Cause-and-Effect Matrix specifications for interlock based systems

Borja Fernández Adiego **(CERN)**

Contains Joint work of

Enrique Blanco, Roberto Speroni (CERN)

H. Hamisch, M. Bonet, M. H. de Queiroz (Universidade Federal de Santa Catarina, Florianópolis, Brazil)

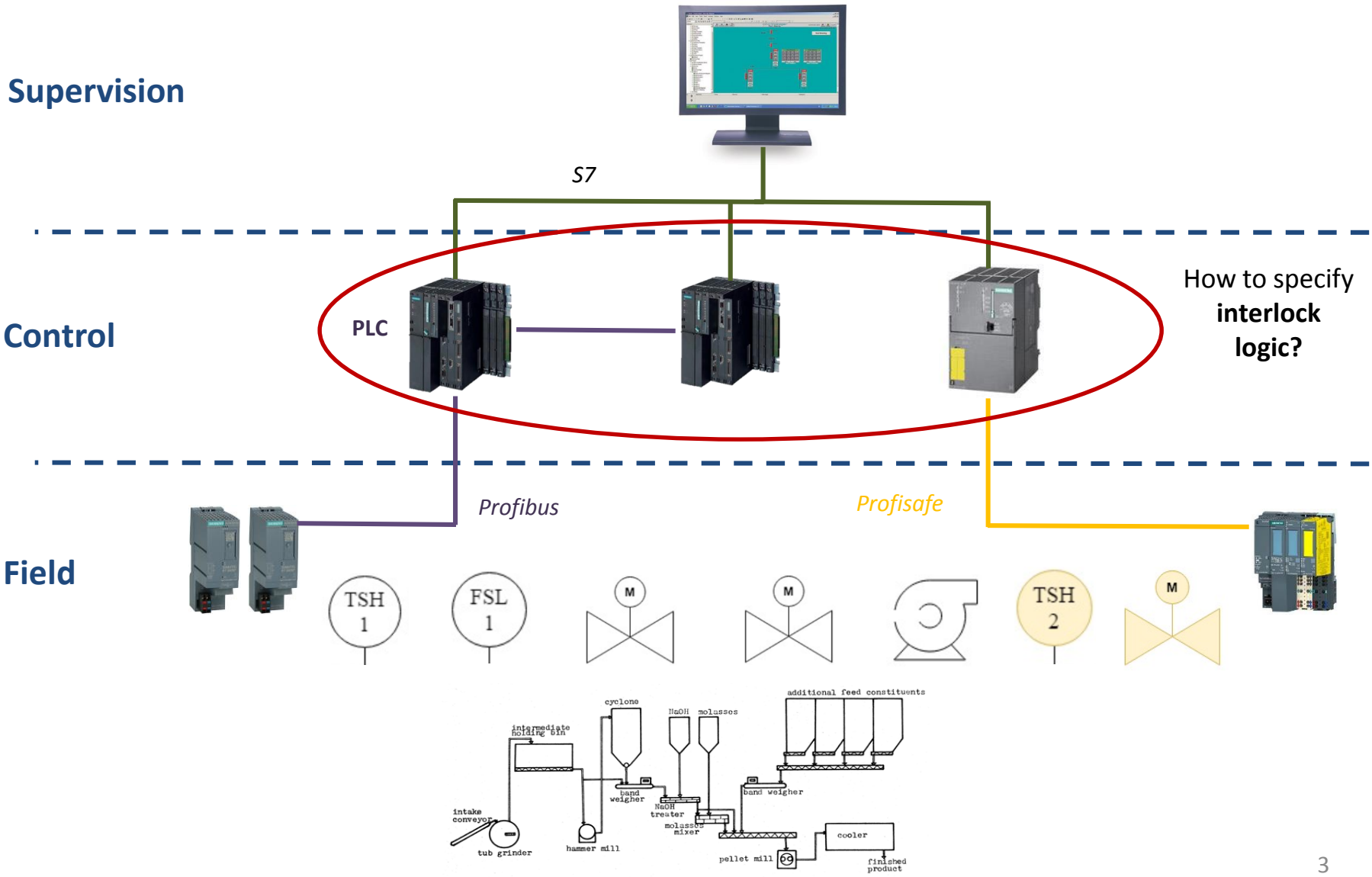
Context

Specifications for interlock logic in

Industrial controls and
Safety Systems

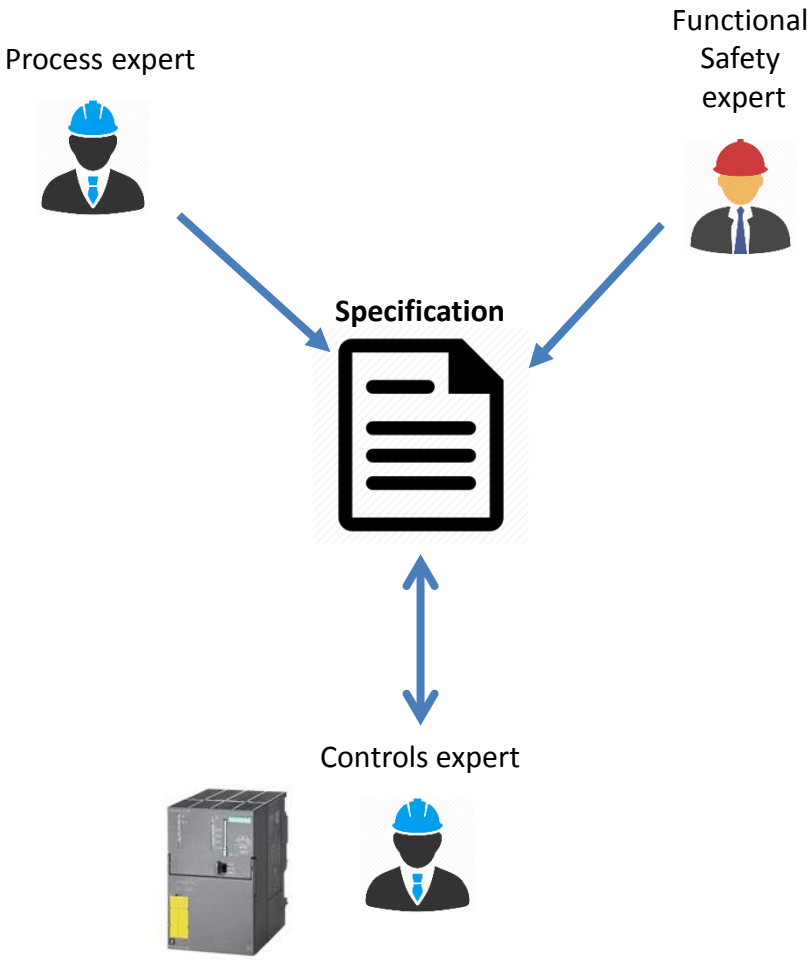
Industrial controls

Safety Systems



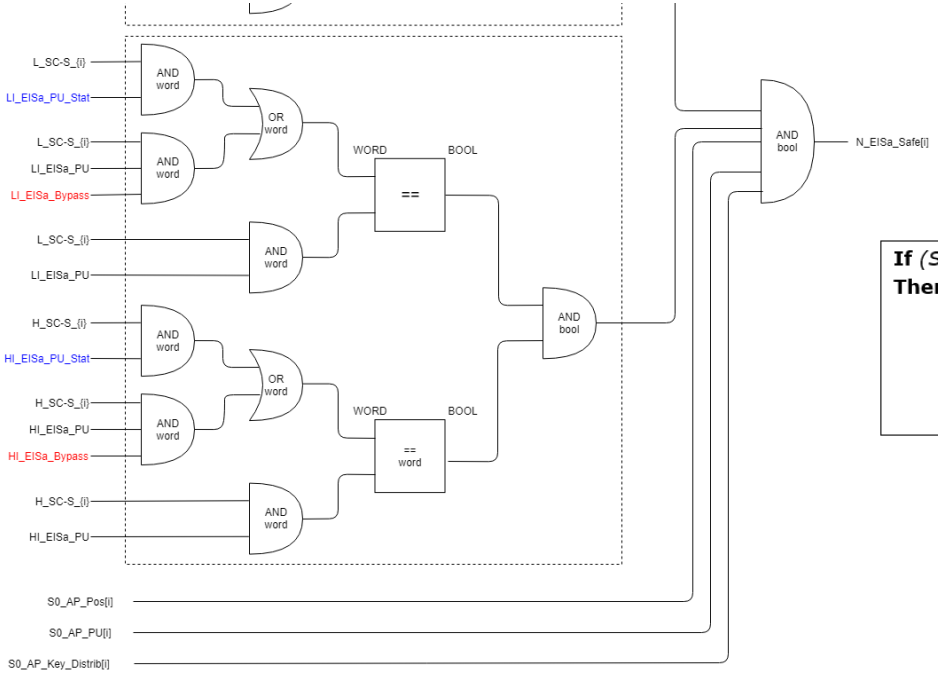
Main problems with specifications

1. **Ambiguous** specification
2. **Incomplete** specification
3. **Complex** specification



Specification options for stateless logic (some examples)

Logic diagram



Boolean expression

If *(SC-S_{i}[n]* **and** *I_EISa_Pos[n])*
Then*:*

N_EISa_Safe_{i}[n] **=** *(I_EISa_Bypass[n]* **or** *I_EISa_Pos_Stat[n])* **and** *(I_EISa_Bypass[n]* **or** *I_EISa_PU_Stat[n])* **and** *S0_AP_Pos[i]* **and** *S0_AP_PU[i]* **and** *S0_AP_Key_Distrib[i]*

Specification options for stateless logic (some examples)

Cause and Effect Matrix

StateOfElementsSC{1}		Description			
		Tag	N_EISa_Safe{1}[1]	N_EISa_Safe{1}[2]	N_EISa_Safe{1}[3]
Description	**Tag**		1	2	3
Assignment of element [n] to safety chain {i}	**SC-S{1}[1]**	1	N,A1,A2,A3,A4		
Installation of door contact [n]	**I_EISa_Pos[1]**	2	A3,A4		
Installation of emergency handle [n]	**I_EISa_PU[1]**	3	A2,A4		
Feedback of door contact [n]	**I_EISa_Pos_Stat[1]**	4	A1,A2		
Feedback of emergency handle [n]	**I_EISa_PU_Stat[1]**	5	A1,A3		
Bypass on element (both door contact and emergency handle) [n]	**I_EISa_Bypass[1]**	6	A2,A3,A4		
Assignment of element [n] to safety chain {i}	**SC-S{1}[2]**	7		N,A1,A2,A3,A4	
Installation of door contact [n]	**I_EISa_Pos[2]**	8		A3,A4	
Installation of emergency handle [n]	**I_EISa_PU[2]**	9		A2,A4	
Feedback of door contact [n]	**I_EISa_Pos_Stat[2]**	10		A1,A2	
Feedback of emergency handle [n]	**I_EISa_PU_Stat[2]**	11		A1,A3	
Bypass on element (both door contact and emergency handle) [n]	**I_EISa_Bypass[2]**	12		A2,A3,A4	
Assignment of element [n] to safety chain {i}	**SC-S{1}[3]**	13			N,A1,A2,A3,A4
Installation of door contact [n]	**I_EISa_Pos[3]**	14			A3,A4
Installation of emergency handle [n]	**I_EISa_PU[3]**	15			A2,A4
Feedback of door contact [n]	**I_EISa_Pos_Stat[3]**	16			A1,A2
Feedback of emergency handle [n]	**I_EISa_PU_Stat[3]**	17			A3,A1
Bypass on element (both door contact and emergency handle) [n]	**I_EISa_Bypass[3]**	18			A2,A3,A4

Outline

- Case Study
- Applicability of CEM
- Conclusions

Case Study – CERN test bench facility

- Test benches for superconducting magnets (**SM18**, FAIR, B311)

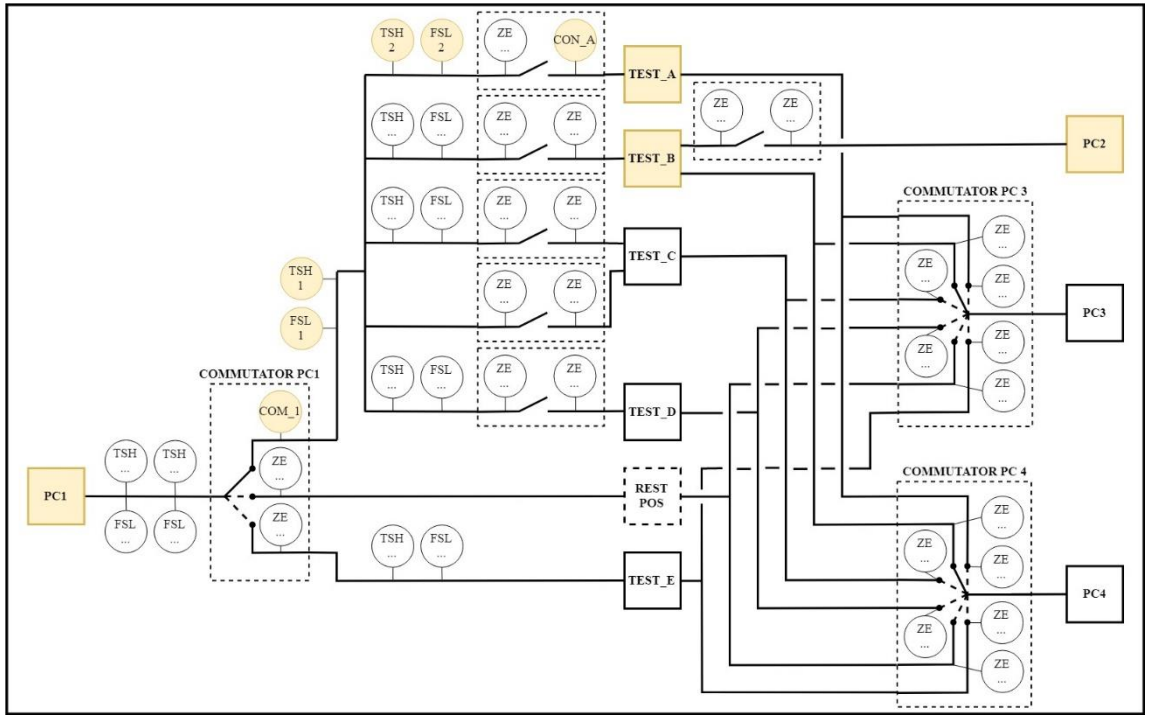
- **Risks** to personnel and equipment
  - Cryogenics
  - Vacuum
  - Power converters
  - Cooling & ventilation

- Need for **Safety Instrumented Systems (IEC 61511 standard)**

- Specification was divided in **Operational requirements** and **Safety requirements**

Case Study – CERN test bench facility

- **5 test benches** and **4 different power converters**
- **42 analogue input signals** (e.g. temperature and voltage sensors)
- **130 digital input signals** (e.g. flow switches, commutators feedbacks)
- **56 output signals** (e.g. digital relays to operate the power converters)



Case Study – Operational specification

Test Types

SCADA Commands

Process Inputs

Process Outputs

TYPE OF TEST TO SELECT

		Signal name	LONGUE	HFM
TEST CONFIG.	Par.	MTBG_Q_TO_CRYO_MIN_CUR_PC20	xxx A	xxx A
		MTBG_Q_TO_CRYO_MIN_CUR_PC10		
		PC selection (PC20, PC10, PC600_1, PC600_2)		
		QH_selection (QH 1- 8)		
		PC10_INV_POL_selection (POLA or POLB)		
		TEST_selection_on _DIODE_STATION (DIODE / LEAD)		
		LEAD3_INSTALLED_on_LONGUE		
		MTBG_QH_MIN_VOLT	xxx V	xxx V
		MTBG_MAGNET_PHASE		
	31	MTBG_TROLLEY_REST_DIODES	if PC = PC20, 1	if PC = PC20, 1
	32	MTBG_TROLLEY_CONN_AUX	if PC = PC20, 0	if PC = PC20, 0
	33	MTBG_TROLLEY_REST_AUX	if PC = PC20, 1	if PC = PC20, 1
	34	MTBG_COM20_CC	if PC = PC20, 0	if PC = PC20, 0
	35	MTBG_COM20_BUSBAR	if PC = PC20, 1	if PC = PC20, 1

TYPE OF TEST TO SELECT

		Signal name	LONGUE	HFM
TEST CONFIG.	Par.	MTBG_Q_TO_CRYO_MIN_CUR_PC20	xxx A	xxx A
		MTBG_Q_TO_CRYO_MIN_CUR_PC10		
		PC selection (PC20, PC10, PC600_1, PC600_2)		
		QH_selection (QH 1- 8)		
		PC10_INV_POL_selection (POLA or POLB)		
		TEST_selection_on _DIODE_STATION (DIODE / LEAD)		
		LEAD3_INSTALLED_on_LONGUE		
		MTBG_QH_MIN_VOLT	xxx V	xxx V
		MTBG_MAGNET_PHASE		
OUTPUT SIGNALS	DIGITAL OUTPUTS 26	MTBG_Q_TO_CRYO_DIODES		
	27	MTBG_Q_T_CRYO_AUX		
	28	MTBG_PC20_CUR_TO_CRYO	MTBG_PC20_CUR	MTBG_PC20_CUR
	29	MTBG_PC10_CUR_TO_CRYO	MTBG_PC10_CUR	MTBG_PC10_CUR
	31	MTBG_PC600_2_CUR_TO_CRYO	MTBG_PC600_2_CUR	MTBG_PC600_2_CUR
	32	MTBG_QH_CONN_CHECK	ACTION TAKEN BY OPERATOR	ACTION TAKEN BY OPERATOR
	33	MTBG_QH_CONN_CHECK_2		
	34	MTBG_CMD_QH_SWITCH_LONGUE	ACTION TAKEN BY OPERATOR executed only if MTBG_V_QH1-16 = 0)	0
	35	MTBG_CMD_QH_SWITCH_HFM	0	ACTION TAKEN BY OPERATOR executed only if MTBG_V_QH1-16 = 0)
	36	MTBG_CMD_QH_SWITCH_DIODES	0	0
	37	MTBG_CMD_QH_SWITCH_AUX	0	0
	38	MTBG_CMD_INV_POLA		if PC = PC10, 1 when POLA selected
	39	MTBG_CMD_INV_POLB		if PC = PC10, 1 when POLB selected
	40	MTBG_PC600_1_PERMIT	if PC = PC600_1, 1 when all input conditions fullfilled	if PC = PC600_1, 1 when all input conditions fullfilled
	41	~~MTBG_PC600_1_DIRECT_PA?~~		
	42	MTBG_PC600_2_PERMIT	if PC = PC600_2, 1 when all input conditions fullfilled	if PC = PC600_2, 1 when all input conditions fullfilled
	43	~~MTBG_PC600_2_DIRECT_PA?~~		
	44	MTBG_PC10_PERMIT		if PC = PC10, 1 when all input conditions fullfilled
	45	MTBG_PC10_DIRECT_PA		
	46	MTBG_PC10_MCB_CMD		if PC =PC10, [pulse of 1s to 0, 100ms after MTBG_NO_Q_DETECT_HFM = 0 ; 1 if MTBG_NO_Q_DETECT_HFM = 1]
	47	MTBG_PLC_EE10_OPEN_RQ		if PC = PC10, [1 if MTBG_PC10_EE_OPEN_RQ = 1]
	48	MTBG_CLOSE_EE10 (500ms positive pulse)		if PC = PC10, ACTION taken by OPERATOR - See graphcet

Case Study – Operational specification

	Condition	Test_A	Test_B
SCADA	SEL_PC	PC1 / PC3 / PC4	PC1 / PC2 / PC3 / PC4
	...	...	...
Process Sensors	CRYO_A	1	
	CRYO_B		1
	DAQ_A	1	
	DAQ_B		1
	...	...	...
Process Actuators	PC1_OPER	if PC1, 1 when all conditions fulfilled	if PC1, 1 when all conditions fulfilled
	PC2_OPER		if PC2, 1 when all conditions fulfilled
	...	...	...

- **Simple** and **convenient** formalism for the process engineer
- but **ambiguous** specification

Case Study – Safety specification

FMEA risk analysis

Repère	Principal équipement en rapport avec le PLC (Inputs / Outputs)	Principaux composants Associés à la fonction	Fonction	Modes de défaillance potentielle	Effets de la défaillance	Causes potentielles	Événements redoutés pour la sécurité des opérateurs	Paramètre Sécurité des personnes				Niveau SIL cible (Sécurité)
								C	F	P	W	
1	WCC	Contrôleur de débit TOR PLC	Détecter un débit d'eau	Indication erronée	Plus de débit d'eau	Contrôleur de débit hors service	Dommages aux équipements : Brûlure des câbles, explosion des flexibles. Eau sur les équipements électriques. Brûlure par contact. Brûlure par projection d'eau chaude. Effet domino : Incendie	1	/	/	3	Pas d'exigence de sécurité particulière
2		Sondes de température PLC	Mesurer la Température de l'eau	Lecture erronée	Pas de refroidissement des câbles Cuivre.	Sondes de température défectueuse		1	/	/	3	SIF1 (SIL1)

Safety Function Specification

Reference	**SIF1_PC10**
Related risk	Risk analysis references 1 and 2
Functionality	Shutdown the PC (10KA) if the corresponding temperature of the cable is high (thermoswitch signal = 0) or the water flow is low (switch signal = 0)
Formalized functionality	**If** (**NOT** MTBG_WCCF_HFM_BIS_P **OR** **NOT** MTBG_WCCF_HFM_BIS_M **OR** **NOT** MTBG_WCCT_PC10_EE10 **OR** **NOT** MTBG_WCCT_EE10_INV **OR** **NOT** MTBG_WCCT_INV_HFM) **Then** (MTBG_PC10_PERMIT_Q = FALSE)
Safety level	SIL1
Safety mode	Low demand

- **Unambiguous** specification
- But **no tool support:**
  - **Test cases** generation
  - **Verification cases** generation
  - **Code** generation

Cause and Effect Matrix (CEM)

- A compact and intuitive **graphical** representation of **Boolean expressions**
- Adequate to **represent stateless logic**, where a given output depends only on a combination of the current input signals
- There are **many variants of CEMs** and the companies adopt the **semantics that best adapt to their processes and engineering practices**
  - SIMATIC Safety Matrix (Siemens Product)
  - IEC 62881:2018. Cause and effect matrix

Cause and Effect Matrix (CEM)

$$\begin{bmatrix} Q01 \\ Q02 \end{bmatrix} = \begin{bmatrix} I01 \vee TON(I02, 20s) \vee (\neg I03 \wedge I04) \\ I02 \wedge (I03 \vee \neg I04) \end{bmatrix}$$

Cause \ Effect	Q01	Q02
I01	X	
I02	TON20	A1,A2
I03	NA1	A1
I04	A1	NA2

Cause and Effect Matrix (CEM)

	Condition	Test_A	Test_B
SCADA	SEL_PC	PC1 / PC3 / PC4	PC1 / PC2 / PC3 / PC4
	...	...	...
Process Sensor	CRYO_A	1	
	CRYO_B		1
	DAQ_A	1	
	DAQ_B		1
	...	...	...
Process	PC1_OPER	if PC1, 1 when all conditions fulfilled	if PC1, 1 when all conditions fulfilled
	PC2_OPER		if PC2, 1 when all conditions fulfilled
	...	...	...

Reference	**SIF1**
Related risk	Risk analysis reference 1
Functionality	Shutdown the power converter if the corresponding temperature of the water-cooled cable is high (*FALSE*) or the water flow is low (*FALSE*)
Formalized functionality	*If* $(COM\_1 \wedge CON\_A \wedge (\neg TSH1 \vee \neg TSH2 \vee \neg FSL1 \vee \neg FSL2))$ *Then* $PC1\_PP = 0$
Safety Level	SIL2
Operation mode	Low demand

Variable discretization

(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	
...		...

Cause and Effect Matrix (CEM)

(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

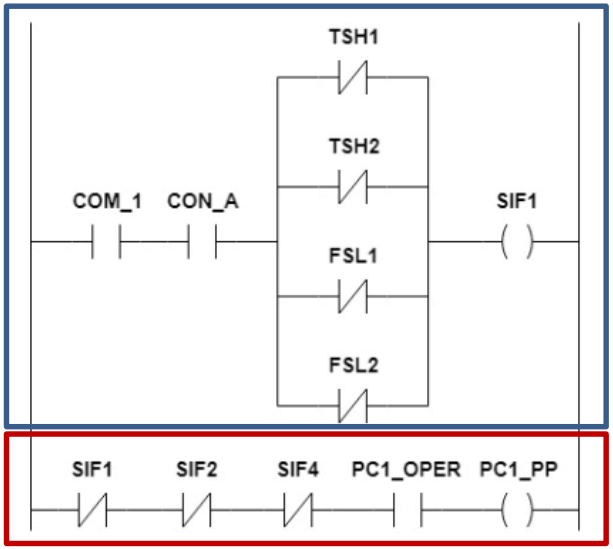
Cause \ Effect	PC1_PP	PC2_PP
SIF1	NA1	
SIF2	NA1	
SIF3		NA1
SIF4	NA1	NA1
PC1_OPER	A1	
PC2_OPER		A1

(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

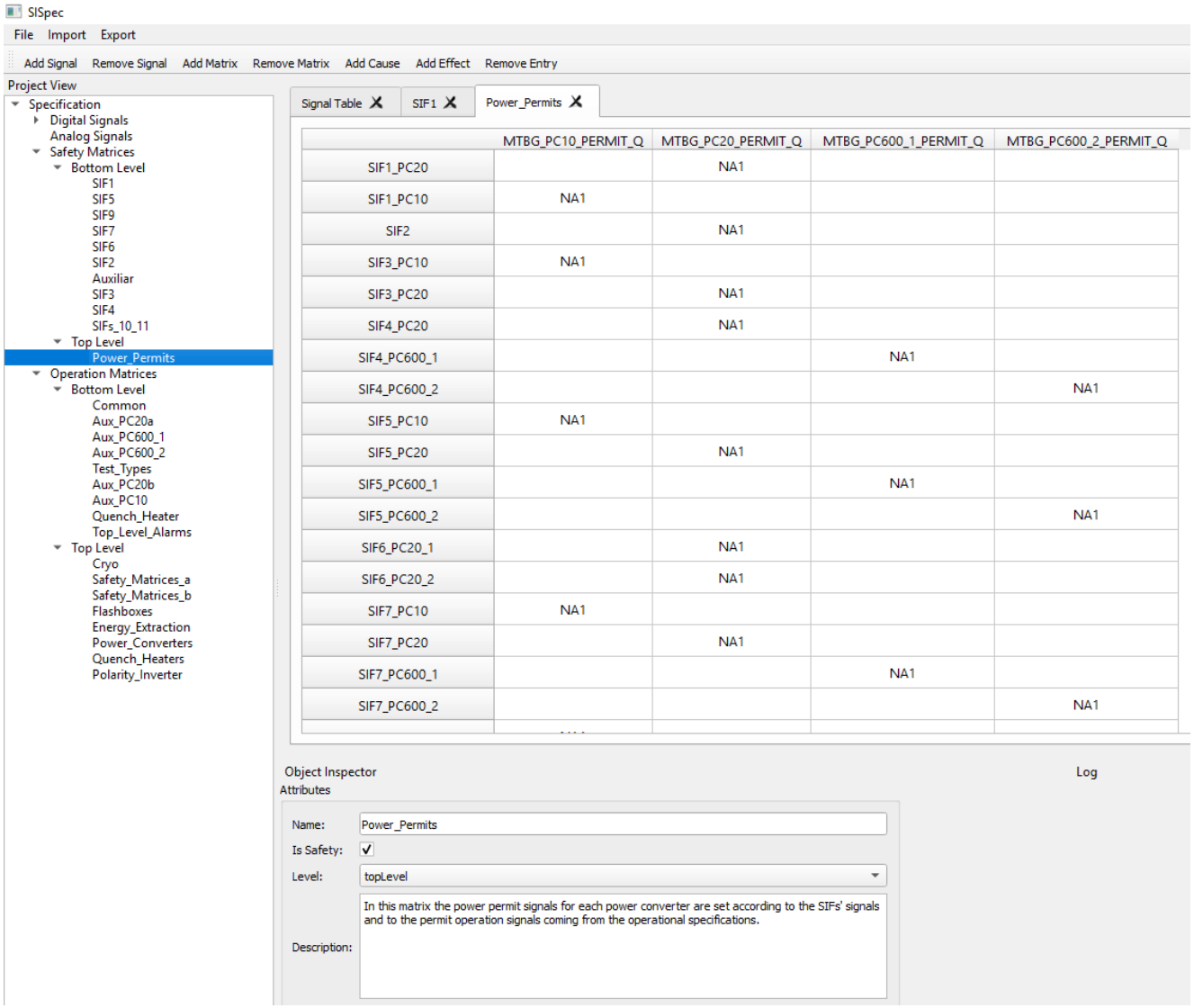
(d) Bottom Safety CEM

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



- **Code** generation (when possible)
- **Test** case generation
- **Verification** cases generation

SISpec: CEM Editor



Conclusions

CEM pros	CEM cons	Future directions
• **Simple** and **graphical** mechanism • Allows a **better communication** between control, process and safety experts • **Trivial** generation of the **PLC code** • Allows **automatic generation of test and verification** cases • Improved **maintainability** of the PLC code and **traceability** of the whole project	• **Not appropriate** for **all types of processes.** Mainly convenient for stateless interlock logic • Certain Boolean logic may be difficult to express in one single CEM (auxiliary CEMs may have to be Included)	• Extension of the **CEM semantics** to different activation logics (rising edges, pulses, etc.) • **PLC code generation and integration** in the development cycle of SISs and interlock-based control systems