CAUSE-AND-EFFECT MATRIX SPECIFICATIONS FOR SAFETY CRITICAL SYSTEMS AT CERN

B. Fernández, E. Blanco, M. Charrondiere, O. Ditsch, R. Speroni CERN, Geneva, Switzerland
H. Hamisch, M. Bonet, M. H. de Queiroz, Universidade Federal de Santa Catarina, Florianópolis, Brazil

MOPHA041

Motivation

- Provide a **simple**, **unambiguous** and **compact specification** method to express interlock logic
- Potential use cases:
  - **Safety Instrumented Systems** (SIS)
  - Any **interlock system** with **stateless logic**

How?

Cause and Effect Matrix (CEM)
a compact and intuitive **graphical** representation of **Boolean expressions**

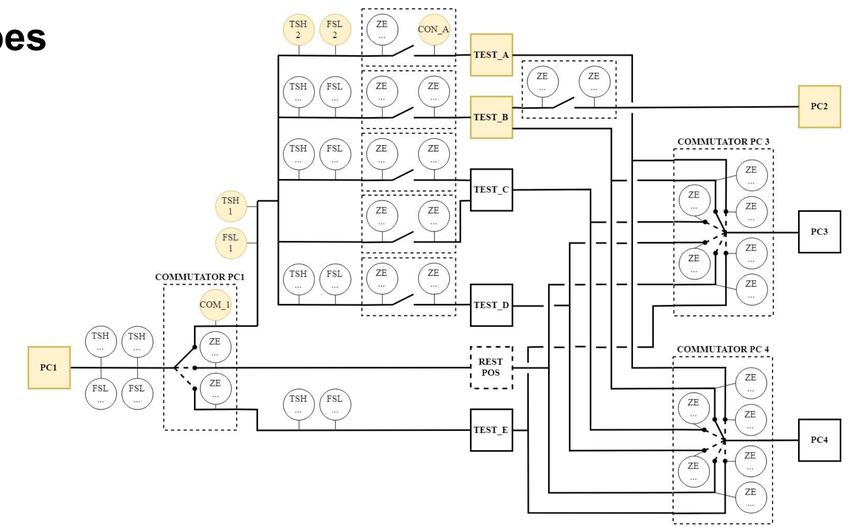
$$\begin{bmatrix} Q01 \\ Q02 \end{bmatrix} = \begin{bmatrix} I01 \vee TON(I02, 20s) \vee (\neg I03 \wedge I04) \\ I02 \wedge (I03 \vee \neg I04) \end{bmatrix}$$

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

Case Study – A CERN magnet test bench facility

Facility to **test new magnet prototypes**

Process description



- 5 test benches and 4 different power converters
- **Several hazards** of electrical and cryogenic nature
- Specification divided in **Operational requirements** and **Safety requirements**

Operational requirements

Simple but ambiguous specification

	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
	...	...	...

Safety requirements

Unambiguous but no tool support

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

New CEM-based specification

(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

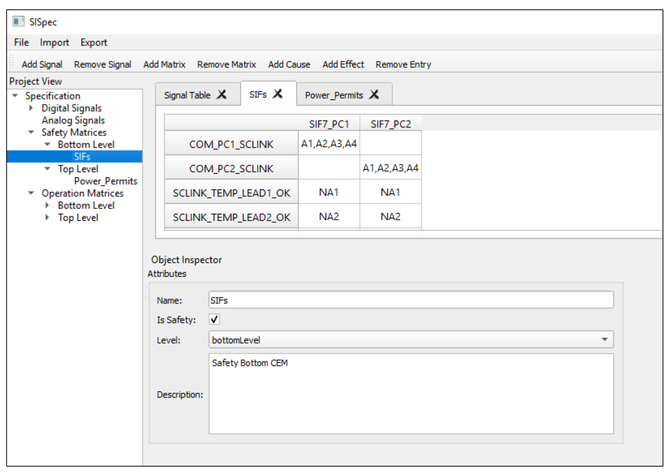
Cause \ Effect	TEST_A	TEST_B
SEL_TEST_A	A1	
SEL_TEST_B		A1
CRYO_A	A1	
CRYO_B		A1
DAQ_A	A1	
DAQ_B		A1

(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	
...	...	...

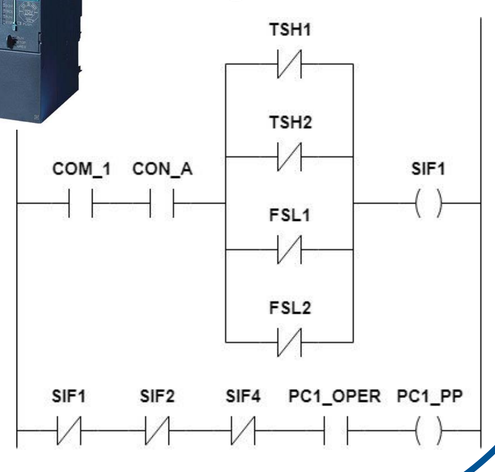
SISpec tool

Graphical editor for CEMs and **test and verification cases generation**



PLC program

implementation out of the CEMs is **straightforward**



Conclusions and future

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

CERN Beams Department
Industrial Controls and Safety Systems Group (ICS)

ICALEPCS 2019