub-categories of requirements:

- Hardware safety integrity ("HSIL")
- Software safety integrity ("SoftSIL")
- Systematic safety integrity ("SystSIL")

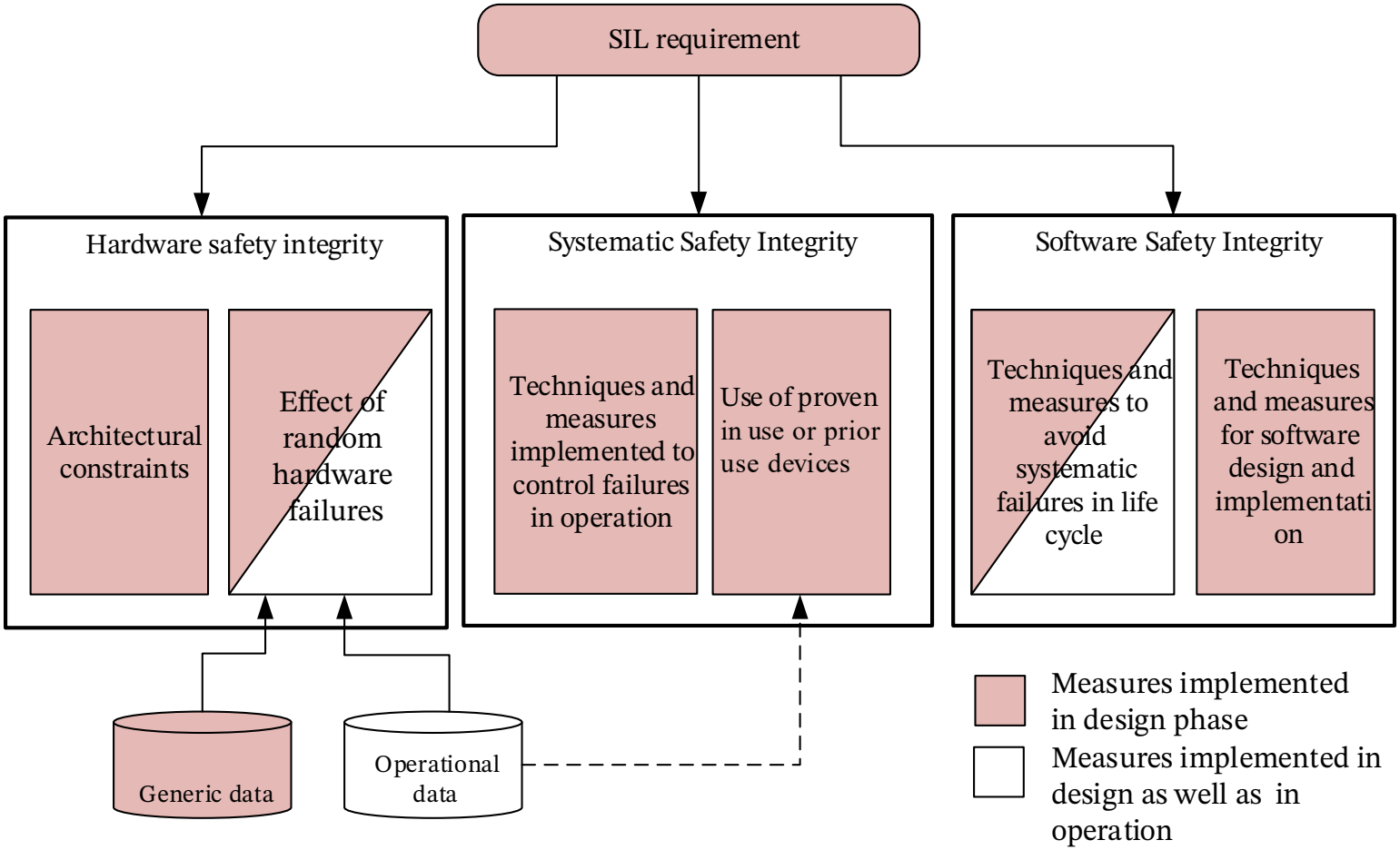
The design processes focuses on demonstrating compliance to these set of requirements.

Requirements from all three categories must be fulfilled (at the level assigned by SIL) in order to claim a SIL level ("No chain is stronger than the weakest link").

Required/Claimed/Achieved SIL (detailed)



Implications of SIL requirement



Hardware Safety Integrity

☞ Hardware safety integrity: Part of the safety integrity of a safety-related system relating to random hardware failures in a dangerous mode of failure

[IEC 61508]

Hardware safety integrity requirements are split into two parts:

- Demonstrating by probabilistic calculations that the failure measure (PFD or PFH) is within the specified SIL range
- Demonstrating that the design has been selected according to the requirements for architectural constraints

Software safety Integrity

☞ Software safety integrity: Part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure that are attributable to software

[IEC 61508]

Ensuring adequate software safety integrity level include selection of suitable techniques in checklists for:

- Software specification (e.g. formal or semi-formal methods, computer-aided specification tools)
- Sofware design and development technques (e.g. Modular approach, fault detection, graceful degradation, choice of compilator)
- Programming language (e.g. full variability language, limited variability language)
- Testing and integration (e.g. probabilistic testing, model-based testing, formal verification, static or dynamic testing)

Fulfilment of requirements associated with software safety integrity requires competence in programming and programming tools.

Systematic safety Integrity

☞ Systematic safety integrity: Part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure

[IEC 61508]

Ensuring adequate systematic safety integrity level include selection of suitable techniques in checklists for:

- Detect hardware faults (e.g. program sequence monitoring, diagnostics, code protection)
- Avoid influence from environmental stresses or influences (e.g. separation, monitoring of temperatures, vibration, etc)
- Prevent introducing errors in operation (e.g. modification protection)
- Avoid introducing mistakes in specification (e.g. having proper project management, use of semi-formal methods, checklists, computer-aided specification tools)
- Avoid introducting mistakes during integration and testing
- Avoid introducing mistakes during operation and maintenance (user friendliness, documentation, using skilled operators)

Some of the measures seem rather obvious, while other measures must be evaluated in light of its context and use.

Why SIL?

Why introducing SIL and not just specifying a reliability target?

Reliability measures (like PFD and PFH) mainly covers hardware aspects, which is not sufficient for a software intensive system...

However, the reliability of SIS is influenced by several factors such as:

- Errors in the functional specifications
- Random hardware failure rates
- Programming errors
- Other errors and faults introduced during design, installation, operation, and maintenance errors

SIL requirements give rules, restrictions, and guidance that ensure the neglibible impact of non-random failure causes.