Extension to Chapter 2. Architectural Constraints

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

The main learning objectives associated with these slides are to:

- To become familiar with motivation for having requirements about architectural design
- To become familiar with key concepts in relation to architectural constraints
- Be able to use the rules for architectural constraints in IEC 61508
- Be able to identify some pros and cons of applying architectural constraints

The slides provide additional information on some selected topics in Chapter 2 in **Reliability of Safety-Critical Systems: Theory and Applications**. DOI:10.1002/9781118776353.

Outline of Presentation

Safety Integrity

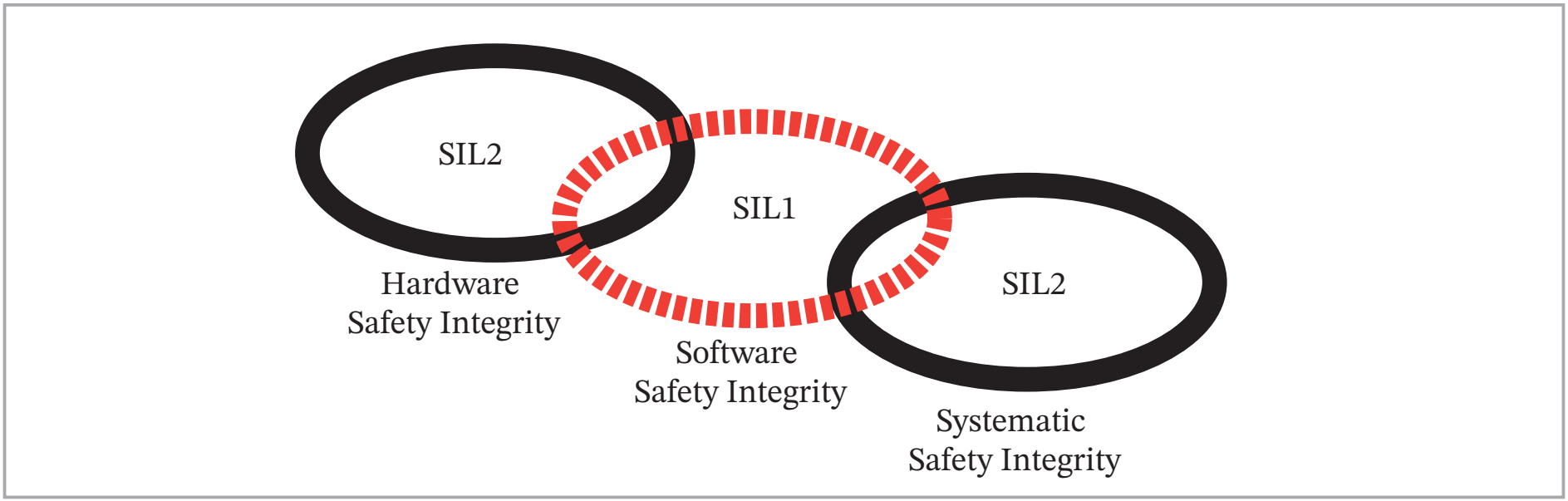
Recall that safety integrity (and associated SIL requirements) is split into three categories:

- Hardware safety integrity, which relates to the safety integrity after having considered system architecture and failure probability due to physical degradation.
- Systematic safety integrity, which relates to the safety integrity achieved after having considered measures to avoid and control mistakes in design, installation, and use.
- Software safety integrity, which relates to the safety integrity achieved by having adapted restrictions for application programming methods, tools, and associated procedures.

A system cannot meet a SIL requirement without fulfilling requirements associted with **ALL THREE** categories.

Weakest Link Principle

That the system cannot meet a SIL requirement without fulfilling requirements associted with **ALL THREE** categories can be seen as the weakest link principle.



In the model above, we see that the SIF or the product can only claim SIL 1, since software safety integrity is demonstrated for this level only.

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]

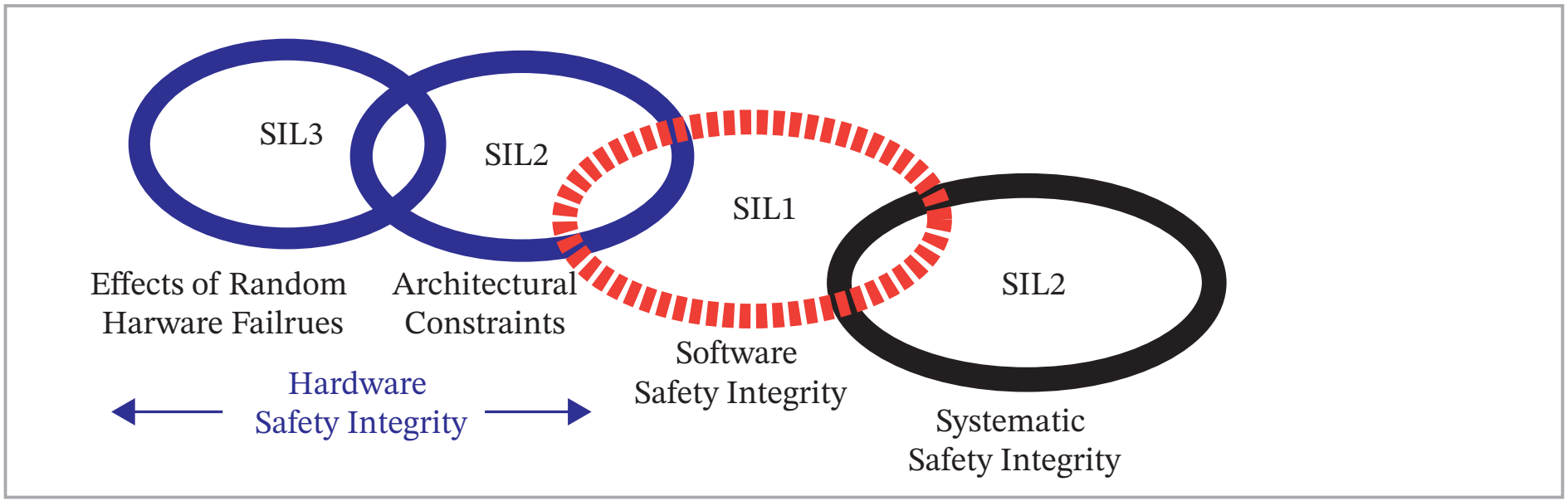
Hardware safety integrity requirements are split into two parts:

- Demonstrating that the target failure measure (PFD or PFH) is within the specified range of the SIL requirement
- Demonstrating that the hardware is configured according to thearchitectural constraints

BOTH need to be demonstrated to fulfil a SIL requirement with respect to hardware safety integrity. The weakest link principle applies here as well.

Weakest Link Principle

The weakest link principle applies also to hardware safety integrity. Even if the effects of random hardware failures (as PFD or PFH) indicate SIL 3, the hardware safety integrity is limited to SIL 2 due to the architectural constraints complying to SIL 2.



What is Architectural Constraints

Architectural constraints is about:

- **Limiting the freedom** in selecting hardware configuration in light of the SIL requirement and properties of the involved components.

The purpose of these constraints is to avoid that **overly optimistic values of PFD or PFH** are used as arguments for selecting too simplistic architectures.

There are two routes (or options) for how to determine the architectural constraints in IEC 61508:

- Route 1_H.
- Route 2_H.

A variant of these routes has been adapted by IEC 61511 for use in process industry sector. We will first focus on route 1_H.

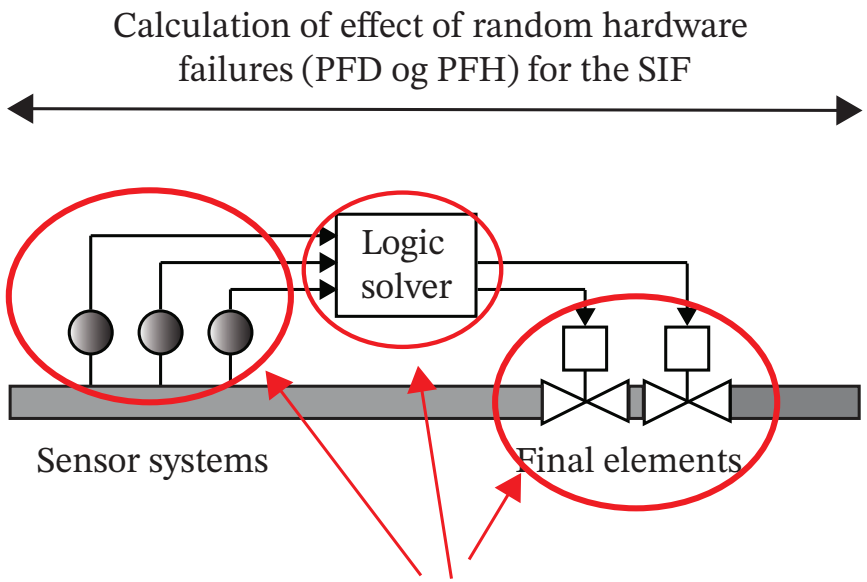
Important Parameters)

There are three important parameters to consider:

- Minimum hardware fault tolerance (minimum HFT)
- Category A and B
- Safe failure fraction (SFF)

Application of Archtectural Constraints

Architectural constraints are applied at the subsystem level, one by one, so that in the end the whole SIF is covered.



Minimum HFT

Recall the definition of HFT:

☞ Hardware fault tolerance (HFT): Number of dangerous failures tolerated before the sub-system looses its safety function.

HFT for a $koon$ voted system is equal to $n - k$. A 2oo4 voted system tolerates 2 dangerous failures so that HFT = 2.

The minimum HFT specifies (as the name reads) the minimum of what is acceptable in light of the SIL requirement.

☞ Minimum HFT: The HFT mandated by the architectural constraints in light of the SIL requirement

Safe Failure Fraction (SFF)

Safe failure fraction (SFF) is a measure of how safe the component respond in the presence of faults.

☞ Safe failure fraction (SFF):

$$\text{SFF} = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}}$$

Notations: λ is the failure rate, and the subscripts give the failure category: S for safe, DU for dangerous undetected, and DD for dangerous detected.

The SFF has two interpretations:

1. The fraction of all failures that are "safe", meaning that they are either safe per definition in IEC 61508 or dangerous detected (DD).
2. The probability that a failure is "safe", given that a failure has occured.

Type A and Type B

Type A or type B are two categories used to distinguish proven/low-compexity components from unproven/more complex components

An component is classified as **type A** if **ALL** the following criteria are fulfilled:

1. Failure modes of the element (and all its constituent components) are well defined
2. The behavior of the element under fault conditions can be completely determined
3. There is sufficient dependable failure data to show that the claimed rates of failure for DD and DU failures are met

An element is **type B** if one or more of the above criteria are not met.

Discussion of Classification

In what category would you place:

- A shutdown valve?
- A solenoid valve?
- A pressure transmitter
- A push button?
- A circuit braker?
- A logic solver?

Explain why.

Route 1H and 2H

There are two routes or options to how architectural constraints are applied:

- Route 1_H:
  Determining minimum HFT with SFF
  This route is explained in more detail on the following slides.
- Route 2_H:
  Determining minimum HFT without SFF.
  This route can only be applied when extensive field data is available. The approach does not allow only point-values for PFD or PFH, but requires also that the confidence level is determined.

Route 1_H is focused in this presentation.

Route 1_H

Route 1_H defines the minimum HFT with basis in the:

- The SIL requirement
- The *safe failure fraction* (SFF) of subsystem component(s)/elements.
- The component category, type A or type B, defined on the basis of system complexity and maturity

It is assumed first that each subsystem with redundancy has identifical components.

Route 1_H

The following minimum HFT-SFF-SIL relationship is proposed for subsystems of identifical components:

	minimum HFT with type A			minimum HFT with type B		
SFF	0	1	2	0	1	2
<60%	SIL1	SIL2	SIL3	-	SIL1	SIL2
≥60%, <90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
≥90%, <99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

Example

A smart sensor is often classified as type B. Assume that the SFF has been calculated to 85%. If a SIL 2 requirement is specified, it is necessary to select an architecture with minimum HFT of 1. This could be a 1oo2 architecture or a 2oo3.

What if Non-Identical Components?

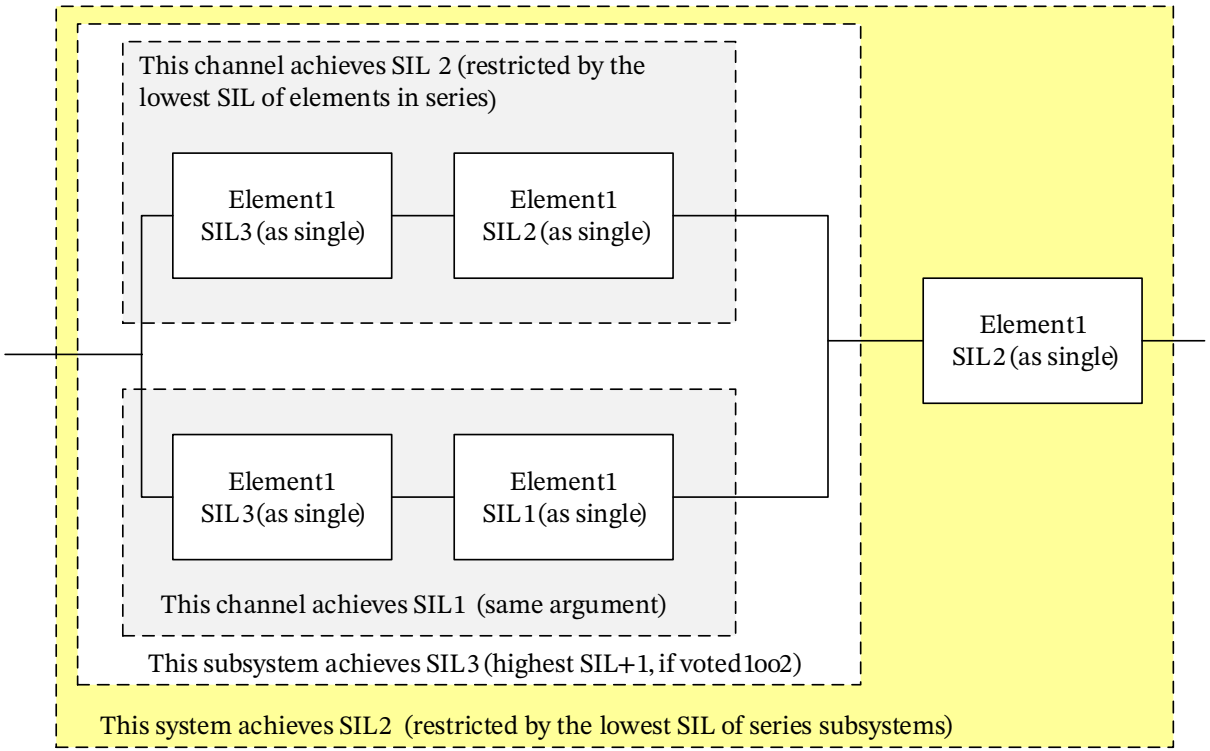
The HFT table cannot be used directly if the subsystem consist of non-identical components. In this situation, IEC 61508 suggests the following approach (by us called“merging rules”):

1. Study each channel separately:
   - Decide what SIL to claim for each channel as single, considering the principle of weak links if the channel has more than one component
2. Calculate the SIL level of the subsystem by using “merging rules”:
   - Merging rule: The maximum SIL that can be claimed for at subsystem is determined by the highest SIL level claimed by one of the channels + HFT of the configuration.
3. The ‘’merging rules” are more easily illustrated in a practical example.

*Remark.*The same approach applies to route 2_{H}, but then the SIL-level of each element is determined without the SFF.

Route 1_H

Example of using merging rules



Remark: General rule for redundant channels is highest SIL + X, where X is the HFT of the subsystem.

Critique I

Is the SFF a good measure?

- Is a DD failure "safe" and under what conditions?
- SFF is a relative measure, and it can be problematic to use SFF as a measure for comparing two products

Further reading: See this article:
`http://dx.doi.org/10.1016/j.ress.2008.06.003`

Critique II

On what basis has the minimum HFT-SFF-SIL relationship been established?

- Can such prescriptive rules be a false comfort?
- What would be the alternative(s)?

After all, it seems like architectural constraints is a useful concept as a preservation of best practise rules.