ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-MOPHA041

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

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

Abstract

One of the most critical phases in the development of a Safety Instrumented System (SIS) is the functional specification of the Safety Instrumented Functions (SIFs). This step is carried out by a multidisciplinary team of process, controls and safety experts. This functional specification must be simple, unambiguous and compact to allow capturing the requirements from the risk analysis, and facilitating the design, implementation and verification of the SIFs. The Cause and Effect Matrix (CEM) formalism provides a visual representation of Boolean expressions. This makes it adequate to specify stateless logic, such as the safety interlock logic of a SIS. At CERN, a methodology based on the CEM has been applied to the development of a SIS for a magnet test bench facility. This paper shows the applicability of this methodology in a real magnet test bench and presents its impact in the different phases of the IEC 61511 safety lifecycle.

INTRODUCTION

The European Organization for Nuclear Research (CERN) operates the largest particle physics laboratory in the world. This research laboratory hosts many critical industrial installations that are necessary for the numerous experiments performed here. Some examples are cryogenics plants, cooling and ventilation processes, powering systems, superconducting magnet test benches and many more. A failure in these industrial installations or in their control systems may have catastrophic consequences, such as enormous economic losses, environmental damages or even human causalities. For that purpose, at CERN, many Safety Instrumented Systems (SISs) have been engineered to mitigate the risks of these industrial processes.

Safety Instrumented Systems

A SIS is a prevention mechanism designed to reduce the probability of occurrence of hazardous events. The IEC 61511 standard [1] provides the so-called safety life cycle, which provides guidelines to develop, maintain and manage a SIS for the process industry. Once the unacceptable risks are identified by the risk analysis, the process and safety experts must specify the necessary Safety Instrumented Functions (SIFs) to reduce the probability of occurrence of these risks. A SIF specification must contain at least the following elements:

- The functionality of the SIF: a precise description of the required SIF logic.
- The target Safety Integrity Level (SIL): a quantitative measure of the risk reduction.
- The operation mode required for the SIF: low, high or continuous demand, depending on the nature of the process and risk.

Nowadays, Safety PLCs (Programmable Logic Controllers) are widely used in SISs and the functionality of the SIFs is implemented in the PLC programs.

The specification method to express the functionality of a SIF must be simple, unambiguous and compact to allow capturing the requirements from the risk analysis, and facilitate the design and implementation of the PLC program. There are many specification methods to express unambiguously the functionality of a SIF, for example, a textual boolean expression, a logic diagram or a Cause and Effect Matrix (CEM).

Objectives

This paper presents a real case study at CERN of the usage of a CEM-based specification to express the interlock logic of a magnet test bench installation. The benefits and limitations of this approach in comparison with the previously adopted methods are also summarized.

The paper is structured as follows: first, the paper introduces the basic concepts and adopted CEM semantics for this project. Second, the case study is described, including the process description and an example of the CEM usage. Finally, the analysis and conclusions of this study are presented.

CAUSE AND EFFECT MATRIX

Cause and Effect Matrix is a compact and intuitive graphical representation of boolean expressions. This makes it adequate to represent stateless logic, where a given output depends only on a combination of the current input signals. CEM is generally well accepted to specify interlock logic in the process and manufacturing industries. However there are many variants of CEMs and the companies adopt the semantics that best adapt to their processes and engineering practices. Some PLC providers have included the CEM in their engineering tools. This is the case of Siemens Industrial Automation, which provides the SIMATIC Safety Matrix [2]. This tool allows the use of CEM as a specification mechanism but imposes a specific software architecture,

[*] borja.fernandez.adiego@cern.ch

their own engineering tools, SCADA (Supervisory Control And Data Acquisition), etc. The International Electrotechnic Commission published in 2018 the IEC 62881 standard [3], describing a widely accepted semantics of a CEM.

In this project, the CEM has been applied to specify the interlock logic of a magnet test bench installation. The CEM semantics have been defined by adapting the specific standards adopted by the oil and gas industry [4] to the engineering practices of CERN.

Semantics

The matrix consists of rows of signals (the causes) and columns of signals (the effects), as seen in Table 1. The intersection (cell) between a cause and an effect denotes how the cause influences the effect, according to the following basic rules:

- X: the cause, when active, triggers the effect (OR logic);
- N: the cause, when inactive, triggers the effect (OR NOT logic);
- (N)Ai: the effect is triggered when all the causes with the Ai entry (where i = 1, 2, ...) are simultaneously active, or inactive if the prefix N is present (AND logic);
- TONx: the cause, if active for more than x seconds, triggers effect (IEC 61131-3 [5] TON logic);
- TOFx: the cause, when active, triggers the effect and the effect remains active for x seconds after the cause becomes inactive (IEC 61131-3 [5] TOF logic);
- Multiple entries in a single column, or separated by "," in a single cell, are combined with OR logic;
- The same effect may appear in multiple matrices, the resulting expression for this effect is an OR logic between the activations of each matrix.

Table 1 illustrates an example of a couple of timed boolean expressions (1) in this CEM notation.

$$\begin{bmatrix} Q01 \\ Q02 \end{bmatrix} = \begin{bmatrix} I01 \lor TON(I02, 20s) \lor (\neg I03 \land I04) \\ I02 \land (I03 \lor \neg I04) \end{bmatrix} \tag{1}$$

Table 1: CEM Example

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

To support the described semantics and apply them to real cases, a Python-based prototype tool has been developed at CERN: *SISpec*. The tool provides a user-friendly graphical interface to build the CEMs and provides syntax and semantic validation to avoid specification errors. In addition, the CEM can be exported to different formats (e.g. *xlsx* files for visualization with Microsoft Excel) and test and verification cases can be automatically generated.

CASE STUDY

This section presents a CERN case study of the applicability of the CEM formalism to specify the functional logic of a SIS and of an interlock-based control system.

Process Description

The selected process is the so-called *ClusterG* magnet test bench. This facility is mainly designed to test the superconducting magnet prototypes for the High Luminosity LHC project [6], protection diodes, current leads and high temperature superconducting (HTS) future generation magnets. *ClusterG* consists of five test benches, where magnets under test are installed, and four different power converters, providing the required current to the benches. Moreover, four mechanical commutators connect the power converters and the benches. To optimize the operation time of the facility, two benches can be powered at the same time.

The process instrumentation consists of: (1) forty-two analogue input signals, mainly analogue sensors such as the current lead temperatures and voltages; (2) one hundred and thirty digital input signals, including digital sensors such as temperature and flow switches of the water cooled cables, the commutators feedbacks, a few signals indicating the data acquisition and cryogenic statuses, etc.; (3) fifty-six output signals, consisting in digital relays to operate the quench protection matrix, the power converters, etc.

A simplified schema of the process is shown in Figure 1. The highlighted elements (e.g. TSH1, FSL1) are used later in the paper to present the specification examples.

The process experts provided the specification to develop the control system to operate this facility. In addition, a risk analysis based on the Failure Mode and Effect Analysis (FMEA) of the process was performed and several hazards of electrical and cryogenic nature to the workers and the installation itself were detected. As a consequence a SIS was designed to mitigate these risks, following the IEC 61511 directives.

Operational Requirements

The operational requirements for this installation were expressed in a formalism designed by the process experts, based on a table where the logic to operate the test bench was included. The logic of the table connects the SCADA commands, the test types to be performed (one per test bench), the input signals (sensors) and the output signals (actuators).

In the simplified example shown in Table 2, for the *Test_A*, the operator selects the power converter to be used in this test (e.g. *PC1*), and the control system checks the correct status of the process inputs for the specific test, in this case *CRYO_A* and *DAQ_A* (statuses of the cryogenics and data acquisition systems). If the conditions are met for the specific test, the control system gives the authorisation to the power

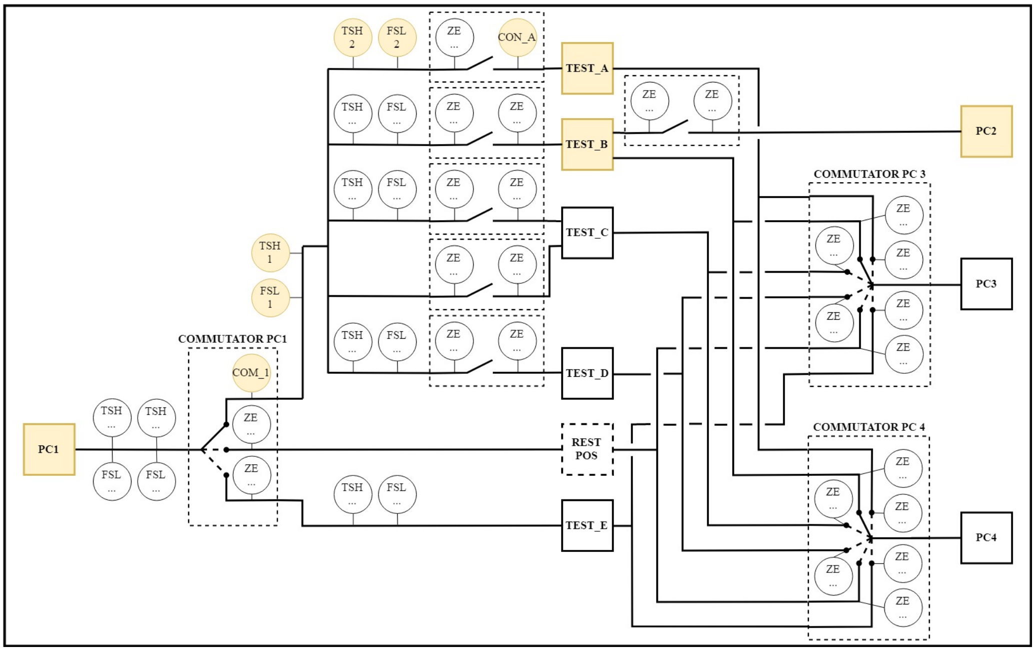

Figure 1: Simplified *ClusterG* process schema.

converters to power the test bench. The real specification table for this project has around two hundred and fifty rows and eight columns.

In the cells of this table, selectors (e.g. *PC1*), boolean values (e.g. 1), empty cells and plain text (e.g. "if PC1, 1 when all conditions fulfilled") are mixed to express the desired logic. However while this table is convenient for the process experts, it is an ambiguous requirements description and makes the translation to PLC code open to interpretation and error prone. Moreover, the lack of formal semantics makes impossible the generation of test or verification cases.

Safety Requirements

The outcome of the risk assessment was the specification of 28 SIFs to be included in a SIS. Table 3 shows a simplified example of a particular SIF (SIF1), where a reference to the risk analysis, the functionality and its formalization, the associated target SIL and the operation mode (low, high or continuous demand) are included.

This specification is unambiguous but written in a Microsoft Word document, which prevents the automatic generation of test and verification cases. In addition, when the number of variables to be included in the boolean formula is significant, or when the logic is complex with many parenthesis and boolean operators, a textual representation may be very complex and it might be difficult to detect human mistakes during the specification.

New CEM-based Specification

The ambiguity of the operational requirements and the lack of tools and proper visualization for the safety requirements were the main motivation to analyse the potential benefits that the CEM could bring to this project.

However, just by using the CEM method, the specification of the project would still be rather complex. The significant number of sensors, actuators and test types obliged us to split the specification into several CEMs. Otherwise the result would have been a CEM with hundreds of causes and dozens of effects.

The strategy adopted to express the operational and safety specification is presented in Table 4. It separates the operational and safety requirements and each of them is divided in two levels, top and bottom, in order to split the specification in smaller and simpler units, as follows:

- The bottom operational CEMs have process sensors and SCADA commands (inputs) as causes and test types (operational functions) as effects;
- The top operational CEMs have test types (operational functions) and SCADA commands (inputs) as causes and actuators as effects.
- The bottom safety CEMs have safety sensors (safety inputs) as causes and SIFs as effects;
- The top safety CEMs have SIFs as causes and safety actuators as effects.

The Tables 5a, 5b, 5c and 5d show the previously presented specifications expressed in the CEMs. The *SEL_PC* variable is discretized in several Boolean variables for the Top Operational CEM (only two of them are shown in Tables 5a). The effects of the bottom CEMs are the causes of the top CEMs. Finally, if an actuator is common for the operational and the safety requirements, e.g. *PC1*, the effect of the Top Operational CEM is a cause in the Top Safety CEM (see *PC1_OPER* and *PC1_PP* in Tables 5a and 5b).

Table 2: Simplified Example of the Operational Requirements

	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
	...	...	...

Table 3: Simplified SIF Specification

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

Table 4: Selected Strategy to Split the CEM Specification

Top Operational CEMs Effects: actuators Causes: *operational functions*	**Top Safety CEMs** Effects: safety actuators Causes: *SIFs*
Bottom Operational CEMs Effects: *operational functions* Causes: inputs	**Bottom Safety CEMs** Effects: *SIFs* Causes: safety inputs

PLC Program Implementation

Both the operational and safety requirements have been implemented in a S7-317F Siemens Safety PLC. The operational requirements have been implemented using the UNICOS framework [7] and the safety requirements using the Distributed Safety Library [8] and the LADDER programming language. Figure 2 shows a part of the PLC program corresponding to the Tables 5b and 5d, containing the logic for the *SIF1* and the logic for the actuator, the power permit of the power converter 1 (*PC1_PP*). As it can be observed, the implementation of the PLC program out of the CEMs is straightforward and a well-defined program architecture is established.

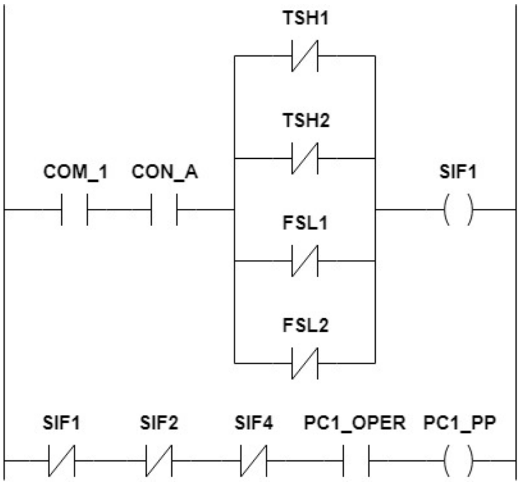

Figure 2: LADDER PLC program example.

Verification and Test Case Generation

CEM facilitates the verification and testing activities against the PLC programs thanks to its formalized semantics. In this project, both verification and test cases were automatically generated by the *SISpec* tool from the CEMs. The verification cases were executed by the PLCverif tool [9] (PLC formal verification tool developed at CERN) and the test cases were generated based on the algorithms presented in [4] and executed in a test platform.

ANALYSIS

This section presents the benefits and limitations of the usage of CEM to the *ClusterG* project. Regarding the benefits and improvements we can emphasize the following ones:

- CEM provides a fairly simple and graphical mechanism for the process and safety experts to express the desired logic;
- The unambiguous specification simplifies the communication between the control, process and safety experts;
- The translation of CEM logic to the PLC program is trivial and automatic code generation is possible;

Table 5: Simplified Example of the CEM Usage for the *ClusterG* Project

(a) Top Operational CEM

Effect Cause	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

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

(c) Bottom Operational CEM

Effect Cause	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

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

- The automatic generation of test and verification cases is possible and particularly important when code generation is not an option, for example in the case of Siemens safety PLC programs;
- The presented specification strategy and the usage of CEM improved significantly the maintainability of the project by having a well-defined program architecture and the traceability between the PLC program, the CEM specification and the risk assessment.

There are certain limitations or drawbacks of this method:

- CEM is not appropriate to all types of processes. While CEM is convenient for stateless interlock logic, other methods should be applied for different processes;
- Certain boolean logic may be difficult to express in one single CEM and thus auxiliary CEMs may have to be included. This was the case of the SIF2 for *ClusterG*.

CONCLUSIONS

This paper presents a CERN case study of the usage of a CEM-based specification for the interlock logic of a control system and a SIS. The paper analyses this new approach by presenting the main benefits and limitations in comparison with the previous specification methods.

The results are positive, especially in terms of removing the ambiguity of previous specification methods and adding capabilities such test and verification cases generation. The future of this project will be focussed in two directions. First, the extension of the semantics to different activation logics that are common in our systems, for example rising edges, pulses, etc. Second, the improvement of our CEM tool, *SISpec*, in terms of usability, new features such as code generation and integration in the development cycle of interlock-based control systems and SISs.

REFERENCES

[1] IEC 61511:2018, *Functional safety - Safety instrumented systems for the process industry sector*.

[2] *SIMATIC Safety Matrix, Siemens Industrial Automation. Product ID: 6ES7833-1SM03-0YA5*.

[3] IEC 62881:2018, *Cause and effect matrix*.

[4] *Veiga, H. W.; de Queiroz, M. H.; Farines, J.-M.; de Lima, M. L.*, "Automatic conformance testing of safety instrumented systems for offshore oil platforms", in Proc. 17th Int. FMICS-AVoCS'17 Workshop, Turin, Italy, September 2017, pp 51-65, doi:10.1007/978-3-319-67113-0_4

[5] IEC 61131-3:2013, *Programmable controllers - Part 3: Programming languages*.

[6] High Luminosity LHC Project, https://hilumilhc.web.cern.ch

[7] About UNICOS (UNified Industrial Control System), http://www.cern.ch/unicos

[8] *Distributed Safety Library, Siemens Industrial Automation. Product ID: 6AU1837-0EA10-0DX1*.

[9] *D. Darvas and E. Blanco*, "PLCverif Re-engineered: An Open Platform for the Formal Analysis of PLC Programs", presented at ICALEPCS'19, New York, USA, October 2019, paper MOBPP01, this conference.