ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-MOPHA078

RENOVATION OF THE SPS PERSONNEL PROTECTION SYSTEM: A CONFIGURABLE APPROACH

T. Ladzinski, B. Fernandez Adiego, F. Havart, CERN, Geneva, Switzerland

Abstract

The renovation of the SPS Personnel Protection System (PPS) comprises the installation of industrial access control solutions and the implementation of a new safety instrumented system tailored to the particular needs of the accelerator. The SPS has been a working horse of the CERN accelerator complex for several decades and its configuration has changed through the many years of operation. The classic solutions for safety systems design, used in the LHC and PS machines, have not been judged adequate for this accelerator undergoing perpetual changes, composed of many sites forming several safety chains. In order to avoid expensive software modifications, each time the accelerator configuration evolves, a configurable safety software design was proposed. This paper presents the hardware architecture of the PLC-based SPS PPS and the configurable software architecture proposed. It further reports on the testing and formal verification activities performed to validate the safety software and discusses the pros and cons of the configurable approach.

INTRODUCTION

The Super Proton Synchrotron (SPS), CERN's second largest accelerator, was put in service in 1976. Its access control and safety interlock system, also known as the Personnel Protection System was upgraded in the beginning of the nineties. However, after nearly three decades of use, it has reached its end of life, with further upgrades no longer possible due to lack of spare-parts and more severe safety constraints.

During the ongoing Long Shutdown (2019-2020) of the CERN accelerator complex the SPS PPS is being fully replaced. This major project will complete the renovation process of the Personnel Protection Systems, providing the same level of safety across the CERN accelerator complex. In the design of the system, feedback from the implementation and operation of personnel protection systems of the Large Hadron Collider (LHC) [1] and Proton Synchrotron (PS) [2] has been taken into account. At the same time, as a new industrial partner was chosen for the implementation, certain parts of the design have been completely reviewed and new solutions proposed. In particular, it was considered that the very rigid implementation of the LHC PPS resulted in high total cost of ownership of the system. The accelerator evolves with time as new access zones are added or existing ones modified. Each zone is a development apart, albeit sharing the same library of components, and implementation of a new site or simply an addition or removal of one door has proven very expensive in the past, especially in terms of testing and validation. In order to improve the situation for the SPS PPS, it was proposed to design a configurable system, expanding the concepts already introduced in the past for the protection of personnel in the secondary beam line experimental areas at CERN [3].

SPS INTERLOCKED ZONES

The SPS accelerator is a circular machine housed in a 7 km long tunnel 60 m under the ground. In addition to the main ring tunnel, the SPS complex includes the transfer tunnels linking the ring with the PS and the LHC machines as well as several experimental areas. The SPS is currently used to deliver beams to the LHC and to three experimental regions: the North Area, as well as the HiRadMat and the AWAKE [4] facilities. In the past the SPS was used as a collider with clockwise and counter clockwise beams circulating in opposing directions.

Access from the outside to the SPS zones is strictly controlled and is only possible using dedicated access points. Once the current project is completed, they will be composed of a Personnel Access Device (PAD) [5] and a Material Access Device (MAD). Sixteen access points are present in the SPS, each leading to an access zone. Access control is managed at access zone level, with authorisations delivered to adequately trained personnel performing approved works in a given access zone.

Several access zones which are always interlocked with the same elements inhibiting operation with beam form a safety chain. In every safety chain there are at least three important safety elements capable of stopping the beam. In general two are of magnetic type and one is a beam line obstructer. Figure 1 represents graphically the relationship between the safety chains (also referred to as "interlocked zones") of the SPS complex.

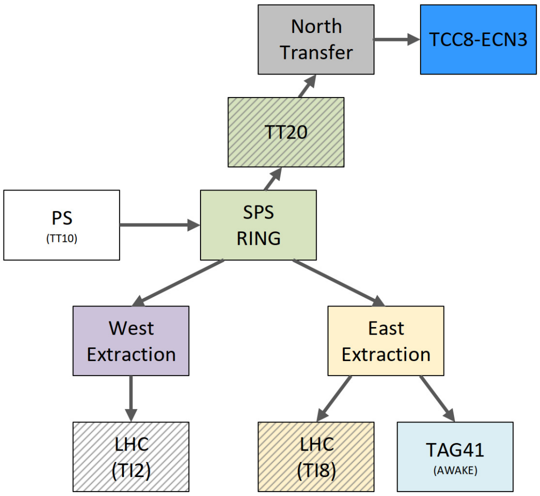


Figure 1: SPS Safety Chains with arrows representing proton beam direction.

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-MOPHA078

FROM SECTORISATION TO IMPLEMENTATION MODEL

The details of each access zone are recorded in the so-called *sectorisation* drawings, where each access point, door, patrol checkpoint etc. is shown on simplified plans of the facility. These drawings are similar to process instrumentation diagrams and are a basis for a detailed design of the personnel protection system as well as an important source of information for operators and equipment groups preparing maintenance and upgrades. Figure 2 shows an example drawing for two of the SPS access zones. Each access zone is divided into several sectors. The subdivision of access zones into sectors has been introduced in order to facilitate patrolling of the facility. Prior to any beam operation the access zones are patrolled for absence of people. By dividing the zones into smaller segments, this procedure is easier to organise. In case of an intrusion, only the concerned sectors need to be patrolled, thus reducing accelerator downtime.

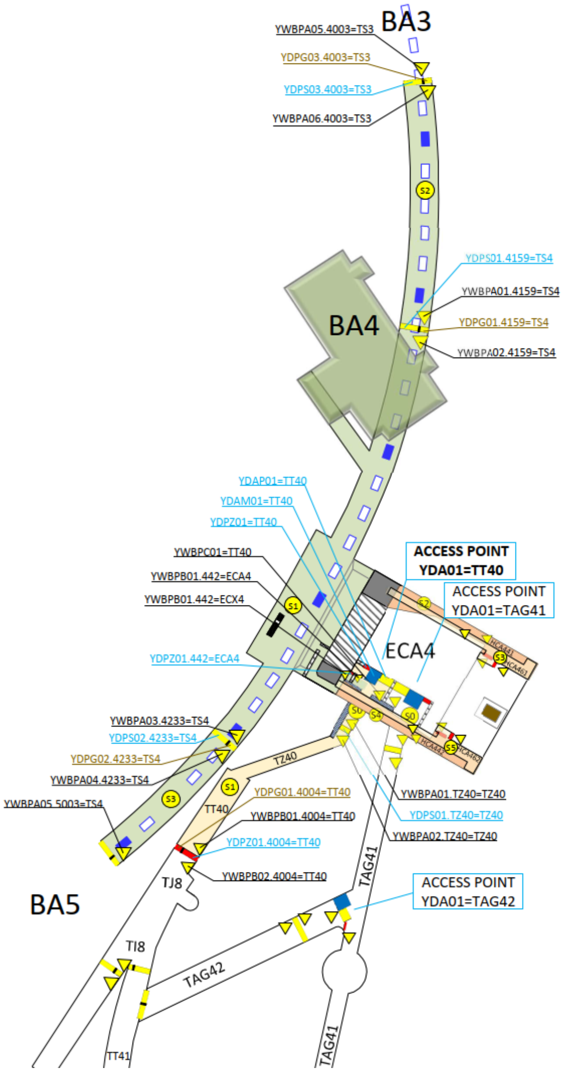


Figure 2: Sectorisation document – BA4 access zone is represented in green, while light orange colour is used for TT40 access zone.

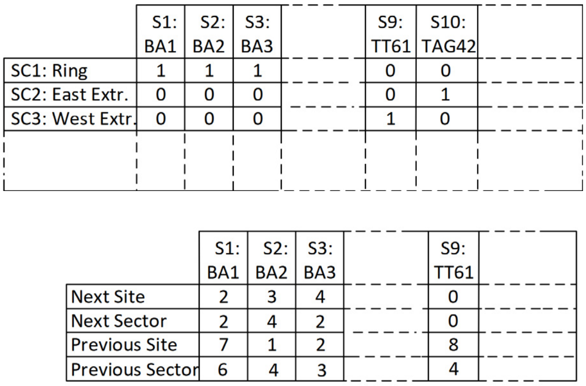
In the traditional approach to safety system design the sectorisation drawings have served as a basis for electrical single line diagrams and in parallel for the implementation of the access zone PLC code. In a configurable approach, a generic access zone code has to be designed and implemented. This code is then instantiated for each access zone controller. The geographical and logical relationships of the different components of each access zone are represented in the form of configuration tables and the complete PPS is also represented as a matrix of interlocked zones composed of one or more access zones (also referred to as sites). Given the history of the evolutions of the SPS machine, the maximum possible size of the installation was set, as described in Table 1.

Table 1: Dimensioning the SPS PPS

Item	Maximum Config.	Current Config.
safety chains (including extraction chains)	16	6 (9)
access zones (sites)	32	16
access points per site	1	1
access elements per site	32	3-25
beam elements per chain	16	3
sectors per site	16	2-12

Several tables have been introduced to store the configuration of the SPS PPS, either at central or at site level.

Safety chains table holds information about the configuration of each chain in terms of sites composing it. Each row represents a safety chain and the columns the sites. The inter-site relationship table holds information about adjacent sectors belonging to different sites. Figure 3 graphically represents these tables, which are stored centrally.



	S1: BA1	S2: BA2	S3: BA3		S9: TT61	S10: TAG42	
SC1: Ring	1	1	1		0	0	
SC2: East Extr.	0	0	0		0	1	
SC3: West Extr.	0	0	0		1	0	

	S1: BA1	S2: BA2	S3: BA3		S9: TT61	
Next Site	2	3	4		0	
Next Sector	2	4	2		0	
Previous Site	7	1	2		8	
Previous Sector	6	4	3		4	

Figure 3: Global configuration tables.

Each site controller holds information about the different access safety elements constituting the site. Information is stored in several tables, where a row indicates an access element and the tables describe if it contains position contacts, emergency passage, a controllable lock etc. In addition, configuration tables describe the sectors structure in each access zone, indicate which access elements belong to which sector and which patrol checkboxes are associated to which access element.

The core of the safety program is then developed using interlock matrices, where a status matrix is calculated locally in each site controller and is permanently fed to the central (or global) interlock controller which evaluates if a safety action (veto) should be applied to the elements of a given site (see Fig. 4).

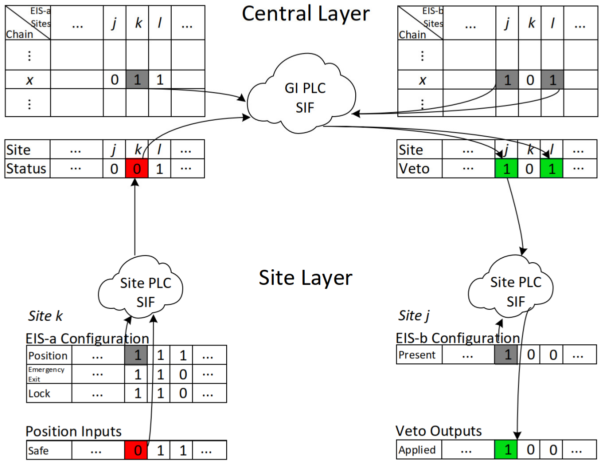

EIS-a Sites / Chain | ... | j | k | l | ...
⋮
x | | 0 | 1 | 1 |
⋮
Central Layer
GI PLC SIF
EIS-b Sites / Chain | ... | j | k | l | ...
⋮
x | | 1 | 0 | 1 |
⋮
Site | ... | j | k | l | ...
Status | ... | 0 | 0 | 1 | ...
Site | ... | j | k | l | ...
Veto | ... | 1 | 0 | 1 | ...
Site Layer
Site PLC SIF
Site k
EIS-a Configuration
Position | ... | 1 | 1 | 1 | ...
Emergency Exit | ... | 1 | 1 | 0 | ...
Lock | ... | 1 | 1 | 0 | ...
Position Inputs
Safe | ... | 0 | 1 | 1 | ...
Site PLC SIF
Site j
EIS-b Configuration
Present | ... | 1 | 0 | 0 | ...
Veto Outputs
Applied | ... | 1 | 0 | 0 | ...

Figure 4: Interlock matrices principle.

SYSTEM HARDWARE ARCHITECTURE

The SPS PPS safety-interlock part is based on Siemens F1500 series of PLC controllers. It is composed of the Global Interlock (GI) controller forming the Central Layer and sixteen Site controllers at the Site Layer. In addition, at the Equipment Layer, each PAD is equipped with a Siemens F Open Controller. The later one is composed of a safety part (monitoring of door and token distributor contacts) and non-safety part (interfaces with: access control database, biometry iris recognition system, dosimeter check etc.) [5]. The GI and Site controllers are linked together by a ring type dedicated fiber network using Ethernet Profisafe protocol. Figure 5 shows a vertical slice of the PLC architecture with only one of the sixteen sites represented.

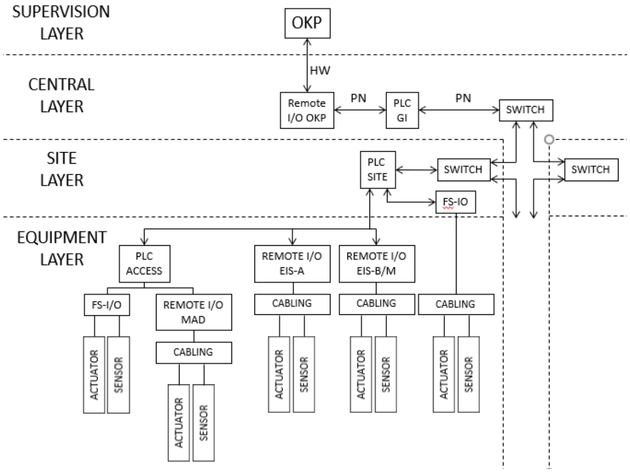
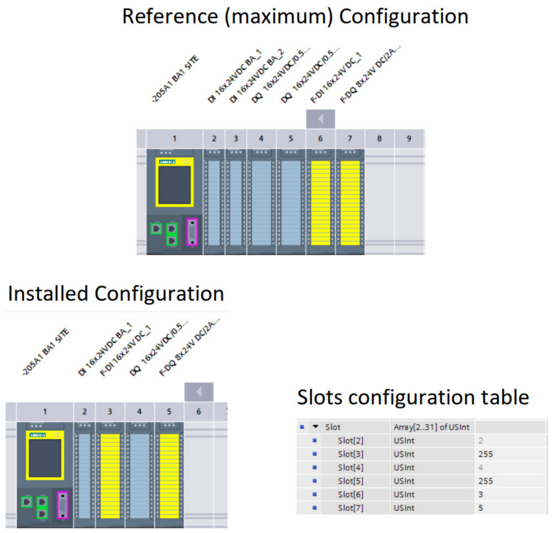


Figure 5: Safety PLC architecture overview.

The hardware configuration of each site controller is set to the maximum possible site size (compare Table 1). However, having sixteen identical site racks was not a feasible option. The SPS sites differ a lot in actual size, the equipment is expensive and cubicle space limited. This problem was overcome using the Siemens *Configuration Control Option Handling* mechanism. Option handling allows to have a maximum reference configuration which is then reduced to the actual one installed by deactivating unused interface modules by editing a database entry. Figure 6 represents option handling example.



Slot	Array[2..31] of USInt	
Slot[2]	USInt	2
Slot[3]	USInt	255
Slot[4]	USInt	4
Slot[5]	USInt	255
Slot[6]	USInt	3
Slot[7]	USInt	5

Figure 6: Hardware configuration option handling.

SAFETY FUNCTIONS SPECIFICATION

Safety functions have been traditionally specified in terms of concise natural language statements (e.g. *When an emergency exit is used, apply veto to the beam elements.*). The initial SPS PPS safety functions specification was prepared using simple *if-else* conditional statements that contain Boolean expressions to remove the natural language ambiguity and describe the system in an easily implementable manner. It was based on a methodology introduced for the PS personnel protection system specification [6].

In the configurable approach used in the SPS, the actual implementation differs significantly from the initial specification as the system configuration has to be taken into account. Thus, the specification describing the pure functionality should be considered together with the configuration tables to understand the PLC program implementation. For this reason, implementation of the safety functions in the PLC program contains many extra input variables, corresponding to configuration variables (e.g. indicating how many access doors are installed in an access zone). The input variables of a safety function are no longer Boolean variables representing for example the state of a particular sensor, but rather 16-bit Word variables, where individual bits have to be checked using a mask from the configuration table.

As a consequence of the configurable software design, the testing activities become very complex since the number of combinations to check for the system is very high. An example PLC program, which implements only one safety function specified with a few conditional statements and Boolean formulas has 115 Word input variables. Testing exhaustively all the combinations is practically impossible (around 10^{553} combinations to check) and a different approach is needed.

VERIFICATION & VALIDATION

The verification and validation of the SPS PPS follows a rigorous approach with multiple stages of tests and procedural verifications, involving several independent teams.

Software verification activities of the SPS PPS focus on two principal axes: verification of the functions manipulating the configuration tables and verification of the actual safety functions. This approach helps limit the number of test combinations. In each case, truth tables are used to check the correctness of the output variables of individual functions against possible combinations of input variables.

The combined software is then validated in a test platform environment. The SPS PPS test platform is composed of a Global Interlock PLC, a Site PLC and a complete access point including its PLC. The test platform is representative of the site installation in terms of controller architecture (compare Fig. 5). However, it uses Siemens SIMIT modules for I/O simulation [7]. For the already installed sites manual tests were conducted for all the safety relevant cases, observing the state of the outputs, the HMI and the state of internal variables, where appropriate. The test platform has not only proven useful to perform the tests of the safety program but also to check the ergonomics and the correct implementation of the human machine interfaces prior to real life operation of the system. Only software validated in the test platform was deployed on site, this way the site commissioning could focus on the correct functioning of the site installation, not on debugging the software.

In addition, formal verification techniques to check that the PLC program fulfils the specification have been considered for the SPS PPS safety software. In particular, *model checking* was used. The PLCverif tool [8], developed at CERN, can automatically generate the formal models out of the PLC programs, create the temporal logic formula out of a given specification and invoke external model checkers to perform model checking. The complexity of applying model checking is hidden from the user of the tool, who only has to provide the PLC program and the specification to be checked. The most common limitation of model checking is the state space explosion when the number of combinations to be checked is too big. The first trials with PLCverif and the SPS PPS PLC programs have shown promising results. So far, only one formal model of the safety functions had a state space that could not be verified by the model checkers integrated in the tool. PLCverif has allowed spotting a few potential problems in the PLC software implementation such as use of undocumented bypass flags or an unknown operation mode that could result from a double sensor error in the operator key panel.

Further work to increase the coverage of the previous testing activities is being conducted. This autumn the test platform will be equipped with two additional site controllers and two access point controllers emulating PAD and MAD devices. This will allow to test three access zones simultaneously and verify the correct functioning of safety chains composed of multiple sites. In addition, automatized tests that can perform the verification of the combined software (i.e. configuration management functions and safety functions) are being investigated. Since automatic testing can be performed at any time on the test platform, this could increase the test coverage by performing more exhaustive tests and be used to verify the complete implementation as well as future upgrades.

COMMISSIONING OBSERVATIONS

The validated software has already been deployed in eight freshly installed access points and two access zones. The TAG41 access zone, housing the AWAKE facility, is a location where R&D activities continue despite the accelerator shutdown. In order to meet the research schedule milestones, the new system had to be commissioned in advance of the rest of the SPS.

The commissioning started with systematic electrical continuity tests of the field instrumentation. Using the Siemens *Configuration Control Option Handling* made these tests more challenging than in classical installations. A very small error in the option handling configuration can easily be misinterpreted as a systematic error in cabling or instrumentation.

A feature of the configurable approach, resulting from the introduced complexity is the abandoning of the commonly used input/output names which usually are derived from single line diagram equipment codes. Therefore, one cannot quickly identify which physical object a given variable corresponds to and needs to consult a translation table.

In the long term perspective the advantages of having both hardware and software developed in a way that is easily expandable and independent of instrumentation naming convention is definitely beneficial, but the additional effort with system commissioning should not be underestimated.

CHANGE MANAGEMENT

For each site controller the safety software is composed of core safety blocks (FB, FC) and of configuration data blocks (DB). The safety blocks form the reference program, which is identical in all the site controllers; its version can easily be traced with a safety signature. Software for each controller is instantiated with the site configuration information in the data blocks. A change request may be of configuration or functional nature. In the first case, only the corresponding data block needs to be modified. In the second case, no data blocks are modified, only the reference program.

For the most recurrent modification, which concerns change in the size of an installation (e.g. addition of a new door), the validation can be limited to a sensor-actuator on-site test. This will ensure that the change in the configuration corresponds to the actual change in the field elements and is anyway a mandatory step in case of any safety installation modification. Simple comparison of safety signature ensures that the modification is only limited to configuration and the reference program remains unchanged. Therefore intermediate testing phases do not need to be repeated, provided the reference program has been fully tested and validated before.

In case of changes not related to configuration, but to functionality, the configurable approach can also be beneficial. Although the modification is usually more complex to specify and to test, it only needs to be tested in the reference program once and then instantiated with the already used configuration DB in each site controller. This general schema requires that all the site controllers have the same program loaded, hence any modification of the reference program requires uploading it in all the site controllers, which may at times be problematic due to operational constraints. However, one must not forget that the common program is used in all the site controllers; if a functional modification is required, it is required everywhere and should be deployed everywhere.

Site specific software blocks, that is software blocks implemented only for a particular site (e.g. to protect from Laser related hazard present in the AWAKE experiment), are not part of the configurable approach. Their modification is not related to the reference program and has to be treated on a case by case basis. It is worth noting that so far site specific functions only had to be implemented in one out of the sixteen site controllers.

The SPS PPS is instantiated with the current field configuration, hence configuration changes such as addition of a new door or area are not expected in the immediate future, but the software is ready to accept them. Most user feedback obtained so far, concerned the implementation of the access point software, which may require implementation changes. Although not directly part of site configuration management, the fact that the software was designed to pass only resultant status between different layers of controllers facilitates testing and deployment of the access point software upgrades.

CONCLUSIONS

A configurable approach for the design of a large safety interlock system has been proposed and is being implemented for the SPS Personnel Protection System. It has been successfully deployed on the first sites of the SPS, including the TAG41 access zone housing the AWAKE experiment. In addition to complex patrol management common to all the sites, the AWAKE specific safety functions (Laser and Electron Gun interlocks) have been fully validated and work is on-going to thoroughly test the system and validate it for the protection of personnel against hazards from proton beams. This is done in parallel to the site installation works scheduled to last till summer 2020. More testing efforts and more challenging commissioning resulting from added software complexity require additional resources during the project phase, but simplify the operation and maintenance activities. The system's design should allow much easier integration of future changes in the SPS, such as addition of new elements or of a new interlocked area, as well as faster validation of upgrades.

ACKNOWLEDGEMENTS

The authors are greatly indebted to J. Ortiz, lead developer at Procon Systems and his colleagues for many fruitful discussions and the implementation of the system. The authors would also like to express their thanks to the past and present colleagues from the SPS Personnel Protection System project team for their contributions, especially to F. Valentini for the initial safety functions specification and E. Sanchez for driving the test platform verification efforts.

REFERENCES

[1] T. Ladzinski *et al.,* "The LHC access system", in *Proc. ICALEPCS'09*, Kobe, Japan, Oct 2009, paper WEP102, pp. 600-602.

[2] P. Ninin *et al.,* "Refurbishing of the CERN PS complex personnel protection system", in *Proc. ICALEPCS'13*, San Francisco, USA, Oct. 2013, paper MOPPC059, pp. 234-237.

[3] F. Havart, R. Nunes, D. Chapuis, D. Vaxelaire, "Achieving a highly configurable personnel protection system for experimental areas", in *Proc. ICALEPCS'13*, San Francisco, USA, Oct. 2013, paper MOPPC061, pp. 238-241.

[4] AWAKE, `http://awake.web.cern.ch`

[5] T. Ladzinski *et al.,* "New concepts for access devices in the SPS personnel protection system", in *Proc. ICALEPCS'17*, Barcelona, Spain, Oct. 2017, pp. 1608-1612. `doi:10.18429/JACoW-ICALEPCS2017-THPHA099`

[6] F. Valentini, T. Hakulinen, L. Hammouti, T. Ladzinski, P. Ninin, "Formal methodology for safety-critical systems engineering at CERN", in *Proc. ICALEPCS'13*, San Francisco, USA, Oct. 2013, paper TUCOCA04, pp. 918-921.

[7] Siemens SIMIT Simulation, `https://new.siemens.com/global/en/products/automation/industry-software/simit.html`

[8] D. Darvas, B. Fernandez, E. Blanco, "PLCverif: a tool to verify PLC programs based on model checking techniques", in *Proc. ICALEPCS'15*, Melbourne, Australia, Oct. 2015, paper WEPGF092, pp. 911-914.