

# SISpec - A Tool for Safety Requirements

## Summer student 2024 report

Dhruv Tyagi

Supervisor: Andrea Germinario, Alexandros Foivos Kostopoulos

August 26, 2024



### **Abstract**

At CERN, ensuring proper safety measures is a critical prerequisite for any project. To achieve high safety standards in PLC programs, defining clear safety requirements is essential. To assist with this, a tool called *SISpec* is being developed. *SISpec* enables system and control engineers to define safety requirements using method called Cause Effect Matrices (CEM) and a User friendly GUI. Although still in the development phase, the tool has already been used to define software specification for the PLC programs deployed in some experiments, where it has proven to be highly useful. In this report, I present the work I completed as a Summer Student in 2024 to enhance *SISpec*. My contributions have focused on improving user experience, refining functionalities, and establishing robust pipelines, all of which have advanced the tool from its development phase to its first release.

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Background Work</b>	<b>2</b>
<b>3</b>	<b>Contributions</b>	<b>3</b>
3.1	Methodology . . . . .	3
3.2	Core Functionalities . . . . .	3
3.2.1	File Exporting and Saving Issues . . . . .	3
3.2.2	PLC Verif . . . . .	4
3.2.3	UAB Spec Generation . . . . .	4
3.3	Testing and Maintenance . . . . .	4
3.3.1	Basic Tests . . . . .	4
3.3.2	Unit Tests for GUI Testing . . . . .	4
3.3.3	Running Local Tests on Pipeline . . . . .	5
3.4	User Experience . . . . .	5
3.4.1	Popups . . . . .	5
3.4.2	Signal Table and Project Tree . . . . .	6
3.4.3	Object Inspector . . . . .	6
3.4.4	Miscellaneous . . . . .	6
<b>4</b>	<b>Conclusion</b>	<b>7</b>

## 1 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. BE-ICS Department focuses on delivering technical solutions, engineering expertise, and development for industrial controls throughout the CERN complex. This group is tasked with recommending, acquiring, and supporting key industrial control technologies used across both accelerators and experiments. They develop and maintain a range of control systems, including process control, interlocks, and supervisory systems, catering to various applications such as Detector Control Systems, Electrical Distribution, and Machine Protection. BE-ICS is the department responsible for the development of *SISpec*, a tool that helps the engineers to define specification in a standard way to generate artifacts and code for industrial control.

## 2 Background Work

The Cause and Effect Matrix (CEM) [1] is a compact and intuitive graphical representation of Boolean expressions, designed to clearly illustrate the relationships between causes and effects within a system. This method is particularly effective for representing stateless logic, where outputs are determined solely by the current combination of input signals. CEM-based specifications are commonly used for defining the interlock logic of control systems and Safety Instrumented Systems (SIS). To facilitate the specification of interlock logics using CEMs, CERN developed a prototype application called *SISpec*. This tool helps minimize specification errors by incorporating syntax and specification checks. Once a CEM is finalized and validated within *SISpec*, it can be exported in XML format. The CEMs generated by *SISpec* offer a detailed and unambiguous blueprint of the software to be developed, enabling generation of multiple artifacts such as: PLCverif verification cases[2], UAB specification templates[3] and the Ladder code that respects the given specification. Additionally, *SISpec* provides

a graphical interface that significantly reduces both the time required and the likelihood of errors, while ensuring compliance with the IEC 61508 Standard.

## 3 Contributions

Despite the fact that the tool was still in development phase, BE-ICS experts were using it on a regular basis to design control systems at CERN. My role as a summer student was to remove the obstacles that stood between the current status of the tool and its first release. The work done focused on addressing client requirements and , removing the bugs that made the system user unfriendly and making the software more maintainable for future developers. The contributions made can be categorized into three main areas:

- Core Functionalities
- Testing and Maintenance
- User Experience

### 3.1 Methodology

For working effectively, we structured the work in the following manner:

- Associated a Jira ticket to every bug to solve/new feature to implement.
- Planned the weekly tasks to be performed using a Kanban Board.
- Created a dedicated branch on project's gitlab for each separate ticket.
- Before merging the code to the main branch, it was reviewed by at least one reviewer.

### 3.2 Core Functionalities

The contributions related to the core functionalities, which are crucial for developing accurate specifications, are discussed below:

#### 3.2.1 File Exporting and Saving Issues

- **SISPEC-2**

**Title:** Removing a signal from Signal List makes impossible to Save.

**Description:** Fixed the code to make sure that all signals are removed from all the intermediate lists and matrices.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-2>

- **SISPEC-26**

**Title:** Open file in SISpec makes it crash sometimes.

**Description:** Fixed the issue of opening error due to None Type converting to string instead of object.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-26>

### 3.2.2 PLC Verif

- **SISPEC-58**

**Title:** Update 'Export Effect Activation'.

**Description:** Changed how PLCverif assertions are created. Produce 1 vc3 file per matrix and 2 txt file with assertions, one for safety matrices and one for non-safety matrices.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-58>

- **SISPEC-59**

**Title:** Inserted 'code tag' instead of 'name' when exporting effect activation.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-59>

### 3.2.3 UAB Spec Generation

- **SISPEC-56**

**Title:** Not able to generate UAB Spec

**Description:** Resolved the issue of repeating columns by using standard start\_table and start\_data variable values provided by Uabpyxl.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-56>

## 3.3 Testing and Maintenance

### 3.3.1 Basic Tests

- **SISPEC-33**

**Title:** Design one (or more) automatic test that performs all the basic functionalities.

**Description:** Wrote the test that can do all the basic functionalities required by the *SISpec*.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-33>

- **SISPEC-29**

**Title:** Stop ignoring "test\_spec\_to\_uab.py"

**Description:** Fixed and rewrote the complete test.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-29>

### 3.3.2 Unit Tests for GUI Testing

- **SISPEC-36**

**Title:** Unit Test: Add Signal.

**Link to Jira Issue** <https://its.cern.ch/jira/browse/SISPEC-36>:

- **SISPEC-37**

**Title:** Unit Test: Remove Signal.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-37>

- **SISPEC-38**

**Title:** Unit Test: Add Matrix.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-38>

- **SISPEC-39**

**Title:** Unit Test: Remove Matrix.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-39>

- **SISPEC-40**

**Title:** Unit Test: Add Cause.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-40>

- **SISPEC-41**

**Title:** Unit Test: Add Effect.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-41>

- **SISPEC-42**

**Title:** Unit Test: Remove Entry.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-42>

### 3.3.3 Running Local Tests on Pipeline

- **SISPEC-44**

**Title:** Instantiate a SISpec application in pipeline.

**Description:** Changed the execution of tests to make sure that all the tests can be executed in a single go on pipeline. Made sure that only one instance is being present at a single time. Further added the support for uabpyxl dependency on pipeline.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-44>

## 3.4 User Experience

### 3.4.1 Popups

- **SISPEC-23**

**Title:** Throw a pop-up window when an error is thrown in SISpec.

**Description:** The pop-up window is thrown with the most common errors (like: "Non-existing signal type" or "Already used name") and exceptions.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-23>

- **SISPEC-18**

**Title:** Open a pop-up windows when creating a new Matrix.

**Description:** Created a pop-up panel where the user can insert the info about the matrix. The pop-up will check the data, ask user confirm and create the matrix.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-18>

- **SISPEC-16**

**Title:** Open a pop-up windows when inserting a new signal.

**Description:** Created a pop-up that asks the user the info for the new signal, checks these info, and creates the signal only when the user confirms.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-16>

### 3.4.2 Signal Table and Project Tree

- **SISPEC-15**

**Title:** Make the signal table available from the Project View menu.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-15>

- **SISPEC-31**

**Title:** When adding new signal, the Signal Table does not update.

**Description:** Fixed the code to make sure that the signal Table gets updates after adding new signal even after it is closed and re-opened.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-31>

- **SISPEC-55**

**Title:** Open Signal Table when double-clicking on a Signal in Project Tree.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-55>

- **SISPEC-27**

**Title:** Make Signal Table entries Cascade Buttons.

**Description:** Added cascade drop down menus for all the parameters in signal table.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-27>

- **SISPEC-63**

**Title:** Improve switching tab experience.

**Description:** Added the functionality to select the signal table when clicked on add signal from task bar or signal from the project view.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-63>

### 3.4.3 Object Inspector

- **SISPEC-19**

**Title:** Fix the 'isSafety' checkbox in the object inspector.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-19>

- **SISPEC-43**

**Title:** Object Inspector does not get updated after the component is deleted.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-43>

### 3.4.4 Miscellaneous

- **SISPEC-53**

**Title:** Log the successful operations

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-53>

- **SISPEC-60**

**Title:** Enforce group number with 'AND' logic.

**Description:** Made system to enforce the user to generate atleast one group of 'AND' logic in

the cells. with group 'None'.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-60>

- **SISPEC-62**

**Title:** Improve 'add\_signal' experience.

**Description:** Assigned a custom standard name to the newly added signal: "new\_signal\_\*" where \* is an increasing integer starting from 1. Apart from that added focus/opening of signal table whenever a new signal is added.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-62>

- **SISPEC-54**

**Title:** Update Project Tree when Digital Signal turns Analogue.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-54>

- **SISPEC-24**

**Title:** Make top Buttons be task specific.

**Description:** Just displayed the button in task menu that are relevant to the window that the user have opened currently.

**Link to Jira Issue:** <https://its.cern.ch/jira/browse/SISPEC-24>

## 4 Conclusion

This report highlights the various contributions made to improve the *SISpec*. The improvements primarily focused on enhancing functionalities, user experience, and maintenance. The work mentioned above turned *SISpec* from a tool that only experts can use, still in development to a released product ready for unexperienced users. We successfully released a stable version of *SISpec* : **SISpec v1.0.0** which is available on Gitlab.

The tool will be soon added to AccPy to make it available CERN-wide and will be presented to other sections which have shown interests in it in the past. While the tool is now suitable for client use, further work is needed to optimize it.

## References

- [1] B. Fernández, E. Blanco, M. Charrondiere, R. Speroni, CERN, H. Hamisch, M. Bonet, M. H. de Queiroz, and B. Universidade Federal de Santa Catarina, Florianópolis, "17th int. conf. on acc. and large exp. physics control systems," *CAUSE-AND-EFFECT MATRIX SPECIFICATIONS FOR SAFETY CRITICAL SYSTEMS AT CERN*, 2019.
- [2] B. Viñuela, E. (CERN), Darvas, D. (CERN), Molnár, and T. U. Vince (Budapest, "Pleiverif re-engineered: An open platform for the formal analysis of plc programs," *17th Biennial International Conference on Accelerator and Large Experimental Physics Control Systems (ICALEPCS), New York, United States, 5 - 11 Oct 2019, pp.21*, 2019.
- [3] B. C. Fernandez Adiego and I. C. Blanco Vinuela, E (CERN) aznd Prieto Barreiro, "Unicos cpc6: Automated code generation for process control applications," *Conf. Proc. C111010 (2011) pp.WEPKS033*, 2011.