Towards the optimization of the Safety Life-Cycle for Safety Instrumented Systems

(WEBR02)

B. Fernández, G. De Assis, R. Speroni, T. Otto and E. Blanco

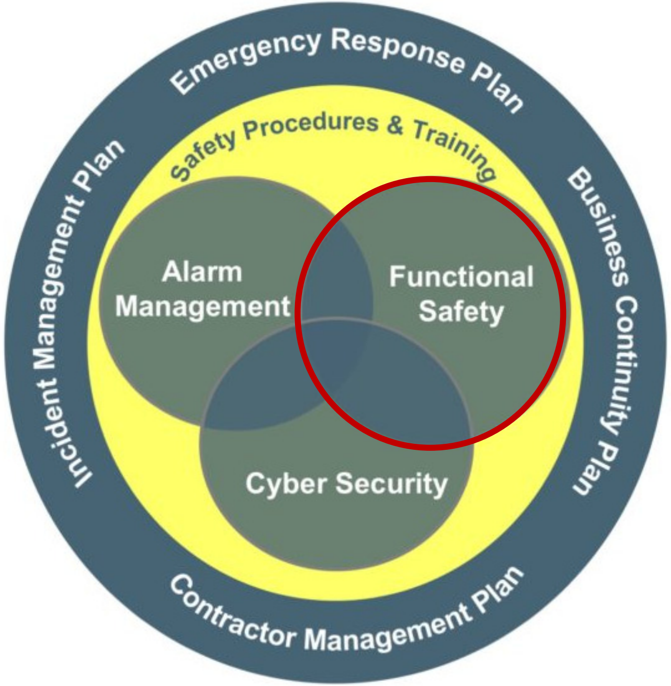
20/10/2021

Context

- The goal is to **ensure safety** in our industrial installations

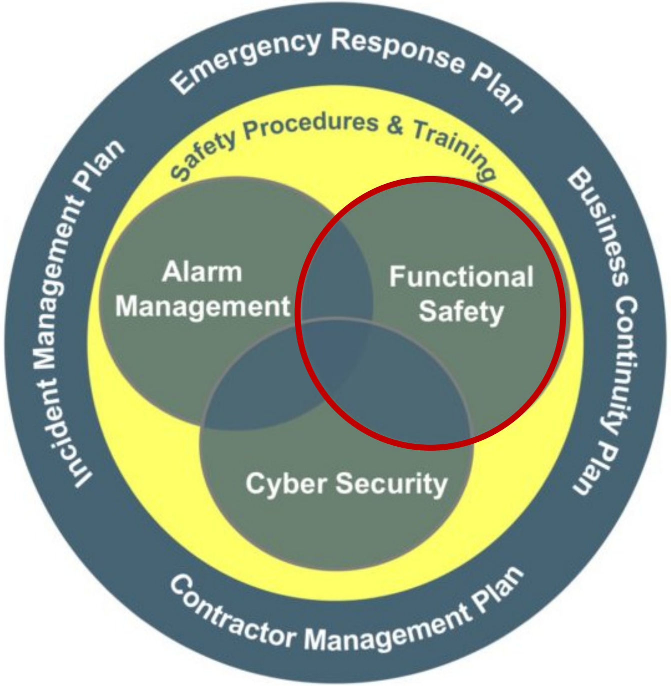
Context

- The goal is to **ensure safety** in our industrial installations
- … by developing **Safety Instrumented Systems (SIS)** based on the **Functional Safety standards**



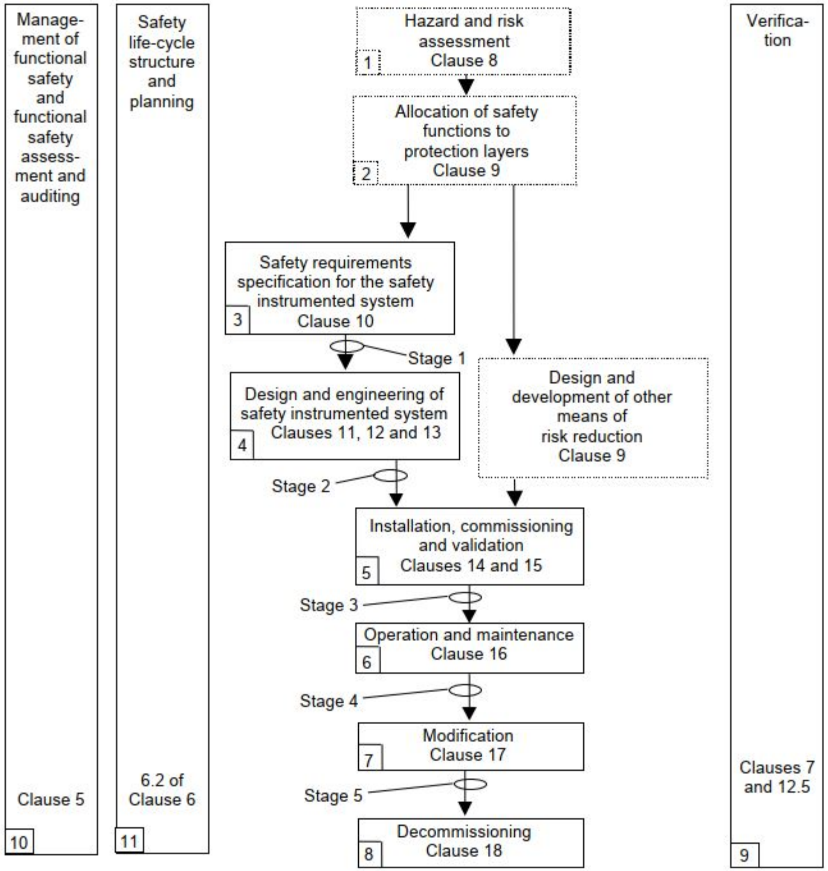
Context

- The goal is to **ensure safety** in our industrial installations
- … by developing **Safety Instrumented Systems (SIS)** based on the **Functional Safety standards**
- **IEC 61511** standard - **SIS** (Safety Instrumented Systems) for the **industrial process sector**



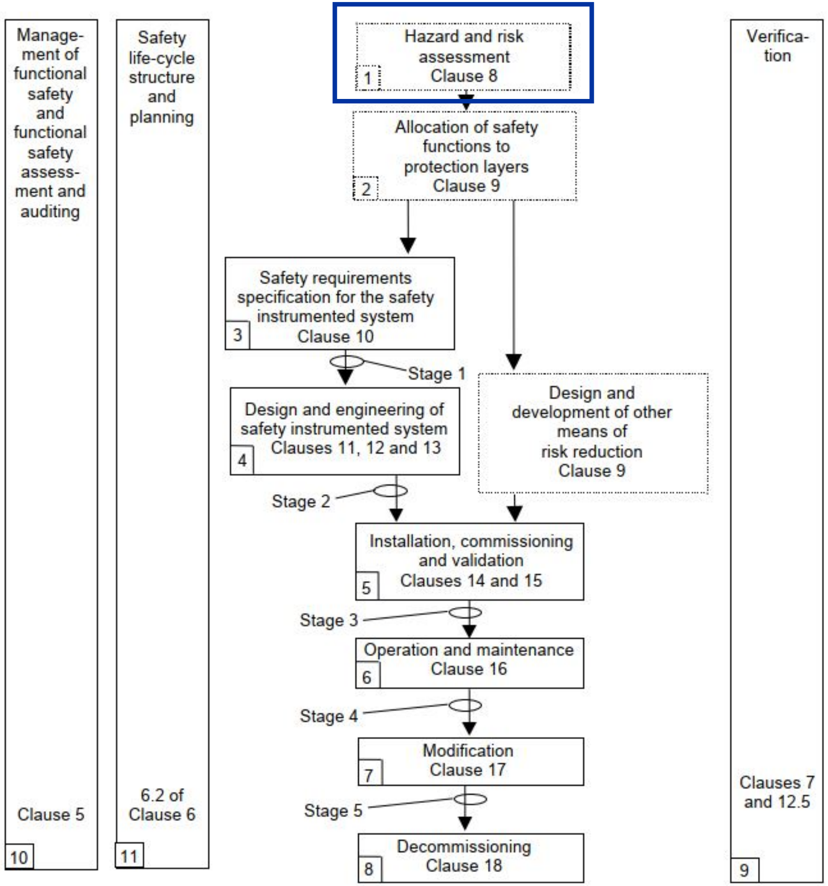
Context

- The goal is to **ensure safety** in our industrial installations
- … by developing **Safety Instrumented Systems (SIS)** based on the **Functional Safety standards**
- **IEC 61511** standard - **SIS** (Safety Instrumented Systems) for the **industrial process sector**
- It provides the **safety life-cycle**:
  - 11 phases (to complete the project)
  - 19 Clauses (**requirements**)



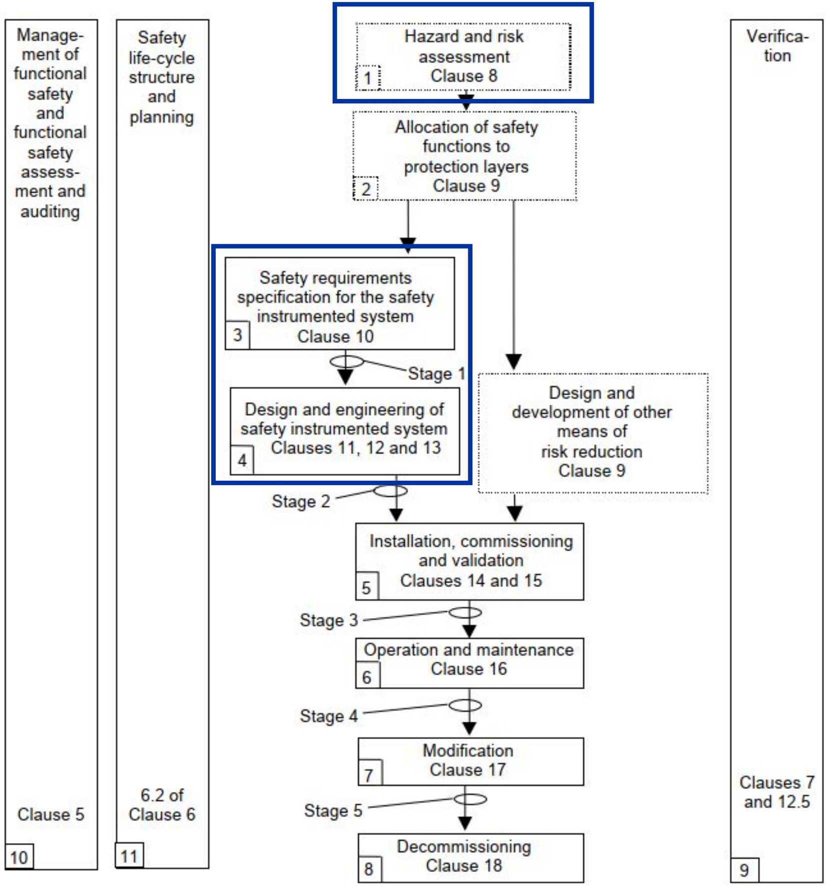
Context

- The goal is to **ensure safety** in our industrial installations
- … by developing **Safety Instrumented Systems (SIS)** based on the **Functional Safety standards**
- **IEC 61511** standard - **SIS** (Safety Instrumented Systems) for the **industrial process sector**
- It provides the **safety life-cycle**:
  - 11 phases (to complete the project)
  - 19 Clauses (**requirements**)



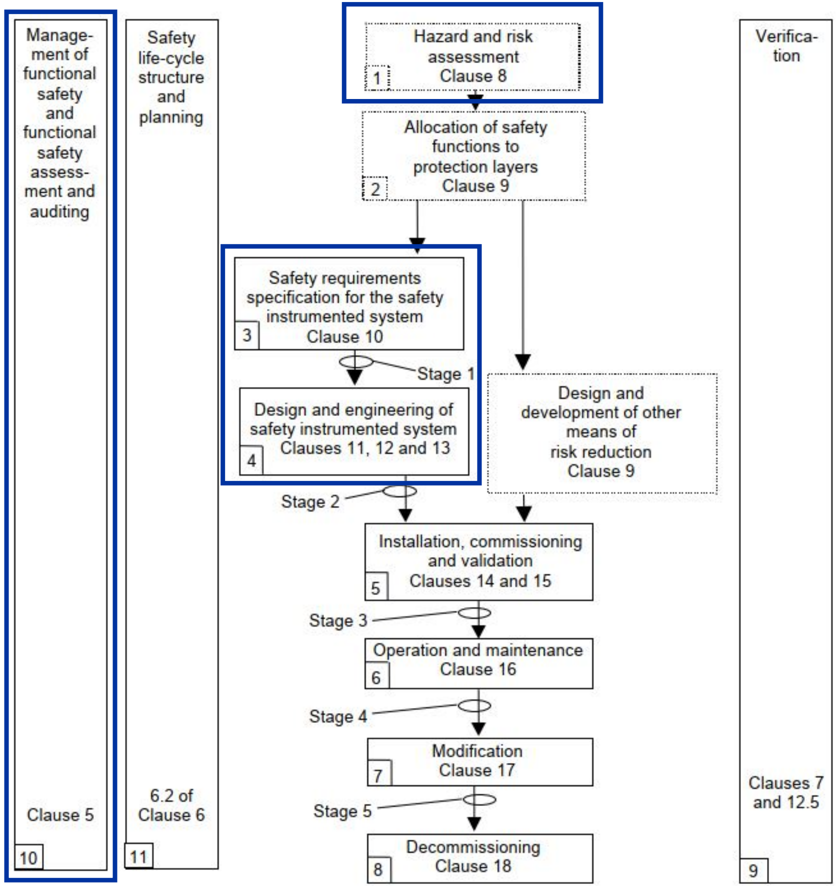
Context

- The goal is to **ensure safety** in our industrial installations
- … by developing **Safety Instrumented Systems (SIS)** based on the **Functional Safety standards**
- **IEC 61511** standard - **SIS** (Safety Instrumented Systems) for the **industrial process sector**
- It provides the **safety life-cycle**:
  - 11 phases (to complete the project)
  - 19 Clauses (**requirements**)



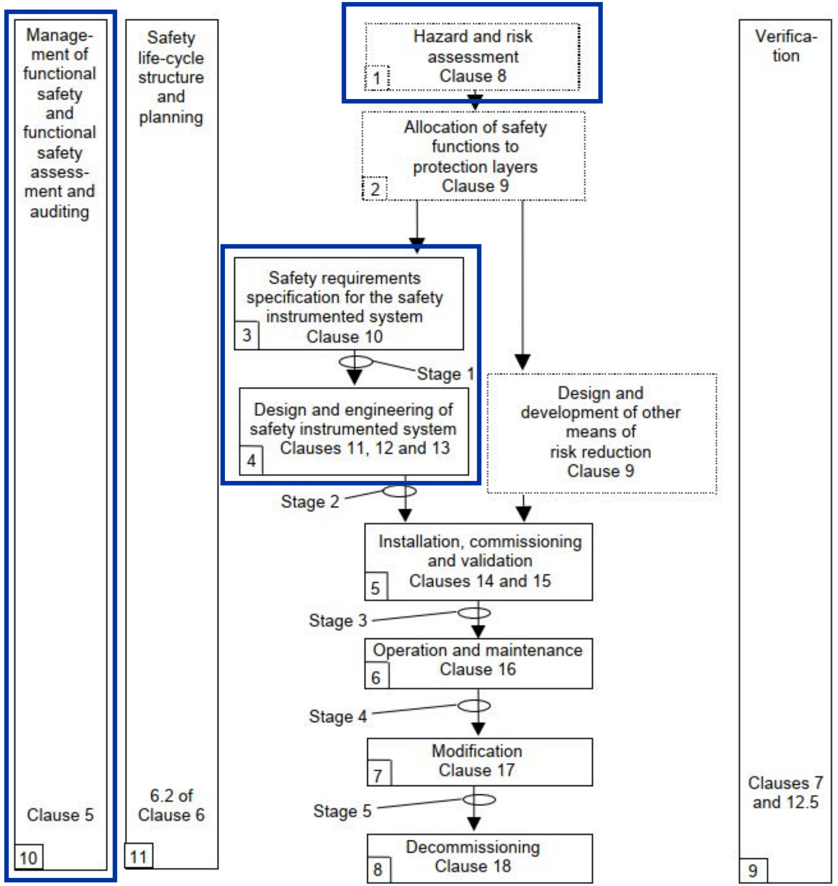
Context

- The goal is to **ensure safety** in our industrial installations
- … by developing **Safety Instrumented Systems (SIS)** based on the **Functional Safety standards**
- **IEC 61511** standard - **SIS** (Safety Instrumented Systems) for the **industrial process sector**
- It provides the **safety life-cycle**:
    - 11 phases (to complete the project)
    - 19 Clauses (**requirements**)



Context

- The goal is to **ensure safety** in our industrial installations
- … by developing **Safety Instrumented Systems (SIS)** based on the **Functional Safety standards**
- **IEC 61511** standard - **SIS** (Safety Instrumented Systems) for the **industrial process sector**
- It provides the **safety life-cycle**:
  - 11 phases (to complete the project)
  - 19 Clauses (**requirements**)
- Very **challenging** task **to implement** all the requirements (lots of resources and time-consuming)



Challenges and objectives

Some major challenges:

Objectives:

Challenges and objectives

Some major challenges:

1. Proving the **compliance with the standard**:
   - **Technical** challenges
   - **Management** challenges

Objectives:

Challenges and objectives

Some major challenges:

1. Proving the **compliance with the standard**:
   - **Technical** challenges
   - **Management** challenges
2. Deal with the **constant evolution** of the particle accelerators and experimental areas

Objectives:

Challenges and objectives

Some major challenges:

1. Proving the **compliance with the standard**:
   - **Technical** challenges
   - **Management** challenges

2. Deal with the **constant evolution** of the particle accelerators and experimental areas

3. Keep the **traceability** between the phases

Objectives:

Challenges and objectives

Some major challenges:

1. Proving the **compliance with the standard**:
   - **Technical** challenges
   - **Management** challenges
2. Deal with the **constant evolution** of the particle accelerators and experimental areas
3. Keep the **traceability** between the phases

Objectives:

1. Ensure safety
2. SIS compliant with the IEC standards

Challenges and objectives

Some major challenges:

1. Proving the **compliance with the standard**:
   - **Technical** challenges
   - **Management** challenges
2. Deal with the **constant evolution** of the particle accelerators and experimental areas
3. Keep the **traceability** between the phases

Objectives:

1. Ensure safety
2. SIS compliant with the IEC standards
3. Find **solutions to optimize the implementation** of the safety life-cycle:
   - Apply the recommended **methods**
   - Integrate existing **tools** to the safety life-cycle
   - Create **report templates**
   - Improve of our **management procedures**

Challenges and objectives

Some major challenges:

1. Proving the **compliance with the standard**:
   - **Technical** challenges
   - **Management** challenges
2. Deal with the **constant evolution** of the particle accelerators and experimental areas
3. Keep the **traceability** between the phases

Objectives:

1. Ensure safety
2. SIS compliant with the IEC standards
3. Find **solutions to optimize the implementation** of the safety life-cycle:
   - Apply the recommended **methods**
   - Integrate existing **tools** to the safety life-cycle
   - Create **report templates**
   - Improve of our **management procedures**

Challenges and objectives

Some major challenges:

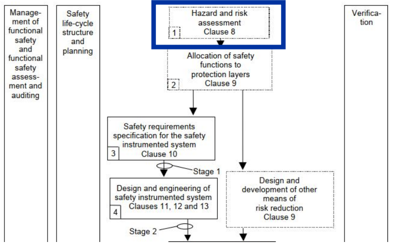
1. Proving the **compliance with the standard**:
   - **Technical** challenges
   - **Management** challenges
2. Deal with the **constant evolution** of the particle accelerators and experimental areas
3. Keep the **traceability** between the phases

Objectives:

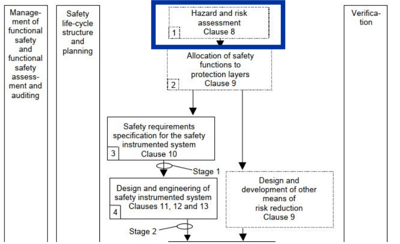
1. Ensure safety
2. SIS compliant with the IEC standards
3. Find **solutions to optimize the implementation** of the safety life-cycle:
   - Apply the recommended **methods**
   - Integrate existing **tools** to the safety life-cycle
   - Create **report templates**
   - Improve of our **management procedures**

This paper analyses **some** of the most challenging **phases (1, 3, 4 and 10)** and presents the **adopted solutions**

Phase 1 - Hazard and risk assessment

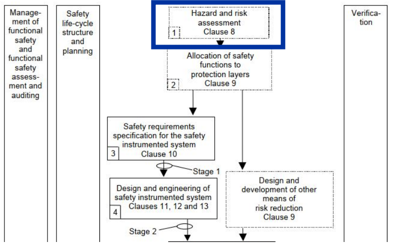


Phase 1 - Hazard and risk assessment



Identify the hazards, the risks and **evaluate** the necessary **risk reduction - Target Safety Integrity Level (SIL)**

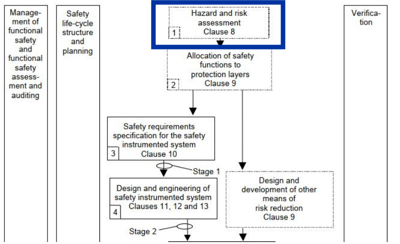
Phase 1 - Hazard and risk assessment



Identify the hazards, the risks and **evaluate** the necessary **risk reduction - Target Safety Integrity Level (SIL)**

FMEA (Failure Mode and Effect Analysis)

Subsystem	Failure Mode	Effects	Causes	Current mitigation measures
Water-cooled system	High temperature	Melting insulation, short circuit and electrocution	Water leak	None



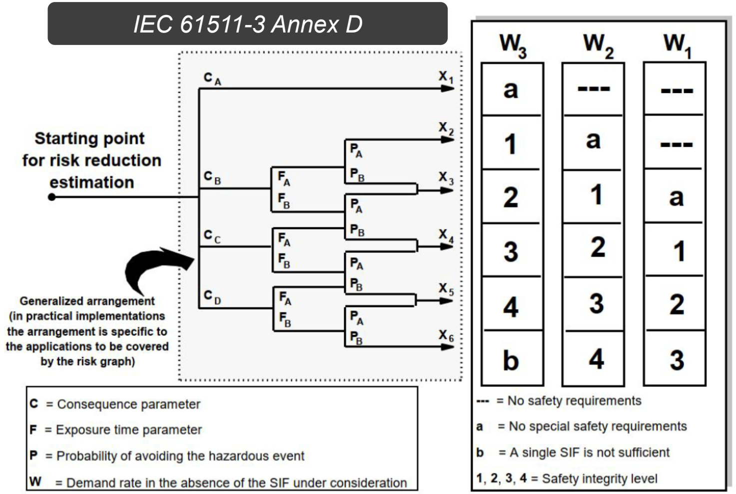
Phase 1 - Hazard and risk assessment

Identify the hazards, the risks and **evaluate** the necessary **risk reduction - Target Safety Integrity Level (SIL)**

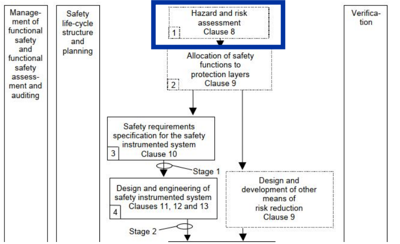
FMEA (Failure Mode and Effect Analysis)

Subsystem	Failure Mode	Effects	Causes	Current mitigation measures
Water-cooled system	High temperature	Melting insulation, short circuit and electrocution	Water leak	None

Calibrated risk graph method for each failure mode



Phase 1 - Hazard and risk assessment



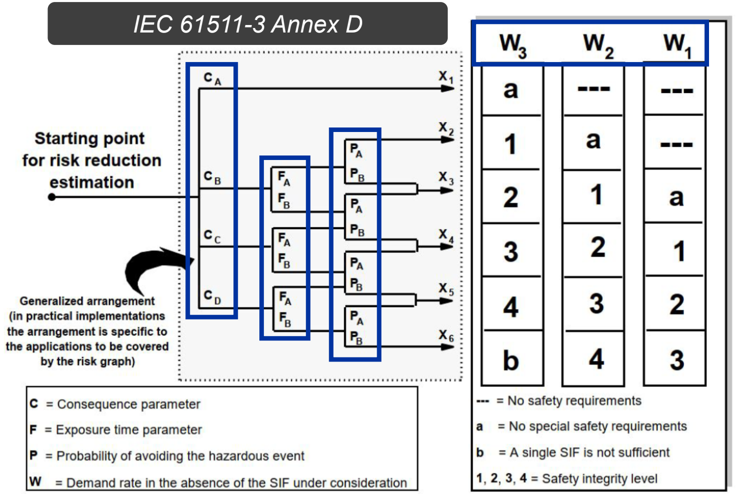
Identify the hazards, the risks and **evaluate** the necessary **risk reduction - Target Safety Integrity Level (SIL)**

FMEA (Failure Mode and Effect Analysis)

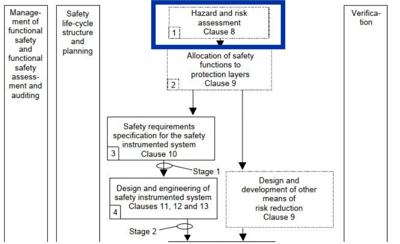
Subsystem	Failure Mode	Effects	Causes	Current mitigation measures
Water-cooled system	High temperature	Melting insulation, short circuit and electrocution	Water leak	None

Calibrated risk graph method for each failure mode

- Consequence (C)
- Exposure time (F)
- Prob. of avoiding the hazardous event (P)
- Demand rate (W)



Phase 1 - Hazard and risk assessment



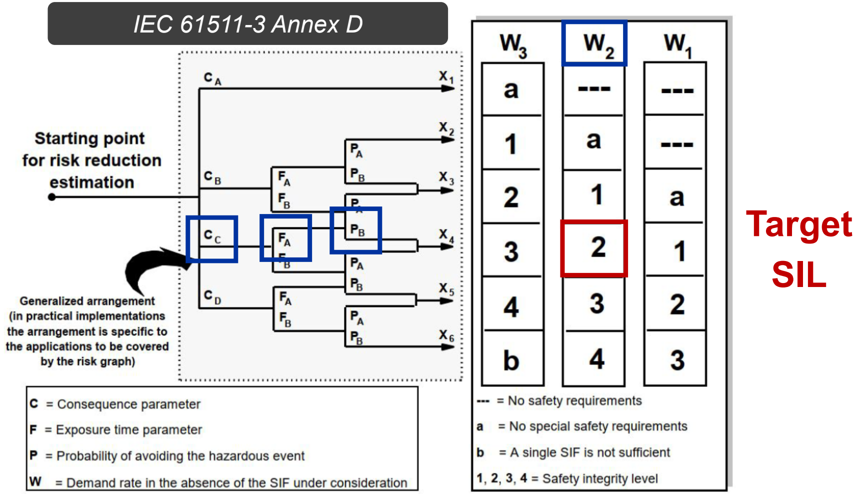
Identify the hazards, the risks and **evaluate** the necessary **risk reduction - Target Safety Integrity Level (SIL)**

FMEA (Failure Mode and Effect Analysis)

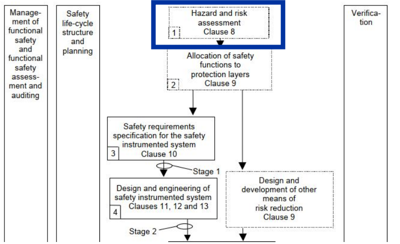
Subsystem	Failure Mode	Effects	Causes	Current mitigation measures
Water-cooled system	High temperature	Melting insulation, short circuit and electrocution	Water leak	None

Calibrated risk graph method for each failure mode

- Consequence (C)
- Exposure time (F)
- Prob. of avoiding the hazardous event (P)
- Demand rate (W)



Phase 1 - Hazard and risk assessment



Identify the hazards, the risks and **evaluate** the necessary **risk reduction - Target Safety Integrity Level (SIL)**

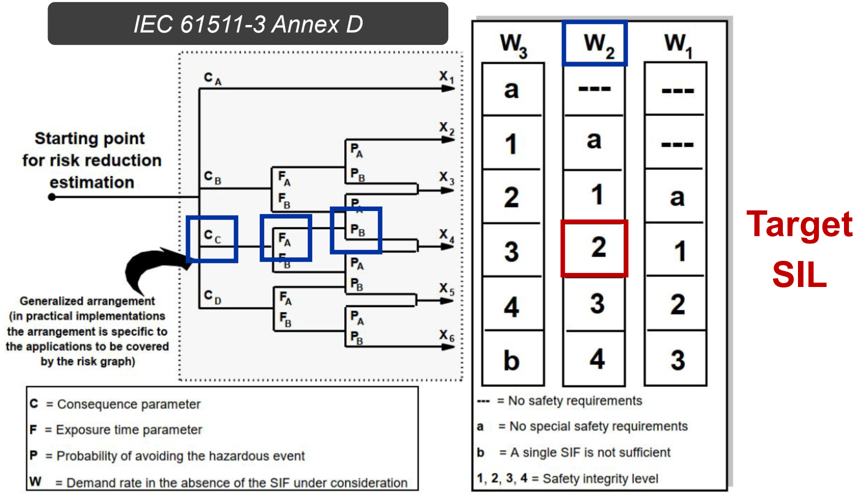
FMEA (Failure Mode and Effect Analysis)

Subsystem	Failure Mode	Effects	Causes	Current mitigation measures
Water-cooled system	High temperature	Melting insulation, short circuit and electrocution	Water leak	None

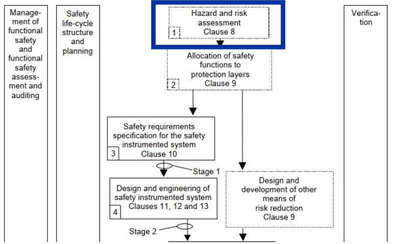
Calibrated risk graph method for each failure mode

- Consequence (C)
- Exposure time (F)
- Prob. of avoiding the hazardous event (P)
- Demand rate (W)

For **personnel**, **machine** and **environmental** protection

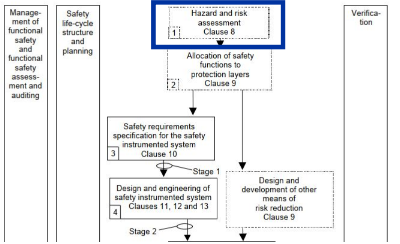


Phase 1 - Hazard and risk assessment



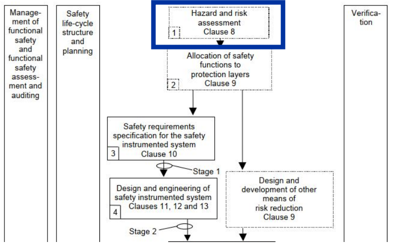
- **Challenges:**

Phase 1 - Hazard and risk assessment

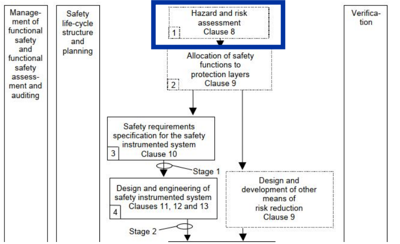


- **Challenges:**
  - Define the **tolerable risk** for **personnel** and **machine** protection – **risk graph calibration**

Phase 1 - Hazard and risk assessment



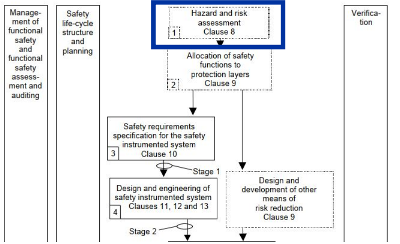
- **Challenges:**
  - Define the **tolerable risk** for **personnel** and **machine** protection – **risk graph calibration**
  - **Personnel** protection: **examples** from IEC 61511-3:2016 Annex D or IEC 61508-5:2010 Annex E



Phase 1 - Hazard and risk assessment

- **Challenges:**
  - Define the **tolerable risk** for **personnel** and **machine** protection – **risk graph calibration**
  - **Personnel** protection: **examples** from IEC 61511-3:2016 Annex D or IEC 61508-5:2010 Annex E
  - **Machine** protection (asset loss): corporative decision

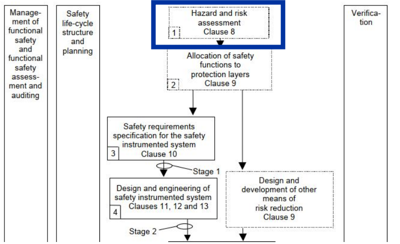
Phase 1 - Hazard and risk assessment



- **Challenges:**
  - Define the **tolerable risk** for **personnel** and **machine** protection – **risk graph calibration**
  - **Personnel** protection: **examples** from IEC 61511-3:2016 Annex D or IEC 61508-5:2010 Annex E
  - **Machine** protection (asset loss): corporative decision

Consequence		**Occupancy**		**Possib. of avoidance**		**Prob. of failure**	
CA	delay < few hours	FB	always	PA	automatic system that detects and alerts the operators	W1	< 1 failure per 10 years
CB	few hours < delay < few days			PB	There is not	W2	< 1 failure per year
CC	few days < delay < few weeks					W3	> 1 failure per year
CD	delay > a month or cancellation of test program						

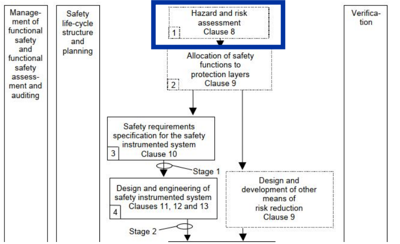
Phase 1 - Hazard and risk assessment



- **Challenges:**
  - Define the **tolerable risk** for **personnel** and **machine** protection – **risk graph calibration**
  - **Personnel** protection: **examples** from IEC 61511-3:2016 Annex D or IEC 61508-5:2010 Annex E
  - **Machine** protection (asset loss): corporative decision

Consequence		**Occupancy**		**Possib. of avoidance**		**Prob. of failure**	
CA	delay < few hours	FB	always	PA	automatic system that detects and alerts the operators	W1	< 1 failure per 10 years
CB	few hours < delay < few days			PB	There is not	W2	< 1 failure per year
CC	few days < delay < few weeks					W3	> 1 failure per year
CD	delay > a month or cancellation of test program						

Phase 1 - Hazard and risk assessment

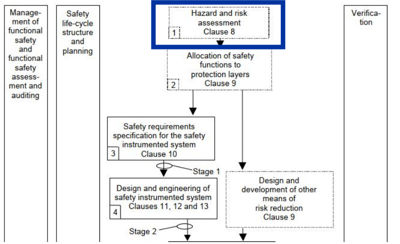


- **Challenges:**
  - Define the **tolerable risk** for **personnel** and **machine** protection – **risk graph calibration**
  - **Personnel** protection: **examples** from IEC 61511-3:2016 Annex D or IEC 61508-5:2010 Annex E
  - **Machine** protection (asset loss): corporative decision

Consequence		**Occupancy**		**Possib. of avoidance**		**Prob. of failure**	
CA	delay < few hours	FB	always	PA	automatic system that detects and alerts the operators	W1	< 1 failure per 10 years
CB	few hours < delay < few days			PB	There is not	W2	< 1 failure per year
CC	few days < delay < few weeks					W3	> 1 failure per year
CD	delay > a month or cancellation of test program						

e.g. a failure provoking a damage of a magnet in the LHC accelerator would imply a **delay of more than 1 month**

Phase 1 - Hazard and risk assessment



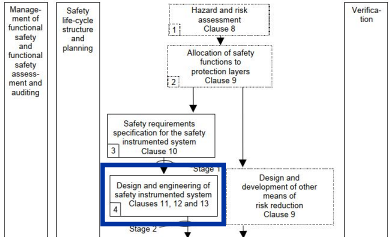
- **Challenges:**
  - Define the **tolerable risk** for **personnel** and **machine** protection – **risk graph calibration**
  - **Personnel** protection: **examples** from IEC 61511-3:2016 Annex D or IEC 61508-5:2010 Annex E
  - **Machine** protection (asset loss): corporative decision

Consequence		**Occupancy**		**Possib. of avoidance**		**Prob. of failure**	
CA	delay < few hours	FB	always	PA	automatic system that detects and alerts the operators	W1	< 1 failure per 10 years
CB	few hours < delay < few days			PB	There is not	W2	< 1 failure per year
CC	few days < delay < few weeks					W3	> 1 failure per year
CD	delay > a month or cancellation of test program						

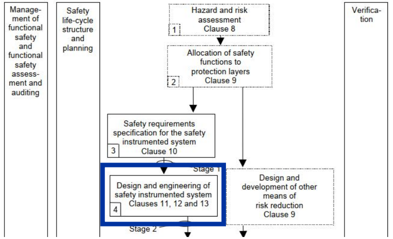
e.g. a failure provoking a damage of a magnet in the LHC accelerator would imply a **delay of more than 1 month**

- **Adopted solutions:**
  - **FMEA** + **calibrated risk graph**
  - Hazard and risk analysis and assessment **report templates**

Phase 4 - SIS design and engineering

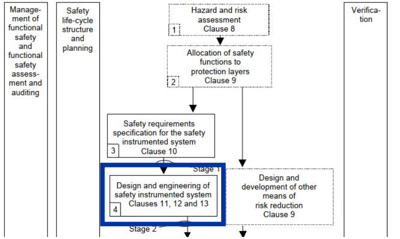


Phase 4 - SIS design and engineering



Design a SIS compliant with the SRS (Safety Requirements Specification)

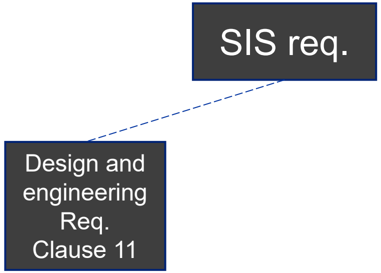
Phase 4 - SIS design and engineering



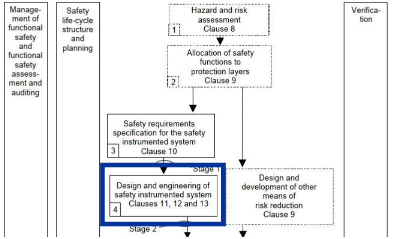
Design a SIS compliant with the SRS (Safety Requirements Specification)

Challenges:

1. **Design and engineering requirements**: *IEC 61511-1:2016 Clause 11*
   - **Hardware Fault Tolerance** (11.4)
   - Selection of the devices (11.5)
   - **Hardware random failures** (11.9)
   - Others (System behaviour on detection of a fault, field devices, interfaces, maintenance, etc.)



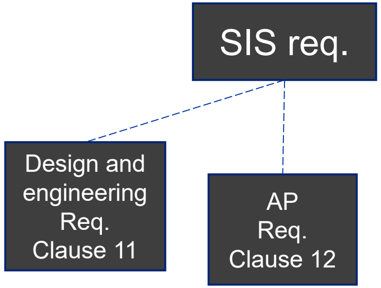
Phase 4 - SIS design and engineering



Design a SIS compliant with the SRS (Safety Requirements Specification)

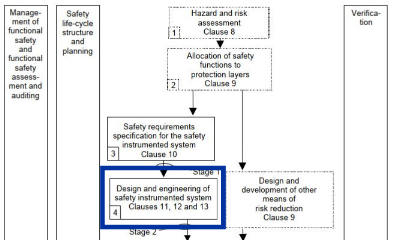
Challenges:

1. **Design and engineering requirements**: *IEC 61511-1:2016 Clause 11*
   - **Hardware Fault Tolerance** (11.4)
   - Selection of the devices (11.5)
   - **Hardware random failures** (11.9)
   - Others (System behaviour on detection of a fault, field devices, interfaces, maintenance, etc.)



2. **Application program (AP) Requirements** *IEC 61511-1:2016 Clause 12*

Phase 4 - SIS design and engineering



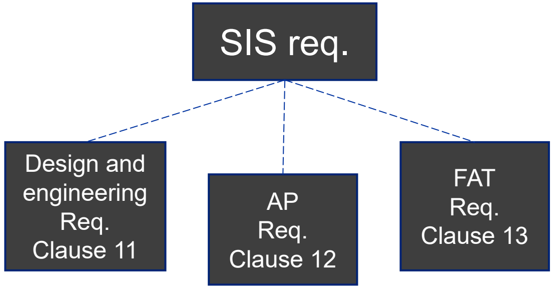
Design a SIS compliant with the SRS (Safety Requirements Specification)

Challenges:

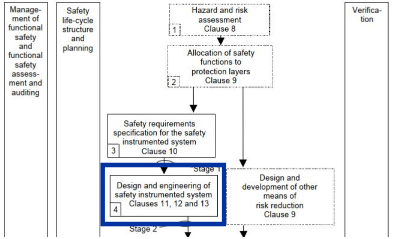
1. **Design and engineering requirements**: *IEC 61511-1:2016 Clause 11*
   - **Hardware Fault Tolerance** (11.4)
   - Selection of the devices (11.5)
   - **Hardware random failures** (11.9)
   - Others (System behaviour on detection of a fault, field devices, interfaces, maintenance, etc.)

2. **Application program (AP) Requirements** *IEC 61511-1:2016 Clause 12*

1. Factory Acceptance Test (FAT) requirements *IEC 61511-1:2016 Clause 13*



Phase 4 - SIS design and engineering



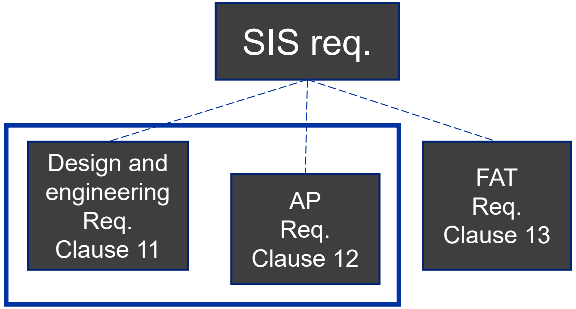
Design a SIS compliant with the SRS (Safety Requirements Specification)

Challenges:

1. **Design and engineering requirements**: *IEC 61511-1:2016 Clause 11*
   - **Hardware Fault Tolerance** (11.4)
   - Selection of the devices (11.5)
   - **Hardware random failures** (11.9)
   - Others (System behaviour on detection of a fault, field devices, interfaces, maintenance, etc.)

2. **Application program (AP) Requirements** *IEC 61511-1:2016 Clause 12*

1. Factory Acceptance Test (FAT) requirements *IEC 61511-1:2016 Clause 13*



SIS design and engineering – Hardware Random Failures

- **Challenges:**

SIS design and engineering – Hardware Random Failures

- **Challenges:**
  - **Collect the reliability data** for each element of the Safety Instrumented Function

SIS design and engineering – Hardware Random Failures

- **Challenges:**
  - **Collect the reliability data** for each element of the Safety Instrumented Function
  - **Build the reliability model** (sensors + controller + actuators) : Reliability Block Diagram or Fault Tree

SIS design and engineering – Hardware Random Failures

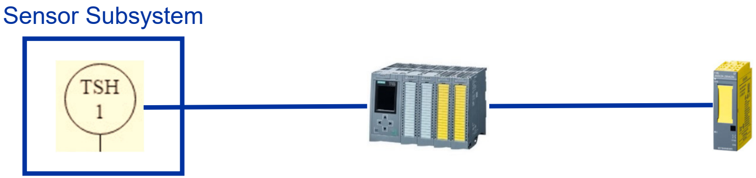
- **Challenges:**
  - **Collect the reliability data** for each element of the Safety Instrumented Function
  - **Build the reliability model** (sensors + controller + actuators) : Reliability Block Diagram or Fault Tree
  - **Apply the tables and formulas** from the standard

SIS design and engineering – Hardware Random Failures

- **Challenges:**
  - **Collect the reliability data** for each element of the Safety Instrumented Function
  - **Build the reliability model** (sensors + controller + actuators) : Reliability Block Diagram or Fault Tree
  - **Apply the tables and formulas** from the standard

SIS design and engineering – Hardware Random Failures

- **Challenges:**
  - **Collect the reliability data** for each element of the Safety Instrumented Function
  - **Build the reliability model** (sensors + controller + actuators) : Reliability Block Diagram or Fault Tree
  - **Apply the tables and formulas** from the standard



Example 1oo1

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

Average Probability of Failure
On Demand for the sensor group

IEC 61508-6:2010 Annex B

SIS design and engineering – Hardware Random Failures

- **Challenges:**
  - **Collect the reliability data** for each element of the Safety Instrumented Function
  - **Build the reliability model** (sensors + controller + actuators) : Reliability Block Diagram or Fault Tree
  - **Apply the tables and formulas** from the standard

Sensor Subsystem

Example 1oo1

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

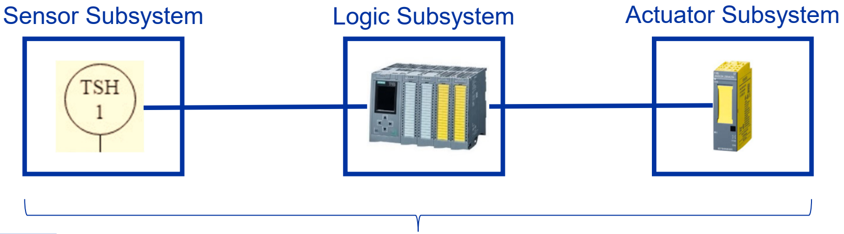
Average Probability of Failure
On Demand for the sensor group

$$PFD_{avg} \approx PFD_{avg} + PFD_{avg} + PFD_{avg}$$

IEC 61508-6:2010 Annex B

SIS design and engineering – Hardware Random Failures

- **Challenges:**
  - **Collect the reliability data** for each element of the Safety Instrumented Function
  - **Build the reliability model** (sensors + controller + actuators) : Reliability Block Diagram or Fault Tree
  - **Apply the tables and formulas** from the standard



Example 1oo1

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_{avg} \approx PFD_{avg} + PFD_{avg} + PFD_{avg}$$

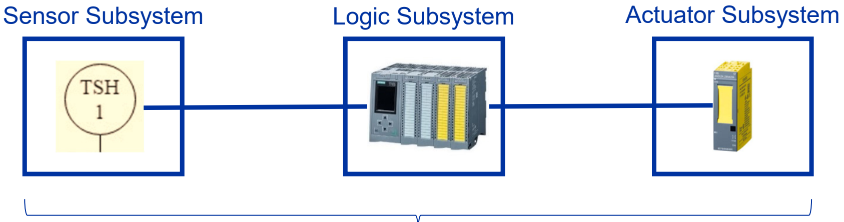
$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

Average Probability of Failure On Demand for the sensor group

IEC 61508-6:2010 Annex B

SIS design and engineering – Hardware Random Failures

- **Challenges:**
  - **Collect the reliability data** for each element of the Safety Instrumented Function
  - **Build the reliability model** (sensors + controller + actuators) : Reliability Block Diagram or Fault Tree
  - **Apply the tables and formulas** from the standard



Example 1oo1

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

Average Probability of Failure On Demand for the sensor group

$$PFD_{avg} \approx PFD_{avg} + PFD_{avg} + PFD_{avg}$$

IEC 61508-6:2010 Annex B

Demand Mode of Operation		
Safety Integrity Level (SIL)	PFD_{avg}	Required risk reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	$> 10^4$ to $\leq 10^5$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$> 10^3$ to $\leq 10^4$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$> 10^2$ to $\leq 10^3$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$> 10^1$ to $\leq 10^2$

SIS design and engineering – Hardware Fault Tolerance

- **Challenges:**

SIS design and engineering – Hardware Fault Tolerance

- **Challenges:**
  - Even if the prob. of failure is compliant with target SIL**, we may need to apply redundancy**

SIS design and engineering – Hardware Fault Tolerance

- **Challenges:**
  - Even if the prob. of failure is compliant with target SIL**, we may need to apply redundancy**
  - **Use the reliability model** (sensors + controller + actuators) and **analyze the SIF architecture**

SIS design and engineering – Hardware Fault Tolerance

- **Challenges:**
  - Even if the prob. of failure is compliant with target SIL**, we may need to apply redundancy**
  - **Use the reliability model** (sensors + controller + actuators) and **analyze the SIF architecture**

Hardware Fault Tolerance
IEC 61511-1:2016 Clause 11.4

SIL	Minimun HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode) or continuous mode)	1
4 (any mode)	2

HFT (Hardware Fault Tolerance)

SIS design and engineering – Hardware Fault Tolerance

- **Challenges:**
  - Even if the prob. of failure is compliant with target SIL**, we may need to apply redundancy**
  - **Use the reliability model** (sensors + controller + actuators) and **analyze the SIF architecture**

Hardware Fault Tolerance
IEC 61511-1:2016 Clause 11.4

SIL	Minimun HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode) or continuous mode)	1
4 (any mode)	2

HFT (Hardware Fault Tolerance)

SIS design and engineering – Hardware Fault Tolerance

- **Challenges:**
  - Even if the prob. of failure is compliant with target SIL**, we may need to apply redundancy**
  - **Use the reliability model** (sensors + controller + actuators) and **analyze the SIF architecture**

Hardware Fault Tolerance
IEC 61511-1:2016 Clause 11.4

SIL	Minimun HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode) or continuous mode)	1
4 (any mode)	2

HFT (Hardware Fault Tolerance)

Redundancy is needed, if continuous mode

SIS design and engineering – Hardware Fault Tolerance

- **Challenges:**
  - Even if the prob. of failure is compliant with target SIL**, we may need to apply redundancy**
  - **Use the reliability model** (sensors + controller + actuators) and **analyze the SIF architecture**

Hardware Fault Tolerance
IEC 61511-1:2016 Clause 11.4

SIL	Minimun HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode) or continuous mode)	1
4 (any mode)	2

Architectural Constraints
IEC 61508:2010-2 Clause 7.4.4 Route 1H or 2H

HFT (Hardware Fault Tolerance)

Redundancy is needed, if continuous mode

SIS design and engineering – Hardware Fault Tolerance

- **Challenges:**
  - Even if the prob. of failure is compliant with target SIL**, we may need to apply redundancy**
  - **Use the reliability model** (sensors + controller + actuators) and **analyze the SIF architecture**

Hardware Fault Tolerance
IEC 61511-1:2016 Clause 11.4

SIL	Minimun HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode) or continuous mode)	1
4 (any mode)	2

HFT (Hardware Fault Tolerance)
SFF (Safe Failure Fraction)

Architectural Constraints
IEC 61508-2:2010 Clause 7.4.4 Route 1H

SFF	HFT		
	0	1	2
$SFF < 60\%$	SIL1	SIL2	SIL3
$60\% \leq SFF < 90\%$	SIL2	SIL3	SIL4
$90\% \leq SFF < 99\%$	SIL3	SIL4	SIL4
$SFF \geq 99\%$	SIL3	SIL4	SIL4

Example for **type A** devices (without processor)

Redundancy is needed, if continuous mode

SIS design and engineering – Hardware Fault Tolerance

- **Challenges:**
  - Even if the prob. of failure is compliant with target SIL**, we may need to apply redundancy**
  - **Use the reliability model** (sensors + controller + actuators) and **analyze the SIF architecture**

Hardware Fault Tolerance
IEC 61511-1:2016 Clause 11.4

SIL	Minimun HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode) or continuous mode)	1
4 (any mode)	2

HFT (Hardware Fault Tolerance)
SFF (Safe Failure Fraction)

Architectural Constraints
IEC 61508-2:2010 Clause 7.4.4 Route 1H

SFF	HFT		
	0	1	2
$SFF < 60\%$	SIL1	SIL2	SIL3
$60\% \leq SFF < 90\%$	SIL2	SIL3	SIL4
$90\% \leq SFF < 99\%$	SIL3	SIL4	SIL4
$SFF \geq 99\%$	SIL3	SIL4	SIL4

Example for **type A** devices (without processor)

Redundancy is needed, if continuous mode

SIS design and engineering – Hardware Fault Tolerance

- **Challenges:**
  - Even if the prob. of failure is compliant with target SIL**, we may need to apply redundancy**
  - **Use the reliability model** (sensors + controller + actuators) and **analyze the SIF architecture**

Hardware Fault Tolerance
IEC 61511-1:2016 Clause 11.4

SIL	Minimun HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode) or continuous mode)	1
4 (any mode)	2

HFT (Hardware Fault Tolerance)

SFF (Safe Failure Fraction)

Architectural Constraints
IEC 61508-2:2010 Clause 7.4.4 Route 1H

SFF	HFT		
	0	1	2
$SFF < 60\%$	SIL1	SIL2	SIL3
$60\% \leq SFF < 90\%$	SIL2	SIL3	SIL4
$90\% \leq SFF < 99\%$	SIL3	SIL4	SIL4
$SFF \geq 99\%$	SIL3	SIL4	SIL4

Example for **type A** devices (without processor)

Redundancy is needed, if continuous mode

Redundancy is **not** needed, if SFF ≥ 60% for type A devices

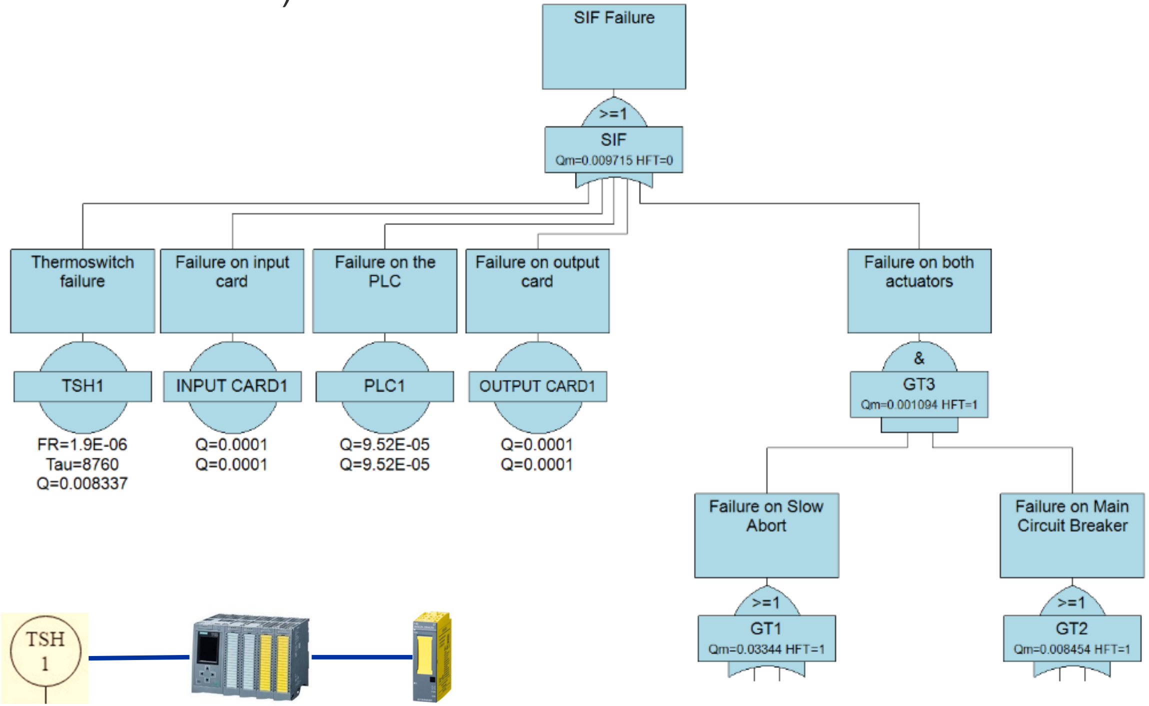
Phase 4 - SIS design and engineering (both)

Phase 4 - SIS design and engineering (both)

- **Adopted solution: Isograph's Reliability workbench** (**both** for hardware random failures and architectural constraints)

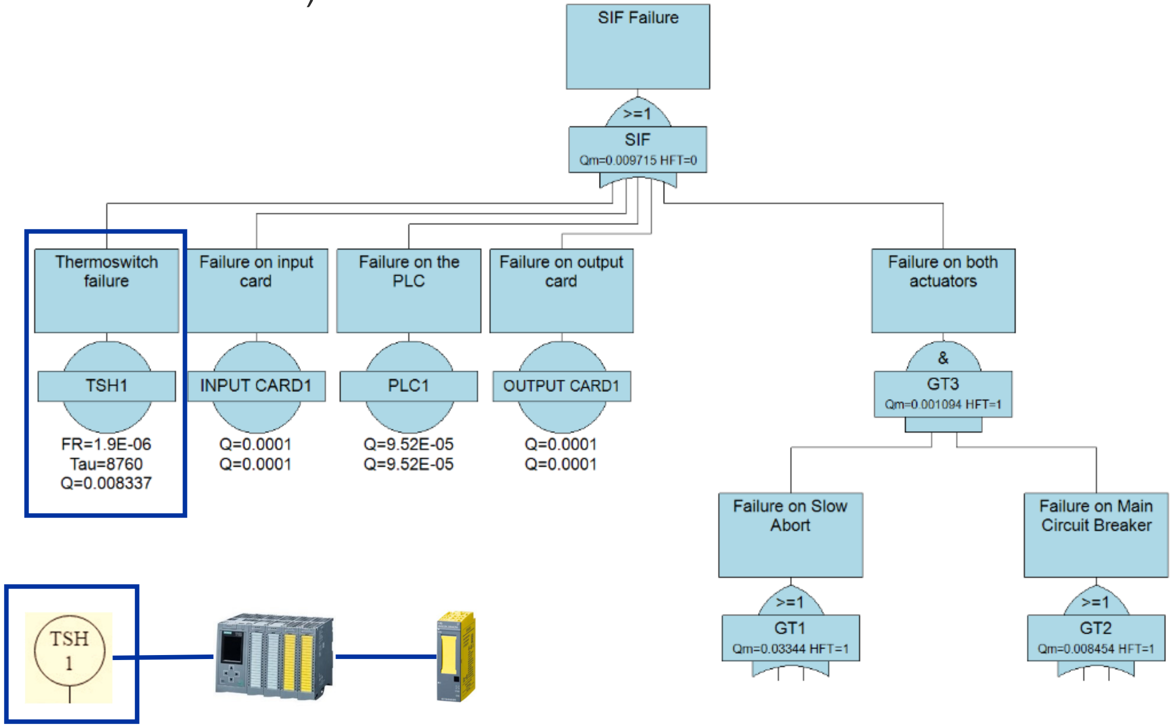
Phase 4 - SIS design and engineering (both)

- **Adopted solution: Isograph's Reliability workbench** (**both** for hardware random failures and architectural constraints)



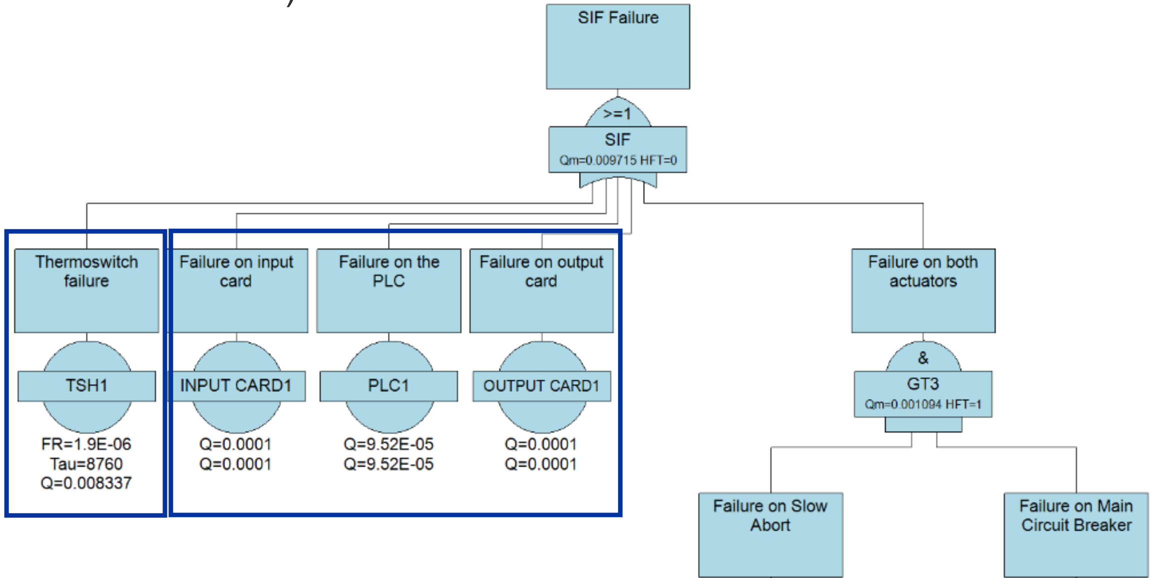
Phase 4 - SIS design and engineering (both)

- **Adopted solution: Isograph's Reliability workbench** (**both** for hardware random failures and architectural constraints)



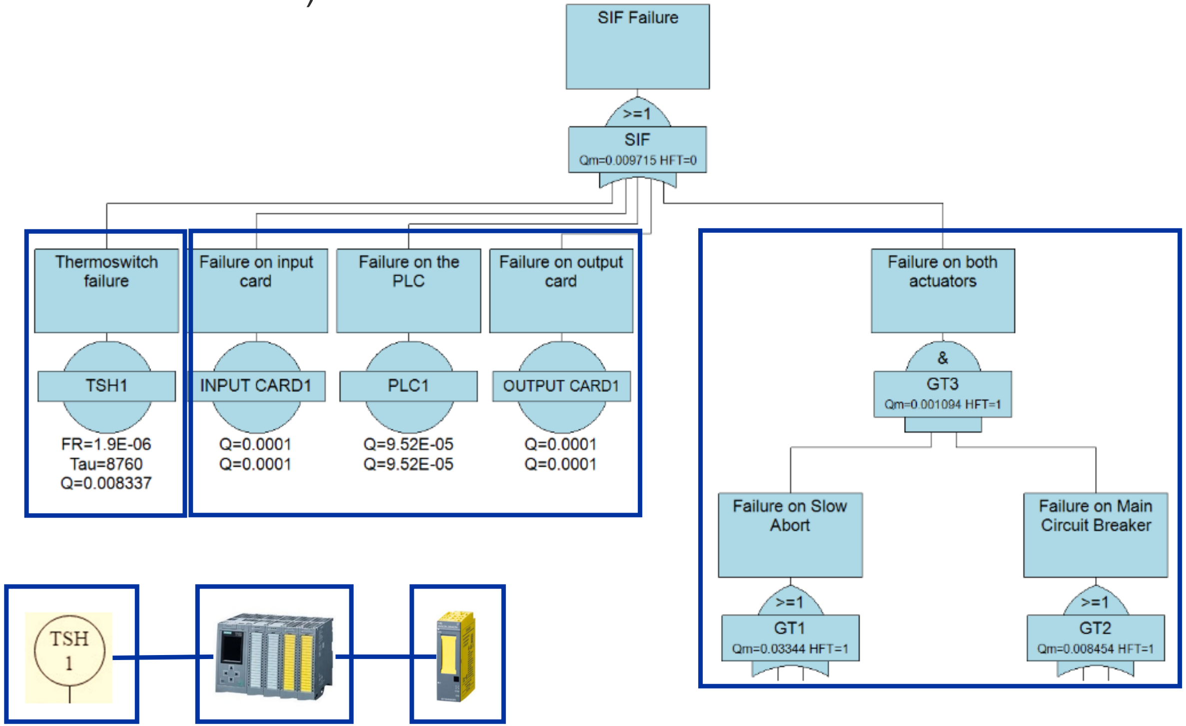
Phase 4 - SIS design and engineering (both)

- **Adopted solution: Isograph's Reliability workbench** (**both** for hardware random failures and architectural constraints)



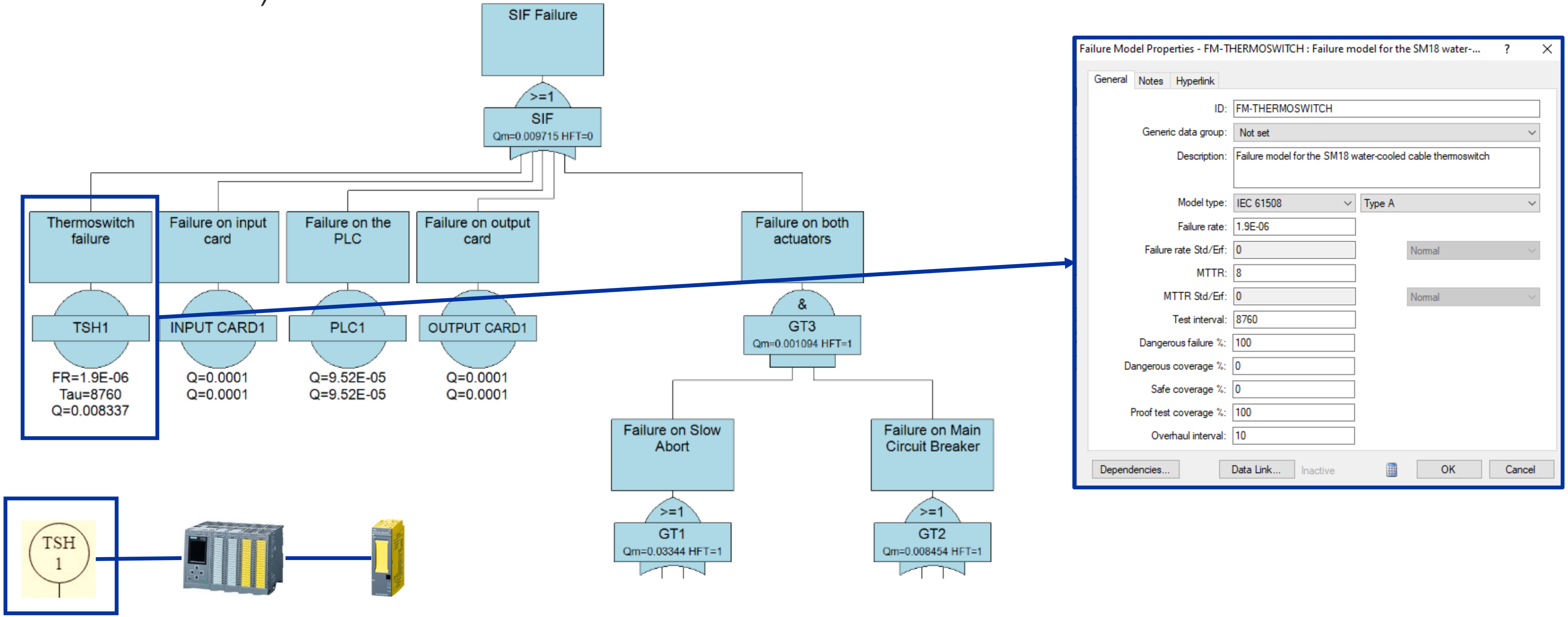
Phase 4 - SIS design and engineering (both)

- **Adopted solution: Isograph's Reliability workbench** (**both** for hardware random failures and architectural constraints)



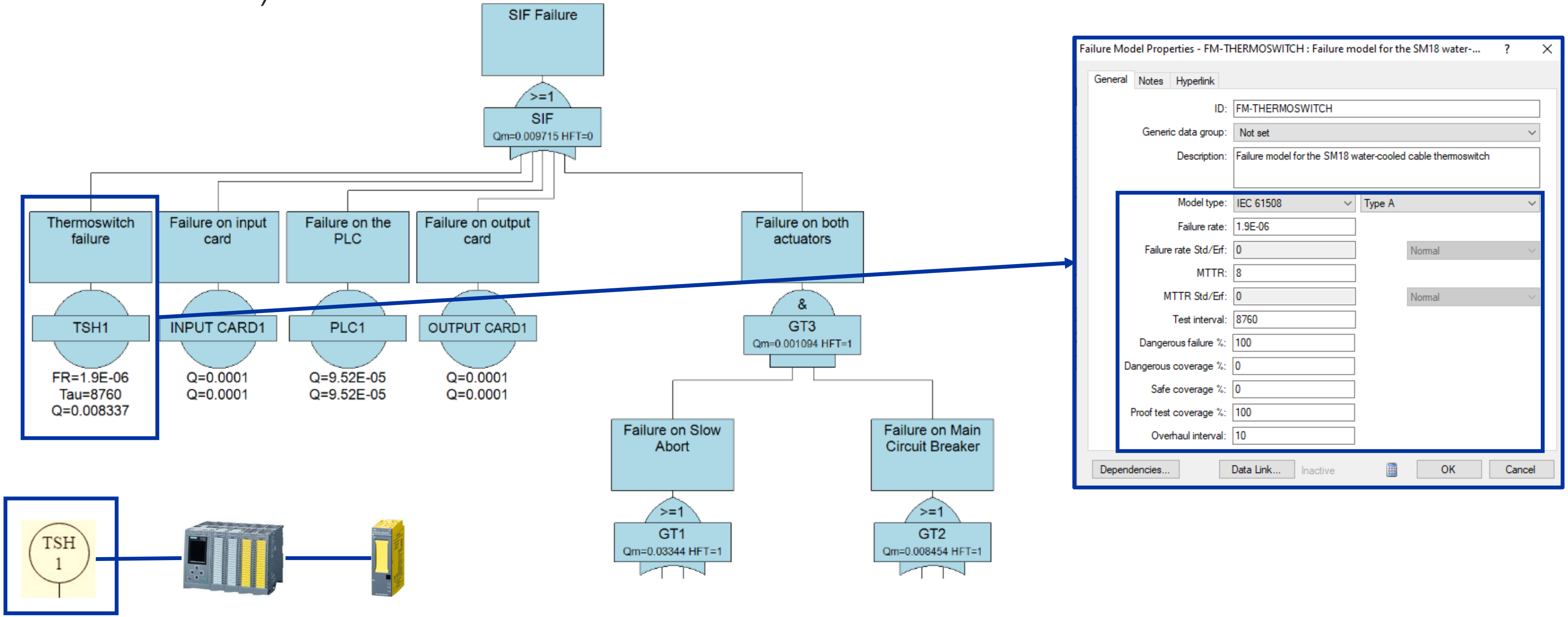
Phase 4 - SIS design and engineering (both)

- **Adopted solution: Isograph's Reliability workbench** (**both** for hardware random failures and architectural constraints)



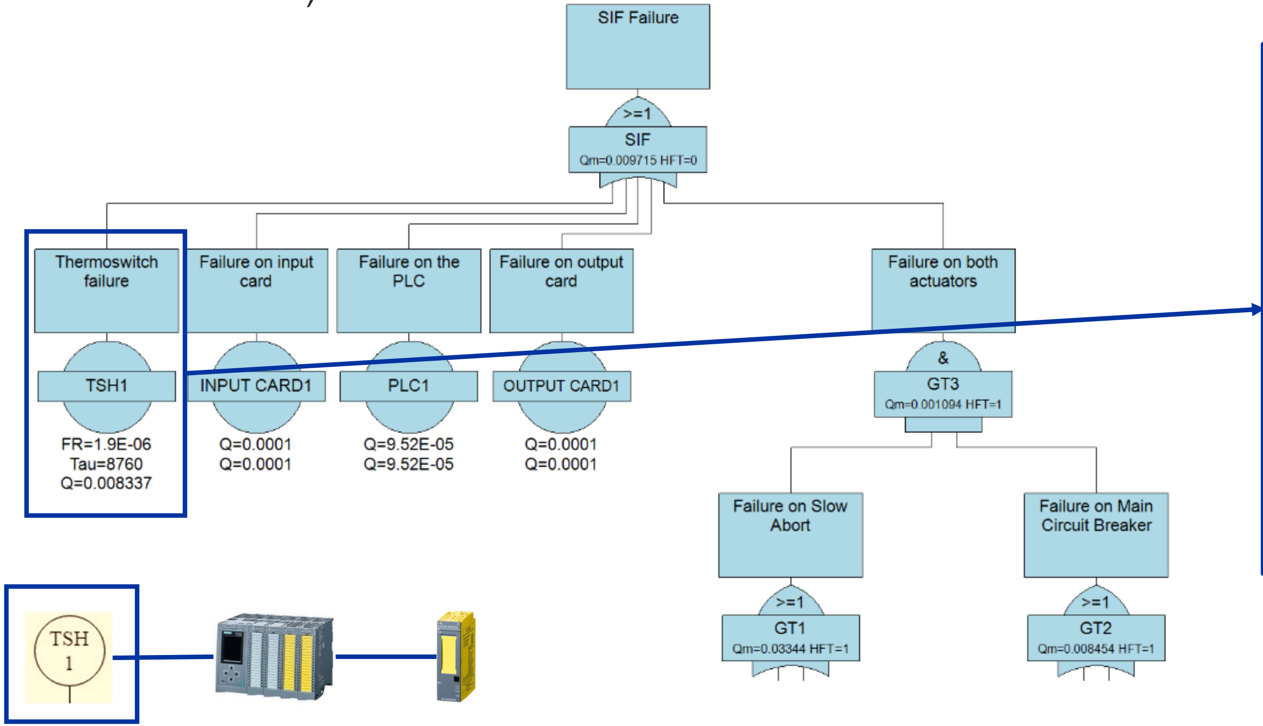
Phase 4 - SIS design and engineering (both)

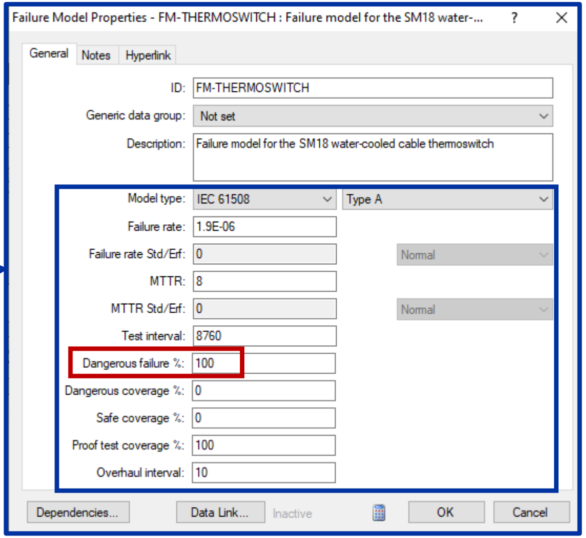
- **Adopted solution: Isograph's Reliability workbench** (**both** for hardware random failures and architectural constraints)



Phase 4 - SIS design and engineering (both)

- **Adopted solution: Isograph's Reliability workbench** (**both** for hardware random failures and architectural constraints)





Related to SFF (Safe Failure Fraction)

SIS design and engineering – Application Program (AP)

SIS design and engineering – Application Program (AP)

- **Challenges:**
  - Requirements to **design**, **implement** and **verify APs**

IEC 61511-1: 2016 Clause 12

SIS design and engineering – Application Program (AP)

- **Challenges:**
  - Requirements to **design**, **implement** and **verify APs** *IEC 61511-1: 2016 Clause 12*
- **Guidelines** (examples and recommendations) *IEC 61511-2:2016 Annex B*

SIS design and engineering – Application Program (AP)

- **Challenges:**
  - Requirements to **design**, **implement** and **verify APs**

IEC 61511-1: 2016 Clause 12

- **Guidelines** (examples and recommendations)

IEC 61511-2:2016 Annex B

*"The traditional **text based approach of safety AP specification is not efficient** enough to handle the advanced, complex safety requirements commonly found in SIF specifications. The most efficient tool to address these challenges is the **Model-based design (MBD)**..."*

SIS design and engineering – Application Program (AP)

- **Challenges:**
  - Requirements to **design**, **implement** and **verify APs** *IEC 61511-1: 2016 Clause 12*
- **Guidelines** (examples and recommendations) *IEC 61511-2:2016 Annex B*

*"The traditional **text based approach of safety AP specification is not efficient** enough to handle the advanced, complex safety requirements commonly found in SIF specifications. The most efficient tool to address these challenges is the **Model-based design (MBD)**..."*

SIS design and engineering – Application Program (AP)

- **Challenges:**
  - Requirements to **design**, **implement** and **verify APs**

IEC 61511-1: 2016 Clause 12

- **Guidelines** (examples and recommendations)

IEC 61511-2:2016 Annex B

*"The traditional **text based approach of safety AP specification is not efficient** enough to handle the advanced, complex safety requirements commonly found in SIF specifications. The most efficient tool to address these challenges is the **Model-based design (MBD)**..."*

*"… **specification** should be implemented in the **graphical language of the model checking workbench** environment...*

SIS design and engineering – Application Program (AP)

- **Challenges:**
  - Requirements to **design**, **implement** and **verify APs**

IEC 61511-1: 2016 Clause 12

- **Guidelines** (examples and recommendations)

IEC 61511-2:2016 Annex B

*"The traditional **text based approach of safety AP specification is not efficient** enough to handle the advanced, complex safety requirements commonly found in SIF specifications. The most efficient tool to address these challenges is the **Model-based design (MBD)**..."*

*"... **specification** should be implemented in the **graphical language of the model checking workbench** environment...*

SIS design and engineering – Application Program (AP)

- **Challenges:**
  - Requirements to **design**, **implement** and **verify APs**

IEC 61511-1: 2016 Clause 12

- **Guidelines** (examples and recommendations)

IEC 61511-2:2016 Annex B

*"The traditional **text based approach of safety AP specification is not efficient** enough to handle the advanced, complex safety requirements commonly found in SIF specifications. The most efficient tool to address these challenges is the **Model-based design (MBD)**..."*

*"... **specification** should be implemented in the **graphical language of the model checking workbench** environment...*

- **Adopted solutions:**

SIS design and engineering – Application Program (AP)

- **Challenges:**
  - Requirements to **design**, **implement** and **verify APs**

IEC 61511-1: 2016 Clause 12

- **Guidelines** (examples and recommendations)

IEC 61511-2:2016 Annex B

*"The traditional **text based approach of safety AP specification is not efficient** enough to handle the advanced, complex safety requirements commonly found in SIF specifications. The most efficient tool to address these challenges is the **Model-based design (MBD)**..."*

*"… **specification** should be implemented in the **graphical language of the model checking workbench** environment...*

- **Adopted solutions:**
  - MBD for the **SRS** (Safety requirements Specification) - **phase 3** = logic to be implemented in the PLC:
    - **CEM** (Cause and Effect Matrix) – **SISpec** tool*
    - **LD** (Logic Diagrams) – **Grassedit** tool*
  - **Model Checking** for the PLC program verification – **PLCverif** tool*

*developed at CERN

SIS design and engineering – AP specification

SIS design and engineering – AP specification

CEM (Cause and Effect Matrix) - **SISpec**
More details: MOPHA041

Cause \ Effect	SIF1
COM_1	A1,A2,A3,A4
CON_A	A1,A2,A3,A4
TSH1	NA1
TSH2	NA2
FSL1	NA3
FSL2	NA4

Cause \ Effect	PC1_PP
SIF1	NA1
SIF2	NA1
SIF3	
SIF4	NA1
PC1_OPER	A1

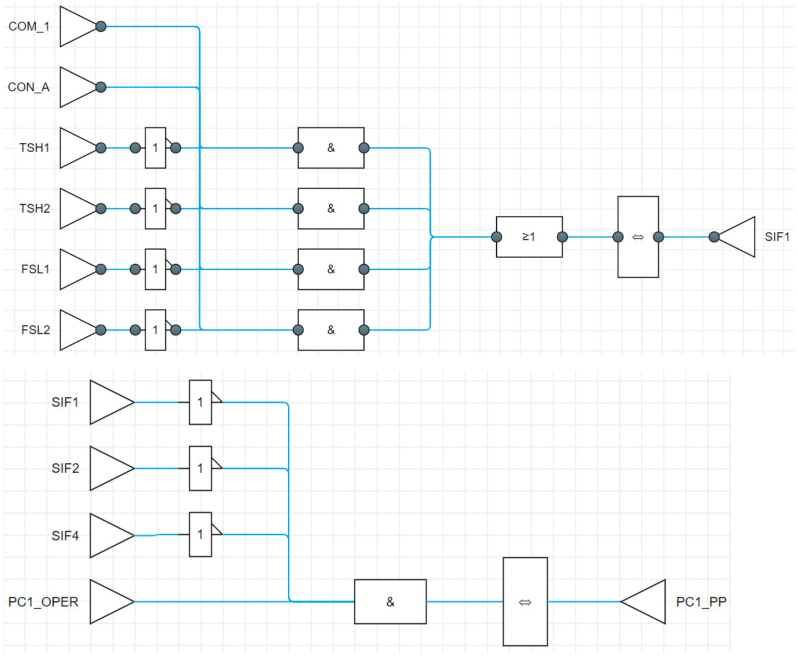
SIS design and engineering – AP specification

CEM (Cause and Effect Matrix) - **SISpec**
More details: MOPHA041

Cause \ Effect	SIF1
COM_1	A1,A2,A3,A4
CON_A	A1,A2,A3,A4
TSH1	NA1
TSH2	NA2
FSL1	NA3
FSL2	NA4

Cause \ Effect	PC1_PP
SIF1	NA1
SIF2	NA1
SIF3	
SIF4	NA1
PC1_OPER	A1

LD (Logic Diagrams) - **Grassedit**



Simulation, **test** and **verification** case generation and **code generation** is possible

SIS design and engineering – Application Program

SIS design and engineering – Application Program

AP specification

AP development

AP verification

SIS design and engineering – Application Program

AP specification

AP development

AP verification

SISpec

(a) Top Operational CEM

Cause \ Effect	PC1_OPER	PC2_OPER
SEL_PC1	A1,A2,A3,A4,A5	
SEL_PC2		A1
TEST_A	A1	
TEST_B	A2	A1
TEST_C	A3	
TEST_D	A4	
TEST_E	A5	

(b) Top Safety CEM

Cause \ Effect	PC1_PP	PC2_PP
SIF1	NA1	
SIF2	NA1	
SIF3		NA1
SIF4	NA1	NA1
PC1_OPER	A1	
PC2_OPER		A1

(c) Bottom Operational CEM

Cause \ Effect	TEST_A	TEST_B
SEL_TEST_A	A1	
SEL_TEST_B		A1
CRYO_A	A1	
CRYO_B		A1
DAQ_A	A1	
DAQ_B		A1

(d) Bottom Safety CEM

Cause \ Effect	SIF1	SIF2
COM_1	A1,A2,A3,A4	
CON_A	A1,A2,A3,A4	
TSH1	NA1	
TSH2	NA2	
FSL1	NA3	
FSL2	NA4	
...		...

SIS design and engineering – Application Program

AP specification

AP development

AP verification

SISpec

(a) Top Operational CEM

Cause \ Effect	PC1_OPER	PC2_OPER
SEL_PC1	A1,A2,A3,A4,A5	
SEL_PC2		A1
TEST_A	A1	
TEST_B	A2	A1
TEST_C	A3	
TEST_D	A4	
TEST_E	A5	

(b) Top Safety CEM

Cause \ Effect	PC1_PP	PC2_PP
SIF1	NA1	
SIF2	NA1	
SIF3		NA1
SIF4	NA1	NA1
PC1_OPER	A1	
PC2_OPER		A1

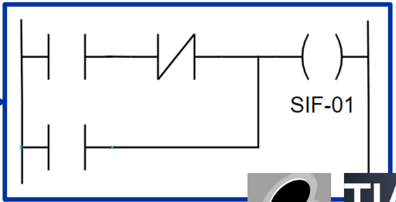
(c) Bottom Operational CEM

Cause \ Effect	TEST_A	TEST_B
SEL_TEST_A	A1	
SEL_TEST_B		A1
CRYO_A	A1	
CRYO_B		A1
DAQ_A	A1	
DAQ_B		A1

(d) Bottom Safety CEM

Cause \ Effect	SIF1	SIF2
COM_1	A1,A2,A3,A4	
CON_A	A1,A2,A3,A4	
TSH1	NA1	
TSH2	NA2	
FSL1	NA3	
FSL2	NA4	
...		...

PLC program



SIS design and engineering – Application Program

AP specification | *AP development* | *AP verification*

SISpec

(a) Top Operational CEM

Cause \ Effect	PC1_OPER	PC2_OPER
SEL_PC1	A1,A2,A3,A4,A5	
SEL_PC2		A1
TEST_A	A1	
TEST_B	A2	A1
TEST_C	A3	
TEST_D	A4	
TEST_E	A5	

(b) Top Safety CEM

Cause \ Effect	PC1_PP	PC2_PP
SIF1	NA1	
SIF2	NA1	
SIF3		NA1
SIF4	NA1	NA1
PC1_OPER	A1	
PC2_OPER		A1

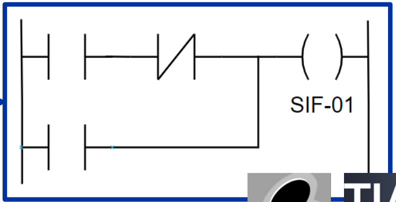
(c) Bottom Operational CEM

Cause \ Effect	TEST_A	TEST_B
SEL_TEST_A	A1	
SEL_TEST_B		A1
CRYO_A	A1	
CRYO_B		A1
DAQ_A	A1	
DAQ_B		A1

(d) Bottom Safety CEM

Cause \ Effect	SIF1	SIF2
COM_1	A1,A2,A3,A4	
CON_A	A1,A2,A3,A4	
TSH1	NA1	
TSH2	NA2	
FSL1	NA3	
FSL2	NA4	
...		...

PLC program



Verification cases

```
//#ASSERT(
    (
        NOT Inputs.In1 OR
        NOT Inputs.In2
    )
    --> (Out1 = FALSE)
): SIF01;
```

SIS design and engineering – Application Program

AP specification

SISpec

(a) Top Operational CEM

Cause \ Effect	PC1_OPER	PC2_OPER
SEL_PC1	A1,A2,A3,A4,A5	
SEL_PC2		A1
TEST_A	A1	
TEST_B	A2	A1
TEST_C	A3	
TEST_D	A4	
TEST_E	A5	

(b) Top Safety CEM

Cause \ Effect	PC1_PP	PC2_PP
SIF1	NA1	
SIF2	NA1	
SIF3		NA1
SIF4	NA1	NA1
PC1_OPER	A1	
PC2_OPER		A1

(c) Bottom Operational CEM

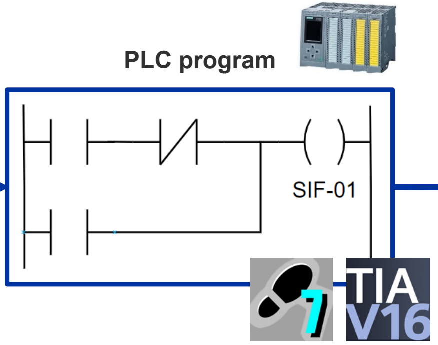
Cause \ Effect	TEST_A	TEST_B
SEL_TEST_A	A1	
SEL_TEST_B		A1
CRYO_A	A1	
CRYO_B		A1
DAQ_A	A1	
DAQ_B		A1

(d) Bottom Safety CEM

Cause \ Effect	SIF1	SIF2
COM_1	A1,A2,A3,A4	
CON_A	A1,A2,A3,A4	
TSH1	NA1	
TSH2	NA2	
FSL1	NA3	
FSL2	NA4	
...		...

AP development

PLC program



AP verification

Exported source code

Verification cases

```
//#ASSERT(
    (
        NOT Inputs.In1 OR
        NOT Inputs.In2
    )
    --> (Out1 = FALSE)
): SIF01;
```

SIS design and engineering – Application Program

AP specification | *AP development* | *AP verification*

SISpec

(a) Top Operational CEM

Cause \ Effect	PC1_OPER	PC2_OPER
SEL_PC1	A1,A2,A3,A4,A5	
SEL_PC2		A1
TEST_A	A1	
TEST_B	A2	A1
TEST_C	A3	
TEST_D	A4	
TEST_E	A5	

(b) Top Safety CEM

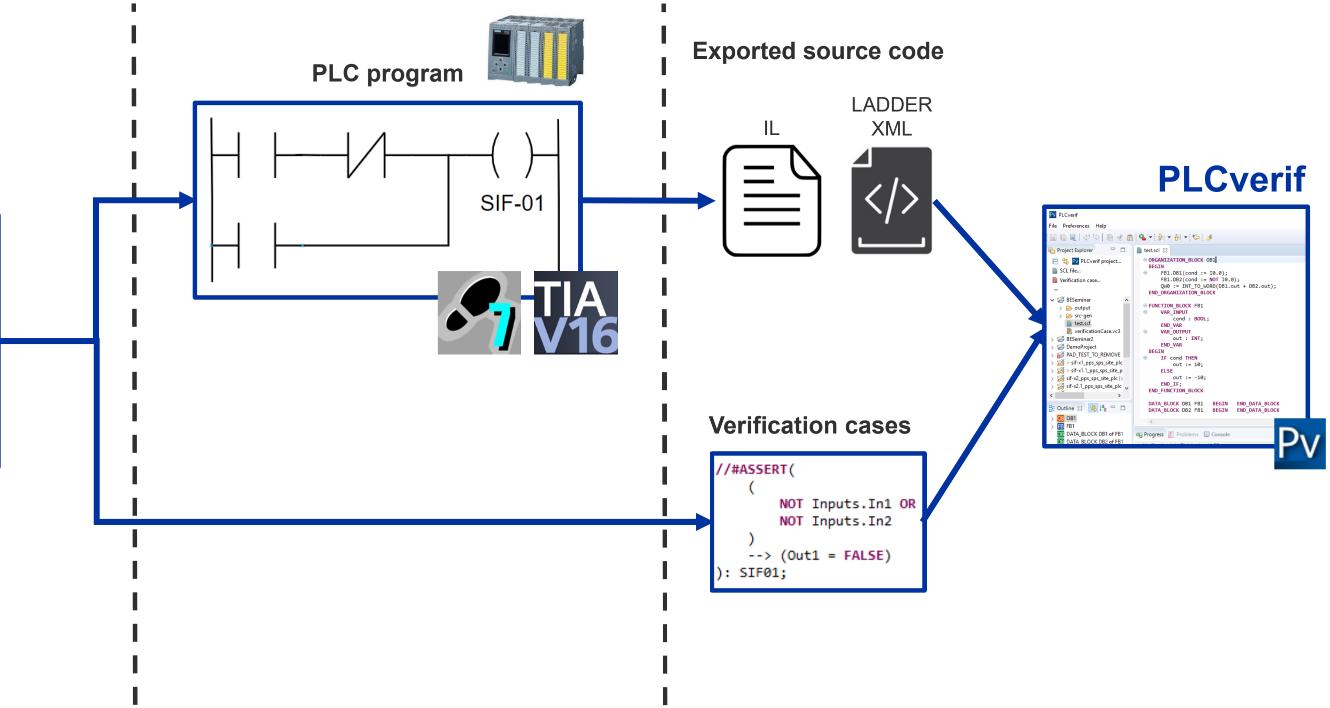
Cause \ Effect	PC1_PP	PC2_PP
SIF1	NA1	
SIF2	NA1	
SIF3		NA1
SIF4	NA1	NA1
PC1_OPER	A1	
PC2_OPER		A1

(c) Bottom Operational CEM

Cause \ Effect	TEST_A	TEST_B
SEL_TEST_A	A1	
SEL_TEST_B		A1
CRYO_A	A1	
CRYO_B		A1
DAQ_A	A1	
DAQ_B		A1

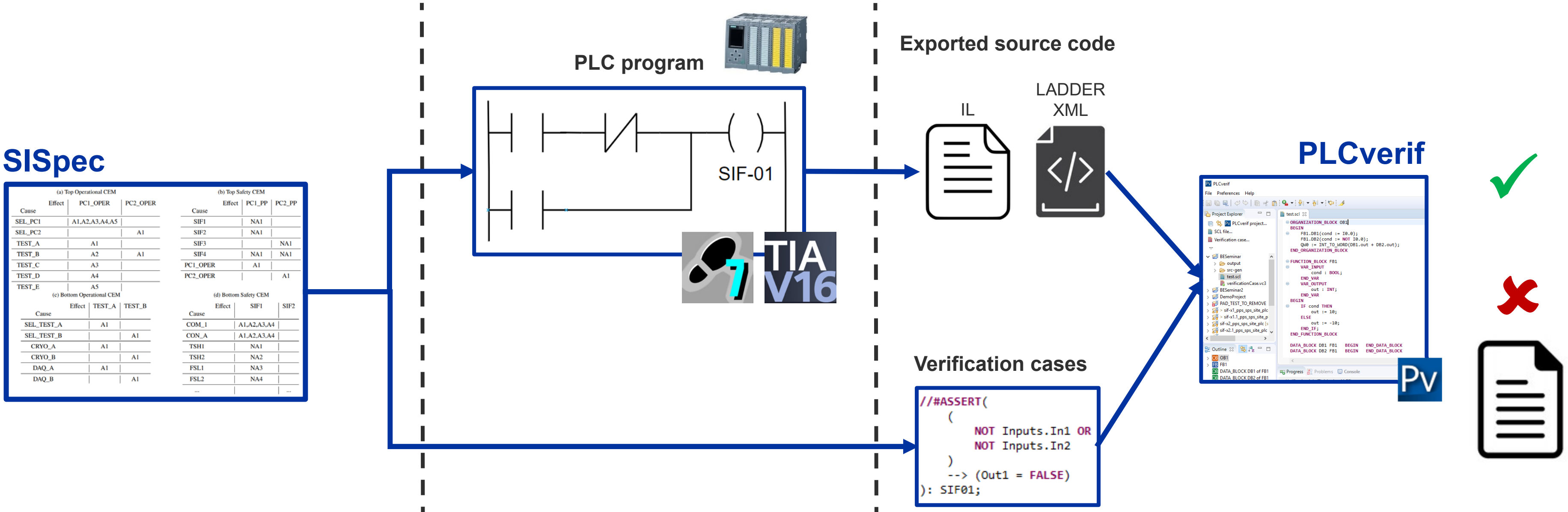
(d) Bottom Safety CEM

Cause \ Effect	SIF1	SIF2
COM_1	A1,A2,A3,A4	
CON_A	A1,A2,A3,A4	
TSH1	NA1	
TSH2	NA2	
FSL1	NA3	
FSL2	NA4	
...		...



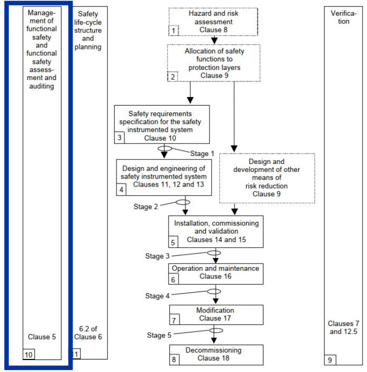
SIS design and engineering – Application Program

AP specification | *AP development* | *AP verification*

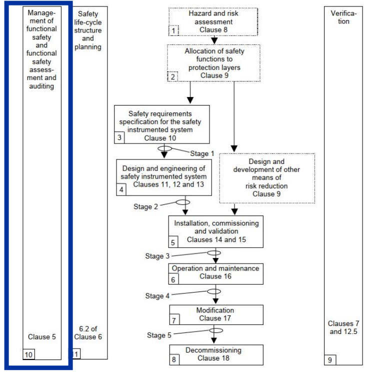


PLCverif more details:
https://cern.ch/plcverif
MOPV042, WEPV042, etc.

Phase 10 - Management of an FS project

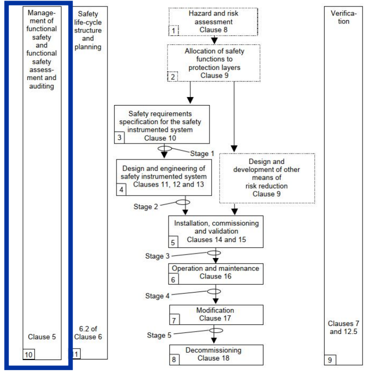


Phase 10 - Management of an FS project



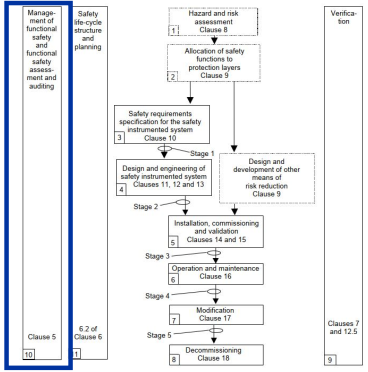
- **Challenges:**
  - Define the **roles** and **responsibilities** of the project members
  - Define the **workflow** and **documentation to coordinate all project members**

Phase 10 - Management of an FS project



- **Challenges:**
  - Define the **roles** and **responsibilities** of the project members
  - Define the **workflow** and **documentation to coordinate all project members**
- **Adopted solutions:**
  - Definition of roles and responsibilities – ongoing work (**example** below)
  - Report templates
  - Functional Safety projects workflow – ongoing work

Phase 10 - Management of an FS project

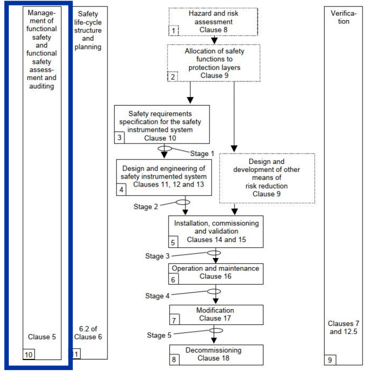


- **Challenges:**
  - Define the **roles** and **responsibilities** of the project members
  - Define the **workflow** and **documentation to coordinate all project members**

- **Adopted solutions:**
  - Definition of roles and responsibilities – ongoing work (**example** below)
  - Report templates
  - Functional Safety projects workflow – ongoing work

Role	Responsibilities
Functional Safety (FS) expert	Apply the FS standards
Process expert	Process knowledge and risk analysis
Instrumentation and controls expert	Design and implementation of the safety system
Departmental Safety Officer (DSO)	Risk graph calibration and safety support
Health & Safety and Environmental Protection (HSE) unit representative	Safety support and safety audits

Phase 10 - Management of an FS project



- **Challenges:**
  - Define the **roles** and **responsibilities** of the project members
  - Define the **workflow** and **documentation to coordinate all project members**

- **Adopted solutions:**
  - Definition of roles and responsibilities – ongoing work (**example** below)
  - Report templates
  - Functional Safety projects workflow – ongoing work

Role	Responsibilities
Functional Safety (FS) expert	Apply the FS standards
Process expert	Process knowledge and risk analysis
Instrumentation and controls expert	Design and implementation of the safety system
Departmental Safety Officer (DSO)	Risk graph calibration and safety support
Health & Safety and Environmental Protection (HSE) unit representative	Safety support and safety audits

Conclusions and future work

Conclusions:

Conclusions and future work

Conclusions:

- We have **integrated new tools** to the safety life-cycle

Safety life-cycle phase	Tools	Methods	Report templates
H&R assessment	-	FMEA and calibrated risk graph	Risk assessment report
SRS	SISpec and Grassedit	CEM and Logic Diagrams	SRS report
Design and engineering	Isograph, PLCverif and UNICOS (future work)	FTA, RBD, model checking and FAT	Design and verification report
Validation	-	-	Proof test
Management	-	-	FSA and safety manual

Conclusions and future work

Conclusions:

- We have **integrated new tools** to the safety life-cycle
- We are now applying **recommended methods** from IEC 61511

Safety life-cycle phase	Tools	Methods	Report templates
H&R assessment	-	FMEA and calibrated risk graph	Risk assessment report
SRS	SISpec and Grassedit	CEM and Logic Diagrams	SRS report
Design and engineering	Isograph, PLCverif and UNICOS (future work)	FTA, RBD, model checking and FAT	Design and verification report
Validation	-	-	Proof test
Management	-	-	FSA and safety manual

Conclusions and future work

Conclusions:

- We have **integrated new tools** to the safety life-cycle
- We are now applying **recommended methods** from IEC 61511
- We have created **report templates**

Safety life-cycle phase	Tools	Methods	Report templates
H&R assessment	-	FMEA and calibrated risk graph	Risk assessment report
SRS	SISpec and Grassedit	CEM and Logic Diagrams	SRS report
Design and engineering	Isograph, PLCverif and UNICOS (future work)	FTA, RBD, model checking and FAT	Design and verification report
Validation	-	-	Proof test
Management	-	-	FSA and safety manual

Conclusions and future work

Conclusions:

- We have **integrated new tools** to the safety life-cycle
- We are now applying **recommended methods** from IEC 61511
- We have created **report templates**

Future work:

- **Traceability** (explore commercial tools)
- **Workflow** procedures
- **Code generation** of application programs
- **Integration** in our frameworks (e.g. UNICOS)

Safety life-cycle phase	Tools	Methods	Report templates
H&R assessment	-	FMEA and calibrated risk graph	Risk assessment report
SRS	SISpec and Grassedit	CEM and Logic Diagrams	SRS report
Design and engineering	Isograph, PLCverif and UNICOS (future work)	FTA, RBD, model checking and FAT	Design and verification report
Validation	-	-	Proof test
Management	-	-	FSA and safety manual

CERN

ICALEPCS 2021

home.cern